Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Der Bundesrat

Bern, 26. November 2025

Digitale Souveränität der Schweiz

Bericht des Bundesrates in Erfüllung des Postulats 22.4411 Z'graggen, 14.12.2022

Inhaltsverzeichnis

1 Zusammenfassung 1

2 Das Postulat 1

3 Ausgangslage 2

4 Was heisst digitale Souveränität 3

4.1 Souveränität im Allgemeinen 3
4.2 Souveränität im digitalen Raum 4
4.3 Digitale Souveränität im internationalen Diskurs 5

5 Definition des Bundesrates und Zielbild 6

5.1 Definition 6
5.1.1 Betroffenheit einer staatlichen Aufgabe 7
5.1.2 Bezug zum digitalen Raum 8
5.1.3 Sicherstellung der erforderlichen Kontroll- und Handlungsfähigkeit 8

5.2 Verortung und Abgrenzung 9
5.2.1 Verortung der Definition im nationalen Diskurs 9
5.2.2 Thematische Abgrenzung der Definition 10

5.3 Zielbild 12

6 Stand der digitalen Souveränität der Schweiz 13

6.1 Bestehende Strukturen und laufende Massnahmen 13
6.1.1 Bestehende Strukturen 13
6.1.2 Laufende Massnahmen 14

6.2 Prüfung des Stands der digitalen Souveränität 17
6.2.1 Ziel 1: Bewusstsein für die Nutzung digitaler Ressourcen 17
6.2.2 Ziel 2: Bewusstsein für die Relevanz digitaler Ressourcen 18
6.2.3 Ziel 3: Bewusstsein über Kontroll- und Handlungsfähigkeit und Entscheidungen über gezielte Stärkung 18
6.2.4 Ziel 4: Implementierung gezielter Massnahmen 20

6.3 Handlungsbedarf 21

7 Strategie für die digitale Souveränität der Schweiz 22

7.1 Gesamtsicht und Koordination 23
7.2 Identifikation und Einschätzung von Risiken 23
7.3 Identifikation und Umsetzung von Massnahmen 23

Anhang Parlamentarische Vorstösse zur Thematik der digitalen Souveränität 25

1 Zusammenfassung

Digitale Souveränität wird sowohl in der Schweiz als auch international unterschiedlich verstanden. Im Vordergrund steht der Anspruch eines bestimmten Akteurs (z. B. Staat, Unternehmen oder Bürgerinnen und Bürger) auf Unabhängigkeit und Selbstbestimmtheit im digitalen Raum. Dabei werden teilweise weitreichende Forderungen an den Staat und seine Rolle in wirtschaftlichen und gesellschaftlichen Fragen formuliert. Der Bundesrat versteht die digitale Souveränität als die erforderliche Kontroll- und Handlungsfähigkeit des Staates im digitalen Raum, um die Erfüllung staatlicher Aufgaben sicherzustellen. Dabei stützt er sich auf die verfassungsmässigen Grundsätze der Subsidiarität, der Verhältnismässigkeit und der individuellen Verantwortung.

Im Bericht wird auf Grundlage dieser Definition geprüft, wie der Stand der digitalen Souveränität der Schweiz ist. Dabei ist entscheidend, ob die Akteure, die mit staatlichen Aufgaben betraut sind, über die erforderliche Kontroll- und Handlungsfähigkeit im digitalen Raum verfügen. Dies ist dann der Fall, wenn ein Bewusstsein über die eingesetzten digitalen Ressourcen, deren Relevanz für die Aufgabenerfüllung sowie den Grad der Abhängigkeit von diesen digitalen Ressourcen besteht. Die daraus resultierenden Risiken müssen regelmässig überprüft und Massnahmen zu ihrer Reduktion auf ein hinnehmbares Niveau ergriffen werden.

Die Analyse ergibt, dass der Bund über zahlreiche bestehende Strukturen und laufende Massnahmen verfügt, die zur Wahrung und Stärkung der digitalen Souveränität der Schweiz beitragen. Insbesondere die Übersicht über die genutzten digitalen Ressourcen und deren Relevanz ist durch das bestehende Risikomanagement des Bundes sowie das Informationssicherheitsrecht gegeben.

Allerdings ist die Einschätzung der Risiken deutlich komplexer geworden. Die zunehmende Bereitschaft von Staaten, den Zugang zu den von ihnen beherrschten digitalen Technologien als Druckmittel einzusetzen, stellt hochdigitalisierte Staaten wie die Schweiz vor Herausforderungen. Deshalb soll die im Bericht vorgenommene Gesamtsicht über bestehende Strukturen und Massnahmen weiter aktualisiert und eine verstärkte Abstimmung der einzelnen Massnahmen vorgenommen werden. Ebenso sollen aussen- und sicherheitspolitische Faktoren bei der Bereitstellung von digitalen Ressourcen stärker einbezogen werden.

Zu diesem Zweck wird die interdepartementale Arbeitsgruppe *Digitale Souveränität* (IDAG) eingesetzt (Massnahme 1). Sie soll die Gesamtsicht der laufenden Arbeiten der Bundesbehörden zur Stärkung der digitalen Souveränität weiterführen und die Arbeiten bei Bedarf koordinieren (Massnahme 2). Die IDAG soll ausserdem aussen- und sicherheitspolitische Risiken für digitale Ressourcen identifizieren und einschätzen (Massnahme 3). Schliesslich soll sie technische und (völker-)rechtliche Massnahmen zur Stärkung der Kontroll- und Handlungsfähigkeit der Schweiz ausarbeiten (Massnahme 4).

2 Das Postulat

Am 14. Dezember 2022 reichte Ständerätin Heidi Z'graggen das Postulat 22.4411 «Strategie digitale Souveränität der Schweiz» ein:

> Der Bundesrat wird beauftragt, Bericht zu erstatten, wie er «Digitale Souveränität» für die Schweiz definiert; wie er den Stand der digitalen Souveränität unseres Landes beurteilt; welche übergeordnete, umfassende Strategie zur Stärkung der staatspolitisch,

wirtschaftlich und gesellschaftlich als von höchster Bedeutung einzuordnende digitale Souveränität unseres Landes er zu ergreifen gedenkt.

Der Bericht definiert gestützt auf diese übergeordnete Strategie allenfalls gesetzgeberischen Handlungsbedarf, Prioritäten, einen Zeitplan für die Umsetzung der notwendigen Massnahmen und macht Aussagen zur Bereitstellung der notwendigen Mittel, um die dringendsten und erfolgversprechendsten Projekte zur Stärkung/Erreichung der digitalen Souveränität rasch umzusetzen.

Am 15. Februar 2023 beantragte der Bundesrat die Annahme des Postulats. Der Ständerat nahm das Postulat am 16. März 2023 an.

3 Ausgangslage

Der Begriff der «digitalen Souveränität» gewann im politischen Diskurs der Schweiz 2020 durch den Bericht zur Bedarfsabklärung für eine Swiss Cloud[1] an Bedeutung. Darin prüfte das damalige Informatiksteuerungsorgan des Bundes (heute: Bereich Digitale Transformation und IKT-Lenkung der Bundeskanzlei, BK-DTI) aufgrund der steigenden Nutzung von Cloud-Dienstleistungen, ob Bedarf an einer vom Bund kontrollierten oder unterstützten und Privaten offenstehenden Cloud-Infrastruktur besteht. Dies insbesondere für Infrastrukturen, die zwingend krisenresistent sein müssen.

Das Informatiksteuerungsorgan kam im Bericht zum Schluss, dass kein Bedarf für eine eigenständige öffentlich-rechtliche Cloud-Infrastruktur in der Schweiz besteht. Hingegen wurden verschiedene Fragen zum (völker-)rechtlichen Rahmen der Nutzung von Cloud-Dienstleistungen identifiziert, insbesondere in den Bereichen Datenzugriff sowie Daten-, Informations- und Geheimnisschutz. Das Eidgenössische Departement für auswärtige Angelegenheiten (EDA) wurde auf Grundlage dieser Bedarfsabklärung vom Bundesrat damit beauftragt, diese Fragen gemeinsam mit den anderen involvierten Bundesbehörden zu vertiefen.

Das Bundesamt für Justiz (BJ) hat 2021 und 2023 im Bereich des grenzüberschreitenden Zugriffs auf elektronische Beweismittel im Rahmen von Strafverfahren in zwei Berichten ausserdem den US CLOUD Act[2] sowie das e-Evidence-Paket der EU[3] untersucht. Bei beiden Regulierungen steht die Möglichkeit für Strafverfolgungsbehörden im Vordergrund, im Rahmen von Strafverfahren erleichterten Zugriff auf im Ausland gelagerte strafrechtlich relevante Daten zu erhalten. Zumal Strafverfolgung und -verfahren zu den hoheitlichen Aufgaben eines Staates gehören, berührt die Frage des zwischenstaatlichen Zugriffs auf Daten in gewissen Konstellationen die Souveränität.

---

[1] Bericht zur Bedarfsabklärung für eine «Swiss Cloud» des Informatiksteuerungsorgan des Bundes vom Dezember 2020, abrufbar unter: www.bk.admin.ch > Digitale Transformation und IKT-Lenkung > Bundesarchitektur > Cloud > Swiss Cloud (Stand 22.10.2025).

[2] Im März 2018 haben die USA den sogenannten **C**larifying **L**awful **O**verseas **U**se of **D**ata **Act** (CLOUD Act) verabschiedet. Ausführlich hierzu: Bericht zum US CLOUD Act des Bundesamts für Justiz vom 17. September 2021, abrufbar unter: www.bj.admin.ch > Publikationen & Service > Berichte, Gutachten und Verfügungen > Berichte und Gutachten > Bericht zum US CLOUD ACT (Stand 22.10.2025).

[3] Das e-Evidence-Paket der EU besteht aus einer Richtlinie, welche die wichtigsten Grundsätze der Vorlage festlegt, und aus einer Verordnung mit detaillierten Bestimmungen. Ausführlich hierzu: Bericht zur e-Evidence-Vorlage der EU des Bundesamts für Justiz vom 24. Oktober 2023, abrufbar unter: www.bj.admin.ch > Publikationen & Service > Berichte, Gutachten und Verfügungen > Berichte und Gutachten > Bericht zur e-Evidence-Vorlage der EU (Stand 22.10.2025).

Ferner wurden in der *Strategie Digitalaussenpolitik 2021–24*[4] des Bundesrates bereits für die digitale Souveränität der Schweiz relevante Aspekte, wie geopolitische Spannungen, der Technologiewettlauf oder die steigende Rechtsunsicherheit thematisiert. Die digitale Souveränität bildete 2022 einen der drei Schwerpunkte der *Beiratstreffen Digitale Schweiz*[5]. Seit 2023 ist die digitale Souveränität ein Fokusthema der *Strategie Digitale Schweiz*[6] des Bundesrates. Die Förderung der digitalen Souveränität ist ausserdem Teil der Aussenpolitischen Strategie 2024–27[7] des Bundesrates. Gemäss dieser fördert die Schweiz die digitale Souveränität, indem sie sich dafür einsetzt, dass Daten von Staaten und internationalen Organisationen auch dann Unverletzlichkeit geniessen, wenn sie in Clouds in anderen Staaten gespeichert sind. Schliesslich ist die digitale Souveränität einer von sieben Schwerpunkten der im Dezember 2023 verabschiedeten *Strategie Digitale Bundesverwaltung*[8].

Der Begriff der digitalen Souveränität ist auf strategischer Ebene bereits verankert. Im vorliegenden Bericht definiert der Bundesrat den Begriff genauer, macht eine Bestandesaufnahme der bestehenden Strukturen und laufenden Massnahmen und schlägt zusätzliche Massnahmen vor, um die digitale Souveränität der Schweiz weiter zu stärken.

4 Was heisst digitale Souveränität

4.1 Souveränität im Allgemeinen

Souveränität ist kein statischer Begriff. Er wurde im Laufe der Zeit mit unterschiedlichen Inhalten und Schwerpunkten gefüllt – abhängig von den vorherrschenden politischen und rechtlichen Rahmenbedingungen.[9] Das moderne Staats- und Völkerrecht versteht unter Souveränität die höchste Staatsgewalt. Diese drückt sich gegen innen in der Selbstbestimmtheit bei der Rechtsetzung, der Verwaltungsausübung und der Justiz aus. Gegen aussen manifestiert sie sich im Anspruch auf Unabhängigkeit und Gleichbehandlung[10] gegenüber anderen Staaten beziehungsweise in der Verantwortung und Freiheit, das Wohlergehen des eigenen Staates zu gestalten.[11] Um diese Ansprüche erfüllen zu können, muss der Staat kontroll- und handlungsfähig sein.

---

[4] Strategie Digitalaussenpolitik 2021–2024 des Bundesrats vom 4. November 2020, erhältlich unter: www.eda.admin.ch > EDA > Publikationen > Strategie Digitalaussenpolitik (Stand: 22.10.2025).

[5] Medienmitteilung des Bundesrates vom 2. Februar 2022, Bundesrat legt aktuelle Schwerpunkte für die Digitalisierung fest, abrufbar unter: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-87029.html (Stand: 22.10.2025).

[6] Monitoringbericht zur Strategie Digitale Schweiz 2023, veröffentlicht am 8. Dezember 2023, abrufbar unter: www.bk.admin.ch > Digitale Transformation und IKT-Lenkung > Digitale Schweiz > Monitoringbericht zur Strategie Digitale Schweiz 2023 (Stand: 22.10.2025).

[7] Aussenpolitische Strategie 2024–2027, veröffentlicht am 31. Januar 2024, abrufbar unter: www.eda.admin.ch > EDA > Publikationen > Aussenpolitische Strategie 2024–2027 (Stand: 22.10.2025).

[8] Strategie Digitale Bundesverwaltung, veröffentlicht am 12. Dezember 2023, abrufbar unter: www.bk.admin.ch > Digitale Transformation und IKT-Lenkung > Digitale Bundesverwaltung > Strategie Digitale Bundesverwaltung (Stand: 22.10.2025).

[9] FRANZ PERREZ, Cooperative Sovereignty, S. 2.

[10] THOMAS MAISSEN; ANDREAS KLEY: «Souveränität», in: Historisches Lexikon der Schweiz (HLS), Version vom 08.01.2013; abrufbar unter: www.hls-dhs-dss.ch > Themen > Souveränität (Stand: 22.10.2025).

[11] FRANZ PERREZ, Cooperative Sovereignty, S. 335.

4.2 Souveränität im digitalen Raum

Das Prinzip der Souveränität gilt auch im digitalen Raum – dies wurde im Rahmen der Vereinten Nationen bereits mehrfach von der Staatengemeinschaft anerkannt.[12] Auch die Schweiz hat diese Auffassung in ihrem Positionspapier von 2021 zur Anwendung des Völkerrechts im Cyberraum bekräftigt.[13] Sie hält darin auch fest, dass die Konkretisierung des völkerrechtlichen Prinzips der Souveränität im digitalen Raum eine Herausforderung darstellt.

Zur Ausübung der äusseren Souveränität – das heisst der Abgrenzung von Herrschafts- bzw. Kompetenzansprüchen mehrerer Staaten – kommt dem Territorialitätsprinzip in der analogen Welt eine zentrale Bedeutung zu: Spielt sich ein Vorgang auf dem Territorium eines Staates ab, so ist dieser grundsätzlich in seiner Souveränität betroffen. Im digitalen Raum verliert das Territorialitätsprinzip jedoch an Trennschärfe. So ist einerseits oftmals nicht auf den ersten Blick ersichtlich, auf wessen Territorium sich ein digitaler Vorgang abspielt. Andererseits kann ein digitaler Vorgang elementare Interessen eines Staates betreffen, ohne sich auf dessen Territorium abzuspielen.

Beispiel 1 – Abgrenzung Souveränitätsansprüche (äussere Souveränität)
Sensible Daten des Staates A sind auf Servern des Staates B gespeichert und werden dort von Hackern gelöscht. Gemäss Territorialitätsprinzip wäre lediglich Staat B in seiner Souveränität betroffen, obwohl es um sensible Daten von Staat A geht.

Das Beispiel führt vor Augen, dass zur Abgrenzung beziehungsweise Identifizierung von staatlichen Souveränitätsansprüchen im digitalen Raum zusätzliche Kriterien herangezogen werden müssen. Über diese herrscht in der Staatengemeinschaft bisher jedoch noch kein Konsens.

Doch auch die innere Souveränität des Staates – das heisst das Primat des Staates als höchste rechtliche Autorität und ordnungsgebende Macht – gerät im digitalen Raum unter Druck. Im Unterschied zum analogen Raum, in dem der Staat grosse Teile der Infrastruktur (z. B. Verkehr, Postwesen, Land) zur Verfügung stellt und damit auch kontrolliert, wird digitale Infrastruktur vorwiegend durch private Akteure bereitgestellt. Dies hat zur Folge, dass mehr Gestaltungsmacht bei privaten Akteuren liegt, die mit ihren Entscheidungen grossen Einfluss auf Staat und Gesellschaft haben können. Ausserdem muss der Staat regelmässig auf private Akteure zurückgreifen, um seinen Handlungen im digitalen Raum Wirkung zu verleihen.

Beispiel 2 – Staat versus private Akteure (innere Souveränität)
Wollen Strafverfolgungsbehörden eine Website schliessen, die illegale Dienstleistungen in der Schweiz anbietet, sind sie auf die Mitarbeit des entsprechenden Hostinganbieters angewiesen, der oftmals im Ausland domiziliert ist.

Wie Staat und Gesellschaft mit dieser Verschiebung der Gestaltungsmacht weg vom Staat und hin zu privaten Akteuren umgehen wollen, ist nicht abschliessend geklärt.

Die staatliche Souveränität im digitalen Raum wird durch die genannten Besonderheiten herausgefordert. Damit geht eine erhebliche Unsicherheit, nicht zuletzt auch eine Rechtsunsicherheit, einher. Entsprechend stellt sich die Frage, ob der Staat im digitalen Raum hinreichend

---

[12] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, para 20, abrufbar unter: www.docs.un.org/en/A/68/98 (Stand: 22.10.2025); Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, paras. 27 and 28 b, abrufbar unter: www.docs.un.org/en/a/70/174 (Stand: 22.10.2025).

[13] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, UN General Assembly, A/76/136, Switzerland, S. 85–105, abrufbar unter: https://digitallibrary.un.org/record/3933543?ln=en&v=pdf (Stand: 22.10.2025).

kontroll- und handlungsfähig ist, um die Unabhängigkeit von anderen Staaten und die Selbstbestimmtheit seiner inneren Ordnung zu garantieren. Der stetig wachsende Diskurs um die digitale Souveränität ist nicht zuletzt eine Reaktion auf diese Unsicherheit.

Souveränität im digitalen Raum ist somit zwar mit dem Begriff der Souveränität verbunden, weist aber wichtige Eigenheiten auf.

4.3 Digitale Souveränität im internationalen Diskurs

Die Verwendung des Begriffs *Digitale Souveränität* ist im internationalen Diskurs nicht einheitlich. Den verschiedenen Definitionsvorschlägen ist gemein, dass sie mit der Verwendung des Begriffs den Anspruch eines Akteurs auf Unabhängigkeit und Selbstbestimmtheit im digitalen Raum meinen. Im Unterschied zur Souveränität im klassischen Sinne wird dieser Anspruch aber nicht nur von Staaten, sondern auch von Akteuren aus Wirtschaft und Zivilgesellschaft erhoben.

China hat das Konzept der digitalen Souveränität – wobei China von «Cybersouveränität» spricht – als einer der ersten Staaten zu einer politischen Priorität erklärt. China empfand den rasanten Aufstieg des offenen Internets, und dadurch die potenzielle Einflussnahme einer kaum zu kontrollierenden Anzahl von Akteuren, als Bedrohung für sein Staatssystem. Als Reaktion darauf entwickelte China ein kontrollorientiertes Verständnis von Souveränität, bei dem der Staat die höchste Autorität im digitalen Raum[14] innehat. Nach chinesischer Leseart soll jeder Staat das Recht haben, national abgrenzbare Bereiche im digitalen Raum zu errichten und zu kontrollieren.[15] Damit rechtfertigt China, dass die nationale Kommunikationsinfrastruktur einer strengen Kontrolle unterstellt worden ist. China geht damit von einem sehr hohen Kontrollanspruch aus, der nicht nur die staatliche, sondern auch die höchstpersönliche Ebene der Bürgerinnen und Bürger betrifft. Auch **Russland** und der **Iran** sind dem chinesischen Beispiel gefolgt.

Weniger stark auf inhaltliche Aspekte, dafür auf das Territorium ausgerichtet ist der Ansatz **Indiens**, das mögliche Abhängigkeiten vom Ausland unter anderem mit einem gesetzlichen Erfordernis der lokalen Datenverarbeitung verhindern will.[16]

In einem Gegensatz dazu steht der **Ansatz der liberalen Staaten des Westens**, die den Aufstieg des freien Internets zunächst nicht als Bedrohung für ihr Staatssystem, sondern als Möglichkeit zur Stärkung der Demokratie und der individuellen Selbstverwirklichung sahen. Diese Vorstellung des digitalen Raums wurde in den letzten Jahren jedoch relativiert. Die zunehmende Anzahl von Cyberangriffen, der Aufstieg multinationaler, datengetriebener Grosskonzerne und die Enthüllungen über die Überwachung des Internetverkehrs durch Geheimdienste wie beispielsweise jene von Edward Snowden führten vor Augen, dass der digitale Raum auch als Mittel zur Machtausübung eingesetzt wird. Als Konsequenz dieser Entwicklungen mehrten

---

[14] Unter dem Begriff «digitaler Raum» wird in diesem Bericht, in Anlehnung an die Nationale Cyberstrategie, die Gesamtheit der Informations- und Kommunikationsinfrastrukturen (Hard- und Software), die untereinander Daten austauschen, diese erfassen, speichern, verarbeiten oder in (physische) Aktionen umwandeln, und der dadurch ermöglichten Interaktionen zwischen Personen, Organisationen und Staaten, verstanden.

[15] ROGIER CREEMERS, China's Approach to Cyber Sovereignty, 2020, S. 6, abrufbar unter: https://www.kas.de/documents/252038/7995358/China%E2%80%99s+Approach+to+Cyber+Sovereignty.pdf/2c6916a6-164c-fb0c-4e29-f933f472ac3f?version=1.0&t=1606146961537 (Stand: 22.10.2025).

[16] MATTHIAS STÜRMER, Technologische Perspektive der digitalen Souveränität: Blick auf die Schweiz, internationale Trends sowie Empfehlungen für die «Strategie Digitale Souveränität der Schweiz», 2024, S. 16 f., abrufbar unter: https://www.bfh.ch/dam/jcr:77087ce2-5802-4c76-9ea7-21f8fe01fa87/Studie_Technologische%20Perspektive%20der%20digitalen%20Souveraenitaet%2012%20Juni%202024_Matthias%20St%C3%BCrmer.pdf (Stand: 22.10.2025).

sich die Stimmen, welche im Namen der digitalen Souveränität mehr Unabhängigkeit und Selbstbestimmtheit im digitalen Raum einforderten.

Vor dem Hintergrund steigender geopolitischer Spannungen ist der Blick auf die **USA** und ihre politischen Massnahmen, welche die digitale Souveränität der USA betreffen (jedoch ohne eine klare eigene Definition derselben auszuweisen), von besonderer Relevanz. Trotz einem traditionell liberalen wirtschaftspolitischen Ansatz greift die US-Regierung in jüngster Zeit mit bedeutenden industriepolitischen und tarifären Massnahmen sowie unilateralen Exportbeschränkungen in den internationalen Markt und die Weltpolitik ein. Sie tut dies insbesondere mit Blick auf die Entwicklung von IT-Technologien und die Herstellung von dafür relevanten Produkten. Auch die Gesetzgebung mit extraterritorialen Auswirkungen, insbesondere mit Blick auf den Zugriff auf Daten, nimmt zu.

Die **EU** nutzt den Begriff der digitalen Souveränität in verschiedenen Kontexten, präsentiert dabei aber ebenfalls keine eigene Definition. Sie orientiert sich am Konzept der strategischen Souveränität und setzt dabei mit dem wohl bekanntesten Projekt «GAIA-X» auf Interoperabilität, Standardisierung und den Aufbau von Datenräumen. Einen besonderen Fokus legt die EU auf den Schutz der Privatsphäre. Zudem existieren in der EU verschiedene private Initiativen, wie beispielsweise die EuroStack-Initiative[17], die im Namen der digitalen Souveränität ein stärkeres industriepolitisches Eingreifen verlangt.

Innerhalb der EU ist schliesslich **Deutschland** hervorzuheben. So hat Deutschland 2021 eine Strategie verabschiedet und 2022 ein Zentrum für digitale Souveränität eröffnet. In der deutschen Strategie wird digitale Souveränität als «die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können» definiert.[18]

5 Definition des Bundesrates und Zielbild

5.1 Definition

Der Bundesrat ist der Ansicht, dass sich die Definition der digitalen Souveränität der Schweiz an bewährten verfassungsmässigen Grundsätzen der Schweizer Staatsordnung orientieren soll. Dazu gehören der Schutz der Freiheit und der Rechte des Volkes sowie der Unabhängigkeit und Sicherheit des Landes (Art. 2 Abs. 1 BV). Hinzu kommen ausserdem das Legalitäts- und Verhältnismässigkeitsprinzip (Art. 5 Abs. 1 und 2 BV), das Subsidiaritätsprinzip (Art. 5a BV) und die individuelle Verantwortung jedes Einzelnen (Art. 6 BV) sowie die Grundsätze der Wirtschaftsordnung (Art. 94 BV). Ausgehend von diesen Grundsätzen verortet der Bundesrat die digitale Souveränität der Schweiz in erster Linie beim Staat und definiert sie wie folgt:

> «Digitale Souveränität bedeutet, als Staat über die erforderliche Kontroll- und Handlungsfähigkeit im digitalen Raum zu verfügen, um die Erfüllung staatlicher Aufgaben sicherzustellen.»

Diese enge Definition bringt es mit sich, dass die Kontroll- und Handlungsfähigkeit der Wirtschaft und Zivilgesellschaft im digitalen Raum nicht im Zentrum stehen. Wenngleich in diesen

[17] Mehr Informationen abrufbar unter: www.eurostack.eu > The White Paper (Stand: 22.10.2025).

[18] Bericht «Stärkung der digitalen Souveränität der öffentlichen Verwaltung, Eckpunkte – Ziel- und Handlungsfelder», Version 1.0.1. vom 31. März 2020, herausgegeben vom Beauftragten der Bundesregierung für Informationstechnik, abrufbar unter https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/eckpunktpapier-digitale-souveraenitaet.pdf?__blob=publicationFile&v=4 (Stand: 22.10.2025).

Bereichen ebenfalls Klärungsbedarf besteht, konzentriert sich der vorliegende Bericht auf die Kontroll- und Handlungsfähigkeit des Schweizer Staates.

Für die Anwendung der Definition ist somit zu klären, wann eine staatliche Aufgabe betroffen ist und ob ein Bezug zum digitalen Raum besteht. Sind beide Voraussetzungen gegeben, gilt es, die erforderliche Kontroll- und Handlungsfähigkeit des Staates sicherzustellen.

5.1.1 Betroffenheit einer staatlichen Aufgabe

Die staatlichen Aufgaben werden durch die Bundes- und Kantonsverfassungen sowie durch Gesetze festgelegt und in erster Linie Staatsorganen (Legislative, Exekutive und Judikative) zugewiesen. Teilweise werden sie auch anderen Personen des öffentlichen oder privaten Rechts übertragen (vgl. Art. 178 Abs. 3 BV). Sie dienen der Erfüllung der in den Verfassungen definierten Staatszwecke.

Der Bestand staatlicher Aufgaben unterliegt aufgrund Verfassungs- und Gesetzesänderungen einem stetigen Wandel. Durch die Anknüpfung des Begriffs der digitalen Souveränität an jenen der staatlichen Aufgabe ist sichergestellt, dass sich auch der Begriff der digitalen Souveränität veränderten Umständen und Erwartungen anpasst.

Staatsorgane
Primär erfüllen die Staatsorgane – Legislative, Exekutive und Judikative auf Bundes- und Kantonsebene – die staatlichen Aufgaben gestützt auf Verfassung, Gesetz und Verordnung. Ihre Tätigkeit ist zunehmend von digitalen Ressourcen abhängig, mittel- oder unmittelbar. Die Überwachung des Luftraums ist beispielsweise ohne digitale Infrastruktur nicht möglich (unmittelbare Abhängigkeit), während etwa die digitale Erfassung von Arbeitszeiten nur mittelbar mit der Aufgabenerfüllung verbunden ist (mittelbare Abhängigkeit). Insgesamt wäre die Arbeit der Staatsorgane – und damit die Erfüllung staatlicher Aufgaben – ohne digitale Ressourcen heute kaum vorstellbar.

Unternehmen
Unternehmen können auf verschiedene Arten an der Erfüllung staatlicher Aufgaben beteiligt sein:

1. Formelle Privatisierung (Organisationsprivatisierung[19]): Eine staatliche Einrichtung wird in ein privatrechtliches Unternehmen umgewandelt, bleibt aber mehrheitlich im Eigentum des Staates. Der Staat handelt dabei selbst in privatrechtlicher Form.
2. Erfüllungsprivatisierung[20]: Der Staat überträgt die Aufgabe an Private, behält aber die Verantwortung und greift nur bei Schlechterfüllung ein.
3. Mittelbare Beteiligung: Private Unternehmen stellen dem Staat Mittel zur Verfügung, etwa als Betreiber kritischer Infrastrukturen, Lieferanten oder IT-Dienstleister auf vertraglicher Basis.

Auch in Unternehmen hat die Digitalisierung Prozesse grundlegend verändert. Tätigkeiten ohne digitale Ressourcen sind ebenso wenig vorstellbar wie für den Staat. Somit sind auch die von Unternehmen erfüllten staatlichen Aufgaben von digitalen Ressourcen abhängig.

Bürgerinnen und Bürger
Die Bürgerinnen und Bürger der Schweiz sind in ihrer privaten Funktion nicht direkt an der Erfüllung staatlicher Aufgaben beteiligt. Dennoch ist es wichtig, dass die Bürgerinnen und Bürger selbstbestimmt und unabhängig im digitalen Raum handeln können. Dies ist in der Schweiz

[19] DOMINIK ELSER, Die privatisierte Erfüllung staatlicher Aufgaben, S. 28 f.

[20] DOMINIK ELSER, Die privatisierte Erfüllung staatlicher Aufgaben, S. 22.

im Konzept der digitalen Selbstbestimmung verankert, zu deren Stärkung bereits Massnahmen bestehen (vgl. Ziff. 5.2.2 und 6.1.2).

Zudem sind Bürgerinnen und Bürger der Schweiz mögliche Fachkräfte für Staatsorgane und Unternehmen. Je mehr Fachwissen in der Bevölkerung vorhanden ist, desto mehr digitale Ressourcen kann ein Staat potenziell selbst und ohne Rückgriff auf Dritte bereitstellen (vgl. Ziff. 6.1.2).

5.1.2 Bezug zum digitalen Raum

Ein Bezug zum digitalen Raum liegt vor, wenn die Erfüllung einer staatlichen Aufgabe von der Verwendung einer digitalen Ressource abhängt.

Als **digitale Ressourcen** im Sinne dieses Berichts zählen:

- *Informations- und Kommunikationstechnologien Infrastruktur (IKT-Infrastruktur)*: Jegliche Mittel, die zur digitalen Kommunikation und zur digitalen Verarbeitung von Informationen notwendig sind. Dazu gehören sowohl Hard- als auch Software wie beispielsweise Rechenzentren, Speicherkapazitäten, Komponenten zur Datenübertragung und Anwendungen.
- *Digitale Daten- und Informationssammlungen*: Dazu gehören unter anderem Datenbanken, digitale Archive und das digitale Wissensmanagement.

5.1.3 Sicherstellung der erforderlichen Kontroll- und Handlungsfähigkeit

Falls eine staatliche Aufgabe betroffen ist und deren Erfüllung massgeblich von einer digitalen Ressource abhängt, so muss der Staat die erforderliche Kontroll- und Handlungsfähigkeit in Bezug auf die entsprechende digitale Ressource sicherstellen können. Folgende zwei Fragen müssen beantwortet werden: (1) Welcher Grad an Kontroll- und Handlungsfähigkeit soll erreicht werden? (2) Welche Massnahmen müssen ergriffen werden, um diesen Grad der Kontroll- und Handlungsfähigkeit sicherzustellen?

(1) Welcher Grad an Kontroll- und Handlungsfähigkeit erreicht werden soll – ob nur eine autarke Lösung akzeptabel ist oder auch ein gewisser Grad an Abhängigkeit von Dritten in Kauf genommen werden kann – ist eine politische und strategische Entscheidung. Der Grad an (Un-)Abhängigkeit – und im Umkehrschluss der Kontroll- und Handlungsfähigkeit – unterscheidet sich nach der digitalen Ressource.

Grundlage für die Entscheidung über den angestrebten Grad der (Un-)Abhängigkeit bilden insbesondere folgende Aspekte:

- Bedeutung der staatlichen Aufgabe (wie wichtig ist die Erfüllung der staatlichen Aufgabe für das Gemeinwesen?)
- Bedeutung der digitalen Ressource (wie stark hängt die erfolgreiche Erfüllung der staatlichen Aufgabe von der digitalen Ressource ab?)
- Praktikabilität (in welchem Verhältnis stehen Kosten und Nutzen zueinander?)

(2) Wie ein bestimmter Grad an Kontroll- und Handlungsfähigkeit in Bezug auf eine digitale Ressource sichergestellt werden kann, hängt von der digitalen Ressource ab:

- Die Kontroll- und Handlungsfähigkeit in Bezug auf IKT-Infrastruktur hängt insbesondere vom Standort, der Betreiberin, der verwendeten Software und den ergriffenen Sicherheitsvorkehrungen ab. Autarkie in Bezug auf IKT-Infrastruktur ist nur dann erreicht,

wenn der Staat die Infrastruktur (Hard- und Software) durch eigenes Personal in der Schweiz bauen und betreiben lässt. Vollständige Abhängigkeit in Bezug auf IKT-Infrastruktur besteht hingegen dann, wenn der Staat die Infrastruktur durch einen Dritten im Ausland unter Verwendung fremder Hard- und Software betreiben lässt, die Einhaltung der vereinbarten Sicherheitsvorkehrungen nicht kontrollieren kann und auch keine Möglichkeit besteht, bei Bedarf den Leistungserbringer zu wechseln.

- Die Kontroll- und Handlungsfähigkeit in Bezug auf Daten- und Informationssammlungen hängt massgeblich von den drei Grundprinzipien der Informationssicherheit ab: Verfügbarkeit, Integrität und Vertraulichkeit. Autarkie in Bezug auf Daten ist dann erreicht, wenn der Staat über alle drei Parameter volle Kontrolle hat, weil er die Daten auf einer eigenen Infrastruktur verwaltet und sowohl die Hard- wie auch die Software durch eigenes Personal gewartet wird. In vollständiger Abhängigkeit befindet sich der Staat, wenn die Verfügbarkeit, Integrität und Vertraulichkeit von einem Dritten verantwortet werden, ohne dass der Staat den Dritten kontrollieren und bei Bedarf wechseln kann.

Um den jeweils erforderlichen Grad an Kontroll- und Handlungsfähigkeit in Bezug auf eine digitale Ressource sicherzustellen, kommen technische, organisatorische und rechtliche Massnahmen in Frage.

5.2 Verortung und Abgrenzung

Der Begriff der digitalen Souveränität wird nicht nur international diskutiert. Auch in der Schweiz wird der Begriff immer öfter verwendet. Es bietet sich deshalb an, die vorgeschlagene Definition im nationalen Diskurs zu verorten (Ziff. 5.2.1) und von anderen Begriffen der digitalpolitischen Landschaft der Schweiz abzugrenzen (Ziff. 5.2.2).

5.2.1 Verortung der Definition im nationalen Diskurs

In der Schweiz haben sich in den vergangenen Jahren bereits verschiedene Interessensverbände und akademische Institutionen mit dem Begriff der digitalen Souveränität auseinandergesetzt und Definitionen vorgeschlagen. Hier betrachtet werden die Definitionen von vier in diesem Bereich relevanten Akteuren: der *Swiss Data Alliance* (SDA), der *Conférence latine des directeurs du numérique* (cldn), der *Berner Fachhochschule* (BFH) sowie von *Innovate Switzerland* (Innovate).

Swiss Data Alliance	Conférence latine des directeurs du numérique (cldn)
«Digitale Souveränität ist die Fähigkeit eines Staates im digitalen Raum, seine Zuständigkeit international zu definieren (unter Berücksichtigung der anerkannten Souveränität anderer Staaten), seine inneren Angelegenheiten zu gestalten und beides zu verteidigen.»[21]	« La capacité des autorités à maintenir leur autonomie stratégique, soit à pouvoir utiliser et contrôler de manière autonome les biens matériels et immatériels et les services numériques qui impactent l'économie, la société et la démocratie. »[22]
Innovate Switzerland	Berner Fachhochschule

[21] «Digitale Souveränität: Grundlagen», Grundlagendokument der Swiss Data Alliance, 2024, S. 20, abrufbar unter: www.swiss-dataalliance.ch > Publikationen > Digitale Souveränität (Grundlagen & Whitepaper) > Grundlagen PDF (Stand: 22.10.2025).

[22] «Souveraineté numérique – Etude pluridisciplinare» de la Conférence latine des directeurs du numérique, 2023, S. 4, abrufbar unter: www.cldn.ch > Actualités > 11.05.2023 > Souveraineté numérique, Etude pluridisciplinaire (Stand: 22.10.2025).

«Digitale Souveränität beschreibt die Art und Weise, wie eine Nation freien Datenfluss ermöglicht und gleichzeitig bestmöglich schützt.»[23]	«Digitale Souveränität eines Staates oder einer Organisation umfasst zwingend die vollständige Kontrolle über gespeicherte und verarbeitete Daten sowie die unabhängige Entscheidung darüber, wer darauf zugreifen darf. Sie umfasst weiterhin die Fähigkeit, technologische Komponenten und Systeme eigenständig zu entwickeln, zu verändern, zu kontrollieren und durch andere Komponenten zu ergänzen.»[24]

Die vier Definitionen verorten die digitale Souveränität bei unterschiedlichen **Akteuren**. Die Definitionen der SDA, der cldn und der BFH richten den Anspruch an den Staat, der über bestimmte Fähigkeiten verfügen soll. Die Definitionen der BFH und von Innovate öffnen den Kreis für Akteure aus Wirtschaft und Zivilgesellschaft. Der vorliegende Bericht verortet die digitale Souveränität demgegenüber primär beim Staat. Die Ansicht, dass auch private Akteure souverän – oder in anderen Worten: selbstbestimmt – agieren können sollen, ist in der Schweiz im Konzept der digitalen Selbstbestimmung verankert, welche der Bund bereits fördert (vgl. Ziff. 5.2.2 und 6.1.2).

Auch wenn sich die Formulierungen in Details unterscheiden, so sind sich die vier Definitionen im Grundsatz einig, dass digitale Souveränität **Kontroll- und Handlungsfähigkeit** voraussetzt, um die jeweiligen Ziele zu erreichen. In dieser Hinsicht stimmen sie mit der Definition des Bundesrates überein.

In Bezug auf die **Zielvorstellungen** lassen sich Unterschiede ausmachen. Während Innovate den freien Datenfluss betont, Individualrechte anspricht und die politische Gestaltung miteinbezieht, fokussiert die cldn stärker auf die Handlungsfähigkeit der Behörden und deren strategische Autonomie. In eine ähnliche Richtung geht auch die Definition der SDA, die die Fähigkeit des Staates betont, sich eigenständig positionieren und sich gegenüber anderen Akteuren verteidigen zu können. Sie nennt dabei die internationale Abgrenzung zwischen einzelnen Staaten. Die BFH fordert dagegen explizit «*vollständige Kontrolle*» über Daten und die Fähigkeit, «*Komponenten und Systeme eigenständig zu entwickeln, zu verändern, zu kontrollieren und durch andere Komponenten zu ergänzen*». Den verschiedenen Zielvorstellungen liegen unterschiedliche Ansichten in Bezug auf die Rolle des Staates und die Ansprüche an ihn zugrunde. Die Definition des Bundesrates trägt dieser politischen Realität Rechnung, indem sie mit dem Begriff der «Erfüllung staatlicher Aufgaben» das Ziel der digitalen Souveränität entwicklungsfähig belässt, statt mit einer detaillierten Definition den Begriff einzuengen. Dies gilt insbesondere auch für den angestrebten Grad der erforderlichen Kontroll- und Handlungsfähigkeit.

5.2.2 Thematische Abgrenzung der Definition

Das Konzept der digitalen Souveränität ist verwandt mit anderen Bereichen und Begriffen der digitalpolitischen Landschaft. Im Folgenden wird die digitale Souveränität einerseits abgegrenzt und zum anderen werden thematische Bezüge aufgezeigt.

---

[23] «Swiss Digital Sovereignty», Positionspapier von Innovate Switzerland, 2023, S. 1, abrufbar unter: www.innovate-switzerland.ch > Publications > Swiss Digital Sovereignty (Stand: 22.10.2025).

[24] MATTHIAS STÜRMER, Technologische Perspektive der digitalen Souveränität: Blick auf die Schweiz, internationale Trends sowie Empfehlungen für die «Strategie Digitale Souveränität der Schweiz», 2024, S. 6.

Digitale Selbstbestimmung und digitale Souveränität
Im Gegensatz zur digitalen Souveränität, die definitionsgemäss beim Staat und der Erfüllung staatlicher Aufgaben verortet ist, bezweckt die digitale Selbstbestimmung die Befähigung von Individuen, Unternehmen und der Gesellschaft als Ganzes, das eigene Handeln im digitalen Raum selbst festzulegen. Das Konzept ist eng mit dem Recht auf informationelle Selbstbestimmung verbunden, geht jedoch darüber hinaus: Individuen, Unternehmen und die Gesellschaft als Ganzes sollen nicht nur geschützt, sondern durch innovative Datennutzungskonzepte auch darin gefördert werden, ihre Daten zu teilen und somit nutzbar zu machen, ohne darüber die Kontrolle zu verlieren.

Die digitale Selbstbestimmung hat die Unabhängigkeit und Selbstbestimmtheit des Individuums (bzw. der Gesellschaft) zum Ziel, während die digitale Souveränität als staatliches Konzept die Kontroll- und Handlungsfähigkeit des Staates zum Ziel hat. Trotzdem stehen die Konzepte in einem engen Zusammenhang: Sollten die Schweizer Bürgerinnen und Bürger ihre Unabhängigkeit und Selbstbestimmtheit im digitalen Raum verlieren, wäre mittelfristig auch die Kontroll- und Handlungsfähigkeit des Staates und damit die digitale Souveränität der Schweiz betroffen. Ebenso ist es auch Aufgabe des Staates, für die Verwirklichung der Grundrechte zu sorgen (Art. 35 BV). Entsprechend besteht eine Wechselwirkung zwischen den Arbeiten zur digitalen Selbstbestimmung (vgl. Ziff. 6.1.2.) und denjenigen zur digitalen Souveränität.

Cybersicherheit und digitale Souveränität
Cybersicherheit hat in den vergangenen Jahren stark an Bedeutung gewonnen. Sie ist ein zentraler Faktor für den Wirtschaftsstandort und für die Sicherheit der Bevölkerung im digitalen Raum. Sie spielt zudem eine wichtige Rolle in der Aussen- und Sicherheitspolitik. Die Gewährleistung der Cybersicherheit ist deshalb zu einer unverzichtbaren Aufgabe des Bundes geworden.[25] Bundesrat und Kantone haben im April 2023 die aktuelle «Nationale Cyberstrategie (NCS)» gutgeheissen.[26] Die Strategie zeigt auf, mit welchen Zielen und Massnahmen der Bund und die Kantone gemeinsam mit der Wirtschaft und den Hochschulen den Cyberbedrohungen begegnen wollen.

Auch in der Diskussion um digitale Souveränität spielt Cybersicherheit eine zentrale Rolle. Sicherheit bleibt jedoch unabhängig von der Kontroll- und Handlungsfähigkeit in Bezug auf die digitale Ressource essenziel. So stellt sich beispielsweise sowohl bei einer vollständig selbst entwickelten, gebauten und unterhaltenen IKT-Infrastruktur als auch bei einer von einem einzigen Anbieter dominierten IKT-Infrastruktur die Frage, wie man grösstmögliche Sicherheit gewährleisten kann. Cybersicherheit ist somit ein integraler Bestandteil digitaler Souveränität. Eine vertiefte Behandlung dieses Aspekts erfolgt jedoch nicht in diesem Bericht, weil dieser in der NCS und den dort verankerten Zielen und Massnahmen behandelt wird.

Künstliche Intelligenz und digitale Souveränität
Der rasante technologische Fortschritt wirft in Bezug auf die Nutzung und Bereitstellung von IKT-Infrastruktur (z. B. Cloudnutzung und Rechenzentren) eine Vielzahl regulatorischer, ethischer und technologischer Fragen auf. Dies gilt für künstliche Intelligenz (KI), der innerhalb der digitalen Transformation aufgrund der enormen Entwicklungsgeschwindigkeit eine prominente Rolle zukommt, in besonderem Masse. Aus der Definition der digitalen Souveränität lassen sich Massnahmen ableiten, die auch die Herausforderungen der unterschiedlichen IKT

[25] Ausführlicher hierzu hier: www.ncsc.admin.ch > Über das BACS > Bundesamt für Cybersicherheit (Stand: 22.10.2025).

[26] Medienmitteilung des Bundesrates vom 13. April 2023, Der Bundesrat und die Kantone legen die neue Nationale Cyberstrategie fest, abrufbar unter: https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/medienmitteilungen/newslist.msg-id-94237.html (Stand: 22.10.2025).

adressieren. Der Bundesrat hat am 12. Februar 2025 den Bericht «Auslegeordnung zur Regulierung von künstlicher Intelligenz» verabschiedet. Die Auslegeordnung definiert drei übergreifende Ziele, die durch eine Schweizer Regulierung im Bereich KI erfüllt werden sollten: (i) die Stärkung des Innovationsstandorts Schweiz, (ii) die Wahrung des Grundrechtsschutzes inklusive Wirtschaftsfreiheit und (iii) die Stärkung des Vertrauens der Bevölkerung in KI. Diese Aspekte werden im Rahmen des vorliegenden Berichts nicht weiter vertieft. Es wird auf die Auslegeordnung und ihre Folgearbeiten verwiesen.[27]

5.3 Zielbild

Aus der Definition und den Abgrenzungen lässt sich das Zielbild der digitalen Souveränität für die Schweiz ableiten:

> Die mit staatlichen Aufgaben betrauten Akteure in der Schweiz verfügen über die erforderliche Kontroll- und Handlungsfähigkeit im digitalen Raum, um die Erfüllung der ihnen übertragenen staatlichen Aufgaben sicherzustellen.

Aus diesem Zielbild lassen sich vier aufeinander aufbauende Ziele konkretisieren, die gleichzeitig als Massstab zur Prüfung des Stands der digitalen Souveränität der Schweiz dienen können:

- **Ziel 1: Bewusstsein für die Nutzung digitaler Ressourcen**:
  Die Akteure, die mit der Erfüllung staatlicher Aufgaben betraut sind, sind sich der digitalen Ressourcen bewusst, von denen die Erfüllung der staatlichen Aufgabe abhängt.

- **Ziel 2: Bewusstsein für die Relevanz digitaler Ressourcen**:
  Die Akteure sind sich der Relevanz der digitalen Ressourcen für die Erfüllung der staatlichen Aufgaben bewusst.

- **Ziel 3: Bewusstsein über die Kontroll- und Handlungsfähigkeit und Entscheidungen über gezielte Stärkung**:
  Die Akteure sind sich bewusst, welchen Kontroll- und Handlungsgrad sie über die entsprechenden digitalen Ressourcen haben und treffen eine bewusste Entscheidung darüber, ob sie eine allfällige Abhängigkeit in Kauf nehmen oder die Kontroll- und Handlungsfähigkeit stärken wollen.

- **Ziel 4: Identifikation und Implementierung gezielter Massnahmen**:
  Die Akteure identifizieren und implementieren gezielte Massnahmen, um die Kontroll- und Handlungsfähigkeit in Bezug auf die digitalen Ressourcen zu stärken, von denen eine Abhängigkeit festgestellt wurde, die nicht zu verantworten ist, beziehungsweise unter dem angestrebten Niveau liegt.

[27] Bericht an den Bundesrat über die Auslegeordnung zur Regulierung von künstlicher Intelligenz» des Bundesamtes für Kommunikation vom 12. Februar 2025, abrufbar unter: www.bj.admin.ch > Staat & Bürger > Laufende Rechtsetzungsprojekte > Künstliche Intelligenz (Stand: 22.10.2025).

6 Stand der digitalen Souveränität der Schweiz

Um den Stand der digitalen Souveränität der Schweiz zu ermitteln, muss erstens eine Gesamtsicht der bestehenden Strukturen und laufenden Massnahmen erstellt werden, die für die digitale Souveränität der Schweiz relevant sind und sie bereits heute stärken (vgl. Ziff. 6.1). Zweitens wird ein Abgleich der bestehenden Strukturen und Massnahmen mit den vier identifizierten Zielen vorgenommen (vgl. Ziff. 6.2). Aus diesem Abgleich wird drittens der zusätzliche Handlungsbedarf abgeleitet (vgl. Ziff. 6.3).

Die Ausführungen beziehen sich auf den Bund, da Kantone und Gemeinden weitgehend unabhängig in der Gestaltung ihrer Prozesse sind (Organisationsautonomie der Kantone, Art. 47 Abs. 2 BV). Zudem beschränkt sich die Prüfung auf die Verwaltungsbehörden. Die im Folgenden thematisierten Prozesse und Verantwortlichkeiten (insb. Risiko- und Kontinuitätsmanagement und Informationssicherheitsgesetze) existieren jedoch in weitgehend vergleichbarer Form auch bei der Legislative und der Judikative sowie auf kantonaler Ebene. Die gewonnenen Erkenntnisse sind entsprechend für sämtliche Staatsorgane relevant, wobei im Einzelfall auf die Eigenheiten des spezifischen Staatsorgans einzugehen wäre.

6.1 Bestehende Strukturen und laufende Massnahmen

Auf Stufe Bund bestehen bereits zahlreiche Strukturen und Massnahmen, die der Stärkung der digitalen Souveränität der Schweiz dienen oder damit verknüpft sind.

6.1.1 Bestehende Strukturen

Die Bereitstellung digitaler Ressourcen sowie die Erfassung und Steuerung von Risiken, die sich aus deren Einsatz ergeben, werden auf Bundesebene durch drei komplementäre Bereiche geregelt: die Digitalisierungsverordnung (DigiV, SR 172.019.1), das Risikomanagement und das Informationssicherheitsrecht.

Die **Digitalisierungsverordnung** regelt die Bereitstellung von digitalen Diensten in der Bundesverwaltung (Art. 1 Bst. a DigiV). Jedes Departement und die Bundeskanzlei verfügen über höchstens einen IKT-Leistungserbringer (Art. 10 Abs. 1 DigiV). Diese stellen ihren Verwaltungseinheiten die notwendigen digitalen Ressourcen zur Verfügung. Die Gesamtsteuerung der Digitalisierung der Bundesverwaltung obliegt dem Delegierten für digitale Transformation und IKT-Lenkung (DTI-Delegierter), welcher der BK-DTI vorsteht (vgl. Art. 27 und Art. 28 DigiV). Dieser erarbeitet die *Strategie Digitale Bundesverwaltung*, welche die Ziele der digitalen Transformation innerhalb der Bundesverwaltung und die entsprechenden Handlungsfelder festlegt. Ebenso erstellt er die *Strategie Digitale Schweiz*, die die Leitlinien des staatlichen Handelns und die Bereiche der Zusammenarbeit zwischen Behörden, Wirtschaft, Wissenschaft, Zivilgesellschaft und politischen Akteuren im digitalen Kontext definiert (Art. 7 i.V.m. Art 8 DigiV). Zudem kann die BK-DTI zentrale IKT-Mittel bereitstellen, deren Nutzung anordnen sowie Weisungen im Bereich der digitalen Transformation und IKT-Lenkung erlassen (Art. 11 Abs. 1 DigiV). Der Digitalisierungsrat berät den DTI-Delegierten sowie die Verwaltungseinheiten bei der departementsübergreifenden Koordination in Fragen der digitalen Transformation und IKT-Lenkung (Art. 29 DigiV). Er setzt sich aus Vertreterinnen und Vertretern der Departemente, relevanter Organisationen und Fachstellen zusammen (Art. 30 DigiV).

Die Erfassung von Risiken im Zusammenhang mit der Nutzung digitaler Ressourcen erfolgt durch das **Risikomanagement**. Der einschlägige rechtliche Rahmen findet sich in den Weisungen über die Risikopolitik des Bundes (nachfolgend «Weisungen»).[28] Diese Weisungen definieren die Grundsätze des Risko- und Kontinuitätsmanagement des Bundes und werden in Richtlinien[29] und Handbüchern[30] konkretisiert. Unter Risiko werden dabei Ereignisse und Entwicklungen verstanden, die wesentliche negative Auswirkungen auf die Erfüllung staatlicher Aufgaben haben können (vgl. Art. 2 Abs. 1 Weisungen). Die Verantwortung für die Erfassung, Bewertung und Überwachung von Risiken liegt zunächst bei den Departementen sowie den Leitenden der untergeordneten Verwaltungseinheiten. Die Verwaltungseinheiten melden ihre Risiken an die jeweiligen Departemente, die wiederum den Bundesrat informieren. Die Eidgenössische Finanzverwaltung (EFV) übernimmt dabei eine koordinierende Rolle. Auf einer übergeordneten Ebene prüft die Generalsekretärenkonferenz (GSK) die wesentlichen Risiken der Verwaltungseinheiten auf Vollständigkeit, konsolidiert und priorisiert Querschnittsrisiken, bevor sie dem Bundesrat zur weiteren Behandlung vorgelegt werden (vgl. Art. 5 der Weisungen).

Für das **Informationssicherheitsrecht** findet sich der einschlägige rechtliche Rahmen im Informationssicherheitsgesetz (ISG, SR 128) und der Informationssicherheitsverordnung (ISV, SR 128.1). Sie definieren Massnahmen technischer und organisatorischer Natur, um Risiken im Zusammenhang mit dem Einsatz von digitalen Ressourcen zu reduzieren. Konkret soll die Vertraulichkeit, die Verfügbarkeit und die Integrität von digitalen Ressourcen sichergestellt werden (vgl. Art. 6 Abs. 2 ISG). Im Bereich der Informationssicherheit ist jede durch das ISG verpflichtete Stelle[31] angewiesen, eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten (ISB) zu ernennen. Diese unterstützen ihre Stelle bei der Umsetzung der gesetzlichen Vorgaben, steuern die Informationssicherheit und das zugehörige Risikomanagement, überprüfen die Einhaltung der Vorgaben und beantragen bei Bedarf Massnahmen. Die Konferenz der Informationssicherheitsbeauftragten sorgt für einen einheitlichen Vollzug des Gesetzes, wirkt an der Standardisierung von Anforderungen und Massnahmen mit und fördert den Informationsaustausch zu Risiken, Problemen und Vorfällen. Die Fachstelle des Bundes für Informationssicherheit (FS BIS) berät und unterstützt die verpflichteten Stellen sowie deren ISB, koordiniert wichtige behördenübergreifende Projekte, ist nationale und internationale Ansprechstelle für Fachfragen und berichtet dem Bundesrat jährlich über den Stand der Informationssicherheit des Bundes (vgl. Art. 81 ff. ISG).

6.1.2 Laufende Massnahmen

Der Bundesrat hat in den vergangenen Jahren bereits folgende Massnahmen ergriffen, welche die Kontroll- und Handlungsfähigkeit der Schweiz im digitalen Raum stärken.

Förderung von Open Source Software

Der Einsatz und die Freigabe von Open Source Software kann Herstellerabhängigkeiten reduzieren und dadurch die Handlungsfreiheit des Staates erhöhen. Bereits 2018 wurde ein

---

[28] Weisungen über die Risikopolitik des Bundes, BBl 2024 1662.

[29] Richtlinien über das Risikomanagement Bund, Version vom 2. Dezember 2024, abrufbar unter: www.efv.admin.ch > Themen > Finanzpolitik, Grundlagen > Risiko- und Versicherungspolitik > Richtlinien über das Risikomanagement Bund (Stand: 22.10.2025).

[30] Handbuch zum Risikomanagement Bund, Version vom 16. September 2024, abrufbar unter: www.efv.admin.ch > Themen > Finanzpolitik, Grundlagen > Risiko- und Versicherungspolitik > Handbuch zum Risikomanagement Bund (Stand: 22.10.2025).

[31] Als verpflichtete Stellen gelten die in Art. 2 ISG aufgeführten Behörden und Organisationen. Dazu gehören auch der Bundesrat und die Bundesverwaltung.

«Strategischer Leitfaden Open Source Software in der Bundesverwaltung»[32] und ein «Praxis-Leitfaden Open Source Software in der Bundesverwaltung»[33] publiziert. Beide wurden aktualisiert und zuletzt am 25. Februar 2025 freigegeben.

Am 1. Januar 2024 ist zudem das Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG, SR 172.019) in Kraft getreten. Artikel 9 EMBAG sieht vor, dass der Bund künftig eigens entwickelte oder durch Externe realisierte Software grundsätzlich unter einer Open Source Lizenz veröffentlicht. Durch die Stärkung und den Aufbau von Open Source Kapazitäten kann der Bund für seine Individualentwicklungen einen Markt von Dienstleistern aufbauen und dadurch die Herstellerabhängigkeiten reduzieren.

Ausserdem begann die BK-DTI 2024 mit einer Machbarkeitsstudie zum Einsatz von Open Source Software für die Büroautomation der Bundesverwaltung.[34] Die Studie evaluiert die Eignung von Open Source Software als Rückfalllösung zur Bearbeitung sensitiver Daten im Falle eines Ausfalls der primären Büroautomationslösung.

Strategie für Hybrid Multi-Cloud

Am 11. Dezember 2020 verabschiedete der Bundesrat die Cloud-Strategie der Bundesverwaltung.[35] Darin wird ein Hybrid-Multi-Cloud-Ansatz verfolgt: Bundesbehörden sollen sowohl bundesinterne als auch externe Cloud-Dienste mehrerer Anbieter beziehen und miteinander kombinieren können. Je nach Anforderung an den Schutzbedarf steht jeweils ein anderer Anbieter zur Verfügung. Die sensibelsten Daten können in der Secure Private Cloud des Informatik Service Center des Eidgenössischen Justiz- und Polizeidepartements (ISC-EJPD) gespeichert werden. Mit diesem Ansatz will die Strategie die Vorteile privater Cloud-Anbieter nutzen, ohne den Informationsschutz und damit die digitale Souveränität der Behörden zu kompromittieren.

Revision des Fernmeldegesetzes

Im Bereich der Fernmelde- und digitalen Infrastrukturen hat der Bundesrat im Bericht in Erfüllung des Postulats 20.3984 Pult «Digitale Infrastruktur. Geopolitische Risiken minimieren» festgehalten, dass er die Sicherheit der Schweiz erhöhen will.[36] Dazu sollen nach dem Vorbild der 5G-Toolbox der EU verschiedene Massnahmen ergriffen werden, um eine Diversifizierung der Lieferanten von Ausstattungen für Mobilfunknetze und von als risikobehaftet geltenden Ausrüstungen erreichen. Diese Massnahmen werden im Rahmen der laufenden Revision des Fernmeldegesetzes (SR 784.10) behandelt. Es soll ausserdem eine neue Bestimmung eingeführt werden, die dem Bundesrat die Möglichkeit gibt, bei Eintreten eines geopolitischen Risikos die erforderlichen Massnahmen zu ergreifen. Insbesondere soll er die Beschaffung, die Errichtung und den Betrieb von Ausrüstungen verbieten können, welche von Lieferanten stammen, die als problematisch für die Sicherheit der Schweiz gelten oder die sich im Besitz, unter

---

[32] Strategischer Leitfaden: Open Source Software in der Bundesverwaltung, veröffentlicht am 24.02.2025, abrufbar unter: www.bk.admin.ch > Digitale Transformation und IKT-Lenkung > Bundesarchitektur > Open-Source-Software (OSS) > Em002 Strategischer Leitfaden (Stand: 22.10.2025).

[33] Praxis-Leitfaden: Open Source Software in der Bundesverwaltung, veröffentlicht am 25.02.2025, abrufbar unter: www.bk.admin.ch > Digitale Transformation und IKT-Lenkung > Bundesarchitektur > Open-Source-Software (OSS) > Em002-1 Praxis Leitfaden (Stand: 22.10.2025).

[34] Machbarkeitsstudie PoC BOSS vom 14.05.2024, www.bk.admin.ch > Digitale Transformation und IKT-Lenkung > Standarddienste > Büroautomation > PoC BOSS > Machbarkeitsstudie PoC BOSS (Stand: 22.10.2025).

[35] Cloud-Strategie der Bundesverwaltung, veröffentlicht am 18. Dezember 2020, abrufbar unter: www.bk.admin.ch > Digitale Transformation und IKT-Lenkung > Bundesarchitektur > Cloud > Cloud Strategie Bund (Stand: 22.10.2025).

[36] Bericht des Bundesrates über «Digitale Infrastruktur. Geopolitische Risiken minimieren» in Erfüllung des Postulates 20.3984 Pult vom 15. Dezember 2023, abrufbar unter: https://www.newsd.admin.ch/newsd/message/attachments/85382.pdf (Stand: 22.10.2025).

der Kontrolle oder dem Einfluss eines ausländischen Staates befinden, der ein geopolitisches Risiko für die Schweiz darstellt.

Elektronische Beweismittel: US CLOUD Act und e-Evidence-Paket der EU
Der US CLOUD Act und das e-Evidence-Paket der EU stellen einen Paradigmenwechsel in der Rechtshilfe dar. Angesichts dieser Entwicklungen hat der Bundesrat das EJPD am 9. April 2025 beauftragt, die Schaffung einer gesetzlichen Grundlage zu prüfen, welche die Herausforderungen der Strafverfolgungsbehörden bei der grenzüberschreitenden Beschaffung elektronischer Daten adressiert. Die gesetzliche Grundlage soll Rechtssicherheit bezüglich Zugriffsmöglichkeiten im Rahmen ausländischer Strafverfahren in der Schweiz und umgekehrt schaffen sowie Rechtskollisionen vermeiden. Auch hat der Bundesrat das EJPD beauftragt, im Rahmen von Sondierungsgesprächen zu evaluieren, ob in diesem Bereich enger mit der EU zusammengearbeitet werden kann.[37]

Desinformationskampagnen
Am 19. Juni 2024 verabschiedete der Bundesrat in Erfüllung des Postulats 22.3006 einen Bericht zu Beeinflussungsaktivitäten und Desinformationskampagnen.[38] Im Bericht stellt der Bundesrat fest, dass die Schweiz mit ihrem direktdemokratischen System, in dem die Bevölkerung regelmässig politische Entscheide fällt, sowie als aussenpolitische Akteurin und Gastgeberin zahlreicher internationaler Organisationen ein geeignetes Ziel für Beeinflussungsakteure sein kann. Sie ist als Staat in Europa und Teil der westlichen Wertegemeinschaft sowie wegen ihrer starken internationalen wirtschaftlichen und politischen Vernetzung schon länger indirekt Ziel von allgemeinen, auf westliche Staaten abzielenden Beeinflussungsaktivitäten. Die Schweiz ist zunehmend auch direktes Ziel von auf sie zugeschnittenen Aktivitäten. Im Bericht kommt der Bundesrat zum Schluss, dass die Bekämpfung von Beeinflussungsaktivitäten und Desinformation durch ein koordiniertes Vorgehen der Bundesverwaltung und auch externen Partnern vertieft beziehungsweise ergänzt werden soll. Konkret soll ein besonderer Fokus auf die Lagebeobachtung, die Früherkennung und die Abstimmung der sicherheitspolitischen Gremien des Bundes gesetzt werden.

E-ID und Vertrauensinfrastruktur
Das Stimmvolk hat am 28. September 2025 eine staatliche E-ID angenommen (Bundesgesetz vom 20. Dezember 2024 über den elektronischen Identitätsnachweis und andere elektronische Nachweise; BBL 2025 20). Im Vorfeld hatte sich das Stimmvolk gegen eine von einem privaten Anbieter angebotene E-ID ausgesprochen. Die staatliche E-ID soll den drei Grundsätzen «Privacy-by-design», «Datensparsamkeit» und «dezentrale Datenhaltung» entsprechen. Der Bundesrat hat ausserdem beschlossen, die dafür erforderliche Vertrauensinfrastruktur nicht nur für die E-ID zu nutzen, sondern diese auch Behörden und Unternehmen zur Verfügung zu stellen. Auf dieser Grundlage können Behörden und Unternehmen auch andere elektronische Nachweise ausstellen.

Mit Blick auf die digitale Souveränität der Schweiz ist die E-ID ein Anwendungsfall einer staatlichen Aufgabe (Ausgabe von Ausweisdokumenten) im digitalen Raum.

Digitale Selbstbestimmung
Neben jener der Behörden ist auch die Stärkung der Unabhängigkeit und Selbstbestimmtheit der Bürgerinnen und Bürger – die sogenannte digitale Selbstbestimmung – ein Anliegen des

[37] Medienmitteilung des Bundesrates vom 9. April 2025, Internationale Strafverfolgung: Elektronische Beweismittel einfacher sicherstellen, abrufbar unter: https://www.news.admin.ch/de/nsb?id=105595 (Stand: 22.10.2025).

[38] Bericht des Bundesrates über die «Beeinflussungsaktivitäten und Desinformation» in Erfüllung des Postulats 22.3006 SiK-N vom 9 Juni 2024, abrufbar unter: https://www.parlament.ch/centers/eparl/curia/2022/20223006/Bericht%20BR%20D.pdf (Stand: 22.10.2025).

Bundesrates. Zu diesem Zweck beschloss der Bundesrat am 30. März 2022 Massnahmen, um in der Schweiz und im Ausland vertrauenswürdige Datenräume und die digitale Selbstbestimmung zu fördern.[39] Am 8. Dezember 2023 beschloss der Bundesrat zudem den Aufbau der Anlaufstelle Datenökosystem Schweiz, die seit ihrer Betriebsaufnahme im Januar 2025 Datenraumvorhaben in der Schweiz unterstützt und koordiniert.[40] Diese Massnahmen sind Ausdruck der staatlichen Aufgaben bei der Verwirklichung individueller Rechte. Entsprechend besteht ein enger Bezug der bereits laufenden Prozesse zur Förderung der digitalen Selbstbestimmung und zur Stärkung der digitalen Souveränität. Ferner laufen Arbeiten zur Umsetzung der Motion 22.3890 «Rahmengesetz für die Sekundärnutzung von Daten».

Digitale Kompetenzen

Die digitale Bildung zielt im formalen Bildungssystem darauf ab, allen Schülerinnen und Schülern die digitalen Kompetenzen zu vermitteln, die sie für das Leben in einer digitalisierten Gesellschaft benötigen, und damit die Chancengleichheit zu gewährleisten. So sind digitale Kompetenzen in den Lehrplänen aller Bildungsebenen integriert.[41] Der Anteil junger Menschen mit geringen digitalen Kompetenzen ist vergleichsweise gering. Die Weiterbildung ist in erster Linie Sache jeder und jedes Einzelnen.[42] Die Arbeitgeber sollen die Weiterbildung ihrer Mitarbeitenden begünstigen. Bund und Kantone tragen in Ergänzung zur individuellen Verantwortung und zum Angebot Privater dazu bei, dass sich Personen ihren Fähigkeiten entsprechend weiterbilden können.[43] So ist der Bund aktiv in der Förderung von Grundkompetenzen Erwachsener, zu denen auch die Informations- und Kommunikationstechnologien gehören. Der Bundesrat wird die Frage im Rahmen der Beantwortung des Postulats 23.3621 «Digitale Kluft. Eine Zweiklassengesellschaft vermeiden» vertiefen.

6.2 Prüfung des Stands der digitalen Souveränität

Der vorliegende Bericht schafft eine Gesamtsicht der bestehenden Strukturen und laufenden Massnahmen. Diese zeigt, dass bereits zahlreiche Instrumente bestehen, um die Kontroll- und Handlungsfähigkeit der Schweiz im digitalen Raum bei der Erfüllung staatlicher Aufgaben zu überprüfen und zu stärken.

Ergänzend ist zu prüfen, ob darüber hinaus Handlungsbedarf besteht und dadurch zusätzliche Massnahmen angezeigt sind. Diese Prüfung erfolgt im Abgleich der bestehenden Strukturen und Massnahmen mit den vier identifizierten Zielen (vgl. Ziff. 5.3).

6.2.1 Ziel 1: Bewusstsein für die Nutzung digitaler Ressourcen

Damit die erforderliche Kontroll- und Handlungsfähigkeit im digitalen Raum sichergestellt werden kann, muss in einem ersten Schritt geprüft werden, ob ein Bewusstsein dafür besteht, welche digitalen Ressourcen zur Erfüllung staatlicher Aufgaben eingesetzt werden.

---

[39] Bericht des UVEK und des EDA an den Bundesrat zur «Schaffung von vertrauenswürdigen Datenräumen basierend auf der digitalen Selbstbestimmung» vom 30. März 2022, abrufbar unter: https://www.newsd.admin.ch/newsd/message/attachments/70841.pdf (Stand: 22.10.2025).

[40] Medienmitteilung des Bundesrates vom 8. Dezember 2023, Bundesrat schafft Grundlagen für Schweizer Datenökosystem, abrufbar unter: https://www.news.admin.ch/de/nsb?id=99268 (Stand: 22.10.2025).

[41] Bericht des SBFI vom August 2025 über die Digitalisierung im BFI-Bereich, Übersicht über Massnahmen und Aktivitäten mit Schwerpunkt Digitalisierung, abrufbar unter: www.sbfi.admin.ch > BFI-Politik > Bildungs-, Forschungs- und Innovationspolitik des Bundes 2025–2028 > Transversale Themen im BFI-Bereich > Digitalisierung im BFI-Bereich > PDF-Datei: «Aktivitäten Digitalisierung im BFI-Bereich» (Stand: 22.10.2025).

[42] Weiterbildungsgesetz (WeBiG; SR 419.1.).

[43] Art. 5 WeBiG.

Das ISG und die ISV enthalten hierzu einschlägige Bestimmungen. Sie sehen eine Erfassung sämtlicher digitaler Ressourcen bereits vor. Die IT-Abteilungen der Departemente sowie der Bundeskanzlei sind dazu verpflichtet, ein Inventar über die von ihnen verwendeten digitalen Ressourcen zu führen (Art. 7 Abs. 1 und 2 i. V. m. Art. 2 Abs. 1 Bst. c ISV). Artikel 7 Absatz 1 ISV spricht von «Schutzobjekten», wobei dessen Definition deckungsgleich mit dem in diesem Bericht verwendeten Begriff der digitalen Ressourcen (vgl. Ziff. 5.1.2) ist.

Somit ist festzuhalten, dass ein Bewusstsein für und eine Übersicht über genutzte und angebotene digitale Ressourcen bei der Bundesverwaltung besteht.

Hinsichtlich Ziel 1 besteht kein Handlungsbedarf.

6.2.2 Ziel 2: Bewusstsein für die Relevanz digitaler Ressourcen

Der zweite Schritt, um die erforderliche Kontroll- und Handlungsfähigkeit im digitalen Raum sicherzustellen, besteht darin, die Relevanz der digitalen Ressourcen für die Erfüllung einer staatlichen Aufgabe zu erheben.

Die Erhebung der Relevanz digitaler Ressourcen für die Erfüllung staatlicher Aufgaben ist Teil des Risiko- und Kontinuitätsmanagement des Bundes (vgl. Ziff. 6.1.1). Die Verwaltungseinheiten sind dazu verpflichtet, allfällige Risiken für die Erfüllung ihrer Aufgaben auszuweisen (Art. 5 Abs. 3 und 4 Weisungen).

Für digitale Ressourcen enthält das ISG spezifische Vorgaben, wie diese Risikoeinschätzung vorzunehmen ist. Für jede eingesetzte digitale Ressource muss vor deren Einsatz (und danach in periodischer Überprüfung) eine Schutzbedarfsanalyse durchgeführt werden. Im Rahmen dieser Analyse muss auch die Relevanz der digitalen Ressource für staatliche Aufgaben festgehalten werden. Abhängig davon wird sie einem Schutzniveau (Grundschutz, hoher Schutz, höchster Schutz) zugeteilt (Art. 16 f. ISG und Art. 27 f. ISV).

Die Bundesverwaltung schätzt somit regelmässig die Relevanz digitaler Ressourcen für die Erfüllung ihrer Aufgaben ein.

Hinsichtlich Ziel 2 besteht kein Handlungsbedarf.

6.2.3 Ziel 3: Bewusstsein über Kontroll- und Handlungsfähigkeit und Entscheidungen über gezielte Stärkung

In einem dritten Schritt muss die aktuelle Kontroll- und Handlungsfähigkeit in Bezug auf die digitale Ressource eingeschätzt und, falls notwendig, über eine gezielte Stärkung entschieden werden.

Der Grad an Kontroll- und Handlungsfähigkeit in Bezug auf digitale Ressourcen wird ebenfalls im Rahmen des Risikomanagements des Bundes erhoben. Die Verwaltungseinheiten müssen periodisch beurteilen, welche Risiken ihre Kontroll- und Handlungsfähigkeit in Bezug auf digitale Ressourcen schwächen könnten.

In Anlehnung an Artikel 6 Absatz 2 ISG unterscheidet das Handbuch zum Risikomanagement Bund[44] vier Arten von Risiken für digitale Ressourcen:

a. Ausfall von Anwendungen und/oder Nichtverfügbarkeit von Daten (Verfügbarkeitsrisiko)
b. Abfluss von sensiblen Daten (Vertraulichkeitsrisiko)

[44] Handbuch zum Risikomanagement Bund, S. 86.

c. Manipulation von Daten (Integritätsrisiko)
d. Daten können unbemerkt verändert werden (Nachvollziehbarkeitsrisiko und Integritätsrisiko)

Die Einschätzung dieser Risiken umfasst die Erarbeitung konkreter Risikoszenarien und die Bewertung ihrer Eintrittswahrscheinlichkeiten. Diese Aufgabe ist äusserst anspruchsvoll. Die zunehmende Bereitschaft von Staaten, die im digitalen Bereich über marktdominierende Positionen verfügen (insbesondere Grossmächte), ihre Interessen durch Machtpolitik durchzusetzen und dazu auch den Zugang zu den von ihnen beherrschten Technologien als Druckmittel einzusetzen, stellt hochdigitalisierte Staaten wie die Schweiz vor grosse Herausforderungen. Neben technischen Risiken treten deshalb zunehmend auch geopolitische Risiken in den Vordergrund. Drei Beispiele:

Beispiel 1 – Extraterritoriale Rechtsdurchsetzung
Der US CLOUD Act erlaubt es amerikanischen Strafverfolgungsbehörden, auf Daten zuzugreifen, die amerikanische Technologieunternehmen kontrollieren, auch wenn diese Daten auf Servern ausserhalb des Staatsgebiets der USA gespeichert sind. Wie sich dieses Gesetz zu den völkerrechtlichen Immunitäten anderer Staaten verhält, ist nicht abschliessend geklärt. In Situationen, in denen Schweizer Behörden ihre Daten bei einem amerikanischen Unternehmen speichern, ist deshalb unklar, ob die Vertraulichkeit der Daten sichergestellt ist oder ob amerikanische Strafverfolgungsbehörden auf diese Daten unabhängig von ihrem Standort Zugriffsrechte durchsetzen können.

Beispiel 2 – Technologiesanktionen
Die meisten Staaten kennen die Möglichkeit des Erlasses umfassender Sanktionen, welche sich auch ausserhalb ihres Staatsgebiets auswirken. Diese Sanktionen können Risiken für die Verfügbarkeit von digitalen Ressourcen darstellen. Verbietet beispielsweise der sanktionierende Staat Unternehmen in seinem Staatsgebiet, mit einem anderen Staat Transaktionen zu tätigen, verliert der sanktionierte Staat unter Umständen vollständig die Kontroll- und Handlungsfähigkeit in Bezug auf digitale Ressourcen, die er bis anhin bei Technologieunternehmen des sanktionierenden Staates eingekauft hat.

Beispiel 3 – «Vendor-Lock-in»
Zu denken ist an marktbeherrschende IT-Dienstleister, von deren Dienstleistungen die Behörde in hohem Masse abhängig ist. Das entstehende Abhängigkeitsverhältnis kann ein Risiko für die Kontroll- und Handlungsfähigkeit in Bezug auf die digitale Ressource darstellen. So kann beispielsweise der Wechsel zu einem anderen Anbieter mit unverhältnismässig hohen Kosten verbunden sein und nicht kurzfristig vorgenommen werden.

Die umfassende Einschätzung von IKT-Risiken erfordert deshalb nicht nur technische, sondern zunehmend auch (völker-)rechtliche Kenntnisse sowie die Antizipation künftiger sicherheits- und aussenpolitischer Entwicklungen. Es ist fraglich, ob die mit der Erstellung der Risikoanalyse befassten Personen (insbesondere die verantwortliche Person und der ISB der betroffenen Verwaltungseinheit) über die notwendigen Kapazitäten verfügen, um diese Risiken umfassend zu prüfen. Zudem stehen übergeordnete Hilfestellungen für solche geopolitischen Risiken, anders als für klassische technische Risiken, nicht standardmässig zur Verfügung.

Der Bund verfügt zwar mit der FS BIS über eine Stelle, welche die verpflichteten Behörden bei der Umsetzung des ISG und damit auch bei der Einschätzung von IKT-Risiken berät. Dabei handelt es sich jedoch primär um eine technische Stelle. Sie ist ebenfalls nicht darauf ausgelegt, internationale sicherheitspolitische Entwicklungen zu verfolgen oder das mögliche zukünftige Verhalten von Staaten einzuschätzen und daraus prospektive Risikoszenarien für digitale Ressourcen zu entwickeln.

Es lässt sich ableiten, dass Risiken, die sich aus dem Einsatz von digitalen Ressourcen ergeben, bis anhin nicht systematisch und vollumfänglich erfasst werden. Diese Erkenntnis deckt sich mit jener in der Nationalen Cyberstrategie (NCS), die der Schweiz einen Handlungsbedarf bei der systematischen Analyse von Abhängigkeiten und Risiken mit Bezug zu IKT-Produkten attestiert.[45]

Hinsichtlich Ziel 3 besteht Handlungsbedarf.

6.2.4 Ziel 4: Implementierung gezielter Massnahmen

Der letzte Schritt zur Sicherstellung der Kontroll- und Handlungsfähigkeit im digitalen Raum ist die Implementierung gezielter Massnahmen, um nicht hinnehmbaren Abhängigkeiten entgegenzuwirken.

Das Risikomanagement verlangt neben der Erarbeitung von konkreten Risikoszenarien und der Bewertung ihrer Eintrittswahrscheinlichkeit auch die Definition von Massnahmen zur Risikominderung. Diese Massnahmen werden durch das Informationsschutzrecht definiert. Dieses bestimmt, dass alle digitalen Ressourcen, unabhängig von ihrem Schutzniveau, durch ein Mindestmass an technischen Schutzmassnahmen (sog. IKT-Grundschutz) geschützt werden müssen.[46] Für digitale Ressourcen mit erhöhtem Schutzbedarf müssen die verantwortlichen Verwaltungseinheiten eine erweiterte Risikoanalyse durchführen und darauf aufbauend zusätzliche Massnahmen zur Reduktion der identifizierten Risiken umsetzen.

Die Schutzziele Vertraulichkeit und Integrität können grundsätzlich schon mit der Umsetzung der im IKT-Grundschutz enthaltenen Massnahmen massgeblich gestärkt werden. Die dazu vorgeschlagenen technischen Massnahmen (z. B. Einsatz von Verschlüsselungssoftware zur Sicherstellung der Vertraulichkeit; Implementierung von Datenvalidierungsalgorithmen zur Sicherstellung der Integrität) basieren auf international anerkannten Standards und Best Practices. Ihre Wirksamkeit ist breit anerkannt.

Falls die digitale Ressource nicht von einer Verwaltungseinheit selbst, sondern von einem Dritten zur Verfügung gestellt wird, kann das Schutzziel der Vertraulichkeit nicht immer allein durch technische Massnahmen garantiert werden. In diesem Kontext ist der Unterschied zwischen kundenseitiger und serverseitiger Verschlüsselung von grosser Bedeutung.

- Von kundenseitiger Verschlüsselung spricht man, wenn der Leistungsbezüger die Daten verschlüsselt und erst dann an den Leistungserbringer übermittelt.
- Im Falle der serverseitigen Verschlüsselung erfolgt die Verschlüsselung durch den Leistungserbringer. Daraus ergibt sich für den Leistungserbringer die faktische Möglichkeit, auf die unverschlüsselten Daten zuzugreifen.

Der IKT-Grundschutz verlangt zwar, dass Daten verschlüsselt werden. Er setzt aber nicht voraus, dass dies kundenseitig geschieht. Dabei handelt es sich um eine bewusste Entscheidung, denn viele Funktionen moderner Office-Applikationen (z. B. gleichzeitige Bearbeitung eines Dokuments durch mehrere Personen) setzen voraus, dass der Leistungserbringer die Daten entschlüsseln kann. Das eröffnet die Möglichkeit, dass Daten der Bundesverwaltung über den Leistungserbringer abfliessen können und beispielsweise in Anwendung des US CLOUD Act einem anderen Staat übermittelt werden. In diesem Fall kann die Vertraulichkeit

[45] Nationale Cyberstrategie (NCS), 2023, S. 17, abrufbar unter: https://www.newsd.admin.ch/newsd/message/attachments/76793.pdf (Stand: 22.10.2025).

[46] Zum IKT-Grundschutz allgemein siehe: www.ncsc.admin.ch > Dokumentation > Informatiksicherheitsvorgaben Bund > Grundschutz. (Stand: 22.10.2025).

der Daten beziehungsweise der Ausschluss des Zugriffs anderer Staaten nicht garantiert werden.

Falls eine digitale Ressource von einem Dritten zur Verfügung gestellt wird, sind technische Massnahmen allein auch zur Sicherstellung des Schutzziels der Verfügbarkeit unzureichend. Deshalb schliessen IKT-Leistungsbezüger mit dem IKT-Leistungserbringer oftmals sogenannte Service Level Agreements (SLA) ab, in denen die Verfügbarkeit eines Systems vertraglich vereinbart wird. Ein SLA kann beispielsweise definieren, dass der IKT-Leistungserbringer zur ordentlichen Erfüllung des Vertrages eine zeitliche Verfügbarkeit von 99,9 Prozent sicherstellen muss. Diese Massnahmen, sowohl die technischen wie auch die vertraglichen, vermögen es jedoch nicht, den oben beispielhaft aufgeführten Risiken auf Grund von geopolitischen Spannungen bzw. Problemen der Wertschöpfungskette zu begegnen. Im Falle geopolitischer Spannungen kann beispielsweise nicht allein auf die privatrechtliche Bindungswirkung von SLAs vertraut werden, um die Verfügbarkeit einer digitalen Ressource zu garantieren. Auch können weder technische noch privatrechtliche Massnahmen verhindern, dass der Leistungserbringer aus eigenem Antrieb die Dienstleistung einstellt.

Diesen Risiken kann dadurch begegnet werden, dass die digitale Ressource durch die Bundesverwaltung selbst bereitgestellt wird (sog. Autarkie). Dabei handelt es sich jedoch um eine oft kostspielige Lösung, die nicht in allen Fällen umsetzbar sein dürfte.

Aktuell fehlt es der Bundesverwaltung an einem Massnahmenkatalog, um die Verfügbarkeit und die Vertraulichkeit von digitalen Ressourcen gezielt zu stärken.

Hinsichtlich Ziel 4 besteht Handlungsbedarf.

6.3 Handlungsbedarf

Die erfolgte Überprüfung der Ziele kann wie folgt zusammengefasst werden:

	Ziel	**Stand**	**Handlungsbedarf**
1	**Bewusstsein für die Nutzung digitaler Ressourcen:** Akteure, die mit der Erfüllung staatlicher Aufgaben betraut sind, sind sich der digitalen Ressourcen bewusst, von denen die Erfüllung der Aufgabe abhängt.	Die IT-Abteilungen der Bundesverwaltung führen Inventare zu den sich im Gebrauch befindenden digitalen Ressourcen.	Nein
2	**Bewusstsein für die Relevanz digitaler Ressourcen:** Akteure sind sich der Relevanz der digitalen Ressourcen für die Erfüllung der staatlichen Aufgabe bewusst.	Das Risikomanagement des Bundes definiert bereits einen Prozess, um die Relevanz von digitalen Ressourcen und damit einhergehenden Risiken systematisch zu erfassen.	Nein
3	**Bewusstsein über Kontroll- und Handlungsfähigkeit und Entscheidungen über gezielte Stärkung:** Akteure sind sich bewusst, welchen Kontroll- und Handlungsgrad sie in Bezug auf	Die Identifikation und Einschätzung von IKT-Risiken (insbesondere für die Verfügbarkeit von digitalen Ressourcen) ist äusserst komplex. Zurzeit bestehen keine	Ja

	die entsprechenden digitalen Ressourcen haben, und treffen eine bewusste Entscheidung darüber, ob sie eine allfällige Abhängigkeit in Kauf nehmen oder die Kontroll- und Handlungsfähigkeit stärken wollen.	genügenden Hilfsmittel, um etwa (völker-)rechtliche und geopolitische Risiken systematisch miteinzubeziehen.	
4	**Identifikation und Implementierung gezielter Massnahmen:** Akteure identifizieren und implementieren gezielte Massnahmen, um die Kontroll- und Handlungsfähigkeit in Bezug auf die digitalen Ressourcen zu stärken, von denen eine Abhängigkeit festgestellt wurde, die nicht zu verantworten ist bzw. unter dem angestrebten Niveau liegt.	Massnahmen zur Sicherstellung der Verfügbarkeit und Vertraulichkeit von digitalen Ressourcen stehen nicht in ausreichendem Masse zur Verfügung.	Ja

Die Überprüfung der vier Ziele zeigt in Bezug auf den Handlungsbedarf Folgendes:

Der Stand der digitalen Souveränität ist bei der Bundesverwaltung mit Blick auf das Bewusstsein für die Nutzung (Ziel 1) und die Relevanz der digitalen Ressourcen (Ziel 2) gut. Es besteht eine Übersichtüber die vorhandenen digitalen Ressourcen und es ist bekannt, welche digitalen Ressourcen wichtig und welche weniger wichtig zur Erfüllung der staatlichen Aufgaben sind.

Handlungsbedarf besteht demgegenüber bei den Zielen 3 und 4. Der Handlungsbedarf kann in die folgenden zwei Handlungsfelder gegliedert werden:

- **H1**: **Identifikation und Einschätzung von Risiken**: Die Identifikation und Einschätzung von IKT-Risiken (insbesondere für die Verfügbarkeit und die Vertraulichkeit von digitalen Ressourcen) muss gestärkt werden.
- **H2**: **Identifikation und Umsetzung von Massnahmen**: Es müssen Massnahmen identifiziert und umgesetzt werden, um diesen Risiken zu begegnen und insbesondere um Abhängigkeiten zu reduzieren beziehungsweise zu diversifizieren.

Wie eingangs angekündigt, orientierte sich die Überprüfung der Ziele an den Prozessen und Verantwortlichkeiten der Bundesverwaltung. Die gewonnenen Erkenntnisse sind jedoch für sämtliche Bundesbehörden und gegebenenfalls für kantonale Behörden relevant, wobei im Einzelfall auf die Eigenheiten einer spezifischen Behörde einzugehen ist.

7 Strategie für die digitale Souveränität der Schweiz

Die Überprüfung des Stands der digitalen Souveränität zeigt, dass der Bund über eine Vielzahl an Instrumenten zur Wahrung und Stärkung der digitalen Souveränität der Schweiz verfügt.

Dennoch kann die digitale Souveränität weiter gestärkt werden. Einerseits sollen die im Bericht vorgenommene Gesamtsicht der bestehenden Strukturen und Massnahmen laufend aktualisiert und die Arbeiten der Bundesbehörden zur Stärkung der digitalen Souveränität der Schweiz koordiniert werden. Andererseits sollen zusätzliche Massnahmen ergriffen werden, um dem bei den Zielen 3 und 4 ausgewiesenen Handlungsbedarf gerecht zu werden.

7.1 Gesamtsicht und Koordination

Die in Kapitel 6.1 erstellte Gesamtsicht über bestehende Strukturen und laufende Massnahmen zeigt, dass die digitale Souveränität sowohl inhaltlich als auch organisatorisch ein Querschnittsthema darstellt. Die laufenden und künftigen Massnahmen zur Stärkung der digitalen Souveränität sollen vom jeweils zuständigen Departement weitergeführt werden. Gleichzeitig soll jedoch die Gesamtsicht laufend aktualisiert und die Koordination zwischen den Departementen und ihren jeweiligen thematischen Zuständigkeiten gestärkt werden.

Massnahme 1: Das VBS (Staatssekretariat für Sicherheitspolitik SEPOS) wird beauftragt, in Zusammenarbeit mit dem EDA (Direktion für Völkerrecht DV), eine interdepartementale Arbeitsgruppe *Digitale Souveränität* einzusetzen. Die Arbeitsgruppe ist auf Ende 2027 befristet. Dem Bundesrat ist einmal jährlich über ihre Arbeit Bericht zu erstatten.

Massnahme 2: Die interdepartementale Arbeitsgruppe *Digitale Souveränität* wird beauftragt, die in diesem Bericht erstellte Gesamtsicht der Arbeiten der Bundesbehörden zur Stärkung der digitalen Souveränität laufend zu aktualisieren und die Arbeiten bei Bedarf zu koordinieren. Sie stellt sicher, dass (neue) Fragestellungen im Querschnittsthema der digitalen Souveränität durch die beteiligten Stellen in die Arbeitsgruppe eingebracht und dort abgestimmt werden können.

7.2 Identifikation und Einschätzung von Risiken

Wie in Kapitel 6.2.3 ausgeführt, besteht bei der Identifikation und Einschätzung von IKT-Risiken Handlungsbedarf.

Die Herausforderung besteht darin, dass komplexe IKT-Risiken in einem geopolitisch dynamischen Umfeld analysiert werden müssen. Von den im dezentral organisierten Risikomanagementprozess verantwortlichen Personen kann realistischerweise nicht erwartet werden, dass sie über genügend Kapazitäten verfügen, um diese Risiken umfassend zu beurteilen. Zwar gibt es für klassische technische Risiken übergeordnete Hilfestellungen, für geopolitische Risiken stehen solche jedoch nicht standardmässig zur Verfügung. Zudem ist die Entwicklung geopolitischer Risikoszenarien sehr zeitaufwendig, weshalb ihre dezentrale Erstellung auch unter Effizienzgesichtspunkten hinterfragt werden kann.

Sowohl aus Gründen der Komplexität als auch der Effizienz drängt sich deshalb auf, dass ein interdisziplinäres und departementsübergreifendes Gremium die unterschiedlichen Risiken für die digitalen Ressourcen des Bundes interdisziplinär antizipiert, bewertet und entsprechende Empfehlungen und Hilfsmittel erarbeitet. Die interdepartementale Arbeitsgruppe *Digitale Souveränität* soll künftig diese Aufgabe übernehmen.

Massnahme 3: Die interdepartementale Arbeitsgruppe *Digitale Souveränität* wird beauftragt,

- **I)** sicherheits- und aussenpolitische Risiken für die digitalen Ressourcen des Bundes zu identifizieren sowie
- **II)** Empfehlungen und Hilfsmittel zur Risikoeinschätzung für die Informationssicherheitsbeauftragten der Bundesbehörden zu erarbeiten.

7.3 Identifikation und Umsetzung von Massnahmen

Wie in Kapitel 6.2.4 ausgeführt, besteht bei der Fähigkeit der Behörden, den identifizierten Risiken mit geeigneten Massnahmen entgegenzutreten, Handlungsbedarf. Angesichts der veränderten geopolitischen Gegebenheiten und der daraus resultierenden Risiken für die Kontroll- und Handlungsfähigkeit der Behörden in Bezug auf digitale Ressourcen müssen die Effektivität bisheriger Massnahmen überprüft und neue Massnahmen erarbeitet werden.

Die offensichtlichste Massnahme zur Sicherstellung der Verfügbarkeit und der Vertraulichkeit und der gleichzeitigen Verhinderung von Abhängigkeiten von Dritten ist die selbständige Bereitstellung von digitalen Ressourcen durch den Bund (sog. Autarkie). Diese Massnahme dürfte auch die kostspieligste sein. Für die Schweiz dürften diese Kosten deutlich stärker ins Gewicht fallen als in den grossen Wirtschaftsblöcken USA oder EU. So hat die Schweiz nicht nur einen verhältnismässig kleinen Binnenmarkt mit begrenzten Skaleneffekten, sondern auch relativ hohe Preise und Löhne.[47] Zudem wäre es auch mit hohem Finanzaufwand kaum realistisch, dass ein hochintegriertes Land wie die Schweiz in allen relevanten Bereichen eigene digitale Ressourcen bereitstellt. Dies allein schon deshalb, weil die Schweiz nicht über alle für den Bau von IKT-Infrastruktur benötigten Ressourcen – wie beispielsweise seltene Erden – verfügt. Die Schweiz wird deshalb weiterhin von anderen Staaten und deren Ressourcen und Dienstleistungen abhängen.

In Fällen, in denen eine Abhängigkeit von Dritten unumgänglich ist, muss das Risiko mit Massnahmen eingegrenzt werden. In Frage kommen sowohl technische als auch rechtliche Massnahmen. Auf technischer Ebene sind insbesondere Massnahmen zur Reduktion einseitiger Abhängigkeiten – etwa Multi-Vendor-Ansätze oder Exit-Strategien – zu prüfen. Risiken, die sich technisch nicht ausreichend begrenzen lassen, sind ergänzend durch geeignete rechtliche Vorkehrungen abzusichern. Auf zwischenstaatlicher Ebene ist insbesondere die Minimierung geopolitischer Risiken durch völkerrechtliche Mittel anzustreben. In diesem Bereich besteht grosser Klärungsbedarf. Das Völkerrecht enthält zwar Prinzipien, welche staatlich genutzten digitalen Ressourcen einen gewissen Schutz einräumen. Dazu gehört zum Beispiel die Immunität von Staaten, die grundsätzlich auch staatliche Dokumente und damit auch digitale Daten umfasst. Die genauen Anwendungsmodalitäten dieser Regeln sind jedoch für den digitalen Raum noch nicht geklärt, weshalb sich die Schweiz weiterhin mit gleichgesinnten Staaten dafür einsetzt, dass der Konsens bezüglich der Geltung der Staatenimmunität für digitale Dokumente gestärkt und seine Tragweite geklärt wird.

Auf rechtliche Vereinbarungen kann jedoch nur dann vertraut werden, wenn davon ausgegangen werden kann, dass sie von den Vertragsstaaten eingehalten werden. Dies wiederum hängt einerseits von der allgemeinen Verlässlichkeit des Vertragspartners, der Stärke der bilateralen Beziehung und dem Vorhandensein von Sanktionsmechanismen im Falle einer Verletzung einer völkerrechtlichen Pflicht ab. Rechtliche Massnahmen sollten deshalb von politischen und antizipatorischen Massnahmen begleitet werden, um die Einhaltung der völkerrechtlichen Pflichten fortlaufend zu überprüfen und mögliche künftige Veränderungen frühzeitig zu antizipieren.

Massnahme 4: Die interdepartementale Arbeitsgruppe *Digitale Souveränität* wird beauftragt,

- **I)** Empfehlungen für Massnahmen zur Sicherstellung der Verfügbarkeit und Vertraulichkeit von digitalen Ressourcen auszuarbeiten;
- **II)** notwendige Anpassungen der anwendbaren nationalen Rechtsgrundlagen vorzuschlagen; sowie
- **III)** völkerrechtliche Instrumente zur Stärkung der digitalen Souveränität der Schweiz zu prüfen und Vorschläge für rechtliche Absicherungen insbesondere der Staatenimmunität von behördlichen Daten zu unterbreiten.

[47] Zu den umfangreichen Risiken von industriepolitischen Initiativen vgl. Lagebericht des Bundesrates vom 22. Mai 2024 zur Schweizer Volkswirtschaft 2024, verfügbar unter: www.seco.admin.ch > SECO - Staatssekretariat für Wirtschaft > Publikationen & Dienstleistungen > Publikationen > Strukturwandel und Wachstum > Wachstum > Lagebericht zur Schweizer Volkswirtschaft 2024 (Stand: 22.10.2025).

Anhang Parlamentarische Vorstösse zur Thematik der digitalen Souveränität

Nummer	Titel	Art des Vorstosses	Eingereicht von	Eingereicht im
25.4348	Gibt die Schweiz ihre digitale Souveränität auf?	Interpellation	Gugger Niklaus-Samuel	Nationalrat
25.4336	Impact environnemental du numérique : où va-t-on ?	Interpellation	Clivaz Christophe	Nationalrat
25.4235	Stärkung der digitalen Souveränität durch gerechte Besteuerung und Förderung der Entwicklung alternativer Lösungen	Motion	Marti Min Li	Nationalrat
25.4055	Schweizer Zahlungsverkehr im Griff von US-Giganten: digitale Souveränität stärken	Interpellation	Müller Damian	Ständerat
25.3947	Versorgungssicherheit mit strategischen Rohstoffen und Halbfabrikaten als Bestandteil von Freihandelsabkommen	Motion	Aussenpolitische Kommission	Nationalrat
25.3918	Stärkung der landwirtschaftlichen Resilienz durch Förderung einer unabhängigen Datenwertschöpfung	Motion	Müller Leo	Nationalrat
25.3838	Digitale Versorgung der Schweiz. Haben wir eine Strategie?	Interpellation	Chappuis Isabelle	Nationalrat
25.3705	Rechtsgrundlagen für eine nationale Datenpolitik. Analyse des Handlungsbedarfs	Postulat	Silberschmidt Andri	Nationalrat
25.3704	Stärkung der digitalen Souveränität: Welche Massnahmen plant die Schweiz?	Interpellation	Silberschmidt Andri	Nationalrat
25.3659	Digitale Souveränität. Wo steht die Schweiz?	Postulat	Häberli-Koller Brigitte	Ständerat
25.3586	Digitale Souveränität der Schweiz ist Realität!	Interpellation	Imark Christian	Nationalrat

25.3532	Ein gemeinschaftlicher, öffentlicher Ansatz zum Aufbau und langfristigen Betrieb der Swiss Government Cloud (SGC)	Motion	Finanzkommission	Nationalrat
25.3530	Für einen souveränen, sicheren und kontextsensitiven KI-Assistenten für die Ratsmitglieder	Motion	Sicherheitspolitische Kommission	Nationalrat
25.3506	Bericht zu Zielen und Massnahmen zur Sicherstellung digitaler Unabhängigkeit und Souveränität der Schweiz	Motion	Badran Jacqueline	Nationalrat
25.3383	Risikobeurteilung der Cloud-Version von Microsoft	Interpellation	De Ventura Linda	Nationalrat
25.3359	Schützt die Schweiz den freien Zugang zu sicheren und neuen Technologien hinreichend?	Interpellation	Candinas Martin	Nationalrat
25.3197	Künstliche Intelligenz. Europäischen Effort und Zusammenarbeit stärken	Postulat	Marti Min Li	Nationalrat
25.3190	Flächendeckende und krisensichere Internetanbindung für öffentliche und private Nutzer durch den raschen Beitritt zu IRIS2 garantieren	Interpellation	Molina Fabian	Nationalrat
25.1046	Nutzung des Supercomputers Alps	Anfrage	Badran Jacqueline	Nationalrat
25.1033	Digitale Abhängigkeiten der Schweiz vom Ausland. Welche Prioritäten?	Anfrage	Badran Jacqueline	Nationalrat
25.1000	USA vs. CH: Beschränkung der Ausfuhr von amerikanischen KI-Chips in die Schweiz	Dringliche Anfrage	Gianini Simone	Nationalrat
24.3810	Durchführung dringend notwendiger Cybersicherheitsprüfungen	Motion	Sicherheitspolitische Kommission	Ständerat
24.3363	Für eine souveräne digitale Infrastruktur in der Schweiz im Zeitalter der künstlichen Intelligenz	Motion	Chappuis Isabelle	Nationalrat

23.3866	Eine schweizerische Halbleiterstrategie (Swiss Chip Strategy)	Postulat	Cottier Damien	Nationalrat
23.3543	Systematische Versorgungsstrategie für essenzielle und kritisch-strategische Güter	Postulat	Marti Samira	Nationalrat
23.3147	Regulierung der künstlichen Intelligenz in der Schweiz	Interpellation	Bendahan Samuel	Nationalrat
23.3002	Mehr Sicherheit bei den wichtigsten digitalen Daten der Schweiz	Motion	Dittli Josef	Ständerat
22.4510	Strategische wirtschaftliche Abhängigkeit von China	Postulat	Molina Fabian	Nationalrat
22.4411	Strategie Digitale Souveränität der Schweiz	Postulat	Z'graggen Heidi	Ständerat
22.3414	Schutz der kritischen Infrastruktur vor Einflussnahmen anderer Staaten	Motion	Sozialdemokratische Fraktion	Nationalrat
22.3405	Folgen des Krieges in der Ukraine. Langfristige strategische Abhängigkeiten evaluieren und reduzieren	Postulat	Sozialdemokratische Fraktion	Nationalrat
21.495	Cybersicherheit. Schaffung einer eigenständigen digitalen Infrastruktur und Erarbeitung von Standards im Sicherheitsmanagement.	Parlamentarische Initiative	Moret Isabelle	Nationalrat
21.4187	Unsere KMU und öffentlichen Verwaltungen vor Cyberangriffen schützen	Motion	Gapany Johanna	Ständerat
21.3951	Digitale Souveränität. Wie will der Bundesrat die Begrenzung der Überwachung der Schweizer Telekommunikationsnetze durch Huawei gewährleisten, und welche Massnahmen wird er treffen?	Interpellation	Sommaruga Carlo	Ständerat
21.3676	Auftrag für die Mitwirkung an der europäischen Regulierung der Digitalisierung	Motion	Chassot Isabelle	Nationalrat
20.3984	Digitale Infrastruktur. Geopolitische Risiken minimieren	Postulat	Pult Jon	Nationalrat

20.3433	Auslandabhängigkeit vermindern, souveräner und krisenresistenter werden	Postulat	Reimann Lukas	Nationalrat
20.3409	Öffentliche Beschaffungen. Sicherheit und Verlässlichkeit von Lieferketten berücksichtigen	Motion	Würth Benedikt	Ständerat
20.3268	Essentielle Güter. Wirtschaftliche Abhängigkeit verringern	Motion	Häberli-Koller Brigitte	Ständerat
19.3884	Eine Strategie für die digitale Souveränität der Schweiz	Motion	Derder Fathi	Nationalrat
18.3511	Nutzen der strategischen Vorteile der Schweiz bei der Entwicklung eines sicheren digitalen Hardware-Markts	Interpellation	Vonlanthen Beat	Ständerat
17.3849	Schweizer Armee. Wie können unsere Souveränität und Unabhängigkeit sichergestellt werden, wenn mit der Digitalisierung die gegenseitigen Abhängigkeiten immer mehr zunehmen?	Motion	Béglé Claude	Nationalrat
17.3783	Digitale Souveränität der Schweizer Bundesverwaltung	Interpellation	Fricker Jonas	Nationalrat
13.4308	Sicherheit und Unabhängigkeit der Schweizer Informatik verbessern	Postulat	Graf-Litscher Edith	Nationalrat