



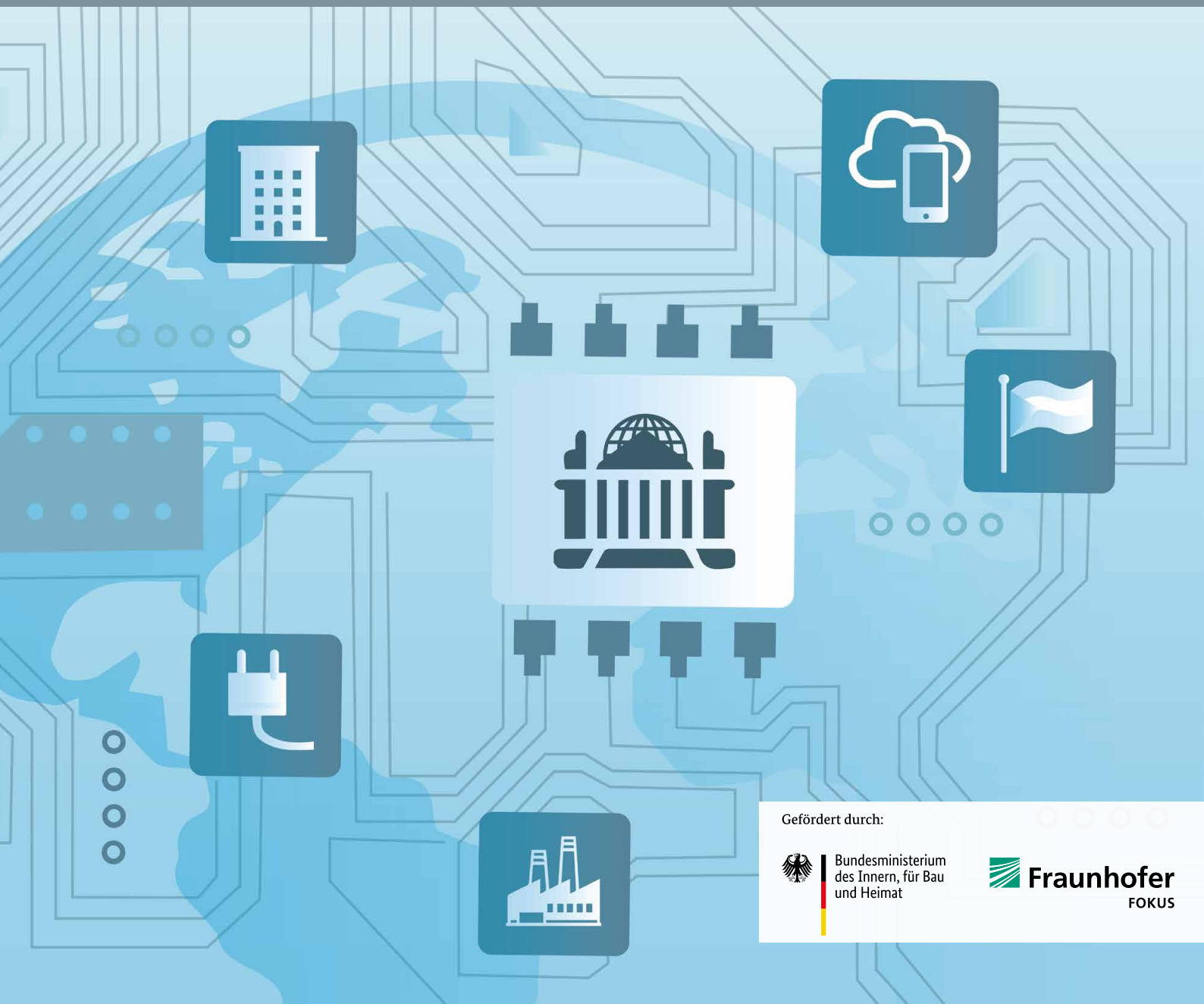
Kompetenzzentrum
Öffentliche IT

FORSCHUNG FÜR DEN DIGITALEN STAAT

DIGITALE SOUVERÄNITÄT ALS STRATEGISCHE AUTONOMIE

Umgang mit Abhängigkeiten im digitalen Staat

Resa Mohabbat Kar, Basanta E. P. Thapa



Gefördert durch:



Bundesministerium
des Innern, für Bau
und Heimat



Fraunhofer
FOKUS

IMPRESSUM

Autoren:

Resa Mohabbat Kar, Basanta E. P. Thapa,

Gestaltung:

Reiko Kammer

Herausgeber:

Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin
Telefon: +49-30-3463-7173
Telefax: +49-30-3463-99-7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

ISBN: 978-3-948582-02-9

1. Auflage September 2020

Dieses Werk steht unter einer Creative Commons Namensnennung 3.0 Deutschland (CC BY 3.0) Lizenz. Es ist erlaubt, das Werk bzw. den Inhalt zu vervielfältigen, zu verbreiten und öffentlich zugänglich zu machen, Abwandlungen und Bearbeitungen des Werkes bzw. Inhaltes anzufertigen sowie das Werk kommerziell zu nutzen. Bedingung für die Nutzung ist die Angabe der Namen der Autor:innen sowie des Herausgebers.

Von uns verwendete Zitate unterliegen den für die Quelle geltenden urheberrechtlichen Regelungen.

Links:

Alle im Dokument angegebenen Links wurden zuletzt am 6. August 2020 aufgerufen.

INHALTSVERZEICHNIS

Das Wichtigste in Kürze	5
Einleitung: Digitale Souveränität als neue Staatsaufgabe?	6

A.	Hintergrund	7
1.	Ausgangssituation: Die Entdeckung von »Schmerzpunkten« bei digitalen Abhängigkeiten	7
1.1	Abhängigkeiten, technische und nicht-technische »Schmerzpunkte«	7
1.2	Alte Abhängigkeiten in neuem Licht	8
1.3	Digitale Souveränität: Chiffre für die (Neu-)Konfiguration von Machtbeziehungen	9
1.4	Window of Opportunity mit Risiken und Nebenwirkungen	9
2.	Digitale Souveränität als strategische Autonomie im Digitalen	10
2.1	Digitale Souveränität meint: Schmerzpunkte absorbieren, Handlungsspielräume erweitern	10
2.2	Wozu strebt der Staat nach strategischer Autonomie im Digitalen?	11
3.	Zusammenfassung: Hintergrund	11

B.	Analyseraster	12
1.	Das Digitale in digitaler strategischer Autonomie	12
2.	Souveränitätsdimensionen	13
3.	Ist- und Soll-Analyse strategischer Autonomie im Digitalen	16
3.1	Ist-Analyse der strategischen Autonomie im Digitalen	16
3.2	Soll-Analyse der strategischen Autonomie im Digitalen	17
3.3	Strategische Vorausschau	19
4.	Zusammenfassung: Analyseraster	19

C.	Lösungsansätze	21
1.	Gestaltungsoptionen für strategische Autonomie im Digitalen	21
1.1	Änderungen an Prozessen und Technologie-Bündeln	21
1.2	Leistungstiefe und Steuerungsinstrumente	22
1.3	Technologiepolitische Strategien für Schlüsseltechnologien	23
1.4	Spielraum strategischer Autonomie	24
2.	Zusammenfassung: Lösungsansätze	25
3.	Handlungsempfehlungen	26

Referenzen	27
------------	----

DAS WICHTIGSTE IN KÜRZE

Digitale Technologien sind existenziell wichtig für Staat und Gesellschaft und führen aufgrund ihrer global arbeitsteiligen Erstellung zu einem komplexen Geflecht an Abhängigkeiten. Vor dem Hintergrund der sich verändernden Beziehungen zwischen Staaten sowie zwischen Staaten und nicht-staatlichen Akteuren werden bei diesen Abhängigkeiten zunehmend »Schmerzpunkte« wahrgenommen. Die daraus erwachsene Debatte um die digitale Souveränität des Staates dient dabei als Projektionsfläche für verschiedene Interessen und politische Projekte.

Wir verstehen digitale Souveränität nicht als absoluten Zustand, sondern als eine facettenreiche strategische Autonomie, die durch den bewussten Umgang mit und das gezielte Steuern von gegenseitigen Abhängigkeiten in der Digitalisierung hergestellt wird.

Abhängigkeiten und Bedarfe strategischer Autonomie des Staates können ermittelt werden, indem öffentliche Leistungen in Prozessschritte, die dabei eingesetzten Technologien und die Souveränitätsdimensionen der Technologien – also die zu ihrer Erforschung, Entwicklung, Fertigung sowie zu ihrem Betrieb und ihrer Nutzung erforderlichen Fähigkeiten und Ressourcen – ausdifferenziert werden. Dabei hilft es, die strategische Relevanz der Leistung, die prozedurale Relevanz der technischen Komponenten für die öffentliche Leistungserstellung, Kosten-Nutzen-Verhältnisse unterschiedlicher Gestaltungsoptionen sowie die genauen Steuerungsziele zu beachten. Zusätzlich sollte strategisch auf zukünftige Entwicklungen in Staat, Technik und Markt vorausgeschaut werden.

Um mit Abhängigkeiten im Digitalen umzugehen und die strategische Autonomie zu erhöhen, können:

- Prozesse und technische Lösungen verändert werden, um Abhängigkeiten zu vermeiden;
- verschiedene Konstellationen zur Leistungserstellung – zwischen staatlicher Eigenerstellung und Fremdbezug am Markt – sowie staatliche Steuerungsinstrumente wie Regulierung, Finanzierung, Strukturierung und Überzeugungsmaßnahmen angewandt werden, um die Steuerungsfähigkeit in einzelnen Souveränitätsdimensionen einer Technologie zu verbessern;
- für Schlüsseltechnologien technologiepolitische Strategien wie Risikomanagement, strategische Partnerschaften und ein Gemeingüteransatz verfolgt werden.

Aus der Betrachtung gelangen wir zu sechs grundsätzlichen Handlungsempfehlungen:

- Abhängigkeiten systematisch identifizieren und verstehen, um diese steuern zu können.
- Abhängigkeiten durch institutionelle Arrangements managen.
- Den Hebel gemeinsamen europäischen Handelns nutzen.
- Strategische Autonomie mit strategischer Vorausschau in die Zukunft denken.
- Digitale Technologien aufgrund ihrer Querschnittsfunktion politikfeldübergreifend steuern.
- Die besondere Rolle von Wissens-, Forschungs- und Betriebssouveränität beachten.

EINLEITUNG: DIGITALE SOUVERÄNITÄT ALS NEUE STAATSAUFGABE?

Digitale Souveränität wird derzeit auf allen politischen Ebenen – von den Kommunen über den Bund bis zur EU – kontrovers diskutiert.¹ Aber was soll das überhaupt sein? Der Begriff ist auch deshalb so beliebt, weil er sich als Projektionsfläche für verschiedenste politische Forderungen eignet.

Dass Abhängigkeiten von Rohstoffquellen, Märkten und Entscheidungen ausländischer Regierungen die Erfüllung staatlicher Aufgaben beeinträchtigen können, haben nicht zuletzt die Lieferengpässe und zwischenstaatliche Konkurrenz bei medizinischen Gütern während der Corona-Pandemie gezeigt.²

Digitale Technologien sind dabei besonderer Aufmerksamkeit würdig, da sie einerseits in komplexe Netze aus Abhängigkeiten eingebunden sind, andererseits integrale Querschnittsfunktionen für die Handlungsfähigkeit des Staates erfüllen.

Ziel strategischen Handelns zur digitalen Souveränität des Staates ist der »selbstständige, selbstbestimmte & sichere Zugang«³ zu Digitaltechnologien, damit der Staat öffentliche Leistungen verlässlich erbringen kann. Im Umkehrschluss ist zu vermeiden, dass der Staat durch fehlenden Zugang zu oder unzureichende Kontrolle über Digitaltechnologien in seiner Entscheidungs- und Handlungsfreiheit eingeschränkt wird.

Dass dies keine reinen Gedankenspiele sind, zeigen die staatlichen Maßnahmen zur Eindämmung der Corona-Pandemie: So verweigerten die Hersteller von Betriebssystemen für mobile Endgeräte die Öffnung der Schnittstellen für die zentrale Daten-

bankarchitektur einer Corona-Warn-App, die einige europäische Staaten zwischenzeitlich präferierten.⁴ Staaten konnten somit nicht unabhängig von privaten Technologieunternehmen die Abwägung zwischen Datenschutz und Infektionsschutz treffen.

Mit der Digitalisierung der Gesellschaft erstreckt sich staatliche Souveränität zunehmend auch auf das Digitale. Digitale Souveränität ist also nicht als digitalpolitischer Modebegriff abzutun, sondern als dauerhafte Staatsaufgabe zu begreifen.

Zum vorliegenden Whitepaper

Dieses Whitepaper fokussiert die digitale Souveränität des Staates, nicht die der Bürger:innen und Organisationen.⁵ Dabei folgen wir dem Verständnis von **strategischer Autonomie im Digitalen** als dem Vergrößern staatlicher Handlungsräume durch den bewussten, **strategischen Umgang mit Abhängigkeiten in der Digitalisierung**. Hierzu gehen wir in drei Schritten vor:

1. **Hintergrund** der Debatte um digitale Souveränität und Einordnung des Begriffs.
2. **Analyseraster** zur Bewertung von digitalen Abhängigkeiten und strategischer Autonomie durch Differenzierung von Prozessschritten der Leistungserstellung, der dabei eingesetzten Technologie-Bündel und ihrer Souveränitätsdimensionen.
3. **Lösungsansätze** durch Änderungen an Prozessen und Technologien, durch Regulierung und Arrangements der Leistungserstellung sowie durch technologiepolitische Strategien.

¹ »Digitale Souveränität« bzw. »technologische Souveränität« findet prominente Erwähnung in zahlreichen aktuellen politischen Maßnahmen- und Strategiepapieren, wie etwa im Eckpunktepapier »Stärkung der digitalen Souveränität der öffentlichen Verwaltung« (IT-Planungsrat 2020), der »Industriestrategie 2030« (BMW 2019), den »Eckpunkten einer Datenstrategie der Bundesregierung« (Bundesregierung 2019), im »Weißbuch zur Künstlichen Intelligenz« (EU-Kommission 2020a) oder in der »Europäischen Datenstrategie« (EU-Kommission 2020b).

² Bundesministerium für Arbeit und Soziales (2020).

³ Siehe Goldackers Definition digitaler Souveränität, wonach diese »die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen [umfasst], ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können«. Goldacker, G. (2017: 3).

⁴ tagesschau.de (2020), golem.de (2020).

⁵ Siehe hierfür Goldacker, G. (2017).

A. HINTERGRUND

In diesem Abschnitt zeichnen wir nach, welche »Schmerzpunkte« Abhängigkeiten im digitalen Staat erzeugen, welche Faktoren zu einer Neubewertung von Abhängigkeiten führen und in welchen Aushandlungsprozessen diese Abhängigkeiten aktuell problematisiert werden. Anschließend legen wir dar, warum wir von digitaler strategischer Autonomie statt von digitaler Souveränität sprechen.

1. Ausgangssituation: Die Entdeckung von »Schmerzpunkten« bei digitalen Abhängigkeiten

Das Schlagwort digitale Souveränität erfährt in Deutschland und Europa spätestens seit dem Bekanntwerden der weitgehenden Zugriffsmöglichkeiten von US-Nachrichtendiensten auf IT-Systeme im Jahr 2013 politische Aufmerksamkeit. Die strategischen Diskussionen um das tolerierbare Maß technologischer Abhängigkeiten von Dritten kreisen dabei um unterschiedliche Vulnerabilitäten bzw. »Schmerzpunkte«.

1.1 Abhängigkeiten, technische und nicht-technische »Schmerzpunkte«

Deutschland und die EU sind in kritischen gesellschaftlichen Bereichen auf digitale Dienste, Infrastrukturen und Komponenten angewiesen, deren Entwicklung, Produktion und Betrieb maßgeblich nicht der eigenen Kontrolle und Verfügungsgewalt unterliegen. Derartige Abhängigkeiten wurden z.B. für den Einsatz proprietärer Softwareprodukte in der Bundesverwaltung⁶ und außereuropäischer Mikroelektronik in ganzen Branchen problematisiert.⁷

Abhängigkeiten führen zu Unsicherheit über *potenziell* negative Folgewirkungen, stellen also Schmerzpunkte dar. Schmerzpunkte können eher technischer Natur sein, wie z. B. eine unge-

⁶ PwC Strategy& (2019).

⁷ Handelsblatt (2019a), accenture (2020).

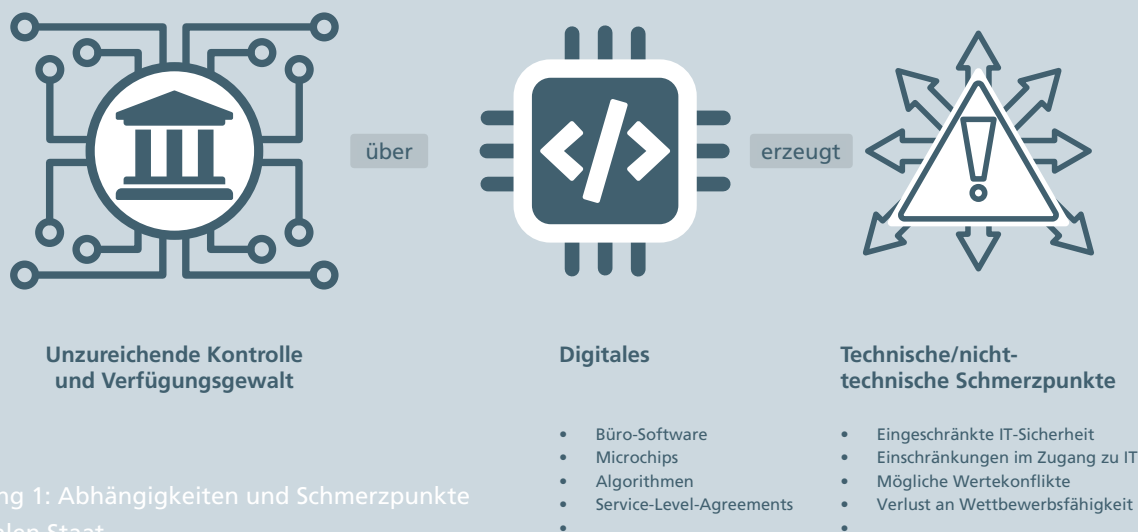


Abbildung 1: Abhängigkeiten und Schmerzpunkte im digitalen Staat

nügende Zugriffs- und Angriffssicherheit von IT-Systemen oder die mögliche Remote-Abschaltung von Softwarefunktionalitäten.⁸ Die lauter werdenden Rufe nach digitaler Souveränität rühren auch aus der Beobachtung bzw. Antizipation nicht-technischer Schmerzpunkte her, die sich in Deutschland und Europa im Wesentlichen um zwei Bereiche herum kristallisieren: Erstens geht es um Befürchtungen, dass in der digitalen Transformation technologische Abhängigkeiten zu einem Verlust der internationalen Wettbewerbsfähigkeit europäischer Industrien und Wirtschaftsakteure führen. Zweitens wird die unzureichende rechtliche Durchsetzungsfähigkeit gegenüber großen Technologieunternehmen diskutiert: In den digitalen Technologien außerhalb europäischer Unternehmen seien Wertvorstellungen von z. B. Selbstbestimmung, der Zulässigkeit von Inhalten oder Datenschutz eingeschrieben, die deutschen und europäischen Werten vielfach zuwiderlaufen würden.⁹

1.2 Alte Abhängigkeiten in neuem Licht

In einer globalisierten, vernetzten und arbeitsteiligen Welt sind Abhängigkeiten und die damit einhergehenden Schmerzpunkte weder neu noch außergewöhnlich. Warum werden sie für digitale Technologien mit zunehmender Dringlichkeit kritisiert? Bei ihrer (Neu-)Bewertung spielt das Zusammentreffen verschiedener, sich gegenseitig verstärkender Faktoren eine wichtige Rolle:

- **Verständnis für die systembestimmende Funktion moderner IT:** Politische Akteure sind sich zunehmend der Systemrelevanz von Informationstechnik für fast sämtliche Bereiche von Staat, Wirtschaft und Gesellschaft bewusst. Kaum ein politisches Ziel, von der nationalen Sicherheit über die Innovations- und Wettbewerbsfähigkeit der Wirtschaft bis hin zum gesellschaftlichen Zusammenhalt, ist nicht von digitalen Dynamiken beeinflusst.
- **Volatilität der regelbasierten internationalen Ordnung:** In den internationalen Beziehungen zeichnet sich eine Schwächung der regelbasierten liberalen internationalen Ordnung ab. Angefacht durch das Verhalten internationaler Schlüsselakteure verlieren internationale Organisationen, internationale Abkommen und sogar zwischenstaatliche

Allianzen an Bindungskraft. In der Folge ertönt der Ruf nach einem Europa, das sein Schicksal selbst in die Hand nimmt, immer lauter.¹⁰

- **Digitale Geopolitik:** Es zeichnet sich eine zunehmende Politisierung internationaler Handelsbeziehungen inklusive digitaler Dienste und Produkte ab.¹¹ Dabei herrscht nicht mehr ausschließlich eine marktwirtschaftliche Logik, sondern digitale Strukturen werden zunehmend als Instrumente wertebbezogener Politik und internationaler Einflussnahme erkannt.
- **Steuerungsfähigkeit in der digitalen Vernetzung:** Die technologische Basis der digitalen Transformation von Gesellschaften und globalen Märkten zeichnet sich durch zunehmend komplexer werdende, softwarebasierte vernetzte Systeme aus, die immer stärker auch im Hinblick auf die Implikationen für die staatliche Kontroll- und Steuerungsfähigkeit kritisch gewürdigt werden. Komplexe IT-Systeme können – wie das Beispiel der 5G-Technologie exemplarisch verdeutlicht – von den Betreibern kaum noch vollumfänglich nachvollzogen werden und entziehen sich so auch teilweise ihrer Kontrolle.

Im Zusammenwirken dieser Faktoren erscheinen alte Abhängigkeiten in neuem Licht. In ihnen werden zunehmend Schmerzpunkte und mögliche Eintrittspforten für ganz unterschiedliche Gefährdungen antizipiert. Die strategische Dimension des Digitalen rückt stärker in den Blick. Damit entsteht auch ein größerer staatlicher Gestaltungs- und Steuerungsanspruch, der sich vielfach unter dem Label digitaler Souveränität äußert.

⁸ Siehe für weitere Beispiele in der Bundesverwaltung PwC Strategy& (2019: 17ff).

⁹ Siehe etwa Kagermann, H und Wilhelm, U. (2020).

¹⁰ Siehe Rede der Bundeskanzlerin in Handelsblatt (2017) und des ehemaligen EU-Kommissionspräsidenten Juncker in Kölnische Rundschau (2018). Allgemein zu den strukturellen Veränderungen in den internationalen Beziehungen und den Implikationen für Deutschlands und Europas Positionierung: Lippert, B., von Andarza, N., Perthes, V. (2019).

¹¹ Seit 2019 gibt es ein einheitliches europäisches Rahmenwerk zur Durchführung einer politischen Bewertung ausländischer Direktinvestitionen – insbesondere in Bereichen mit Schlüsseltechnologien – im Hinblick auf die Auswirkungen auf die strategischen Interessen Europas, siehe EU-Kommission (2019); Die »5G Toolbox« der EU sieht u. a. eine politische Bewertung der Vertrauenswürdigkeit ausländischer 5G-Ausrüster vor, siehe EU-Kommission (2020c); Zu geopolitischen Dimensionen internationaler Handelsbeziehungen und digitaler Technologien im Allgemeinen siehe Bendiek, A., Schallbruch, M. (2019); Bendiek, A., Godehardt, N., Schulze, D. (2019); Schlembach, C. (2020).



Abbildung 2: Wichtige Treiber für die strategische Neubewertung technologischer Abhängigkeiten und für die Entstehung eines stärkeren staatlichen Steuerungsanspruchs in der Digitalisierung.

1.3 Digitale Souveränität: Chiffre für die (Neu-)Konfiguration von Machtbeziehungen

Aus den teils sehr spezifischen, parallel laufenden Fachdebatten um digitale Souveränität kristallisiert sich ein roter Faden heraus:¹² digitale Souveränität als Abwehr von Fremdkontrolle im Digitalen, und zwar sowohl gegenüber Staaten als auch gegenüber privatwirtschaftlichen Akteuren.

Rekonfiguration von (Macht-)Beziehungen zwischen Staaten: Mit dem grenzüberschreitenden Charakter digitaler Technologien entstehen neue Möglichkeiten der Machtausübung und Einflussnahme im Herrschaftsgebiet anderer Staaten.¹³ Digitale Souveränität soll vor diesem Hintergrund die Herstellung nationaler hoheitlicher Kontrolle und Verfügungsgewalt ermöglichen. Digitale Sphären werden zunehmend als Arena für die Austragung staatlicher Konkurrenz- und Machtkämpfe wahrgenommen. Dieses Verständnis liegt zugrunde, wenn die

Gründung »nationaler Champions«¹⁴ und das Erringen »technologischer Vorherrschaft«¹⁵ als politische Ziele diskutiert werden.

Begrenzung neuer Machtmöglichkeiten privatwirtschaftlicher Akteure: Mit wachsender Bedeutung digitaler Technologien für Staat und Gesellschaft wachsen auch die Machtmöglichkeiten ihrer Hersteller, gerade in den Bereichen, in denen diese Quasi-Monopole genießen. Dabei geht es nicht nur um die direkte technische und wirtschaftliche Abhängigkeit, etwa in Lock-in-Situationen. Insbesondere die Such- und Filter-Algorithmen der großen Plattformanbieter, aber auch die Frage, wofür diese Anbieter die gesammelten Daten nutzen, sind inzwischen von zentraler gesellschaftlicher Bedeutung.¹⁶ Aus dieser Perspektive speisen sich Rufe nach starker Regulierung oder nach der Zerschlagung und Vergemeinschaftung bedeutender Digitalunternehmen bzw. ihrer »Datenschätze«.

1.4 Window of Opportunity mit Risiken und Nebenwirkungen

Der Begriff der digitalen Souveränität ist zu einer Projektionsfläche für zahlreiche digitalpolitische Befürchtungen und Wünsche geworden. Die aktuelle Debatte und der offensichtliche Wille zum staatlichen Handeln eröffnen ein politisches »Window of Opportunity«, durch welches sich ganz unterschiedliche digital- und technologiepolitische Forderungen zu drängen versuchen.

¹² Für eine ausführliche Analyse der Entwicklung des Souveränitätsverständnisses in Digitalisierungsdiskursen bzw. in der Digitalpolitik vgl. Thiel, T. (2019) und Pohle, J., Thiel, T. (2019).

¹³ Siehe z. B. Deutscher Bundestag, Ausschuss Digitale Agenda (2019); Zettl, K. (2019); Spiegel.de (2014); Zeit Online (2019).

¹⁴ Hannoversche Allgemeine Zeitung (2019).

¹⁵ Roth, M., Staatsminister für Europa im Auswärtigen Amt (2020).

¹⁶ Allgemein zu gesellschaftlichen und politischen Fragestellungen der »Datafizierung« und »Algorithmisierung« siehe: Mohabbat Kar, R., Thapa, B. und Parycek, P. (2018).

Jede dieser Forderungen sollte kritisch auf Risiken und Nebenwirkungen geprüft werden, die im Eifer eines »Abwehrkampfes« gegen Fremdkontrolle im Digitalen leicht übersehen werden können. Die im Zusammenhang mit digitaler Souveränität diskutierten Maßnahmen zur Umsetzung eines »Schengen-Routing« oder zu Datenlokalisierungen¹⁷ zeigen exemplarisch das Schadenspotenzial: Sie können z. B. ungeeignet sein, Vertraulichkeit und Integrität von IT-Systemen zu gewährleisten und ein falsches Gefühl von Sicherheit und Kontrolle erzeugen oder zur Fragmentierung globaler Kommunikationsinfrastrukturen und Wirtschaftsräume führen.¹⁸

2. Digitale Souveränität als strategische Autonomie im Digitalen

Souveränität ist heute ein schillernder, historisch mit vielfachen Bezügen aufgeladener Begriff, der konzeptionell schwer zu greifen ist. Wir schlagen stattdessen eine Arbeitsdefinition von »digitaler strategischer Autonomie« vor, mit der wir in den folgenden Kapiteln weiter argumentieren.

2.1 Digitale Souveränität meint: Schmerzpunkte absorbieren, Handlungsspielräume erweitern

Der auf den Staat gerichtete alltagsprachliche Gebrauch des Souveränitätsbegriffs bezieht sich heute in der Regel auf die innen- wie außenpolitische Handlungs- und Interaktionsfähigkeit. Dem liegt häufig ein absolutes, binäres Verständnis von Souveränität oder Nicht-Souveränität zugrunde, das einen differenzierteren Blick auf die staatliche Handlungsfreiheit erschwert. Realpolitisch finden wir staatliche Selbstbestimmung eher in Abstufungen und verschiedenen Dimensionen. Niemand würde der Bundesrepublik Deutschland die Souveränität absprechen, wenn auf ihrem Staatsgebiet 5G-Komponenten ausländischer Fabrikanten eingesetzt würden. Dennoch wür-

den sich Abhängigkeiten von ausländischer 5G-Technologie vermutlich auf staatliche Handlungsspielräume auswirken.

Um die Auswirkungen technologischer Abhängigkeiten auf staatliche Entscheidungs- und Handlungsspielräume differenziert zu erfassen und ihnen zu begegnen, greifen wir auf den Begriff der »strategischen Autonomie« zurück, der die komplexe Realität von Globalisierung und digitaler Vernetzung leichter abbildet.

»Strategische Autonomie« ist ein Begriff der internationalen Beziehungen, in denen er – vor dem Hintergrund der oben beschriebenen globalen Dynamiken – vermehrt zur Beschreibung der Weiterentwicklung der Rolle und Position Europas vis-à-vis anderen internationalen Akteuren verwendet wird.¹⁹ In Anlehnung hieran schlagen wir folgende Arbeitsdefinition für strategische Autonomie im Digitalen vor:

»Strategische Autonomie im Digitalen umfasst die Fähigkeiten des Staates, eigene politische, gesellschaftliche und wirtschaftliche Prioritäten umsetzen zu können, ohne dabei in ungewünschtem Maße durch Abhängigkeiten in der Digitalisierung eingeschränkt zu werden.«

Strategische Autonomie fokussiert auf die staatliche Handlungsfreiheit als relative und mehrdimensionale Größe. Die Arbeitsdefinition verdeutlicht, dass die unterschiedlichen Grade von Handlungsfreiheit durchaus von verschiedensten, z. B. wirtschaftlichen, militärischen und politischen Abhängigkeiten geprägt sein können. Das **politische Ziel** strategischer Autonomie ist somit ein **Zuwachs** an Handlungs- und Entscheidungsfreiheit, unter Abwägung der damit einhergehenden (politischen, wirtschaftlichen etc.) Kosten. Strategische Autonomie zielt also nicht auf Abschottung oder Autarkie, die insbesondere in der Informationstechnik unrealistisch sind. Sie zielt vielmehr auf die Schaffung der Fähigkeiten und Ressourcen, um mögliche negative Auswirkungen (Schmerzpunkte) bestehender Abhängigkeiten beurteilen und kompensieren zu können und zugleich den Spielraum eigener Entscheidungs- und Handlungsfreiheit zu erweitern. Dabei ist strategische Autonomie

¹⁷ Unter dem Schlagwort »Schengen-Routing« wurden nach Bekanntwerden der NSA-Abhörpraktiken Möglichkeiten für regional begrenztes Routing des Datenverkehrs im nationalen oder europäischen Raum diskutiert. Datenlokalisierung setzt – aus deutscher bzw. europäischer Perspektive – voraus, dass private Diensteanbieter ihre Server zur Speicherung und Verarbeitung von Daten im deutschen bzw. europäischen Raum aufstellen. Beide Maßnahmen sollen die Zugriffs- und Angriffssicherheit von Daten europäischer Bürger:innen und Organisationen erhöhen.

¹⁸ Maurer, T. et al. (2014).

¹⁹ Die Stiftung Wissenschaft und Politik definiert strategische Autonomie wie folgt: »Strategische Autonomie wird hier als die Fähigkeit definiert, eigene außen- und sicherheitspolitische Prioritäten zu setzen und Entscheidungen zu treffen, sowie die institutionellen, politischen und materiellen Voraussetzungen, um diese in Kooperation mit Dritten oder, falls nötig, eigenständig umzusetzen.« Lippert, B., von Ondarza, N., Perthes, V. (2019: 5). Vgl. auch Masala, C. (2019).

kein Selbstzweck, sondern dient politischen Zielen. Digitale strategische Autonomie stellt somit auf den **bewussten Umgang mit und das gezielte Steuern von gegenseitigen Abhängigkeiten** in der Digitalisierung ab.

2.2 Wozu strebt der Staat nach strategischer Autonomie im Digitalen?

Der Grad der gegebenen strategischen Autonomie im Digitalen bestimmt den Manövrierraum, in dem der Staat seine Ziele verfolgen und Verantwortungsbereiche gestalten kann – vom Schutz der körperlichen Unversehrtheit seiner Bürger:innen oder der Vertraulichkeit und Integrität von Kommunikation bis hin zur Gestaltung »gleichwertiger Lebensverhältnisse« oder des gesamtwirtschaftlichen Gleichgewichtes. Durch die digitale Transformation der Gesamtgesellschaft einschließlich ihrer Teil- und Subsysteme wandelt sich die Rolle von IT für das Staatshandeln in vielen Bereichen von einem unterstützenden zu einem bestimmenden Faktor.

Durch die zunehmend elektronische öffentliche Verwaltung haben digitale Technologien Anteil an nahezu jeder Form staatlichen Handelns. Die Bedeutung von IT ist von einem Hilfsmittel für Verwaltungsaufgaben bis zu komplexen E-Government-Lösungen im Laufe der Zeit deutlich gewachsen. Und dennoch steht die Verwaltung erst am Anfang ihrer digitalen Transformation. Neben der Verantwortung für die IT innerhalb der öffentlichen Verwaltung trägt die öffentliche Hand auch eine darüber hinausgehende Verantwortung im Rahmen der Daseinsvorsorge. Wie in vielen anderen Bereichen von Wirtschaft und Gesellschaft zeichnen sich auch die kritischen Infrastrukturen Energie, Wasser, Ernährung, IT und Telekommunikation, Gesundheit, Finanz- und Versicherungswesen, Transport und Verkehr, Staat und Verwaltung sowie Medien und Kultur durch die zunehmende Implementierung vernetzter Informationstechnologien aus, wodurch unter anderem die Potenziale der Digitalisierung für Effizienz- und Produktivitätssteigerungen ausgeschöpft werden sollen. Vernetzte Informationstechnik bildet mittlerweile die Grundlage moderner Kontroll-, Steuerungs- und Wartungssysteme in kritischen Infrastrukturen wie Stromnetzen, der Wasserversorgung, Transport und Verkehr oder Banken und Finanzwesen. Die Bedeutung von IT in kritischen

Infrastrukturen wird auch durch entsprechende gesetzgeberische Maßnahmen untermauert.²⁰

Vor diesem Hintergrund nehmen der selbstbestimmte Zugang zu und Gebrauch von digitalen Technologien eine strategisch kritische Rolle für den Staat ein. Der Grad der Handlungsfreiheit im Digitalen erweitert oder beschränkt zunehmend die strategische Autonomie eines Staates insgesamt.

3. Zusammenfassung: Hintergrund

Die arbeitsteilige Bereitstellung digitaler Technologien führt bei ihrem Einsatz stets zu Abhängigkeiten. Diese führen im digitalen Staat insbesondere dort zu Schmerzpunkten, wo durch den Wandel von Beziehungen zwischen Staaten aber auch zwischen Staaten und nicht-staatlichen Akteuren ein Kontrollverlust für den Staat zu drohen scheint. Daraus speist sich die aktuelle Debatte um digitale Souveränität, die zur Projektionsfläche vieler Wünsche und Interessen wird. Wir verstehen digitale Souveränität nicht als einen absoluten Zustand, sondern als facettenreiche strategische Autonomie im Digitalen, die durch das gezielte Steuern von Abhängigkeiten hergestellt wird. Strategische Autonomisierung zielt auf die Herstellung von Fähigkeiten und Ressourcen, um Schmerzpunkte bestehender Abhängigkeiten beurteilen und kompensieren zu können und zugleich den Spielraum eigener Entscheidungs- und Handlungsfreiheit zu erweitern.

²⁰ Siehe etwa die Überarbeitung des IT-Sicherheitsgesetzes, das laut Referentenentwurf Sicherheitsvorgaben für IKT in KRITIS deutlich verschärft, siehe it-daily.net (2019).

B. ANALYSERASTER

Dieser Abschnitt bietet einen vertiefenden Einblick in eine Systematik zur Bewertung von Abhängigkeiten im digitalen Staat. Hierfür müssen öffentliche Leistungen in ihre Prozessschritte zerlegt und alle zur Leistungserstellung eingesetzten technischen Komponenten als Technologie-Bündel erfasst werden. Die mit der Bereitstellung und Nutzung der technischen Komponenten einhergehenden Anforderungen an die Entscheidungs- und Handlungsfreiheit differenzieren wir in verschiedene Souveränitätsdimensionen. Das dadurch entstehende Analyseraster ermöglicht die Ist- und Soll-Analyse sowie die strategische Vorausschau der digitalen strategischen Autonomie.

1. Das Digitale in digitaler strategischer Autonomie

Die Herstellung strategischer Autonomie im Digitalen ist anspruchsvoll: So ist nicht nur fast jede digitale Anwendung in ein ganzes Netz technischer Abhängigkeiten verwebt, sondern die einzelnen Komponenten dieses Netzes werden auch in internationaler Arbeitsteilung und Kooperation bereitgestellt. Bereits vermeintlich simple Aktivitäten wie das Versenden einer E-Mail sind erst durch eine Vielzahl technischer und organisatorischer Abhängigkeiten möglich.

Die konkret gewählten Kombinationen informationstechnischer Komponenten für die Erfüllung einer bestimmten Aufgabe bezeichnen wir im Folgenden als Technologie-Bündel. In einem generischen Modell besteht das Technologie-Bündel aus Netzen, Hardware, Software, Daten und Plattformen, die wir als technische Schichten bezeichnen (Abbildung 3). Die für die öffentliche Leistungserstellung eingesetzten Komponenten können in den verschiedenen Prozessschritten der Leistungserbringung (im Folgenden »Leistungskette«) variieren. Zur Erbringung einer Leistung können etwa diverse Softwarekomponenten, wie z.B. Arbeitsplatzbetriebssysteme, Serverbetriebssysteme oder Fachverfahrenssoftware, sowie verschiedene Netze zur Datenübertragung oder diverse Hardware wie PCs, Router und Smartphones erforderlich sein. Das Technologie-Bündel einer öffentlichen Leistung umfasst alle technischen Komponenten in jedem einzelnen Schritt der Leistungskette (Abbildung 4). Somit können organisatorische Veränderungen der Leistungskette Änderungen im Technologie-Bündel nach sich ziehen.

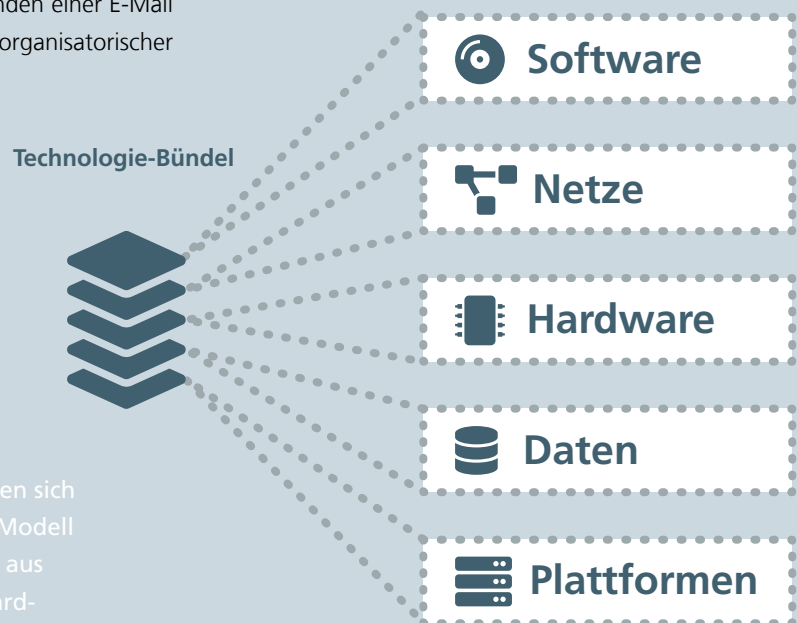


Abbildung 3: Digitale Systeme lassen sich in einem abstrakten, generischen Modell als Technologie-Bündel bestehend aus den Schichten Software, Netze, Hardware, Daten und Plattformen darstellen.

Die Aufteilung eines generischen Technologie-Bündels in die Schichten Netze, Hardware, Software, Daten und Plattformen dient lediglich als Heuristik, denn in realen Systemen sind die Schichten häufig kaum voneinander zu unterscheiden. So fungiert das Internet in vielen Technologie-Bündeln als Netz, kann aber bei genauerem Hinsehen auch als Plattform für die Kommunikation zwischen kleinteiligen Netzen klassifiziert werden, die wiederum aus eigenen Technologie-Bündeln aus u. a. Steuerungssoftware und zugehöriger Hardware bestehen.

Moderne digitale Anwendungen bauen also auf komplexen Verschachtelungen informationstechnischer Systeme auf. Dies verdeutlicht, warum strategische Autonomie im Digitalen realistisch die Steuerung, nicht aber die vollständige Vermeidung von Abhängigkeiten bedeuten kann.

2. Souveränitätsdimensionen

Die digitalen Produkte und Dienste eines Technologie-Bündels sind die Ergebnisse langer Wertschöpfungsketten, deren einzelne Stufen – von der Forschung für ein Produkt über seine Entwicklung und Fertigung bis hin zum Betrieb und zur Nutzung – jeweils ganz eigene Anforderungen an die Handlungs- und Entscheidungsfreiheit des Staates stellen können. Reicht es, die für eine strategisch hoch relevante öffentliche Leistung

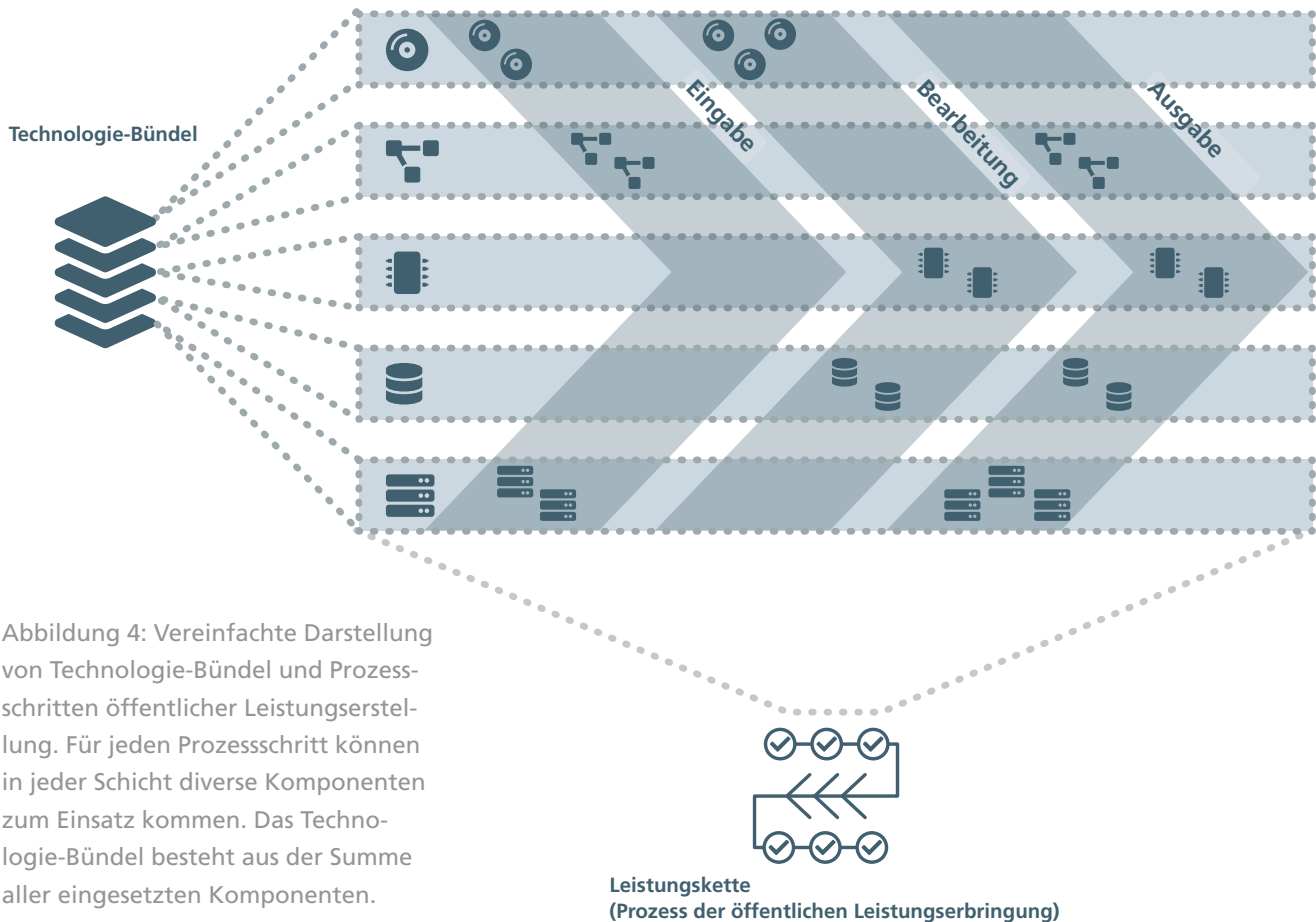


Abbildung 4: Vereinfachte Darstellung von Technologie-Bündel und Prozessschritten öffentlicher Leistungserstellung. Für jeden Prozessschritt können in jeder Schicht diverse Komponenten zum Einsatz kommen. Das Technologie-Bündel besteht aus der Summe aller eingesetzten Komponenten.

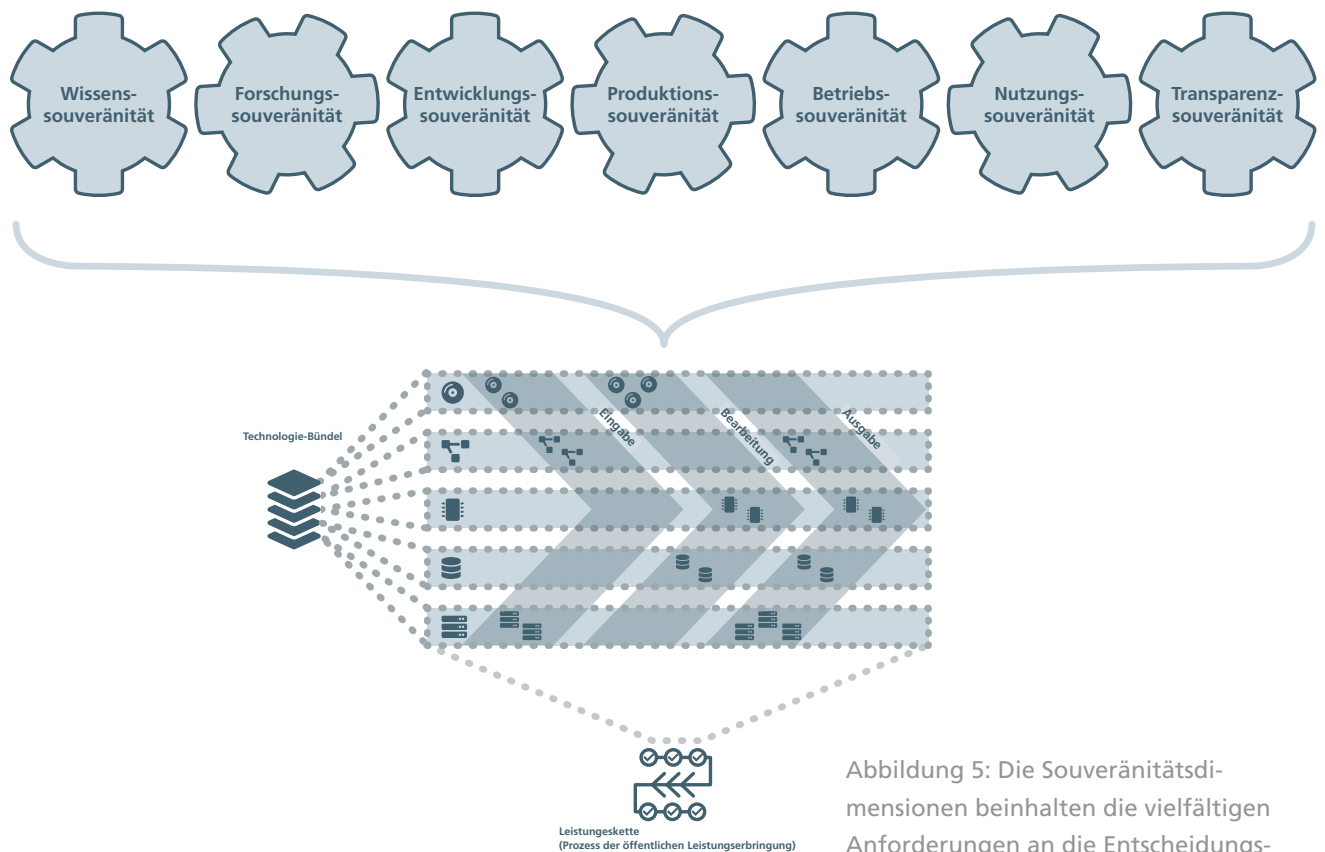


Abbildung 5: Die Souveränitätsdimensionen beinhalten die vielfältigen Anforderungen an die Entscheidungs- und Handlungsfreiheit strategischer Autonomie im Digitalen. Die Dimensionen können für jede einzelne Komponente des Technologie-Bündels einer Leistungskette betrachtet werden.

unerlässliche Datenbank durch den öffentlichen IT-Dienstleister betreiben zu lassen? Ist eventuell auch bei der von privatwirtschaftlichen Herstellern bezogenen zugehörigen Datenbanksoftware weniger Abhängigkeit und mehr staatliche Steuerung strategisch wünschenswert? Ist vielleicht sogar der Fortschritt bei den eingesetzten Patenten und Algorithmen so strategisch bedeutsam, dass Abhängigkeiten von Forschungseinrichtungen, die unter der Außenwirtschaftskontrolle anderer Staaten stehen, zu reduzieren sind?

Wo sich ganz allgemein bei der Bereitstellung und Nutzung digitaler Anwendungen Abhängigkeiten manifestieren können bzw. welche diversen Anforderungen sich an digitale Souveränität ergeben können, beschreibt der »VDE Verband der Elektrotechnik Elektronik Informationstechnik« in zehn »Ausprägungen technologischer Souveränität«, die er aus einer generischen

technologischen Wertschöpfungskette ableitet.²¹ In Anlehnung hieran schlagen wir sieben Souveränitätsdimensionen vor, auf die sich die Entscheidungs- und Handlungsfreiheit strategischer Autonomie im Digitalen erstrecken können: Von der Forschungssouveränität, ob also grundlegende Forschung für die Technologie durchgeführt werden kann, über die Produktionssouveränität, ob die Fähigkeit zur Fertigung der technischen Komponenten besteht, bis hin zur Betriebsouveränität, ob also Instanzen der Technologie unter eigener Regie installiert und betrieben werden können.

²¹ VDE ITG Informationstechnik (2020:13ff).

Souveränitätsdimensionen

Wissenssouveränität

- Zugang zu Informationen und Wissen über Anwendungsmöglichkeiten, Nutzung und Betrieb von Digitaltechnologien
- Fähigkeiten und Ressourcen, um Komponenten und Systeme bewerten zu können
- Verfügbarkeit von Expert:innen, die dieses Wissen aufbauen und in Aus- und Weiterbildung vermitteln können

Forschungssouveränität

- (Politische) Entscheidungsfreiheit beim Aufgreifen und Fördern von Forschungsthemen (z. B. an Hochschulen)
- Zugang zu Ressourcen (wie z. B. Rohstoffen, Algorithmen, Rechenleistung etc.), um Forschungsarbeiten wie Experimente durchführen zu können
- Fähigkeiten und Ressourcen zur Überführung fundierter Forschungsarbeiten in die internationale Standardisierung

Entwicklungssouveränität

- Entscheidungs- und Handlungsfreiheit bei der Konzeption, Ausgestaltung und Umsetzung eines Produktes
- Zugang zu erforderlichen Ressourcen, z. B. für Prototypenentwicklung und Tests
- Zugang zu erforderlichen Kenntnissen, sowohl im Kerngebiet als auch in den für das Produkt relevanten anderen Fachgebieten
- Fähigkeiten und Ressourcen zur Entwicklung bzw. Anpassung von Software an die eigenen Anforderungen; dies erfordert die Sicherstellung des Zugangs zu Entwicklungswerkzeugen, Software-Bibliotheken und Expert:innen

Produktionssouveränität

- Zugang zu Fähigkeiten und Ressourcen für die Fertigung und Qualitätssicherung von Produkten, wie z. B. Tools und Komponenten, Produktions- und Prüfungsanlagen

Betriebssouveränität

- Zugang zu Ressourcen und Fähigkeiten, um den gewünschten Betriebszustand von Komponenten und digitalen Systemen einrichten, steuern und wiederherstellen zu können
- Zugang zu Fähigkeiten und Ressourcen, um sichere, vertrauenswürdige und resiliente digitale Systeme aufbauen bzw. die Funktionalität, Sicherheit und Vertrauenswürdigkeit von Komponenten und Systemen bewerten zu können

Nutzungssouveränität

- Zugang zu Fähigkeiten und Ressourcen, um digitale Technologien gemäß den eigenen institutionellen Anforderungen und Prioritäten erfolgreich, effizient und (rechts-)sicher nutzen zu können

Transparenzsouveränität

- Zugang zu Fähigkeiten und Ressourcen, um die Ergebnisse von Softwareberechnungen («Entscheidungen«, Empfehlungen) nachvollziehen und begründen und gegebenenfalls durch menschliches Eingreifen beeinflussen, anfechten oder revidieren zu können

3. Ist- und Soll-Analyse strategischer Autonomie im Digitalen

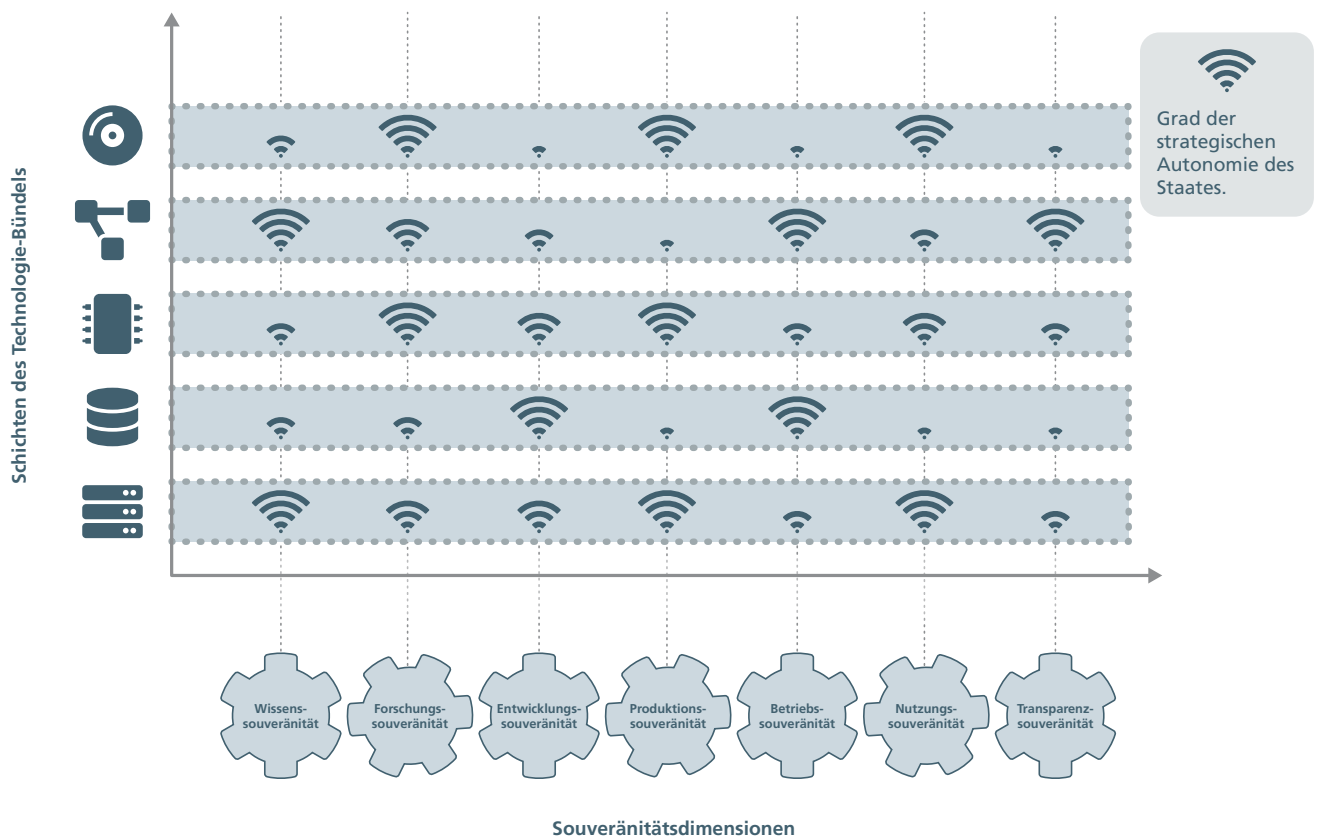
Das Betrachten der verschiedenen Souveränitätsdimensionen für alle Elemente des Technologie-Bündels einer öffentlichen Leistung schafft den Überblick über die möglichen Abhängigkeiten und Ansatzpunkte für die strategische Steuerung der digitalen Strukturen einer staatlichen Leistung.

Steuerungsfähigkeit erlaubt dem Staat das aktuell vorgefundene institutionelle Arrangement (siehe C.1.2)? Aus der Zusammenschau der Souveränitätsdimensionen ergibt sich so die strategische Autonomie mit Blick auf die einzelne technische Komponente. Gewichtet man diese Einschätzungen nach der Bedeutung der technischen Komponente für die gesamte Leistungskette, ergibt sich die bestehende digitale strategische Autonomie für die untersuchte öffentliche Leistung. Wenn beispielsweise in einer Leistungskette alle eingesetzten Software-

3.1 Ist-Analyse der strategischen Autonomie im Digitalen

Die Ist-Analyse ist ein Bottom-up-Prozess. Zunächst wird jede technische Komponente im Technologie-Bündel einer Leistungskette betrachtet. In jeder Souveränitätsdimension stellen sich die Fragen: Wie bedeutsam, oder prozedural relevant, ist diese Souveränitätsdimension, um etwa Verfügbarkeit oder Qualität der technischen Komponente zu steuern? Wieviel

Abbildung 6: Matrix zur Bewertung von Autonomiegraden im Digitalen. Vertikal die generischen Schichten des Technologie-Bündels zur Erfüllung einer Aufgabe. Horizontal die Souveränitätsdimensionen. An den Kreuzungen von technischen Schichten und Souveränitätsdimensionen sind beispielhafte Ist- oder Soll-Grade der strategischen Autonomie des Staates abgebildet.



produkte von öffentlichen IT-Dienstleistern entwickelt und betrieben werden, spricht dies zunächst für einen hohen Grad digitaler strategischer Autonomie für diese Leistung. Tauschen die Softwareinstanzen ihre Daten jedoch über einen Server außerhalb des deutschen Rechtszugriffs aus, reduziert sich insgesamt die strategische Autonomie, da die Steuerungsfähigkeit bei einer kritischen Komponente des Technologie-Bündels gering ausfällt.

3.2 Soll-Analyse der strategischen Autonomie im Digitalen

Die Soll-Analyse ist ein Top-down-Prozess, invers zur Ist-Analyse. Zunächst wird die **strategische Relevanz** der untersuchten öffentlichen Leistung insgesamt aus staatlicher Sicht bewertet (siehe B.3.2.1). Je höher die strategische Relevanz der Leistung, desto mehr strategische Autonomie ist bei der Leistungserstellung insgesamt anzustreben. Doch wo genau sind Maßnahmen zur Erhöhung der strategischen Autonomie sinnvoll? Aus der Bedeutung der einzelnen technischen Komponenten für die Erstellung der öffentlichen Leistung lässt sich ihre Priorität für eine eventuell notwendige Steigerung der staatlichen Steuerungsfähigkeit ermitteln (siehe B.3.2.2). Wie lässt sich für priorisierte technische Komponenten eine größere staatliche Steuerungsfähigkeit erzielen? Die Stellschrauben hierfür liegen in den Souveränitätsdimensionen, die für jede technische Komponente neu zu betrachten sind. So mag bei vielen digitalen Diensten die Kontrolle z. B. über den Betrieb der konkreten Instanz ausreichend strategische Autonomie sichern (»Betriebsouveränität«), bei einigen technischen Komponenten aber auch ihre Produktion (»Produktionssouveränität«) oder sogar die Forschung (»Forschungssouveränität«) daran staatlich zu gewährleisten sein. Die Optionen zur Steigerung der strategischen Autonomie bezüglich einer technischen Komponente (siehe C.) – vom Austausch gegen eine andere technische Lösung über die Umgestaltung des Leistungserstellungsprozesses bis hin zu Regulierungsmaßnahmen und institutionellen Arrangements in den verschiedenen Souveränitätsdimensionen – sind dabei auch auf ihre **Wirtschaftlichkeit** zu bewerten. So zeigt die Abwägung zwischen **prozeduraler Relevanz** der Komponente für die Leistungserstellung einerseits und Wirtschaftlichkeit der möglichen Gestaltungsoptionen andererseits sinnvolle Handlungsalternativen auf (siehe B.3.2.2). Dabei hilft es, die angestrebten Steuerungsziele (siehe B.3.2.3) zu unterscheiden, beispielsweise ob bereits die Einhaltung von Quali-

tätsstandards auch ohne staatliche Betriebsouveränität einen ausreichenden Beitrag zur strategischen Autonomie leistet.

3.2.1 Strategische Relevanz der öffentlichen Leistung

Strategische Relevanz stellt die Frage danach, wie wichtig ein Produkt oder eine Dienstleistung für das Erreichen staatlicher Ziele ist. Zeigt beispielsweise die Webseite einer Kommunalverwaltung lediglich die Öffnungszeiten des Bürgeramtes an, sind Abhängigkeiten bei der Bereitstellung der Webseite weitgehend unproblematisch. Ist diese Webseite jedoch im Katastrophenfall als zentrale Informationsquelle für die Bürger:innen der Gemeinde designiert, besteht ein größerer Bedarf nach strategischer Autonomie.

Als Faustregeln für eine hohe strategische Relevanz gelten beispielsweise Leistungen,

- deren Mangel Staat und Bürger:innen existenziell gefährdet,
- deren Erstellung eines weitreichenden Zugriffs auf Verwaltungsinformationen bedarf oder mit Geheimhaltungspflichten verbunden ist,
- die kritische Bausteine langfristiger Pläne sind,
- die hohe Bedeutung für die äußere Sicherheit haben,
- deren Fremdbezug überbordende Kontrollkosten erzeugt.²²

Einfließen kann auch das Risiko möglicher negativer Folgen, falls die Leistung nicht erbracht wird. Das Risiko ergibt sich aus der geschätzten Eintrittswahrscheinlichkeit der negativen Folgen und der resultierenden Schadenshöhe.²³

Die strategische Relevanz, die einer öffentlichen Leistung beigegeben wird, bedingt auch den Grad der strategischen Autonomie, den der Staat bei der Erstellung dieser Leistung im Idealfall innehaben sollte.

3.2.2 Strategische Autonomie im Technologie-Bündel: Prozedurale Relevanz und Wirtschaftlichkeit

Wie ist die insgesamt angestrebte strategische Autonomie einer öffentlichen Leistung über die Souveränitätsdimensionen des Technologie-Bündels hinweg wirtschaftlich zu realisieren? Dies

²² Naschold, F. et al. (1996: 45f).

²³ Romeike, F. (2018).

ergibt sich aus dem Abwägen von drei Aspekten: Prozedurale Relevanz, Wirtschaftlichkeit und Spezifität, einer Sonderform der Wirtschaftlichkeit.²⁴

Prozedurale **Relevanz** bemisst einerseits in Bezug auf eine technische Komponente, wie wichtig diese für die Erstellung einer öffentlichen Leistung ist. Hat eine technische Komponente im Technologie-Bündel lediglich Zusatzfunktion und ihr Ausfall würde die Leistungserstellung nicht grundsätzlich gefährden? Oder spielt der digitale Dienst eine Schlüsselfunktion im Bündel, weil er etwa essenzielle Datenflüsse gewährleistet?

Mit Blick auf die Souveränitätsdimensionen bewertet prozedurale Relevanz andererseits, wie wichtig eine Souveränitätsdimension für die Steuerbarkeit einer technischen Komponente ist. Wird die staatliche Handlungsfähigkeit bezogen auf eine einzelne technische Komponente eher durch Betriebsouveränität gewährleistet, beispielweise bei der Datenhaltung in Rechenzentren, oder durch die Forschungs- und Entwicklungsoveränität, etwa bei kryptografischen Verfahren? Diese Bewertung kann je nach angestrebtem Steuerungsziel – etwa Wirkung, Qualität oder Aspekte des Erstellungsprozesses einer öffentlichen Leistung (siehe B.3.2.3) – unterschiedlich ausfallen.

²⁴ Naschold, F. et al. (1996).

²⁵ In Anlehnung an Naschold, F. et al. (1996).

Wirtschaftlichkeit erwägt das Kosten-Nutzen-Verhältnis verschiedener Gestaltungsoptionen (siehe C.) in den Souveränitätsdimensionen: Was kosten mögliche Umsetzungsvarianten und welche Vor- und Nachteile bringen sie mit sich? So drängt sich gerade in strategisch sensiblen Anwendungsfeldern schnell die Erstellung in staatlicher Eigenregie als Präferenz auf. Die Betrachtung der Kosten weitet jedoch den Blick für leistungs- und politikfeldübergreifende Abwägungen, ob etwa die nötigen Mittel nicht für andere Zwecke wirkungsvoller einzusetzen sind.

Spezifität bewertet, wie spezifisch die Produktionsfaktoren einer technischen Komponente in ihren verschiedenen Souveränitätsdimensionen sind. Können z. B. Wissen, Hard- und Software sowie Infrastrukturen auch für andere Zwecke eingesetzt werden, senkt dies die Spezifität. Ursache hoher Spezifität sind oft Anforderungen oder Einsatzzwecke, die nur im öffentlichen Sektor vorkommen, etwa im Sicherheitsbereich. Hohe Spezifität führt bei staatlicher Eigenerstellung oft zu hohen Kosten und bei Fremdbezug zu stärkerer Abhängigkeit von einzelnen Anbietern, etwa in Lock-in-Situationen.²⁶

So können prozedurale Relevanz einerseits sowie Spezifität und Wirtschaftlichkeit andererseits als zwei Seiten einer Waage verstanden werden, die es auszutarieren gilt. Diese Balance gibt

²⁶ Thapa, B. (2019).



eine gute Orientierung, welcher Grad strategischer Autonomie und somit auch welche Leistungstiefe – also Art und Umfang staatlicher Beteiligung an der Leistungserstellung – bei der einzelnen Leistung und je Prozessschritt der Leistungserstellung anzustreben ist.

3.2.3 Steuerungsziele: Wirkung, Qualität, Prozess

Strategische Autonomie muss nicht bedeuten, dass sämtliche Facetten einer öffentlichen Leistung und ihrer Erstellung staatlichem Einfluss unterliegen. Die Konkretisierung und Priorisierung der Steuerungsziele hilft dabei, das erforderliche Maß digitaler strategischer Autonomie festzustellen und die effizienteste Gestaltungsoption zur Erreichung desselben zu identifizieren: Sind beispielsweise Wirkung, Qualität und/oder Erstellungsprozess einer Leistung strategisch relevant?²⁷

- **Wirkung:** Steuerung, damit eine gewünschte Wirkung erzielt wird, beispielsweise Internetzugang für 90 Prozent aller Privathaushalte. Es ist zunächst irrelevant, wie diese Wirkung zustande kommt, solange sie zuverlässig abgerufen werden kann.
- **Qualität:** Vorgeben von Eigenschaften einer Leistung, beispielsweise Geschwindigkeit und Preise der Internetanschlüsse. Welche Wirkung die Leistung hat, ist zunächst nicht von Interesse.
- **Prozess:** Vorgaben zu Aspekten der Leistungserstellung, beispielsweise Arbeitsbedingungen oder Umweltfolgen der Internetanbieter. Wirkung und Qualität der Leistung sind hier zunächst ohne Belang.

3.3 Strategische Vorausschau

Eine so erfolgte Ist- und Soll-Analyse ist eine Momentaufnahme, sowohl was die bestehenden Abhängigkeiten als auch was die strategischen Relevanzen angeht. Strategie ist jedoch per Definition langfristig ausgerichtet. Entsprechend empfiehlt sich ein Blick auf die Matrix mit möglichst informierten Projektionen zur zukünftigen Entwicklung von **Technologie, Prozessen** und **strategischem Umfeld**.

Gerade digitale **Technologien** sind zum Teil disruptivem, raschem Wandel unterworfen. Nicht nur die eingesetzten Technologien in einzelnen technischen Schichten können sich mittelfristig verändern, sondern das gesamte Technologie-Bündel kann obsolet werden. Dabei geht es nicht nur um die Frage, welche konkreten Produkte zukünftig für die Leistungserstellung eingesetzt werden, sondern auch darum, wie sich technische Entwicklungen darüber hinaus auf die staatliche Aufgabe und das Technologie-Bündel insgesamt auswirken. So wird beispielsweise schon lange davor gewarnt, dass mit dem am Durchbruch stehenden Quantencomputing aktuelle Verschlüsselungsverfahren auf einen Schlag unsicher werden könnten.

Da das eingesetzte Technologie-Bündel von der Organisation der **Prozesse** zur Aufgabenerfüllung abhängt, sind auch mögliche Veränderungen der Prozesse in die strategische Vorausschau einzubeziehen. Kommen so vielleicht neue Technologien hinzu oder fallen bisher genutzte digitale Lösungen aus dem Technologie-Bündel? Können Prozesse so gestaltet werden, dass kritische Abhängigkeiten obsolet werden?

Bei der Bewertung von Abhängigkeiten sind auch absehbare Veränderungen des **strategischen Umfeldes** einzubeziehen. Zeichnet sich in einem Lieferantenmarkt eine monopolartige Situation ab? Bedroht ein möglicher Handelskonflikt die Zuverlässigkeit internationaler Bezugsquellen? Steht eine bestehende Technologiepartnerschaft durch ein diplomatisches Zerwürfnis auf dem Spiel?

Indem Varianten des Technologie-Bündels gegen verschiedene Szenarien durchgespielt und bewertet sowie entsprechende Entscheidungen getroffen werden, lässt sich die strategische Autonomie im Digitalen möglichst zukunftsfest gestalten.

4. Zusammenfassung: Analyseraster

In jedem Prozessschritt zur Erstellung einer öffentlichen Leistung werden digitale Lösungen eingesetzt, die sich in die technischen Schichten Software, Daten, Hardware, Netze und Plattformen unterscheiden lassen. Zusammen bilden sie das Technologie-Bündel der öffentlichen Leistung. Jede technische Komponente dieses Bündels besitzt mehrere Souveränitätsdimensionen, orientiert an der Wertschöpfungskette ihrer Erstellung. Dies kann beispielweise die Forschung an der Technologie, die Entwicklung konkreter Produkte und Dienste oder der Betrieb einzelner Instanzen sein. In diesen Souveränitätsdimen-

²⁷ Naschold, F. et al. (1996: 57f).

sionen ist mehr oder weniger staatliche Steuerung möglich. Hieraus ergibt sich zusammengefasst also die staatliche Steuerungsfähigkeit der technischen Komponente. Entlang dieses Rasters lassen sich Ist und Soll der strategischen Autonomie für die technischen Komponenten einer öffentlichen Leistung ermitteln. Dabei hilft die Bewertung von strategischer Relevanz der Leistung, prozeduraler Relevanz der technischen Komponenten sowie Spezifität und Wirtschaftlichkeit der verschiedenen Gestaltungsoptionen ihrer Bereitstellung. Ebenso wichtig ist die Frage, ob für die strategische Autonomie die Steuerbarkeit von Wirkung, Qualität oder Prozess ausschlaggebend ist. Zuletzt sind diese Bewertungen auch mit Blick auf zukünftige Entwicklungen zu prüfen.

C. LÖSUNGSANSÄTZE

Dieser Abschnitt zeigt Handlungsoptionen zur Steigerung der strategischen Autonomie des digitalen Staates auf. Dabei stehen Änderungen an Prozessen und Technologie-Bündeln, die institutionellen Arrangements bei der Erstellung von technischen Komponenten oder ganzen öffentlichen Leistungen sowie technologiepolitische Strategien für Schlüsseltechnologien zur Auswahl. Welche dieser Optionen tatsächlich infrage kommen, hängt von Ressourcen und Fähigkeiten ab, die wir im Überblick darlegen. Darauf aufbauend geben wir einige generelle Handlungsempfehlungen für den deutschen Staat ab.

1. Gestaltungsoptionen für strategische Autonomie im Digitalen

Welche Gestaltungsoptionen stehen dem Staat offen, um seine strategische Autonomie in der digitalen Verwaltung zu beeinflussen? Wir stellen hier drei grundsätzliche Handlungsfelder vor: Veränderungen an Prozess und Technologie-Bündel der Leistungserstellung, Gestaltungsoptionen bei der Bereitstellung von öffentlichen Leistungen oder ihrer technischen Komponenten sowie technologiepolitische Strategien. Welche Optionen

offenstehen, hängt maßgeblich von den gegebenen Ressourcen und Fähigkeiten ab.

1.1 Änderungen an Prozessen und Technologie-Bündeln

Führen einzelne Komponenten eines Technologie-Bündels zu problematischen Abhängigkeiten, können diese eventuell entfernt werden. Im einfachsten Fall kann eine solche Komponente im Bündel ausgetauscht werden, etwa durch den Wechsel zu einem Hardwaremodell aus anderen Bauteilen oder zu einem Anbieter unter anderer Rechtshoheit. Ist dies nicht möglich oder mit zu vielen Nachteilen verbunden, können auch der organisatorische Prozess der Leistung oder die technische Architektur des Technologie-Bündels angepasst werden, um problematische technische Komponenten überflüssig zu machen oder ihre Bedeutung zu mindern. So können zum Beispiel die hohen Autonomieanforderungen aus der Aufbewahrung sensibler Daten oft vermieden werden, indem der Prozess dezentralisiert wird, sodass keine zentrale Datenhaltung nötig ist.

Eigenerstellung	Behörden (ITZ Bund), Eigenbetrieb (Stadtwerke), AöR (ITDZ Berlin)
Nonprofit-Sektor	Stiftungen (Stiftung Datenschutz), Vereine (Fraunhofer-Gesellschaft), Wohlfahrsträger (Deutsches Rotes Kreuz)
freie Wirtschaft	Hersteller von IT-Hardware und Software
Crowd	Crowdsourcing, bürgerschaftliche Koproduktion, Open Source
Mischformen	ÖPP (DFKI), orchestrierte Aktion, »Pakte«, Runde Tische

Abbildung 8: Verschiedene Konstellationen der Erstellung öffentlicher Leistungen.

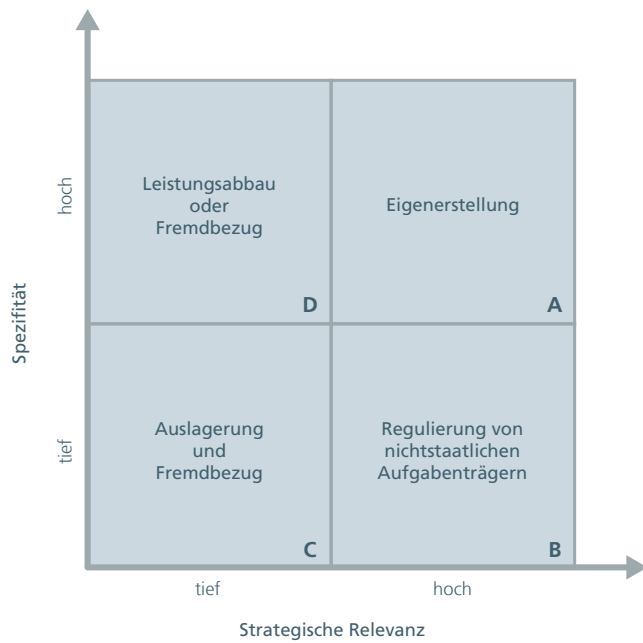


Abbildung 9: Vier-Felder-Matrix zur Bestimmung der Leistungstiefe nach Spezifität und Relevanz.²⁸

Abbildung 10: Diverse staatliche Steuerungsinstrumente zur Beeinflussung der strategischen Autonomie bei der Leistungserstellung.

Regulative Politik	Verbote, Lizenzen, Marktzutrittschranken, Ein- und Ausfuhrbestimmungen
Finanzierung	Steuern, Einkauf, Förderprogramme (inkl. Kriterien und Vertragsgestaltung)
Strukturierung	Institutionelle Musterlösungen, Beteiligungsangebote, Koordinationsgremien, Selbstverwaltung
Überzeugung	Appelle, Empfehlungen, Kampagnen

1.2 Leistungstiefe und Steuerungsinstrumente

Die staatliche Steuerungsintensität einer öffentlichen Leistung oder ihrer technischen Komponenten kann durch das Arrangement von Leistungstiefe, etwa staatlicher Eigenerstellung oder Fremdbezug am Markt, und Steuerungsinstrumenten wie z. B. Förderprogrammen oder Qualitätsstandards justiert werden. Diese institutionellen Arrangements sind stets in Kombination zu denken: So mag der Fremdbezug am freien Markt unter strenger Regulierung Steuerbarkeit wirksamer und kostengünstiger ermöglichen als die Eigenerstellung durch eine öffentliche Anstalt unter schwachen Vorgaben.

Auf die klassische »Make or buy«-Frage kann der öffentliche Sektor mit zahlreichen Varianten der Leistungstiefe antworten.²⁹ Dabei ist die Vier-Felder-Matrix aus Spezifität und Relevanz (Abbildung 9) nur als erste Annäherung zu sehen, da sich aus dem Zusammenspiel mit weiteren staatlichen Steuerungsinstrumenten vielfältige Gestaltungsoptionen ergeben.

Zur Beeinflussung von Verhalten stehen dem Staat diverse Steuerungsinstrumente zur Wahl.³⁰ Am direktesten wirken dabei regulative Instrumente wie Sicherheitsauflagen, Bedingungen für den Marktzutritt oder sogar Verbote. Bei derartigen regula-

²⁸ Quelle: Naschold, F. et al. (1996).

²⁹ Ritz, A., & Thom, N. (2006).

³⁰ Braun, D. und Giraud, O. (2003).

tiven Eingriffen ist jedoch mit politischem Widerstand zu rechnen. Eher als Anreize wirken Finanzierungsinstrumente wie Steuervergünstigungen, die öffentliche Beschaffung oder Förderprogramme, durch die etwa durch Vertragsgestaltung und Förderkriterien ganz unterschiedliche Steuerungsziele (siehe B.3.2.3) umgesetzt werden können. Entscheidend für die Steuerungswirkung sind hier meist die Zielgenauigkeit der Anreize, die eingesetzten Finanzvolumina und die Marktsituation. Sanft steuern Instrumente der Überzeugung und der Strukturierung, die auf die Nutzung freiwilliger Angebote und das Begleiten von Aushandlungsprozessen setzen. Diese Instrumente sind politisch leicht durchzusetzen, bleiben bei abweichenden Interessen aber oft wirkungslos.

Nicht alle Steuerungsinstrumente und Leistungstiefen sind für alle öffentlichen Leistungen, technischen Komponenten und Souveränitätsdimensionen möglich oder wirtschaftlich sinnvoll (siehe auch C.1.4).

1.3 Technologiepolitische Strategien für Schlüsseltechnologien

Schlüsseltechnologien für die strategische Autonomie besitzen zentrale Bedeutung über mehrere essenzielle öffentliche Leistungen hinweg oder werden diese gemäß der strategischen Vorausschau zukünftig einnehmen.³¹ Für diese hervorgehobenen Technologien sollten übergeordnete technologiepolitische Strategien entwickelt werden.

Prinzipiell stehen dabei für jede Technologie drei strategische Ansätze zur Wahl: »Risikomanagement«, »strategische Partnerschaften« und »Gemeingüter«.³² Die Wahl und Kombination der Ansätze ist zuvorderst eine politische Frage, wird aber auch vom bestehenden Spielraum strategischer Autonomie bestimmt (siehe C.1.4). Der gewählten Strategie sollten auch die Gestaltung von Leistungstiefe und Steuerungsinstrumenten für diese Technologie folgen.

1.3.1 Risikomanagement und Resilienz

Risikomanagement zielt auf größtmögliche Resilienz gegenüber Risiken und Bedrohungen, die hier im Speziellen aus dem Einsatz einer digitalen Technologie herrühren. Grundannahme ist dabei, dass die Integrität und das Verhalten von Technologien in komplexen Systemen nicht vollständig kontrolliert werden können: »Buyers must accept that what suppliers provide cannot be fully kept under control.«³³

Staatliche Anstrengungen zielen also entlang des Resilienz-Zyklus auf die Vorbereitung auf Schadensereignisse (prepare), das Reduzieren von Risikofaktoren (prevent), das Herstellen von Schutzsystemen (protect), das Aufrechterhalten essenzieller Funktions- und Reaktionsfähigkeit (respond) und die eigenständige Erholung und Lernfähigkeit von Systemen (recover).³⁴

Technisch kann dies einen verstärkten Fokus auf resiliente IKT-Architekturen, bei denen z. B. Redundanzen das Gesamtsystem gegen den Ausfall von Teilsystemen schützen, oder auf Software für Systemmonitoring und Bedrohungsdetektion bedeuten. Typische Regulierungen wären etwa Berichts-, Melde- und Kooperationspflichten, verpflichtende Sicherheitszertifizierungen und zentrale Anlaufstellen für präventive und reaktive Maßnahmen.³⁵

1.3.2 Strategische Partnerschaften

Durch strategische Partnerschaften soll durchdacht mit gemeinsamen oder wechselseitigen Abhängigkeiten umgegangen werden. Staaten und nicht-staatliche Akteure arbeiten auf Grundlage von Vertrauen und geteilten Werten zu ausgewählten Technologien zusammen, um durch die gemeinsame Generierung und Kontrolle digitalrelevanter Fähigkeiten und Ressourcen ihre strategische Autonomie im Digitalen zu erhöhen.³⁶ Beispiele sind die deutsch-französischen Kooperationen zu

³¹ So verweist z. B. die »Industriestrategie 2030« der Bundesregierung auf die Bedeutung von bestimmten Schlüsseltechnologien für das »nationale politische und wirtschaftliche Interesse« und sieht verschiedene Maßnahmen vor, um möglichst weitgehende Kontrolle und Zugang zu entsprechenden Technologien im eigenen Land zu behalten, siehe BMWi (2019).

³² Wir folgen hierbei den Vorschlägen von Timmers, P. (2019).

³³ Timmers, P. (2019: 13).

³⁴ Siehe acatech Resilienz-Zyklus in Menz, N. et al. (2015: 16,17).

³⁵ Z. B. EU-Richtlinie zur Netzwerk- und Informationssicherheit, EU Cybersecurity Act, IT-SiG, DSGVO, KRITIS-Verordnung bzw. BSI, CERTs, ENISA.

³⁶ Timmers spricht von »like-minded partners«, also staatlichen Akteuren, die sich aus EU-Perspektive z. B. durch die Wahrung individueller Bürger- und Freiheitsrechte, die Befolgung liberaler, marktwirtschaftlicher Politiken, eine unabhängige Justiz, freie Wahlen etc. als vertrauenswürdige Partner qualifizieren sollen. Timmers, P. (2019: 15).

künstlicher Intelligenz³⁷, die gemeinsame »Normungsroadmap Künstliche Intelligenz« zwischen DIN, VDE und BMWi³⁸ oder die europäische Infrastrukturinitiative GAIA-X³⁹. Auch die wechselseitige Anerkennung politikfeldspezifischer Regulierungen ist eine schwache Form strategischer Partnerschaften, etwa die mit Drittstaaten ausgehandelten Angemessenheitsbeschlüsse der EU-Kommission zum Datenschutz.

Bei strategischen Partnerschaften mit außereuropäischen Akteuren ist die klare Formulierung politischer Kriterien für die Partnerschaft eine wesentliche Herausforderung. Das gezielte Ausschließen oder Erschweren der Zusammenarbeit mit bestimmten Akteuren kann als negative strategische Partnerschaft verstanden werden. So kann gerade in komplexen technischen Systemen die ungewollte Abhängigkeit von Akteuren, zu denen wenig Vertrauen besteht oder die stark abweichende Werte besitzen, vermieden werden. Angesichts der festgestellten Volatilität der regelbasierten internationalen Ordnung nehmen solche Fälle zu, beispielsweise der geplante Ausschluss chinesischer 5G-Ausrüster aus zahlreichen europäischen und US-amerikanischen Netzen oder der geplante Ausschluss des Vereinigten Königreiches aus sensiblen Bereichen des europäischen Galileo-Navigationssystems im Zuge des britischen EU-Austritts.⁴⁰

1.3.3 Gemeingüter

Im Gemeingüteransatz werden Recht, Technologie und Governance so gestaltet, dass sie gleichberechtigte und selbstbestimmte Nutzung der betroffenen Technologien und Systeme ermöglichen.

Abhängigkeiten werden hier reduziert, indem kein Akteur die Technologie exklusiv kontrollieren kann. Zusätzlich werden Gemeingüter ohne die Möglichkeit von Zugangsbeschränkungen nur schwer Gegenstand von Rivalitäten. Eine Governance-Herausforderung ist das Trittbrettfahrerproblem bei der Weiterentwicklung der Technologien: Warum sollte ein Akteur in die Entwicklung und Bereitstellung investieren, wenn er durch Warten auf die Investition eines anderen Akteurs den gleichen Nutzen ohne eigene Kosten erzielt? Dies kann in eine Pattsituation führen, die es zu durchbrechen gilt.

³⁷ BMBF (2019).

³⁸ BMWi, VDE und DIN (2019).

³⁹ BMWi (2020).

⁴⁰ Neue Zürcher Zeitung (2018).

Herausragendes Beispiel für ein solches Gemeingut ist das Internet. Mit seiner dezentralen Architektur, den offenen Standards und Protokollen sowie der inklusiven Multi-Stakeholder-Governance ist es prinzipiell darauf angelegt, die Entstehung von Machtkonzentrationen zu vermeiden und lädt zur selbstbestimmten Entwicklung alternativer Nutzungen ein. Dabei zeigt die zunehmende Politisierung der Internet-Governance aber auch die Grenzen eines solchen Ansatzes auf.⁴¹

Die staatliche Nutzung und Förderung von Open-Source-Lösungen entsprechen ebenfalls dem Gemeingüteransatz, da die so geschaffenen Technologien für alle Akteure offenstehen und ein hohes Maß strategischer Autonomie in der Herstellung, Nutzung und Weiterentwicklung ermöglichen.⁴²

1.4 Spielraum strategischer Autonomie

Nicht alle Gestaltungsoptionen stehen in allen Situationen zur Auswahl. Wie sich Prozesse der staatlichen Aufgabenerfüllung umgestalten lassen, welche Leistungstiefen und Steuerungsinstrumente wirksam und wirtschaftlich und welche technologiepolitischen Strategien gangbar sind, unterscheidet sich je nach Ressourcen und Fähigkeiten von Staat und Verwaltung im jeweiligen Anwendungsfeld. Eine Reihe von Faktoren erweitern oder verringern die Gestaltungsoptionen für die strategische Autonomie im Digitalen.

Technische Voraussetzungen: etwa die vorliegenden Kommunikationsnetze, die allgemeine informationstechnische Ausstattung der Verwaltung (wie bestehende Zentralregister), und Schnittstellen, aber auch Legacy-Systeme. So mag beispielsweise die technische Struktur der öffentlichen Datenhaltung bestimmte Veränderungen am Technologie-Bündel vereinfachen und andere erschweren.

Standortgegebenheiten: wie die Kapazitäten und die Ausrichtung der heimischen Hard- und Softwareindustrie, der Forschungslandschaft und des Bildungssystems. So ist die Forschungssouveränität für hochkomplexe Mikroprozessoren wesentlich schwerer zu erreichen, wenn das Land bisher keine entsprechenden Forschungseinrichtungen besitzt.

⁴¹ Siehe z. B. Thapa, B., Opiela, N. und Tiemann, J. (2019).

⁴² Free Software Foundation & Kompetenzzentrum Öffentliche IT (2020).



Abbildung 11: Der Gestaltungsspielraum zur Beeinflussung der strategischen Autonomie hängt von den verfügbaren Ressourcen und Fähigkeiten ab.

Verwaltungskapazitäten, etwa die Personal- und Ressourcenausstattung, aber auch die Koordinationsfähigkeit, um etwa rechtliche Vorgaben durchzusetzen, externe Leistungserstellung kompetent zu steuern oder gegebenenfalls einzelne technische Systeme in staatlicher Vollzugsverantwortung umzusetzen. Sonst können selbst Verbote unbeachtet bleiben, wenn die Verwaltung ihre Einhaltung nicht prüfen kann.

Rechtliche Rahmen: wie internationale Abkommen oder geltendes nationales oder supranationales Recht. So bestimmen etwa bestehende Handelsverträge mit, wie Außenhandelsregulierung als Steuerungsinstrument eingesetzt werden kann, oder das geltende Subventionsrecht, wie Partnerschaften zwischen Staat und Privatwirtschaft ausgestaltet werden können.

Die **Verhandlungsmacht** sowohl bei internationalen Verhandlungen oder Geschäftsverhandlungen mit Auftragnehmern als auch in internationalen Organisationen wie Standardisierungsgremien. Verhandlungsmacht kann von zahlreichen Faktoren abhängen, etwa wirtschaftlichem und militärischem Gewicht, Stimmenzahl in Gremien, historischer Verbundenheit, Verhandlungsgeschick, Verbündeten und vielem mehr.⁴³ Je nach Konstellation stehen einem Staat mehr oder weniger strategische Optionen offen.

Ressourcenausstattung und Fähigkeiten bestimmen also nicht nur, welche Grade strategischer Autonomie im Digitalen realistisch zu erreichen sind, sondern auch, welche Strategien für jeden einzelnen Staat am effizientesten sind.

Insgesamt gilt es vor allem, bestehende Stärken vorteilhaft einzubringen und Schwächen sowie die sich daraus ergebenden Schmerzpunkte durch den gezielten Aufbau geeigneter Ressourcen und Fähigkeiten bzw. das geschickte Ausspielen von Stärken auszugleichen.

2. Zusammenfassung: Lösungsansätze

Zur Steuerung der strategischen Autonomie des digitalen Staates stehen verschiedene Ansätze offen: Durch Veränderungen an Prozessen der Leistungserstellung oder an einzelnen Komponenten im Technologie-Bündel kann bestehenden Abhängigkeiten ausgewichen werden. Mit institutionellen Arrangements der Leistungserstellung, von der staatlichen Eigenerstellung bis zum Fremdbezug am freien Markt, sowie den verschiedenen Instrumenten staatlicher Steuerung – von Regulierung über Finanzierung und Strukturierung bis hin zu Überzeugungskampagnen – kann der Staat seine Entscheidungs- und Handlungsfreiheit in einzelnen Souveränitätsdimensionen technischer Komponenten gestalten. Zuletzt stehen für Schlüsseltechnologien mit Risikomanagement, strategischen Partnerschaften und dem Gemeingüteransatz drei große technologiepolitische Strategien zur Wahl. Welche der Lösungsansätze tatsächlich realisierbar sind, hängt von den bestehenden Ressourcen und Fähigkeiten ab, vom rechtlichen Rahmen über wirtschaftliche Standortgegebenheiten bis hin zur internationalen Verhandlungsmacht.

⁴³ Bailer, S. (2010).

3. Handlungsempfehlungen

Dieses Papier nähert sich dem Thema »digitale Souveränität« konzeptionell: Wir zeichnen die bestehende Debatte nach, bieten ein Denkmuster für die Ist- und Soll-Analyse staatlicher digitaler Souveränität und zeigen grundlegende Gestaltungsoptionen auf. Diese gilt es auf den Einzelfall anzuwenden und zu schärfen.

Doch bereits diese abstrakten Überlegungen legen einige allgemeine Handlungsempfehlungen für die strategische Autonomie der Bundesrepublik Deutschland im Digitalen nahe.

Abhängigkeiten identifizieren und verstehen.

Wie strategisch autonom ist der deutsche Staat im Digitalen? Eine empirisch fundierte Antwort auf diese Frage ist Voraussetzung für strategisches Handeln, fehlt jedoch mit Ausnahme einzelner Schlaglichter. Das systematische Durchleuchten von Prozessschritten der Leistungskette, der eingesetzten Technologie-Bündel und der zu deren Bereitstellung relevanten Souveränitätsdimensionen ist zumindest für strategisch bedeutsame öffentliche Leistungen unerlässlich.

Strategische Autonomie ist das Ziel, Abhängigkeitsmanagement die Aufgabe.

Ein bewusster Umgang mit Abhängigkeiten in der Digitalisierung setzt die Einsicht voraus, dass Abhängigkeiten unvermeidbar und nicht in jedem Fall problematisch sind. Vielmehr geht es um die planvolle Wahl von Abhängigkeitsgraden. So wird das übergeordnete Ziel *strategischer* Autonomie erreicht, indem kleinteiliges *Abhängigkeitsmanagement* betrieben wird. Abhängigkeiten können vernachlässigbar sein, durch institutionelle Arrangements eingehegt werden, unvermeidbar oder kritisch sein und deshalb den Aufbau von Risikomanagement und Resilienz erfordern oder in strategischen Partnerschaften bewusst gewählt werden.

Europäisch denken.

Deutschland vergrößert seine strategische Autonomie im Digitalen signifikant, wenn es diese europäisch denkt. Die gemeinsame Ressourcenausstattung der EU bietet einen beeindruckenden Hebel für den strategischen Spielraum, von Standortgegebenheiten wie Forschungs- und Industrielandschaft über den (digitalen) Binnenmarkt bis hin zur Verhandlungs-

macht in der Vertragsgestaltung mit privatwirtschaftlichen Anbietern oder in internationalen Standardisierungsgremien. Die EU bietet sich durch geteilte Werte und bestehende Governance-Mechanismen als dauerhafte strategische Partnerschaft an.

Strategische Autonomie in die Zukunft denken.

Digitale Technologien, Prozesse, Märkte und internationale Beziehungen können hochdynamisch sein. Strategische Autonomie im Digitalen kann also nicht einmal hergestellt und abgehakt werden, sondern bedarf ständiger Überprüfung. Dabei kann helfen, Technologie-Bündel und Abhängigkeiten mithilfe strategischer Vorausschau möglichst zukunftsfest zu gestalten.

Politikfeldübergreifend denken.

Digitale Technologien wirken als Querschnittsfunktion in viele Politikfelder. Gleichzeitig wird die strategische Autonomie im Digitalen von vielen Politikfeldern beeinflusst: Industrie-, Forschungs-, Bildungs-, Verwaltungs-, Außen- und Sicherheitspolitik, um nur offensichtliche Beispiele zu nennen. In jedem dieser Politikfelder konkurriert digitale strategische Autonomie mit bestehenden politischen Zielen und Logiken. Konzertiertes Handeln zur Steigerung der strategischen Autonomie im Digitalen bedarf der Mitarbeit zahlreicher Ressorts und Akteure.

Besondere Rolle von Wissens-, Forschungs- und Betriebs-souveränität beachten.

Die öffentliche IT in Deutschland basiert in vielen Bereichen auf Produkten und Dienstleistungen, die international bezogen werden müssen – seien es Aktualisierung und Wartung oder einzelne Komponenten von digitalen Systemen, die von Dritten entwickelt und gefertigt werden. Hiermit gehen Schmerzpunkte einher, z. B. bezüglich der Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen und Daten. Zur Gewährleistung strategischer Autonomie sollte vor diesem Hintergrund besonderer Fokus gelegt werden auf den Aufbau von Wissen, Fähigkeiten und Ressourcen, welche Souveränität in der Systemintegration, im Systembetrieb und in der Beurteilungsfähigkeit von Sicherheit und Vertraulichkeit ermöglichen. Wissens-, Forschungs- und Betriebs-souveränität tragen hierzu in besonderem Maße bei.

Referenzen

Accenture (2020): Globality and Complexity of the Semiconductor Ecosystem. https://www.accenture.com/_acnmedia/PDF-119/Accenture-Globality-Semiconductor-Industry.pdf#zoom=50.

Bailer, S. (2010): What factors determine bargaining power and success in EU negotiations? In: *Journal of European Public Policy*, 17(5), 743 – 757.

Bendiek, Annegret; Godehardt, Nadine; Schulze, David (2019): Das Zeitalter der digitalen Geopolitik. In: *Internationale Politik und Gesellschaft*. <https://www.ipg-journal.de/rubriken/aussen-und-sicherheitspolitik/artikel/das-zeitalter-der-digitalen-geopolitik-3579/>.

Bendiek, Annegret; Schallbruch, Martin (2019): Europas dritter Weg im Cyberraum. Stiftung Wissenschaft und Politik. https://www.swp-berlin.org/fileadmin/contents/products/aktuell/2019A60_bdk_Schallbruch_WEB.pdf.

Bundesregierung (2019): Eckpunkte einer Datenstrategie der Bundesregierung. <https://www.bundesregierung.de/resource/blob/975226/1693626/60b196d5861f71cdefb9e254f5382a62/2019-11-18-pdf-datenstrategie-data.pdf?download=1>.

Bundesministerium für Bildung und Forschung (BMBF, 2019): Roadmap for a Research and Innovation Network on Artificial Intelligence between the Governments of the French Republic and the Federal Republic of Germany. https://www.bmbf.de/files/191016_Roadmap_FRA_GER_AI_Network.pdf.

Bundesministerium für Wirtschaft und Energie (BMW, 2019): Industriestrategie 2030. Leitlinien für eine deutsche und europäische Industriepolitik. https://www.bmwi.de/Redaktion/DE/Publikationen/Industrie/industriestrategie-2030.pdf?__blob=publicationFile&v=20.

Bundesministerium für Wirtschaft und Energie (BMW, 2020): GAIA-X: Das europäische Projekt startet in die nächste Phase. https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/gaia-x-das-europaeische-projekt-startet-in-die-naechste-phase.pdf?__blob=publicationFile&v=18.

Bundesministerium für Wirtschaft und Energie, VDE Verband der Elektrotechnik Elektronik Informationstechnik und Deutsches Institut für Normung (BMW, VDE und DIN 2019): Künstliche Intelligenz braucht Normen und Standards. <https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2019/20191016-kuenstliche-intelligenz-braucht-normen-und-standards.html>.

Bundesministerium für Arbeit und Soziales (BMAS, 2020): Versorgungssicherheit bei Atemschutzmasken sichern. <https://www.bmas.de/DE/Presse/Pressemitteilungen/2020/versorgungssicherheit-bei-atemschutzmasken-sichern.html>.

Braun, Dietmar; Giraud, Olivier (2003): Steuerungsinstrumente. In: Schubert, Klaus; Nils Bandelow (Hg.): *Lehrbuch der Politikfeldanalyse*, S. 147 – 174.

Deutscher Bundestag, Ausschuss Digitale Agenda (2019): Digitale Wahlbeeinflussung. <https://www.bundestag.de/presse/hib/635124-635124>.

EU-Kommission (2019): Foreign Investment Screening: new European framework to enter into force in April 2019. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1532.

EU-Kommission (2020a): Weißbuch Zur Künstlichen Intelligenz. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_de.pdf.

EU-Kommission (2020b): Europäische Datenstrategie. <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020DC0066>.

EU-Kommission (2020c): Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures. <https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>.

Free Software Foundation & Kompetenzzentrum Öffentliche IT (2020): Public Money – Public Code. Modernisierung der öffentlichen Infrastruktur mit freier Software. <https://www.oefentliche-it.de/publikationen?doc=119321>.

- Goldacker, Gabriele (2017):** Digitale Souveränität. Kompetenzzentrum Öffentliche IT. <https://www.oeffentliche-it.de/publikationen?doc=71579>.
- Golem.de (2020):** Apple gibt Frankreichs Forderungen nicht nach. <https://www.golem.de/news/corona-app-apple-gibt-frankreichs-forderungen-nicht-nach-2005-148287.html>.
- Handelsblatt (2017):** Wir Europäer müssen unser Schicksal in unsere eigene Hand nehmen. <https://www.handelsblatt.com/politik/deutschland/angela-merkel-wir-europaeer-muessen-unser-schicksal-in-unsere-eigene-hand-nehmen/19861340.html>.
- Handelsblatt (2019):** Die Chipindustrie erlebt ein schwarzes Jahr. <https://www.handelsblatt.com/technik/it-internet/elektro-nik-die-chipindustrie-erlebt-ein-schwarzes-jahr/25303862.html?ticket=ST-5796577-IZGMFvf7uej36HcVKcQF-ap1>.
- Hannoversche Allgemeine Zeitung (2019):** Altmaier verspricht eine neue Strategie. <https://www.haz.de/Nachrichten/Wirtschaft/UVN-Industrieforum-Altmaier-verspricht-eine-neue-Strategie>.
- Hoepner, Petra; Weber, Mike; Tiemann, Jens; Welzel, Christian; Goldacker, Gabriele; Stemmer, Michael; Weigand, Florian; Fromm, Jens; Opiela, Nicole; Henckel, Lutz (2016):** Digitalisierung des Öffentlichen. Kompetenzzentrum Öffentliche IT. <https://www.oeffentliche-it.de/publikationen?doc=61787>.
- It-daily.net (2019):** Das IT-Sicherheitsgesetz 2.0 und KRITIS. <https://www.it-daily.net/it-sicherheit/enterprise-security/22286-das-it-sicherheitsgesetz-2-0-und-kritis>.
- IT-Planungsrat (2020):** Stärkung der digitalen Souveränität der öffentlichen Verwaltung. Eckpunkte – Ziele und Handlungsfelder. https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/32_Umlaufverfahren_Eckpunktepapier/Entscheidungsniederschrift_Umlaufverfahren_Eckpunktepapier.pdf?__blob=publicationFile&v=3.
- Kagermann, H.; Wilhelm, U. (2020) (Hg.):** European Public Sphere. Gestaltung der digitalen Souveränität Europas (acatech IMPULS). <https://www.acatech.de/publikation/european-public-sphere/>
- Kölnische Rundschau (2018):** Juncker im Europaparlament »Europa muss sein Schicksal selbst in die Hand nehmen«. <https://www.rundschau-online.de/news/politik/juncker-im-europaparlament--europa-muss-sein-schicksal-selbst-in-die-hand-nehmen--31256386>.
- Lippert, Barbara; von Andarza, Nicolai; Perthes, Volker (2019):** Strategische Autonomie Europas. Akteure, Handlungsfelder, Zielkonflikte. Stiftung Wissenschaft und Politik. https://www.swp-berlin.org/fileadmin/contents/products/studien/2019S02_lpt_orz_prt.pdf.
- Löffler, E. (2015):** Koproduktion mit Bürgern und gemeinnützige Öffentlich-Private Partnerschaften. In: VM Verwaltung & Management, 21(6), S. 317 – 325.
- Masala, Carlo (2019):** Europa braucht strategische Autonomie! In: Auslandsinformationen 2/2019. Konrad-Adenauer-Stiftung. <https://www.kas.de/de/web/auslandsinformationen/artikel/detail/-/content/europa-braucht-strategische-autonomie>.
- Maurer, Tim et al. (2014):** Technological Sovereignty: Missing the Point? An Analysis of European Proposals after June 5, 2013. Transatlantic Dialogues on Security and Freedom in the Digital Age. https://www.newamerica.org/downloads/Technological_Sovereignty_Report.pdf.
- Menz, Nadja et al. (2019):** Safety und Security aus dem Blickwinkel der öffentlichen IT. Kompetenzzentrum Öffentliche IT. <https://www.oeffentliche-it.de/publikationen?doc=31236>.
- Mohabbat Kar, Resa; Tiemann, Jens; Welzel, Christian (2019):** Der Staat auf dem Weg zur Plattform. Kompetenzzentrum Öffentliche IT. <https://www.oeffentliche-it.de/publikationen?doc=113399>.
- Mohabbat Kar, Resa; Thapa, Basanta; Parycek, Peter (Hg.) (2018):** (Un)Berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft. Kompetenzzentrum Öffentliche IT. <https://www.oeffentliche-it.de/publikationen/unberechenbar>.
- Naschold, Frieder et al. (1996):** Leistungstiefe im öffentlichen Sektor: Erfahrungen, Konzepte, Methoden.

Ritz, Adrian; Thom, Norbert (2006): Public management. Innovative Konzepte zur Führung im öffentlichen Sektor.

Neue Zürcher Zeitung (2018): Die britische Galileo-Beteiligung wird zum Brexit-Konflikt. <https://www.nzz.ch/wirtschaft/britische-galileo-beteiligung-wird-zum-brexite-konflikt-id.1386801>.

Pohle, Julia; Thiel, Thorsten (2019): Digitale Vernetzung und Souveränität. Genealogie eines Spannungsverhältnisses. In: Isabelle Borucki; Wolf Jürgen Schünemann (Hg.): Internet und Staat. Perspektiven auf eine komplizierte Beziehung. Staatsverständnisse, Nr. 127, S. 57 – 80.

PwC Strategy & (2019): Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern. Eine Studie im Auftrag des BMI. https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.pdf?__blob=publicationFile.

Romeike, Frank (2018): Risikomanagement.

Roth, Michael (2020): Europa muss den Aufbruch in die digitale Selbstbestimmung wagen. Auswärtiges Amt. <https://www.auswaertiges-amt.de/de/newsroom/roth-handelsblatt/2303882>.

Schlembach, Claudia (2020): Globale Handelsbeziehungen: Europa in der Offensive. In: Aktuelle Analysen 75, S. 4 – 9. Hanns Seidel Stiftung. https://www.hss.de/download/publications/AA_75_Handelsbeziehungen_01_neu.pdf.

Spiegel.de (2014): Das sind Snowdens wichtigste Enthüllungen. <https://www.spiegel.de/netzwelt/netzpolitik/snowden-enthuellungen-und-nsa-skandal-im-raster-der-geheimdienste-a-972830.html>.

Stiftung Neue Verantwortung (2020): Akteure und Zuständigkeiten in der deutschen Cybersicherheitspolitik. <https://www.stiftung-nv.de/de/publikation/akteure-und-zustaendigkeiten-der-deutschen-cybersicherheitspolitik>.

Tagesschau.de (2020): Kräftemessen mit Apple und Google. <https://www.tagesschau.de/inland/corona-app-spahn-103.html>.

Thapa, Basanta (2019): Strategische Beschaffung in der IT-Konsolidierung. Kompetenzzentrum Öffentliche IT. <https://www.oeffentliche-it.de/publikationen?doc=102761>.

Thapa, Basanta EP; Nicole Opiela; Jens Tiemann (2019): Internet Governance as an Arena of International Politics. In: Key Issues, Special Issue, S. 1 – 8.

Thiel, Thorsten (2019): Souveränität. Dynamisierung und Kontestation in der digitalen Konstellation. In: Hofmann, Jeanette et al. (Hg.): Politik der digitalen Gesellschaft. Zentrale Problemfelder und Forschungsperspektiven. S. 47 – 60.

Timmers, Paul (2019): Challenged by »Digital Sovereignty«. In: Journal of Internet Law, 23 (6), S. 1 – 20.

VDE ITG Informationstechnik (2020): Technologische Souveränität: Vorschlag einer Methodik und Handlungsempfehlungen. VDE Positionspapier.

Voss, Axel (2019): Ein Manifest für die digitale Souveränität und geopolitische Wettbewerbsfähigkeit Europas. EVP Fraktion, Europäisches Parlament.

Zeit Online (2019): Huawei – Konzern unter Verdacht. <https://www.zeit.de/2019/09/huawei-mobiles-internet-5g-china-spiionageverdacht-konzern>.

Zettl, Kerstin (2019): Lesson learned? Demokratische Resilienz gegenüber digitaler Wahlbeeinflussung in den USA und Deutschland. In: Zeitschrift für Außen- und Sicherheitspolitik 12, S. 429 – 451.

KONTAKT

Resa Mohabbat Kar
Kompetenzzentrum Öffentliche IT (ÖFIT)
Tel.: +49 30 3463-7173
Fax: +49 30 3463-99-7173
info@fokus.fraunhofer.de

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de
www.oeffentliche-it.de
Twitter: @OeffentlicheIT

ISBN: 978-3-948582-02-9

