emergenCITY

Resiliente Informations- und Kommunikationstechnologie für ein krisenfestes Deutschland

Autorenteam:
Matthias Hollick, Jens Ivo Engels, Cornelia Fraune,
Bernd Freisleben, Gerrit Hornung, Michèle Knodt, Max Mühlhäuser

emergenCITY Policy Paper No. 1 | Oktober 2020
DOI: doi.org/10.5281/zenodo.4066319
policy@emergencity.de | www.emergencity.de
emergenCITY | die resiliente digitale Stadt | LOEWE-Zentrum

LOEWE
Exzellente Forschung für Hessens Zukunft

Executive Summary

Die aktuelle Corona-Krise verdeutlicht: Deutschland ist katastrophengefährdet. Informations- und Kommunikationstechnologie (IKT) spielt bei der Reaktion auf diese Krise und bei ihrer fortdauernden Bewältigung eine entscheidende Rolle. Der hohe Nutzen von IKT in der Krise begründet damit gleichzeitig aber auch eine starke Abhängigkeit von IKT.

Angesichts der steigenden Bedeutung von IKT in allen gesellschaftlichen Bereichen muss sichergestellt werden, dass IKT mit Funktionsstörungen und -beeinträchtigungen während einer Krise umgehen kann. Über IT-Sicherheit und Ausfallsicherheit hinaus muss IKT in die Lage versetzt werden, mit erheblichen System-Beeinträchtigungen, wie Überlastungen, technischen Fehlern, Cyberangriffen, längeren Stromausfällen oder materiellen Schäden, zurechtzukommen.

Hält die IKT solchen Belastungen nicht stand, so führt dies zum Zusammenbruch von kritischen Infrastrukturen (KRITIS). IKT vernetzt unterschiedliche KRITIS und schafft damit Interdependenzen, die im schlimmsten Fall zu kaskadierendem Versagen führen können.

Seit Jahren zeigt IKT eine steigende Fragilität und abnehmende Resilienz, verursacht u. a. durch (i) Effizienz als primäres Optimierungsziel, die aufwändige Resilienzmaßnahmen verhindert; (ii) fehlende Diversität in vielen IKT-Systemen, die großflächige, systemweite und anbieterübergreifende Ausfälle begünstigt; (iii) fehlender Einbau der Möglichkeit eines “Notbetriebs”; (iv) Fehlen angemessener Governanceprozesse; und (v) nicht auf IKT-Resilienz fokussierte Regulierungsmechanismen.

Um eine nachhaltig verlässliche IKT für ein krisenfestes Deutschland zu schaffen, empfehlen wir:

1. Resilienz und Effizienz müssen gleichrangige Optimierungsziele sein, d.h. Effizienzverbesserungen müssen unter Wahrung hinreichender Resilienzvorgaben erfolgen.
2. IKT-Systeme müssen redundant, divers und für den Krisenfall adäquat dimensioniert sein.
3. IKT-Systeme müssen wandlungsfähig konzipiert werden, um sich an eine Krise anpassen und die zur Bewältigung notwendigen Funktionalitäten zur Laufzeit ausbilden zu können.
4. Resilienzvorgaben müssen durch Prozesse der positiven Koordination auf den jeweiligen Ebenen sowie ebenenübergreifend erarbeitet werden.
5. Mittels technikadäquater Regulierung müssen Resilienzvorgaben gemacht werden, unter deren Wahrung eine Effizienzoptimierung nach Marktregeln erfolgen kann.

Es ist aus unserer Sicht dringend notwendig, die Resilienz heutiger und künftiger Informations- und Kommunikationstechnologie (IKT) zu erhöhen und nachhaltig zu gewährleisten. Wir bezeichnen IKT als resilient, wenn sie trotz signifikanter Beeinträchtigungen eine akzeptable Mindest- bzw. Ersatzfunktionalität aufrechterhalten kann und für die zügige Rückkehr zum Normalverhalten gerüstet ist.

Vulnerabilität unserer Hightech-Gesellschaft im Krisenfall durch Fragilität von IKT

Unsere moderne Gesellschaft zeichnet sich durch anpassungsfähige und effiziente (kritische) Infrastrukturen (KRITIS) in den Sektoren Energie, Informations- und Kommunikationstechnologie, Verkehr und Logistik, Gesundheit, Ernährung, Wasser, Finanz- und Versicherungswesen, sowie Staat und Verwaltung aus. Entscheidend für die Anpassungsfähigkeit und Effizienz ist der allgegenwärtige Einsatz von IKT, der durch Synergie- und Netzwerkeffekte zu disruptiven Verbesserungen führt, aber auch die Interdependenzen zwischen den KRITIS-Sektoren verstärkt. Gleichzeitig werden nichtöffentliche Bereiche wie Privathaushalte, Individualverkehr und Wirtschaft verstärkt und mit hoher Innovationsfrequenz von IKT durchdrungen.

Der störungsfreie und nahtlose Betrieb von Infrastruktursystemen repräsentiert das Selbstverständnis und den Zustand der technischen, sozialen und politischen Stabilität hochtechnisierter Gesellschaften. Mit IKT durchsetzte sozio-technische Systeme ermöglichen die vereinfachte Zirkulation von Personen, Gütern, Stoffen und Informationen.

Signifikante Systemschwankungen, Schock- oder Krisenereignisse (nachfolgend als Krisen bezeichnet) bedrohen diesen Zustand, indem sie die Verfügbarkeit der (kritischen) Infrastrukturen beeinträchtigen. Ein systematisches Verständnis der Verwundbarkeit einer von IKT durchdrungenen Gesellschaft und wirksame Maßnahmen zur Erhöhung ihrer Resilienz sind dringend erforderlich, fehlen aber bisher. Ein besonderer Schwerpunkt der nachfolgenden Betrachtung liegt hierbei auf digitaler Kommunikation. Sie fungiert als “Nervensystem” moderner Informationssysteme und damit unserer zunehmend digitalisierten Gesellschaft und vernetzt alle weiteren Infrastrukturen miteinander. Damit werden erhebliche Abhängigkeiten begründet. Viele der hieraus gewonnenen Erkenntnisse sind darüber hinaus für IKT im Allgemeinen gültig.

Die Rolle von IKT in Krisen

Krisen verändern die Rahmenbedingungen für IKT und zeigen die (nicht/teilweise) zu beobachtende Resilienz existierender IKT-Infrastrukturen zum adäquaten Umgang mit diesen neuen Rahmenbedingungen. Gleichzeitig kann IKT jedoch auch den Umgang mit Krisen verbessern. Nachfolgend veranschaulichen wir die Auswirkung von Krisen auf IKT anhand drei ausgewählter Krisenszenarien:

Naturereignisse: Infolge des Tohoku-Seebebens vor Japan und des darauf folgenden Tsunamis im Jahr 2011 stieg der Kommunikationsverkehr direkt nach dem Schadenseintritt um den Faktor 50 bis 60 an. Gleichzeitig war die Kommunikationsinfrastruktur in den betroffenen Landesteilen großflächig zerstört. Aufgrund des hohen Kommunikationsbedarfs musste die Nutzung für 80 bis 90% der Festnetztelefone und 70 bis 95% der Mobiltelefone eingeschränkt werden. Diese Beschränkungen bestanden insbesondere im Mobilfunknetz in der kritischen Phase nach der Katastrophe, da Mobilkommunikation *das* Mittel der Wahl für die Bevölkerung war. Paketbasierte Kommunikation wie Kurznachrichten wurden zwar weniger beschränkt, aufgrund der hohen Last allerdings verzögert ausgeliefert. Der aus dem Tsunami resultierende Kollaps fast aller kritischen Infrastrukturen behinderte die Reaktion

auf die Krise und verzögerte deren Bewältigung. Bevölkerung, Unternehmen und staatliche Einrichtungen waren hiervon gleichermaßen und über Wochen hinweg betroffen. Der gesamtwirtschaftliche Schaden ohne Berücksichtigung des Fukushima-Kernkraftwerkes wurde auf rund 240 Mrd. US-Dollar beziffert.

Auch Naturkatastrophen wie Starkwetterereignisse können zu einem Totalausfall der Kommunikationsnetze in den betroffenen Gebieten führen, wie bspw. nach dem Taifun Haiyan auf den Philippinen in 2013 oder der Hurrikan-Saison 2017 in den USA in Texas, Florida und Puerto Rico. Insbesondere in der Reaktionsphase nach Kriseneintritt wurde hierdurch die Bergung und Rettung von Betroffenen erheblich erschwert. Während in Texas und Florida das Netz vergleichsweise schnell wieder etabliert werden konnte, vergingen auf den Philippinen und in Puerto Rico teilweise Monate, bevor eine verlässliche Kommunikation der Bevölkerung wieder möglich war. Ein entscheidender Faktor für die Verwundbarkeit von Kommunikationsnetzen ist deren Zentralisierungsgrad. Ein zentral optimierter Netzbetrieb hilft Effizienzgewinne zu realisieren, wirkt aber der Resilienzerhöhung entgegen, da ein Ausfall systemkritischer zentraler Komponenten als *"single point of failure"* einen Komplettausfall des Systems nach sich ziehen kann.

Blackouts: Der Stromausfall im gesamten Nordosten der USA vom August 2003 betraf rund 50 Mio. Bürgerinnen und Bürger in acht US-Staaten und zwei kanadischen Provinzen. Er dauerte regional bis zu zwei Tage an und verursachte volkswirtschaftliche Kosten von 7 bis 10 Mrd. US-Dollar. Grund war eine komplexe Mischung aus elektrischen, betrieblichen und IKT-spezifischen Problemen, die zu sich gegenseitig verstärkenden Effekten und zu kaskadierenden Ausfällen führten. Auf Grund fehlerhafter IKT-Anwendungen lagen fehlerhafte Lagebildinformationen vor, die zu menschlichen Fehlentscheidungen des Betriebspersonals führten. Der Stromausfall hatte Auswirkungen insbesondere auf die IKT und damit auf sämtliche Infrastrukturen. Die Effekte waren dramatisch und betrafen Wasserversorgung (Ausfall elektrischer Pump- und Leitsysteme), Transport, Verkehr und Logistik (Ausfall von Bahnsystemen, Verkehrsleitsystemen, Lieferketten), Gesundheitswesen (Notbetrieb in Krankenhäusern) und Nahrungsmittelversorgung (Ausfall von Bezahlsystemen).

Über großflächige Stromausfälle wird regelmäßig berichtet. So waren im August 2019 mehr als 100 Millionen Menschen von einem Blackout auf Indonesien betroffen, der je nach Region zwischen 9 und 20 Stunden anhielt und das öffentliche Leben massiv beeinträchtigte. In den meisten Fällen sind Kommunikationsnetze nur für kurzzeitige Unterbrechungen der Energieversorgung gerüstet: damit ist die KRITIS IKT direkt von Blackouts betroffen. Diese Abhängigkeit wirkt sich somit auch auf weitere durch IKT vernetzte KRITIS aus, selbst wenn diese für einen Stromausfall gerüstet sind. Umgekehrt kann die Abhängigkeit Energie–Kommunikation genutzt werden, um aus Kommunikationsausfällen auf Stromausfälle zurückzuschließen.

SARS-CoV-2 und COVID-19: IKT als kritische Infrastruktur war in der aktuellen Corona-Krise bislang überwiegend verfügbar. Die Bevölkerung nutzte IKT in hohem Maße für die Reaktion auf die Krise. Auch die aktuelle Krisenbewältigung ist stark durch den Einsatz von IKT-Systemen geprägt. Kommunikationsnetze und Datenzentren konnten den gestiegenen Datenverkehr bisher gut bewältigen und ermöglichten damit bspw. eine nahezu nahtlose Transition weiter Teile unserer Gesellschaft in die Heimarbeit. Die Verteilung des Datenverkehrs im Internet hat sich infolge der Corona-Krise in kürzester Zeit deutlich geändert. Eine

abrupte Verschiebung des Datenverkehrs während der üblichen Geschäftszeiten hin zu privaten Teilnehmeranschlüssen fand statt. Ähnliche Verlagerungen der Nutzungsarten vollziehen sich im Normalfall eher in Monaten bis Jahren. Insbesondere stieg die Internetnutzung in Privathaushalten für Telearbeit, Handel und Ausbildung, aber auch für Unterhaltung.

Die Zugangsnetze und das Internet waren für den dadurch erzeugten eher moderaten Anstieg um rund 15 bis 20% innerhalb einer Woche gut gerüstet, auch da das jährliche Wachstum des Datenverkehrsaufkommens im Internet in der jüngeren Vergangenheit rund 30% betrug. In einer künftigen Krise kann der Zuwachs aber durchaus stärker ausfallen und damit die Funktionsfähigkeit der IKT infrage stellen. Gleichzeitig sind, auch während der aktuellen Corona-Krise, fortlaufende Cyberangriffe auf IKT in privaten und öffentlichen Bereichen sowie KRITIS zu verzeichnen, die die Verfügbarkeit von IKT bedrohen. Die Schadenshöhe dieser Angriffe wird von BITKOM für 2018/19 auf mehr als 100 Mrd. EUR jährlich geschätzt.

Resilienz *für* und *durch* IKT

Unsere Empfehlungen zielen darauf ab, die Krisenresilienz unserer Gesellschaft nachhaltig zu erhöhen. Dabei kommt den (kritischen) Infrastrukturen eine Schlüsselrolle zu: Ohne resiliente KRITIS kann auch die Gesellschaft insgesamt nicht resilient werden. Mit unseren Empfehlungen sollen die KRITIS unter Einsatz von IKT auf ein krisenfestes Maß gehoben werden. Dies setzt voraus, dass die IKT selbst resilient ist: Als übergeordnetes Ziel muss unsere IKT jederzeit verfügbar, verständlich und beherrschbar bleiben, um im kompletten Verlauf einer Krise deren Management bestmöglich zu unterstützen (vgl. Abbildung 1).

Neben unseren Empfehlungen existieren eine Reihe von offenen Forschungsfragen, die in diesem Policy Paper nicht weiter detailliert werden. So sind bspw. die Abhängigkeit zwischen IKT und anderen KRITIS sowie die komplexen Systemzusammenhänge vernetzter KRITIS bisher nur unzureichend untersucht worden. Forschungsbedarf besteht ebenfalls hinsichtlich der verbesserten Messbarkeit und Bewertbarkeit von IKT-Resilienz, die Voraussetzung für eine gezielte Resilienzerhöhung auf ein vorgegebenes Maß ist.

Resilienz bezeichnet die Fähigkeit eines Systems, Krisen zu *absorbieren*, sich von diesen *zeitnah und nachhaltig zu erholen* oder durch *Wandlung* vergleichbare bzw. neuartige Funktionsfähigkeit zu erlangen:

- Absorption durch Widerstandsfähigkeit, Elastizität und Anpassungsfähigkeit
- Erholung durch Rückführung in den Normalzustand (short-term coping, bouncing back)
- Wandlung durch Überführung/Substitution (long-term coping, bouncing forward)
- Nachhaltigkeit durch Lernen aus der Krise sowie Reifung und Weiterentwicklung (improving)

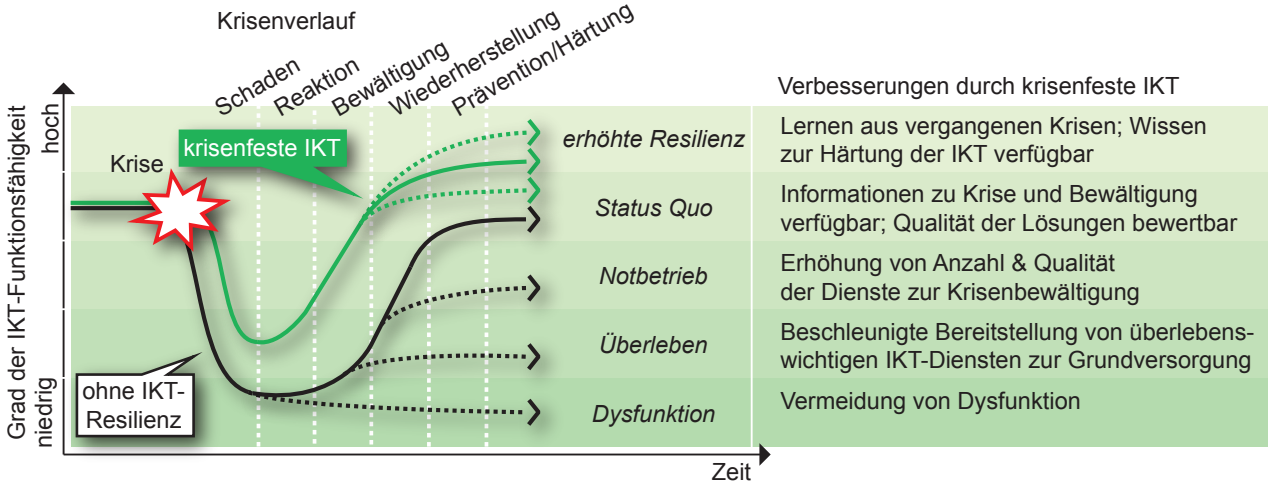

Abbildung 1. Krisenmanagement mit IKT-Unterstützung: Schematische Darstellung des Krisenverlaufs für resiliente vs. herkömmliche IKT-Systeme.
Ausgehend vom Normalbetrieb beeinträchtigt eine Krise die Funktionsfähigkeit von KRITIS. Eine Erhöhung der IKT-Resilienz verspricht, den Umgang mit der Krise in sämtlichen Phasen des Krisenverlaufs zu verbessern. Das während der Krise gewonnene Wissen dient dazu, die IKT zu härten und Prävention für künftige Krisen zu ermöglichen.

Empfehlung: Resilienz gleichrangig mit Effizienz

Resilienz und Effizienz müssen als gleichrangige Optimierungsziele gesetzt werden. Im Rahmen der fortschreitenden digitalen Transformation muss in einem ersten Schritt ein Bewusstsein für die Erforderlichkeit von Resilienz und ein hinreichendes Maß an Resilienz geschaffen werden. Effizienzverbesserungen müssen unter Wahrung von Resilienzvorgaben erfolgen, ohne dabei automatisch für alle Anwendungsbereiche nach höchstmöglicher Resilienz zu streben. Die Fähigkeit von IKT, auch mit unvorhergesehenen Störungen umgehen zu können, muss eine inhärente Systemeigenschaft werden. Hierzu ist es notwendig, redundante aber gleichzeitig diversifizierte Systeme zu betreiben und Überkapazitäten bereitzuhalten. Die Ertüchtigung kritischer Infrastrukturen durch resiliente IKT bereitet uns besser auf den Umgang mit künftigen Krisen vor. Energie- und Kommunikationsnetze müssen einen echten Notbetrieb und einen nahtlosen Übergang zurück zum Normalbetrieb unterstützen. Lösungsansätze, die hybride Netzarchitekturen beinhalten, d.h. einen schnellen Zerfall in autonome Inselnetze und deren schrittweise Vereinigung zu Verbundnetzen – sowohl für den Kommunikations-, als auch den Energiesektor – ermöglichen, können eine nachhaltige Resilienzsteigerung herbeiführen.

Das Prinzip der Gleichrangigkeit von Resilienz und Effizienz stellt eine Herausforderung an bisherige Grundsätze sowohl der ingenieurtechnischen Entwicklung, als auch an Wirtschaftlichkeitserwägungen dar. Hier ist nichts weniger als ein Paradigmenwechsel erforderlich, der allen Akteuren tiefgreifendes Umdenken abverlangt.

Empfehlung: Redundanz, Diversität und Überkapazität

IKT-Systeme folgen häufig gleichartigen Konstruktionsprinzipien und basieren auf identischen Basiskomponenten (z.B. Prozessoren, Betriebssysteme, Internet-Technologie). Die Systeme der Marktführer sind dabei oftmals geschlossen und proprietär. Um großflächigen, systemweiten und anbieterübergreifenden Ausfällen entgegenzuwirken, ist es notwendig, dass Systeme ein ausreichendes Maß an Redundanz und Diversität besitzen. Für den Bereich der Kommunikationsnetze gilt es, heterogene und redundante Netzzugangstechnologien bereitzustellen (Festnetze, zellulare, aber auch zentrale drahtlose Netze, Satellitennetze etc.), die technisch wie organisatorisch unabhängig voneinander betrieben werden.

Redundanz wirkt einzelnen Ausfällen entgegen. Hierbei können insbesondere dezentrale IKT-Ressourcen einen Beitrag zur Resilienzsteigerung leisten, wenn diese im Krisenfall weiter funktionsfähig bleiben. Heterogenität bzw. Diversität verhindert, dass Fehler oder Angriffe alle Systeme gleicher Konstruktionsart beeinträchtigen oder durch die Abhängigkeit von einzelnen Anbietern lock-in Effekte bzw. Pfadabhängigkeiten entstehen. Offenen Systemen (Open Source Software/Hardware) kommt hierbei eine besondere Rolle zu, da sie die Abhängigkeiten gegenüber marktbeherrschenden Anbietern reduzieren können. Für die zu erwartenden Lastspitzen im Krisenfall muss eine strategische Überkapazität bereitgehalten werden, d.h. die Systeme müssen nicht für den durchschnittlichen Betriebsfall, sondern für den Krisenfall dimensioniert werden.

Empfehlung: Wandlungsfähigkeit von IKT

COVID-19 zeigt: Wir wissen im Vorhinein nicht, welche Krisen uns erwarten und welche Herausforderungen sie an uns stellen werden. Um zukunftsfähig zu sein, müssen IKT-Systeme daher funktional wandlungsfähig sein, um sich an eine Krise anzupassen. Ziel ist es, dass auch derzeit eingesetzte Systeme die zur Bewältigung notwendigen Funktionalitäten zur Laufzeit ausbilden können, selbst wenn diese zum Entwurfszeitpunkt nicht geplant und implementiert wurden. In IKT-Systemen kann hierdurch ein Notbetrieb ermöglicht werden, der die für den Umgang mit der Krise notwendige Mindest- bzw. Ersatzfunktionalität bereitstellt. Darüber hinaus können notwendige Synergien zwischen KRITIS auch im Krisenfall weiter genutzt bzw. erschlossen werden und somit kaskadierende Fehlerketten vermieden werden. Beispielsweise benötigen Energienetze IKT zur Koordination. Ein geeigneter Notbetrieb von Kommunikationsnetzen kann damit helfen, die Energieversorgung sicherzustellen und damit weitere KRITIS zu schützen, die ihrerseits von der KRITIS Energie abhängen. Eine Reihe von technologischen Ansätzen können hierzu Beiträge leisten: Software-definierte Systeme bieten hohe Adaptivität und Wandlungsfähigkeit, offene Hardware und Software unterstützen die Verständlichkeit und Beherrschbarkeit und ermöglichen im Krisenfall niederschwellig Anpassungsmaßnahmen bzw. Weiterentwicklungen. Technologische Souveränität ist daher ein weiterer wichtiger Baustein, um die Wandlungsfähigkeit von IKT im Krisenfall zu ermöglichen.

Empfehlung: Governance

Die Transformation hin zu einer resilienten IKT vor allem durch Resilienzvorgaben wird Probleme des kollektiven Handelns erbringen, denn sie wird gleichzeitig Aufgabe der europäischen, Bundes-, Landes- und lokalen Ebene sein und in der Umsetzung nicht ohne Kooperation mit den betroffenen privaten Akteuren auskommen. Diese Herausforderungen werden von der politikwissenschaftlichen Governanceforschung adressiert, welche Interdependenzen in der Problemlösung zwischen unabhängigen Akteuren, hier Staat und privatwirtschaftliche Akteure, auf mehreren Ebenen in den Blick nimmt. Hier empfehlen wir auf den jeweiligen Ebenen sowie ebenenübergreifend Prozesse der positiven Koordination. Die kooperative Bearbeitung von Produktions- und Verteilungsproblemen wird mittels positiver Koordination ermöglicht, indem die beteiligten Akteure sich gemeinsam auf Resilienzvorgaben einigen und auf dieser Grundlage dann Verteilungsfragen verhandeln. Im Gegensatz zur negativen Koordination beruht positive Koordination somit auf einer gemeinsamen Problemdefinition, welche den kollektiven Nutzen, bzw. das Gemeinwohl einer Strategie berücksichtigt. Der kooperative Ansatz, der seit einigen Jahren im Hinblick auf den Schutz kritischer Infrastrukturen verfolgt wird und auch im Rahmen der Entwicklung des IT-Sicherheitsgesetzes zum Tragen kam, muss auch in der Netzinfrastrukturpolitik etabliert werden.

Empfehlung: Resilienzvorgaben durch Regulierung

Aufbauend auf Strategien positiver Koordination erfordert umfassende Resilienz eine technikadäquate Regulierung. Marktförmige Mechanismen allein sind nicht geeignet, um Resilienz und Effizienz gleichrangig zu optimieren, da der Anbieter eines effizienten, aber nicht resilienten Systems üblicherweise Wettbewerbsvorteile durch Kostenersparnisse beim Aufbau sowie Betrieb realisieren kann. Mittels Regulierung können jedoch Resilienzvorgaben gemacht werden, unter deren Wahrung eine Effizienzoptimierung nach Marktregeln erfolgen kann. Hierzu gibt es eine Reihe von Ansatzpunkten. Im Verbraucherbereich können entsprechende Resilienzvorgaben im Rahmen von Produktzertifizierung erfolgen und damit einen Regulierungsrahmen für alle Anbieter bieten. Für den Bereich der KRITIS gelten bereits verschärfte Regeln im Bereich der IT-Sicherheit, aber nicht für das umfassendere Ziel der Resilienz. Weiterführend empfehlen wir, die Betreiberpflichten um die bisher nur in Teilen betrachteten Systemabhängigkeiten und hieraus hervorgehenden Kaskadeneffekte noch stärker zu berücksichtigen. Dies kann gestärkt werden durch rechtliche Transparenzpflichten wie bspw. die Pflicht der gegenseitigen Information über Risiken, Abhängigkeiten sowie Vorfälle. Normative Anforderungen könnten einen wichtigen Beitrag leisten, um Resilienz zu einer verpflichtenden Eigenschaft von IKT-Systemen zu machen. Dieses Potenzial wird bisher noch nicht hinreichend ausgeschöpft.

Schlussbemerkung

Es ist aus unserer Sicht dringend notwendig, die **Resilienz heutiger und künftiger IKT-Infrastrukturen zu erhöhen und nachhaltig sicherzustellen**. Wir benötigen Resilienz *für* und *durch* IKT. Nur resiliente IKT kann im Sinne einer Allgefahrenabwehr sicherstellen, dass unsere Gesellschaft im Krisenfall handlungsfähig bleibt; gleichzeitig zeigt die aktuelle Corona-Krise, dass eine funktionierende IKT die Resilienz der Gesellschaft signifikant erhöhen kann.

Wir möchten die Dringlichkeit der in diesem Policy Paper behandelten Thematik nachdrücklich hervorheben. Deutschland liegt international nicht im Spitzenfeld bei der Digitalisierung von Infrastrukturen und generell in der öffentlichen Verwaltung. Um als führende Industrienation international wettbewerbsfähig zu bleiben, müssen in den nächsten Jahren große Anstrengungen zur Erneuerung dieser Infrastrukturen unternommen werden. Wir müssen Infrastrukturen dabei im Kern digital denken. Um gleichzeitig die Krisenfestigkeit dieser Infrastrukturen zu erreichen, muss IKT-Resilienz nachhaltig gewährleistet werden. Lösungen hierfür "aus der Schublade" existieren in weiten Teilen nicht, vielmehr besteht ein hoher Forschungs- und Entwicklungsbedarf, um **Resilienz für und durch IKT** zu erreichen sowie solide Grundlagen für die Betrachtung von Resilienz in komplexen und vernetzten IKT-Systemen bereitzustellen. Eine abgestimmte Governance und die verbindliche Festsetzung von Resilienzvorgaben durch Regulierung sind dabei notwendige Begleitmaßnahmen.