Kompetenzzentrum Öffentliche IT

Forschung für den digitalen Staat

Abb. 2

Dr. Karoline Krenn, Gabriele Goldacker, Jana Plomin

Resilienz im digitalen Kontext

Im digitalen Kontext wird Resilienz oft und zugleich sehr verschieden thematisiert: Sei es, indem Digitalisierung in verschiedenen Zusammenhängen als Resilienz steigernd beschrieben wird, oder sei es, dass Digitalisierungsprozesse oder der Umgang mit Digitalem resilient gegenüber Herausforderungen sein sollen.

Um sich der Breite des Themas zu nähern, erscheint zunächst eine Definition hilfreich: Laut Duden ist Resilienz »psychische Widerstandskraft; Fähigkeit, schwierige Lebenssituationen ohne anhaltende Beeinträchtigung zu überstehen«. Verallgemeinert lässt sich Resilienz als Widerstandsfähigkeit der Gesellschaft, von Organisationen und Individuen angesichts von Störungen, Krisen oder Vulnerabilitäten verstehen. Dabei wird davon ausgegangen, dass es neben Normalzuständen »kritische« Ausnahmezustände gibt. Resilienz bedeutet dann, effektiv und effizient zum Normalzustand zurückkehren bzw. sich anpassen und nachhaltig einen neuen, akzeptablen Zustand erlangen zu können. Noch allgemeiner wird Resilienz als Fähigkeit verstanden, auf kritische Entwicklungen, Ereignisse oder Zustände (»kEEZ«) beliebiger Art so zu reagieren, dass Schäden und Nachteile vermieden werden und Chancen zur eigenen Weiterentwicklung nicht ungenutzt bleiben. Krisen können so zum Katalysator für Wandel werden.

Resilienz wird in einem gestaffelten Aktionsraum entwickelt. Es geht um konkrete Vorbereitung auf erwartbare Störungen, aber auch um Strategien für unvorhergesehene Ereignisse. Im Kern müssen kEEZ antizipiert und deren Bewältigung in Form von Wiederherstellung, Anpassung oder Vermeidung auf verschiedenen sozialen Ebenen wie Teams, Organisationen oder übergreifenden Allianzen vorbereitet und organisiert werden (s. Abb. 1).

Resilienz steigernde Maßnahmen sollten stets anhand einer Bewertung der möglichen kEEZ-Folgen auf Basis gemeinschaftlich akzeptierter Werte vereinbart werden.

Dieser Impuls soll das Bild schärfen, welche

- Phänomene im Schnittbereich von Digitalität und Resilienz zu beobachten sind,
- Maßnahmen zur Erreichung bzw. Steigerung von Resilienz jeweils förderlich sind und
- Kräfte und Allianzen es zur Vermeidung negativer kEEZ-Folgen braucht.

Resilienz im digitalen Kontext stellt sich für uns als elastisches Bauwerk dar (s. Abb. 2), das aus einem Dach – dem Ziel bzw. Versprechen – besteht, welches auf drei Säulen – den notwendigen Voraussetzungen für die stabile Lage des Daches – ruht.

Das Dach: Resilienz durch Digitalisierung und Digitalität

Digitalisierung und Digitalität versprechen primär, zur Lösung gesellschaftlicher, organisationaler oder individueller Herausforderungen beizutragen, also die Resilienz gegenüber diesen zu erhöhen (oder überhaupt erst herzustellen).

Die Säulen

Das Dach kann Resilienz allerdings nur dann fördern, wenn die Digitalisierungsprozesse und das Digitale (Produkte, Dienstleistungen, Infrastrukturen usw.) selbst resilient sind und wirkungsvolle Strategien für den Umgang mit den Herausforderungen der Digitalität existieren.

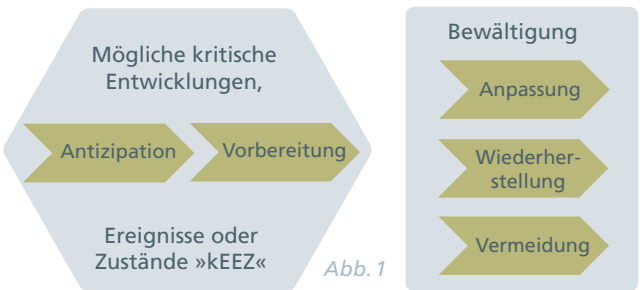

Abb. 1

Das Dach: Resilienz durch Digitalisierung und Digitalität

Primärer Anspruch bzw. primäres Versprechen Resilienz fördernder Digitalisierung und Digitalität ist, gesellschaftliche, organisationale oder individuelle Herausforderungen zu lösen oder zu verringern bzw. zu solchen Lösungen beizutragen, also die Resilienz gegenüber diesen Herausforderungen zu erhöhen (oder überhaupt erst herzustellen).

Moderne Gesellschaften stehen vor vielfältigen Herausforderungen, die gleichzeitig und auf verschiedenen Ebenen angegangen werden müssen. Für viele der Herausforderungen liefert die Digitalisierung bzw. die daraus resultierende (teilweise) Digitalität zumindest einen Beitrag zur Lösung:

Erderwärmung verringern bzw. Folgen reparieren

- »Intelligente«, digital und sensorisch gesteuerte Heiz- und Kühlsysteme arbeiten nur wenn und nur so viel wie nötig, digital unterstützte Verkehrs- und Logistiksysteme vermeiden energieineffiziente Situationen wie Staus oder die Unternutzung von Transportmitteln.
- Immer bessere Sensorik und vor allem Auswertesysteme für die gewonnenen Daten helfen, die Vorhersage von klimabedingten Ausnahmesituationen wie Überschwemmungen oder Stürmen zu verbessern und die Zeitfenster für akute Schutzmaßnahmen zu vergrößern.

(Kritische) Entwicklungen und Ereignisse bewerten und einordnen

- Eine konsequente offene Bereitstellung insbesondere nicht personenbezogener Daten und deren sinnvolle und verantwortungsbewusste (Nach-)Nutzung für die datengestützte Vorbereitung auf kEEZ kann zum Verständnis und zur Einordnung unterschiedlicher Entwicklungen und Ereignisse beitragen, wie u. a. die Auswertung von Abwasserdaten im Corona-Zusammenhang und das Waldbrand-Cockpit von ÖFIT zeigen.

Inklusion

- Digitale Medien erleichtern gesellschaftliche Teilhabe. Flexible Untertitelung und Audiodeskription von Fernseh- und Streamingangeboten ermöglichen Teilhabe von bisher oft von Medienangeboten ausgeschlossenen Bevölkerungsgruppen, Übersetzungen »on the fly« helfen bei der Verständigung in Beruf und Privatleben.

Arbeitskräftemangel und menschenfreundliche Arbeitsbedingungen

- Automatisierung kann in vielen Branchen und im öffentlichen Sektor dazu beitragen, den demografisch bedingten Arbeitskräftemangel abzumildern, die verfügbaren Arbeitskräfte effizienter einzusetzen, ohne sie dabei zu überlasten, und menschliche Arbeitskraft an für Menschen gefährlichen Stellen zu ersetzen, z. B. in kontaminierten Umgebungen.

Vereinbarkeit von Beruf und Privatleben

- Digitale Werkzeuge und Telekommunikation können helfen, orts- und (teilweise) zeitunabhängig zusammenzuarbeiten, ebenso wie sie dabei unterstützen können, unterschiedliche Aufgaben und Bedürfnisse besser zu vereinbaren, z. B. Beruf mit Pflege, Kindererziehung oder Fortbildung.

Neben solchen großen, langfristigen und gezielt geschaffenen digitalen Resilienzbeiträgen sind auch kurzfristigere und kleinere, zum Teil improvisierte (d. h., durch spontane neuartige Nutzung digitaler Lösungen realisierte) Beiträge nicht zu unterschätzen:

- Digitale Technik – wie Videokonferenzen oder Online-Datenspeicher – ermöglicht neue Formen der Partizipation und Kollaboration. Online-Hackathons sind ein Beispiel dafür, wie ortsunabhängig digital vernetzt innerhalb eines sehr kurzen Zeitraumes kreative digitale Lösungen für gesellschaftliche Herausforderungen gefunden werden können.
- Die Kontaktbeschränkungen in der Coronapandemie führten zur ersatzweisen Nutzung von zuvor im Bildungs- und im privaten Bereich eher wenig verbreiteten Diensten wie Videotelefonie und Video- oder Audiokonferenzen. Dadurch war Schulunterricht weiter möglich und digitale Kontakte halfen gegen Vereinsamung.

Damit Digitalisierung und Digitalität Resilienz fördernd genutzt werden können, muss für viele Einsatzbereiche zunächst eine bedarfsgerechte, stabile und sichere digitale Basis geschaffen werden, die v. a. für die intendierten Nutzenden geeignet ist und von diesen angenommen wird. Was das im Einzelnen bedeutet und welche Maßnahmen dazu beitragen können, wird in den drei folgenden Abschnitten zu den tragenden Säulen von Resilienz im digitalen Kontext erläutert.

Säule: Resilienz von Digitalisierungsprozessen

Digitalisierungsprozesse werden resilienter, wenn die notwendigen Prozessschritte zur bedarfsorientierten Umsetzung der Gestaltungsaufgabe durch die Beteiligten offen für das Vorhaben und konstruktiv aufeinander aufbauend abgestimmt werden.

Digitalisierungsprozesse können je nach Phase mit verschiedenen Störungen konfrontiert werden, z. B. interne Verzögerungen wegen mangelnder Abstimmung, Fachkräftemangel, Lieferschwierigkeiten oder Kostenexplosion. Grundsätzlich fördern essenzielle Eigenschaften und Fähigkeiten »guter« Prozessgestaltung die Resilienz von Digitalisierungsprozessen. Digitalisierungsprozesse verlaufen in Phasen. Sie beginnen mit einer Identifizierung von Bedarfen und Zielen, die in Abgleich mit einem Ist-Zustand durch digitale Prozesse aufgesetzt werden sollen. Anschließend wird die Gestaltungsaufgabe festgelegt und das Vorhaben konzeptioniert, bevor es an die Umsetzung in der Praxis geht. Über alle Phasen hinweg wichtig, aber notwendig vor allem vor der Realisierung und Implementierung digitaler Lösungen, ist eine offene Haltung der Beteiligten zum Vorhaben. Mit einer Etablierung neuer Lösungen ist der Digitalisierungsprozess allerdings nie abgeschlossen, stetige Weiterentwicklungsbedarfe sind die Regel. Generell gilt: Aus ausgelassenen oder unvollständigen Schritten im Digitalisierungsprozess erwachsen Hürden und Reibungsverluste für den gesamten Prozess. Neben ausreichenden Ressourcen steht und fällt die Resilienz von Digitalisierungsprozessen mit einer Organisationskultur, die einen offenen Umgang mit Fehlern und Schwächen sowie geistige, organisatorische und Ressourcen-Flexibilität, z. B. bei erweiterten Bedarfen, fördert. Ebenso braucht es Verbündete und Pat:innen, die Digitalisierungsvorhaben durch Überzeugungsarbeit voranbringen.

Digitalisierungsprozesse beginnen mit der Formulierung von Aufgaben oder Bedarfen. Häufig existiert dabei die Erwartung, dass digitale Prozesse einfacher und schneller ablaufen, beispielsweise im Hinblick auf die Kommunikation oder die Abwicklung von Dienstleistungen. In dieser Anfangsphase stellen sich Störungen ein, wenn keine Einigkeit über Bedarfe, deren Wichtigkeit oder allgemeine Ziele erreicht wird bzw. darüber, ob diese miteinander vereinbar sowie unter den als gesetzt geltenden Vorgaben erreichbar sind. Störungsursachen können auch sein, dass nicht ausreichend Daten aus der Ist-Analyse zur Verfügung stehen bzw. diese falsch eingeschätzt werden oder nicht schon zu Beginn alle relevanten Stakeholdergruppen – z. B. diejenigen, die digitale Lösungen entwickeln, finanzieren oder Angebote und Leistungen nutzen – beteiligt werden. Störungen können dazu führen, dass das Momentum verpasst wird, den Digitalisierungsprozess fortführen zu können.

Gelangt ein Vorhaben in die Konzeptionierungsphase, geht es sowohl um die inhaltliche als auch die organisatorische Planung des Vorhabens. Mögliche Störungen ergeben sich hier wiederum durch eine unzureichende Beteiligung relevanter Stakeholder oder durch Uneinigkeit über das Konzept und seine Vorteile. Störungen ergeben sich in dieser Phase auch dann, wenn Personen fehlen, welche die Konzeptentwicklung koordinieren, vorantreiben oder als Expert:innen unterstützen, oder wenn eingeplante Fördermittel ausbleiben.

In der Realisierungsphase kann das Fehlen sowohl von Fachkräften als auch von Hardware (z. B. durch Engpässe bei Lieferketten) oder Nutzungsrechten (z. B. Lizenzen) dazu führen, dass die Zeitziele nicht eingehalten werden können. Unterbleiben frühzeitige Tests, ob eine digitale Lösung die Aufgabe wie konzeptioniert erfüllt und ausreichend skalierbar ist, verschiebt sich die Problemerkennung in spätere Phasen.

Störungen ergeben sich während der Etablierung der neuen Lösung v. a. durch mangelnde Kompetenz aufgrund von Schulungsdefiziten, mangelnde Usability bspw. aufgrund nicht ausreichender Möglichkeit zum Feedback und mangelnde Akzeptanz verursacht durch Versäumnisse in der Abstimmung. Es geht bei Digitalisierungsprozessen nicht nur um ein technisches Gestalten, sondern auch um Prozesse der individuellen Aneignung durch die Nutzer:innen. Wird der Nutzen für den eigenen Aufgabenbereich, z. B. als Vereinfachung und Beschleunigung von Arbeitsabläufen, den Beteiligten nicht ausreichend ersichtlich, verringert sich die Bereitschaft zur Einarbeitung. Lebenslanges Lernen ist aber eine essenzielle Voraussetzung jeder resilienten Digitalisierung, da digitale Prozesse häufige Anpassungen erfordern.

Manchmal offenbaren sich für Anwender:innen nicht bereits im Test-, sondern erst im Wirkbetrieb die Grenzen einer Lösung. Unverständnis über die Abfolge von Aufgaben innerhalb der Lösung oder Ineffizienzen, beispielsweise weil es zu Medienbrüchen kommt, können dazu führen, dass Digitalisierungsangebote für den entsprechenden Zweck generell abgelehnt werden. Solche Störungen eines Digitalisierungsprozesses können zu generellen Barrieren für die Durchsetzung digitaler Lösungen werden.

Da vielen Störungen durch sorgfältige Vorbereitung – z. B. durch ausreichende Information und durch Einfühlungsvermögen in verschiedene Stakeholdergruppen – im Vorlauf begegnet werden kann, wird Resilienz hier vor allem eine Frage organisatorischer bzw. personeller Entscheidungen: Für die Auswahl der Koordinator:innen von Digitalisierungsvorhaben sollten neben

fachlichen Kriterien auch methodische Kompetenzen berücksichtigt werden, welche für die erfolgreiche Umsetzung dieser Aufgabe erforderlich sind.

Die Resilienz von Digitalisierungsprozessen wird durch Anpassungs-, Bewältigungs- und Vermeidungsfähigkeiten verschiedener sozialer Einheiten wie Arbeitsgruppen, Organisationen oder interorganisationalen Allianzen gesteigert. Das erreichte Ausmaß an Resilienz hängt vom erfolgreichen Zusammenspiel derjenigen ab, von und mit denen die notwendigen Strategien und Maßnahmen organisiert und ausgeführt werden müssen. Falls bestehende Funktionen nicht ausreichen, um hierfür Orientierung und Anleitung zu geben, könnten neue Rollen wie Resilienzlots:innen entstehen. Beispiele für Resilienz steigernde Maßnahmen sind: Ziele werden abgestuft nach verfügbaren Ressourcen festgelegt. Agile Digitalisierungsprozesse ermöglichen, bei Störungen schnell auf alternative Lösungsbausteine (z. B. Zulieferer) umzuschwenken. Dezentrale Architekturen für hochfrequentierte Anwendungen wirken z. B. durch Lastverteilung und kürzere Wege von vornherein »Flaschenhälsen« im späteren Wirkbetrieb entgegen. Tests von (Teil-)Lösungen, auf die Feedbackschleifen in Produktion und Schulungen erfolgen, erleichtern auf einzelne Module begrenzte Anpassungen. Um optimal aus Best Practices oder Fehlern zu lernen, ist organisationales Wissensmanagement notwendig. Allianzen und Netzwerke – innerhalb von und zwischen Organisationen - fördern den Wissenstransfer über Best Practices und organisationsübergreifend geeignete (Teil-)Lösungen. Wird Code – bestenfalls basierend auf offenen Standards und Schnittstellen – offengelegt, kann die digitale Community diesen kommentieren und ggf. auch aktiv an der Gestaltung beteiligt werden. Das Beispiel der Corona-Warn-App zeigt, dass damit nicht nur Transparenz und Vertrauen in den Digitalisierungsprozess wachsen, sondern auch Schwachstellen und Sicherheitslücken zügiger und effizienter gefunden sowie behoben werden können.

Bei Digitalisierungsprozessen sind oft nur die beteiligten IT-Expert:innen mit der Beschreibung technischer Lösungswege vertraut, was deren Vermittlung und die Abstimmung mit den anderen Beteiligten erschwert. Maßnahmen, die auf das zielorientierte Zusammenwirken von IT-Expert:innen, Fachexpert:innen und Anwender:innen einzahlen, steigern die Resilienz dieser Prozesse. Expert:innen für einzelne Arbeitsbereiche oder Anwender:innen im Wirkbetrieb – z. B. Menschen mit Behinderungen, die Rückmeldungen zur Barrierefreiheit liefern – können wiederum wichtige Hinweise zur Gestaltung der digitalen Prozesse liefern, die IT-Expert:innen häufig verborgen bleiben.

Anpassung	Individuum + Organisation	• Schulungsangebote und lebenslanges Lernen • Organisationskultur, die »digitale Pioniere« fördert
Wiederherstellung	Organisation + Individuum	• Modulare Konzepte mit priorisierten Zielen und alternativen Lösungen • Offensive Fehlerkultur und frühzeitige Feedbackschleifen
Vermeidung	Organisation + Gesellschaft + Technik	• Eine Partizipation fördernde Umgebung, damit (insbes. Anfangs-)Phasen der Digitalisierung konstruktiv durchlaufen werden können • Resiliente (z. B. dezentrale) technische Architektur priorisieren

Tabelle 1: Resilienz von Digitalisierungsprozessen auf einen Blick

Anpassung	Individuum + Organisation + Technik	• Information und Wachsamkeit bzgl. neuer Angriffsformen • Umstieg auf resilienzförderliche, modulare Komponenten
Wiederherstellung	Organisation + Technik	• Redundanz • Notfallpersonal
Vermeidung	Organisation + Technik	• »Sicherheitszentrale« • Technische Verhinderung digitaler Einbrüche (Intrusion-Prevention-Systeme)

Tabelle 2: Resilienter Betrieb digitaler Technik und digitaler Infrastrukturen auf einen Blick

Säule: Resilienter Betrieb digitaler Technik und digitaler Infrastrukturen

Der Betrieb digitaler Technik und digitaler Infrastrukturen ist resilient, wenn Leistungsengpässe, Aktualisierungsbedarfe, Fehlfunktionen, Ausfälle und Angriffe schnell erkannt und angemessen bekämpft bzw. behoben werden können. Da viele Störungen erwartbar sind, können und müssen dazu in der Regel Vorsorgemaßnahmen getroffen werden.

Digitale Komponenten und Infrastrukturen sind für viele Alltäglichkeiten inzwischen essenziell oder zumindest das Mittel der Wahl. Sie können allerdings (selbst bei unwirtschaftlich hohem Mitteleinsatz, z. B. für Redundanz, Überwachung der Systeme und vorbeugende Wartung) niemals völlig fehler- und ausfallsicher gestaltet werden. Arbeiten sie nicht wie erwartet, kann es zu Störungen und Ausfällen bei den unterstützten Diensten und Funktionen kommen. Bewältigungsstrategien spielen daher eine immer wichtigere Rolle.

Jeder Betreiber digitaler Technik sollte angemessene Fähigkeiten besitzen und Mittel einsetzen, um bevorstehende Fehler und Ausfälle sowie Angriffe nach Möglichkeit rechtzeitig erkennen und schadensvermeidend bzw. -mindernd reagieren zu können.

Betreiber digitaler Infrastrukturen sollten darüber hinaus Resilienz leben, indem sie routinehaft:

- digitale Komponenten bevorzugen, die sich z. B. leicht überwachen und warten sowie im Bedarfsfall modular austauschen lassen;
- über ein umfassendes, aktuelles und gut verfügbares Wissen über die möglichen Ursachen von Fehlern und Ausfällen verfügen;
- die möglichen Auswirkungen von Fehlern und Ausfällen kennen;
- wirksame Mechanismen einsetzen, um – insbesondere bei über das Internet erreichbaren bzw. das Internet nutzenden Komponenten und Infrastrukturen – Angriffe möglichst frühzeitig zu erkennen und nach Möglichkeit abzuwehren bzw. deren Auswirkungen zu begrenzen;
- wirksame Mechanismen einsetzen, um bevorstehendes technisches Versagen möglichst frühzeitig zu erkennen;
- sich auf Fehler und Ausfälle so vorbereiten (z. B. durch die Priorisierung bestimmter Wiederherstellungsmaßnahmen), dass die Auswirkungen möglichst gering gehalten werden können;
- ausreichend Ressourcen für das schnelle Wiedererreichen eines – möglicherweise auch nur vorübergehenden – Normalzustandes nach einer Störung vorhalten;
- möglichst (alternative) Kommunikationsmittel bereithalten, um über Störungen und Ausfälle zeitnah informieren zu können;
- auch die Verfügbarkeit notwendiger digitaler Funktionen und Dienste von Dritten überwachen und auf beobachtbare kEEZ angemessen reagieren können und
- Erfahrungen aus eigenen und fremden kEEZ-Situationen nutzen, um die eigenen Resilienzmaßnahmen ständig weiterzuentwickeln.

Für einige der hier genannten Resilienzmaßnahmen existieren erprobte Handreichungen wie bspw. das IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik.

Zwei kEEZ sind in diesem Zusammenhang erwartbar:

- Digitale Infrastrukturen können – nicht nur bei unvorhergesehenen Lastspitzen – an ihre Leistungsgrenze stoßen. Unter Resilienzgesichtspunkten muss daher die Auslastung angemessen überwacht und insbesondere bei gravierenden Nutzungsänderungen vorausschauend mitbedacht werden. Absehbaren Engpässen sollte vorbeugend begegnet werden.
- Digitale Technik und Infrastrukturen veralten schnell, sei es in Bezug auf Sicherheitsaspekte oder bezüglich der Erwartungen an die Nutzungsfreundlichkeit. Demgemäß ist auch hierzu eine angemessene, fortlaufende Überwachung, Bewertung und Anpassung (z. B. durch Updates) erforderlich.

Insbesondere bei möglicher Gefahr für Leib und Leben oder bei kritischen Infrastrukturen können neben den von den Betreibern im Eigeninteresse durchgeführten Resilienzmaßnahmen auch regulative Vorgaben notwendig sein.

Für den Erfolg von Resilienzstrategien und -maßnahmen ist ein Zusammenwirken von Akteuren verschiedener Ebenen und Organisationen notwendig. U. a. sind organisationale Rahmenbedingungen wichtig, die Mitarbeiter:innen jenseits formaler Hierarchien ermutigen, frühzeitig auf Probleme und Missstände digitaler Technik hinzuweisen und eigene Fehler im Umgang mit digitaler Technik einzugestehen. Institutionalisierte interne und externe Kooperationen wie bspw. die Allianz für Cyber-Sicherheit erleichtern den Austausch über Gefährdungen und Resilienz steigernde Maßnahmen.

Säule: Resilienz gegenüber den Herausforderungen der Digitalität

Digitalität fordert Individuen, Organisationen und Gesellschaften in zweierlei Weise heraus: Einerseits kommt sie nicht allen gleichermaßen zugute, wodurch sich strukturelle Ungleichheiten weiter zuspitzen oder neue entstehen. Andererseits kann die Nutzung digitaler Möglichkeiten dem Gemeinwesen selbst und allen Ebenen einer Gesellschaft (beabsichtigt oder unbeabsichtigt) Schaden zufügen und kEEZ auslösen. Resilient zu sein heißt, gegen nicht erwünschte Entwicklungen wirksame Gegenmaßnahmen zu setzen.

Zugang zum Digitalen

Ein inklusiv orientiertes Gemeinwesen kann durch gezielte Maßnahmen darauf einwirken, dass die Chancen und Komfortgewinne durch Digitalisierung möglichst alle gesellschaftlichen Gruppen gleichermaßen erreichen. Ungleiche Gesellschaften gelten generell als weniger resilient gegen Krisen, da sie weniger gut kollektive Strategien zur Bewältigung von Herausforderungen entwickeln. *Resilient gegen digitale Spaltungen zu sein bedeutet auch, bei der Umsetzung von digitalen Lösungen immer Alternativen für solche gesellschaftlichen Gruppen mitzudenken, die aufgrund ökonomischer, physischer oder kognitiver Barrieren keinen unmittelbaren Zugang zu den primären Lösungen finden.*

Resilienzmaßnahmen sollten auf eine Vermeidung sozialer Ausschlüsse vom Digitalen zielen. Dazu gehört insbesondere die Vermeidung oder Herabsetzung von Zugangsbarrieren. Oft wird von dem »Normalzustand« ausgegangen, dass alle über (mobile) internetfähige Geräte verfügen und diese adäquat bedienen können. Auf fehlende Ausstattung benachteiligter Gruppen kann mit öffentlichen Internetzugängen oder subventionierter Hardware reagiert werden. Kompetenzen können in Form von Bildungsangeboten oder Anlaufstellen für (anleitende) Unterstützungsleistungen gefördert werden. Vorteilhaft ist, dies an bestehende kommunale Angebote wie Bibliotheken oder an Vereine, karitative Organisationen und Kirchen anzubinden. Maßnahmen zur Vermeidung sozialer Ausschlüsse vom Digitalen sollten aber u. a. auch bei der digitalen Ausgestaltung von Arbeitsplätzen, bspw. beim Einsatz von Robotik, berücksichtigt werden.

Nutzer:innenfreundliches Design erhöht die Bereitschaft, sich auf digitale Lösungen einzulassen, und erleichtert die Bewältigung auftretender Probleme, ohne über professionelles IT-Wissen verfügen zu müssen. Ein Schlüssel für die einfache Nutzung digitaler Angebote ist neben guten Orientierungshilfen der Einsatz von zielgruppenspezifischer (ggf. Leichter) Sprache, beispielsweise bei Gebrauchsanleitungen, um Anfangshürden zu vermeiden. Besonders förderlich sind partizipative Designansätze und Methoden, die heterogene Bedarfe und Gewohnheiten unterschiedlicher Nutzer:innen von Beginn an in die Gestaltung miteinbeziehen.

Umgang mit Digitalem

Die gesellschaftliche, organisationale und individuelle Resilienz gegenüber digitalen Herausforderungen hängt auch von der Art des Gebrauchs digitaler Technologien ab. Resilienz bedeutet in diesem Zusammenhang, darauf vorbereitet zu sein, dass technische Möglichkeiten zum fremden oder eigenen Schaden eingesetzt werden, und mit geeigneten Strategien und Maßnahmen darauf zu reagieren.

Die Nutzung digitaler Angebote kann nachteilige Folgen für Individuen haben:

- Die oft unbegrenzte Verfügbarkeit digitaler Angebote kann in Kombination mit Suchtdispositionen insbesondere bei Kindern und jungen Erwachsenen gesundheitsschädliche Wirkungen entfalten.
- Cybermobbing oder Hatespeech im Internet eskalieren häufig und sind schwer zu ahnden, weil die Täter:innen weitgehend anonym vorgehen können.

Digitale Möglichkeiten können nachteilig für das (demokratische) Gemeinwesen genutzt werden. Desinformationskampagnen in sozialen Medien, z. B. mithilfe von Deepfakes, zählen ebenso hierzu wie die Verbreitung illegaler Inhalte (z. B. Kinderpornografie). Aufgrund der starken und oft unkritischen Nutzung digitaler Massenmedien bergen diese Manipulationsmöglichkeiten essenzielle gesellschaftliche Krisenpotenziale. Dazu zählen Gefahren wie die Einflussnahme auf politische Wahlen, aber auch der Vertrauensverlust in digitale Medien allgemein. Generell können kollektive Erschöpfungs- und Überforderungseffekte auftreten, die aus der Schwierigkeit resultieren, medial vermittelte Informationen hinsichtlich ihrer Glaubwürdigkeit einzuordnen. Dies kann zu digitalem Rückzug führen und damit dem Ziel, durch Digitalisierung Teilhabe zu steigern, entgegenwirken.

Bislang werden Resilienzmaßnahmen zum Umgang mit Digitalem vor allem von zivilgesellschaftlichen Akteur:innen angestoßen und vorangetrieben. Zu den wünschenswerten regulatorischen

Resilienzmaßnahmen gehören einerseits die Erweiterung von Lehrplänen, die auf neue individuelle Kompetenzen im Umgang mit digitalen Angeboten abzielen, und andererseits mit dem Wert der Meinungsfreiheit abgewogene Maßnahmen gegen Hatespeech (vgl. die Diskussion um den Digital Services Act). Dem Staat kommt hier eine zentrale Rolle zu, aber auch Dienstanbieter sind in der Pflicht. Technische Maßnahmen wie der Ausbau von Präventions- und Aufdeckungstechnologien, bspw. Faktencheckern, können Schutz bieten. Zur Bewältigung trüge auch eine stärkere finanzielle oder organisatorische Unterstützung der gesellschaftlichen Gruppen und Organisationen bei, die Aufdeckungs- und Eindämmungsmaßnahmen und -mittel entwickeln. Im Kontext von Suchtdispositionen kann der Staat Resilienz fördern, indem Expert:innen gezielt mit der Erkennung von Risiken beauftragt und gefährdete Gruppen bzw. ihre Angehörigen frühzeitig sensibilisiert sowie Unterstützungsangebote flächendeckend bereitgestellt werden.

Digitale Möglichkeiten können weitere nicht intendierte nachteilige Folgen für Einzelne, Organisationen und die Gesellschaft mit sich bringen, beispielsweise im Bereich des hochautomatisierten Fahrens: Während völlig autonome Prozesse auf absehbare Zeit schwer umsetzbar scheinen, findet diese Zwischenstufe immer breitere Anwendung: Dem Menschen werden repetitive Tätigkeiten abgenommen, gleichzeitig aber auch nicht vollständig, da in kritischen Momenten menschliches Eingreifen wieder erforderlich ist. Gerade in der Rolle des passiven Überwachers und als letzte Instanz in Ausnahmesituationen werden aber Grenzen menschlicher Fähigkeiten sichtbar und Überforderung deutlich: Aufgrund der eingeschränkten Aufmerksamkeitsspanne des Menschen in monotonen Umgebungen bleibt rechtzeitiges Eingreifen fraglich, zumal ein Übervertrauen in Automation die Überwachung beeinträchtigen kann. Durch die Seltenheit des Eingreifens nimmt die Handlungskompetenz schlussendlich ab oder wird erst gar nicht aufgebaut. Resilient zu sein bedeutet in diesem Kontext, dem Menschen nur Rollen zu übertragen, die er aufgrund menschlicher Kapazitäts- und Fertigkeitsgrenzen beherrschen kann. Es verlangt einen erweiterten gesellschaftlichen Diskurs und gesetzliche Nachbesserung, inwieweit Menschen einerseits Autonomie entzogen, aber andererseits die Verantwortung in letzter Instanz übertragen werden kann.

Resilienz in der Mensch-Technik-Interaktion kann durch eine menschzentrierte Technikgestaltung befördert werden, die im Design neben den Bedürfnissen auch Grenzen stärker berücksichtigt. Hierfür müssen Entwickler:innen u. a. Konzepte zu menschlicher Wahrnehmung, Aufmerksamkeit, Kompetenz und Situationsbewusstsein in der Gestaltung des Digitalen noch mehr einbeziehen.

Anpassung	Individuum + Organisation + Gesellschaft	• Bildungs- und Weiterbildungsangebote, lebenslanges Lernen • Akzeptanz von Unterstützungsangeboten • Sensibilisierung für neue Risiken • transparente Abwägung positiver und negativer Effekte der Digitalität
Wiederherstellung	Gesellschaft + Organisation + Technik	• Initiativen zur Aufdeckung- und Eindämmung von Manipulationsstrategien unterstützen und weiter ausbauen • Gezielter Ausbau von Gesundheitsangeboten
Vermeidung	Organisation + Gesellschaft + Technik	• Menschenzentriertes, barrierefreies Design und Maßnahmen zur Herabsetzung von Zugangsbarrieren • Technische Lösungen bspw. für den Jugendschutz • Schutz durch strafbewehrte gesetzliche Verbote, z. B. der Verbreitung bestimmter Inhalte oder der Nutzung bestimmter Darstellungsformen

Tabelle 3: Resilienz gegenüber den Herausforderungen der Digitalität auf einen Blick

Quellen:
Beer, F. & S. Rammler. 2021. »Zwischen den Zeitenwenden: Transformative Resilienz als Leitbild der Zukunftsgestaltung«, S. 17 – 25 in: *Resiliente Zukünfte: Mut zum Wandel*, Zeitschrift politische ökologie Band 166, Jahrgang 39, hg. von oekom e. V.: oekom Verlag.
Hutter, G. & D. Lorenz. 2018. »Social Resilience«, S. 190 – 213 in: *Vulnerability and Resilience to Natural Hazards*, hg. von S. Fuchs & T. Thaler: Cambridge University Press.
Menz, N. et al. 2015. »S²: Safety und Security aus dem Blickwinkel der Öffentlichen IT«. Kompetenzzentrum Öffentliche IT. https://www.oeffentliche-it.de/publikationen?doc=31236.
Gumz, J. & N. Hajinejad. 2022. »Waldbrände mit Daten löschen«. Kompetenzzentrum Öffentliche IT. https://www.oeffentliche-it.de/-/waldbraende-mit-daten-loeschen.

Resilient digital in die Zukunft!

Die Resilienz des digitalen Gemeinwesens bestimmt sich aus der »Statik« seines Gebäudes. So, wie physische Gebäude in manchen Regionen elastisch gegenüber Erschütterungen konstruiert werden, beschreibt Resilienz im digitalen Kontext, bei der Metapher aus dem Bauwesen bleibend, eine Elastizität von Dach und Säulen gegenüber erwartbaren wie unvorhergesehenen kritischen Entwicklungen, Ereignissen und Zuständen (kEEZ). Digitalisierung kann zur gesellschaftlichen, organisationalen und individuellen Resilienz beitragen. Damit dieses Dach trägt, müssen die drei Säulen, auf denen es steht, auf kEEZ vorbereitet sein: Es braucht resiliente Digitalisierungsprozesse, resilienten Betrieb digitaler Technik und digitaler Infrastrukturen und es braucht Resilienz gegenüber Herausforderungen der Digitalität.

Lösungsorientiert wandlungs- und zukunftsfähig werden

Resilienz im digitalen Kontext erfordert Anpassungsfähigkeit an sich wandelnde Herausforderungen und Krisen und Offenheit für verschiedene Lösungsansätze. Das gilt für individuelle Gewohnheiten ebenso wie für Organisationskulturen. Um Erstarrungen zu vermeiden, braucht es die Bereitschaft, unsichere Zukünfte zu akzeptieren und in verschiedenen Szenarien zu denken.

Resilienz leben

Resilienz ist v. a. dann stark, wenn sie zum Entscheidungskriterium im Alltag wird. Merksätze wie S-U-P-E-R (mehr dazu s. S-U-P-E-R.ch) können z. B. dabei helfen, Maßnahmen routinehaft umzusetzen. Strategien, die Resilienz fördern, müssen systematisch ein Teil jeder digitalen (Organisations-)Kultur werden. Für die Entwicklung dieser Kultur müssen Bildungs- und Förderprogramme geschaffen werden.

Resilienz von Anfang an, nicht nur als *»nice-to-have«*

Bei allen Digitalisierungsaktivitäten sollten von Beginn an ausreichend Ressourcen für Resilienz fördernde Maßnahmen in allen drei Säulen bereitgestellt werden, obwohl sich Aufbau und Erhaltung von Resilienz eventuell erst langfristig rechnen. Aber speziell (noch) unvorhergesehene kEEZ können umfangreiche Reaktionen erfordern. Zu den Maßnahmen gehören u. a. die Auswahl und die Aktualisierung resilienter digitaler Technik.

Wissen und Erfahrungen nutzen, weitergeben und sinnvoll einbinden

Um Wissen über Störungspotenziale und -szenarien sowie Maßnahmen nutzen zu können, braucht es organisationales Wissensmanagement. Dabei sollten unterschiedliche Deutungen und Bewertungen von Störungen und Lösungen durch verschiedene Akteur:innen berücksichtigt werden. Klare Regeln und Routinen für den Umgang mit Wissensspeichern ebenso wie gezielter Wissenstransfer helfen, Wissen so zu verstetigen, dass es Mehrwerte stiften kann.

Neue Allianzen jenseits von Hierarchie und Wettbewerb aufbauen

Kooperation macht das digitale Gemeinwesen elastischer gegenüber Störungen. Förderlich ist die Zusammenarbeit auch zwischen Wettbewerbern und über formale Hierarchien hinweg. Strukturen und Allianzen wie das Netzwerk Bildung Digital (https://www.netzwerk-bildung-digital.de/) können als Beispiel dienen. Neue Rollen wie Resilienzlots:innen unterstützen dies.

Sensibilität für kEEZ fördern und belohnen

Die beste Resilienzstrategie ist stetige Sensibilität für kEEZ. Dazu gehört auch, kEEZ-Deutungen zu aktualisieren und auf individueller, organisationaler und gesellschaftlicher Ebene die Entdeckung und Meldung von kEEZ zu fördern und zu belohnen.

Kontakt

Dr. Karoline Krenn
Kompetenzzentrum Öffentliche IT (ÖFIT)
Tel.: +49 30 3463-7173
Fax: +49 30 3463-99-7173
info@oeffentliche-it.de
www.oeffentliche-it.de
Twitter: @OeffentlicheIT

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin
info@fokus.fraunhofer.de
www.fokus.fraunhofer.de
Twitter: @fraunhoferfokus

Das letzte Abrufdatum der Onlinequellen ist der 21.12. 2022.

Gefördert durch:
Bundesministerium des Innern und für Heimat
Fraunhofer FOKUS