St. Pölten University of Applied Sciences

/informatik & security

/fh/// st. pölten

Cyber Resilience: Eine systematische Literatur Analyse

Diplomarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieur/in

eingereicht von

Traude Lang
IS201809

im Rahmen des
Studiengangs Information Security an der Fachhochschule St. Pölten

Betreuung
Betreuer/Betreuerin: FH-Prof. Dr. Simon Tjoa
Mitwirkung: -

Wien, 16.01.2024

(Unterschrift Autor/Autorin)

(Unterschrift Betreuer/Betreuerin)

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.

- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Der Studierende/Absolvent räumt der FH St. Pölten das Recht ein, die Diplomarbeit für Lehre- und Forschungstätigkeiten zu verwenden und damit zu werben (z.B. bei der Projektevernissage, in Publikationen, auf der Homepage), wobei der Absolvent als Urheber zu nennen ist. Jegliche kommerzielle Verwertung/Nutzung bedarf einer weiteren Vereinbarung zwischen dem Studierenden/Absolventen und der FH St. Pölten.

Wien, 16.01.2024

(Unterschrift Autor/Autorin)

Diese Arbeit ist meiner Mutter gewidmet.
Lang Maria (Hausfrau, 1945 – 2022)
Ohne sie wäre ich nie so weit gekommen.

Zusammenfassung

Die Welt hat sich geändert. Das Internet ist aus dem Alltag nicht mehr wegzudenken und die Gesellschaft wird immer abhängiger von verschiedensten Internet Services. Auf der anderen Seite sind kritische und hochsensible Systeme nicht weiter isoliert sondern hochgradig vernetzt und kommunizieren untereinander. All das wird zunehmend von Cyber-Kriminellen genutzt und die Zahl der Angriffe steigt stetig. Herkömmliche Methoden wie Risk-Assessments bieten keinen ausreichend Schutz, um immer komplexer werdende Systeme abzusichern. Cyber Resilience ist eine Möglichkeit diesem Umstand zu begeben. Diese systematische Literaturanalyse (SLR) betrachtet das Thema Cyber Resilience in der aktuellen Forschung, welche Bereiche, Branchen und Methoden adressiert werden und wo weiterer Bedarf besteht. Bisherige Arbeiten beleuchten nur Teilaspekte zu Cyber Resilience, keine behandeln das Thema ganzheitlich, um aufzuzeigen was bereits gut erforscht ist und wo es Lücken gibt.

Studien zu Cyber Resilience werden mehrheitlich in Amerika und da vor allem in den USA veröffentlicht und vorgestellt. Europa ist mit in etwa 30% der Studien an zweiter Stelle. Bei Kooperationen mit unterschiedlichen Institutionen zeigt sich, dass Amerika und hier wieder vornehmlich die USA mit der Hälfte der Studien Kooperationen im eigenen Land bevorzugen, während Europa mit mehr als zwei Drittel gar keine Kooperationen eingeht. Asien hingegen steht mit 50% der Studien internationalen Kooperation am offensten gegenüber. Analysiert man die Branchen der jeweiligen Studien erkennt man zum einem, dass 45% der Studien keine eindeutige Zuordnung zulassen. Unterteilt man diesen Bereich weiter und summiert alle Branchen die der kritischen Infrastruktur angehören ergeben sich 55% aller Studien in diesem Bereich. Gering fällt die Rate mit unter 10% auf reine IT-Services und Brachen um Gesellschaft oder Politik aus. Forschungsfelder widmen sich zum Teil der Analyse und Definition von Cyber Resilience, diese machen ungefähr ein Drittel aller Studien aus. Die restlichen Studien setzen sich mit der Umsetzung von CR in Frameworks, Architekturen, Assessmentmodelle, Systemmodellierung und technischen Systemen auseinander. Systemmodellierung zur Verhaltensanalyse machen ein Viertel aller Studien aus und stellen somit einen wichtigen Bereich in der Forschung zu Cyber Resilience dar. Dieser Bereich hat zusammen mit den Assessmentmodellen den Schwerpunkt der Messung von Cyber Resilience in unterschiedlichen Kontexten. Ebenso Systemmodellierungen aber auch Frameworks und Architekturen haben einen deutlichen Fokus auf der Erkennung und Abwehr von Angriffen. Cyber Resilience in Organisationen finden sich auf der einen Seite in Verbindung mit Frameworks aber auch in der Analyse und Bedarfs- sowie Statuserhebung zu Cyber Resilience wieder. Die bevorzugenden Methoden in Studien zu Cyber Resilience sind Modellierungen, Simulationen und Experimente, neben der klassischen Literaturanalyse. Weiters wurden die genannten Bereiche gegenübergestellt sowie künftige Forschungsbereiche erhoben. Hier seien die Messung und adäquate Messdaten aber auch Aspekte wie Socio-ökonomische Faktoren oder Technologien um e-Mobility und autonome Systeme als empfohlene Forschungsfelder genannt. Es konnten außerdem keine Studien zu kritischen Bereichen wie Gesundheitsversorgung oder Finanzwesen erhoben werden was einen Forschungsbedarf, auch speziell zur Statuserhebung, erkennen lässt.

Die Studien dieser SLR wurden im April 2023 erhoben, es wurden aus 1208 Studien nach zuvor definierten Auswahlkriterien insgesamt 80 Studien aus den Datenbanken ACM Digital Library, IEEE Xplore Digital Library und SienceDirect ausgewählt. Die Studien aus den Jahren 2018 – 2023 sind Peer-Reviewed Primär-Studien und behandeln Cyber Resilience ganzheitlich und umfassend. Mittels qualitativer Inhaltsanalyse und der Erhebung statistischer Daten wurden die Ergebnisse erfasst. Die Studienauswahl und Datenextrakation wurde ausschließlich von der Autorin durchgeführt, dies stellt eine Limitierung und mögliche Unschärfen in den Ergebnissen dar.

Abstract

The world has changed. The Internet has become an integral part of everyday life and society is becoming more and more dependent on various Internet services. On the other hand, critical and highly sensitive systems are no longer isolated but are highly networked and communicate with each other. All of this is increasingly being used by cyber criminals and the number of attacks is constantly increasing. Conventional methods such as risk assessments do not offer sufficient protection to secure increasingly complex systems. Cyber resilience is one way to address this situation. This systematic literature review (SLR) looks at the topic of cyber resilience in current research, which areas, industries and methods are addressed and where further needs exist. Previous works only shed light on partial aspects of cyber resilience; none deal with the topic holistically to show what has already been well researched and where there are gaps.

Studies on cyber resilience are mostly published and presented in America, especially in the USA. Europe is in second place with approximately 30% of studies. When it comes to collaborations with different institutions, it can be seen that America, and here again especially the USA, prefers collaborations in their own country with half of the studies, while Europe, with more than two thirds, does not enter into any collaborations at all. Asia, on the other hand, is the most open to international cooperation with 50% of the studies. If you analyze the industries of the respective studies, you can see that 45% of the studies do not allow a clear classification. If you further divide this area and add up all the industries that belong to critical infrastructure, you get 55% of all studies in this area. The rate is low at less than 10% for pure IT services and sectors related to society or politics. Research fields are partly dedicated to the analysis and definition of cyber resilience; these make up around a third of all studies. The remaining studies deal with the implementation of CR in frameworks, architectures, assessment models, system modeling and technical systems. System modeling for behavior analysis accounts for a quarter of all studies and therefore represents an important area in research on cyber resilience. This area, together with assessment models, focuses on measuring cyber resilience in different contexts. System modeling as well as frameworks and architectures have a clear focus on detecting and defending against attacks. Cyber resilience in organizations can be found on the one hand in connection with frameworks but also in the analysis and survey of needs and status of cyber resilience. The preferred methods in cyber resilience studies are modeling, simulations and experiments in addition to classic literature analysis. Furthermore, the areas mentioned were compared and future research areas were identified. Measurement and adequate measurement data as well as aspects such as socio-economic factors or technologies related to e-mobility and autonomous systems are recommended research fields. Furthermore, no studies could be conducted on critical areas such as healthcare or finance, which indicates a need for research specifically on status assessment.

The studies in this SLR were collected in April 2023; a total of 80 studies were selected from 1208 studies from the ACM Digital Library, IEEE Xplore Digital Library and SienceDirect databases according to previously defined selection criteria. The studies from 2018 – 2023 are peer-reviewed, primary studies and address cyber resilience holistically and comprehensively. The results were recorded using qualitative content analysis and the collection of statistical data. The study selection and data extraction were carried out exclusively by the author, which represents a limitation and possible uncertainty in the results.

Inhaltsverzeichnis

1. Einleitung

Das Thema Cyber Resilience (CR) gewinnt immer mehr an Bedeutung. Cyber Angriffe nehmen jährlich an Zahl zu, während Cyber-Kriminelle immer professioneller werden. Bekanntgewordene 0-Day-Verwundbarkeiten werden in nahezu Echtzeit ausgenutzt. Das IT-Personal steht einer neuen Herausforderung gegenüber, einen sicheren Betrieb zu gewährleisten und gleichzeitig ein schnelles und effizientes Patchmanagement zu etablieren. Alles unter dem Aspekt das Ressourcen und Zeit begrenzt zur Verfügung stehen. Ständig wachsende Bedrohungen wie Ransomware Angriffe, Supply Chain Angriffe, Datendiebstahl oder Social Engineering aber auch gezielte Angriffe von Advanced Persistent Threats (APT) machen die Notwendigkeit einer Security Strategie deutlich [1] [2]. Klassische Methoden wie Risikomanagement und damit einhergehend das Absichern erkannter Risiken ist in der heutigen Zeit mit immer neueren Bedrohungen, die sich im Auftreten und Auswirkung nicht immer bestimmen lassen, oft unzureichend. Auf der anderen Seite werden Systeme immer komplexer und durch vermehrte Vernetzung werden Abhängigkeiten nicht erkannt oder falsch eingeschätzt. Das Ergebnis ist entweder eine ungenügende Behandlung von Risiken oder sehr kostenintensive Sicherheitslösungen zur Absicherung möglicher Szenarien. Die Verbesserung der Cyber Resilience von komplexen Systemen kann nach der Absicherung aller wirtschaftlich vertretbaren Maßnahmen den entscheidenden Faktor darstellen mit dynamischen ständig veränderten Bedingungen kosteneffizient und risikoarm umzugehen [3].

Statistica gibt in einem Dossier zum Thema Ransomware [4] ein klares Bild zum Anstieg und dem enormen Ausmaß dieser Bedrohung. Im Zeitraum Jänner – Februar 2021 waren durchschnittlich 66% aller Organisationen weltweit von Ransomware-Angriffen betroffen während Österreich die höchste Rate mit 84% aufwies. Eine weitere Messung zeigt einen Anstieg von 55,1% im Jahr 2018 auf 71% im Jahr 2022, in welchen Organisationen von Ransomware betroffen waren. Die weltweite Anzahl von Malware-Angriffen, gemessen von 2015-2021, ist zwar von 8,2 auf 5,4 Milliarden jährlich gesunken zeigt aber in 2018 einen Anstieg von 10,5 Milliarden auf. Auf der anderen Seite lässt die Anzahl von Ransomware-Angriffen seit 2016 wieder eine steigende Tendenz aufweisen, diese hat sich von 304,6 Millionen in 2020 auf 623,3 Millionen in 2022 verdoppelt.

Die Dringlichkeit einer verbesserten Resilienz von IT-Infrastrukturen wurde durch die EU (European Union) erst unlängst durch zwei Richtlinien unterstrichen. Mit der Richtlinie DORA (Digital Operational Resilience Act) werden verpflichtende Vorgaben zur CR im Finanzsektor umgesetzt und mit der NIS-2 Richtlinie die bestehende NIS-1 Richtlinie weiter verbessert und nachgeschärft [5] [6]. Diese und ähnliche EU-Vorgaben [7] zielen darauf ab den europäischen Raum und deren kritische Infrastrukturen vor Cyber-Angriffen und anderen Bedrohungen zu stärken und die entsprechenden Organisationen und Institutionen in die Pflicht zu nehmen.

Bestehende Systematische Literatur Analysen (SLR) beschäftigen sich mit einem Teilaspekt der CR oder haben den Fokus klar auf eine spezifische Branche wie die der kritischen Infrastrukturen. Eine Erhebung früherer Arbeiten kann in die Bereiche Studien zu CR-Frameworks, Awareness und Trainings, CR in kritischen Infrastrukturen und Supply Chain eingeteilt werden.

Nachfolgende Studien beschäftigen sich mit bestehenden CR-Frameworks und CR-Architekturen in unterschiedlichen Ausprägungen und Zielen. [8] untersucht existierende CR-Frameworks für Cyber Physical Systems (CPS) in Smart Cities. Es wird untersucht, inwieweit einzelne Aspekte von CPSs untereinander in Verbindung stehen, um die CR vor allem in Bezug auf digitaler Forensik und Incident Response zu verbessern. In [9] werden 5 CR-Frameworks identifiziert und mit dem Impact-Wave Analogy (IWA) Framework bezüglich Flexibilität und Anpassbarkeit verglichen. Das Ergebnis zeigt, dass die Frameworks Human Resilient Behaviour, BFT++, AWaRE, Network and Information Security (NIS) Direktive, NIST und IWA unterschiedliche Funktionsbreiten aufweisen, wobei IWA und AWaRE auch reaktive Komponenten und das IWA-Framework Schwächen im Bereich Entwicklung und Implementierung aufwiesen. In [10] aus 2020 wird eine Analyse der Literatur zu Cyber Resilience Frameworks (CRF) vorgestellt. Diese umfasst die

Darstellung von Forschungsarbeiten über die Zeit, wobei ein starker Anstieg ab 2013 zu erkennen ist. Es wurden Forschungsbereiche, Institutionen und deren Kooperationen sowie Angriffsklassen und deren Anwendungsgebiete analysiert und gegenübergestellt. Die Einordnung der CRFs nach den Wave-Analogy-Modell-Kategorien zeigt das die meisten der Kategorie „Pre-Event Knowledge Management“ zugeordnet werden können gefolgt von „Security of Cyber Physical Systems“. Diese Betrachtung zeigt das die meisten Frameworks sich auf die operativen Aspekte fokussieren und Governance sowie Soziale Themen eher selten adressiert werden. Mit sozialtechnischen Systemen hingegen befasst sich [11] indem CR-Management-Frameworks auf deren Defizite hin untersucht und analysiert werden. Die SLR in [12] untersuchte Resilience in Enterprise Architekturen, der Focus liegt darauf wie Resilience definiert und analysiert wird, welche Arten von Resilience betrachtet werden, wie diese gemessen werden und welche Charakteristiken sie aufweisen. Es zeigte sich das Resilience auf unterschiedlichen Ebenen gesehen wird, auf Enterprise Architekturebene auf Organisationsebene sowie auf Informationssicherheitsebene, wobei erstgenannte nachfolgende Ebenen jeweils einschließen. Die Arten von Resilience umfassen neben den oben genannten Ebenen aber auch Domänen wie Kritische Infrastrukturen, bzw. die rein technische Sicht auf CR. Interessant war die Erkenntnis das der Focus auf die CR-Phase der Wiederherstellung liegt und Studien die CR-Phase der Anpassung an Ereignisse eher vernachlässigen.

Kritische Infrastrukturen und Behörden sind ein beliebter Bereich in dem CR erforscht wird. [13] adressiert CR in aktuellen Studien bezüglich kritischer Infrastruktur in der Wasser- und Abwasserwirtschaft. Wohingegen [14] eine SLR über Resilience von sogenannten Active Distribution Systems (ADS) in Stromnetzen vorstellt. Hierbei werden 3 Aspekte adressiert. Erstens der Überblick über wetterabhängige Szenarien, eine Übersicht der Härtung von ADS, unterschiedliche Modelle und zukünftige Pläne. Zweitens werden Studien klassifiziert nach Arbeiten mit Fokus auf Planung, Betrieb und der Mix aus beiden. Und drittens werden die wichtigsten Beiträge, meistverwendeten Modelle sowie Funktionen der untersuchten Studien herausgehoben. Das Ergebnis zeigt, dass in Bezug auf Naturkatastrophen quantifizierte Modelle nötig sind und weitere Verbesserung der Modelle zur Planung und Betrieb mit Fokus auf schnelle Wiederherstellbarkeit stattfinden sollten. Außerdem wurde die Kosten-Nutzen-Analyse von resilienten Frameworks noch wenig erforscht und stellt ein künftiges Forschungsfeld dar. Ebenso in [15] wird die Resilience kritischer Infrastrukturen analysiert wobei die Bedrohungen jeglicher Natur herangezogen werden und neben Naturkatastrophen, veraltete Infrastruktur, Kontamination von Wasser oder kaskadierende Fehler auch Terror- und Cyber-Angriffe inkludiert. Die Arbeit geht einen Schritt weiter und stellt mögliche Strategien für Regierungen vor die einerseits die Entwicklung von Fähigkeiten im privaten wie im öffentlichen Sektor bz. Resilience vorsieht. Diese umfassen Fähigkeiten in der Governance, im technischen und betrieblichen Bereich, wobei schneller und zielgerichteter Informationsaustausch, Risikopläne, aktuelle und gewartete IT-Infrastrukturen vordergründig genannt werden. Andererseits ist die Soziopolitische und wirtschaftliche Situation ebenso wenig zu vernachlässigen speziell im städtischen Bereich aber auch auf mögliche Terroristische Aktivitäten hin. Außerdem wird als wichtiger Faktor die Beobachtung der Entwicklung von Makro-Ökonomischen Indikatoren empfohlen. Eine allgemein gehaltene Studie wird in [16] abgehandelt, die aktuelle Forschungstrends, deren regionale Verbreitung sowie Methoden zur Erreichung von CR in kritischen Infrastrukturen aufzeigt. Diese zeigt unterschiedliche Entwicklungen von Methoden zur Infrastruktur-Resilience-Erhebung, Cyber-Resilience-Assessments und leistungsorientierte Infrastruktur-Resilience-Methoden, welche die Leistung bei einer Unterbrechung bewerten, auf.

Cyber Security Trainings und Awareness sind ein wichtiger Bestandteil, um einen Sicherheitsvorfall zu vermeiden sowie diesen möglichst schnell zu erkennen. Gerade ein schnelles Erkennen und richtiges Handeln kann sich Signifikat auf die Folgen für ein Unternehmen auswirken. In [17] werden Cyber Security Trainings in den Branchen Luftfahrt, Energie und Kernkraft sowie Trainings allgemein zu "Critical Infrastructure Protection" beleuchtet. Es werden sowohl Trainingsmethoden und Lösungen als auch KPI's zur Messung deren Effektivität erhoben. In [18] wird ebenso eine SLR zu Security Trainings vorgestellt, hier allerdings mit Fokus auf Industrial Internet of Things (IIoT). In dieser Arbeit werden Konzepte von Security Trainings und Techniken zur Erhöhung des Awareness Levels, den Industrie-Kontext der Studien sowie der Nutzen von groß angelegten Trainings herausgearbeitet.

Die Studien [19] [20] aus 2015 zeigen sowohl die Notwendigkeit als auch die fehlende Forschung zu CR im Supply Chain Umfeld. Es gibt keine spezifischen Frameworks, um Cyber-Risken und Risiken in Lieferketten abzudecken. Bestehende Supply Chain Frameworks sollten um Aspekte wie Zusammenarbeit und Unternehmenskultur erweitert werden. Generell sollte das Thema um Cyber-Risk und Resilience in Lieferketten breiter erforscht werden. Auch in [21] wird auf das Thema Cyber-Risk und Supply Chain im Rahmen einer SLR erarbeitet. Es zeigt sich das Risiken bezüglich menschlichen Verhaltens einerseits als kritisch identifiziert werden und auf der anderen Seite dieses Thema in der Literatur stiefmütterlich behandelt wird und sich vielmehr auf technische Aspekte (Daten, Applikationen und Netzwerke) fokussiert. Es wird auch der Bedarf von Studien zu Cyber-Risiko-Awareness und spezifische Risikothemen aufgezeigt. Weiteres werden Strategien für ein übergreifendes Risikomanagement sowie empirische Modelle für Supply-Chain-CR empfohlen.

Die Abhandlung zeigt, dass eine SLR die das Thema CR ganzheitlich betrachtet nicht vorliegt. Auch wenn Teilaspekte wie Frameworks hinsichtlich Branchen und Methoden erarbeitet wurden oder auch CR in der kritischen Infrastruktur gut beleuchtet scheint, können mit einer ganzheitlichen Betrachtung von CR mögliche Trends, offene Forschungsfelder oder vernachlässigte Branchen herausgehoben werden. Diese Arbeit soll diesen Bedarf abdecken und einen Beitrag zur ganzheitlichen Sicht von CR in der aktuellen Forschung leisten.

Die vorliegende Arbeit ist wie folgt gegliedert. Das Kapitel 1 beschreibt die Motivation und Wichtigkeit zu einer SLR zu Cyber Resilience. Es werden weiteres frühere Arbeiten und SLRs mit Bezug auf CR zusammengefasst. Kapitel 2 beschreibt die Definitionen von Cyber-Resilienz im allgemeinen sowie CR und andere Konzepte die mit CR in Verbindung gebracht werden. Kapitel 3 befasst sich mit Methodik der vorliegenden SLR inklusive Suchstrategie, Auswahlkriterien und Datenmanagement, Studien-Auswahlprozess, Datenextraktion und Auswertung sowie Limitierungen. In Kapitel 4 finden sich die Auswertungen der Daten in beschreibender und grafischer Darstellung wieder. Kapitel 5 widmet sich der Diskussion der Ergebnisse und Kapitel 6 kommt mit der Zusammenfassung und dem Ausblick zum Abschluss der Arbeit.

2. Begriffsdefinition Cyber Resilience

Die Definition von CR findet sich in der Literatur oft unterschiedlich dargestellt und unterschiedliche Konzepte werden einerseits als integraler Bestandteil der CR oder aber als eigenständiges Modell beschrieben. Meistens ist die jeweilige Definition in Bezug auf eine Situation oder Bereich ausgelegt. Im folgenden Kapitel soll eine kompakte Abhandlung zu den wichtigsten Definitionen sowie Konzepten gegeben werden.

Das Wort Cyber leitet sich als eine verkürzte Form vom englischen Wort cybernetics ab. Oder auch Kybernetik, die *„Wissenschaft von den Steuerungs- und Regelungsvorgängen“* [22], die Systeme unterschiedlicher Art *„auf selbsttätige Regelungs- und Steuerungsmechanismen hin untersucht.“* Der Wortursprung entspringt aus dem griechischem *„kybernētikḗ“* für Steuermannskunst bzw. *„kybernḗtēs“* für Steuermann [23]. Es wird als Wortbildungselement verwendet und *„drückt aus, dass das mit dem Zweitglied Bezeichnete auf computergesteuerte Prozesse und durch diese generierte virtuelle Welten bezogen bzw. auf solche zurückzuführen ist*“ [24]. Das National Institute of Standards and Technology (NIST) besagt das Cyber sich auf Informations- und Kommunikationsnetzwerke bezieht [25]. Ebenso bezeichnet International Organization for Standardization (ISO) den Cyberspace als eine verbundene digitale Umgebung aus Netzwerken, Service, Systemen, Menschen, Prozessen und Organisationen. In [26] wird Cyber als Bestimmungswort gesehen, um die Zugehörigkeit bzw. Einbeziehung des Cyberspace oder die Anbindung an ein Kommunikationsnetzwerk zu bezeichnen. Ganz allgemein wird das Wort Cyber mit dem Internet oder vernetzen Systemen assoziiert.

Der Begriff Resilienz bzw. Resilience hat seinen Ursprung im Lateinischen *„resilire“* und bedeutet zurückspringen. Der Duden bezeichnet Resilienz im Sprachgebrauch der Psychologie als *„psychische Widerstandskraft; Fähigkeit, schwierige Lebenssituationen ohne anhaltende Beeinträchtigung zu überstehen*“ [27]. Auch die Brockhaus Enzyklopädie hat den gleichen Wortsinn und bezeichnet es als die *„psychische Widerstandsfähigkeit von Menschen, die es ermöglicht, selbst widrigste Lebenssituationen und hohe Belastungen“ [28]* zu überstehen. Die Encyclopedia Britannica führt den Begriff ökologische Resilienz und beschreibt diese als Fähigkeit eines Ökosystems seine Funktionen aufrechtzuerhalten bzw. wiederherzustellen wenn es durch Störungen Schaden erleidet. Der Begriff Robustheit wird als synonym mit denselben Eigenschaften verwendet [29]. Bezugnehmend auf Organisationen bezeichnet die European Union Agency for Cyber-Security (ENISA) mit Resilienz die Fähigkeit die Auswirkungen einer Geschäftsbeeinträchtigung zu absorbieren und ein als Minimum definiertes Level an Leistung zu bringen [30]. Die EU Richtlinie 2022/2557 *„über die Resilienz kritischer Einrichtungen“* lässt die Stadien der Resilienz erkennen indem sie sie als *„die Fähigkeit einer kritischen Einrichtung, einen Sicherheitsvorfall zu verhindern, sich davor zu schützen, darauf zu reagieren, einen solchen abzuwehren, die Folgen eines solchen Vorfalls zu begrenzen, einen Sicherheitsvorfall aufzufangen, zu bewältigen und sich von einem solchen Vorfall zu erholen“* bezeichnet [7]. Die Definition von NIST und ISO zeigt ebenfalls die Stadien der Resilienz indem sie sie als Fähigkeit bezeichnet sich auf veränderte Bedingungen wie Angriffe, Unfälle oder natürliche Ereignisse vorzubereiten, sich diesen anzupassen, diesen zu widerstehen und bei Unterbrechungen sich rasch zu regenerieren [31]. Beide Institutionen bezeichnen auf der anderen Seite den Begriff Robustheit bzw. Robustness als Fähigkeit von Systemen seien Funktionen zuverlässig und sicher aufrechtzuerhalten wenn diese unter einer Vielzahl an Vorkommnissen beeinträchtigt werden [32] [33]. Dies lässt erkennen das die Grenzen der Begrifflichkeiten verschwimmen und in bestimmten Situationen als Synonym verwendet werden. Auch in [3] wird aufgezeigt das Robustheit aber auch Risiko-Management den Fokus auf das Vermeiden von Schäden bzw. deren Begrenzung bei Aufrechterhaltung des Betriebes haben. Resilienz zeichnet sich durch die Besonderheit einer schnellen Wiederherstellung und einer Anpassung an die Situation aus. Bezogen auf Organisationen scheinen die ähnlichen Aspekte des Business Continuity Management (BCM) offensichtlich und in der Literatur vermischen sich die Definitionen und Beschreibungen entsprechend des betrachteten Themas. [34] besagt *„Business Continuity bringt uns dorthin zurück, wo wir vor einem Ereignis waren, während organisationale Resilienz dabei hilft, sich als Organisation weiterzuentwickeln und zu wachsen.“* Im Gegensatz dazu wird im BSI Standard 200-4 BCM sehr wohl die Fähigkeit der Weiterentwicklung als Notwendigkeit angesehen, wobei hier die organisatorische Resilienz im Vordergrund steht [35]. Zu einem ähnlichen Schluss kommt auch [36], Resilienz wird je nach Gesichtspunkt unterschiedlich interpretiert wenn es um den Vergleich mit Security geht und ob diese getrennt von Resilienz zu sehen ist oder doch als integraler Bestandteil.

Der Begriff Cyber Resilience erweitert sich in der Definition, um die Dimension das die Resilienz abhängig von oder durch *„Cyber Ressources*“ [37] ist. Im Unterschied zur Cyber Security , welche als Schutz vor Cyber-Angriffen bzw. Cyber-Risiken bezeichnet wird [38] [39] [40] [41], umfasst CR zusätzlich ein viel breiteres Spektrum und findet für komplexe Systeme und Strukturen seine Anwendung. [26] und [42] beschreiben, dass CR wie Cyber Security alle Bedrohungen gegen Cyber-Ressourcen adressieren, aber der Fokus bei CR liegt vor allem im Umgang mit besonders fortschrittlichen und gefährlichen Angreifern die auch als APTs bezeichnet werden. Wenn Bedrohungen dieser Art standgehalten werden können, können auch eine breite Menge anderer Bedrohungen abgewehrt werden. CR wird zugeschrieben, schnell auf nicht vorhersehbare und schwere Ereignisse reagieren zu können und die Funktionalität des Systems oder der Organisation auf einem definierten Minimum aufrecht zu erhalten. [42] beschreibt CR in einer Analogie zum menschlichen Körper, der sich von Krankheiten oder Unfällen erholen kann, aber nicht uneingeschränkt belastbar ist und bei sehr schweren Vorfällen unter Umständen sich auch nicht vollständig regeneriert.

Ein Ziel von CR ist sich an Bedingungen anzupassen bzw. sich zu entwickeln. Ein sehr ähnliches Konzept ist die Anti-Fragilität. Kurz gesagt geht es darum, dass ein System sein Verhalten dynamisch anpasst wenn die Umstände es verlangen. Die Eigenschaften von Anti-Fragilität sind anpassen und entwickeln, wobei es bei Robustheit um Standhalten und Resilienz geht. Ein sehr ähnliches Konzept ist das der Wandelbarkeit (changeability) wo Resilienz durch Verlässlichkeit und Wandelbarkeit erreicht wird [26]. Diese Konzepte werden in [26] den Evolvability Design Prinzipien zugeordnet, welche sich für das Design von Cyber Resilience Architekturen eignen und im beschriebenen CR-Design-Framework Eingang finden.

Dieses CR-Design-Framework zusammen mit [43] beschreibt das Cyber Resiliency Engineering Framework (CREF) . Auch NIST beschreibt das gleiche Framework im Standard SP 800-160 [42]. Es werden CR-Ziele, Vorgaben (Objectives) und Praktiken vorgestellt, ein Threat Model für CR und anwendbare Architekturen. Die Ziele sind in den Status Erkennen (Anticipate) , Standhalten (Withstand), Wiederherstellen (Recover) und Weiterentwickeln (Evolve) definiert. Um diese zu konkretisieren sind die als Vorgaben definierten Eigenschaften „*understand, prepare, prevent, constrain, continue, reconstitute, transform,“* und *„re-architect“* auf Systeme oder Business Modelle anzuwenden, um die Resilienz zu verbessern. Und um wiederum diese zu erreichen, werden CR-Praktiken (Techniques bzw. Practices) wie zum Beispiel Monitoring, Rechteverwaltung oder Redundanz angewendet. Abbildung 1 zeigt das Zusammenspiel von Zielen, Aufgaben, Praktiken zusammen mit den Design Prinzipien.

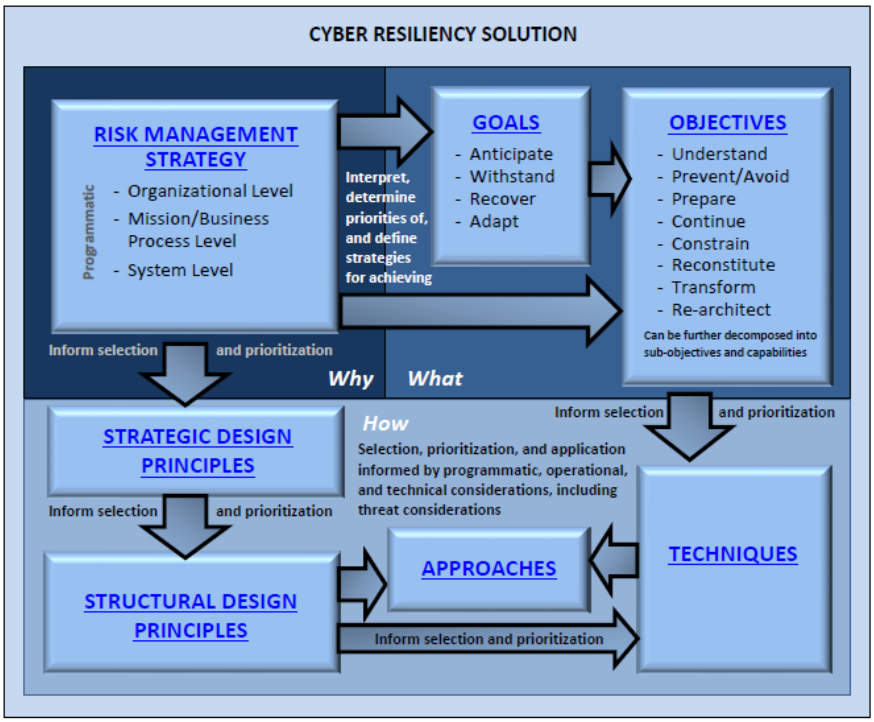

Abbildung 1 : CREF Übersicht [42]

[3] unterteilt die Erreichung von CR-Systemen in Metrik-basierenden und Model-basierenden Ansätzen. Model-basierende Ansätze wie das CSRF verwenden physische Modelle und erfordern das der Kontext des zu schützenden Systems evaluiert und einbezogen wird. Der Metrik-basierende Ansatz misst und überwacht Eigenschaften von Systemen, um deren Performance und damit die CR-Fähigkeit zu messen. Metrik-basierende Ansätze haben aufgrund der fehlende Standardisierung von Metriken den Nachteil das Frameworks nur individuell entwickelt werden und kaum fertige Konzepte vorliegen [3] [36]. [44] beschreibt ein Metrik-basierendes Model wo Metriken anhand der Phasen *„Plan and Prepare“, „Absorb“, „Recover from“* und *„Adopt to“* und den Bereichen *„Physische Resourcen“, „Informationen“, „Kognitiv“* und *„Sozial“* erarbeiten wurden. Der Bereich Kognitiv beschreibt die Verbindung der ersten beiden Bereiche und „Sozial“ stellt die organisatorische Struktur und Kommunikation dar.

Um die erwähnten Konzepte noch einmal anders dazustellen soll die Darstellung von Organisationen aus [34] erwähnt werden. Es wird angenommen, dass sich Organisationen im Laufe der Zeit weiterentwickeln, und zwar von einer fragilen zu einer antifragilen Organisation. Wobei fragil als nicht anpassungsfähig und daher zerbrechlich dargestellt ist. Eine robuste Organisation hingegen kann eine Reihe im Voraus geplanter Veränderungen bewältigen. Eine Resiliente Organisation kann zusätzlich auch auf unvorhergesehene Ereignisse reagieren. Und eine antifragile Organisation übersteht diese Ereignisse nicht nur sondern gedeiht durch diese und wird besser.

Die unterschiedlichen Publikationen und deren Definitionen zeigen die Komplexität der Resilienz bzw. CR auf und das durch die Verschmelzung verschiedener Konzepte CR nicht immer eindeutig definiert wird. CR hat den Zweck vernetzte Systeme unterschiedlicher Art zu schützen, und zwar auch und vor allem vor unvorhersehbaren und aggressiven Ereignissen. Aber vielmehr noch steht das Widerstehen dieser Vorfälle und die Aufrechterhaltung der Funktionen im Fokus. Ein weiterer wichtiger Aspekt ist das CR davon ausgeht das ein System nie vollständig abgesichert ist und auch kompromittiert sein kann. Das unterscheidet CR von den klassischen IT-Security oder Cyber Security Konzepten.

3. Methodik

Die vorliegende SLR ist nach der PRISMA 2020 Methode [45] durchgeführt. Um die Vollständigkeit und Nachvollziehbarkeit zu gewährleisten finden die Checklisten für Protokolle [46], Abstract [45] und SLR [47] Berücksichtigung, diese finden sich in Anhang A wieder. Die SLR wurde mittels SLR-Protokoll sorgfältig geplant und dem Betreuer dieser Diplomarbeit zur Qualitätssicherung vorgelegt. Da PRISMA 2020 für SLRs medizinischer Studien konzipiert wurde, können nicht alle Checklisten Punkte angewendet werden, des Weiteren wird das Protokoll nicht veröffentlicht. Abweichungen in den Checklisten aufgrund der medizinischen Spezifika sind dokumentiert und mit den Methoden nach Kitchenham [48] abgeglichen, um eine weitmöglichste Umsetzung zu gewährleisten.

3.1. Forschungsfragen und Motivation

Die Wichtigkeit einer SLR ist weitgehend in der Einleitung abgehandelt. Bestehende SLRs zum Thema CR sind nur sehr spezifisch und befassen sich mit Details einzelner Aspekte. Einen Vergleich von Branchen, Forschungsgebieten, Methoden, Techniken sowie aktueller Trends findet man in aktueller Literatur nicht. Daher stellt diese Arbeit einen wichtigen Beitrag dar, um fehlende Forschungen zum Thema CR sichtbar zu machen und Trends sowie Lücken aufzuzeigen.

Es sind 4 Forschungsfragen definiert, eine Übersicht findet sich in Tabelle 2 wieder. Diese sind nach den PICOC Kriterien [48] entwickelt, die Darstellung dazu zeigt sich in Tabelle 1.

PICOC Kriterien	**Beschreibung**	**Forschungsfragen**
Population	CR, ganzheitliche Sicht gegen Cyber Angriffe und Bedrohungen	Q1, Q2
Intervention	Domänen (Forschungsbereich), Branchen, Methoden und Techniken zu CR in wissenschaftlichen Arbeiten	Q1, Q2
Comparison	Domänen, Methoden und Techniken je Branche	Q1, Q2
Outcome	Aktuelle Trends in CR, mögliche künftige Forschungsfelder, Abdeckung Domänen und Branchen	Q3, Q4
Context	Akademische Studien	-

Tabelle 1 : Forschungsfragen nach PICOC [48]

In Q1 sollen Domänen beziehungsweise Forschungsfelder sowie Methoden und Techniken erhoben werden. Welche Bereiche werden in aktuellen Forschungen adressiert und in welcher Häufigkeit? Dies können Studien zu technischen Umsetzungen oder organisatorischen Frameworks sein oder ob CR in Umwelt, Politik und kulturelle Einflüsse betrachtet wird. Der zweite Teil der Frage befasst sich mit den verwendeten Methoden und Techniken, die eingesetzt werden. Was sind die verbreiteten Techniken und ist eine Verbindung zu Forschungsfeldern oder Branchen (Q2) zu erkennen? In Zusammenhang mit den Domänen aber auch Methoden können auch fehlende Studienbereiche gemäß der analysierten Literatur aufgezeigt werden.

Q2 beschreibt welche Branchen in Studien adressiert werden. Dabei sollen Klassen und Unterklassen einen Überblick über besonders häufige, aber auch vernachlässigte Branchen aufzeigen. Die Frage soll auch Erkenntnis darüber bringen warum diese gewählt wurden und welche Unterschiede zu erkennen sind.

Mit Q3 wird die Motivationen in aktuellen Forschungen erhoben. Welche Risiken und Bedrohungen werden behandelt und können hier Parallelen zu Branchen und Forschungsfelder gezogen werden. Werden staatliche oder behördliche Vorgaben berücksichtigt? Steht der Schutz von Systemen im Vordergrund oder sind höhere Ziele wie Menschenleben oder die Stabilität der Gesellschaft ausschlaggebend?

In Q4 soll schließlich aufzeigen welche Trends zu erkennen sind. Gibt es hier über die Zeit, über Branchen oder Forschungsfelder erkennbare Trends? Was sollen künftige Forschungsfelder sein? In welchen Regionen ist die CR-Resilience-Forschung besonders aktiv und können Aussagen bezüglich Zeit oder Branchen getroffen werden? Diese Frage wird auch Parallelen zu den anderen Forschungsfragen aufzeigen, wie Forschungsfelder zu Domänen.

Q1:Welche Domänen, Methoden und Techniken werden in aktuellen Forschungen zu Cyber Resilience behandelt?
Q2:Welche Branchen werden in Studien zu CR vorrangig adressiert und warum?
Q3:Was sind die Motivationen, um CR zu erforschen?
Q4:Welche Trends sind bz. Cyber Resilience zu erkennen?

Tabelle 2 : Forschungsfragen

3.2. Suchstrategie und Datenquellen

Für die Erhebung der Studien werden die Datenbank ACM Digital Library, IEEE Xplore Digital Library und ScienceDirect herangezogen.

Die Suchstrings sind je Datenbank wie in Tabelle 3 angeführt definiert. Die Anpassung der Suchstrings sind an die optimale Trefferquote je Datenbank angepasst. Aufgrund eingeschränkter Ressourcen wurde die Suchstrategie auf ein Ergebnis von ca. 1000 Artikel angepasst. Des Weiteren gibt es je Datenbank starke Unterschiede ob nach dem zusammenhängenden Suchstring "Cyber Resilience" oder nach den Wörtern „Cyber“ und „Resilience“ gesucht wird. Ebenso gibt es starke Schwankungen ob über alle Daten oder nur Titel und Abstrakt gesucht wird. Die Suche ist unter Berücksichtigung dieser Aspekte optimiert, um eine adäquate Anzahl an Studien je Datenbank zu erzielen.

Die Suche wurde im Mai 2023 durchgeführt und hat für die Datenbank ACM 615 Artikel, für IEEE 402 Artikel und für ScienceDirect 191 Artikel als Ergebnis gebracht.

Datenbank	Abfragesyntax
ACM Digital Library	""query"": { Title:(cyber resilience) AND Abstract:(cyber resilience) } ""filter"": { ACM Pub type: Proceedings, Article Type: Research Article, E-Publication Date: (01/01/2018 TO 12/31/2023), ACM Content: DL }
IEEE Xplore Digital Library	(""All Metadata"":""cyber resilience"") Zusätzliche Einschränkungen (in der Ergebnisübersicht): Year: 2018-2023 Journals and Conferences
ScienceDirect	Year: 2018-2023; Find articles with these terms: “cyber resilience”; Article Type: Research Article

Tabelle 3 : Abfragesyntax

3.3. Auswahlkriterien und Datenmanagement

Für den Auswahlprozess wurden die Auswahlkriterien anhand 100 zufällig gewählter Studien entwickelt. Dies hat insbesondere Auswirkung auf die inhaltbezogenen Ausschlussgruppen. Die Studien sind Primärstudien, Bücher oder Sekundärstudien sowie Reviews werden nach Möglichkeit bereits bei der Suche ausgeschlossen. Um die Qualitätskriterien zu erhöhen, werden nur Studien die Peer-Reviewed sind zugelassen. Im Zuge der Entwicklung der Suchstrategie wurde festgestellt das die Menge an möglichen Studien keine großen Zeitspannen zulassen, daher ist der Zeitrahmen auf 2018 – 2023 eingeschränkt. Die Studien dürfen nur die Sprache Deutsch oder Englisch aufweisen. Des Weiteren werden Duplikate in den unterschiedlichen Abschnitten des Auswahlprozesses entfernt. Die Studien der ausgewählten Datenbanken sind weiters öffentlich zugänglich oder über den Studienzugang der FH St. Pölten zu beziehen, gesperrte Inhalte werden nicht gesondert angefordert.

Die inhaltbezogenen Ausschlussgruppen sollen sicherstellen, dass der Inhalt sich auf die Resilience / Wiederstandfähigkeit vor Cyber-Angriffen bezieht. Im Zuge der Entwicklung der Auswahlkriterien wurde aufgrund der allgemeinen Forschungsfragen und daher sehr allgemein gehaltenen Suche festgestellt, dass eine sehr große Anzahl der Studien auswählbar ist. Daher werden folgende Ausschlussgruppen aufgestellt, um die Anzahl der zu analysierenden Studien auf unter 90 zu begrenzen.

Ausschlussgruppe 1: kein oder zu wenig Bezug auf Cyber Resilience

Die Studien haben entweder keinen Bezug zu Cyber Resilience, diese umfassen das Thema nicht ganzheitlich oder CR wird als Motivation der Studie genannt aber die Auswirkung auf diese wird nicht betrachtet. Hierzu seien folgende Beispiele zur Verdeutlichung genannt.

In [49] wird auf die Nutzung von Informations- und Kommunikationstechnik (IKT) und die Notwendigkeit der Etablierung einer Sicherheitskultur zur Sicherstellung der CR eingegangen. Allerdings steht die Bildung der Sicherheitskultur als solche im Fokus. [50] behandelt sicherheitsrelevante Bedrohungen in Robotik-Systemen für ein CIA-Modell (Confidentiality, Integrity, Availability), eine Behandlung der CR ist nicht gegeben. [51] entwickelt eine Risikobewertung von Bedrohungen im E-Waste-Sektor, wobei der Fokus in der Erhebung und Bewertung von Risiken steht. Auch in [52] wird ein Cyber-Risk-Framework zur Erhebung des Reifegrads von Organisationen vorgestellt. Beide Beispiele fokussieren sich auf die Risikoerhebung und betrachten nicht die Auswirkung auf CR. In [53] oder [54] ist CR ist nur ein Aspekt der behandelt wird, im Fokus steht die Resilience vor Störungen unterschiedlichster Art wie Naturereignisse, technisch bedingte Ausfälle oder Materialermüdung.

Ausschlussgruppe 2: CR ist sehr eingeschränkt oder zu spezifisch

Die Studie bezieht sich auf CR, allerdings auf einen sehr spezifischen Gesichtspunkt wie eine einzelne Schwachstelle, eine einzelne und spezifische Komponente oder einzelne spezifische Angriffe. Beispiele können wie folgt genannt werden.

Als zu spezifisch ist die Analyse des Umgangs mit der „ROCA“ Verwundbarkeit in IKT-Systemen der estländischen Regierung gesehen [55]. Als Beispiele für spezifische Angriffe kann der Schutz von Cyber-Physical-Systems (CPS) vor Denial of Service (DOS) Angriffen genannt werden [56] oder auch der Schutz von Organisationen vor Ransomware [57].

Für das Datenmanagement wird das Tool Citavi für das Importieren der Quellen aus den Datenbanken und die Auswahl der Studien für die Volltextsuche verwendet. Für die Datenextraktion und weitere Dokumentation wird Excel verwendet.

3.4. Studien-Auswahlprozess

Der Auswahlprozess findet in den Phasen Identifikation und Screening statt, wobei das Screening in 2 weiteren Stufen erfolgt. Die Phase Identifikation ist die Datenbanksuche selbst, definiert nach Suchstring je Datenbank wie in Tabelle 3 beschrieben. In dieser Phase erfolgt auch ein teilweiser Ausschluss von Sekundärstudien, die Einschränkung auf Studien die Peer-Reviewed sind sowie den Zeitraum.

Screening Stufe 1 beinhaltet die Überprüfung der Ausschlusskriterien unter Bezugnahme von Abstrakt und Titel. Eine Dokumentation der ausgeschlossenen Studien erfolgt mittels definierter Ausschlussgruppen und ist in Abbildung 2 abgebildet. Beide Phasen des Screenings erfolgen durch die Autorin selbst. Somit gibt es in dieser Phase auch keine Qualitätssicherung. Diese erfolgt erst in der 2ten Screening-Stufe durch den Betreuer. Hierbei werden nach Zufallsprinzip 10% der Studien ausgewählt, um deren Ausschluss erneut zu prüfen. Weiteres ist in der 2ten Screening-Stufe die Volltextsuche der Studien nach den gleichen Ausnahmekriterien vorgesehenen. In dieser Phase können Studien auch aufgrund der fehlenden Verfügbarkeit ausgeschlossen werden. Zusätzlich erfolgt hier der Ausschluss von Studien aufgrund der definierten Qualitätskriterien. Die Fragen aus Tabelle 4 dienen der weiteren Reduktion von Studien mit dem Ziel qualitativ hochwertige Studien für die Datensynthese zu gewährleisten.

QS1	Ist die Problemstellung zu CR eindeutig zu erkennen und wird das Thema ganzheitlich adressiert?
QS2	Sind die Ziele der Studie klar erkennbar und werden diese ausreichend adressiert?
QS3	Sind die Studien Peer-Reviewed?
QS4	Ist eine ausreichende Qualität und Genauigkeit der durchgeführten Methoden erkennbar?

Tabelle 4 : Qualitätssicherung im Auswahlprozess

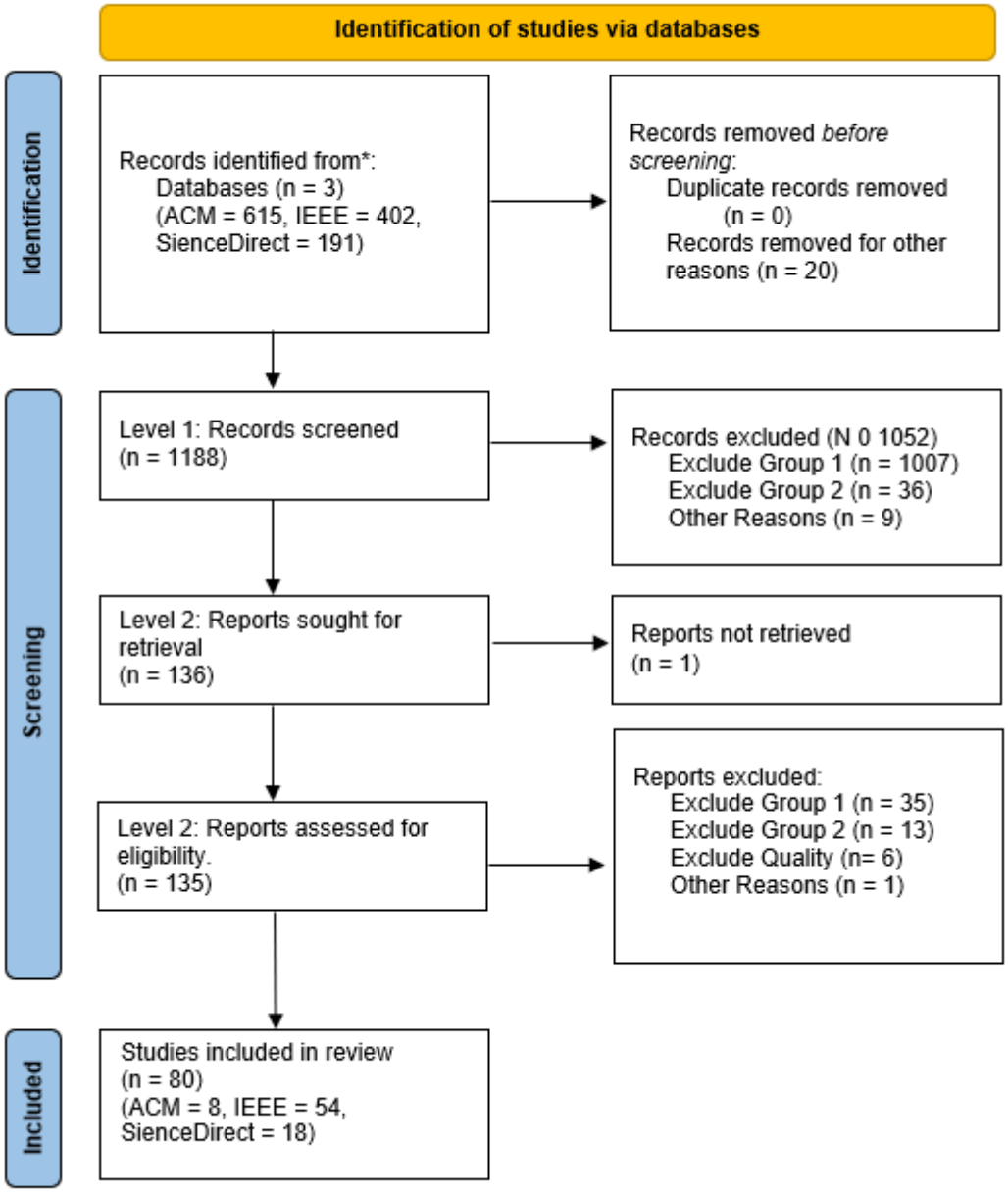

Abbildung 2 : Schema Selektionsprozess inkl. Ergebnisse nach PRISMA 2020

3.5. Datenextraktion und Auswertung

Die Datenextraktion wird im Zuge der Volltextsuche anhand eines vorab definierten Formulars manuell durchgeführt. Dieses ist nach den definierten Forschungsfragen entwickelt und wird in Anhang B abgebildet. Es erfolgt ebenso eine beschreibende Datenextraktion je Studie zum Inhalt, diese werden in einem Kapitel nach Forschungsdomänen zusammengefasst. Es erfolgt eine erneute Duplikatsentfernung, sofern diese im Screening nicht schon erfolgt ist. Da keine Datensätze bzw. quantitative Daten erhoben werden gibt es keine Strategie für das Zusammenführen und Vereinheitlichen von Daten. Sämtliche Empfehlungen zur Behandlung von quantitativen Daten finden in dieser SLR keine Anwendung. In medizinischen SLR-Studien

wird, um die Qualität der Studien zu prüfen, auf Tools zurückgegriffen. Diese sind für technische Studien nicht anwendbar. Der Faktor Risk of Bias wird nur über Qualitätskriterien behandelt, um möglichst nur qualitativ hochwertige Studien zu evaluieren.

Die Auswertung der Daten erfolgt vornehmlich qualitativ. Da keine quantitativen Daten erhoben werden bzw. vorliegen gibt es diesbezüglich nur die Auswertung der Eckdaten der Studien wie Anzahl nach Branchen oder Forschungsbereiche, Veröffentlichungsjahr und Ort sowie Konferenzen oder Zitate je Publikation.

Die Darstellung qualitativer Inhalte ist beschreibend dargestellt, ebenso der Vergleich einzelner Eigenschaften (z.B. Branchen vs. Motivation oder Methoden). Letztere sind im Sinne der Forschungsfragen vergleichend gegenübergestellt, um diese zu beantworten. Daten wie Publikationen je Jahr, Region, Autorin / Autor, Brachen usw. werden graphisch und tabellarisch dargestellt. Die Qualität der Studien werden in der Datensynthese in zwei Aspekte berücksichtigt. Zum einen sind Widersprüche einzelner Studien , sofern ersichtlich, qualitativ beschrieben. Zum anderen sind die Studien, sofern anwendbar nach deren Ranking aufgelistet bzw. dargestellt.

3.6. Limitierungen

Da die SLR im Rahmen einer Diplomarbeit stattfindet erfolgt die Suche sowie die Entwicklung der Suchstrategie, die meisten Tätigkeiten im Auswahlprozess sowie die Datenextraktion ausschließlich durch die Autorin selbst. Die Inhalte der Studien werden aufgrund des damit verbundenen Aufwands ebenso nicht auf ihre Richtigkeit geprüft. Außerdem wird kein Kontakt zu den Autoren aufgenommen. Damit sind mögliche Einbußen der Qualität der Studien gegeben. Die entwickelnden Qualitätskriterien sollen diesem weitgehend entgegenwirken. Ebenfalls aus Ressourcengründen wird verzichtet nicht veröffentlichte Studien oder Quellen aus bisherigen SLRs mit in den Auswahlprozess aufzunehmen. Dies sei nur aus Gründen der Vollständigkeit erwähnt, es wird nur eine nicht veröffentlichte Studie ausgeschlossen.

Durch die Tatsache das die Screening- und Auswahltätigkeit durch die Autorin stattfindet bedingt das eine Anfälligkeit für Bias besteht. Dieser kann sich durch unbeabsichtigte subjektive Auswahl von Studien zeigen. Ein anderer Faktor ist aber durch die sehr offene Auswahl der Studien über alle Branchen und Forschungsbereiche bedingt, dass Spezialgebiete (z.B. Militär) und spezifische Forschungen je Branchen (z.B. Implementierungen von CPS) die Auswahl durch fehlende Fachkenntnisse beeinflussen kann.

4. Systematische Literatur Analyse

4.1. Darstellung der Studien nach Geografie, Veröffentlichung und Verbreitung

Nach der Screening Stufe 2 verbleiben 80 Studien für die Datenextraktion und Auswertung. Davon sind 8 aus ACM Digital Library (ACM), 54 aus IEEE Xplore Digital Library (IEEE) sowie 18 der Datenbank von SienceDirect entnommen. Die Auflistung der Studien findet sich in Tabelle 5 wieder. In Abbildung 3 ist dargestellt wie viele Studien nach Jahren veröffentlicht wurden. Da die Suche Veröffentlichungen im Jahr 2023 nur Studien bis Ende April einschließt, ist dieses Jahr nicht repräsentativ. Es zeigt sich, dass ein steter Anstieg der Studien zu CR gegeben ist, auch wenn es in den Jahren 2019 und 2021 Einbrüche gab.

Datenbank	**Studien / Artikel Quelle**
ACM Digital Library (ACM)	[58], [59], [60], [61], [62], [63], [64], [65]
IEEE Xplore Digital Library (IEEE)	[66], [67] , [68], [69], [70], [71], [72], [73], [74], [75], [76], [77], [78], [79], [80], [81], [82], [83], [84], [85], [86], [87], [88], [89], [90], [91], [92], [93], [94], [95], [96], [97], [98], [99], [100], [101], [102], [103], [104], [105], [106], [107], [108], [109], [110], [111], [112], [113], [114], [115], [116], [117], [118], [119]
Sience Direct	[120], [121], [122], [123], [124], [125], [126], [127], [128], [129], [130], [131], [132], [133], [134], [135], [136], [137]

Tabelle 5: Studien nach Datenbanken

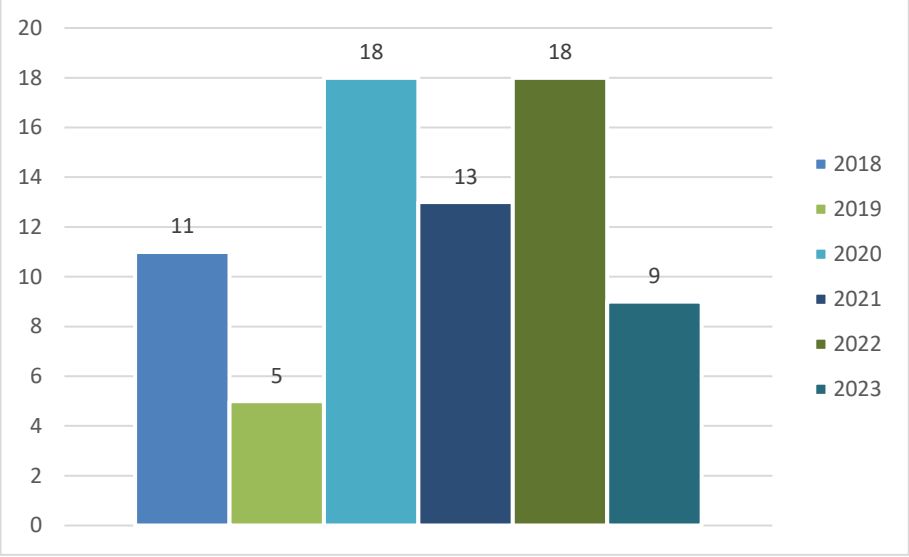

Abbildung 3 : Studien aufgelistet nach Veröffentlichung

Wie in Kapitel Methodik erwähnt soll die Bewertung der Studien nach Rankingsystem dargestellt werden. Eine Darstellung der Konferenzen und Journale mittels des CORE Rankings Portals ist aufgrund der

geringen Trefferquote nicht umsetzbar [138]. Die Publikationen können aber mittels Google Scholar Metriken dargestellt werden. Es werden der h-Index sowie der h-Median dargestellt. Der h-Index sagt aus, dass zumindest h Artikel einer Publikation mindestens h mal zitiert wurden. Damit kann dieser nie höher sein als die Anzahl der zitierten Artikel. Der h-Meridian wird aus dem Meridian des h-Core berechnet, wobei der h-Core alle Zitate der Top-Artikel oder der Artikelanzahl des h-Indexes darstellt. [139].

Tabelle 6 zeigt eine Übersicht der Studien nach Ranking-Stufen, in Anhang C findet sich die gleiche Auflistung mit den Journal- oder Konferenznamen sowie die gesamte Liste mit h-Index und h-Meridian aller Studien wieder.

h-Index	Studien / Artikel Quelle
> 100	[82], [100], [102], [112], [114], [115], [126], [131], [137]
75 - 99	[106], [120], [121], [122], [125], [127], [132], [135]
50 - 74	[63], [71], [107], [130], [133], [135]
25 - 49	[61], [62], [86],[91], [95], [103],[123], [128], [129]
0 - 24	[76], [77], [78], [79], [81], [83], [84], [87], [89], [90], [92], [93], [94], [97], [101], [105], [108], [109], [111], [113]
Nicht angeführt	[58], [59], [60], [64], [65], [66], [67], [69], [70], [74], [80], [81], [85], [88], [96], [98], [99], [104], [110], [116], [117], [118], [119], [124], [134], [136]

Tabelle 6 : Journale oder Konferenzen nach Google Scholar h-Metriken (h-Index)

Tabelle 7 zeigt die Anzahl der Zitate je Studie, wobei die meisten Artikel in einem Bereich von 0 – 19 Zitaten liegen. Eine Auflistung aller Zitate findet sich in Tabelle 26 in Anhang C wieder. Eine Darstellung der Zitate zum h-Index wird in Abbildung 4 gezeigt, hier sind die Studien mit den meisten Zitaten zum h-Index gut erkennbar. Zum Beispiel wird das Journal IEEE Access mit einem h-Index von 233, welches in der vorliegenden Arbeit 4 Studien mit Zitaten zwischen 1 und 37 hält, gezeigt was ebenfalls in der Abbildung 4 gut erkennbar ist.

Zitate von bis	Anzahl Studien	Studien / Artikel Quelle
60 - 76	3	[61], [100], [125]
40 - 59	3	[63], [79], [137]
20 - 39	9	[62], [71], [74], [77], [102], [106], [114], [127], [133]
10 - 19	14	[75], [80], [82], [85], [87], [90], [91], [92], [103], [117], [119], [123], [130], [136]
6 - 9	15	[64], [68], [72], [83], [86], [89], [95], [96], [99], [105], [111], [116], [122], [132], [135]
0 - 5	36	[58], [59], [60], [65], [66], [67], [69], [70], [73], [76], [78], [81], [84], [88], [93], [94], [97], [98], [101], [104], [107], [108], [109], [110], [112], [113], [115], [118], [120], [121], [124], [126], [128], [129], [131], [134]

Tabelle 7 : Anzahl wie häufig Studien zitiert wurden

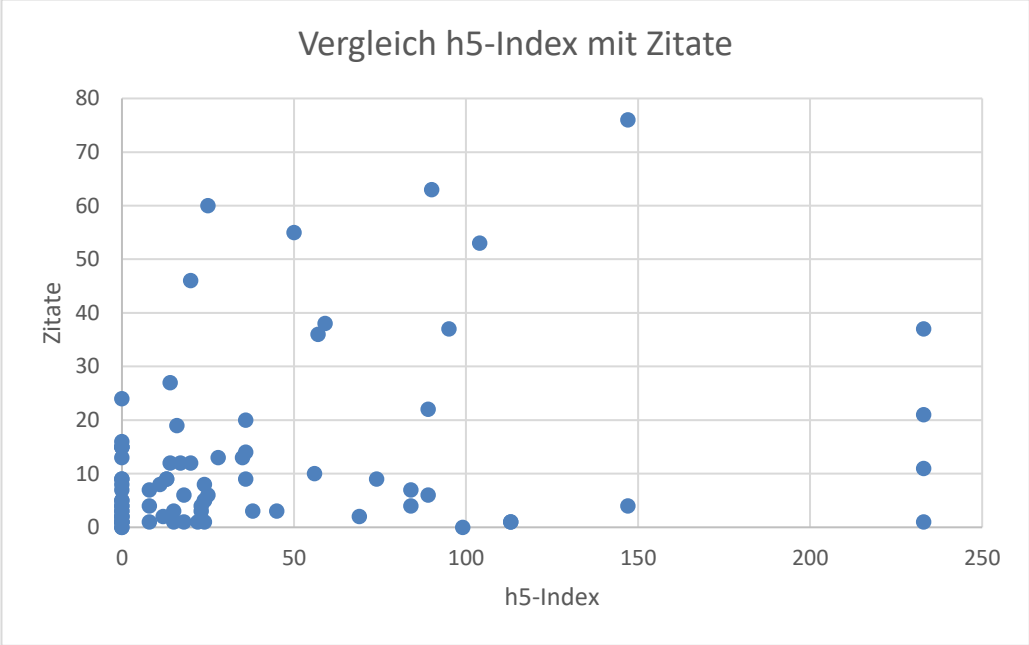

Abbildung 4 : Vergleich h5-Index zu Zitate

Die analysierten Studien nach abgehaltenen Kongressen, wie in Abbildung 5 zu sehen, zeigen das Amerika und Europa mit 29% die meisten Kongresse zur Vorstellung der Studien halten. Kongresse, die in Amerika abgehalten wurden, fanden mit einer Ausnahme alle in den USA statt. Die Gruppe Sonstige mit 33% beinhaltet 24 Studien, die nie auf einer Konferenz vorgestellt wurden sondern ausschließlich in schriftlicher Form veröffentlicht wurden sowie 2 Onlinekongresse im Jahre 2021 und 2022. Ein interessantes Detail ist, dass 13 der Kongresse in den Jahren 2020 und 2021, die im Zeichen der Corona-Pandemie standen, gehalten wurden und davon nur ein Kongress Online stattfand. In Afrika wurde nur ein Kongress abgehalten, im asiatischen Raum wurden 5 Kongresse abgehalten und in Australien fanden 2 Kongresse statt.

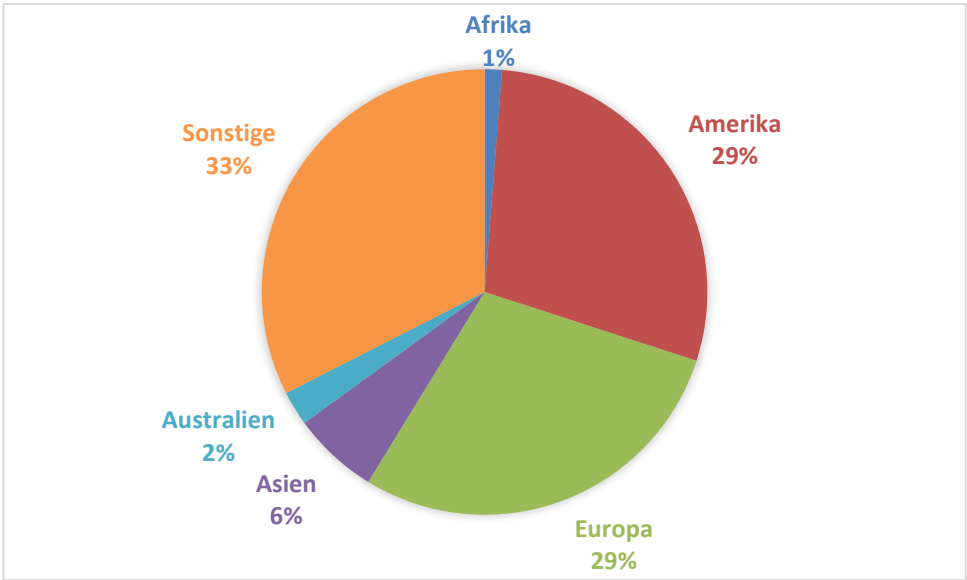

Abbildung 5 : Länder der Kongresse der analysierten Publikationen

Vergleicht man die geografische Verteilung der Kongresse dargestellt in Abbildung 6, mit denen der publizierenden Institution aus Abbildung 5 zeigt sich ein leicht verändertes Bild. Im Vergleich zu den Kongressen wo Amerika und Europa doch immerhin knapp 60% aller Kongresse halten entfallen bei der Publikationserstellung mehr als dreiviertel der Studien auf Amerika und Europa. An den Daten aus Amerika erkannt man deutlich, dass die USA im Bereich Forschungen zu IT Security und CR die Nase vorn hat. Mit 30 von 35 Studien hält sie den größten Teil in Amerika. Lediglich eine Studie wurde von der Universität de los Andes aus Kolumbien gestellt, die restlichen 4 entfallen auf Kanada. Auch insgesamt liegt Amerika mit 44% der Studien weit vorne. In Asien ist China mit 3 von 10 Studien das häufigste Land, die restlichen Studien sind im asiatischen Raum gut durchmischt. Europa hält 34% aller Studien und weist ebenfalls eine gute Durchmischung auf, 7 der 27 Studien entfallen auf das Vereinte Königreich von Großbritannien, 5 auf Italien und 3 auf Spanien. Eurasien wurde als eigene Kategorie definiert da Russland nicht nur einem Kontinent zugeordnet werden kann und hält 2 Studien. Schließlich verbleiben 2 Studien der Gruppe Sonstige, die entweder keiner Institution zugeordnet sind oder vom internationalen Konzern NXP Semiconductors initiiert wurden.

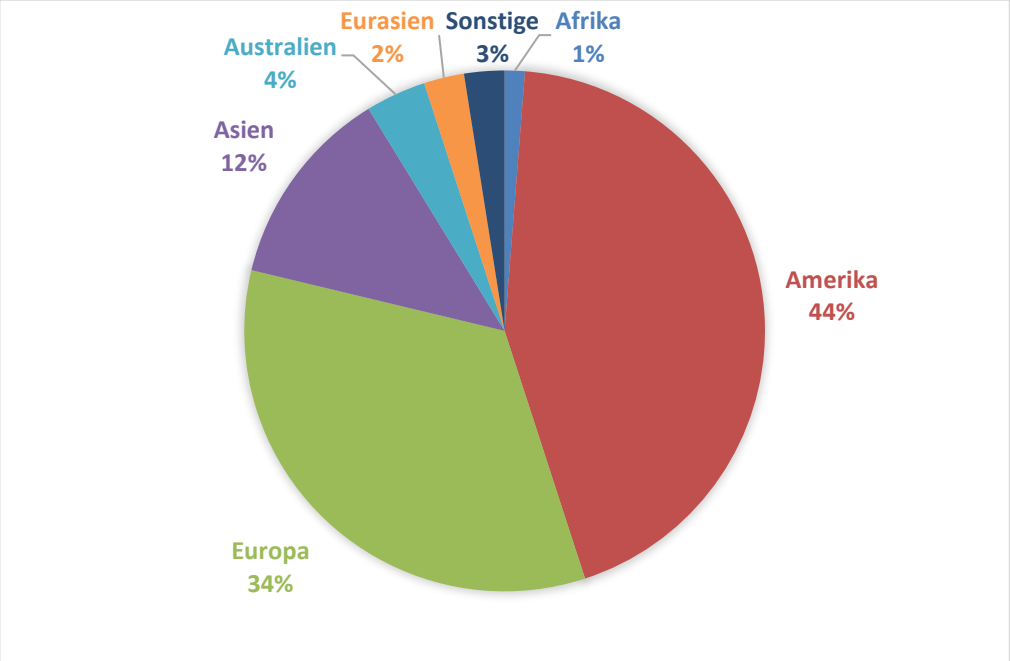

Abbildung 6 : Institutionen nach Ländern

Abbildung 7 zeigt wie Kooperationen mit anderen Institutionen verteilt sind. Dabei wird geprüft, ob eine oder mehrere Institutionen oder Universitäten im gleichen Land an einer Studie beteiligt waren. Weiters werden internationale Kooperationen, also wenn Institutionen oder Universitäten aus mehr als einem Land beteiligt sind berücksichtigt. Europa sowie Eurasien (Russland) bleiben offenbar gerne unter sich und weisen einen sehr hohen Anteil an Studien die keine Kooperationen eingehen auf. Auch die Gruppe der Sonstigen, also wo keine Institution angegeben wurde oder ein Konzern hinter der Studie steht, entwickelten ihre Studien ohne Kooperationen. Amerika weist mit knapp 50% Kooperationen im eigenen Land in dieser Kategorie die höchste Rate auf. Bei internationalen Kooperationen ist Asien mit 50% im Spitzenfeld, in Amerika und Europa forschen nur in etwa 15 % in länderübergreifenden Kooperationen.

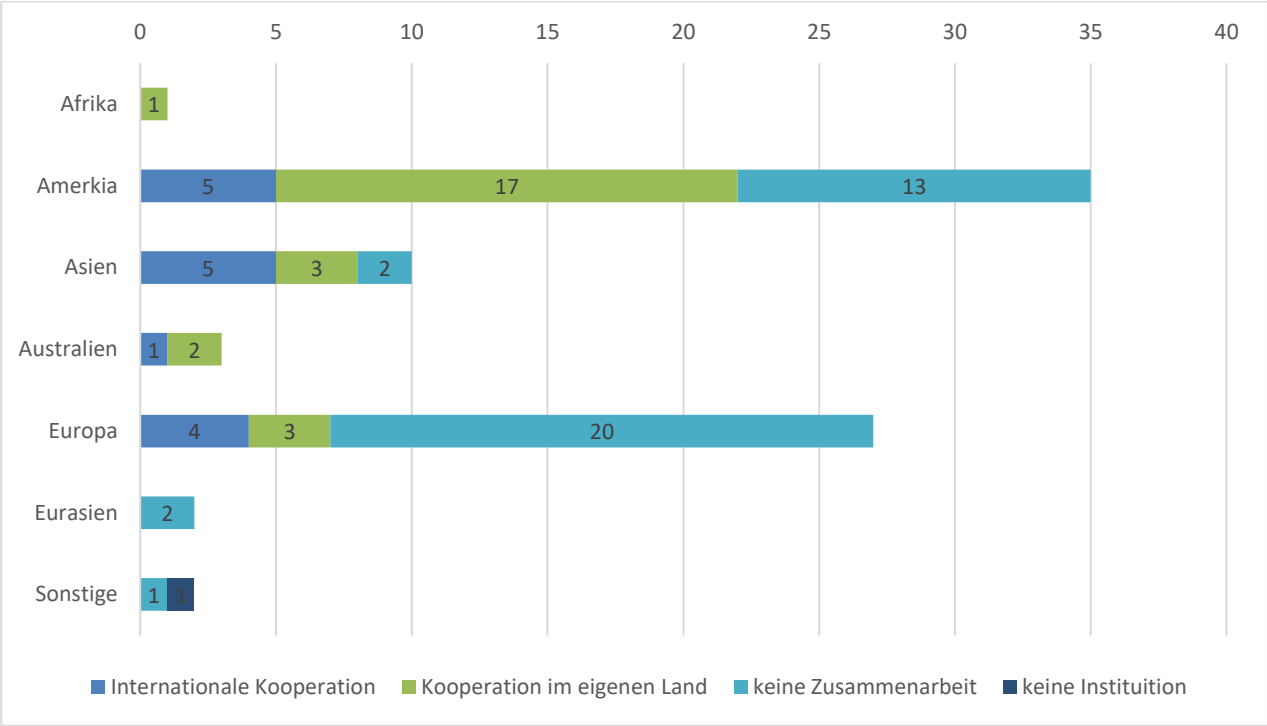

Abbildung 7 : Kooperationen mit anderen Institutionen und Länder

Autorinnen und Autoren sind mit wenigen Ausnahmen der gleichen Nationalität zuzuordnen wie die Institution selbst. Die Nationalität der Autorinnen und Autoren, und hier die der ersten Autorin / des ersten Autors der Publikation, wurde über die Informationen der jeweiligen Datenbank oder der Publikation selbst entnommen. War beides nicht aussagekräftig, wurde mittels Google-Suche nach öffentlichen Social Media Profilen gesucht. Im Zweifelsfall wurde das Land der Institution für die Nationalität herangezogen. Des Weiteren erfolgte die Analyse, sofern nicht anders angegeben immer auf Basis der erstgenannten Autorin / dem erstgenannten Autor.

Bei der Analyse der Autoren gab es keine nennenswerten Ergebnisse. Keine Autorin / kein Autor ist öfter als 4 mal vertreten, wobei hier alle Autoren je Publikationen berücksichtigt wurden. Tabelle 8 zeigt die Zitatsgruppe von über 60 Zitate nach Autoren und deren Institutionen. Hier zeigt sich das Autorinnen und Autoren von Institutionen aus den USA zu den meist zitierten gehören. Beobachtet man alle Studien bis zu 20 Zitaten stellen die USA 50% der Studien.

Autorin / Autor	Nationalität Autorin /Autor	Universität / Institution	Zitate via Google Scholar	Studien / Artikel Quelle
Abdi, Fardin	USA	University of Illinois at Urbana-Champaign	60	[61]
Chen, Yuqi	China	Singapore University of Technology and Design	55	[63]
P. Wang	USA	GE Global Research	76	[100]
Radu F. Babiceanu	USA	Embry-Riddle Aeronautical University	63	[125]

Tabelle 8 : meist zitierte Autoren

Abschließend wird die Datenextraktion zu Sponsoren beleuchtet, die aufgrund von wenig Daten nicht sehr aussagekräftig ist, aber der Vollständigkeitshalber erwähnt wird. Diese zeigt das 29 Studien oder 36% mit finanziellen Mitteln unterstützt wurden. 6 Studien wurden vom Ministerium für Energie des United States Government gefordert. Weitere Zusammenhänge zu Branche, Land oder Kooperationen konnten nicht erkannt werden.

4.2. Darstellung der Studien nach Branchen, Methoden und Techniken sowie Forschungsbereiche

Brachen sind an jenen von Statista.com [140] angelehnt und die Kategorien werden weitgehend übernommen. Die Branchen sind in Hauptkategorien und Subkategorien unterteilt. Vielen Studien kann keine eindeutige Branche zugeordnet werden, diese übergreifenden Branchen werden als solche in der Hauptkategorie geführt und in den Subkategorien unterteilt:

- Übergreifende Branchen allgemein
- Übergreifende Branchen IoT, AI, autonome Systeme
- Übergreifende Branchen Industrie und Produktion
- Übergreifend, kritische Infrastrukturen , Industrie, Produktion
- Small Medium Business (SME)

Weiters wurde die Hauptkategorie „Facility Management“ hinzugefügt, um eine klare Beschreibung der betreffenden Studien zu schaffen. Im Nachfolgenden sind die Schwerpunkte je Kategorie und Subkategorie beschrieben, eine Übersicht der dazugehörigen Studien findet sich in Tabelle 9 wieder.

Die Hauptkategorie **Facility Management** und die gleichnamige Subkategorie beschreibt Themen rund um Gebäudeverwaltung einschließlich technischer Lösungen zur Steuerung des Betriebs von Gebäuden.

Gesellschaft als Hauptkategorie hält die Subkategorien **Verbände und Organisationen** und **Bildung & Forschung**. Erstere beschreibt auf der einen Seite Organisationen, diese können öffentlich oder privat sein. Damit sind sowohl Unternehmen als auch Organisationen gemeint. Bildung und Forschung betrifft wie schon der Name sagt Forschungseinrichtungen aller Art.

Energie und Umwelt beinhaltet in vorliegender Arbeit ausschließlich kritische Infrastrukturen. Dazu gehören die Subkategorie **Energiewirtschaft**, diese beschreibt alle Branchen zur Energieversorgung wie Windkraft, Wasserkraft aber auch Atomstromerzeugung. Die zweite Subkategorie ist **Wasserwirtschaft** und beschreibt alle Themen zur Wasserversorgung und Aufbereitung.

Die Hauptkategorie **Metall und Elektronik** hält die Subkategorie **Kraftfahrzeugbau**. Damit sind Unternehmen die sich mit der Herstellung von Fahrzeugen beschäftigen gemeint. Autonomes Fahren und die zugehörige Infrastruktur findet sich in der Kategorie Fahrzeuge & Straßenverkehr wieder.

Telekommunikation, IT und Consumer Electronis beinhaltet die Subkategorien **IT-Services** und **Software**. IT-Services sind alle Dienstleistungen rund um IT-Infrastruktur. In dieser Arbeit betrifft dies das Design und den Betrieb von Netzwerken. Die Subkategorie Software beschreibt alles rund um Softwareentwicklung.

Verkehr und Logistik hält 5 Subkategorien die alle zu den kritischen Infrastrukturen zählen. **Bahn- & Schienenverkehr** beschreibt wie der Name schon sagt alle Bereiche der Bahninfrastruktur, in dieser Arbeit das Design der Bahninfrastruktur. **Fahrzeuge & Straßenverkehr** umfasst die Infrastruktur im Straßenverkehr wie Verkehrsanlagen im herkömmlichen Sinne aber auch für vernetze oder autonome Fahrzeuge, sogenannte Vehicular CPS. **Logistik und Transport** beinhaltet alle Branchen im Logistik Bereich und beinhaltet Themenfelder wie Supply Chain Sicherheit. Die Subkategorie **Luft- und Raumfahrt** beschäftigt wie der Name schon sagt mit Flugzeugbau und Flughäfen sowie der Raumfahrt. Und schließlich die Subkategorie **Öffentlicher Personenverkehr**, in dieser Arbeit sind hier Studien zur Umsetzung der Sicherheit von Public Transport auf Staatsebene inkludiert.

Die Hauptkategorie **Wirtschaft und Politik** hält die Subkategorien **Öffentliche Verwaltung** und **Verteidigung**. Öffentliche Verwaltung beschäftigt sich mit Themen zur Verwaltung auf Staatsebene wohingegen Verteidigung den Bereich rund um Militärwesen abdeckt.

Die allgemeine Hauptkategorie **Übergreifende Branchen** wird für die Darstellung der Studien in 4 Subkategorien eingeteilt. Die Subkategorie **Übergreifende Branchen Industrie und Produktion** befasst sich mit Themen im Industriesektor. Hier sind vornehmlich Bereiche rund um OT (*Operation Technologie)* und Internet of Things (IoT) sowie Produktions-CPS aber auch Kooperationen im Industrieumfeld platziert. Die Subkategorie **Übergreifende Branchen IoT, AI, autonome Systeme** halten Spezialthemen zu IoT, Artificial Itelligence (AI) und autonome Systeme im allgemeinen Sinn. Die Subkategorie **Übergreifend, kritische Infrastrukturen , Industrie, Produktion** befassen sich vornehmlich mit CPS die in Industrie und kritischer Infrastruktur eingesetzt werden können wie zugrundeliegende SCADA Netzwerke. Schließlich wird in **Small Medium Business (SME)** auf die Bedürfnisse von Klein- und Mittelunternehmen eingegangen. Tabelle 9 zeigt die Brachen in Haupt- und Subkategorien und die dazugehörten Studien.

Branchen Hauptkategorien	**Branchen Subkategorie**	**Anzahl**	**Studien / Artikel Quelle**
Facility Management	Facility Management	1	[96]
Gesellschaft	Verbände und Organisationen	5	[131], [108], [137], [110], [71]

Gesellschaft	Bildung & Forschung	2	[88], [126]
Energie und Umwelt	Energiewirtschaft	18	[59], [117], [67], [101], [66], [86], [99], [100], [85], [120], [122], [127] ,[118], [112], [124], [128], [69], [65]
Energie und Umwelt	Wasserwirtschaft	2	[115], [132]
Metall und Elektronik	Kraftfahrzeugbau	1	[111]
Telekommunikation, IT und Consumer Electronis	IT-Services	3	[109], [77], [74]
Telekommunikation, IT und Consumer Electronis	Software	2	[107], [93]
Übergreifende Branchen	Übergreifende Branchen Industrie und Produktion	6	[81], [95], [136], [134], [123], [125]
Übergreifende Branchen	Übergreifende Branchen IoT, AI, autonome Systeme	5	[80], [78], [119], [75], [135]
Übergreifende Branchen	Übergreifend, kritische Infrastrukturen , Industrie, Produktion	17	[91], [13], [133], [103], [129], [98], [89], [61],[62],[60], [68], [83], [87], [63], [58], [79], [92]
Übergreifende Branchen	Small Medium Business (SME)	5	[72], [70], [105], [82], [114]
Übergreifende Branchen	Übergreifende Branchen allgemein	3	[84], [116], [90]
Verkehr und Logistik	Bahn- & Schienenverkehr	1	[64]
Verkehr und Logistik	Fahrzeuge & Straßenverkehr	2	[102], [106]
Verkehr und Logistik	Logistik und Transport	1	[121]
Verkehr und Logistik	Luft- und Raumfahrt	1	[94]
Verkehr und Logistik	Öffentlicher Personenverkehr	1	[130]
Wirtschaft und Politik	Öffentliche Verwaltung	1	[76]
Wirtschaft und Politik	Verteidigung	3	[73], [104], [97]

Tabelle 9 : Übersicht Branchen (Abgeleitet von Statista) [140] nach Hauptkategorien und Subkategorien

Sieht man sich die Verteilung der Studien in den Hauptkategorien an, wie in Abbildung 8 gezeigt, fällt eine große Gruppe in den Übergreifenden Branchen auf, die 45 % ausmachen. Energie und Umwelt machen weiters 25% aller Studien aus. Ebenso zu kritischen Infrastrukturen gehören Verkehr und Logistik mit 9%. Gesellschaft die Forschung und Organisationen aller Art beherbergen machen 9% aus, die Kategorie

Wirtschaft und Politik die in dieser Arbeit staatsnahen Bereichen gewidmet ist macht 5% aller Studien aus. Die restlichen Branchen belaufen sich auf jeweils lediglich ungefähr 8%.

Da 21% in der Hauptkategorie „Übergreifende Branchen“ auch zu den kritischen Infrastrukturen gezählt werden können und Energie und Umwelt sowie Verkehr und Logistik ebenso dazuzählen, werden in Abbildung 9 alle Kategorien die den kritischen Infrastrukturen zugehörig sind gesondert dargestellt. Diese machen so 55% aller Studien aus, was die Wichtigkeit und den Bedarf von CR in kritischen Infrastrukturen erkennen lässt. Zählt man die allgemein auf CPS zugeschnitten Studien aus der Kategorie „Übergreifend, kritische Infrastrukturen , Industrie, Produktion“ zur Kategorie der Energiewirtschaft käme man auf über 40% aller Studien, die sich mit der Stromerzeugung und Bereitstellung beschäftigen.

Interessant ist das Bereiche die die Gesellschaft in einem Staatenverbund betreffen sowie Militär in der vorliegenden Arbeit nur in etwa 5% ausmachen. Denkbar wäre das Studien im militärischen Bereich aufgrund ihrer Sensibilität und besonderen Vertraulichkeit nicht veröffentlicht werden. Branchen die dem Gesundheitswesen zuzuordnen sind, sind in keiner Studie vorzufinden. Ebenso ist die reine IT-Infrastruktur in der Kategorie Telekommunikation, IT und Consumer Electronis mit 6% eher gering vertreten. Ein in Zukunft immer wichtiger werdender Bereich autonomes Fahren ist in der Hauptkategorie Verkehr und Logistik die 4 Subkategorien hält mit nur 2 Studien vertreten, das entspricht in etwa 2%. Es gibt weiters nur eine Studie die sich mit dem Finanzwesen beschäftigt und das auch nur zum Teil. Diese findet sich in der Kategorie Gesellschaft die Verbände und Organisationen wieder. Andere wichtige Bereiche einer Gesellschaft wie Lebensmittelversorgung, der Schutz und die Versorgung der Zivilbevölkerung abseits von Militär oder Smart Cities und deren Versorgung sind ebenso nicht zu finden.

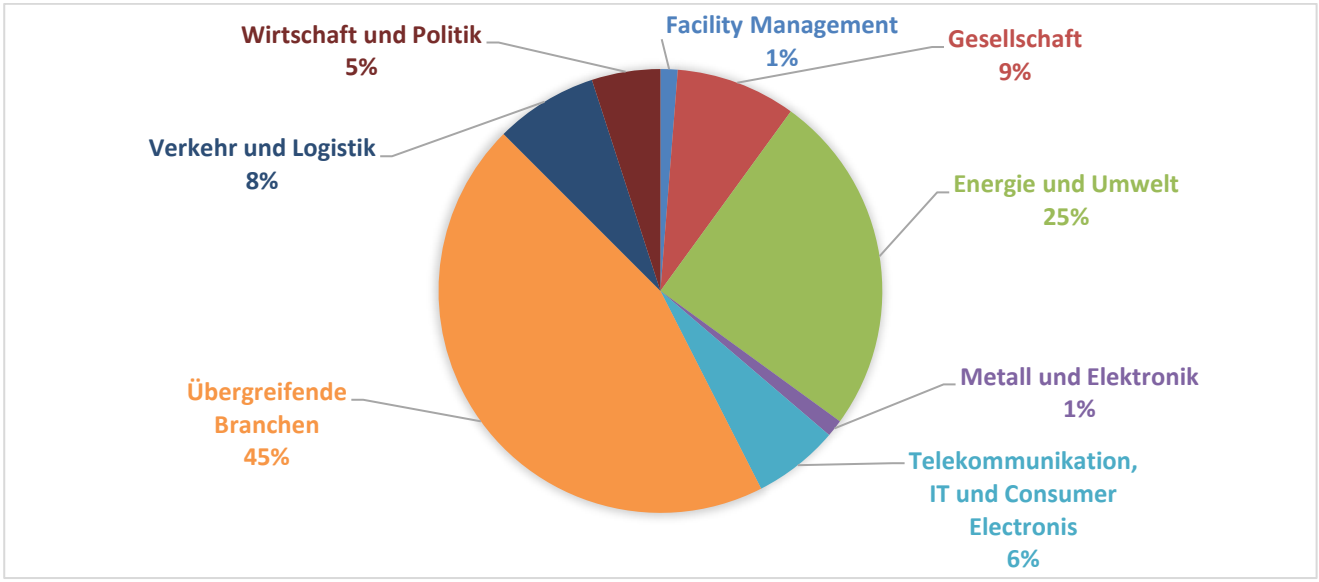

Abbildung 8 : Branchen nach Hauptkategorien

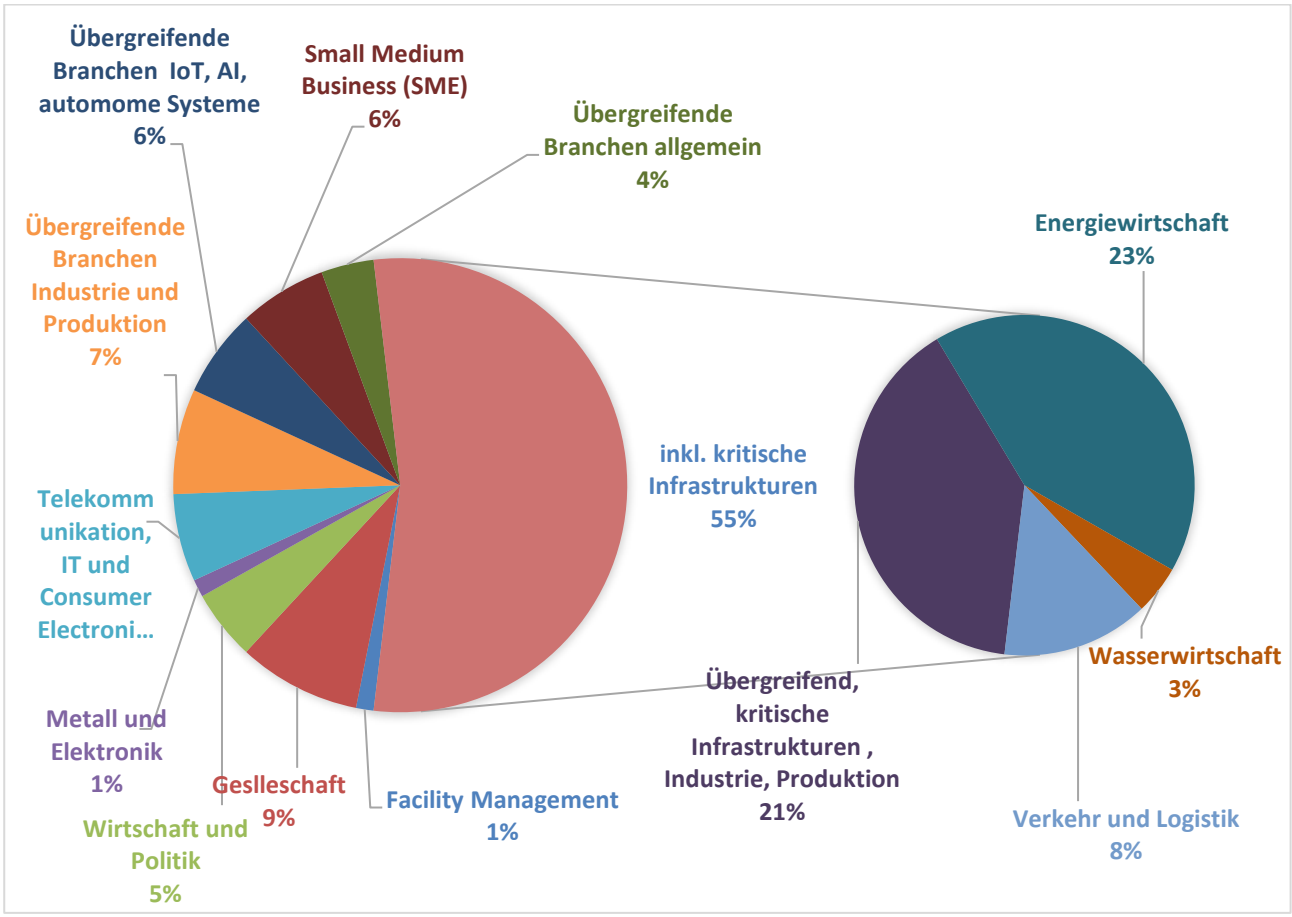

Abbildung 9 : Darstellung kritische Infrastrukturen zu andern Branchen

Wie schon in der allgemeinen Abhandlung der Branchen, wird der Vergleich zu Branchen und Kontinente in den reinen Hauptkategorien sowie der Sicht mit Fokus auf kritische Infrastrukturen in Abbildung 10 und Abbildung 11 dargestellt. Mit Blick auf Branchenübergreifende Studien liegt Australien mit 3 von Studien vorne, sieht man sich die Subkategorien an wird sichtbar, dass der Fokus hier klar bei der produzierenden Industrie liegt. Asien weist mit 60% der Studien ohne Branchenzugehörigkeit die nächsthöhere Position auf. Bei Europa und Amerika sind es in etwa ein Drittel. Bei der Betrachtung von Studien mit Fokus auf kritischen Infrastrukturen sieht man, dass Amerika hier mit in etwa zwei Drittel die meisten Studien aufweist, gefolgt von Europa mit knapp weniger als die Hälfte aller Studien in Europa. Die Mehrheit der Studien in Asien haben eher einen Fokus auf Industrie- oder Produktion, dennoch zielen 40% der Studien ebenso auf kritische Infrastrukturen ab. Europa, dass im Vergleich zu Amerika oder Asien mit kleineren Staaten andere Unternehmens- und Organisationsgrößen aufweist, hat den größten Anteil an Studien zu Klein und Mittelunternehmen. Studien zu staatsnahmen Verwaltung und Verteidigung finden sich nur in Amerika und Asien wieder. Hier sei nochmal erwähnt, dass es andere Gründe haben kann, dass Studien bezüglich Verteidigung und Militär nicht veröffentlicht sind.

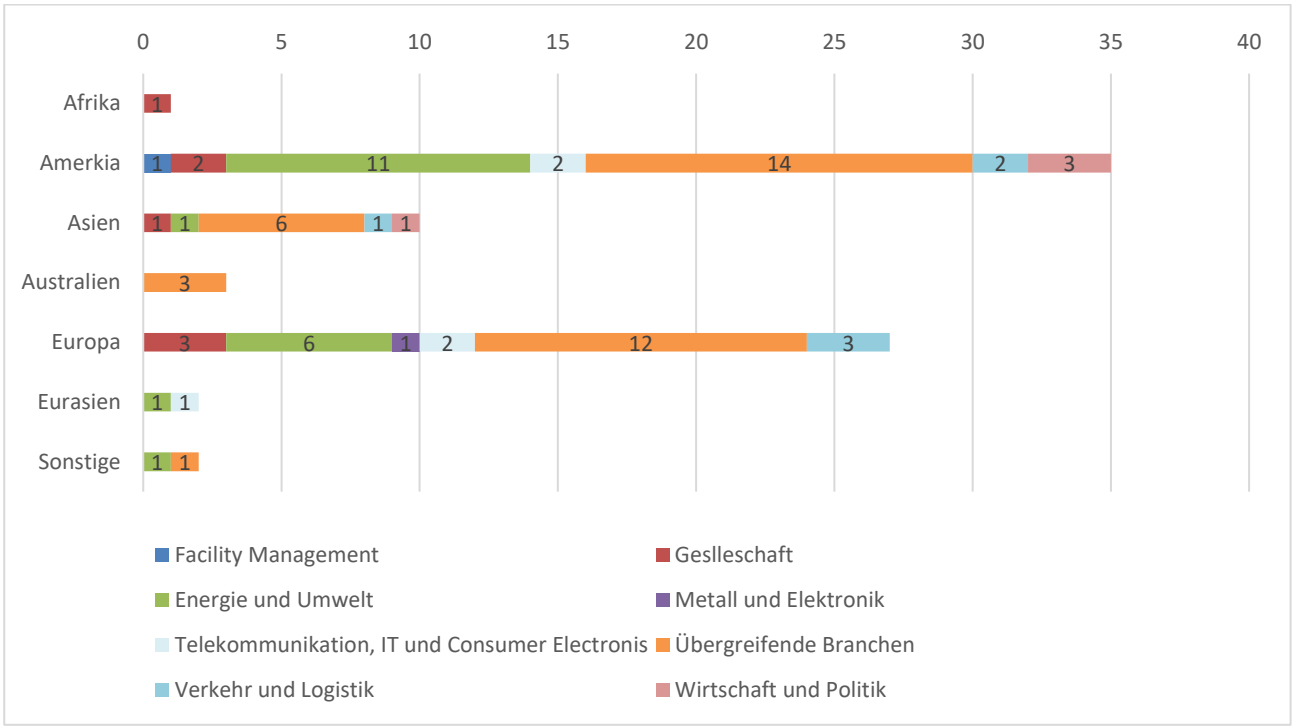

Abbildung 10 : Verteilung Brachen über Kontinente

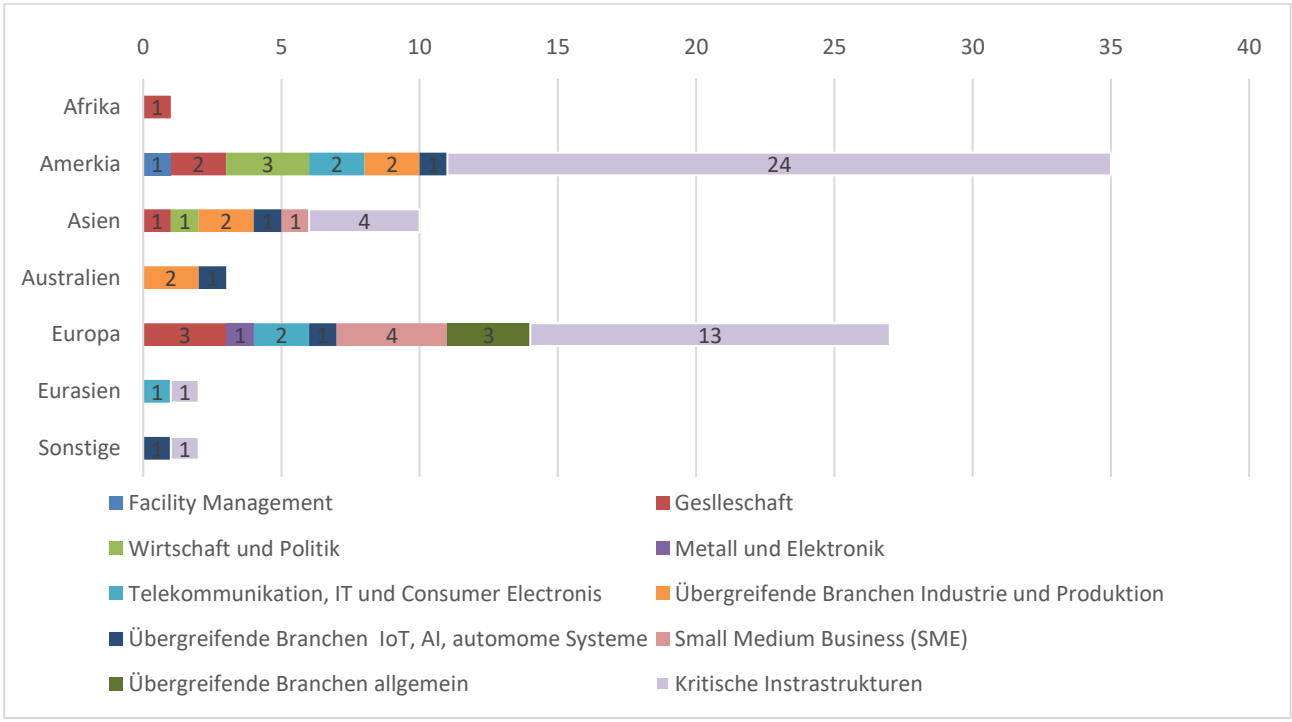

Abbildung 11 : Verteilung Branchen über Kontinente mit zusammengefassten Kategorien kritischer Infrastrukturen

Die Forschungsbereiche wurden anhand der Inhalte der analysierten Studien erstellt. Dabei wurden 8 Kategorien definiert. Diese lassen sich in 2 Bereiche teilen. Erstens Studien die der Analyse und Erhebung unterschiedlicher Themen zu CR gewidmet sind und zweitens Studien die sich mit der Entwicklung und Umsetzung von Themen zu CR beschäftigen. Studien zur Analyse und Definition zu CR sind mit den Kategorien „Analyse zu CR Definition und Frameworks“, „Statuserhebung von CR in Unternehmen/Organisationen/Länder“ und „Evaluierung und Bedarfserhebung zu CR“ versehen. Kategorien die sich mit der Entwicklung und Umsetzung von CR beschäftigen sind „CR-Framework“, „CR-Architektur“, „CR-Assessmentmodell“, „Systemmodellierung zur Verhaltensanalyse“ sowie „Technische Systeme“. Wenn sich Studien nicht eindeutig zu Kategorien zuweisen lassen, wird jenes Forschungsgebiet zugeordnet, welches den größten Fokus in der Arbeit hat. So werden z.B. die Entwicklung von Frameworks und Architekturen sehr oft mit Systemmodellierungen und Simulationen validiert. Liegt hier die Framework-Entwicklung im Fokus oder ist sie das Ziel der Arbeit wird eben diese Kategorie zugeordnet.

Studien in der Kategorie **„Analyse zu CR Definition und Frameworks“** beschäftigen sich mit der reinen Analyse von CR in unterschiedlichen Facetten. Die Arbeiten erklären wie CR definiert, dargestellt und gemessen werden kann. Auch eine Aufstellung vorhandener Frameworks und Vergleiche zu anderen Konzepten wie Cyber Security sind hier zu finden. Mit **„Statuserhebung von CR in Unternehmen / Organisationen / Länder“** werden Studien beschrieben die sich mit der Statuserhebung der Umsetzung oder Verankerung von CR in unterschiedlichen Bereichen beschäftigen. Hier finden sich auch Empfehlungen zur Verbesserung, allerdings liegt hier der Fokus klar bei der Erhebung wo man bezüglich CR steht. **„Evaluierung und Bedarfserhebung zu CR“** befasst sich mit der Analyse und Bedarfserhebung zu spezifischen Fragen zu CR. Dies ist auch die Abgrenzung zur erst genannten Kategorie, dass sich eine Analyse auf eine spezifische Fragestellung bezieht. Die Evaluierung kann weiter gefasst sein wie der Erhebung von Anforderungen für zum Beispiel autonome Systeme oder einen engen Fokus auf CPS und Angriffserkennung haben.

CR-Frameworks und **CR-Architekturen** beschäftigen sich damit wie CR etabliert oder umgesetzt werden kann. Frameworks helfen Strukturen aufzubauen die CR in bestehenden oder neuen Systemen umsetzen. Architekturen beschäftigen sich mit dem Systemdesign in der Hard- und Softwareentwicklung aber auch im Systemdesign. Da beide Bezeichnungen manchmal synonym verwendet werden, wird versucht nach der beschriebenen Erklärung die Studien den jeweiligen Kategorien zuzuordnen. Bezeichnet eine Studie ihr entwickeltes Modell konsequent als Framework oder Architektur wird diese für die Zuordnung der jeweiligen Kategorie verwendet. **CR-Assessmentmodell** behandelt Frameworks oder Modelle mit dem klaren Fokus auf der Messung und Bewertung von CR. Hier kann CR mittels Metriken gemessen werden aber auch eine Reifegraderhebung fällt unter diesem Bereich. Die nächste Kategorie **„Systemmodellierung zur Verhaltensanalyse“** hat speziell mit CR-Assessmentmodelle eine große Überschneidung. Liegt der Fokus in der Entwicklung oder Umsetzung der Messung auf Basis von Modellierungen und Simulationen wird diese Kategorie zugewiesen. **„Technische Systeme“** beschäftigen sich zu guter Letzt mit der praktischen Umsetzung von Lösungen mittels Frameworks oder Architekturen. Diese Studien lassen sich nicht eindeutig den anderen Umsetzungskategorien zuordnen haben aber einen klaren Fokus zu einer technischen Lösung.

Um im Kapitel zur inhaltlichen Analyse der Studien eine klarere Struktur geben zu können werden Subkategorien entwickelt. Aber auch um z.B. Frameworks für die Messung oder zur Abwehr von Angriffen besser trennen und sichtbar machen zu können. Diese beschreiben die Studien in ihren Forschungsbereichen somit genauer auf ein spezifisches Gebiet. Die Kategorien wurden wiederum anhand der Inhalte gewählt und können je Studie auch mehrfach zugeordnet werden. Teilweise sind die Subkategorien an den Hauptkategorien angelehnt da sonst keine Zuordnung möglich wäre. So sind zum Beispiel CR Definitionen oder Assessment und Messung in Haupt- wie Subkategorie zu finden.

Die Subkategorie **„CR Definition“** beschreibt, welche Studien sich ausschließlich der Definition widmen und sind somit der Hauptkategorie sehr ähnlich. Das gleiche gilt für **„Bedarfserhebung in Entwicklung und Design“** , wobei hier der Fokus auf Systemdesign liegt und die Hauptkategorie hier weitergefasster ist. **„Assessment und Messung von CR“** findet sich in vielen Hauptkategorien wieder. Die Messung von CR

stellt einen sehr wichtigen Faktor in der Forschung zu CR dar und ist somit auch entsprechen oft vertreten. Die Subkategorie **Metriken** ist wie die Messung ein sehr wichtiger Bereich in der Forschung zu CR, ist aber stark von dahinterliegenden Frameworks und Assessmentmodellen abhängig. Außerdem gibt es kaum Studien die sich nur der Entwicklung von Metriken widmen, der Aspekt des dazugehörigen Assessment von CR ist immer erkennbar. Die Subkategorie **„CR in Organisationen“** umfasst Arbeiten die sich mit CR in Organisation oder der organisatorischen Resilienz beschäftigen.

Die Subkategorie **„Erkennung von Verwundbarkeiten“** und **„Erkennung und Abwehr von Cyber-Angriffen“** findet sich in Umsetzungslösungen zu CR wieder und beschreibt wie der Name erkennen lässt den Schutz und Abwehr von Angriffen. Schließlich wird mit Kategorie **„CR mit Fokus auf Recovery“** der Recovery-Aspekt von CR abgedeckt, dieser hängt oft mit der gleichzeitigen Erkennung and Abwehr von Angriffen zusammen.

In Tabelle 10 sind die Anzahl der Studien nach Forschungsbereiche angeführt, in Tabelle 11 sind die Hauptkategorien und die Subkategorien mit den jeweiligen Studien abgebildet. Hier sieht man das die Umsetzung von CR vor der reinen Evaluierung von CR klar im Fokus aktueller Forschung steht, wobei Systemmodellierung weit vorne liegt. Würde man Frameworks und Architekturen sowie Assessmentmodelle die oft in der Form von Framework vorliegen zusammenzählen wäre dies die größte Kategorie an Forschungsbereichen. Dennoch beschäftigen sich ungefähr ein Viertel der Studien mit der Analyse und Evaluierung von CR Themen. Das Bild deckt sich somit mit der Aussage aus [88], dass die aktuelle Forschung sich dem vertiefen und verbessern von CR widmet.

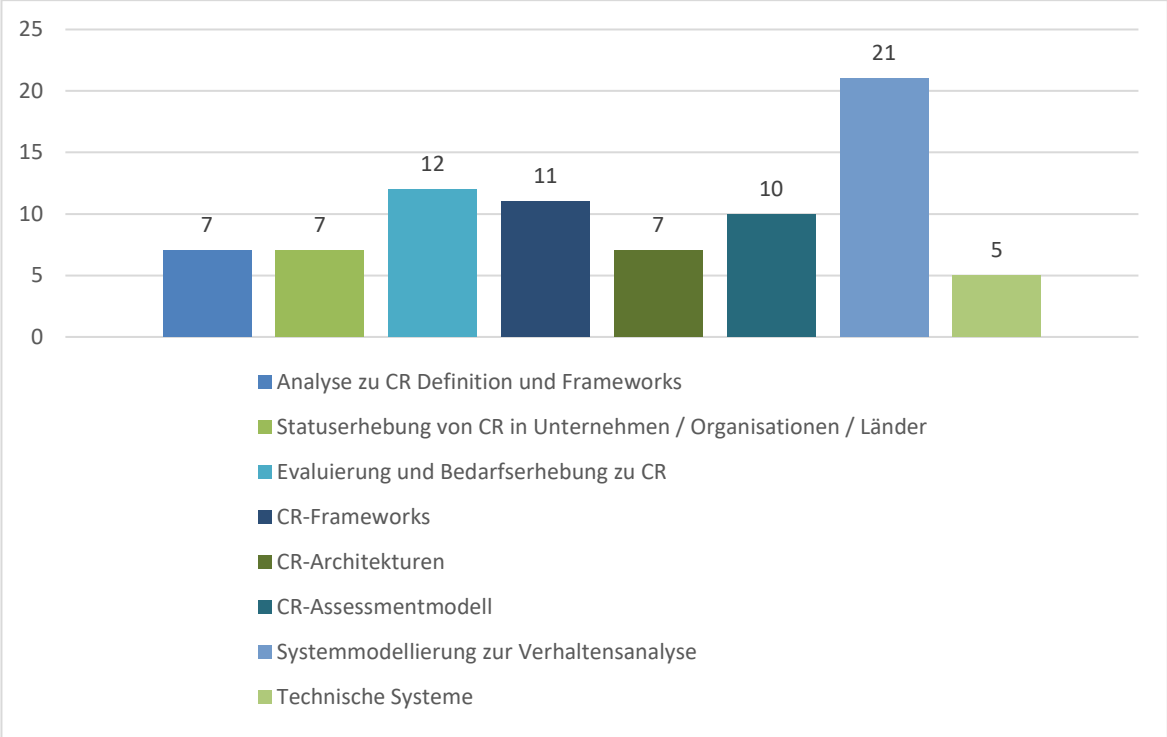

Tabelle 10 : Forschungsbereich nach Kategorien

Kategorie / Subkategorie	CR Definition	Bedarfs-erhebung in Entwicklung und Design	Assessment und Messung von CR	Metriken	CR in Organisationen	Erkennung von Verwundbarkeiten	Erkennung und Abwehr von Cyber Angriffe	CR mit Fokus auf Recovery
Analyse zu CR Definition und Frameworks	[126], [88],[116] [84],[134]		[126], [88], [116], [113]				[134], [102]	
Statuserhebung von CR in Unternehmen / Organisationen / Länder					[128],[94], [76], [130],[110], [108], [137]			
Evaluierung und Bedarfserhebung zu CR		[118], [119], [135], [89], [87]	[91], [98]	[87]	[72], [121], [136]		[69], [133]	
CR-Frameworks			[82]		[70], [71], [82], [114] , [131]	[112], [120], [66], [93],[75],[112] [120], [66][93], [75]		[90]
CR Architekturen				[122]			[122], [127], [111], [107], [78], [61], [68]	
CR Assessment-modell			[67], [124], [101][95], [123], [81], [79], [103], [58], [92]	[123], [81] [79], [103] [58], [92]				
System-modellierung zur Verhaltensanalyse			[62],[63],[64],[80] [85],[99], [74], [129][60], [73], [104][97], [115], [132]	[85], [99], [117], [73] [104], [97] [115]		[59], [117], [125]	[65],[59], [99], [106], [109], [74], [77], [80], [125],[62],[63], [73], [104], [97]	
Technische Systeme						[100], [96], [105], [83]		[86], [105]

Tabelle 11 : Forschungsbereich nach Kategorien und Subkategorien

Eine andere Art der Darstellung der Forschungsbereiche soll mittels der Kategorien des NIST CSF [141] dargestellt werden und ist in Tabelle 12 : Zuordnung Kategorien zu NIST CSF Kategorien [141]Tabelle 12 abgebildet. Dabei sei dazugesagt das einige Studien sich mehr mit der Erhebung von Status und Bedarf zu CR beschäftigen und daher eine Einordnung meist nur zu Identity definiert wurde. Dies dient der besseren Übersicht, wenn beispielsweise die Statuserhebung alle Kategorien erfragt aber auf der anderen Seite keine Lösungs- oder Umsetzungsdetails genannt wurden.

Kategorie / NIST CSF Kategorie	**Identify**	**Protect**	**Detect**	**Respond**	**Recover**
Analyse zu CR Definition und Frameworks	[134],[88],[102] [126],[84],[116], [113]	[102]	[102]	[102]	
Statuserhebung von CR in Unternehmen / Organisationen / Länder	[110], [108], [130], [128], [137], [76], [94]				
Evaluierung und Bedarfserhebung zu CR	[118], [98], [135], [121], [89], [72], [91]	[136], [119], [135], [133]	[119], [69], [118], [98], [133]	[136], [119], [69], [133]	[136]
CR-Frameworks	[70], [131], [82] [114], [71], [93]	[131], [71]	[70], [66], [112], [120], [93], [75]	[66], [112],[131] [120], [93], [75]	[90]
CR-Architekturen	[122]	[61], [68], [127] [78]	[122], [107], [61], [111], [68], [127], [78]	[122], [107], [61], [111], [68], [127], [78]	[122], [107], [61], [68]
CR-Assessmentmodell	[124], [101],[58] [67], [95], [123], [103], [79], [92], [81]	[103]	[58], [67], [103]	[103], [124]	[124]
Systemmodellier-ung zur Verhaltensanalyse	[104], [80], [74], [64], [99], [117], [85], [60], [129], [63], [62], [73], [97], [115],[132]	[104], [109], [77], [64], [65], [125]	[104], [80], [74], [109], [77], [64], [65], [99], [117], [106], [129], [125], [63], [62], [73], [97], [115], [132], [59]	[104], [80], [74], [109], [77], [64] [65], [99], [106], [129], [125],[63] [62], [73], [97], [115], [132],[59]	[109], [77]
Technische Systeme		[86], [105]	[96], [100], [86], [105], [83]	[96], [100], [86], [105], [83]	[86], [105]

Tabelle 12 : Zuordnung Kategorien zu NIST CSF Kategorien [141]

Vergleicht man nun welche Branchen welchen Forschungsbedarf haben zeigt sich an Abbildung 12, dass sich Studien die keinen eindeutigen Fokus auf eine spezifische Branche haben durch fast alle Forschungsbereiche ziehen. Es ist hier auch schon deutlich erkennbar das Energie und Umwelt, welche ausschließlich Studien mit Bezug zu Stromversorgung hält in fast allen Forschungsbereichen zu finden ist.

In Abbildung 13, wo wieder Branchen aus kritischen Infrastrukturen zusammengefasst sind, ist erkennbar das alle Forschungsfelder einen starken Fokus darauf haben. Insbesondere die Systemmodellierung für beispielsweise CPS macht zwei Drittel aus. Ebenfalls zwei Drittel der Studien zu kritischer Infrastruktur fallen auf die Evaluierung und Bedarfserhebung. Der Forschungsbereich CR-Assessment hält ausschließlich Studien aus der produzierenden und kritischen Infrastruktur, 75% davon fallen auf letztere. Sehr gemischt sind die Studien bei den Bereichen zur Analyse von CR und CR-Frameworks.

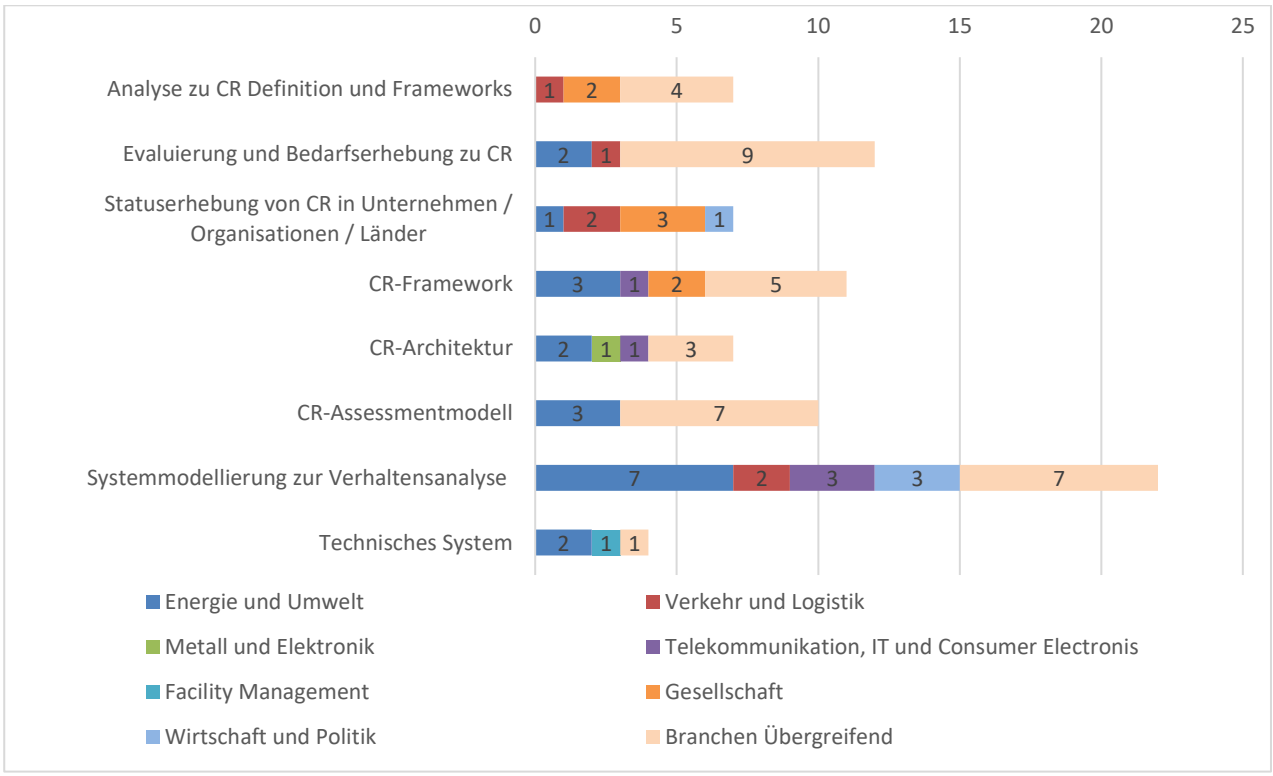

Abbildung 12 : Branchen je Forschungsbereich

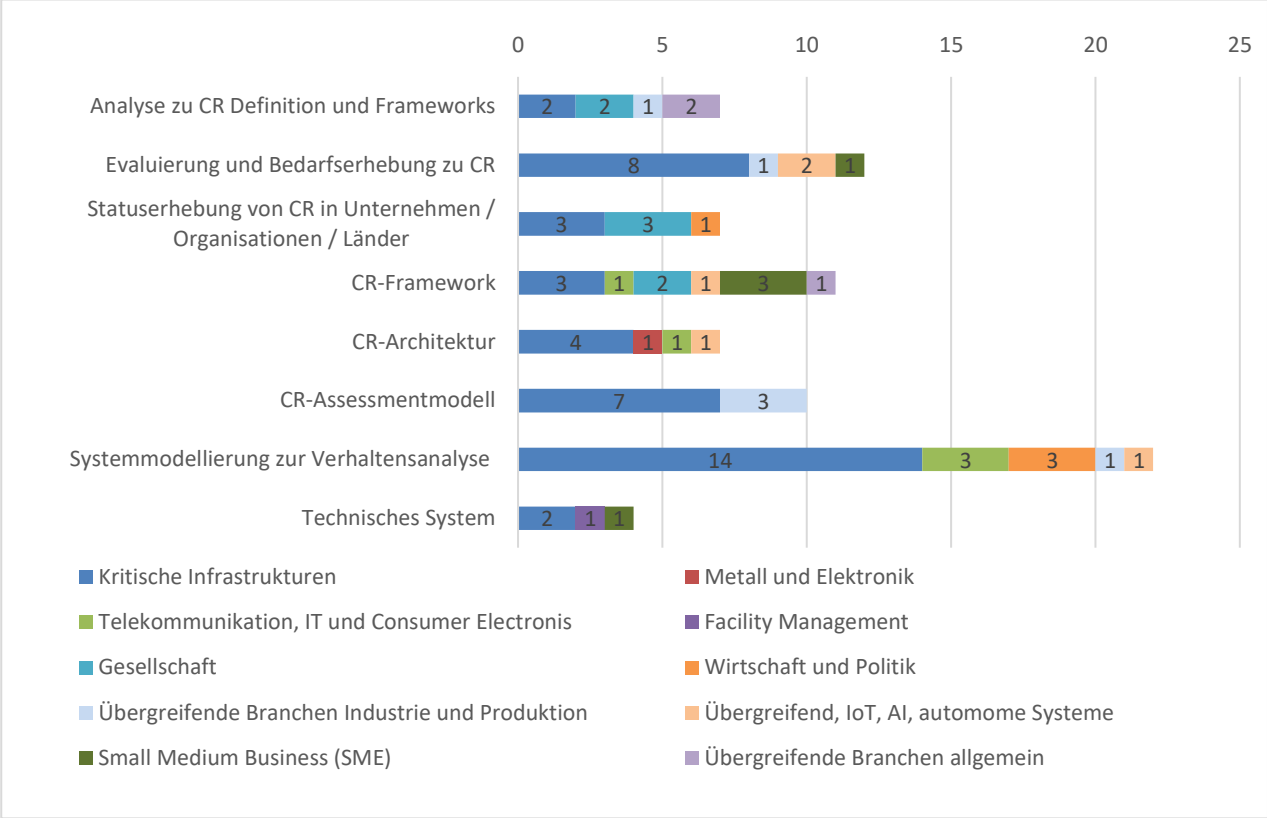

Abbildung 13: Branchen je Forschungsbereich inkl. kritische Infrastrukturen

Die Methoden und Techniken die in Studien angewandt werden, werden in acht Kategorien eingeteilt, eine Mehrfachzuordnung je Studie ist möglich. Die Erhebung und Beurteilung der Qualität anhand der Methoden ist insofern schwierig als die analysierten Studien sehr unterschiedlich in der Ausführung sind. Längere Studien die bis zu 35 Seiten umfassen beinhalten oft sehr detaillierte Beschreibung der angewandten Methodik wohingegen Studien mit 4 bis 6 Seiten diese gar nicht erwähnen. Viele Publikationen beschäftigen sich mit der Entwicklung von Frameworks und bleiben dabei offen welche Methodik sie zur Entwicklung angewandt haben. Diese wurden der Kategorie „Andere“ zugeordnet. Die Kategorie hält weiters spezifische Methoden wie Dempster-Shafer Theorie oder Analytical Hierachical Prozess die nur wenige Male genannt wurden. Betrachtet man die Ergebnisse sind Experimente, Case Studies sowie Modellierungen und Simulationen als auch die Literaturanalyse die häufigsten Methoden die für die Forschung zu CR verwendet werden.

Vergleicht man nun die Methoden mit den Branchen, wie in Abbildung 15 und Abbildung 16 gezeigt, sieht man bei der Übersicht der reinen Hauptkategorien, welche die übergreifenden Branchen allgemein darstellt, dass diese Studien sich aller Methoden und Techniken gleichermaßen bedienen. Die Kategorie Energie und Umwelt bedient sich stark der Techniken um Simulationen und Experimenten. Stellt man die kritischen Infrastrukturen wie in Abbildung 16 heraus, erkennt man das dieser Trend weit deutlicher ausfällt. Umfragen und Interviews werden mehrheitlich für Studien im Bereich Gesellschaft und Organisationen genutzt.

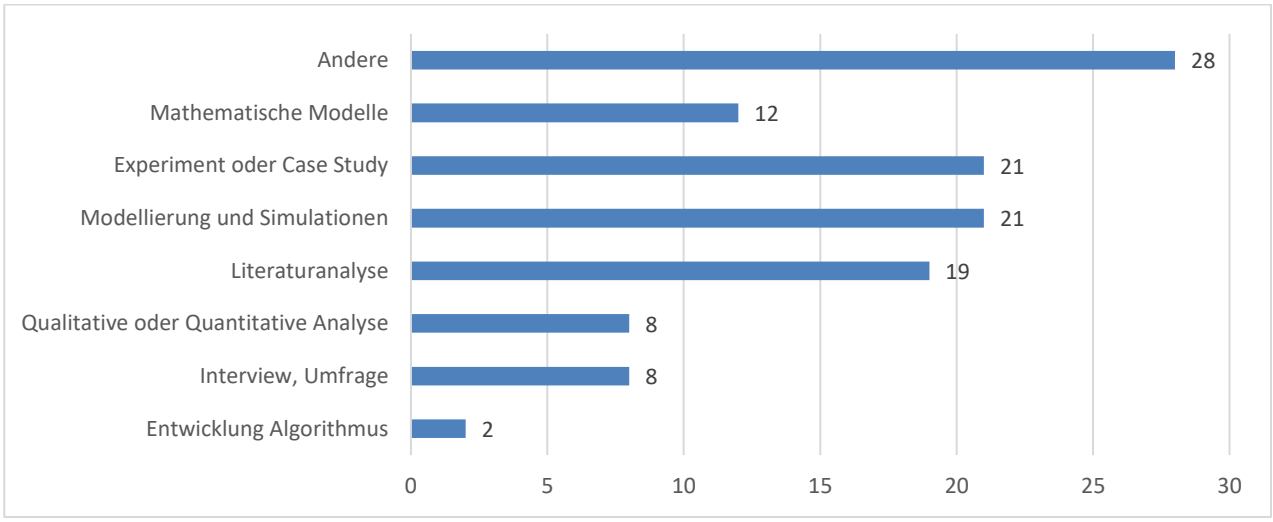

Abbildung 14 : Methoden und Techniken über alle Publikationen

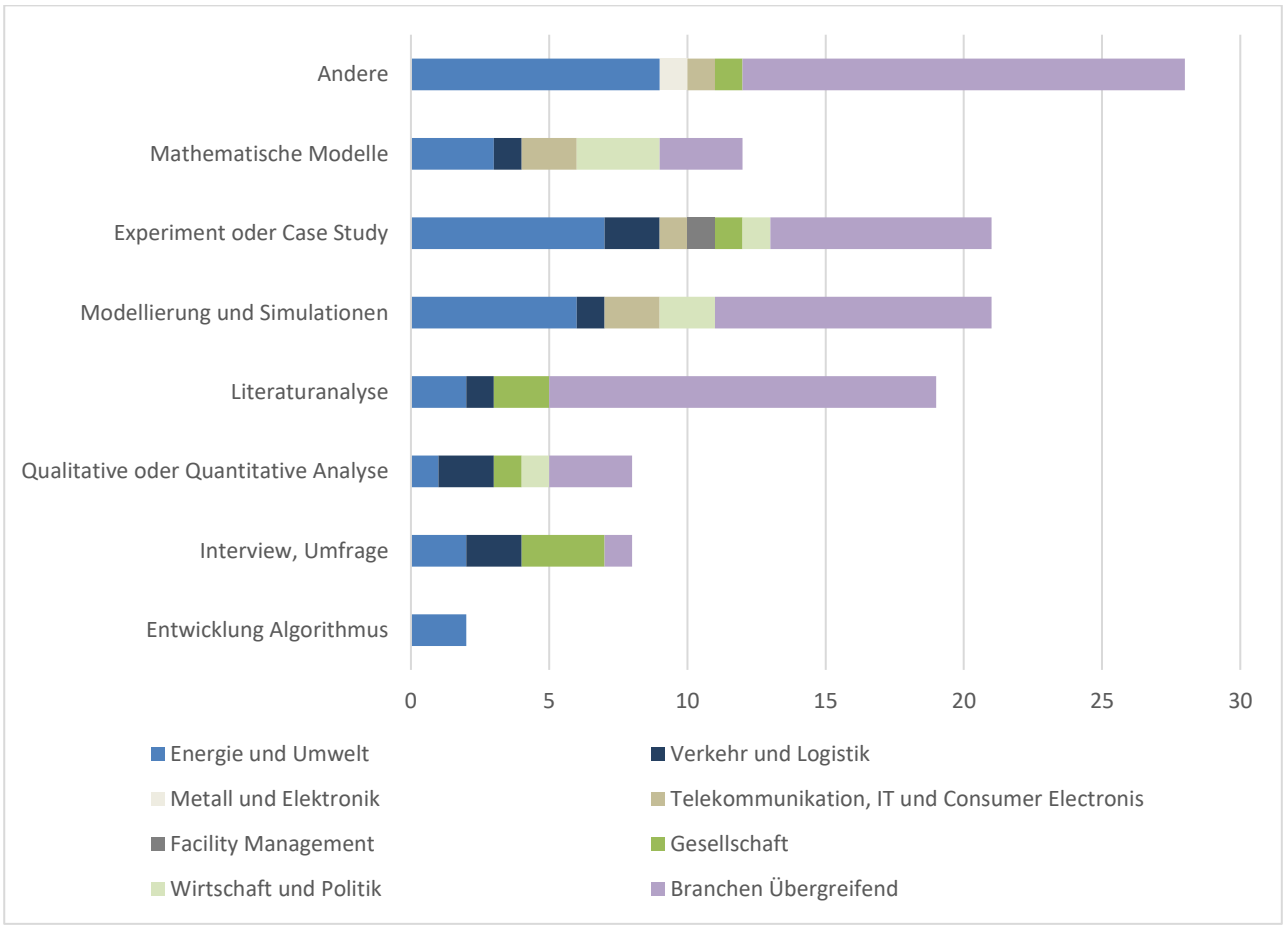

Abbildung 15 : Methoden und Techniken zu Branchen im Vergleich, Übergreifende Branchen aggregiert

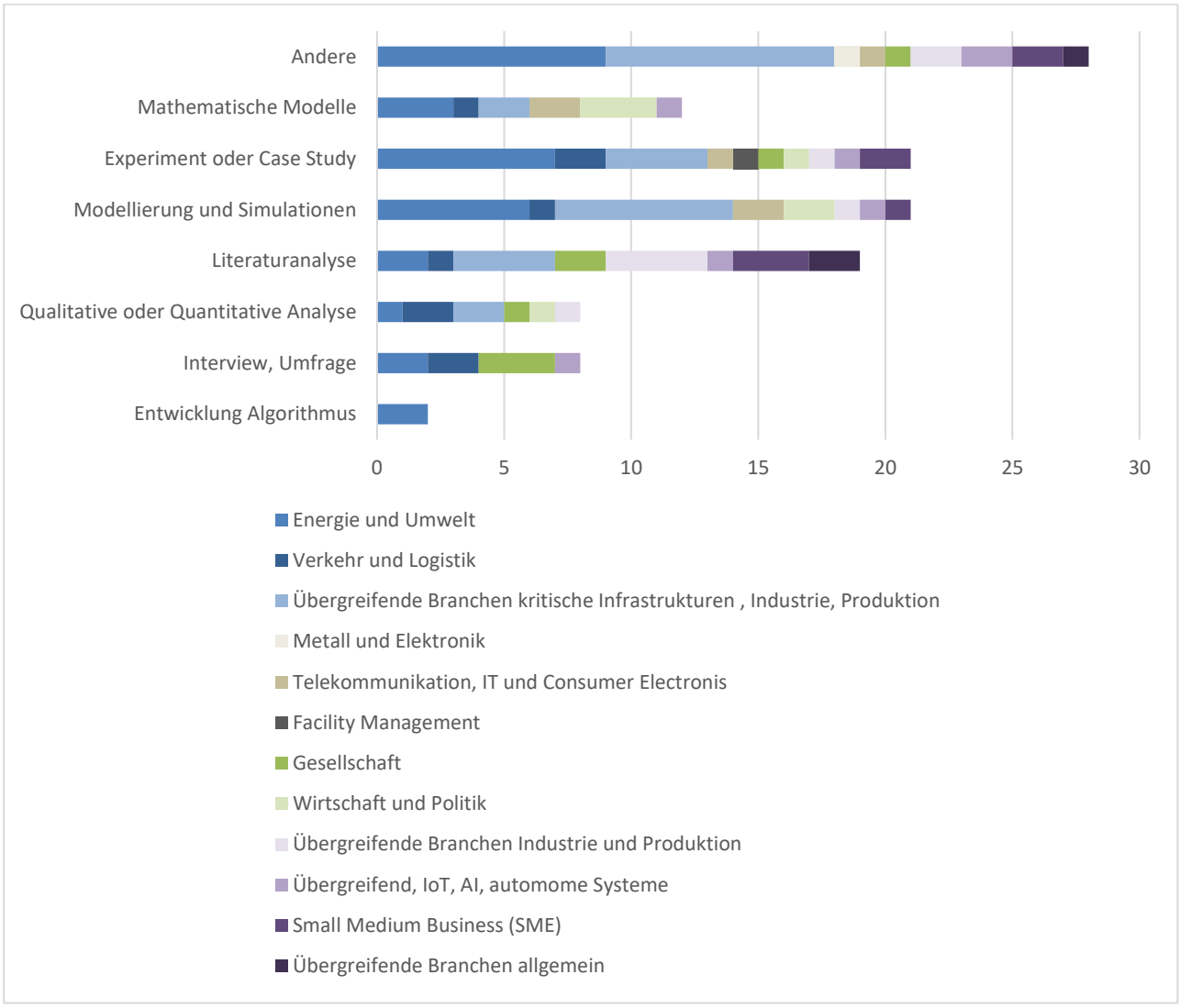

Abbildung 16 : Methoden und Techniken zu Branchen im Vergleich mit Fokus auf kritische Infrastrukturen

Stellt man Methoden und Techniken mit dem Forschungsbereich gegenüber, sieht man, dass die Analyse von CR sich der Methodiken der Literaturanalyse und Interviews oder Umfragen bedient. Die Umsetzung von CR in Form von Frameworks, Architekturen und Modellierung gehen ganz klar in Richtung mathematische Modelle, Experimente sowie Modellierungen und Simulationen. Die Qualitative und Quantitative Analyse ist gleichermaßen über alle Forschungsbereiche verteilt.

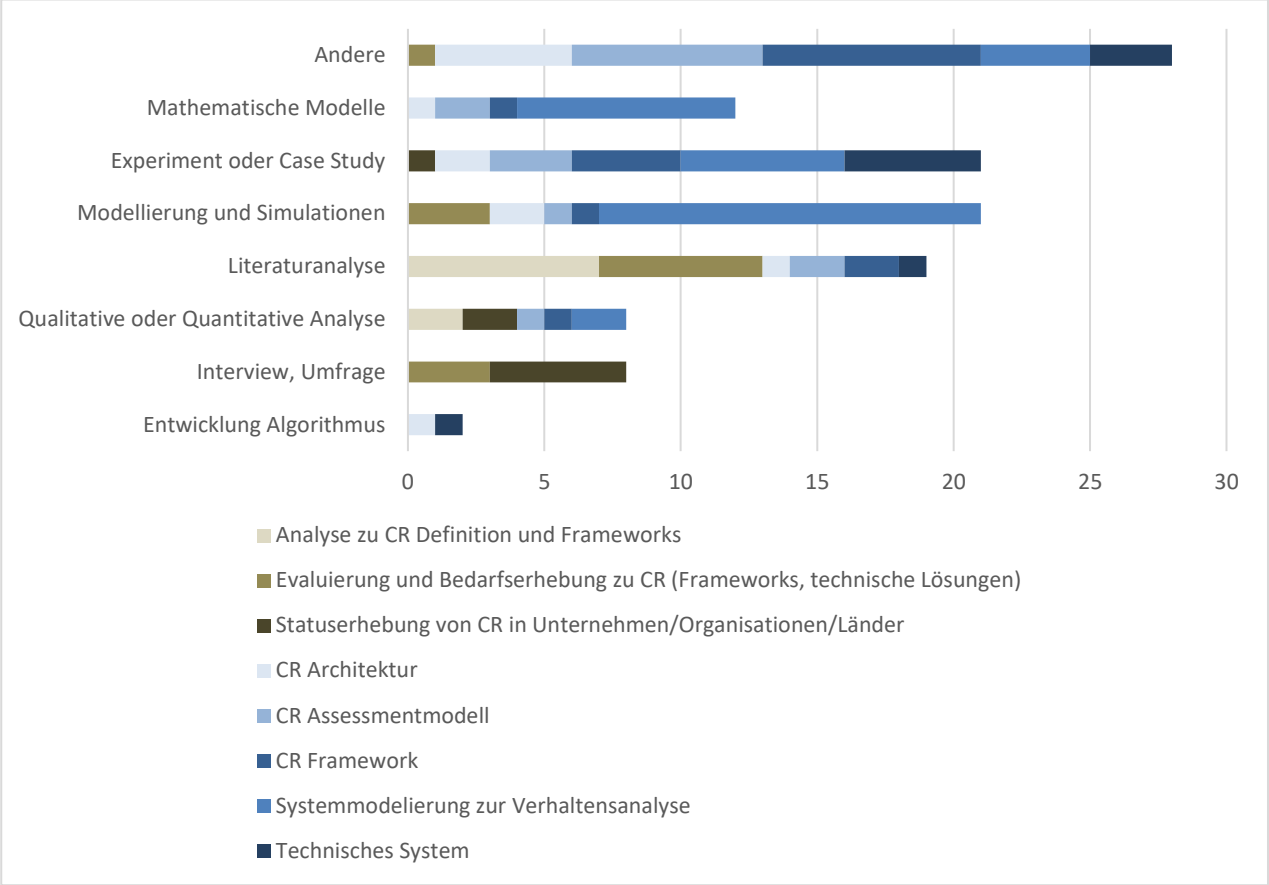

Abbildung 17 : Methoden und Techniken im Vergleich zum Forschungsbereich

4.3. Darstellung der Studien nach Motivation und Risiken

Die Motivationen von Studien können in zwei Bereiche eingeteilt werden. Es gibt Studien mit klaren Forschungsbedarf zu einem spezifischen Thema, diese beschreiben mehr oder weniger ausführlich, dass es keine aktuellen Forschungen zu ihrem Themengebiet gibt und formulieren daraus ihre Motivation. Und es gibt Studien, die die Motivation entweder nicht herausgestellt haben oder in der Einleitung auf die Notwendigkeit des jeweiligen Forschungsthemas mit eher allgemein gefassten Motivationen und oft gemeinsam mit daraus resultierenden Risiken beschrieben haben. Dazu zählen die rasante Entwicklung im IKT-Betrieb sowie die steigende Anzahl von Cyber-Angriffen. Es wird bei Cyber-Angriffen außerdem auf die Auswirkung auf die Gesellschaft unterschieden. Diese Kategorie inkludiert neben der zivilen Gesellschaft auch Organisationen im allgemeinen Sinn sowie die Auswirkungen von Terrorismus durch Ausfälle von Systemen die beispielsweise Stromversorgung, Wasserversorgung oder Onlineservices zur Verfügung stellen. In Abbildung 18 sind die definierten Kategorien abgebildet und es ist deutlich erkennbar, dass allgemein gefasste Motivationen ganz klar vorne liegen. Allem voran die steigende Anzahl und Komplexität von Cyber-Angriffen sowie immer komplexer werdende technische Systeme und damit verbundene Risiken.

Risiken die in Studien adressiert werden können drei Bereichen zugeordnet werden. Diese sind Risiken verursacht durch Cyber-Angriffe, durch Störungen aller Art und Risiken mit Auswirkungen auf die Gesellschaft. Damit ist gemeint, dass explizit der Schaden für die Gesellschaft erwähnt wurde, dieser kann durch Störungen aller Art somit auch durch Cyber-Angriffe verursacht werden. Der Risikobereich Störungen aller Art inkludiert natürlich auch Cyber-Angriffe, diese Studien beziehen sich aber auch auf Ausfallsrisiken ungeachtet der Ursache. Abbildung 19 zeigt die Verteilung der adressierten Risken über die analysierten Studien.

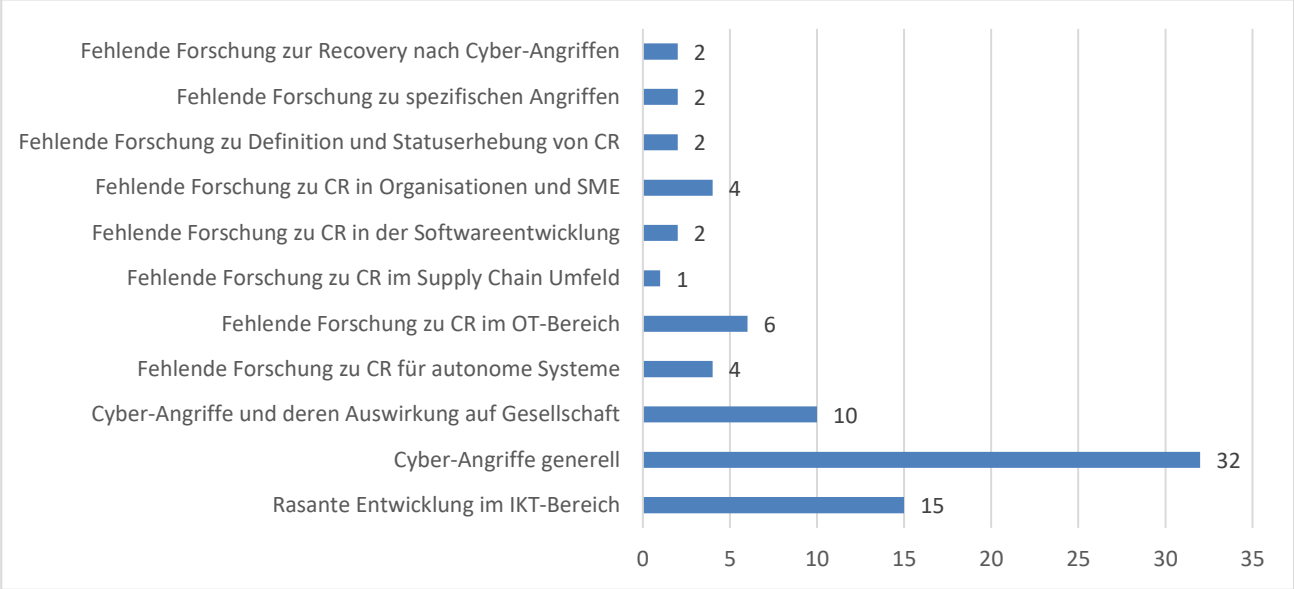

Abbildung 18 : Motivationen für Studien zu CR

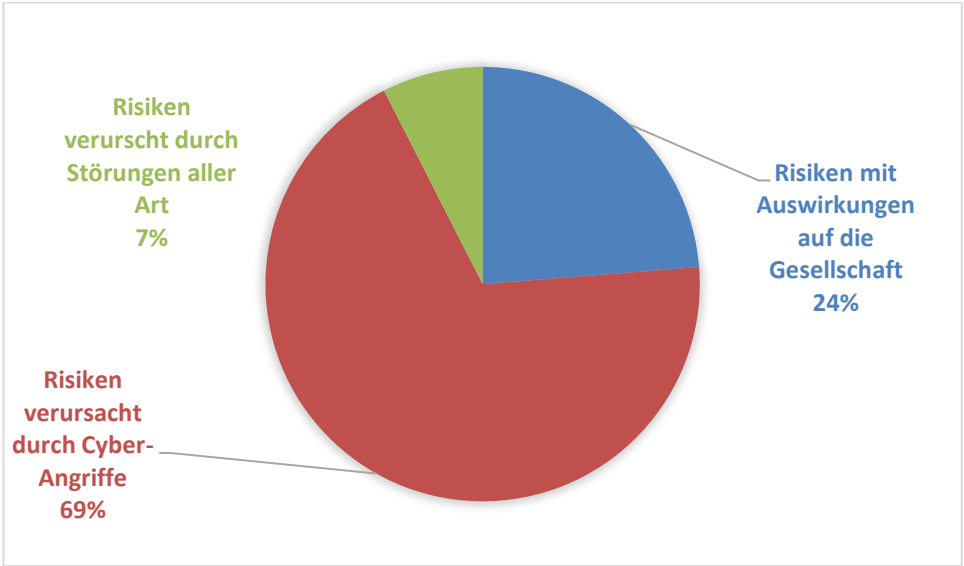

Abbildung 19 : Adressierte Risiken in Studien zu CR

In Abbildung 20 ist gut erkennbar welche Motivationen für die jeweiligen Branchen ausschlaggebend war und das die allgemein gefassten Motivation über alle Bereiche teilweise sogar ausschließlich genannt wurden. Fehlende Forschung zu spezifischen Angriffen wurden ausschließlich für CPS angeführt und finden sich daher in den Branchen für kritische Infrastrukturen und der produzierenden Industrie. Andere spezifische Motivationen sind passend in den jeweiligen Branchen erkennbar. Abbildung 21 stellt die adressierten Risiken je Branche gegenüber. Hier sei erwähnt das Studien die Risiken in aller Art von Störungen sehen, sich fast ausschließlich in den kritischen Infrastrukturen befinden. Studien zu CPS, die in kritischen Infrastrukturen Anwendung finden, heben stets die Notwendigkeit von resilienten Systemen hervor. Das ist eine mögliche Erklärung für die allgemeiner gefassten Risiken.

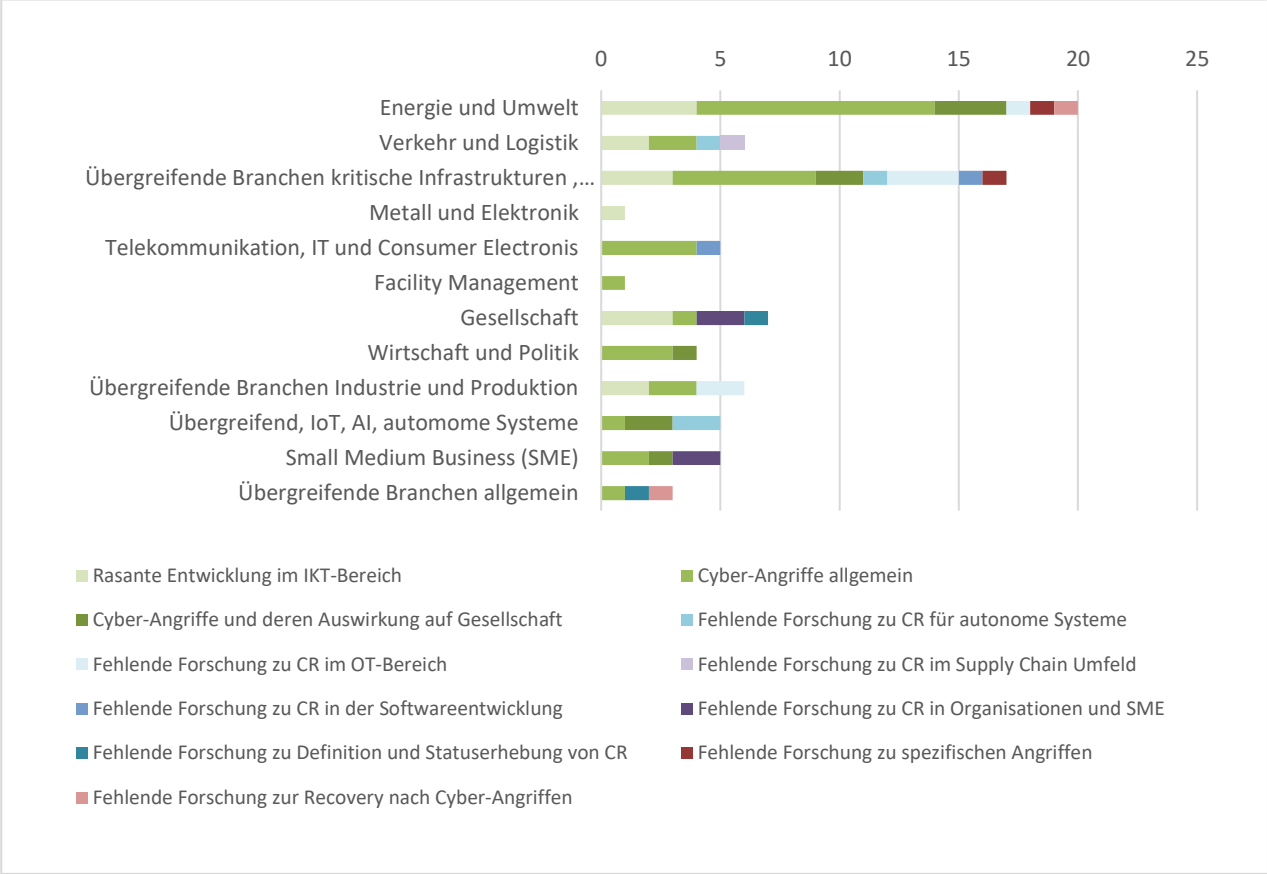

Abbildung 20 : Branchen in Vergleich zu Motivation

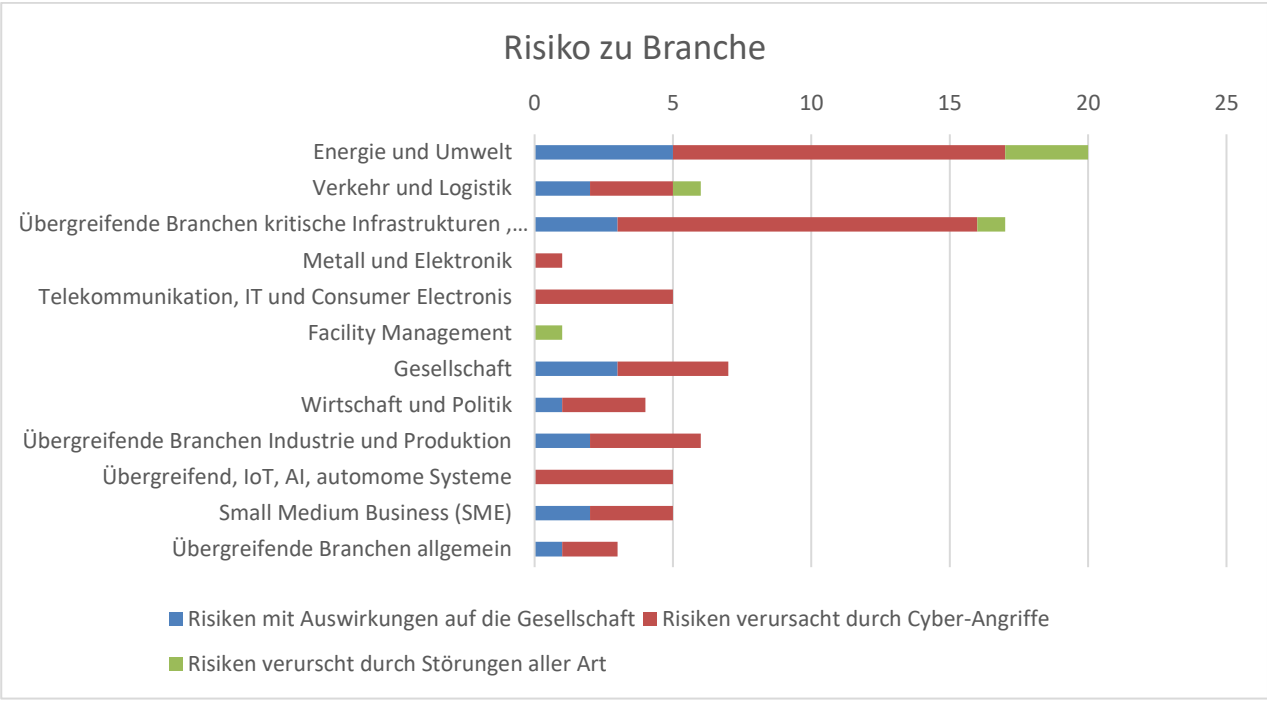

Abbildung 21 : Risiken im Vergleich zur Branche

Forschungsbereiche lassen sich wie schon erwähnt in die Bereiche Analyse und Definition sowie Entwicklung und Umsetzung von CR trennen. In Abbildung 22 sieht man, dass Studien zur Analyse und Definition von CR eher dazu neigen spezifische Motivationen anzuführen. Studien zur Systemmodellierung haben mehrheitlich Cyber-Angriffe als Motivation erwähnt. In Abbildung 23Abbildung 22 sieht man die Risiken zu Forschungsbereichen, hier sind zum Unterschied zu den Branchen die Risiken, die mit Störungen aller Art einhergehen gleichmäßig verteilt. Mit der Ausnahme der Kategorie Evaluierung und Bedarfserhebung zu CR kann im Vergleich zu Abbildung 22 eine ähnliche Häufigkeit zur Motivation bezüglich Cyber-Angriffe erkannt werden.

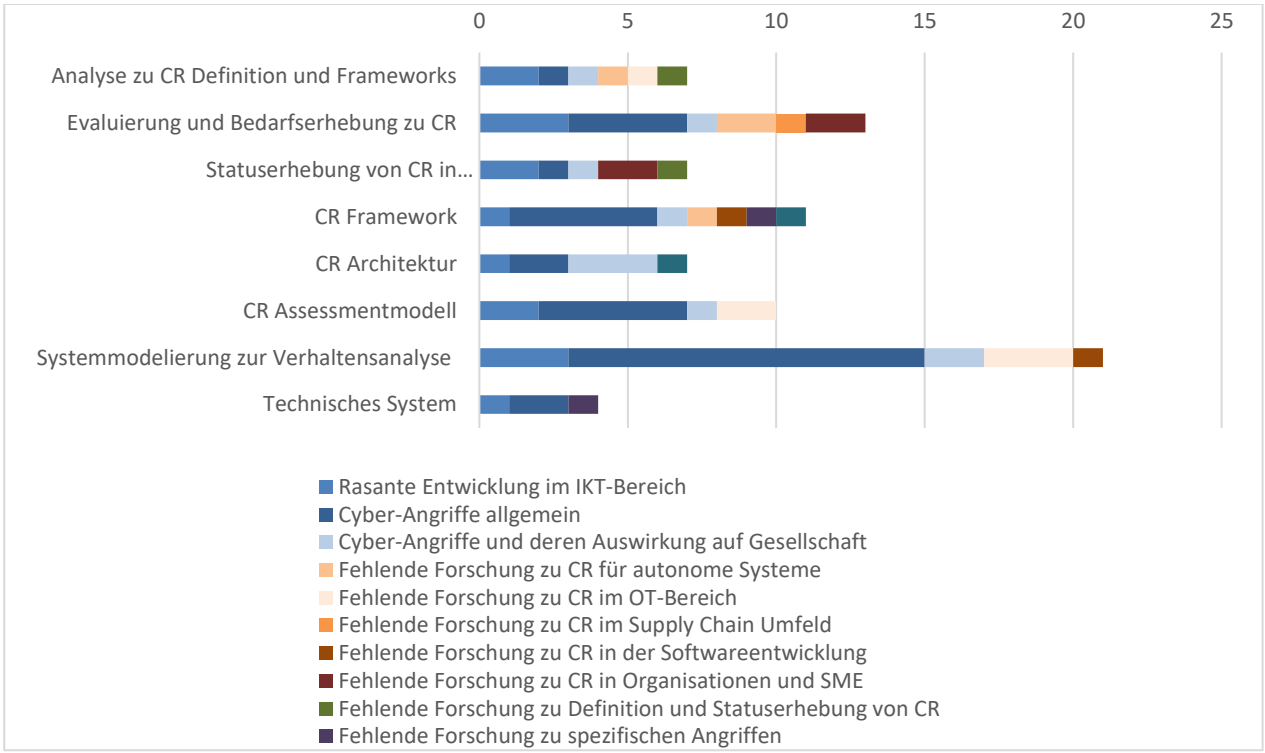

Abbildung 22 : Motivation im Vergleich zum Forschungsbereich

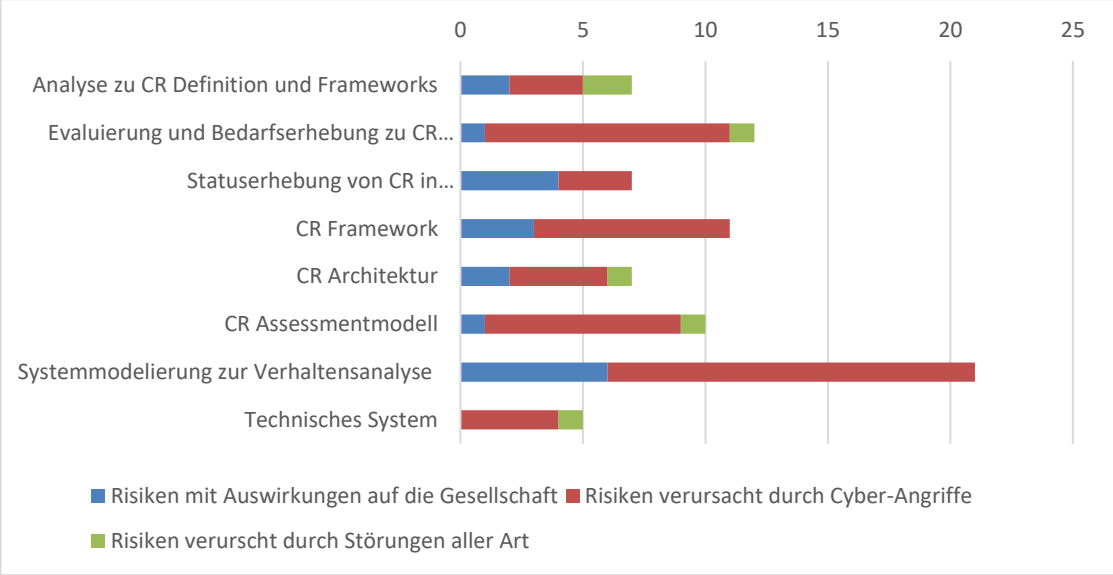

Abbildung 23 : Risiken im Vergleich zum Forschungsbereich

4.4. Analyse zu Limitierungen und Future Works

Bei den erhobenen Daten zu Limitierungen und Future Works konnten keine Zusammenhänge zu anderen Kategorien erkannt werden. Beide Kategorien werden zum einen nicht angeführt, was die Anzahl reduziert und beziehen sich oft auf den Studieninhalt und nicht auf Forschung zu CR selbst. Bei der Kategorie Limitierungen kommt hinzu, dass diese sich ausschließlich auf den Studieninhalt beschränken. Es kann allerdings gesagt werden, dass fehlende oder einseitige Daten eine Limitierung darstellt und realistische Datenquellen und deren Erzeugung ein notwendiger Bereich in der CR-Forschung einnimmt.

49 der Studien benennen künftige Forschungsfelder, davon haben 16 eine weitergefasste Vorstellung was zum Thema CR geforscht werden soll oder schlagen zumindest eigenständige Themen vor die sich aus den vorgestellten Arbeiten ergeben. Die anderen 33 beziehen sich auf die dedizierte Weiterentwicklung der vorgestellten Arbeit.

Die Arbeiten [126], [113] empfehlen Forschung zur quantitativen Messung von CR. [113] und [91] stellen den Bedarf an realistischer Messung durch realitätsnahe Angriffsszenarien oder Testbeds heraus. [132] lässt die Notwendigkeit erkennen, dass die Messung von CR ein lohnendes und wichtiges Forschungsfeld ist. [98] sieht Bedarf in der ganzheitlichen Betrachtung von Cyber Effects und der Analyse der Auswirkungen.

Allgemein gehaltene Verbesserung von CR werden in [88] und [69] gegeben. [88] empfiehlt die CR-Eigenschaften bezüglich der CR-Weiterentwicklung und Widerstandsfähigkeit zu erforschen. [69] zeigt die Notwendigkeit die Komplexität und Skalierbarkeit von Cyber-Angriffs-Erkennung zu untersuchen.

[118], [121], [110] und [115] beschäftigen sich mit Socio-ökonomischen Aspekten von CR und wie diese in Organisationen verbessert werden kann. [118] empfiehlt das Cross-Training von IT / OT Personal sowie Studien, um die geistige und mentale Belastung von IT / OT Personal zu erfassen, um geeignete Tools entwickeln zu können. In [121] wird auf die Effekte der unausgeglichenen Entwicklung in Bezug auf Digitalisierung und der Nutzung neuer Technologien zwischen Käufer und Lieferant sowie wie einflussreiche Lieferanten zur Supply Chain Visibility beisteuern können hingewiesen. Auch in [110] wird auf die Erforschung von Faktoren hingewiesen die Organisationen an der Realisierung von CR-Programmen beeinflussen. [115], welches Systeme unter Berücksichtigung Socio-Technischen Eigenschaften analysiert, empfiehlt die Untersuchung der einzelnen CR Dimensionen; Mirco Resilience meint die Resilienz einzelner Komponenten, Meso Resilience beschreibt den Umgang zu Resilienz über die ganze Organisation, Macro Resilience meint die gesellschaftliche Resilienz und die Erforschung von Gruppendynamiken und Cross-Scale Resilience, diese bezieht zu den social Aspekten auch die Umwelten mit ein.

CR von autonomen Systemen durch Nachahmung der Natur wird in [91] und [119] als lohnendes Forschungsfeld dargestellt. In [119] werden weitere Forschungsfelder für autonome Systeme evaluiert und empfohlen. Das ist zum einen wie resiliente Systeme entwickelt werden können, die aus einzelnen verwundbaren Komponenten bestehen. Oder ML-Algorithmen resilienter zu machen indem beim Design auf Resilienz geachtet wird sowie die Erkennung und Mitigation von Verwundbarkeiten zu automatisieren. Der Aspekt der automatisierten Konfiguration von Systemen wird ebenso erwähnt sowie das die benötigte Rechenleistung auf den einzelnen Komponenten verlagert wird. Es soll weiters Approximate Computing und der Einsatz in High Performance Computing berücksichtigt werden.

Forschungsempfehlungen zu CR in CMS wie die Berücksichtigung ökonomischer Faktoren werden in [135] und [134] gegeben. [59] zeigt die Notwendigkeit zur Forschung der Resilienz von Power Grids gegen e-Mobility Angriffen auf da diese mit dem Zunehmen von e-Mobilität in der Gesellschaft ein wichtiges Thema werden wird. [133] beschäftigt sich mit spezifischen Themen zu Reinfocrement Learning im Bereich System- und Performancebeschränkungen sowie der Verbesserung der Lerngeschwindigkeit der Algorithmen.

4.5. Qualitative Analyse der Publikationen

Im folgenden Kapitel werden die Inhalte der Publikationen inhaltlich qualitativ beschrieben und nach Themenbereichen abgebildet. Die zugrundeliegenden Kategorien der Forschungsbereiche wurden im

vorigen Kapitel beschrieben. Diese sind in zwei Blöcke geteilt. Die Kategorien „Analyse zu CR Definition und Frameworks“, „Statuserhebung von CR in Unternehmen/Organisationen/Länder“ und „Evaluierung und Bedarfserhebung zu CR“ können als Analyse zu CR Definition, Frameworks sowie deren Statuserhebung zusammengefasst werden. Die restlichen Kategorien beschäftigen sich mit der Umsetzung der Etablierung von CR auf unterschiedlichen Ebenen wie Frameworks, Architekturen oder Assessmentmodelle für das Systemdesign, Umsetzung in Organisationen oder technischen Systemen. Die Publikationen werden weiters in den Subkategorien zusammengefasst, die je Kategorie Forschungsbereiche wie Definitionen, Status- und Bedarfserhebung, Messung von CR sowie dazugehörige Metriken aber auch die Etablierung von CR mittels Verwundbarkeits- und Angriffserkennung und deren Mitigation umfassen. Je Unterkapitel werden die enthaltenen Studien nach der Subkategorie und den NIST CSF [141] Kategorien zur besseren Übersicht dargestellt.

4.5.1. Analyse zu CR Definition und Frameworks

Forschungsfeld Unterkategorie / NIST CSF Kategorie	Identify	Protect	Detect	Respond	Recover
CR Definition	[88], [84], [116],[134]				
Assessment und Messung von CR	[88], [126], [116],[113]				
Erkennung und Abwehr von Cyber-Angriffen	[134],[102]	[102]	[102]	[102]	

Tabelle 13 : Studien des Forschungsbereichs Analyse zu CR Definition und Frameworks nach Unterkategorien und NIST CSF [141] Kategorien

Die ursprüngliche Annahme, dass die Mehrzahl der Publikationen Definitionen zu CR bereitstellen, um Klarheit sowie die richtige Abgrenzung zum Forschungsthema zu ermöglichen ist nicht eingetreten. Mehr als die Hälfte gibt gar keine Definition an, der Haupttenor geht in Richtung der Fähigkeit von Systemen Angriffe zu erkennen, diesen zu widerstehen sowie deren Wiederherstellbarkeit. Die Aufrechterhaltung einer definierten Leistung unter Angriffen findet sich ebenfalls häufig wieder. Die Arbeiten [134], [116], [88] und [84], beschäftigen sich eingehender mit der Definition von CR, wobei dies eng mit der Fähigkeit der Messung dieser einhergeht. [116] beschreibt CR anhand von Konzepten und kommt zum Schluss, dass CR ein Multi-Faced-Konzept ist, welches unterschiedliche Themen abdeckt und speziell für komplexe Systeme, die auch soziale Bereiche einschließen, berücksichtigt werden sollte. [134], [88] und [84] haben hingegen eine klassische Definition von CR im Sinne des obig genannten.[84] beschäftigt sich gänzlich mit der Definition und geht auf den Unterscheid zu Cyber Security und deren Wechselwirkung ein. Es zeigt sich, dass die Definition Security und Resilience unscharfen aufweisen und oft ähnlich beschrieben werden. Ziel der Arbeit ist die europäische Rechtslage zu CR und Cyber Security zu beleuchten und Unterschiede sowie Gemeinsamkeiten aufzuzeigen. Dabei wird das Konzept CR kritisch hinterfragt. Die in vielen EU Regulatorien zitierten Konzepte *Security by Design* und *Security by Default* zeigen eindeutige Gemeinsamkeiten von Cyber Security und CR auf. Auf der einen Seite wird im Standard ISO 27001 mehr Wert auf die kontinuierliche Verbesserung der Security Maßnahmen gelegt als auf den kontinuierlichen Betrieb von Services. Auf der anderen Seite sind andere ISO Standards (z.B. ISO 22301) auf Business Continuity spezialisiert, setzen dafür auf eine ISO 27001 Struktur auf. Der Autor kommt zum Schluss das Cyber Security in aktuellen Gesetzen und Regulatorien nicht durch CR ersetzt wird, sondern zum Beispiel im Datenschutzbereich explizit gefordert wird. Alles in allem kann gesagt werden, dass die Unterschiede nicht das Ausmaß annehmen, welches so manche Autoren darstellen. Dies zumindest im Hinblick auf neue Gesetze die eine größere Flexibilität von Cyber Security fordern. Die Arbeit zeigt auf, dass eine adäquat entwickelte Cyber Security Strategie zwar langsamer ans Ziel kommt als eine flexible CR-Strategie, aber dennoch gleich akzeptable Ergebnisse erzielt.

Die Arbeiten [126], [113], [116] und [88] analysieren die Möglichkeiten von Assessment und Messung von CR. In [126] werden mittels Literatur Analyse Case Studies analysiert und Möglichkeiten der Messung von CR beschrieben. Dabei wurden die Bereiche Risikoanalyse und Risk-Management untersucht. Diese zeigen, dass zyklische Risk-Management-Ansätze oder die Risikoanalyse spezialisiert auf komplexe Systeme einen wichtigen Beitrag zu CR leisten können. Weiters wurden Studien zu bestehenden Frameworks wie NIST Cyber Security Framework (CSF) [141] und die damit verbundene Erhebung und Messung von CR beleuchtet. Zuletzt wird die Wichtigkeit von neuen Frameworks hervorgehoben. Hier wird der Bedarf von Frameworks für komplexe Systemen oder Organisationen oder der Bedarf an einfachen und günstigen Frameworks für SME genannt. Als Ausblick empfiehlt die Studie weiters, dass mehr Fokus auf die Quantitative Analyse von CR zum Beispiel anhand von Factor Analysis Information Risk (FAIR), ein quantitatives Modell zur Analyse von Cyber und operationalen Risiken, gelegt wird. [88] ist eine Abhandlung zu CR anhand von Definitionen, Frameworks und Messung in der aktuellen Forschung. Darin werden die Frameworks aus [43] und [42] als dedizierte CR-Frameworks hervorgehoben. Es werden Forschungen zur Messung von CR in den Kategorien „Qualitative Messung von Systemeigenschaften“, „Modeling und Simulation“ sowie „Metrik-basierte Messung“ dargestellt. Die Beziehung CR zu Network Security zeigt, dass diese unterschiedliche Aspekte behandeln. Network Security fokussiert sich mehr auf die Erkennung und den Schutz vor Angriffen. CR bringt den Faktor mit, dass ein System nie zu 100% sicher sein kann und ein Maß an garantierter Leistung im Falle eines Angriffes in Form von Response und Recovery. Ein kombinierter Ansatz kann so optimale Ergebnisse erzielen. Des Weiteren wird die Historie zu Cyber Security und CR aufgearbeitet. Es zeigt das die aktuelle Forschung sich immer noch im Stadium des Vertiefens und verbessern von CR befindet. Abschließend werden Entwicklungen von neuen Technologien wie Zero Trust und Endogenous Security hervorgehoben.

[116] ist eine Abhandlung und Zusammenfassung von CR-Konzepten mit dem Ziel eine Domain-basierte Ontologie für CR zu erstellen. Dabei wird CR meistens in 2 Arten gemessen, direkt quantitativ über die Messung von Systemkomponenten und deren Funktionsfähigkeit während eins Cyber Events und die indirekte quantitative Messung über die potenzielle Fähigkeit der Resilienz. Aus der zugrundeliegenden Analyse werden 2 Ansätze abgeleitet. Der Funktions-basierte Ansatz; Hier werden typischerweise die 4 zeitlich abhängigen Phasen Plan / Prepare, Absorb, Recover und Adopt behandelt und gemessen. Zwischen den Phasen Absorb und Recover liegt die messbare Resilienz eines Systems. Diese Messung hat ihre Schwächen bei einem sogenannten "unknown unknown" Event. Und dem Capability-basierten Ansatz; Hier werden Respond oder „Knowing what to do“, Monitor oder „Knowing what to look for“, Anticipate oder „Knowing what to expect“ und Learn oder „Knowing what has happened“ betrachtet. Hier spielt auch die Belastbarkeit durch Redundanz und Flexibilität des Systems eine wichtige Rolle. Es gilt die Balance zu halten, Ressourcen möglichst auszulasten aber bei einem Event ausreichen Kapazität zu haben, um die Funktion des Systems aufrecht zu erhalten. Laut der Studie kann eine Messung von Resilienz nur gelingen wenn die Aspekte Anpassungsfähigkeit und Belastbarkeit (Bewältigung oder Coping) berücksichtigt werden. Dies wird in der entwickelten Ontologie dargestellt. Diese leitet sich von den 2 Assessment-Ansätzen ab, die in den Aspekten Anpassungsfähigkeit und Belastbarkeit repräsentiert werden wie in Abbildung 24 gezeigt.

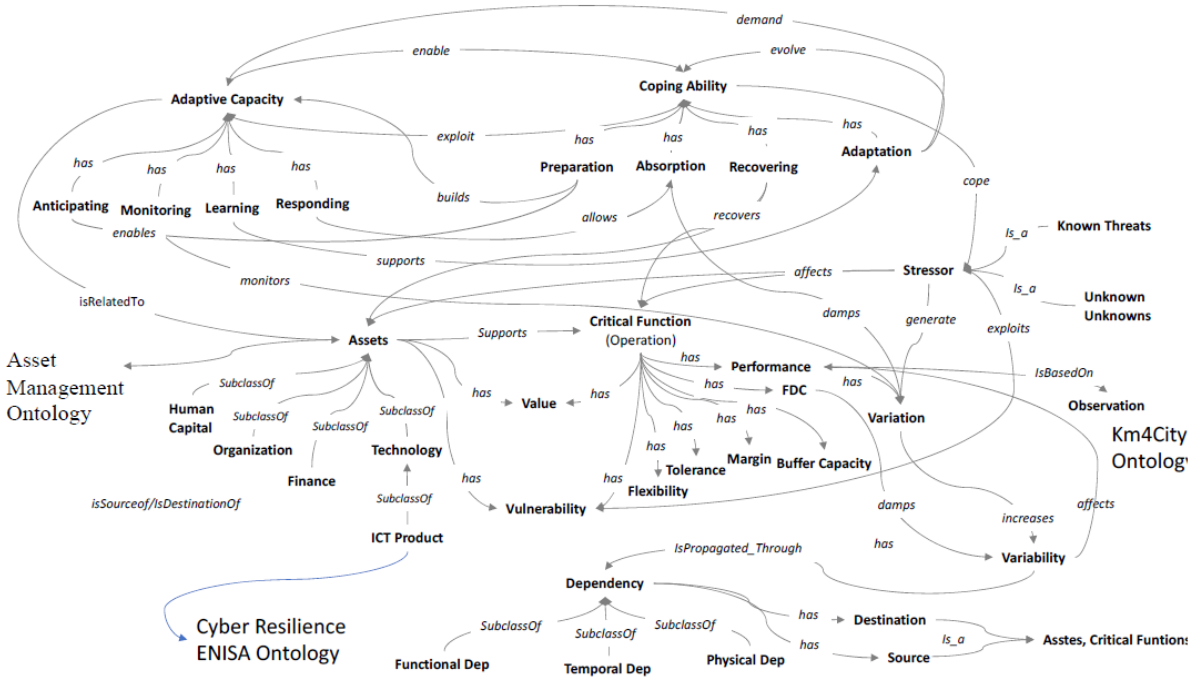

Abbildung 24 : CR-Ontologie nach [116]

In [113] werden unter der Nutzung des R4-Frameworks mit der Erweiterung von Resilience Eigenschaften bestehende Methoden zur Messung von CR analysiert, verglichen und dargestellt. Mittels Literaturanalyse werden verfügbare CR-Assessment-Methoden beleuchtet und nach ihren Eigenschaften beschrieben. Diese werden in Metric-Based und Model-Based unterschieden. In der Metric-Based-Methode misst man die Overall-System-Performance durch die Messung spezifische Attribute. Diese können in zwei Kategorien unterteilt werden, Performance-Based und Attribute-Based. Ersteres misst die Funktionen und deren Performance über die Zeit. Attribute-Based Metriken messen wie Eigenschaften die sich auf die Resilienz auswirken, diese können zum Vergleich von verschiedenen Systemen genommen werden. Im Model-Based-Ansatz werden Vorhersage und Messung durch Systemmodellierung und Szenarioanalyse erreicht. Hier kann in drei Ansätzen unterscheiden werden. Physical-Model-Based-Modelle analysieren das Verhalten des Systems im normalen Zustand und während eines Ereignisses, hier ist ein genaues mathematisches Modell des Systems nötig. Graph-Theoretic-Model-Based-Ansätze stellen das System mittels Graphen dar und analysieren die Effekte und Ausbreitung eines Ereignisses. Und Probabilistic-Model-Based-Techniken sind auf die Unsicherheiten in komplexen Systemen zugeschnitten und messen die Wahrscheinlichkeit einer Störung. Die Arbeit leitet davon einen Ausblick für fortführende Forschungen ab die bezüglich CR-Messung in CPS benötigt werden. Dieser bezieht sich auf die nicht vorhandene Flexibilität von CR-Messung und Metriken, die Notwendigkeit Cyber Angriffe realistischer darzustellen sowie diese zu kategorisieren. Testbeds würden mit realitätsnahmen oder physischen Komponenten bessere Ergebnisse bringen.

Die Arbeiten [102] und [134] beschäftigen sich mit der Analyse und Darstellung von Erkennungs- und Abwehrmethoden in CPS und Cyber Manufacturing Systems (CMS). In [102] wird die Internet Architektur Named Data Network (NDN) vorgestellt und wie diese intrinsisch CR bereitstellt. Die Arbeit beschreibt die Architektur und Funktionen von NDN ganz allgemein sowie intrinsischen CR-Funktionen im Detail. Die NDN-Architektur hat Sicherheitsmechanismen und Funktionen, um unterschiedlichen Angriffen entgegenzuwirken beziehungsweise diese zu vermeiden. Durch intensiven Gebrauch von Kryptographie für Verschlüsselung und signieren auf Header-, Content- und Paketebene wird die Vertraulichkeit und Integrität geschützt und mögliche Angriffe massiv erschwert. Dadurch kann auch die Authentizität des Absenders geprüft werden. Für die Threat-Erkennung werden die Netzwerkpakete überwacht, so können Distributed Denial of Service

(DDoS) Angriffe erkannt werden und darauf reagiert werden. Diese werden durch Dropping oder Blockieren mitigiert, im Zuge dessen werden andere Netzwerkgeräte in der Umgebung gewarnt. Es werden mögliche Angriffsvektoren in Vehicular-CPS aufgezeigt und wie NDN diesen entgegenwirkt. Als Beispiele werden genannt; DDoS, Man-in-The-Middle Attack (MiTM), Packet Injection. Außerdem werden die Herausforderungen von NDN wie Access Control, Anonymität von Komponenten in Vehicular-CPS oder Real-Time-Anforderungen behandelt. Diesen sollen sich künftige Arbeiten widmen. [134] beleuchtet die Resilienz von CMS, und erhebt Resilienz- erhöhende Mechanismen und deren Bedeutung für CMS. Mittels Literaturanalyse wird die Definition von Resilienz in Systemen beleuchtet, um Klassen für Resilienz-Mechanismen zu entwickeln. Dabei werden 4 Klassen definiert. Diese sind „Wahrscheinlichkeit eines erfolgreichen Cyber Angriffes reduzieren“, „Zeit der Angriffserkennung reduzieren“, „Die Auswirkungen eines Angriffes reduzieren“ und „Zeit der Wiederherstellung reduzieren“. Diese Klassen werden mit aktueller Forschung analysiert, um mögliche Techniken aufzuzeigen. Die Arbeit kommt zum Schluss das viel Forschung zu CPS betrieben wird, aber sehr wenig zur CMS. Bestehende Frameworks zu CPS sind für CMS nicht ausreichend und müssen dafür weiterentwickelt werden.

4.5.2. Statuserhebung von CR in Unternehmen/Organisationen/Länder

Forschungsfeld Unterkategorie / NIST CSF Kategorie	Identify	Protect	Detect	Respond	Recover
CR in Organisationen	[110],[108] [130],[128] [137], [76], [94]				

Tabelle 14 : Studien des Forschungsbereichs Statuserhebung von CR in Unternehmen/Organisationen/Länder nach Unterkategorien und NIST CSF [141] Kategorien

Nachfolgende Arbeiten befassen sich mit der Erhebung von CR und welchen Stand oder Reifegrad in Organisationen oder staatlichem Umfeld vorzufinden ist. Die Motivation solcher Erhebungen ist das sich rasch ändernde Umfeld in kritischen Infrastrukturen und öffentlichen Bereichen.

[128] analysiert in einer nationalen Online-Umfrage im Schweizer Energiesektor deren Cyber Security und CR-Maturity. Die Umfrage erhebt den Reifegrad von IT und Operation Technologie (OT) nach Domänen des NIST CSF [141] (Indentify, Protect, Detect, Respond, Recover) in den Reifegradstufen 0 bis 4, wobei 0 ein Basisniveau darstellt und 4 optimierte und laufend angepasste Prozesse sicherstellt. Das Ergebnis zeigt ein eher mageren Reifegrad von ungefähr 1 über alle Bereiche. Gründe dafür sind unter anderem, dass im Schweizer Energiesektor keine verpflichteten Regulatorien existieren. Außerdem zeigt sich, dass Unternehmen die keine klare Strategie und Verantwortlichkeit zu Cyber Security entwickeln, wesentlich unter 1 liegen und damit ebenfalls den Durchschnitt reduzieren. Außerdem gaben 90% der Firmen an Cyber Security Aspekte beim bevorstehenden Rollout von Smart Meters zu berücksichtigen. Ein weiterer Teil der Arbeit war der Vergleich mit europäischen Nachbarländern sowie die Erhebung der dort gültigen Regulatorien und eine Empfehlung zur Erstellung von Richtlinien für den Schweizer Energiesektor. Im Gegensatz zu Europa hat die Schweiz weder verpflichtende Richtlinien noch ganzheitliche regulative Frameworks oder Guidelines. Der Vergleich zeigt auf der einen Seite das bestehende nationale Maßnahmen weitest mit denen der NIS-Richtlinie [6] übereinstimmen. Auf der anderen Seite gibt es klare Abstriche im Verglich zum ACER-Framework, ein von der CEER, der Council of European Energy Regulators, entwickeltes Instrument um spezifische Cyber Security -Maßnahmen vorzugeben. Abschließend wurden Empfehlungen für regulative Vorgaben im Schweizer Energiesektor definiert, die unter anderem denen der NIS-Direktive [6] ähneln.

[94] besagt das die fortschreitende Digitalisierung und Bedeutung von Flughäfen eine verbesserte Sicherheitskultur notwendig macht. Mittels Umfragen an Airports in USA und Europa wurden die Bereiche technischer und organisatorischer Natur, Erhebung von Sicherheitspolicies und Praktiken auf mögliche

Sicherheitslücken hin analysiert. Dabei wurden die Ergebnisse nach Airports je Reifegrad evaluiert. Die Reifegrade richten sich nach einer Basic-, Agile- und Smart-Ausstattung von Flughäfen. Das Ergebnis zeigte größere Lücken in Flughäfen der Kategorie Basic, die anderen Kategorien schnitten jeweils besser ab. Verbesserungsbedarf besteht vor allem bei Awareness Trainings für Mitarbeiter aber auch für externe Parteien. Weiters scheint es eine Lücke bei der Implementierung von Intrusion Detection Systeme (IDS) zu geben auf der anderen Seite ist die Nutzung von Standardlogins weitverbreitet. Dazu kommt das BYOD Controls schlecht, bis gar nicht implementiert sind. Die Ergebnisse zeigen das weitere Anstrengung zu Cyber Security und Resilience-Konzepten und deren Umsetzung nötig sind.

[76] ist eine Studie zu nationalen Cyber Security Strategien von Asia-Pazifischen Ländern. Es wird anhand der öffentlich verfügbaren Cyber Security Guidelines der Länder erhoben wie das Kommitment und die Umsetzung von Cyber Security und dem Umgang mit Cyber-Bedrohungen in diesen Ländern voranschreitet. Es wird als Beispiel Neuseeland mit einem hohen Reifegrad hervorgehoben und dessen weiten CR-Fokus der bis in die Zivilgesellschaft reicht. Generell sieht man das eher der öffentliche und private Sektor gesteuert und gefördert wird und für die Zivilbevölkerung wenig Angebot vorhanden ist. Hier wurden neben dem Schutz von vulnerablen Gruppen wie Kinder und Jugendliche auch öffentliche Portale zur Meldung aber auch Meinungsbildung zur Cyber Crime genannt. [130] identifiziert hingegen Elemente, die CR im Bereich Public Transport beeinflussen. Ein Vergleich statistischer Daten der Visegrad Four (V4) Länder, die Tschechische Republik, Ungarn, Polen und Slowakei, soll den CR-Status der Länder aufzeigen. Diese wurden gewählt da ähnliche Vorgaben aus dem V4-Framework einen Vergleich möglich machen. Dazu werden fünf Kategorien definiert „Nationale Strategien für Bildung“, „Bekämpfung von Cyber Crime“, „Fähigkeiten Cyber-Angriffen zu begegnen“ und „Unterstützung für die Weiterentwicklung und internationale Kooperationen mit Fokus auf Transportwesen“. Die Daten wurden weiteres mit den 2017 Global Cyber Security Index (GCI) verglichen. So kann die CR-Readiness bezüglich des Transportwesens der genannten Länder dargestellt werden. Polen gefolgt von Tschechien sind aufgrund deren nationalen Strategien für Bildung und Training sowie der Bekämpfung von Cyber Crime vorne auf. Alle 4 Länder hingegen zeigen ähnliche Werte gemäß dem GCI-Index auf. Die Arbeit bietet weiters Empfehlungen zur Steigerung der CR je Kategorie.

In [110], [108] und [137] wird auf die CR in Organisationen eingegangen. [110] beschäftigt sich mit einer Umfrage wie Unternehmen Security und Resilience für Enterprise Netzwerke sicherstellen und die Auswirkung auf CR. Dabei wurden Unternehmen aus 3 Sektoren Banken, Öl und Gas sowie höhere Bildung aus Port Harcourt im Niger Delta befragt. Die Lage wurde wegen ihrer Bedeutung für Nigeria und dessen schnellen Wachstum und Anpassung der dortigen Kommunikationsnetze gewählt. Die Fragen waren neben statistischen Daten Themen zu Erfahrung in Cyber Security , CR-Strategien und Governance sowie Praktiken bezüglich CR und Security in Enterprise-Netzwerken sowie Incident Response und Vulnerability Management. Das Ergebnis zeigt das die Sektoren Banken und Gas und Öl die besten CR-Praktiken sowie Strategien und Programme haben. Alle Sektoren sind sich der Notwendigkeit von CR bewusst und bringen ein ausreichendes Verständnis zu CR mit. Der Bildungssektor weist allerdings Schwächen in Security-Praktiken auf. [137] erhebt mittels Interviews wie das Verständnis zu CR in Organisation verbessert werden kann und zeigt bestehende Herausforderungen auf. Es wurden insgesamt 25 Interviews mit Führungskräften und Vorstandsmitgliedern geführt. Das Ergebnis kann in 4 Aspekte geteilt werden. Erstens, die Position des CISOs in der Organisation, diese sollte mit möglichst kurzen Kommunikationswegen dem CEO zugänglich sein. Es zeigt sich wenn die CISO-Rolle in einer Organisation sozusagen versteckt wird und eine direkte Kommunikation nicht erfolgt, die Organisation Fähigkeiten zur CR einbüßt. Das zweite Konzept widmet sich der Stellung von Personen und Kultur. Zum einen wird gezeigt das Awareness und das Aufbrechen von Silos in der Organisation maßgeblich für die Verbesserung von CR ist. In diesem Zuge wird die Unternehmenskultur als wichtiger Faktor bewertet. Drittens wird das Verständnis für CR und Cyber Security für das Top-Management herausgehoben. Das Top-Management muss laufend über Aktivitäten zu CR und Security informiert werden und ein Verständnis für die Materie entwickeln. Dieses Thema stellt für viele Organisationen nach wie vor eine Herausforderung dar. Schließlich wird auf die Governance rund um Cyber hingewiesen. Es wird die Notwendigkeit einer Strategie sowie Investments betont. Nur mit einem ganzheitlichen Risikoansatz sowie Governance kann eine gute CR in Organisationen erreicht werden. In

[137] wird der Umgang und das Management von CR in Organisationen anhand von 6 Unternehmensanalysen analysiert. Dabei soll ein kontextbasiertes Framework zum Management von CR entwickelt werden. Weiters werden die Zusammenhänge der unterschiedlichen Unternehmen nach Kontext erhoben. Die Studie erhebt bestehende Frameworks und ordnet sie den Kontextfaktoren „Infrastruktur“ (kritisch und Nicht-Kritisch), „Industrie“ (Consumer oder Customer-oriented) und „Ownership“ sowie private oder öffentliche Unternehmen zu. Die Case Studies oder Unternehmensanalysen werden anhand von Interviews durchgeführt, wobei die Fragen für die zwei Bereiche „Cyber Resilience Context“ und „Actions for Cyber Resilience“ entwickelt werden. Das Ergebnis zeigt, dass Customer-orientierte Unternehmen sich auf die Protection Phase von CR konzentrieren. Werden kritische Strukturen festgestellt rücken Technologien wie SIEM in den Vordergrund und bei privaten Organisationen wird der Fokus auf Prevention gelegt. Alle Unternehmen legen großen Wert und sehen die Wichtigkeit auf Training zu Cyber Security sowie AI als Chance für die Zukunft um CR im Unternehmen sicherzustellen.

4.5.3. Evaluierung und Bedarfserhebung zu CR

Forschungsfeld Unterkategorie / NIST CSF Kategorie	Identify	Protect	Detect	Respond	Recover
Bedarfserhebung in Entwicklung und Design	[118],[135] [89],[87]	[119], [135]	[118], [119]	[119]	
Assessment und Messung von CR	[98], [91]		[98]		
Metriken	[87]				
CR in Organisationen	[121], [72]	[136]		[136]	[136]
Erkennung und Abwehr von Cyber-Angriffen		[133]	[69], [133]	[69], [133]	

Tabelle 15 : Studien des Forschungsbereichs Evaluierung und Bedarfserhebung zu CR nach Unterkategorien und NIST CSF [141] Kategorien

Neben der Statuserhebung stellt die Erhebung von Bedarf zu CR in unterschiedlichen Kontexten einen wichtigen Bereich in der aktuellen Forschung dar. [91] und [98] widmen sich der Bedarfserhebung zur Messung von CR im CPS-Umfeld. [91] zeigt Möglichkeiten und Herausforderung bei der Messung von CR in CPS oder anderen Systemen unter der Zuhilfenahme von autonomen Agents. Folgende Ansätze zur Messung von CR wurden herausgestellt; Qualitative Messung der betroffenen Systeme, Wahrscheinlichkeitsschätzung durch Experten wie etwa mittels Risiko-Matrix oder System Modeling sowie Simulationen zur Messung der Auswirkungen von Ereignissen. Ähnlich zu Simulationen, sind Wargaming und Red Teaming Übungen oder Penetrationtests. Diese sind flexibler in ihrer Ausführung und können leichter an realistische Szenarien angepasst werden. Im Unterschied zu Simulationen sind diese Varianten für die einmalige Durchführung gedacht. Spezifisch für die Messung von Resilienz sind Ansätze wie die Messung der Wiederstandfähigkeit und Recovery über die Zeit, oder aber die Messung der Leistung im Sinne von "Mission Accomplish" sowie den Aufwand den ein Angreifer und die Abwehr davon benötigt. Für die Messung mit autonomen Agents bietet sich eher die Messung der Komponenten, auf denen der Agent läuft an, als die Messung des gesamten Systems. Denkbar ist auch eine zentrale Stelle die Daten mehrerer Agents sammelt. [98] hingegen beschreibt das Zusammenspiel von Cyber-Sicherheit und Resilience in der Messung mit bekannten Metriken im Umfeld von CPS. Dabei wird der Impact Subscore (ISC) von Common Vulnerability Scoring System (CVSS) herangezogen um die Sicherheit zu bewerten sowie die Metriken der Infrastructure Resilience Analysis Methodology (IRAM); Systemic Impact (SI), Total Recovery Effort (TRE) und Recovery Dependent Resilience (RDR), um die Resilience von Kontrollsystemen zu erheben. Es werden 9 Szenarien ausgewählt, um die Metriken zu testen. Dies wird in einem Experiment an einem Load Frequency Controler umgesetzt. Das Ergebnis zeigt, dass die Prioritäten von Security und Resilience nicht immer übereinstimmen und eine komplementäre Sichtweise ein ganzheitliches Bild auf die Auswirkung von

Cyber Events schaffen. So sind einige Szenarien aufgrund ihrer Auswirkung auf Sicherheit als Low eingestuft, die Auswirkungen auf die Resilience sind allerdings wesentlich höher oder umgekehrt.

Die Arbeiten [118], [119], [135], [89] und [87] beschäftigen sich mit der Bedarfserhebung in Design und Entwicklung neuer Lösungen in der Software- und Hardwareentwicklung aber auch im Systemdesign von technischen Lösungen. In [118] wird das Design von Security-Tools im IT / OT Umfeld behandelt. Es werden Anforderungen an künftige Tools und Konzepte anhand von Interviews von IT / OT Experten erhoben. Besonders herausgesellt werden die Soft-Facts, Herausforderungen der gemeinsamen Kommunikation, des übergreifenden Monitoring und Tracking von Ereignissen über IT und OT-Systeme und eine einfache Usability um neue Tools mit möglichst wenig Aufwand und Training zu migrieren. Ein zentrales Tool bezüglich Monitoring von Ereignissen und Workflows wurde mehrfach hervorgehoben. Denn wachsende Komplexität von Tools und Systemen überfordert das Personal und kann so zu einer schlechteren CR führen. [119] ist eine Abhandlung von CR in autonomen Systemen für Design, Resilienz Bedarf sowie künftige Forschungsbereiche. Es werden zwei Aspekte von CR herausgehoben, „CR by Design“, also das Design und die Entwicklung von resilienten Systemen und „CR by Reaction“, also wie auf ein Ereignis reagiert wird. Hier kann zwischen Fehler natürlichen Ursprunges, bösartigen Angriffen oder unerwarteten Ereignissen durch Interaktion mit dem Umfeld unterschieden werden. Im Design von resilienten autonomen Systemen können die Herausforderungen bei der Entwicklung von ML-Algorithmen und deren Absicherung, verwundbare Komponenten ganz allgemein und der Validierung in der automatisierten Entwicklung von Programmen genannt werden. Im Bereich „CR by Reaction“ sind Themen wie Live-Rekonfiguration, Anomalie-Erkennung, Approximate Computation und Resilience genannt. Diese werden mit einer Problemstellung und Verbesserungsbedarf sowie einer Art Roadmap welche Prioritäten zu setzen sind detailliert beschrieben. In [89] werden bestehende Frameworks und Techniken evaluiert, um die Notwendigkeit aber auch die Charakteristiken für cyber-resiliente Microarchitekturen für Embedded Systeme in kritischen Infrastrukturen zu erarbeiten. Die betrachteten Frameworks und Regulatorien sind NIST Risk-Management Framework (RMF), NIST CSF, NSCS Security of Network und Information Systems Regulations. Wobei die Domänen Identify, Protect, Detect, Respond und Recover des NIST CSF für eine Gegenüberstellung der Frameworks sowie der existierenden Praktiken im Bereich Embeeded System Development verwendet werden. Es werden weiters die Herausforderungen sowie die Schwachstellen der bestehenden Security Design Prinzipien im System Design vorgestellt. Zum Abschluss werden Empfehlungen zum Design von Cyber-resilienten Embeeded Systemen beschrieben. [135] beschäftigt sich mit möglichen und wünschenswerten Forschungsfeldern für sicheres Smart Manufacturing im Kontext von Industrie 4.0. Dahingegen ist das Ziel von [87] das Design von CPS und deren Resilienz zu evaluieren. Hier werden Metriken zur Messung von CR in CPS bezüglich Stabilität und Performance entwickelt und in einer Simulation getestet. Abschließend werden Empfehlungen des CPS Design in einem Stufenmodell vorgestellt.

Wie CR in Organisationen etabliert werden kann wird in [136], [121] und [72] behandelt. [136] erhebt Anforderungen und Best Practice Ansätze für CR in Multinationalen Kooperationen (MNC) im Industrieumfeld. Es werden die Herausforderungen vom MNC vorgestellt, wie zum Beispiel höchste Automatisierung oder der Vernetzung von sehr großen Systemen. Es werden 4 Schlüsselbereiche für eine praktikable und effektive CR in MNC herausgestellt. Das ist zum einen das Infrastruktur Design im Sinne von Security, Redundanz und Diversity, welche die Resilienz maßgeblich erhöhen. Wobei Diversity in Plattformen bei Industrieanlagen (zum Beispiel bei der Trennung von Monitor- von der Produktionseinheiten) und Backup herausgestrichen werden. Weiteres das Change Management, hier wird die Wichtigkeit herausgehoben das Änderungen gesteuert werden müssen, um Ausfälle und Inkompatibilität zu vermeiden. Der dritte Bereich sind Backups, hier werden Anregungen zum sicheren Betrieb einer Backup Infrastruktur gegeben. Und viertens Resourcing, damit ist gemeint das man den Herausforderungen der Wartung und Instandhaltung begegnen muss. Dabei wird der externe Support und damit bedingt die Erreichbarkeit aus der Ferne sowie der interne Druck bezüglich Kostenminimierung besonders hervorgehoben. Abschließend werden folgende Empfehlungen gegeben. Das Bewusstsein bezüglich der Wichtigkeit und Tatsache dass Industry Control Systems (ICS) ein Spezialfeld in der Cyber Security ist zu stärken und das dafür oft externe Spezialisten

benötigt werden. Dabei darf das Testing und der Rollout oder Patching-Prozesse nicht außer Acht gelassen werden. Außerdem wird darauf hingewiesen das Cyber Security bezüglich Supply Chain zu beachten ist und so der Nutzen hier für alle Beteiligten gesteigert werden kann. Ebenfalls der Thematik Supply Chain widmet sich [121] . Es werden die „Absorptive Capacity „ (die Fähigkeit neue Technologien zu absorbieren) sowie „Supply Chain Power“ (der Einfluss auf Lieferanten / Käufer) als Stufen der Visibilität vorgestellt und wie sie sich auf CR auswirken. Dafür wurden 2 empirische Studien mittels Umfragen durchgeführt. Studie 1 beschäftige sich mit der Frage wie Absorptive Capacity und Supply Chain Power sich auf Supply Chain Visibilität und damit auf die CR auswirken. Studie 2 befasst sich mit den Unterschieden von einflussreichen Käufern versus einflussreichen Lieferanten und deren Auswirkung auf die Supply Chain Visibilität. Das Ergebnis zeigt bezüglich der Fähigkeit neue Technologien zu absorbieren, dass sowohl Käufer- und Lieferantenseite dadurch positive Auswirkungen auf Supply Chain Visibilität und CR erzielen. Wie die Studie angenommen hat, wirkt sich ein einflussreicher Käufer positive auf Supply Chain Visibilität und Information Sharing aus, wobei ein starker Lieferant geneigt ist Information zurück zu halten, was sich wiederum negativ auf CR auswirken kann. Absorptive Capacity sollte in Supply Chain als Priorität angesehen werden da so schneller eine Supply Chain Visibilität aufgebaut werden kann. Diese wiederum sollte dazu genutzt werden, um die CR im Bereich Data Breaches und Cyber-Angriffe zu stärken. [72] stellt ein systemdynamisches Simulationsmodell für SME vor, um die Effekte für CR bei Investment in Training und Awareness versus Investment in Technologie darzustellen. Dabei wurden 3 Kausalschleifen identifiziert die CR in SME beeinflussen. Eine Kausalschleife besagt das Awareness Trainings die Awareness in Technologie und Training zu investieren exponentiell erhöht und damit die CR selbst. Die zweite Schleife "Investment in Training um CR zu erhöhen" besagt, dass ein Erhöhen von CR den Schaden durch Serviceausfälle verringert und dies wiederum hat zur Folge hat, dass die Wahrnehmung für Notwendigkeit von CR abnimmt und daher Awareness Trainings vernachlässigt werden. Das gleiche gilt auch in umgekehrter Folge, was diese Schleife zu einer balancierenden Schleife macht. Die dritte Schleife besagt, dass ein investieren in Cyber-Technologie die CR erhöht, was wiederum dazu führt das die Servicekontinuität verbessert wird. Auch hier gilt, dass dies wieder bedingen kann, dass Investitionen in Cyber-Technologie weniger Ausfälle erzeugen und daher ein falsches Sicherheitsbewusstsein entstehen kann. Setzt man die Verhaltensschleifen in die Extremfälle das nur in Training oder nur in Technologie investiert wird, kommt man zum Schluss das durch die verbesserte technische Sicherheit und damit einhergehende CR die Awareness und letztendlich auch die CR abnimmt, da man sich weniger verwundbar sieht. Ein reines Investieren in Training bedingt das man kurzfristig eine geringere CR aufweist, dies aber über die Zeit steigt da ein ständiges Bewusstsein für Investment in Training und Technologie entwickelt wird. Die Autoren kommen zu dem Schluss das ein Fokus auf Awareness Training am Ende zu einer höheren CR führt.

Die Arbeiten [69] und [133] haben den Fokus bei der Erhebung von Erkennungs- und Abwehrmechanismen im Design von Systemen. [69] beschreibt die Erhebung und Analyse von Cyber Security und CR-Methoden um Smart Grids vor typischen Angriffen wie False Data Injection (FDI) und DDoS zu schützen. Der Vergleich von bestehenden Methoden wird mittels Literatur Analyse durchgeführt. Es wurde herausgestellt, dass eine akkurate Erkennung, genügend Rechenleistung und die Robustheit gegen externe Faktoren die größten Herausforderungen darstellen. Es wird in Model-Dependent und Model-Driven-Methoden (Data-Driven) unterschieden, letzteres weist Methoden auf, die alle drei Bereiche adressieren. Wobei die akkurate Erkennung von Angriffen sich bei Data-Driven-Methoden als schwierig herausstellt. Die Rechenleistung ist ein notwendiges Übel, dass für stabile und sichere Power Grids zu akzeptieren ist. Die Arbeit zeigt, dass die Robustheit gegen externe Einflüsse als wichtig erkannt wurde aber in aktuellen Studien wenig adressiert wird. [133] beleuchtet Reinforcement Learning (RL)-Algorithmen und wie diese in Cyber-Resilience-Mechanismen-Designs und Applikationen gegen Cyber-Angriffe eingesetzt werden. Zuerst werden 3 Arten von Verwundbarkeiten klassifiziert. Posture-related, diese beziehen sich auf die verfügbaren (geringen) Ressourcen der Verteidiger und der daraus ergebenden Angriffsfläche. Information-Based bezieht sich auf Verwundbarkeiten bezüglich der verfügbaren Information über die Angreifer und Verteidiger, wobei hier davon ausgegangen wird das die Angreifer hier im Vorteil sind. Und Human-Based-Verwundbarkeiten, diese sind auf die Schwachstelle Mensch zurückzuführen. Dies kann sich auf Social Engineering oder der begrenzten Belastbarkeit und Fehleranfälligkeit von menschlichen Verhalten beziehen. Den

Verwundbarkeiten soll in Cyber-Resilience-Mechanismen-Designs wie Moving Targed Defense, Defensive Cyber Deception sowie unterstützende Humansicherheitstechnologien entgegengewirkt werden. Es werden je Verwundbarkeitsklasse Anwendungen vorgestellt sowie ein Angreifer-Modell für RL-Applikationen. Neue Technologien im Bereich von RL sind der Schutz von Wireless Systemen vor Jamming und Spoofing Angriffen, Technologien im IoT und CPS Bereich aber auch Cyber-Versicherungen, als CR-Aspekt, um ökonomische Auswirkungen bei einem Cyber Vorfall zu reduzieren.

4.5.4. CR-Frameworks

Forschungsfeld Unterkategorie / NIST CSF Kategorie	Identify	Protect	Detect	Respond	Recover
Assessment und Messung von CR	[82]				
CR in Organisationen	[70],[131], [82],[114], [71]	[131], [71]	[70]	[131]	
Erkennung und Abwehr von Cyber-Angriffen	[93]		[66],[112], [120],[93], [75]	[66],[112], [120],[93], [75]	
CR mit Fokus auf Recovery					[90]

Tabelle 16 : Studien des Forschungsbereichs CR-Frameworks nach Unterkategorien und NIST CSF [141] Kategorien

Die analysierten Publikationen zu CR-Frameworks können fast ausschließlich in Frameworks für Organisationen und sowie Frameworks mit Fokus auf der Erkennung und Abwehr von Angriffen unterteilt werden.

In [71] wird AMBI-CYBER vorgestellt. Dieses beschreibt CR in einem ambidextren Modell. Dabei geht es um die Balance von Exploitation (vorhandene Ressourcen optimal nutzen) und Exploration (flexibel und innovativ Chancen erkennen und nutzen) und so effiziente und effektive Cyber Security und CR sicherzustellen. AMBI-CYBER bedient sich zum einen dem Konzept Cyber Security Efficient Frontier (CSEF) wo der Fokus klar in der Entwicklung von neuen und innovativen Technologien steht, um so die Grenzen der Effizienz zu erweitern. Auf der anderen Seite wird das 7Ps Stufen Modell (Patient, Persistent, Persevering, Proactive, Predictive, Preventive, and Preemptive) vorgestellt, welches das proaktive Verhalten erweitert. Ein weiterer Aspekt der Studie ist die Betrachtung des gesellschaftlichen und politischen Kontextes und zeigt die Wichtigkeit das CR von Regierungen und Behörden definiert und mittels Standards vermittelt wird. Ein ähnlicher Ansatz wird in [131] vorgestellt, das Framework FLEXI, ein Ansatz der davon ausgeht das Fehler im System vorhanden sind und zeigen will, dass diese genutzt werden können um neue Wege zu gehen. So können Organisationen eine CR-Kultur entwickeln und sich rasch an Ereignisse anpassen und reagieren. In [114] wird ein Framework entwickelt, um CR in SMEs zu etablieren die bisher wenig bis keine Aufmerksamkeit auf CR gelegt haben. Die umfassende Arbeit evaluiert 18 CR-Frameworks auf die Anwendbarkeit für SME. Das Ergebnis bringt ein Framework mit 10 Domänen und 32 Unterkategorien. Sowohl die Entwicklung als auch die Evaluierung wurden mit mehreren Experten durchgeführt, um die Anwendbarkeit und praktische Implementierung für SME sicherzustellen. In [82] wird das Framework und eine Implementierungshilfe erweitert sowie ein Self-Assessment-Tool (CR-SAT) vorgestellt. Dieses stellt die Maturity und Progression dar und wird via Webinterface zur Verfügung gestellt. Eine Evaluierung des Ansatzes wird schließlich in 3 Case Studies an drei Unternehmen unterschiedlicher Branchen evaluiert. In [70] werden mittels Literarturanalyse technische Architekturen zur Erkennung und Monitoring von Cyber Events erhoben und in einem CR-Modell für SME beschreiben. Die Ansätze und Techniken der erhobenen Studien werden in ein 5-Stufen-Modell integriert, das CD-Modell. Jede Stufe beschreibt die technische Architektur und deren Aufbau. Stufe 1 beschreibt die Services wie beispielsweise DNS, welches für SME als

fundamentales Service dargestellt wird und häufig für Angriffe genutzt wird. Stufe 2 verarbeitet die Daten der Services und bereitet sie für die höheren Stufen vor. In Stufe 3 werden mittels verschiedenen mathematischen Modellen und ML-Techniken ein Monitoring der Daten ermöglicht. Stufe 4 und 5 dienen der Anomalie-Erkennung und Darstellung wobei Stufe 5 auch die Messung und Darstellung des Resilience-Scales über die Zeit gewährleistet. Die Studie hebt hervor das SME nur limitierte Ressourcen hat, um CR im Unternehmen zu implementieren, bleibt aber schuldig wir das CR-Modell implementiert oder umgesetzt werden kann.

[112], [120], [66] stellen CR-Frameworks für CPS in der kritischen Infrastruktur mit Fokus auf Erkennung und Abwehr von Angriffen vor. [112] behandelt CR für Large-Scale-Wind-Parks. Das entwickelte Framework stellt einen resilienten Betrieb unter DoS und Deception-Angriffen sicher. Wind-Parks sind anfällig für sogenannte Sub-Synchronous Interaction (SSI), eine Schwäche im Bereich der Systemstabilität. Die Studie präsentiert einen SSI-dämpfenden Controller, welcher ein gewünschtes Maß an Resilienz sicherstellt und in der Lage ist DDoS oder Deception-Angriffe zu erkennen und abzuwehren. Weiters wird das dazugehöriges "*Takagi-Sugeno (T-S) Fuzzy Framework*" entwickelt, um die Unbeständigkeit in Energiesystemen von Windparks zu simulieren und den Controller darauf abzustimmen. Durchgeführte Simulationen zeigen wie das entwickelte Framework zufriedenstellende Ergebnisse bei der Erkennung und Abwehr von DDoS und Deception-Angriffen leistet. In [120] wird ein Kontrollansatz zur Absicherung von Islands Micro Grids vor hybriden Cyber-Angriffen, DDoS und False Data Injection, vorgestellt. Dabei wird ein CR-Ansatz entwickelt, welcher die Secundary-Control-Methoden verbessert. Diese sind aufgrund der Eigenschaften in Islands Micro Grids nötig, um Abweichungen im Primär-Control-Systemen abzufangen. Dieser wird weiters mittels Simulation in einem OPAL-RT Simulator durchgeführt. Das Ergebnis zeigt, dass die entwickelte Methode Hybrid-Angriffen effizient entgegenwirken kann. [66] entwickelt das HMADS-Framework, ein Hirachical Multi-Agent Dynamic System zur Sicherstellung von CR in Control Systems im Energiesektor. Diese umfasst ein Tiering Modell aus den Tiers „Orchestration“ zur Cyber Defense Definition und Priorisierung, „Intermediate Defense“ zur Netzwerkanalyse und Anomalie-Erkennung und dem dritten und niedrigsten Tier „Distribution Defense“, welches motivierende Aktionen setzt. Es werden Cyber als auch physische Interaktionen berücksichtigt, um eine vollständige Sicht sowie Reporting von Cyber Angriffen zu ermöglichen. HMADS bietet mit Feedbackmethoden einen Response Mechanismus der anderen Frameworks überlegen ist.

[93] stellt ein Framework zur Systementwicklung unter Berücksichtigung von CR-Aspekten vor. Dabei werden CR und Systemanforderungen in Form von Graphen unter Verwendung von Model Based System Engineering (MBSE) Tools dargestellt. Der Fokus bei CR-Anforderungen liegt auf Cyber Effekts im Sinne von Störungen und Angriffe und nicht auf Verwundbarkeiten. Durch definierte Schwellwerte für Vertraulichkeit, Verfügbarkeit und Integrität aber auch der Anzahl und Intensität von Vorfällen sollen Schwachpunkte im Design aber auch in den Schnittstellen des Systems aufgezeigt werden. Die Arbeit zeigt, dass es keine Daten gibt die allgemein benutzt werden können und diese individuell entwickelt werden müssen. Außerdem können bestehende MBSE-Tools das Graphen-Framework nicht integrieren und sämtliche Darstellungen sind gesondert zu erstellen. Dennoch ist es ein deutlicher Mehrwert die Auswirkung von Cyber Effekten auf die CR in jedem einzelnen Entwicklungsschritt darzustellen.

Ein weiteres Framework wird in [75] vorgestellt. AWaRE soll genutzt werden, um autonome Systeme mittels Selbstverwaltung resilient vor Angriffen oder sonstigen Anomalien zu machen. Es wird die Architektur sowie die Prototypinstallation vorgestellt. Das Framework ermöglicht mit einem State-Space-basierten Konzept ein resilientes Systemdesign, dabei werden Systemkomponenten durch definierte Eigenschaften in Zustände eingeordnet. Eine (Re-)Konfiguration wird mittels Abhängigkeiten der Zustände realisiert. Das AWaRE-Framework kann mittels Domain-Specific-Language (DSL) modelliert werden.

Schließlich wird in [90] ein CR-Recovery-Framework vorgestellt. Es soll sicherzustellen, dass besonders kritische Bereiche und Assests akkurat und resilient wiederhergestellt werden. Das Framework umfasst 9 Hauptkategorien (Identify, Control, Map, Plan, Playbook, Measure, Test und Improve) und 41 Subkategorien. Daraus können Organisationen ein für sie passendes CR-Recovery-Konzept entwickeln.

4.5.5. CR-Architekturen

Forschungsfeld Unterkategorie / NIST CSF Kategorie	Identify	Protect	Detect	Respond	Recover
Metriken	[122]		[122]	[122]	[122]
Erkennung und Abwehr von Cyber-Angriffen	[122]		[122],[107], [61],[111], [68],[127], [78]	[122],[107], [61],[111], [68],[127], [78]	[122],[107], [61],[68]
CR mit Fokus auf Recovery	[122]		[122]	[122]	[122], [61]

Tabelle 17 : Studien des Forschungsbereichs CR-Architekturen nach Unterkategorien und NIST CSF [141] Kategorien

:Die Schwerpunkte der analysierten CR-Architekturen liegen in der Erkennung und Abwehr von Cyber Angriffe, [61] und [122] stellen dieses durch Recovery-Konzepte sicher.

In [61] wird ein Modell vorgestellt, dass embedded Control Units in CPS sicher vor Veränderungen macht und somit eine garantierte physische Sicherheit für das CPS bereitstellt. Dies soll erzielt werden in dem der Zeitpunkt zur sicheren Wiederherstellung im Falle einer Kompromittierung berechnet wird und die Control Unit mittels vollständigem Systemneustart in einen sauberen Zustand wiederhergestellt wird. Damit ist ein Systemneustart und das Laden eines Read-Only Images sowie das Laden der benötigten Programme gemeint. Die Zeit zwischen den Reboots werden in sogenannten Secure Execution Intervals (SEI) berechnet. Diese sind an definierte Bedingungen geknüpft sowie einem Mechanismus, der sicherstellt das ein Reboot mittels Timer gesetzt wird. Letzteres ist in einer eigenen Unit vor Veränderung geschützt. Das Modell wurde an 2 Prototypen evaluiert, die Steuerung einer hochdynamischen Drohne sowie eines eher stabilen Temperaturmessers. Es zeigt sich das hoch dynamische Systeme (z.B. eine Drohne) sehr häufige Restarts benötigen, was sich negativ auf die Verfügbarkeit auswirken kann. Auch ist der Ansatz nicht geeignet wenn das Zeitfester bis zum nächsten Restart kürzer als die gesamte Startphase ist. Es gibt aber viele Anwendungsfälle, wo ein Einsatz vielversprechend ist (z.B. Temperaturmessung für CPS). [122] stellt ein resilientes Recovery Schema für Smart Grids, basierend auf Cyber-Physical Mulit-Aspect Resilience-Based Recovery Metric (CPARM) vor. Es werden Aspekte berücksichtigt bevor ein Angriff zu Störungen in CPS führen. Dabei werden 4 Aspekte der Operabilität von CPS berücksichtigt, Leistungsbedarf, verfügbare Reservekapazität, verfügbare Leitungskapazität und Stromnetz-Zuverlässigkeit. Diese werden unter Physical-Side Resilience (PsR) Metriken zusammengefasst. Ebenso wird die Metrik Cyber-Side Resilience (CsR) in Betracht gezogen, damit ist der maximal tragbare Effekt von Cyber Angriffen auf ein CPS gemeint. Das Backup Schema sowie der Wiederherstellungspfad mehrerer Knoten wird mittels eines Algorithmus berechnet. Dieser berechnet den Wiederherstellungspfad, der die meiste Resilience bietet.

[127] analysiert den Bedarf von CR im Bereich Incident Prevention and Response für Critical Cyber Infrastructure (CCI). Daraus wird ein Konzeptmodel für Incident Prevention and Response in CCI entwickelt. Es werden Anforderungen an das Umfeld im Sinne von Beachtung von Regulatorien und Gesetzen, organisatorische Faktoren sowie technische Aspekte berücksichtigt. Das Modell sieht Simulationen mittels Digital Twins vor, anhand dieser werden Incident Response Szenarien generiert, um so dynamische und angepasste Trainingsumgebungen für CCI-Operatoren zu ermöglichen. Die Arbeit beschränkt sich auf die Konzepterstellung und sieht weitere Forschung in der Evaluierung des Modells. In [111] wird anhand der SPMT-Methode das Design Framework Resilient Shield entwickelt. Dafür werden die Phasen von SPMT durchlaufen, diese sind Start, Predict, Mitigate und Test wobei die Phase Test in späteren Arbeiten behandelt werden soll. In der Start-Phase wird ein Threat-Modell mit High Level Goals entwickelt. Diese sind in Kommunikationstechnologien, Hardware, Software, Speicher sowie Akteure und ihre Motivationen eingestuft. In der Predict-Phase wird ein Attack-Modell erstellt, es werden hierfür die STRIDE Kategorien (Spoofing, Tampering, Repudiation, Information Disclosure, DoS, Evaluation of Privilege) genutzt, um unter Verwendung einer Literaturanalyse und des definierten Threat-Modells Risiken zu identifizieren. Das

Ergebnis sind 6 Listen (nach den STRIDE Kategorien) mit insgesamt 37 Angriffen. Schließlich wird in der Mitigate-Phase das Resilient Shield ein Design-Konzept mit Sicherheitszielen (z.B. Secure Communication) und Maßnahmen (z.B. Authentication) anhand der ersten beiden Phasen entwickelt. In [78] wird eine Architektur vorgestellt die resiliente IoT-Geräte sicherstellen soll. Der Fokus liegt in der Architektur und möglichen Techniken. Es werden Mechanismen beschrieben, die die Kommunikation überwachen und sicherstellen, dass Befehle und Daten übermittelt werden. Dies soll sicherstellen, dass die Wiederherstellung in einen sicheren Zustand im Falle einer Kompromittierung stattfindet. Die Angriffserkennung wird mittels unsupervised ML-Techniken bereitgestellt. Durch die Kombination von lokalen Komponenten und einer zentralen Instanz (Cloud) ist ein rasches Reagieren vor Ort sowie ein umfassendes Monitoring möglich. Die Implementierung kann virtualisiert oder Hardware-basiert erfolgen. [68] stellt eine CR-Architektur für Programmable Logic Controller (PLC) vor. PLCs werden in ICS in kritischen Infrastrukturen aber auch in immer weiteren Bereichen des Lebens eingesetzt. Das Design ist üblicherweise auf Redundanz und Ausfälle ausgelegt. Cyber Angriffe die manipulativ wirken werden daher nicht so leicht erkannt. Die vorgestellte Quad-Redundant-Architektur bringt folgende Eigenschaften mit sich die genutzt werden, um Cyber Angriffe zu erkennen. Erstens wird der Output von redundanten PLCs paarweise verglichen, um Anomalien zu erkennen. Dann wird durch Software-Diversifikation sichergestellt, dass der gleiche Angriff unterschiedliche Reaktion im PLC auslöst und so den Angriff erschwert. Eine Fail-Over-Technik die bei Erkennung von Anomalien eine Synchronisation unterbindet stellt sicher, dass die sekundäre PLC als primäre PLC nur umgeschrieben wird wenn diese sich in einem sicheren Zustand befindet. Der vierte Mechanismus stellt einen durch Software-Diversifikation erstellten PLC zur Verfügung, welcher dem kompromittierten PLC überschreibt bezoehungsweise ersetzt. Die Architektur konnte schließlich in einer Simulation belegen, dass die CR von PLCs so maßgeblich erhöht werden kann.

[107] widmet sich dem sicheren Systemdesign und verfolgt einen Ansatz für Archtitecture Resilience Tactics. Archtitecture Tactics sind Design-Vorgaben wie Systeme einen oder mehrere Qualitätsaspekte implementieren. Der Ansatz beschäftigt sich mit der Validierung von Detection- und Recovery-Mechanismen für jede Archtitecture Tactic. Die Modellierungstaktiken werden in der Modellierungssprache Event-B formuliert und stellen so einen Code-Synthesis-Ansatz, basierend auf dem EventB2Java Tool, dar. Es werden eine Reihe an Qualitätseigenschaften für jede Archtitecture Tactic bereitgestellt sowie eine Certified Code Implementierung für die genannten Eigenschaften. Die Anwendbarkeit wird in einer Autonomous Vehicle System Simulation demonstriert.

4.5.6. CR-Assessmentmodell

Forschungsfeld Unterkategorie / NIST CSF Kategorie	Identify	Protect	Detect	Respond	Recover
Assessment und Messung von CR	[124],[101], [58],[67], [95],[123], [103],[79], [92],[81]	[103]	[58],[67], [103]	[124], [103]	[124]
Metriken	[58],[123], [103],[79], [92],[81]	[103]	[58], [103]	[103]	

Tabelle 18 : Studien des Forschungsbereichs CR-Assessmentmodell nach Unterkategorien und NIST CSF [141] Kategorien

Die Kategorie „CR-Assessmentmodell“ hält neben „Systemmodellierung zur Verhaltensanalyse“ die meisten Publikation, die sich mit der Subkategorie Metriken beschäftigen. Die Entwicklung von Metriken stellt einen wesentlichen Bereich in der Forschung dar, die Publikationen zeigen zum einen das Metriken meist spezifisch auf das zu untersuchende System erstellt werden. Auf der anderen Seite werden nicht nur

Systemeigenschaften gemessen oder berechnet sondern mittels Experteninterviews erhoben. So sollen realistische Werte ermittelt werden beziehungsweise Faktoren wie Wichtigkeit berücksichtigt werden. Alle vorgestellten Arbeiten haben den Fokus auf kritische oder produzierende Systeme.

[123] zeigt die Erarbeitung eines Frameworks für CR von Additive Manufacturing Supply Chain. Additive Fertigung ist einfach ausgedrückt, dass Design und die Herstellung von Produkten mittels 3D-Druck. Der Input für das Modell sowie das HER-Framework werden mittels Literaturanalyse und Experten Interviews erhoben. Im ersten Schritt liefert das HER-Framework 8 CR-Faktoren, Confidentiality, Integrity, Availability, Authenticity, Non-Repudiation, Possession, Utility und Completeness. Dabei werden die Faktoren mit Graden von Poor bis Excellent bewertet. Diese Faktoren werden benutzt, um CR mittels Experteninterviews sowie Daten der Organisation selbst zu berechnen (beispielsweise Anzahl der Mitarbeiter mit Zugriff auf definierte Daten, um die Confidentiality zu bestimmen). Dabei werden die Faktoren genutzt, um einen CR-Index zu erstellen. Das Modell wurde mittels Case Study an einer Additive Manufacturing Organisation evaluiert, und ermittelte in dem Fall einen Wert von ~0,6 (0,5 kennzeichnet den Durchschnitt). Die Methode zeigt außerdem, dass die Berechnung des Indexes mit jeder Änderung in der Organisation über die Zeit gemessen werden kann und daher ein Trend ersichtlich wird. Es ist weiters möglich das Organisationen mit der Methode eigene Attribute erstellen und so ihre CR besser bewerten können. In [81] wird ein CR-Assessment-Framework mit Integration von CVSS vorgestellt. Dabei wird ein bereits entwickeltes Framework CVSS IoT-ICS zur Darstellung von Verwundbarkeiten in OT und IoT Netzen genutzt. Das genannte Framework wird neben einem erweiterten Environmental-Score um einen Node-Resilience-Index erweitert. Dieser gibt die Widerstandsfähigkeit der gemessenen Komponente an und wird aus Parametern zu zeitlich definierten Resilienz-Werten berechnet; der Protection Time, Degradation Time, Identification Time und der Recovery Time. Das Modell wird in einer Case Study validiert und zeigt, dass der Node-Resilience-Index, die Resilienz der jeweiligen Komponenten realistisch darstellen kann. Dadurch können Systemadministratoren bessere Entscheidungen zum Schutz des Netzwerkes oder des Systems treffen.

In [79] wird CRAM ein Cyber-Resilience-Assessment-Model vorgestellt. Dieses leitet sich vom R4-Framework ab und die dort beschriebenen Metriken Robustness, Redundancy, Resourcefulness, und Rapidity die in weitere Sub-Metriken eingeteilt werden. Die Metriken werden den Domänen Physical, Organisational und Technical zugeordnet und davon werden ICS relevante Themenfelder abgeleitet die die Physische Sicherheit, die organisatorischen Maßnahmen und technische Implementierung eines ICS wiederspiegeln, siehe auch Abbildung 25. Die Metriken und Sub-Metriken werden mit jeder Domäne verbunden und einer Bewertung zugeordnet (Hoch, Mittel, Niedrig). ICS-Spezialisten werden mittels Umfrage zu den einzelnen Eigenschaften befragt. So sollen realistische Werte ermittelt werden. Die Bewertung in Hoch, mittel, niedrig ermöglicht die Überleitung in ein mathematisches Modell. Die Fragen sind so aufgebaut das eine Gewichtung der Domänen je Sub-Metrik ermöglicht wird. Aus dieser wird ein normalisierter Wert erstellt, der die Wichtigkeit je Metrik darstellt. Weiters wird ein CR-Framework für ICS entwickelt. Dieses basiert auf dem entwickelten CRAM-Assessment-Model und abstrahiert aus den Ergebnissen der Submetriken relevante Eigenschaften, um resiliente ICS in unterschiedlichen Industrien entwickeln zu können. [92] baut auf dem CRAM-Framework aus [79] auf und entwickelt daraus das Cyber Resilience Assessment Tool (CRAT), um CR Metriken aus qualitativen Daten zu generieren. Da das CRAM-Framework auf Umfragewerte angewiesen ist sollen unabhängig von der Anzahl der Teilnehmer Empfehlungen sowie verlässliche Reports durch das entwickelte Assessment generiert werden. Dies wird durch die entwickelten Metriken, Gewichtungen sowie dem zusätzlich erfragten Confidence Level ermöglicht.

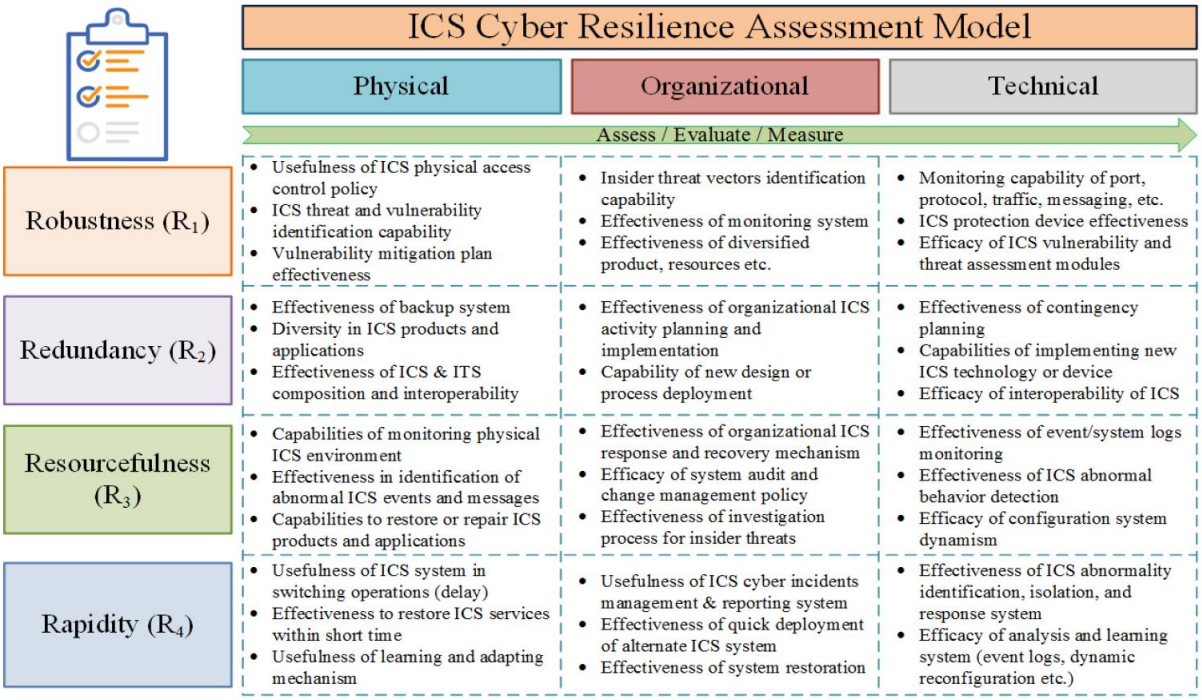

Abbildung 25 : CRAM-Assessment-Modell

In [103] werden CR-Metriken vorgestellt die für die Analyse von Stromnetzen und anderen ICS herangezogen werden können. Diese entwickelt für die Performance-Messung werden genutzt, um die Effektivität von Artificial Diversity and Defense Security (ADDSec), einer Moving Target Defense (MTD) Technik, in einem ICS zu messen. In einer Case Study zu einem Micro Grid, konfiguriert mit ADDSec, wird mittels Angriffssimulationen versucht Reconnaissance im Netzwerk zu erreichen. Es zeigt sich, dass die Erkundung von Hosts in einem Netzwerk merklich für einen Angreifer erschwert werden kann. Die Metriken zeigen, dass die Performance die ADDSec für die dynamische Rekonfiguration benötigt das System nicht negativ beeinflussen. [58] stellt die Advancing Resilience Of Control Systems (ADROC) Plattform vor, um Resilience-Assessments für CPS und ICS durchzuführen. Dafür werden das zu untersuchende System und deren Komponenten in einer SCEPTRE Emulation dargestellt. Bedrohungen und Angriffe werden mittels der MITRE CALDERA Lösung implementiert, die so gestaltete Simulation wird über ein Set aus Python Scripts namens REsilience VeRification UNit (RevRun) gestartet, um Daten zu sammeln und Metriken zu berechnen und darzustellen. Die Metriken selbst sind auf das jeweilige System zugeschnitten. In der Studie wurde die Plattform auf einem hypothetischen Nuklear Reaktor getestet, hier wurden Metriken wie zum Beispiel "*erste Überschreitung der Temperatur auf 580K*" definiert. Die Arbeit und die durchgeführte Simulation zeigt das dieses auf CPS und ICS zugeschnittene Framework einen wichtigen Beitrag zur CR und deren Messung in kritischen Infrastrukturen leisten kann.

In [67] wird eine Cyber-Resiliente Risk-Assessmentarchitektur für Wind Parks vorgestellt. Dabei werden 5 Level des Betriebs von Windparks beziehungsweise Energie Systemen beschrieben, die für ein Risk-Assessment herangezogen werden. Diese reichen von der lokalen Installation bis zur Marktintegration von Energie Systemen. In der Architektur werden die Levels zur Identifikation von möglichen Bedrohungen und Anhängigkeiten beziehungsweise Schnittstellen herangezogen. Die Risikobetrachtung umfasst die Einbeziehung von Threats, Verwundbarkeiten und Auswirkung, wobei von Threats und Verwundbarkeiten die Wahrscheinlichkeit eines Ereignisses abgeleitet werden. In allen drei Komponenten kann in weiterer Folge durch mitigierende Maßnahmen das Risiko reduziert werden. Bei Threats werden Bereiche wie Intent also was ein Angreifer erreichen will, Capability also die Fähigkeit eines Angreifers und Opportunity also die

Angriffsfläche die ein Angreifer hat (zum Beispiel Insider versus Extern) unterschieden. Bei Verwundbarkeiten wird zwischen Bereiche wie Hard- und Software, aber auch Firmware, Netzwerk und Prozess unterschieden. Schließlich wird bei Auswirkung in Kategorien von Verlust, Denial und Manipulation unterschieden. Die Arbeit bietet weiters Empfehlungen für das Assessment von Wind Parks anhand deren Bedürfnisse. [124] stellt ein CR-Assessment für Dispatchsysteme von Stromnetzen vor. Es wurden Ursachen für Cyber Security Verletzungen und Auswirkungen von schädlichen Ereignissen analysiert. Dabei wurde festgestellt, dass Response und Recovery auf Cyber Events die größten Faktoren für die CR darstellen. Weiters wurde ein Fuzzing Model vorgestellt, diese evaluiert CR-Indikatoren für Dispatchsysteme. Der entwickelte Algorithmus wird verwendet, um effektive Maßnahmen zur Erhöhung von CR und der Reduzierung von Cyber-Risiken zu erarbeiten. Auch [101] entwickelt ein Logic-Linguistic Modell (LLM) für das Assessment von CR im Energiesektor. Dabei werden Daten zu den CR-Domänen Preventive, Absorptive, Adaptive und Restorative erhoben. Diese werden anhand von Eigenschaften eines Systems extrahiert und als Variablen Hoch, Mittel, Niedrig gespeichert, um quantitative Daten zu generieren und eine Bewertung berechnen zu können

Schließlich wird in [95] das ProGReSS Maturity Model zur Messung der CR für den Industriewirtschaftssektor vorgestellt. Durch die Betrachtung von fünf "*Domains of Practice*", Organisation, Prozesse, Personal, Tools und Compliance kann in sogenannten Expression Sets, eine Sammlung an Aussagen und Indikatoren, zu jeder Domain der Reifegrad bezüglich CR erhoben werden. Das Modell ist mehrstufig aufgebaut und bietet mit der Erhebung der Maturity Möglichkeiten und Empfehlungen diese weiter zu erhöhen.

4.5.7. Systemmodellierung zur Verhaltensanalyse

Forschungsfeld Unterkategorie / NIST CSF Kategorie	**Identify**	**Protect**	**Detect**	**Respond**	**Recover**
Assessment und Messung von CR	[104],[80], [74],[64], [99],[85], [60],[129], [63],[62], [73],[97], [115],[132]	[104],[64]	[104],[80], [74], [64], [99], [129], [63], [62], [73], [97], [115], [132]	[104],[80], [74], [64], [99], [129], [63], [62], [73], [97], [115], [132]	
Metriken	[117], [85], [115]		[117], [115]	[115]	
Erkennung von Verwundbarkeiten	[117]	[125]	[117], [125], [59]	[125], [59]	
Erkennung und Abwehr von Cyber-Angriffen	[104], [80], [74], [99], [63], [62], [73], [97]		[104], [80], [74], [109], [77], [99], [125], [63], [62], [73], [97], [59]	[104], [80], [74], [109], [77], [99], [125], [63], [62], [73], [97], [59]	[109], [77]

Tabelle 19 : Studien des Forschungsbereichs Systemmodellierung zur Verhaltensanalyse nach Unterkategorien und NIST CSF [141] Kategorien

Systemmodellierung zur Verhaltensanalyse stellt die größte Gruppe in der Forschung zu CR dar. Diese eignen sich besonders für Analysen von komplexen Netzwerken und Systemen, weiters werden Simulationen genutzt, um Metriken zu berechnen aber auch um Daten für andere Modelle zu erzeugen.

Die Arbeit [80] erweitert bestehende Arbeiten im Cyber Trust EU Projekt um CR im Kontext von IoT. Es werden Simulationen zur Messung der Resilienz bei Malwareausbrüchen ähnlich der Ausbreitung einer Epidemie vorgestellt. Hierbei wird angenommen das ähnlich einer Epidemie die Verbreitung von Malware durch die Häufigkeit von Kontakten (Erreichbarkeit im Netzwerk) ausschlaggeben ist. Die Wahrscheinlichkeit des Risikos eines Malwareausbruchs wird in der Arbeit mittels mathematischer Modelle berechnet. Gegengesteuert kann dies durch die Verringerung der Konnektivität der Geräte werden. Beides hat Auswirkung auf die Verfügbarkeit beziehungsweise Resilienz. Um nicht zu große Bereiche zu isolieren, wird die Wahrscheinlichkeit der Infektion der Nachbarn berechnet und zentral gespeichert. So soll ab einem definierten Level von Infektionen gegengesteuert werden.

In [125] wird ein Integrated Modeling Environment vorgestellt, dass für das Design von Security und CR in SDN-basierten Produktionsnetzwerken und Applikationen herangezogen werden kann. Dabei wird eine Cyber Security Resilience Ontologie vorgestellt die Anforderungen an die Sicherheit und Mechanismen zur Resilienz definiert. Wobei Resilienz in diesem Zusammenhang Mechanismen beinhalten die ein Minimum an Performance im System sicherstellen und in der Lage sind selbständig das normale Leistungsniveau wiederherzustellen. Dies soll durch dynamische Netzwerkkonfiguration ermöglicht werden. Es gibt auf der einen Seite Cyber Security Maßnahmen die immer aktiv und vorbeugender Natur sind. Fallen diese aus oder werden als ineffektiv erkannt wird das aufgezeigt und der Resilience Mechanismus aktiviert. Eine Herausforderung in diesem Zusammenhang ist das Zusammenspiel von Legacy Systemen und IIoT sowie diese Komponenten in einem SDN-basierten Systemdesign zu integrieren. In [65] wird eine Co-Simulation-Based Plattform zur Modellierung und Implementierung von SDN-Technologien in Power Grids vorgestellt. Diese werden zur Simulation von False Telecontrol Command Angriffen genutzt. Case Studies zeigen, dass durch den Einsatz der SDN-Techniken Whitelisting und Deny-by-Default die CR signifikant erhöht werden kann.

[74] stellt eine Analytical Modellierung von Cyber Angriffen zum Assessment von CR auf Basis von Stochastic Network Conversion vor. Das mathematische Modell zeigt Indikatoren der Resilience in stochastischen Netzwerken auf. Es kann für Analysen vor einem Angriff, während eines Angriffs und bei der Wiederherstellung angewandt werden. Die so gewonnenen Indikatoren können für die Analyse von Bedrohungen oder als Basis für Anforderungen an die Netzwerksicherheit dienen. [77] und [109] beschäftigt sich mit mathematischen Modellen für Fast Rerouting. [77] erstellt ein Modell für Traffic Engineering Fast Rerouting (TE FRR) mit Traffic Policy Unterstützung. Dabei werden Bedingungen wie Mulitpath Routing, Veränderungen in der Flow Conversion sowie Traffic Policies am Perimeter berechnet. Außerdem werden Bedingungen von Links, Knoten und Brandbreite miteinbezogen. Mittels numerischer Analyse wird der Wirkungsgrad und die Effizienz des Modells bestätigt. Das Ergebnis zeigt, dass ein effizienter und angemessener Einsatz der vorgestellten TE FRR Methode möglich ist. So werden bestehende Netzwerkressourcen geschont , die Berechnungskomplexität reduziert, was zu einer Erhöhung der CR führt. Die Arbeit ist die Weiterentwicklung frühere Arbeiten in denen separate Lösungen zu Loadbalancing und Traffic Policing behandelt wurden. In [109] werden hingegen Metriken entwickelt und angewandt, um die beste Netzwerkroute mit der Geringsten Wahrscheinlichkeit einer Kompromittierung zu verwenden.

Die nächsten drei Arbeiten beschäftigen sich mit der Simulation von Wasseraufbereitungsanlagen. [115] beschreibt die Modellierung von Cyber-Socio-Technical-Systemen zur Analyse von Cyber Threats. Mittels der System Theoretic Process Analysis for Security through Simulations (STPA-Sec/S) Methode werden CR Metriken kalkuliert. STPA-Sec/S ist um eine Bedrohungsanalyse erweitert, um Angriffe in IT-Systemen zu analysieren und wurde ursprünglich zur Erkennung von fehlerhaften Safty Designs entwickelt. Um die entwickelten Metriken für ein CR-Assessment zu nutzen wird System Theoretic Accident Modelling and Processes (STAMP) ein Model-Based Ansatz zur Modellierung und Simulation genutzt. STAMP wird weithin genutzt, um Socio-Technical-Systeme dazustellen und Mensch-Maschine Interaktionen zu simulieren. Die Simulation wird mittels Case Study einer hypothetischen Wasseraufbereitung durchgeführt. Testbeds sind eine Möglichkeit Simulationen und Modelle umzusetzen. Ein systemdynamischer Modellierungsansatz, welcher mittels Threat Models die Konstruktion von CPS Modellen unterstützt wird in [60] vorgestellt. Dieser wird für Simulationen genützt, um zusammenhängende Auswirkungen von Angriffen zu evaluieren. Der

Ansatz wird in einem Secure Water Treatment Testbed (SWaT) umgesetzt. Quantitativer Metriken wie Impact Ratio, also die Abweichung der normalen Leistung eines Systems während eines Angriffes und Time-To-Critical-State, der Zeitraum wie lange ein System einem Angriff widerstehen kann werden für die Messung der Resilience genutzt. In [132] wird eine 6-stufige Methodik angewandt, um ein simulations-basiertes CR-Assessment für kritische Infrastrukturen zu erstellen. Zuerst wird die Problemstellung definiert die für die Entwicklung der Simulationsumgebung, der Modellierung des Testbeds und der Definition von Angriffen herangezogen wird. Weiters werden SMART Metriken anhand der Eigenschaften des Modells definiert, diese werden schließlich für das CR Assessment selbst herangezogen. Die Validierung des Modells erfolgt mittels einer Case Study an der Wasseraufbereitungsanlage Seawater Reserve Osmosis. Die Metriken wurden auf das Wasserversorgungssystem zugeschnitten und beschreiben die Wasserqualität, die Wassermenge und eine Kombination aus beiden sowie der Messung der Gesamtmenge und je Verteilerpunkt. Weiters werden die Werte anhand einer Zeit-Ereignis-Leiste gemessen (Normale Leistung, Angriff, gestörter Betrieb, Recovery Phase).

In [85] wird ein Testbed für das IEEE 2030.5 Protokoll unter Verwendung von OpenDSS Power System Software entwickelt, um die Anwendbarkeit des Protokolls für Micro Grids und Distributed Energy Ressources (DER) im Hinblick auf CR zu evaluieren. Es wird dafür das RC-Framework vorgestellt, dieses berechnet Metriken aus Faktoren zur Topologie, physischer Beschaffenheit des Micro Grids und Verwundbarkeiten des Netzwerks nach CVSS. Aus den separat berechneten Metriken wird der Cyber-Physical-Resilience-Score gebildet. Es werden Simulationen und Tests mit dem vorgestellten Testbed zu Berechnung der genannten Metriken umgesetzt. Dafür wird ein Militär Micro Grid herangezogen. Diese zeigen die Schwächen des Systems, durch die Berechnung des Cyber-Physical-Resilience-Score in Echtzeit auf. So kann die Situational Awareness von Administratoren gesteigert werden, um auf eine sinkende Resilienz zu reagieren. Auch [62] stellt ein Testbed für CPSs vor. Das Testbed unterstützt Model-Based Simulationen und zwar sowohl deren Parametrierung, Design sowie Durchführung von Tests und Angriffssimulationen selbst. Für die Skalierbarkeit der Simulationen gibt es eine Cloud Unterstützung. Eine modulare Angriffsbibliothek ermöglicht das Konfigurieren und Entwickeln unterschiedlicher Simulationen, diese werden in einem Red-Team Game ausgeführt. Des Weiteren wird eine Modellierungs- und Experimentumgebung mittels sogenannten Courses-of-Action geboten, um unterschiedliche What-If-Szenarien in Simulationen durchzuspielen. Für Simulationen die physische Hardware benötigen wird ein Hardware-in-the-Loop Testbed geboten. Schließlich wird in [64] eine Plattform für Bahninfrastruktur vorgestellt, um Cyber Angriffe zu modellieren und simulieren und deren Auswirkungen zu messen. Dieses soll bei der Entwicklung neuer und sicherer Bahntechnologie unterstützen. Dafür wird das HIL-Testbed genutzt und eine Case Study mit Simulation der Washington D.C. Metro durchgeführt, um die Plattform zu evaluieren.

Modelle benötigen Daten, diese werden in [63] mittels einem Smart Fuzzing Tool generiert. Dies ist ein automatisiertes ML-unterstütztes Tool, dass Testsätze oder Benchmarks für Security Tests an CPS erzeugt. Zur Generierung der Testsätze sind lediglich die normalen Zustände des zugrundeliegenden CPS nötig. Dabei wird zuerst das CPS gelernt, um anschließend Test-Angriffe zu erstellen, die das CPS in einen unsicheren Zustand bringt. Bei der Entwicklung wurde auf ein allgemein gültiges Modell gesetzt, das eine Vielzahl an CPS unterstützt und durch eine umfassende Integration alle Eigenschaften mittels Angriffsszenarien testen zu können. Außerdem wurde auf eine effiziente und praktische Implementierung wert gelegt.

Systemmodellierung zur Verhaltensanalyse und Anomalie-Erkennung erfordern oft mathematische Modelle. Diese werden in [99] vorgestellt, um das Verhalten von Energie Systemen während des Auftretens von Cyber Incidents zu analysieren. CR kann in einen Energy Delivery System (EDS) Netzwerk dargestellt werden, indem die Critical System Functionality berechnet wird und das Verhalten im Zuge eines Incidents beschrieben wird. In der Arbeit werden mathematische Modelle für das Systemverhalten unter Cyber Angriffen aber auch zur Berechnung der Cyber Resilience und Metriken für Critical Devices und Control Functions geboten. Die Modelle werden abschließend in Simulationen validiert. Das vorgestellte Modell soll Entscheidungshilfen für künftige Forschungen geben, um CR und System Funktionalität in EDS zu

ermöglichen. Im Projekt Quantitative Measurement of Cyber Resilience (QMoCR) [97] werden quantitative Charakteristiken von Systemen und wie diese auf Kompromittierungen reagieren identifiziert. Dafür werden mehrere sich ergänzende mathematische Modelle zur Analyse von CR entwickelt. Mittels der Berechnung von Parameter und Metriken werden die Auswirkungen von Malware und deren Abwehr gegenübergestellt. Die Modelle sollen in Simulationen genutzt werden. Dafür werden militärische Fahrzeuge und deren Cyber Defense Funktionen mittels Testbed dargestellt. [73] ist eine erweiterte Arbeit von [97] und stellt eine kosteneffektive Experimentumgebung vor die in einer Case Study mit einem generischen Military Ground Vehicle validiert wird. Die Umgebung wird mit dem PASTA-Testbed, entwickelt von Toyota, umgesetzt. Unity eine Multi-Plattform-Spieleentwicklungsumgebung und eine Eigenentwicklung der DEVCOM Army Redeveloped Laboratory dem Active Defense Framework (ADF) sowie eine OpenTAP Test Automation setzen die Modelle um. Die Case Study zeigt, dass die gemessenen Daten für die Messung von zuvor vorgestellten Metriken oder Key Performance Parameters herangezogen werden können und adäquate Ergebnisse liefert. [104] entwickelt die Modelle aus [97] weiter und inkludiert Piecewise Linear Malware und Bonware (Cyber Defense Software) Aktivitäten.

Die Arbeit [129] will die Effizienz von Digital Twins in Modellierungen und Simulationen zur Analyse von CR untersuchen. Des Weiteren sollen Herausforderungen für Simulationen mit Digital Twins aufgezeigt werden die sich aus der Anwendung und Kombination von Cyber Security Standards wie CVSS und Cyber Modelling und Simulation Standards ergeben. Mittels Literatur Analyse zu Digital Twins für Security Analyse wurden Simulationsstandards und Standards zur Beschreibung von Verwundbarkeiten sowie anderen Cyber Security Definitionen analysiert und Lücken hinsichtlich Herausforderungen für den Einsatz in Modellierung und Simulationen herausgehoben. Ein CR Testbed mittels Digital Twin wird als PoC für die Effekte und Auswirkung der Nutzung von CR-Standards und neuen Modellierungstechniken eingesetzt. Es werden Angriffe im Hafen von Southampton simuliert und Verbesserung der CR anhand von 6 Metrik Kategorien aufgezeigt. Es zeigt sich das Standards sowohl für Simulationen und Modellierung als auch Cyber Security Standards ein hohes Maß an Anpassung und Integration benötigen. Legacy Geräte und die Vielzahl an Komponenten und IoT Geräten stellen zusätzliche Herausforderungen dar. Auch bei der Anwendung von Metriken, auf der einen Seite stellt sich CVSS als vielversprechend heraus und andererseits sind Metriken meist individuell and systemspezifisch anzupassen.

ML-basierte Ansätze finden sich in Forschungen zu CR und Security ebenfalls immer wieder. In [106] wird der Ansatz verfolgt, mittels proaktiver Anomalie-Erkennung zur Abwehr von Cyber Angriffen die CR zu erhöhen. Die Anomalie-Erkennung wird mittels Recursive Bayesian Estimation in einem supervised ML-Algorithmus in Echtzeit realisiert. Die Daten werden einerseits aus Verkehrsdaten und anderseits aus Profilingdaten aus der Verhaltensanalyse von Fahrergruppen bereitgestellt. Als Case Study wurden Daten für eine vordefinierte Strecke auf einer deutschen Autobahn verwendet. Es wird ein Hijacking Versuch simuliert, der ein Umleiten des Autos auf ein anderes Ziel durchführt. Der Algorithmus soll ein verändertes Verhalten der Fahrposition erkennen und melden. Der Versuch zeigt das die Anomalie-Erkennung eindeutig angezeigt wird. Die eingesetzte Methode ist außerdem Effizienz in der Berechnungsleistung gegenüber anderen Methoden. Weitere Arbeiten könnten sich auf die spezifische Analyse von Fahrergruppen beschäftigen oder Daten von mehreren Fahrzeugen sammeln und analysieren.

Ein interessanter Ansatz wird in [117] vorgestellt und zwar ein Modell das die Chancen eines Angreifers mittels Metriken berechnet und so kritische Hosts in einen EDS-Netzwerk identifiziert. Die erste Metrik berechnet die Netzwerk-Topologie und Erreichbarkeit von Hosts. Zuerst werden die Netzwerkpfade anhand von Firewall-Regeln berechnet. Danach werden jedem Knoten die Eigenschaften Verwundbarkeit (nach CVSS), Operating System (für Diversität) und Isolation Pattern (Firewall, Authentifizierung) zugeordnet. So wird jeder Pfad zu jedem Host berechnet und attraktive Hosts und deren Erreichbarkeit bestimmt. Die zweite Metrik bestimmt die Angreifbarkeit via Social Engineering. Hier werden Eigenschaften für Verbreitung, Ausnutzung und Exekution herangezogen. Die letzte Metrik beschreibt die Infektionsverbreitung durch Prozesse, Dateien und Sockets die mit denen Hosts interagieren. Dieses wird auch in Relation mit der Zeit gesetzt, um so verwundbare Hosts über die Zeit zu erkennen. Die Arbeit zeigt das eine Berechnung der Kritikalität von Hosts anhand der Erreichbarkeit via Netzwerk, Benutzerzugriff, Interaktion mit anderen

Systemen und Verwundbarkeiten versus der reinen Verwundbarkeit die CR erhöhen kann indem der Fokus auf die kritischen Bereiche gerichtet wird.

Schließlich wird in [59] ein Framework vorgestellt, welches die Auswirkung von e-Mobility-Angriffen bezüglich der Resilience von Power Grids simuliert und analysiert. Dabei werden Modelle aus e-Mobility und Power Grids kombiniert und unter unterschiedlichen Angriffen auf mögliche großflächige Stromausfälle analysiert. So kann die Tageszeit in denen Angriffe am einfachsten durchgeführt werden können und wie viele Komponenten betroffen sein müssen, um einen großflächigen Ausfall zu provozieren bestimmt werden. Die Studie zeigt das Potential von Angriffen auf die e-Mobilitätsinfrastruktur auf auch wenn diese zur Zeit noch kein hohes Risiko aufweisen.

4.5.8. Technische Systeme

Forschungsfeld Unterkategorie / NIST CSF Kategorie	Identify	Protect	Detect	Respond	Recover
Assessment und Messung von CR		[105]	[105]	[105]	[105]
Erkennung von Verwundbarkeiten			[96], [100] [105], [83]	[96], [100], [105], [83]	
CR mit Fokus auf Recovery		[86]	[86]	[86]	[86]

Tabelle 20 : Studien des Forschungsbereichs Technische Systeme nach Unterkategorien und NIST CSF [141] Kategorien

In folgenden Arbeiten werden neben Frameworks und Modellen auch explizit deren Umsetzung in technische Systeme beschrieben. [86] entwickelt ein selbstheilendes PMU-Netzwerk für Stromnetze . Dieses wird mittels der Erstellung eines Prototyps auf Effizienz getestet. Es zeigt sich das alle kompromittierten oder deaktivierten Knoten erkannt und wiederhergestellt werden können. Mittels eines SDN-basierten Netzwerkschemas ist eine Wiederherstellung der Konfiguration je Gerät in kürzester Zeit möglich. Der Fokus der Arbeit liegt bei Entwicklung und Evaluierung des Selbstheile-Schemas. In [100] wird ein dezentrales SIP (System Integrity Protection) für Smart Grids entwickelt und vorgestellt das auf einer Multi Agent System Lösung basiert, um die CR in Smart Grids zu erhöhen. Das System bringt eine Anomalie-Erkennung mittels supervised Multi-Class-Classification-Algorithmus mit, die in die selbstregulierende Load Shedding Funktion integriert wird. Die Lösung konnte in einem Experiment angemessen auf DoS Angriffe reagieren. So konnte gezeigt werden das, dass dezentralisierte Multi-Agent-Design, gegeben über einem zentralisierten SIP, mehr Resilienz bietet. [83] stellt die Entwicklung eines Cyber-Aware State Estimator für CPS zur Erhöhung der CR vor. Es wird weiters eine Klassifizierungsmethode von Cyberangriffsdaten entwickelt. Mittels Zustandsbestimmung können Cyber-Angriffe identifiziert und gemessen werden.

Die Entwicklung eines Prototyps namens Hydra zur Erkennung und Abwehr von Angriffen für Gebäudesysteme, einem sogenannten Building Automation System (BAS) wird in [96] behandelt. Ein Gebäudemanagementsystem und deren Komponenten liegen in der Regel in einem flachen Netzwerk und das verwendete Netzwerkprotokoll BACnet weist durch seine Architektur Sicherheitsmängel auf. Die entwickelte Applikation soll diesem entgegenwirken und zu derzeit üblichen Lösungen auch eine Responsefunktionalität und Wiederherstellung mitbringen. Die Erkennung von abnormalen Netzwerkpaketen wird über mehrere Sensoren realisiert, diese messen den gesamten Netzwerkverkehr. Ein Artificial Neural Network wird trainiert, um Anomalien von normalen Netzwerkverkehr zu unterscheiden. Werden Anomalien erkannt, wird die Quelle identifiziert und automatisch via Firewall-Regeln blockiert. Die Lösung wurde in Experimenten erfolgreich getestet, das einfache Setup lässt für weitere Arbeiten Potential für Verbesserungen.

Als letzte Publikation wird in [105] das EU Projekt PALANTIR vorgestellt, ein Cyber Security Framework mit starkem CR Fokus für SMEs. Dieses wird über eine Cloud Lösung als Secaas (Security as a Service) angeboten in dem verschiedene Services von SME genutzt werden können. Dazu gehören ein Security

Orchestration für das Verwalten von Security Capabilities, ein Risk Analyse Framework, Threat Itelligence, Incident Erkennung sowie Recovery Funktionen. Die Beleuchtung von Einsatzgebieten wie kleinere Medizinische Unternehmen zeigen den praktikablen Ansatz von PALANTIR. Weiteres werden Herausforderungen beleuchtet, die für die Weiterentwicklung genutzt werden.

5. Diskussion

Im folgenden Kapitel werden die Ergebnisse gemeinsam gegenübergestellt, um die Forschungsfragen zu beantworten. Es werden Parallelen zur Einleitung, der Darstellung der Studien sowie deren Inhalten gezogen und zusammengefasst.

Q1:Welche Domänen, Methoden und Techniken werden in aktuellen Forschungen zu Cyber Resilience behandelt?

Ein Teilaspekt in der Forschung zu CR ist deren Analyse und Definition. Die Definition von Begrifflichkeiten ist allgemein ein wichtiges Thema, um Eindeutigkeit und Klarheit zu schaffen. Die Mehrheit der Studien ist sich bei der Definition von CR einig und beschreibt diese als Fähigkeit eines Systems Angriffe zu erkennen, diesen zu widerstehen und ein definites Ausmaß an Leistung unter einem Angriff zu erhalten sowie die Wiederherstellung des Ausgangsniveaus zu gewehrleisten. Dennoch gibt es Studien wie [84] die den Begriff CR kritisch hinterfragen und Parallelen zu Cyber Security ziehen. Wie im Kapitel Einleitung festgestellt verschwimmen die Begrifflichkeiten Cyber Security und CR, dies wurde auch in den analysierten Studien festgestellt. [98] kommt treffend zum Schluss das eine Kombination aus Cyber Security und CR die besten Effekte haben, da zum einen Sicherheitsaspekte und Verwundbarkeiten und damit der Schutz berücksichtigt wird und zum anderen wird auf Resilienz und dem Fortführen des Betriebs Wert gelegt. Ebenfalls eine treffende Aussage, die speziell in komplexen Strukturen aller Art gegeben ist, wird in [71] und [131] beschrieben. Und zwar den Umstand, dass CR von Unsicherheiten und der Tatsache das Systeme nie ganz sicher sind ausgeht und diesem begegnet.

Die Messung von CR wird in den vorliegenden Arbeiten konsequent in Model-Based und Metric-Based getrennt, wobei es hier meist eigene Definitionen samt Unterteilungen gibt. [116] beschreibt Metric-Based als indirekte quantitative Messung über die potenzielle Fähigkeit der Resilienz. Dabei werden Eigenschaften und Fähigkeiten von Systemen gemessen. [113] und [88] schließen die Performance Messung mit ein, wobei erstere Studie auch die Messung der Eigenschaften mitangibt. Der Model-Based Ansatz zeichnet sich durch die Verhaltensmessung eines Systems während eines Ereignisses aus. [113] unterscheidet hier neben der reinen Verhaltensanalyse auch die Messung und Darstellung der Ausbreitung eines Ereignisses, eine andere Variante beschäftigt sich mit Wahrscheinlichkeiten und Unsicherheiten, die durch Simulationen gemessen werden können. Ein anderer Aspekt in der Messung und Darstellung von CR ist die Hinzunahme der zeitlichen Komponenten. Hier wird auf die Phasen Plan / Prepare, Absorb, Recover und Adopt eingegangen und der Belastbarkeit eines Systems während der Dauer eines Ereignisses, wie in Abbildung 26 anhand des R-4-Frameworks dargestellt.

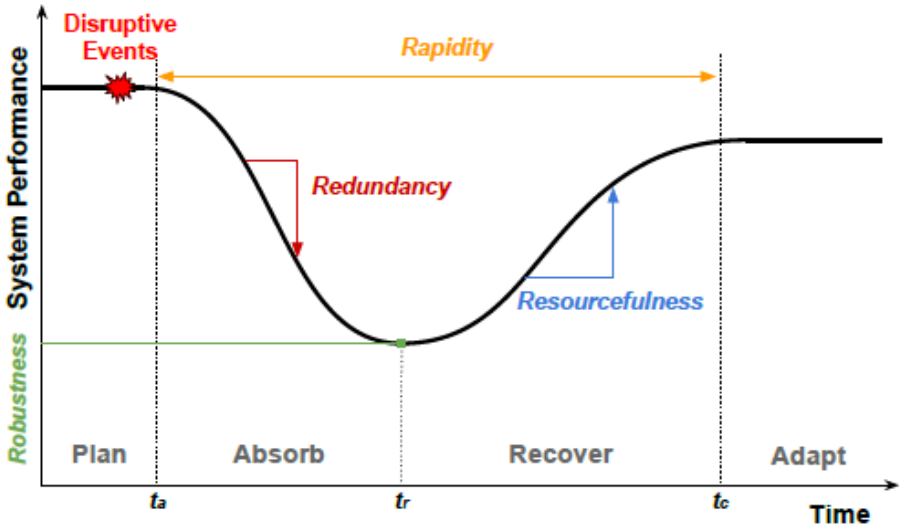

Abbildung 26 : R4-Framework Resilienz-Kurve [113]

Ein Teil der Studien beschäftigt sich mit der Statuserhebung zu CR von Unternehmen, Großteils in der kritischen Infrastruktur. Zwei der Studien, [76] und [130], beschäftigen sich ausschließlich mit der Erhebung von CR-Strategien im staatlichen und gesellschaftlichen Umfeld. Dennoch gibt es hier wenige Studien. Eine Erhebung von CR auf nationaler Ebene zum Schutz der kritischen Infrastruktur und der Gesellschaft wäre ein lohnender Bereich. Interessant wäre hier ein Vergleich europäischer Staaten in Bezug zu EU Richtlinien wie NIS2 [6] oder DORA [5] und deren Umsetzungsstatus.

Neben der Statuserhebung ist die Bedarfserhebung ein weiterer Forschungsbereich. Diese findet sich in den Gebieten der Messung von CR in CPS, in der resilienten Softwareentwicklung und System Design, der Bedarfserhebung von CR in Organisationen aller Größen aber auch im SME-Umfeld oder wie Cyber-Angriffe in unterschiedlichen Kontexten erkannt und abgewehrt werden können. [133] untersucht beispielsweise, wie ML-Algorithmen und speziell RL dieses Thema adressiert und wie es eingesetzt werden kann. Hier sei gesagt, dass es relativ wenige Studien gibt die AI-basierte Technologien und deren Einsatz für CR untersuchen.

Ein sehr intensiv erforschtes Gebiet mit unterschiedlichsten Richtungen gibt es in Bezug auf Umsetzungslösungen wie Frameworks, Architekturen, Assessment-Modelle oder Systemmodellierungen und Simulationen. Dieser Bereich macht den größten Teil verfügbarer Studien aus, ist aber dennoch nicht übersättigt da unterschiedlichste Varianten und Einsatzbereiche erarbeitet werden. Während sich CR-Frameworks und Architekturen meist mit der Erkennung und Abwehr von Angriffen beschäftigen sind Assessment-Modelle mit der Messung von CR beschäftigt. Die Systemmodellierung vereint beide Richtungen und unterstützt somit vor allem die Messung von Angriffen und deren Auswirkungen.

Es gibt aber auch einige Frameworks, die sich mit der Umsetzung von CR in Organisationen aller Größen oder speziell im SME-Umfeld beschäftigen. Hier gibt es interessante Ansätze wie AMBI-CYBER aus [71], eine Lösung die sich auf einem ambidextren Modell stützt. Dabei gilt es die Balance zwischen dem intensiven Einsatz neuer Technologien und der optimalen Nutzung vorhandener Ressourcen zu wahren, um so effizient wie möglich zu arbeiten und dadurch die CR zu erhöhen. [131] will die Kultur rund um CR in Organisationen verbessern, um den Umstand zu begegnen das in komplexen Strukturen immer Fehler vorhanden sind und eine rasche und flexible Herangehensweise nötig ist. Die meisten analysierten Assessment-Modelle zeichnen sich dadurch aus, dass sie einen umfassenden Blick auf Systeme haben und auch den organisatorischen und menschlichen Faktor miteinbeziehen.

Ein guter Teil der Studien findet sich in der Systemmodellierung zur Verhaltensanalyse wieder. Diese werden oft zum Design von Systemen genutzt, um CR-Aspekte schon bei der Planung validieren zu können. Etliche Arbeiten befassen sich mit der Analyse von Netzwerken und deren unterschiedlichen Konfigurationen. Hierfür werden vornehmlich Simulationen zur reinen Angriffserkennung und Reaktion sowie der gleichzeitigen Analyse und Messung genutzt. Das gleiche gilt für die Analyse und Messung von CPS in kritischen Infrastrukturen. Einige Arbeiten lassen erkennen, dass die Messung mit der Qualität der Daten steht und fällt. Auch das qualitativ hochwertige Daten nicht einfach zu bekommen oder generieren sind. [63] hat als einzige Studie seiner Art dafür ein Modell entwickelt, welches Daten aus einem zuvor definierten Systemmodell generiert und diese für Frameworks einsetzbar macht. Weiters kommen in diesem Forschungsfeld unterschiedlichste Testbeds oder Digital Twins zum Einsatz beziehungsweise werden in diesen Arbeiten entwickelt und vorgestellt. Systemmodellierung wird gern für die Messung von Systemen herangezogen, dadurch finden sich in diesen Studien zusammen mit Assessmentmodellen die meisten Vorstellungen von Metriken wieder. Metriken müssen fast immer an das jeweilige System angepasst werden, finden aber immer wieder Anlehnung an Standards wie CVSS wieder. Die fehlenden Standardisierung und den daraus ergebenden Umstand das Frameworks und Metriken meist individuell für jedes System zugeschnitten werden wurde auch durch die ENISA bestätigt, ebenso wie die Notwendigkeit hier einheitliche Standards zum Vergleich zu entwickeln [36].

Bei den verwendeten Techniken und Methoden findet sich natürlich die Literaturanalyse an einem prominenten Platz. Dass kommt allerdings davon, da die Literaturanalyse als zusätzliche Methode oder als Methode für die Erhebung des eigentlichen Studieninhalts herangezogen wird. Wie schon bei den Forschungsbereichen erkennbar, sind Simulationen und Modellierungen sehr verbreitete Techniken in Studien zu CR. Auch Experimente und Case Studies finden sich sehr häufig. Letzteres auch für Analysen im organisatorischen und gesellschaftlichen Umfeld. Interviews und Umfragen sind vor allem in der Statuserhebung und Bedarfsanalyse zu CR stark gefragt. Aber auch in einigen Assessment-Modellen finden sich qualitative Aspekte in Form von Umfragen und Interviews wieder [79], [123].

Q2:Welche Branchen werden in Studien zu CR vorrangig adressiert und warum?

Betrachtet man die adressierten Branchen fällt auf der einen Seite auf das allgemeine und übergreifende Brachen 45% aller Studien ausmachen. Analysiert man auf der anderen Seite diese, erkennt man das hier viel Fokus auf CPS im Allgemeinen gelegt wird und diese Studien daher der produzierenden Industrie und der kritischen Infrastruktur zugeordnet werden können. Aggregiert man diese Studien nun sieht man wie in Abbildung 9 gezeigt, dass 55% aller Studien sich auch der kritischen Infrastruktur widmen. Diese Kategorie fasst die Branchen Energiewirtschaft (23%), Wasserwirtschaft (3%), Branchen um Verkehr und Logistik (8%) sowie 21% wo sich Studien mit Themen für die produzierende Industrie und der kritischen Infrastruktur im Allgemeinen beschäftigt zusammen. Keine Studien die in die Bereiche der kritischen Infrastruktur fallen gibt es zu Gesundheitswesen, Versorgung des täglichen Bedarfs oder dem Finanzwesen. Letzteres wird in nur einer Studie als Teilaspekt behandelt [110].

Alle anderen Branchen bleiben jeweils unter 10%. IT-Services die alle Bereiche der IT-Infrastruktur und Softwareentwicklung halten sind mit nur 6% wenig vertreten. Man erkennt in diesem Zusammenhang das CR vorrangig für komplexe System wie CPS herangezogen wird. Hier haben wir eine Mischung von IT und OT die in Studien analysiert werden aber nicht unter IT-Services fallen. Viele Frameworks sind für Organisationen zugeschnitten, diese enthalten ebenfalls Teilaspekte der IT die oft unter Technik aufscheint. Somit sind Branchen rund um IT-Services indirekt viel häufiger vertreten.

Es finden sich 3 Studien die sich mit CR im militärischen Umfeld beschäftigen wieder, was keine 3% ausmacht. Wenn man bedenkt, dass AI, autonome Systeme und die starke Abhängigkeit von vernetzen Systemen die auch mit dem Internet kommunizieren müssen immer mehr Einzug in jede Landesverteidigung findet, ist die Anzahl der Studien erschreckend gering. Eine Erklärung dafür ist, dass

Studien in diesem Bereich aufgrund der besonderen Vertraulichkeit nicht veröffentlicht werden und das der eingeschränkte Auswahlprozess hier ebenfalls zu Unschärfen führt.

Studien die CR-Aspekte im öffentlichen Leben und der Gesellschaft behandeln, finden sich in mehreren Branchen wieder, bleiben dort aber die Ausnahme. Dazu gehören die öffentliche Verwaltung mit einer Studie zur Statuserhebung von CR-Strategien von Staaten [76] und eine Studie zur Erhebung der CR im Public Transport [130]. Möglicherweise finden sich Studien zur Auswirkung auf die Gesellschaft durch Störungen in Form von Katastrophen wieder, welche aber nicht Teil dieser Arbeit sind.

Warum die Studien sich der jeweiligen Branchen gewidmet haben, wird auch in der nächsten Forschungsfrage zur Motivation mitbeantwortet. In Studien wird grundsätzlich nicht darauf eingegangen, warum eine Branche ausschlaggebend ist. Ein Indiz sind die adressierten Risiken und der Wichtigkeit der Branchen. So sind zum Beispiel Risiken, die sich mit Auswirkungen auf die Gesellschaft beschäftigen vor allem in der kritischen Infrastruktur aber auch in Branchen zur öffentlichen Verwaltung, Verkehr und Logistik oder für Organisationen erwähnt. Ein weiters Risko das immer wieder angesprochen wurde ist die Gefahr und Auswirkung von Cyber-Angriffen. Auch hier haben wir den deutlichsten Verweis aus Studien zur kritischen Infrastruktur und der produzierenden Industrie. Die rasante Entwicklung im IKT-Bereich ist neben der Gefahr vor Cyber-Angriffen die zweithäufigste Motivation für Studien. Speziell Studien die sich mit CPS befassen, verdeutlichen durch die rasante Entwicklung von Technik und Angriffen die Wichtigkeit der Forschung zu CR. Außerdem finden CR-Konzepte sehr häufig in komplexen Systemen (beziehungsweise CPS) oder Organisationen Anwendung. Bei letzterem wird speziell im OT-Bereich die Resilienz vor anderen Security-Aspekten herausgestellt, was die hohe Präsenz von Branchen in der kritischen Infrastruktur und der produzierenden Industrie erklärt.

Q3:Was sind die Motivationen um CR zu erforschen?

Motivationen können in zwei Unterscheidungen dargestellt werden. Zum einen forschungsspezifische Motivation zugeschnitten auf ein spezielles Thema. Dieser Bereich wird in der Regel durch eine vorherige Literaturanalyse auf fehlende Forschung untersucht und untermauert. Zum anderen sind sehr allgemeine Motivationen zu erkennen. Diese sind Cyber-Angriffe, hier wird zwischen den Gefahren allgemein und den Gefahren für die Gesellschaft unterschieden. Die rasante Entwicklung im IKT-Bereich und der Digitalisierung gehört ebenso zu den allgemeinen Motivationen. Diese machen mit 56 Studien den größten Teil aus. Ebenso sind allgemeiner definierte Motivationen nur in wenigen Studien genauer beschrieben. Am ehesten finden sich explizite Beispiele in der Brachen Energiewirtschaft mit Beispielen zu Angriffen auf Stromnetze.

Forschungsspezifische Motivationen sind fehlende Studien zu autonomen Systemen im OT-Bereich oder zu spezifischen Angriffen. Diese Motivationen sind vor allem in Branchen der kritischen Infrastruktur und der produzierenden Industrie zu finden. Spezifische Angriffe werden immer in Zusammenhang mit CPS analysiert. Eine ähnliche Motivation findet sich in einigen Studien wieder und zwar der noch wenig adressierte CR-Aspekt der Recovery.

Weitere Motivationen sind der Forschungsbedarf zu Statuserhebung und Definition von CR, zu CR in der Supply Chain und der Softwareentwicklung. Außerdem wurde der Forschungsbedarf zu CR für Organisation und hier vor allem für SME hervorgehoben.

Die unter Q2 erwähnten adressierten Risiken, die von Cyber-Angriffen allgemein ausgehen im Vergleich zu Risken mit Auswirkungen auf die Gesellschaft zeigt deutlich das die Resilienz während Cyber-Angriffe eindeutig mehr Studien betreffen. Die Mehrzahl der analysierten Studien befassen sich mit technischen Systemen in unterschiedlichen Kontexten, was die Motivation bezüglich Cyber-Angriffen erklärt. Die Forschungsfrage sollte ursprünglich beantworten ob Gesetze oder Vorgaben eine Rolle in der Forschung zu CR spielen. Das konnte nicht nachgewiesen werden, da nur 4 Studien diese erwähnen und ähnliche Themen auch als Inhalt haben.

Zusammengefasst kann gesagt werden das die Resilienz vor Cyber-Angriffen und der rasant entwickelnde IKT-Bereich die Hauptmotivationen von Studien zu CR ist, selbst in den forschungsspezifischen Motivationen und den adressierten Risiken wird auf diese Thematik eingegangen.

Q4:Welche Trends sind bz. Cyber Resilience zu erkennen?

Die Verteilung der Veröffentlichungen über die Zeit zeigt, dass ein leichter steter Anstieg zu beobachten ist, im Durchschnitt sind es 12 Publikationen pro Jahr. Durch die kurze Zeitspanne von 5 Jahren lässt sich nicht erkennen, ob die Forschung zu CR merklich zunimmt oder nicht.

Die Verteilung der Studien nach Kongressen sowie Institutionen über die Kontinente zeigt, dass Amerika weit vorne liegt. Bei den herausgebenden Institutionen ist Amerika mit 44% knapp bei der Hälfte aller Studien zu CR. Und im Ländervergleich ist die USA mit ungefähr 85% das Land, welches die meiste Forschung zu CR bewerkstelligt. Europa hält mit ungefähr 30% bei Kongressen sowie Institutionen den zweiten Platz. Die analysierten Studien wurden dahingehend untersucht ob die Institutionen Kooperationen im eigenen Land oder International eingehen. Europa ist am wenigsten aktiv was Kooperationen betrifft und zwei Drittel der Studien wurden von nur einer Institution erstellt. Amerika hingegen betriebt übergreifende Forschung vornehmlich im eigenen Land. Nur im asiatischen Raum sind Kooperationen Länderübergreifend mit 50% am meisten verbreitet.

Die Studien wurden auch auf Sponsoren die Studien finanziell unterstützen untersucht. Die Mehrheit der ungefähr 30 Studien die Unterstützung erhielten sind in der kritischen Infrastruktur angesiedelt. Es konnten sonst keine Auffälligkeiten erkannt werden.

Wie schon in der Frage zur Motivation ist deutlich, dass die kritische Infrastruktur und produzierende Industrie aufgrund vermehrter Cyber-Angriffe und der wachsenden Komplexität sowie der schnellen Entwicklung im IKT- und OT-Bereich stark im Fokus von Forschung zu CR steht. Es wird auch weiterer Bedarf gesehen in diesem Bereich zu forschen. Einige Studien die Themen um CPS behandeln, vornehmlich im Energiesektor, geben auch an das die geopolitische Lage und mögliche Spannungen CR immer wichtiger machen.

Spätere Forschungen sollen sich weiter mit der quantitativen Messung von CR beschäftigen [113] , [91]. Ein Augenmerkt liegt in der realitätsnahen Messung und Angriffserkennung [69]. Gerade in den wenigen Studien zu CR in Organisationen empfehlen diese die Socio-ökonomischen Aspekte von CR genauer zu untersuchen [118], [121], [110], [115]. Diese Faktoren sollen ebenso im CMS Umfeld erforscht werden [135], [134]. Weitere Felder die künftig erforscht werden sollten, sind CR in autonomen Systemen oder der e-Mobilität [59], [91], [119].

6. Zusammenfassung und Ausblick

Die stetig steigenden Zahlen von Cyber-Angriffen [4] in Kombination von immer komplexer werdenden Systemen die zunehmend miteinander vernetzt sind und interagieren macht die Notwendigkeit deutlich das mehr zum Schutz und Resilienz dieser Strukturen getan werden muss. Komplexe Systeme bringen viele Abhängigkeiten mit sich. Diese werden oft nicht erkannt und können dadurch verkettete Störungen bei einem Vorfall auslösen. Das macht es zunehmend schwieriger mit klassischen Methoden wie Risk-Management die adäquaten Maßnahmen zum Schutz und der Widerstandsfähigkeit umzusetzen. CR ist eine Möglichkeit umfassend auf den Schutz und der Resilienz von technischen Lösungen aber auch organisatorischen Strukturen einzugehen.

Diese Arbeit betrachtet aktuelle Forschungen zum Thema CR, um aufzuzeigen welche Bereiche bereits gut beleuchtet wurden und wo es Lücken gibt. Aber auch um aufzuzeigen, wo weiterer Forschungsbedarf empfohlen wird. Es gibt etliche SLRs die Teilaspekte zu CR betrachten, aber keine widmet sich diesem Thema ganzheitlich. Daher leistet diese Arbeit einen wichtigen Beitrag CR holistisch zu betrachten und einen umfassenden Blick auf die aktuelle Forschung zu geben. Als Methodik wurde eine SLR nach PRISMA 2020 gewählt. Dabei wurden aus 1208 Studien 80 für die Analyse mittels den zuvor definierten Auswahlkriterien erhoben. Das Ergebnis zeigt einen leichten Anstieg von Studien zu CR über die analysierten 5 Jahre. Die meisten Studien zu CR wurden in Amerika und da allem voran den USA mit ungefähr 85% aller Studien im amerikanischen Raum veröffentlicht. Dahinter steht Europa mit 30% aller veröffentlichten Studien. Ein sehr ähnliches Bild der geographischen Verteilung zeigt sich auch bei der Präsentation der Studien auf Kongressen. Kooperationen mit anderen Institutionen im eigenen Land werden vor allem in den USA gern eingegangen. Asien hat mit 50% aller Studien die meisten wo eine internationale Kooperation stattfand und europäische Studien werden größtenteils von nur einer Institution veröffentlicht. Beim Branchenvergleich fällt auf, dass die Gruppe der nicht eindeutig zuordenbaren also übergreifenden Branchen die größte Gruppe darstellt. Diese 45% große Gruppe ergibt sich daraus da CR in CPS oder CR in Organisationen in unterschiedlichen Kontexten häufig erforscht wird. Unterteilt man diese Gruppe weiter sieht man, dass alles um kritische Infrastrukturen ca. 55% aller Studien ausmacht. Ein weiterer großer Teil entfällt auf die produzierende Industrie, die sich in unterschiedlichen Branchenkategorien summieren lässt. CR im IT-Infrastrukturbereich oder Softwareentwicklung ist mit 6% vergleichsweise gering vertreten. Branchen die öffentliche Verwaltung, Verteidigung und Gesellschaftliche Bereiche einschließen sind ebenfalls sehr gering vertreten.

Die analysierten Studien beschäftigen sich zum einen mit der Analyse und Definition von CR in unterschiedlichen Kontexten. Dazu gehören was CR ist und wie diese dargestellt und gemessen werden kann. Auch die Statuserhebung vor allem für Organisationen im privaten und öffentlichen Bereich ist ein weiterer Forschungsbereich, wo auch durchaus mehr Studienbedarf gesehen wird. Weitere Forschungsbereiche sind in der Umsetzung von CR durch Frameworks, Architekturen, Assessmentmodelle, Modellierungen und technische Lösungen zu finden. Frameworks konzentrieren sich zum einen mit der Umsetzung von CR in Organisationen und zum anderen auf die Erkennung von Verwundbarkeiten. CR-Architekturen die sich vornehmlich durch die Hard- und Softwareentwicklung sowie Systementwicklung auszeichnen haben meist einen Fokus auf der Erkennung und Abwehr von Cyber-Angriffen. Assessmentmodelle und Modellierungen haben neben der Erkennung und Abwehr von Cyber-Angriffen das Hauptaugenmerk auf der Messung von CR. Schließlich gibt es einige Studien deren Fokus auf der Entwicklung und Umsetzung von technischen Lösungen liegen.

Die Motivation CR zu erforschen, hängt zum einen mit spezifischen Fragestellungen zu CR zusammen, zum Beispiel im OT-Bereich oder CR für autonome Systeme. Auf der anderen Seite sind Motivationen, um CR zu erforschen eher allgemein gehalten. Hier wurden die Motivationen Gefahr durch Cyber-Angriffe sowie deren Auswirkungen auf die Gesellschaft erkannt. Dies war bei einem Großteil der Studien ausschlaggebend für den Zweck des jeweiligen Forschungsgegenstandes. Auch die rasante Entwicklung im IKT-Bereich stellt einen beträchtlichen Teil der in Studien genannten Motivation dar. Die adressierten Risiken sind den

Motivationen Cyber-Angriffe und deren Auswirkung auf die Gesellschaft sehr ähnlich und wurden indirekt als Motivation genannt.

Forschungslücken wurden zum Teil in den erhobenen Studien selbst herausgestellt andere ergeben sich aus den Ergebnissen. Wie auch im Kapitel 4.4 angeführt gibt es Forschungsbedarf in der adäquaten Messung von CR in unterschiedlichen Kontexten. Darunter zählen die Messung mit quantitativen Daten [126], [113]. Aber auch das realitätsnahe Messungen und Modelle entwickelt werden, um Cyber Effects und Angriffe ganzheitlich zu analysieren und so realistische Ergebnisse zu erhalten [113], [91], [89]. In diesem Zusammenhang steht auch der Bedarf in der Verbesserung der Angriffserkennung bezüglich Skalierbarkeit und Komplexität [69]. Wie in [36] festgestellt ist die Messung von CR ein wichtiges Gebiet, Metriken sind oft nicht Standardisiert und sehr individuell angepasst. Einige Arbeiten bestätigen diese Aussage, auch das einseitige Daten und fehlende realistische Datenquellen eine Limitierung darstellen. [63] ist die einzige Studie, die sich der Generierung von Testdaten für Frameworks widmet. Dies zeigt deutlich, dass obwohl die Messung von CR in den analysierten Studien ein vorherrschendes Thema ist, hier aber mehr getan werden muss um eine bessere Standardisierung voranzutreiben und realistischere Ergebnisse zu erzielen.

In Forschungen zu organisationalen Resilienz sollen mehr Socio-ökonomischen Aspekte untersucht werden [118], [121], [110], [115]. Dies wird auch für Forschungen zu CMS empfohlen [135], [134]. Zu CMS sei gesagt das beide Studien die Forschung zu CMS und Industrie 4.0 in der Produktion als zu gering einschätzen und Herausforderungen in der Governance, Resilience Engineering und Kultur sehen und hier weitere Forschung empfehlen. Frameworks zur Etablierung von CR in Organisationen unterschiedlicher Größe gibt es viele, auch in den analysierten Studien. Die Faktoren Mensch und deren Einfluss auf die Technik und Aspekte wie Awareness, Kultur und Kommitment sind nicht zu vernachlässigen und sollten in der Forschung besser adressiert werden. Denkbar wären Studien zur Verhaltensanalyse bei gleichzeitiger Erhebung der CR in Unternehmen.

Mittel- bis Langfristig sollen neue Technologien zu autonomen Systemen oder der e-Mobilität besser erforscht werden, auch da neben der geringen Anzahl an Studien in diesen Bereichen diese in den nächsten Jahren stark wachsen und an Bedeutung zunehmen werden [59], [91], [119]. Ähnliches gilt für die AI-unterstützte Umsetzung von CR. In den analysierten Studien beschäftigt sich nur [133] ganzheitlich mit RL-Methoden in CR Lösungen. Andere Studien nutzen zwar oft Algorithmen zur Angriffserkennung und Abwehr aber ein ganzheitlicher Ansatz wie AI-basierte Entscheidungen in resilienten Systemen integriert werden können wäre ein lohnendes Forschungsgebiet. Als Beispiel könnte eine fertige Lösung von der Angriffserkennung, der Abwehr dieser sowie der Wiederherstellung des regulären Betriebs auf Basis von AI- und ML-Technologien genannt werden. In diesem Zusammenhäng drängt sich auch die Absicherung von AI-basierten Lösungen vor Manipulation auf.

Anhand der vorliegenden Daten liegt es nahe, dass es Forschungsbedarf zu CR im Gesundheitswesen und Finanzwesen gibt da hierzu keine Studien erkannt wurden. Es gibt auch sehr wenig Forschung zur Auswirkung auf die Gesellschaft bei fehlender CR. Dies scheint mit Blick auf die Krisen der letzten Jahre ein lohnendes Thema zu sein. Ebenso verhält es sich mit der Statuserhebung mit Blick auf kritische Infrastrukturen und gesellschaftliche Bereiche. Interessant wären Statuserhebungen zur DORA [5] oder NIS2 [6] Readiness von betroffenen Unternehmen oder wie bestehende Industrie Standards wie NIST CSF [141] oder ISO 27001 [142] diese sicherstellen oder unterstützen.

Zusammenfassend kann gesagt werden, dass die Messung von CR und Metriken bezüglich realistischer Daten und Standardisierung besser erforscht werden soll. Weiters ist noch viel Arbeit zu leisten wenn es um aufstrebende und neue Technologien geht. In diesem Zusammenhang werden CPS in kritischen Infrastrukturen aber auch der Produktion durch deren steigenden Komplexität und Vernetzung weiterhin ein anzustrebendes Forschungsfeld bleiben. CR in Organisationen sollte um Aspekte wie Awareness, Kultur und dem Zusammenspiel Mensch und Technik verbessert werden. Außerdem ist zu erkennen das es so gut wie keine Forschung in Branchen zu Gesundheitswesen und Finanzenwesen sowie die Auswirkungen fehlender CR auf die Gesellschaft gibt.

Die vorliegende Arbeit zeigt, welche Bereiche der CR-Forschung bereits gut adressiert sind und wo es Lücken gibt. Dies kann von der Forschung aufgegriffen werden, um zum einen bestehende Ansätze in gut erforschten aber weiterhin verbesserungswürdigen Bereichen wie der kritischen Infrastruktur aufzugreifen und weiterzuentwickeln. Auf der anderen Seite können Studien zur Statuserhebung relevanter Themen abgeleitet werden, um dieses noch gering erforschte Gebiet sinnvoll zu erweitern. Aber auch wenig adressierte Themen zu aufstrebenden Technologien sind offensichtlich ein spannenden und wenig beleuchtetes Forschungsfeld für die Zukunft.

Organisationen und Unternehmen in der Wirtschaft können ihre CR-Strategien anhand der erwähnten Frameworks überarbeiten und weiterentwickeln. Besonders [82] und [105] stellen hier vielversprechende und ausgereifte Modelle für eine Erhebung und Umsetzung von CR dar. Interessante Ansätze finden sich in [71] und [131] wieder, in ersterer wird die Effizienz von Ausnutzung der vorhandenen Ressourcen und der Investition in neue Technologien als Resilienz-fördernd herausgestrichen und in zweitere das Zusammenspiel von der Tatsache das Cyber-Angriffe stattfinden werden und der Kultur die entwickelt werden muss um diesem zu begeben. Aber auch Betreiber von CPS unterschiedlicher Art können von der Vielzahl an Frameworks und Architekturen profitieren und diese auf Anwendbarkeit prüfen beziehungsweise die Entwicklung und Einstellungen von Metriken und Messpunkten abgleichen.

References

Literatur

[1] ENISA, *ENISA Threat Landscape 2022.* [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (accessed: Mar. 4 2023).

[2] ENISA, *Sustained Activity by Threat Actors.* [Online]. Available: https://www.enisa.europa.eu/news/sustained-activity-by-threat-actors (accessed: Mar. 4 2023).

[3] A. Kott and I. Linkov, Eds., *Cyber resilience of systems and networks*. Cham, Switzerland: Springer, 2019.

[4] Statista, *Ransomware attacks.* [Online]. Available: https://www.statista.com/study/43873/ransomware/ (accessed: Mar. 31 2023).

[5] *EUR-Lex - 32022R2554 - EN - EUR-Lex: Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*, 2023. Accessed: Apr. 11 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554&qid=1681218196861

[6] *EUR-Lex - 32022L2555 - EN - EUR-Lex: Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*, 2023. Accessed: Apr. 11 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1681218196861

[7] *EUR-Lex - 32022L2557 - EN - EUR-Lex: Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC*, 2023. Accessed: Apr. 11 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2557&qid=1681218196861

[8] G. Ahmadi-Assalemi, H. Al-Khateeb, G. Epiphaniou, and C. Maple, "Cyber Resilience and Incident Response in Smart Cities: A Systematic Literature Review," *Smart Cities*, vol. 3, no. 3, pp. 894–927, 2020, doi: 10.3390/smartcities3030046.

[9] J. K. Osborn and D. A. Sepulveda-Estay, "A Comparative Analysis of the Impact-Wave Analogy Cyber-Resilience Framework," *2021 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, pp. 333–337, 2021, doi: 10.1109/IEEM50564.2021.9672842.

[10] D. A. Sepúlveda Estay, R. Sahay, M. B. Barfod, and C. D. Jensen, "A systematic review of cyber-resilience assessment frameworks," *Computers & Security*, vol. 97, p. 101996, 2020, doi: 10.1016/j.cose.2020.101996.

[11] D. I. Christine and M. Thinyane, "Socio-technical Cyber Resilience: A Systematic Review of Cyber Resilience Management Frameworks," *Progress in IS*, pp. 573–597, 2022. [Online]. Available: https://ideas.repec.org/h/spr/prochp/978-3-031-15420-1_28.html

[12] A. Aldea, E. Vaicekauskaite, M. Daneva, and J. P. Sebastian Piest, "Assessing Resilience in Enterprise Architecture: A Systematic Review," in *2020 IEEE 24th International Enterprise Distributed Object Computing Conference (EDOC)*, 2020.

[13] N. Tuptuk, P. Hazell, J. Watson, and S. Hailes, "A Systematic Review of the State of Cyber-Security in Water Systems," *Water*, vol. 13, no. 1, p. 81, 2021, doi: 10.3390/w13010081.

[14] D. K. Mishra, M. J. Ghadi, A. Azizivahed, L. Li, and J. Zhang, "A review on resilience studies in active distribution systems," *Renewable and Sustainable Energy Reviews*, vol. 135, p. 110201, 2021, doi: 10.1016/j.rser.2020.110201.

[15] R. Osei-Kyei, V. Tam, M. Ma, and F. Mashiri, "Critical review of the threats affecting the building of critical infrastructure resilience," *International Journal of Disaster Risk Reduction*, vol. 60, p. 102316, 2021, doi: 10.1016/j.ijdrr.2021.102316.

[16] V. Naserinia, "Cyber resilience for critical infrastructure : A systematic review," 2021. [Online]. Available: https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1576950&dswid=-7079

[17] N. Chowdhury and V. Gkioulos, "Cyber security training for critical infrastructure protection: A literature review," *Computer Science Review*, vol. 40, p. 100361, 2021, doi: 10.1016/j.cosrev.2021.100361.

[18] A. Corallo, M. Lazoi, M. Lezzi, and A. Luperto, "Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review," *Computers in Industry*, vol. 137, p. 103614, 2022, doi: 10.1016/j.compind.2022.103614.

[19] Estay, Daniel Alberto Sepulveda and Khan, Omera, "Towards-a-supply-chain-cyber-risk-and-resilience-research-agenda-a-systematic-literature-review," *Reflections on Supply Chain Research and Practice*, pp. 1–12, 2015. [Online]. Available: https://www.researchgate.net/profile/Daniel-Sepulveda-Estay/publication/286342563_Towards_a_supply_chain_cyber-risk_and_resilience_research_agenda_-_a_systematic_literature_review/links/5667f65608ae34c89a029370/Towards-a-supply-chain-cyber-risk-and-resilience-research-agenda-a-systematic-literature-review.pdf

[20] Omera Khan and Daniel A. Sepúlveda Estay, "Supply Chain Cyber-Resilience: Creating an Agenda for Future Research," *Technology Innovation Management Review*, vol. 5, no. 4, 2015. [Online]. Available: https://timreview.ca/article/885

[21] A. Ghadge, M. Weiß, N. D. Caldwell, and R. Wilding, "Managing cyber risk in supply chains: a review and research agenda," *SCM*, vol. 25, no. 2, pp. 223–240, 2019, doi: 10.1108/SCM-10-2018-0357.

[22] Duden, *cyber-.* [Online]. Available: https://www.duden.de/rechtschreibung/cyber_ (accessed: Apr. 11 2023).

[23] Duden, *Kybernetik.* [Online]. Available: https://www.duden.de/rechtschreibung/Kybernetik (accessed: Apr. 12 2023).

[24] PONS Langenscheidt GmbH, *Cyber- - Deutsches Rechtschreibwörterbuch | PONS.* [Online]. Available: https://de.pons.com/%C3%BCbersetzung/deutsche-rechtschreibung/cyber- (accessed: Apr. 11 2023).

[25] National Institute of Standards and Technology, *Cyber - Glossary | CSRC.* [Online]. Available: https://csrc.nist.gov/glossary/term/cyber (accessed: Apr. 11 2023).

[26] Bodeau, Deb, Graubart, and Rich, "Cyber Resiliency Design Principles," The MITRE Corporation. Accessed: Apr. 19 2023. [Online]. Available: https://www.mitre.org/sites/default/files/2021-11/pr-17-0103-Cyber-Resiliency-Design-Principles.pdf

[27] Duden, *Resilienz.* [Online]. Available: https://www.duden.de/rechtschreibung/Resilienz (accessed: Apr. 11 2023).

[28] Brockhaus, *Resilienz (Psychologie) - Enzyklopädie - Brockhaus.at.* [Online]. Available: https://brockhaus.at/ecs/enzy/article/resilienz-psychologie (accessed: Apr. 11 2023).

[29] Encyclopedia Britannica, *Ecological resilience.* [Online]. Available: https://www.britannica.com/science/ecological-resilience (accessed: Apr. 11 2023).

[30] ENISA, *P-Z.* [Online]. Available: https://www.enisa.europa.eu/topics/risk-management/current-risk/bcm-resilience/glossary/p-z (accessed: Apr. 11 2023).

[31] National Institute of Standards and Technology, *resilience - Glossary | CSRC.* [Online]. Available: https://csrc.nist.gov/glossary/term/resilience (accessed: Apr. 12 2023).

[32] International Organization for Standardization, *ISO/IEC TS 5723:2022(en), Trustworthiness — Vocabulary*. resilience, robustness. [Online]. Available: https://www.iso.org/obp/ui#iso:std:iso-iec:ts:5723:ed-1:v1:en:term:3.2.15 (accessed: Apr. 11 2023).

[33] National Institute of Standards and Technology, *robustness - Glossary | CSRC.* [Online]. Available: https://csrc.nist.gov/glossary/term/robustness (accessed: Apr. 12 2023).

[34] E. R. Unkrig, *Resilienz im Unternehmen - den Faktor Mensch fördern: Handlungsempfehlungen und praktische Umsetzung*. Wiesbaden, Heidelberg: Springer Gabler, 2021.

[35] Bundesamt für Sicherheit in der Informationstechnik, "BSI-Standard 200-4 BCM," Bundesamt für Sicherheit in der Informationstechnik, 2022. Accessed: Apr. 21 2023. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4_CD_2_0.pdf?__blob=publicationFile&v=5

[36] ENISA, *Resilience Metrics and Measurements: Challenges and Recommendations.* [Online]. Available: https://www.enisa.europa.eu/publications/metrics-survey?v2=1 (accessed: Apr. 15 2023).

[37] National Institute of Standards and Technology, *cyber resiliency - Glossary | CSRC.* [Online]. Available: https://csrc.nist.gov/glossary/term/cyber_resiliency (accessed: Apr. 11 2023).

[38] Encyclopedia Britannica, *Computer security | Definition & Facts.* [Online]. Available: https://www.britannica.com/technology/computer-security (accessed: Apr. 11 2023).

[39] National Institute of Standards and Technology, *Cyber Security - Glossary | CSRC.* [Online]. Available: https://csrc.nist.gov/glossary/term/cyber_security (accessed: Apr. 12 2023).

[40] International Organization for Standardization, *ISO/IEC TS 27100:2020(en), Information technology — Cybersecurity — Overview and concepts*. Cyberspace, Cyber Security. [Online]. Available: https://www.iso.org/obp/ui#iso:std:iso-iec:ts:27100:ed-1:v1:en:term:3.5 (accessed: Apr. 11 2023).

[41] Duden, *Cybersecurity.* [Online]. Available: https://www.duden.de/rechtschreibung/Cybersecurity (accessed: Apr. 11 2023).

[42] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, and R. McQuaid, "Developing Cyber-Resilient Systems," National Institute of Standards and Technology, Gaithersburg, MD, 2021. Accessed: Apr. 20 2023. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf

[43] Deborah Bodeau, Richard Graubart, Jeffrey Picciotto, Rosalie McQuaid, "Cyber Resiliency Engineering Framework," The MITRE Corporation, 2011. Accessed: Apr. 19 2023. [Online]. Available: https://www.mitre.org/sites/default/files/media/publication/11_4436_2.pdf

[44] I. Linkov, D. A. Eisenberg, K. Plourde, T. P. Seager, J. Allen, and A. Kott, "Resilience metrics for cyber systems," (in En;en), *Environ Syst Decis*, vol. 33, no. 4, pp. 471–476, 2013, doi: 10.1007/s10669-013-9485-y.

[45] M. J. Page *et al.,* "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *BMJ (Clinical research ed.)*, vol. 372, n71, 2021, doi: 10.1136/bmj.n71.

[46] L. Shamseer *et al.,* "Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015: elaboration and explanation," *BMJ (Clinical research ed.)*, vol. 350, g7647, 2015, doi: 10.1136/bmj.g7647.

[47] M. J. Page *et al.,* "PRISMA 2020 expanded checklist," *BMJ (Clinical research ed.)*, vol. 372, n71, 2021, doi: 10.1136/bmj.n71.

[48] S. a. o. Keele, "Guidelines for performing Systematic Literature Reviews in Software Engineering," Technical report, ver. 2.3 ebse technical report. ebse 2.3, 2007. [Online]. Available: https://www.researchgate.net/profile/barbara-kitchenham/publication/302924724_guidelines_for_performing_systematic_literature_reviews_in_software_engineering

[49] Agnieszka Ubowska and Tomasz Królikowski, "Building a cybersecurity culture of public administration system in Poland," *Procedia Computer Science*, vol. 207, pp. 1242–1250, 2022, doi: 10.1016/j.procs.2022.09.180.

[50] Akashdeep Bhardwaj, Vinay Avasthi, and Sam Goundar, "Cyber security attacks on robotic platforms," *Network Security*, vol. 2019, no. 10, pp. 13–19, 2019, doi: 10.1016/S1353-4858(19)30122-9.

[51] Andrea Appolloni, Idiano D'Adamo, Massimo Gastaldi, Ernesto D.R. Santibanez-Gonzalez, and Davide Settembre-Blundo, "Growing e-waste management risk awareness points towards new recycling scenarios: The view of the Big Four's youngest consultants," *Environmental Technology & Innovation*, vol. 23, p. 101716, 2021, doi: 10.1016/j.eti.2021.101716.

[52] Arnau Erola, Ioannis Agrafiotis, Jason R.C. Nurse, Louise Axon, Michael Goldsmith, and Sadie Creese, "A system to calculate Cyber Value-at-Risk," *Computers & Security*, vol. 113, p. 102545, 2022, doi: 10.1016/j.cose.2021.102545.

[53] Aman Ankit, Zhanlin Liu, Scott B. Miles, and Youngjun Choe, "U.S. Resilience to large-scale power outages in 2002–2019," *Journal of Safety Science and Resilience*, vol. 3, no. 2, pp. 128–135, 2022, doi: 10.1016/j.jnlssr.2022.02.002.

[54] Arshad Nawaz, Min Zhou, Jing Wu, and Chengnian Long, "A comprehensive review on energy management, demand response, and coordination schemes utilization in multi-microgrids network," *Applied Energy*, vol. 323, p. 119596, 2022, doi: 10.1016/j.apenergy.2022.119596.

[55] Isabel Skierka, "When shutdown is no option: Identifying the notion of the digital government continuity paradox in Estonia's eID crisis," *Government Information Quarterly*, vol. 40, no. 1, p. 101781, 2023, doi: 10.1016/j.giq.2022.101781.

[56] B. Aubouin–Pairault, A. Perodou, C. Combastel, and A. Zolghadri, "Resilient tube-based MPC for Cyber-Physical Systems Under DoS Attacks," *IFAC-PapersOnLine*, vol. 55, no. 6, pp. 278–284, 2022, doi: 10.1016/j.ifacol.2022.07.142.

[57] Bekkers Luuk, Van 't Hoff-de Goede (Maria) Susanne, Misana-ter Huurne Ellen, Van Houten Ynze, Spithoven Remco, and Leukfeldt Eric Rutger, "Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model," *Computers & Security*, vol. 127, p. 103099, 2023, doi: 10.1016/j.cose.2023.103099.

[138] Computing Research & Education, *CORE Rankings Portal.* [Online]. Available: https://www.core.edu.au/conference-portal (accessed: Sep. 28 2023).

[139] Google, *Google Scholar Metrics Help.* [Online]. Available: https://scholar.google.com/intl/de/scholar/metrics.html#metrics (accessed: Sep. 28 2023).

[140] Statista, *Statista - Das Statistik-Portal.* [Online]. Available: https://de.statista.com/statistik/kategorien/ (accessed: Oct. 7 2023).

[141] National Institute of Standards and Technology, *Cybersecurity Framework | NIST.* [Online]. Available: https://www.nist.gov/cyberframework (accessed: Nov. 20 2023).

[142] International Organization for Standardization, *ISO/IEC 27001:2022.* [Online]. Available: https://www.iso.org/standard/27001 (accessed: Dec. 20 2023).

Literatur SLR

[58] J. Thorpe *et al.,* "A Cyber-Physical Experimentation Platform for Resilience Analysis," in *Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems*, 2022, pp. 3–12.

[59] D. Kern and C. Krau, "Analysis of E-Mobility-Based Threats to Power Grid Resilience," in *Proceedings of the 5th ACM Computer Science in Cars Symposium*, 2021.

[60] Z. Hau, J. H. Castellanos, and J. Zhou, "Evaluating Cascading Impact of Attacks on Resilience of Industrial Control Systems: A Design-Centric Modeling Approach," in *Proceedings of the 6th ACM on Cyber-Physical System Security Workshop*, 2020, pp. 42–53.

[61] F. Abdi, C.-Y. Chen, M. Hasan, S. Liu, S. Mohan, and M. Caccamo, "Guaranteed Physical Security with Restart-Based Design for Cyber-Physical Systems," in *Proceedings of the 9th ACM/IEEE International Conference on Cyber-Physical Systems*, 2018, pp. 10–21.

[62] H. Neema, B. Potteiger, X. Koutsoukos, G. Karsai, P. Volgyesi, and J. Sztipanovits, "Integrated Simulation Testbed for Security and Resilience of CPS," in *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, 2018, pp. 368–374.

[63] Y. Chen, C. M. Poskitt, J. Sun, S. Adepu, and F. Zhang, "Learning-Guided Network Fuzzing for Testing Cyber-Physical System Defences," in *Proceedings of the 34th IEEE/ACM International Conference on Automated Software Engineering*, 2020, pp. 962–973.

[64] H. Neema, X. Koutsoukos, B. Potteiger, C. Tang, and K. Stouffer, "Simulation Testbed for Railway Infrastructure Security and Resilience Evaluation," in *Proceedings of the 7th Symposium on Hot Topics in the Science of Security*, 2020.

[65] A. Kemmeugne, A. A. Jahromi, D. Kundur, and M. Kassouf, "Towards Cyber-Resilient Telecontrol Commands Using Software-Defined Networking," in *Proceedings of the 9th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, 2021.

[66] C. Rieger, C. Kolias, J. Ulrich, and T. R. McJunkin, "A Cyber Resilient Design for Control Systems," in *2020 Resilience Week (RWS)*, 2020, pp. 18–25.

[67] M. J. Culler, S. Morash, B. Smith, F. Cleveland, and J. Gentle, "A Cyber-Resilience Risk Management Architecture for Distributed Wind," in *2021 Resilience Week (RWS)*, 2021, pp. 1–8.

[68] J. Luo *et al.,* "A Quad-Redundant PLC Architecture for Cyber-Resilient Industrial Control Systems," *IEEE Embedded Systems Letters*, vol. 13, no. 4, pp. 218–221, 2021, doi: 10.1109/LES.2020.3011309.

[69] F. Mohammadi, M. Saif, M. Ahmadi, and B. Shafai, "A Review of Cyber–Resilient Smart Grid," in *2022 World Automation Congress (WAC)*, 2022, pp. 28–35.

[70] E. B. Cahyono, S. B. M. Sam, N. H. B. Hassan, N. Mohamed, N. Ahmad, and Y. Yusuf, "A Review on Cyber Resilience Model in Small and Medium Enterprises," in *2022 4th International Conference on Smart Sensors and Application (ICSSA)*, 2022, pp. 114–119.

[71] E. G. Carayannis, E. Grigoroudis, S. S. Rehman, and N. Samarakoon, "Ambidextrous Cybersecurity: The Seven Pillars (7Ps) of Cyber Resilience," *IEEE Transactions on Engineering Management*, vol. 68, no. 1, pp. 223–234, 2021, doi: 10.1109/TEM.2019.2909909.

[72] J. F. Carias, L. Labaka, J. M. Sarriegi, and J. Hernantes, "An Approach to the Modeling of Cyber Resilience Management," in *2018 Global Internet of Things Summit (GIoTS)*, 2018, pp. 1–6.

[73] J. E. Ellis *et al.,* "An Experimentation Infrastructure for Quantitative Measurements of Cyber Resilience," in *MILCOM 2022 - 2022 IEEE Military Communications Conference (MILCOM)*, 2022, pp. 855–860.

[74] I. Kotenko, I. Saenko, and O. Lauta, "Analytical modeling and assessment of cyber resilience on the base of stochastic networks conversion," in *2018 10th International Workshop on Resilient Networks Design and Modeling (RNDM)*, 2018, pp. 1–8.

[75] M. Baruwal Chhetri *et al.,* "AWaRE - Towards Distributed Self-Management for Resilient Cyber Systems," in *2018 23rd International Conference on Engineering of Complex Computer Systems (ICECCS)*, 2018, pp. 185–188.

[76] D. Irene Christine and M. Thinyane, "Comparative Analysis of Cyber Resilience Strategy in Asia-Pacific Countries," in *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, 2020, pp. 71–78.

[77] O. Lemeshko, O. Yeremenko, M. Yevdokymenko, A. Shapovalova, A. M. Hailan, and A. Mersni, "Cyber Resilience Approach Based on Traffic Engineering Fast ReRoute with Policing," in *2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, 2019, pp. 117–122.

[78] M. Medwed, V. Nikov, J. Renes, T. Schneider, and N. Veshchikov, "Cyber Resilience for Self-Monitoring IoT Devices," in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, 2021, pp. 160–167.

[79] M. A. Haque, G. K. De Teyou, S. Shetty, and B. Krishnappa, "Cyber Resilience Framework for Industrial Control Systems: Concepts, Metrics, and Insights," in *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 2018, pp. 25–30.

[80] E. Bellini, F. Bagnoli, A. A. Ganin, and I. Linkov, "Cyber Resilience in IoT Network: Methodology and Example of Assessment through Epidemic Spreading Approach," in *2020 IEEE World Congress on Services (SERVICES)*, 2020, pp. 72–77.

[81] A. Ur-Rehman, J. Kamruzzuman, I. Gondal, and A. Jolfaei, "Cyber Resilience Modelling for the Operations of Hybrid Network," in *2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, 2022, pp. 1–7.

[82] J. F. Carías, S. Arrizabalaga, L. Labaka, and J. Hernantes, "Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs," *IEEE Access*, vol. 9, pp. 80741–80762, 2021, doi: 10.1109/ACCESS.2021.3085530.

[83] S. Hopkins, E. Kalaimannan, and C. S. John, "Cyber Resilience using State Estimation Updates Based on Cyber Attack Matrix Classification," in *2020 IEEE Kansas Power and Energy Conference (KPEC)*, 2020, pp. 1–6.

[84] L. A. Bygrave, "Cyber Resilience versus Cybersecurity as Legal Aspiration," in *2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon)*, 2022, pp. 27–43.

[85] P. S. Sarker, V. Venkataramanan, D. S. Cardenas, A. Srivastava, A. Hahn, and B. Miller, "Cyber-Physical Security and Resiliency Analysis Testbed for Critical Microgrids with IEEE 2030.5," in *2020 8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, 2020, pp. 1–6.

[86] Y. Qu, G. Chen, X. Liu, J. Yan, B. Chen, and D. Jin, "Cyber-Resilience Enhancement of PMU Networks Using Software-Defined Networking," in *2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2020, pp. 1–7.

[87] M. Segovia, J. Rubio-Hernan, A. R. Cavalli, and J. Garcia-Alfaro, "Cyber-Resilience Evaluation of Cyber-Physical Systems," in *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)*, 2020, pp. 1–8.

[88] J. Zuo, Z. Guo, J. Gan, and Y. Lu, "Enhancing Continuous Service of Information Systems Based on Cyber Resilience," in *2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC)*, 2021, pp. 535–542.

[89] F. Siddiqui, M. Hagan, and S. Sezer, "Establishing Cyber Resilience in Embedded Systems for Securing Next-Generation Critical Infrastructure," in *2019 32nd IEEE International System-on-Chip Conference (SOCC)*, 2019, pp. 218–223.

[90] C. Onwubiko, "Focusing on the Recovery Aspects of Cyber Resilience," in *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 2020, pp. 1–13.

[91] A. K. Ligo, A. Kott, and I. Linkov, "How to Measure Cyber-Resilience of a System With Autonomous Agents: Approaches and Challenges," *IEEE Engineering Management Review*, vol. 49, no. 2, pp. 89–97, 2021, doi: 10.1109/EMR.2021.3074288.

[92] M. A. Haque, S. Shetty, and B. Krishnappa, "ICS-CRAT: A Cyber Resilience Assessment Tool for Industrial Control Systems," in *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, 2019, pp. 273–281.

[93] A. Dwivedi, "Implementing Cyber Resilient Designs through Graph Analytics Assisted Model Based Systems Engineering," in *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, 2018, pp. 607–616.

[94] G. Lykou, A. Anagnostopoulou, and D. Gritzalis, "Implementing Cyber-Security Measures in Airports to Improve Cyber-Resilience," in *2018 Global Internet of Things Summit (GIoTS)*, 2018, pp. 1–6.

[95] A. Shaked, L. Tabansky, and Y. Reich, "Incorporating Systems Thinking Into a Cyber Resilience Maturity Model," *IEEE Engineering Management Review*, vol. 49, no. 2, pp. 110–115, 2021, doi: 10.1109/EMR.2020.3046533.

[96] C. B. Jones, C. Carter, and Z. Thomas, "Intrusion Detection & Response using an Unsupervised Artificial Neural Network on a Single Board Computer for Building Control Resilience," in *2018 Resilience Week (RWS)*, 2018, pp. 31–37.

[97] A. Kott, M. J. Weisman, and J. Vandekerckhove, "Mathematical Modeling of Cyber Resilience," in *MILCOM 2022 - 2022 IEEE Military Communications Conference (MILCOM)*, 2022, pp. 849–854.

[98] N. Jacobs, S. Hossain-McKenzie, and E. Vugrin, "Measurement and Analysis of Cyber Resilience for Control Systems: An Illustrative Example," in *2018 Resilience Week (RWS)*, 2018, pp. 38–46.

[99] M. A. Haque, S. Shetty, and B. Krishnappa, "Modeling Cyber Resilience for Energy Delivery Systems Using Critical System Functionality," in *2019 Resilience Week (RWS)*, 2019, pp. 33–41.

[100] P. Wang and M. Govindarasu, "Multi-Agent Based Attack-Resilient System Integrity Protection for Smart Grid," *IEEE Transactions on Smart Grid*, vol. 11, no. 4, pp. 3447–3456, 2020, doi: 10.1109/TSG.2020.2970755.

[101] Y. Brezhniev, "Multilevel Fuzzy Logic-Based Approach for Critical Energy Infrastructure's Cyber Resilience Assessment," in *2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 2019, pp. 213–217.

[102] S. H. Bouk, S. H. Ahmed, R. Hussain, and Y. Eun, "Named Data Networking's Intrinsic Cyber-Resilience for Vehicular CPS," *IEEE Access*, vol. 6, pp. 60570–60585, 2018, doi: 10.1109/ACCESS.2018.2875890.

[103] S. Hossain-McKenzie, C. Lai, A. Chavez, and E. Vugrin, "Performance-Based Cyber Resilience Metrics: An Applied Demonstration Toward Moving Target Defense," in *IECON 2020 The 46th Annual Conference of the IEEE Industrial Electronics Society*, 2020, pp. 766–773.

[104] M. J. Weisman, A. Kott, and J. Vandekerckhove, "Piecewise Linear and Stochastic Models for the Analysis of Cyber Resilience," in *2023 57th Annual Conference on Information Sciences and Systems (CISS)*, 2023, pp. 1–6.

[105] E. Mantas *et al.,* "Practical Autonomous Cyberhealth for resilient Micro, Small and Medium-sized Enterprises," in *2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*, 2021, pp. 500–505.

[106] H. Al-Khateeb, G. Epiphaniou, A. Reviczky, P. Karadimas, and H. Heidari, "Proactive Threat Detection for Connected Cars Using Recursive Bayesian Estimation," *IEEE Sensors Journal*, vol. 18, no. 12, pp. 4822–4831, 2018, doi: 10.1109/JSEN.2017.2782751.

[107] N. Catano, "Program Synthesis for Cyber-Resilience," *IEEE Transactions on Software Engineering*, vol. 49, no. 3, pp. 962–972, 2023, doi: 10.1109/TSE.2022.3168672.

[108] S. Vasudevan, A. Piazza, and M. Carr, "Qualitative Factors in Organizational Cyber Resilience," in *2022 International Conference on Cyber Resilience (ICCR)*, 2022, pp. 1–5.

[109] O. Lemeshko, O. Yeremenko, M. Yevdokymenko, and D. Ageyev, "Redundancy Cyber Resiliency Technique Based on Fast ReRouting under Security Metric," in *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*, 2020, pp. 815–818.

[110] D. U. Irughe, W. Nwankwo, C. P. Nwankwo, and F. Uwadia, "Resilience and Security on Enterprise Networks: A Multi-Sector Study," in *2022 5th Information Technology for Education and Development (ITED)*, 2022, pp. 1–7.

[111] K. Strandberg, T. Rosenstatter, R. Jolak, N. Nowdehi, and T. Olovsson, "Resilient Shield: Reinforcing the Resilience of Vehicles Against Security Threats," in *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*, 2021, pp. 1–7.

[112] A. Amini, M. Ghafouri, A. Mohammadi, M. Hou, A. Asif, and K. Plataniotis, "Secure Sampled-Data Observer-Based Control for Wind Turbine Oscillation Under Cyber Attacks," *IEEE Transactions on Smart Grid*, vol. 13, no. 4, pp. 3188–3202, 2022, doi: 10.1109/TSG.2022.3159582.

[113] H. Lee, S. Kim, and H. K. Kim, "SoK: Demystifying Cyber Resilience Quantification in Cyber-Physical Systems," in *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*, 2022, pp. 178–183.

[114] J. F. Carías, M. R. S. Borges, L. Labaka, S. Arrizabalaga, and J. Hernantes, "Systematic Approach to Cyber Resilience Operationalization in SMEs," *IEEE Access*, vol. 8, pp. 174200–174221, 2020, doi: 10.1109/ACCESS.2020.3026063.

[115] F. Simone, A. J. N. Akel, G. D. Gravio, and R. Patriarca, "Thinking in Systems, Sifting Through Simulations: A Way Ahead for Cyber Resilience Assessment," *IEEE Access*, vol. 11, pp. 11430–11450, 2023, doi: 10.1109/ACCESS.2023.3241552.

[116] E. Bellini and S. Marrone, "Towards a novel conceptualization of Cyber Resilience," in *2020 IEEE World Congress on Services (SERVICES)*, 2020, pp. 189–196.

[117] S. Ullah, S. Shetty, and A. Hassanzadeh, "Towards Modeling Attacker's Opportunity for Improving Cyber Resilience in Energy Delivery Systems," in *2018 Resilience Week (RWS)*, 2018, pp. 100–107.

[118] A. David McKinnon *et al.,* "User-Focused Tools to Enhance IT/OT Cyber Resilience within the Power Grid," in *2022 Resilience Week (RWS)*, 2022, pp. 1–5.

[119] S. Bagchi *et al.,* "Vision Paper: Grand Challenges in Resilience: Autonomous System Resilience through Design and Runtime Measures," *IEEE Open Journal of the Computer Society*, vol. 1, pp. 155–172, 2020, doi: 10.1109/OJCS.2020.3006807.

[120] Yu Wang, Chao Deng, Yun Liu, and Zhongbao Wei, "A cyber-resilient control approach for islanded microgrids under hybrid attacks," *International Journal of Electrical Power & Energy Systems*, vol. 147, p. 108889, 2023, doi: 10.1016/j.ijepes.2022.108889.

[121] Kiarash Sadeghi R., Arash Azadegan, and Divesh Ojha, "A path to build supply chain cyber-resilience through absorptive capacity and visibility: Two empirical studies," *Industrial Marketing Management*, vol. 111, pp. 202–215, 2023, doi: 10.1016/j.indmarman.2023.04.001.

[122] Abolfazl Rahiminejad *et al.,* "A resilience-based recovery scheme for smart grid restoration following cyberattacks to substations," *International Journal of Electrical Power & Energy Systems*, vol. 145, p. 108610, 2023, doi: 10.1016/j.ijepes.2022.108610.

[123] Sazid Rahman, Niamat Ullah Ibne Hossain, Kannan Govindan, Farjana Nur, and Mahathir Bappy, "Assessing cyber resilience of additive manufacturing supply chain leveraging data fusion technique: A model to generate cyber resilience index of a supply chain," *CIRP Journal of Manufacturing Science and Technology*, vol. 35, pp. 911–928, 2021, doi: 10.1016/j.cirpj.2021.09.008.

[124] I. Kolosok and L. Gurina, "Cyber resilience models of systems for monitoring and operational dispatch control of electric power systems," *IFAC-PapersOnLine*, vol. 55, no. 9, pp. 485–490, 2022, doi: 10.1016/j.ifacol.2022.07.084.

[125] Radu F. Babiceanu and Remzi Seker, "Cyber resilience protection for industrial internet of things: A software-defined networking approach," *Computers in Industry*, vol. 104, pp. 47–58, 2019, doi: 10.1016/j.compind.2018.10.004.

[126] João Pavão, Rute Bastardo, Dário Carreira, and Nelson Pacheco Rocha, "Cyber Resilience, a Survey of Case Studies," *Procedia Computer Science*, vol. 219, pp. 312–318, 2023, doi: 10.1016/j.procs.2023.01.295.

[127] Andrea Salvi, Paolo Spagnoletti, and Nadia Saad Noori, "Cyber-resilience of Critical Cyber Infrastructures: Integrating digital twins in the electric power ecosystem," *Computers & Security*, vol. 112, p. 102507, 2022, doi: 10.1016/j.cose.2021.102507.

[128] Fabian Heymann, Stéphane Henry, and Matthias Galus, "Cybersecurity and resilience in the swiss electricity sector: Status and policy options," *Utilities Policy*, vol. 79, p. 101432, 2022, doi: 10.1016/j.jup.2022.101432.

[129] Gregory Epiphaniou, Mohammad Hammoudeh, Hu Yuan, Carsten Maple, and Uchenna Ani, "Digital twins in cyber effects modelling of IoT/CPS points of low resilience," *Simulation Modelling Practice and Theory*, vol. 125, p. 102744, 2023, doi: 10.1016/j.simpat.2023.102744.

[130] Michal Tonhauser and Jozef Ristvej, "Disruptive acts in cyberspace, steps to improve cyber resilience at National Level," *Transportation Research Procedia*, vol. 40, pp. 1591–1596, 2019, doi: 10.1016/j.trpro.2019.07.220.

[131] J. Jeimy and M. Cano, "FLEXI - A Conceptual Model for Enterprise Cyber Resilience," *Procedia Computer Science*, vol. 219, pp. 11–19, 2023, doi: 10.1016/j.procs.2023.01.258.

[132] Riccardo Patriarca, Francesco Simone, and Giulio Di Gravio, "Modelling cyber resilience in a water treatment and distribution system," *Reliability Engineering & System Safety*, vol. 226, p. 108653, 2022, doi: 10.1016/j.ress.2022.108653.

[133] Yunhan Huang, Linan Huang, and Quanyan Zhu, "Reinforcement Learning for feedback-enabled cyber resilience," *Annual Reviews in Control*, vol. 53, pp. 273–295, 2022, doi: 10.1016/j.arcontrol.2022.01.001.

[134] Carlos Espinoza-Zelaya and Young Bai Moon, "Resilience Enhancing Mechanisms for Cyber-Manufacturing Systems against Cyber-Attacks," *IFAC-PapersOnLine*, vol. 55, no. 10, pp. 2252–2257, 2022, doi: 10.1016/j.ifacol.2022.10.043.

[135] Paul Theron, "Through-life cyber resilience in future smart manufacturing environments. A research programme," *Procedia Manufacturing*, vol. 16, pp. 193–207, 2018, doi: 10.1016/j.promfg.2018.10.157.

[136] Michael J. Lees, Melissa Crawford, and Christoph Jansen, "Towards Industrial Cybersecurity Resilience of Multinational Corporations," *IFAC-PapersOnLine*, vol. 51, no. 30, pp. 756–761, 2018, doi: 10.1016/j.ifacol.2018.11.201.

[137] Alessandro Annarelli, Fabio Nonino, and Giulia Palombi, "Understanding the management of cyber resilient systems," *Computers & Industrial Engineering*, vol. 149, p. 106829, 2020, doi: 10.1016/j.cie.2020.106829.

Abbildungsverzeichnis

Tabellenverzeichnis

Glossar

ADDSec *Artificial Diversity and Defense Security*

ADS *Active Distribution Systems*

AI *Artificial Itelligence*

APT *Advanced Persistent Threat*

BAS *Building Automation System*

BCM *Business Continuity Management*

CCI *Critical Cyber Infrastructure*

CEER Council of European Energy Regulators

CMS *Cyber Manufacturing Systems*

CPARM Cyber-Physical Mulit-Aspect Resilience-Based Recovery Metric

CPS Cyber-Physical-Systems

CR *Cyber Resilience*

CREF Cyber Resiliency Engineering Framework

CRF Cyber Resilience Framework

CSEF *Cyber Security Efficient Frontier*

CSF *Cyber Security Framework*

CsR Cyber-Side Resilience

CVSS Common Vulnerability Scoring System

DDoS *Distributed Denial of Service*

DORA Digital Operational Resilience Act

DoS *Denial of Service*

DSL *Domain-Specific-Language*

EDS *Energy Delivery System*

ENISA *European Union Agency for Cyber-Security*

EU European Union

FAIR *Factor Analysis Information Risk*

FDI *False Data Injection*

GCI *Global Cyber Security Index*

ICS Industry Control Systems

IDS *Intrusion Detection System*

IIoT Industrial Internet of Things

IKT *Informations- und Kommunikationstechnik*

IoT *Internet of Things*

IRAM *Infrastructure Resilience Analysis Methodology*

ISO *International Organization for Standardization*

MBSE *Model Based System Engineering*

MiTM *Man-in-The-Middle Attack*

MNC *Multinationalen Kooperationen*

MTD *Moving Target Defense*

NDN Architektur Named Data Network

NIS *Network and Information Security*

NIST *National Institute of Standards and Technology*

OT *Operation Technologie*

PLC *Programmable Logic Controller*

PsR *Physical-Side Resilience*

QMoCR *Quantitative Measurement of Cyber Resilience*

RDR *Recovery Dependent Resilience*

RL Reinforcement Learning

SEI *Secure Execution Intervals*

SI Systemic Impact

SLR *Systematische Literatur Analyse*

SSI *Sub-Synchronous Interaction*

STAMP *System Theoretic Accident Modelling and Processes*

STPA-Sec/S *System Theoretic Process Analysis for Security through Simulations*

TE FRR *Traffic Engineering Fast Rerouting*

TRE *Total Recovery Effort*

V4 *Visegrad Four*

Anhang A

Tabelle 21 zeigt das Protokoll nach PRISMA 2020 [46] mit Referenz auf den Inhalt der Kapitel Einleitung und Methodik. Abweichungen zum initial entwickelten Protokoll und Checklistenpunkte, die nicht anwendbar sind werden in Spalte „Anwendbarkeit und Abweichung“ beschrieben.

Protokoll nach PRISMA2020					
PRISMA-P Checklist					
Kapitel	Thema	Nr.	Beschreibung	Anwendbarkeit und Abweichungen	Seite
Administrative information	Title: Identification	1a	Identify the report as a protocol of a systematic review	Nicht anwendbar, da keine Veröffentlichung	na
	Title: Update	1b	If the protocol is for an update of a previous systematic review, identify as such	Nicht anwendbar, da neue SLR	na
	Registration	2	If registered, provide the name of the registry (such as PROSPERO) and registration number	Nicht anwendbar, da keine Veröffentlichung	na
	Authors: Contact	3a	Provide name, institutional affiliation, e-mail address of all protocol authors; provide physical mailing address of corresponding author	Traude Lang, is201809@fhstp.ac.at	Deckblatt
	Authors: Contributions	3b	Describe contributions of protocol authors and identify the guarantor of the review	Nicht anwendbar	na
	Amendments	4	If the protocol represents an amendment of a previously completed or published protocol, identify as such and list changes; otherwise, state plan for documenting important protocol amendments	Nicht anwendbar	na
	Support: Sources	5a	Indicate sources of financial or other support for the review	Nicht anwendbar	na
	Support: Sponsor	5b	Provide name for the review funder and/or sponsor	Nicht anwendbar	na
	Support: Role of sponsor or funder	5c	Describe roles of funder(s), sponsor(s), and/or institution(s), if any, in developing the protocol	Nicht anwendbar	na

Introduction	Rationale	6	Describe the rationale for the review in the context of what is already known		1-3
	Objectives	7	Provide an explicit statement of the question(s) the review will address with reference to participants, interventions, comparators, and outcomes (PICO)		5-6
Methods	Eligibility criteria	8	Specify the study characteristics (such as PICO, study design, setting, time frame) and report characteristics (such as years considered, language, publication status) to be used as criteria for eligibility for the review	Eingeschränkte Anzahl von in Studien angeführten Angriffen von 3 Angriffstypen auf einem Angriff geändert.	8-9
	Information sources	9	Describe all intended information sources (such as electronic databases, contact with study authors, trial registers or other grey literature sources) with planned dates of coverage		7-8
	Search strategy	10	Present draft of search strategy to be used for at least one electronic database, including planned limits, such that it could be repeated		7-8
	Study records: Data management	11a	Describe the mechanism(s) that will be used to manage records and data throughout the review		9
	Study records: Selection process	11b	State the process that will be used for selecting studies (such as two independent reviewers) through each phase of the review (that is, screening, eligibility and inclusion in meta-analysis)		9-10
	Study records: Data collection process	11c	Describe planned method of extracting data from reports (such as piloting forms, done independently, in duplicate), any processes for obtaining and confirming data from investigators		10-12
	Data items	12	List and define all variables for which data will be sought (such as PICO items, funding sources), any pre-planned data assumptions and simplifications		8

	Outcomes and prioritization	13	List and define all outcomes for which data will be sought, including prioritization of main and additional outcomes, with rationale		na
	Risk of bias in individual studies	14	Describe anticipated methods for assessing risk of bias of individual studies, including whether this will be done at the outcome or study level, or both; state how this information will be used in data synthesis		12
	Data synthesis	15a	Describe criteria under which study data will be quantitatively synthesised		11-12
		15b	If data are appropriate for quantitative synthesis, describe planned summary measures, methods of handling data and methods of combining data from studies, including any planned exploration of consistency (such as I2 , Kendall's τ)		11-12
		15c	Describe any proposed additional analyses (such as sensitivity or subgroup analyses, meta-regression)		11-12
		15d	If quantitative synthesis is not appropriate, describe the type of summary planned		11-12
	Meta-bias(es)	16	Specify any planned assessment of meta-bias(es) (such as publication bias across studies, selective reporting within studies)		12
	Confidence in cumulative evidence	17	Describe how the strength of the body of evidence will be assessed (such as GRADE)		12

Tabelle 21: Protokoll nach PRISMA 2020

Tabelle 21 beschreibt die Erfüllung der PRISAM 2020 Checklist [47] und wo diese in vorliegender Arbeit zu finden sind.

Prisma 2020 Checklist				
Kapitel	**Thema**	**Nr**	**Checklist Beschreibung**	**Seite**
TITLE	Title	1	Identify the report as a systematic review.	Deckblatt
ABSTRACT	Abstract	2	See the PRISMA 2020 for Abstracts checklist.	na
INTRODUCTION	Rationale	3	Describe the rationale for the review in the context of existing knowledge.	1-3
	Objectives	4	Provide an explicit statement of the objective(s) or question(s) the review addresses.	5-6
METHODS	Eligibility criteria	5	Specify the inclusion and exclusion criteria for the review and how studies were grouped for the syntheses.	8-9
	Information sources	6	Specify all databases, registers, websites, organisations, reference lists and other sources searched or consulted to identify studies. Specify the date when each source was last searched or consulted.	7-8
	Search strategy	7	Present the full search strategies for all databases, registers and websites, including any filters and limits used.	7-8
	Selection process	8	Specify the methods used to decide whether a study met the inclusion criteria of the review, including how many reviewers screened each record and each report retrieved, whether they worked independently, and if applicable, details of automation tools used in the process.	9-10
	Data collection process	9	Specify the methods used to collect data from reports, including how many reviewers collected data from each report, whether they worked independently, any processes for obtaining or confirming data from study investigators, and if applicable, details of automation tools used in the process.	10-12
	Data items	10a	List and define all outcomes for which data were sought. Specify whether all results that were compatible with each outcome domain in each study were sought (e.g. for all measures, time points, analyses), and if not, the methods used to decide which results to collect.	8
		10b	List and define all other variables for which data were sought (e.g. participant and intervention characteristics, funding sources). Describe any assumptions made about any missing or unclear information.	na

	Study risk of bias assessment	11	Specify the methods used to assess risk of bias in the included studies, including details of the tool(s) used, how many reviewers assessed each study and whether they worked independently, and if applicable, details of automation tools used in the process.	12
	Effect measures	12	Specify for each outcome the effect measure(s) (e.g. risk ratio, mean difference) used in the synthesis or presentation of results.	na
	Synthesis methods	13a	Describe the processes used to decide which studies were eligible for each synthesis (e.g. tabulating the study intervention characteristics and comparing against the planned groups for each synthesis (item #5)).	8-9
		13b	Describe any methods required to prepare the data for presentation or synthesis, such as handling of missing summary statistics, or data conversions.	11-12
		13c	Describe any methods used to tabulate or visually display results of individual studies and syntheses.	11-12
		13d	Describe any methods used to synthesize results and provide a rationale for the choice(s). If meta-analysis was performed, describe the model(s), method(s) to identify the presence and extent of statistical heterogeneity, and software package(s) used.	11-12
		13e	Describe any methods used to explore possible causes of heterogeneity among study results (e.g. subgroup analysis, meta-regression).	na
		13f	Describe any sensitivity analyses conducted to assess robustness of the synthesized results.	na
	Reporting bias assessment	14	Describe any methods used to assess risk of bias due to missing results in a synthesis (arising from reporting biases).	12
	Certainty assessment	15	Describe any methods used to assess certainty (or confidence) in the body of evidence for an outcome.	12
RESULTS	Study selection	16a	Describe the results of the search and selection process, from the number of records identified in the search to the number of studies included in the review, ideally using a flow diagram.	11

		16b	Cite studies that might appear to meet the inclusion criteria, but which were excluded, and explain why they were excluded.	11, Studien nicht zieitert, Citavi Export als Zusatzmaterial enthält excudierte Studien
	Study characteristics	17	Cite each included study and present its characteristics.	ab 13
	Risk of bias in studies	18	Present assessments of risk of bias for each included study.	na
	Results of individual studies	19	For all outcomes, present, for each study: (a) summary statistics for each group (where appropriate) and (b) an effect estimate and its precision (e.g. confidence/credible interval), ideally using structured tables or plots.	36-52
	Results of syntheses	20a	For each synthesis, briefly summarise the characteristics and risk of bias among contributing studies.	13-35
		20b	Present results of all statistical syntheses conducted. If meta-analysis was done, present for each the summary estimate and its precision (e.g. confidence/credible interval) and measures of statistical heterogeneity. If comparing groups, describe the direction of the effect.	13-35
		20c	Present results of all investigations of possible causes of heterogeneity among study results.	na
		20d	Present results of all sensitivity analyses conducted to assess the robustness of the synthesized results.	na
	Reporting biases	21	Present assessments of risk of bias due to missing results (arising from reporting biases) for each synthesis assessed.	na
	Certainty of evidence	22	Present assessments of certainty (or confidence) in the body of evidence for each outcome assessed.	na
DISCUSSION	Discussion	23a	Provide a general interpretation of the results in the context of other evidence.	53-57
		23b	Discuss any limitations of the evidence included in the review.	35, 57
		23c	Discuss any limitations of the review processes used.	57
		23d	Discuss implications of the results for practice, policy, and future research.	53-57

OTHER INFORMATION	Registration and protocol	24a	Provide registration information for the review, including register name and registration number, or state that the review was not registered.	na
		24b	Indicate where the review protocol can be accessed, or state that a protocol was not prepared.	na
		24c	Describe and explain any amendments to information provided at registration or in the protocol.	na
	Support	25	Describe sources of financial or non-financial support for the review, and the role of the funders or sponsors in the review.	na
	Competing interests	26	Declare any competing interests of review authors.	na
	Availability of data, code and other materials	27	Report which of the following are publicly available and where they can be found: template data collection forms; data extracted from included studies; data used for all analyses; analytic code; any other materials used in the review.	na

Tabelle 22 : PRISAM 2020 Checklist und deren Anwendbarkeit

Tabelle 23 beschreibt die Erfüllung der PRISMA 2020 Checklist for Abstracts [45].

Prisma 2020 Checklist for Abstracts				
Sektion	**Thema**	**Nr**	**Checklist Beschreibung**	**Umsetzung**
TITLE	Title	1	Identify the report as a systematic review.	erfüllt
BACKGROUND	Objectives	2	Provide an explicit statement of the main objective(s) or question(s) the review addresses.	erfüllt
METHODS	Eligibility criteria	3	Specify the inclusion and exclusion criteria for the review.	teilweise erfüllt
	Information sources	4	Specify the information sources (e.g. databases, registers) used to identify studies and the date when each was last searched.	erfüllt
	Risk of bias	5	Specify the methods used to assess risk of bias in the included studies.	nicht anwendbar
	Synthesis of results	6	Specify the methods used to present and synthesise results.	erfüllt
RESULTS	Included studies	7	Give the total number of included studies and participants and summarise relevant characteristics of studies.	erfüllt

	Synthesis of results	8	Present results for main outcomes, preferably indicating the number of included studies and participants for each. If meta-analysis was done, report the summary estimate and confidence/credible interval. If comparing groups, indicate the direction of the effect (i.e. which group is favoured).	erfüllt
DISCUSSION	Limitations of evidence	9	Provide a brief summary of the limitations of the evidence included in the review (e.g. study risk of bias, inconsistency and imprecision).	erfüllt
	Interpretation	10	Provide a general interpretation of the results and important implications.	erfüllt
OTHER	Funding	11	Specify the primary source of funding for the review.	nicht anwendbar
	Registration	12	Provide the register name and registration number.	nicht anwendbar

Tabelle 23 : Checklist for Abstracts nach PRISAM 2020

Anhang B

Tabelle 1Tabelle 24 zeigt die extrahierten Daten und deren Bezug zu den Forschungsfragen.

Eigenschaft	**Forschungsfrage**
Titel der Studie	allgemein
Autoren der Studie (erst angeführter Autor/Autorin)	allgemein, Q4
Nationalität Autor /Autorin (erst angeführter Autor/Autorin)	allgemein, Q4
Sponsor sofern anwendbar	allgemein, Q4
Universität oder Institution	allgemein, Q4
Herkunftsland Universität oder Institution	allgemein, Q4
Publikationsjahr	allgemein, Q4
Datenbank	allgemein, Q4
Journal/Zeitschrift	allgemein, Q4
Ranking des Journals	allgemein, Q4
Zitiert Häufigkeit (Google Scholar)	allgemein, Q4
Angewandte Methoden / Techniken	Q1,Q4
Forschungsdomäne / Bereich	Q1, Q4
Motivation für Studie	Q2, Q3, Q4
Inhalte und Ergebnisse der Studien (qualitative)	Q1-4
Future Works Empfehlungen	Q4
Limitierungen die in Studien erkannt wurden	Q4, Q1
Branche	Q2
Adressierte Risiken	Q2,Q3
Definition CR in Studie	allgemein
verwendete Keywords	allgemein

Tabelle 24: Datenextraktionsformular

Anhang C

Tabelle 25 und Tabelle 26 zeigen die h-Metriken sowie Zitate der ausgewählten Studien und deren Veröffentlichungen.

h-Index	Journal / Konferenz	Studien / Artikel Quelle
> 100	IEEE Access	[82], [100], [102], [112], [114], [115], [126], [131], [137]
	IEEE Transactions on Smart Grid	
	Procedia Computer Science	
75 - 99	Computers & Industrial Engineering	[106], [120], [121], [122], [125], [127], [132], [135]
	Industrial Marketing Management	
	IEEE Sensors Journal	
	Computers in Industry	
	Computers & Security	
	Reliability Engineering & System Safety	
	International Journal of Electrical Power & Energy Systems	
	International Journal of Electrical Power & Energy Systems	
50 - 74	Procedia Manufacturing	[63], [71], [107], [130], [133], [135]
	IEEE Transactions on Software Engineering	
	Annual Reviews in Control	
	IEEE Transactions on Engineering Management	
	Transportation Research Procedia	
	IEEE International Conference on Automated Software Engineering (ASE)	
25 - 49	Simulation Modelling Practice and Theory	[61], [62], [86], [91], [95], [103], [123], [128], [129]
	Utilities Policy	
	ACM Symposium on Applied Computing	
	IEEE Engineering Management Review	
	CIRP Journal of Manufacturing Science and Technology	
	Annual Conference of Industrial Electronics Society	
	IEEE International Conference on Smart Grid Communications (SmartGridComm)	
	IEEE/ACM International Conference on Cyber-Physical Systems (ICCPS)	
0 - 24	Global Internet of Things Summit (GIoTS)	[76], [77], [78], [79], [81], [83], [84], [87], [89], [90], [92], [93], [94], [97], [101], [105], [108], [109], [111], [113]
	IEEE International Conference on Dependable Systems, Services and Technologies (DESSERT)	
	IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)	
	Military Communications Conference MILCOM	
	International Scientific-Practical Conference Problems of Infocommunications Science and Technology	
	IEEE International Conference on Intelligence and Security Informatics (ISI)	

	IEEE International Symposium on Network Computing and Applications	
	IEEE Embedded Systems Letters	
	International Conference on Cyber Conflict (ICCC)	
	International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)	
	IEEE International Conference on Intelligent Data and Security (IDS)	
	IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC)	
	IEEE International Conference on Engineering of Complex Computer Systems	
	IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications	
	IEEE Conference on Vehicular Technology (VTC)	
	IEEE International SOC Conference	
	International Conference on Cyber Resilience (ICCR)	
	IEEE Kansas Power and Energy Conference	
	IEEE International Conference on Cyber-Security and Resilience (CSR)	
	IEEE International Mediterranean Conference on Communications and Networking (MeditCom)	
Nicht erkannt	Annual Conference on Information Sciences and Systems (CISS)	[58], [59], [60], [64], [65], [66], [67], [69], [70], [74], [80], [81], [85], [88], [96], [98], [99], [104], [110], [116], [117], [118], [119], [124], [134], [136]
	IEEE International Conference on Data Science in Cyberspace (DSC)	
	IEEE Open Journal of the Computer Society	
	IEEE World Congress on Services (SERVICES)	
	IFAC-PapersOnLine	
	Information Technology for Education and Development (ITED)	
	International Conference on Smart Sensors and Application (ICSSA)	
	International Workshop on Reliable Networks Design and Modeling (RNDM)	
	Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems	
	Proceedings of the 5th ACM Computer Science in Cars Symposium	
	Proceedings of the 6th ACM on Cyber-Physical System Security Workshop	
	Proceedings of the 7th Symposium on Hot Topics in the Science of Security	
	Proceedings of the 9th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems	
	Proceedings of the Biannual World Automation Congress	
	Resilience Week (RWS)	
	Workshop Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)	

Tabelle 25 : Journale und Konferenzen mit Verweis auf Google h-Index und dazugehörige Studien

H5-Index	H-Meridian	Zitate aus Google Scholar	Titel der Studie	Studien / Artikel Quelle	Journal oder Konferenzname
na	na	5	Resilience Enhancing Mechanisms for Cyber-Manufacturing Systems against Cyber-Attacks	[134]	10th IFAC Conference on Manufacturing Modelling, Management and Control MIM 2022
na	na	2	Cyber resilience models of systems for monitoring and operational dispatch control of electric power systems	[124]	11th IFAC Symposium on Control of Power and Energy Systems CPES 2022
na	na	15	Towards Industrial Cybersecurity Resilience of Multinational Corporations	[136]	18th IFAC Conference on Technology, Culture and International Stability TECIS 2018
na	na	1	Piecewise Linear and Stochastic Models for the Analysis of Cyber Resilience	[104]	Annual Conference on Information Sciences and Systems (CISS)
na	na	3	Enhancing Continuous Service of Information Systems Based on Cyber Resilience	[88]	IEEE International Conference on Data Science in Cyberspace (DSC)
na	na	15	Vision Paper: Grand Challenges in Resilience: Autonomous System Resilience through Design and Runtime Measures	[119]	IEEE Open Journal of the Computer Society
na	na	9	Towards a novel conceptualization of Cyber Resilience	[116]	IEEE World Congress on Services (SERVICES)
na	na	16	Cyber Resilience in IoT Network: Methodology and Example of Assessment through Epidemic Spreading Approach	[80]	IEEE World Congress on Services (SERVICES)
na	na	0	Resilience and Security on Enterprise Networks: A Multi-Sector Study	[110]	Information Technology for Education and Development (ITED)
na	na	2	A Review on Cyber Resilience Model in Small and Medium Enterprises	[70]	International Conference on Smart Sensors and Application (ICSSA)
na	na	24	Analytical modeling and assessment of cyber resilience on the base of stochastic networks conversion	[74]	International Workshop on Reliable Networks Design and Modeling (RNDM)
na	na	3	A Cyber-Physical Experimentation Platform for Resilience Analysis	[58]	Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems
na	na	4	Analysis of E-Mobility-Based Threats to Power Grid Resilience	[59]	Proceedings of the 5th ACM Computer Science in Cars Symposium
na	na	4	Evaluating Cascading Impact of Attacks on Resilience of Industrial Control Systems: A Design-Centric Modeling Approach	[60]	Proceedings of the 6th ACM on Cyber-Physical System Security Workshop

na	na	7	Simulation Testbed for Railway Infrastructure Security and Resilience Evaluation	[64]	Proceedings of the 7th Symposium on Hot Topics in the Science of Security
na	na	1	Towards Cyber-Resilient Telecontrol Commands Using Software-Defined Networking	[65]	Proceedings of the 9th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems
na	na	1	A Review of Cyber–Resilient Smart Grid	[69]	Proceedings of the Biannual World Automation Congress
na	na	1	A Cyber-Resilience Risk Management Architecture for Distributed Wind	[67]	Resilience Week (RWS)
na	na	5	A Cyber Resilient Design for Control Systems	[66]	Resilience Week (RWS)
na	na	0	User-Focused Tools to Enhance IT/OT Cyber Resilience within the Power Grid	[118]	Resilience Week (RWS)
na	na	2	Measurement and Analysis of Cyber Resilience for Control Systems: An Illustrative Example	[98]	Resilience Week (RWS)
na	na	8	Modeling Cyber Resilience for Energy Delivery Systems Using Critical System Functionality	[99]	Resilience Week (RWS)
na	na	13	Towards Modeling Attacker's Opportunity for Improving Cyber Resilience in Energy Delivery Systems	[117]	Resilience Week (RWS)
na	na	9	Intrusion Detection & Response using an Unsupervised Artificial Neural Network on a Single Board Computer for Building Control Resilience	[96]	Resilience Week (RWS)
na	na	15	Cyber-Physical Security and Resiliency Analysis Testbed for Critical Microgrids with IEEE 2030.5	[85]	Workshop Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)
233	350	21	Named Data Networking's Intrinsic Cyber-Resilience for Vehicular CPS	[102]	IEEE Access
233	350	11	Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs	[82]	IEEE Access
233	350	37	Systematic Approach to Cyber Resilience Operationalization in SMEs	[114]	IEEE Access
233	350	1	Thinking in Systems, Sifting Through Simulations: A Way Ahead for Cyber Resilience Assessment	[115]	IEEE Access
147	193	4	Secure Sampled-Data Observer-Based Control for Wind Turbine Oscillation Under Cyber Attacks	[112]	IEEE Transactions on Smart Grid
147	193	76	Multi-Agent Based Attack-Resilient System Integrity Protection for Smart Grid	[100]	IEEE Transactions on Smart Grid
113	166	1	Cyber Resilience, a Survey of Case Studies	[126]	CENTERIS – International Conference on ENTERprise Information Systems / ProjMAN – International Conference on Project MANagement / HCist – International Conference on Health and Social Care Information Systems and Technologies
113	166	1	FLEXI - A Conceptual Model for Enterprise Cyber Resilience	[131]	Procedia Computer Science
104	151	53	Understanding the management of cyber resilient systems	[137]	Computers & Industrial Engineering

99	137	0	A path to build supply chain cyber-resilience through absorptive capacity and visibility: Two empirical studies	[121]	Industrial Marketing Management
95	128	37	Proactive Threat Detection for Connected Cars Using Recursive Bayesian Estimation	[106]	IEEE Sensors Journal
90	143	63	Cyber resilience protection for industrial internet of things: A software-defined networking approach	[125]	Computers in Industry
89	131	22	Cyber-resilience of Critical Cyber Infrastructures: Integrating digital twins in the electric power ecosystem	[127]	Computers & Security
89	121	6	Modelling cyber resilience in a water treatment and distribution system	[132]	Reliability Engineering & System Safety
84	107	7	A resilience-based recovery scheme for smart grid restoration following cyberattacks to substations	[122]	International Journal of Electrical Power & Energy Systems
84	107	4	A cyber-resilient control approach for islanded microgrids under hybrid attacks	[120]	International Journal of Electrical Power & Energy Systems
74	112	9	Through-life cyber resilience in future smart manufacturing environments. A research programme	[135]	7th International Conference on Through-life Engineering Services
69	113	2	Program Synthesis for Cyber-Resilience	[107]	IEEE Transactions on Software Engineering
59	103	38	Reinforcement Learning for feedback-enabled cyber resilience	[133]	Annual Reviews in Control
57	85	36	Ambidextrous Cybersecurity: The Seven Pillars (7Ps) of Cyber Resilience	[71]	IEEE Transactions on Engineering Management
56	75	10	Disruptive acts in cyberspace, steps to improve cyber resilience at National Level	[130]	TRANSCOM 2019 13th International Scientific Conference on Sustainable, Modern and Safe Transport
50	81	55	Learning-Guided Network Fuzzing for Testing Cyber-Physical System Defences	[63]	IEEE International Conference on Automated Software Engineering (ASE)
45	69	3	Digital twins in cyber effects modelling of IoT/CPS points of low resilience	[129]	Simulation Modelling Practice and Theory
38	53	3	Cybersecurity and resilience in the swiss electricity sector: Status and policy options	[128]	Utilities Policy
36	69	9	Incorporating Systems Thinking Into a Cyber Resilience Maturity Model	[95]	IEEE Engineering Management Review
36	69	14	How to Measure Cyber-Resilience of a System With Autonomous Agents: Approaches and Challenges	[91]	IEEE Engineering Management Review
36	47	20	Integrated Simulation Testbed for Security and Resilience of CPS	[62]	ACM Symposium on Applied Computing
35	48	13	Assessing cyber resilience of additive manufacturing supply chain leveraging data fusion technique: A model to generate cyber resilience index of a supply chain	[123]	CIRP Journal of Manufacturing Science and Technology
28	41	13	Performance-Based Cyber Resilience Metrics: An Applied Demonstration Toward Moving Target Defense	[103]	Annual Conference of Industrial Electronics Society

25	50	60	Guaranteed Physical Security with Restart-Based Design for Cyber-Physical Systems	[61]	IEEE/ACM International Conference on Cyber-Physical Systems (ICCPS)
25	38	6	Cyber-Resilience Enhancement of PMU Networks Using Software-Defined Networking	[86]	IEEE International Conference on Smart Grid Communications (SmartGridComm)
24	37	5	Implementing Cyber Resilient Designs through Graph Analytics Assisted Model Based Systems Engineering	[93]	IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)
24	35	8	An Approach to the Modeling of Cyber Resilience Management	[72]	Global Internet of Things Summit (GIoTS)
24	35	5	Implementing Cyber-Security Measures in Airports to Improve Cyber-Resilience	[94]	Global Internet of Things Summit (GIoTS)
24	32	1	Multilevel Fuzzy Logic-Based Approach for Critical Energy Infrastructure's Cyber Resilience Assessment	[101]	IEEE International Conference on Dependable Systems, Services and Technologies (DESSERT)
23	40	4	An Experimentation Infrastructure for Quantitative Measurements of Cyber Resilience	[73]	Military Communications Conference MILCOM
23	40	3	Mathematical Modeling of Cyber Resilience	[97]	Military Communications Conference MILCOM
22	26	1	Redundancy Cyber Resiliency Technique Based on Fast ReRouting under Security Metric	[109]	International Scientific-Practical Conference Problems of Infocommunications Science and Technology
20	31	46	Cyber Resilience Framework for Industrial Control Systems: Concepts, Metrics, and Insights	[79]	IEEE International Conference on Intelligence and Security Informatics (ISI)
20	29	12	Cyber-Resilience Evaluation of Cyber-Physical Systems	[87]	IEEE International Symposium on Network Computing and Applications
18	30	6	A Quad-Redundant PLC Architecture for Cyber-Resilient Industrial Control Systems	[68]	IEEE Embedded Systems Letters
18	27	1	Cyber Resilience versus Cybersecurity as Legal Aspiration	[84]	International Conference on Cyber Conflict (ICCC)
17	28	12	Focusing on the Recovery Aspects of Cyber Resilience	[90]	International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)
16	27	19	ICS-CRAT: A Cyber Resilience Assessment Tool for Industrial Control Systems	[92]	IEEE International Conference on Intelligent Data and Security (IDS)
15	22	1	Cyber Resilience Modelling for the Operations of Hybrid Network	[81]	IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC)
15	22	3	Comparative Analysis of Cyber Resilience Strategy in Asia-Pacific Countries	[76]	IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC)
14	21	12	AWaRE - Towards Distributed Self-Management for Resilient Cyber Systems	[75]	IEEE International Conference on Engineering of Complex Computer Systems
14	19	27	Cyber Resilience Approach Based on Traffic Engineering Fast ReRoute with Policing	[77]	IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications
13	18	9	Resilient Shield: Reinforcing the Resilience of Vehicles Against Security Threats	[111]	IEEE Conference on Vehicular Technology (VTC)

13	16	9	Establishing Cyber Resilience in Embedded Systems for Securing Next-Generation Critical Infrastructure	[89]	IEEE International SOC Conference
12	15	2	Qualitative Factors in Organizational Cyber Resilience	[108]	International Conference on Cyber Resilience (ICCR)
11	16	8	Cyber Resilience using State Estimation Updates Based on Cyber Attack Matrix Classification	[83]	IEEE Kansas Power and Energy Conference
8	10	1	SoK: Demystifying Cyber Resilience Quantification in Cyber-Physical Systems	[113]	IEEE International Conference on Cyber Security and Resilience (CSR)
8	10	4	Cyber Resilience for Self-Monitoring IoT Devices	[78]	IEEE International Conference on Cyber Security and Resilience (CSR)
8	9	7	Practical Autonomous Cyberhealth for resilient Micro, Small and Medium-sized Enterprises	[105]	IEEE International Mediterranean Conference on Communications and Networking (MeditCom)

Tabelle 26 : h-Metriken und Zitate nach Studien und deren Veröffentlichung