universität wien

MASTER THESIS

Titel der Master Thesis / Title of the Master‘s Thesis

„Schutz Kritischer Infrastrukturen
durch die NIS-Gesetzgebung
–
Bedeutung für den Wiener Gesundheitssektor“

verfasst von / submitted by

Mag. Matthias Ponweiser, BSc

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Science (MSc)

Wien, 2022 / Vienna 2022

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	UA 992 242
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Risikoprävention und Katastrophenmanagement
Betreut von / Supervisor:	Dipl.-Ing. Dr. Stefan Schauer

I. Eidesstattliche Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und ohne unerlaubte fremde Hilfe angefertigt, keine anderen als die angegebenen Quellen und Hilfsmittel verwendet und die den verwendeten Quellen und Hilfsmitteln wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

…… ……

(Datum) (Unterschrift)

Matthias Ponweiser

II. Inhaltsverzeichnis

III. Abbildungs- und Tabellenverzeichnis

IV. Abkürzungsverzeichnis

AKH Wien	Allgemeines Krankenhaus der Stadt Wien
AMPDS	Advanced Priority Dispatch System (Standardisiertes Notrufabfragesystem)
APCIP	Austrian Program for Critical Infrastructure Protection (Österreichisches Programm zum Schutz Kritischer Infrastrukturen)
APCIPL	APCIP-Länder
APG	Austrian Power Grid
APT	Advanced Persistent Threats (fortgeschrittene anhaltende Bedrohungen)
Art.	Artikel
BABS	Bundesanstalt für Bevölkerungsschutz (Schweiz)
BfV	Bundesamt für Verfassungsschutz (Deutschland)
BKA	Bundeskanzleramt (Österreich)
BMASGK	Bundesministerium für Arbeit, Soziales, Gesundheit und Konsumentenschutz (Österreich)
BMdI	Bundesministerium des Inneren (Deutschland)
BMEIA	Bundesministerium für Europa, Integration und Äußeres (Österreich)
BMI	Bundesministerium für Inneres (Österreich)
BMLV	Bundesministerium für Landesverteidigung (Österreich)
BRH	Bundesrechnungshof (Österreich)
BSI	Bundesamt für Sicherheit in der Informationstechnik (Deutschland)
B-VG	Bundes-Verfassungsgesetz der Republik Österreich
BVT	Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (Österreich)

BwD	Betreiber wesentlicher Dienste
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer (Informationssicherheitsmanager*in)
DDoS	Distributed Denial of Service (verteilte Dienstverweigerung)
DSN	Direktion für Staatsschutz und Nachrichtendienste (Österreich)
EKI	Europäische Kritische Infrastrukturen
EPCIP	European Program for Critical Infrastructure Protection (Europäisches Programm zum Schutz Kritischer Infrastruktur)
EU	Europäische Union
GPS	Global Positioning System
IIoT	Industrual Internet of Things
IKDOK	Innerer Kreis der operativen Koordinierungsstruktur (Österreich)
IKT	Informations- und Kommunikationstechnologie
ISMS	Informationssicherheitsmanagementsystem
ISPK	Institut für Sicherheitspolitik an der Universität Kiel
KAKuG	Krankenanstalten und Kuranstaltengesetz
KRITIS	Kritische Infrastruktur
LVT	Landesamt für Verfassungsschutz und Terrorismusbekämpfung (Österreich)
MA 70	Magistratsabteilung 70 – Berufsrettung Wien
MilKdoW	Militärkommando Wien
NIS	Netz- und Informationssystemsicherheit
NÖZSV	Niederösterreichischer Zivilschutzverband
ORKB	Oberste Rechnungskontrollbehörde der Europäischen Union

OSCE	Organisation for Security and Cooperation in Europe
ÖSCS	Österreichische Strategie Cybersicherheit
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
PDD	Presidential Decision Directive (Präsidiale Entscheidungsrichtlinie)
QuaSte	Qualifizierte Stelle
RKE	Richtlinie über die Widerstandsfähigkeit Kritischer Einrichtungen
RL	Richtlinie
RTR	Rundfunk und Telekom Regulierungs-GmbH
SKI	Schutz Kritischer Infrastrukturen
SPOC	Single Point of Contact
StGB	Strafgesetzbuch
StRH	Stadtrechnungshof
TKG	Telekommunikationsgesetz
WIGEV	Wienergesundheitsverbund
WRKG	Wiener Rettungs- und Krankentransportgesetz
Z	Zahl

1. Einleitung

Mit Ausbruch der COVID-19 Pandemie Anfang 2020 rückte das Thema Schutz der Kritischen Infrastruktur verstärkt in das öffentliche Bewusstsein. Die Bedeutung eines funktionierenden Gesundheitssystems war nahezu täglich Gegenstand von Pressekonferenzen und Medienberichterstattungen. Die Überlastung der Krankenanstalten zu vermeiden begründet Maßnahmen zur Eindämmung der Virusausbreitung (vgl. Blasche et al. 2021: 3).

Kritische Infrastrukturen sind per Definition für den Erhalt gesellschaftlicher Funktionen und des Zusammenlebens essenziell. Der Begriff, was unter Kritischer Infrastruktur zu verstehen ist, kann weit gefasst werden. Im Österreichischen Programm zum Schutz Kritischer Infrastruktur (*Austrian Programme for Critical Infrastructure Protection* – APCIP) wurde die nachfolgende Begriffsbestimmung gewählt: „*Kritische Infrastrukturen sind jene Infrastrukturen oder Teile davon, die eine wesentliche Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen haben und deren Störung oder Zerstörung schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl der Bevölkerung oder die effektive Funktionsweise von Regierungen haben würde*.“ (APCIP 2015: 6)

Der Namensbestandteil „kritisch“ ergibt sich aus der Unterversorgung mit diesen Leistungen bzw. dem Mangel dieser Dienste. Folglich führt ein Fehlen einzelner oder aller Bereichen der Kritischen Infrastruktur zu zumindest negativen, wenn nicht sogar katastrophalen Auswirkungen für die Kohärenz einer modernen Gesellschaft (vgl. Krings 2020: 577; Knauf 2020: 11). Von staatlicher Seite besteht aus diesem Grund ein Interesse am Schutz der Kritischen Infrastruktur (vgl. APCIP 2015: 4).

Aufgrund der Vernetzung der Kritischen Infrastrukturen sowohl über Sektor- als auch über Staatsgrenzen hinweg, bestehen starke, nichtlineare gegenseitige Abhängigkeiten voneinander. Diese Interdependenzen führen dazu, dass Störungen in einem Land infolge eines Kaskadeneffekts ganze Regionen in Mitleidenschaft ziehen. Das Elektrizitätsübertragungssystem nimmt innerhalb der Kritischen Infrastrukturen eine zentrale Stelle ein. Sowohl Kommunikation, Transport und Verkehr sowie das moderne Finanzwesen benötigen eine verlässliche Stromversorgung (OSCE 2016: 7). „*Die gegenwärtige Gesellschaftsform ist die einer Netzwerkgesellschaft geworden* […] *Eine essentielle Rolle in komplexen*

Gesellschaftsstrukturen hat zweifelsohne die Versorgung mit elektrischer Energie übernommen. Bricht die Stromversorgung großflächig und für längere Zeit zusammen, so droht ein Kollaps ungeahnten Ausmaßes“ (Blaschke 2017: VII). Störungen der Versorgung mit elektrischer Energie stellen somit eine erhebliche Bedrohung für die moderne Gesellschaft dar. Die Verfügbarkeit von Elektrizität hat für die Gesellschaft eine zentrale Bedeutung. Strom und Energie spielen im Alltag eine wichtige Rolle. Ein Stromausfall kann dabei durch zahlreiche Ursachen ausgelöst werden. Durch kaskadenartige Ausfälle von weiteren Stromleitungen besteht die Gefahr, dass sich ein lokaler Störfall zu einer Katastrophe entwickelt. Als Worst-Case-Szenario wird ein langandauernder überregionaler Stromausfall, ein Blackout, angesehen (vgl. Saurugg 2021: 330). Die Lebensmittel-, Wasser-, Abwasser- und die medizinische Versorgung werden ohne Strom sehr problematisch. Auch ein Großteil des Transportwesens kommt zum Erliegen. Die Informationstechnik und Telekommunikation, wie etwa Rundfunk, Telefonie oder Internet sind nur kurzfristig ohne kontinuierlicher Stromzufuhr funktionsfähig. (vgl. Birkmann et al. 2010: 13ff.)

Stromausfälle können mannigfaltige Ursachen zugrunde liegen. Netzwerkstörungen, Systemfehler oder Naturgefahren sind Beispiele für deren Auslöser. Zur Erhöhung der Resilienz und Autarkie sind Krankenanstalten gegen Stromversorgungs-unterbrechungen mit gesetzlich vorgeschriebenen Notstromaggregaten abgesichert. Rettungsdienste verfügen ebenfalls darüber. Damit wird der gesetzliche Anspruch wonach der Betrieb von Einsatzleitstellen rund um die Uhr gewährleistet sein muss, erfüllt (vgl. § 21 Abs. 2 WRKG).

Der Begriff Autarkie steht im Zusammenhang mit Kritischen Infrastrukturen nach Ansicht von Expert*innen im Widerspruch zu der Vernetzung dieser, für die Gesellschaft wichtigen, Einrichtungen. Dauert ein Ausfall bzw. die Unterbrechung mehrere Tage und geht diese einher mit Störungen anderer Kritischer Infrastrukturen, sind auch Krankenanstalten in einem hohen Maße vulnerabel.

Die Gesellschaft ist dank Digitalisierung vernetzter denn je und die technische und prozessuale Vernetzung hat alle Lebensbereiche durchdrungen. Der daraus entstandene Cyberraum hat sich als Teil des gesellschaftlichen Zusammenlebens etabliert. Ein stabiler und sicherer Cyberraum wird als Grundlage für die positive Entwicklung Österreichs und der Europäischen Union angesehen (vgl. ÖSCS 2021: 11f.).

Eine Bedrohung für den Cyberraum besteht dabei nicht ausschließlich in Form von Stromstörungen. Auch Cybersicherheitsvorfälle sind ein weiteres immanentes Risiko. Cyberattacken auf einzelne Informationssysteme stören die Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit dieser. Einschränkungen bis hin zu Ausfällen einzelner oder aller Dienste können erhebliche Auswirkungen zur Folge haben. Madnick (2022: 5) attestiert in einem Artikel des Harvard Business Review ernsthaften Cyberangriffen ein gleichwertiges Schadenspotential wie es Naturkatastrophen inhärent ist. Den Risiken durch Cyberangriffe wird durch einen Maßnahmenmix begegnet. Dadurch soll erreicht werden, sowohl die Eintrittswahrscheinlichkeiten als auch die Auswirkungen zu reduzieren. Verschiedene Vorschriften definieren dabei die Anforderungen an die Sicherheitsmaßnahmen zum Schutz des virtuellen Raums und vernetzter Informationsdienste.

Auf supranationaler Ebene wurde die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (kurz NIS-RL) erlassen. Mit der Richtlinie wird die Zielsetzung verfolgt, das allgemeine Niveau der Netz- und Informationssicherheit zu erhöhen. Die einzelnen Mitgliedstaaten der Europäischen Union wurden dazu angehalten eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen festzulegen und nationale Behörden zu implementieren. (vgl. Mayer 2020: 3)

In Österreich wurde im Jahr 2018 ein Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (NIS-Gesetz) vom Nationalrat beschlossen. Vom Bundesministerium für EU, Kunst, Kultur und Medien folgte eine dazugehörige Verordnung zur Festlegung von Sicherheitsvorkehrungen und näheren Regelungen zu den Sektoren sowie zu Sicherheitsvorfällen nach dem Netz- und Informationssystemsicherheitsgesetz (Netz- und Informationssystemsicherheitsverordnung). Hierin wurden sieben Sektoren festgelegt welche Betreiber sogenannter wesentlicher Dienste benennen. Das Gesundheitswesen ist einer dieser Sektoren. (vgl. § 8 NISV)

Krankenanstalten mit ihren hochspezialisierten Abteilungen kommt eine tragende Rolle in der Gesundheitsversorgung zu. Man kann sie als das Herzstück des Gesundheitswesens in Österreich bezeichnen. Die Ausstattung zur Diagnose, Behandlung und Rehabilitation von Erkrankungen bzw. Verletzungen greift dort wo der

extramurale Sektor an die Grenzen seiner Möglichkeiten stößt (vgl. § 1 KAKuG). Das Verbindungsglied zwischen dem extra- und intramuralen Bereich stellt der Rettungs- und Krankentransportdienst dar (vgl. § 1 WRKG). Dieser stellt den fachgerechten Transport Erkrankter oder Verunfallter zu der Behandlungseinrichtung sicher. Der Rettungsdienst führt am Notfallort lebensrettende Sofortmaßnahmen durch und stellt die Transportfähigkeit der Patient*innen her. Die präklinische Notfallmedizin, als Teil der Daseinsvorsorge, ist folglich ebenso Teil der besagten Kritischen Infrastruktur (vgl. § 8 Abs. 1 Z 2 NISV).

Gemäß der Bundesverfassung sind die Bundesländer sind für die Organisation des Rettungsdienstes zuständig und haben die allgemeine Regelungskompetenz. Daher sind Aufgaben, Struktur und Organisation des Rettungswesens in neun Landesgesetzen unterschiedlich geregelt. (vgl. BRH 2020: 7) Folglich ist das Österreichische Rettungswesen heterogen und von der föderalen Struktur gekennzeichnet. Dessen Organisation unterscheidet sich in der Stadt Wien unterscheidet sich in einigen Kriterien von den übrigen Bundesländern. Im Rahmen dieser Arbeit konzentriert sich der Betrachtungsraum auf die notfallmedizinische Versorgung in der Bundeshauptstadt Wien. Unterschiede der rettungsdienstlichen Versorgung zwischen dem ländlichen und dem urbanen Raum werden nicht thematisiert.

Ob und wie sich die Rechtsvorschriften auf den Prozess der Patient*innenversorgung auswirken wird in dieser wissenschaftlichen Arbeit ergründet. Im Fokus befindet sich die Schnittstelle zwischen der präklinischen und der intramuralen Versorgung von Notfallpatient*innen. Im Gegensatz zu einer Vielzahl von elektiven Behandlungen handelt es sich bei medizinischen Notfällen um zeitkritische Ereignisse. Auch unter den erschwerten Bedingungen von Krisen oder eines Katastrophenereignisses muss die Gesundheitsversorgung und insbesondere die notfallmedizinische Versorgung der Bevölkerung gewährleistet und ohne Zeitverzug erbracht werden können. Daher ist es von Interesse die Effekte einer EU Richtlinie die Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen bezweckt näher zu untersuchen.

1.1. Hypothesen und Forschungsfragen

In diesem Unterkapitel der Forschungsarbeit werden die Hypothesen und leitenden Fragen vorgestellt. Das Forschungsinteresse richtete sich vordergründig auf die Schnittstelle zwischen der präklinischen und der intramuralen Notfallmedizin. Die gebildeten Hypothesen mitsamt der grundsätzlichen Fragestellung wurden im Verlauf der Forschungstätigkeit adaptiert. Die konkreten Beweggründe sind im Abschnitt Conclusio dargelegt.

Hypothese 1

Der Begriff Autarkie, im Zusammenhang mit Resilienz unserer modernen Gesellschaft, steht im Widerspruch zur Vernetzung von Systemen.

Forschungsfrage 1

Wo sehen Expert*innen einen Steigerungsbedarf um die Resilienz von Kritischen Infrastrukturen zu erhöhen?

Forschungsfrage 2

Welche Maßnahmen erscheinen notwendig um die Resilienz der Gesellschaft zu stärken?

Hypothese 2

Durch das Netz- und Informationssystemsicherheitsgesetz werden die intersektorale Konnexität und Interdependenzen nicht beachtet.

Forschungsfrage 3

Wie bewerten Expert*innen das Netz- und Informationssystemsicherheitsgesetz im Fokus der beiden Hypothesen?

Forschungsfrage 4

Gegen welchen Bedrohungen müssen Kritische Infrastrukturen nach Meinung von Expert*innen wappnen?

1.2. Aufbau der Arbeit

In diesem Abschnitt wird die grundlegende Struktur der wissenschaftlichen Abschlussarbeit umrissen. Ein wesentliches Kennzeichen von wissenschaftlichen Arbeiten stellt die strukturierte, nachvollziehbare und übersichtliche Aufbereitung eines Themas dar. Die Gliederung der Masterarbeit teilt sich grob in zwei Abschnitte, einen theoretischen und einen empirischen Teil. Aufeinander aufbauende Kapitel ermöglichen die geordnete Aufarbeitung von Forschungsfragen.

Mittels Literaturrecherche werden die elementaren Begriffe herausgearbeitet. Sie bietet eine Reflektion des derzeitigen Stands der Wissenschaft und erlaubt eine breite Betrachtung des Themenfelds. Der Mix aus verschiedenen Quellen fließt in die erläuternden Kapitel ein. Dies ermöglicht es einen Bezug zur forschungsleitenden Fragestellung und den Hypothesen für die empirische Forschungstätigkeit herzustellen. Die Kriterien und das Vorgehen zur Auswahl der Literatur werden im Rahmen des Abschnitts über die empirische Forschung beschrieben.

Kapitel zwei befasst sich mit den Hypothesen und Forschungsfragen. In dem Teilstück werden die Fragestellung und die entwickelten Hypothesen vorgestellt. Des Weiteren werden das Interesse am Forschungsfeld und vorangegangene Überlegungen beschrieben.

Die Methodik zur Falsifikation bzw. zur Verifikation der Hypothesen ist Gegenstand des dritten Kapitels. Hier werden das Vorgehen für die Literaturrecherche und die Auswahl der Expert*innen wiedergegeben.

Im vierten Kapitel liegt der Fokus auf dem Begriff der Kritischen Infrastruktur. Sowohl die gängigen Definitionen als auch generelle Kennzeichen werden hier anhand der Basisliteratur zusammengefasst. Primäre Quellen stellen hierbei die unterschiedlichen einschlägigen Rechtsvorschriften und Sicherheitsstrategie-Papiere dar. Dieses Segment der Arbeit liefert die Hintergrundinformationen und dient der Vorbereitung auf das Folgekapitel.

Das fünfte Kapitel beinhaltet europäische und österreichische Strategien zum Schutz Kritischer Infrastruktur. Im zweiten Subkapitel dieses Passus werden die NIS-Richtlinie der Europäischen Union mitsamt den daraus abgeleiteten nationalen Rechts-vorschriften, dem NIS-Gesetz und der NIS-Verordnung, erklärt.

Das dritte Segment des Kapitels befasst sich mit Normen-Reihen welche beim Schutz von Organisationen und Systemen Anwendung finden.

Zwei zentrale Bedrohungen für Kritische Infrastrukturen, Blackout und Cyberangriffe, werden in den darauffolgenden Kapiteln behandelt. Anhand der beiden Szenarien sollen die gesellschaftlichen Risiken durch eine Störung der Kritischen Infrastrukturen aufgezeigt und verdeutlicht werden.

Dem Bezug zum Rettungswesen und der Fragilität gegenüber den zuvor aufgezeigten Bedrohungen ist das achte Kapitel gewidmet. Es wird der Behandlungspfad von Notfallpatient*innen skizziert. Die Stakeholder und bestimmende Systemkomponenten der Rettungskette werden darin ebenfalls vorgestellt. Das gestattet Leser*innen, welche mit der Systematik der medizinischen Notfallversorgung nicht vertraut sind, einen Zugang zur Materie. Damit wird der Theorieteil der Arbeit abgeschlossen.

Der empirische Teil wird mit Kapitel neun eröffnet. Kriterien für die Auswahl der Literatur des Theorieteils und der Expert*innen für die Interviews werden darin transparent gemacht. Für die Herleitung der Ergebnisse erfolgt eine qualitative Inhaltsanalyse nach Mayring. Interviewergebnisse und zentrale Aussagen der Expert*innen finden sich ebenfalls in diesem Kapitel.

Das vorletzte Kapitel vergleicht die Interviewergebnisse des empirischen Teils mit den Aussagen des Theorieteils. Es dient der Vorbereitung auf die finale Conclusio im elften Kapitel. Neben einer Zusammenfassung der einzelnen Ergebnisse liegt das Schwergewicht auf der Überprüfung der einzelnen Hypothesen. Weiters wird ein Ausblick auf die NIS 2-Richtlinie und die Richtlinie über die Widerstandsfähigkeit Kritischer Einrichtungen (RKE) geboten.

2. Methodik

Damit die beiden Hypothesen verifiziert sowie die abgeleiteten Forschungsfragen beantwortet werden können, wird in dieser Abschlussarbeit zunächst eine einleitende Erläuterung von zentralen Begriffen vorgenommen. Die Begrifflichkeiten wurden anhand eines literaturbasierten Vorstudiums recherchiert. Vorhandenes Vorwissen wurde hierbei vertieft und weitere Quellen wurden sukzessive in die Arbeit aufgenommen.

2.1. Literaturrecherche

Die Basis für die wissenschaftliche Arbeit ist eine gediegene Überprüfung des Status quo. Durch die Evaluierung des aktuellen Stands der Wissenschaft werden unterschiedliche Ansichten erfasst und vorhandene Kenntnisse kritisch reflektiert sowie weiter vertieft. Für die Literaturrecherche eignen sich nicht alle Schriftstücke gleichermaßen. In dieser Arbeit wird Literatur der Typen der Primär- und Sekundärliteratur herangezogen. Graue Literatur, Broschüren und Internetquellen, werden weitestgehend vermieden.

Auf Basis der gesichteten Schriften wurden in weiterer Folge ein Interviewleitfaden konzipiert. Die Interviews mit Expert*innen des Themengebiets dienten der Vertiefung des Erkenntnisstands sowie der Verifikation oder zur Falsifizierung der Hypothesen und Klärung der Forschungsfrage. Bei der Selektion von geeigneten Gesprächspartner*innen wurde Wert auf eine ausgewogene Zusammensetzung gelegt. Sowohl der klinische Sektor, als auch die Präklinik sollten vertreten sein. Zudem sollten Personen aus dem Bereich Schutz/Sicherheit ihre Kenntnisse und Meinungen einbringen. Durch diese Auswahl wurde eine geeignete Ergänzung der Ergebnisse aus der vorangegangenen Literaturrecherche ermöglicht werden.

Für die Suche nach geeigneter Literatur kam anfangs eine systematische Schlagwortsuche zum Einsatz. Bei der Recherche wurden die Literaturdatenbank der Universität Wien und die Suchmaschinen google.com sowie scholar.google.com herangezogen. Schlüsselwörter wurden dafür in Datenbanken von Bibliotheken abgefragt.

Folgende Datenbanken bzw. Suchmaschinen wurden verwendet:

- U:search der Universitätsbibliothek Wien (https://usearch.univie.ac.at)
- Google Scholar (https://scholar.google.com)
- Google (https://google.com)

Neben den zentralen Begriffen Blackout und Cyberangriff wurde auch nach Resilienz, Stromausfall und Kritischer Infrastruktur gesucht. Die nachfolgende Tabelle zeigt eine Auswahl der gewählten Schlüsselwörter für die Stichwortsuche:

Tabelle 1: Wichtigste Schlagwörter für die Literaturrecherche

Schlagwort	Suchmaschinen
Blackout	U:search Google Scholar Google
Stromausfall	
Kritische Infrastruktur	
Critical infrastructure	
Power shortage	
Healthcare	
Gesundheitssektor	
Cyberangriff	
Cyberattack	
Cybersicherheit	
Cyberwarfare	
Cyberwar	

Durch das Voranschreiten bei der Suche wurden weitere Wörter und Derivate der initialen Bezeichnungen sowie Kombinationen von Begriffen verwendet.

Die Informationen aus den Texten dienten, wie eingangs erwähnt, als Grundlage für den Theorieteil dieser Arbeit und als Orientierung zur Erstellung des Interview-leitfadens.

2.2. Expert*inneninterviews

Im Gegensatz zu standardisierten Interviews, bei denen sowohl die Fragen als auch die Antwortmöglichkeiten vorgegeben sind, wurde eine offene Antwortmöglichkeit als sinnvoll erachtet. Die Entscheidung fiel zugunsten leitfadengestützter Interviews mit Expert*innen welche anschließend genauer untersucht wurden. Eine Inhaltsanalyse der Interviews nach Mayring (vgl. 2015) schien eine geeignete Methode zur Untersuchung von Kernaussagen zu sein. Sie bezweckt detaillierte und dennoch differenzierte Informationen von Kenner*innen der Materie zu erhalten. Ein narratives Interview wurde im Vergleich als zu umfangreich für einen fristgerechten Abschluss der Forschungstätigkeit angesehen. Der Leitfaden sorgt nicht nur für einen *roten Faden* bei der Gesprächsführung, sondern sorgt zudem für eine Vergleichsbasis ohne dabei die Expert*innen bei den Antworten einzuschränken.

Für die Analyse der einzelnen Antworten erfolgte deren Reduktion auf ihre Kernaussage. Ein Überblick und die Vergleichbarkeit von den Meinungen der Expert*innen werden dadurch erleichtert. Danach erfolgte ein Diskurs, wobei auf Gemeinsamkeiten und Widersprüche besonders eingegangen wird.

Von Mitte April bis Ende Mai 2022 fanden die Gespräche mit den verschiedenen ausgewählten Expert*innen statt.

2.2.1. Expert*innenauswahl

Am Beginn der empirischen Forschungstätigkeit wurden leitfadengestützte Interviews mit Expert*innen aus dem Bereich Rettungsdienst, klinisches Notfallmanagement und Schutz Kritischer Infrastrukturen geführt. Mit einem überwiegenden Teil der Gesprächspartner*innen bestand bereits im Vorfeld ein beruflicher Kontakt. Die Personen wurden primär per E-Mail kontaktiert und erhielten den Interviewleitfaden nach Zusage des Gesprächstermins. Teilweise ergaben sich Rückfragen durch die Betroffenen welche telefonisch geklärt wurden.

Bei der Auswahl wurde auf einen ausgewogenen Mix aus den Bereichen Schutz/Sicherheit, Rettungsdienst und Krankenanstalten geachtet. Auf Seite 14 sind die Expert*innen mit Name, Funktion und weiteren Anmerkungen in einer Tabelle aufgezählt.

2.2.2. Experte Auer

Für die Rettungsleitstelle der Berufsrettung Wien war Herr Mag. Alexander Auer, MSc als Chief Information Security Officer (CISO) tätig. Davor war er mehrere Jahre der Stellvertretende Leiter der Wiener Rettungsakademie. Im Rahmen des Krisenmanagements engagierte sich Herr Mag. Auer, MSc im Einsatzstab der Magistratsabteilung 70. Die Räumlichkeiten der Berufsrettung dienten als Kulisse für den Meinungsaustausch.

Das Wissen über die Strukturen der Berufsrettung Wien und die Detailkonzepte zur Steigerung der Resilienz der Rettungsleitstelle machten den CISO der Magistratsabteilung 70 zu einem attraktiven Gesprächspartner.

2.2.3. Experte Baron

Von der Leiterin des Journaldienstes des Wiener Gesundheitsverbunds wurde Herr Karl Baron als Experte für das Interview nominiert. Er ist mit der Konzeptionierung eines Informationssicherheitsmanagementsystems betraut. Außerdem befasst sich Herr Baron mit der Erfüllung der Vorgaben des NISG und der dazugehörigen Verordnung im Allgemeinen Krankenhaus der Stadt Wien (AKH Wien).

Das Interview erfolgte in den Büroräumlichkeiten des Experten im Allgemeinen Krankenhaus. Das Gespräch wurde wegen eines technischen Gebrechens des Aufnahmegeräts nicht aufgezeichnet weshalb die erhaltenen Informationen als Hintergrundinformationen behandelt wurden. Sie sind damit nicht im Diskurs und der Inhaltsanalyse enthalten.

2.2.4. Experte Eisenburger

Herr Primar Universitätsprofessor Dr. Eisenburger leitete die Notfallklinik der Klinik Floridsdorf im Norden von Wien. Das Gespräch fand im Sekretariat der Klinikabteilung statt.

In den Zuständigkeitsbereich von Prof. Dr. Eisenburger fiel die Vorbereitung der Krankenanstalt auf Krisenszenarien und Katastrophen. Durch die Wahl dieses Experten sollte die Perspektive um die klinische Facette erweitert werden. Die Informationen von Herrn Chefarzt Dr. Krammel aus der Präklinik wurden damit ergänzt und der Behandlungspfad von Notfallpatient*innen konnte abgedeckt werden.

2.2.5. Experte Glaninger

Als Leiter der Rettungsleitstelle Wien war Herr Patrick Glaninger ein weiterer Experte des Wiener Rettungswesens. Im oblag die Organisation und Koordination der technischen und personellen Ressourcen damit die Rettungsleitstelle rund um die Uhr erreichbar war und das geeignetste Rettungsmittel zum Notfallgeschehen entsenden konnte. Ein Arbeitsschwerpunkt lag in der Umsetzung des Notfall-, Krisen- und Kontinuitätsmanagementplans in der Organisationsstruktur im Zusammenhang mit der NIS-Gesetzgebung.

Mit Herrn Glaninger wurde in seinem Büro neben der Rettungsleitstelle gesprochen.

2.2.6. Expertin Heissenberger

Frau Dipl.-Ing.in Sandra Heissenberger, MBA war Chief Information Security Officer (CISO) der Stadt Wien. Sie trug in dieser Funktion die Verantwortung für die Netzwerksicherheit der Stadt Wien. Als solche koordinierte sie die Maßnahmen zur Erfüllung der NIS-Vorgaben innerhalb der Gemeinde und des Landes Wien. Ihr Input deckt sowohl organisatorische als auch strategische Dimensionen bei der Implementierung der NIS-Vorgaben ab.

Zur Erörterung der einzelnen Fragen fand das Interview persönlich in ihrem Büro in Wien statt. Mit der CISO besteht seit einigen Jahren ein beruflicher Kontakt wodurch es erleichtert wurde einen Gesprächstermin zu vereinbaren.

2.2.7. Experte Hellwagner

Herr Prof. Dr. Klaus Hellwagner, LL.M war Notarzt und zudem mehrere Jahre Bataillonsarzt eines Milizverbands des Österreichischen Bundesheeres. Die Milizfunktion wechselte zwischenzeitlich. Er übernahm die Aufgaben des Leitenden Sanitätsoffiziers für das Militärkommando Wien. Neben den Erfahrungen als Stabsoffizier verfügt der Arzt über präzise Kenntnisse der Notfallmedizin und der Wiener Gesundheitslandschaft. Zudem konnte er ein klares Verständnis für Rechtsmaterien vorweisen was einen zusätzlichen Anreiz bot, ihn um ein Interview zu bitten.

Für die Befragung fand ein Treffen in privater Umgebung statt.

2.2.8. Experte Krammel

Der erste Interviewpartner war Herr Chefarzt Dr. Krammel. Er leitete den ärztlichen und medizinischen Bereich der Magistratsabteilung 70 – Berufsrettung Wien. In dieser Funktion ist der ärztliche Leiter der Berufsrettung Wien für die notärztliche Versorgung der Wiener Bevölkerung im Regelrettungsdienst, bei Großschadenslagen sowie bei Krisen und im Katastrophenfall zuständig. Chefarzt Dr. Krammel wird wegen seines Wissens um die präklinische Notfallmedizin im Besonderen sowie des Wiener Rettungswesens hierfür besonders geschätzt.

Das Interview fand persönlich unter Einhaltung von COVID-19 Schutzmaßnahmen in einem Büro der Berufsrettung Wien statt.

2.2.9. Expertin LVT

Die dritte Expertin war im Landesamt für Verfassungsschutz und Terrorismusbekämpfung (LVT) in Wien tätig. Das Interview erfolgte per Telefon. Eine namentliche Nennung wurde von der Gesprächspartnerin abgelehnt.

Sie wurde durch den zuständigen Leiter des Referats Schutz Kritischer Infrastruktur der Abteilung II S4 Schutz und Sicherheit empfohlen. Zu ihrem Aufgabengebiet zählten die Beratung von Kritischen Infrastrukturen in Wien und die Unterstützung beim Etablieren von Schutzkonzepten. Ihre Einschätzung von Sicherheitsaspekten bzw. Bedrohungen für Kritische Infrastrukturen sollte diesen Bereich abdecken.

2.2.10. Expertin Mayer

Frau Ing.^{in} Mag.^{a} Dr.^{in} Sylvia Mayer, MA von der Direktion Staatsschutz und Nachrichtendienste erklärte sich bereit als zweite Interviewpartnerin zur Verfügung zu stehen. Der Kontakt wurde über das Landesamt für Verfassungsschutz hergestellt und das Gespräch erfolgte in den Räumlichkeiten der Nachfolgeorganisation des Bundesamts für Verfassungsschutz (BVT).

Die Dissertation von der Interviewpartnerin behandelt [*r*]*echtliche Fragestellungen in der nationalen Umsetzung der Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen (NIS-RL)*. Zudem war sie mehrere Jahre für den Schutz Kritischer Infrastrukturen in Österreich im Rahmen ihrer beruflichen Tätigkeit zuständig. Als Expertin für das

NIS-Gesetz war es ein Anliegen sie als Interviewpartnerin zu gewinnen. Durch die Befragung sollten Spezifika des Gesetzes und der ihm zugrundeliegenden EU-Richtlinie genauer erörtert werden. Mehrere Passagen dieser Arbeit stützen sich auf ihre Sachkenntnis.

*Tabelle 2: Übersicht Expert*innen*

Expert*in	**Organisation**	**Funktion und Anmerkung**
Auer	MA 70	CISO der MA 70
Baron	AKH Wien	CISO des AKH Wien
Eisenburger	Klinik Floridsdorf	Leiter der Zentralen Notaufnahme
Glaninger	MA 70	Leiter der Rettungsleitstelle Wien
Heissenberger	Magistratsdirektion	CISO der Stadt Wien
Hellwagner	MA 70 und MilKdoW	Notarzt und Stabsoffizier
Krammel	MA 70	Chefarzt der MA 70
LVT-Expertin	LVT	Anonym
Mayer	DSN	Expertin für das NISG

3. Kritische Infrastrukturen

Das Kapitel zeigt Kriterien für die Klassifikation von Infrastrukturen damit diese als Kritische Infrastruktur (KRITIS) gelten. Dafür wurden Definitionen aus Strategiepapieren sowie von Rechtsquellen herangezogen. Die Begriffsbestimmung ist bei einer internationalen Betrachtung nicht einheitlich. Die gewählte Interpretation des Begriffs orientiert sich für diese Arbeit an österreichischen Dokumenten bzw. an Texten der Europäischen Union.

3.1. Definitionen für Kritische Infrastrukturen

Im Strategiepapier der Republik Österreich sind „*Kritische Infrastrukturen jene Einrichtungen (Systeme, Anlagen, Prozesse, Netzwerke oder Teile davon), die eine wesentliche Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen haben und deren Störung oder Zerstörung schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl großer Teile der Bevölkerung oder das effektive Funktionieren von staatlichen Einrichtungen haben würde“* (APCIP 2015: 6).

Der Rat der Europäischen Union verwendet in Richtlinie 2008/114/EG eine ähnliche Begriffsbestimmung für Kritische Infrastruktur. Demzufolge handelt es sich dabei um „*die in einem Mitgliedstaat gelegene Anlage, ein System oder ein Teil davon, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind und deren Störung oder Zerstörung erhebliche Auswirkungen auf einen Mitgliedstaat hätte, da diese Funktionen nicht aufrechterhalten werden könnten*; […]“ (Art. 2 RL 2008/114).

Zum Vergleich mit der EU seien die Vereinigten Staaten von Amerika genannt. Dort werden andere Dienste als Kritische Infrastruktur bezeichnet, als dies durch die Europäischen Kommission der Fall ist. Beispielsweise wurden das Polizei- und Feuerwehrwesen in der *Presidential Decision Directive 63* (PDD-63) von 1998 zu den KRITIS gezählt. In der *National Strategy for Homeland Security* aus dem Jahr 2002 finden sich u.a. die Chemieindustrie, die Landwirtschaft oder auch die Verteidigungsindustrie bei der Aufzählung von Kritischen Infrastrukturen. (vgl. Moteff und Parfomak 2004: 5)

Die Daseinsvorsorge für die Bevölkerung baut auf der ständigen Verfügbarkeit und dem reibungslosen Ablauf vielfältiger Infrastrukturen auf. Dabei handelt es sich nicht ausschließlich um Objekte oder Bauten im eigentlichen Sinn. Gewisse Dienstleistungen werden ebenfalls zu diesem Themenbereich gezählt. Eine Störung oder Verknappung von manchen Leistungen oder Gütern kann schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl der Bevölkerung haben. Diese Effekte können bis hin zu negativen Folgen auf die Stabilität der Gesellschaft reichen. Das Fehlen dieser ist daher als kritisch anzusehen. Kritisch wird eine Infrastruktur folglich dann, wenn ihre Bedeutung für den Staat oder die darin lebende Gesellschaft so weit gestiegen ist, dass durch deren Ausfall ein deutlicher Wohlstandsverlust für die Bürger*innen des Staates, eintreten würde. Im schlimmsten Fall kann der Staat im Falle ihrer Störung nicht mehr funktionieren. (vgl. Kuhn 2005: 4; APCIP 2015: 4; Mayer 2020: 1)

Aufgrund der diversen Arbeitsteiligkeit ergibt sich folglich, dass es nicht die e*ine Kritische Infrastruktur* gibt. Vielmehr handelt es sich um einen Verbund an Verfahrensweisen, Leistungen und Produkten die für den sozialen Frieden und die gesellschaftliche Kohärenz wichtig sind. Zudem bestehen lineare sowie direkte und indirekte Abhängigkeiten von Kritischen Infrastrukturen untereinander. Alle sind auf die Verfügbarkeit von elektrischer Energie angewiesen. Dennoch hat der Energiesektor, auch wenn ihm eine zentrale Rolle zukommt, keinen alleinigen Anspruch auf die Bezeichnung Kritische Infrastruktur. (vgl. Saurugg 2022: 208)

Auf Seite 18 zeigt Abbildung 1 von *Cyber Security Austria* die Verflechtung der verschiedenen Branchen untereinander. Jede für sich und alle gemeinsam haben einen hohen Stellenwert für die moderne Gesellschaft. Das Spektrum welche Dienstleistungen, Güter und Systeme als wesentlich betrachtet werden und daher als Kritische Infrastruktur zu werten sind reicht von Energie und Wasser über Bankwesen und die Finanzmarkinfrastruktur bis zum Gesundheitswesen sowie der Verkehrs- und der Digitalen Infrastruktur. (vgl. APCIP 2015: 4f.; Pausch 2017: 4; Krings 2020: 577)

Die Wechselbeziehung von Kritischen Infrastrukturen und die Bedeutung von deren Vernetzung fasst das Deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) 2004 folgendermaßen zusammen: „*Kritische Infrastrukturen sind Organisationen oder Einrichtungen mit (lebens-)wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Störung für größere Bevölkerungsgruppen nachhaltig wirkende Versorgungsengpässe oder andere dramatische Folgen eintreten. […] Sind einzelne solcher Infrastrukturen von gezielten Störungen (Information Warfare, terroristische Angriffe etc.) bzw. Ausfällen ihrer Informationstechnik betroffen, könnte dadurch eine Kettenreaktion von Störungen auch in anderen Bereichen ausgelöst werden* […]“ (zitiert nach Kuhn 2005: 5f.).

Mit dem Begriff der Kettenreaktion wird die wahrscheinliche Kaskade an Folgewirkungen einer Störung bei einer Kritischen Infrastruktur angesprochen. Die meisten Systeme sind heutzutage in irgendeiner Form miteinander verbunden. Beeinträchtigungen in einem Bereich können in andere Standorte, Branchen oder Sektoren hineinwirken. Das ursprüngliche Schadensgebiet weitet sich aus. Das Schadensausmaß überwindet dabei mitunter nationale, geographische oder sektorale Grenzen. (vgl. BMdI 2011: 7)

Auswirkungen auf die Betriebs- und Versorgungssicherheit werden anhand der Effekte für den Gesundheitssektor in dieser Arbeit behandelt. Die Verfügbarkeit von Gesundheitsleistungen ist in der Verfassung der Republik Österreich genannt (vgl. Art. 10 Abs. 1 Z 12 B-VG).

Die Versorgung mit lebenswichtigen Gütern und Dienstleistungen ist für den sozialen Frieden und die staatliche Kohärenz essenziell. Der Staat leistet einen wesentlichen Beitrag zur Steigerung der Resilienz und Sicherheit Österreichs durch Bereitstellung von Mitteln und durch die Gesetzgebung (vgl. APCIP 2015: 4).

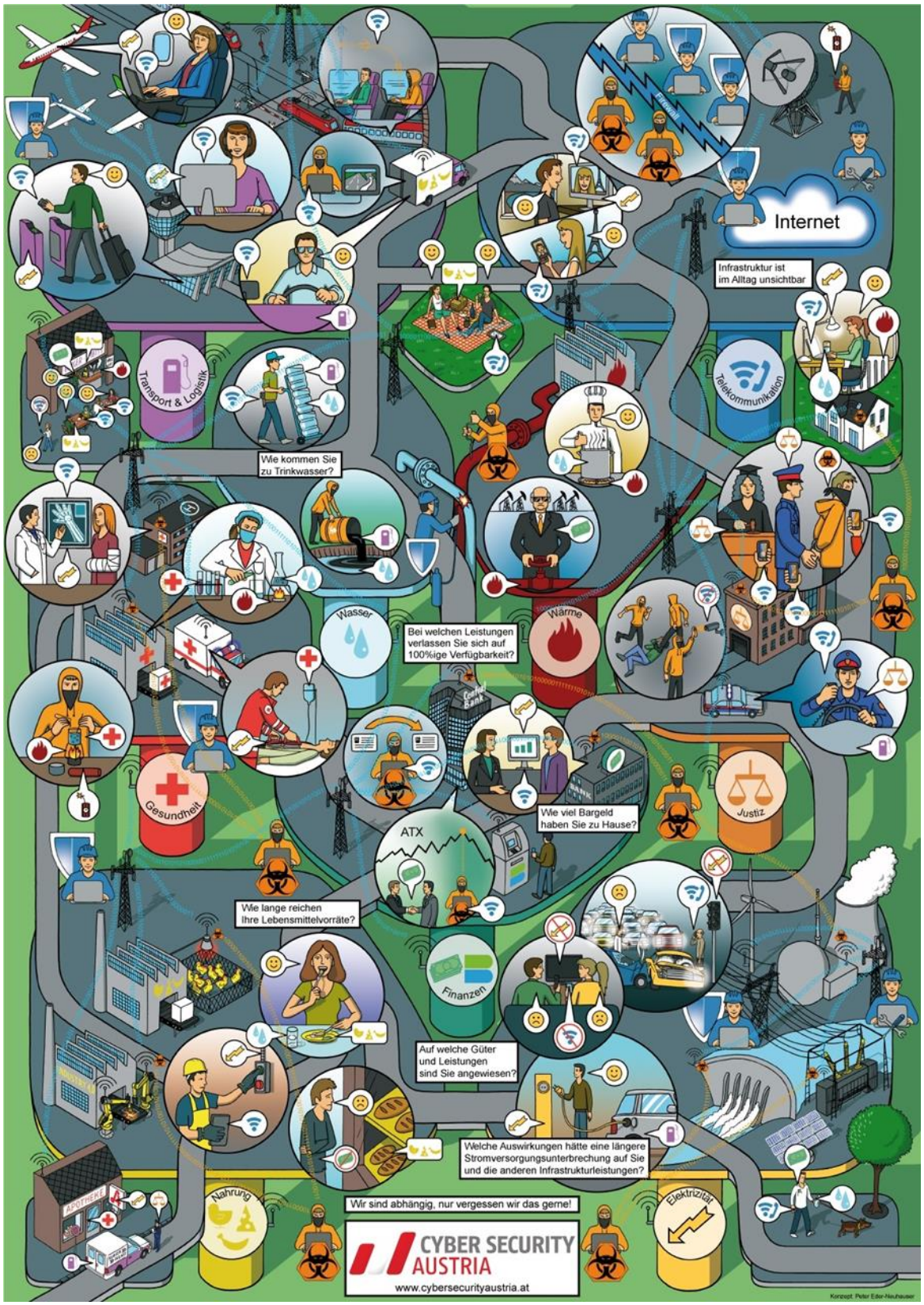

Abbildung 1: Wechselseitige Abhängigkeiten (Quelle: Cyber Security Austria)

Der Schutz von Kritischen Infrastrukturen vor Gefahren dient der Sicherstellung der unterbrechungsfreien Bereitstellung bedeutsamer Leistungen. Deren Einschränkung oder der Ausfall stellen eine Bedrohung für die Bevölkerung und die gesellschaftliche Kohärenz dar. (vgl. Krings 2020: 577) Kritische Infrastrukturen sind als Grundpfeiler der modernen Gesellschaft unterschiedlichen Bedrohungen ausgesetzt. Die Österreichische Bundesministerin für Landesverteidigung äußert sich zu dem Bedrohungsspektrum folgendermaßen: „*Blackouts gehören neben den Gefahren von Naturkatastrophen, Cyberangriffen, Terroranschlägen und Pandemien zu den sicherheitspolitischen Bedrohungsszenarien des 21. Jahrhunderts*“ (Tanner 2022: 7; vgl. Reisner 2021: 335).

Nach Ansicht des Europäischen Parlaments und des Rats der Europäischen Union zählen gemäß *Richtlinie (EU) 2016/1148* verschiedenste Systeme und Dienstleistungen zur Kritischen Infrastruktur. Organisationen oder Institutionen, die gewisse Leistungen für die Gesellschaft erbringen oder bereitstellen, wurden in der Richtlinie zu Sektoren zusammengefasst. In der Richtlinie ist in diesem Zusammenhang auch die Rede von Betreibern wesentlicher Dienste. Die Sektoren umfassen die Bereiche Energie, Verkehrs-, Banken- und Gesundheitswesen sowie weitere. Sie sind in Tabelle 3 auf Seite 29 detailliert aufgelistet. Kröger betrachtet dabei das Elektrizitätsübertragungssystem als die Entscheidendste unter den Kritischen Infrastrukturen. Zahlreiche weitere Bereiche wie etwa die Industrie, der Verkehr oder die Kommunikation funktionieren nicht ohne elektrische Energie. (vgl. Kröger 2016: 7)

Energiesysteme sind hochkomplexe Systeme mit großer Wichtigkeit für die moderne Gesellschaft, befinden auch Alhelou et al. (vgl. 2019: 1) in ihrer Arbeit über Blackouts von Energiesystem und Kaskadeneffekten. Die Fragilität des Systems „Energieversorgung“ hat in den vergangenen Jahren stetig zugenommen. Das Risiko eines Ausfalls der Versorgung mit Elektrizität wird Saurugg (vgl. 2022: 208) zufolge jedoch weiterhin unterschätzt.

Maßnahmen zur Vorbereitung auf einen Stromausfall beschränken sich laut Saurugg lediglich auf die Bewältigung des Ereignisses Stromausfall. Die Dauer der Versorgungsunterbrechung inklusive der Zeitspanne für die Synchronisation von Stromnetzen und das Wiederanlaufen der Versorgungsprozesse nach einem umfassenden Stromausfall können gegenwärtig nicht genau abgeschätzt werden.

Gefordert wird daher eine koordinierte Vorgangsweise zur Abfederung einer länger anhaltenden Versorgungsunterbrechung. (Saurugg 2022: 211; Saurugg 2021: 330)

Eine weitere Bedrohungsform die im Rahmen dieser Forschung untersucht wird sind Cyberangriffe. Eine immer größer werdende Anzahl an Bedrohungen verlagert sich in den virtuellen Raum. Bereits das Jahr 2021 war von einem starken Anstieg an Vorfällen im Cyberraum geprägt. Geopolitische Spannungen und Konflikte können die Europäische Union und Österreich betreffen können. Humenberger (vgl. 2022: 205) erwartet für das Jahr 2022 eine fortschreitende Zunahme an Cybersicherheitsvorfällen.

3.2. Bedrohungen für Kritische Infrastrukturen

Kritische Infrastrukturen sehen sich einer großen Anzahl an Bedrohungen gegenüber. Gleichzeitig ist der Schutz vor negativen Folgen von Vorfällen gerade bei diesen von großem Interesse und Wichtigkeit für die Gesellschaft. Staatliche Einrichtungen wie das Innen- und Verteidigungsministerium sind in der Republik Österreich mit dem Schutz Kritischer Infrastrukturen betraut. (vgl. Mayer 2020: 20ff.)

Die nachstehende Grafik zeigt gemäß dem Deutschen Bundesministerium des Inneren vier Risikokategorien welche zu einer erheblichen Schädigung oder Beeinträchtigung von Prozessen der Kritischen Infrastrukturen hervorrufen können (vgl. BMdI 2011: 5).

Die Kritischen Infrastrukturen und somit die Gesellschaft werden auf abstrakter Ebene von

- technischem und/oder menschlichem Versagen
- vorsätzliche Handlungen mit kriminellem oder terroristischem Hintergrund
- Krieg
- Naturereignissen

bedroht (vgl. ebenda).

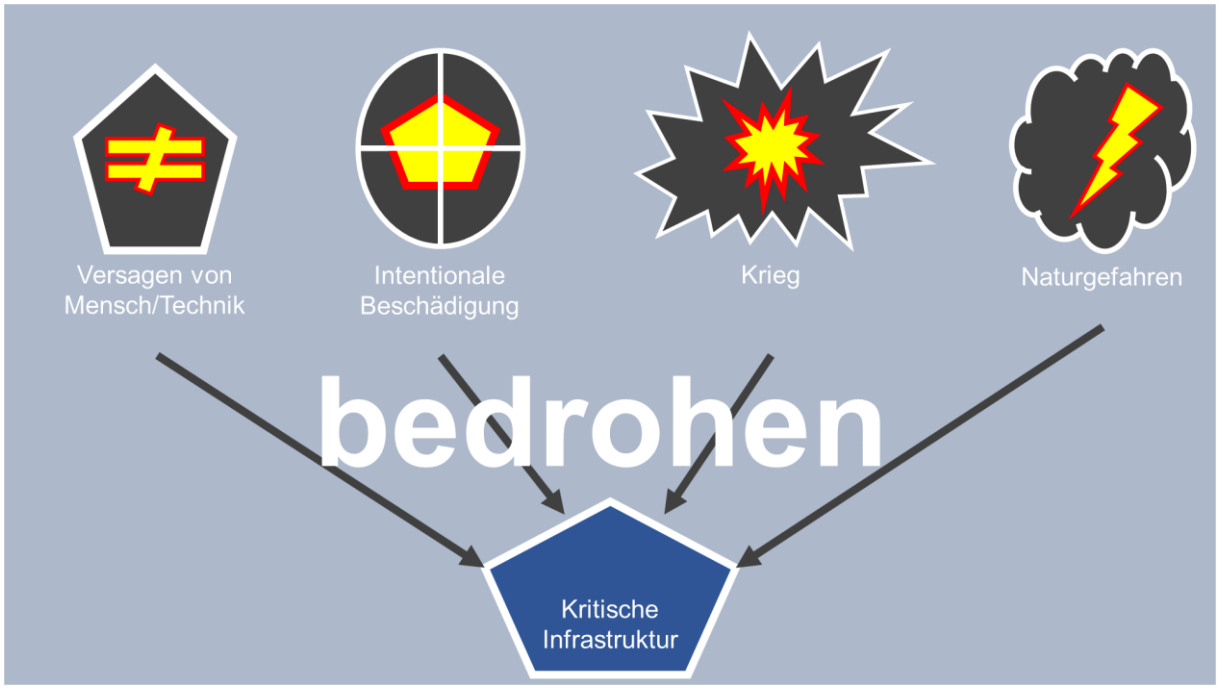

Abbildung 2: Bedrohungen für KRITIS (eigene Darstellung nach BMdI 2011: 5)

Diese Schlagwörter beinhalten eine weitere Menge an Risiken. Tabelle 3 gibt dazu nähere Auskunft. Verantwortliche der Kritischen Infrastrukturen müssen sich der Risiken bewusst sein und Vorkehrungen für deren Reduktion treffen.

Tabelle 3: Risiken mit Auswirkungen für KRITIS (Quelle: BMdI 2011: 46ff.)

Kategorie	Risiko	Auswirkung
Versagen von Mensch/Technik	Menschliches Versagen	Schalt-, Programmierfehlerfehler, Unaufmerksamkeit
	Systemische und/oder organisatorische Mängel	Netzaufsplitterung, übertriebenes Gewinnstreben
	Technisches Versagen	Wartungsmängel, Überalterung von Anlagen, Fehldimensionierung von Betriebsmitteln,

		mangelhafte Planung und Umsetzung Materialversagen, Produktionsfehler, Ausfall von zentralen Betriebs-mitteln
Intentionale Beschädigung	Kriminalität/Terrorismus	Betrug, Erpressung, Sabotage, Anschläge, Angriffe aus Steuerungssysteme Angriffe auf Personal
Krieg	Bewaffnete Konflikte	Zerstörung oder Störung von Verteilernetzwerken, Einsatz von koordinierten Cyber-angriffen
Naturgefahren	Pandemie	Krankheitsbedingter Ausfall von Personal
	Ressourcenmangel/-ausfall	Wassermangel, Wind, Öl, Gas, Kohle

	Klima- und Naturereignisse	Blitzschlag, Stürme, Hochwasser, Schnee/Eis, Erdbeben, Sonneneruption Hitze

Angriffe und Störfälle können nicht gänzlich ausgeschlossen werden. Sie treten zumeist ohne ausreichender Vorwarnzeit auf. Beeinträchtigungen kritischer Prozesse von Infrastruktursystemen können weitreichende soziale und ökonomische Folgen nach sich ziehen. Daher sind Vorkehrungen zu Abwendung der Bedrohung zu treffen. Damit die Schutzmaßnahmen für alle Stakeholder optimal umgesetzt werden können, ist ein kooperatives Handeln von den staatlichen Institutionen mit den Betreiber*innen der Infrastruktureinrichtungen notwendig. (vgl. BVT 2014: 1)

Auf Ebene der Europäischen Union wurden die Bedeutung und Notwendigkeit des Schutzes ihrer Kritischen Infrastruktur erkannt. Eine entsprechende Richtlinie (Richtlinie 2008/114/EG) wurde im Dezember 2008 veröffentlicht. Inhaltlich behandelt sie die Ermittlung und Ausweisung so genannter Europäischer Kritischer Infrastrukturen (EKI). Das sind jene Objekte, Institutionen und Systeme, deren Störung oder Zerstörung erhebliche grenzüberschreitende negative Auswirkungen zur Folge hat. Gemäß Artikel 2 dieser Richtlinie sind davon jene Anlagen und Systeme bzw. auch Teile dieser erfasst, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind. (vgl. Mayer 2020: 26f.)

Der zunehmenden Bedrohung der EKI und ihren Netzwerken aus dem Cyberraum wird mit der Richtlinie (EU) 2016/1148 begegnet. Sie unterscheidet sich von der zuvor genannten EU-Richtlinie insofern, dass unterschiedliche Begrifflichkeiten verwendet werden. Wo in der EKI-RL von Kritischen Infrastrukturen handelt, ist in der NIS-RL von

Betreibern wesentlicher Dienste (BwD) die Rede. Zudem liegt der Fokus der jüngeren Richtlinie deutlicher auf der nationalen Ebene. Schlussendlich erfolgte in der EKI-RL kein Einbezug des Sektors Informations- und Kommunikationstechnologie. (vgl. Mayer 2020: 27)

Eingangs wurde erklärt, worunter Kritische Infrastrukturen verstanden werden. Es folgte die Skizzierung von Bedrohungen dieser Einrichtungen, Anlagen bzw. Systeme. Im nächsten Kapitel werden nun Schutzkonzepte für diese beschrieben.

4. Schutz Kritischer Infrastrukturen

Das Wort Infrastruktur bezeichnet im Zusammenhang mit Kritischer Infrastruktur (KRITIS) nicht ausschließlich Bauwerke wie Gebäude und Verkehrs- bzw. Transportwege. Vielmehr werden darunter auch Anlagen, Systeme oder Netzwerke inklusive Teile derer subsummiert, die eine besondere Bedeutung für gesellschaftliche Funktionen aufweisen. (vgl. Art. 2 lit. a RL 2008/114/EG 2008)

Die Funktionsstörung oder Zerstörung einer oder mehrere KRITIS durch Beschädigung hat weitreichende Folgen für die Gesellschaft. Störungen oder Zerstörungen können durch Naturgefahren, Terrorismus, Kriminalität oder vorsätzliche Handlungen verursacht werden. Die Sicherheit und der Wohlstand der Bevölkerung können dadurch ernsthaft bedroht sein. Diese Bedrohung sind nicht erst in den letzten Jahren aufgetreten. Sie bestehen bereits seit längerer Zeit, weshalb es bereits vor Inkrafttreten der NIS-Richtlinie mehrere Regelungen zur Erhöhung der Abwehrbereitschaft sowie der Steigerung der Resilienz existieren. Mehrere Projekte haben den Schutz Kritischer Infrastrukturen (SKI) und das Mindern der negativen Auswirkungen von Störungen dieser zum Ziel. Die Vulnerabilität dieser Einrichtungen soll durch ein Bündel mit Schutz- und Sicherheitsmaßnahmen gemildert werden. (vgl. APCIP 2015: 4; RL 2008/144/EG 2008)

Unter Schutz werden „*alle Tätigkeiten zur Gewährleistung der Funktionsfähigkeit, der Kontinuität und der Unversehrtheit [K]ritischer Infrastrukturen und zur Abwendung, Minderung oder Neutralisierung einer Bedrohung, eines Risikos oder einer Schwachstelle*“ im Sinne der EU RL 2008/114/EG verstanden (Art. 2 lit. a RL 2008/114/EG 2008).

In Folge werden SKI-Maßnahmen vorgestellt. Ausgang nimmt der Exkurs bei Strategien wie der EU Richtlinie 2008/114/EG über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern. Danach werden die Schwerpunkte des nationalen Österreichischen Programms zum Schutz Kritischer Infrastruktur (APCIP) – Masterplan 2014 behandelt.

4.1. EPCIP

Im Zuge des Kampfes gegen den Terrorismus wurde die Europäische Kommission vom Rat der Europäischen Union mit der Erstellung einer Strategie zum Schutz der Europäischen Kritischen Infrastruktur beauftragt. Nach Ersuchen des Rates der Europäischen Union wurde das Konzept zur Prävention, Vorbereitung und Reaktion auf terroristische Angriffe Namens *European Programme for Critical Infrastructure Protection* (EPCIP) im Jahr 2008 veröffentlicht. Die Umsetzung der Rahmenvorgaben soll dem Schutz von KRITIS dienen und diesen verbessern. (vgl. COM(2006) 786 2006: 2)

Die Implementierung von EPCIP (vgl. COM(2006) 786 2006: 3) folgt sechs Prinzipien. Diese sind:

1. Subsidiarität
2. Komplementarität
3. Vertraulichkeit
4. Kooperation
5. Verhältnismäßigkeit und ein
6. sektorenweiser Ansatz

Mit der aus dem Programm hervorgegangenen EU-Richtlinie 2008/114/EG wird ein Verfahren zur Ermittlung und Ausweisung Europäischer Kritischer Infrastrukturen eingeführt. Laut Artikel zwei der Richtlinie handelt es sich um jene KRITIS deren Störung oder Zerstörung erhebliche Auswirkungen auf mindestens zwei Mitgliedstaaten hätte (Art. 2 lit. b 2008/114/EG 2008). Das besagte Rahmenwerk zeigt Charakterzüge einer Leitlinie. Es wird den EU Mitgliedstaaten Ratschläge gegeben, wie die nationalen Kritischen Infrastrukturen zu identifizieren, Ressourcen bereitzustellen und Strukturen zum Schutz zu schaffen sind (vgl. COM(2006) 786 2006: 3f.). Die Empfehlungen reichen von der Ermittlung welche Infrastrukturen als Europäische Kritische Infrastrukturen anzusehen sind über die Bekanntgabe dieser und Mindestanforderungen für die Erstellung von Sicherheitsplänen. Ferner werden das Berichts- und Meldewesen behandelt. (vgl. Art. 3ff. 2008/114/EG 2008)

Die Richtlinie 2008/114/EG und die NIS-RL scheinen einige Ähnlichkeiten aufzuweisen. Trotzdem unterscheiden sich diese in grundlegenden Punkten voneinander. Während EPCIP von Kritischer Infrastruktur spricht, weist die NIS-RL auf

Betreiber wesentlicher Dienste (BwD) hin. Zudem stellt die Abhängigkeit von IKT-Systemen ein zentrales Auswahlkriterium in der NIS-RL dar. Des Weiteren sind zahlreiche Sektoren, welche in der NIS-RL erfasst sind, nicht im EPCIP enthalten. EPCIP behandelt lediglich die Sektoren Energie mit Strom, Öl und Gar sowie Verkehr inklusive Straßen-, Schienen- und Flugverkehr sowie die Schifffahrt. Zu einer Ausweitung auf weitere Sektoren, wie es in der Richtlinie zur Netz- und Informationssystemsicherheit der Fall ist, erfolgte bislang nicht. Die Richtlinie zum EPCIP hat daher weiterhin neben der NIS-Richtlinie Gültigkeit. (vgl. Art. 4 Z 4 NIS-RL; Mayer 2020: 26f.)

4.2. APCIP

Die Umsetzung von EPCIP erfolgt in Österreich durch den *Austrian Programm for Infrastructure Protection* (APCIP). Das *Österreichische Programm zum Schutz Kritischer Infrastruktur – Masterplan 2014* ist in der Österreichischen Sicherheits-strategie eingebettet. Das Dokument wurde im Jänner 2015 vom Bundeskanzleramt veröffentlicht (vgl. APCIP 2015: 4f.; Mayer 2020: 8f.). Dort ist auch die zentrale Koordination des Schutzes Kritischer Infrastruktur angesiedelt. Sie erfolgt zusammen mit dem Bundesministerium für Inneres sowie unter Einbindung weiterer betroffener Ministerien. (vgl. APCIP 2015: 10)

In Österreich folgt der Schutz Kritischer Infrastruktur (SKI) einem All-hazards-approach. Es gilt die KRITIS vor einem breiten Spektrum potentieller Bedrohungen zu schützen. Diese reichen von technischen und Naturgefahren bis hin zu intentionalen Angriffen oder Störversuchen. Der umfassende Risikoansatz findet sich in den Prinzipien des Masterplans wieder. (vgl. Mayer 2020: 10)

Im Masterplan 2014 zum Schutz der Österreichischen Kritischen Infrastruktur werden leitende Prinzipien für die Umsetzung von Schutzmaßnahmen beschrieben. Wie schon der Name des Masterplans verdeutlicht, handelt es sich dabei um kein Gesetz oder eine Verordnung. Mayer (2020: 9) sieht die staatliche Aufsicht über die Einhaltung der definierten Vorgaben durch ministerielle Weisung gegeben.

Die Prinzipien des Masterplans sind:

1. „Operator based approach“
2. Subsidiarität und Selbstverpflichtung der Unternehmen
3. Komplementarität
4. Vertraulichkeit
5. Kooperation
6. Verhältnismäßigkeit
7. All-hazards-Ansatz

Damit gleichen sie jenen des EPCIP bzw. sind teilweise ident. Der Kern des Masterplans liegt darin, strategische Unternehmen bei der Implementierung einer umfassenden Sicherheitsarchitektur zu unterstützen. (vgl. APCIP 2015: 8)

Den Bundesländern kommen im Rahmen des Subsidiaritätsprinzips gewisse Kompetenzen zu. Von ihnen ist jeweils eine zuständige Stelle betreffend Umsetzung und Zusammenarbeit mit der Polizei zu benennen. Hinzu kommen Steuerungsaufgaben, die Ausweisung der Kritischen Infrastruktur im Bundesland und die Beratung von diesen, soweit sie in den Zuständigkeitsbereich der Länder fallen. (vgl. APCIPL 2016: 6)

Die Bundesländer werden in der gesamtstaatlichen Risikoanalyse eingebunden. Vom Bund erstelle operative Analysen können als Grundlage für die eigenen Risikoanalysen herangezogen werden. Die identifizierten Betreiberorganisationen sind beim Etablieren einer Sicherheitsarchitektur zu unterstützen. Beispielsweise wird der Leitfaden „*Sicherheit in Unternehmen mit strategischer Bedeutung für Österreich*“ von den Bundeländern zur Verfügung gestellt. (vgl. APCIPL 2016: 8)

4.3. NIS-Richtlinie, -Gesetz, -Verordnung

Strategien als solches weisen keine rechtliche Verbindlichkeit auf. Häufig nennen sie Ziele ohne deren Erreichung explizit zu definieren. Gleichfalls bieten Strategien keine Sanktionsmöglichkeiten bei Abweichungen von den Vorstellungen oder Vorgaben. Rechtsnormen sind hingegen bei der Formulierung eines gewollten Zustands oder Verhaltens konkreter. Der direktive oder vielmehr dogmatische Charakter äußert sich durch Strafandrohungen bei Abweichungen von der Rechtsvorschrift. (vgl. Gießе 1962: 17f.; Auer 2018: 18) Es wird damit eine gewisse Verbindlichkeit geschaffen.

Mit der *EU-Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union* soll ein hohes Sicherheitsniveau von Netz- und Informationssystemen der Mitgliedsstaaten etabliert und gewährleistet werden. Damit wird die Steigerung der Resilienz der EU mit ihren Mitgliedstaaten gegenüber Bedrohungen beabsichtigt. Von der Republik Österreich wurde die Richtlinie (EU) 2016/1148 des Europäischen Parlament und des Rates in nationales Recht übertragen. Das Österreichische NIS-Gesetz wird durch eine NIS-Verordnung weiter präzisiert. (vgl. Erläuterungen-NISG 2018: 1ff.)

Netz- und Informationssysteme mit den zugehörigen Diensten spielen eine zentrale Rolle in der heutigen Gesellschaft. Sie sind für Gesellschaft sowie für wirtschaftliche und gesellschaftlichen Tätigkeiten und insbesondere für den Binnenmarkt wichtig. Für wirtschaftliche und gesellschaftliche Tätigkeiten ist es daher von entscheidender Bedeutung, dass sie verlässlich und sicher sind. Die Tragweite, Häufigkeit und Auswirkungen von Sicherheitsvorfällen nehmen zu und stellen eine erhebliche Bedrohung für den störungsfreien Betrieb von ihnen dar. Insbesondere die Gefahr durch Cyberangriffe ist rapide gestiegen. Auch die Anzahl an Systemfehlern die zu erheblichen Störungen führten nimmt stetig zu. (vgl. Erläuterungen-NISG 2018: 1ff.)

4.3.1. NIS-Richtlinie

Am 8. August 2016 ist die Richtlinie (EU) 2016/1148 in Kraft getreten. Mit dieser *Richtlinie des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union* (im Folgenden: NIS-RL), soll EU-weit ein hohes Sicherheitsniveau der Netz- und Informationssysteme erreicht werden. Sie bezweckt die stärkere Zusammenarbeit der einzelnen Mitgliedsstaaten in strategischer und operationaler Hinsicht. (Erläuterungen-NISG 2018: 1)

Die *Richtlinie (EU) 2016/1148 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union* bezweckt das verlässliche und sichere Funktionieren von Netz- und Informationssysteme mit den zugehörigen Diensten. (vgl. Mayer 2020: 2ff.)

Bereits mit dem einleitenden Absatz werden der Schwerpunkt dieser Vorschrift und der Unterschied zur davor beschriebenen Richtlinie 2008/114/EG deutlich. Kritische Infrastrukturen nutzen Netz- und Informationssysteme. Durch den sicheren Betrieb der IKT-Systeme wird folglich auch eine verbesserte Resilienz von KRITIS erreicht.

Ein weiterer augenscheinlicher Unterschied ist die Umsetzung der Richtlinie in Österreich. Die Richtlinie über die Ermittlung und Ausweisung *Europäischer Kritischer Infrastrukturen* (EKI) und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern wurde mit in das *Austrian Programm for Infrastructure Protection – APCIP* in die Österreichische Sicherheitsstrategie übernommen. Die NIS-Richtlinie sollte nicht nur in einer nationalen Strategie für die Sicherheit von Netz- und Informationssysteme münden. Sie musste bis zum Jahr 2018 in nationales Recht übernommen werden und führte daher zu einem Bundesgesetz, dem NISG.

In Anhang II der Richtlinie werden einzelne Sektoren aufgezählt, welche nach Ansicht des Europäischen Parlaments und des Rates wesentliche Dienste für die Gesellschaft in Europa erbringen. Die Angaben durch die Untergliederung in Teilsektoren weiter präzisiert. (vgl. ebenda)

Neben den Sektoren Energie und Verkehr die bereits in der Richtlinie 2008/114/EG genannt wurden finden sich weitere, für die Gesellschaft bedeutsame, Bereiche in der

Aufzählung. An dritter Stelle ist das Bankwesen, gefolgt von der Finanzmarktinfrastruktur erfasst. Die Plätze fünf und sechs nehmen das Gesundheitswesen und die Lieferung bzw. Versorgung mit Trinkwasser ein. An letzter Stelle befindet sich die Digitale Infrastruktur. (vgl. ebenda)

Um diese Sektoren vor Schädigungen zu schützen sind von den nationalen Behörden sogenannte *Computer Security Incident Response Teams* (CIRTs) zu etablieren. Diese Computer Sicherheitsvorfall-Eingreifteams mit den notwendigen Ressourcen auszustatten damit sie den Aufgaben nachkommen können fällt ebenfalls in den Zuständigkeitsbereich der einzelnen Nationalstaaten. Die Anforderungen an CIRTs und die Aufgaben sind in Anhang I der NIS-RL beschrieben. (vgl. ebenda Anhang I)

Eigentumsverhältnisse der Kritischen Infrastrukturen stellen kein bestimmendes Kriterium für die Auswahl von Betreiberorganisationen wesentlicher Dienst dar. Es kann sich sowohl um öffentliche als auch private Einrichtungen handeln. Maßgeblich sind Schwellwerte für die Versorgungsleistung und die Abhängigkeit von IT-Systemen.

In der Richtlinie sind unter Anhang II (Teil-)Sektoren aufgelistet. Tabelle 4 auf den Seiten 31 und 32 zeigt diese Kategorien von Kritischen Infrastrukturen. Des Weiteren sind die einzelnen Arten von Einrichtungen, welche zu den jeweiligen Sektoren und Teilsektoren gezählt werden, angeführt.

Tabelle 4: Teilsektoren der NIS-RL (Quelle: NIS-RL Anhang II)

Sektor	Teilsektor	Art der Einrichtung
Energie	Elektrizität	Elektrizitätsunternehmen
		Verteilernetzbetreiber
		Übertragungsnetzbetreiber
	Erdöl	Betreiber von Erdöl-Fernleitungen
		Betreiber von Anlagen zur Produktion, Raffination und Aufbereitung von Erdöl sowie Betreiber von Erdöllagern und Erdöl-Fernleitungen
	Erdgas	Versorgungsunternehmen
		Verteilernetzbetreiber
		Fernleitungsnetzbetreiber

		Betreiber von Speicheranlagen
		Betreiber von LNG-Anlagen
		Erdgasunternehmen
Verkehr	Luftverkehr	Luftfahrtunternehmen
		Flughafenleitungsorgane
		Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen
	Schienenverkehr	Infrastrukturbetreiber
		Eisenbahnunternehmen
	Schifffahrt	Passagier- und Frachtbeförderungsunternehmen
		Leitungsorgane von Häfen
		Betreiber von Schiffverkehrsdiensten
	Straßenverkehr	Straßenverkehrsbehörden
		Betreiber intelligenter Verkehrssysteme
Bankwesen		Kreditinstitute
Finanzmarkt-infrastruktur		Betreiber von Handelsplätzen
		Zentrale Gegenparteien
Gesundheitswesen	Einrichtungen der medizinischen Versorgung (inkl. Krankenanstalten)	Gesundheitsdienstleister
Trinkwasserlieferung und -versorgung		Lieferant*innen von und Unternehmen der Versorgung mit „Wasser für menschlichen Gebrauch“
Digitale Infrastruktur		IXPs
		DNS-Dienstanbieter
		TLS-Name-Registries

Gemäß Art. 7 NIS-RL hat jeder Mitgliedstaat eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen festzulegen. Folgende Bereiche soll solch eine nationale Cybersicherheitsstrategie beinhalten:

a) die Ziele und Prioritäten der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen;

b) ein Steuerungsrahmen zur Erreichung der Ziele und Prioritäten der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen, einschließlich der Aufgaben und Zuständigkeiten der staatlichen Stellen und der anderen einschlägigen Akteure;

c) die Bestimmung von Maßnahmen zur Abwehrbereitschaft, Reaktion und Wiederherstellung, einschließlich der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor;

d) eine Aufstellung der Ausbildungs-, Aufklärungs- und Schulungsprogramme im Zusammenhang mit der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen;

e) eine Angabe der Forschungs- und Entwicklungspläne im Zusammenhang mit der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen;

f) ein Risikobewertungsplan zur Bestimmung von Risiken;

g) eine Liste der verschiedenen Akteure, die an der Umsetzung der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen beteiligt sind.

4.3.2. NIS-Gesetz

Kritische Infrastrukturen sehen sich einer großen Anzahl an Bedrohungen gegenüber. Gleichzeitig ist der Schutz vor negativen Folgen von Vorfällen gerade bei Kritischen Infrastrukturen von großem Interesse und Wichtigkeit für die Gesellschaft. Staatliche Einrichtungen wie das Innen- und Verteidigungsministerium sind mit dem Schutz betraut. (vgl. Mayer 2020: 20ff.)

Angriffe können nicht gänzlich ausgeschlossen werden. Daher sind Vorkehrungen zu Abwendung der Bedrohung zu treffen. Damit die Schutzmaßnahmen für alle Stakeholder optimal umgesetzt werden können, ist ein kooperatives Handeln von den

staatlichen Institutionen mit den Betreiber*innen der Infrastruktureinrichtungen notwendig. (BVT 2014: 1)

Von der Europäischen Union wurde die Bedeutung und Notwendigkeit des Schutzes ihrer Kritischen Infrastruktur erkannt und dazu die Richtlinie 2008/114/EG im Dezember 2008 veröffentlicht. Sie behandelt die Ermittlung und Ausweisung so genannter Europäischer Kritischer Infrastrukturen (EKI). Das sind jene Objekte, Institutionen und Systeme, deren Störung oder Zerstörung erhebliche grenzüberschreitende negative Auswirkungen zur Folge hat. Gemäß Artikel 2 dieser Richtlinie sind davon jene Anlagen und Systeme bzw. auch Teile davon erfasst, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind. (vgl. Mayer 2020: 26f.)

Mit der Richtlinie (EU) 2016/1148 wird der zunehmenden Bedrohung der EKI und ihren Netzwerken aus dem Cyberraum begegnet. Sie unterscheidet sich von der zuvor genannten EU-Richtlinie 2008/114/EG dadurch, dass unterschiedliche Begrifflichkeiten verwendet werden. In der EKI-RL werden Kritische Infrastrukturen behandelt, wohingegen in der NIS-RL von Betreibern wesentlicher Dienste (BwD) die Rede ist. Zudem liegt der Fokus der jüngeren Richtlinie weniger auf der transnationalen europäischen Ebene. Den Nationalstaaten wird mehr Kompetenz in der Ausweisung der betroffenen Dienste zugebilligt. Schlussendlich erfolgte in der EKI-RL kein Einbezug des Sektors Informations- und Kommunikationstechnologie. (vgl. Mayer 2020: 27)

Das Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG) übernimmt die NIS-RL des Europäischen Parlaments und des Rates in nationales Recht. Die Vorschriften fallen zum überwiegenden Teil in die Gesetzgebungs- und Vollziehungszuständigkeit des Bundes. Der sachliche Anwendungsbereich wird in § 2 des NISG festgelegt. (vgl. § 2 NISG) Die eben unter dem vorangegangenen Punkt 4.3.1 vorgestellten Sektoren finden sich hier wieder.

Der zweite Abschnitt des Bundesgesetzes regelt die Zuständigkeiten des Bundeskanzlers*der Bundeskanzlerin sowie des Bundesministers*der Bundesministerin für Inneres. Während ersterem*ersteren die strategischen Aufgaben

zukommen, ist der*die Innenminister*in für eine Fülle von operativen Agenden zuständig. (vgl. §§ 4 und 5 NISG)

Des Weiteren wird die Errichtung einer zentralen Anlaufstelle (*Single Point Of Contact* – SPOC) zur Entgegennahme und Weitergabe von Informationen zur Sicherheit von Netz- und Informationssystemen vorgeschrieben. Einlangende Meldungen werden von dort an andere Mitgliedsstaaten oder Computer-Notfallteams weitergegeben. Dem SPOC kommt bei der Koordinierung eine wichtige Funktion als Informationsdrehscheibe bei Cyberkrisen zu. Die zentrale Anlaufstelle dient der Gewährleistung und Erleichterung der grenzüberschreitenden Zusammenarbeit und Kommunikation zwischen den Mitgliedstaaten der Europäischen Union im Bereich der Sicherheit von Netz- und Informationssystemen. (vgl. § 6 NISG; Erläuterung-NISG 2018: 8f.)

Innerhalb der eigenen staatlichen Behörden sind die operativen Strukturen für Cybernotfälle und -krisen einzurichten. Mehrere Bundesministerien bilden gemeinsam den Inneren Kreis der operativen Koordinierungsstruktur (IKDOK). Neben dem Bundesministerium für Inneres (BMI) zählen das Bundesministerium für Landesverteidigung (BMLV) und das Bundeministerium für Europa, Integration und Äußeres (BMEIA) dazu. Im Bereich der Cyberverteidigung handelt es sich beim BMLV um einen wesentlichen Akteur. (Erläuterung-NISG 2018: 8f.) Das Vorliegen einer Cyberkrise wird durch die/den Bundesminister*in für Inneres festgestellt. Dabei gilt es abzuklären, ob bei einer vorhandenen schweren Anomalie im Cyberraum die Voraussetzungen einer Cyberkrise im Sinne des § 3 Z 22 NISG vorliegen und ruft diese gegebenenfalls aus. Zur Entscheidungsfindung kommt einem interministeriell besetzten Gremium, dem Koordinationsausschuss, eine beratende Funktion zu (vgl. § 25 NISG).

Zur Erörterung und Vervollständigung eines gesamtheitlichen Lagebilds wird ein äußerer Kreis mit der Bezeichnung OpKoord gebildet. Hierzu werden Computer-Notfallteams einbezogen und gegebenenfalls Vertreter*innen der Bundesländer eingebunden. (vgl. § 3 Z 5 NISG; Erläuterung-NISG 2018: 9)

Während der*dem Bundeskanzler*in im Rahmen der strategischen Kompetenzen die Ermittlung von BwD zufällt, obliegt der*dem Bundesminister*in für Inneres die Überprüfung der Sicherheitsmaßnahmen der identifizierten Betreiberorganisationen.

In regelmäßigen Intervallen von längstens drei Jahren haben BwD gemäß § 17 NISG einen Nachweis über NIS-konforme Sicherheitsvorkehrungen zu erbringen.

Zu diesem Zweck bedient sich die*der Bundesminister*in sogenannter Qualifizierter Stellen (QuaSte). Erfordernisse, die eine qualifizierte Stelle zu erfüllen hat, werden per Verordnung des Bundesministers*der Bundesministerin für Inneres im Einvernehmen mit der*dem Bundeskanzler*in festgelegt.

Ergänzende Präzisierungen zum NISG finden sich in der *Verordnung des Bundesministers für EU, Kunst, Kultur und Medien zur Festlegung von Sicherheitsvorkehrungen und näheren Regelungen zu den Sektoren sowie zu Sicherheitsvorfällen nach dem Netz- und Informationssystemsicherheitsgesetz* oder kurz Netz- und Informationssystemsicherheitsverordnung (NISV). Diese wird nachfolgend vorgestellt.

4.3.3. NIS-Verordnung

Die NISV wurde von dem Bundesminister für EU, Kunst, Kultur und Medien im Einvernehmen mit dem Bundesminister für Inneres erlassen. Sie dient der Begriffsbestimmung der wesentlichen Dienste und von Sicherheitsvorfällen. Im zweiten Abschnitt werden meldepflichtige Vorfälle anhand von Grenzwerten reglementiert (vgl. §§ 4ff. NISV). Beispielhaft wird hier auf den Sektor Gesundheitswesen des § 8 NISV eingegangen.

Als Betreiber eines wesentlichen Dienstes werden solche angesehen, die für die Aufrechterhaltung des öffentlichen Gesundheitsdienstes im Sinne des § 16 Abs. 2 NISG Leistungen erbringen. Dabei handelt es sich gemäß Zahl 1 um die medizinische Versorgung in den Bereichen Diagnose, Therapie und Pflege als akutstationäre Versorgung oder akutambulante ärztliche Versorgung in einer Spitalsambulanz durch Krankenanstalten. Der Grenzwert liegt bei zwei Betten je 1.000 Einwohner*innen in Bundesländern mit großem Einzugsgebiet und drei Betten je 1.000 Einwohner*innen in allen übrigen Versorgungsregionen (vgl. § 8 Abs. 1 Z 1 lit. a und b NISV). Außerdem wird in Absatz 2 des Paragraphen der Betrieb einer Rettungsleitstelle zu den wesentlichen Diensten gerechnet. Hierbei sind in der NISV keine Richtwerte angeführt.

Ein meldepflichtiger Sicherheitsvorfall liegt gemäß dieser Verordnung vor, wenn der Dienst für mehr als drei Stunden ausfällt oder auch nur eingeschränkt verfügbar ist.

Angaben zu den Einschränkungen des Dienstes sind in der Verordnung nicht näher spezifiziert.

Am Ende der Verordnung befindet sich eine Anlage mit elf Sicherheitsmaßnahmen. Sie dienen den BwD zur Orientierung und Unterstützung beim Aufbau und der Implementierung und Betreiben eines Informationssicherheitsmanagementsystems (ISMS) um ein hohes Schutzniveau zu erzielen. Es handelt sich um:

1. Governance und Risikomanagement
2. Umgang mit Dienstleister*innen, Lieferant*innen und Dritten
3. Sicherheitsarchitektur
4. Systemadministration
5. Identitäts- und Zugriffsmanagement
6. Systemwartung und Betrieb
7. Physische Sicherheit
8. Erkennen von Vorfällen
9. Bewältigung von Vorfällen
10. Betriebskontinuität
11. Krisenmanagement

Die Detailbeschreibung der einzelnen Punkte liefert die Tabelle des nächsten Unterkapitels.

4.3.4. Sicherheitsmaßnahmen

Betreiber*innen wesentlicher Dienste sollen ein hohes Schutzniveau ihrer IKT-Systeme aufweisen. In der NISV sind mehrere Kategorien von sicherheitsrelevanten Aspekten angeführt.

Der Aktionsradius reicht von der Risikoanalyse bis hin zu Konzepten für die Bewältigung von Vorfällen. Eine proaktive Auseinandersetzung mit Gefahren und das Setzen von präventiven Handlungen sollen die Eintrittswahrscheinlichkeit reduzieren. Möglichkeiten zur Erkennung von Ereignissen sollen die Reaktionsfähigkeit erhöhen und den frühzeitigen Start von Gegenmaßnahmen fördern. Vorgänge und Pläne für Notfälle dienen der Sicherstellung der Betriebskontinuität bzw. Aufrechterhaltung von Kernprozessen im Zusammenhang mit dem wesentlichen Dienst.

Tabelle 5 zeigt die einzelnen Maßnahmenpakte zur Erhöhung und Gewährleistung eines hohen Schutzniveaus für Netz- und Informationssysteme.

Tabelle 5: Sicherheitsmaßnahmen gem. NISV (Quelle: NISV Anlage 1)

Sicherheitsmaßnahmen gem. NISV	
1.	**Governance und Risikomanagement**
1.1	Eine Risikoanalyse der Netz- und Informationssysteme ist durchzuführen. Spezifische Risiken müssen ermittelt werden.
1.2	Eine Sicherheitsrichtlinie ist zu erstellen. Diese muss periodisch aktualisiert werden.
1.3	Ein Überprüfungsplan für die periodische Kontrolle der NIS-Sicherheit ist festzulegen.
1.4	Die erforderlichen Ressourcen für ein funktionstüchtiges NIS sind einzuplanen und bereitzustellen.
1.5	Periodische Kontrollen des ISMS sind zu planen und durchzuführen.
1.6	In den Prozessen des Personalwesens sind sicherheitsrelevante Aspekte zu berücksichtigen und umzusetzen.
2.	**Umgang mit Dienstleistern, Lieferanten und Dritten**
2.1	Anforderungen an die drei genannten Gruppen sind festzulegen und regelmäßig zu überprüfen.
2.2	Leistungsvereinbarungen mit Dienstleistern und Lieferanten sind periodisch zu überprüfen und zu überwachen.
3.	**Sicherheitsarchitektur**
3.1	NIS sind sicher zu konfigurieren. Sie ist strukturiert zu dokumentieren. Diese Dokumentation muss aktuell sein.
3.2	Vermögenswerte im Zusammenhang mit NIS sind strukturiert zu analysieren und zu dokumentieren.
3.3	Netzwerke des NIS sollen abhängig vom Schutzbedarf segmentiert werden.
3.4	An den Schnittstellen zwischen den Netzwerksegmenten und innerhalb dieser ist die Sicherheit zu gewährleisten.
3.5	Durch den Einsatz kryptographischer Verfahren sind die drei Schutzziele der Informationssicherheit sicherzustellen

4.	**Systemadministration**
4.1	Administrative Zugriffsrechte sind nach einem Minimalprinzip zu vergeben. Die Vergabe ist periodisch zu überprüfen und gegebenenfalls anzupassen.
4.2	Die Sicherheit von Systemen und Anwendungen zur Systemadministration ist zu gewährleisten und nur zu dem Zweck zu verwenden.
5.	**Identitäts- und Zugriffsmanagement**
5.1	Verfahren und Technologien sollen die Identifikation und Authentifikation von Nutzer*innen und Diensten gewährleisten.
5.2	Unauthorisierte Zugriffe sind durch geeignete Verfahren und Technologien zu unterbinden.
6.	**Systemwartung**
6.1	Eine periodische Überprüfung von Abläufen und Vorgängen soll die Betriebssicherheit von NIS gewährleisten.
6.2	Fernzugriffe sind einzuschränken und zeitlich begrenz zu vergeben. Diesbezügliche Rechte sind periodisch zu überprüfen.
7.	**Physische Sicherheit**
7.1	Der Schutz von NIS hat durch physische Schutzmaßnahmen zu erfolgen. Das Verhindern unbefugter Zutritte ist sicherzustellen.
8.	**Erkennen von Vorfällen**
8.1	Damit Vorfälle bemerkt werden sind geeignete Mechanismen einzuführen und diese zu bewerten.
8.2	Mechanismen zu Protokollierung, insbesondere von essenziellen Vorgängen und Tätigkeiten zur Erbringung des wesentlichen Dienstes sind umzusetzen.
8.3	Mechanismen zur Erkennung von Vorfällen mitsamt deren Bewertung auf Basis von Analysen sind umzusetzen.
9.	**Bewältigung von Vorfällen**
9.1	Prozesse zur Reaktion auf Vorfälle sind zu erstellen, aufrechtzuerhalten und zu erproben.
9.2	Prozesse für die interne und externe Meldung von Vorfällen sind zu erstellen, aufrechtzuerhalten und zu erproben.
9.3	Vorfälle sollen analysiert und bewertet werden und relevante Informationen sind zu Prozessoptimierung zu sammeln.

10.	**Betriebskontinuität**
10.1	Die Wiederherstellung des wesentlichen Dienstes auf einem festgelegten Qualitätsniveau muss nach Sicherheitsvorfällen gewährleistet sein.
10.2	Notfallpläne sind zu erstellen, anzuwenden, zu evaluieren und zu erproben.
11.	**Krisenmanagement**
11.1	Prozesse zur Aufrechterhaltung wesentlicher Dienste vor und bei Sicherheitsvorfällen müssen implementiert, trainiert und erprobt sein.

Durch die Umsetzung der aufgelisteten Themen innerhalb der Kritischen Infrastruktur ist eine hohe Widerstandsfähigkeit gegenüber Cyberangriffen und anderen Bedrohungen zu erreichen.

Im nächsten Kapitel werden verschiedene Eskalationsstufen des Szenarios Stromausfall beschrieben. Unterbrechungen der Stromversorgung stellen eine gravierende Gefahr für IKT-Systeme dar. Deren Auswirkungen und Präventionsmaßnahmen zur Milderung der Folgen werden in Kapitel 5 näher betrachtet.

5. Stromversorgungsstörung

Die Bedeutung eines sicheren und stabilen Stromnetzwerks wurde eingangs erläutert. Damit ein Energienetzwerk konstant und zuverlässig mit einer Frequenz von 50 Hertz funktioniert, ist eine Balance zwischen der Energieproduktion und dem Energieverbrauch notwendig. Ein Ungleichgewicht führt zu Spannungs- oder Frequenzabfall und resultiert in einem Störfall. (vgl. Kröger 2016: 8)

Stromausfälle können mannigfaltige Ursachen aufweisen. Die OSZE zählte im Zeitraum von Jahr 2000 bis 2015 etwa 20 große Stromausfälle (vgl. Kröger 2016: 9). Netzwerkstörungen, Systemfehler oder Naturgefahren sind Beispiele für deren Ursache. Energie und insbesondere der elektrische Strom übernehmen, bedingt durch den verstärkten Einsatz von Elektrizität, eine wichtige Rolle im Alltag. Ein Stromausfall kann durch zahlreiche Gründe ausgelöst werden. (vgl. Kröger 2016: 7ff.; Ladinig und Saurugg 2012: 36f.; Lorenz 2010: 12f.) Infolge kaskadenartige Verbreitung führt dies zu weiteren Ausfällen und eskaliert schließlich zu einer Katastrophe. Einem Blackout. (vgl. ebenda)

Krankenanstalten sind gegen Stromversorgungsunterbrechungen mit gesetzlich vorgeschriebenen Notstromaggregaten abgesichert (vgl. StRH 2010: 4ff.). Rettungsdienste verfügen ebenfalls über solche Vorkehrungen gegen Stromunterbrechungen (vgl. § 21 Abs. 3 WRKG). Dauert die Unterbrechung mehrere Tage und geht diese einher mit Störungen anderer Kritischer Infrastrukturen, sind auch Krankenanstalten in einem hohen Maße vulnerabel.

In den nächsten Unterabschnitten erfolgt die Differenzierung der Begriffe Stromausfall, Strommangellage und Blackout. Zudem werden die daraus resultierenden Folgen sowie Schutz- und Präventionsmaßnahmen dargelegt.

5.1. Stromausfall

In Österreich wurde der Energiemarkt in den Jahren 2001 und 2002 liberalisiert. Den Wettbewerb unter verschiedenen Anbietern von Elektrizität und Erdgas beaufsichtigt eine Regulierungsbehörde, die E-Control. Dadurch soll sowohl der Wettbewerb als auch die Versorgungssicherheit gewährleistet werden. Bei dem, 2001 als Energie-Control GmbH gegründeten, Regulator handelt es sich seit 2011 um eine Anstalt öffentlichen Rechts. Die Zuständigkeiten und Aufgaben sind im Bundesgesetz über die

Regulierungsbehörde in der Elektrizitäts- und Erdgaswirtschaft, auch Energie-Control-Gesetz oder E-ControlG, festgelegt. (vgl. §§ 2 ff. E-ControlG)

Sowohl die E-Control als auch der Bundesrechnungshof als unabhängige Prüfinstanz für die Republik Österreich attestieren eine sehr gute Verfügbarkeit und Versorgungszuverlässigkeit des elektrischen Stroms in Österreich. Europaweit zählt Österreich zu den Staaten mit der geringsten Stromversorgungsunterbrechung (vgl. BRH 2007: 4). Der diesbezügliche Bericht aus dem Jahr 2007 hat nach 15 Jahren noch immer Gültigkeit. Der Energiesektor betreibt viele Anstrengungen um Unterbrechungen der Stromversorgung gering und kurz zu halten. (vgl. APG 2020: 9; E-Control 2021: 10)

Nicht jeder Stromausfall bedeutet, dass es sich um einen Blackout handelt. In der gegenständigen Abhandlung wird ein Stromausfall als örtlich und zeitlich begrenzte Unterbrechung der Stromversorgung verstanden. Störfälle dieser Art treten relativ häufig auf. Die Auswirkungen eines solchen Szenarios sind für gewöhnlich gering. Diese Ausfälle beschränken sich auf ein Gebiet und die Ursachen können schnell beseitigt werden. Die nachfolgende Abbildung 3 zeigt die Länge der Versorgungsunterbrechung je Stromverbraucher*in in Österreich in den Jahren von 2005 bis 2020. Seit 2014 dauern Stromunterbrechungen konstant weniger als eine halbe Stunde. Im Jahr 2020 betrug der Durchschnittswert von Stromversorgungsunterbrechungen in Österreich rund 27 Minuten je Verbraucher*in. (vgl. E-Control 2021: 16)

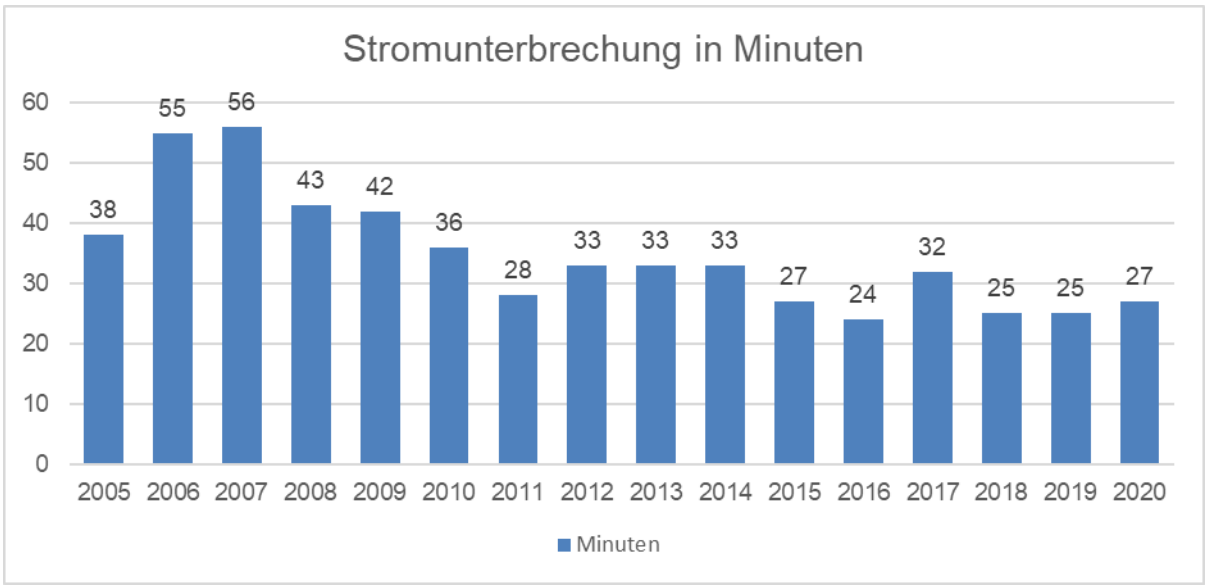

Abbildung 3: Stromunterbrechungen 2005-2020 (Quelle: E-Control 2021: 16)

Der E-Control wurden für das Jahr 2020 insgesamt 18.850 Versorgungsunterbrechungen gemeldet, die länger als eine Sekunde gedauert haben. Etwas mehr als 60% entfielen auf ungeplante Versorgungsunterbrechungen. Diese traten in Zusammenhang mit Anlagenausfällen, anderen Störungen oder äußeren Einflüssen auf. (vgl. E-Control 2021: 9ff.)

Welche Auswirkungen ein Stromausfall in einem Krankenhaus verursachen kann wird in der nächsten Tabelle 6 exemplarisch aufgezeigt. Durch die Vorhaltung einer Notstromversorgung können anfangs die meisten Aufgaben in der Klinik unbeeinträchtigt weitergeführt werden. Zu gewissen Einschränkungen kommt es im organisatorischen Bereich durch den Ausfall von IKT-Strukturen sowie bei der Diagnostik. (vgl. Breuer et al. 2021: 507f.)

Im Zeitraum von zwei bis acht Stunden nimmt die Behinderung von Büroabläufen zu. Zudem ist die ordnungsgemäße Lagerung mancher Arzneimittel und Medizinprodukte gefährdet. (vgl. ebenda)

Ab acht Stunden ohne externe Stromversorgung muss das Angebot der medizinischen Versorgung reduziert werden. Gleichzeitig steigt die Anzahl an Selbsteinweisungen. Notspitäler sollen die Krankenanstalt entlasten. Zusätzlich werden Leichtverletzte und Genesene vorzeitig aus der stationären Behandlung in die extramurale Versorgung entlassen. Die Dokumentation und Administration von Patient*innen erfolgt zu diesem Zeitpunkt ausschließlich manuell. Die Versorgung mit Lebensmitteln ist gestört und führt bei der Betreuung der anstaltspflichtigen Personen und bei der Belegschaft zu Problemen. (vgl. ebenda)

Dauert ein Stromausfall mehrere Tage kommt es zu Engpässen bei Blutprodukten, Medikamenten und Spezialnahrung. Die Lage wird durch problematische Hygienebedingungen verschärft. (vgl. ebenda)

Tabelle 6: Chronologie Stromausfall (Quelle: Datengrundlage Breuer et al. 2021: 507)

Chronologie der Beeinträchtigungen für Krankenanstalten im Falle eines Stromausfalls	
Bis 2 Stunden	Ausfall der IKT-Infrastruktur Organisatorische Beeinträchtigung Apparative Diagnostik eingeschränkt
2 bis 8 Stunden	Ausfall der Bürotätigkeiten Arbeitsabläufe zunehmend behindert Patient*innendaten nicht mehr einsehbar und bearbeitbar Überlastung der Telefonzentrale Korrekte Lagerung von Arzneimitteln und Medizinprodukten gefährdet Küche nicht mehr funktionsfähig Trinkwasserknappheit
8 bis 24 Stunden	Deutliche Beeinträchtigung der medizinischen Versorgung Notwendigkeit der Entlassung von Leichtverletzte/Genesenen Notwendigkeit für die Errichtung von Behelfskrankenhäusern Patient*innendokumentation nur noch manuell Zahl der Selbsteinweisungen steigt Gestörte Speiseversorgung
1 Tag und länger	Engpässe bei der Versorgung mit Blutprodukten, Insulin, Spezialnahrung Einzelne Medikamente knapp Hygienische Probleme aufgrund von beeinträchtigter Entsorgung

5.2. Strommangellage

Mit dem Fachterminus „Strommangellage“ wird ausgedrückt, dass eine uneingeschränkte und ununterbrochene Versorgung mit elektrischer Energie aus dem Stromnetz nicht mehr sichergestellt ist. Versorgungseinschränkungen sind die Folge. Zwischen den Produktionskapazitäten und dem Stromverbrauch ist ein Gleichgewicht herzustellen damit ein Zusammenbruch des Energienetzwerks verhindert werden

kann. Dazu sind Lenkungsmaßnahmen, durch die E-Control als Aufsichtsbehörde notwendig um die Stabilität des Stromnetzes sicherzustellen. Operativ greift die *Austrian Power Grid AG* (APG) regulierend in die Stromverteilung ein. Es erfolgt eine Rationierung bzw. Kontingentierung der Stromabnahme, sodass Endverbraucher*innen, insbesondere Großabnehmer*innen, bewusst vom Stromnetz getrennt werden, damit eine Parität zwischen Erzeugung und Abnahme hergestellt wird. Eine Überlastung des Stromnetzwerks soll durch diese Verbrauchsbeschränkungen vermieden werden. Andernfalls kann das Missverhältnis von Angebot und Nachfrage zu einem ausgedehnten Störfall und durch Kaskadeneffekte zu einem Blackout führen. (vgl. APG 2020: 19f.; BABS 2020: 1)

5.3. Blackout

„*Blackout ist ein Schlüsselszenario. Es besitzt Wechselwirksamkeiten mit anderen lebenswichtigen Infrastrukturen und hat Auswirkungen auf nahezu alle Lebens- und Geschäftsbereiche*.“ (Ladinig und Saurugg 2012: 45)

Unter Blackout wird ein Totalausfall des Stromnetzes verstanden. Einen weiteren zentralen Aspekt des Begriffs stellt die räumliche Ausdehnung dar. Vereinfacht ausgedrückt handelt es sich um eine sehr großflächige, über Staatsgrenzen reichende, und lange, bis zu mehrere Tage, anhaltende Unterbrechung der Stromversorgung. (vgl. Reisner 2021: 335; NÖZSV 2020: 8, Ladinig und Saurugg 2012: 35) Ein Eintritt dieses Ereignisses wird in den kommenden Jahren als nahezu sicher von unterschiedlichen Expert*innen angenommen (vgl. Reisner 2021: 335). Die Ursachen für ein solches Szenario sind mannigfaltig. Als potentielle Ausgangslage werden aktuell extreme Wetterereignisse, technisches Gebrechen, menschliches Fehlverhalten und intentionale Gefahren wie Terroranschläge oder Cyberangriffe erwogen. Ein vollständiger Netzausfall hat zur Folge, dass auch die einzelnen Kraftwerke keinen Strom beziehen können. Diesen benötigen sie in der Mehrzahl allerdings um wieder starten zu können. Lediglich jene Energielieferant*innen, welche keine externe Stromzufuhr benötigen sind dann dazu in der Lage den Betrieb wiederaufzunehmen. (vgl. Saurugg 2021: 330; NÖZSV 2020: 8)

Die Perspektive eines Blackout-Szenarios beschränkt sich nicht ausschließlich auf die Dimension eines großflächigen Stromausfalls. Ein schwerwiegender und länger andauernder Versorgungsausfall, gefolgt von erheblichen Versorgungsengpässen

resultiert daraus. (vgl. Saurugg 2021: 330) Ein Blackout hat somit weitreichende und komplexe Folgen für die gesamte Gesellschaft.

Ein Vorfall dieses Ausmaßes gliedert sich in mehrere Phasen. Saurugg unterscheidet drei Phasen vom initialen Ereignis bis zur vollständigen Wiederherstellung des ursprünglichen Zustands. Die erste Phase eines Blackouts beginnt wenige Stunden nach dem Vorfall auszuwirken. Sie ist dadurch gekennzeichnet, dass für Haushalte, Betriebe und Anlagen ohne Notstromaggregate die Stromversorgung ausfällt. Elektrisches Licht, Heizungen bzw. Klimageräte sowie Informations- und Kommunikationstechnologie aber auch die Behebung von Bargeld am Bankomat stehen dann nicht mehr zur Verfügung. Gekühlte oder gefrorene Lebensmittel tauen und beginnen zu verderben. Ampelanlagen fallen aus. (vgl. Pausch 2017: 21ff.; Saurugg 2021: 330)

Es wird angenommen, dass in dieser Phase die Spitäler zusätzlich mit einer Zunahme von Verletzten konfrontiert sein werden. Der ungeregelte Straßenverkehr führt zu mehr Verkehrsunfällen wodurch dieser völlig zum Erliegen kommt. Außerdem wird mangels adäquater Beleuchtung in den Abend- und Nachtstunden generell die Unfallhäufigkeit steigen. Das sei auf den Mangel adäquater Beleuchtung zurückzuführen. Gleichzeit fehlt es für den Mehrbedarf an Behandlungen an Krankenhauspersonal (vgl. Pausch 2017: 24)

Ab 24 Stunden nach dem Zusammenbruch des Stromnetzwerks setzt die zweite Phase des Blackouts ein. Diese ist durch einen Zusammenbruch der Logistik sowie durch zunehmende Problemen mit der Wasserver- und -entsorgung gekennzeichnet. Einsatz- und Hilfsorganisationen werden bald die Grenzen ihrer Ressourcen erreichen da die Materialreserven schwinden. Die dritte Phase beginnt ab ca. 72 Stunden und manifestiert sich durch eine Verschlechterung der Sicherheitslage, speziell im urbanen Raum. Die Bevorratung mit Treibstoff, Lebensmitteln und anderen Dingen des täglichen Bedarfs ist aufgebraucht. Eine Landflucht setzt ein. (vgl. Pausch 2017: 25ff.; Saurugg 2021: 331f.)

Das Wiederhochfahren der Infrastruktur und die Wiederherstellung der Versorgung wird Saurugg (2021: 330) zufolge eine Zeitspanne von mehreren Wochen bis Monaten in Anspruch nehmen.

Die Abhängigkeit unserer modernen Gesellschaft von elektrischer Energie ist offenkundig. Eine längerfristige Unterversorgung oder ein Ausfall von Strom stellt eine Bedrohung für diese und den Staat als ganzen dar. Das verteidigungspolitische Risikobild der Republik Österreich bewertet die Eintrittswahrscheinlichkeit eines Blackouts in den kommenden Jahren als sehr wahrscheinlich. Auslöser für ein solches Ereignis können Infrastrukturgebrechen sein. (vgl. Saurugg 2021: 335)

Ein Blackout kann jedoch auch eine Folge von einer intentionalen Schädigung sein. In diesem Fall zielt ein Angriff auf die Kritische Infrastruktur ab, um den Staat zu schädigen und zu destabilisieren. In den letzten Jahren kam es wiederholt zu Attacken auf Strombetreiber. Die Invasion der Ukraine durch russische Streitkräfte Anfang 2022 wurde von Cyberangriffen auf Umspannwerke begleitet. (vgl. ISPK 2022: 10; BfV 2022: 1)

In Tabelle 7 werden die einzelnen Aspekte der zuvor beschriebenen Kategorien der Stromunterbrechungen zusammenfassend dargestellt.

Tabelle 7: Übersicht Stromunterbrechungen

	Zeitfaktor	**Räumliche Ausdehnung**	**Anzahl der Betroffenen**
Stromausfall	Einige Minuten bis Stunden	Lokal begrenzt	Wenige
Strommangellage	Einige Tage bis Wochen	Bundesweit	Einige Millionen
Blackout	Mehrere Tage bis Wochen	Europaweit	Mehrere Millionen

Ein Blackout kann durch einen Angriff auf Strombetreiber oder Stromverteilernetze hervorgerufen werden. Anschläge auf Kritische Infrastrukturen zählen mittlerweile zum Standardrepertoire hybrider Konflikte. In vielen Fällen können sie abgewehrt werden. Häufig finden diese Schädigungsversuche im Cyberraum statt. In den letzten Jahren wurde eine Zunahme solcher Sicherheitsvorfälle verzeichnet. (vgl. BKA 2021: 55ff.) Das nächste Subkapitel ist daher der Bedrohung durch Cyberangriffe gewidmet.

6. Cyberkrise

Die heutige Gesellschaft ist durch eine umfassende Vernetzung der Lebensbereiche determiniert. Die Digitalisierung und damit die Verlagerung vieler Lebensbereiche in den virtuellen Raum schreitet schnell voran. Der Ausbau der Digitalisierung führt zu einer positiven gesellschaftlichen und wirtschaftlichen Entwicklung. (vgl. Leopold 2017: 1) „*Energienetze und Wasserpumpen werden über zentrale Server gesteuert, Patientendaten in Krankenhäusern ausschließlich über digitale Systeme verwaltet und Transaktionen mehrheitlich über bargeldlosen Zahlungsverkehr abgewickelt*“ (Mayer 2020: 1).

Viele Erledigungen können auf diese Weise schnell online koordiniert, gesteuert und ausgeführt werden. Diese Annehmlichkeiten bergen auf der anderen Seite auch Risiken in sich. Werte müssen im Cyberraum im selben Ausmaß geschützt werden wie dies in der realen Welt gängige Praxis ist. Cybersicherheit gewinnt zunehmend an Bedeutung. Eine Studie aus 2021 offenbart, dass 60 Prozent der untersuchten Unternehmen zu Opfern von Cyberangriffen wurden. (vgl. BMLV 2022: 206)

In den beiden nachfolgenden Kapiteln werden zunächst Bedrohungen aus dem Cyberraum skizziert und dann Cybernotfälle anhand von Cybersicherheitsvorfällen und Cyberangriffen genauer beschrieben.

6.1. Cyberbedrohungen

Unter Cybersicherheit werden Tätigkeiten verstanden, „*die notwendig sind, um Netz- und Informationssysteme sowie die Nutzer*innen solcher Systeme vor Bedrohungen aus dem Cyberraum zu schützen*“ (ORKB 2020: 10). Dazu zählen die Verhütung, Aufdeckung, Reaktion und die Beseitigung der Folgen von Cybersicherheitsvorfällen. Die Grundsätze der Cyber- und Informationssicherheit sind die Verfügbarkeit, Vertraulichkeit und Integrität von Daten. Diese Werte werden durch verschiedene Risiken bedroht. (vgl. ORKB 2020: 10f.)

Die Auswirkungen könne in der Preisgabe vertraulicher Informationen, der Veränderung, der Zerstörung oder der Zugriffverweigerung (Denial of Service) von Daten liegen. Die nachfolgende Abbildung 4 zeigt einen Überblick der Auswirkungen von unbefugten Zugriffen auf die drei Assets der Informationssicherheit. Die Effekte

der einzelnen Kategorien wirken sich auf die jeweiligen Schutzziele unterschiedlich aus. (vgl. ebenda)

Das Vorhängeschloss symbolisiert die Sicherheit im Angriffsfall wohingegen das Ausrufezeichen deren Gefährdung anzeigt.

Abbildung 4: Bedrohung der Informationssicherheit (Quelle: ORKB 2020: 12)

Im Jahr 2019 wies EUROPOL (2019: 15f.) auf eine Reihe von Cyberbedrohungen hin. Die wirtschaftlichen Auswirkungen von Cybervorfällen sind erheblich. „*Diese Vorfälle können vorsätzlich oder unbeabsichtigt herbeigeführt werden und reichen von der versehentlichen Preisgabe von Informationen bis hin zu Angriffen auf Unternehmen und kritische Infrastrukturen, zum Diebstahl personenbezogener Daten und sogar zu einer Störung demokratischer Prozesse, einschließlich der Einflussnahme auf Wahlen, sowie zu allgemeinen Desinformationskampagnen zur Beeinflussung öffentlicher Debatten*“ (ORKB 2020: 10).

6.2. Cybersicherheitsvorfall

Unter virtuellem bzw. Cyberraum wird das weltweite Verbindungsnetz, das Internet, verstanden. Dieses öffentlich zugängliche Netzwerk ist durch beliebige andere Datennetze erweiterbar (vgl. Mayer 2020: 12). In der Industrie hat sich der Begriff Industrial Internet of Things (IIoT) etabliert. Industrialisierte Prozesse erfordern die Zusammenarbeit mit Einheiten und Umgebungen auf der ganzen Welt auf unterschiedlichen Ebenen und in verschiedenen Systemen, wie sie auch in Kritischen Infrastrukturen verwendet werden. Dieses stark anwachsende Segment verbindet weltweit Milliarden von Gerätschaften miteinander. Das führt zu erheblichen Sicherheitsrisiken, da sie als ein attraktives Ziel für Angriffe aus dem Cyberraum erscheinen. Eine der größten Herausforderungen für eine größere Konnektivität ist die Sicherheit. Die Entwicklung der Komponenten erfolgte dabei ohne besonderen Augenmerk auf Sicherheitsaspekte. (vgl. Bajramovic et al. 2019: 247f.)

Mit der Zunahme an Informations- und Kommunikationssystemen (IKT-Systemen) in der Arbeitswelt hat der Bedarf an Schutzmaßnahmen für diese Systeme gleichermaßen zugenommen. Die Informations- bzw. IKT-Sicherheit nennt drei Schutzziele. Diese sind die Vertraulichkeit, die Integrität und die Verfügbarkeit von Informationen. Diese Werte lassen sich, ob der Verlagerung in den virtuellen Raum, auf den Cyberraum übertragen. Es gilt die selbe Intention. (vgl. BSI 2020: 5ff.; Mayer 2020: 12)

Die aktuelle Österreichische Sicherheitsstrategie erwähnt Cybersicherheit an mehreren Stellen. Angriffe auf die IT-Systeme stellen Herausforderungen, Risiken und Bedrohungen für die Kritischen Infrastrukturen in Österreich dar. Die Kooperation und Zusammenarbeit von Staat und Privaten ist insbesondere bei der Cybersicherheit wesentlich. Einerseits befinden sich zahlreiche Kritische Infrastrukturen in privatem Besitz, andererseits fungieren Private als Hersteller*innen von Soft- und Hardwareelementen, die von Kritischen Infrastrukturen benötigt und genutzt werden. Vorbeugung und Prävention vor Cyberkriminalität zählen genauso dazu wie die Fahndung nach Delikten. (vgl. Mayer 2020: 8ff.)

Cybersicherheitsvorfälle können sich unterschiedlich äußern. Es handelt sich um all jene Vorfälle die eine Verfügbarkeit, die Integrität oder die Vertraulichkeit von Daten aus dem virtuellen Raum beeinträchtigen.

6.3. Cyberangriff

Während des Informationszeitalters hat das Internet Erleichterungen gebracht und die Kommunikation verbessert. Diese Form der Globalisierung hat zu einem verbesserten Lebensstandard in den Entwicklungsländern geführt. Es hat aber auch Personen, Gruppen und Staaten eine neue Waffe im Arsenal beigegeben, die für kriminelle oder kriegerische Machenschaften verwendet wird. (vgl. Herzog 2011: 50). Cyberangriffe weisen eine hohe Wirkasymmetrie auf. Angriffe mit geringem technischen Aufwand und niedrigen Kosten können zu dramatischen Auswirkungen führen. Das gilt umso mehr, wenn das betroffene Ziel zur Kritischen Infrastruktur zählt. Potentielle Folgen eines Stromausfalls wurden bereits im vorangegangenen Abschnitt behandelt. In den letzten Jahren wird der Cyberraum zunehmend für militärische Zwecke genutzt und als Waffe eingesetzt. Er gilt heute neben Land, See, Luft und Weltraum als fünfte Dimension der Kriegsführung. (vgl. ORKB 2020: 34)

Cyberangriff ist ein neuer Ausdruck für eine neue Angriffsform. Dabei kann es sich sowohl um die Bezeichnung für den Angriffsvektor, als auch um das Angriffsziel handeln. Cyberangriffe bezwecken, Systeme zu blockieren oder außer Betrieb zu setzen, Daten zu stehlen bzw. sie zu manipulieren oder auch ein angegriffenes Computersystem zu übernehmen und so für weitere Angriffe zu nutzen. Eine der zahlenmäßig häufigsten Arten von Cyberangriffen sind DDoS-Attacken. Prominente Vertreter der Kategorie sind die Cyberangriffe auf Estland 2007, Georgien 2009 und Stuxnet 2010 (vgl. Werkner und Schörnig 2019: 7f.). Das Österreichische Außenministerium wurde 2016 und 2020 zum Ziel eines solchen Anschlags mit DDoS-Attacke (vgl. BKA 2021: 59).

Wie zuvor gezeigt wurde, eignen sich Cyberattacken für kriegerische Auseinandersetzungen. Im Rahmen einer hybriden Kriegsführung kommen sie seit einigen Jahren zum Einsatz. Die Invasion der Ukraine durch die russische Armee wurde von Cyberangriffen auf die Kritische Infrastruktur der Ukraine begleitet. Der Sicherheitsfirma Eset und dem ukrainischen CERT zufolge wurden von Russland aus Cyberangriffe auf die Strom-Infrastruktur in der Ukraine durchgeführt (vgl. golem.de 2022, online) Reuters berichtet im März 2022 zudem von Angriffen auf die IT-Infrastruktur des staatlichen Telekommunikationsbetreibers Ukrtelecom. Zuvor wurde bereits ein kleineres Telekommunikationsunternehmen der Ukraine attackiert. (vgl. reuters.com 2022, online)

Auch ohne kriegerischen Akts kommt es zu Angriffen von Hacker*innen auf Schwachstellen in den Netzwerken von Kritischen Infrastrukturen. Ein Hacker*innenangriff auf die Universitätsklinik in Düsseldorf hatte weitreichende Folgen für die Versorgung von Patient*innen der Krankenanstalt. Die Cyberattacke führte dazu, dass die Informations- und Kommunikationstechnik ausfiel. Die Notaufnahme musste geschlossen und Operationstermine mussten verschoben bzw. Behandlungstermine abgesagt werden. Dieser Zustand hielt für etwa zwei Wochen an. (Langguth und Pretzell 2020: 1f.)

Welche Auswirkungen eine gestörte IKT-Infrastruktur im Gesundheitswesen zur Folge haben kann, wird im folgenden Kapitel fünf aufgezeigt. Anhand des Behandlungspfades von Notfallpatient*innen, der Rettungskette, werden einzelne Komponenten und deren Rolle beim Zusammenspiel in der Prozesskette vorgestellt.

Abschließend listet Tabelle 8 auf der nächsten Seite Cyberangriffsarten mitsamt einer Übersicht der dazugehörigen Kennzeichen auf.

Tabelle 8: Arten von Cyberangriffen (Quelle: Datengrundlage ORKB 2020: 13)

Angriffsart	Vorgehen und Angriffsziel
Malware	Schadsoftware wie etwa Viren, Trojaner, Ransomware oder Würmer schädigt Geräte, Anwendungen oder Netzwerke.
Ransomware	Daten werden verschlüsselt, sodass Nutzer*innen erst nach Zahlung eines Lösegelds wieder auf diese zugreifen können.
DDoS	Distributed-Denial-of-Service bedeutet, dass durch übermäßige Anfragen wird ein System überlastet wodurch es ausfällt und nicht weiter zur Verfügung steht.
Phishing	Nutzer*innen werden durch vertrauenswürdige E-Mail-Nachrichten zur Preisgabe von Informationen verleitet oder durch Anklicken eines Links erfolgt ein Download von Schadsoftware.
APT	Advanced Persistent Threats sind fortgeschrittene andauernde Bedrohungen. Es werden dabei langfristig Daten ausgespäht, gestohlen und manchmal korrumpiert oder vernichtet.

7. Sektor Gesundheitswesen

Vorliegende Arbeit betrachtet die Auswirkungen der NIS-Gesetzgebung mit Fokus auf den Gesundheitssektor. In diesem Kapitel wird zunächst das Gesundheitswesen in Österreich beschrieben. Darauf aufbauend wird die gesellschaftliche Bedeutung hervorgestrichen und der Konnex zu zwei zentralen Bedrohungsszenarien, Stromausfall und Cybernotfall, hergestellt.

7.1. Gesundheitswesen in Österreich

„*Die Österreichische Gesundheitspolitik folgt dem Leitmotiv, den Zugang zu qualitativ hochwertiger Versorgung für alle gleich und unabhängig von Einkommen, Alter und Geschlecht sicherzustellen*“ (Hofmarcher 2013: XIV). Österreich verfügt über einen hohen Standard in der Medizin und bei der Gesundheitsversorgung, wenngleich auch ein gewisser Verbesserungsbedarf von Hofmarcher (vgl. 2013) attestiert wird.

In einer 2017 veröffentlichten Studie der Universität Washington über den Zugang und die Qualität des Gesundheitssystems erzielte Österreich 88 von 100 Punkten (vgl. Murray 2017: 8ff.). Damit liegt Österreich im Spitzenfeld zusammen mit Frankreich und Belgien. Das Österreichische Gesundheitssystem liegt bei der Platzierung vor Deutschland mit 86 Punkten. Die skandinavischen Länder Norwegen, Schweden und Finnland weisen 90 Punkte aus. Noch besser schnitt das Gesundheitssystem der Schweiz ab. Sie erreichte 92 Punkte und damit Platz 3 im Ranking. Mit 95 Punkten erhielt die Gesundheitsversorgung Andorras die Topplatzierung, gefolgt von Island mit 94 Punkten. Somalia (34 Punkte), Afghanistan (32 Punkte) und die Zentralafrikanische Republik belegen die letzten Plätze beim globalen Ranking. Die Studienergebnisse, wie sie in Tabelle 9 gezeigt werden, wurden in der Fachzeitschrift *The Lancet* (2017) veröffentlicht.

Tabelle 9: Ranking der Gesundheitssysteme (Quelle: Datengrundlage The Lancet 2017: 238ff.)

Platzierung	Staat	Punkte
1	Andorra	95
2	Island	94
3	Schweiz	92
4	Schweden	90
5	Norwegen	90
6	Australien	90
7	Finnland	90
8	Spanien	90
9	Niederlande	90
10	Luxemburg	89
11	Japan	89
12	Italien	89
13	Irland	88
14	Österreich	88
15	Frankreich	88
16	Belgien	88
17	Kanada	88
18	Slowenien	87
19	Griechenland	87
20	Deutschland	86

Der Österreichischen Bevölkerung wird ein einfacher und schneller Zugang zum Gesundheitssystem ermöglicht. Ein Netzwerk aus extra- und intramuraler Gesundheitsdienstleister*innen steht allen zur Verfügung. Die Kranken- und Unfallversicherung stellt die Bezahlung der medizinischen und diagnostischen Leistungen sicher. Hierzu zählen auch die Transportkosten, falls die An- und Rückreisereise zum Behandlungsort nicht selbstständig möglich sein sollte. (vgl. BRH 2020: 19ff.; Hofmarcher 2013: 85f.; Reisinger 2012: 68f.)

Im Falle eines akuten Leidens führen Rettungs- und Krankentransportdienste den Transport der erkrankten bzw. verletzten Person zur nächstgelegenen Gesundheitseinrichtung durch. Der Rettungsdienst wird bei medizinischen Notfällen oder Unfällen über die bundesweit einheitliche Notrufnummer 144 angefordert (vgl. RTR 2022: o.S.; Hofmarcher 2013: 210f.; Reisinger 2012: 10). Sanitätspersonal gewährleistet eine suffiziente medizinische Versorgung am Notfallort und die fachgerechte Betreuung während der Fahrt. Die Übergabe von Patient*innen durch die Rettungskräfte erfolgt in den Kliniken mitsamt einem Übergabegespräch und der Einsatzdokumentation. An das medizinische oder das Pflegepersonal werden dabei wesentliche Informationen über den Gesundheitszustand weitergegeben. So soll eine redundante Anamneseerhebung vermieden werden. Die intramuralen Gesundheitseinrichtungen verfügen über eine umfangreiche Palette an diagnostischen, therapeutischen und pflegerischen Möglichkeiten für die weitere Behandlung des Leidens. Je nach Erfordernis bzw. Ausprägung der Erkrankung oder Verletzung erfolgt die Therapie ambulant oder stationär. (vgl. BRH 2020: 16; BMASGK 2019: 19ff.; Hofmarcher 2013: 210f.)

Die Verpflichtung bei Notfällen, Erste Hilfe zu leisten, ergibt sich indirekt aus § 95 des Österreichischen Strafgesetzbuchs (StGB). Hierin ist unter Absatz 1 festgelegt, dass das Unterlassen einer Hilfeleistung strafbar ist. Eine Ausnahme sieht dieses Bundesgesetz nur in besonderen Fällen, insbesondere dann, wenn Gefahr für Leib oder Leben besteht, vor. (vgl. § 95 StGB) Auf dem Gebiet des Bundeslands Wien besteht eine ausdrückliche Verständigungspflicht bei Gefahren für das Leben oder die Gesundheit. Das Wiener Rettungs- und Krankentransportgesetz (WRKG) verpflichtet in § 27 Absatz 1 dazu, einen Rettungsdienst zu rufen, wenn sonst keine Möglichkeit besteht adäquat Hilfe zu leisten. (vgl. § 27 Abs.1 WRKG)

Bei einem Notfall ist es wichtig, dass so schnell wie möglich Hilfe vor Ort ist. Ein wichtiges Glied in der Rettungskette ist die Alarmierung der richtigen Rettungskräfte. Das Rettungswesen ist von der Bundeskompetenz im Gesundheitswesen ausgenommen. Die Gesetzgebungskompetenz liegt hierbei bei den Bundesländern. Die Organisation fällt in die Zuständigkeit der Gemeinden. Sie haben einen organisierten Rettungsdienst in ihrem Verwaltungsbereich zu schaffen. Dabei sind die erforderliche Qualität und ausreichende Verfügbarkeit zu gewährleisten. Zumeist wird

die Aufgabe an anerkannte Hilfsorganisationen, wie beispielsweise dem Roten Kreuz, übertragen. (vgl. BRH 2020: 7; Achleitner 2015: 2ff.; Reisinger 2012: 5f.)

Der landesgesetzliche Auftrag, das Rettungswesen in der Stadt zu organisieren und durchzuführen, wird von der Magistratsabteilung 70 – Berufsrettung Wien erfüllt. Die Bundeshauptstadt weist mit der Magistratsabteilung 70 (MA 70) eine Besonderheit gegenüber allen anderen Gemeinden in Österreich auf. Der Rettungsdienst wird durch die Stadt selbst erbracht. (vgl. BRH 2020: 16; Reisinger 2012: 27f.)

Von der Rettungsleitstelle der Berufsrettung Wien werden täglich etwa 1.100 Notrufe abgewickelt. Die durchschnittliche Hilfsfrist, von der Notfallmeldung bis zum Eintreffen am Notfallort, beträgt acht bis zwölf Minuten. Um diese Responsezeit zu gewährleisten verfügt die Berufsrettung Wien über zwölf Rettungsstationen sowie sechs Stützpunkte für Notarzteinsatzfahrzeuge im Stadtgebiet. Dort versehen rund 900 hauptberufliche Sanitäter*innen ihren Dienst. Die MA 70 ist damit die größte Rettungsorganisation in der Gemeinde Wien. (vgl. BRH 2020: 26f.; Reisinger 2012: 27f.)

Neben der Magistratsabteilung 70 sind sechs weitere Rettungsdienste in der Bundeshauptstadt tätig. Vier davon sind explizit im Wiener Rettungs- und Krankentransportdienstgesetz (WRKG) genannt. Es handelt sich laut § 34 Abs. 1 WRKG um den Arbeiter-Samariter-Bund Österreichs, die Johanniter-Unfall-Hilfe in Österreich, der Malteser Hospitaldienst Austria und das Österreichische Rote Kreuz (vgl. WRKG). Zusätzlich sind das Grüne Kreuz, welches 2015 vom Roten Kreuz als eigenständige Teilorganisation übernommen wurde, und der Sozialmedizinische Dienst zum Wiener Rettungsverbund hinzugekommen. (vgl. BRH 2020: 37f.)

Die gemeinnützigen privaten Rettungsdienste stellen ihre Rettungsmittel für die Berufsrettung Wien zur Verfügung. Damit wird eine gleichmäßige Auslastung erreicht und punktuelle Spitzen bzw. Ressourcenmangel in Stadtregionen vermieden. Alle Einsatzmittel werden zentral von der Rettungsleitstelle disponiert. (vgl. BRH 2020: 26f.)

7.2. Krankenanstalten in Wien

Insgesamt sind 44 Krankenanstalten bzw. Pflegewohnhäuser und Rehabilitationszentren mit 15.144 systematisierten Betten in der Stadt Wien ansässig. Etwa die Hälfte der Spitalsbetten entfällt auf gemeinnützige Krankenanstalten unter

öffentlicher Verwaltung gemäß §16 Abs. 1 des Krankenanstalten- und Kuranstaltengesetzes (KAKuG). (vgl. Magistrat der Stadt Wien 2021: 106f.)

Von der Stadt Wien sind die kommunalen Krankenanstalten und Pflegewohnhäuser in einer Unternehmung organisatorisch zusammengeschlossen. Die Pflegewohnhäuser und Geriatriezentren sowie das Allgemeine Krankenhaus der Stadt Wien stellen Teilunternehmungen dar. Tabelle 9 zeigt die Kliniken welche von der Stadt Wien verwaltet werden, deren Standort und die Bettenanzahl.

Der Wiener Gesundheitsverbund (WIGEV) weist 7.339 systematisierte Betten in seinen Spitälern aus. Die acht Kliniken des WIGEV verzeichnen jährlich rund 234.000 stationäre Aufnahmen von Patient*innen sowie weitere 4,3 Millionen Ambulanzbesuche. Von den Kliniken werden damit ¾ der Spitalsversorgungsleistung erbracht. Die nachfolgende Tabelle zeigt die, vom Wiener Gesundheitsverbund verwalteten, Spitäler mitsamt der systematisierten Bettenkapazität.

Tabelle 10: Kommunale Krankenanstalten in Wien (Quelle: Datengrundlage Magistrat der Stadt Wien 2021: 106)

Krankenanstalt unter öffentlicher Verwaltung	**Bezirk (Postleitzahl)**	**Systematisierte Betten**
Allgemeines Krankenhaus der Stadt Wien	1090	1.726
Klinik Landstraße	1030	699
Klinik Favoriten	1100	781
Klinik Hietzing	1130	983
Klinik Penzing	1140	453
Klinik Ottakring	1160	978
Klinik Floridsdorf	1210	756
Klinik Donaustadt	1220	963
		Summe: 7.339

Der Wiener Stadtrechnungshof misst der gesamten Anlagentechnik, den medizinischen Geräten und der Ausstattung an Informations- und Kommunikationstechnik (IKT) eines Krankenhauses einen besonderen Stellenwert für die Betriebssicherheit bei. Während ein Stromausfall in der Regel in Wohngebäuden

oder bei gewerblichen Betrieben überschaubare Auswirkungen mit sich bringt, kann schon eine kurze Unterbrechung der Versorgung eines Krankenhauses mit elektrischer Energie weitreichende und auch lebensbedrohliche Folgen haben. Aus diesem Grund sind sowohl die Planung, die Konzeption und die Ausführung als auch der Betrieb der elektrischen Anlage unter dem Gesichtspunkt größtmöglicher Sicherheit gegen Ausfall vorzunehmen. Es ist überdies Vorsorge zu treffen, dass bei einer Störung der öffentlichen Stromversorgung zumindest die, für die Patient*innen und für das Personal, als wesentlich deklarierten Einrichtungen fortwährend betrieben werden können. Die Errichtung einer geeigneten Notstromversorgung wird den Betreiber*innen von Krankenanstalten daher im Zuge der Betriebsbewilligung vorgeschrieben (vgl. StRH 2010: 4f.)

7.3. Aufbau der Rettungskette

Abbildung 5 zeigt die einzelnen Glieder des Behandlungspfades von der Ersten Hilfe durch Lai*innen über den Rettungsdienst bis hin zur klinischen Versorgung. Ahnefeld (vgl. 2003: 521f.) prägte für den Ablauf den Begriff *Rettungskette*.

Im Rahmen der Ausführung werden die einzelnen technischen Komponenten, die ein Ineinandergreifen der Glieder ermöglichen, im Folgekapitel vorgestellt.

Die Verständigung von Hilfs- und Einsatzkräften erfolgt zumeist via (Mobil)Telefon. Für Smartphones gibt es mittlerweile eine alternative Kommunikationsmöglichkeit mit der Leitstelle eines Rettungsdienstes, die Notruf-App. Diese Applikation für Smartphones kann per Knopfdruck den Notruf an die Rettungsleitstelle absetzen und auch gleichzeitig die Standortdaten übermittelt werden. Damit dieses Netzwerk auch in einer Strommangellage oder bei einem Blackout eine gewisse Zeit lang aufrechterhalten werden kann, sind Anbieter*innen per Gesetz verpflichtet, technische Einrichtungen zur Ausfallsicherheit bereitzuhalten. (vgl. § 123 TKG 2021)

Von der Rettungsleitstelle werden relevante Einsatzinformationen nach einem standardisierten Muster abgefragt. Dieses, aus den Vereinigten Staaten von Amerika stammende, Abfrageschema ist *AMPDS – Advanced Medical Priority Dispatch System*. (vgl. BRH 2020: 26f.)

Die erfragten Daten werden von speziell ausgebildeten Telefonist*innen in einem Einsatzleitsystem eingegeben. Erforderlichenfalls kann das Leitstellenpersonal den Laien Ratschläge in der Ersten Medizinischen Hilfeleistung geben. Diese Bediensteten in Rettungsleitstellen verfügen auch über eine Qualifikation als Sanitäter*in. Bei lebensbedrohenden Zuständen leiten sie die Maßnahmen für die Reanimationen, Geburten oder zur Stillung von starken Blutungen am Telefon an. (vgl. ebenda)

Medizinische Notleiden, denen keine Indikation für eine Hospitalisierung innewohnt, werden von der Gesundheitsberatung 1450 bearbeitet. Die Gesundheitsberatung ist ohne Vorwahl unter der Rufnummer 1450 bundesweit zu erreichen. Besonders medizinisch geschulte diplomierte Krankenpflegepersonen beraten am Telefon und geben passende Empfehlungen. Sollte sich ein Leiden als akut herausstellen, wird unmittelbar die Entsendung eines Rettungsdienstes veranlasst. Bei weniger dringlichen Anliegen werden Empfehlungen für die weitere Behandlung und Abklärung gegeben. Die telefonische Gesundheitsberatung ersetzt folglich keine medizinische Behandlung und stellt auch keine Diagnosen. Mit der Telefonnummer 1450 wird Patient*innen ein Wergweiser durch das große Angebot an Gesundheitsdienstleister*innen geboten. (vgl. Grethe 2019: 501ff.)

Sobald die Einsatzadresse und die Notfallindikation im Einsatzleitsystem der Rettungsleitstelle aufscheinen, wird das nächste Rettungsmittel ausgewählt und zu dem Notfallgeschehen entsandt. Die erhobenen Einsatzdaten werden vom Einsatzleitrechner digital an den Bordcomputer des Einsatzfahrzeugs übermittelt. Zeitgleich erfolgt eine Alarmierung der Besatzung des Rettungsfahrzeugs per Pager oder SMS (*Short Message Service* - Kurznachrichtendienst). Zusätzlich besteht die Möglichkeit das Notfallteam per Funksprechgerät zu kontaktieren. Die Verbindung zwischen der Rettungsleitstelle und den Rettungsmitteln ist mehrfach abgesichert und somit hochgradig redundant. Das alarmierte Einsatzfahrzeug erhält die Ortsangaben sowie weitere einsatzrelevante Informationen übermittelt. Mittels satellitengestützter *Global Positioning System* (GPS) wird die kürzeste Fahrstrecke bzw. schnellste Route zum Notfallort gewählt. (vgl. Reisinger 2012: 73f.)

Am Einsatzort wird parallel mit den qualifizierten Maßnahmen die Anamnese erhoben und dokumentiert (vgl. § 15 Abs.5 WRKG). Weitere Angaben zu der verletzten oder erkrankten Person werden in einem tragbaren Computer eingegeben. Via Laptop kann zudem eine geeignete Zielklinik für die weitere Versorgung selektiert werden. Mit der Auswahl der Krankenanstalt wird das Einsatzprotokoll digital über das Funknetz an diese Gesundheitseinrichtung geschickt.

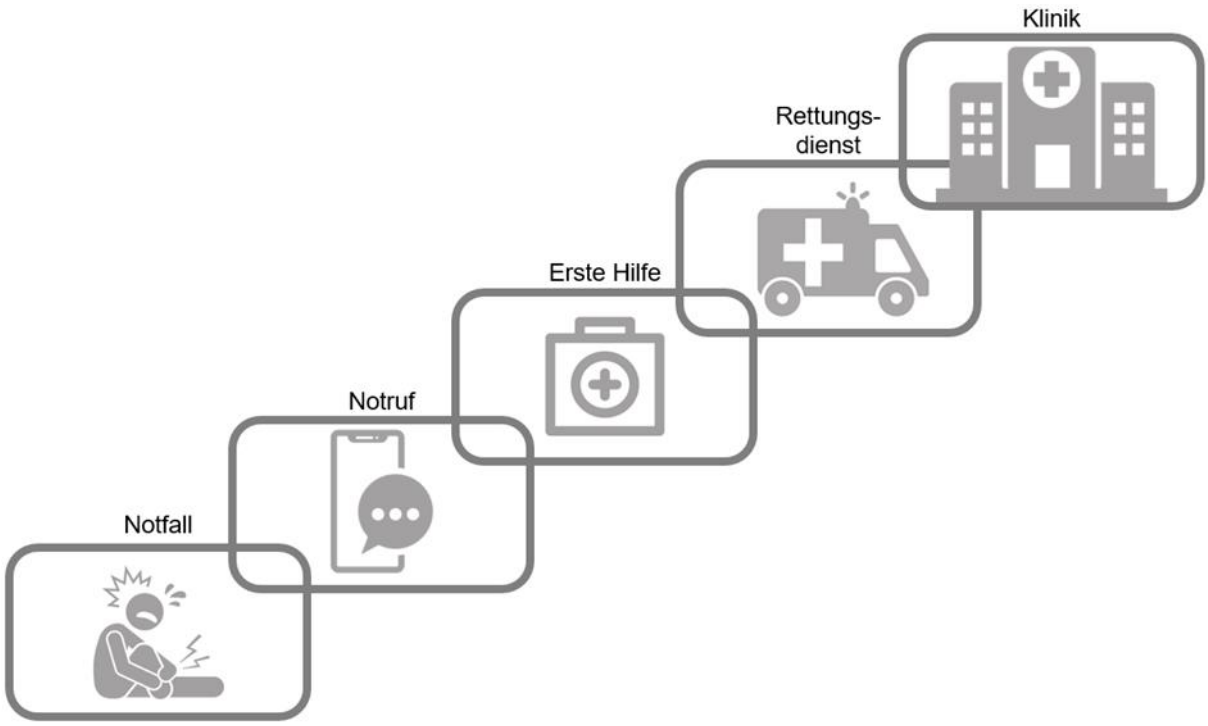

Abbildung 5: Rettungskette (Quelle: Ahnefeld 2003: 521)

Im nächsten Unterkapitel werden Bedrohungen für den Gesundheitssektor mitsamt den Auswirkungen für Teile der Bevölkerung aufgezeigt. Einschränkungen bei Gesundheitsleistungen haben einen negativen Impact auf die Gesellschaft. Welche das im Detail sind wurde anhand eines Stromausfalls in einer Krankenanstalt in Tabelle 6 auf Seite 44 demonstriert.

7.4. Bedrohungen für den Gesundheitssektor

Die vorgestellten Bedrohungsszenarien gelten für das Gesundheitswesen gleichermaßen wie auch für die übrigen Sektoren der Kritischen Infrastrukturen. Der wirtschaftliche Schaden durch Angriffe auf den Gesundheitsbereich steht dabei nicht im Vordergrund der gegenständigen Betrachtung. Mängel, Störungen oder Versorgungsengpässe in diesem Bereich wirken sich unmittelbar negativ auf das Leben eines gewissen Bevölkerungsanteils aus. Einschränkungen bei medizinischen Leistungen die der Lebensrettung, einer Wiederherstellung oder dem Erhalt der Gesundheit dienen, können zum Tod von vulnerablen Menschen führen.

Die Abhängigkeit von elektrischer Energie ist in der modernen Medizin offensichtlich. Labordiagnostik, Röntgengeräte und die gesamte IKT-Infrastruktur zur Administration und Verwaltung der Patient*innen benötigen elektrischen Strom für den Betrieb. Notstromaggregate und besondere Verfahren bei Stromausfällen sollen gewährleisten, dass die wichtigsten Behandlungsprozesse fortgesetzt werden. (vgl. Breuer et al. 2021: 507; Pausch 2017: 24)

Breuer et al. (2021: 507f.) zeigten anschaulich welche Folgen ein anhaltender Stromausfall auf das gesamte System Krankenhaus haben kann. Infolge des Mangels an elektrischer Energie für den Betrieb von wichtigen technischen Anlagen und Systemen tritt die sukzessive Reduktion des Leistungsangebots ein.

Ob das Fehlen von elektrischer Energie als eine Begleiterscheinung auftritt und durch ein Naturereignis oder ein technisches Gebrechen hervorgerufen wurde, ist für eine Gesundheitsversorgungeinrichtung von nachgeordneter Bedeutung. Denkbar ist gleichermaßen, dass der Stromausfall ein Resultat von Sabotage ist. Diese kann gezielt gegen die Krankenanstalt gerichtet sein oder es handelt sich um einen Kollateralschaden. In diesem Fall stellt das eigentliche Ziel die Stromerzeugung oder -verteilung dar. Das Spital als solches ist ein indirektes Opfer des Angriffs.

Im zunehmenden Maße sind Einrichtungen des Gesundheitsbereichs in den Fokus von Angreifer*innen geraten. Weltweit zeigen Beispiele von Cyberangriffen auf Krankenanstalten drastisch welche Auswirkungen diese Sicherheitsvorfälle auf die Versorgung der Patient*innen haben. Seit Beginn der COVID-19 Pandemie nahmen diese Attacken auf Gesundheitseinrichtungen zu. (vgl. Moran et al. 2021: 2ff.)

Ransomeware-Attacken verschlüsseln Dateien. Das Spitalspersonal kann daher nicht auf Informationen von Patient*innen, der Behandlungsdokumentation und andere Daten zugreifen. Eine Beeinträchtigung oder der Ausfall von Kommunikationsanwendungen wie zum Beispiel E-Mails als alternierender Angriffsvektor erschwert den Krankhausbetrieb.

In den vorangegangenen Kapiteln wurde der Begriff Kritische Infrastruktur erläutert. Die Rechtsvorschriften, welche zur Erhöhung der Resilienz von Kritischen Infrastrukturen beitragen, wurden vorgestellt. Anhand zweier ausgewählter Bedrohungsszenarien wurde die Verwundbarkeit von Einrichtungen des Gesundheitssektors dargestellt. Im nachfolgenden Kapitel acht werden die Interviewergebnisse von Gesprächen mit unterschiedlichen Expert*innen präsentiert.

8. Interviewergebnisse

Im vorangegangenen Abschnitt wurden das methodische Vorgehen skizziert sowie, für das Verständnis des Forschungsgegenstands erforderliche, Bergriffe und Zusammenhänge erklärt und das Forschungsumfeld beschrieben. In gegenständigen Kapitel werden die Interviews mit Expert*innen aus den Bereichen der medizinischen Versorgung und der Sicherheit bzw. dem Schutz Kritischer Infrastrukturen behandelt.

Im Zeitraum von April bis Mai 2022 erfolgten die leitfadengestützten Gespräche mit den Expert*innen. Die Transkripte der einzelnen Dialoge befinden sich im Anhang. Die Transkription der Befragungen erfolgte nicht persönlich, sie wurde an ein darauf spezialisiertes Institut ausgelagert. Die verschriftlichten Gesprächsdateien wurden danach für eine Inhaltsanalyse nach Mayring aufbereitet.

Die Methode nach Mayring (vgl. 2015) ist ein etabliertes Verfahren um die Essenz von Interviews zu erfassen. In einem mehrstufigen Prozess erfolgt die Reduktion der Aussagen auf die Kernaussagen. Damit die Antworten der Expert*innen, deren Kernaussagen und die daraus resultierenden Erkenntnisse einfacher erfasst werden können, sind diese in den nachfolgenden Tabellen zusammengefasst.

Ausgehend von den zusammengefassten Meinungen werden die Meinungen zu den einzelnen Themen diskutiert und für die Diskussion rezipiert. Die Transkripte der einzelnen Interviews sind im Anhang angefügt.

Die Einzelergebnisse auf den Folgeseiten sind in alphabetischer Folge gereiht.

8.1. Ergebnis Experte Auer

Mag. Auer, MSc äußerte seine positive Ansicht zur NIS-Gesetzgebung. Organisationen und Firmen könnten sich auf freiwilliger Basis der Einhaltung von Normen verpflichten. Durch ein Gesetz seien diese Standards zu exekutieren und Verstöße zu ahnden. Er gab des Weiteren zu bedenken, dass auch kleine Betreiber als KRITIS gelten könnten.

Bezüglich möglicher Risikoszenarien folgte der Gesprächspartner einem All-hazards-Ansatz. Risiken müssten umfassend betrachtet und dabei keine Bedrohung von vornherein ausgeschlossen werden. Zu der Gefahr von erheblichen Auswirkungen eines Cyberangriffs auf Deutschland für Österreich vertrat Herr Mag. Auer, MSc die Ansicht, dass die Stromversorgung im Vergleich zur Logistikkette und der Produktion relativ schnell wiederhergestellt sei. Dennoch attestierte er, wie die vorangegangenen Expert*innen, die gravierenden Effekte auf das Stromnetz in Österreich. Von ihm wurde ebenfalls eine Verbesserung bei der Aufklärung der Bevölkerung gewünscht.

Die system- und sektorenübergreifenden Prozesse müssten nach Aussage des Experten als Gesamtes betrachtet werden. Anstelle eines sektorenzentrierten Ansatzes empfahl er die Orientierung an Prozessen für die Bewertung von Risiken. Mit Blick auf das Kontinuitätsmanagement wurde von ihm geraten basale Tätigkeiten ohne IKT-Unterstützung zu trainieren.

Nachfolgende Tabelle 11 zeigt das Ergebnis des Interviews am 17.05.2022 mit Herrn Mag. Auer, MSc.

Tabelle 11: Interviewergebnis Auer

Dimension	Aussage
Notwendigkeit für gesetzliche Regelung	Positiv Nicht nur große Unternehmen sind KRITIS
Bedeutung ÖSCS gegenüber NISG	Normen sind freiwillig Sicherstellung von Leistungen als Mehrwert für die Gesellschaft
Risikoszenarien für KRITIS	Viele Bedrohungen, Cyberkriminalität Anschläge, Stromausfälle All-hazards-Ansatz
Kollateralschaden durch Cyberangriff auf deutsche KRITIS	Sehr hohe Auswirkung Strom relativ schnell wieder verfügbar Logistik braucht länger
Maßnahmen für Blackout-Szenario	Stromunabhängige Kommunikation Einbindung anderer wichtig
KRITIS sind nicht als Betreuungs-einrichtung ausgelegt	Aufklärungsarbeit bei der Bevölkerung Bevorratungsproblem bei kleinen Haushalten
Berücksichtigung von wechselseitigen Abhängigkeiten der KRITIS im NISG	Gehärtete eigene Infrastruktur führt zu erschwerter Kommunikation zwischen Organisationen Gesamtheitliche Betrachtung notwendig
Autarkie im Zusammenhang system-übergreifender Prozessketten	Alle sind voneinander abhängig Übergreifende Betrachtungsweise bei systemübergreifenden Prozessen
Medizinische Basisversorgung der Wiener Bevölkerung sicherstellen	Trainings Nicht immer nur auf die Technik verlassen

8.2. Ergebnis Experte Eisenburger

Nachfolgende Tabelle 12 zeigt das Ergebnis des Interviews am 22.04.2022 mit Herrn Primar Universitätsprofessor Dr. Eisenburger.

Um die notwendigen finanziellen Zuwendungen zur Umsetzung von Vorhaben zu erhalten sei eine rechtliche Grundlage von Vorteil, meinte Primar Universitätsprofessor Dr. Eisenburger. Ein vorrangiges Risiko für Krankenanstalten sei die physische Gewalt. Dem Schutz vor Gewalt durch Terror müsse eine erhöhte Aufmerksamkeit entgegengebracht werden.

Der Leiter der Zentralen Notaufnahme in der Klinik Floridsdorf schloss sich der vorherrschenden Meinung an, wonach ein Cyberangriff auf Deutschland negative Auswirkungen auf Österreich hätte. Ebenso war er der Meinung die Aufklärungsarbeit bei der Bevölkerung gehöre verstärkt. Die Betroffenen müssten vor dem Ereignisfall über die Strategien und Planungen der Behörden bzw. Verantwortlichen vorab informiert sein. Nicht nur die Kommunikation mit der Bevölkerung müsse immer aufrechterhalten bleiben, auch jene zwischen den Einsatzorganisationen und Bereichen, die mit der Katastrophenbewältigung betraut sind, müsse funktionieren.

Tabelle 12: Interviewergebnis Eisenburger

Dimension	Aussage
Notwendigkeit für gesetzliche Regelung	Gesetz ist unflexibel aber fundiert die Argumentation von Bedarfen
Bedeutung ÖSCS gegenüber NISG	Keine Antwort
Risikoszenarien für KRITIS	Schutz vor Gewalt durch Terror
Kollateralschaden durch Cyberangriff auf deutsche KRITIS	Problematisch für Österreich
Maßnahmen für Blackout-Szenario	Maßnahmen nur zur Überbrückung
KRITIS sind nicht als Betreuungs-einrichtung ausgelegt	Aufklärungsarbeit: Lösung muss Bevölkerung bekannt sein, bevor sie passiert
Berücksichtigung von wechselseitigen Abhängigkeiten der KRITIS im NISG	Keine Antwort

Autarkie im Zusammenhang system-übergreifender Prozessketten	Vernetzung im Widerspruch zu Autarkie Zustrom weniger das Problem als der Abfluss
Medizinische Basisversorgung der Wiener Bevölkerung sicherstellen	Kommunikation muss funktionieren Bevölkerung muss wissen wo ihr geholfen wird

8.3. Ergebnis Experte Glaninger

Für den Leiter der Rettungsleitstelle Wien war die gesetzliche Regelung zum Schutz Kritischer Einrichtungen bereits seit längerem notwendig. Sein Fokus lag beim physischen Objektschutz. Das Aufrechterhalten der Kommunikation stellte einen weiteren Schwerpunkt dar.

Im Gegensatz zu einigen anderen Expert*innen zeigte sich Herr Glaninger davon überzeugt, dass die Resilienz des Gesamtsystems gegeben sei, wenn alle Sektoren die Vorschriften und Empfehlungen einhielten.

Nachfolgende Tabelle 13 zeigt das Ergebnis des Interviews am 23.05.2022 mit Herrn Glaninger.

Tabelle 13: Interviewergebnis Glaninger

Dimension	Aussage
Notwendigkeit für gesetzliche Regelung	Gesetzliche Regelung war notwendig
Bedeutung ÖSCS gegenüber NISG	Gesetze müssen befolgt werden Ob Normen erfüllt werden ist nicht wichtig
Risikoszenarien für KRITIS	Gebäudeschutz ist wichtig Schutz vor intentionalen Gefahren
Kollateralschaden durch Cyberangriff auf deutsche KRITIS	Wird als sehr hoch eingeschätzt
Maßnahmen für Blackout-Szenario	Erreichbarkeit der Einsatzmittel durch redundante Systeme sichergestellt und regelmäßig überprüft

KRITIS sind nicht als Betreuungs-einrichtung ausgelegt	Für alle KRITIS ein Problem Mannschaft kann drei Tage versorgt werden Bevölkerung nicht
Berücksichtigung von wechselseitigen Abhängigkeiten der KRITIS im NISG	Jeder Sektor hat seine Vorgaben und damit wird das Gesamtsystem abgedeckt
Autarkie im Zusammenhang system-übergreifender Prozessketten	Basisanforderung an Autarkie muss von allen erfüllt werden
Medizinische Basisversorgung der Wiener Bevölkerung sicherstellen	Im Vergleich mit den übrigen Bundesländern am besten vorbereitet

8.4. Ergebnis Expertin Heissenberger

Nachfolgende Tabelle 14 zeigt das Ergebnis des Interviews am 11.05.2022 mit Frau Dipl.-Ing.in Heissenberger, MBA.

Die CISO der Stadt Wien bewertete die Rechtsgrundlage des NISG als einen wesentlichen Beitrag um ein einheitliches Niveau für alle Kritischen Infrastrukturen zu erreichen. Ihr zufolge handelte es sich bei Normen um freiwillige Selbstverpflichtungen ohne Sanktionsmöglichkeiten. Zudem wären Überprüfungen auf Basis der NIS-Gesetzgebung detaillierter als jene im Rahmen von Normenüberprüfungen.

Für Dipl.-Ing.in Heissenberger, MBA waren die Bedrohungen für IKT-Systeme das vorherrschende Risikoszenario. Österreich stände in Abhängigkeit von Systemen in Deutschland. Daher wäre Österreich bei Cyberangriffen auf das Nachbarland ebenfalls betroffen. Kontinuitätspläne seien ihr zufolge erstellt damit die Kernprozesse auch im Falle eines Blackouts weiterhin aufrecht erhalten blieben.

Der wechselseitigen Abhängigkeit von Systemen und Kritischen Infrastrukturen untereinander würde das NISG unzureichend abgebildet sein, meinte die Expertin.

Tabelle 14: Interviewergebnis Heissenberger

Dimension	Aussage
Notwendigkeit für gesetzliche Regelung	Einheitliches Niveau
Bedeutung ÖSCS gegenüber NISG	Normen sind freiwillig NISG geht einen Schritt weiter
Risikoszenarien für KRITIS	Bedrohung für IT-Systeme
Kollateralschaden durch Cyberangriff auf deutsche KRITIS	Abhängigkeit Österreichs von Deutschland
Maßnahmen für Blackout-Szenario	Kontinuitätspläne
KRITIS sind nicht als Betreuungs-einrichtung ausgelegt	Nicht Thema der IKT
Berücksichtigung von wechselseitigen Abhängigkeiten der KRITIS im NISG	Hochkomplexe Angelegenheit Im NISG nicht abgebildet
Autarkie im Zusammenhang system-übergreifender Prozessketten	Heutzutage nicht mehr gegeben
Medizinische Basisversorgung der Wiener Bevölkerung sicherstellen	Übungen damit es im Krisenfall funktioniert

8.5. Ergebnis Experte Hellwagner

Herrn Professor Dr. Hellwagner, LL.M. zufolge könnten gewinnorientierte Organisationen nur durch gesetzliche Vorschriften zu Investitionen in Sicherheit bewogen werden. Daraus ergäbe sich der Mehrwert für die Gesellschaft aus der Gesetzgebung. Hinsichtlich der Risiken und Bedrohungsszenarien könne nichts ausgeschlossen werden. Aufgrund von Verflechtungen und wechselseitigen Abhängigkeiten über Sektoren und Staatengrenzen hinweg werde Österreich bei einem Cyberangriff auf Deutschland mitgerissen. Dieser Umstand sei vielen nicht bewusst und müsste stärker betont werden.

Umseitige Tabelle 15 zeigt das Ergebnis des Interviews am 19.05.2022 mit Herrn Professor Dr. Hellwagner, LL.M.

Tabelle 15: Interviewergebnis Hellwagner

Dimension	Aussage
Notwendigkeit für gesetzliche Regelung	Auf Gewinn ausgerichtete Betreiber*innen machen es nur, wenn gesetzlich vorgeschrieben
Bedeutung ÖSCS gegenüber NISG	Mehrwert gegeben weil die Gesellschaft resilienter wird
Risikoszenarien für KRITIS	Nichts kann ausgeschlossen werden
Kollateralschaden durch Cyberangriff auf deutsche KRITIS	Österreich wird mitgerissen
Maßnahmen für Blackout-Szenario	Notstromaggregate Nachschub von Betriebsmitteln problematisch
KRITIS sind nicht als Betreuungs-einrichtung ausgelegt	Sicherheitsinseln sind ein verfehltes Konzept Dort wo Krisenmanagement erfolgt kann nicht Basisversorgung stattfinden Bevorratung kostet Geld und muss deshalb vorgeschrieben werden
Berücksichtigung von wechselseitigen Abhängigkeiten der KRITIS im NISG	Vernetzung der KRITIS ist Vielen nicht klar Genauso ist Personal mehrmals verplant
Autarkie im Zusammenhang system-übergreifender Prozessketten	Kommunikation ist essenziell Abtransport aus Spitälern berücksichtigen
Medizinische Basisversorgung der Wiener Bevölkerung sicherstellen	Gedanken machen welche Versorgung noch angeboten wird Versorgungsbereiche einrichten

8.6. Ergebnis Experte Krammel

Nachfolgende Tabelle 16 zeigt das Ergebnis des Interviews am 14.04.2022 mit Herrn Chefarzt Dr. Krammel.

Für Dr. Krammel stellten rechtliche Normen eine qualitätssichernde Maßnahme durch den Staat dar. Wenngleich keine Auskunft zu den Sicherheitsstrategien der Republik Österreich gegeben werden konnte, erfolgte eine umfangreiche Betrachtung von potentiellen Bedrohungen für Kritische Infrastrukturen. Ein vorrangiges Ziel der präklinischen Notfallversorgung sei es, das Katastrophengeschehen nicht von der Straße in die Krankenanstalten zu verlagern. Dazu sei eine Triage, bereits ab dem ersten Notrufgespräch am Telefon, notwendig.

Der Ansicht des Gesprächspartners zufolge müsse die Bevölkerung verstärkt zur Bevorratung mit lebenswichtigen Gütern aufgefordert werden. Des Weiteren betonte er die Wichtigkeit von Kooperationen zur Krisen- und Katastrophenbewältigung.

Tabelle 16: Interviewergebnis Krammel

Dimension	Aussage
Notwendigkeit für gesetzliche Regelung	Sichert einheitliche Qualität Einhaltung von Standards/Normen ist nicht verpflichtend
Bedeutung ÖSCS gegenüber NISG	Keine Antwort
Risikoszenarien für KRITIS	Nicht nur physische Zerstörung ist gefährlich Blackout, Terror, Naturkatastrophen
Kollateralschaden durch Cyberangriff auf deutsche KRITIS	Indirekte Auswirkung
Maßnahmen für Blackout-Szenario	Katastrophe nicht von der Straße in die Krankenhäuser verlagern Vortriage am Notruf
KRITIS sind nicht als Betreuungs-einrichtung ausgelegt	Aufklärungsarbeit bei der Bevölkerung Versorgungszentren vorbereiten KRITIS gehören geschützt

Berücksichtigung von wechselseitigen Abhängigkeiten der KRITIS im NISG	Keine Antwort
Autarkie im Zusammenhang system-übergreifender Prozessketten	Zusammenarbeit und Abstimmung notwendig Nur den eigenen Bereich zu betrachten wird in der Krise nicht helfen
Medizinische Basisversorgung der Wiener Bevölkerung sicherstellen	Triage am Notruf

8.7. Ergebnis Expertin LVT

Nachfolgende Tabelle 17 zeigt das Ergebnis des Interviews am 20.04.2022 mit einer Expertin aus dem Landesamt für Verfassungsschutz und Terrorismusbekämpfung in Wien.

Nachdem Normen lediglich eine Selbstverpflichtung bedeuten sei die gesetzliche Verpflichtung, nach Ansicht der LVT Expertin, ein entscheidender Vorteil. Dadurch werde die Widerstandsfähigkeit erhöht und ergebe einen gesamtgesellschaftlichen Mehrwert. Für die Dame stellte die Bedrohung der Energieversorgung ein vorrangiges Risiko dar. Wegen der Vernetzung quer durch Europa hätte ihrer Meinung nach ein Cyberangriff auf die Energienetze in Deutschland folgenschwere Auswirkungen auf Österreich.

Damit die Resilienz der Gesellschaft erhöht werden könne, empfahl die Expertin diesbezügliche Aufklärungsarbeit und Sensibilisierung bei der Bevölkerung ab dem Schuleintritt.

Die Triage durch den Rettungsdienst, damit die Ressourcen von Krankenanstalten geschont werden, bewertete die Mitarbeiterin des LVT als wichtige Maßnahme.

Tabelle 17: Interviewergebnis LVT-Expertin

Dimension	Aussage
Notwendigkeit für gesetzliche Regelung	Vorteil gesetzlicher Regelung Anwendung von Normen ist nicht verpflichtend
Bedeutung ÖSCS gegenüber NISG	Vorarbeit beim Risikomanagement Beratung durch LVT eingeführt
Risikoszenarien für KRITIS	Energieversorgung vorrangig
Kollateralschaden durch Cyberangriff auf deutsche KRITIS	Große Auswirkung auf Österreich und Europa aufgrund von Vernetzung
Maßnahmen für Blackout-Szenario	Keine Antwort
KRITIS sind nicht als Betreuungs-einrichtung ausgelegt	Sensibilisierung bereits in Schule notwendig Strom wird nicht immer verfügbar sein Mehr Medienarbeit und Aufklärung
Berücksichtigung von wechselseitigen Abhängigkeiten der KRITIS im NISG	Keine Antwort
Autarkie im Zusammenhang system-übergreifender Prozessketten	Wegen der Vernetzung kann nicht von Autarkie gesprochen werden
Medizinische Basisversorgung der Wiener Bevölkerung sicherstellen	Triage durch Rettungsdienst wegen endenwollenden Ressourcen im Spital

8.8. Ergebnis Expertin Mayer

Nachfolgende Tabelle 18 zeigt das Ergebnis des Interviews am 20.04.2022 mit Frau Ing.in Mag.a Dr.in Sylvia Mayer, MA.

Sie sah in der gesetzlichen Regelung von Sicherheitsstandards ein adäquates Mittel um ein einheitliches und hohes Sicherheitsniveau zu erreichen. Der Anreiz durch einen Wettbewerbsvorteil bei der Erfüllung von Sicherheitsnormen gelte für viele Bereiche der Daseinsvorsorge nicht.

Vorrangig seien der Energie- und Finanzsektor im Fokus von Cyberangriffen. Daher hätten sich dort bereits seit längerem entsprechend hohe Sicherheitsstandards etabliert. Durch die COVID-19 Pandemie sei eine Verlagerung der Angriffsziele hin zu anderen Sektoren zu beobachten gewesen. Die Bevölkerung müsse über die Bedeutung von KRITIS sensibilisiert werden. Gleichzeitig sollte das Awareness für Cybersicherheit gesteigert werden.

Tabelle 18: Interviewergebnis Mayer

Dimension	Aussage
Notwendigkeit für gesetzliche Regelung	Notwendig für alle Betreiber*innen hohe Standards einzuführen
Bedeutung ÖSCS gegenüber NISG	Normen sind freiwillig einziger Anreiz Wettbewerbsvorteil genauso Strategien nicht ausreichend verpflichtend
Risikoszenarien für KRITIS	Cyberangriffe auf Energiesektor und Banken Physische Angriffe in Spitälern neu
Kollateralschaden durch Cyberangriff auf deutsche KRITIS	Hohes Risiko von Ausfällen in Österreich
Maßnahmen für Blackout-Szenario	Lebenswichtige Bereiche müssen weiter funktionieren Abstimmung ist wichtig
KRITIS sind nicht als Betreuungs-einrichtung ausgelegt	Schutzkonzepte für KRITIS Sensibilisierung der Bevölkerung
Berücksichtigung von wechselseitigen Abhängigkeiten der KRITIS im NISG	NISG geht auf Interdependenz ein Pflicht zur unmittelbaren Vorfallmeldung im Energiesektor
Autarkie im Zusammenhang system-übergreifender Prozessketten	In heutiger wirtschaftlicher Zeit nicht mehr möglich
Medizinische Basisversorgung der Wiener Bevölkerung sicherstellen	Awareness für Cybersicherheit steigern

	Kooperation innerhalb des Gesundheitssektors zur Sicherstellung der Versorgung von Patient*innen

8.9. Interviewzusammenfassung

Aus den durchgeführten Interviews mit Expert*innen lassen sich diverse Ableitungen anstellen. In mehreren Punkten können Gemeinsamkeiten erkannt werden. In diesem Abschnitt werden die Einzelergebnisse zu einem Gesamtergebnis zusammengeführt.

Die Gesprächsauswertung zeigt, dass generell eine Notwendigkeit für gesetzliche Regelungen über den Schutz Kritischer Infrastrukturen von den Expert*innen gesehen wird. Nach Ansicht der meisten Gesprächspartner*innen sind Normen freiwillige Richtlinien. Deren Nichtbefolgung könne durch den Staat nicht sanktioniert werden. Daher wird von den interviewten Personen eine gesetzliche Verpflichtung begrüßt. Mit der Festlegung von einem gesetzlichen Standard hinsichtlich der Sicherheitsanforderungen lassen sich nach Ansicht mancher Expert*innen Bedarfe leichter argumentieren. Die erforderlichen Budgetmittel für die Umsetzung der Schutz und Sicherheitsmaßnahmen ließen sich dadurch einfacher lukrieren.

Staatlichen Strategien wird im Wesentlichen eine ähnliche Bedeutung wie den Normen zugedacht. Auch diese seien bei Verstößen nicht zu sanktionieren.

In Bezug auf potentielle Risiken und davon abgeleiteten Szenarien sind zwei Dinge auffällig. Einerseits wurde von Expertinnen aus dem Bereich Sicherheit die Cyberbedrohung vorrangig genannt. Diese Damen sind im Vergleich zu den interviewten Ärzten und dem Leiter der Rettungsleitstelle im strategischen Bereich tätig. Die vier Herren, die eher zur operativ/taktischen Hierarchieebene zu zählen sind, sahen das eigene Personal und den Objektschutz bedroht.

Von allen interviewten Expert*innen wurde die Wahrscheinlichkeit von Kollateralschäden in Österreich durch Cyberangriffe auf Kritische Infrastrukturen in Deutschland als hoch eingestuft.

Der Kommunikation zwischen Organisationen wurde im Fall eines Blackouts eine hohe Bedeutung zugebilligt. Diese sei erforderlich um die systemübergreifenden Prozesse weiterhin aufrecht erhalten zu können. Absprachen und die Abstimmung von Abläufen

seien bereits vor dem Ereigniseintritt durchzuführen und Vorbereitungen gemeinsam zu treffen. Dies sei den Auskünften zufolge bisher nur unzureichend erfolgt.

Betreffend die Frage, inwiefern die NIS-Gesetzgebung auf die wechselseitige Interdependenz der KRITIS eingeht, gab es differenzierte Meinungen. Diese reichten von keiner über zustimmende bis ablehnende Antworten. Der Begriff Autarkie steht im Zusammenhang mit Kritischen Infrastrukturen nach Ansicht von Expert*innen im Widerspruch zu der Vernetzung dieser, für die Gesellschaft wichtigen, Einrichtungen.

Neben der Abstimmung zwischen den beteiligten Organisationen zur Vorbereitung auf ein Blackout-Szenario oder eine Cyberkrise sei die Überlegung, welche Leistungen von den verschiedenen Kritischen Infrastrukturen aufrechtzuerhalten wären, zu berücksichtigen. Durch die Leistungsreduktion bei Kritischen Infrastrukturen können sich zwangsläufig Leistungseinschränkungen bei weiteren KRITIS ergeben. Es ist zu empfehlen, potentielle Auswirkungen die sich aus den Restriktionen ergeben, durch die, vom Kaskadeneffekt betroffenen Stakeholder, vorab zu analysieren. Abbildung 1 auf Seite 18 liefert hierzu einen Überblick.

9. Diskussion

Den Abschluss der empirischen Forschung stellt die Gegenüberstellung der Hypothesen mit den Aussagen der Expert*innen dar. Es wird der Bezug zwischen den Annahmen und den Antworten der Expert*innen hergestellt und diskutiert. Die zwei Hypothesen sowie die forschungsleitenden Fragen sind in Tabelle 19 dargestellt.

Tabelle 19: Übersicht Hypothesen und Forschungsfragen

H1	Der Begriff Autarkie, im Zusammenhang mit Resilienz unserer modernen Gesellschaft, steht im Widerspruch zur Vernetzung von Systemen.
F1	Wo sehen Expert*innen einen Steigerungsbedarf um die Resilienz von Kritischen Infrastrukturen zu erhöhen?
F2	Welche Maßnahmen erscheinen notwendig um die Resilienz der Gesellschaft zu stärken?
H2	Durch das Netz- und Informationssystemsicherheitsgesetz werden die intersektorale Konnexität und Interdependenzen nicht beachtet.
F3	Wie bewerten Expert*innen das Netz- und Informationssystem-sicherheitsgesetz im Fokus der beiden Hypothesen?
F4	Gegen welchen Bedrohungen müssen Kritische Infrastrukturen nach Meinung von Expert*innen wappnen?

H … Hypothese, F … Forschungsfrage

Bei der Rekrutierung der Expert*innen für die Interviews wurde auf eine differenzierte Zusammensetzung geachtet. Sowohl in hierarchischer Hinsicht, als auch beim beruflichen Hintergrund sollte der Mix zu einer umfassenden Betrachtung des Themenfeldes beitragen. Umso auffallender waren übereinstimmende Ansichten bei mehreren Fragestellungen.

Die erste Hypothese zeigte die Problematik bei dem Versuch, die Resilienz von Organisationen zu erhöhen, indem deren Autarkie forciert wird. In Zeiten von optimierten und spezialisierten Systemen die zu einer weitreichenden Vernetzung geführt haben, könne mittlerweile kaum mehr die Unabhängigkeit voneinander

bewerkstelligt werden. Diese Ansicht wurde von den Expert*innen geteilt. Demnach gilt die erste Hypothese als verifiziert.

Augenscheinlich war die einhellige Meinung zur Abhängigkeit von Elektrizität und einem intakten Stromnetz. Die externe Stromversorgung lässt sich mittels eigener Stromaggregate für gewisse Teilbereiche temporär ersetzen. Allerdings besteht bei dieser Substitution wiederum eine Abhängigkeit von Betriebsmitteln, hauptsächlich Kraftstoff, für den Betrieb der Generatoren. Die damit verbundenen Versorgungsprobleme wurden bereits von seit längerem von Ladinig und Saurugg (vgl. 2012: 38) bzw. Lorenz (vgl. 2010: 63f.) thematisiert und waren den Personen bewusst.

Zu der Bedeutung des Netz- und Informationssystemsicherheitsgesetzes im Zusammenhang mit intersektoralen Konnexitäten und Interdependenzen wurden differenzierte Aussagen getätigt. Hierzu enthielten sich drei der Interviewpartner*innen. Bei den übrigen reichten die Antworten von einer zustimmenden bis zu einer ablehnenden Meinung. Hypothese zwei ist folglich weder verifiziert noch falsifiziert.

Die Auffassung, wonach Sektoren ausreichend vor schädlichen Einflüssen geschützt seien, wenn jede*r der darin benannte Betreiber*in wesentlicher Dienste die Richtlinien umsetze und befolge, ist trügerisch. Wie die Vergangenheit gezeigt hat ist kein System zu 100 Prozent vor erfolgreichen Angriffen sicher. Dieser Tatsache war sich die Gesetzgebung offenbar bewusst. Mehrere Bereiche der NIS-Vorschriften widmen sich dem Erkennen von Vorfällen und Reagieren auf Sicherheitsverstöße sowie Maßnahmen zur Gewährleistung der Betriebskontinuität wesentlicher Dienste bei Notfällen (vgl. § 11 NISV).

Hinsichtlich der Bedrohungslage für Kritische Infrastrukturen konnte festgestellt werden, dass unterschiedliche Meinungen vertreten wurden. Personen deren beruflicher Hintergrund die Sicherheit von Informations- und Kommunikationstechnologie-Netzwerken war, nannten vorrangig Bedrohungen aus dem Cyberraum. Angehörige von Organisationen mit medizinischen Aufgaben räumten der Bedrohung durch physische Angriffe einen hohen Stellenwert ein.

Von den interviewten Expert*innen wurde ein breites Spektrum an Risiken aufgezeigt. Dieses deckt sowohl intentionale Bedrohungen als auch Naturgefahren ab. Damit wurde dem All-hazards-Ansatz aus der Strategie APCIP entsprochen. Wie in Kapitel 4

beschrieben, zielt diese Herangehensweise darauf ab, ein umfassendes Bild von potentiellen Risiken zu erhalten und so ein vielseitiges Sicherheitsverständnis zu erreichen als auch geeignete Maßnahmen abzuleiten (vgl. APCIP 2015: 6).

Kritische Infrastrukturen verfügen im Blackout-Fall weiterhin über Elektrizität, Licht und Wärme. Es wird erwartet, dass hilfesuchenden Menschen diese Objekte, auch als Lichtinseln bezeichnet, aufsuchen werden. Gerade öffentliche Einrichtungen wie Krankenanstalten stehen vor dem Problem, dass sie ohne Barrieren errichtet wurden. Der Mangel an baulichen Schutzmaßnahmen ermöglichen einen relativ leichten Zutritt zu den Krankenanstalten. Deshalb wird erwartet, dass sie sich in einem erhöhten Maße um den Schutz ihrer Betriebsobjekte oder um die Betreuung von Hilfesuchenden kümmern müssten. Die Expert*innen stimmten darüber überein, dass die Bevölkerung durch Aufklärungsarbeit im Vorfeld eines Blackouts über Verhaltensweisen informiert werden müsse. Andernfalls würden Kritische Infrastrukturen bei einem Blackout von ihren Kernaufgaben und der Krisenbewältigung abgehalten werden.

Ladinig und Saurugg (2012: 45) forderten bereits vor zehn Jahren „*sowohl die Risikosteuerung als auch das Krisenmanagement müssen von einer sektoralen Betrachtung zu einer prozessualen und ganzheitlichen Betrachtung führen*.“ Mit der NIS-Richtlinie und den daraus resultierenden nationalen Rechtsvorschriften wurde ein weiterer Schritt zum Ausbau der Widerstandsfähigkeit von Kritischen Einrichtungen unternommen. Durch die Betrachtung von einzelnen Sektoren haben die gesetzgebenden Organe jedoch auf einen Prozessansatz oder eine prozessuale Betrachtungsweise verzichtet.

Von einigen der interviewten Expert*innen wurde ebenso postuliert den Fokus hin zu Prozessabläufen zu richten. Ein Wechsel der Gesinnung der gesetzgebenden Institutionen sowie die damit verbundene organisatorische und technische Umsetzung dieses Ansinnens erscheint allerdings äußert aufwändig. Eine diesbezügliche Änderung des NISG muss im Einklang mit der NIS-RL erfolgen. Somit müsste zunächst dort eine ganzheitliche Betrachtungsweise von kritischen Prozessen angeregt werden.

10. Conclusio

Das übergeordnete Themengebiet lautete Schutz Kritischer Infrastrukturen vor Bedrohungen und Risikoprävention. Das Gesundheitswesen mit den Teilsektoren Krankenanstalten und Rettungsdienst zählt gemäß Netz- und Informationssystemsicherheitsgesetz zur Kritischen Infrastruktur. Die Schnittstelle zwischen der präklinischen und der klinischen Versorgung von Notfallpatient*innen sollte unter den Aspekten des NIS-Regimes betrachtet und näher untersucht werden.

Anhand der ausgewählten Literatur konnte ein umfassendes Verständnis für zwei wesentliche Bedrohungen von Kritischen Infrastrukturen erreicht werden. Mittels leitfadengestützten Interviews mit Expert*innen war die Verifikation bzw. Falsifikation zweier Hypothesen geplant.

Von den befragten Damen und Herren wurde die erste Hypothese bestätigt. Unsere moderne Gesellschaft ist von vernetzten Systemen geprägt. Der Begriff Autarkie von Organisationen steht dieser Verflechtung entgegen. Dies deckt sich mit den unterschiedlichen Literaturquellen.

Wenngleich die erste Annahme Zustimmung fand, so konnte zu der zweiten Behauptung keine einstimmige und abschließende Aussage erreicht werden. Intersektorale Interdependenzen wurden von allen Expert*innen genannt. Inwieweit die NIS-Gesetzgebung diesem Umstand Rechnung trägt wurde kontrovers bewertet.

In den weiteren Subkapiteln werden nun die einzelnen Themen des Untersuchungsgegenstands genauer erörtert.

10.1. Staatliche Reglements

Die Antwortauswertung ergab eine hohe Zustimmung zu gesetzlichen Vorschriften über den Schutz Kritischer Infrastrukturen bei den Interviewten. Sie beurteilen zum überwiegenden Teil die aktuellen nationalen und supranationalen Anstrengungen, die nationalen Kritischen Infrastrukturen auf Basis von gesetzlichen Vorschriften zu schützen, positiv. Die NIS-Vorschriften wurden als geeignete staatliche Regulierungsmaßnahme bewertet, um ein gleiches hohes Sicherheitsniveau bei Kritische Infrastrukturen in Österreich zu erzielen. Sie ist damit eine notwendige

Ergänzung zu bereits bestehenden Informationssicherheitsmanagementsystemen dieser wichtigen Einrichtungen in Österreich.

Durch ein hohes Schutzniveau für die Netzwerke und Informationstechnologien werde die Resilienz der Gesellschaft erhöht. Das ergebe folglich einen Mehrwert für diese, da ihre Existenz, der soziale Frieden und der Wohlstand gesichert seien. Die Expert*innen vertraten die Auffassung, dass Normen und Branchenstandards von Organisationen lediglich auf freiwilliger Basis befolgt würden. Mögliche Sanktionen bei Verstößen würden durch den Markt erfolgen. Der *Return on Investment* bei Ausgaben bzw. Investitionen in den Schutz und die Sicherheit lasse sich schwer abbilden. Der Betrieb eines Sicherheitsmanagementsystems sei relativ teuer. Den Expert*innen zufolge garantiere deshalb ein entsprechendes Gesetz die Umsetzung von Sicherheitsmaßnahmen.

10.2. Bedrohungen

Eine detaillierte Analyse von Risikobewertungen entsprach nicht der Zielsetzung dieser Arbeit. Staatliche Institutionen sind hiermit betraut. Sowohl das Bundesministerium für Inneres als auch jenes für Landesverteidigung unterhalten Lagezentren, berichten ihre Erkenntnisse und Einschätzungen an die zuständigen Stellen. In regelmäßigen Abständen werden zudem Weißbücher herausgebracht. Diese Dokumente stehen der Öffentlichkeit auf den Homepages des jeweiligen Ministeriums zum Download zur Verfügung.

Die gesellschaftlichen Folgen eines Cybernotfalls wurden von den befragten Expert*innen gegenüber jenen eines Blackouts als geringer eingeschätzt. Die medizinische Basisversorgung der Bevölkerung werde, zusammen mit anderen lebensnotwendigen Dingen, auch unter den erschwerten Bedingungen einer Katastrophe in der Bundeshauptstadt Wien fortgesetzt werden können.

Einschränkungen bei den Versorgungsprozessen wären durch einen Ausfall der IKT-Infrastruktur in unterschiedlichem Maße gegeben. Die Auswirkungen eines Blackouts wurden jedoch als gravierender eingestuft. Während bei einem Cyberangriff nur Teile der Gesellschaft unmittelbar betroffen wären, verhalte sich die Situation bei einem großflächigen und langanhaltenden Stromausfall anders. Es herrschte die übereinstimmende Meinung vor, dass ein Blackout sämtliche Gesellschaftsteile betreffen würde.

Mit Fortschreiten der Forschungsarbeit eskalierte die Situation an Europas östlicher Grenze. Das bis dahin abstrakte Risiko einer kriegerischen Auseinandersetzung wurde am 24.02.2022 Realität. Trotz der geopolitischen Entwicklung wurde der Umfang des Aspekts *Cyberwar* in der gegenständigen Abschlussarbeit nicht weiter ausgebaut.

10.3. Notwendigkeit zur Abstimmung

Die Interviewpartner*innen waren sich darüber einig, dass zur Bewältigung von Krisen und Katastrophen eine Kooperation über Systemgrenzen hinweg erforderlich sei. Einer gesamtgesellschaftlichen Bedrohung könne den Expert*innen zufolge auch nur dadurch begegnet werden, indem alle Involvierten zusammenarbeiten. Die Interviewpartner*innen betonten die große Bedeutung von Abstimmungen im Vorfeld und während dem Krisen- bzw. Katastrophenzustand.

Die tägliche Arbeit ist von Datentransfers, Informationsweitergaben und dem Teilen von Wissen geprägt. Digitale Systeme und Netzwerke unterstützen diese Prozesse und erleichtern die Tätigkeit. (vgl. Art. 4 Abs. 1 NIS-RL) Mit der Vernetzung von Systemen erhöht sich das Risiko der Ausbreitung von schädlichen Programmen. Das vollständige Abschotten des eigenen Netzwerks nach außen hin um dieses zu schützen steht im Widerspruch zum Bedarf des Informations- und Datenaustauschs. Folglich ergibt sich für die IKT-Sicherheitsverantwortlichen die Herausforderung der Gradwanderung zwischen einem reibungslosen Datentransfer einerseits und dem hohen Schutz der Netzwerke und Systeme andererseits.

11. Ausblick

Kritische Infrastrukturen sehen sich mit einer Vielzahl an Bedrohungen konfrontiert. Mit der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (kurz NIS-RL), wurde eine gesetzliche Grundlage für ein EU-weit harmonisiertes hohes Schutzniveau gegenüber Risiken für Netzwerke und Informationssysteme geschaffen.

Die aktuell thematisierte NIS-Richtlinie befindet sich in Überarbeitung und soll durch die sogenannte NIS 2 Richtlinie ersetzt werden. Sie wird die Grundlage für Maßnahmen des Cybersicherheitsmanagements bilden. Es ist beabsichtigt, nationale Unterschiede innerhalb der Europäischen Union mit der Richtliniennovelle zu reduzieren. (vgl. 2020/0359 (COD))

In den letzten Jahren und der jüngsten Vergangenheit wurden zwei abstrakte Risiken Realität. Sowohl die COVID-19 Pandemie als auch ein Krieg an Europas Grenze beherrschen täglich die Medienlandschaft. Die Europäische Union und die Republik Österreich blieben bisher von einer groß angelegten und koordinierten Cyberattacke verschont. Bisherige Cyberangriffe beschränkten sich auf einzelne Institutionen mit geringen Auswirkungen für die Bevölkerung. Auch ein großflächiger Stromausfall konnte bisher mit den etablierten Notfallverfahren abgewendet werden.

In welchem Ausmaß die NIS-Richtlinie unterstützt, Auswirkungen von Angriffen auf Kritische Infrastrukturen zu reduzieren, wird möglicherweise die nahe Zukunft zeigen. Der anhaltende kriegerische Konflikt in der Ukraine wird von feindseligen Handlungen im Cyberraum begleitet (vgl. BfV 2022: 1f.; HHS 2022: 1ff.; ISPK 2022: 10).

Ein weiteres Kapitel in der hybriden Feindseligkeit stellen reduzierte Gaslieferungen in EU-Mitgliedstaaten dar. Gaskraftwerke sind derzeit für den sicheren Betrieb des Stromnetzes von wesentlicher Bedeutung. Sie werden kurzfristig aktiviert und decken damit Lastenspitzen ab umso das Stromnetz stabil zu halten. (vgl. APG 2020: 31) Mit Einschränkung oder gar dem Wegfall dieser Steuerungsmöglichkeit erhöht sich die Gefahr eines umfassenden Stromausfalls welcher sich zu einem Blackout ausweiten könnte.

Die Awareness für Bedrohungen der Gesellschaft und die Unterstützung der Bevölkerung bei der Bevorratung von lebenswichtigen Gütern sollte gefördert werden. Diese Empfehlung ist an sich nicht neu. In der Zeitschrift Truppendienst wurde das Szenario Blackout bereits vor zehn Jahren behandelt (vgl. Ladinig und Saurugg 2012: 34ff.). Auch der Österreichische Zivilschutzverband erinnert regelmäßig an die Notwendigkeit zur Bevorratung von Lebensmitteln und anderen Gütern des täglichen Bedarfs (vgl. NÖZSV 2020: 20f.).

Wenngleich die Bedrohungslage eines Blackout-Szenarios zunehmend von Medien in die Öffentlichkeit getragen wird, ist fraglich, ob die erforderlichen Vorbereitungen vom Großteil der Gesellschaft ergriffen werden. Eine gesetzliche Verpflichtung für Privathaushalte, ein Notfalldepot anzulegen, erscheint jedoch nicht erstrebenswert.

Kurzfassung

Kritische Infrastrukturen sind per Definition für den Erhalt gesellschaftlicher Funktionen und des Zusammenlebens essenziell. Sie sehen sich einer Vielzahl von Gefahren ausgesetzt. Mit der NIS-Richtlinie soll in der gesamten Europäischen Union ein hohes und einheitliches Schutzniveau vor Bedrohungen aus dem Cyberraum erreicht werden. 2018 wurde in Österreich auf Basis der NIS-Richtlinie das NISG veröffentlicht.

Gegenständige Arbeit betrachtet die Umsetzung des Gesetzes durch Kritische Infrastrukturen des Wiener Gesundheitswesens. Der Fokus liegt auf der Gewährleistung einer präklinischen Notfallversorgung durch den kommunalen Rettungsdienst und der Folgebehandlung in den Wiener Krankenanstalten. Diese muss auch unter den Auswirkungen eines umfassenden Cyberangriffs auf Kritische Infrastrukturen oder bei einem Blackout-Szenario sichergestellt sein.

Mit der Umsetzung von Vorgaben aus der NIS-Gesetzgebung sollen die Effekte von Cyberangriffen abgeschwächt werden. Die Arbeit beschreibt Folgen erfolgreicher Attacken auf die Netzwerke von Kritischen Infrastrukturen. Diese Einrichtungen sind für den Erhalt gesellschaftlicher Funktionen und für das Zusammenleben von größter Bedeutung. Welche Anlagen und Organisationen als kritisch einzustufen sind wird anhand einschlägiger Definitionen in den Anfangskapiteln erläutert.

Aufgrund der Vernetzung der Kritischen Infrastrukturen sowohl über Sektoren- als auch Staatsgrenzen hinweg, bestehen starke, nichtlineare gegenseitige Abhängigkeiten voneinander. Diese Interdependenzen werden aufgezeigt und am Beispiel des Gesundheitssektors detaillierter dargestellt.

Das Ergebnis leitfadengestützter Interviews mit Expert*innen ergab eine positive Bewertung der gesetzlichen Verpflichtungen für Betreiber*innen Kritischer Infrastrukturen, ihre Netz- und Systemlandschaft gegenüber Angriffen zu härten. Aufholbedarf orteten die befragten Personen bei der Awareness breiter Bevölkerungsanteile für den Blackout-Fall. Die Bevorratung von lebensnotwendigen Gütern in Privathaushalten sollte demnach forciert werden. Nach Ansicht eines überwiegenden Teils der Expert*innen erscheint die Betrachtung von einzelnen abgegrenzten Sektoren wie sie in der EU-Richtlinie erfolgt, überholt. Ein prozessorientierter Ansatz entspricht deren Meinung nach eher der Notwendigkeit. Der Bedarf ergäbe sich aus der Vernetzung der Abläufe und involvierten Systemen.

Abstract

Critical Infrastructures are, by definition, crucial for the maintaining of societal function and co-existence as a whole. These functions are exposed to a myriad amount of threats. For top, and uniform, levels of consistency the NIS guideline is established for the European Union as a whole. This is to provide a consistent level of protection in cyberspace. In 2018 Austria published the NIS law, which is based on the NIS guideline.

This paper views the implementation of the law for the Critical Infrastructure of the Viennese Health Care System. The focus of it is the assurance of the preclinical Emergency Care, by municipal Ambulance and follow up care in Viennese hospitals. This has to happen, even in the events of cyberattacks on Critical Infrastructures, or in case of a blackout.

With the implementation of the given specifications pf the NIS-legislation the effects of Cyberattacks should be weakened. This paper describes the consequences of successful attacks on critical infrastructure networks. These institutions, necessary for the upkeep of societal functions and society, are of greatest importance. Which investments and organizations have to be seen as critical, is explained by the relevant definitions in the beginning chapters.

Because of the integration of critical infrastructures, spanning sectors and national borders, there exist a strong non-linear dependency on one another. This interconnectedness is shown and explained through the Healthcare sector in greater detail.

The outcome of guided expert interviews shows a positive evaluation of the legal obligations of the operators of critical infrastructures, their network and system landscape, to strengthen their defence against such attacks. Improvements, according to the people in question, are necessary at the awareness level of the broader public in case of a blackout. The necessity of life-saving goods in private households should be a bigger focus. The view of most experts is that the consideration of individual, closed-in sectors, according to EU Legislation, is obsolete. A process oriented approach, based on their opinion, is the more sensible approach that comes from the network of integrated systems.

Quellenverzeichnis

2020/0359(COD) (2021): Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 – Brüssel.

ACHLEITNER F. (2015): Öffentlich-rechtliche Grundlagen des österreichischen Rettungs- und Krankentransportwesens unter näherer Betrachtung der Situation in der Steiermark. – Diplomarbeit – Graz.

AHNEFELD F.W. (2003): Die Rettungskette. – In: Notfall & Rettungsmedizin. – Heidelberg.

ALHELOU H.A., HAMEDANI-GOLSHAN M.E., NJENDA T.C. und SIANO P. (2019): A Survey on Power System Blackout and Cascading Events. Research Motivations and Challenges. – In: Energies – Basel.

APCIP (2015): Österreichisches Programm zum Schutz kritischer Infrastruktur. – Wien.

APCIPL (2016): Beteiligung der Bundesländer am APCIP. Länderprogramm Schutz kritischer Infrastruktur (APCIP Länder) – o.O.

APG (2020): Geschäftsbericht 2019. Austria Power Grid. – Wien.

AUER M. (2018): Rechtswissenschaft zwischen Rechtsdogmatik und Grundlagenfächern. – In: Zum Erkenntnisziel der Rechtstheorie. Philosophische Grundlagen multidisziplinärer Rechtswissenschaft – Baden-Baden. Band 54.

BABS (2020): Katastrophen und Notlagen Schweiz 2020 / Gefährdungsdossier. – Bern.

BAJRAMOVIC E., GUPTA D., GUO Y., WAEDT K. und BAJRAMOVIC A. (2019): Security Challenges and Best Practices for IIoT. – Bonn.

BfV (2022): Bundesamt für Verfassungsschutz. – Sicherheitshinweis für die Wirtschaft | 01/2022 | 04.03.2022 – Betreff | Krieg in der Ukraine. – Berlin.

BIRKMANN J., BACH C., GUHL S., WITTING M., WELLE T. und SCHMUDE M. (2010): Forschungsforum Öffentliche Sicherheit. – In: Schriftenreihe Sicherheit Nr. 2. – Berlin.

BKA (2021): Bundeskanzleramt. – Bericht Cybersicherheit für das Jahr 2020. – Wien.

BLASCHE G., WEITENSFELDER L., DEBLOOM J. und GOLLNER (2021): Studie über den Effekt des CoViD-19 assoziierten Lockdowns in Österreich auf Erholung und Wohlbefinden – Zwischenergebnis auf Basis der ersten Befragung vom 19.1.-7.2.2021. – Wien.

BLASCHKE W. (2017): Auswirkungen eines längerdauernden großflächigen Stromausfalls auf kritische Infrastrukturen, mit Berücksichtigung der Stromeigenerzeugung der ÖBB. – Masterthesis. – Wien.

BMASGK (2019): Bundesministerium für Arbeit, Soziales, Gesundheit und Konsumentenschutz. – Das österreichische Gesundheitssystem: Zahlen – Daten – Fakten. – Wien.

BMdI (2011): Bundesministerium des Inneren. – Schutz Kritischer Infrastrukturen. – Risiko- und Krisenmanagement: Leitfaden für Unternehmen und Behörden. – Berlin.

BMLV (2022): Bundesministerium für Landesverteidigung. – Sicher. Und morgen?: Risikolandschaft Österreich 2022. – Wien.

BREUER F., BRETTSCHNEIDER P., KLEIST P., POLOCZEK S., POMMERENKE C. und DAHMEN J. (2021): Erkenntnisse aus 31 Stunden Stromausfall in Berlin Köpenick – medizinische Schwerpunkte und Herausforderungen. – In: der Anaesthesist. – online Publikation. – o.O.

BRH (2020): Bundesrechnungshof. – Rettungswesen in Wien. – Bericht des Rechnungshofes: Anhang 3. – Wien.

BSI (2020): Bundesamt für Sicherheit in der Informationstechnik. – Informationssicherheit mit System. – Der IT-Grundschutz des BSI. – Bonn.

B-VG (1994): Bundes-Verfassungsgesetz. – Wien.

BVT (2014): Sicherheitsinformation für Eigentümer/Betreiber Kritischer Infrstruktureinrichtungen in Österreich. – Informationsbroschüre. – Wien.

COM(2006) 786 (2006): Commission oft he European communities. – Communication from the commission on a European Programme for Critical Infrastructure Protection. – Brüssel.

E-CONTROL (2021): Ausfall- und Störungsstatistik für Österreich 2021. – Ergebnisse für das Jahr 2020. – Wien.

E-CONTROLG (2022): Bundesgesetz über die Regulierungsbehörde in der Elektrizitäts- und Erdgaswirtschaft (Energie-Control-Gesetz – E-ControlG). – Wien.

ERLÄUTERUNGEN-NISG (2018): 369 der Beilagen XXVI. GP - Regierungsvorlage – Erläuterungen. – Wien.

GIESE F. (1962): Rechtsentstehung. – In: Recht und Rechtswissenschaft. Wiesbaden.

GOLEM.DE (2022): https://www.golem.de/news/malware-russischer-cyberangriff-auf-ukrainisches-stromnetz-2204-164582.html. – abgerufen 17.07.2022

GRETHE C. (2019): Gesundheitsberatung 1450. – In: Soziale Sicherheit. – Wien.

HERZOG S. (2011): Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. – In: Journal of Strategic Security. – online Publikation. – o.O.

HHS (2022): HHS Cybersecurity Program. – The Russia-Ukraine Cyber Conflict and Potential Threats tot he US Health Sector. – online Publikation. – o.O.

HOFMARCHER M. (2013): Das österreichische Gesundheitssystem. – Akteure, Daten, Analysen. – Wien.

HUMENBERGER M. (2022): Herausforderungen im und aus dem Cyberraum. – In: Bundesministerium für Landesverteidigung. – Sicher. Und morgen?. – Risikolandschaft Österreich 2022. – Wien.

ISPK (2022): Institut für Sicherheitspolitik an der Universität Kiel. – Die militärische Lage in der Ukraine zwei Monate nach Beginn des Überfalls und die Aussichten für eine Beendigung des Krieges. – online Publikation. – Kiel.

TANNER C. (2022): Mit voller Energie gegen den Blackout. – In: iv-positionen. – Das Magazin der Industrie. – Wien.

KAKUG (2022): Bundesgesetz über Krankenanstalten und Kuranstalten (KAKuG). – Wien.

KNAUF A. (2020): Urbane Resilienz gegenüber Stromausfällen in deutschen Großstädten. – Wiesbaden.

KRINGS S. (2020): Doppelt relevant: Kritische Infrastrukturen der Daseinsvorsorge. – In: Raumforschung und Raumordnung. – online Publikation. – o.O.

KRÖGER W. (2016): Den Stromfluss sicherstellen. – In: Sicherheitsgemeinschaft. – Das OSZE Magazin. – Wien.

KUHN J. (2005): Der Schutz Kritischer Infrastrukturen. – Unter besonderer Berücksichtigung von kritischen Informationsstrukturen. – Hamburg.

LADINIG U. und SAURUGG H. (2012): Blackout. – In: Truppendienst. – Wien. Nr. 325

LANGGUTH A. und PRETZELL M. (2020): Kleine Anfrage 4528 der Abgeordneten Alexander Langguth und Marcus Pretzell. – Auf neuem Höchststand: Hacker-Angriffe auf Krankenhäuser und Kritische Infrastrukturen. In: Landtag Nordrhein-Westfahlen. – Nordrhein-Westfalen.

LEOPOLD H. (2017): Cyber Security für Kritische Infrastrukturen. – Erhöhte Cyber-Sicherheit für unsere kritischen Infrastrukturen verlangen umfassende gemeinsame Forschungsaktivitäten aller Stakeholder. – In: Elektrotechnik & Informationstechnik. – Wien.

LORENZ D. (2010): Kritische Infrastrukturen aus Sicht der Bevölkerung. – Berlin.

MADNICK S. (2022): What Russia’s Ongoing Cyberattacks in Ukraine Suggest About the Future of Cyber Warfar. – In: Harvard Business Review. – online Publikation. – o.O.

MAGISTRAT DER STADT WIEN (2021): Statistisches Jahrbuch der Stadt Wien 2021. – Wien in Zahlen. – Wien.

MAYER S. (2020): „Rechtliche Fragestellungen in der nationalen Umsetzung der Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen (NIS-RL)“. – Dissertation. – Wien.

MAYRING P. (2015): Qualitative Inhaltsanalyse. – Grundlagen und Techniken. – 12. Auflage. – Weinheim/Basel.

MOTEFF J. und PARFOMAK P. (2004): CRS Report for Congress. – Critical Infrastructure and Key Assets: Definition and Identification. – Washington.

MORAN STRITCH, M., WINTERBURN, M. und HOUGHTON, F. (20121): The Conti Ransomware Attack on Healthcare in Ireland: Exploring the impacts of a Cybersecurity Breach from a Nursing Perspective. – In: Canadian Journal of Nursing Informatics. – online Publikation. – o.O.

MURRAY C. (2017): Healthcare Access and Quality Index based on mortality from causes amenable to personal health care in 195 countries and territories, 1990–2015: a novel analysis from the Global Burden of Disease Study 2015. – In: The Lancet. – online Publikation. – o.O. – Band 390.

NISG (2018): Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG). – Wien.

NIS-RL (2016): RICHTLINIE (EU) 2016/1148 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union. – Brüssel.

NISV (2019): Verordnung des Bundesministers für EU, Kunst, Kultur und Medien zur Festlegung von Sicherheitsvorkehrungen und näheren Regelungen zu den Sektoren sowie zu Sicherheitsvorfällen nach dem Netz- und Informationssystemsicherheitsgesetz (Netz- und Informationssystemsicherheitsverordnung – NISV). – Wien.

NÖZSV (2020): Safety-Ratgeber Blackout. – Was tun ohne Strom. – Tulln.

ORKB (2020): Prüfungskompendium. – Cybersicherheit in der EU und ihren Mitgliedstaaten. – Brüssel.

OSCE (2016): Protecting Electricity Networks from Natural Hazards. – Wien.

OSCE (2022): Cyber/ICT Security. – Wien.

ÖSCS (2021): Österreichische Strategie für Cybersicherheit 2021, - Wien.

PAUSCH G. (2017): Blackout und seine Folgen. – Fallstudie. – o.O.

REISINGER A. (2012): Rettungsdienst in Österreich. – Herausforderungen an Ausbildung und strukturelle Entwicklung. – Masterarbeit. – Linz.

REISNER M. (2021): Blackout – Wenn unsere Resilienz gefordert ist. – In: Truppendienst. – Wien. – Nr.382.

REUTERS.COM (2022): https://www.reuters.com/world/europe/ukrainian-government-foreign-ministry-parliament-websites-down-2022-02-23/. – abgerufen 18.07.2022

RL 2008/114/EG 2008 (2008): RICHTLINIE 2008/114/EG DES RATES vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern. – Brüssel.

RTR (2022): Rundfunk und Telekom Regulierungs-GmbH, https://www.rtr.at/TKP/was_wir_tun/telekommunikation/konsumentenservice/information/informationen_fuer_konsumenten/TKKS_Notrufe.de.html. – abgerufen 15.07.2022.

SAURUGG H. (2021): Blackout. – Ist die Bevölkerung vorbereitet?. – In: Truppendienst. – Wien. – Nr.382.

SAURUGG H. (2022): Potenzielle Systemkrise Blackout. – Der unterschätzte Lieferkettenkollaps. – In: Bundesministerium für Landesverteidigung. – Sicher. Und morgen?: Risikolandschaft Österreich 2022. – Wien.

StRH (2010): Unternehmung "Wiener Krankenanstaltenverbund", Notstromaggregate in Krankenanstalten. – Tätigkeitsbericht 2010. – Wien.

TKG 2021 (2021): Bundesgesetz, mit dem ein Telekommunikationsgesetz (Telekommunikationsgesetz 2021 – TKG 2021) erlassen wird. – Wien.

WERKNER I. und SCHÖRNIG N. (2019): Cyberwar – die Digitalisierung der Kriegsführung. – Wiesbaden.

WRKG (2019): Wiener Rettungs- und Krankentransportgesetz – WRKG. – Wien.

Anhang

Interviewleitfaden in der Version 1.1 vom 10.04.2022

1. Die Europäische Richtlinie (EU) 2016/1148 des Europäischen Parlaments wurde mit dem Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG) in Österreich umgesetzt. Bereits zuvor existierten Konzepte bei den verschiedenen Kritischen Infrastrukturen um ein hohes Schutzniveau vorzuweisen. Seit 2008 gibt es die EU Richtlinie 2008/114/EG mit EPCIS.

    a. **Wie ordnen Sie die Notwendigkeit für eine gesetzliche Regulierung zur Einhaltung von IKT-Sicherheitsstandards ein, zumal von vielen KRITIS ein ISMS implementiert wurde und betrieben wird?**

    b. **Worin liegt Ihrer Meinung nach der Mehrwert für die Gesellschaft durch die bundesgesetzliche Regelung?**

2. Der Schutz Kritischer Infrastruktur inklusive Cybersicherheit ist in Österreich grundsätzlich im Österreichischen Programm zum Schutz Kritischer Infrastruktur (APCIP) seit 2008 beschrieben. Diese Strategie zählt bereits eine Vielzahl an Infrastrukturen mitsamt deren Systemen, Anlagen, Netzwerken usw. auf, welche als für das gesellschaftliche Gefüge notwendig erachtet werden. Zusätzlich wurde im Jahr 2013 die Österreichische Strategie für Cybersicherheit (ÖSCS) veröffentlicht. Beide Sicherheitsstrategien wurden inzwischen erneuert. APCIP im Jahr 2014 und ÖSCS zuletzt 2021. Weiters wurden von der Internationalen Organisation für Normung – ISO – mehrere Standards veröffentlicht die die Sicherheit von Organisationen erhöhen sollen.

    a. **Welche Bedeutung messen Sie diesen beiden Strategien und Normen im Vergleich zum NIS-G bei?**

3. Organisationen sind einem breiten Spektrum an Bedrohungen ausgesetzt. Sicherheits- und Risikomanagement stellen per se Querschnittsmaterien dar um Gefahrenpotentiale möglichst vollständig zu identifizieren und zu analysieren. Das Regime der NIS-Richtlinie befasst sich folglich nicht ausschließlich mit Beeinträchtigungen der Netz- und Informationssysteme durch Cyberangriffe. Auch technische Gebrechen oder Naturgefahren die zu Störungen oder gar Ausfällen

führen können sind von der NIS-RL erfasst. Risikomanagement befindet sich am Anfang von elf Punkten betreffend Sicherheitsmaßnahmen laut NIS-Verordnung.

   a. **Welche Risikoszenarien für Kritische Infrastrukturen kommen Ihnen in den Sinn und welche betrachten Sie aktuell als vorrangig?**

4. Neben Kriminellen sind auch staatliche Akteure im Cyberraum als Hacker aktiv. Moderne militärische Konfliktszenarien sind durch eine hybride Kriegsführung geprägt. Cyberattacken sind mittlerweile als fester Bestandteil einer kriegerischen Handlung anzusehen und begleiten diese. Der Cyberwar beschränkt sich dabei nicht nur auf die militärische IKT-Infrastruktur. Zivile Einrichtungen die zur Kritischen Infrastruktur zählen, wie etwa Banken, Krankenhäuser und Energieversorgungssysteme wurden beispielweise 2007 in Estland und jüngst in der Ukraine im Cyberraum angegriffen. Solche Attacken zielen auf eine weitere Destabilisierung des angegriffenen Landes ab.

   Die US-Behörde Cybersecurity and Infrastructure Security Agency (CISA) warnte, dass Russland mit seinen Cyberattacken auch Ziele außerhalb der Ukraine ins Visier nehmen könnte. Auch deutsche Sicherheitsbehörden rechnen mit weiteren Angriffen. Das BSI in Deutschland sieht aktuell eine erhöhte Bedrohungslage für Kritische Infrastrukturen. Es veröffentlichte am 17.03.2022 einen Sonderlagebericht im Zusammenhang mit der russischen Invasion der Ukraine. Darin wird vor möglichen Angriffen auf sogenannte Hochwertziele, z.B. Energieversorger, gewarnt.

Aufgrund des derzeitigen Engagements ist anzunehmen, dass andere europäische Staaten eher ins Visier von russischen Hackern genommen werden, als Österreich. Erfolgreiche Cyberattacken auf das Deutsche Energienetz haben allerdings auch negative Auswirkungen auf andere EU Länder. Ein weitreichender Stromausfall – Blackout – wäre eine mögliche Folge.

   a. **Wie schätzen Sie die Bedrohung für Österreich durch einen solchen Kollateralschaden ein?**

5. Ein Blackout im Sinne eines überregionalen, mehrere Tage andauernden Stromausfalls stellt eine erhebliche Bedrohung für das gesellschaftliche Gefüge dar. Der Eintritt eines solchen Ereignisses wird von mehreren Expertinnen und Experten innerhalb der nächsten fünf Jahre erwartet. Ein potentielles Blackout wird häufig als Worst-case-Szenario als Belastungstest des Betriebskontinuitätsmanagements herangezogen. Krisen- bzw. Katastrophenpläne von KRITIS zielen auf die Bewältigung eines solchen Ereignisses ab.

   a. **Welche Maßnahmen hat Ihre Organisation gesetzt um auf ein Blackout-Szenario vorbereitet zu sein?**

   b. **Inwieweit werden andere Interessensgruppen dabei berücksichtigt?**

6. Die vernachlässigte Eigenbevorratung im urbanen Raum wird durch mehrere Studien belegt. Aus diesem Grund muss bei einem Blackout-Ereignis davon ausgegangen werden, dass die (Wiener) Bevölkerung mangels Eigenbevorratung spätestens nach einigen Tagen jene Objekte aufsuchen wird, die weiterhin eine gewisse rudimentäre Versorgung mit Wasser, Wärme und Strom bewerkstelligen können. Diese sind in erster Linie zu den KRITIS zu zählen. KRITIS sind jedoch nicht als Betreuungseinrichtungen für Betroffene ausgerichtet.

   a. **Wie soll Ihrer Meinung nach diesem Problem begegnet werden?**

7. An erster Stelle ist der Energiesektor im NIS-G und der NIS-Verordnung genannt. Bei allen modernen Systemen besteht eine hohe Abhängigkeit von elektrischem Strom. Die komplexe Vernetzung des Stromsektors mit anderen Kritischen Infrastrukturen ist offensichtlich. Ihm kommt somit eine zentrale Bedeutung zu. Dennoch darf die Aufzählung von Sektoren nicht mit einer Wertung bzw. prioritären Reihung gleichgesetzt oder so interpretiert werden.

   a. **Geht die NIS-Gesetzgebung Ihrer Meinung nach ausreichend auf die wechselseitigen Interdependenzen ein?**

8. Die medizinische Behandlung von Erkrankten oder Verletzten kann als ineinandergreifende Kette von Behandlungsprozessen angesehen werden. Der Behandlungspfad beginnt mit der Ersten Hilfe durch Laien mitsamt der Notrufmeldung über die qualifizierte Erste medizinische Hilfe durch Rettungsteams und den Transport bis hin zu den einzelnen fachmedizinischen und diagnostischen Leistungen im Krankenhaus.

   a. **Wie beurteilen Sie den Begriff „Autarkie“ im Rahmen vernetzter und systemübergreifender Prozessketten?**

9. Von der Berufsrettung Wien und deren Partnerorganisationen im Rettungsverbund werden täglich zwischen 800 und 1.000 Notfallpatient*innen in Wiener Krankenanstalten zur medizinischen Folgeversorgung gebracht. Zusätzlich versorgen die Spitäler in Wien tausende weitere Personen im Rahmen von Selbsteinweisungen und in der ambulanten Nachsorge. Die Kapazitäten und Strukturen der Krankenhäuser sind dabei auf die individualmedizinische Versorgung unter „normalen“ Betriebsbedingungen ausgelegt.

   a. **Welche Maßnahmen erachten Sie als sinnvoll damit eine medizinische Basisversorgung eines Großteils der Betroffenen auch unter negativen Auswirkungen eines Cybernotfalls oder eines Blackouts sichergestellt werden kann?**

Interview mit Herrn Mag. Auer am 17.05.2022

A: 17. Mai. 2022, Interview mit Hrn. Mag. Auer, Berufsrettung Wien. Sehr geehrter Herr Mag., die europäische Richtlinie zur Stärkung des Netz- und Informationssicherheitssystems, wird in Österreich mit einem Gesetz umgesetzt. Vorab gab es bereits im Rahmen von Bemühungen zur Stärkung der Resilienz europäischer kritischer Infrastrukturen, das Absys und das Absip Programm, wie ordnen Sie die Notwendigkeit für eine zusätzliche Regulierung zur Einhaltung von IKT Sicherheitsstandards ein, zumal bereits viele kritische Infrastrukturen ein Informationssicherheitsmanagementsystem implementiert haben und betreiben?

B: Meiner Meinung nach ist prinzipiell eine gesetzliche Regelung zu begrüßen, aus dem einfachen Grund, dass es ja nicht überall große Unternehmen sind, die kritische Infrastruktur betreiben, wie z.B. kleine Leitstellen im Burgenland usw. Die müssten natürlich einen weitaus höheren und prozentuellen Bedarf auftreiben, auch an Budget um minimale Standards auch tragen zu können. Der Datenaustausch findet auch trotzdem mit anderen Unternehmen statt, also ist es sicher wichtig, dass man einen Mindeststandard definiert, der auch eingehalten wird.

A: Und das eben per Gesetz und nicht per Normen oder dergleichen?

B: Das Problem der Normen ist immer, dass sie umgesetzt werden sollten, aber nicht zwingend erforderlich sind, die Kontrolle von Normen auch weitaus schwieriger ist. Weil man dann einen Anlassfall braucht, den man bei einem gesetzlichen nicht so ist.

A: Und worin liegt jetzt konkret der Mehrwert für die Gesellschaft durch eine bundesgesetzliche Regelung?

B: Prinzipiell wäre es mir egal, wenn es jetzt eine landesgesetzliche Regelung oder eine bundesgesetzliche Regelung ist, der Mehrwert ist ganz einfach da und auch die Sicherheit der Bevölkerung mehr gegeben ist, wenn man schaut, dass diese ganzen Systeme aufrecht erhalten bleiben, solange es geht.

A: Gut, ich habe es schon erwähnt, der schutzkritische Infrastruktur inkl. Cybersicherheit ist bereits im österreichischen Programm zum Schutz kritischer Infrastruktur Absip seit 2008 beschrieben. Diese Strategie zählt bereits eine Vielzahl an Infrastrukturen mitsamt deren Systemen, Anlagen und Netzwerken auf. Welche

Bedeutung messen Sie den beiden Strategien, eben Absip auf der einen Seite und Normen auf der anderen Seite, wie die ISO27000 im Vergleich zum NIS-Gesetz, bei?

B: Kann ich mich nur von vorher wiederholen. Normen und Strategien sind sehr schön und müssen nicht umgesetzt werden, können umgesetzt werden, können auch erst im Anlassfall kontrolliert werden und Gesetze können auch vorgeschrieben werden, sind auch vorgeschrieben und können in weiterer Folge dann auch exekutiert werden, wenn etwas nicht so passt.

A: Gut danke. Organisationen sind einem breiten Spektrum an Bedrohungen ausgesetzt. Sicherheitsmanagement, Risikomanagement sind per se ja Querschnittsmaterien und es ist Ziel die Gefahrenpotentiale möglichst vollständig zu identifizieren und zu analysieren. Welche Risikofaktoren für kritische Infrastrukturen kommen Ihnen in den Sinn und welche betrachten Sie aktuell als vorrangig?

B: Oh, da gibt es viele. Schon alleine aus dem Hintergrund, dass viele Daten ausgetauscht werden zwischen vielen kritischen Infrastrukturen, wobei es ja nicht nur alleine die Datenlage ist, wir haben immer noch die Bedrohung von Cyberkriminalität, weil wir jetzt gerade darüber reden, aber natürlich auch Anschläge, Stromausfälle, sonstiges. Welches das höchste Risikoszenario ist, lässt sich in der heutigen Zeit nicht wirklich einschätzen. Man muss sie alle betrachten und meiner Meinung nach einfach das Beste dagegen tun, ob es jetzt ausreicht, wird die Zukunft weisen.

A: Die kriminellen Cyberaktivitäten sind schon angesprochen worden, dann gibt es natürlich auch staatliche Akteure im Cyberraum, die Hackerangriffe durchführen. Jetzt durch den Ukrainekrieg sind immer wieder auch Institutionen aus den baltischen Staaten Opfer von solchen Attacken geworden. Im Zusammenhang mit dem Ukraine-Konflikt hat sich die österreichische Bundesregierung klar zu einer neutralen Haltung positioniert, im Gegensatz zu Deutschland. Deutschland liefert unter anderem auch Waffensysteme und es könnte daher sein, dass das deutsche Energienetz im Rahmen von Repressalien gehackt wird und es zu einem Stromausfall kommt. Wie schätzen Sie die Bedrohung von Österreich durch einen Kollateralschaden, wenn das deutsche Stromnetz beschädigt wird, für Österreich ein?

B: Prinzipiell sehr hoch, da wir meines Wissens auch Strom aus Deutschland beziehen. Wobei ich eher die Kollateralschäden in einem eher späteren Zeitpunkt sehe. Der Strom wird, wie es viele Studien auch zeigen, relativ schnell wieder

hergestellt sein, die Logistik und die Datenstruktur wird sehr lange Zeit brauchen, bis sie wieder hergestellt ist und da wir doch sehr viel Datenaustausch meines Wissens nach, auch mit Deutschland haben, wir doch auch viele Produkte aus Deutschland beziehen, wird der Kollateralschaden sich nicht momentan zeigen, meiner Meinung nach, sondern erst Tage später, aber dafür umso größer, als der fehlende Strom bei uns sich auswirken wird.

A: Blackout wird verstanden als ein überregionaler, über mehrere Tage andauernder Stromausfall. Und stellt natürlich auch eine Bedrohung für das gesellschaftliche Gefüge dar, da heutzutage alle modernen System mit Strom betrieben werden. Experten schätzen die Möglichkeit eines Blackouts ein, dass das innerhalb der nächsten 5 Jahre zu erwarten sein wird. Welche Maßnahmen hat Ihre Organisation gesetzt, um ein Blackoutszenario, um darauf vorbereitet zu sein?

B: Das ist jetzt außer dem Protokoll, bitte nicht mitschreiben, dass musst du besser wissen als ich bei unserer Organisation, streichen, Ende. Prinzipiell sind unsere Einsatzstellen alle mit Notstromaggregaten ausgerüstet, es werden, oder sind Pläne ausgearbeitet, wie bei einem Blackout vorzugehen ist, es gibt mobile Tankstellen, um auch die Notstromaggregate wieder zu befüllen, die Pläne werden laufend evaluiert. Derzeit findet eine ganz große Evaluation statt, man schaut, dass man auch mit anderen Organisationen gemeinsame Pläne erarbeitet, wie z.B. mit der Polizei, die dann auch Sicherheitsplätze usw. einrichtet, wo dann auch das Personal auch Ihre Angehörigen abgeben kann, oder dort hinverbringen kann, während sie im Dienst sind und in Sicherheit wissen. Ich glaube, dass da sehr viel gerade im Entstehen ist, was ich schade finde, ist dass sehr gerne auch für einen kurzzeitigen, 20-minütigen Stromausfall in einem Wiener Gemeindebezirk als Blackout bezeichnet wird. Ich glaube, dass da Abgrenzung zu den wirklich kleinen Stromausfällen zu einem wirklichen Blackout noch viel mehr publiziert werden müssten, bekannt gemacht werden müsste.

A: Verstehe okay, gut. Ja aus dem Grund eben auch diese klare Abgrenzung, dass es eben auch nicht nur mehrere Tage dauert, sondern auch noch überregional ist, diese Faktoren müssen eben zusammenspielen, um wirklich von einem Blackoutszenario sprechen zu können. Und Sie haben es auch schon angesprochen, es werden noch andere Interessensgruppen bei der Erstellung von Blackoutkonzepten Ihrer

Organisation mit eingebunden, berücksichtigt, so dass das nicht nur im stillen Kämmerchen entsteht und dann unabgestimmt im Anlassfall aktiviert wird.

B: Genau, z.B. eines der Beispiele ist eine nicht stromabhängige Telefonleitung zu den anderen Einsatzorganisationen, um auch Kommunikation im stromlosen Zustand zu haben.

A: Kommen wir kurz zur Bevölkerung, es gibt unzählige Studien, wonach die Eigenbevorratung im urbanen Raum eher vernachlässigt ist. Man ist es heutzutage gewohnt, wenn man Hunger hat, man bestellt sich etwas im Internet oder geht zum Nahversorger. Jetzt ist davon auszugehen, dass bei einem längeranhaltenden Blackout-Ereignis die Wiener Bevölkerung mangels Eigenbevorratung, dann Objekte aufsuchen wird, wo nach wie vor rudimentäre Wasser- , Strom- und Wärmeversorgung gewährleistet ist. Das ist wiederum nicht die Hauptaufgabe von kritischen Infrastrukturen, die Bevölkerung dann mit Essen und Wärme oder Strom zu versorgen. Wie sollte, Ihrer Meinung nach, dem Problem begegnet werden, dass dann eben die Bevölkerung kritische Infrastrukturen aufsuchen wird, um sie als Betreuungseinheit zu nutzen?

B: Ich glaube, das ist die Gretchenfrage, auf die man so wirklich keine Antwort hat. Wichtig wäre es und wird auch laufend von uns betrieben, nicht mit dem Nachdruck wie ich es mir wünschen würde, einfach Aufklärungsarbeit zu leisten. Ich verstehe es auch teilweise, wenn man sich die Wohnungsbedingungen vieler Teile der Bevölkerung anschaut, in kleinen Wohnungen, in kleinen Kellerabteilen dann noch Essensvorräte auf Lager zu legen ist oft doch eine logistische Herausforderung den Platz einmal überhaupt zu haben. Inwieweit da die Stadtregierung oder generell einmal die öffentliche Verwaltung da einmal entgegenwirken kann, habe ich keine Idee.

A: Kommen wir noch zum Thema Strom. Der Energiesektor ist im NIS-Gesetz und in der Verordnung an erster Stelle genannt. Bei modernen Systemen besteht eine hohe Abhängigkeit vom elektrischen Strom und die komplexe Vernetzung des Stromsektors ist mittlerweile auch der breiten Bevölkerung bekannt und vielerlei auch bewusst. Geht Ihrer Meinung nach, die NIS-Gesetzgebung ausreichend auf die wechselseitige Abhängigkeit von kritischen Infrastrukturen untereinander ein?

B: Nein. Warum nicht – weil jeder Sektor einzeln betrachtet wird. Und ich glaube, dass auch da, gehen wir jetzt einmal weg vom Stromsektor, aber wenn man da die

Krankenhausinfrastruktur, die Rettungsleitstellen betrachtet, dann werden beide auch immer extra genannt im Gesetz. Was bedeutet, sie härten alle ihre Systeme, was ich auch sehr gut finde, aber ich glaube auch, dass es dazu führt, dass die Kommunikation zwischen den Organisationen weitaus schwieriger wird und die gesamtheitliche Betrachtung vollkommen fehlt. Meiner Meinung nach gehören gerade für den Gesundheitsbereich eigene Netze geschaffen, die untereinander kommunizieren und gemeinsam abgehärtet werden und nicht Firewall zu Firewall es immer schwieriger macht, zu kommunizieren und auch Daten auszutauschen.

A: Das ist eine hervorragende Überleitung zur vorletzten Frage, ich betrachte die medizinische Behandlung von Erkrankten oder von verletzten Personen als einen Behandlungsprozess, also einem Pfad vom Notruf bis zur finalen Versorgung durch eine Krankenanstalt, mit viele Prozessschritten dazwischen und Sie haben es schon angesprochen, wenn jetzt jeder für sich schaut, dass er entsprechend autark ist, kann das an den Schnittstellen zu Problemen führen, wie beurteilen Sie den Begriff „Autarkie“ im Rahmen dieser vernetzten und systemübergreifenden Prozesskette am Beispiel der medizinischen Versorgung von NotfallpatientInnen?

B: Wir sind alle nicht mehr autark, das muss uns ganz klar sein, wenn man sich nur das Wiener System anschaut, wir haben halbautomatische Defibrillatoren, die selber die Rettung rufen, da beginnt schon der erste Kontakt, der auch bei Cyberkriminalität schon eine Eintrittspforte sein könnte, wenn ich das jetzt so abhärte, würde ich ein System komplett abdrehen müssen. Die Daten werden dann an den Rettungsdienst übermittelt, der übermittelt die Daten dann an das Krankenhaus, die teilweise ihre Systeme erst starten können, wenn sie die Daten haben, d.h. autark ist hier keiner mehr, wir sind alle voneinander abhängig. Wir betrachten die Systeme gerne jedes für sich, bewerten die Systeme auch jedes für sich, aber übergreifende Prozesse bräuchten meiner Meinung nach auch übergreifende Betrachtungssichtweisen und auch übergreifende Regelungen.

A: Gut, kommen wir zur letzten Frage, von der Berufsrettung Wien werden, zusammen mit den Partnerorganisationen, zwischen 800 und 1000 Notfallpatienten am Tag in den Wiener Krankenanstalten versorgt, hinzu kommen dann noch Selbsteinweiser und mehrere 1000 Krankentransporte. Die Kapazitäten der Krankenanstalten sind natürlich nur auf einen Normalbetrieb ausgelegt, welche Maßnahmen erachten Sie als sinnvoll, damit eine medizinische Basisversorgung eines Großteils der Bevölkerung auch unter

den negativen Auswirkungen eines Cybernotfalls oder eines Blackouts sichergestellt werden kann?

B: Es braucht sicher gute Strukturpläne, die auch zu einem Teil auf analoger Basis noch immer funktionieren, hier sollte es, meiner Meinung nach, auch in der Ausbildung wieder in diese Richtung gehen, dass wir nicht uns immer auf die Technik verlassen, sondern auch immer wieder trainieren, mit gelindesten Mitteln eine Erstversorgung sicherzustellen. Natürlich müssen diese Systeme auch arbeiten, sollten die Systeme auch arbeiten, wenn sie oder auch Teile der Systeme, wenn sie, je nachdem ob es ein Cyberangriff ist, oder ein Blackout, beim Cyberangriff kann es ja sehr viele verschiedene Systeme betreffen oder aber auch nur ein einziges, aber der Rest sollte dann möglicherweise abgeschottet werden können, bzw. auch normale Arbeiten. Aber auch immer wieder das Personal arbeiten lassen, auf Trainingsbasis, ohne oder mit so wenig wie möglich technischer Unterstützung, um einfach eine Basisversorgung auf analoger Basis auch zu bewerkstelligen. Beispiel Leitstelle auch immer wieder mit diesem (unv.) System arbeiten lassen und nicht zwangsweise jetzt diese computerunterstützte Abfrage dann durchführen. Ob es dann im Notfall etwas wirkt oder nicht, ist die Frage wieder, wie die Systeme übergreifend funktionieren, ich glaube, dass es viel mehr trainiert gehört und viel mehr in die Köpfe der Menschen hineinmuss, wenn es passiert, dass man auch kurzfristig ohne Bildgebung, sonst irgendetwas, irgendeine Diagnose stellen kann und eine Basisversorgung sicherstellen kann.

A: Herzlichen Dank für die Erläuterungen und schönen Tag.

B: Danke.

Interview mit Herrn Prof. Dr. Eisenburger am 22.04.2022

A: 22. April 2022. Interview mit Primar Universitätsprofessor Dr. Eisenburger. Herr Professor, das NIS-Gesetz ist jetzt eine bundesweite Vorgabe, um den Schutz kritischer Infrastrukturen zu verbessern. Wie ordnen Sie persönlich die Notwendigkeit einer gesetzlichen Regelung zur Einhaltung von IKT-Sicherheitsstandards ein? Zumal viele kritische Infrastrukturen ohnehin ein Informationssicherheitsmanagementsystem implementiert haben und betreiben.

B: Also da muss ich sagen, bin ich meinungslos. Ich weiß, es braucht einen Plan. Und ich glaube ein gesetzlich untermauerter Plan ist grundsätzlich, hat aber eine höhere Neigung, eingehalten zu werden, würde ich jetzt vermuten, also jetzt nicht als Experte, sondern als Staatsbürger. Ist aber auch unflexibler. Also wenn man da was verbessern kann, dann ist es nicht so leicht, ein Gesetz, das einmal beschlossen wurde, geschwind einmal zu ändern. Und wenn eine Stadtverordnung oder ein Stadtbeschluss oder ein regionaler Was-auch-immer-Plan ein Upgrade braucht, dann glaube ich, geht das leichter, wenn dass das SKKM Wien sagt: Das machen wir jetzt anders. Aber grundsätzlich diese, die sozusagen das ins Bewusstsein des Gesetzgebers zu rufen, dass kritische Infrastruktur nicht nur besteht, sondern auch bestehen können muss in besonderen Situationen und dann auch Unterstützung braucht, Schutz braucht, Technik braucht, Support braucht, proaktives Herantreten an die diversen infrastrukturellen Einrichtungen, Krankenhäuser, Flugrettung, Berufsrettung, Leitstelle, Feuerwehr, Apotheken. Eben mit dem Thema Blackout zum Beispiel. Da komme ich noch dazu. Es ist jetzt ein Stromausfall. Es ist ein Kommunikationsausfall. Wir wissen, ihr werdet etwas brauchen. Wir fragen euch statt, dass wir darauf warten, dass wir von euch etwas hören. Solche Kleinigkeiten. Und ich würde vermuten, dass das mit Gesetzesbasis besser fundiert ist und nicht so leicht wegzudiskutieren ist.

A: Abgesehen von der gesetzlichen Vorgabe gibt es ja auch bestehende internationale anerkannte Normen, speziell auch im Bereich der Qualität des Sicherheitsmanagements und für die IT. Wie ordnen Sie die in Bezug auf die Hierarchie, die Normen und das Gesetz ein?

B: Da kann ich nichts sagen. Das weiß ich nicht. Weder von der vom Plan noch von der Umsetzung habe ich kein Detailwissen.

A: Herr Professor, im Vorfeld haben wir gesprochen, dass Risikomanagement eine Querschnittsmaterie darstellt. Welche Risikoszenarien für Ihre kritische Infrastruktur für die Klinik für Ohlsdorf kommen Ihnen in den Sinn und welche betrachten Sie dabei als vorrangig?

B: Ja. Zweierlei. Wir hatten, also ich war bei diesem Terrorabend bin ich hereingekommen und war schon unterwegs nicht sicher, ob es eine gute Idee ist, mit dem Auto zu fahren, zu Fuß zum Auto zu gehen, einen Kilometer. Weil ich war da nicht zu Hause und so weiter. Aber dann auch, wie ich hier reingekommen bin ins Krankenhaus, habe ich gesehen, da steht ein Security Mensch, der nicht bewaffnet ist und ist vielleicht, das war natürlich nicht, (aber?) das wissen wir, (er war?) in Gedanken habe ich es (unv.). Der einzige Türsteher zwischen mir und einem bewaffneten Menschen. Und jetzt sind Krankenhäuser klassischerweise nicht Ziele von Terroranschlägen, aber auch nicht null Mal. Und das heißt, es geht um den Schutz vor Gewalt bei Terror. Es geht um den Schutz vor Zudringlichkeit bis Gewalt oder bis Überzeugung mit Waffen Argumenten. Zum Beispiel bei Blackout, wenn ein besorgter Angehöriger für seinen Vater in der Apotheke nicht mehr Medikamente bekommen kann, weil die Apothekentür nicht aufgeht, weil sie barrierefrei ist, also elektrisch, also zubleibt. Und da kommt der ins Krankenhaus und sagt: Ich hätte gerne die Medikamente für meinen Vater. Und argumentiert das mit Kraft statt mit Worten. Dann brauchen wir da Schutz. Das ist das eine. Das andere ist, das, was ich als kritische Infrastruktur. Ich bin jetzt damit (sehr?) (unv.) nicht hier anmaßen und natürlich nicht der ärztliche Direktor, weil ich bin der stellvertretende Katastrophenreferent des Hauses. Wir wissen, dass die sozusagen das ganze Logistiksystem im Gesundheitsbereich ein sehr hohes Standgas hat und mit diesen ganzen just-in-time-Lieferungen. Wir haben wenig Lagerbestände allgemein. Das heißt, wenn ein Blackout ist oder wenn ein Lieferausfall ist oder wenn alle (Drummerbrücken?) auf einmal kaputt sind, dann sind wir sehr, sehr schnell, erheblich schneller als uns lieb ist, am Ende unserer Versorgungskapazität, der hausinternen. Das ist Essen, ist oder Diesel für den Notstrom oder Medikamente. Das weiß ich nicht. Wäsche kommt über Wäschelieferfirmen, Wäscheautomaten. Aber in der Minute, wo ein Blackout losgeht. Sollte ich herausfinden, ist das ein lokales Problem, weil hier der Strom ausgefallen ist? Ist das ein Bezirksproblem? Ist die ganze Stadt finster? Ist ganz Europa finster? Und muss in der Stunde des Blackout-Beginns anfangen, Ressourcen zu sparen? Aber was ich auch erwarte oder brauche, bräuchte und nicht weiß, ob das kommt, ist,

dass eine Stadt Wien, eine Generaldirektion, eine kritische Infrastruktur-Versorgungsnetz bereitstellende Organisation, welcher Art auch immer, an uns herantritt und sagt: Wie schaut es aus? Was braucht ihr? (Arg?) proaktiv. Bis hin zum, allen Ernstes jetzt, berittenen Botenfahrrad, (den?) irgendwer, der mit der Wunschliste kommt und sagt: Was braucht ihr jetzt? Was braucht ihr in einem halben Tag? Was braucht ihr in drei Tagen? Antibiotika, OP-Tassen, Essen, Wäsche, was auch immer. Also die Gesamtlogistik, die nicht von selbst kommt, weil irgendwelche Lieferketten unterbrochen sind. Und unter Umständen auch die Kommunikation, dass wir diesen Bedarf nicht decken können, entweder sehr schwer ist oder nicht an der üblichen Stelle geht, das heißt, man muss immer ewig herumprobieren, mit wem rede ich überhaupt, wenn mein Medikamentenlieferant nicht liefert? Wer sorgt dafür, dass ich vorrangig manche Dinge bekomme? Zu wessen Lasten? Wer hat da Nachrang? Wer tritt an mich heran? Ich würde vermuten, dieser tritt (niemand?) an uns heran, sondern man kann irgendwo versuchen, Wünsche zu deponieren. Aber (unv.) wo und wie, unter welcher Nummer.

A: Gilt es noch zu definieren.

B: Ist ja, aber das ist dann, da es dann zu definieren ist, zu spät. Vorher ist die Frage, wer ist da die Adresse.

A: Ich verstehe.

B: Also eigentlich als Kernthema Lieferlogistik und Schutz vor Gewalt oder Schutz vor Zudringlichkeit oder Begehrlichkeit im unangenehmen Sinn sind die Dinge, die von außen kommen müssen. Die können wir als Haus nicht.

A: Kannst (unv.)

B: Auf die Beine stellen.

A: Gut. Ein kurzer Themenwechsel. Ziemlich zeitgleich mit dem Beginn der Masterthesis ist der Ukraine-Krieg ausgebrochen. Österreich hat sich klar zur Neutralität bekannt und beschränkt sich mit Unterstützung der Ukraine mit humanitärer Hilfe. Anders sieht es aus in Deutschland. Deutschland liefert Defensivwaffen und Ähnliches. Setzt sich damit aber auch der Gefahr von Gegenangriffen in Form von Hackangriffen auf die kritische Infrastruktur, da vornehmlich das Strom- und Energienetz, aus. Wenn nun das deutsche Energienetz betroffen sein sollte durch so

eine Hackattacke. Wie hoch schätzen Sie oder schätzen Sie es als Möglichkeit eines Kollateralschaden, dass auch Österreich von so etwas betroffen ist, ein?

B: Also ich habe überhaupt keine Ahnung, aber das, was ich in der Zeitung lese, ist, dass schon Resonanzausreißer von wenigen Millisekunden im europäischen Stromnetz, Power Grid und so weiter dazu reichen, ein System aus der Resonanz rausscheppern zu lassen. Und dann ist es einmal im Eck. Wie auch immer das dann ist. Ich habe da wirklich kein technisches Grundverständnis. Aber ich glaube, wenn ganz Deutschland schwarz wäre, dann ist es extrem schwierig in Österreich, eine koordinierte Stromversorgung aufrechtzuerhalten. Wie auch immer das sozusagen begründet wäre, aber ich würde da vermuten von wenig Sachwissen, sondern eher so Populärliteratur, Blackout und Zeitungsartikel, dass das auf uns überschwappt, und zwar in der Millisekunde.

A: Gut. Bleiben wir noch kurz beim Thema Blackout. Ich oder Experten definieren es als ein überregionales und über mehrere Tage andauernden Stromausfall. Das hat natürlich dann auf das Kontinuitätsmanagement von sämtlichen Organisationen von der gesamten Gesellschaft gravierende Auswirkungen. Welche Maßnahmen hat Ihre Organisation gesetzt, um ein Blackout-Szenario darauf vorbereitet zu sein und die Folgen davon abzumildern?

B: Also wir haben eine A4-Seite, was tun bei Stromausfall. Mit der sehr rudimentären Unterscheidung. Man prüft einmal, habe ich hier im Haus einen Stromausfall, und das aus irgendeinem Grund geht der Notstrom nicht, oder wir sind auf Notstrom. Ist da eben. Sind die Straßenlaternen finster? Ist der ganze Bezirk oder die ganze Stadt ohne Strom und wir haben schon Strom, aber es ist an sich ein Stromproblem? Wenn es nur ein Hausstromproblem ist und draußen leuchtet der (Billa?) und so weiter, dann wird das demnächst gelöst und zur Not kriegen. Das hat man im alten Krankenhaus Floridsdorf schon. Da war ein Stromausfall und der Notstromgenerator hat auch nicht funktioniert. Und das ist natürlich blöd für ein Krankenhaus und.

A: Absolut.

B: Von aller kürzester Zeit gehen die Akkus von Beatmungsgeräten sehr zurück und so weiter. Und dann hat die Feuerwehr einen riesen, also so richtig containergroßen Notstromdings da hergestellt. Wie auch immer die den angeschlossen haben ans Hausnetz und die Sache war erledigt und dazwischen war eben der Gedanke, dass

haben wir nicht gebraucht. Das wir eben von der Feuerwehr lauter kleine Einzelgeneratoren für die Intensivstationen aufstellen lassen, damit eben Beatmungen, OPs und so weiter.

A: Also gar nicht mal eine Evakuierung dann?

B: Nein, wohin denn? Und Evakuierung haben wir auch gehabt. Aber wenn das jetzt ein Wien-weites Thema wäre.

A: Dann freut das natürlich nicht.

B: (unv.) nicht willkommen in anderen Häusern, die das gleiche Problem haben, das heißt und vor allem bis zur Evakuierung bis wir, wenn wir Wiener Rettung anrufen, sagen, (so wie?) die Landstraße, wo dieser Brand war. Sind alle tot, wenn wir. Wenn die. Bis die wo angekommen sind. Wenn wir keine Zwischenlösung haben.

A: Verstehe.

B: Theoretisch, de facto gibt es natürlich gibt es ein bisschen einen Spielraum. Das stimmt schon, aber wir wissen, wie die Akkuladestände sind von manchen Geräten, die dauernd geladen werden und immer am Strom hängen und dann doch einen Memory-Effekt hatten, obwohl es versprochen wurde, das nicht. Also mich fix darauf zu verlassen, dass wir jetzt 120 Minuten kein Problem haben, spüre ich Skepsis. Kann es nicht (unv.).

A: Verstehe ich, ja. Inwieweit werden bei diesem A4-Zettel, den Sie angesprochen haben, auch andere Interessensgruppen berücksichtigt? Oder ist da der Fokus lediglich auf? Was machen wir, ohne dass da auch Kontakt mit anderen Playern, Feuerwehr, Rettungsdienste, Polizei, Stromversorgern Kontakt aufgenommen wird?

B: Muss ich jetzt noch einmal nachschauen. Wir haben einen separaten Zettel der Evakuierung, mit dem einerseits mit (unv.). Das ist eine Checkliste für unseren Oberarztdienst, der Evakuierung im Haus muss etwas evakuiert werden. Haben wir auch im anderen Haus, wo so ein Sauerstoffventil rausgehaut hat und die ganze Intensivstation war schlagartig ohne Sauerstoff. Das heißt, es war in der Minute (bei Nacht?) beatmete Patienten von der Anästhesie zu evakuieren. Ein anderes (unv.) für (den?) im Haus, im Alter. Das heißt, wir haben eine Checkliste. Wir helfen bei Evakuierung einer anderen Abteilung und fragen einfach: Können wir helfen? Sollen

wir Patienten zum Beatmen übernehmen bis was auch immer. Externe Hilfe und Evakuierung kommt von außen und wir werden anevakuiert, sozusagen, angeschwappt und da, wie gesagt, da steht halt wieder Rettungsleitstelle kontaktieren (unv.)-journal, also (Gesundheitsverbundjournal?) und Feuerwehr kontaktieren. Aber so dieses und hausintern ist es eben. Wir rufen den Oberarzt Anästhesie an: Braucht ihr Hilfe? Er sagt: Passt schon. Dann ist erledigt. Ja, wir haben (viele?) Patienten, die wir nicht unter (unv.). Aber sie können da nicht ewig bleiben. Wenn sie mal da sind und an der Luft hängen, geht es halt dann. Aber sie ist keine Haus-weite-Vorgabe, sondern ist immer abteilungsintern.

A: Ein kurzer Themenwechsel, raus aus dem Spital, rein mit in die Stadt. Das Thema der (unv.) Bevorratung im urbanen Raum ist auch ein Problem, sage ich einmal. Einige Studien belegen, dass die Wienerinnen und Wiener oder generell die Stadtbevölkerung die Vorzüge des modernen Lebens genießt. Auch just-in-time dann Essen holt oder sich liefern lässt, wenn es. Wenn man Hunger hat. Im Falle eines Blackouts, Sie haben es schon angesprochen, ist von einer Minute auf die andere unter Umständen nichts mehr da. Wie meinen Sie, sollte Ihrer Meinung nach das Problem begegnet werden, dass kritische Infrastrukturen von einer hungrigen Bevölkerung, der kalt ist, gestürmt werden, weil eben ein Krankenhaus im Speziellen über einen längeren Zeitraum noch über Wärme, Energie und Essen verfügt?

B: Also Wärme ist sicher das am schwierigsten zur Lösung der Thema, abgesehen von der Empfehlung, dass man einen (unv.)Pullover anzieht. Ich glaube, es muss quasi unaufgefordert und dann nicht mehr, auch nicht mehr gescheit kommunizierbar, die Lösung der Bevölkerung bekannt sein, bevor es passiert. Wie auch immer. Genauso wie, wie man. Es gibt am Flughafen den Meetingpoint. Es gibt bei uns noch nicht, das ist gerade in Reflexion, aber im (Böhler?) Krankenhaus gibt es schon die Katastrophenzonen eins, zwei, drei, die Triage- und die Behandlungszonen im Regelfall, damit es alle (Rettungen?) wissen: Ah, wenn das ist, dann ist das (gleiche?). Und wenn wir im 16. Bezirk ein Schild haben: Liebe Bevölkerung, wenn es kurz scheppert oder wenn alles ausfällt, kommt hier an diesen Platz, hier kriegt ihr Trinkwasser, hier kriegt ihr eine warme Suppe und hier werden die essenziellen Medikamente ausgegeben, die die Apotheken nicht geben können, weil die Apotheken zu haben, weil die Tür nicht aufgeht, die barrierefreie. Geht nicht ins Krankenhaus. Hier kriegt ihr, was ihr braucht. Dann ist das für Essen, für Trinken und für

Medikamente machbar. Nicht leicht, aber es sollte der Bevölkerung, bevor es passiert, bekannt sein. Und dann grätzelweise und nicht alles am Stephansplatz für ganz Wien, sondern wirklich verteilt, lokoregionär oder sozusagen angeboten werden. Wärme ist da viel schwieriger, weil die Leute. Wer hat schon einen Kachelofen daheim und die Gasheizung fällt aus oder sie zündet nicht, weil der Strom nicht da ist. Ist erheblich schwieriger. Dann muss man den Leuten (wie gesagt kalt?), du machst die Fenster zu, ziehst Pullover an, aber das sagt sich so leicht. Aber die, sozusagen das, was das Krankenhaus belasten würde, ist in meiner Vermutung und in meinem Kino im Kopf. Aber seitdem ich dieses Blackout-Buch als Hörbuch gehört habe, dass eben nicht wie bei jeder 0815 Großschadensereignis, Katastrophe da im Routinefall die Patienten durch den Haupteingang kommen und sagen: Hier bin ich, nehme mich zur Kenntnis, sondern durch den Hintereingang kommen, weil sie mein Klopapier stehlen wollen und ihr Handyladegerät anstecken wollen und meine Medikamentenkassen plündern wollen, weil der Vater sonst, wie sie glauben, sofort stirbt.

A: Verstehe.

B: Und entweder im Stillen stehlen oder im Aggressiven sagen: Her damit. Das auch (unv.) hollywood-artig. Es ist nicht sehr sachlich, aber sie sagt das, man kommt nicht ganz umhin, das so ein bisschen als Szenario zu haben, dass ein blöder Typ, zig, zig Mannschaften in Erregung versetzt, weil der eine blöde Typ nicht nur sich stark hinstellt, sondern mit einem Messer fuchtelt. Haben wir mit normalen Patienten auch. Messer-Fuchtler, Waffen-Wackler, die sich irgendwie Respekt verschaffen wollen und das könnte ich mir vorstellen. Oder stelle ich mir schon vor, dass das zum Beschaffen von privatem Bedarf aus dem Krankenhaus, die ja Leuchtinseln sind. Die ganze Stadt ist finster und ein paar Inseln leuchten und wie die Motten zum Licht kommen die Leute dorthin und erwarten sich (ihre Lösung?). Aber wie gesagt, nicht auf dem offiziellen Weg. Also ich glaube, dass die das mit Rundfahrten per Lautsprecher, liebe Bevölkerung von Floridsdorf, alles was ihr braucht oder was ihr akut braucht, gibt es in jeder Ecke, gibt es am Spitz, gibt es dort und da, gibt es in der Shoppingcity, was weiß ich. (Trailerpark?) an vier Standorten, das hat er relativ schnell, aber da waren Tage und Wochen Vorlaufzeit und jetzt hätten wir paar Stunden Vorlaufzeit. Da klappt das mit PCR, mit sonstigen Geschichten, mit Schnupfen, Boxen ist da ja relativ viel Logistik schnell entstanden. Die müsste halt auf einen Knopfdruck geplant schon sein. Also aktiviert werden nur, wenn sie schon geplant ist. Aber eben Trinken, Essen,

Medikamentenausgabe einerseits und andererseits eben an uns die aktive Frage. Es wird der Lastwagen zweimal am Tag kommen. Was soll bei der nächsten Lieferung sein? Was kann auf die übernächste Lieferung warten? Dann geben wir Wunschlisten ab.

A: Sind schon sehr konkrete auch Lösungsansätze inkludiert. Gut. Beim nächsten Thema muss ich wieder ein bisschen auf das NIS-Gesetz pochen. Es ist.

B: (unv.)

A: Ja, also das Netz- und Informationssicherheitsgesetz, wo auch die Abhängigkeit des elektrischen Stroms sehr offenkundig wird.

B: Ja.

A: Geht Ihre Meinung. Ich stell jetzt einfach die Frage ganz direkt. Geht Ihrer Meinung nach die NIS-Gesetzgebung ausreichend auf die wechselseitige Abhängigkeit von kritischen Infrastrukturen auf Energie und sonstiges ein?

B: Weiß ich nicht. Kann ich nicht beantworten. Ich kenne das Gesetz nicht.

A: Dann widmen wir uns wieder mehr dem Gesundheitssektor. Es geht hier um die Rettungskette. Ich verstehe die Behandlung beziehungsweise die Genesung vom Patienten ab dem Notfall bis zur vollständigen Entlassung, Gesundung nach einem Spitalsaufenthalt als einen Behandlungspfad, der natürlich ineinandergreifen muss. Der setzt sich zusammen auch aus dem Bereich Rettungsdienst als eine Größe und das Spital auf der anderen Seite. Beide Bereiche versuchen, möglichst resilient und autark funktionieren zu können. Wie beurteilen Sie den Begriff Autarkie im Rahmen vernetzter und systemübergreifender Prozessketten?

B: Es widerspricht sich fast, dass man einerseits autark ist, also unabhängig von den anderen und andererseits aber eine Vernetzung braucht und. Also was weiß ich. Wir können dieses Krankenhaus wenige Stunden betreiben und dann ist vorbei mit der angenehmen Atmosphäre, wenn wir Entlassungen nicht vornehmen können. Wofür wir ganz viele Krankentransporte brauchen, wofür wir erstens den anfordern können müssen, sicherstellen, dass dem Patienten, der pflegebedürftig ist, zu Hause irgendjemand entgegennimmt, dass jemand die Tür aufsperrt und dass dann dort eine Versorgung (hat, damit?) er nicht verhungert und in sechs Wochen als Teil des

Teppichs gefunden wird. Das heißt, diese, die Autarkie, dass wir sagen, wir können Patient behandeln, ist unweigerlich ein Teil unserer großen Prozesse Einfluss, Behandlung und Ausfluss. Und wenn der Ausfluss nicht klappt. Beim Zustrom mache ich mir keine Sorgen. Erstens, weil ich mir keine Sorgen machen will, weil ich mir denke: Wer nicht kommt, ist nicht.

A: (unv.).

B: Das ist nicht mein Problem. Das stimmt nicht, aber es ist halt momentan nicht angenehm. Und billige (unv.) Behandlung ist, wie sie ist, problematisch oder nicht. Aber der Abfluss ist ein sofortiges Thema. Ja, jetzt um dreiviertel elf. Wenn jetzt die nächsten sechs Stunden keine Entlassungen stattfinden, haben wir die ganze restliche Woche ein Problem, das wir nicht lösen können. Und somit sind wir nicht autark in unserem Wunsch, Patienten auch loszuwerden. Ja, wir sind abhängig von Abtransport und dass, wenn man das jetzt nicht gut vernetzen kann, nicht gut anmelden kann, nicht gut sicherstellen kann, die Angehörigen nicht erreichen kann, kommen sie nicht den Vater abholen, weil das Telefon nicht geht oder weil die Straßen sperren. Was auch immer an technischen oder Großkino und Mariupol-artigen Monsterszenarien ist oder nur Kleinigkeiten, dass eben ich bin nicht (werde?). Das macht uns als eben, sage ich immer, mit dem hohen Standgas. Wir sind ein total vernetztes Turbosystem. Man sieht es, was passiert, wenn eine Schnellbahn stehenbleibt am Praterstern oder zwischen Praterstein und Traisengasse. Ja, dann steht da zigtausend Menschen stehen dann. Wie sich das wieder aufgelöst hat und die Umgebung (unv.). Bei der Krankenhauslogistik, (unv.) Gesundheitslogistik genau das Gleiche. Wenn wir nur hier sind und nur machen müssen, was wir machen und wir können miteinander reden und wir können im Krankenhaus sagen, wenn der Lautsprecher noch funktioniert. Es gibt eine Katastrophenbesprechung. Eine Abteilung entsendet dann kommt zu jeder vollen Stunde dort und dahin ins Veranstaltungszentrum. Dann kann man bald einmal autark sich fühlen. Aber wir sind nicht autark, weil wir eben die Patienten loswerden müssen. Ja. Also.

A: Danke vielmals für diese Klarstellung. Das ist. Deckt sich auch mit meiner Überzeugung und wird ziemlich.

B: (unv.) da sind wir wieder beim Anfang. Wenn wir anfangen nachzudenken und dann anfangen, zu organisieren und zu kommunizieren in Zeiten von Stromausfall, von

Telekommunikationsausfällen (unv.) die Heimtransporte von Patienten, wo dann ich die Idee habe, die geht sicher schon zigfach von den anderen besser. Es kommt der Stadt Wien Citybus, der kleine Elektrobus mit 20 Sitzen und fährt zu Entlassungszonen, nimmt die Leute, die selber gehen können, aber die kein Taxi haben und klappert wie der Schulbus den 21. Bezirk ab. Und dann kommt der Bus für (unv.) und da kommt der Bus für Südwien. Was auch immer. Diese Entlassungsbusse und wahrscheinlich werden die brauchen wir auch einen (unv.)-Bus. Aber die Rettung wird mit ganz anderen Themen, die ich jetzt nicht im Detail durchgedacht habe, auch zu tun haben. Dass die nicht alarmiert werden können, dass die patrouillieren müssen, dass Leute auf der Straße stehen und ein Auto aufhalten und sagen: Stopp, du kommst jetzt mit. Mein Großvater liegt da, der ist (unv.) und hat seine (Haxen?) gebrochen. Der kann zu seinem Einsatz nicht weiterfahren. Das wird es leider so eine Vertausendfachung vom gelegentlichen Einsatz geben.

A: Sie denken da eh sehr, sehr (breit?).

B: Lauter solche Sachen. Aber aus unserer Sicht ist der Zustrom weniger das Problem. Also es ist verhundertfacht. Aber wenn er weniger ist, ist es weniger mein Problem als meine Sorge. (Wurst?), aber der Abfluss, der gehört vorab geplant.

A: Ja, Sie haben im Vorgang auch schon einiges von der nächsten Frage vorweg gegriffen. Der Vollständigkeit halber, werde ich sie dennoch stellen. Es ist ja so, dass die Berufsrettung Wien mit zusammen mit den anderen Partnerorganisationen des Rettungsverbunds etwa 1000 Patienten am Tag in Kliniken zur weiteren Behandlung bringt.

B: Ist das wirklich so?

A: Ja.

B: 1000 Transporte?

A: Also zwischen 800 und 1000. In der Hochsaison.

B: Okay. Zu uns, weil wir.

A: Nein, nein, nicht exklusiv die Klinik Floridsdorf, aber auch sämtliche Wiener Spitäler.

B: (unv.) Wenn wir sagen die. Natürlich, es ist nicht mein Geschäft. Ich weiß Einsätze, aber nicht Transporte. Tausend.

A: Ja. Es ist ein bisschen.

B: (unv.) Supervisor, Oberarzt und ein Transport. Aber wir kriegen. Wir kriegen. Das (Wilhelminisch?) Spital kriegt an den Weltuntergangstagen. Da kriegen sie 115 Rettungen. Nur die Notfall, dann kriegt die Rettung-, die Unfall noch einmal 80 und das (unv.) ist aber nicht mal fünf. Also es wird schon viel sein. (Überhaupt?) keine Zweifel. Aber das ist ja, kann auch völlig wurst sein. Jedenfalls sind viele.

A: Geht es auch um Belastungen, Todesfälle und dergleichen. Aber das ist nicht der Kernpunkt, sondern die aktuellen Versorgungsstrukturen sind ja auf den Normalbetrieb, also auch Notfall in dem Fall als Normalbetrieb angesehen, ausgelegt. Welche Maßnahmen erachten Sie als sinnvoll, damit eine medizinische Basisversorgung eines Großteils der Bevölkerung auch unter den negativen Auswirkungen eines Cybernotfalls, also Ausfall der Kommunikation in erster Linie, und der Administration oder gar eines Blackouts sichergestellt werden können.

B: Ja, also allem voran, mit riesengroßen Abstand ist: Krankenhäuser brauchen Strom. Wenn bei uns die Lifte ausfallen, dann kommen alle Patienten, die ins Krankenhaus kommen, von der Ebene eins nicht weg. Und alle Patienten, die bei einer Station sind, kommen nicht nach Hause. Außer sie können gehen, die stiegen runter. Aber wenn die Lifte ausfallen, dann geht nichts. Und Patienten in Betten (überstiegen?) ist kein Thema. Also es muss der Krankenhausstrom gewährleistet sein. Lückenlos, immer, wochenlang. Wie auch immer, jetzt, da wird es wahrscheinlich einen Waffen bewachten Dieseltransport geben müssen, der nicht überfallen werden darf und nicht gekidnappt werden darf und nicht am Schwarzmarkt verklopft (dann da und so weiter?). Was auch immer mir da einfällt, nicht nach Ukraine (abgeben?) und so weiter. Also. Das ist jetzt. Als Hauptding müssen wir schauen, dass unsere Prozesse möglichst normal laufen. Und das heißt, wir müssen proaktiv vorab, auch hausintern natürlich, kommunizieren. Was lässt sich streichen? Was lässt sich verschieben? Wohin verschieben? Wann ist das dann nachzuholen? Was passiert mit dem Patient in der Zwischenzeit? Geht er daheim oder muss er im Haus bleiben? Sonst verschieben wir es lieber nicht. Und lauter so Sachen. Das um und auf ist die Kommunikation. Und wir hatten einmal einen, in der ersten Woche des Betriebs dieses Hauses hatten wir einen Ausfall von einer kompletten Telefonanlage. Alle (Deks?), alle Festnetze haben nicht funktioniert. Und das heißt, der (Herzalarm?) kann nicht gehen. Und dann muss man einmal händisch oder zu Fuß abklappern und sagen: Wenn bei

euch etwas ist, das (A1?)-Festnetz geht. Das ist eine (A1?)-Festnetznummer, die haben wir jetzt am Oberarzttelefon auserkoren sowie auf dem Kabel dann geschrieben, unter der sind wir erreichbar. Das ist die einzige Nummer des Hauses, die von extern erreichbar ist. Und wir haben dieses Telefon, also (A1?)-Telefon als Backup und lauter solche Sachen, aber das dauert eineinhalb Stunden, bis der eine Bote alle Stationen abgeklappert hat, (unv.) Herzalarm sein sollte. Da kann man nicht nur sagen viel Glück, sondern wir kommen aber nur unter der Nummer. Leider so (unv.) Details. Also Kommunikation ist das um und auf. Und das geht, dann muss man nicht jedes Mal auffordern, sondern, da muss man sagen, eben alle vollen Stunden und dann immer später, alle sechs Stunden oder einmal pro Tag ist die und die Besprechung. Wie bei einer 08/15 länger dauernden Pandemie haben wir es auch gekannt. 7:00 Uhr früh Besprechung, jeden Tag Briefing. Und so weiter. Und sonst sind da waren noch ein paar Details von den Fragen habe ich wieder vergessen. Lesen Sie die Frage noch einmal vor. (unv.)

A: Welche Maßnahmen erachten Sie als sinnvoll, damit eine medizinische Basisversorgung des Großteils der Bevölkerung auch unter negativen Auswirkungen eben eines Cyberausfalls sichergestellt werden können?

B: Genau. Wenn wir aus dem Krankenhaus rausgehen, dann muss da auch Medizin passieren können. Oder (unv.)-Medizin, die natürlich ein Vielfaches von der Krankenhausmedizin jeden Tag ist. Wir tun uns immer leid, wenn die Patienten sagen: (so kann jetzt keiner?) in die Ordi gehen, aber x-mal so viele Patienten gehen in Ordinationen und das darf nicht zusammenbrechen. Das heißt, wenn wir die ganzen eben barrierefrei heißt elektrische Tür und heißt Lift oder Rampe, wenn es ebenerdig ist, Ordninationstüren müssen aufgehen. Wenn das nicht geht, dann muss der Ordinationsarzt vor der Tür, im Zelt oder im Gemeinschaftszelt eben am Grätzelplatz neben dem Brunnen und der Medikamentenausgabe ordinieren. Da müssen die leute wissen, hoppala, wenn ich etwas habe, dann gehe ich dorthin und nicht zum Reflex machen. Da gehe ich halt ins Krankenhaus, weil wir haben ganz andere Sorgen. Und das muss die Leute erreichen, bevor sie darüber nachdenken. Wenn sie nachdenken, wie sie ins Krankenhaus (unv.) Krankenhaus ist doch viel besser kenne ich alles. Die haben nur auf mich gewartet. Diese ganzen Geschichten müssten einen Plan haben, einen geografischen Plan, eine inklusive Temperatur und Entsorgung von Grünspateln oder chirurgischen (Futzeleien?), was halt irgendwelche HNO, irgendetwas. Das muss

alles gereinigt werden, da braucht man dahinter diese alten Reinigungsplan. Was auch immer an wieder Verbrauchsmateriallogistik für die Einzelordination oder die Gemeinschaftsordination den zweiten Tag dann möglich macht. Am ersten Tag geht viel. Da ist auch viel Geduld möglich. Aber am vierten Tag sind die Leute. Das ist jetzt halt. Also ich glaube, die Versorgung des dritten, vierten, fünften, sechsten Tages beginnt in der ersten Stunde und nicht am zweiten Tag. Sofort einsparen, (jetzt?) im Haus sofort. Welcher Patient braucht wirklich ein (unv.) Antibiotikum? Was geht nicht (oral?)? Haben wir alles versucht? Wir haben nur 2000 Flaschen, die sind übermorgen alle weg. Und dann sterben Leute, weil wir heute nicht angefangen zu sparen. Wenn ich meine Wäsche einen Automaten zurückgebe, wenn er die überhaupt annimmt, dann kriege ich die nie wieder im Blackout. Dann kann ich im Privaten mich anschreiben lassen. Das heißt, ich muss sagen, liebes Team, lasst eure Wäsche an, auch wenn sie grauslich ist und auch wenn ihr stinkt. Das ist okay oder macht es privat. Aber dann erkennt euch wieder keiner. Am ersten Tag riecht das nicht dann, wenn es schon weg ist. Solche Sachen. Also die Bremsen muss man gleich ziehen. Unmittelbar.

A: Herzlichen Dank für die aufschlussreichen Antworten.

B: (unv.). Na bitte.

Interview mit Herrn Glaninger am 23.05.2022

A: 23. Mai 2022, Interview mit dem Leiter der Rettungsleitstelle Wien, Hrn. Patrick Glaninger. Herr Glaninger, die europäische Richtlinie zum Schutz oder zur Erhöhung des Sicherheitsniveaus vom Netz und Informationssystemen, wird jetzt in Österreich mittels Gesetz umgesetzt. Bereits zuvor existierten Gesetze bei den verschiedenen ethischen Infrastrukturen, um ein hohes Schutzniveau anzustreben. Seit 2008 gibt es beispielsweise das Konzept Absys, die europäische kritische Infrastrukturschutz. Also jetzt konkret die Frage, wie ordnen Sie die Notwendigkeit für eine gesetzliche Regulierung zur Einhaltung von IKT-Sicherheitsstandards ein, zumal viele kritische Infrastrukturen bereits ein Informationssicherheitsmanagementsystem implementiert haben, oder betreiben?

B: Die Frage war, wie wichtig ich das halte?

A: Ja. Dass es eben eine gesetzliche Basis für diese Richtlinie gibt.

B: Ja, ich meine, wir können eh ganz normal reden, oder?

A: Ja.

B: Ja das war eh schon höchste Zeit, dass soetwas kommt. Meines Erachtens nach hat es soetwas de facto nicht gegeben, meines Wissens hat es nur die Vorgaben gegeben bei Leitstellen Neubauten, was alles für Schutzmaßnahmen einzubauen sind, aber puncto IKT-Sicherheit ist es eigentlich nur um die bauliche Struktur gegangen und nicht um die Infrastruktur, also es war eh schon höchste Zeit, dass soetwas kommt.

A: Und worin liegt jetzt ihrer Meinung nach der Mehrwert für die Gesellschaft durch eine bundesgesetzliche Regelung?

B: Dass einfach alle dazu verpflichtet sind, diese auch umzusetzen. Wie gesagt, Betreibung wesentlicher Dienste ist nun mal für die Bevölkerung da und soll auch immer funktionieren und soll auch bestmöglich geschützt sein. Da profitiert die Bevölkerung auch davon, ja.

A: Bevor es das NIS-Gesetz gegeben hat, gab es bereits das österreichische Programm zum Schutz kritischer Infrastruktur, Absip, bei uns mit schutzkritischer Infrastruktur in Verbindung und davon losgelöst dann ab 2013 die österreichische Strategie für Cybersicherheit, ÖSCS. Beide Strategien wurden inzwischen erneuert

und dazu gibt es dann noch ergänzend Normen, wie die ISO27000. Welche Bedeutung messen Sie diesen beiden Strategien, also Absip und ÖSCS und den Normen wie ISO27000 und weiteren im Vergleich zum NIS-Gesetz bei?

B: Ich kann das leider nicht sagen, weil ich kenne diese zwei Normen nicht, die wurden mir nie präsentiert oder vorgestellt und ISO27000 oder ISO27001, da ist das NIS-Gesetz noch mehr in die Tiefe, glaube ich. Also ob man jetzt die Zertifizierung macht, oder nicht macht, stellt für mich jetzt nicht das Wesentliche dar, das Wesentliche ist, dass man die Bundesgesetzvorgaben einhält, das NIS-Gesetz.

A: Gut, kritische Infrastrukturen sind natürlich einem breiten Spektrum an Bedrohungen ausgesetzt. Sicherheitsmanagement, Risikomanagement sind per se Querschnittsmaterien, ist notwendig die gesamte Organisation zu betrachten und so potentielle Gefährdungen zu identifizieren. Bei den unterschiedlichen Risikoszenarien, welche kommt Ihnen in den Sinn und betrachten Sie aktuell als vorrangig?

B: Ja für mich ist einmal vorrangig, hat uns auch der 02.11. auch gelehrt, der Gebäudeschutz. D.h. das ist für mich das allerwichtigste, weil wie wir auch gesehen haben, Terroranschlag war ja gar nicht so weit weg entfernt von uns, von unserer Zentrale und es hätte durchaus sein können, dass wenn es mehrere Täter waren, dass sie sogar in der Nähe vorbeikommen und vielleicht auch hier – ah, Rettung, legen wir lahm – der Gebäudeschutz ist einmal das Allerwichtigste. Rettungsleitstelle kann ich nicht outsourcen, da haben wir Gottseidank eine Redundanz mit der zweiten Leitstelle und dann ist das Wichtigste eben, nicht nur der Schutz und dann auch der bauliche Schutz für die Rettungsleitstelle muss eh, wie es jetzt im Gesetz auch vorgibt, muss das viel mehr abgekapselt und unzugänglich sein. Und das Wesentlichste ist der Parteienverkehr, der hat in einer Leitstelle, in der Nähe einer Leitstelle nichts zu suchen. Und natürlich dann halt in weiterem Sinne dann noch die ganzen anderen Schutzmaßnahmen, eben wie eine USV oder vor äußerlichen Einflüssen, dass man das gesichert hat. Aber das ist für mich mal das Wichtigste.

A: Also der Schutz vor Bedrohungen durch intentionale Gewalt.

B: Genau, ja.

A: Kommen wir jetzt zu den Cyberrisiken, die österreichische Bundesregierung hat sich klar zur Neutralität bekannt und unterstützt die Ukraine im aktuellen Konflikt mit

humanitärer Hilfe, ganz im Gegensatz zu Deutschland, die auch Kriegswaffen in die Ukraine liefern. Jetzt ist anzunehmen, dass Deutschland oder speziell das deutsche Energienetz von Hackern in Form von Repressalien angegriffen wird. Wenn nun das deutsche Energienetz zu Schaden kommt, sind durch Kaskadeneffekte auch Auswirkungen auf das österreichische Stromnetz zu erwarten. Wie hoch schätzen Sie die Bedrohung für Österreich durch so einen Kollateralschaden ein, wenn eben das deutsche Stromnetz crasht, dass auch wir davon betroffen wären?

B: Ich schätze das sehr hoch ein, ich schätze auch, dass das nur eine Frage der Zeit sein wird, aber dadurch, dass wir ausreichende Vorsorgemaßnahmen getroffen haben, habe ich jetzt nicht wirklich Angst davor.

A: Bezogen auf die Berufsrettung Wien.

B: Genau. Was andere Magistratsabteilungen wie Feuerwehr, etc. machen, weiß ich nicht, wie weit sie da fortgeschritten sind mit dieser, aber es ist auch in der Magistratsdirektion gibt es auch schon Pläne, also ich glaube, die Stadt Wien wäre ganz gut gerüstet.

A: Gut, bleiben wir noch beim Blackoutszenario, Blackout wird als ein überregionales, über mehrere Tage andauernder Stromausfall angesehen und das bringt natürlich das gesellschaftliche Gefüge durcheinander und stellt natürlich eine Bedrohung dar. Welche Maßnahmen hat Ihre Organisation gesetzt, um auf ein solches Blackoutszenario vorbereitet zu sein? Also die Notstromaggregate sind schon mal erwähnt worden.

B: Genau, wir haben die, ja da muss ich das Protokoll aufmachen, dass ich alles vorlesen kann, was wir schon alles gemacht haben. Nein, aber es fällt mir schnell ein, dass wir die Erreichbarkeit der Fahrzeuge immer gegeben haben, sowohl mittels Funk, weil der sollte ja weiterhin funktionieren mindestens 3 Tage. Wir sind beim Implementieren von diversen Pagern, sollte das auch irgendwann einmal nicht mehr gehen, die Dateneingaben der Patienten haben wir sichergestellt, mit der Stromversorgung (unv.), mit den Zigarettenanzündern. Also prinzipiell sollten wir, sollten wir ein Blackout haben, von der Berufsrettung haben wir sichergestellt die Verbindungen teilweise in die Krankenhäuser, weil die ja auch mit Strom laufen, von den alten Kupferleitungen, die haben die teilweise auch noch auf den Stationen. Wir haben sichergestellt, momentan die Erreichbarkeit zu den Stationen mittels BOS, da

finden regelmäßig Überprüfungen statt, also im Falle eines Blackouts sind wir, sind die Dieselsachen, Sprit ist soweit gesichert, die USV sind gesichert, also von daher sehe ich einem Blackout, speziell bei der Berufsrettung, will ich nicht sagen positiv entgegen, aber wir sind sicher eine der bestens gerüsteten Magistratsabteilungen.

A: Inwieweit wurden andere Interessengruppen bei der Erstellung von Krisen- und Katastrophenplänen denn berücksichtigt?

B: Andere was?

A: Interessensgruppen, eben Spitäler sind genannt worden, inwieweit findet da mit Polizei, anderen Einsatzkräften die Abstimmung statt?

B: Naja, an und für sich von unserer Seite noch nicht wirklich. Das ist alles erst, wir arbeiten ja mit Hochdruck erst seit einem halben Jahr daran, davor war es immer nur so ein Step by Step Thema. Aber seit Jänner arbeiten wir jetzt mit Hochdruck daran. Ja, Wigef tausche ich mich jetzt demnächst aus, wie die das planen, von unserer Seite, von der Berufsrettung Wien Seite, ist ja alles gesichert. Wir fahren notfalls in das nächstgelegene Krankenhaus, da fährt die Eisenbahn drüber. Soll aber nicht sein, deswegen soll man es ja auch in so einem Fall gut koordinieren, vor allen Dingen um dann auch bei kritischeren Patienten das richtige Spital dann auch anzufahren. Deswegen gibt es da demnächst einen Austausch, Feuerwehr habe ich noch keinen Austausch diesbezüglich, da hat die Magistratsdirektion zum Teil, da gibt es eigene Pläne. Und Polizei auch noch nichts diesbezüglich.

A: Kommen wir zu einem anderen Thema, mehr in Richtung der Bevölkerung und deren Schutz. Es ist durch mehrere Studien belegt, dass die urbane Bevölkerung in puncto Eigenbevorratung eher schleissig vorgeht, man ist es gewohnt, wenn man Hunger hat, wird just in Time eine Pizza bestellt oder einfach das nächste Lokal aufgesucht, bzw. den Nahversorger. Jetzt ist es so, dass im Falle eines Blackouts die kritischen Infrastrukturen weiterhin Wärme, Wasser und Strom zur Verfügung haben. Sie aber gleichzeitig nicht für die Betreuung von Betroffenen ausgelegt sind, sondern eben andere Kernaufgaben haben. Wie soll Ihrer Meinung nach mit der Problematik umgegangen werden, dass eben dann die notleidende Bevölkerung kritische Infrastrukturen aufsuchen wird, um dort eben Wasser, Wärme und Strom und Essen zu bekommen.

B: Ja ist eine gute Frage, weil wie wir wissen aufgrund vom Hauptinspektionsoffizier gibt es die Möglichkeit, dass uns die Nahversorger trotzdem noch kurz versorgen mit Lebensmitteln, weil das dient hauptsächlich natürlich mal der Mannschaft. Inwieweit das dann für die Bevölkerung tragend wird, was sicherlich verständlich ist, dass die das aufsuchen, ist spannend, kann ich dir aber leider nicht beantworten. Weil auch dort wird keine Kassa mehr funktionieren, da wird kein Kühlsystem mehr funktionieren, deswegen sage ich ja, es sollte jeder mindestens für 1,2,3 Tage Vorräte im Haus haben, das sollte standardmäßig sein. Aber wie es genau dann für die Gesamtbevölkerung ausschaut, wobei es im urbanen Bereich, ich glaube, dass dann schon egal ob am Land oder in der Stadt, das wird für alle ein Problem werden. Aber ich habe jetzt auch keine Ideen, wo ich jetzt sagen kann, das ist es. Aber zumindest ist sichergestellt, dass die Mannschaft die nächsten 3 Tage versorgt werden kann, seitens Berufsrettung. Der Bevölkerung muss ich leider einen Passus geben, das kann ich leider nicht sagen.

A: Gut, heutzutage sind ja sämtliche modernen Systeme auf elektrischen Strom angewiesen, der Energiesektor hat die prominente erste Stelle im NIS-Gesetz und in der NIS-Verordnung, beim Strom ist also die Vernetzung von kritischen Infrastrukturen vollkommen klar und liegt auf der Hand. Anders sieht es bei anderen Bereichen, wie beispielsweise der Gesundheitsbranche aus. Geht Ihrer Meinung nach die NIS-Gesetzgebung ausreichend auf die wechselseitige Abhängigkeit kritischer Infrastrukturen ein?

B: Ich glaube schon. Weil es ist so detailliert, dass jeder seine Vorgaben hat, die er erfüllen muss und somit sehe ich da das vollkommen abgedeckt vom NIS-Gesetz.

A: Gut, kommen wir jetzt zur medizinischen Versorgung der Wiener Bevölkerung mit den letzten beiden Fragen. Die medizinische Behandlung wird als Versorgungsprozess, als Behandlungsprozess von Beginn an mit dem Notruf, bis zur endgültigen Versorgung im Krankenhaus als ein Behandlungspfad angesehen, mit mehreren Subprozessen dazwischen. Wenn nun jeder Bereich, sei es die Telekommunikation, Rettungsdienst und Krankenhaus für sich autark funktioniert, wie beurteilen Sie diesen Begriff „Autarkie“ im Rahmen vernetzter und systemübergreifender Prozessketten?

B: Können Sie mir das verdeutschen?

A: Wenn jeder für sich funktioniert, sollte ja an und für sich ja das gesamte System auch funktionieren, sehen Sie das auch so.

B: Genau.

A: Wird diese Ansicht geteilt?

B: Auf Minimumanforderung auf jeden Fall. Das was es tun soll, wird es können, alles andere wird natürlich, ich meine da reden wir jetzt von Wartezeiten etc., das wird natürlich nicht so professionell ablaufen, aber das was Wien können muss, das wir das auch können. Davon bin ich sicher überzeugt.

A: Gut und zu guter Letzt, von der Berufsrettung Wien und den Partnerorganisationen wie dem Rettungsverbund werden täglich zwischen 800 und 1000 Notfallpatienten behandelt. Ein Gutteil davon in Wiener Krankenanstalten zur medizinischen Folgeversorgung gebracht. Zusätzlich versorgen die Wiener Spitäler auch tausende weitere Personen im Rahmen von Selbsteinweisungen oder ambulanter Nachversorgung. Die Kapazitäten und Strukturen der Krankenhäuser sind dabei auf die Individualmedizinische Versorgung unter normalen Betriebsbedingungen ausgelegt. Jetzt zur konkreten Frage, welche Maßnahmen erachten Sie als sinnvoll, damit eine medizinische Basisversorgung eines Großteils der Wiener Bevölkerung, auch unter den negativen Auswirkungen eines Cybernotfalls oder eines Blackouts, sichergestellt werden können?

B: Naja, zum Cyberangriff kann ich folgendes sagen, wir haben sich abgesichert dafür, das hat auch sehr viel Geld gekostet, dass man die Server so weit absichern gegen solche Angriffe, d.h. wir sind hier geschützt. Wir sind zwar kurzfristig angegriffen, stellen aber innerhalb von 10min. das System wieder her. Hat auch viel Geld gekostet. Ich hoffe, dass das andere auch machen. Insofern, aber die Frage war konkret ja, ob die Patientenversorgung dann noch weiterhin so funktioniert – ja muss es und davon bin ich überzeugt, weil wenn es in Klagenfurt wo ein Spital ist, wo alles hinkommt, Wien hat über 20 Spitäler, bin ich davon felsenfest überzeugt, dass die Versorgung -

A: Dass die Basisversorgung gewährleistet ist.

B: Ja. Das auf jeden Fall. Nein, muss so sein, ist auch so. Und all die kleinen Probleme, die man im Regeldienst oder im Regelfall hat, die zählen dann in so einem Fall ja auch

nicht. Da greifen ja dann ganz andere Pläne und von daher bin ich überzeugt, dass es Wien sogar am Besten hat, von allen Bundesländern.

A: Herzlichen Dank für die Erläuterungen.

B: Gern.

Interview mit Frau Dipl.-Ing.in Heissenberger, MBA am 11.05.2022

A: 11. Mai 2022. Expertinnen Interview mit Frau Diplomingenieurin Heissenberger. Erste Frage. Die EU-Richtlinie wurde in nationales Recht überführt. Dem NIS-Gesetz und eine dazugehörige NIS-Verordnung. Zielt auf den Schutz der kritischen Infrastrukturen ab. Und wie ordnen Sie die Notwendigkeit für eine gesetzliche Regulierung zu Einhaltung von IKT-Sicherheitsstandards ein? Zumal viele kritische Infrastrukturen bereit sind, Informationssicherheits-Managementsystem implementiert haben und betreiben.

B: Also ich halte das für eine ganz wichtige Sache, dass man IKT-Sicherheitsstandards erstens einmal EU-weit reguliert und hier versucht, ein einheitliches Niveau zu erzeugen und das auch mit einem Gesetz letztendlich verankert. Weil zum einen viele, einige betreiber-kritische Infrastrukturen gar kein ISMS implementiert haben und zum Zweiten es nicht ausreicht, ein ISMS zu implementieren, sondern man muss eben, wenn man Sicherheit wirklich lebt, viel mehr als sozusagen in die Tiefe gehen, auch inhaltlich. Und die Dinge auch dann wirklich umsetzt und nicht nur einer Norm gegenüber, also einer Norm gegenüber einem Auditor nachweisen, sondern das muss auch wirklich überprüft werden. Und das halte ich für die IT-Sicherheit und das Sicherheitsniveau für Österreich sehr wichtig.

A: Und worin liegt Ihrer Meinung nach der Mehrwert für die Gesellschaft durch eine bundesgesetzliche Reglementierung, wenn es eben dazu schon Normen gegeben hat?

B: Also ich glaube, dass gerade das NIS-Gesetz. Ich kenne ja eigentlich sehr viele Normen im Bereich der Informationssicherheit, das NIS-Gesetz auch noch einen Schritt eben weiter geht, weil es eben die Dinge, die in den Normen stehen, noch detaillierter aus meiner Sicht in manchen Bereichen regelt und vor allem auch die Möglichkeit bietet, wirklich durch eine Behörde auch dann die Maßnahmen zu überprüfen. Das habe ich nicht, wenn ich eine Norm habe. Eine Norm verwende ich freiwillig und lasse mich zertifizieren, wenn ich möchte oder nicht. Ein Gesetz muss ich machen und da habe ich eben auch gegenüber einer Behörde einen Nachweis zu erbringen. Beziehungsweise es wird wirklich aktiv geprüft. Und das ist einfach eine höhere Qualität, dann auch bei der Umsetzung. Es wird ernster genommen. Und letztendlich glaube ich, der Mehrwert ist, dass wir wirklich also umfassendere Sicherheitsmaßnahmen dann in den kritischen Infrastrukturen implementieren. Sie

brauchen, war ja die Frage beim Durchlesen, die habe ich mir eh schon genug durchgelesen. Oder brauchen sie es?

A: Nein, brauche ich nicht extra.

B: Dann beantworte ich einfach zwei A.

A: Gut, ja. Ja gerne.

B: Die Bedeutung. Genau das NIS-Gesetz gegenüber dem österreichischen Programm-Schutz. Ja, genau, (unv.) kritisch und die Strategie. Also nicht, das eine ist der Schutz, das Programm Schutz kritischer Infrastruktur. Das gibt es schon eben seit 2008 und das ist, finde ich, ein guter Ansatz einmal gewesen zu sagen, wir haben kritische Infrastruktur in Österreich, die muss man entsprechend schützen. Aber die ist auch sehr stark auf den also organisatorischen oder, glaube ich, physischen Schutz ausgerichtet gewesen und weniger auf den IT Teil. Ich habe das, glaube ich, damals auch ein bisschen mitverfolgt. Irgendwann ist irgendwo ist dann einmal ein Satz hineingekommen, dass auch die Netz- und Informationssicherheit gewährleistet sein muss. Weil ich glaube, in den Jahren von 2008 bis jetzt hat sich ja sehr viel entwickelt und die Systeme sind immer abhängiger geworden. Das waren nur ein, es hat sicher was gebracht für uns, dass man mal eine Liste gehabt hat, was ist überhaupt kritische Infrastruktur. Und diese Bedeutung auch des Schutzes erkannt hat. Was war das Gesetz. Auf jeden Fall regelt es wirklich, dass man sagt, die Systeme sind ganz stark von der IT abhängig und die brauchen eben technische und organisatorische Sicherheit. Und das eben, da geht es ja nur um die Netz- und Informationssicherheit und nicht um das ganze Drumherum und die Strategie. Also aus meiner Sicht ist auch eine Strategie nie so weitreichend und greift natürlich auch nie so stark wie ein Gesetz oder eine Richtlinie, weil in der Strategie steht da drinnen eine Vision, wo soll man, wo möchte man hin. Ja, und vielleicht sind auch noch Ziele beschrieben, aber es ist meistens nicht ein Umsetzungszwang. Man muss sich dann selbst überlegen, wie man diese Ziele erreicht. Und das NIS-Gesetz gibt halt ganz stringent vor in diesem, ich glaube, zwölf oder elf Kapiteln hat es, weiß ich jetzt nicht genau. Elf. Was zu tun ist in den einzelnen Bereichen.

A: Und eben auch die entsprechende Verpflichtung und eine Strategie.

B: Und eine Verpflichtung eben. Und wenn man sie nicht macht, gibt es eben auch Strafen. Und ich glaube, das ist halt auch wichtig. Und viel, greift eben viel weiter, bringt inhaltlich viel mehr als eine Strategie, die man halt schreibt. Dann die Frage drei. Welche Risiko-Szenarien für kritische Infrastrukturen kommen Ihnen in den Sinn? Also. Ja, wo wir natürlich als Stadt die meiste Sorge haben, ist, dass eben unsere Systeme, unsere IT-Systeme, mit denen wir kritische Infrastruktur betreiben, ausfallen. Und das kann ja aus aufgrund von, eben wie da steht auch schon technischen Gebrechen, Naturgefahren oder Cyberangriffen sein und das Risiko, das wir eigentlich haben. Der Schaden ist eigentlich dann sozusagen das Problem. Das entsteht bei uns nämlich, dass wir wirklich Teile, wichtiger Teile wie Wasser oder eben die Rettung oder eben die Krankenhäuser nicht mehr betreiben können. Und das sind dann die Folge und die Konsequenzen, dass wirklich ein Schaden für die Stadt Wien oder für die Bevölkerung. Und ich glaube, das ist ja auch im NIS-Gesetz so definiert, dass Auswirkungen auf das (unv.) funktionierendes (unv.).

A: Dass die Auswirkungen auf eine gewisse Anzahl an Leute.

B: Wobei das eben dann erst für unsere Stadt natürlich eine Krise ist, wenn es einen größeren Bereich umfasst.

A: Also wenn ein Krankenhaus betroffen wäre, wäre es zwar schlimm, aber eben noch nicht so die Katastrophe.

B: (unv.) sind wir so aufgestellt im Krisenmanagement. Wir haben ja Gott sei Dank auch Versorgungspläne und das wird der Herr (unv.) auch morgen dann erzählen. Da gibt es auch Notfallpläne und Betriebskontinuitäts-Managements ist ja auch überall im Einsatz, das heißt auch in der IT. Wenn ein IT-System ausfällt, soll es einen Notfallplan geben, wenn, was man halt dann tut in der Zeit, bis die IT wieder vorhanden ist. Aber wenn eben größere Dinge passieren, ein Stromausfall zum Beispiel passiert. Dann hat man ja wirklich nur mehr über einen gewissen Zeitraum, nämlich so lange man noch Treibstoff hat für die Diesel-Aggregate. Die Möglichkeit, die IT weiterzubetreiben und das sind eben nicht mehr wie 72 Stunden.

A: Dann Thema vier. Hole ich ein bisschen weiter aus. Da geht es im Wesentlichen drum. Da hat eben die Ukrainekrise mit reingespielt und die österreichische Regierung beteiligt sich ja nur mit humanitärer Hilfe bei der Ukraine-Hilfe. Deutschland hingegen hat sich dazu entschlossen, Waffen zu schicken und setzt sich damit einem erhöhten

Risiko von Cyberangriffen auf die kritische Infrastruktur aus. Und die konkrete Frage ist. Wie schätzen Sie es ein, dass wenn das deutsche Stromnetz gehackt wird oder lahmgelegt wird, ob wir dann als Österreich einen Kollateralschaden davontragen?

B: Das kann ich jetzt nicht so gut beantworten. Das wird der Herr (unv.), sagen können. Ich glaube sehr wohl, dass das eine Auswirkung hat auf Österreich. Weil wir, glaube ich, auch von Deutschland sehr abhängig sind, was die Stromlieferungen betrifft. Aber ich hätte die Frage anders verstanden, ich hätte eher verstanden. Sie meinen, ob wir überhaupt eine Bedrohung durch die Ukraine sehen. Das nicht.

A: Nein.

B: Okay, dann fragen Sie bitte den Herrn, das kann nicht beurteilen. Da bin ich nicht kompetent.

A: Gut, jetzt auf die Organisation Magistrats-Direktion gerichtet, also Organisation der Stadt Wien. Welche Maßnahmen hat die Organisation gesetzt, um auf ein Blackout-Szenario vorbereitet zu sein? Müssen jetzt keine, also sollen keine Geheimnisse sein, sondern einfach nur so grob die Strategie, die verfolgt wird.

B: Was ich weiß, aber das ist eben die Gruppe Krisenmanagement, die da verantwortlich ist, dass wir immer wieder diese, also verschiedene Krisenszenarien, darunter auch Blackouts, quasi diese, wie sagt man da, dass man sich sozusagen, dass man so überlegt, was wir dann machen, in diesem Fall also Notfallpläne macht auch, das weiß ich. Das macht man zu Blackout-Themen. Das machen wir bei Hochwasser, also bei Starkregen-Ereignissen, bei Erdbeben und bei Katastrophen. In der IT selbst kann ich mehr dazu sagen, wenn ein Stromausfall ist, sind unsere Rechenzentren, derzeit geht es eigentlich darum, dass ich dann die IT nicht mehr betreiben kann. Und wir können, unsere Rechenzentren sind so ausgelegt, wir haben ja hochsichere und ausfallsichere Rechenzentren. Wir können 72 Stunden den IT Betrieb aufrechterhalten, weil da haben wir eben Diesel-Aggregate, Strom-Aggregate, die mit Diesel betrieben werden und Diesel, eben Vorräte für 72 Stunden, mehr nicht.

A: Und aber die könnten ja auch nachgefüllt werden.

B: Die können nachgefüllt werden. Nur da gibt es auch Pläne dafür, glaube ich. Das weiß der Herr (unv.). Nur ist es, sage ich immer, wenn wirklich ein Stromausfall in der Stadt hat, gibt es dann auch wieder Anlauf-Pläne, wo man sagt, man fährt zuerst mit

den allerwichtigsten Funktionen in der IT auch hoch, wird nicht eine Vollfunktionalität in einem Rechenzentrum benötigen. Es wird vielleicht auch so sein, dass der Diesel, der dort vorrätig ist, für woanders dann gebraucht wird, (unv.). Also diese ganzen Vernetzungen gibt es da auch, dass man auch sogar, glaube ich, so weit geht, dass man den Diesel vom Rechenzentrum auch für andere Dinge dann verwenden kann. Aber es gibt auch ganz konkrete Katastrophen-Pläne, wo man weiß, in der IT, wenn ich einen Stromausfall habe und dann eben von meinem Strom-Aggregat Systeme betreibe, welche zentralen Systeme betreibe ich. Und das noch mindestens einmal im Jahr getestet, ob diese Anlagen funktionieren.

A: So richtig stromlos gemacht und schauen, ob alles anspringt.

B: Wird geschaut, ob die alle anspringen. Und immer wieder wird Szenario in der IT auch geübt, dass es abgedreht wird und dann wieder hochgefahren, weil man ja in der IT das Problem hat. Aber das heißt ja nicht, wenn man es abdreht, dass (unv.) wieder funktioniert.

A: Gut jetzt, wenn ich mich in Richtung Wiener Bevölkerung. Es gibt Studien dazu, wonach die urbane Bevölkerung die Eigen-Bevorratung vernachlässigt. Man ist gewohnt, wenn man Hunger hat, dann bestellt man sich eine Pizza oder dergleichen oder geht ins nächste Lokal. Aus dem Grund darf davon ausgegangen werden, dass nach etwa zwei bis drei Tagen die Sicherheitslage erheblich verschärft wird, weil die hungrige, frierende Bevölkerung sogenannte Lichtinseln aufsuchen wird. Welche, was meinen Sie, sollte man? Welche Maßnahmen sollte man ergreifen, damit es nicht dazu kommt, dass dann eben eine hungrige Bevölkerung, das allgemeine Krankenhaus oder sonstige kritische Infrastrukturen, die ja weiterhin laufen, dann bevölkert und von der Kerntätigkeit abhält.

B: Um ehrlich zu sein, ich weiß, dass da Sachen gibt bei uns, aber da bin ich eben auch nicht, da müssen Sie den Herrn (unv.) fragen. Der weiß das, der kann (unv.).

A: Der macht das im Rahmen des Hintergrundgesprächs.

B: Der macht das, ja. Also das weiß ich nicht, aus der IT heraus, da können wir, glaube ich, auch aus der IT heraus nix machen.

A: Dann konkreter zum NIS-Gesetz. Der Energiesektor steht sowohl in der Verordnung als auch im Gesetz an erster Stelle. Alle modernen Systeme sind vom Strom abhängig.

Und zeigt doch, wie sehr die kritischen Infrastrukturen untereinander vernetzt sind. Geht Ihrer Meinung nach die NIS-Gesetzgebung auf diese Vernetzung und wechselseitige Abhängigkeit ausreichend ein?

B: Nein, aus meiner Sicht überhaupt nicht. Aus meiner Sicht gibt es auch keine Reihung bei den Sektoren, auch wenn das an erster Stelle steht. Ist das vielleicht zufällig. Ist die sicher der wichtigste Sektor oder einer. Ich würde das nicht sagen. Die Gesundheit ist genauso wichtig. Nein, die gehen ja überhaupt nicht auf die Abhängigkeiten ein. Gar nicht. Das muss man sich selbst in seinem eigenen Krisenmanagement überlegen. Wie man eben dann vorgeht, wenn eben ein Teil vom Stromausfall oder ein Teil vom Rechenzentrum ausfällt oder von den anderen Bereichen. Und da gibt es aber auch, glaube ich, noch ganz wenige Überlegungen. Wir haben einmal ein EU Projekt, ich mit dem Herrn Kneissl gemeinsam gemacht. Und das läuft, glaube ich sogar noch, wo es darum geht, eben so Simulationen zu machen. Wie wirkt sich das in der Stadt aus, wenn eben Strom ausfällt. Dann habe ich keine U-Bahn, dann habe ich eben keine Versorgung mehr. Dann fallen die Kühlungen aus in den Supermärkten. Und wie wirkt sich das auch aus, wenn das nur in einer Region funktioniert. Das ist aber hochkomplex. Da wollten wir mal ein System entwickeln, das ist nachher, ich glaube, das weiß ich gar nicht, was daraus geworden ist. Aber im NIS-Gesetz ist diese Komplexität überhaupt nicht abgebildet. Oder sehen Sie das anders?

A: Sehe ich genauso und freue mich, dass ich da nicht als einziger diese Meinung vertrete. Ja, jetzt hole ich ein bisschen aus. Die medizinische Behandlung von Erkrankten sehe ich als Prozesskette, als einen gesamten Pfad vom Notruf bis zur finalen Versorgung in der Krankenanstalt. Und jetzt versucht natürlich die Krankenanstalten autark zu sein, unabhängig von allen anderen Anbietern. Der Rettungsdienst versucht es, auch der Telekommunikationsbetreiber und wie beurteilen Sie den Begriff Autarkie im Rahmen eines vernetzten und systemübergreifende Prozesskette?

B: Na ja, das ist schwierig. Also ich glaube, wir sind ja in einer total vernetzten Welt. Im gerade zum Beispiel, also Sie wissen es in der Rettung, da ist ihr System in der Rettungsdienst ist in einem eigenen Netzwerk, das heißt, dort kann ich, das ist so abgeschottet, da kann ich vielleicht sogar, da habe ich wenig Schnittstellen, sozusagen zu anderen Netzen auch. Aber autark heißt in Wahrheit. Ich kann selbstständig mich versorgen und bin nicht abhängig von irgendwo. Und das ist halt immer weniger

heutzutage gegeben auch durch, die meiner Meinung nach, IT und Vernetzung. Ja, weil ich eben. Ja, weil es eben alles in einem Netzwerk sich befindet und es sehr, sehr viele Schnittstellen zu anderen Dingen gibt und die Dinge immer komplexer werden. Deshalb ist es irrsinnig schwierig. Ich weiß nur vom allgemeinen Krankenhaus der Stadt, dass das relativ autark betrieben werden kann, auch was die Energie betrifft, weil die ja dort ein eigenes Kraftwerk haben.

A: Und sogar eine eigene Wasserversorgung, wie ich heute gelernt habe.

B: Das wissen Sie wahrscheinlich vom (unv.). Ja, genau, sie haben eine Betriebsfeuerwehr und ich weiß nicht, was alles. Also die sind relativ autark, ist aber auch in dem Fall. Die anderen Spitäler, glaube ich, haben das so nicht. Ich meine Notstromversorgung schon klarer Weise. Aber auch dort weiß ich, dass die OPs auch nicht endlos lang betreiben können, sondern ich glaube, im Katastrophen- und Krisenmanagement sind immer diese 72 Stunden ein Richtwert. Und wenn jetzt aber wirklich der Strom ausfällt und wir so Blackout-Szenario haben, ist es relativ bald dann vorbei. Diese drei Tage, nicht. Und danach muss man eigentlich sagen, wenn das dann aus ist, der ganze Diesel verbraucht ist, der Treibstoff, was ist dann, nicht? Dann müssten wir ja dann mit den Systemen wieder hochfahren. Also das ist, glaube ich, in der heutigen Welt der Vernetzung schwer herzustellen, Autarkie. Oder man hat sozusagen, Autarkie bedeutet dann aber auch Verlust von Informationsaustausch, kostet aber wahrscheinlich dann auch mehr Geld. Und heutzutage ist ja alles ausgerichtet auf Einsparung. Das heißt, man will eben die Dinge nicht redundant auch betreiben. Ja, also ich glaube, dass sich das ein bisschen widerspricht. Umso stärker vernetzt, umso weniger autark, würde ich fast sagen.

A: Ein ähnliches Resümee kann ich bis dato ziehen. Und zu guter Letzt noch eine Frage nahezu nur rettungsdienst-mäßig. Also die Wiener Rettung versorgt am Tag zwischen 800 und 1000 Notfallpatienten, bringt sie dann zu einer Endbehandlung auch ins Spital. Gleichzeitig gibt es dann auch noch Selbst-Einweisungen und Krankentransporte für die Nach-Versorgung und die aktuellen Strukturen und Kapazitäten sind halt auf einen Normalbetrieb ausgelegt. Welche Maßnahmen würden Sie als sinnvoll erachten, um die medizinische Basisversorgung des Großteils der Bevölkerung auch unter den negativen Auswirkungen eines Cyberangriff oder eines Blackouts sicherzustellen?

B: Ich meine, ich glaube, dass man diese Dinge, einen Cyber-Notfall oder muss man schauen, was bedeutet ein Cyber-Notfall dann in diesem Fall. Nämlich wahrscheinlich, dass die Krankenhaus, die wesentlichen Systeme in einem Krankenhaus nicht mehr verfügbar sind und ich die Patienten halt nur mehr, also nicht mehr mit IT unterstützt versorgen kann. Ich glaube, man muss sich überlegen Notfallpläne zu haben für den Fall, dass die IT ausfällt. In beiden Fällen auch im Blackout-Fall. Also im Blackout haben wir ja schon davon gesprochen, dass ja die Krankenhäuser in dem Fall auch einige Zeit lang noch funktionieren, auch die Rechenzentren. Wir haben ja das zentral, das Rechenzentrum für alle Krankenhäuser, das kann noch drei Tage weiter funktionieren beziehungsweise wie ich auch schon gesagt, also wichtig ist glaube ich sich das Szenario zu überlegen, durch zu spielen und auch zu beüben. Also das macht auch der Wiener Gesundheitsreform regelmäßig, dass sie gewisse Krisen und Katastrophenfällen üben. Aber dann, das geht eben auch so weit, dass man dann nicht nur sagt, die IT ist ausgefallen. Und ich kann jetzt den Patienten nicht mehr fassen, was ein großes Problem ist, wenn ich dann nicht mehr weiß, wenn der wohin kommt, wer das ist. Ich kann nirgends mal nachschauen, was der gehabt hat. Ich weiß ja gar nichts mehr zu dem. Ja. Das heißt, theoretisch kann ich ihn auch ganz schwer behandeln, wenn er jetzt nicht (unv.) oder bewusstlos ist. Das ist ja ganz schwierig, wenn die IT ausfällt. Aber die machen ja ganz umfassende, also sehr, sehr viel umfassende Übungen auch immer wieder zu diesen ganzen Krisenfällen, bis hin, dass sie sich auch, glaube ich, überlegen, wie dann die Transporte von den Patienten logistisch erfolgen und in welche Spitäler ich ausweichen kann. Also diese Übungen, glaube ich von den Szenarien sind total wichtig. Ja.

A: Super. Herzlichen Dank.

Interview mit Herrn Prof. Dr. Hellwagner am 19.05.2022

B: (unv.).

A: Doch, doch, ich habe ihn schon begrüßt. 19. Mai 2022, Interview mit Herrn Professor Dr. Hellwagner. Herr Professor, wir widmen uns zunächst einmal der europäischen Richtlinie zur Gewährleistung eines hohen Sicherheitsniveaus von Netz und Informationssystemen, kurz NIS-Gesetz. Wie ordnen Sie die Notwendigkeit einer gesetzlichen Regulierung zur Einhaltung von IKT Sicherheitsstandards ein, zumal von vielen kritischen Infrastrukturen ein Informations- (unv.) System implementiert wurde und betrieben wird?

B: Nein, grundsätzlich ordne ich. Also ich ordne sehr hoch ein, weil mir schon bekannt ist, dass gerade im Bereich der kritischen Infrastruktur die Datensicherheit und die Informationssicherheit und auch die Absicherung der EDV beziehungsweise der Programme elend ist, elend. Es beginnt ja schon in dem Bereich, wo ich bin, in der Sozialversicherung, wo schon mehrfach Daten gestohlen wurden. Das wissen wir. Salzburg Gebietskrankenkasse ist ja schon gehackt worden und wir wissen gerade jetzt auch durch den Konflikt Russland Ukraine, dass diese kritische Infrastruktur ein absolutes Ziel dieser Angriffe ist. Dass dieser Krieg auf der Cyberebene. Der sich eben auf diese Systeme bezieht und auf diese Systeme angreift. Hoch gefährlich und auch wichtig ist, auch für Konfliktparteien wichtig ist, weil die kritische Infrastruktur nur mehr aufgrund dieser Systeme funktioniert. Wir haben keine analogen Resilienz mehr, das heißt, wir funktionieren nur mehr aufgrund dieser software-gestützten Steuereinrichtungen und Überwachungseinrichtungen. Und wenn die ausfallen, dann fällt das ganze Kartenhaus. Weil wir in der Zwischenzeit ja auch so vernetzt sind, vor allem auf Energie-Ebene so vernetzt sind, die Stromnetze so vernetzt sind, dass wenn ein Teil ausfällt, bricht eigentlich ganz Europa zusammen. Das ist ja die große Angst von Blackout. Wenn eine kritische Schaltstelle angegriffen werden kann, dann fällt Europa in einen Blackout. Und das Problem ist, dass das vielen aus meiner Sicht auch Entscheidungsträgern, die sich damit, die das betreiben, nicht bewusst ist, was das heißt und diese Systeme ganz schlecht abgesichert sind. Und ich glaube, dass das rechtlich ein unbedingtes Muss ist, dass man das vorschreibt. Weil das ist teuer, das kostet viel Geld. Diese Firewalls, diese Verschlüsselung, diese krypto-logischen Absicherungen zu schaffen, kostet Geld. Und das machen Betriebe, die auf Gewinn ausgerichtet sind. In der Zwischenzeit ist bei uns alles auf Gewinn ausgerichtet, auch

die Infrastruktur ist ja eigentlich auf Gewinn ausgerichtet. Die Betreiber der (unv.) machen das nur, wenn es ihnen gesetzlich vorgeschrieben wird, weil sonst minimiert es den Gewinn und wenn es den Gewinn minimiert, ist es mit stiefmütterlich behandelt.

A: Und würden Sie sagen, dass dadurch auch der Mehrwert für die Gesellschaft liegt, eben dadurch, dass es bundeseinheitlich geregelt ist?

B: Natürlich, wird die Gesellschaft dadurch resilienter wird. Wir haben ja ständig das Risiko, dass wir durch so einen Angriff, durch so einen Cyberangriff lahmgelegt werden, was ja nicht nur ein Schaden für Einzelne ist und für diese, sondern das ist ja dann ein gesamtgesellschaftlicher Schaden, ein gesamt österreichischer Schaden und eigentlich der Vernetzung innerhalb der EU ein gesamteuropäischer Schaden wird.

A: Nun gab es bereits zwei Strategien der Bundesregierung einerseits zum Schutz der kritischen Infrastruktur und dann noch weiter eine österreichische Strategie für Cybersicherheit. Ja, diese kann in gewisser Weise als Ergänzung zu bestehenden Normen wie der ISO 27000, die sich explizit auf Cybersicherheit fokussiert, gesehen werden. Welche Bedeutung messen Sie den beiden Strategien? Also einerseits Schutz kritischer Infrastruktur und SZ, einmal CS und Normen im Vergleich zum NIS-Gesetz bei?

B: Also das Gesetz kenne ich im Detail nicht, deswegen kann ich mich da im Detail dazu nicht äußern. Und also ich messe meine hohe Bedeutung in der Gesamtstruktur, das Gesamtsicherheitsstruktur bei. Ich kann mich aber im Detail zu diesen Normen nicht äußern, weil ich sie zu wenig kenne. Okay.

A: Gut. Sie haben es bereits erwähnt. Kritische Infrastrukturen sind ja einem breiten Spektrum an Bedrohungen auch ausgesetzt. Sicherheits-Management, Risikomanagement sind per se Querschnitts-Materien, die gesamte Organisationen und Bereiche umfassen müssen, um möglichst alle Gefahren-Potentiale zu identifizieren und zu analysieren. Die NIS-Richtlinie befasst sich da explizit mit Cyberangriffen, aber auch technische Gebrechen und Naturgefahren und sonstige Störungen werden darin berücksichtigt. Welche Risiko-Szenarien für kritische Infrastrukturen kommen Ihnen in den Sinn und welche betrachten Sie aktuell als vorrangig?

B: Ja, Risikoszenarium ist alles, was denkbar ist. Murphys Gesetz. Man kann nichts ausschließen. Ich meine, das, was sicherlich jetzt aktuell am risikoreichsten ist, sind die Angriffe, die erfolgen aus Russland, weil hier doch offensichtlich von russischer Seite eine Hegemonie gegen Europa und gegen die EU verfolgt wird, die lange aufgebaut wurde und die auch mit Angriffen auf diese Infrastruktur verbunden ist, immer wieder verbunden ist und sein dürfte. Aber natürlich unterschätzen wir die natürlichen Gefahren, Katastrophen immens, indem wir überhaupt nicht berücksichtigen, was es heißt, wenn Freiland-Leitungen ausfallen und in großer Fläche plötzlich die Energieversorgung zusammenbricht und mit dem Zusammenbrechen der Energieversorgung, die Rückfallebenen gefordert werden, die Notstromversorgung angefordert werden. Weil gerade in der Cybersicherheit wissen wir braucht es Strom, Energie. Energie ist alles und wenn ich das nicht bereitstellen kann, für einen größeren Zeitraum bereitstellen kann und keine Rückfallebenen habe, dann bricht das System relativ rasch zusammen. Und gerade im Hochfahren der Systeme bin ich wieder verwundbar, weil im Hochfahren der Systeme kann ich nicht sofort alle Firewalls und alle. Also ich bin jetzt kein EDV Experte, aber auch aus dem eigenen Bereich. Wenn ich meinen Computer neu aufsetze, weiß ich im kleinen Bereich, dass das eines der letzten Dinge, die ich in Betrieb setzen kann, ist der Virenschutz und die Firewall. Und bis dahin bin ich offen. Und ich muss aber schon ins Internet, um gewisse Daten von dort zu holen wieder. Wir hängen am Netz. Wir haben nicht mehr alles auf einer Festplatte oder auf einer Hard-Copy zu Hause liegen. Wir holen irrsinnig viele Daten aus dem Netz wieder, aus einem funktionierenden Netz. Das heißt, in dieser Phase des Wiederhochfahren eines Systems, das mir ausgefallen ist, bin ich verwundbar, hochverwundbar. Und das kann natürlich jeder Angreifer ausnutzen. Und damit sind alle denkbaren Risiken, die die Versorgung, die Energieversorgung fordern, eine Katastrophe in Wirklichkeit.

A: Das ist auch schon eine sehr gute Überleitung zur nächsten Frage. Es ist ja so, dass sich die österreichische Bundesregierung klar zur Neutralität bekannt hat und auch Hilfslieferungen an die Ukraine sich auf humanitäre Güter beschränken, im Gegensatz zu Deutschland, die sehr wohl auch Waffen in die Ukraine liefern wollen. Es ist nun anzunehmen, dass als Repressalie russische Hacker das Stromnetz oder andere Infrastrukturen in Deutschland versuchen werden, zu hacken und lahmzulegen. Wenn das deutsche Energienetz gehackt werden sollte und lahm liegt, könnte das auch möglicherweise negative Auswirkungen auf andere EU Länder haben. Ein

weitreichender Stromausfall oder Blackout wäre eine mögliche Folge. Wie schätzen Sie die Bedrohung für Österreich durch einen solchen Kollateralschaden ein, wenn beispielsweise Italien oder Deutschland gehackt werden würden?

B: Das ist für Österreich eine Katastrophe, weil die europäischen Netze eigentlich nicht mehr zum Abschotten sind. Also, auch wenn ich kein Sicherheitsexperte bin. Das ist mir in den Schulungen, auf militärischen Schulungen schon klar geworden, dass wir nicht mehr so einfach abzuschotten sind. Wir können keine Energie-Inseln momentan errichten und das heißt, wenn Deutschland katastrophal abstürzt, dann stürzt auch Österreich großflächig ab.

A: Wird mitgerissen.

B: Wird mitgerissen. Und damit ist so ein Hackerangriff, egal wo in Europa er passiert, für Österreich. Österreich kann sich da nicht rausnehmen, egal, wie neutral wir uns erklären, weil wir einfach nicht mehr in der Lage sind, uns so schnell herauszunehmen aus dem europäischen Netz, durch die Zusammenschaltung. Also das europäische Netz ist ein Gesamt-Netz und da nutzt uns die Neutralität nichts. Das ist ein Schlagwort. Was die Energienetze betrifft, ist Neutralität ein Schlagwort, weil wir da so eng aneinander gebunden sind in der Zwischenzeit. Dass dieses Abschotten mehrere Stunden bis (?dargebraucht). Natürlich ist noch möglich, aber das geht nicht, in dem ich sage: "Ich drücke ein Knopf und bin abgeschottet," sondern das heißt gewisse Schaltungen über mehrere Stunden, sicher mehrere Stunden zu machen, dass man etwas isolieren kann und damit sind wir mal ausgefallen und ein komplett abgestürztes Netz wieder aufbauen, das dauert mehrere Tage. Das wissen wir auch. Und damit ist Österreich der absolute Kollateralschaden.

A: Mittlerweile wird ja von mehreren Experten verlautbart, dass mit einem Blackout als Worst-Case-Szenario innerhalb der nächsten fünf Jahre zu rechnen sein wird. Welche Maßnahmen hat Ihre Organisation gesetzt, um ein Blackout Szenario, um darauf vorbereitet zu sein?

B: Keine. Es gibt keine. Also keine über die derzeit bestehenden oder schon seit Jahrzehnten bestehenden hinaus. Wir wissen, also ich bin im (?Stahl) und medizinischen Bereich tätig. Und die (unv.) Organisationen der, sind wir auch tätig. Wir wissen, dass wir Notstromaggregate haben. Wir wissen, diese Notstromaggregate reichen maximal, wenn man sie (unv.) drei Tage, je nach Befüllung. Wir wissen, dass

bei einem großflächigen Stromausfall die Nachlieferung von Betriebsmitteln wahrscheinlich nicht so einfach sein wird, weil auch alle Pumpen elektrisch betrieben sind. Es hat ja auch die einzige Organisation, die Handpumpen hatte, das österreichische Bundesheer, die großflächig abgebaut in den letzten zehn Jahren. Damit haben wir eine Resilienz für maximal drei. Maximal. Wenn alles gut geht, drei Tage Notstrombetrieb, wenn alle. Und mehr ist es nicht. Da ist nichts drüber. Das haben wir schon seit 25 Jahren, seit dem ich im Spital arbeite gibt es diese Vorkehrung. Und darüber hinaus gibt es nichts. Ja, und dass speziell an der Cybersicherheit gearbeitet würde. Ja, es ist für jeden irgendwie schon bewusst. Und es gibt schon immer wieder die Hinweise, dass die externen Sticks und manchmal werden die USB-Ports gesperrt und so weiter. Aber das hier eine große Strategie wäre, sich auf so etwas vorzubereiten. Nein. Also keiner der Bereiche, in der ich tätig bin. Nicht einmal beim Heer. Nicht einmal beim Heer. Ganz im Gegenteil. Also die letzten 15 Jahre muss man sagen, die letzten 15 Jahre haben gezeigt, dass sich auch das Heer seiner Widerstandsfähigkeit beraubt hat.

A: Kommen wir weg von den staatlichen Organisationen, hin zur Bevölkerung. Es ist in mehreren Studien belegt, dass die urbane Bevölkerung die Eigenbevorratung vernachlässigt. Jeder ist mittlerweile gewohnt, wenn er Hunger hat, dass man sich eine Pizza ruft oder in ein Lokal geht. Auf jeden Fall alles sehr knapp und Basissachen wie Wasser, Wärme und Strom können aber durch einen Blackout in Mitleidenschaft gezogen werden. Jetzt ist es so, dass kritische Infrastrukturen auch bei einem Blackout zumindest noch drei Tage lang in Betrieb aufrechterhalten werden können. Sprich, sie haben Wasser, sie haben Wärme, sie haben Strom und sind dann ein Anziehungspunkt für die notleidende Bevölkerung, werden dann aber dadurch, dass sie nicht durch Betreuungseinrichtung ausgerichtet sind, von ihrer Kerntätigkeit abgehalten. Wie sollte Ihrer Meinung nach mit diesem Problem umgegangen werden oder dem begegnet werden?

B: Erstens halte ich das Konzept, wie es derzeit, dass der Staat seit vier Jahren, glaube ich, verfolgt, dass man militärische Einrichtungen zu Sicherheitsinsel umbauen will, für völlig verfehlt, weil ich damit die Leute genau dorthin hole, wo eigentlich das Krisenmanagement laufen sollte. Aber ja, man sollte sogenannte Sicherheitsinseln schaffen. Das ist meine Meinung, wo man eben Versorgung anbieten kann, Basisversorgung anbieten kann, die auch dafür eingerichtet sind, dort auch in einer

gewissen Weise zu funktionieren. Aber das muss abseits der Bereiche geschehen, wo die Kräfte sich sammeln, die Schutz und Hilfe gewährleisten sollen und von wo sie auch geführt werden soll, wo sie auch ein- und ausrücken sollen, dort kann das nicht stattfinden. Das ist ein katastrophaler Fehlschluss, dass man die Leute dorthin ziehen möchte. Aber ja, ich glaube, dass das Konzept Sicherheitsinsel, aber ja nicht bei den Kasernen. Also das ist für mich der größte Denkfehler, den man gemacht hat in dieser Diskussion, dass man derartige Sicherheitsinseln schaffen sollte, weil die Bevölkerung wird man wahrscheinlich aufgrund auch der Kosten, die so eine Bevorratung bedeutet und dieses Umwälzen wird die Bevölkerung das nicht lange machen. Ich mache es ja. Ich habe entsprechende Vorräte für eine Woche. Ich kann eine Woche. Könnten wir überleben. Aber das kostet Geld. Das heißt, man muss den Brennstoff haben. Man muss sich die entsprechenden Heiz- und Koch-Möglichkeiten beschaffen, man muss regelmäßig kontrollieren und austauschen. Die ablaufenden Dauerwaren, auch die laufen ja noch entsprechend der Zeit, drei bis fünf Jahren einmal ab. Das heißt, die kosten durchaus Geld. Und ich glaube, dass die Bevölkerung gerade in Zeiten, wo die Inflation wieder steigt und in Krisenzeiten ist auch die Inflation ein Thema, dass die nicht bereit sind, diese Vorsorge im ausreichenden Ausmaß zu treffen. Und das muss staatliche Krisenvorsorge sein, das muss so sein und die haben wir gröblich vernachlässigt. Also für mich war das klassische Beispiel. Das ist jetzt schon mehrere Jahre zurück. Aber wo man noch nicht gewusst hat, wie sich die Vogelgrippe zum Beispiel auswirken wird. Und die damalige Bundesministerin Maria (?Rochkallert) ist hergegangen und gesagt, okay, sie legt Grippe-Schutzmasken auf Lager und die ist höhnisch verlacht worden dafür. Zehn Jahre später hat man diese Masken gebraucht wie einen Bissen Brot, weil Österreich für die sich durchaus ankündigte Covidkrise überhaupt nicht vorbereitet hat. Man hätte es wissen müssen. Man hätte auch schon Wochen vorher einkaufen können am Weltmarkt und hat es nicht getan. Bis dann die (unv.). Und dann war man froh, dass man doch noch in den Lagern diese Masken hatte, um diese kurze Delle dieser Versorgungfälle ausgleichen zu können. Nur das muss ich bevorraten, das muss ich wohl lagern. Und Gott sei Dank waren die so gelagert, dass 90 Prozent dieser Masken verwendbar waren, auch wenn sie offiziell abgelaufen waren, aber nach einer kurzen Werkstoff-Prüfung hat man festgestellt, dass (unv.), außer die, die feucht geworden sind, weil sie schlecht gelegen sind, aber 90 Prozent waren verwendbar. Man konnte die Delle, die Versorgungsdelle damit zumindest in den kritischen Bereichen abfangen. Und so etwas muss aber staatlich

gewährleistet. Das kostet Geld und alles was Geld kostet. Und damit kehren wir wieder an den Anfang zurück, muss ich gesetzlich vorschreiben, sonst wird es nicht passieren.

A: Wir haben auch schon erwähnt gehabt, die Vernetzung des Energiesektors. Und der ist auch mehrmals im NIS-Gesetz und in der NIS-Verordnung genannt. Auch wenn Sie kein expliziter Profi auf dem Gebiet der NIS-Gesetzgebung sind, wird Ihrer Meinung nach auf wechselseitige Abhängigkeiten von kritischen Infrastrukturen gegenwärtig ausreichend Rücksicht genommen?

B: Nein, sicher nicht, weil gerade auch den Entscheidungsträgern aus meiner Sicht und so wie ich das sehen kann, natürlich eine subjektive Sichtweise, das ist ganz klar, nicht wie aus meinem verschiedenen Blickwinkeln kommt. Aber diese Vernetzung der Infrastruktur ist überhaupt nicht klar. Und beim einleitenden nicht offiziellen Gespräch haben wir schon festgehalten. Jeder von uns, der in diesen Bereichen gearbeitet, ist zumindest dreimal verplant. Und genau das ist aber, dass es uns nicht bewusst ist, wie wir vernetzt sind, weil jeder glaubt, okay, naja, da beruft mal jemanden ein, nur der, der einberufen wird, fehlt im zivilen Bereich. Das heißt, auch das ist bereits ein sich überlegen: "Habe ich genügend Personal für diese Bereiche?" Auch das ist ja Vernetzung. Personal ist ja auch in diesen Krisenfällen essenziell. Und wenn ich mir diese Vernetzung nicht im Klaren bin, was es heißt, jemanden da herauszureißen, um ihn dort hinzusetzen, was das für diesen Bereich der Infrastruktur heißt, habe ich schon eigentlich die Vernetzung nicht verstanden. Und deswegen glaube ich, dass es uns viel zu wenig bewusst ist, wie diese Bereiche der kritischen Infrastruktur nicht nur verkabelt und informationstechnische, sondern auch personell miteinander vernetzt sind und wir uns überhaupt nicht im Klaren sind, was das heißt.

A: Danke. Kommen wir jetzt eher zum medizinischen Versorgungs-Bereich. Ich betrachte die Versorgung von Notfallpatienten als einen Behandlungspfad, der in mehrere Teilprozesse untergliedert ist. Beginnend vom Notruf bis zur finalen Versorgung im Spital und dazwischen eben die notfallmedizinische Versorgung durch den Rettungsdienst. Wie beurteilen Sie den Begriff Autarkie im Rahmen vernetzt- und systemübergreifender Prozessketten? Wenn jeder Bereich, also der Rettungsdienst, Telekom Betreiber und Spitäler für sich autark sind. Dass dennoch ein Zusammenwirken der einzelnen Bereiche oder Prozesse dann funktioniert.

B: Na ja, ich muss krisensichere Schnittstellen oder Nahtstellen eigentlich definieren. Das heißt, ich muss sagen, wie weit kann ein Bereich versorgen und ab wann, wie sie auf den nächsten Bereich angewiesen. Und ich muss natürlich auch festlegen, wenn die normale Kommunikation ausfällt, auf welcher Ebene findet Kommunikation zwischen diesen Ebenen statt. Und ich glaube, dass wir da derzeit ganz schlecht aufgestellt sind, weil wir uns momentan auf ein System stützen, das unheimlich viel EDV-Unterstützung braucht. Das ganze BOS-System lebt davon, dass die Infrastruktur steht. Wenn diese Infrastruktur fällt, haben wir aus meiner Sicht keine Kommunikationsmöglichkeit mehr, gerade in den notfallmedizinischen Bereichen mehr zwischen den einzelnen Versorgungsebenen. Und wenn wir gerade vom ersten Bereich der Notfallmedizin, vom Rettungsdienst sehen, dann glaube ich, dass wir auch rettungsdienstlich in Wien schlecht aufgestellt sind. Weil wenn das BOS-System ausfällt, dann haben wir das Handysystem. Das ist nichts anderes, das stützt sich genau auf dieselbe Technik. Und wir wissen, dass die Handymasten nicht lange leben und dann sind wir ausgefallen. Analog haben wir kein wirklich, aus meiner Sicht kein wirklich krisensicheres System mehr im Hintergrund laufen, auf das wir zurückgreifen können, das wir aus dem Kasten nehmen können und sagen: "Okay, das ist jetzt nicht optimal, aber es funktioniert, dass wir eine Basis-Kommunikationsstruktur." Und das heißt, der funktioniert innerhalb des Rettungsdienstes in Wien schon nicht, weil wir rettungsdienstlich ja in Wien auch nicht mehr allein sind. Die Berufsrettung ist ja schon angewiesen in der Zwischenzeit und da funktioniert es dann überhaupt nicht mehr diese Abstimmung und schon gar nicht die Abstimmung mehr zu den Spitälern hinein und übergreifend aus den Spitälern heraus funktioniert es auch nicht mehr, weil die Kommunikation mit der Generaldirektion, die dann ja eigentlich die Koordination nach oben führen sollte, auch abreißt. Und ich glaube, dass wir da derzeit zwar innerhalb der einzelnen kleinen Einrichtungen arbeiten, also hinziehen kann, sich sicher für eine Zeit lang abschotten und intern funktionieren. Dann bin ich überzeugt. Das Spital, wo ich bin. Aber nach außen geht nichts mehr, da bricht alles weg. Also wenn die Begleitungen weg sind, ist alles weg. Und ich glaube, die Rettung bricht überhaupt zusammen. Also das (unv.) ich jetzt einmal komplett. Wir haben kein, also ich hätte keinen. Es gibt ja das berühmte Landesgrundgesetz. Aber hängen die Notarztstützpunkte im Landesgrundgesetz. Nein. Wir haben keinen Apparat, wo wir sagen: "Da hängt der Apparat, dass ich zumindest von dort eine Verbindung über das Landesgrundgesetz, das doch noch steht, erreichen kann." Gibt es nicht. Und ich weiß

auch, dass das Landesgrundnetz in der Zwischenzeit auch sehr anfällig ist. Weil man hat es jahrelang in den Kanälen verlegt. Ein bisschen Wissen habe ich schon. Jetzt verlegt man es oben auf den Oberleitungen. Also wir wissen, wenn dort die Bomben hochgeht, dann reißt es das Landesgrundnetz. Und damit ist auch das Landesgrundnetz nicht mehr resilient. Solange. Ich meine natürlich ist dort kanalanfällig, aber da unten passiert weniger, als wenn ich es oben, also (unv.) der Hauptstraße. Weiß ich, dass es oben läuft. Ja, das ist mir bekannt. Damit haben wir kein wirklich resilientes Kommunikationssystem, dass dann diese autarken Körper wieder zusammenschließt. Und die Rettung, das ist jeder Rettungswagen dann eine kleine Einheit. Und sind die Leute darauf geschult, dass sie als Einheit klein funktionieren können, wenn die Kommunikation abreißt?

A: Eher nein.

B: Wir haben überhaupt nicht einmal gedanklich das in irgendeiner Schulung drinnen. Wie reagiere ich, wenn wir überhaupt keinen Kontakt mehr haben? Wo hole ich mir die Information? Früher war es so, wie man keinen Funk gehabt haben in den 50er Jahren, war klar, man holt sich die Informationen vom nächsten Polizei-Wachzimmer. Ist hier eine Vernetzung? Ich weiß nicht genau, wo ich was für eine Verbindungs-Resilienz die einzelnen Polizeiinspektion haben, aber wenn die eine hätten, ist hier eine Absprache getroffen, dass wenn uns unser gesamtes Informationsnetz zusammenbricht. Dass wir dort Information kriegen, sind die Leute. Ich weiß, dass theoretisch unsere Funkgeräte auch analog funken können. Ich weiß aber nicht genau, wie ich auf das Analoge komme und wie das dann, wie dieses Umsteigen auf Analog-Funk funktioniert, hat uns noch keiner gezeigt. Ich weiß nur, dass sie es können. Also da haben wir schon im Rettungsdienst ein dramatisches Problem, aber darauf weise ich auch schon hin, seit ich dabei bin. Ja, jetzt bin ich nicht mehr dabei, jetzt weise ich nicht mehr darauf hin. Ja, jetzt ist es mir wurscht. Aber wie ich noch Personalvertreter war, habe ich auf das mal vorsichtig. Ich wollte mir nicht zwischen alle immer Stühle setzen können. Ich war immer das Böse da wie in der Rettung. Aber auch auf das habe ich vorsichtig hingewiesen, dass wir hier ganz schlecht aufgestellt sind und wie wir sie ausgelagert haben, die Notarztstützpunkte in Spitäler, habe ich auch darauf hingewiesen, dass diese Resilienz der Krisenverbindung eigentlich nicht steht, nicht funktioniert, weil man hätte es auch lösen können. Man sagt okay, es gibt einen Ansprechpartner in der Direktion des Spitals, aber dann muss der auch wissen, dass dort eine Alarmierung

hinkommen könnte. Das muss man auch spielen, die ja dann intern an den Rettungsstützpunkt weitergeben muss oder sage, ich stelle den Notarzt-Rettungsdienst in so einer Krisensituation überhaupt ein, weil das dann, eigentlich brauche dann die Leute, das medizinische Personal im Spital wahrscheinlich mehr und was würden sie draußen machen können, wenn sie abgeschnitten sind? Aber auch das muss ich durchdenken, dass ich sage, okay, ab einer gewissen Ebene der Krise stelle ich den Notarzt-Rettungsdienst ein. Dann gibt es diese Ebene nicht mehr oder nur mehr in ganz eingeschränkten Ausmaß. Auch nicht durchgedacht. Also ich glaube, dass wir da sehr viel eigentlich hätten zum Diskutieren und zum Planen, wenn wir das alles ernst nehmen würden, wo wir uns überhaupt nicht Gedanken gemacht haben noch.

A: Es ist in gewisser Weise eine gute Überleitung zum nächsten. Es ist ja so, dass die Berufsrettung Wien mit den Partnerorganisationen etwa 800 Notfallpatienten am Tag versorgt und dann zu einer weiteren Behandlung in Krankenanstalten transportiert. Zusätzlich kommen mehrere, etwa 1000 Patientinnen und Patienten als Selbsteinweiser oder mit Krankentransport-Organisationen zur ambulanten Nahversorgung. Die vorhandenen Kapazitäten sind und Strukturen in den Krankenanstalten sind natürlich auf einen Normalbetrieb ausgelegt und nicht auf ein permanentes Krisenszenario. Welche Maßnahmen achten Sie als sinnvoll, damit eine medizinische Basisversorgung eines Großteils der Bevölkerung auch unter den negativen Auswirkungen eines Cybernotfalls oder eines Blackouts sichergestellt werden können?

B: Das ist schwer zu beantworten. Also das habe ich schon bei der Beantwortung der letzten Fragen gestellt. Man wird relativ bald einmal sich überlegen müssen, ab wann ich eine gewisse rettungsdienstliche Versorgungsebene nicht mehr biete, weil ich das Personal in den Spitälern brauche. Das ist das Erste oder auf (unv.) Versorgungsstützpunkten lokalisiert brauche. Weil das darf man auch nicht vergessen, wenn so ein Blackout beginnt, beginnt auch ein Sicherheitsrisiko. Das heißt es bedienen sich dann gewisse, eine Zeitlang wird es so funktionieren und dann beginnt es, beginnen sich gewisse marodierende. Ich sage es einmal mit diesem Begriff, Strukturen zu bilden. Und dann wird man wahrscheinlich nicht mehr überall sich so gut und frei bewegen können.

A: Die Polizei spricht dann mehr oder minder offiziell von etwa 72 Stunden, wo dann die Sicherheitslage sich massiv verschärfen könnte.

B: Ja, da geht man auch beim Heer davon aus, dass wir sagen, drei Tage wird es halten und dann muss man. Und dann habe ich aber mehrere Probleme, dann habe ich das Problem, dass ich nicht mehr alle Sicherheitskräfte in den Dienst bekommen werde, weil die auch Familie zu Hause haben, die sie schützen werden und wollen, weil die auch von Informationen abgeschnitten sind. Das heißt, ich muss schon einmal, ich sehe es einmal vorsichtig mit 25 Prozent Ausfall des routinemäßigen Sicherheitspersonal, rechnen auf allen Ebenen, die nicht mehr zur Verfügung stehen werden, aus verschiedensten Gründen. Und dann wird auch die Bewegungsfähigkeit gerade für das medizinische Versorgung-Personal in der Stadt deutlich eingeschränkt. Dann muss ich natürlich auch bei den Wiener Spitälern wie so eine Vogelhäuser, weil wir alte Spitalstrukturen haben, Pavillonsstrukturen haben, die schwer nach außen zu sichern sind. Und Spitäler, weil das weiß die Bevölkerung, sind aber Orte, wo es was gibt. Und ich kann dir aber nach außen schwer schützen. Beziehungsweise ich muss jetzt relativ viel Personal, das ich vielleicht in der Fläche brauchen würde, zum Schutz dieser Strukturen abstellen. Das wird schwierig.

A: Das geht sich irgendwie nicht aus.

B: Und also wir haben es trainiert. Nicht für Spitäler. Aber wir haben ja vor, wieder sechs Jahre jetzt her, wo wir in Wien trainiert haben, den Schutz des ORF, wo sie gezeigt haben, wie schnell der ORF eigentlich zu stürmen ist, wie unsicher der ist und wie viele Kräfte ich brauche. Dass eine Kompanie fast nicht ausreicht, um den ORF rund um die Uhr zu schützen. Auch wenn ich sie vollauf fülle und alles abdecke, nicht ausreicht, um den zu schützen, wenn dort jemand sich Zutritt verschaffen will. Jetzt habe ich die Spitäler zum Schützen, weil dort gibt es.

A: Das sind mehrere in Wien.

B: Und das heißt, ich spiele eigentlich meine Sicherheitskräfte schon für diesen Schutz dieser Infrastrukturen auf, die aber gar nicht voll einsatzfähig sind. Das heißt, ich muss damit rechnen, dass ich mich nicht mehr so bewegen kann. Das heißt, wie bewege ich mich dann in der Stadt weiter? Sind wir darauf trainiert, unter diesen Sicherheitsrisiken uns fortzubewegen, wo ich unter Umständen dann schon das Personal entsprechend ausrüsten muss, weil sie unter Umständen angegriffen werden? Und kann ich es mir

dann leisten, meine Ärzte und mein hochwertigstes Personal hinauszuspielen, die dann dort angegriffen werden? Es ist genauso wenn ich. Warum haben die Amerikaner in den ersten Linien draußen, gerade im militärischen Bereich keine Ärzte? Aus der Erfahrung, dass sie zu wertvoll draußen sind, um ausfallen zu können. Die schicken selbst ihre Medics nicht bis ganz nach vorne, sondern ihre Combat Life-Saver. Denen sind schon die Medics zu wertvoll draußen, sondern die schicken ganz vorne mit ihren Leuten die Combat Life-Saver mit, die ein, zwei höher ausgebildete Soldaten, die diese Erstversorgung machen und dann erst kommt der Medic dazu und relativ weit hinten das hoch-. Das heißt und das jetzt wieder herunterzubrechen auf Zivile. Ich muss mir überlegen, welche Versorgungsebenen kann ich, wo anbieten. Und wie kann ich mich bewegen. Und wahrscheinlich wird man sich nicht mehr viel bewegen können, sondern wird stationäre Versorgungsbereiche schaffen müssen. Und die muss ich dann materiell und personell ausstatten. Und die sind wir auch nicht in der Lage, materiell und personell auszustatten. Wir haben nichts vorgesorgt, weil das muss ich schon ausgelagert, wo vorbereitet haben, wenn ich beginne, Transporte dann von irgendwo hinzuschicken. Also ich muss wissen, dass ich und das könnte man in Wien machen, dass ich im Rathaus so einen Versorgungsstützpunkt mache zum Beispiel oder in den Bezirksämtern so einen Versorgungstützpunkt plane, wo ich schon Räume definiere. Dort wird ein Versorgungsstützpunkt sein, dort können sich die, und von dort kann ich einen geschützten Transport zum Beispiel ins Spital machen, einen geschützten, durch Personal geschützten Transport mit mir ein Fahrzeug ins Spital machen, aber das müsste man vorbereiten und das kostet wieder Geld. Und das muss ich auch trainieren, dass ich sage, okay. Außer in meinen, allen magistratischen Bezirksämtern ist ein ausgelagerter Versorgungstützpunkt, wenn wir einen Blackout haben, wenn die Sicherheitslage nicht mehr entsprechend ist. Der ist unten im Keller geschützt eingerichtet. Dort habe ich auch entsprechendes erstes Basismaterial, wo ich anfangen kann zu versorgen. Dort ist auch das Personal bereits eingewiesen, zugeordnet und das könnte man auch machen. Und so schauen dann die Transporte aus in die Spitäler hinein. Das ist ein Gedankenspiel jetzt, wie ich mir so etwas. Aber wenn man sagt, 72 Stunden kann ich eine Sicherheit aufrechterhalten. Und dann beginnt das Marodieren. Dann muss ich mir überlegen. Was passiert dann. Dann kann ich mein medizinisches Personal nicht mehr so quer durch die Stadt schicken. Und wie schwierig das werden kann, hat ja schon der 2. November 20 gezeigt, wo wir in die Stadt nicht mehr hineingekommen sind, dann ab einem gewissen und dieses Personal,

das dort hinein gespielt war, eigentlich sich nicht mehr bewegen konnte in Wirklichkeit. Und da haben wir dann das Glück gehabt, dass die Polizei das aber relativ rasch eingegrenzt hat, relativ rasch. Wenn das nicht eingrenzbar gewesen wäre, dann wären wir bewegungsunfähig gewesen und dann hätten wir bereits anfangen müssen, Versorgungsbereiche zu schaffen, wo man nicht wegkommt und das, was mich ein bisschen immer, wenn ich dann wieder mal durchdenke und mir sage: "Mir ist es Wurscht, weil ich bin dafür nicht zuständig." Um das ist jetzt ein bisschen historisch zu sagen. Der alte Kaiser Franz Joseph hätte gesagt: "Sind Sie dafür zuständig? Nein. Warum machen Sie sich dann Gedanken darüber?" Aber wenn ich mir Gedanken mache und als (unv.), mache ich mir schon gewisse Gedanken darüber. Dann stelle fest, dass wir da ganz schlecht aufgestellt sind, dass da überhaupt keine Planungsgrößen getroffen wurden und dass wir auch auf den Blackout, was die medizinische Versorgung betrifft, nicht vorbereitet sind. Auch dahingehend nicht, was passiert, wenn die Ding aus, wenn die aufgebraucht sind, die Notstromaggregate. Wo kriegen die Spitäler noch Betriebsmittel her? Wo haben sie Reserven? Wo haben wir Reserve-Einheiten?

A: Und dafür gibt es ja ein übergeordnetes Konzept von der Stadt.

B: Ja. Übergeordnetes Konzept von der Stadt. Funktioniert das auch ohne Strom? Ich weiß es nicht. Ja, ich glaube nicht. So wie ich die Stadt kenne, funktioniert es nicht ohne Strom. Bin ich überzeugt davon. Aber da muss man ganz und ich glaube, dass wir da überhaupt. Also ich bin überzeugt, wir sind, was das betrifft, überhaupt nicht aufgestellt. Und wenn man das dann auf die kleine Einheit herunterbricht, auf die wirkliche operative Versorgungsebene herunterbricht, das schaffen wir nicht.

A: Gut. Danke Herr Professor, für die kritischen Anmerkungen und zahlreichen Denkanstöße. Und ich wünsche noch viel Erfolg für die Zukunft, bis wir uns das nächste Mal über den Weg laufen.

Interview mit Herrn Chefarzt Dr. Krammel am 14.04.2022

A: Donnerstag, 14. April 2022, Interview mit Chefarzt Dr. Krammel. Erste Frage, die europäische Richtlinie des Europäischen Parlaments wurde mit dem Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus vom Netz- und Informationssystemen, kurz NIS-Gesetz, in Österreich umgesetzt. Bereits zuvor existierten Konzepte bei denen verschiedene kritische Infrastrukturen um ein hohes Schutzniveau vorzuweisen, wie ordnen Sie die Notwendigkeit für eine gesetzliche Regulierung zur Einhaltung von IKT-Sicherheitsstandards ein, zumal von vielen Kritis ein Informationssicherheitsmanagementsystem implementiert wurde und betrieben wird.

B: Also ich bin hier nicht der Experte auf diesem Gebiet, denke aber, wenn es gesetzliche Regulierungen gibt, die einheitlich in Österreich bzw. in der EU gelten, so kann das nur gut sein. Um einfach hier die Qualität und die Sicherheit weiter auszubauen und zu fördern.

A: Danke vielmals. Worin liegt Ihrer Meinung nach dann der konkrete Mehrwert für die Gesellschaft durch diese bundesgesetzliche Regelung?

B: Wie eingangs angesprochen, Standards sind gut, aber Standards sind dann oft doch nicht verpflichtend, Standards erlegt man sich selbst auf und wenn man möchte, dass gerade eine kritische Infrastruktur wirklich so abgesichert ist, vernünftig abgesichert ist, dann macht das schon Sinn, bundesweit einheitliche Regelungen, in dem Fall in Form einer Gesetzgebung einzuziehen, um hier wirklich auch jene, die hier nicht die Vorreiter sind, es wird welche geben, die sich selbst Standards auferlegen, die selbst hier wirklich aktiv Arbeit hineinstecken, um die Sicherheitsstandards voranzutreiben, aber ich denke, wenn es eine gesetzliche Regelung gibt, dann hat man einen einheitlichen Mindeststandard. Darüber hinaus kann man ja immer mehr machen, aber es gibt sozusagen gesetzlich verankert dann, bundesweit einen Standard, der mit Gesetz eingezogen ist. Und ich glaube, dass das doch ein Mehrwert, vor allem für kritische Infrastruktursysteme darstellt.

A: Danke. Dann gleich zur nächsten Frage, der Nr. 2. Schutzkritische Infrastruktur inkl. Cybersicherheit ist in Österreich grundsätzlich im österreichischen Programm zum Schutz kritischer Infrastruktur seit 2008 beschrieben. Diese Strategie zählt bereits eine Vielzahl an Infrastrukturen mitsamt deren Systemen, Anlagen, Netzwerken usw. auf,

welche als das für das gesellschaftliche Gefüge erachtet werden, zusätzlich wurde im Jahr 2013 die österreichische Strategie für Cybersicherheit veröffentlicht. Beide Sicherheitsstrategien wurden inzwischen erneuert. Abcyb eben 2014 und die Cybersicherheitsstrategie zuletzt 2021. Weiters wurden von der Internationalen Organisation für Normung ISO, mehrere Standards veröffentlicht, die die Sicherheit von Organisationen erhöhen sollen. Nun zu meiner Frage, welche Bedeutung messen Sie diesen beiden Strategien und Normen im Vergleich zum NIS-Gesetz bei?

B: Ja, das ist so, wie wenn ich Sie fragen würde, wie vergleichen Sie die Egmo-Therapie mit der Maß-Therapie, also da bin ich sicherlich der falsche Ansprechpartner. Muss ich Sie bitten, dass wir einfach zur nächsten Frage weitergehen. Da kann ich, glaube ich, nicht wirklich vernünftig dazu beitragen.

A: Gut, danke vielmals. Die nächste Frage, Organisationen sind einem breiten Spektrum von Bedrohungen ausgesetzt. Sicherheits- und Risikomanagement stellen per se Querschnittsmaterien dar, um Gefahrenpotenziale möglichst vollständig zu identifizieren und zu analysieren. Das Regime der NIS-Richtlinie befasst sich folglich nicht ausschließlich mit Beeinträchtigungen von Netz- und Informationssysteme durch Cyberangriffe. Auch technische Gebrechen und Naturgefahren, die zu Störungen oder gar Ausfällen führen können, sind von der NIS-Richtlinie erfasst. Risikomanagement findet sich am Anfang von 11 Punkten betreffend Sicherheitsmaßnahmen, laut NIS-Verordnung. Welche Risikoszenarien für kritische Infrastrukturen kommen Ihnen in den Sinn und welche betrachten Sie aktuell als vorrangig?

B: Also es ist sicherlich ganz greifbar, wäre z.B. wenn die Rettungsleitstelle, als kritische Infrastruktur heranziehe, der Brandalarm, der Räumungsalarm aufgrund einer Bombendrohung z.B., wäre aber auch ganz einfach Bauarbeiten vorm Haus und es werden hier Kabel durchtrennt. Es wird hier die Datenleitungen, es wird hier die Stromzufuhr aufgrund eines technischen Gebrechens im Rahmen von Bauarbeiten zerstört. Etwas abstrakter, vielleicht nicht ganz so greifbar, oder nicht ganz so realistisch, oder nicht ganz so präsent ist, wenn man an Naturkatastrophen denkt, wenn man an Erdbeben denkt, wenn man an andere Naturgewalten denkt. Für uns bis jetzt noch weniger greifbar, aber doch, wenn man an den November 2020 denkt, Terrorangriffe. Auch hier könnte, gerade der Rettungsdienst doch auch ein Ziel darstellen. Nicht nur auf der Straße, sondern auch wenn ich jetzt zentral die Rettungsleitstelle ausschalte, wäre das doch ein enormer Schaden für die Stadt, für

die Infrastruktur, für die medizinische Versorgung der (unv.), wenn hier die Leitstelle ausgeschalten werden würde. Genauso in diese Richtung, in Richtung Cyberkriminalität, auch hier, es muss ja nicht nur die physische Zerstörung vor Ort sein, es kann ja auch sein, dass hier über Cyberangriffe das Netzwerk lahmgelegt wird. Das ist für uns vielleicht nicht ganz greifbar, aber glaube ich auch das ist durchaus, wie wir mittlerweile wissen, kann es durchaus sehr schnell zur Realität werden. Bzw. auch das Thema Blackout, wir reden ja alle schon lange darüber und auch über die Pandemie haben wir lange gesprochen und keiner hat sich vorstellen können, dass das dann wirklich morgen dann tatsächlich Wirklichkeit wird. Also auch mit diesem Thema beschäftigen wir uns lange und ich glaube, irgendwann wird es uns auch treffen. D.h. auch das sehe ich durchaus als realistische Sache, mit dem wir rechnen müssen.

A: Und Sie sind auch der Überzeugung, Sie haben ja jetzt ein sehr breites Feld auch genannt, mit sehr unterschiedlichen Bedrohungen, also es gibt ja nicht eine spezifische, die nur kritische Infrastrukturen betrifft, sondern eben durch Naturkatastrophen auf der einen Seite, das kann reichen von Erdbeben übers Hochwasser bis sonst irgendetwas, bishin eben zu intentionalen Gefahren, wie ein Terrorangriff, wo die kritische Infrastruktur auch das Ziel sein kann. Gut, danke. Auch die Cyberkriminalität wurde angesprochen und das führt dann zur nächsten Frage, neben kriminellen, sind auch staatliche Akteure im Cyberraum als Hacker aktiv, moderne militärische Konfliktszenarien sind durch eine hybride Kriegsführung geprägt. Ich kürze das ein bisschen ab und gehe gleich auf die konkrete Frage, wie schätzen Sie die Bedrohung für Österreich durch einen solchen Kollateralschaden, gemeint ist damit, Deutschland oder ein anderes EU-Mitgliedsland, dessen kritische Infrastruktur angegriffen wird, wirkt sich dann, hat einen Blackout zur Folge dann, der sich wiederum auf Österreich auswirkt?

B: Also wenn es jetzt zu einem Blackout kommt in Deutschland und dort Systeme dann nicht mehr verfügbar sind, Sie meinen das Stromsystem bei uns würde noch funktionieren, die Stromversorgung, oder?

A: Oder meinen Sie auch, dass wenn es einen erheblichen Vorfall in Deutschland gibt, oder in Italien, oder Ungarn beispielsweise, eben in einem unserer Nachbarländer, dass sich das sehr wohl auch auf Österreich direkt oder indirekt auswirken würde?

B: Das glaube ich schon, weil wir ja von Computersystemen auch abhängig sind, von unseren Partnerländern, jetzt nicht direkt in der Rettungsleitstelle, aber wenn ich jetzt Wien hernehme, gibt es sicherlich auch Bereiche der Öffentlichkeit, oder kritische Infrastruktur, die abhängig von anderen Systemen ist, die eben in Deutschland oder anderen Ländern betrieben werden, oder Systempartner, die hier Wartungen vornehmen, die hier Fehlerbehebungen vornehmen und wenn das dann nicht mehr durchgeführt werden kann, hat das natürlich dann indirekt auch Einfluss auf Österreich und auf die kritische Infrastruktur in Österreich.

A: Als Blackout wird ein überregionales, mehrere Tage andauerndes Strommangel oder Stromausfall betrachtet. Und das hat natürlich eine erhebliche Bedrohung für das gesellschaftliche Gefüge, da alle Bereiche ja mittlerweile von Strom abhängen. So ein Szenario wird von ExpertInnen innerhalb der nächsten 5 Jahre erwartet, es wird auch als Worst-Case Szenario und als Belastungstest für das Kontinuitätsmanagement herangezogen. Krisen- bzw. Katastrophenpläne sind ja für Kritis immer schon da, daher jetzt die Fragen, welche Maßnahmen hat Ihre Organisation, also die Berufsrettung Wien gesetzt, um ein Blackoutszenario, um darauf vorbereitet zu sein.

B: Ja, die Frage müsste ich fast an Sie zurückgeben, Sie sind ja Hr. Mag. Pon sind ja der Mann in dieser Geschichte für die Berufsrettung, also es gibt einen breiten Maßnahmenkatalog, ich selbst darf mich hier einbringen, haben wir schon gesprochen, was machen wir im Bezug auf die medizinische Triage, was jetzt mein Fachgebiet wäre, wie schaffen wir es, wenn jetzt im Rahmen des Blackouts weiterhin, wir haben etwa 1000 Rettungseinsätze pro Tag, die wir bespielen müssen, wenn es hier zu einem Blackout kommt, die Krankenhausaufnahmekapazität dann nicht mehr für, oder die Behandlungskapazität nicht mehr für 1000 Patienten, die aus dem Rettungsdienst neu ins Krankenhaus kommen reicht, müssen wir quasi bereits beim Eingang des Notrufes die medizinische Vortriage vornehmen und das sehe ich als meine Aufgabe, mich hier gemeinsam mit Ihnen einzubringen. Das wird also in den nächsten Monaten erarbeitet und abgesehen davon gibt es eine Vielzahl von Maßnahmen, einen gesamten Maßnahmenkatalog, der die Berufsrettung in den einzelnen Bereichen auf so ein Blackoutszenario vorbereiten soll.

A: Ist Ihnen bekannt, oder wie schätzen Sie es ein, dass da auch auf andere Interessensgruppen Rücksicht genommen wird. Wie weit wird das denn berücksichtigt?

B: Wie meinen Sie das?

A: Ja einerseits, eben Spitäler auf der einen Seite als Anschlusspunkt für die präklinische Notfallversorgung über andere Einsatzorganisationen, die in einer gewissen Abhängigkeit zu uns stehen, dadurch dass sie von der Rettungsleitstelle disponiert werden.

B: Also das betrifft ja nicht nur die Berufsrettung Wien, sondern wir haben in Wien den Rettungsverbund, mittlerweile 6 Rettungsorganisationen, die für uns tätig sind, vor allem im Bereich der niederpriorisierten Einsätze, der Krankentransport abgewickelt ist, die Frage ist, inwieweit der Krankentransport dann noch aufrecht erhalten bleiben kann, muss man sicherlich priorisieren, welche Transporte sind unbedingt notwendig, welche Transporte könnte man aussetzen und natürlich, wenn unser Dispostionssystem nicht mehr funktioniert, muss ich mir auch überlegen, wie bekomme ich die Information des Einsatzes überhaupt zum jeweiligen Fahrzeug, wie dokumentiert dieses Fahrzeug, also es sind natürlich auch alle Systempartner betroffen der anderen Rettungsorganisationen. Natürlich, wenn die Präklinik betroffen ist, ist immer auch die Anschlussversorgung im Krankenhaus betroffen, deswegen vorhin auch angesprochen, die sogenannte medizinische Vortriage, so ähnlich wie wir es ja bei Covid bereits hatten, wo wir einen Oberarzt in der Rettungsleitstelle hatten, der eine medizinische Vortriage vorgenommen hatte. D.h. jeder Patient, der hospitalisiert werden sollte, mit Verdacht auf Covid, hat das nur in Rücksprache mit dem diensthabenden Oberarzt in der Leitstelle stattgefunden, um wirklich die Krankenhäuser zu entlasten. Und ähnlich sehe ich es, wenn wir mit einem Blackoutszenario, dass über mehrere Tage anhält, konfrontiert sind, dass wir eine Vortriage vornehmen müssen, um eben auch die anschlusskritische Infrastruktur, in dem Fall die zentralen Notaufnahmen, die Krankenhäuser, die wir beliefern, hier wirklich schützen und schauen, welcher Patient braucht jetzt wirklich das Krankenhaus und wir hier eine Triage vornehmen, um hier nicht die Krankenhäuser zu überfluten und hier das Problem, wie wir es im (unv.) kennen, es bringt nichts, wenn ich alle gleichzeitig einpacke und in ein Krankenhaus bringen und die Katastrophe von der Straße ins Krankenhaus verlege. Und dann das gesamt Ziel soll ja sein, die Notallmedizinische Versorgung in Wien aufrecht zu erhalten und hier müssen die einzelnen Bereiche, Präklinik und Klinik eng miteinander zusammenarbeiten, hier

müssen wir uns abstimmen und ich glaube, ein wichtiger Punkt, wie gesagt, den haben wir vorher eingangs angesprochen.

A: Jetzt ein anderes Thema, bis zu einem gewissen Grad die urbane Bevölkerung, die vernachlässigte Eigenbevorratung im urbanen Raum, wird durch mehrere Studien belegt. Aus diesem Grund muss bei einem Blackout Ereignis davon ausgegangen werden, dass die Wiener Bevölkerung mangels Eigenbevorratung spätestens nach einigen Tagen jene Objekte aufsuchen wird, die weiterhin eine gewisse rudimentäre Versorgung mit Wasser, Wärme und Strom bewerkstelligen können. Das sind natürlich Organisationen, die kritische Infrastruktur darstellen und die sind für gewöhnlich nicht als Betreuungseinrichtung für Betroffene eingerichtet. Wie soll Ihrer Meinung nach diesem Problem begegnet werden, dass eine kritische Infrastruktur zwar sich selbst versorgen kann, aber dann wahrscheinlich auch Anlaufpunkt für viele Hilfesuchende oder hungrige Menschen sein wird.

B: Also ich glaube, wichtig ist einmal Aufklärungsarbeit. Die Helfer Wiens leisten hier einen wertvollen Beitrag zur Aufklärung der Bevölkerung, die Helfer Wiens, aus dem Wiener Zivilschutzverband herausgegangen der Verein der Helfer Wiens, der jetzt bei der MA68 angegliedert ist, die eine wichtige Rolle spielen um die Bevölkerung eben auch aufzuklären, ausreichend Wasser, ausreichend Nahrung, bis hin zu Batterien, Taschenlampen, Kerze, all das zu bevorraten, was ich brauche um mich selbst für ein bis zwei Wochen versorgen zu können. Einerseits das als wichtige Maßnahme, die Bevölkerung aufzuklären. Auf der anderen Seite wichtig die kritische Infrastruktur zu schützen, denn wenn es, wie Sie angesprochen haben, zu einem mehr Tage dauernden, oder mehrere Wochen dauernden Blackout kommt, wo die Leute dann vielleicht nichts zu essen haben, nicht heizen können, kein Warmwasser, kein Wasser haben und innerhalb der kritischen Infrastruktur würde das noch funktionieren, dann gilt es diese Objekte besonders zu schützen, denn wenn jetzt quasi halb Wien in dieses Gebäude möchte, wo im Prinzip der Krisenstab sitzt, wo die Rettungsleitstelle versucht, den Rettungsdienst in Wien, die klinische Versorgung versucht aufrecht zu erhalten, zu triagieren, dann muss ich dieses Gebäude oder jene Gebäude, dasselbe wäre ja auch bei der Feuerwehr oder bei der Polizei, beim städtischen Krisenstab, muss ich diese Objekte besonders schützen, denn wenn diese Objekte fallen, würde im Prinzip dann auch die restliche Versorgung komplett zusammenbrechen. Und ich glaube das sind zwei Dinge, einerseits Aufklärungsarbeit, dann muss ich die kritische

Infrastruktur schützen und man könnte sich auch überlegen, was mache ich, errichte ich, ähnlich wie wir es jetzt in der Sport und Fun Halle haben, wo ukrainische Flüchtlinge ankommen, richte ich Zentren ein für die Wiener Bevölkerung, wo ich sagen kann, wenn ich mich zu Hause nicht mehr versorgen kann, dann bitte wende dich dorthin, um eben nicht das Problem von der Straße an der Begehrlichkeit zu Objekten hin der kritischen Infrastruktur zu richten, ob ich schaue, dass ich sage, ich richte Sammelzentren ein, wo ich jene Bevölkerung hinschicke, die sich eben nicht mehr selbst zu Hause versorgen kann. Ich glaube, das muss man sich innerhalb der Stadt überlegen, ob das eine Möglichkeit sein kann, aber es gehört abgeklärt. Kritische Infrastruktur gehört geschützt und dann muss man sich überlegen, was mache ich, wenn dann dennoch weitere dastehen, die jetzt eine besondere Betreuung brauchen, wo ich hier z.B. Zentren einrichten kann.

A: Dankesehr. Jetzt ein kurzer Themenwechsel, hin zur Energieversorgung, mittlerweile hängen ja sämtliche moderne System am elektrischen Strom dran, die Vernetzung des Stromsektors ist allgemein bekannt und auch vollkommen klar. Wie meinen Sie, ist die wechselseitige Abhängigkeit von kritischen Infrastrukturen untereinander in der NIS-Gesetzgebung berücksichtigt?

B: Auch das ist eine gute Frage, die ich Ihnen so nicht beantworten kann, das ist halt nicht mein Schwerpunktthema, mit ist das NIS-Gesetz natürlich ein Begriff, aber so im Detail kann ich Ihnen die Frage leider nicht beantworten.

A: Gut, dann eine die sich mehr mit der medizinischen Behandlung von Erkrankten und Verletzten befasst. Nämlich, die Versorgung von Notfallpatienten kann ja als eine ineinandergreifende Kette eines gesamten Pfades angesehen werden, dieser Pfad beginnt mit der ersten Hilfeleistung durch Laien, beinhaltet auch eine Notrufmeldung, führt dann zur qualifizierten ersten Hilfe durch den Rettungsdienst und schlußendlich hin zu einer fachmedizinischen Versorgung, die Diagnose im Krankenhaus. Wie beurteilen Sie den Begriff „Autarkie“ im Rahmen vernetzter und systemübergreifender Prozessketten eben anhand dieses Beispiels? Wenn jetzt nur der Rettungsdienst autark wäre oder eben nur das Krankenhaus, aber eben andere Komponenten nicht.

B: Ich weiß momentan noch nicht ganz, worauf Sie im Detail jetzt hinaus wollen?

A: Es geht darum, wenn ich für mich schaue, dass ich handlungs- und überlebensfähig bin und diesen Blick nur nach innen gerichtet habe, was brauche ich alles, damit ich

handlungsfähig bin, geht dann der Blick soweit, oder mein Horizont so weit, dass ich auch irgendwann überlegen muss, wo ist denn der Anschluss, oder reicht es, wenn ich autark bin, muss ja automatisch alles andere auch damit berücksichtigt werden.

B: Ja, das wäre das Beispiel, dass ich vorhin angesprochen habe. Es bringt mir nichts, die Katastrophe von der Präklinik, von der Straße, jetzt ins Krankenhaus zu verlagern und zu sagen, okay, die Straße ist sauber, wir sind wieder einsatzbereit und das Krankenhaus ist Land unter. Im Endeffekt geht es ja um den Patienten und der Patient durchläuft mehrere Stufen und wenn ich jetzt das Problem ins Krankenhaus verlagere und dort wie gesagt, das Krankenhaus nicht mehr handlungsfähig ist, dann freut das zwar den Rettungsdienst, weil der sagt, okay, Straße alles fein, aber es geht ja nicht darum, sondern es geht ja um den Notfallpatienten. D.h. in dem Fall kann es nicht nur darum gehen, dass ich ein System handlungsfähig halte, sondern und auch da war Covid wieder ein gutes Beispiel dafür, da ist es darum gegangen, sich mit dem Ärztenotdienst, mit 1450, mit der Rettungsleitstelle, mit den zentralen Notaufnahmen abzusprechen und nur wenn wir gemeinsam uns austauschen, gemeinsam eine Strategie erarbeiten, nur dann werden wir es schaffen, den Patienten durch die einzelnen Abschnitte zu begleiten und am Ende gut aus der ganzen Sache wieder entlassen zu können. Und es braucht hier einfach Zusammenarbeit der einzelnen Bereiche, Abstimmung der einzelnen Bereich in der Vorbereitung, aber auch dann wenn eine Krisensituation eintrifft, dass von jedem Bereich jemand im Einsatzstab sitzt um sich hier ganz, ganz eng abzustimmen und wie gesagt, das hat Covid eigentlich sehr gut gezeigt, dass das funktioniert in Wien und das braucht es auf alle Fälle. D.h. zu denken, wenn in meinem Bereich alles passt, ist das gut, wird uns in der Bewältigung solcher Krisen und Ausnahmesituationen nicht helfen.

A: Danke vielmals. Sie haben jetzt eingangs schon erwähnt, pro Tag werden etwa 1000 Notfallpatienten in die Versorgungseinrichtung der Krankenanstalten gebracht und dort versorgt. Zusätzlich gibt es natürlich eine unzählige Anzahl an Selbsteinweisungen von Personen die nicht mit dem Rettungsdienst frisch verletzt dort versorgt werden müssen und jene die einer ambulanten Nachversorgung bedürfen, die also vom Krankentransport gebracht werden. Die Kapazitäten und Strukturen der Krankenhäuser sind dabei auf die Individualmedizinische Versorgung unter normalen Betriebsbedingungen ausgelegt. Welche Maßnahmen erachten Sie als sinnvoll, damit eine medizinische Basisversorgung eines großteils der Betroffenen auch unter

negativen Auswirkungen eines Cybernotfalls oder eines Blackouts sichergestellt werden kann?

B: Also auch das habe ich eingangs eigentlich bei den anderen Fragen schon ein bisschen gestreift, also es wird notwendig sein, hier bereits bei der Notrufannahme, bei der Beschickung der einzelnen Notfälle eine Triage vorzunehmen und hier wirklich zu schauen, welcher Patient muss jetzt wirklich ins Krankenhaus, was kann vor Ort erledigt werden, bzw. was kann man am Telefon schon abfedern, sprich ärztliche Betreuung, ärztliche Beratung am Telefon, sowie wir es ja in Covid Zeiten zu Beginn der Pandemie auch gehabt hatten. Das ist glaube ich, ein wichtiger Punkt.

A: Herzlichen Dank für das Gespräch.

B: Bitte gerne.

Interview mit einer Expertin des LVT am 20.04.2022

A: Ich haben Ihnen vorab den Interviewleitfaden zukommen lassen, oder ich habe

B: (unv.) Oder wann haben Sie das geschickt?

A: Möglicherweise nachdem wir miteinander telefoniert haben, aber es kann auch sein, vielleicht habe ich es verabsäumt.

B: Da ist einmal nichts, dann habe ich ein zweites bekommen, da steht auch nichts.

A: Okay, dann möchte ich mich in aller Form entschuldigen, aber ich lese Ihnen ohnehin die Fragen vor, damit Sie auch wissen, worauf ich denn konkret Bezug nehme, ja.

B: Mhm (zustimmend)

A: Gut, die erste Frage ist gleich einmal in Richtung bezüglich der NIS-Gesetzgebung, es gibt ja neben dem NIS-Gesetz in Österreich und der NIS-Richtlinie auf EU-Ebene bereits andere Reglements wie Normen und dergleichen und jetzt ist die Frage, wie ordnen Sie die Notwendigkeit für eine gesetzliche Regulierung zur Einhaltung von IKT-Sicherheitsstandards ein, zumal es eben auch im Bereich der kritischen Infrastrukturen bereits Informationssicherheitsmanagementsysteme gibt, die implementiert wurden und betrieben werden?

B: Okay, schwierig, ich muss dazu sagen, dass ich technisch nicht sehr affiert bin, aber was ich jetzt sagen kann, ist, es gibt eine Vielzahl dieser Normen und jedes Unternehmen, ja wendet sie auch oder verwendet halt auch unterschiedliche Möglichkeiten an. Ich denke, dass hier eine gesetzliche Regelung schon von Vorteil ist.

A: Weil damit quasi ein Grundstock geboten wird?

B: Genau.

A: Der auf jeden Fall vorhanden sein muss.

B: Genau, der da sein muss.

A: Gut und es gibt eben, wie ich es auch schon erwähnt habe, neben dem Gesetz, gibt es ja auch das österreichische Programm zum Schutz kritischer Infrastruktur, das

Absib, dass sich von Absiss ableitet und das gibt es ja schon recht lange und wie, welche Bedeutung geben Sie da der NIS-Gesetzgebung, im Hinblick darauf, dass es ja bereits eine Strategie gibt und warum erachten Sie es eben als notwendig, dass es eben ein entsprechendes Gesetz jetzt noch als Unterstützung dieses ursprünglichen Programmes bereits gab?

B: Es ist ja nicht eine Strategie und keine gesetzliche Vorgabe, ja. Die Liste kritischer Infrastrukturen, die wir erarbeiten mit den Unternehmen, das passiert alles auf freiwilliger Basis, hier gibt es keine gesetzlichen Vorgaben, dass sie hier dabei sein müssen. Es kann jedes Unternehmen zu uns sagen, sie wollen weg von der Liste, sie wollen nicht draufbleiben, das steht jedem Unternehmen frei und das sagen wir auch immer, wenn wir die Erstgespräche führen.

A: Also wenn jemand sagt, ich verstehe, Sicherheit ist wichtig usw., aber es kostet mir zuviel, dann können die bei der –

B: Da geht es nicht um die Kosten, das ist so. Wir haben eine Strategie, die, das ist 2003 von der EU mehr oder weniger ins Leben gerufen worden. Wir haben eine Liste kritischer Infrastrukturen in Österreich, die wir in regelmäßigen Abständen besuchen. Wir erheben hier Daten, z.B. Ansprechpersonen oder Notfalltelefonnummer, damit wenn wir Kenntnis bekommen sollten, dass hier irgendein, das etwas passiert ist, dass wir diese Unternehmen kontaktieren können. Aber wir sagen dezidiert bei den Erstgesprächen immer, das ist keine Verpflichtung, das ist alles auf freiwilliger Basis. Wir bieten Beratung an und das natürlich alles kostenlos, bis auf eine Kleinigkeit, die Sicherheitsüberprüfungen, die sind sehr wohl zu bezahlen, wenn Sie das wünschen. Aber im Gegensatz zur NIS-Richtlinie, sind die ganzen Empfehlungen, die wir machen für die Bereiche Terrorismus, Extremismus, natürlich auch ein bisschen Risikomanagement, das ist alles kostenlos und passiert mehr oder weniger mit den Unternehmen auf freiwilliger Basis. Keine gesetzliche Verpflichtung. Da muss man sehr aufpassen, das ist ein Unterschied hier. Wir haben uns natürlich auch angelehnt an die Richtlinie und haben uns das angeschaut welche Unternehmen kommen da, da geht es um Schwellenwerte bei Krankenhäusern z.B., wir haben ein paar Krankenhäuser noch zusätzlich aufgenommen, weil die NIS-Behörde hier eine Empfehlung ausgesprochen hat. Also ja, wir versuchen das irgendwie gleich laufen zu lassen. D.h. wir versuchen die Unternehmen aufzunehmen, die auch in der NIS-Richtlinie angeschrieben wurden, bzw. hier auch auf einer eigenen Liste stehen.

A: Und das ist ja dann quasi auch schon eine gewisse Form der Vorarbeit, wenn dann die Richtlinie für resilienzkritische Infrastrukturen verabschiedet werden sollte.

B: Genau. Dann wird es interessant, ja.

A: Gut, dann danke schonmal. Und dann darf ich gleich überleiten zur Frage Nr. 3, die bezieht sich dann mehr auf das Thema Risikomanagement, dass wir jetzt schon mehrmals angesprochen haben, bei Risikomanagement handelt es sich ja um eine Querschnittsmaterie, damit quasi ein All-Hazards Ansatz verfolgt wird und ein möglichst breites Spektrum an möglichen Bedrohungen erfasst werden kann. Welche Risikoszenarien sind aus Ihrer Sicht für kritische Infrastrukturen aktuell denn die Vorrangigsten?

B: Aktuell, die Energieversorgung.

A: Also eh auch quasi gleichlautend mit der NIS, die ohnehin Energie als Top-Level Domäne hat.

B: Genau.

A: Was insofern jetzt recht praktisch ist, weil es mich auch gleich zur nächsten Frage wiederum führt. Energie, alle modernen Systeme sind ja von elektrischem Strom abhängig und auf die Verfügbarkeit darauf und es ist jetzt durch das Eintreten des Ukraine-Russland Konfliktes ein immer wieder propagiertes, potenzielles Szenario Realität geworden. Jetzt ist es so, dass Österreich sich ja im Bereich also klar zur Neutralität bekannt hat, lediglich humanitäre Hilfe in die Ukraine schickt, bei Deutschland ist das eine Spur anders. Jetzt meine konkrete Frage, wie schätzen Sie die Möglichkeit eines Kolleteralschadens ein, wenn das deutsche Stromnetz in Form eines Retaliation, also in Form eines Angriffs durch irgendwelche Hacker als Antwort auf Waffenlieferungen oder dergleichen bedroht werden würde? Also das deutsche Stromnetz wird geschädigt, inwieweit erwarten Sie dadurch Auswirkungen auf unser Stromnetz wiederum?

B: Große Auswirkungen.

A: Also auch, dass das eben nicht nur, die machen ihres, wir machen unseres, sondern, dass das durch die Vernetzung der Energie –

B: Nein, also ganz Europa ist ja ziemlich eng vernetzt miteinander im Strombereich, also da erwarte ich dann, oder da würde, wäre zu befürchten, dass es große Auswirkungen hätte. Betrifft dann überhaupt bei Hackergeschichten, betrifft dann nicht uns, sondern betrifft, das kann man jetzt nicht so lokal sagen, dass dann nur Deutschland betrifft, sondern das würde eigentlich die meisten Länder Europas betreffen.

A: Gut. Ich habe Blackout anhand der Literatur als ein überregionales und mehrtägiges Ereignis definiert, wo das gesellschaftliche Gefüge folglich dann auseinander, also darunter leidet. Welche Maßnahmen hat Ihre Organisation, also ich meine damit das Innenministerium als Gesamtes, für Maßnahmen gesetzt, um auf ein Blackoutszenario vorbereitet zu sein?

B: Das ist jetzt eine sehr schwierige Frage, kann ich Ihnen eigentlich keine Antwort geben.

A: Ist absolut legitim.

B: Es sind Vorbereitungsarbeiten im Gange, es wird darüber diskutiert, inwieweit die gediehen sind, das tut mir leid, da möchte ich auch nicht irgendetwas Falsches sagen, lassen wir die Frage aus bitte.

A: Selbstverständlich. Gut, dann ein Thema, dass die Bevölkerung betrifft. Es gibt mehrere Studien, wonach Eigenbevorratung im urbanen Raum, also ich spreche da speziell die Wiener Bevölkerung an, dass diese Bevorratung eben unzureichend sei.

B: Welche Bevorratung?

A: Die Selbstbevorratung, ja das der typische Wiener oder die typische Wienerin aufgrund der modernen Annehmlichkeiten kaum noch Reserven daheim hat.

B: Ja das stimmt.

A: Und wenn nun ein Blackout eintritt, oder ein Versorgungsengpass welcher Natur auch immer, dann würde, ist anzunehmen, dass diese Bevölkerungsschicht früher oder später dann sogenannte Lichtinseln aufsuchen wird. Dort wo es warm ist, wo es Essen gibt, sprich Spitäler. Wie sollte Ihrer Meinung nach mit diesem Problem umgegangen werden, oder wie sollte man dem begegnen?

B: Mein Wunsch diesbezüglich wäre schon bereits in der Schule zu beginnen, Sensibilisierungsarbeit zu leisten. Das Strom nicht immer und überall zur Verfügung steht. Dass man eben achtsamer mit diesen Ressourcen umgeht, mit wesentlich mehr Informationen über die Medien, mit Wurfsendungen und tatsächlich auch immer wieder, so kleine Trainings, die selbst in Firmen stattfinden können, wo sich eben, wo die Belegschaft eben jetzt auch wieder informiert wird, was kann passieren. Einige unserer Unternehmen machen das schon, wir haben, wir machen selbst jetzt so Blackout-Vorsorge Treffen, in denen darüber diskutiert wird, in denen Beratungen durchgeführt werden, was es im Falle eines Blackouts, was da auf einen Menschen zukommen kann. Aber wie gesagt, es muss, wir sind eigentlich relativ spät dran, es müsste schon in der Schule damit begonnen werden.

A: Ich verstehe, es ist auch eben wieder Strom angesprochen worden, an erster Stelle im NIS-Gesetz steht der Energiesektor und auch in der NIS-Verordnung ist der NIS-Sektor an Platz 1 gereiht. Sämtliche modernen Systeme hängen vom Strom ab und daher ist diese Vernetzung von kritischen Infrastrukturen untereinander durch das Stromnetz offensichtlich. Geht Ihrer Meinung nach das NIS-Gesetz auf diese Abhängigkeit ausreichend ein und auf diese wechselseitige Abhängigkeit? Das einerseits eben beispielsweise die Telekommunikation ein Stromnetz bedarf, aber andererseits auch ein Stromnetzbetreiber bis zu einem gewissen Grad eine Notwendigkeit des funktionierenden Telekommunikationsnetzes hat?

B: Von welchem NIS-Gesetz sprechen wir jetzt?

A: Vom österreichischen.

B: Vom bereits bestehenden?

A: Vom bestehenden, vom aktuellen.

B: Da ist natürlich, da sind noch große Lücken, das ist vollkommen klar, darum soll es ja diese Resilienzrichtlinie geben, worauf dann intensiver auf diese Problematik eingegangen werden kann.

A: Okay.

B: Das ist dann so die Ergänzung so zum ersten Gesetz.

A: Hervorragend, also das deckt sich auch mit meiner Erwartungshaltung, bin ich sehr froh. Meine letzten beiden Fragen fokussieren sich dann mehr auf den Bereich Gesundheitssektor. Und zwar, ich verstehe den Behandlungspfad von einem Notfallpatienten bis zur finalen Behandlung im Spital als eben die Rettungskette und da sind mehrere Player involviert. Wenn jetzt jeder für sich versucht autark zu sein, also der Begriff „autark“ ist ja eher das Gegenteil von vernetzt. Wie beurteilen Sie diesen Begriff „Autarkie“ im Rahmen einer vernetzen, systemübergreifenden Prozesskette?

B: In Verbindung jetzt mit Gesundheit, Krankenhaus und solchen (unv.)

A: Z.B. ja. Oder wenn Sie ein anderes, griffigeres Beispiel haben, können Sie das auch gerne bemühen.

B: Das ist meiner Meinung jetzt, aufgrund dieser extremen Vernetzung fast nicht möglich hier eine Autarkie oder autark, diesen Begriff zu verwenden, nein würde ich nicht sagen.

A: Das deckt sich auch mit der Aussage von Fr. Dr.in Mayer und auch mein vorläufiges Resümee, dass ich aus der gesamten Sache ziehen muss. Gut, nun die finale Frage, die Berufsrettung Wien, mit den Partnerorganisation im Rettungsbund führt etwa 1000 Notfalleinsätze am Tag durch, die dann in Wiener Spitälern medizinisch folgeversorgt werden. Zusätzlich zu diesen 1000 werden weitere tausende Patienten gehen eben in die Ambulanzen als Selbsteinweiser, plus es gibt weitere, die dann zur Nachbehandlung und dergleichen kommen. Welche Maßnahmen und genau, diese Strukturen sind natürlich für den Normalbetrieb ausgelegt. Welche Maßnahmen erachten Sie als sinnvoll, damit so eine medizinische Basisversorgung eines Großteils der Bevölkerung auch unter den negativen Auswirkungen eines Cybernotfalls oder eines Blackouts sichergestellt werden können?

B: Triage. Wir haben oder es wurde ja in den meisten Spitälern ja durchgeführt, aufgrund der Pandemie wurde ja da auch relativ viel schon an Erfahrung gesammelt, diesbezüglich. Aber im Falle eines Blackouts wird das sein müssen. Weil auch das Spital hat endendwollende Ressourcen, das hört irgendwann mal auf. Auch wenn es jetzt eine Zeitlang durch staatliche Hilfe noch einige Tage existieren kann, aber es hört auf. Und das bedeutet, hier muss von Anfang an relativ strikt vorgegangen werden.

A: Ja, diese Ansicht teilt unter anderem auch der Chefarzt, da kristallisiert sich eine eindeutige Aussage heraus. Sehr fein. Herzlichen Dank, das war auch schon wieder die letzte Frage und Sie haben mir da mit einigen Antworten konkret sehr weiterhelfen können und ich freue mich, wenn ich das dann auszugsweise auch in meiner Arbeit auch zitieren dürfte.

B: Natürlich, dürfen Sie.

A: Herzlichen Dank.

B: Anonymisiert?

A: Wenn Sie das wünschen, werde ich nicht sagen, wer meine Expertin in diesem Zusammenhang war.

B: Gut.

A: In Ordnung, herzlichen Dank nochmal und im Bedarfsfall, sollte ich beruflichen Kontext haben.

B: Das wäre, glaube ich, das Wichtigste.

A: Das ist an und für sich ein sehr gutes Aufzeichnungsgerät. 20. April 2022, Interview mit Frau Doktorin Mayer, DSN. Frau Doktor, herzlichen Dank, dass Sie sich die Zeit nehmen. Ich darf gleich mit der ersten Frage starten. Wie ordnen Sie die Notwendigkeit für eine gesetzliche Regulierung zur Einhaltung von IKT-Sicherheitsstandards ein, zumal von vielen kritischen Infrastrukturen ein Informationssicherheits-Managementsystem implementiert wurde und bereits betrieben wird?

B: Also ich kann bestätigen, dass die Unternehmen kritische Infrastruktur in Österreich schon sehr hohe Sicherheitsstandards bereits implementiert haben. Das haben auch die Erfahrungen aus unserer Tätigkeit in der DSN im Bereich Schutz kritischer Infrastruktur gezeigt. Es gibt im Bezug darauf natürlich Unternehmen gewisser Sektoren, die höhere Standards implementiert haben als andere. Als Beispiel darf der Finanzsektor genannt werden, der natürlich aufgrund seiner auch Historie und aufgrund seiner immer schon quasi intendierten, quasi als Ziel für Täter und Täterinnen quasi als Ziel wahrnehmbar war und dementsprechend hohe Sicherheitsstandards implementieren mussten. Also der Finanzsektor ist hier wohl sehr resilient, wohingegen andere Sektoren, die bisher nicht wirklich Ziel von Angriffen waren, eher weniger resilient zu sein scheinen, als Beispiel jetzt wirklich auch wieder der Lebensmittelsektor oder der Gesundheitssektor, die jetzt per se nicht wirklich bisher Angriffen ausgesetzt waren und deshalb auch, im Zuge einer risikobasierten Einschätzung, auch nicht so hohe Sicherheitsstandards implementiert haben. Und aus dem Grund sehe ich die Notwendigkeit schon als sehr groß ein, wirklich einen generellen Standard für kritische Infrastrukturen zu setzen, dass wirklich alle Betreiber hohe Standards einführen müssen, weil wirklich auch alle Unternehmen entsprechend wichtig sind für die Gesellschaft und für die Versorgung.

A: Dass aus dem Gesamten betrachtet. Und damit ist an und für sich auch schon die nächste Frage, worin der Ihrer Meinung nach der Mehrwert für die Gesellschaft durch diese bundesgesetzliche Regelung liegt. Ansatzweise beantwortet also, einfach dass, ich darf einmal daraus schließen, dass durch diese Mindeststandard eines Gesetzes eben alle, die als notwendig oder als für die Gesellschaft wichtig erachtet werden, auf dasselbe Niveau gehoben werden. Zumal ist ja immer die Möglichkeit auch besteht, mehr zu leisten als das, was unmittelbar nur im Gesetz drinsteht.

B: Genau. Also unabhängig davon, ob einzelne Unternehmen Ziel von Tätern und Täterinnen sind oder auch nicht, so kann man doch feststellen, dass alle Betreiber kritischer Infrastruktur eine entsprechende Bedeutung haben für die Gesellschaft und für die Versorgung. Und dementsprechend muss bei allen Unternehmen und allen Betreibern ein hoher Standard erreicht werden, um die Gesellschaft entsprechend resilient zu gestalten.

A: Damit darf ich dann zur nächsten Frage überleiten. Es gab ja bereits, bevor die NIS-Richtlinie implementiert wurde geeignete Strategien der Republik Österreich, eben die österreichische Sicherheitsstrategie, dann eine eigene Cybersicherheitsstrategie und nicht zuletzt auch den Aktionsplan zum Schutz der österreichischen Infrastruktur. Welche Bedeutung messen Sie jetzt den beiden Strategien beziehungsweise auch Normen wie der ISO 27.000 bei, im Vergleich zum NIS-Gesetz?

B: Also ich würde beginnen mit den Normen, die natürlich unter der Leitlinie der Freiwilligkeit stehen und Unternehmen natürlich auf freiwilliger Basis sich bestimmten Normen unterwerfen. Da gab es nur insofern vielleicht unter Anführungszeichen einen Anreiz der Unternehmen, weil zum Beispiel in den Lieferketten andere Unternehmen das voraussetzen, dass ihre Zulieferer zum Beispiel entsprechende Normen zertifiziert haben. Das ist einmal der erste Schritt. Also da gab es eben eigentlich nur diesen Anreiz und den Anreiz der Freiwilligkeit, dass ich mich selbst im gewissen Rahmen (unv.).

A: Also eher durch den Markt bestimmt und nicht durch gesetzliche Regelung.

B: Genau, würde ich. Genau, genau. Der zweite Schritt ist dann die Strategie, einerseits das österreichische Programm zum Schutz kritischer Infrastruktur und auch die Österreichische Cybersicherheitsstrategie. Das würde ich dann auf der nächsten Stufe sehen, weil hier tatsächlich auch der Staat und die Behörden aktiv Maßnahmen gesetzt haben, um Unternehmen in der Umsetzung diverser Sicherheitsstandards zu bekräftigen und zu unterstützen. Das heißt, im Rahmen dieser Strategien haben die Behörden und der Staat tatsächlich Unternehmen dazu aufgefordert, in Beratungsgesprächen, im Rahmen von Veranstaltungen und Sonstigem, dass sie entsprechende Sicherheitsmaßnahmen umsetzen, aber immer noch unter dem Prinzip der Freiwilligkeit, wir haben das damals als Public-private-Partnership bezeichnet.

A: Also es konnte nicht von Seiten des Staates sanktioniert werden. Wenn jetzt ein wichtiger Key Player da sich nicht beteiligen möchte, dann musste das vom Staat so hingenommen werden.

B: Genau. Also man hat so die Unternehmen aufgefordert und hat ihnen die Vorteile einer erhöhten Sicherheit natürlich entsprechend kommuniziert. Aber eine Verpflichtung gab es für die Unternehmen keine. Und darum ist jetzt der nächste Schritt, nämlich die bundesgesetzliche Regelung, so wichtig, weil tatsächlich Unternehmen verpflichtet sind, so einen Mindeststandard umzusetzen und dass auch bei Zuwiderhandeln entsprechend sanktioniert werden kann.

A: Jetzt ist es klar, aus Ihrem beruflichen Umfeld kennen Sie möglicherweise ein weitaus größeres Portfolio an Risikoszenarien. Aber welche kommen Ihnen denn aktuell besonders in den Sinn, wenn es um den Schutz kritischer Infrastrukturen geht?

B: Ja, ich meine natürlich, klar sind Risiken wie Cyberangriffe auf Energieunternehmen beispielsweise, auch Cyberangriffe auf Banken, aber auch physische Angriffe beispielsweise auf Krankenhäuser, wie wir jetzt im Rahmen der Covid-Pandemie auch gesehen haben und wo es entsprechende Sabotageakte gegeben hat, auf Impfstraßen zum Beispiel, ja und auf Gesundheitseinrichtungen generell. Also das sind Angriffe, die wir ohnedies kennen. Wenn man jetzt von Risiken spricht, die sich in der letzten Zeit neu ergeben haben und die wahrscheinlich vorher nicht so ableitbar waren, so ist es die Pandemie als Risiko für Unternehmen, die natürlich mit einem entsprechenden Ausfall von Lieferketten verbunden ist, die mit einem entsprechenden Ausfall von Personal verbunden ist. Durch verstärkte Grenzkontrollen beispielsweise, wie wir am Beginn der Pandemie auch gesehen haben, wo Mitarbeiter, Mitarbeiterinnen dann nicht mehr vor Ort im Büro tätig sein können. Das ist für Unternehmen, die im (unv.) Bereich tätig sind, wohl eher irrelevant, weil auf Homeoffice zurückgegriffen werden konnte. War aber zum Beispiel sehr kritisch in der Lebensmittelindustrie, in der Fleischproduktion und -verwertung, wo sehr viel auf ausländische Arbeitskräfte zurückgegriffen wird, da war es ein massives Problem am Beginn der Pandemie, dass man da bewerkstelligt, dass weiterhin auch alle Arbeitskräfte in die Arbeit kommen können. Also man hat an der Pandemie sehr gut gesehen, dass es sehr wichtig ist, dass Unternehmen ein Risikomanagement durchführen und auch im Zusammenhang mit Black Swan, wenn der Begriff bekannt ist, auch an Risiken denken, die vielleicht jetzt bisher noch nicht vorgekommen sind, die aber möglich wären. Und das ist schon

auch quasi ein Trend, der die Resilienz von Unternehmen entsprechend schwächen könnte und mit dem sich Unternehmen auch auseinandersetzen müssen.

A: Wobei der Black Swan ja nach meinem persönlichen Dafürhalten jetzt ein bisschen auch hinterfragt werden muss, weil auch ein Krieg am Rande von Europa wurde, als unrealistisch eingestuft und nun sind wir mittendrin.

B: Genau. Also der Krieg ist ja wirklich ein sehr aktuelles Beispiel, der auch kritische Infrastrukturen in Österreich betreffen kann. Natürlich. Also je mehr sich Österreich da entsprechend auch positioniert, (so wie alle?) Staaten, desto eher ist man natürlich dann Cyberangriffen von Staaten ausgesetzt, denen dies zuwiderläuft.

A: Das ist eine hervorragende Überleitung zu Frage Nummer vier. Da geht es nämlich konkret darum, Österreich hat sich in der aktuellen Situation mit der Ukraine deutlich auf die Neutralität berufen und lediglich auf Hilfslieferungen, also humanitäre Güter, beschränkt. Hingegen Deutschland hat und wird voraussichtlich auch Waffen, Defensivwaffen liefern. Jetzt könnte natürlich als Repressionsmaßnahme von Russland ein Cyberangriff auf die Infrastruktur in Deutschland führen. Wie schätzen Sie die Auswirkungen oder das Potenzial eines Kollateralschadens auf Österreich ein? Wenn Deutschland beispielsweise das Stromnetz oder die Wasserversorgung oder Ähnliches, das eng mit uns vernetzt ist, also mit Österreich vernetzt ist, betroffen sein sollte?

B: Ja, also für den Fall oder für das Szenario, dass zum Beispiel Infrastruktur, oder kritische Infrastruktur der Energieversorgung in einem der Nachbarstaaten oder generell im europäischen Raum angegriffen werden sollte und ausfallen sollte, dann gäbe es natürlich ein immenses Risiko von Ausfällen auch in Österreich. Das Stromnetz ist ja jetzt, das österreichische Stromnetz ist ja jetzt keine Insellösung, sondern ist verbunden natürlich mit dem europäischen, mit der europäischen Energieversorgung. Und dementsprechend wäre ein großflächiger Stromausfall und großflächige Probleme im deutschen Stromnetz jedenfalls ein sehr hohes Risiko für die Energieversorgung in Österreich. Also nicht nur, dass wir selbst angegriffen werden könnten, unabhängig davon, auch wenn andere Staaten angegriffen werden würden, wird sich daraus ein Risiko für Österreich ergeben.

A: Bleiben wir noch kurz beim Thema Blackout-Szenario. Welche Maßnahmen hat Ihre Organisation gesetzt, um im Falle eines Blackout-Szenarios vorbereitet zu sein?

B: Für uns war ganz wichtig, dass wir uns als Sicherheitsbehörde einerseits und auch als für das staatliche Krisen- und Katastrophenschutzmanagement zuständige Behörde des Bundesministerium für Inneres, dass wir uns da sehr eng mit den Betreibern der sonstigen Versorgung abstimmen und koordinieren. Denn wir können das BMI, das staatliche Krisen- und Katastrophenschutzmanagement, also SKKM, nur dann umsetzen, wenn auch die kritische Infrastruktur in solchen Szenarien funktioniert. Das heißt, wenn wirklich dann auch bei einem Stromausfall trotzdem weiterhin in gewissen Bereichen Wasserversorgung gegeben ist, wenn die Lebensmittelversorgung funktioniert, wenn das Internet, Mobilfunknetz funktioniert, und so weiter. Deshalb haben wir uns einerseits in einzelnen Workshops sehr eng abgestimmt mit Betreibern aller Sektoren, um da Maßnahmen zu erarbeiten, wie wir in solchen Krisenszenarien umgehen würden und auch weiter miteinander kommunizieren würden. Es gibt auch Übungen, die stattgefunden haben, letztes Jahr und vorletztes Jahr, wo man tatsächlich solche Szenarien durchgespielt hat und welche Organisationen dann welche Rolle wahrnehmen und einnehmen würde. Als Beispiel, was die DSN zum Beispiel auch gemacht hat im Bereich des Schutzes kritischer Infrastruktur, war, dass alle Betreiber ein Digitalfunkgerät zur Verfügung gestellt bekommen haben, mit dem dann auch im Fall eines Blackouts und wenn die sonstigen Telefonanlagen nicht mehr funktionieren, danach mit den Betreibern kritischer Infrastruktur weiterhin kommuniziert werden kann über dieses Digitalfunkgerät.

A: Also man kann summieren. Es war eine sehr enge Abstimmung mit den anderen Interessensgruppen, damit eben die Handlungsfähigkeit des Innenministeriums und des DSN gewährleistet bleibt.

B: Genau. Es hat sich auch jetzt während der Covid-Krise gezeigt, dass Zusammenarbeit mit sehr, sehr vielen Organisationen mit das Wichtigste ist und dass es sehr wichtig ist, dass man sich im Vorfeld schon abstimmt, im Vorfeld kennenlernt, im Vorfeld die Ansprechpersonen kennt und die Wege, die kurzen Wege in gewissen Krisenszenarien, damit man dann im Krisenfall besser agieren kann.

A: Dann hole ich kurz aus bei der Frage Nummer sechs. Das Thema Eigenbevorratung der Bevölkerung. Also die Ministerien und kritischen Infrastrukturen sind hier meistens für einige Tage vorbereitet. Nun gibt es Studien, wonach speziell die Wiener Bevölkerung oder die urbane im urbanen Raum durch den Komfort der modernen Zeit

eher nicht Eigenbevorratungen hat. Wie sollte Ihrer Meinung nach diesem Problem begegnet werden? Wäre da möglicherweise auch eine gesetzliche Regelung sinnvoll, sinnstiftend zur Entlastung der kritischen Infrastrukturen?

B: Genau, also bei dieser Frage, wenn ich mir die durchlese, zielt sie eben auch darauf ab, dass bestimmte Gebäude und Objekte, die eben weiterhin Wärme, Wasser, Lebensmittel vorweisen, dann eventuell einem sehr starken Zulauf ausgesetzt wären durch die Bevölkerung.

A: Ja, also ich denke da speziell an die kolportierten Lichtinseln, die dann Krankenanstalten beispielsweise darstellen.

B: Genau, ich wollte gerade auch das Wort Lichtinseln in den Mund nehmen. Genau, wir haben das Risiko schon vor einigen Jahren sehr stark gesehen und haben das und sind dem unter anderem so begegnet, dass es für uns wichtig ist, zum Beispiel Krankenhäuser als solche leuchtenden Inseln in der Stadt im Fall eines Blackouts entsprechend zu schützen. Und wir haben dementsprechend unter anderem auch für Krankenhäuser Schutzkonzepte erarbeitet und entwickelt. Gemeinsam mit den Polizeikräften auch in Wien und unter Mitwirkung der DSN, damit wir im Fall eines Blackouts als Polizei dann auch diese Krankenhäuser durch quasi Sicherheitsposten vor Ort entsprechend schützen können. Also wir sagen, wir haben das Risiko erkannt und würden dem im Falle eines Blackouts auch begegnen.

A: Damit eben die, die Hilfe bekommen, die sie benötigen und nicht die, die sie nur wollen.

B: Genau. Ich meine, der andere Punkt ist natürlich, dass man jetzt im Rahmen des Zivilschutzes natürlich die Bevölkerung oder ich glaube, das wird eh sehr viel und in letzter Zeit sehr verstärkt gemacht hat, auch die Menschen sensibilisiert und Bewusstsein schärft, dass sie sich selbst auch entsprechende Bevorratungen anlegen. Dies ist ohnedies notwendig, und wir müssen natürlich in einem Krisenfall dafür sorgen, dass die Menschen, die das brauchen, dann auch die entsprechenden Lebensmittel, Wasser, Wärme zur Verfügung gestellt bekommen. Das ist das eine und für das muss man natürlich auch sorgen. Das andere ist natürlich, dass wir bestimmte Objekte, wo andere Menschen vor Ort sind, krankheitsbedingt, gesundheitlich bedingte Hilfe brauchen, dass man die auch entsprechend schützt und das sehe ich dann auch im zweiten Blatt Papier. Aber man muss sich natürlich um beides kümmern.

A: Dann bleiben wir auch noch kurz bei der Thematik Energiesektor und NIS-Gesetz. An erster Stelle ist eben der Energiesektor im NIS-Gesetz und in der NIS-Verordnung genannt, als wesentlichster Sektor. Und bei modernen Systemen besteht natürlich eine hohe Abhängigkeit von der Stromversorgung. Im Bereich der Stromversorgung ist eben diese Vernetzung auch hinlänglich bekannt. Bei anderen Infrastrukturen ist das weniger offensichtlich. So, da finde ich. Ja. Geht die NIS-Gesetzgebung Ihrer Meinung nach ausreichend auf die wechselseitige Beziehung von kritischen Infrastrukturen ein?

B: Ich denke, sie geht ausreichend auf die Interdependenzen ein. Sie geht aber nicht im Detail darauf ein. Also die NIS-Gesetzgebung geht ja von unterschiedlichen Sektoren, Teilsektoren und wesentlichen Diensten aus. Und aufgrund dieser Systematik erfolgt dann die Identifizierung von Betreibern wesentlicher Dienste, unabhängig von einer Interdependenz zwischen den einzelnen Sektoren. Das ist das eine. Also diese Kategorisierung und die Struktur ist wohl sehr klar und unabhängig von wechselseitigen Beziehungen. Was die NIS-Gesetzgebung schon macht, ist, dass sie auf die prioritäre Relevanz der Energieversorgung eingeht, nämlich im Rahmen der Meldepflicht von sicherheitsrelevanten Vorfällen. Weil in der NIS-Verordnung ja für die einzelnen Betreiber wesentlicher Dienste beziehungsweise für die einzelnen Sektoren und wesentlichen Dienste unterschiedliche Fristen für die Meldepflicht vorgesehen sind. Heißt, Energieversorger beispielsweise, ist in der NIS-Verordnung nachzulesen, haben Sicherheitsvorfälle größtenteils unmittelbar zu melden. Die Stromversorgung muss man nennen, zum Beispiel im Bereich Öl müssen sich jetzt Vorfälle wieder erst zum Beispiel erst nach zwölf Stunden oder 24 Stunden gemeldet werden. Im Bereich der Stromversorgung sind Sicherheitsvorfälle sofort zu melden, also wenn sofort, nachdem der Vorfall eintritt und nicht erst quasi nach einer bestimmten Zeit, die der Vorfall andauert. Und dementsprechend wurde hier auf die Relevanz der einzelnen Sektoren und Teilsektoren Rücksicht genommen.

A: Dann kommen wir zu meinem Kernsegment, der Gesundheits- und medizinischen Versorgung. Die Behandlung von Erkrankten und Verletzten kann als ein Ineinandergreifen eines großen Behandlungsprozesses angesehen werden, Schlagwort Rettungskette. Der Behandlungspfad beginnt eben mit der Ersten Hilfe durch Laien. Dann kommt es zu einer Notrufmeldung, meist jetzt mit Mobiltelefon. Dann wird qualifizierte Erste Hilfe durch Rettungsmannschaften geleistet und ein

Transport in eine fachmedizinische Klinik durchgeführt. Wie beurteilen Sie den Begriff Autarkie im Rahmen dieser Vernetzung von systemübergreifenden Prozessen? Systemübergreifend im Sinne von Teilsektor Rettungsdienst, Teilsektor Gesundheitseinrichtungen?

B: Also ich denke, mit Fortschreiten der Effizienzsteigerung von Systemen, mit Fortschreiten auch der Digitalisierung natürlich. Und wir haben vorher schon darüber gesprochen, mit der Abhängigkeit von Strom natürlich, von allen Diensten, ist die Autarkie in der heutigen Zeit nur noch sehr schwer zu erreichen. Also jeder wesentliche Dienst ist sehr wohl von sehr vielen anderen Diensten abhängig und muss natürlich danach trachten, auch im Fall des Ausfalls dieser anderen Dienste. Also wir haben schon vom Strom gesprochen, aber man kann auch von Wasser ausgehen oder von der Lebensmittelversorgung oder vom Funktionieren des Mobilfunks beispielsweise. Jedes Unternehmen muss sich im Rahmen der Risikoanalyse einfach Szenarien überlegen, zu welchen Ausfällen es kommen kann und welche Maßnahmen dagegen ergriffen werden können, sei es jetzt durch eine Notstromversorgung zum Beispiel eines Objekts für den Fall eines Stromausfalls. Also wenn Sie mich fragen, wie ich den Begriff beurteile, dann sage ich, grundsätzlich in der heutigen wirtschaftlichen Zeit kaum mehr möglich und nicht mehr gegeben. Aber Unternehmen sollten zumindest für die höchsten Risiken, die es gibt, also für viele relevante Szenarien sich überlegen, wie sie dann ihre Kernprozesse, und darauf kommt es dann an, also wirklich auf die Kernprozesse, wie sie diese weiterhin erbringen können.

A: Danke vielmals. Und nun zur letzten Frage. Es geht da wieder sehr Wien-spezifisch darum, durch den Wiener Rettungsverbund, also die sechs Einsatzorganisationen in Wien, werden etwa 1000 Notfallpatienten in Wiener Krankenanstalten zu einer medizinischen Folgeversorgung gebracht. Zusätzlich versorgen die Wiener Spitäler unzählige weitere Personen, die im Rahmen von Selbsteinweisungen die Spitäler aufsuchen. Und diese Strukturen und Abläufe sind natürlich auf den Normalbetrieb ausgelegt. Welche Maßnahmen erachten Sie nun als sinnvoll, damit eine medizinische Basisversorgung eines Großteils der Betroffenen auch unter negativen Auswirkungen eines Cybernotfalls oder eines Blackouts sichergestellt werden kann?

B: Ja, dazu kann ich eigentlich nicht wirklich etwas sagen, da tue ich mir schwer. Also, ich kann es ja nur aus meiner Sicht und unserer Sicht bewerten. Ganz wichtig ist, dass man sich einfach hinter, dass man in den Krankenhäusern die Sicherheit von IT-

Systemen stärkt. Wir haben dazu sehr viele Workshops auch organisiert in den letzten fünf Jahren in Krankenhäusern und dass man auch die Awareness in den Krankenhäusern stärkt, wie man mit Sicherheit umgeht. Sowohl physische Sicherheit als auch Cybersicherheit, ist das eine. Und das Zweite ist ja, man muss sich sicher da als Wiener Krankenanstaltenverbund einfach Szenarien überlegen, die auf die Gesundheitsversorgung quasi eintreffen könnten und zukommen könnten. Und wie man dem als Verbund begegnet, indem die Krankenhäuser wechselseitig Patienten aufnehmen, und so weiter. Ich denke aber, dass das sowieso in Erarbeitung ist. Und was die Sicherheit betrifft, fahren wir als Sicherheitsbehörden schon sehr viel Kampagnen, um da die Resilienz zu erhöhen.

A: Herzlichen Dank.