



Munich Business School
University of Applied Sciences

MBS Research

**Lohnt sich die Digitalisierung für jedes Unternehmen –
im Hinblick auf hohe Investitionskosten und die Gefahr
durch Cyberkriminalität?
Eine analytische Betrachtung.**

Munich Business School Working Paper

2020-01

Florian Bartholomae, Prof. Dr.

Email: Florian.Bartholomae@munich-business-school.de

Abstract

Many firms have to decide whether and how much of their business activities they want to digitize. Several studies point to considerable differences, especially between small- and large-sized firms. This paper develops a simple model that shows under which conditions digitization can be profitable for a firm. At first, different competitive situations are taken into account and subsequently, the effects of security problems on digitization decisions are examined using the example of the dangers of a cyberattack. The results show that digitization is a dominant strategy, which results in a prisoner's dilemma. Given these challenges, a rather cooperative competitive structure is recommended.

Keywords: Information goods, network effects, cybercrime, digitization decision, dominant strategy, Germany, small and medium-sized business (SME)

Zusammenfassung

Viele Firmen müssen sich entscheiden, ob und wie viel ihrer Geschäftsaktivitäten sie digitalisieren wollen. Mehrere Studien weisen auf erhebliche Unterschiede hin, insbesondere zwischen kleinen und großen Unternehmen. In diesem Beitrag wird ein einfaches Modell entwickelt, das zeigt, unter welchen Bedingungen die Digitalisierung für ein Unternehmen rentabel sein kann. Dabei werden zunächst unterschiedliche Wettbewerbssituationen berücksichtigt und anschließend die Auswirkungen von Sicherheitsproblemen auf Digitalisierungsentscheidungen am Beispiel der Gefahren eines Cyberattacks untersucht. Die Ergebnisse zeigen, dass die Digitalisierung eine dominante Strategie ist, die zu einem Gefangenendilemma führt. Angesichts dieser Herausforderungen empfiehlt sich eine eher kooperative Wettbewerbsstruktur.

Schlüsselwörter: Informationsgüter, Netzwerkeffekte, Cyberkriminalität, Digitalisierungsentscheidung, Dominante Strategie, Deutschland, kleine und mittlere Unternehmen (KMU)

1. Einleitung

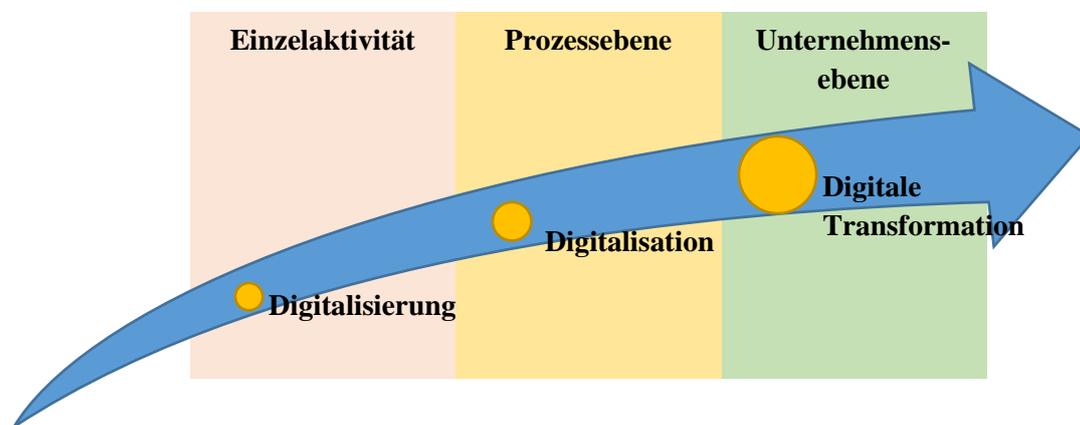
„E-Commerce“, „Industrie 4.0“ oder „Sharing Economy“ sind Begriffe, die für Fortschritt, Innovation und neue Impulse in der Wirtschaft stehen. Als Treiber und Ursache dieser Entwicklungen gilt die „Digitalisierung“, die als Paradigmenwechsel in der Wirtschaft gesehen wird und zu teilweise erheblichen Umwälzungen in Produktion und Organisation führt bzw. führen soll. Die resultierenden Auswirkungen auf Wirtschaft und Gesellschaft sind immer wieder Teil politischer und gesellschaftlicher Diskussionen. Ein Blick auf den Stand der Digitalisierung in der deutschen Wirtschaft zeigt allerdings, dass Digitalisierung noch nicht den Stellenwert einnimmt, wie es die öffentliche Wahrnehmung vermuten lässt und auch international teilweise erheblich zurückbleibt. Eine Umfrage des Bundesverbands Informations-

wirtschaft, Telekommunikation und neue Medien (Bitkom) kommt zu dem Ergebnis, dass sich die deutsche Wirtschaft im Vergleich zu anderen Ländern 2018 bei der Digitalisierung eher im Mittelfeld oder schlechter (71%) einordnet, womit sich ihre Einschätzung gegenüber dem Vorjahr (57%) deutlich verschlechtert hat (Berg 2018, 10). In einer Befragung des deutschen Industrie- und Handelskammertags (DIHK) gaben branchenübergreifend durchschnittlich knapp 40% der Unternehmen an, digital nur wenig entwickelt zu sein – einzig in der Informations- und Kommunikationsbranche sieht dies mit deutlich unter 10% signifikant anders aus (DIHK 2017, 19). Über Branchengrenzen hinweg zeigt sich zudem, dass die Größe des Unternehmens dabei eine erhebliche Rolle zu spielen scheint: Je mehr Mitarbeiter ein Unternehmen beschäftigt, desto eher bezeichnen sie sich als Vorreiter beim Thema Digitalisierung, während sich kleinere Unternehmer demgegenüber zum Großteil als Nachzügler betrachten (Berg 2018, 6; DIHK 2017, 20). Da hierunter insbesondere auch Handwerksbetriebe fallen (vgl. auch Rohleder & Schulte 2017, 10), überrascht es nicht, dass nach einer Studie des Zentralverbands des deutschen Handwerks (ZDH) die Digitalisierung für die Mehrheit der Handwerksbetriebe nicht sonderlich wichtig ist. So setzten 2017 nur 26% der Betriebe Digitalisierungsmaßnahmen um, vor allem für die Optimierung von Geschäftsprozessen (47%), die Erschließung neuer Kundenkreise (43%) und im Bereich Datenschutz und Cybersicherheit (37%) (ZDH 2018, 4). Wiederum planten auch nur 26% eine Umsetzung von Digitalisierungsmaßnahmen für 2018 (ZDH 2018, 6). Allerdings zeigen sich die Handwerksbetriebe damit der Digitalisierung gegenüber deutlich aufgeschlossener als in den Vorjahren. Zusammen mit Bitkom befragte der ZDH Handwerksbetriebe nach den größten Hemmnissen bei der Digitalisierung. Als meistgenannten Gründe wurden die Sorge um IT-Sicherheit und Datenschutz (77%) und hohe Investitionskosten (73%) angegeben (Rohleder & Schulte 2017, 11).

Dieses Paper möchte der Frage nachgehen, von welchen Faktoren grundsätzlich die Digitalisierungsentscheidung in einem Unternehmen abhängt, wobei insbesondere auch auf die beiden letztgenannten Gründe eingegangen wird. Es zeigt sich schließlich, dass Digitalisierung nicht für jedes Unternehmen bzw. jede Unternehmensgröße in Frage kommt und zudem Sicherheitsaspekte ökonomisch effiziente Entscheidungen konterkarieren. Diese einzelnen Aspekte und Zusammenhänge spiegeln sich auch im Aufbau des Papers wider: Zunächst wird herausgestellt, was unter Digitalisierung zu verstehen ist und welche Besonderheiten dadurch entstehende digitale Güter aufweisen. In Abschnitt 3 wird analysiert, wie diese Güter einerseits und die Digitalisierung andererseits den Wettbewerb beeinflusst. Basierend auf den vorgestellten stilisierten Fakten wird in Abschnitt 4 ein einfaches Modell entwickelt, das die Rolle verschiedener Faktoren für Digitalisierungsentscheidung analysiert. Abschnitt 5 erweitert die Überlegung und weist insbesondere auf Gefahren der Digitalisierung hin. Im letzten Abschnitt werden schließlich die Ergebnisse zusammengefasst und Handlungsempfehlungen abgeleitet.

2. Digitalisierung und Informationsgüter

Definitionsgemäß bezeichnet Digitalisierung die Umwandlung von (physischen) Informationen in (elektronische) Bit-Folgen. Bei diesem Transformationsprozess werden analoge Informationen mit stetigen Ausprägungen in diskrete binäre Bits codiert.¹ Die Digitalisierung einzelner Informationen ermöglicht dann eine Digitalisation der Geschäftsprozesse. Hierunter wird die Optimierung der Nutzung der digitalisierten Informationen verstanden, da Prozesse implementiert und verbessert werden können, die etwa eine effizientere Auswertung und Verbindung von Datensätzen erlauben. So kann etwa der Datensatz, der die aktuelle Bestellung eines Kunden enthält, sowohl der Adresse des Kunden als auch den früheren Bestellungen des Kunden zugeordnet werden. Eine Verknüpfung dieses kombinierten Datensatz mit Daten anderer Kunden aus der gleichen Region, kann dann etwa dazu genutzt werden, regionale Bedarfe zu bestimmen, möglicherweise sogar zu prognostizieren und entsprechende Kapazitäten vorzuhalten. Eine konsequente Adaptierung aller Geschäftsprozess kann schließlich zur digitalen Transformation der Unternehmung führen. Dabei entstehen neue Geschäftsideen und -modelle, die auf den Vorteilen der Digitalisation basieren – beispielsweise führte die Digitalisierung von Musik letztlich zur Entstehung von Streaming-Diensten wie Napster oder Spotify. 48% der deutschen Unternehmen geben daher auch an, dass sie als Folge der Digitalisierung neue Produkte und Dienstleistungen anbieten (Berg 2018, 4). Abbildung 1 verdeutlicht den Zusammenhang zwischen diesen drei Prozessen. Zu beachten ist, dass in der öffentlichen Diskussion oftmals alle Prozesse unter Digitalisierung subsumiert werden, was im eigentlichen Bedeutungssinn aber falsch ist.



Quelle: Eigene Darstellung.

Abb. 1: Digitalisierung, Digitalisation und digitale Transformation

Diese Änderungen auf Unternehmensebene führen auch zu gesamtökonomischen Veränderungen. So sind die Basisinnovationen, welche die aktuelle ökonomische Entwicklung bestimmen, im Zuge der

¹ Die beiden Ausprägungen sind 0 bzw. „falsch“ und 1 bzw. „wahr“. Eine Folge von acht Bit bildet ein Byte, wodurch sich $2^8 = 256$ Kombinationsmöglichkeiten ergeben, die zum Beispiel Buchstaben codiert werden können. Der Buchstabe „B“ wird etwa durch die Folge „01000010“ dargestellt und das Wort „Bit“, das aus drei Buchstaben bzw. Bytes besteht, entsprechend durch „01000010 01101001 01110100“. Wie dieses Beispiel zeigt, nimmt mit zunehmender Komplexität der Information auch eine größere Anzahl an Bits und Bytes erforderlich, um diese zu beschreiben.

Theorie der langen Wellen auch als fünfter Kondratjew-Zyklus bezeichnet, auf Fortschritte in Informationstechnologien zurückzuführen (Bartholomae 2018b; Linde & Stock 2011, Kap. 4.1) – als weitere Aspekte dieses aktuellen Zyklus wird oftmals auch auf eine verstärkte Ausrichtung auf nachhaltige und ökologische Innovationen verwiesen.

Abgesehen von der Entwicklung und Ermöglichung neuerer Geschäftsideen in späteren Stufen, ist die anfängliche Digitalisierung vor allem deshalb für Unternehmen vorteilhaft, da digitale Informationen gegenüber ihrem physischen Gegenstück erhebliche Kosteneinsparungen ermöglichen. Diese ergeben sich durch einen deutlich geringeren (physischen) Platzbedarf bei der Speicherung, einer einfacheren und schnelleren Auswertung, Modifikation und Weiterbearbeitung von Daten sowie einer insbesondere durch die mit der Digitalisierung einhergehenden Verbreitung des Internets schnellen und kostengünstigen Übertragung von Informationen. Das Internet erlaubt zudem weitere Einsparungen des physischen Platzbedarfs, da Speicher- und Rechenkapazitäten nicht mehr vorgehalten werden müssen, sondern durch Cloudbasierte Lösungen ersetzbar werden (Armbrust et al. 2010; Nazir 2012; Bartholomae 2018a).

Die Änderung der Kostenstruktur sowie die (allgegenwärtige) Verfügbarkeit der Informationen hat enorme Auswirkungen auf die Wünsche und Präferenzen der Konsumenten, die Ziele und Strategien von Unternehmen und den Bedarf notwendiger rechtlicher Rahmenbedingungen sowie Regulierungen seitens der Politik.

Natürlich können nicht alle physischen Güter und Dienstleistungen digitalisiert werden – so bleibt etwa der Transport von Menschen nur rein physisch möglich. Allerdings können damit verbundenen Dienstleistung (z.B. die Vermittlung zwischen Anbietern und Nachfragern von Transportleistungen) digitalisiert werden (vgl. Uber). Ist eine Digitalisierung möglich, entstehen digitale Produkten bzw. Informationsgüter, die sich in ihrem Gutcharakter von ihrem physischen Pendant teilweise unterscheiden. Im Unterschied zu ihrem physischen Gegenstück weisen sie vier spezifische Besonderheiten auf (Linde 2009, 298; Bartholomae 2014): (1) Tendenz zum öffentlichen Gut, (2) hohe Fixkosten bei geringen variablen Kosten in der Produktion, (3) Informationsasymmetrien zwischen den Marktteilnehmern und (4) Netzwerkeffekte. Die damit verbundenen Besonderheiten werden im Folgenden detaillierter aufgezeigt.

Öffentliche Güter sind dadurch gekennzeichnet, dass zum einen ein Ausschluss vom Konsum dieser Güter nur schwer möglich ist und zum anderen keine Rivalität im Konsum besteht (Pindyck & Rubinfeld 2003, 902). Der Vergleich zwischen dem physischen Buch als privatem Gut (sowohl Ausschließbarkeit als auch Rivalität liegen vor) und der darin enthaltenen Information (die Geschichte oder die vermittelte Idee) als öffentlichem Gut verdeutlicht den Unterschied: Ein Konsument kann von der Nutzung eines Buches ausgeschlossen werden, wenn er nicht bereit ist, für dessen Nutzung zu bezahlen. Prinzipiell besteht bei einer Information zwar auch die Möglichkeit, andere von deren Nutzung auszuschließen (etwa durch Urheberrechte, Patente oder im Falle von Dateien einem Kopierschutz), aber sobald die

Information auch nur kurzfristig ungeschützt verfügbar ist, ist ihre Verbreitung (fast) nicht mehr einzudämmen (Linde 2005, 19) – so reicht schon eine öffentliche Lesung der in dem Buch enthaltenen Information aus, um diese losgelöst vom Buch zu verbreiten. Bei der Nutzung eines Buches besteht auch Rivalität im Konsum: In dem Moment, in dem ein Konsument es liest, kann niemand anderes diese Version des Buches lesen. Hat hingegen ein Konsument die Information, können auch viele andere diese Information haben, ohne dass der Nutzen des ersten Konsumenten davon beeinträchtigt ist – sofern es sich nicht um etwa Insiderinformationen handelt.

Bei der Digitalisierung von Informationen fallen zunächst hohe Fixkosten an, zum Beispiel durch den anfänglichen Aufbau der Informationstechnologieinfrastruktur oder auch das Einpflegen neuer Datensätze in bestehende Datenbanksysteme. Die spätere Nutzung der Daten, wie das Abrufen, die Bearbeitung, die Auswertung oder die Übermittlung der Informationen verursacht hingegen praktisch vernachlässigbare Kosten (Ba et al. 2000, 188f.; Linde 2005, 21f.). Die Digitalisierung eines bislang nur in Papierform vorliegenden Buches erfordert etwa, dass jede Seite eingescannt und der Text mittels entsprechender Software maschinenlesbar gemacht werden muss, die spätere Recherche in einem digitalisierten Buch bzw. die Textentnahme und -bearbeitung ist dann aber mit nur sehr geringem Aufwand möglich.

Informationsasymmetrien liegen dann vor, wenn eine Marktseite (Anbieter) über mehr Informationen über das Gut – beispielsweise die vollständigen Produkteigenschaften und deren Qualität – verfügt als die andere Marktseite (Konsument). Dadurch unterscheiden sich die Preisvorstellungen der beiden Marktseiten – während der Anbieter den wahren Wert des Gutes kennt, kann der Konsument diesen nur schätzen – wodurch ein ökonomisch sinnvoller Handel zwischen den Marktpartnern verhindert bzw. im Extremfall sogar die Existenz des ganzen Markts für dieses Gut gefährdet werden kann (Akerlof 1970). Bei Informationen bzw. digitalen Produkten handelt es sich um sogenannte Erfahrungsgüter (Shapiro & Varian 1999, 5), das heißt, der Nutzer kann erst während oder nach dem Konsum feststellen, inwiefern seine Erwartungen erfüllt wurden bzw. welche Qualität die Information (für ihn) hat. So erfährt der Leser eines Buches erst durch die Lektüre, ob die darin enthaltene Information für ihn den ursprünglichen Kaufpreis rechtfertigt.

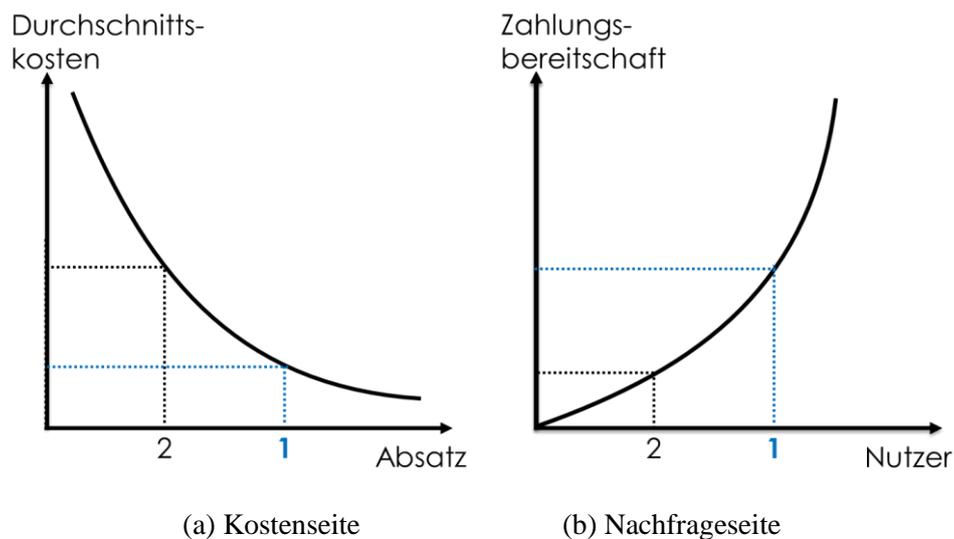
Netzwerkeffekte stellen die wichtigste Eigenschaft von Informationsgütern dar und beschreiben, dass der Nutzen bzw. der Wert des digitalen Produkts für die jeweiligen Konsumenten mit der Anzahl weiterer Nutzer steigt (Katz & Shapiro 1985; Shy 2011) – dies lässt sich gut anhand des Telefons verdeutlichen: Gibt es nur ein Telefon hat dies für den Besitzer keinen Nutzen, erst wenn es weitere Telefonbesitzer gibt, entsteht ein Nutzen. Solche Netzwerkeffekte stellen auch einen wichtigen Aspekt bei der Digitalisierungsentscheidung dar: Ist die Information z.B. in Form eines Dokuments nur für einen Mitarbeiter erforderlich, wird der Nutzen aus der Digitalisierung des Dokuments kaum deren Kosten kompensieren. Benötigen hingegen mehrere Mitarbeiter, womöglich auch noch zur gleichen Zeit und an verschiedenen Orten Informationen aus dem Dokument oder möchten dieses ergänzen, ist der Nutzen

der Digitalisierung schon deutlich höher. Ist das Dokument zudem für Geschäftspartner und Kunden relevant, nimmt die Vorteilhaftigkeit weiter zu. Wichtig ist in diesem Zusammenhang allerdings, dass die Digitalisierung in ein für alle relevanten Akteure lesbares Format erfolgt: Exotische Insellösungen, die entsprechend von nur wenigen genutzt werden können, stiften einen geringeren Nutzen als verbreitete Standardlösungen (Shy 2001a, Kap. 3.3.1).

3. Monopolisierung durch Digitalisierung

Die Eigenschaften von Informationsgütern können enorme Auswirkung auf die Wettbewerbssituation nach sich ziehen und daher Digitalisierungsentscheidungen erheblich beeinflussen. Märkte für durch die digitale Transformation neu entstandene Produkte und Dienstleistungen werden oft von Monopolisten bedient, zumindest aber von nur sehr wenigen Anbietern. Die Ursachen hierfür ergeben sich sowohl aus der Kosten- als auch der Nachfragestruktur bei Informationsgütern, wie im Folgenden kurz aufgezeigt werden soll.

Auf der Kostenseite weist die Produktion digitaler Güter hohe Fixkosten bei gleichzeitig geringen variablen Kosten auf. Beides bedingt, dass die Durchschnitts- bzw. Stückkosten mit zunehmender Ausbringungsmenge sinken. Es resultiert ein natürliches Monopol, da nur ein Unternehmen ausreichend von Größendegressionseffekten profitieren kann und es folglich ökonomisch effizient ist, dass der Markt von nur diesem einem Unternehmen versorgt wird. Abbildung 2a zeigt diesen Zusammenhang, wobei „1“ die Menge bei der Versorgung durch ein Unternehmen kennzeichnet und „2“ die Situation, wenn sich die gleiche Menge auf zwei konkurrierende Unternehmen aufteilt – wie zu erkennen, sind die Durchschnittskosten bei „1“ niedriger, da sich die Fixkosten auf insgesamt mehr Einheiten verteilen.

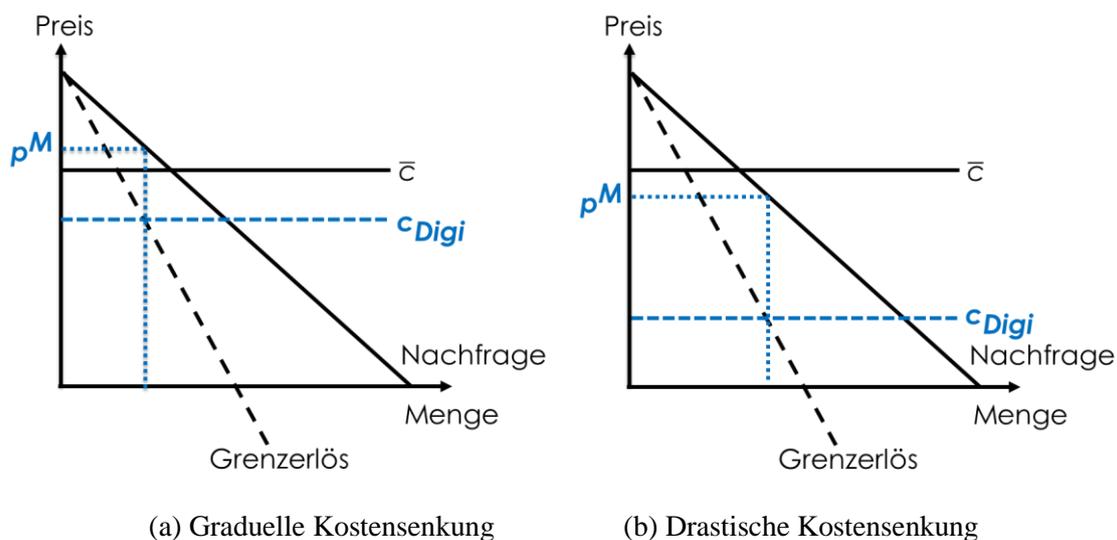


Quelle: Eigene Darstellung.

Abb. 2: Natürliches Monopol: Kostenseite und Nachfrageseite

Netzwerkeffekte auf der Nachfrageseite bedeuten, dass eine größere Nutzerbasis bzw. Bekanntheit eines Angebots den Nutzen aller Konsumenten dieses Guts erhöht. In Abbildung 2b wird dies anhand der Zahlungsbereitschaft der Konsumenten für das Gut verdeutlicht, das dem Metcalfe'schen Gesetz folgend quadratisch in der Nutzerzahl zunimmt (Shapiro & Varian 1999, 184) – die Intuition dahinter ist, dass die Interaktionsmöglichkeiten zwischen den Nutzern bei einem größeren Netzwerk deutlich steigen: Bei nur einem Teilnehmer bestehen keine Interaktionsmöglichkeiten, wohingegen bei zehn Teilnehmern jeder Nutzer potentiell mit neun anderen interagieren kann (Bartholomae 2012, 29). „1“ stellt erneut die Situation bei einem Anbieter dar, während „2“ aufzeigt, welche Zahlungsbereitschaft die Konsumenten für die nur halb so großen Netzwerke zweier Anbieter aufbringen. Selbst wenn der oftmals kritisierte quadratische Zusammenhang zwischen Nutzerzahl und Netzwerkwert als übertrieben angesehen wird, so besteht doch Konsens in einem zumindest überproportionalen Zusammenhang (Zhang et al. 2015), wodurch sich dasselbe Ergebnis einstellt: Ein großes Netzwerk führt zu einer deutlich höheren Zahlungsbereitschaft als viele kleine. Von diesem Effekt profitiert beispielsweise die Auktionsplattform eBay – Verkäufer wissen, dass dort viele potentielle Käufer nach Produkten suchen und auch Käufer wissen, dass viele Verkäufer die Plattform nutzen, um ihre Produkte anzubieten. Sowohl Käufer als auch Verkäufer, die auf weniger bekannte oder weniger große Plattformen ausweichen, werden demgegenüber Schwierigkeiten haben, das passende Produkt zu finden oder zu verkaufen. Somit wird hier durch die Nachfrageseite und die Netzwerkeffekte ein Monopol geschaffen.

Generell überrascht es wenig, dass neue Produkte zunächst von nur einer oder wenigen Firmen angeboten werden, die somit ihren selbst geschaffenen Markt beherrschen. Im Unterschied zu Informationsgütern ist bei traditionellen Gütern die marktbeherrschende Stellung allerdings nicht immanent gegeben. Dennoch kann die Digitalisierung auch in bestehenden traditionellen Industrien dazu führen, dass sich durch die realisierten Kosteneinsparungen Monopole entwickeln. Dies ist umso wahrscheinlicher, je drastischer die Kosteneinsparungen ausfallen (Shy 2001b, Kap. 9.1).



(a) Graduelle Kostensenkung

(b) Drastische Kostensenkung

Quelle: Eigene Darstellung.

Abb. 3: Graduelle vs. drastische Kostensenkung

In Abbildung 3a werden zunächst die Auswirkungen einer graduellen bzw. einer nur geringen Kostensenkung durch Digitalisierung/Digitalisation bei einer Firma in einem kompetitiven Markt dargestellt. Es wird angenommen, dass in diesem Markt sehr viele Firmen aktiv sind, das heißt die einzelne Firma hat keine Marktmacht, die alle ein identisches homogenes Produkt zu Grenzkosten von \bar{c} herstellen. Bei Preiswettbewerb wird der Preis diesen Grenzkosten entsprechen und die Firmen erzielen somit ökonomische Nullgewinne – bei einem höheren Preis als \bar{c} würden die Konsumenten zu den Unternehmen abwandern, die einen geringeren Preis erheben, während Unternehmen, die unterhalb von \bar{c} anbieten, Verluste erzielen. Digitalisierung/Digitalisation erlaubt nun einer Firma ihre Grenzkosten von \bar{c} auf c_{Digi} zu senken. Diese Kosteneinsparung ist im Fall von Abbildung 3a jedoch nicht hoch genug, um in diesem Markt ein Monopol entstehen zu lassen. Generell maximiert ein Monopolist dann seinen Gewinn, wenn der Grenzerlös – der Erlös, den er durch den Verkauf einer zusätzlichen Einheit erzielen kann – gerade den Grenzkosten – die Kosten, die ihm aus der Produktion dieser zusätzlichen Einheit entstehen – entsprechen. Der Grenzerlös verläuft bei linearer Nachfrage mit der doppelten negativen Steigung wie die Nachfragekurve. Aus dem Schnittpunkt zwischen Grenzerlös- und Grenzkostenkurve ergibt sich die Monopolmenge, die wiederum auf der Nachfragekurve den zugehörigen Monopolpreis p^M bestimmt (Shy 2001b, Kap. 5.1). Da dieser im konkreten Fall von Abbildung 3a oberhalb der Grenzkosten \bar{c} und damit dem Preis aller anderen Unternehmen im Markt liegt, wird das Unternehmen diesen nicht wählen, da es zu diesem Preis keine Abnehmer finden wird – schließlich würde es das gleiche Produkt wie alle anderen Unternehmen, jedoch zu einem höheren Preis anbieten. Es wird stattdessen den höchstmöglichen Preis, konkret somit weiterhin den Wettbewerbspreis \bar{c} verlangen, wodurch es aber im Unterschied zu seinen Konkurrenten nun einen (ökonomischen) Gewinn erzielt. Können die Wettbewerber ebenfalls ihre Kosten durch Digitalisierung auf c_{Digi} reduzieren, wird die Kostenersparnis schließlich in Form eines niedrigeren Preises an die Verbraucher weitergereicht und die anfänglichen Gewinne der Pioniere der Digitalisierung werden wieder verschwinden.

In Abbildung 3b wird demgegenüber die Auswirkung einer drastischen Kostensenkung aufgezeigt. Die Grenzkosten c_{Digi} sind hier so stark gesunken, dass der sich dabei ergebende Monopolpreis p^M geringer als der Wettbewerbspreis \bar{c} ist, das heißt, das Unternehmen wird trotz Erhebung des Monopolpreises günstiger als seine Konkurrenten anbieten. Neben dem Unternehmen, das nun einen Monopolgewinn erwirtschaftet, profitieren auch die Verbraucher von einem gesunkenen Preis. Sofern sie über ausreichend Rücklagen verfügen, werden die Konkurrenten sicherlich ihrerseits die Digitalisierung und Digitalisation vorantreiben, um ihre Wettbewerbsfähigkeit wiederherzustellen.

Während die Verbraucher bei einer graduellen Kostensenkung erst nach einiger Zeit von Preissenkungen profitieren, profitieren sie bei einer drastischen Kostensenkung unmittelbar von einem gesunkenen Preis und – sofern genügend Wettbewerber überleben und ihrerseits in der Lage sind die Kosten zu senken – auch von einem langfristig deutlich niedrigeren Preis. Sollte das Monopol aber weiterbestehen, kann es langfristig zu Wohlfahrtseinbußen kommen, da Monopolisten oftmals weitere Innovationen

durch Patente schützen, die ihre Monopolstellung gefährden könnten (Gilbert & Newbery 1982), worunter letztlich die ökonomische Effizienz leidet. Aus volkswirtschaftlicher Sicht stellt sich die Frage, wie diese Marktstrukturen aufgebrochen werden können, wobei grundsätzlich hier dem Staat bzw. Regulierungsbehörden eine entscheidende Rolle zukommt (vgl. Krämer 2019). Aus Sicht eines Unternehmens stellt die Aussicht auf eine drastische Kostenreduktion und damit einhergehend die Möglichkeit, Wettbewerber vom Markt zu verdrängen, eine große Chance dar, die dazu führen kann, erhebliche Anstrengungen in diese Richtung zu unternehmen. Konkret kann dies bedeuten, eine Vorreiterrolle bei der Digitalisierung anzustreben und dabei auch keine Kosten zu scheuen.

4. Einfaches Modell der Digitalisierungsentscheidung

In Deutschland ist die Digitalisierung zwischen den verschiedenen Industriesektoren unterschiedlich stark ausgeprägt. Während bei größeren Industrieunternehmen der Digitalisierungsgrad weit vorangeschritten ist, fallen kleinere Firmen zurück (Kopke et al. 2016, 19). Angesichts des Resultats, das bereits graduelle Kosteneinsparungen den digitalisierenden Unternehmen einen Gewinnzuwachs ermöglicht, stellt sich die Frage, warum nicht alle Unternehmen digitalisieren, um von den Kosteneinsparungen zu profitieren. Oder anders formuliert: Von welchen Faktoren hängt es ab, ob sich Digitalisierung lohnt? Grundsätzlich ergibt sich die Vorteilhaftigkeit einer Maßnahme aus einer Kostenabwägung – schließlich stehen den hohen Investitionskosten in der Anfangsphase erst später erfolgende Kosteneinsparungen gegenüber. Die Kostenersparnis tritt dabei bei jeder einzelnen Nutzung auf, indem Transaktionskosten gespart werden. Am Beispiel eines Kundendatensatz, der zunächst nur physisch auf Papier existiert, lässt sich dies verdeutlichen: Wird dieser benötigt, etwa um die Adresse des Kunden herauszufinden, müssen die entsprechenden physischen Ordner durchsucht werden, um die Information zu erhalten. Es entstehen dabei Zeit- und Suchkosten, die sich etwa in Mitarbeiterstunden beziffern lassen können. Ist der Datensatz jedoch digital in einem System hinterlegt, kann er wesentlich schneller in einer Suchmaske gefunden werden. Dieser Datensatz kann zudem entweder als Kopie allen relevanten Mitarbeitern zur Verfügung gestellt werden – was ungleich kostengünstiger ist als etwa die Bereitstellung entsprechender physischer Ordner – oder online zugänglich sein (Cloud-Lösung), wodurch die höchste Aktualität der Daten sichergestellt ist, da Änderungen augenblicklich an alle Nutzer weitergegeben werden. Konkret bedeutet dies beispielsweise, dass ein Vertriebsmitarbeiter im Außendienst problemlos auf Daten zugreifen kann ohne direkt am Firmensitz die Information suchen bzw. einen Mitarbeiter vor Ort kontaktieren zu müssen. Darüber hinaus kann er Datenänderungen (etwa eine veraltete Adresse) durchführen, die dann allen anderen Abteilungen (Marketing, Kundendienst) sofort zur Verfügung stehen.

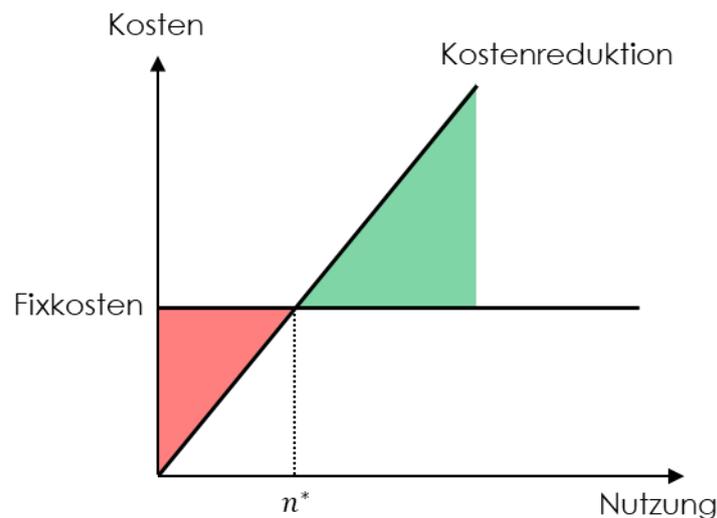
Da das volle Potential der Digitalisierung sich erst durch Ausnutzung der Netzwerkeffekte realisiert, sollte auch immer die Verfügbarkeit der relevanten Daten über Cloud-Lösungen oder andere Online Ressourcen möglich sein. Denn werden Daten nur digitalisiert und lokal auf einem Rechner gespeichert, sind die Vorteile überschaubar – zwar kommt es zu den grundsätzlichen Kosteneinsparungen (geringerer

Platzbedarf, raschere Bearbeitung), aber der große Vorteil, dass viele Nutzer auf die gleichen Informationen Zugriff haben, besteht nicht und zudem wird auch die im Zuge der Digitalisation erfolgende Prozessoptimierung erschwert. In den folgenden Analysen wird daher immer davon ausgegangen, dass die Daten auch online zugänglich sind.

Die Kosten der erstmaligen digitalen Erfassung bestehen zum einen darin, eine geeignete Softwarelösung zu finden, für die entweder bei Eigenentwicklung hohe Entwicklungskosten entstehen oder bei Verwendung von Standardlösungen, Kosten für den Lizenzerwerb der Software anfallen. Zum anderen müssen alle Daten in dieses System eingepflegt werden, wodurch ebenfalls erhebliche Kosten entstehen, ohne dass zunächst ein Nutzen auftritt. Die konkrete Kostenersparnis ergibt sich dabei aus der Nutzung der digitalen Ressourcen und fällt umso höher aus, je öfter die Daten benötigt werden. Diese Kostenabwägung lässt sich durch folgende Ungleichung einfach verdeutlichen:

$$nc > f,$$

wobei n die Anzahl der (erwarteten) Nutzungen, c die Kostenersparnis je Nutzung und f alle im Zuge der Digitalisierung anfallenden Fixkosten (Umwandlung, Implementierung, etc.) darstellen. Nur dann, wenn die (erwartete) Kostenersparnis (linke Seite) größer als die Investitionskosten (rechte Seite) ausfällt, kann die Digitalisierung als lohnenswert angesehen werden und sollte daher durchgeführt werden. Dies hängt, wie auch Abbildung 4 verdeutlicht, von der Nutzungsintensität ab, sodass sich eine Digitalisierung letztlich erst ab einer (erwarteten) Nutzungsintensität von $n > n^* = f/c$ lohnt. Liegt die Nutzung unterhalb dieser Schwelle, wird ein Unternehmen auf die Digitalisierung verzichten, da keine ausreichend hohen Einsparungen erzielt werden können. Dies kann grundsätzlich die Diskrepanz zwischen großen und kleinen Unternehmen erklären.



Quelle: Eigene Darstellung.

Abb. 4: Vergleich Kostenreduktion und Fixkosten zur Bestimmung der Mindestnutzung

Natürlich kann es auch sein, dass die notwendige Nutzungsintensität erst dann erreicht wird, wenn durch die Digitalisierung (ex ante) eine monopolähnliche Stellung (ex post) erreicht wird, die entsprechend hohe Umsätze und damit eine höhere Nutzungsintensität generiert (das heißt, es besteht ein nichtlinearer Zusammenhang zwischen Kostenersparnis und den Fixkosten). Die Fähigkeit, einen geringeren Preis als die Wettbewerber zu setzen, bedingt jedoch, dass die Firma in der Lage ist, den Markt allein zu versorgen. Zwar sinken die Kosten pro Nutzungseinheit durch die Digitalisierung, grundsätzliche Kapazitätsbeschränkungen bleiben dennoch weiterhin bestehen, weshalb die bei der vorherrschenden Nachfrage möglichen Kosteneinsparungen eventuell nicht voll realisiert werden können. Es besteht daher die Gefahr, dass größere Firmen mit entsprechendem Finanzpolster mittelfristig den Wettbewerb durch Investitionen in Digitalisierung zu ihren Gunsten beeinflussen können, vor allem, wenn sie die Kosteneinsparungen (zunächst) direkt an die Verbraucher weitergeben und damit kleinere kapazitätsbeschränkte Unternehmen unter Druck setzen bzw. sie sogar vom Markt vollständig verdrängen können. Dies deckt sich auch mit der Beobachtung, dass hauptsächlich große Unternehmen gezielt die Entwicklung digitaler Geschäftsmodelle investieren (Berg 2018, 10).

Ein weiterer relevanter Faktor ist auch die Kundenbeziehung. Sind die wichtigsten Kunden nicht digitalisiert, entstehen zusätzliche Kosten, wenn die digitalisierten Informationen erst wieder in analoge Form gebracht werden müssen, um sie mit Kunden oder Zulieferern auszutauschen – beispielsweise durch den Ausdruck von Produktbroschüren oder Formularen, die dann später wieder für die eigene Bearbeitung zu digitalisieren sind. Dies kann somit eine nur geringe, und damit für Digitalisierung nicht ausreichend hohe, Nutzungsintensität bei kleinen mittelständischen Unternehmen und Handwerksbetrieben erklären. Dies zeigt die Umfrage von bitkom und ZDH (Rohleder & Schulte 2017, 11): Als Hemmnis für die Digitalisierung werden neben Problemen auf der Mitarbeiterseite, das heißt mangelnde Digitalkompetenz der Mitarbeiter (67%) und Berührungängste der Handwerker gegenüber digitalen Technologien (63%), auch das mangelnde Interesse der Kunden (17%) angegeben. Allerdings ist dies sicherlich nur ein temporärer Faktor, da bei fortschreitender Digitalisation, das heißt der Optimierung der Geschäftsprozesse nach erfolgter Digitalisierung, immer mehr Kunden bzw. Zulieferer ihre Systeme umstellen werden bzw. „digital natives“ eine derartige Entwicklung immer mehr fordern.

Als Zwischenfazit ergibt sich damit, dass ein (momentan) kleiner Markt eine zu geringe Nutzungsintensität bedingt, bei der sich Digitalisierung nicht lohnt. Anders sieht es aber aus, wenn der Markt diese Schwelle überschreitet. In diesem Fall legt auch die, der Abbildung 3 zugrundeliegende, Analyse nahe, dass Unternehmen, sofern sie wettbewerbsfähig bleiben möchten, gezwungen sind, zu digitalisieren, Digitalisierung mithin eine dominante Strategie darstellt. Dieser Digitalisierungsdruck wird vereinfacht durch das in Tabelle 1 dargestellte Spiel verdeutlicht.

U1, U2	Keine Digitalisierung	Digitalisierung
Keine Digitalisierung	(0 , 0)	(-1 , 1)

Digitalisierung	(1 , -1)	(0 , 0)
-----------------	------------	-----------

Quelle: Eigene Darstellung.

Tab. 1: Digitalisierungsdruck

Betrachtet wird hier die strategische Interaktion zwischen den beiden Unternehmen U1 und U2 sowie die Gewinnänderungen, wenn sie bestimmte Strategien verfolgen. Beide Unternehmen stehen vor der Entscheidung, ob sie digitalisieren möchten („Digitalisierung“) oder nicht („Keine Digitalisierung“) – es wird dabei unterstellt, dass der Markt ausreichend groß ist bzw. $n = n^* = f/c$, sodass sich kein unmittelbarer Vorteil aus der Digitalisierung ergibt. Verzichten beide Unternehmen auf die Digitalisierung, so ändert sich für beide der Gewinn nicht, es resultiert die Kombination „(0 , 0)“ – hier gibt der erste Wert die Auszahlung/Gewinnänderung für Unternehmen 1 und der zweite Wert die Auszahlung für Unternehmen 2 an. Digitalisiert ein Unternehmen, während das andere darauf verzichtet, kann das digitalisierende Unternehmen seine Kosten senken, wodurch es in der Lage ist, seine Preissetzung anzupassen und Marktanteile zu gewinnen. Dadurch steigert es seinen Gewinn und seine Auszahlung erhöht sich entsprechend auf 1. Umgekehrt verliert das nicht-digitalisierende Unternehmen Kunden und es muss Verluste hinnehmen, was durch die negative Auszahlung -1 zum Ausdruck gebracht wird. Digitalisieren beide Unternehmen, bleibt ihre relative Kostenstruktur unverändert und somit auch ihr Gewinn (siehe hierzu auch Abbildung 3a). „Digitalisierung“ stellt somit eine dominante Strategie dar (Bartholomae & Wiens 2016, 65ff.): Gegeben, der Konkurrent digitalisiert nicht, lohnt sich die Digitalisierung, da eine Gewinnverbesserung erzielt werden kann. Gegeben, der Konkurrent digitalisiert, lohnt sich die Digitalisierung, da hierdurch Verluste vermieden werden und der Status Quo erhalten bleibt. Das heißt, unabhängig davon, wie sich der Konkurrent entscheidet, ist es immer vorteilhaft zu digitalisieren – es herrscht somit ein Digitalisierungsdruck in Märkten, die diese ermöglichen (das heißt $n \geq n^* = f/c$).

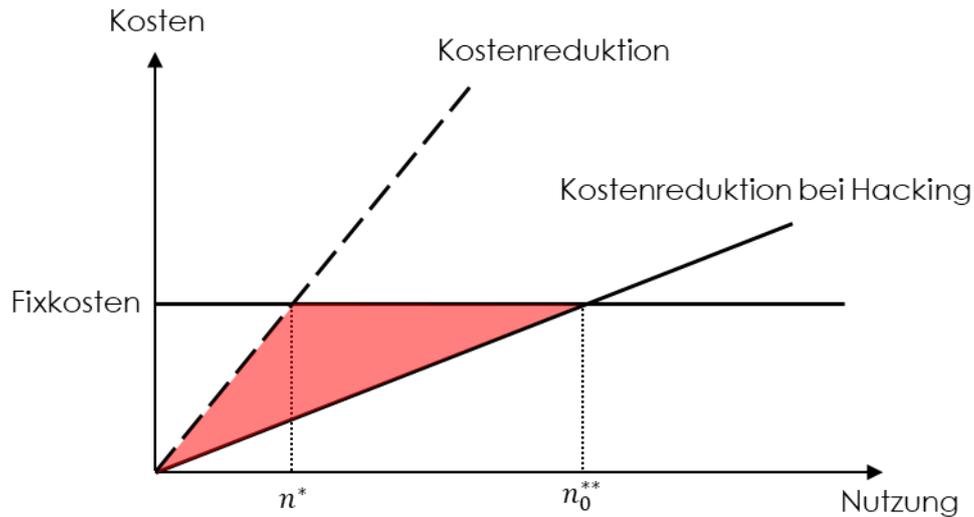
5. Digitalisierung und Cyberkriminalität

Durch die umfassende Digitalisierung wichtiger Betriebsdokumente nehmen die Risiken durch Cyberkriminalität zu. Unter Cyberkriminalität werden alle kriminellen Aktivitäten zusammengefasst, die entweder unter Verwendung von Informationstechniksystemen begangen werden oder sich gegen diese Infrastruktur richten (Kshetri, 2006, 33). Das Gefahrenpotential von Cyberkriminalität insbesondere im Vergleich zu traditioneller Wirtschaftskriminalität ist enorm: Im Unterschied zu analogen Dokumenten, die relativ einfach durch physische Maßnahmen (beispielsweise durch einen Safe) geschützt werden können und nur lokal zugänglich sind, ist ein Zugriff auf digitale Dokumente lokal nicht beschränkt – somit birgt ein wichtiger Vorteil der Digitalisierung gleichermaßen ein erhebliches Gefahrenpotential. Zwar können auch elektronische Daten durch entsprechende Soft- und Hardware geschützt werden, allerdings gibt es weltweit eine deutlich größere Anzahl Krimineller, deren direkte Kosten relativ gering sind – schließlich ist nur ein Computer mit Internetzugang und entsprechendes Fachwissen erforderlich.

Derzeit scheint jedoch die Gefährdung durch internationale Hacker bzw. die Wahrnehmung dieser Gefährdung nicht allzu ausgeprägt zu sein. So gaben deutsche Unternehmen in Befragungen an, dass hauptsächlich ehemalige Mitarbeiter für Datendiebstahl verantwortlich seien, wobei hier teilweise auch nur sorgloser Umgang mit Firmendaten der Grund ist (Bachmann et al. 2015, 20; Kopke et al. 2016, 29). Dennoch weist etwa das Allianz Risikobarometer seit Jahren Cybervorfälle als Toprisiko auf und nimmt dabei sowohl weltweit als auch in Deutschland einen immer größeren Stellwert ein (Allianz 2019).

In Deutschland war im Schnitt bereits jedes zweite Unternehmen schon einmal von Datendiebstahl betroffen (Bachmann et al. 2015, 9). Überdurchschnittlich häufig sind Industrieunternehmen Opfer von Cyberkriminalität, wobei mehr kleine und mittlere als große Industrieunternehmen (ab 500 Mitarbeiter) Ziel der Kriminellen geworden sind (Kopke et al. 2016, 10). Ein Grund hierfür ist sicherlich, dass hauptsächlich weniger digitalisierte Unternehmen betroffen sind (Kopke et al. 2016, 13, 18) und kleinere Unternehmen, wie in Abschnitt 3 aufgeführt, tendenziell weniger stark digitalisiert sind. Je mehr ein Unternehmen die Digitalisierung vorantreibt, desto mehr wird es sich unweigerlich mit Datensicherheit auseinandersetzen müssen und ist damit umso besser gegenüber unberechtigten Zugriffen gewappnet. Da die Kosten für Cyberkriminelle relativ gering sind (Bartholomae 2018a, 302), sind Angriffe auf kleinere Unternehmen nicht nur aufgrund deren oftmals geringeren Schutzes lohnenswert: Die Kosten die sich aus dem Aufwand und der potentiellen Bestrafung ergeben fallen so niedrig aus, dass bereits ein nur geringer Wert der Daten ausreichend Anreize zum Hacking liefert. Bei großen Unternehmen sind vor allem Angriffe auf für Forschung und Entwicklung zuständige Abteilungen festzustellen (Bachmann et al. 2015, 13).

Der Schaden, der durch Cyberkriminalität entsteht, kann für die Unternehmen existenzgefährdend sein. Direkte Kosten fallen unter anderem bei der Wiederherstellung beschädigter oder zerstörter Dateien an oder in Form von Lösegeldern, dass die Kriminellen für die Rückgabe von Dateien erpressen. Oftmals deutlich größer sind jedoch die indirekten Kosten, beispielsweise, wenn Konkurrenzunternehmen Kenntnis essentieller Betriebsgeheimnisse erlangen. So überrascht es nicht, dass unter allen Delikttypen, Plagiate und Patentrechtsverletzungen die höchsten Schäden verursachen (Bachmann et al. 2015, 17; Kopke et al. 2016, 26). Folgend rangieren etwa Schäden, die durch Ausfall und Störungen von Informationstechniksystemen und Betriebsabläufen entstehen. Erhebliche Kosten verursachen aber auch Imageschäden, da insbesondere Kundenbeziehungen auf sensiblen Daten basieren und ein Verlust oder eine Weitergabe dieser Daten wertvolles Vertrauen zerstören kann. Dies ist auch ein Grund, warum sich nach einem Cyberangriff nur jedes fünfte Unternehmen an staatliche Stellen wendet (Bachmann et al. 2015, 24). Hierdurch verschärft sich allerdings die Problematik, da eine Verfolgung der (erfolgreichen) Straftäter unmöglich gemacht wird und diese weitere Unternehmen gefährden können bzw. potentielle Hacker nicht abgeschreckt werden.



Quelle: Eigene Darstellung.

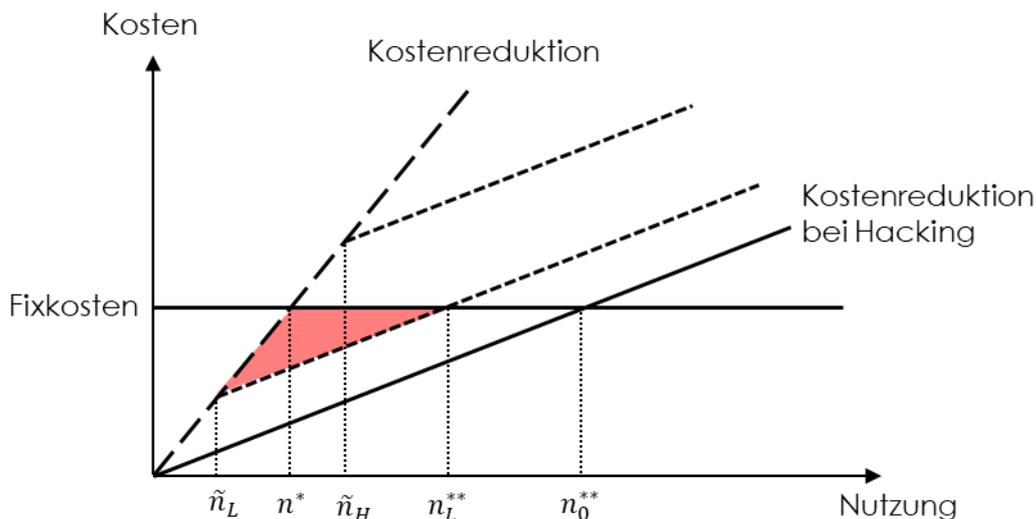
Abb. 5: Berücksichtigung geringerer Kostenersparnis durch potenziellen Schaden

Cyberkriminalität erhöht somit grundsätzlich die (erwarteten) Kosten der Digitalisierung, die bei der Digitalisierungsentscheidung berücksichtigt werden müssen. In einem ersten Schritt kann vereinfacht angenommen werden, dass mit zunehmender Digitalisierung und Digitalisation auch das Risiko steigt, dass es sich für Cyberkriminelle lohnt, die Dokumente zu hacken, wodurch es für das Unternehmen zu einem Schaden kommt. Bezeichne $\rho(n) = \rho n$ das Risiko eines Hacking-Angriffs, das mit der Nutzungsintensität n steigt, und d die Kosten, die dem Unternehmen im Schadensfall entstehen. Somit ändert sich das effiziente Kalkül zu

$$nc > f + \rho nd.$$

Die Kostenersparnis durch Digitalisierung muss nun nicht mehr nur noch die Kosten der Digitalisierung f decken, sondern auch die erwarteten Kosten im Schadensfall eines Hacking-Angriffs ρnd . Somit ergibt sich nun eine höhere Nutzungsintensität, ab der sich Digitalisierung für ein Unternehmen lohnt, $n > n_0^{**} = f/(c - \rho d) > n^*$. Unternehmen sehen sich nun folgendem Trade-off gegenüber: Einerseits nimmt die Kostenersparnis pro Einheit in der Nutzung zu, andererseits steigt aber auch der erwartete Schaden (höhere Wahrscheinlichkeit, dass Daten gehackt werden bzw. höheres Schadensvolumen durch intensivere Nutzung). Dies reduziert die Kostenersparnis und führt dazu, dass sich die Digitalisierung *ceteris paribus* erst ab einer intensiveren Nutzung lohnt – dann, wenn die Kostenersparnis durch die Digitalisierung den potenziellen Schaden überkompensiert (siehe auch Abbildung 5). Übersteigt der erwartete Schaden je Nutzung die Kostenersparnis durch Digitalisierung, $\rho d > c$, wird sich das Unternehmen nie für Digitalisierung entscheiden. Insgesamt führt die Gefahr durch Hacking dazu, dass weniger Firmen bereit sind, zu digitalisieren – worunter letztlich die ökonomische Effizienz leidet, da die Kosteneinsparungen von Firmen im Nutzungsbereich $[n^*, n_0^{**})$ nicht realisiert werden.

Der Umfang der Digitalisierung hat allerdings nicht nur Auswirkungen auf den erwarteten Schaden, sondern auch auf die Anreize der Cyberkriminellen (Bartholomae 2018a, 300). Ist nur wenig digitalisiert, steht den Kosten in Form von Zeit, Aufwand und zu erwartender Strafe, ein relativ geringer Nutzen gegenüber. Dies führt dazu, dass es auch aus Sicht der Cyberkriminellen eine Nutzungsschwelle bzw. Digitalisierungsschwelle \tilde{n} gibt, ab der erst ein ausreichend hoher Nutzen entsteht, sodass sich ein Angriff auf das Unternehmen lohnt. Abbildung 6 verdeutlicht die Effekte: Hier wird anders als in Abbildung 5 davon ausgegangen, dass sich nicht bei jedem Nutzungslevel ein Cyberangriff lohnt. Konkret werden zwei Szenarien mit den Hacking-Schwellen \tilde{n}_H und \tilde{n}_L betrachtet. Diese liegen jeweils oberhalb und unterhalb der Nutzungsintensität n^* , ab der sich Digitalisierung für ein Unternehmen lohnt, das heißt $\tilde{n}_H > n^*$ und $\tilde{n}_L < n^*$. Eine hohe Hacking-Schwelle \tilde{n}_H hat keine Auswirkungen auf das Digitalisierungskalkül des Unternehmens, die einzige Veränderung ist, dass ab \tilde{n}_H der Vorteil der Digitalisierung geringer ausfällt, da das Unternehmen mit Cyberangriffen rechnen muss. Ist die Hacking-Schwelle jedoch niedrig, \tilde{n}_L , erhöht dies die für eine profitable Digitalisierung notwendige Nutzungsintensität auf n_L^{**} . Somit zeigt sich, dass je geringer die Hacking-Schwelle ausfällt, desto größer wird die notwendige Nutzungsintensität sein, ab der sich Digitalisierung für ein Unternehmen lohnt und damit gleichbedeutend: je niedriger die Hacking-Schwelle, desto höher der ökonomische Effizienzverlust.



Quelle: Eigene Darstellung.

Abb. 6: Szenarien für unterschiedliche Netzgrößen/Gefährdungstufen

Die Kenntnis der konkreten Hacking-Schwelle kann auch genutzt werden, um Hacking zu vermeiden: Wird die Digitalisierung auf diese Schwelle begrenzt, wird die Gefahr eines Hacking-Angriffs vernachlässigbar, da „professionelle“ Hacker keinen Anreiz haben, sich der Daten zu bemächtigen (Bartholomae 2018a, 301). Inwiefern es sich hierbei um eine sinnvolle Strategie handelt, hängt stark von der Hacking-Schwelle ab. Während etwa bei \tilde{n}_H trotz Begrenzung Kosteneinsparungen realisiert werden können, ist eine Begrenzung auf \tilde{n}_L nicht zu empfehlen, da hier die Kosteneinsparnis nicht in der Lage

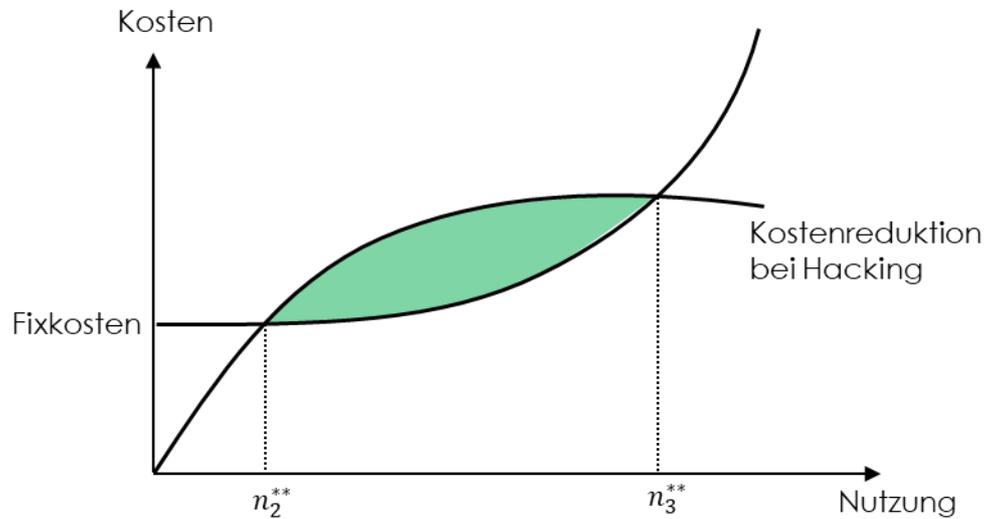
ist, die Digitalisierungskosten zu decken. In diesem Fall muss zur Vermeidung von Hacking vollständig auf Digitalisierung verzichtet werden.

Leider gibt es eine Reihe institutioneller Probleme, die nahelegen, dass eher von einer niedrigen Schwelle wie \tilde{n}_L auszugehen ist (Kshetri 2006, 2010): Zum einen haben Strafverfolgungsbehörden wenig Erfahrung oder Wissen, um mit Cyberkriminalität umzugehen, insbesondere, wenn sie es mit internationalen Hackern außerhalb ihres (nationalen) Zuständigkeitsbereichs zu tun haben. Zum anderen gibt es eine Reihe von Ländern, in denen Cyberkriminalität überhaupt nicht als Straftat verfolgt wird, was insbesondere bei internationalen Unternehmungen problematisch ist.

Da Unternehmen somit nicht auf die abschreckende Wirkung der Strafverfolgung vertrauen können, erscheint es sinnvoll, in eigene Vorsichtsmaßnahmen zu investieren. Diese Maßnahmen müssen dabei allerdings über den reinen Basisschutz, der durch einfachen Passwortschutz, Firewalls oder Virens Scanner gekennzeichnet ist, hinausgehen. Es ist vielmehr erforderlich, auf fortgeschrittene technische Sicherheitsmaßnahmen, wie die Verschlüsselung von Daten und Netzwerkverbindungen, die Absicherung des Firmennetzwerks gegen Datenabfluss, erweiterte Verfahren zur Benutzeridentifikation oder Penetrationstests, zu setzen (Kopke et al. 2016, 51). Darüber hinaus sind zudem bessere Schulungen, vor allem der Mitarbeiter in sensiblen Bereichen, unerlässlich, da auch die besten technischen Vorkehrungen ohne menschliche Sorgfalt nicht wirksam sein können (Bartholomae 2018a, 299). Dies gilt in einer vernetzten Welt nicht nur für die eigenen Mitarbeiter, denn auch durch sorglose Zulieferer und Kunden können Schäden entstehen. Der Schutz der eigenen Daten ist somit nur durch eine gemeinsame Anstrengung aller Stakeholder möglich und erfolgreich, da nicht alle relevanten und sensiblen Informationen wirklich der eigenen Kontrolle unterliegen.

Derartige umfangreiche Maßnahmen werden die Digitalisierungskosten allerdings drastisch erhöhen – wobei sie umso höher ausfallen werden, je intensiver die Nutzung ist. Umgekehrt nimmt das Interesse der Kriminellen mehr und mehr zu, sodass bei einer höheren Digitalisierung auch der erwartete Schaden dank stärkeren Bemühungen der Kriminellen zunimmt. Zudem ist denkbar, dass höhere Sicherheitsmaßnahmen Cyberkriminelle auch besonders herausfordern, da sie bei besonders starken Maßnahmen auch besonders wertvolle Daten vermuten – ein gutes Sicherheitssystem kann in dieser Hinsicht eine negative Signalwirkung entfalten. Jeder Effekt, höhere Investitionskosten und höherer Hacking-Anreiz, für sich bzw. beide Effekte zusammen führen dazu, dass sich die Digitalisierungsentscheidung grundsätzlich ändert und es nur mehr bei bestimmten Nutzungsintensitäten sinnvoll ist zu digitalisieren. Abbildung 7 verdeutlicht diese Überlegung: Bei einer zu geringen Nutzungsintensität sind die Kostensparungen zu gering, um die Digitalisierungskosten zu decken. Bei einer sehr hohen Nutzungsintensität, die demzufolge einen hohen Grad der Digitalisierung erfordert, überwiegen entweder die Nachteile durch höhere Anreize seitens der Kriminellen, wodurch der erwartete Schaden zunimmt und die Kostenersparnis entsprechend reduziert wird. Und/oder die Kosten der Datensicherung nehmen in einem solchen Umfang zu, dass die Digitalisierungskosten zu hoch ausfallen. Nur in einem mittleren Nutzungsbereich halten

sich die Anreize der Cyberkriminellen und die Kosten der Datensicherung in Grenzen und Digitalisierung lohnt sich.



Quelle: Eigene Darstellung.

Abb. 7: Fixkostenanstieg durch Sicherheitsmaßnahmen und höherer Hacking-Anreiz

Zusammenfassend zeigt sich somit, dass die Gefahren der Cyberkriminalität die Kosten der Digitalisierung deutlich erhöhen, sodass sich diese nicht (mehr) für alle Unternehmen lohnt. Kommt ein Unternehmen zu der Entscheidung, dass sich Digitalisierung trotz der Risiken lohnt, kann diese Entscheidung immer nur auf einer erwartenden Einschätzung der Wahrscheinlichkeit und Auswirkungen eines Hacking-Angriffs basieren, da eine hundertprozentige Sicherheit nicht besteht. Es besteht somit immer die Gefahr, dass es zu einem Hacking-Angriff kommt. Dieser kann relativ harmlos verlaufen, sodass ein nur überschaubarer Schaden etwa in Form von Gewinneinbußen entsteht. Allerdings können auch essenzielle Geschäftsgeheimnisse abhandenkommen, was im schlimmsten Fall zum Ende der Firma führen kann. Damit wird Cyberkriminalität zu einer ernststen Gefährdung der Wettbewerbsfähigkeit der Firmen und damit dem Wohlstand der Gesellschaft, insbesondere, wenn gezielt wichtige Branchen eines Landes geschädigt werden. IT-Sicherheit und Datenverschlüsselungstechnologie werden folglich eine immer grundlegendere Bedeutung zukommen, damit die Nachteile die Vorteile der Digitalisierung nicht überwiegen.

Angesichts der Bedrohung und der Risiken durch Cyberkriminalität ist es wenig überraschend, dass jedes Unternehmen so gut es geht versuchen wird, seine eigenen Daten bestmöglich zu sichern. Dies hat allerdings Auswirkungen auf die anderen Unternehmen: Denn je besser die Daten eines Unternehmens geschützt sind, desto relativ schlechter sind die Daten der anderen Unternehmen geschützt. Somit wird ein Hacker seine Bemühungen eher auf andere weniger geschützte Unternehmen richten (Cremonini & Nizovtsev 2006). Tabelle 2 verdeutlicht diese Situation. Betrachtet wird erneut die Interaktion zwischen zwei Unternehmen U1 und U2, die sich entscheiden können, ob sie ihr bisheriges Sicherheitssystem beibehalten möchten oder es verbessern sollen. Behalten beide Unternehmen ihr bisheriges System bei,

so ändert sich die relative Bedrohung durch Cyberkriminelle nicht, was durch die Gewinnänderung „(0, 0)“ für beide verdeutlicht wird. Investiert nun ein Unternehmen in die Verbesserung seines Sicherheitssystems, so profitiert es von einer Änderung der relativen Bedrohung – Cyberkriminelle werden nun eher das andere Unternehmen hacken, da dieses weniger gut geschützt ist. Somit steigt die Nettoauszahlung, die sich aus der Reduktion des erwarteten Schadens und den Kosten für das Sicherheitssystem ergibt, auf „1“. Umgekehrt hat sich die Situation des anderen Unternehmens verschlechtert, da es nun verstärkt Ziel von Hacking-Angriffen wird – seine Auszahlung verschlechtert sich auf „-2“. Investieren beide Unternehmen in ein besseres Sicherheitssystem, profitieren sie nicht von einer Änderung der relativen Bedrohungslage, da der relative Aufwand durch Hacking für beide Unternehmen gleich geblieben ist, allerdings mussten beide in das neue System investieren – es resultiert die Auszahlungskombination „(-1, -1)“. Auch hier haben beide Unternehmen eine dominante Strategie – unabhängig von der Entscheidung des anderen Unternehmens ist es immer besser, in eine Verbesserung des Sicherheitssystems zu investieren. Allerdings ist das aus den dominanten Strategien resultierende Ergebnis nicht effizient: Hätten beide Unternehmen ihr Sicherheitssystem beibehalten, wäre ihre Auszahlung höher als nach der beiderseitigen Verbesserung. Es liegt hier die Struktur des Gefangenendilemmas vor (Bartholomae & Wiens 2016, 92f.) – beide treffen zwar für sich die beste, da dominante Entscheidung, berücksichtigen dabei aber nicht den negativen externen Effekt den sie für den jeweils anderen bewirken (Bartholomae & Wiens 2016, 90).

U1, U2	Beibehalten des Sicherheitssystem	Verbesserung des Sicherheitssystem
Beibehalten des Sicherheitssystems	(0 , 0)	(-2 , 1)
Verbesserung des Sicherheitssystem	(1 , -2)	(-1 , -1)

Quelle: Eigene Darstellung.

Tab. 2: Verbesserung der IT als Gefangenendilemma

Ein Gefangenendilemma kann dadurch gelöst werden, dass der negative Effekt bei der Entscheidung der Akteure internalisiert wird. Dies könnte durch eine Kooperation der Unternehmen auf eine gemeinsame Sicherheitstechnik erreicht werden. Verursacht die Verbesserung des Sicherheitssystems für jedes Unternehmen ohne Kooperation jeweils Kosten von C , so werden diese bei Kooperation von n Unternehmen dennoch nicht auf C/n sinken, da ein Sicherheitssystem, das mehrere Unternehmen abdeckt, auch mehr Cyberkriminelle dazu veranlassen wird, sich Zugang zu verschaffen. Allerdings werden die Kosten je Unternehmen geringer ausfallen als wenn jeder nur sein eigenes System verbessert – da sich die relative Bedrohung für die Unternehmen nicht ändert, wird mehr auf die Gesamtsicherheit des Systems geachtet, das heißt rationale Unternehmen werden bei einer Kooperation Gesamtkosten bis zu $C^* = nC$ akzeptieren.

6. Fazit und Handlungsempfehlungen

Bezogen auf die Wettbewerbsstrukturen zeigte sich, dass diese stark von der Digitalisierung betroffen sein können. In traditionellen Branchen kann es kurzfristig bei drastischen Kosteneinsparungen durch die Digitalisierung zu einer Monopolbildung kommen, während langfristig, wenn mehr Unternehmen in der Branche die Kosteneinsparungen realisieren, der Wettbewerb wieder zunehmen wird. Lediglich die Monopolbildung bei neuen Märkten ist zwiespältig zu betrachten. Zwar werden hier Märkte geschaffen, die es vorher nicht gab – beispielsweise eine weltweite Auktionsplattform wie im Falle von eBay –, wodurch ein Mehrwert für die Gesellschaft geschaffen wird. Allerdings verhindern immanente Eigenschaften von Informationsgütern, wie insbesondere die Netzwerkeffekte, dass sich ein Wettbewerb etabliert. Dies kann dazu führen, dass das langfristige Innovationspotential in diesen Märkten nicht ausgeschöpft wird.

In einem einfachen Modell wurde aufgezeigt, dass zur Realisierung ausreichender Kostenersparnisse, eine Mindestnutzung digitalisierter Informationen erforderlich ist, um die Fixkosten der Digitalisierung zu kompensieren. Dies ist insbesondere nur dann möglich, wenn alle Vorteile digitaler Informationen, wie der von Ort und Zeit losgelöste Online-Zugriff, erlaubt wird. Dennoch werden gerade kleinere Unternehmen nicht in der Lage sein, wirkliche Kostenersparnisse zu erzielen, wenngleich auch auf ihnen ein Digitalisierungsdruck lastet, der aus der (strategischen) Dominanz dieser Maßnahmen entsteht. Allerdings ergab die explizite Berücksichtigung der Risiken durch Cyberkriminalität, dass sich dadurch Digitalisierung als noch weniger vorteilhaft herausstellt, da nun berücksichtigt werden muss, dass Daten gehackt und enorme Schäden für das Unternehmen entstehen können. Bei nicht-linearen Anreizen der Cyberkriminellen und Kosten ergibt sich sogar, dass Digitalisierung gegebenenfalls sogar für große Unternehmen nachteilig sein kann, da der potenzielle Schaden bei ihnen deutlich höher ausfallen kann bzw. sie Investitionen in Sicherheitsmaßnahmen überproportional steigen.

Welche Handlungsempfehlungen lassen sich nur für Unternehmen ableiten? Berg (2018, 3) sieht für eine erfolgreiche digitale Transformation drei Punkte als essenziell an: die Entwicklung und Implementierung einer Digitalstrategie, ausreichenden Investitionen an Zeit und Geld sowie den Einsatz von Zukunftstechnologien. Aus der erfolgten Analyse lassen sich diese Bausteine weiter präzisieren.

Grundsätzlich müssen Unternehmen alle Vor- und Nachteile der Digitalisierung abwägen. Bei aller Euphorie gegenüber neuen Technologien und der sich scheinbar bietenden endlos neuen Möglichkeiten, gibt es doch auch viele Unsicherheiten und Kosten zu berücksichtigen, die sich etwa bereits bei der grundlegendsten Entscheidung, wie digitalisiert werden soll, zeigen. Hier ist etwa darauf zu achten, dass Softwarelösungen und Formate gewählt werden, die zwar zuallererst den eigenen Bedürfnissen gerecht werden müssen, aber dann auch kompatibel mit allen relevanten aktuellen und potenziell künftigen Geschäftspartnern. Andernfalls können die positiven Netzwerkeffekte nicht vollständig realisiert werden und es entstehen möglicherweise erheblich Konvertierungskosten.

Ist die Entscheidung zugunsten der Digitalisierung gefallen, ist zu prüfen, ob alle Bereiche gleichermaßen davon betroffen sein sollten. Angesichts der Gefährdung durch Cyberkriminalität ist es ratsam, trotz gegebenenfalls geringerer positiver Netzwerkeffekte, sensible Bereiche bei der Digitalisierung außen vorzulassen. Geschäfts- und Prozessgeheimnisse sind möglicherweise besser in einem physischen Safe geschützt als auf einem mit dem Internet verbundenen Computer, der somit weltweit gehackt werden kann und dadurch möglicherweise die Existenz des Unternehmens gefährdet. Im Abwägungsprozess bei der Digitalisierung muss daher auch immer berücksichtigt werden, welche Kosten entstehen, sollten diese Informationen in die falschen Hände geraten. Nur dann, wenn diese Kosten in einem akzeptablen Bereich sind und zudem ausreichend Effizienzsteigerungen durch die Digitalisierung entstehen, sollte diese angestoßen werden. Natürlich können auch Daten rein lokal und somit für potentielle Hacker unzugänglich gespeichert werden, allerdings wird dann nur ein Bruchteil der mit der Digitalisierung verbundenen Vorteile realisiert und es ist fraglich, ob der geringere Nutzenzuwachs die Kosten der Digitalisierung rechtfertigt.

Letztlich wird Digitalisierung nur dann wirklich für alle gewinnbringend sein, wenn ein Umdenken stattfindet – sowohl gesellschaftlich, was den richtigen Umgang mit Daten betrifft, als auch auf Unternehmensebene. Aus reinem Wettbewerb, der durch opportunistisch agierende Firmen gekennzeichnet ist, muss ein Kooperationswettbewerb (Coopetition) werden, in dem auch Konkurrenten, die miteinander in starkem Wettbewerb stehen, in grundsätzlichen Bereichen, wie dem Datenschutz oder der Datensicherheit, zusammenarbeiten, da nur so die Basis für eine effiziente und nachhaltige wirtschaftliche Entwicklung gewährleistet werden kann.

Um die Transformationsphase zu diesem eher langfristigen Ziel zu nutzen und auch kurz- bis mittelfristig eine Verbesserung der Bedingungen zu erreichen, ist wiederum die Politik gefordert, dafür zu sorgen, dass die Chancen der Digitalisierung genutzt werden können bei gleichzeitiger Abmilderung der Risiken. Chancen gehen vor allem dadurch verloren, dass der Wirtschaft immer weniger qualifizierte Arbeitskräfte zur Verfügung stehen und derzeitige Mitarbeiter, insbesondere aus der Babyboomer-Generation, über nur mangelnde Digitalkompetenz verfügen (Rohler & Schulte 2017, 13). Entsprechen sind Rahmenbedingungen zu schaffen, welche diese Situation verbessern (beispielsweise mehr Investitionen in digitale Infrastrukturen in Bildungseinrichtungen, gezielte Förderungen in Jobcentern, Förderung qualifizierter Einwanderung, u.ä.). Die Reduktion von Risiken kann hauptsächlich durch eine Verbesserung des institutionellen Rahmens erreicht werden, um Cyberkriminelle und Hacker effizienter abzuschrecken. Härtere Strafen und verbesserte Strafverfolgung führen zwar zu höheren Kosten, senkt aber dennoch die Kosten je Bürger und Unternehmen, da weniger in Sicherheit investiert werden muss.

Wenngleich diese Handlungsempfehlungen aus deutscher Sicht argumentiert wurden, stellen sie nichtsdestotrotz auch allgemeingültige globale Empfehlungen dar. Insbesondere Cyberkriminalität stellt ein grenzüberschreitendes Problem dar, sodass zudem eine internationale Zusammenarbeit sowie eine Verbesserung aller strafverfolgenden Institutionen weltweit unverzichtbar ist (Bartholomae 2018b).

Literatur

- Akerlof, G. A. (1970): The Market for “Lemons”: Quality Uncertainty and the Market Mechanism, *The Quarterly Journal of Economics*, 84 (3), 488-500.
- Allianz (2019). Allianz Risk Barometer—Top Business Risks for 2019. München: Allianz Global Corporate & Specialty SE, url: https://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2019.pdf.
- Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. & Zaharia, M. (2010): A View of Cloud Computing, *Communications of the ACM*, 53, 50–58.
- Ba, S., Whinston, A. B. & Zhang, H. (2000): Small Companies in the Digital Economy, in: Brynjolfsson, E. & Kahin, B. (Hrsg.): *Understanding the Digital Economy. Data, Tools, and Research*, Cambridge, MA: The MIT Press, S. 185-200.
- Bachmann, M., Shahd, M. & Grimm, F. (2015): Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter, Berlin: Bitkom e.V., url: <https://tinyurl.com/bitkom2015>.
- Bartholomae, F. (2012): Social Games: Im Netz von Facebook, *Wirtschaftsinformatik & Management*, 5/2012, 28-33.
- Bartholomae, F. (2014): Der Markt für Social Games, *Der Betriebswirt*, 2/2014, 23-28.
- Bartholomae, F. (2018a): Cybercrime and Cloud Computing. A Game Theoretic Network Model, *Managerial and Decision Economics*, 39 (3), 297-305.
- Bartholomae, F. (2018b): Digital Transformation, International Competition and Specialization, *CESifo Forum*, 19 (4), 23-28.
- Bartholomae, F. & Wiens, M. (2016): *Spieltheorie. Ein anwendungsorientiertes Lehrbuch*, Wiesbaden: Springer Gabler.
- Berg, A. (2018): *Digitalisierung der Wirtschaft*, Berlin: bitkom.
- Cremonini, M. & Nizovtsev, D. (2006): Understanding and influencing attackers’ decisions: Implications for security investment strategies, in: *Proceedings of 5th Workshop on the Economics of Information Security (WEIS 2006)*, Cambridge (UK).
- DIHK (2017): *Wachsende Herausforderungen treffen auf größeren Optimismus. Das IHK-Unternehmensbarometer zur Digitalisierung 2017*, Berlin: DIHK.
- Gilbert, R. J. & Newbery, D. M. G. (1982): Preemptive Patenting and the Persistence of Monopoly, *The American Economic Review*, 72 (3), 514-526.

- Katz, M. & Shapiro, C. (1985): Network Externalities, Competition, and Compatibility, *The American Economic Review*, 75 (3), 424-440.
- Kopke, C., Petri, A., Kob, T., Sopha, S. M., Holz, W., Seyerlein-Klug, A., Schulz, M., Geschonneck, A., Kröger, S. & Münstermann, M. (2016): Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie, Berlin: Bitkom e.V., url: <http://tinyurl.com/bitkom2016>.
- Krämer, Hagen (2019): Digitalisierung, Monopolbildung und wirtschaftliche Ungleichheit, *Wirtschaftsdienst*, 99(1), 47-52.
- Kshetri, N. (2006): The Simple Economics of Cybercrimes, *IEEE Security & Privacy*, 4(1), 33-39.
- Kshetri, N. (2010): The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives. Heidelberg: Springer.
- Linde, F. (2005): *Ökonomie der Information*, Göttingen: Universitätsverlag Göttingen.
- Linde, F. (2009): Ökonomische Besonderheiten von Informationsgütern, in: Keuper, F. & Neumann, F. (Hrsg.): *Wissens- und Informationsmanagement. Strategie, Organisation und Prozesse*, Wiesbaden: Gabler, S. 291-320.
- Linde, F. & Stock, W. G. (2011): *Information Markets. A Strategic Guideline for the I-Commerce*, Berlin: De Gruyter.
- Nazir, M. (2012): Cloud Computing: Overview & Current Research Challenges, *IOSR Journal of Computer Engineering*, 8, 14-22.
- Pindyck, R.S. & Rubinfeld, D.L. (2003): *Mikroökonomie*, 5., aktual. Aufl., München: Pearson.
- Rholeder, B. & Schulte, K.-S. (2017): *Digitalisierung des Handwerks*, Berlin: bitkom.
- Shapiro, C. & Varian, H. R. (1999): *Information Rules. A Strategic Guide to the Network Economy*, Boston, MA: Harvard Business Review Press.
- Shy, O. (2001a): *The Economics of Network Industries*, Cambridge, MA: Cambridge University Press.
- Shy, O. (2001b): *Industrial Organization. Theory and Applications*, Cambridge, MA: The MIT Press.
- Shy, O. (2011): A short Survey of Network Economics, *Review of Industrial Organization*, 38, 119-149.
- ZDH (2018): *Digitalisierung der Handwerksbetriebe. Ergebnisse einer Umfrage unter Handwerksbetrieben im ersten Quartal 2018*, Berlin: ZDH.
- Zhang X.-Z., Liu J.-J. & Xu Z.-W. (2015): Tencent and Facebook Data Validate Metcalfe's Law, *Journal of Computer Science and Technology*, 30 (2), 246–251.