

The world is how we shape it

sopra  steria



# Souveränität neu justieren

Strategische Handlungsfähigkeit  
für den digitalen Staat

# Was öffentliche Organisationen souverän macht

## Warum wir Souveränität neu justieren müssen

Der Staat wird an seiner Souveränität gemessen – gerade in Krisen. Doch in der aktuellen politischen Debatte wird Souveränität häufig auf Autarkie verkürzt. Der Fokus liegt auf technologischer Selbstversorgung und dem Schutz kritischer Infrastrukturen. Beides ist wichtig. Aber Souveränität erschöpft sich nicht im Rückzug auf das Eigene. Sie entsteht durch Kompetenz, Resilienz, die Fähigkeit zur Kooperation – und durch ein kluges Management von Schnittstellen, Datenflüssen und Entscheidungsprozessen.

Wer in einer vernetzten, digitalen Welt handlungsfähig bleiben will, muss Souveränität daher neu definieren: **als intelligentes Management von Abhängigkeiten, dessen Ziel es ist, die Handlungsfähigkeit zu sichern und die selbständige Gestaltungsmacht zu erhalten.**

Dieses Positionspapier bietet einen Denkraum für die Neujustierung des Souveränitätsbegriffs. Denn Souveränität ist keine abstrakte Vision. Sie entscheidet darüber, ob die öffentliche Verwaltung auch morgen noch handlungsfähig bleibt – und ihre Verantwortung im digitalen Staat erfüllen kann.



# Was Souveränität heute ausmacht – fünf Dimensionen

Souveränität entsteht nicht aus einem einzelnen Merkmal. Sie ist das Ergebnis eines Zusammenspiels unterschiedlicher Fähigkeiten, die öffentliche Organisationen strategisch entwickeln müssen. Fünf Dimensionen bilden das Fundament für ein modernes Verständnis von staatlicher Handlungsfähigkeit:

# 1.

## Fähigkeits-Souveränität

Sie beschreibt die individuelle und institutionelle Fähigkeit, mit Unsicherheit, Wandel und Komplexität umzugehen. Dazu zählen Kompetenzen wie Problemlösungsfähigkeit, Innovationskraft, Anpassungsfähigkeit und vorausschauendes Denken.

# 2.

## Wissens-Souveränität

Sie umfasst den freien Zugang zu relevantem Wissen sowie die Fähigkeit, Wissen eigenständig zu generieren, kritisch zu hinterfragen und verantwortungsvoll zu nutzen. So entsteht die Grundlage für fundierte Entscheidungen in Staat und Gesellschaft.

# 3.

## Technologische Souveränität

Damit ist die Fähigkeit gemeint, zentrale Schlüsseltechnologien unabhängig zu entwickeln, zu betreiben und strategisch weiterzuentwickeln – mit dem Ziel, technologische Abhängigkeiten, insbesondere von nicht-europäischen Anbietern, gezielt zu reduzieren.

# 4.

## Digitale Souveränität

Sie umfasst die Kontrolle über Daten, die Gestaltung wirksamer digitaler Schnittstellen und Standards sowie die Fähigkeit, regulatorische Rahmenbedingungen selbstbestimmt zu definieren und umzusetzen.

# 5.

## Betriebs-Souveränität

Sie beschreibt die Fähigkeit, kritische Prozesse, operative Abläufe und Systeme auch unter Störbedingungen oder in Krisensituationen stabil, transparent und steuerbar zu halten. Ziel ist es, handlungsfähig zu bleiben und Resilienz zu sichern.

Diese Dimensionen beschreiben den Zielraum moderner Souveränität. Die folgenden sechs Designprinzipien zeigen, wie sich dieser Zielraum konkret in Organisationen verankern lässt.

# Wie Souveränität gelingt – sechs Designprinzipien

Ein moderner Souveränitätsbegriff bleibt nicht abstrakt. Er wird wirksam, wenn er sich auf Strukturen, Prozesse und Entscheidungen in der öffentlichen Verwaltung übertragen lässt. Es geht darum, die richtigen Bedingungen zu schaffen – strategisch, technologisch, organisatorisch.

So kann Souveränität im Verwaltungsalltag verankert werden:

## Entscheidungsfähigkeit sichern

In einer Welt permanenter Unsicherheit ist Souveränität untrennbar mit der Fähigkeit verbunden, schnell und wirksam zu entscheiden – auch unter Zeitdruck und bei unvollständiger Informationslage. Voraussetzung sind adaptive Entscheidungsprozesse, klare Verantwortlichkeiten und eine Governance, die operative wie strategische Handlungsfähigkeit stärkt.

## Resilienz systematisch aufbauen

Souveränität setzt Sicherheit und Krisenfestigkeit voraus. Resiliente Systeme erkennen Schocks frühzeitig, reagieren flexibel und passen sich an veränderte Bedingungen an. Der Schutz kritischer Infrastrukturen – physisch wie digital – ist dabei von zentraler Bedeutung. Einheitliche Standards, belastbare Notfall- und Wiederanlaufpläne sowie eine starke Cybersicherheitsarchitektur sichern die Funktionsfähigkeit auch in Ausnahmesituationen.

## Regulatorische Steuerung bewusst nutzen

Souveränität bedeutet auch, dass Staaten und Organisationen externe Technologien strategisch integrieren – und gleichzeitig eigene Steuerungsmechanismen etablieren. Dazu braucht es regulatorische Gestaltungsmacht, rechtliche Absicherung und die Fähigkeit, den Einfluss internationaler Plattformanbieter zu begrenzen.

## Interoperabel denken, Abhängigkeiten managen

Technologische Offenheit schafft Anpassungsfähigkeit. Standardisierte Schnittstellen, modulare Architekturen und die Kombination unterschiedlicher Anbieter ermöglichen Flexibilität – und verringern Lock-in-Effekte. Ein aktives Abhängigkeitsmanagement durch Risikoanalysen, Redundanzen, Substitutionen und Partnerschaften ist Voraussetzung für strategische Handlungsfähigkeit.

## Kompetenzen gezielt aufbauen

Souveränität entsteht dort, wo Schlüsselkompetenzen vorhanden sind – und dauerhaft gehalten werden. Entscheidend ist eine strategische Make-or-buy-or-cooperate-Abwägung: Interne Entwicklung kritischer Kompetenzen, gezielter externer Zukauf und starke Partnerschaften müssen sich ergänzen. Bildung, internes Lernen und Wissensmanagement sichern langfristige Anpassungsfähigkeit.

## Innovation strategisch verankern

Innovationsführerschaft ist ein Hebel souveräner Steuerung. Wer innovieren kann, bleibt auch in dynamischen Umfeldern handlungsfähig. Ein souveränes Innovationssystem kombiniert nationale Strategien mit europäischen Förderinstrumenten, investiert in F&E, Transferstrukturen und Start-up-Ökosysteme – und stärkt so technologische Unabhängigkeit auf Dauer.

Diese sechs Designprinzipien bilden das Fundament für mehr Handlungsfähigkeit in Staat und Verwaltung. Entscheidend ist, sie nicht nur zu benennen, sondern in konkreten Bereichen umzusetzen. Wie das gelingen kann, zeigen die folgenden Praxisbeispiele – von der Beschaffung über das Risikomanagement bis zur Organisationsentwicklung.

# Vom Prinzip zur Praxis – wo Souveränität konkret beginnt

Souveränität lässt sich gestalten – aber nur, wenn der Schritt vom Anspruch zur Umsetzung gelingt. Dafür braucht es Klarheit über das Was und das Wie: Was sind die zentralen Herausforderungen – und wie lassen sie sich strategisch bewältigen?

Genau diesen Weg haben wir exemplarisch für fünf zentrale Handlungsfelder aufgezeigt: Beschaffung, Risikomanagement, Organisationsentwicklung, Cybersicherheit sowie Innovations- und Technologietransfer. Die folgenden Anwendungsbeispiele zeigen, wie sich ein moderner Souveränitätsbegriff konkret verankern lässt – nicht abstrakt, sondern im operativen Alltag öffentlicher Organisationen.

## Strategische Beschaffung – Wirtschaftlichkeit neu bewerten

Die öffentliche Beschaffung steuert mit Milliardenbudgets Märkte, Technologieentwicklung und strategische Abhängigkeiten. Sie entscheidet darüber, ob Schlüsseltechnologien und kritische Infrastruktur aus Europa oder aus Drittstaaten stammen. Ein zentrales Steuerungsinstrument der öffentlichen Beschaffung ist die **Wirtschaftlichkeitsbetrachtung (WiBe)** nach § 7 der Bundeshaushaltsordnung (BHO). In ihrer aktuellen Form sieht sie den Fokus auf **Wirtschaftlichkeit und Sparsamkeit**. Dabei werden primär kurzfristige Kosten bewertet. Strategische Autonomie, Cybersicherheit oder geopolitische Abhängigkeiten besitzen dabei keine Dominanz. Internationale Techgiganten können durch ihre Marktmacht günstigere Angebote unterbreiten als Wettbewerber, die sich in der Aufbauphase befinden. Dadurch schneiden EU-Anbieter in WiBe-Bewertungen schlechter ab – mit der Folge, dass strategisch wichtige Technologien unterfinanziert bleiben.

**Was das bedeutet:** Die WiBe muss weiterentwickelt werden – hin zu einem Instrument, das nicht nur Kosten vergleicht, sondern auch Risiken bewertet. Nur so können strategische Ziele wie digitale Souveränität und technologische Handlungsfreiheit systematisch einbezogen werden.

## Risikomanagement neu ausrichten – BCM souverän denken

Business Continuity Management (BCM) ist die Voraussetzung dafür, dass die Verwaltung in Krisensituationen steuerungs-fähig bleibt. Dies betrifft kritische Infrastrukturen, Cybersicherheit und die Handlungsfähigkeit in Krisenzeiten. BCM ist damit ein zentraler Bestandteil digitaler Souveränität, da es nicht nur betriebliche Kontinuität sichert, sondern auch strategische Handlungsfähigkeit und Resilienz gegenüber externen Abhängigkeiten gewährleistet. Die bestehenden Standards, insbesondere die **DIN EN ISO 22301 und der BSI-Standard 200-4**, fokussieren sich auf betriebliche und IT-sicherheits-bezogene Aspekte, berücksichtigen jedoch nicht explizit geopolitische Abhängigkeiten und die Notwendigkeit technologischer Souveränität.

**Was das bedeutet:** BCM sollte systematisch um eine souveränitätsorientierte Perspektive erweitert werden – mit Risikoanalysen zu geopolitischen Abhängigkeiten, resilienten IT-Architekturen und diversifizierten Bezugsquellen. So wird BCM zum strategischen Instrument für digitale Resilienz.



## Organisationsentwicklung weiterdenken – Souveränitätskritik ergänzen

Die klassische Aufgabenkritik analysiert, ob Aufgaben notwendig und effizient erfüllt werden. Im **Organisationshandbuch des Bundes** wird die **Aufgabenkritik** traditionell in zwei Dimensionen unterteilt: Die **Zweckkritik** hinterfragt, ob eine Aufgabe notwendig ist und weiterhin erfüllt werden sollte; die **Vollzugskritik** analysiert die Effizienz und Effektivität der Aufgabenerfüllung. Allerdings fehlt bislang eine systematische Bewertung, ob Aufgaben zur langfristigen **Souveränität, Resilienz und Wettbewerbsfähigkeit** der Verwaltung beitragen. In Anbetracht geopolitischer Unsicherheiten, technologischer Abhängigkeiten und wirtschaftlicher Disruptionen muss die Verwaltung nicht nur effizient, sondern auch resilient und wettbewerbsfähig sein.

**Was das bedeutet:** Das Organisationshandbuch sollte um eine „Souveränitätskritik“ ergänzt werden. Ziel ist, Verwaltungsstrukturen nicht nur auf Effizienz, sondern auch auf Resilienz, Innovationsfähigkeit und langfristige digitale Handlungsfähigkeit zu prüfen.

## Cyberproofing – Sicherheitsfolgen systematisch prüfen

Digitalisierung vernetzt kritische Infrastrukturen zunehmend. Von Stromnetzen bis zur Wasser- oder Gesundheitsversorgung – kritische Infrastrukturen sind heute so eng miteinander verflochten, dass ein Ausfall in einem Bereich ganze Systemketten gefährden kann. Umso wichtiger ist es, bereits im Gesetzgebungsprozess sicherzustellen, dass neue Regelungen bestehende Schutzmaßnahmen nicht untergraben oder widersprüchliche Anforderungen erzeugen.

**Was das bedeutet:** Cybersicherheits-Folgenabschätzungen sollten analog zu Artikel 35 DSGVO verpflichtend eingeführt werden. Sie verhindern regulatorische Widersprüche, stärken die sektorübergreifende Resilienz – und machen Cybersicherheit zu einem festen Bestandteil vorausschauender Gesetzgebung.

## Innovationsförderung neu ausrichten – gezielt Souveränität stärken

Innovation ist der Schlüssel zu technologischer Souveränität, wirtschaftlicher Resilienz und globaler Wettbewerbsfähigkeit. Doch das bestehende Fördersystem ist in seiner Wirkung begrenzt. Nationale Förderprogramme agieren häufig isoliert mit mangelnder Verzahnung untereinander und mit europäischen Initiativen wie Horizon Europe, dem European Innovation Council oder IPCEI.

**Was das bedeutet:** Eine zentrale Innovationsagentur mit klarem Mandat, agiler Struktur und europäischer Anbindung sollte vorangetrieben werden. Sie kann gezielt Schlüsseltechnologien wie KI, Quantentechnologie oder grüne Energie stärken. Mit Transferfokus, technologieoffener Förderung und straffer Governance bündelt sie Synergien, beschleunigt Innovationen – und wird so zum strategischen Hebel für mehr technologische Souveränität in Europa.

## Cloud-Transformation: Souveräne Technologieentscheidungen für eine handlungsfähige Verwaltung

Die Nutzung von Cloud-Diensten steht vor einem strategischen Wendepunkt. Neue Angebote sogenannter „sovereäner Hyperscaler“ auf Basis US-amerikanischer Technologien sowie das wachsende Ökosystem europäischer Cloud-Anbieter und Open-Source-Initiativen eröffnen neue Optionen – fordern jedoch eine realistische Auseinandersetzung mit geopolitischen Abhängigkeiten, technologischem Rückstand und erheblichen Kosten.

**Was das bedeutet:** Souveränität in der Cloud ist kein Selbstläufer: Sie verlangt bewusstes Abwägen, strategische Investitionen und mitunter funktionale Kompromisse. Eine resiliente, interoperable und anbieterunabhängige Multi-Cloud-Architektur bedeutet Investition. Europäische Lösungen erreichen derzeit (noch) nicht das Leistungsniveau großer US-Hyperscaler – bieten aber die Chance, langfristige Handlungsfähigkeit zu sichern. Eine souveräne Cloud-Strategie muss daher technologische Exzellenz mit rechtlicher Absicherung, operativer Resilienz und Innovationsfähigkeit verbinden. Digitale Souveränität kostet – aber sie ist der Preis für unabhängige Gestaltungsmacht im digitalen Staat.

# Fazit: Souveränität beginnt beim Handeln

Ein moderner Staat braucht mehr als Gesetze und Infrastruktur. Er braucht die Fähigkeit, unter veränderten Bedingungen zu entscheiden, zu steuern und handlungsfähig zu bleiben. Genau das macht Souveränität im 21. Jahrhundert aus.

Ob in der Beschaffung, in der IT-Sicherheit oder bei der Bewertung staatlicher Aufgaben – die öffentliche Verwaltung verfügt über die Hebel, um Resilienz, Innovationskraft und digitale Eigenständigkeit zu stärken. Aber sie nutzt sie noch zu selten strategisch.

Dieses Positionspapier zeigt: Souveränität ist nicht abstrakt – sie ist gestaltbar. Und sie beginnt dort, wo Prinzipien in Prozesse übersetzt werden, wo Strategien in Entscheidungen münden, wo Verwaltung nicht nur verwaltet, sondern Verantwortung für Zukunftsfähigkeit übernimmt.

Dabei geht es nicht um Abschottung, sondern um Steuerungsfähigkeit. Nicht um Ideologie, sondern um kluge Praxis. Und nicht allein um nationale Lösungen – sondern um europäische Handlungsfähigkeit im globalen Wettbewerb.

Jetzt ist der Moment, Souveränität als strategisches Querschnittsthema zu begreifen – und sie zur Richtschnur für konkrete Entscheidungen zu machen. Der Weg dorthin ist machbar. Und er beginnt genau dort, wo Verwaltung täglich Wirkung entfaltet.

*„Die Souveränität eines Staates konzentrierte sich früher auf robuste Einzelteile. In der digitalen Welt braucht es aber ein intelligentes Zusammenspiel. Dabei verstehen wir unter Souveränität mehr als nur technologische Selbstversorgung. Es geht um strategische Handlungsfähigkeit im globalen Wettbewerb, um das intelligente Management von Abhängigkeiten.“*

**Ron de Jonge**

**Head of Public Sector  
Sopra Steria**



# Key-Findings

Das Positionspapier zeigt, wie ein moderner, handlungsorientierter Souveränitätsbegriff in der öffentlichen Verwaltung konzipiert und umgesetzt werden kann. Die wichtigsten Erkenntnisse auf einen Blick:

## **1. Souveränität bedeutet Gestaltungsfähigkeit, nicht Autarkie.**

Ein moderner Staat steuert Abhängigkeiten strategisch, anstatt eine vollständige Abhängigkeit in jedem Bereich anzustreben.

## **2. Fünf Dimensionen machen souveränes Verwaltungshandeln aus.**

Fähigkeits-, Wissens-, technologische, digitale und Betriebs-Souveränität bilden den Rahmen für zukunftsfähiges Handeln.

## **3. Souveränität braucht strategische Prinzipien – nicht nur Technik.**

Entscheidungskraft, Resilienz, regulatorische Steuerung, Interoperabilität, Kompetenzaufbau und Innovationskraft sind von zentraler Bedeutung.

## **4. Die öffentliche Beschaffung ist ein zentraler Hebel – aber falsch justiert.**

Aktuelle WiBe-Methoden berücksichtigen bestehende Abhängigkeiten und Lock-In-Effekte nicht ausreichend.

## **5. Risikomanagement muss geopolitisch und technologisch denken lernen.**

BCM-Standards sollten um souveränitätsrelevante Aspekte erweitert werden.

## **6. Die klassische Aufgabenkritik greift zu kurz.**

Sie sollte um eine Bewertung staatlicher Aufgaben im Hinblick auf Resilienz und digitale Souveränität ergänzt werden.

## **7. Cybersicherheitsfolgen gehören in jede Gesetzesfolgenabschätzung.**

Analog zur Datenschutz-Folgenabschätzung sollte eine Cyber-Folgenabschätzung eingeführt werden.

## **8. Innovation braucht eine strategische Förderlogik.**

Eine zentrale Innovationsagentur mit Fokus auf europäischer Handlungsfähigkeit ist ein notwendiger Schritt.

## Autoren:

Yannick Thiele  
Dr. Josef Mauermair  
Ulf Glöckner

## Kontakt:

Sopra Steria SE  
Hans-Henny-Jahnn-Weg 29  
22085 Hamburg  
T. 040 22703-0  
E. [info.de@soprasteria.com](mailto:info.de@soprasteria.com)