HMD (2023) 60:214–229
https://doi.org/10.1365/s40702-022-00888-3

SPEKTRUM

Cyberrisiken – Vom Begriffswirrwarr zu einem einheitlichen Begriffsverständnis

Daniel Zängerle · Dirk Schiereck

Eingegangen: 16. November 2021 / Angenommen: 15. Juni 2022 / Online publiziert: 6. Juli 2022

Zusammenfassung Vor dem Hintergrund einer hochdynamischen Entwicklung weltweiter Cybervorfälle und der stetig wachsenden Bedeutung der Cyberforschung untersucht dieser Beitrag anhand einer systematischen und strukturierten Inhaltsanalyse die in der Wissenschaft und praxisnahen Literatur postulierten Definitionsansätze des Terminus Cyberrisiko und leitet ein disziplinübergreifendes Begriffsmodell als Basis für die künftige Cyberforschung und das operationelle Risikomanagement ab. Die Ergebnisse zeigen, dass es bislang keine einheitliche Begriffsdefinition für das Cyberrisiko gibt und die analysierten Definitionsansätze eine Vielzahl an unterschiedlichen Kernmerkmalen des Cyberrisikos zusammenfassen. Besonders häufig werden direkte und indirekte Auswirkungen, physische und digitale Risikoobjekte sowie beabsichtigte und sonstige Bedrohungen in den untersuchten Definitionen identifiziert, obgleich unbeabsichtigte Bedrohungen, insbesondere durch den Faktor Mensch als Einfallstor, nicht zu vernachlässigen sind. Das auf der Inhaltsanalyse basierende Begriffsmodell stellt eine umfassende Alternative zu den bisherigen, eher disziplinspezifischen Definitionsansätzen dar und trägt als elementarer Baustein in der Erarbeitung und dem aktuellen Diskurs über eine einheitliche Cyberterminologie bei.

Schlüsselwörter Cyberrisiko · Definition · Inhaltsanalyse · Cyberterminologie

Daniel Zängerle (✉) · Dirk Schiereck
Fachgebiet Unternehmensfinanzierung, Technische Universität Darmstadt,
Hochschulstr. 1, 64289 Darmstadt, Deutschland
E-Mail: daniel.zaengerle@stud.tu-darmstadt.de

Dirk Schiereck
E-Mail: dirk.schiereck@tu-darmstadt.de

Cyber Risks—From a Maze of Terms to a Uniform Terminology

Abstract In light of the highly dynamic developments in worldwide cyber incidents and the ever-growing importance of cyber research, this article examines, based on a systematic and structured content analysis, definitions of the term cyber risk postulated in academia and practice-oriented literature in order to derive a comprehensive and cross-disciplinary taxonomy as a basis for future cyber risk research and operational risk management. The results show that there is no uniform definition of the term cyber risk and that the analyzed definitions summarise a variety of different key characteristics. Direct and indirect impacts, physical and digital risk objects, and malicious and other threats are particularly frequently identified in the analyzed definitions, although unintentional and non-malicious threats, especially through the human factor as the main vulnerability, are not to be neglected. The new proposed cyber risk taxonomy represents a comprehensive alternative to the previous, more discipline-specific definitions and contributes as an elementary building block in the elaboration and current discourse on a unified cyber terminology.

Keywords Cyber risk · Definition · Content analysis · Cyber terminology

1 Ausgangssituation und Zielsetzung

Cyberrisiken zählen zu den weltweit größten Bedrohungen des 21. Jahrhunderts (WEF 2021). Zahlreiche Statistiken belegen ihre dramatische Zunahme. So werden die weltweiten Schadenskosten durch Cybereereignisse auf mehr als 1 Billion US-Dollar, alleine in Deutschland auf mehr als 100 Mio. € geschätzt (Bitkom 2019; McAfee 2020). Bundesweit wurden 2020 mehr als 108.000 Fälle von Cyberkriminalität und damit doppelt so viele Fälle wie noch in 2015 registriert (BKA 2021). Unklar bleibt dabei aber oft, was jeweils als Cyberrisiko oder Schaden erfasst wurde. Da die Gefahrenpotenziale von Cyberrisiken nicht nur private Internetnutzer betreffen, sondern vor allem Unternehmen und Organisationen sowohl im öffentlichen als auch privaten Sektor vor neue Herausforderungen stellen (Aldasoro et al. 2020; Bendovschi 2015; Choudhry 2014; Njegomir und Marović 2012; Wrede et al. 2018), ergibt sich auch die Frage der Versicherbarkeit und Messung von Cyberrisiken (Biener et al. 2015; Eling und Schnell 2016). Durch die weiter voranschreitende, weltweite Vernetzung der IT und die Nutzung von IT-Produkten und -Dienstleistungen, wie zum Beispiel cloudbasierten Systemen und künstlicher Intelligenz, hat sich die existentielle Bedrohung der Wettbewerbsfähigkeit und des Unternehmenserfolgs durch Cyberrisiken weiter verschärft (Aldasoro et al. 2020; Rakes et al. 2012). Selbst Cyberrisiken ohne schwerwiegende volkswirtschaftliche Implikationen können sich für ein einzelnes Unternehmen durch finanzielle Schäden sowie Image- und Reputationsverluste als existenzbedrohend herausstellen (Cavusoglu et al. 2004; Kamiya et al. 2021; Wrede et al. 2018).

Vor diesem Hintergrund ist sowohl die wissenschaftliche als auch praxisnahe Forschung zum Thema Cyberrisiko über das vergangene Jahrzehnt exponentiell gewachsen (Eling 2020). Allerdings befindet sich das Forschungsfeld immer noch in

den Anfängen und ist durch interdisziplinäre Barrieren und den Mangel an holistischen Ansätzen geprägt (Falco et al. 2019). Zur hinreichenden Vernetzung von forschungs- und praxisnaher Expertise ist es unabdingbar, ein einheitliches Verständnis für den Begriff Cyberrisiko zu entwickeln.

Das Ziel dieser Untersuchung ist die systematische und strukturierte inhaltliche Auswertung der in der theorie- und praxisnahen Literatur bekannten Definitionen des Terminus Cyberrisiko und die Ableitung eines disziplinübergreifenden Begriffsmodells (Taxonomie).[1] Basierend auf einer systematischen Literaturrecherche werden mehr als 140 relevante Textpassagen und Äußerungen von 26 Definitionsansätzen des Begriffes Cyberrisiko auf inhaltliche Kriterien untersucht. Durch Kodierung und Paraphrasierung des extrahierten Materials werden relevante und allgemeingültige Eigenschaften von Cyberrisiken abgeleitet und eine neue umfassende Definition innerhalb eines Begriffsmodells postuliert.

Während die meisten wissenschaftlichen Artikel auf eine bereits bestehende Definition referenzieren (Strupczewski 2021), finden sich nur wenige Beiträge, die die theoriegeleitete Definition von Cyberrisiken untersuchen. Beispielsweise nennen Wrede et al. (2018) 12 ausgewählte forschungs- und anwendungsbezogene Definitionsansätze und resümieren, dass kein einheitliches Begriffsverständnis besteht. Umfangreicher ist die Untersuchung von Eling und Schnell (2016), in der im Rahmen einer systematischen Literaturrecherche 20 Definitionen identifiziert werden und eine neue Begriffserklärung vorgeschlagen wird, wobei der Fokus auf dem Cyberrisiko aus Versicherungsperspektive liegt. Strupczewski (2021) hingegen untersucht in einer komparativen Inhaltsanalyse insgesamt 19 Definitionen und kommt zu der Erkenntnis, dass nur eine dieser Definitionen umfassend formuliert ist. Sein Beitrag kommt der hier vorgestellten Untersuchung am nächsten, unterscheidet sich jedoch in drei wesentlichen Aspekten. Bei einem vergleichbaren Such- und Auswahlprozess werden weniger Definitionen (19) in einem kürzeren Zeitraum (2000 bis 2018) ausgewertet, während dieser Beitrag auf insgesamt 26 Definitionsansätzen aus dem Zeitraum 2000 bis 2020 und somit auf einer aktuelleren und umfassenderen Datengrundlage basiert. Hinsichtlich der methodologischen Vorgehensweise mangelt die Inhaltsanalyse von Strupczewski (2021) an der gegenseitigen Exklusivität des Kategoriensystems (GAO 1996). Gemäß einer „vorläufigen Überprüfung der identifizierten Definitionen“ legt der Autor ohne theoriegeleitete Validierung drei Kategorien fest. Weiter schlussfolgert er, dass nur die Definitionen, die alle drei Kategorien erfüllen, vollständig formuliert sind. Im Unterschied dazu ist das hier vorgestellte Kategoriensystem aus der Cyberrisikoliteratur abgeleitet und umfasst insgesamt fünf Haupt- und 15 Subkategorien. Die identifizierten Begriffserklärungen werden in mehr als 140 Textpassagen unterteilt und einer Kategorie zugeordnet, wodurch die gegenseitige Exklusivität des Kategoriensystems sichergestellt ist. Ferner analysiert dieser Beitrag keine einzelne Definition auf Vollständigkeit, vielmehr liegt der Fokus auf der Ableitung relevanter Kerneigenschaften und eines disziplinübergreifenden Begriffsmodells. Zur Erreichung der Zielsetzung wird in Kap. 2 das methodologische Vorgehen der Studie beschrieben. Kap. 3 stellt die Ergebnisse der

[1] Die Begriffe „Taxonomie“ und „Begriffsmodell“ werden synonymisch verwendet.

strukturierten Inhaltsanalyse vor, während in Kap. 4 das abgeleitete Begriffsmodell postuliert wird. Kap. 5 diskutiert und fasst die Ergebnisse dieser Studie zusammen.

2 Methodologie und Daten

2.1 Methodologie

Nachfolgend wird die strukturierte inhaltliche Analyse von Definitionen des Begriffes „Cyberrisiko" erläutert und die Proposition eines umfassenden Begriffsmodells hergeleitet. Abb. 1 zeigt das gewählte Forschungsdesign und methodologische Vorgehen in Anlehnung an Mayring (2015).

Basierend auf einer systematischen Literaturrecherche des Begriffes „Cyber risk" in EBSCOhost[2] und Web of Science, den beiden größten Literaturdatenbanken, wird das relevante Auswahlmaterial identifiziert (Randolph 2009). Nach Konsolidierung und Prüfung auf Dubletten von Titel und Zusammenfassung werden insgesamt 120 Artikel aus dem Zeitraum von 2000 bis 2020 als relevant eingestuft und auf Begriffsdefinitionen untersucht. Weitere, teils praxisnahe Publikationen werden nach dem Schneeballverfahren ergänzt. Die abschließende Inklusionsprüfung ergibt 26 Definitionen in der Grundgesamtheit (Tabelle A des Online Materials). Als Auswertungseinheit werden alle relevanten Textpassagen der Grundgesamtheit verstanden, die in eine der inhaltlichen Kategorien fallen. Alle im Sinne des Kategoriensystems irrelevanten Äußerungen bleiben unberücksichtigt und werden bei der Kodierung übergangen (Früh 2017). Hinsichtlich der inhaltlichen Strukturierung wird das Kategoriensystem deduktiv gebildet (Mayring 2015) und beruht auf dem Cyberrisikokaskadenmodell von Böhme et al. (2019), welches in Abb. 2 dargestellt ist. Da Strupczewski (2021) drei der fünf Kategorien verwendet, wird das gewählte Kategoriensystem als tragfähig eingestuft. Zusätzlich wird dessen Angemessenheit im Rahmen eines Testdurchlaufes des Ausgangsmaterials bestätigt.

Nachfolgend werden aus den identifizierten Definitionsansätzen alle relevanten Textpassagen extrahiert und einer (Sub-)Kategorie zugeordnet. Ziel dabei ist, das Material aufgrund bestimmter, quantitativer Kriterien zu bewerten (Mayring 2015).

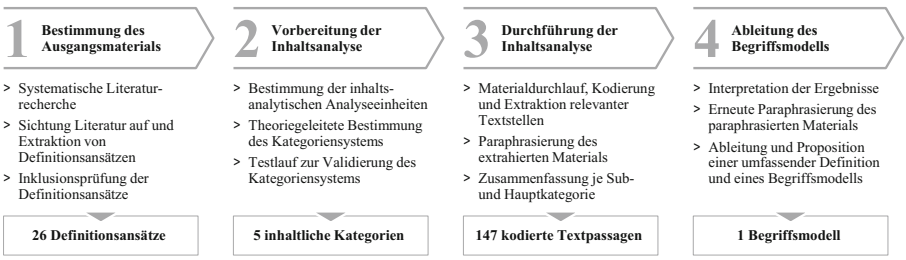

Abb. 1 Forschungsdesign und methodologisches Vorgehen der Studie

[2] Akademische Fachzeitschriften der Fachdatenbanken Business Source Premier, EconLit, Inspec®, LISTA, MathSciNet® und MEDLINE.

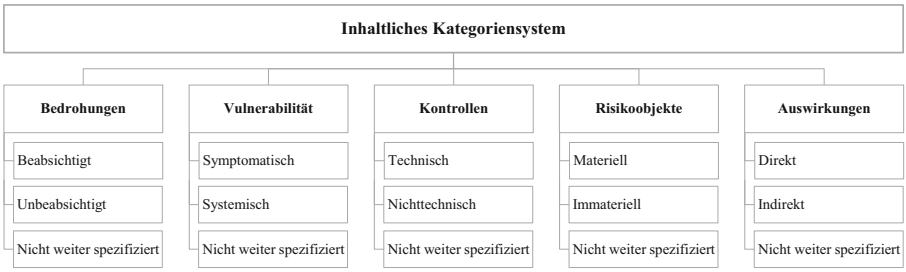

Abb. 2 Kategoriensystem in Anlehnung an Böhme et al. (2019)

Um weitere qualitative Merkmale der Begriffsdefinitionen zu entnehmen, werden die identifizierten Äußerungen je Subkategorie paraphrasiert, zusammengefasst sowie auf eine einheitliche grammatikalische und sprachliche Ebene transformiert (Mayring 2015). Dadurch können die Kernmerkmale von Cyberrisiken je Sub- und Hauptkategorie abgeleitet, inhaltliche Besonderheiten herausgearbeitet sowie eine umfassende Definition und Taxonomie des Terminus Cyberrisiko postuliert werden.

2.2 Daten

Nach 2000 erschienen erste Definitionsansätze in Artikeln im Fachgebiet Informatik (Eling 2020), in denen Cyberrisiken mit Bedrohungen aus dem Internet sowie aus Informations- und Technologiesystemen assoziiert werden (Böhme und Kataria 2006; Gordon et al. 2003). Ferner waren wesentliche Elemente die zunehmende Vernetzung von Computern und Systemen (Öğüt et al. 2011), die Verarbeitung von digitalen Informationen (Haas und Hofmann 2014) beziehungsweise die Fehlfunktion digitaler Systeme oder beschädigte Daten (Nieuwesteeg et al. 2018). Cebula und Young (2010) interpretieren Cyberrisiken als Teil des operationellen Risikos, was in der mathematischen und aktuarswissenschaftlichen Literatur intensiv diskutiert wird (Eling 2020; Eling und Loperfido 2017; Eling und Schnell 2016; Eling und Wirfs 2016; Romanosky 2016). Mukhopadhyay et al. (2013) sprechen von bösartigen elektronischen Ereignissen, während weitere Studien generalisierte Definitionsansätze postulieren (Biener et al. 2015; Böhme et al. 2019; Hiller und Russell 2013). Besonders hervorzuheben ist die Definition von Eling et al. (2016), die als mögliche Auswirkung eines Cyberrisikos den Zusammenbruch der kritischen Infrastruktur nennt.

Bezüglich der praxisnahen Definitionsansätze hat bereits 2012 das World Economic Forum (WEF) den Terminus Cyberrisiko als „[...] ein Ereignis im Bereich der vernetzten Informationssysteme“ beschrieben (WEF 2012). Des Weiteren konstatierten das CRO Forum (2016) respektive IRM (2014) praxisnahe Definitionsansätze, in denen eine Vielzahl beispielhafter Ausprägungen eines Cyberrisikos genannt sind. Vor dem Hintergrund der Versicherbarkeit von Cyberrisiken thematisieren der Versicherer Willis Towers Watson (2013) und die Broker Guy Carpenter (2013) und Lloyd's (2015) in praxisnahen Veröffentlichungen das Cyberrisiko und beschreiben eigene Definitionen. Um 2015 wird der Terminus von der Finanzaufsicht und öffentlichen Organisationen des Finanzwesens betrachtet und in regulatorischen Richtli-

nien und Lexika (BIS 2016; EBA 2019; FSB 2018) sowie in Arbeitspapieren (Aldasoro et al. 2020) verankert. Für industrieübergreifende und weltweite Standards im (Cyber-)Risikomanagement können die Definitionen der international führenden Organisationen ISO/IEC (2018) und NIST (2017) Anwendung finden. Abschließend hervorzuheben ist der Beitrag des WEF (2016), welcher systemische Cyberrisiken vor dem Hintergrund eines möglichen Zusammenbruchs der kritischen Infrastrukturen diskutiert und eine entsprechende Begriffsdefinition darlegt.

Zusammenfassend kann festgehalten werden, dass keine einheitliche Definition des Begriffs Cyberrisiko – weder in den forschungsnahen noch in den praxisnahen Publikationen – existiert. Vielmehr hat sich ein Begriffswirrwarr ergeben, welches die unterschiedlichen Bedrohungen und Auswirkungen, die im Zusammenhang mit dem Internet, dem Einsatz von IT und dem Cyberraum stehen, aufgreift.

3 Ergebnisse

Im Rahmen der strukturierten Inhaltsanalyse werden 147 relevante Textpassagen aus den 26 Definitionsansätzen extrahiert und den fünf Haupt- und 15 Subkategorien zugeordnet sowie paraphrasiert, um relevante Kerneigenschaften abzuleiten. Tab. 1 zeigt die konsolidierten Ergebnisse der durchgeführten Inhaltsanalyse.

Mehr als jede fünfte der identifizierten Textpassagen handelt von Bedrohungen (22 %), jede dritte von betroffenen Risikoobjekten (31 %) oder von möglichen Auswirkungen von Cyberrisiken (39 %). Die Kategorie Schwachstellen wird elf Mal (7 %) identifiziert, wohingegen nur eine Textstelle der Kategorie Kontrollen zugeordnet ist. In den Äußerungen werden unterschiedliche Begriffe der Kategorie *Bedrohungen* genannt, unter anderem Cyberangriff, Cyberkriminalität, Cyberterror und Cyberkrieg (beabsichtigt) sowie Cyberbedrohung, (operationelles) Risiko, Naturkatastrophen und sonstige Ereignisse (nicht weiter spezifiziert). Lediglich eine Textpassage spricht von unbeabsichtigten Aktivitäten. Hinsichtlich der Kategorie *Vulnerabilität* werden symptomatische Schwachstellen (5 %) in den (IT-)Systemen, den internen Prozessen und der Systemintegrität adressiert. Zusätzlich trägt die mangelnde Agilität und der Faktor Mensch zu einer erhöhten Risikosituation bei. Es kann keine explizite Aussage zu systemischen Schwachstellen gefunden werden.[3] Nicht weiter spezifizierte Schwachstellen werden viermal (2 %) identifiziert. Die Kategorie *Kontrollen* wird in nur einer Definition im Sinne der „Mitigation" von Cyberrisiken genannt. Weitere, insbesondere technische und nichttechnische Kontrollen werden nicht erwähnt. Die von Cyberrisiken betroffenen *Risikoobjekte* finden sich in jeder dritten Textpassagen (46 Mal, 31 %). Hierbei ist die relative Aufteilung in materielle (15 %) und immaterielle Objekte (14 %) beinahe identisch. Nur vier Definitionen nennen nicht weiter spezifizierte Objekte (2 %). Unter den materiellen Objekten werden unter anderem Computer-, Informations- und Techno-

[3] Unter systemischen Schwachstellen sind mehrere Unternehmen (zum Beispiel aufgrund von Fehlern in einer Standardsoftware) betroffen, während von symptomatischen Schwachstellen nur ein einzelnes Unternehmen (zum Beispiel wegen der Nutzung einer unternehmensspezifischen Software) betroffen ist (vgl. Bandyopadhyay et al. 2009; Böhme et al. 2019).

Tab. 1 Ergebnisse der strukturierten Inhaltsanalyse

Kategorie	#	%[a]	Auszug der Paraphrasierung	Referenzen[b]
Bedrohungen	*33*	*22*		
Beabsichtigt	11	7	Cyberangriff, Cyberkriminalität, Cyberterror und Cyberkrieg	[7–10], [15], [18], [20]
Unbeabsichtigt	2	1	Unbeabsichtigte oder versehentliche Aktivität	[10], [15]
Nicht weiter spezifiziert	20	14	Cyberbedrohung, operationelles Risiko, Naturkatastrophen, sonstige unerwünschte/unerwartete Ereignisse	[2], [3], [5], [6], [8–12], [14–16], [20], [22–26]
Vulnerabilitäten	*11*	*7*		
Symptomatisch	7	5	Schwachstellen in den (IT-)Systemen, internen Prozessen und der Systemintegrität; mangelnde Agilität; Faktor Mensch	[1], [4], [8], [9], [15]
Systemisch	–	–	–	–
Nicht weiter spezifiziert	4	*2*	(Sonstige) Schwachstelle	[2], [14–16]
Kontrollen	*1*	*1*		
Technisch	–	–	–	–
Nicht technisch	–	–	–	–
Nicht weiter spezifiziert	1	1	Mitigation	[14]
Risikoobjekte	*46*	*31*		
Materiell	22	15	Informations- und Kommunikationstechnologie (IKT)-Systeme und -Ressourcen; Netzwerke und sonstige Technologiegüter; Mensch(en)	[1], [3–7], [9], [10], [15–17], [19], [20], [22], [24], [25]
Immateriell	20	14	Digitale Güter und Assets; Daten, Informationen und deren Verwendung, Transfer und Speicherung	[3], [5–7], [9], [10], [12–14], [16], [17], [19–22], [24]
Nicht weiter spezifiziert	4	2	Eigentum, Dienstleistung, individuelle Komponente(n)	[19], [22], [25], [26]
Auswirkungen	*56*	*39*		
Direkt	20	14	Finanzieller, ökonomischer Verlust; Disruption und (Geschäfts-)Unterbrechung; Haftungen; materieller Schaden	[1], [7–9], [15], [17–20], [23]
Indirekt	23	16	Verlust von Daten, Informationen, der Reputation, der Vertraulichkeit und der Integrität; Verletzung von Richtlinien und Sicherheitsverfahren	[1], [4], [6–10], [15], [17], [19], [20], [25], [26]
Nicht weiter spezifiziert	13	9	Konsequenzen, Zusammenbruch kritischer Infrastruktur	[2], [3], [9], [10], [16], [17], [20], [25], [26]
Summe	*147*	*100*		

[a]Rundungsdifferenzen in (Prozent-)Summen möglich
[b]Siehe Nummerierung der Definitionsansätze in Tabelle A des Online Materials

logiesysteme sowie allgemein elektronische Systeme und miteinander verbundene Netzwerke verstanden. Des Weiteren können nicht nur Güter sondern auch Menschen von Cyberrisiken betroffen sein. Unter immateriellen Objekten werden vor allem Daten respektive deren Verwendung, Transfer und Speicherung verstanden. Etwas allgemeiner wird in einigen Definitionen von Informationsgütern, digitalen und elektronischen Informationen gesprochen. Cyberrisiken bedrohen somit sowohl materielle Objekte wie Internet-, Kommunikations- und Technologiesysteme oder -ressourcen, als auch Menschen sowie jegliche Art von immateriellen Gütern, die durch Verwendung, Transfer oder Speicherung von Informationen entstehen. *Auswirkungen* von Cyberrisiken sind vielfältig und umfassen einerseits direkte Auswirkungen (14 %), wie zum Beispiel finanzielle und ökonomische Verluste, Disruption und Geschäftsunterbrechungen, materielle Schäden und Haftungen, andererseits indirekte Auswirkungen (16 %), unter anderem Daten- und Informationsverluste sowie Schäden der Reputation, der Vertraulichkeit und Integrität. Cyberrisiken gefährden einzelne und vernetzte Organisationen und können bei systemischen Risiken zum Zusammenbruch der kritischen Infrastruktur führen.

Abschließend lässt sich resümieren, dass Definitionen von Cyberrisiken eine Vielzahl unterschiedlicher Kerncharakteristika aufweisen. In den analysierten Textpassagen werden häufig materielle (15 %) und immaterielle (14 %) Risikoobjekte sowie direkte (14 %) und indirekte (16 %) Auswirkungen genannt. Im Hinblick auf die zugrundeliegende Bedrohung wird vor allem von beabsichtigten Aktivitäten (7 %) sowie allgemeinen Bedrohungen (14 %) und (operationellen) Risiken gesprochen, obgleich unbeabsichtigte Aktivitäten (1 %) nicht zu vernachlässigen sind. Denn der Faktor Mensch ist neben unzureichenden internen Prozessen, fehlender Systemintegrität und mangelnder Agilität eine der relevanten Schwachstellen (7 %), die die Materialisierung einer Cyberbedrohung ermöglichen.

4 Vom Begriffswirrwarr zu einem einheitlichen Begriffsverständnis

4.1 Ableitung einer umfassenden Definition und Taxonomie

Aufgrund der Ambivalenz bestehender Definitionsansätze bedarf es eines umfassenden, einheitlichen und allgemeingültigen Begriffsmodells, das zur Vereinheitlichung der Cyberterminologie beiträgt und als Basis für die zukünftige Cyberrisikoforschung dient. Dazu werden die identifizierten Kernmerkmale des Cyberrisikos (Tab. 1) weiter paraphrasiert, um einerseits alle Charakteristika zu berücksichtigen (Sicherstellung der Vollständigkeit) und andererseits eine allgemeingültige Definition abzuleiten (Sicherstellung der Akzeptanz). Ergänzt um die Erkenntnisse aus der Literaturrecherche zeigt Tab. 2 das abgeleitete Begriffsmodell (vgl. Cebula und Young 2010), welches in den folgenden Definitionsvorschlag des Terminus Cyberrisiko mündet:

Tab. 2 Abgeleitetes Begriffsmodell des Terminus Cyberrisiko in Anlehnung an Cebula und Young (2010)

1. Bedrohungen	2. Schwachstellen	3. Risikoobjekte	4. Auswirkungen
1.1 Beabsichtigt	*2.1 Hardware*	*3.1 Materiell*	*4.1 Direkt*
1.1.1 Betrug	2.1.1 Kapazität	3.1.1 Hardware	4.1.1 Schäden
1.1.2 Sabotage	2.1.2 Leistung	3.1.2 Software	4.1.2 Betrieb
1.1.3 Diebstahl	2.1.3 Instandhaltung		4.1.3 Finanzen
1.1.4 Vandalismus			
1.2 Unbeabsichtigt	*2.2 Software*	*3.2 Immateriell*	*4.2 Indirekt*
1.2.1 Fehler	2.2.1 Design	3.2.1 Informationen	4.2.1 Sicherheit
1.2.2 Irrtum	2.2.2 Integrität	3.2.2 Dienstleistungen	4.2.2 Reputation
1.2.3 Versäumnis	2.2.3 Komplexität		4.2.3 Rechtsbelange
	2.3 Organisation	*3.2 Menschen*	*4.3 Dritte*
	2.3.1 Prozesse	3.2.1 Physisch	4.3.1 Direkt
	2.3.2 Kenntnisse	3.2.2. Psychisch	4.2.2 Indirekt
	2.3.3 Menschen		

Cyberrisiken umfassen Bedrohungen aus dem Cyberraum[4], welche aufgrund einer Schwachstelle sowohl materielle als auch immaterielle Werte als auch Menschen gefährden, was zu direkten und indirekten Schäden einer betroffenen Einheit und von Dritten führen kann.

Cyberrisiken können sich aus *beabsichtigten* oder *unbeabsichtigten* Bedrohungen ergeben. Damit sind neben betrügerischen Aktivitäten (z. B. Cyberangriff, Cyberkriminalität, Cyberterror und Cyberkrieg), Sabotage, Diebstahl und Vandalismus auch unbeabsichtigte Bedrohungen wie Fehler, Irrtümer oder Versäumnisse inkludiert. Ferner entstehen Cyberrisiken durch Aktivitäten im Cyberraum (Refsdal et al. 2015). Unter diesem Oberbegriff lassen sich spezifische Tätigkeiten wie zum Beispiel die Verarbeitung von digitalen Informationen (Hiller und Russell 2013), unter anderem in der Cloud oder dem Metaverse, sowie internetbezogene Risiken (Gordon et al. 2003) subsumieren. Da der Begriff des Cyberraums bereits durch das BSI (2021) als zuständige Cybersicherheitsbehörde des Bundes definiert ist, kann die Verwendung dieses Glossarbegriffes zur Akzeptanz der neu postulierten Definition beitragen. Obwohl manche Definitionsansätze nicht nur digitale sondern auch physische Bedrohungen (z. B. Schaden an einem Netzwerkkabel, Brand eines Serverraums) als Cyberrisiko kategorisieren (Aldasoro et al. 2020; Böhme et al. 2019; Strupczewski 2021), werden solche Risiken in diesem Beitrag als operationelle Risiken beziehungsweise IT-Risiken verstanden (Seibold 2006; Wrede et al. 2018), um eine eineindeutige Abgrenzung verwandter Begrifflichkeiten herzustellen (vgl. Abschn. 4.2).

Des Weiteren nutzen Cyberrisiken Vulnerabilitäten in der *Hardware* oder *Software*, beispielsweise von Informations- und Kommunikationstechnologiesystemen

[4] „Der Cyberraum ist der virtuelle Raum aller weltweit auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme. Dem Cyberraum liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, welches durch beliebige andere Datennetze erweitert werden kann.“ (BSI 2021).

(IKT-Systeme), oder in der *Organisation*, durch mangelhafte Prozesse, Kenntnisse oder den Faktor Mensch als Einfallstor. Die von Cyberrisiken betroffenen Risikoobjekte umfassen *materielle* und *immaterielle* Güter wie zum Beispiel IKT-Systeme und Netzwerke (Hardware und Software) sowie (digitale) Informationsgüter, Daten sowie deren Verwendung, Transfer und Speicherung (Informationen und Dienstleistungen). Besonders hervorzuheben ist der *Mensch* als potenzielles Risikoobjekt. Weiter beinhaltet das Begriffsmodell *direkte* Auswirkungen wie materielle Schäden, betriebliche Effekte (z. B. Geschäftsunterbrechungen) und finanzielle Verluste. Zu den *indirekten* Auswirkungen gehören der Verlust der Vertraulichkeit, Verfügbarkeit und Integrität von Informationen und Dienstleistungen (*Sicherheit*; Königs 2017) sowie Reputations- und rechtliche Auswirkungen. Ferner sind direkte und indirekte Auswirkungen bei *Dritten*, bis hin zum Zusammenbruch der kritischen Infrastruktur, nicht auszuschließen.

Hinsichtlich der Vollständigkeit hat bereits Strupczewski (2021) gezeigt, dass nur die Definition von Eling et al. (2016) umfassend formuliert ist. Zusätzlich gibt es keine weitere forschungsnahe oder praxisnahe Definition aus der analysierten Grundgesamtheit, welche umfassender als der Vorschlag von Eling et al. (2016) verfasst ist.[5] Bezüglich der Vollständigkeit decken sowohl Eling et al. (2016) als auch die in diesem Beitrag postulierte Definition die vier Kategorien Bedrohungen, Vulnerabilitäten, Risikoobjekte und Auswirkungen ab. Bezüglich der Allgemeingültigkeit zeigt die Definition von Eling et al. (2016) jedoch Schwächen auf. Insbesondere die Nennung (finanz-)mathematischer Eigenschaften ist zwar für Aktuare und Assekuranzen relevant, spielt jedoch für andere Bereiche und die disziplinübergreifende Cyberforschung eine untergeordnete Rolle. Des Weiteren wirken bundesweite und internationale Programme zur Förderung und zum Aufbau von Cyberdatenbanken beispielsweise durch MELANI in der Schweiz oder das BSI in Deutschland der in der Definition genannten „Unsicherheiten in den Daten und der Modellierung" langfristig entgegen (Eling 2020). Trotz des ausführlichen und wertvollen Definitionsvorschlags von Eling et al. (2016) ist diese Definition nicht allgemeingültig und somit als fachspezifisch einzustufen.

Im Vergleich dazu bietet der neue Definitionsvorschlag eine umfassende und allgemeingültige Alternative zu den bisherigen, disziplinspezifischen Definitionsansätzen. Die Ableitung des Begriffsmodells ergänzt die abstrakt formulierte Definition und deckt alle fachlichen Aspekte ab. Zudem kann die Taxonomie durch fachspezifische Bedürfnisse erweitert werden, beispielsweise um ein passendes Cyberrisikomodul für das unternehmensinterne Informationssicherheitssystem (ISMS) zu entwickeln.

[5] Die Definition der EBA (2019) spricht von Informations- und Kommunikationstechnologierisiken (IKT-Risiken) sowie Sicherheitsrisiken, was zwar Cyberrisiken inkludiert aber auch andere Nicht-Cyberrisiken umfasst. Im Hinblick auf eine klare Abgrenzung zu anderen Risiken, wie zum Beispiel IT-Risiken und Informationssicherheitsrisiken (Seibold 2006; Königs 2017; Wrede et al. 2018) stellt dieser Definitionsansatz keinen passenden Standard für die Cyberterminologie dar.

4.2 Abgrenzung zu verwandten Begrifflichkeiten

Aufgrund der Vielzahl an unterschiedlichen Definitionsansätzen des Cyberrisikobegriffes gibt es keine eindeutige Abgrenzung zu verwandten Begrifflichkeiten, wie zum Beispiel Informationstechnologierisiko (IT-Risiko) und Informationssicherheitsrisiko (IS-Risiko). In Forschung und Praxis haben sich in Bezug auf die beiden letztgenannten Begriffe eine vage Abgrenzung herausgebildet: Während das IT-Risiko eher technische Risiken umfasst, ausgehend von der Informationstechnologie hin zu denjenigen, die sie anwenden, besteht das IS-Risiko aus eher inhaltlich orientierten Risiken, ausgehend von den (Geschäfts-)Prozessen und den mit ihnen befassten Rollen hin zu notwendigen technischen Voraussetzungen (Knoll und Strahringer 2017). Bei genauerer Betrachtung ergeben sich Überschneidungen zwischen dem IT- und IS-Risiko (Königs 2017). Zusätzlich führt das Begriffswirrwarr des Terminus Cyberrisiko dazu, dass ein theoretisches Konstrukt zur eindeutigen Abgrenzung der Begrifflichkeiten erforderlich ist (Eling 2018).

Vor diesem Hintergrund stellt Tab. 3 eine strukturierte Abgrenzung von Cyber-, IT- und IS-Risiko anhand der Kategorien *Bedrohungen* und *Risikoobjekte* dar. Analog des Begriffsmodells (Tab. 2) wird zwischen materiellen, immateriellen Risikoobjekten und dem Menschen unterschieden. Die Kategorie Bedrohungen wird anhand von Aktivitäten aus dem Cyberraum respektive Nicht-Cyberraum gemäß der postulierten Definition separiert.

Cyberrisiken sind Bedrohungen aus dem Cyberraum und gefährden sowohl materielle als auch immaterielle Werte als auch Menschen. IT-Risiken hingegen sind eher technischer, also materieller Natur – eine Unterscheidung in Cyber- und Nicht-Cyberraum ist für das IT-Risiko nicht erforderlich. Analog sind IS-Risiken eher immaterieller Natur. Überschneidungen ergeben sich insbesondere bei der Separierung in materielle (vorwiegend IT) und immaterielle (vorwiegend IS) Werte.

Zur Illustration der Abgrenzung können verschiedene Szenarien eines (Hacker-) Angriffes auf ein Rechenzentrum beispielhaft herangezogen werden. Unter der Annahme, dass es Hackern gelingt, das Rechenzentrum über den Cyberraum zu infiltrieren und lahmzulegen, handelt es sich um ein Cyber- beziehungsweise IT-Risiko. Werden anstatt des Servers geheime Unternehmens- und Patientendaten angegriffen, ergibt sich ein Cyber- beziehungsweise IS-Risiko. Stehen anstatt Server und Daten Menschen im Vordergrund, beispielsweise durch Cybermobbing von Mitarbeitern, spricht man von einem Cyberrisiko. Analog handelt es sich um kein Cyberrisiko,

Tab. 3 Abgrenzung der Begrifflichkeiten Cyberrisiko, Informationstechnologierisiko (IT-Risiko) und Informationssicherheitsrisiko (IS-Risiko)

Bedrohungen							
		Cyberraum			*Nicht-Cyberraum*		
		Cyberrisiko	IT-Risiko	IS-Risiko	Cyberrisiko	IT-Risiko	IS-Risiko
Risikoobjekte	Materiell	X	X	(X)	–	X	(X)
	Immateriell	X	(X)	X	–	(X)	X
	Menschen	X	–	–	–	–	–

X Trifft zu, *(X)* Trifft in Teilen zu, – Trifft nicht zu

wenn das Rechenzentrum aufgrund eines Kabelbrandes ausfällt (IT-Risiko) oder Unternehmensdaten verloren gehen (IS-Risiko).

Diese Abgrenzung zeigt sowohl die Gemeinsamkeiten als auch die Unterschiede der drei Begrifflichkeiten auf. Die Anwendung des Cyberraumes ermöglicht eine strukturierte Abgrenzung des Begriffes Cyberrisiko von verwandten Fachbegriffen wie IT- und IS-Risiko.

5 Zusammenfassung, Diskussion und Schlussbemerkung

Dieser Beitrag untersucht anhand einer strukturierten Inhaltsanalyse wissenschaftliche und praxisnahe Definitionsansätze des Terminus Cyberrisiko und leitet eine umfassende Definition und Taxonomie ab. Durch Paraphrasieren der analysierten Begriffsdefinitionen werden qualitative Kernmerkmale des Cyberrisikos herausgearbeitet und ein Cyberrisikobegriffsmodell postuliert, das sowohl die disziplinübergreifende Klammer um die bisherigen Definitionsansätze bildet als auch zur Standardisierung und Vereinfachung der künftigen Cyberforschung beitragen kann. Ebenso profitieren Unternehmen und die Wirtschaft von einer einheitlichen Cyberrisikoterminologie, beispielsweise bei der Implementierung von „Cybermodulen“ im Rahmen des ISMS.

In Anbetracht der qualitativ ausgerichteten Vorgehensweise weist die vorliegende Untersuchung Limitationen auf. Trotz der umfassenden Literaturrecherche kann eine Vollständigkeit des Auswahlmaterials abschließend nicht garantiert werden, weshalb die Verallgemeinerbarkeit der gewonnenen Erkenntnisse eingeschränkt sein kann. Des Weiteren basiert die dargelegte Analyse auf einer Aufnahme der Vergangenheit, welche aufgrund der dynamischen Eigenschaften des Cyberrisikos nicht zwingend auf die Zukunft projiziert werden kann. Obgleich die Kategorisierung der identifizierten Textstellen deduktiven Kriterien folgt, beruht die Einstufung der Textphrasen auf der subjektiven Wahrnehmung der Autoren, was zu Verzerrungen der Erkenntnisse führen kann.

Ungeachtet dieser Einschränkungen unterstreichen die Ergebnisse dieser Studie, dass einerseits Cyberrisiken hochkomplex und dynamisch sind (Eling 2020), andererseits die bisherige Cyberrisikoforschung von disziplinübergreifenden Barrieren geprägt ist (Falco et al. 2019). Dadurch haben sich über die letzten zwei Jahrzehnte eine Vielzahl an forschungsnahen und praxisnahen Definitionsansätzen etabliert. Insbesondere im öffentlichen Diskurs wurde das Cyberrisiko mehrfach neu oder umdefiniert, um gerade die Aspekte widerzuspiegeln, die ein Autor als wichtig erachtet (Ale et al. 2015; Strupczewski 2021). Daraus ergibt sich die Notwendigkeit einer einheitlichen Taxonomie, welche die unterschiedlichen Sichtweisen aus Wissenschaft, Industrie, Regulatorik und Politik vereinheitlicht und verständlicher darstellt. Erste terminologische Standards haben sich zwar in ausgewählten Interessensvertretungen (CRO Forum 2016; IRM 2014), Organisationen (WEF 2012), Aufsichtsbehörden (BIS 2016; EBA 2019; FSB 2018) und nationalen Institutionen (BSI 2021; NIST 2017) gebildet. Diese Entwicklung kann nur als erster Schritt in Richtung einer einheitlichen Cyberterminologie betrachtet werden. Insbesondere zur Prävention systemischer Cyberrisiken, die sowohl industrie- als auch grenz-

überschreitend eintreten können, ist ein global einheitliches Begriffsverständnis von Nöten. Hierzu bedarf es jedoch mehr als nur eines umfassenden Begriffsmodells wie in diesem Beitrag vorgeschlagen, obgleich dies eine notwendige Grunderfordernis darstellt.

In der Praxis kann das vorgeschlagene Modell als Grundlage für ein einheitliches Begriffsverständnis genutzt werden, beispielsweise im Rahmen der Einführung eines unternehmensweiten Glossars. Hierbei sollten nicht nur relevante Begrifflichkeiten wie Cyberrisiko oder IT-Risiko definiert, sondern auch voneinander abgegrenzt werden. Zur stetigen Verbesserung des gemeinsamen Verständnisses können einerseits interne Cyberreports an das Management und andererseits die externe Entwicklung von taxonomischen Industriestandards diese Entwicklung vorantreiben.

Trotz der wachsenden Anzahl an wissenschaftlicher und praxisnaher Literatur (Eling 2020) ist die Theorie und Terminologie von Cyberrisiken ein eher unerforschter Teilbereich. Daher sollte sich die weitere Forschung auf eine tiefere Integration verschiedener Sichtweisen zur Definition von Cyberrisiken konzentrieren (Strupczewski 2021). Ein weiterer relevanter Forschungsschwerpunkt hinsichtlich einer einheitlichen Terminologie könnte die Zusammenfassung und Integration sowie Abgrenzung der unterschiedlichen Cyberbegrifflichkeiten wie zum Beispiel Cyberrisiko, Cyberangriff, Cybervorfall, Cyberterror und Cyberkrieg sein. Die sich daraus ergebende Ableitung eines einheitlichen Cyberframeworks in Zusammenarbeit mit unterschiedlichen Interessensvertretungen, Industrien, Ländern und (inter-)nationalen Organisationen stellt eine weitere, wenn auch herausfordernde Forschungstätigkeit dar. Durch die charakterisierte Komplexität und Dynamik des Cyberrisikos entwickelt sich ein relevantes Forschungsfeld, welches in Zeiten von Internet der Dinge, Kryptowährungen und künstlicher Intelligenz weiter an Bedeutung gewinnen wird.

Zusatzmaterial online Zusätzliche Informationen sind in der Online-Version dieses Artikels (https://doi.org/10.1365/s40702-022-00888-3) enthalten.

Funding Open Access funding enabled and organized by Projekt DEAL.

Literatur

Aldasoro I, Gambacorta L, Giudici P, Leach T (2020) The drivers of cyber risk. https://www.bis.org/publ/work865.pdf. Zugegriffen: 20. Mai 2021 (Bank for International Settlements)

Ale B, Burnap P, Slater D (2015) On the origin of PCDS—(probability consequence diagrams). Saf Sci 72:229–239. https://doi.org/10.1016/j.ssci.2014.09.003

Bandyopadhyay T, Mookerjee VS, Rao RC (2009) Why IT managers don't go for cyber-insurance products. Commun ACM 52:68–73. https://doi.org/10.1145/1592761.1592780

Bendovschi A (2015) Cyber-attacks—trends, patterns and security countermeasures. Procedia Econ Financ 28:24–31. https://doi.org/10.1016/S2212-5671(15)01077-1

Biener C, Eling M, Wirfs J (2015) Insurability of cyber risk: an empirical analysis. Geneva Pap Risk Insur Issues Pract 40:131–158. https://doi.org/10.1057/gpp.2014.19

BIS – Bank for International Settlements (2016) Guidance on cyber resilience for financial market infrastructures. https://www.bis.org/cpmi/publ/d146.pdf. Zugegriffen: 6. Apr. 2021

Bitkom – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (2019) Wirtschaftsschutz in der digitalen Wirtschaft. https://www.bitkom.org/sites/default/files/2019-11/bitkom_wirtschaftsschutz_2019_0.pdf. Zugegriffen: 20. Apr. 2021

BKA – Bundeskriminalamt (2021) Cybercrime; Bundeslagebild 2020. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2020.html?nn=28110. Zugegriffen: 11. Mai 2021

Böhme R, Kataria G (2006) Models and measures for correlation in cyber-insurance. https://core.ac.uk/download/pdf/162458449.pdf. Zugegriffen: 11. Febr. 2021 (Workshop on the Economics of Information Security)

Böhme R, Laube S, Riek M (2019) A fundamental approach to cyber risk analysis. Casualty Actuar Soc 12:161–185

BSI – Bundesamt für Sicherheit in der Informationstechnik (2021) Glossar der Cyber-Sicherheit. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html;jsessionid=326A2F2D3A41CC886D6B4B2B4F7D21A4.internet082?nn=522504&cms_lv2=132798. Zugegriffen: 7. Apr. 2021

Carpenter G (2013) Tomorrow never knows; emerging risks report. https://www.curie.org/sites/default/files/Emerging-Risks-Report-Sept-2013.pdf. Zugegriffen: 7. Apr. 2021

Cavusoglu H, Mishra B, Raghunathan S (2004) The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers. Int J Electron Commer 9:69–104. https://doi.org/10.1080/10864415.2004.11044320

Cebula JJ, Young LR (2010) A taxonomy of operational cyber security risks. https://apps.dtic.mil/sti/pdfs/ADA537111.pdf. Zugegriffen: 10. Febr. 2021 (Software Engineering Institute)

Choudhry U (2014) Der Cyber-Versicherungsmarkt in Deutschland; Eine Einführung. Springer Gabler, Wiesbaden

CRO Forum (2016) Concept paper on a proposed categorisation methodology for cyber risk. https://www.thecroforum.org/2016/06/20/concept-proposal-categorisation-methodology-for-cyber-risk/. Zugegriffen: 6. Apr. 2021

EBA – European Banking Authority (2019) Final report: EBA guidelines on ICT and security risk management. https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management. Zugegriffen: 7. Apr. 2021

Eling M (2018) Cyber risk and cyber risk insurance: status quo and future research. Geneva Pap Risk Insur Issues Pract 43:175–179. https://doi.org/10.1057/s41288-018-0083-6

Eling M (2020) Cyber risk research in business and actuarial science. Eur Actuar J 10:303–333. https://doi.org/10.1007/s13385-020-00250-1

Eling M, Loperfido N (2017) Data breaches: goodness of fit, pricing, and risk measurement. Insur Math Econ 75:126–136. https://doi.org/10.1016/j.insmatheco.2017.05.008

Eling M, Schnell W (2016) What do we know about cyber risk and cyber risk insurance? JRF 17:474–491. https://doi.org/10.1108/JRF-09-2016-0122

Eling M, Wirfs JH (2016) Modelling and management of cyber risk. http://www.actuaries.org/oslo2015/papers/iaals-wirfs&eling.pdf. Zugegriffen: 5. Apr. 2021

Eling M, Schnell W, Sommerrock F (2016) Ten key questions on cyber risk and cyber risk insurance. https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber-risk-10_key_questions.pdf. Zugegriffen: 6. Apr. 2021

Falco G, Eling M, Jablanski D, Weber M, Miller V, Gordon LA, Wang SS, Schmit J, Thomas R, Elvedi M, Maillart T, Donavan E, Dejung S, Durand E, Nutter F, Scheffer U, Arazi G, Ohana G, Lin H (2019) Cyber risk research impeded by disciplinary barriers. Science 366:1066–1069. https://doi.org/10.1126/science.aaz4795

Früh W (2017) Inhaltsanalyse; Theorie und Praxis. UVK, Konstanz, München

FSB – Financial Stability Board (2018) Cyber lexicon. https://www.fsb.org/wp-content/uploads/P121118-1.pdf. Zugegriffen: 6. Apr. 2021

GAO – United States General Accounting Office (1996) Content analysis: a methodology for structuring and analyzing written material. https://www.gao.gov/assets/pemd-10.3.1.pdf. Zugegriffen: 18. Mai 2021 (GAO/PEMD-10.3.1)

Gordon LA, Loeb MP, Sohail T (2003) A framework for using insurance for cyber-risk management. Commun ACM 46:81–85. https://doi.org/10.1145/636772.636774

Haas A, Hofmann A (2014) Risiken aus der Nutzung von Cloud-Computing-Diensten: Fragen des Risikomanagements und Aspekte der Versicherbarkeit. Z Ges Versicherungswiss 103:377–407. https://doi.org/10.1007/s12297-014-0285-3

Hiller JS, Russell RS (2013) The challenge and imperative of private sector cybersecurity: an international comparison. Comput Law Secur Rev 29:236–245. https://doi.org/10.1016/j.clsr.2013.03.003

IRM – The Institute of Risk Management (2014) Cyber risk—resources for practitioners. https://www.theirm.org/media/7237/irm-cyber-risk-resources-for-practitioners.pdf. Zugegriffen: 6. Apr. 2021

ISO/IEC – International Standard Organisation (2018) ISO/IEC 27000:2018; information technology—security techniques—information security management systems—overview and vocabulary. https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en. Zugegriffen: 20. Apr. 2021

Kamiya S, Kang J-K, Kim J, Milidonis A, Stulz RM (2021) Risk management, firm reputation, and the impact of successful cyberattacks on target firms. J financ econ 139:719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

Knoll M, Strahringer S (2017) IT-GRC-Management im Zeitalter der Digitalisierung. In: Knoll M, Strahringer S (Hrsg) IT-GRC-Management—Governance, Risk und Compliance: Grundlagen und Anwendungen. Springer, Wiesbaden, S 1–24 https://doi.org/10.1007/978-3-658-20059-6_1

Königs H-P (2017) IT-Risikomanagement mit System; Praxisorientiertes Management von Informationssicherheits-, IT- und Cyber-Risiken. Springer Vieweg, Wiesbaden

Lloyd's (2015) A quick guide to cyber risk. https://www.lloyds.com/news-and-insights/news/a-quick-guide-to-cyber-risk. Zugegriffen: 7. Apr. 2021

Mayring P (2015) Qualitative Inhaltsanalyse; Grundlagen und Techniken. Beltz, Weinheim

McAfee (2020) The hidden costs of cybercrime. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf. Zugegriffen: 20. Apr. 2021 (Report)

Mukhopadhyay A, Chatterjee S, Saha D, Mahanti A, Sadhukhan SK (2013) Cyber-risk decision models: To insure IT or not? Decis Support Syst 56:11–26. https://doi.org/10.1016/j.dss.2013.04.004

Nieuwesteeg B, Visscher L, de Waard B (2018) The law and economics of cyber insurance contracts: a case study. Eur Rev Priv Law 26:371–420

NIST – National Institute of Standards and Technology (2017) Cybersecurity framework manufacturing profile. NISTIR, Bd. 8183. U.S. Department of Commerce, Washington, D.C. https://doi.org/10.6028/NIST.IR.8183

Njegomir V, Marović B (2012) Contemporary trends in the global insurance industry. Procedia—social Behav Sci 44:134–142. https://doi.org/10.1016/j.sbspro.2012.05.013

Öğüt H, Raghunathan S, Menon N (2011) Cyber security risk management: public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. Risk Analysis 31:497–512. https://doi.org/10.1111/j.1539-6924.2010.01478.x

Rakes TR, Deane JK, Paul Rees L (2012) IT security planning under uncertainty for high-impact events. Omega 40:79–88. https://doi.org/10.1016/j.omega.2011.03.008

Randolph J (2009) A guide to writing the dissertation literature review. Pract Assess Res Eval. https://doi.org/10.7275/B0AZ-8T74

Refsdal A, Stølen K, Solhaug B (2015) Cyber-risk management. Springer, Heidelberg

Romanosky S (2016) Examining the costs and causes of cyber incidents. J Cyber Secur 2:121–135. https://doi.org/10.1093/cybsec/tyw001

Seibold H (2006) IT-Risikomanagement. De Gruyter, Oldenbourg

Strupczewski G (2021) Defining cyber risk. Saf Sci 135:105143. https://doi.org/10.1016/j.ssci.2020.105143

WEF – World Economic Forum (2012) Partnering for cyber resilience; risk and responsibility in a hyperconnected world—principles and guidelines. http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf. Zugegriffen: 7. Apr. 2021

WEF – World Economic Forum (2016) Understanding systemic cyber risk; global agenda council on risk & resilience. http://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf. Zugegriffen: 7. Apr. 2021

WEF – World Economic Forum (2021) The global risks report 2021; 16th edition. Insight report. http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf. Zugegriffen: 10. Mai 2021

Willis Towers Watson (2013) Willis report: Majority of Public Companies Indicate Cyber Attack Would Cause "Serious Harm" or "Adversely Impact" Their Firms. Willis Towers Watson, London

Wrede D, Freers T, Graf von der Schulenburg J-M (2018) Herausforderungen und Implikationen für das Cyber-Risikomanagement sowie die Versicherung von Cyberrisiken – Eine empirische Analyse. Z Ges Versicherungswiss 107:405–434. https://doi.org/10.1007/s12297-018-0425-2