Oxford Internet Institute
University of Oxford
Republic of Estonia
Ministry of Economic Affairs and Communications
rit Estonian IT Centre
Nortal

RESILIENZ VON REGIERUNGEN IM DIGITALEN ZEITALTER

Tallinn 2024

AUTOR*INNEN

Andres Raieste
Senior Vice President, Public Sector (Global), Nortal

Andri Rebane
Direktor der Abteilung für Informationssicherheit, Estnisches IT-Zentrum

Madis Tapupere
Chief Technology Officer, Ministerium für Wirtschaft und Kommunikation, Estland

Dr. Keegan McBride
Dozent für KI, Regierung und Politik, Oxford Internet Institute

Adjunct Senior Fellow für Nationale Sicherheit und Technologie, Center for a New American Security

Dieser Text kann als „Raieste, A., Rebane, A., Tapupere, M., McBride, K. (2024). Resilienz von Regierungen im digitalen Zeitalter“ zitiert werden.

Rezensionen und Beiträge:
Martin Sepp, Ergo Tars, Toomas Vaks

Dieses gemeinsame Dokument ist das Ergebnis einer Arbeitsgruppe, die sich aus Expert*innen aus dem öffentlichen Sektor, der Privatwirtschaft und der Wissenschaft zusammensetzt.

Das Oxford Internet Institute ist eine multidisziplinäre Forschungs- und Lehrabteilung der Universität Oxford, die sich mit der Sozialwissenschaft des Internets beschäftigt.

Das Estonian IT Centre (RIT) versorgt den öffentlichen Sektor der Republik Estland mit einer sicheren IT-Infrastruktur und zentralen Diensten.

Nortal ist ein globales Unternehmen für strategische Innovation und Technologie und ein geschätzter Partner für Regierungen, Gesundheitseinrichtungen, führende Unternehmen und Fortune-500-Unternehmen.

INHALT

KURZFASSUNG

Die heutige Welt ist von digitalen Technologien geprägt und Staaten, die in diesem Umfeld bestehen wollen, müssen ihre Strukturen und Prozesse digitalisieren. Andernfalls riskieren sie, an Bedeutung zu verlieren. Diese Entwicklung ist kein neues Phänomen, sondern ein langjähriger Prozess, der bereits seit den 1990er Jahren mit der Einführung des Internets begonnen hat. Seither bemühen sich Staaten weltweit, die Potenziale der Digitalisierung zu nutzen.

Viele Staaten haben frühzeitig erhebliche Investitionen in die Digitalisierung getätigt. Sie konzentrierten sich darauf, zentrale Datenbestände zu modernisieren und papierbasierte Verwaltungsdienste in digitale Formate zu überführen. Diejenigen, die in diesem Bereich entschlossen vorangingen, profitieren heute von effizienteren Verwaltungen und einer besseren Anpassungsfähigkeit an neue Herausforderungen. Diese Staaten sind nicht nur besser aufgestellt, sondern sichern sich auch geopolitische Vorteile in der entstehenden digitalen Ordnung.

Für Länder, die die Digitalisierung bisher vernachlässigt haben, wurden jüngste globale Krisen zu einem Wendepunkt. Diese Ereignisse haben die Dringlichkeit unterstrichen, digitale Technologien in den Mittelpunkt staatlicher Strategien zu stellen, um die Anforderungen einer modernen Staatsführung im 21. Jahrhundert zu erfüllen.

Die Welt befindet sich in einer Phase beispielloser Herausforderungen, geprägt von miteinander verwobenen Krisen – einer sogenannten Polykrise. Die COVID-19-Pandemie legte im Jahr 2020 weite Teile des öffentlichen und wirtschaftlichen Lebens lahm und führte dazu, dass viele Staaten grundlegende Funktionen und Dienstleistungen nicht aufrechterhalten konnten. Hinzu kommen die zunehmenden Auswirkungen des Klimawandels: Extremwetterereignisse wie häufigere und intensivere Waldbrände, Überschwemmungen oder sogar der Verlust ganzer Gebiete – wie etwa in Tuvalu – bedrohen die Stabilität von Staaten. Gleichzeitig eskalieren geopolitische Spannungen wie der Krieg in der Ukraine oder die Rivalität zwischen den USA und China, die sich zunehmend auf Taiwan konzentriert.

Auch innerhalb demokratischer Gesellschaften entstehen neue Herausforderungen. Demokratien kämpfen mit sinkender Wahlbeteiligung, wachsender politischer Unzufriedenheit und dem Risiko demokratischer Rückschritte. Staaten stehen vor der Aufgabe, eine Vielzahl von Krisen gleichzeitig zu bewältigen – sowohl auf nationaler als auch internationaler Ebene. Dies geschieht meist unter schwierigen Bedingungen: schrumpfende Budgets, begrenzte personelle Ressourcen und steigende Erwartungen an Effizienz und Effektivität im öffentlichen Sektor.

Die einzige praktikable Lösung besteht darin, digitale Technologien strategisch einzusetzen. Staaten, die dies erfolgreich tun, sind deutlich resilienter. Während der COVID-19-Pandemie bewiesen Staaten, die einen hohen Grad an Digitalisierung ihrer öffentlichen Verwaltung aufweisen konnten, ihre Fähigkeit, schneller und effektiver auf die Krise zu reagieren. Ähnlich entscheidend sind digitale Technologien bei der Überwachung, Bewältigung und Eindämmung von Naturkatastrophen oder der Optimierung datengesteuerter Entscheidungsprozesse im Rahmen von Konflikten. Sie bieten Staaten, die sie nutzen, einen erheblichen strategischen Vorteil.

Gleichzeitig führt diese digitale Transformation zu einer fundamentalen Abhängigkeit von Technologien. Die Staaten, die sich zu digitalen Vorreitern entwickeln, gestalten nicht nur die Zukunft, sondern schaffen auch neue Risiken, da das Funktionieren des Staates zunehmend von der Stabilität und Sicherheit digitaler Systeme abhängt.

Dies sollte keine Furcht auslösen, sondern vielmehr Anlass zur Überlegung sein. Staaten, die sich auf den Weg der Digitalisierung begeben, müssen der langfristigen Resilienz der entstehenden digitalen Infrastruktur oberste Priorität einräumen. Nur durch ein vorausschauendes und strategisches Management kann gewährleistet werden, dass diese Systeme den künftigen Herausforderungen gewachsen sind und ihre Funktionalität auch in Krisenzeiten bewahren.

Das vorliegende Dokument dient als Leitfaden für politische Entscheidungsträger*innen, die sich der Herausforderung widmen, widerstandsfähigere und leistungsfähigere digitale Staaten zu entwickeln. Er bietet zunächst einen Überblick über die wesentlichen Fortschritte, die zur Stärkung der Resilienz von Regierungen im digitalen Zeitalter erzielt wurden, und beleuchtet zugleich die historische Entwicklung der gegenwärtigen digitalen Weltordnung. Anschließend wird im Dokument ein szenariobasierter Ansatz angewendet, um typische Krisensituationen zu skizzieren, auf die Staaten ihre digitale Infrastruktur vorbereiten müssen. Aufbauend auf diesen Szenarien formuliert der Bericht sieben zentrale politische Empfehlungen, die gezielt darauf abzielen, die Resilienz der digitalen Infrastruktur zu sichern und nachhaltig zu stärken.

→ **Setzen Sie bei öffentlichen Diensten und Registern auf einen “digital first”-Ansatz. Priorisieren Sie digitale Lösungen bei sämtlichen Diensten, die für die Kontinuität des Staates von essenzieller Bedeutung sind.**

→ **Ermöglichen Sie den Übergang zu Remote-Arbeitsplätzen im öffentlichen Sektor. Stellen Sie sicher, dass Verwaltungsaufgaben und Regierungsfunktionen auch außerhalb von Büros reibungslos durchgeführt werden können.**

→ **Stellen Sie die Sicherheit digitaler Infrastruktur und Dienste in den Mittelpunkt. Investieren Sie in umfassende Schutzmaßnahmen, um digitale Systeme vor Angriffen oder Störungen zu bewahren.**

→ **Betrachten Sie den Internetzugang als kritische Infrastruktur und sichern Sie eine stabile Konnektivität. Der Zugang zum Internet ist essenziell für die Funktion und Resilienz moderner Staaten.**

→ **Minimieren Sie physische Bedrohungen für digitale Infrastrukturen. Entwickeln Sie Strategien, um das Risiko physischer Eingriffe zu reduzieren, die die Funktionsfähigkeit digitaler Systeme beeinträchtigen könnten.**

→ **Etablieren Sie ein nachhaltiges Risikomanagement für Abhängigkeiten von Drittanbietern. Entwickeln Sie Mechanismen, die die technologischen Innovationen bewahren und gleichzeitig die Resilienz gegenüber externen Risiken stärken.**

→ **Implementieren Sie einen kohärenten Ansatz für digitale Resilienz der gesamten öffentlichen Verwaltung. Ein abgestimmtes Vorgehen über alle Ebenen und Ressorts hinweg ist notwendig, um die Ziele der digitalen Resilienz systematisch zu erreichen.**

Die Umsetzung dieser Maßnahmen ermöglicht es Staaten, eine robuste digitale Infrastruktur aufzubauen, die auch in Krisensituationen betriebsfähig bleibt. Ein solcher digitaler Staat könnte seine kritischen Dienstleistungen auch dann aufrechterhalten, wenn sein Staatsgebiet temporär oder dauerhaft nicht zugänglich ist. Dies markiert einen fundamentalen Wandel im Verständnis staatlicher Souveränität und Resilienz im digitalen Zeitalter. In einer Welt, in der technologische Systeme zunehmend die physische Welt ergänzen oder ersetzen, müssen Staaten ihre strategischen Ansätze entsprechend anpassen.

Die Zukunft der Demokratie ist digital. In den Jahren 2020 bis 2022 während der Pandemie haben fast 30 Prozent der Staaten in Europa die Wahlen verschoben [10], was dem demokratischen Prozess geschadet hat. Digitale staatliche Prozesse sind zu einer Notwendigkeit geworden, um Staaten in Krisenzeiten besser zu schützen.

EINLEITUNG

Nach dem Zweiten Weltkrieg entwickelte die Weltgemeinschaft die Grundlagen für eine neue geopolitische Ordnung, die sich an liberalen Werten orientierte. Die Zahl der demokratischen Staaten begann im gleichen Zeitraum zu wachsen; die Demokratie stand für die Hoffnung auf eine bessere Zukunft. Nach der Auflösung der Sowjetunion in den 1990er Jahren nahm der Optimismus weiter zu. Zum ersten Mal in der Geschichte lebte die Mehrheit der Weltbevölkerung in Staaten, die von liberalen und demokratischen Werten geprägt waren [1].

In dieser Zeit trat eine weitere Grundlage der heutigen Welt in den Vordergrund: das Internet. Das Internet und seine globale Verbreitung veränderten die Art und Weise, wie die Welt kommuniziert, und stärkten die Werte der Freiheit, der Demokratie und des Rechts. In einer Rede im Jahr 1994 äußerte Vizepräsident Al Gore die Hoffnung, dass “Mittel- und Osteuropa die Technologie und den freien Markt nutzen kann, um Demokratie aufzubauen und nicht, um sie zu verhindern. [2]” Einige Monate später wiederholte er seinen Glauben an das positive Potenzial des Internets, um “robusten und nachhaltigen wirtschaftlichen Fortschritt, starke Demokratien [und] bessere Lösungen für globale und lokale Umweltprobleme zu schaffen. [3]” Es war klar, dass die Technologie, insbesondere das Internet, das Denken der Welt über Staaten und öffentliche Verwaltungen verändern konnte.

Zwar begannen viele Staaten mit der neuen Technologie zu experimentieren, um ihre Verwaltungen umzugestalten, doch nicht alle hatten dabei auch Erfolge aufzuweisen. Einige Staaten sahen in der Technologie auch eine potenzielle Bedrohung für den Staat. Es wurde argumentiert, dass die Computerisierung der Gesellschaft “das gesamte Nervensystem der sozialen Organisation” verändern könne und diese Entwicklungen “die Souveränität” infrage stelle [4], da private Unternehmen statt des Staates die Kontrolle über die Kommunikation übernehmen könnten. Im Gegensatz dazu ist Estland, das 1991 seine Unabhängigkeit wiedererlangte, eines der wenigen Länder, das sich schon früh umfänglich der Technologie verschrieben hat. Estlands erster Plan zur Entwicklung der Informationstechnologie, “The Estonian Road to an Information Society”, wurde 1994 veröffentlicht und konstatierte, dass die Technologie eine entscheidende Rolle für die Zukunft des Staates spiele, indem sie seine Effizienz verbessere und ihm helfe, Kultur, Souveränität und Sicherheit zu stärken und zu sichern. Diese Strategie sah den Privatsektor nicht als Hindernis oder Herausforderung für den Staat an, sondern als Schlüsselkomponente, die der Regierung

hilft, ihr Digitalisierungsziel zu erreichen.

Heute, mehr als drei Jahrzehnte später, kann auf diese frühen Überzeugungen über die liberale geopolitische Ordnung, die Demokratie, die Staaten, die öffentliche Verwaltung, die Technologie und die Beziehungen zwischen ihnen zurückgeblickt werden. Es entsteht das Bild einer neuen digitalen Welt. In dieser neuen Welt stehen die demokratischen Staaten jedoch der Infragestellung der Demokratie [5], einer sinkenden Wahlbeteiligung [6] und einer zunehmenden Unzufriedenheit unter den Wähler*innen [7] gegenüber. Während sie um die Aufrechterhaltung ihrer demokratischen Systeme kämpfen und den wachsenden globalen Einfluss des Autoritarismus zurückdrängen [8], müssen die demokratischen Staaten beispiellose Herausforderungen ihrer Stabilität und Sicherheit meistern. Die COVID-19-Pandemie im Jahr 2020 hat viele überrascht und zahlreiche Schwachstellen in den staatlichen Abläufen aufgedeckt. Die Pandemie zeigte jedoch auch, dass die Staaten, die Daten und Technologie effektiver nutzen konnten, die Krise besser bewältigt haben [9]. Die Pandemie hat dazu geführt, dass fast 30 Prozent der Staaten in Europa die Wahlen in den Jahren 2020 bis 2022 verschoben haben [10], was dem Ansehen der Demokratie geschadet hat. Noch weniger Staaten waren in der Lage, ihre Schulen nahtlos in den digitalen Fernunterricht wechseln zu lassen, was der Bildung der Kinder geschadet hat. Auch der Klimawandel macht sich zunehmend bemerkbar: Naturkatastrophen treten immer häufiger auf und nehmen an Intensität zu. Einige Staaten tragen hier eine besonders schwere Last, denn ihr gesamtes Territorium wird in absehbarer Zeit verschwinden [11].

Wenn es früher möglich war, die Vorteile und das positive Potenzial der Digitalisierung staatlicher Aufgaben zu ignorieren, ist dies heute nicht mehr der Fall. Staaten, die sich nicht digitalisieren, werden zurückbleiben und in einer von Technologie bestimmten Welt zunehmend angreifbar sein. Technologie muss als ein wesentlicher und integraler Bestandteil des Staates betrachtet werden, um die wachsende Komplexität der Welt zu bewältigen. Viele Staaten sind sich dessen bewusst und investieren große Summen in die Digitalisierung. Allein die Europäische Union hat mehr als 100 Mrd. EUR bereitgestellt, um die Entwicklung eines digitalen und resilienten Europas zu unterstützen [12]. Die Digitalisierung wird die Effektivität und Effizienz von Staaten verbessern, aber sie bringt auch neue Herausforderungen und Bedrohungen mit sich.

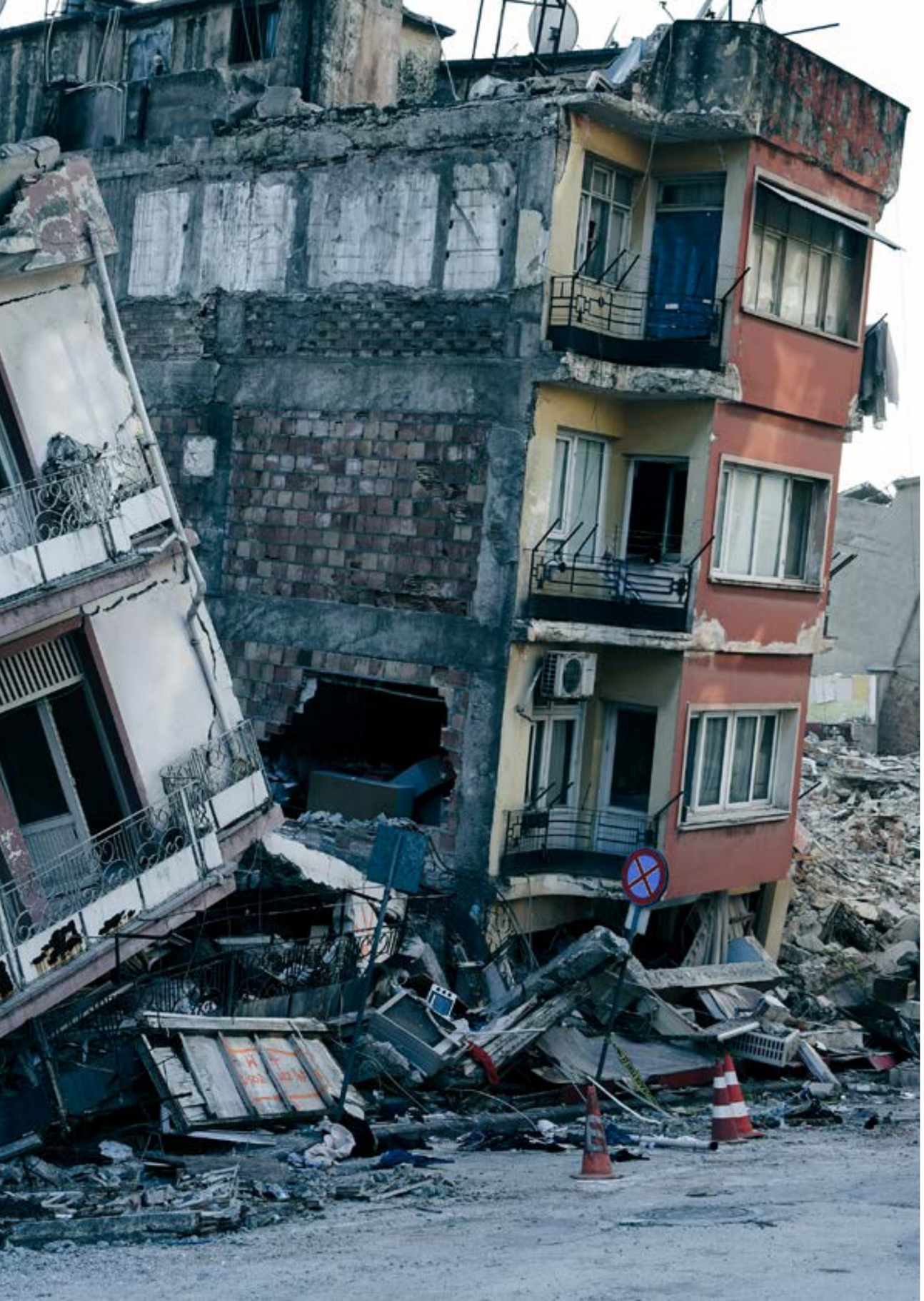
Viele Staaten sind nicht in der Lage, die von ihnen benötigten digitalen Infrastrukturen und Technologien eigenständig zu entwickeln, aufzubauen oder aufrechtzuerhalten, und haben sich daher in großem Umfang an private Technologieunternehmen gewandt [13]. Diese wachsende Abhängigkeit vom Privatsektor hat Politiker*innen und Wissenschaftler*innen zu der Behauptung veranlasst, ein “Putsch” [14] sei im Gange, bei dem Technologieunternehmen den Staat verdrängten und seine Ressourcen aufbrauchten. Diese Befürchtungen sind umso stärker, wenn die Unternehmen, auf die der Staat sich stützt, im Ausland ansässig sind. Es besteht ein wachsendes Interesse an Maßnahmen zur Förderung der “digitalen Souveränität” und der “Datensouveränität” [15], um diesen Befürchtungen entgegenzuwirken. Solche Bedenken sind zwar verständlich, aber

durch die Bindung der digitalen Infrastruktur an das Gebiet eines bestimmten Landes werden neue Schwachstellen geschaffen. In ähnlicher Weise wird durch den Versuch, die Macht der größten Technologiekonzerne zu beschneiden, auch die Fähigkeit des Staates geschwächt, sich im Cyberbereich zu verteidigen. Auch in der digitalen Welt gibt es keinen Frieden mehr und die digitale Infrastruktur eines Staates ist ein klares Angriffsziel. Der Privatsektor spielt eine entscheidende Rolle bei der Verteidigung von Staaten gegen umfassende tägliche Cyber-Bedrohungen [16]. Diese Bedrohungen sind keineswegs bloße Fiktion. Im Jahr 2007 wurde Estland von einem groß angelegten Cyberangriff heimgesucht, der das Land erheblich beeinträchtigte. Im Krieg gegen die Ukraine nutzt Russland sowohl digitale als auch physische Mittel, um die Fähigkeit der Ukraine zu sabotieren, digital zu operieren [17].

Da die militärischen Spannungen zwischen Taiwan und China weiter zunehmen, wird vermutet, China werde als einen der ersten Schritte die kritische digitale Infrastruktur Taiwans ins Visier nehmen [18].

Da die Zahl der Bedrohungen des physischen Territoriums von liberalen und demokratischen Staaten aufgrund von Konflikten und anderen Faktoren weiter zunimmt, ist von großer Bedeutung, robustere und resilientere digitale Strukturen aufzubauen.

Der Aufbau und die Investitionen in eine bessere, stärkere und resilientere digitale Zukunft werden nicht nur dazu beitragen, die Langlebigkeit der demokratischen Staaten selbst sicherzustellen, sondern bieten ihnen auch neue Möglichkeiten, ihre Vision einer digitalen geopolitischen Ordnung zu verkaufen. Das vorliegende Dokument stellt einen ersten Schritt zur Konzeptualisierung eines resilienten digitalen Staates dar. Dazu werden mehrere Szenarien aufgezeigt, mit denen Staaten in den kommenden Jahrzehnten konfrontiert werden können, und es wird untersucht, wie digitale Technologien eingesetzt werden können. Im Anschluss an diese Untersuchung werden politische Maßnahmen und Bausteine für den Aufbau robusterer und resilienterer digitaler Staaten vorgestellt.



HERAUSFORDERUNGEN FÜR DIE KONTINUITÄT DES STAATES

Krisen und Naturkatastrophen waren schon immer ein Teil unserer Welt. Krisen, die aus politischen, wirtschaftlichen, sozialen oder umweltbedingten Faktoren entstehen können, haben oft ähnliche Merkmale und führen zu tiefgreifenden Auswirkungen auf Gesellschaften und Einzelpersonen. Historisch gesehen haben Krisen oft eine zentrale Rolle bei Entwicklung von Staaten gespielt. Die Geschichte ist voll von Beispielen, die zeigen, wie Staaten, die nicht in der Lage sind, die Herausforderungen einer Krise zu bewältigen, an Macht und Einfluss verlieren oder sogar aufhören zu existieren [19].

Zwar sind die Ursachen vieler Krisen heute noch ähnlich wie vor Jahrhunderten, z. B. Naturkatastrophen, Kriege oder Pandemie, doch ist die Welt von heute stärker vernetzt als je zuvor. Dies hat zur Folge, dass die Komplexität der Krisenbewältigung rapide zugenommen hat und die potenziellen Auswirkungen größer sind. Aufgrund des digitalen und integrierten Charakters der Welt sind die Staaten von globalen Lieferketten, Ressourcen und Technologien abhängig [20]. Jüngste Beispiele hierfür sind die COVID-19-Pandemie, die zu einer weltweiten bis heute anhaltenden Unterbrechung der Lieferketten führte [21], der Ransomware-Angriff WannaCry und der Krieg in der Ukraine.

Da die heutige Welt digital ist, ist es nicht mehr möglich, die physische und die virtuelle Welt zu trennen. In jedem der oben aufgeführten Beispiele waren erhebliche Auswirkungen in beiden Bereichen gleichzeitig zu spüren.

> **Heute kann die Zerstörung der virtuellen Umgebung oder kritischer Datensätze mehr Schaden anrichten als die Zerstörung eines Gebäudes oder der physischen Infrastruktur.**

In Zeiten von Konflikten, die selber immer digitaler werden, könnte eine ablehnende Haltung zu Cyberspace und zu digitalen Diensten das Funktionieren des Staates zum Erliegen bringen.

Der zunehmende Grad an Digitalisierung und technologischer Innovation schafft zwar neue Schwachstellen für Staaten, bietet aber auch die Möglichkeit, Gesellschaften resilienter zu machen als je zuvor. Durch technologische Entwicklung und eine strategische, umfassende Digitalisierung der Gesellschaft können Staaten ihre Resilienz erhöhen, indem sie alternative Strukturen schaffen und ihre Flexibilität stärken.

Im nächsten Kapitel geht das Dokument näher darauf ein, welche Maßnahmen ergriffen werden können, um die öffentliche Verwaltung im digitalen Zeitalter resilienter zu gestalten.

WORIN BESTEHT DIE BEDROHUNG? BEISPIEL FÜR EIN KRISENSZENARIO

DER BEGINN DER KRISE:

Naturkatastrophen, Pandemien oder militärische Konflikte führen zu erheblichen Störungen der normalen Abläufe in den öffentlichen Verwaltungen von Staaten. In bestimmten Fällen können diese völlig handlungsunfähig werden.

Die unmittelbare Folge dieser Katastrophen zeigt ein düsteres Szenario, in dem kritische Infrastrukturen in hohem Maße beschädigt wurden. Zahlreiche inländische Datenzentren wurden zerstört, sodass ein erheblicher Teil des nationalen digitalen Backbones nicht mehr funktionsfähig ist. Die Stromversorgung ist unterbrochen und die Kontinuität der Kraftstoffversorgung gefährdet. Außerdem ist die Telekommunikationsinfrastruktur schwer beschädigt, was eine effektive Kommunikation behindert.

Parallel dazu kann es auch zu Cyberangriffen oder zur Zerstörung der digitalen Infrastruktur kommen, wodurch Dienste dauerhaft oder vorübergehend nicht mehr erreichbar sind. Die wechselseitigen Abhängigkeiten zwischen Datenbeständen und Diensten können zu Kaskadeneffekten führen, sodass ganze Bereiche nicht mehr funktionsfähig sind. In solchen Fällen müssen alternative Betriebsverfahren aktiviert werden.

Dies kann zur Folge haben, dass es unmöglich wird, eine moderne Lebensweise aufrechtzuerhalten. Die Abhängigkeiten zwischen Datenbeständen, verschiedenen Informationssystemen und nationalen Diensten, wie z. B. der elektronischen Identifizierung, sind deutlich zutage getreten.

Das Ausmaß der Krise und der geringe Grad der Vorbereitung haben dazu beigetragen, dass große Schäden entstanden sind. Als Reaktion darauf wurden einige Datenbestände (in Papierform oder digital) möglicherweise in sicherere Zonen verlegt, während andere vorübergehend oder dauerhaft offline bleiben. Im schlimmsten Fall könnten wichtige Datenbestände und ihre Sicherungen dauerhaft zerstört oder

unwiderruflich beschädigt sein, was zu einem verheerenden Datenverlust führt. Der Staat und die Dienste, die auf diese Datenbestände angewiesen sind, stehen vor großen Herausforderungen; einige funktionieren noch, andere haben ihre Arbeit eingestellt, weil wichtige Daten fehlen.

Diese Verschlechterung der öffentlichen Dienstleistungen wirkt sich auf die öffentliche Meinung und Stimmung aus. Der Zugang zu Informationen ist stark eingeschränkt, was zu Angst und Unsicherheit in der Bevölkerung führt. Der Staat steht nun vor der gewaltigen Aufgabe, die Aufrechterhaltung der Staatsführung zu gewährleisten.

FORTDAUER DER KRISE:

Aufgrund der anhaltenden Krise ist ein erheblicher Teil des Staatsgebiets unbewohnbar geworden. Die öffentliche Verwaltung kämpft um ihr Überleben und erwägt gleichzeitig die Möglichkeit, Operationen im Exil durchzuführen.

Der Erhalt der Widerstandsfähigkeit der demokratischen Institutionen sowie die langfristige Erhaltung der Nation und ihres kulturellen Erbes haben sich angesichts des andauernden Konflikts als strategische Ziele erwiesen. Da der Staat gezwungen ist, mit einer geringeren Anzahl von Dienstleistungen zu funktionieren, ist es unerlässlich, dass er weiterhin Informationen über Bürger*innen, Eigentum, kulturelles Erbe usw. aktualisiert, um die Kontinuität der Nation zu gewährleisten.

Außerdem benötigen die Bürger*innen im Exil Zugang zu staatlichen Dienstleistungen. Bestimmte Informationen aus den nationalen Datenbeständen werden an ausländische Register übertragen, um die Inanspruchnahme grundlegender Dienste wie medizinischer und bildungsbezogener Daten zu erleichtern. Es ist von entscheidender Bedeutung, dass Bildungsressourcen wie Schulbücher und virtueller Unterricht zur Verfügung gestellt werden.

Werden solche Dienstleistungen nicht angeboten, verlieren die Bürger*innen schließlich die Bindung an ihr Heimatland. Diese allmähliche Erosion der nationalen Identität wird dazu führen, dass die Nation ihre politische und kulturelle Besonderheit verliert. Infolgedessen wird der Einzelne sich nicht mehr zugehörig fühlen, was dazu führt, dass die Kontinuität des Staates gefährdet ist und unter äußerem Druck nicht mehr aufrechterhalten werden kann.

STRATEGIEN ZUM AUFBAU RESILIENTER DIGITALER STAATEN

In den beiden vorangegangenen Kapiteln wurde dargelegt, wie digitale Technologien und Krisen die heutige Welt zunehmend bestimmen. Um wettbewerbsfähig zu bleiben, müssen Staaten digitalisieren – das ist mittlerweile unverzichtbar. Da immer mehr staatliche Aufgaben digital erledigt werden, ist es entscheidend, die langfristige Stabilität und Verlässlichkeit dieser Systeme zu sichern. Dies ist besonders wichtig, da Staaten weltweit mit zahlreichen, miteinander verbundenen Krisen wie Kriegen, Pandemien und dem Klimawandel konfrontiert sind. Jede dieser Krisen kann das Funktionieren des Staates erheblich stören, etwa durch Internetausfälle, die Schließung von Ämtern/Behörden oder die Zerstörung wichtiger Datenbestände.

Im Zuge der Umgestaltung von Staaten in digitale Staaten ist es von größter Bedeutung, zielgerichtet darüber nachzudenken, wie eine robuste und resiliente digitale Infrastruktur aufgebaut werden kann. Ausgehend von den Herausforderungen, die sich als Antwort auf eine Krise wie die beschriebene stellen können, werden in diesem Abschnitt sieben Empfehlungen zur Stärkung der digitalen Resilienz des Staates gegeben.

> **Die Umsetzung dieser Empfehlungen wird dazu beitragen, dass ein digitaler Staat auch in den schwierigsten Krisen funktionieren kann.**

Sie können einen Staat sogar in die Lage versetzen, auch dann digital zu funktionieren, wenn er keine Kontrolle mehr über sein Territorium hat.

01 ENTWICKLUNG UND UMSETZUNG EINES KONZEPTS FÜR DIE DIGITALISIERUNG WICHTIGER ÖFFENTLICHER DIENSTE UND DATENBESTÄNDE

Digitale Register und Dienste sind zuverlässiger und effizienter als Datenbestände in Papierform, insbesondere in Krisensituationen. Leider haben viele Staaten ihre kritischen Dienste, die für die Kontinuität in Krisenzeiten sorgen, nicht digitalisiert. Um die Zuverlässigkeit und Resilienz des Staates zu erhöhen, muss der Digitalisierung solcher Dienste Priorität eingeräumt werden.

02 SCHAFFUNG VON "REMOTE-FIRST"- UND "REMOTE-ENABLED"-ARBEITSPLÄTZEN IN DER ÖFFENTLICHEN VERWALTUNG

Mitarbeiter*innen der öffentlichen Verwaltung, die die Kontinuität digitaler öffentlicher Infrastrukturen und Dienste sicherstellen, sind von Krisen genauso betroffen wie der Rest der Bevölkerung. Um die nationale Resilienz zu erhöhen, müssen die Arbeitsplätze im öffentlichen Sektor remote erreicht werden können.

03 SICHERN DER DIGITALEN INFRASTRUKTUR UND DIENSTE DES STAATES

Kritische digitale Daten, Dienste und Register müssen vor Manipulation und Angriffen erfolgreich geschützt werden. Die Festlegung verbindlicher Sicherheitsstandards und -anforderungen für öffentliche Dienste und Infrastrukturen zum Schutz vor internen und externen Bedrohungen ist unumgänglich, um die Cyber-Resilienz des Staates zu erhöhen.

04 SICHERSTELLEN EINES WEIT VERBREITETEN UND BEZAHLBAREN ZUGANGS ZU KOMMUNIKATION

Im heutigen digitalen Zeitalter ist der Zugang zum Internet genauso wichtig wie der Zugang zu anderen Infrastrukturen und Einrichtungen. Der Staat muss alle technologischen Möglichkeiten ausloten, um Resilienz zu gewährleisten.

05 AUFBAU VON REDUNDANZ IN DER DIGITALEN ÖFFENTLICHEN INFRASTRUKTUR

Die Staaten müssen gewährleisten, dass digitale öffentliche Dienste und Infrastrukturen vor Zerstörung durch den Betrieb dieser digitalen Dienste in einem begrenzten physischen Raum geschützt werden. Dies kann bedeuten, dass zumindest ein Teil der Infrastruktur außerhalb der eigenen Territorialgrenzen positioniert werden muss. Dabei müssen auch Fragen des gegenseitigen Vertrauens zwischen Staaten geklärt werden.

06 BEWÄLTIGEN DES DRITTPARTEIRISIKOS BEI GLEICHZEITIGER WAHRUNG DER TECHNOLOGISCHEN INNOVATION

Fast alle digitalen öffentlichen Dienste und Infrastrukturen enthalten technologische “Black Boxes”, die transparent sind und die sogar die digitale Souveränität des Staates infrage stellen können. Mit der fortschreitenden Digitalisierung der Welt wird sich dieser Trend fortsetzen. Es sollten Verfahren eingeführt werden, um dieses Risiko auf ein vernünftiges Maß zu begrenzen, das Innovationen nicht ernsthaft behindert, jedoch eine Überregulierung vermeidet.

07 SCHAFFUNG INSTITUTIONELLER KAPAZITÄTEN FÜR DIE ENTWICKLUNG DER RESILIENZ VON ÖFFENTLICHEN VERWALTUNGEN

Die Resilienz der öffentlichen Verwaltung erfordert, dass jeder Bereich eigenverantwortlich handelt. Gleichzeitig ist es wichtig, dass alle Aktivitäten durch eine zentrale, gut abgestimmte Koordination gelenkt werden, um Ausfälle, die sich gegenseitig verstärken könnten, zu verhindern. Es wird empfohlen, ein zentrales Gremium zu ernennen, das die Umsetzung von Maßnahmen zur Erhöhung der Resilienz auf allen Verwaltungsebenen überwacht und sicherstellt.

01 EIN DIGITALES KONZEPT FÜR WICHTIGE ÖFFENTLICHE DIENSTE UND REGISTER EINFÜHREN

Eine Schlüsselkomponente für jeden digitalen Staat ist die Entwicklung und Pflege digitaler Register. Diese Register sind für die Pflege aktueller Informationen über alle Aspekte des Staates, von der Registrierung von Geburten bis zur Verwaltung von Immobilieneigentum von Bedeutung. Damit ein solches Register-System effektiv funktioniert, sind die Staaten auf das Vertrauen der Öffentlichkeit in die staatlichen Institutionen sowie auf ein Rechtssystem angewiesen, das die Rechte der Bürger*innen angemessen schützt.

Im digitalen Zeitalter werden die Eigentumsverhältnisse größtenteils durch Daten in digitalen Registern und verschiedenen Systemen definiert, die über den öffentlichen und privaten Sektor verteilt sind. Das Eigentum an zentralen Aspekten des Lebens – wie Elternschaft, Besitztümern, Bildung, Erbschaft, Gesundheitsdaten, Aktien oder Vermögen – ist zunehmend digital verankert. In einem solchen System nehmen digitale Daten und Informationen eine vorrangige Rolle gegenüber physischen Alternativen ein, da diese die effizienteste und widerstandsfähigste Grundlage für die Governance in der modernen Welt bieten.

Die meisten modernen Verwaltungen haben inzwischen digitale Register und Online-Dienste eingeführt, doch die Transformation bleibt häufig fragmentarisch und unvollständig. So ist es in einigen Staaten beispielsweise möglich, einen Führerschein online zu beantragen, während die physische Abholung des Dokuments weiterhin erforderlich bleibt – ein hybrider Ansatz, der das Potenzial digitaler Prozesse nur teilweise ausschöpft. Die Grenzen einer breiteren Digitalisierung hängen fast immer direkt mit veralteten Verfahren, rechtlichen Rahmenbedingungen oder mangelndem Vertrauen zusammen.

Aus diesem Grund dürfen digitale Staaten nicht nur in Technologie investieren, sondern müssen ihre internen Prozesse und Abläufe erneuern. Dies kann dadurch geschehen, dass sie einen “Digital-First”-Ansatz für den öffentlichen Sektor wählen. Die digitalen Register, Dienste und Informationen, die für den Fortbestand des Staates von entscheidender Bedeutung sind, müssen von überall aus zugänglich sein (d. h. digital) und durchgängige Ergebnisse liefern.

Damit dies gelingt, müssen die Staaten festlegen, welche Register, Dienste und Informationen als “kritisch” für die langfristige Resilienz des digitalen Staates eingestuft werden.

Im Folgenden werden vier Kategorien vorgestellt, die sich nach ihrer Bedeutung für die Kontinuität des Staates und nach ihrer Relevanz für die Sicherstellung kritischer öffentlicher Dienstleistungen weiter unterteilen lassen.

1. **Öffentliche Verwaltung.** Zu den Dienstleistungen dieser Kategorie gehören Wahlen und Abstimmungen, die Dokumentation von Gesetzen und Vorschriften, staatlichen Entscheidungen und staatlichen Bekanntmachungen. Langfristige Krisen wie ein Krieg haben wahrscheinlich erhebliche Auswirkungen auf diese Kategorie.

2. **Register für Eigentum, Steuer und Recht.** Zu dieser Kategorie gehören die wichtigsten Register: Melderegister, Unternehmensregister, Eigentumsregister (Kataster, Fahrzeuge usw.), Steuern, Strafregister und Register für andere rechtliche Fakten.

3. **Dienstleistungen für Bürger*innen.** Zu dieser Kategorie gehören Dienstleistungen wie die Beschaffung neuer Pass- und Identitätsdokumente, international anerkannte Lizenzen und Zertifikate (z. B. über die Ausbildung), der Bezug von Sozialleistungen und die Zahlung von Steuern. Sie umfasst auch Dienstleistungen im Zusammenhang mit der Bewahrung der nationalen Identität, wie z. B. den Zugang zum nationalen Archiv, zum Archiv des öffentlichen Rundfunks, zu Bibliotheken und allgemein den Zugang zu Bildungsmaterialien.

4. **Internationale Zusammenarbeit mit Nachbarstaaten.** Diese Kategorie umfasst Dienste, die den Austausch von Informationen über Ländergrenzen hinweg ermöglichen. Solche Dienste sind besonders hilfreich in Krisen, wenn viele Menschen in ein anderes Land flüchten. Sie können den Betroffenen beispielsweise eine digitale Identität bereitstellen, die problemlos mitgenommen und genutzt werden kann.

Für Dienste, die von Dritten (z. B. privatwirtschaftlichen Einrichtungen) verwaltet werden oder in deren Besitz sind, könnte ein Mechanismus eingeführt werden, der Anreize für die digitale Entwicklung schafft. Bei der Beschaffung von Lehrbüchern für Kinder sollten z. B. auch digitale Versionen verlangt werden. Im Gegensatz zu Büchern, die beschädigt oder unzugänglich werden können, bleiben digitale Lehrmaterialien auch in Krisenzeiten weiter zugänglich.

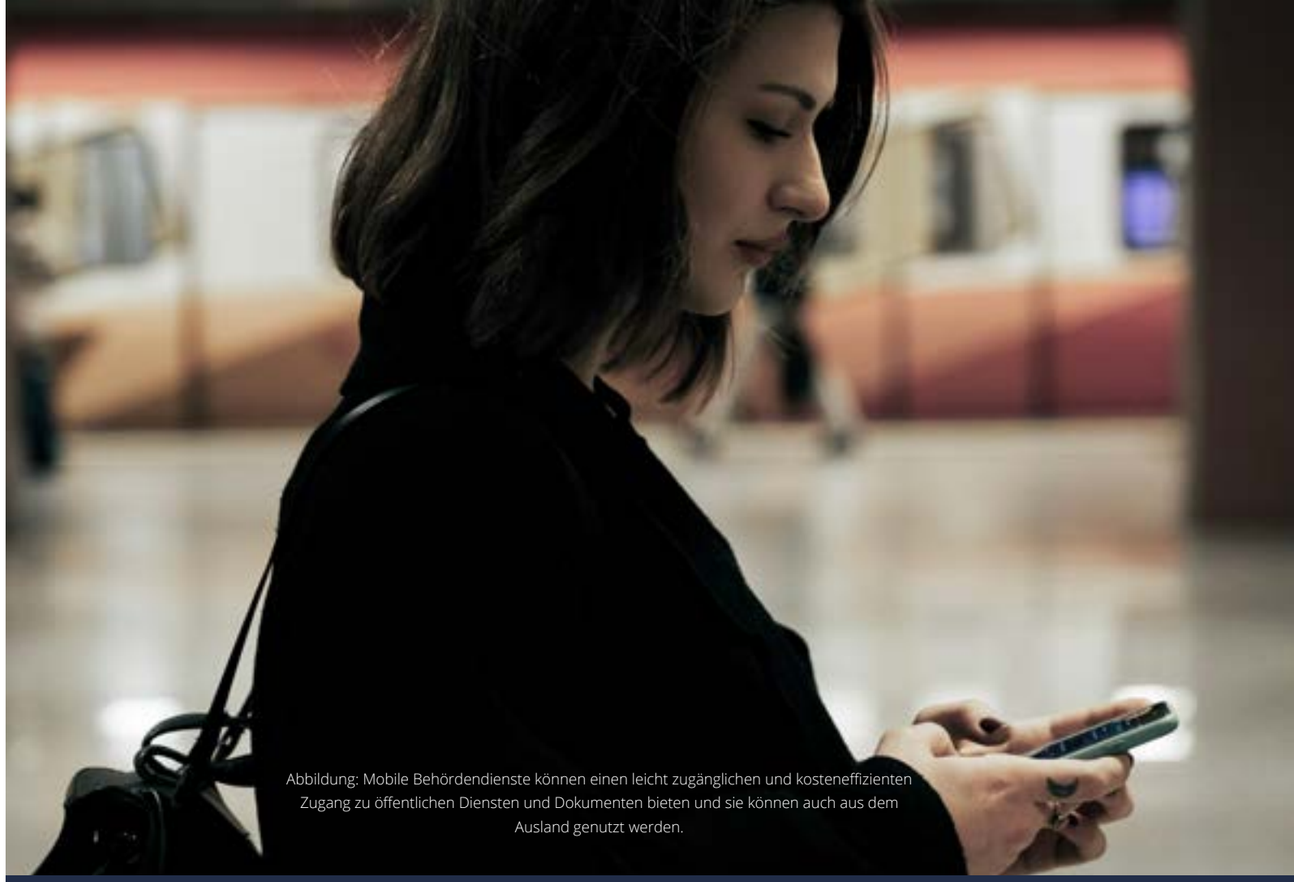


Abbildung: Mobile Behördendienste können einen leicht zugänglichen und kosteneffizienten Zugang zu öffentlichen Diensten und Dokumenten bieten und sie können auch aus dem Ausland genutzt werden.

WICHTIGE EMPFEHLUNGEN:

- → Identifizieren Sie Dienste und Register, die für die Kontinuität des Staates und in verschiedenen Notstandsszenarien entscheidend sind.
- → Installieren Sie eine Politik, die die digitale Transformation jener öffentlichen Dienste vorschreibt, die für den langfristigen Fortbestand des Staates als unerlässlich gelten.
- → Verabschieden Sie Gesetze, die der Entwicklung von Digital-First-Diensten und -Assets Vorrang einräumen und die die Einhaltung etablierter Sicherheitsstandards und -anforderungen gewährleisten.

02 ZU “REMOTE-FIRST”- UND “REMOTE-ENABLED”-ARBEITSPLÄTZEN IM ÖFFENTLICHEN SEKTOR ÜBERGEHEN

Die Einführung digitaler Ansätze in der Bereitstellung öffentlicher Dienstleistungen macht diese effizienter, automatisierter und vorausschauender. Dadurch werden Personalressourcen entlastet. Dennoch bleibt es Aufgabe der öffentlichen Bediensteten, die Systeme funktionsfähig und sicher zu halten.

Besonders in Krisenzeiten ist es entscheidend, dass Mitarbeiter*innen, die an kritischen Diensten arbeiten, ihre Aufgaben erfüllen können – selbst wenn Notfälle oder andere Einschränkungen wie das Arbeiten vor Ort dies erschweren.

Eine Lösung besteht darin, diesen Mitarbeiter*innen die Möglichkeit zu geben, vollständig remote zu arbeiten. Um ein “remote-first”-Modell für den öffentlichen Sektor erfolgreich einzuführen, müssen drei zentrale Aspekte beachtet werden:

1. Die Umstellung auf sichere, digitale Kommunikationskanäle.

2. Gewährleistungen des remote zugänglichen Betriebs interner Systeme, Software und Infrastruktur.

3. Schaffung neuer digitaler Strukturen für Führung, Prozesse und Prüfmechanismen, die speziell auf Remote-Arbeit ausgerichtet sind.

Diese Veränderungen sind zwar herausfordernd, aber essenziell, um die langfristige Resilienz eines digitalen Staates zu sichern. In den meisten Fällen stellt die Digitalisierung eines Dienstes oder seiner Infrastruktur den vergleichsweise einfachen Teil der Lösung dar.

> **Der schwierigste Teil ist die Umgestaltung der Organisation selbst, ihrer Entscheidungs-prozesse und ihrer Kultur.**

Häufig verlassen sich Behörden und Ämter auf Papier oder andere Ressourcen, auf die nur lokal zugegriffen werden kann, was die Möglichkeiten für Veränderungen und Remote-Zugriffe einschränkt.

Um diese Herausforderung zu meistern, kann ein Modell entwickelt werden, das zwischen “remote-first”- und “remote-enabled”-Jobs unterscheidet. „Remote-first”-Arbeitsplätze sind solche, bei denen es zwingend erforderlich ist, langfristig remote arbeiten zu können, wobei alle organisatorischen Prozesse und Systeme dies unterstützen. Remote-fähige Arbeitsplätze sind diejenigen, die unter bestimmten Bedingungen remote arbeiten könnten.

Es genügt nicht, lediglich Richtlinien oder Strategien für die Remote-Arbeit zu entwickeln – ihre konsequente Umsetzung ist entscheidend.

Ein digitaler Staat, der tatsächlich in der Lage ist, vollständig remote zu operieren, stärkt seine Resilienz gegenüber potenziellen Störungen erheblich. Diese Bereitschaft kann durch die Durchführung von Krisenübungen weiter optimiert werden. In kontrollierten Simulationen werden Krisenszenarien nachgestellt, um zu überprüfen, ob die etablierten Remote-Arbeitsprozesse den Anforderungen standhalten und wie geplant funktionieren. Solche Tests tragen wesentlich dazu bei, Schwachstellen zu identifizieren und die Resilienz des Systems weiter zu erhöhen.

WICHTIGE EMPFEHLUNGEN:

- → Identifizieren Sie Behörden und Schlüsselpositionen, die für die Aufrechterhaltung kritischer staatlicher Dienste essenziell sind. Entwickeln Sie ein System zur Kategorisierung von Rollen, die entweder vorrangig für Remote-Arbeit ausgelegt sein sollten oder eine flexible Remote-Arbeitsfähigkeit erfordern.
- → Identifizieren Sie Infrastrukturen und Systeme, die aus der Remote-First-Perspektive nicht zugänglich sind.
- → Legen Sie eine langfristige IT- und Organisationsstrategie für die Umstellung auf remote-first und remote-fähige Arbeitsplätze fest.
- → Richten Sie eine unabhängige Stelle ein, die für die Bewertung der organisatorischen Hindernisse für den Übergang zur Remote-Arbeit zuständig ist und die jährlich oder vierteljährlich Übungen durchführt, bei denen die Fähigkeit, unter Remote-Bedingungen zu arbeiten, getestet wird.

03 DIGITALE ÖFFENTLICHE INFRASTRUKTUREN UND DIENSTE SICHERN

Im digitalen Zeitalter hat sich der Begriff des Konflikts verändert. Cyberangriffe sind an der Tagesordnung und ein unvermeidlicher Teil der neuen digitalen Realität. Im Zuge der fortschreitenden Digitalisierung der Staaten ist es unerlässlich, die Cybersicherheit und den Schutz der digitalen Infrastruktur zu gewährleisten. Estland wurde im Jahr 2007 Opfer einer der ersten landesweiten Cyberangriffe der Welt. Daraufhin führte Estland neue Gesetze und Vorschriften ein, entwickelte Standards und setzte große Mengen an Ressourcen zur Verbesserung seiner Cyberabwehrkapazitäten ein. In den vergangenen Jahren ist es Estland gelungen, zahlreiche massive Cyberangriffe erfolgreich abzuwehren, ohne dass es zu nennenswerten Störungen der digitalen Infrastruktur kam. In den meisten Fällen haben die Bürger*innen Estlands nicht einmal bemerkt, dass solche Ereignisse stattgefunden haben.

Diese Bedrohung wird jedoch immer vorhanden sein. Da ein großer Teil der kritischen Infrastruktur eines Staates digital funktioniert – sogar physische Infrastrukturen wie Kraftwerke oder Krankenhäuser – muss der Cyberschutz nationale Priorität sein. In den vergangenen Jahrzehnten hat sich zunehmend gezeigt, dass es zwar technisch möglich ist, Systeme durch robuste Abwehrmaßnahmen und schützende Barrieren abzusichern, jedoch bleibt kein System unkompromittierbar. Ein entschlossener Angreifer mit ausreichenden Ressourcen und großer Zielstrebigkeit wird Wege finden, die Verteidigungsmechanismen zu überwinden und Zugang zu seinem Ziel zu erlangen.

> **Da es im Cyberspace keinen Frieden gibt, müssen digitale Systeme immer unter dem Gesichtspunkt der Resilienz im Kriegsfall entwickelt werden.**

Investitionen in die Cybersicherheit können nicht nachträglich getätigt werden, sondern müssen von Anfang an umgesetzt werden. Die effektivste langfristige Strategie für einen digitalen Staat besteht darin, klare Grundsätze zu entwickeln, die – sofern konsequent umgesetzt – die Kosten und den Zeitaufwand für potenzielle Angreifer erheblich steigern. Da Bedrohungen jedoch stetig komplexer und dynamischer werden, müssen auch die Abwehrmaßnahmen kontinuierlich weiterentwickelt werden.

Digitale Staaten sollten moderne Technologien und Lösungen einsetzen, um Cybervorfälle proaktiv zu überwachen, zu analysieren und zu bekämpfen. Dazu gehören der Einsatz von cloudbasierten Bedrohungsplattformen, maschinellem Lernen und künstlicher Intelligenz, um Angriffsstrategien zu erkennen und zu antizipieren.

Die gesammelten Bedrohungsdaten müssen in Echtzeit über nationale und internationale Kooperationsplattformen geteilt werden, insbesondere mit gleichgesinnten Staaten. Dieser Austausch stärkt die Fähigkeit zur Koordination und schnellen Reaktion, wodurch die Resilienz gegenüber Cyberbedrohungen maßgeblich verbessert wird.

Zusätzlich zu den externen Bedrohungen müssen die Länder den digitalen Staat auch vor internen Bedrohungen schützen. Die Datenintegrität muss zur Priorität gemacht werden, damit niemand Daten ändern kann, ohne Spuren zu hinterlassen. Die estnische Regierung hat damit begonnen, Technologien wie Blockchain zu nutzen, um sicherzustellen, dass wichtige Register nicht manipuliert werden können [22].

Um die Cybersicherheit in den Vordergrund zu stellen, muss ein digitaler Staat seine nationalen und institutionellen Cyberkapazitäten ausbauen. Durch die Zusammenarbeit zwischen Behörden, Dienstleistern, Forschung, Universitäten und Unternehmen ist es möglich, zur Entwicklung entsprechenden Fachwissens beizutragen.

WICHTIGE EMPFEHLUNGEN:

- → Gewährleisten Sie die landesweite Einhaltung von Cybersicherheitsstandards und bewährten Praktiken der Branche. Berücksichtigen Sie dabei nationale Risikoszenarien und setzen Sie entsprechende Mindestsicherheitsmaßnahmen durch..
- → Stufen Sie die Informationssysteme nach ihrer Sicherheit und Kritikalität ein und stellen Sie die gegenseitigen Abhängigkeiten dieser Systeme dar. Priorisieren Sie die Aufrechterhaltung der Kontinuität der Systeme mit den größten Auswirkungen.
- → Konsolidieren Sie die Überwachung und Analyse von Cybervorfällen in einer zentralen Stelle, um ein umfassendes Situationsbewusstsein auf nationaler Ebene zu schaffen und eine schnelle Eindämmung sowie Reaktion auf Vorfälle zu ermöglichen.
- → Stellen Sie sicher, dass ein ausreichendes, kontinuierliches Budget für Investitionen in Cybersicherheit zur Verfügung steht, um das Risiko in einem schnelllebigen Bedrohungsumfeld zu minimieren. Es wird empfohlen, mindestens 10 Prozent des IT-Budgets für Cybersicherheit zu verwenden.
- → Verbessern Sie die nationalen und institutionellen Fähigkeiten im Bereich der Cybersicherheit. Stärken Sie die Zusammenarbeit mit Forschungseinrichtungen und vertrauenswürdigen Partnern, um die Schutzstandards kontinuierlich zu verfeinern und so neuen sowie zukünftigen Bedrohungen wirksam zu begegnen.
- → Ernennen Sie eine Organisation, die für die Cybersicherheit im Land verantwortlich ist und über die nötigen Durchführungsbefugnisse für alle oben genannten Maßnahmen verfügt.

04 EINEN WEIT VERBREITETEN, ERSCHWINGLICHEN ZUGANGS ZU KONNEKTIVITÄT UND REDUNDANZ GEWÄHRLEISTEN

Jeder Verlust der Verbindung während einer Krise führt dazu, dass die Menschen praktisch vom Staat und seinen Dienstleistungen abgeschnitten sind. In der heutigen digitalen Welt ist der Zugang zum Internet genauso wichtig wie der Zugang zu grundlegenden Infrastrukturen und wichtigen Versorgungseinrichtungen.

Länder wie Finnland und Estland haben politische Maßnahmen ergriffen, um den Internetzugang als grundlegende Infrastruktur – oder sogar als Menschenrecht – zu betrachten. Sie haben es zur nationalen Priorität gemacht, allen Bürger*innen einen Breitbandzugang zu ermöglichen. Diese Länder zeigen auch eine starke Verbindung zwischen der Verfügbarkeit von Internet und dem Fortschritt in der Digitalisierung insgesamt.

Der Internetzugang muss daher nicht nur weit verbreitet, sondern auch robust und widerstandsfähig gegenüber Manipulationen und äußeren Angriffen sein. Staaten sollten gezielt daran arbeiten, den Zugang zum Internet und dessen Abdeckung auf ihrem gesamten Gebiet zu verbessern. Wo immer möglich, sollten sie kostenlose öffentliche Zugangspunkte bspw. an Schulen, Bibliotheken und anderen zentralen Einrichtungen einrichten.

Der freie Markt und der Wettbewerb sollten gewährleistet sein, um die Kosten für den Internetzugang zu senken und eine größere Vielfalt an Angeboten zu erreichen.

Staaten können Anreize, Subventionen, Steuerbefreiungen, lizenzfreie Erleichterungen usw. für neue Telekommunikationsunternehmen schaffen, die in den lokalen Markt eintreten, um den Wettbewerb zu erhöhen.

Mit einer flächendeckenden und erschwinglichen Breitbandverbindung könnten Staaten auch in Betracht ziehen, eine begrenzte, kostenfreie 4G/5G-Option anzubieten. Diese könnte ausschließlich für den Zugang zu bestimmten Diensten wie Nachrichten oder öffentlichen Dienstleistungen genutzt werden.

Der Aufbau von Redundanz in der Konnektivität ist entscheidend für die Resilienz in Krisenzeiten. In Konflikten kann die Internetinfrastruktur selbst gefährdet sein: Unterseekabel sind anfällig für Sabotage und Zerstörung. Staaten müssen dies berücksichtigen und in neue Kommunikationstechnologien investieren. Ein Beispiel hierfür wäre die Einführung von Satellitenkommunikationssystemen, die helfen können, Störungen herkömmlicher Internetverbindungen zu überwinden.

Um die Resilienz im Krisenfall weiter zu erhöhen, sollten Netzbetreiber zu Interoperabilität verpflichtet werden. Grenzüberschreitende Interoperabilität erhöht die Resilienz weiter. Der Staat sollte für die erforderlichen Vereinbarungen zwischen den Telekommunikationsanbietern sorgen. Das beste Beispiel für diesen Ansatz ist die Ukraine. Wenige Tage nach Beginn der russischen Invasion in der Ukraine im Jahr 2022 aktivierten die drei wichtigsten Mobilfunkbetreiber des Landes einen kostenlosen Roaming-Dienst zwischen ihren jeweiligen Netzen [23]. Wenn das Signal des Mobilfunknetzes für Nutzer*innen nicht mehr verfügbar ist, wird ihnen geraten, es bei einem der beiden anderen Anbieter zu versuchen.

WICHTIGE EMPFEHLUNGEN:

Richten Sie eine Stelle ein (z. B. National Connectivity Board), die folgende Aufgaben umfasst:

- → Sicherstellen, dass es für alle Bürger*innen erschwingliche Internetanschlussmöglichkeiten gibt.
- → Durchführung einer Risikoanalyse der bestehenden nationalen Verbindungsoptionen und Einführung einer strategischen Diversifizierung der Verbindungsarten.
- → Übungen zur Kontinuität der nationalen digitalen Infrastruktur in Szenarien mit reduzierter Internetverbindung. Implementierung strenger Testprotokolle, um sicherzustellen, dass kritische Systeme auch bei Netzunterbrechungen betriebsbereit bleiben.
- → Senkung der Kosten für die Anbindung entweder durch Subventionen und Anreize für neue Telekommunikationsanbieter oder durch direkte Vorteile für die Endnutzer*innen.
- → Schaffung von Interoperabilität zwischen Telekommunikationsanbietern

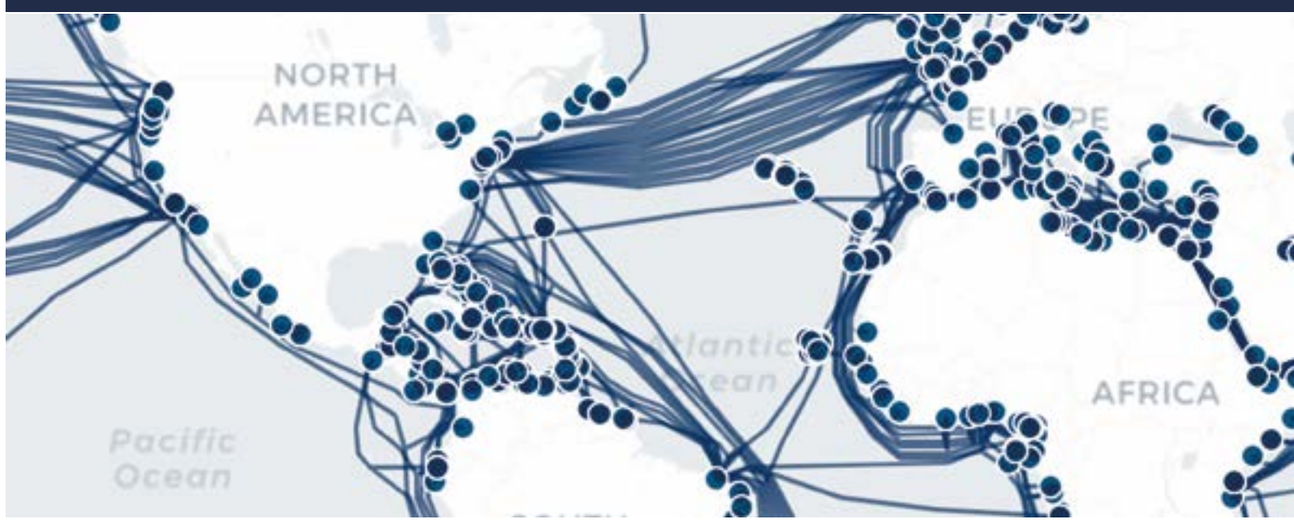


Abbildung: Unterseekabel verbinden die digitale Welt miteinander, sind aber auch anfällig für Sabotage.
Die Staaten müssen ihre Konnektivität durch mehrere Technologieoptionen verbessern.

05 REDUNDANZ IN DER DIGITALEN ÖFFENTLICHEN INFRASTRUKTUR AUFBAUEN

Das Ausmaß, in dem sich moderne Gesellschaften auf digitale Register und öffentliche digitale Infrastruktur verlassen, ist enorm. Die meisten staatlichen Datenbanken sind digital und im Falle von Ländern wie Estland sind es sogar fast alle öffentlichen Dienste. Die Zerstörung wichtiger Register oder der digitalen Infrastruktur wäre verheerend.

Eine zentrale Schwachstelle digitaler Staaten liegt in der Abhängigkeit ihrer digitalen Daten und Vermögenswerte von physischen Standorten. Sind diese Standorte bekannt, können sie gezielt beschädigt oder zerstört werden. Ohne adäquate Backups wäre der Staat dann nicht mehr in der Lage, essenzielle Dienstleistungen aufrechtzuerhalten. Im Extremfall könnte eine solche Krise die Legitimität des Staates schwer erschüttern. Darüber hinaus bergen zentrale digitale Register ein erhebliches Risiko, falls sie in die Hände eines Gegners geraten. Ein solcher Zugriff könnte dazu genutzt werden, den Datenbestand massiv zu kompromittieren – etwa durch das Löschen von Personen- oder Unternehmensdaten, die Manipulation von Eigentumsrechten oder sogar durch Eingriffe in die finanziellen Systeme des Staates.

Aus diesem Grund versuchen sich Staaten auf ein potenzielles Katastrophenszenario vorzubereiten, bei dem öffentliche Daten, die für die Kontinuität und Legitimität des Staates notwendig sind, unter keinen Umständen manipuliert oder zerstört werden können.

Eine Lösung hierfür ist die estnische Datenbotschaft [24], in der wichtige staatliche Register und digitale Vermögenswerte auf dem Gebiet eines anderen souveränen Landes gesichert und gespeichert werden. Im Falle einer Katastrophe können die in der Datenbotschaft gespeicherten Daten genutzt werden, um den rechtmäßigen Zustand des Staates wiederherzustellen und sicherzustellen, dass keine Manipulationen vorgenommen wurden. Als diese Strategie konzipiert wurde, war sie logisch. Es gab weniger Systeme, die Abhängigkeiten waren überschaubar und die Menge der Daten war deutlich geringer.

Es wurde auch angenommen, dass Bedrohungen nur kurzfristig auftreten und Krisen wenige Tage, Wochen oder Monate andauern würden. Heute ist klar, dass diese Sichtweise zu optimistisch war.

In einer Zeit, in der digitale Systeme eng vernetzt und komplex sind, müssen langfristige Lösungen sicherstellen, dass Daten und Systeme nicht nur geschützt, sondern auch weiterhin betriebsfähig bleiben – sei es vor Ort oder von anderen Standorten im Land aus.

> **Anstelle einer landesweiten Archivierungslösung ist es umso wichtiger, eine Idee einer digitalen Botschaft im Ausland weiterzuentwickeln.**

Diese Lösung würde es ermöglichen, eine souveräne Cloud auf fremdem Staatsgebiet zu duplizieren und digitale Dienste von dieser Botschaft aus zu betreiben.

Der Krieg in der Ukraine hat die praktische Notwendigkeit einer solchen Lösung deutlich gemacht. Als Kiew 2022 teilweise eingekesselt war, wurde deutlich, dass die Ukraine in eine schwierige Lage geraten würde, wenn sie den Zugang zu ihren wichtigsten digitalen Diensten verliert. Nach dem Vorbild der estnischen Datenbotschaft wurden Anstrengungen unternommen, Datenzentren in befreundete Länder zu verlagern [25]. Die digitale Kontinuität der Ukraine wird aktuell durch NATO-Länder und in NATO-Gebieten tätige Unternehmen gewährleistet wird.

Der Aufbau einer resilienten und flexiblen Cloud-Umgebung wird keine leichte Aufgabe werden. Staaten sollten sich zuerst darauf konzentrieren, kritische öffentliche Dienste und Infrastrukturen in lokale oder internationale Clouds zu verlagern. Dieser Wandel braucht umfassende Unterstützung durch Gesetze und Vorschriften. Das bedeutet, bestehende rechtliche Hürden abzubauen und gleichzeitig die nötigen Kapazitäten zu schaffen – besonders im Bereich der internationalen Zusammenarbeit.

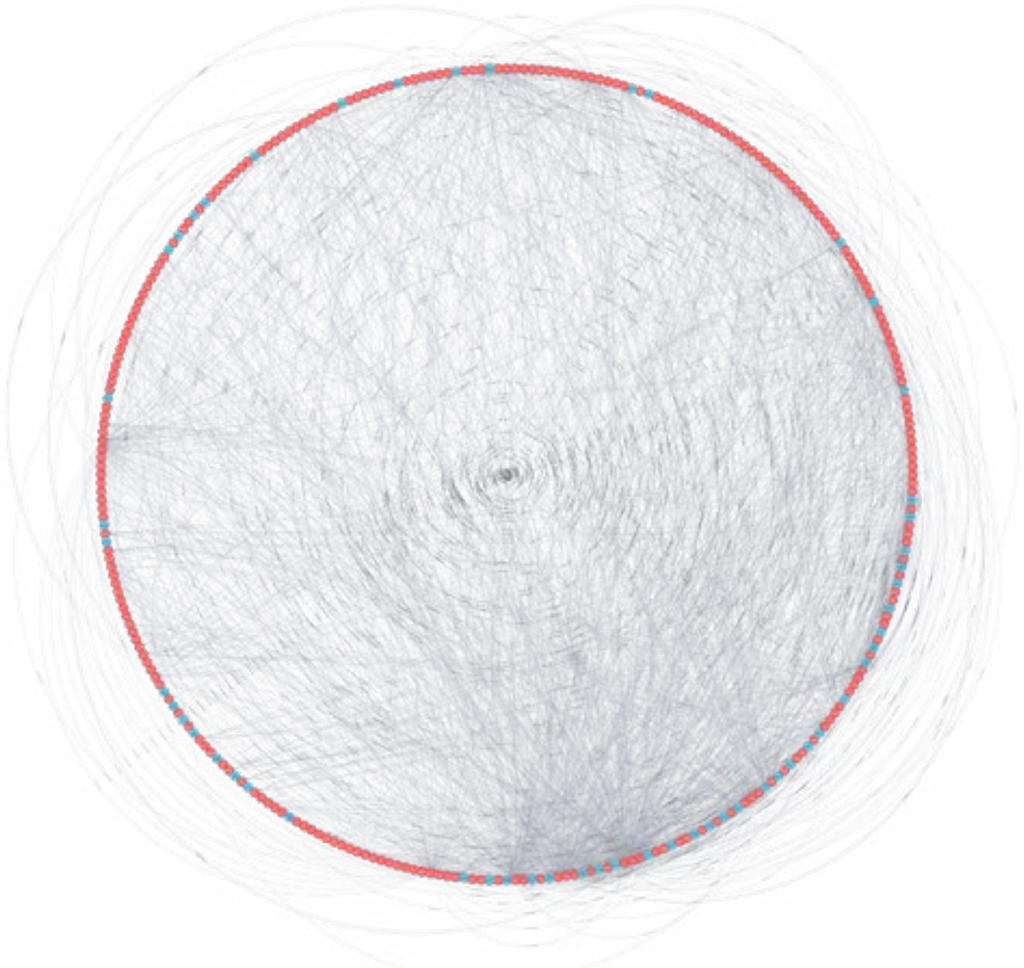


Abbildung: Integration und Datenaustausch von digitalen Verwaltungssystemen in Estland. Ohne einen ganzheitlichen Ansatz für die Resilienz könnte ein einzelnes ausfallendes kritisches System einen sich ausbreitenden Kaskadenausfall verursachen.

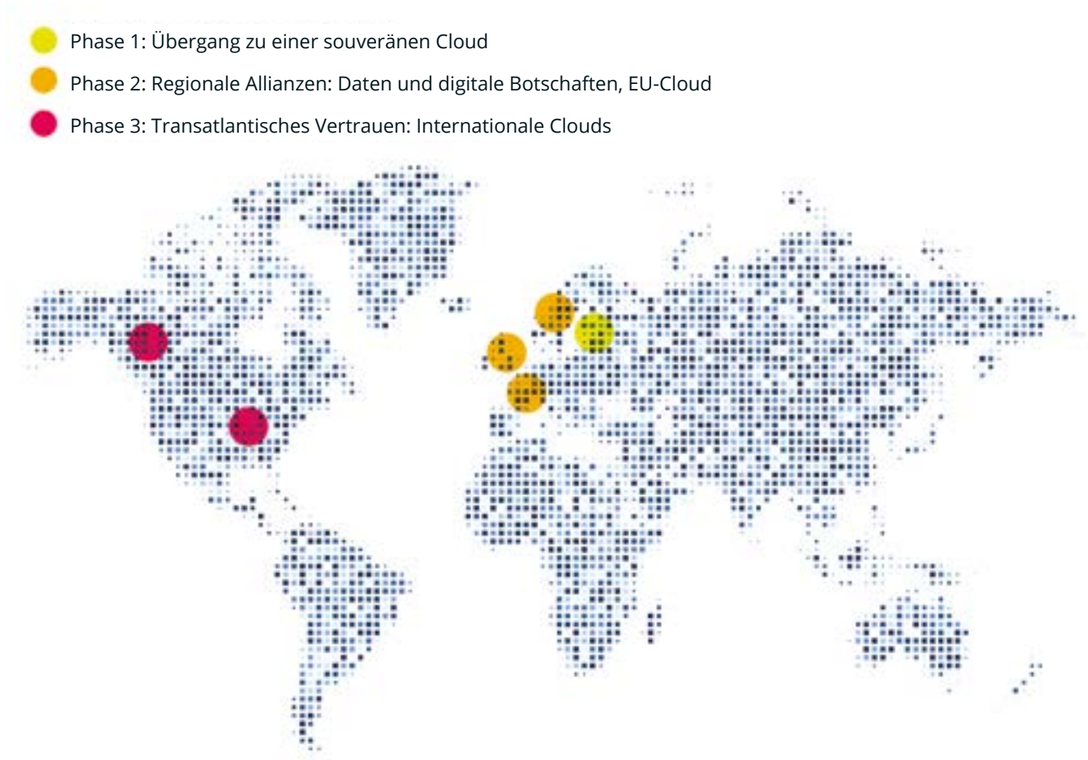


Abbildung: Schrittweiser Übergang zu breiteren internationalen Allianzen auf der Grundlage von gegenseitigem Vertrauen und Vereinbarungen. Die Orte auf der Karte dienen nur zur Veranschaulichung.

WICHTIGE EMPFEHLUNGEN:

- → Definieren Sie nationale Standards: Legen Sie verbindliche Standards fest, die sicherstellen, dass kritische öffentliche Dienste und Infrastrukturen innerhalb eines festgelegten Zeitrahmens cloudkompatibel werden. Stellen Sie sicher, dass diese Standards verpflichtend für alle staatlichen Systemanschaffungen und internen Entwicklungen gelten.
- → Analysieren Sie bestehende Strukturen: Führen Sie eine umfassende Bewertung der aktuellen kritischen öffentlichen Dienste und Infrastrukturen durch, um Schwachstellen zu identifizieren, die den Übergang zur Cloud behindern könnten.
- → Fördern Sie internationale Kooperationen: Arbeiten Sie eng mit multinationalen Partnern und Regulierungsbehörden zusammen, um Vertrauen und Kontrolle bei der Nutzung von Cloud-Diensten sicherzustellen.
- → Etablieren Sie eine nationale Koordinierungsstelle: Gründen Sie ein National Cloud Governance Centre, das als zentrale Instanz für die Verwaltung der Cloud-Infrastrukturen dient. Übertragen Sie dieser Stelle die Verantwortung für Marktforschung, Risikomanagement, Beschaffung, Interoperabilität und die Definition von Mindestsicherheitsanforderungen. Fördern Sie darüber hinaus den Übergang zur Cloud, indem Sie Behörden mit gezielten Anreizen unterstützen.

06 DAS DRITTPARTEIRISIKO BEI GLEICHZEITIGER WAHRUNG DER TECHNOLOGISCHEN INNOVATION BEWÄLTIGEN

Da die digitale Welt zunehmend global und vernetzt wird, gewinnt das Risikomanagement von Drittanbietern an strategischer Bedeutung. Viele Technologien basieren auf Komponenten von externen Lieferanten, was bedeutet, dass ein Angriff auf einen Teil der Liefer- oder Abhängigkeitskette gravierende Folgen haben kann. Nur durch umfassende Sicherheitsmaßnahmen und die Einhaltung von Vorschriften entlang der gesamten Kette können Systeme als sicher gelten. Ein bekanntes Beispiel für einen solchen Angriff ist der Vorfall bei SolarWinds, der massive Auswirkungen auf die nationale Sicherheit der USA hatte [26].

Das Management von Risiken durch Drittanbieter ist komplex und wird zunehmend anspruchsvoller. Staaten müssen strategische Entscheidungen darüber treffen, welche Software und Hardware sie nutzen und gleichzeitig die Fähigkeit entwickeln, die globale digitale Lieferkette kontinuierlich zu überwachen. Während die Sicherheit und Konformität einiger weniger Produkte überprüft werden kann, ist es nahezu unmöglich, die vollständige Einhaltung für alle digitalen öffentlichen Dienste, Infrastrukturen und deren Abhängigkeiten in vollem Umfang sicherzustellen. Dies übersteigt die Kapazitäten der Regulierungsbehörden.

Je nach Staat und seiner Haltung gegenüber der internationalen Gemeinschaft können unterschiedliche Ansätze zur Bewältigung dieser Herausforderungen gewählt werden. Ein risikoabgewogener Ansatz könnte beispielsweise darin bestehen, je nach Bedeutung und Kritikalität eines Dienstes eine risikoorientierte Strategie zu verfolgen. In diesem Fall würden für besonders wichtige Systeme strengere Anforderungen gelten, während weniger kritische Systeme möglicherweise weniger intensiven Prüfungen unterzogen werden oder nur freiwillige Einhaltung gefordert wäre.

Es ist jedoch wichtig zu beachten, dass nicht alle Risiken vollständig beseitigt werden können. Viele Staaten sind auf ausländische Technologien angewiesen, für die es oft keine Alternativen gibt. Ein Beispiel dafür ist das Global Positioning System (GPS), das eine grundlegende Technologie für viele moderne Dienste mit begrenzter Konkurrenz und geringer Akzeptanz für

diese Alternativen darstellt. Auch wenn größere Staaten möglicherweise eigene Systeme entwickeln können, werden sie in der Regel auf Drittanbieter-Komponenten angewiesen sein. Aus diesem Grund arbeiten Regulierungsbehörden daran, langfristige Service-Level-Vereinbarungen (SLAs) zu entwickeln, die sicherstellen, dass nationale Anforderungen eingehalten werden.

Die Hauptaufgabe beim Risikomanagement für Drittanbieter besteht darin, ein Gleichgewicht zwischen der Förderung von Offenheit und Innovation einerseits und der notwendigen Regulierung sowie Risikominderung andererseits zu finden.

Um dem Risiko einer Einschränkung der Innovation entgegenzuwirken, sollte eine risikotolerante Ausweichstrategie angewandt werden. Beispielsweise sind KI-Tools meist cloudbasiert und ihr Einsatz im Rahmen des digitalen Staates könnten eine “Black Box”-Abhängigkeit schaffen. Mit einer risikofreudigen Herangehensweise könnte diese Abhängigkeit zwar nicht komplett entfernt, jedoch so gestaltet werden, dass sie bei Bedarf ausgeschaltet werden kann. Das könnte die Nutzererfahrung beeinträchtigen, doch es würde verhindern, dass der Dienst bei Störungen aufgrund dieser Abhängigkeit komplett ausfällt.

WICHTIGE EMPFEHLUNGEN:

- → Legen Sie eine landesweite Risikomanagement-Strategie für den Umgang mit Risiken durch Drittanbietern fest. Diese Politik sollte klare Regeln definieren, welche Systeme herstellereigene Technologien nutzen dürfen und welche nicht. Außerdem sollte festgelegt werden, ob ein System in Notfällen auch ohne diese Technologien funktionsfähig bleiben muss. Achten Sie darauf, dass die Regeln praktikabel, umsetzbar und leicht überprüfbar sind.
- → Setzen Sie das Risikomanagement für Drittanbieter gemäß den gängigsten Technologie- und Sicherheitsstandards durch eine zentrale Behörde um. Diese Behörde muss in der Lage sein, Veränderungen in der Lieferkette zu überwachen und darauf zu reagieren sowie kosteneffiziente und risikominimierende Alternativen zu identifizieren.
- → Richten Sie eine Prüfbehörde ein, die die Einhaltung der festgelegten Risikomanagementpolitik für kritische öffentliche Dienste und Infrastrukturen überwacht.
- → Testen Sie regelmäßig die Resilienz gegenüber Risiken durch Drittanbieter, indem Sie die relevanten Aspekte der Risikomanagementpolitik prüfen und üben.
- → Arbeiten Sie eng mit multinationalen Regulierungsbehörden zusammen, um die globalen Risiken durch Drittanbieter zu managen und das Wissen mit Partnern in Staaten, die ähnliche Werte und Prinzipien haben, zu teilen.

07 INSTITUTIONELLE KAPAZITÄTEN FÜR DIE ENTWICKLUNG DER RESILIENZ VON REGIERUNGEN SCHAFFEN

Die Resilienz der öffentlichen Verwaltung und Pläne zur Aufrechterhaltung des staatlichen Betriebs betreffen alle Bereiche des Staates. Jede Behörde sollte dafür verantwortlich sein, ihre eigene Resilienz sicherzustellen, was bedeutet, dass ein dezentraler Ansatz notwendig ist. Das umfasst sowohl konkrete Notfallpläne als auch die kontinuierliche Verbesserung der Fähigkeiten, digitale Dienstleistungen aufrechtzuerhalten. Es wird empfohlen, in jeder Behörde eine*n speziellen Resilienzbeauftragte*n zu ernennen, der*die die Pläne entwickelt und die Zusammenarbeit mit anderen Behörden und Partnern aus dem Privatsektor koordiniert.

Um jedoch die Risiken eines kaskadenartigen Ausfalls von digitalen Diensten zu mindern und die praktischen Herausforderungen der Zusammenarbeiten vieler Behörden zu bewältigen, wird ein zusätzlicher Top-down-Ansatz empfohlen. Die Einführung einer landesweiten Politik erfordert in der Regel eine zentrale Ebene, die über die nötige Autorität und langfristige Stabilität verfügt, um die Umsetzung effektiv durchzusetzen.

Staaten sollten ein zentrales Gremium schaffen, das für die Überwachung, Koordination und Umsetzung von Maßnahmen zur Erhöhung der Resilienz der öffentlichen Verwaltung und der Sicherstellung der staatlichen Kontinuität zuständig ist. Diese Einheit sollte an einer geeigneten Stelle angesiedelt sein, beispielsweise im Staatssekretariat oder einer ähnlichen zentralen Funktion, um effektiv arbeiten zu können.

Das Gremium wäre zuständig für:

1. Krisenpläne in allen Behörden
2. Analyse der wechselseitigen Abhängigkeiten zur Ermittlung von Kaskadenfehlern und deren Beseitigung
3. Durchführung von Übungen zur Resilienz von öffentlichen Verwaltungen und Prüfung der Resilienz von Regierungsorganisationen
4. Aufbau von Krisenmanagementkompetenz
5. Durchführung der Koordinierung des Krisenmanagements in einer Krise mit vertikaler Machtstruktur
6. Politische Analyse und Koordinierung der erforderlichen Änderungen der Rechtsvorschriften

BEISPIEL FÜR EINE RESILIENZÜBUNG DER ÖFFENTLICHEN VERWALTUNG.

→ In einem Beispielszenario eines staatlichen Bekanntmachungsdienstes sind alle Mitarbeiter*innen gezwungen, remote zu arbeiten, weil das Dienstgebäude abgeriegelt wird, um ein schweres Krisenszenario zu simulieren. Gleichzeitig wird eine künstliche Belastungsspitze des Dienstes erzeugt, um zu simulieren, dass Menschen aufgrund der Art der Krise auf den Dienst zugreifen. Um die Situation realistisch zu gestalten, ist der Dienst auch einem extremen Cyberangriff ausgesetzt, der den digitalen Zugang zum Dienst verwehrt. In einem idealen Ergebnis der Übung bestehen lediglich minimale bis gar keine Dienstunterbrechungen für die Bürger*innen.

DIE ZUKUNFT RESILIENTER DIGITALER STAATEN

Der künftige resiliente digitale Staat nutzt die Möglichkeiten der Digitalisierung, um seine Kontinuität zu gewährleisten. Er ist vollständig digitalisiert und weist eine geografische Standortunabhängigkeit für seine digitalen Kerndienste auf. Die Art und Weise, wie ein Staat dieses Ziel erreicht, hängt von dem jeweiligen Kontext ab, erfordert aber sicherlich, dass er zumindest einen Teil seiner digitalen Kerninfrastruktur außerhalb seiner territorialen Grenzen unterbringt. Dies stellt erhebliche Anforderungen an die Fähigkeiten des Staates, da die Sicherstellung des digitalen Betriebs ein höheres Maß an Reife und Koordinierung erfordert, als es derzeit der Fall ist.

Die oben aufgeführten Empfehlungen wurden aus der Perspektive der Entwicklung zunehmend resilienter digitaler Staaten gegeben. Diese Empfehlungen sollten jedoch nicht nur aus dem Blickwinkel der Unterstützung von Staaten bei der Bewältigung von Krisen betrachtet werden. Vielmehr können sie auch als Teil der Entwicklung verstanden werden, die die Welt durchläuft. Die digitalen Technologien verändern unsere Welt und die Art und Weise, wie wir in ihr leben, und auch die Staaten sind vor diesem Wandel nicht gefeit. Ohne Digitalisierung werden die Staaten nicht in der Lage sein, die wachsende Zahl und Komplexität der Krisen, mit denen sie in den kommenden Jahren konfrontiert sein werden, wirksam zu bewältigen. Während digitale Technologien wie KI unsere Welt weiter umgestalten, müssen auch die Staaten ihre Bereitschaft zur Anpassung zeigen.

Der Schlüssel zu dieser Anpassung wird die Fähigkeit eines Staates sein, die digitale Technologie in sein Verständnis selbst zu integrieren. Auch für die internationale Gemeinschaft hat die Chance, ihre Sichtweise auf neu entstehende digitale Staaten zu überdenken und anzupassen. Wie könnte es aussehen, wenn ein Staat aufgrund eines Konflikts die Souveränität über sein Territorium verliert oder wenn sein Territorium aufgrund einer Naturkatastrophe oder einer anderen Krise verschwindet? Was würde es bedeuten, wenn ein Staat in der Lage wäre, seine öffentlichen Dienste, seine nationale Identität und sein demokratisches System mit virtuellen Mitteln aufrechtzuerhalten?

Diese digitalen Staaten könnten eine Zukunft einleiten, in der Governance, Kultur und Gemeinschaft nicht unbedingt nur durch das Territorium definiert werden, in dem ein Individuum geboren wird, sondern auch davon, wie aktiv und engagiert eine Person im digitalen Raum ist.

Dies ist kein abstraktes Gedankenexperiment, sondern ein Aufruf zum Handeln an die internationale Gemeinschaft, dieses Thema ernst zu nehmen. Dies sind Probleme, mit denen sich die Welt in naher Zukunft auseinandersetzen muss, denn einige Staaten sind bereits auf dem besten Weg, ihr Territorium durch den steigenden Meeresspiegel zu verlieren.

LITERATURVERZEICHNIS

1. D. DeSilver, “More countries are now democratic than at any point since World War Two,” World Economic Forum, 11 12 2017. [Online]. Available: https://www.weforum.org/agenda/2017/12/more-countries-are-now-democratic-than-at-any-point-since-world-war-two/. [Accessed 23 10 2024].

2. A. Gore, “The National Information Infrastructure,” 11 01 1994. [Online]. Available: https://www.speeches-usa.com/Transcripts/al_gore-internet.html. [Accessed 10 2024].

3. A. Gore, “VP Remarks -- International Telecommunications Union,” 21 03 1994. [Online]. Available: https://clintonwhitehouse1.archives.gov/White_House/EOP/OVP/html/telunion.html. [Accessed 10 2024].

4. S. Nora and A. Minc, The computerization of society: a report to the President of France, Cambridge, Massachusetts: MIT Press, 1980.

5. The Economist Intelligence Unit, “Global democratic backsliding seems real, even if it is hard to measure,” The Economist, 12 09 2023. [Online]. Available: https://www.economist.com/interactive/graphic-detail/2023/09/12/democratic-backsliding-seems-real-even-if-it-is-hard-to-measure.

6. F. Kostelka and A. Blais, “The Generational and Institutional Sources of the Global Decline in Voter Turnout,” vol. 73, no. 4, 2021.

7. F. Lewsey, “Global dissatisfaction with democracy at a record high,” University of Cambridge, 2020. [Online]. Available: https://www.cam.ac.uk/stories/dissatisfactiondemocracy.

8. A. Polyaakova and C. Meserole, “Exporting digital authoritarianism: The Russian and Chinese models,” Brookings, 2019.

9. M. Mazzucato and R. Kattel, “COVID-19 and public-sector capacity,” vol. 36, no. 1, 2020.

10. T. S. James, A. Clark and E. Asplund, “Elections during Emergencies and Crises,” International Institute for Democracy and Electoral Assistance (International IDEA), 2023.

11. S. Stolzoff, “This Pacific island country is disappearing. What happens next?,” National Geographic, 08 07 2024. [Online]. Available: https://www.nationalgeographic.com/environment/article/tuvalu-islands-sea-level-rise-climate-change.

12. D. Herszenhorn and L. Bayer, “EU leaders agree on €1.82T budget and coronavirus recovery package,” POLITICO, 21 07 2020. [Online]. Available: https://www.politico.eu/article/eu-leaders-reach-deal-on-coronavirus-recovery-fund/.

13. K. McBride, “Regulation is Not Enough: A Blueprint for Winning the AI Race,” Just Security, 29 06 2023. [Online]. Available: https://www.justsecurity.org/87005/regulation-is-not-enough-a-blueprint-for-winning-the-ai-race/.

14. M. Schaake, The Tech Coup: How to Save Democracy from Silicon Valley, Princeton: Princeton University Press, 2024.

15. M. Scott and K. Komaitis, “Reenvisioning Europe’s digital sovereignty,” POLITICO, 23 09 2024. [Online]. Available: https://www.politico.eu/article/europe-ursula-von-der-leyen-tech-brussels-digital/ .

16. T. Burt, “Escalating Cyber Threats Demand Stronger Global Defense and Cooperation,” Microsoft On the Issues, 15 10 2024. [Online]. Available: https://blogs.microsoft.com/on-the-issues/2024/10/15/escalating-cyber-threats-demand-stronger-global-defense-and-cooperation/.

17. B. Smith, “Defending Ukraine: Early Lessons from the Cyber War,” Microsoft, 22 06 2022. [Online]. Available: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/. [Accessed 23 10 2024].

18. J. A. Lewis, “Cyberattack on Civilian Critical Infrastructures in a Taiwan Scenario,” CSIS, 11 08 2023. [Online]. Available: https://www.csis.org/analysis/cyberattack-civilian-critical-infrastructures-taiwan-scenario.

19. K. Butzer, “Collapse, environment, and society,” Proceedings of the national Academy of Sciences, vol. 109, no. 10, 2012.

20. B. Hammi, S. Zeadally and J. Nebhen, “Security threats, countermeasures, and challenges of digital supply chains,” ACM Computing Surveys, vol. 55, no. 14s, 2023.

21. R. Panwar, J. Pinkse and V. De Marchi, “The future of global supply chains in a post-COVID-19 world.,” California Management Review, vol. 64, no. 2, 2022.

22. S. Semenzin, D. Rozas and S. Hassan, “Blockchain-based application at a governmental level: disruption or illusion? The case of Estonia,” vol. 41, no. 3, 2022.

23. European Commission, “Joint Statement by EU and Ukrainian operators to help refugees from Ukraine stay connected,” 05 04 2022. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/joint-statement-eu-and-ukrainian-operators-help-refugees-ukraine-stay-connected.

24. T. Kotka and I. Liiv, “Concept of Estonian Government Cloud and Data Embassies,” Valencia, Spain, 2015.

25. C. Stupp, “Ukraine Has Begun Moving Sensitive Data Outside Its Borders,” Wall Street Journal, 06 14 2022. [Online]. Available: https://www.wsj.com/articles/ukraine-has-begun-moving-sensitive-data-outside-its-borders-11655199002.

26. D. Temple-Raston, “A ‘Worst Nightmare’ Cyberattack: The Untold Story Of The SolarWinds Hack,” NPR, 16 04 2021. [Online]. Available: https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.