Bundesministerium
Innovation, Mobilität
und Infrastruktur

Technologiesouveränität im europäischen Kontext

Endbericht

Wien, März 2026

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundesministerium für Innovation, Mobilität und Infrastruktur,
Radetzkystraße 2, 1030 Wien
Autor: DDr. Erich Prem, eutema
Wien, 2025. Stand: 24. März 2026

Disclaimer:
Diese Studie gibt die Meinung des Studienautors wieder.

Rückmeldungen: Ihre Überlegungen zu vorliegender Publikation übermitteln Sie bitte an georg.sedlbauer@bmimi.gv.at.

Inhalt

Zusammenfassung

Dieser Endbericht beschreibt das dreijährige Projekt „Technologiesouveränität im europäischen Kontext“, das Österreichs Beitrag zur europäischen strategischen Autonomie – insbesondere bei digitalen Schlüsseltechnologien – auslotet und umsetzbare Instrumente für FTI-Politiken entwickelt. Im Mittelpunkt stehen die begriffliche Klärung von Technologiesouveränität, ein Indikatorenset für FTI-Projekte, dialogorientierte Veranstaltungen sowie konkrete Empfehlungen für die EU und Österreich

Im Projekt wurde Technologiesouveränität als Fähigkeit definiert, kritische Technologien ohne einseitige strukturelle Abhängigkeiten zu entwickeln bzw. zu beziehen, ohne Autarkie anzustreben. Es wurden Teilaspekte wie Wissens-, Forschungs-, Entwicklungs-, Produktions-, Betriebs-, Nutzungs-, Daten-, Plattform- und Transparenzsouveränität herausgearbeitet, um FTI-Projekte systematisch analysieren zu können.

Es wurde ein Leitfragen-basiertes Schema zur Selbsteinschätzung von Technologiesouveränität in FTI-Projekten erarbeitet, das Abhängigkeiten nach Kategorien (Hardware, Software, Daten, Infrastruktur, Wissen, rechtliche/organisatorische Faktoren) sowie Mitigationsstrategien (Monitoring, Ersatztechnologien, alternative Bezugsquellen, organisatorische Maßnahmen, Partnerschaften) erfasst. Dieses Schema wurde in zwei FFG-Ausschreibungen getestet und zeigte typische Abhängigkeiten (z.B. KI-Komponenten, Cloud-Dienste, Spezialsoftware, implizites Expertenwissen), aber auch Unterschätzungen etwa bei Nicht-EU-Clouds und Lizenzrisiken.

Das Projekt organisierte mehrere öffentliche Veranstaltungen und Workshops, darunter eine Auftaktdiskussion im Rahmen der IMAGINE 2023, zwei Workshops mit FFG-Projektteilnehmenden, einen Indikatoren-Workshop sowie eine Abschlussveranstaltung bei IMAGINE 2025. Diese Formate dienten dazu, den Begriff der Technologiesouveränität zu schärfen, Projektperspektiven einzubeziehen, Erfahrungen mit den Indikatoren auszuwerten und Österreichs Rolle im europäischen Souveränitätsdiskurs zu diskutieren.

Ergänzend wurden Entwicklung und Verwendung der Begriffe strategische Autonomie, Resilienz und wirtschaftliche Sicherheit in der EU, rechtliche und politische Grundlagen sowie der besondere Stellenwert von KI und Quantentechnologien als strategische

Schlüsseltechnologien für Europa aufgearbeitet. Der Bericht zeigt, dass die EU trotz starker Forschungsbasis in Quanten und eines umfassenden KI-Regulierungsrahmens bei Infrastruktur, Investitionen und Marktmacht deutlich hinter den USA und China zurückliegt.

Empfehlungen: Strategische Autonomie als politisches Leitkonzept
EU und Österreich sollen strategische Autonomie ausdrücklich als zentrale Voraussetzung für Souveränität und Überlebensfähigkeit in einer von Krisen, geopolitischen Spannungen und technologischen Umbrüchen geprägten Welt verankern. Politik soll antizipativ, entschlossen, kohärent, win-win-orientiert und realistisch agieren und alle relevanten Instrumente – von Regulierung über Investitionen bis zur Außen- und Sicherheitspolitik – auf dieses Ziel ausrichten.

Quantentechnologien
Österreich soll einen nationalen Quantenaktionsplan mit klaren Kooperationsrahmen, Investitionsschwerpunkten und technologischen Fokusfeldern ausarbeiten und sich aktiv an der Ausgestaltung einer EU-weiten Quantum-Agenda beteiligen. Es wird empfohlen, das Quantenökosystem in sicherheitskritische Komponenten mit nationaler Kontrolle, europäische Souveränitätsbereiche und Felder globaler Kooperation (z.B. im Rahmen der UNO) zu differenzieren und entsprechend zu priorisieren.

Künstliche Intelligenz
Auf Basis der KI-Strategie sollen Umsetzung und Skalierung beschleunigt werden, mit Fokus auf KI-Adoption durch KMU, Integration von Risikoanalysen strategischer Autonomie und enger Verzahnung mit EU-Zielen. Empfohlen werden substanzielle nationale und europäische Mittel für die KI-Transformation, aktive Mitgestaltung europäischer Datenräume und globaler Datenstandards sowie eine praxisnahe, innovationsfreundliche, wertbasierte KI-Regulierung im Sinne des digitalen Humanismus.

FTI-Ausschreibungen sollen klare, verbindliche Souveränitätsziele definieren; Abhängigkeiten sind als Teil des Risikomanagements systematisch zu erfassen, insbesondere Lizenzmodelle, Cloud-Abhängigkeiten und Datenzugänge. Vorgeschlagen werden mehrjährige thematische Calls zur Sicherung von Kontinuität, strengere Souveränitätsanforderungen für höhere TRL-Stufen und KET-Projekte, einfache, projektbezogene Metriken mit Schwerpunkt auf der Nutzungsphase sowie gegebenenfalls ein zweckklar definiertes Monitoring von Abhängigkeiten im Projektverlauf.

Summary

This final report describes the three-year project "Technological Sovereignty in a European Context," which explores Austria's contribution to European strategic autonomy—particularly about to key digital technologies—and develops implementable instruments for R&D policies. The focus is on clarifying the concept of technological sovereignty, establishing a set of indicators for R&D projects, facilitating dialogue-oriented events, and providing concrete recommendations for the EU and Austria.

In the project, technological sovereignty was defined as the ability to develop or acquire critical technologies without one-sided structural dependencies and without striving for autarky. Sub-aspects such as knowledge, research, development, production, operation, use, data, platform, and transparency sovereignty were identified to enable the systematic analysis of R&D projects.

A guiding-question-based framework for the self-assessment of technology sovereignty in R&D projects was developed. This framework captures dependencies by category (hardware, software, data, infrastructure, knowledge, legal/organizational factors) as well as mitigation strategies (monitoring, alternative technologies, alternative sources of supply, organizational measures, partnerships). This framework was tested in two FFG calls for proposals and revealed typical dependencies (e.g., AI components, cloud services, specialized software, implicit expert knowledge), but also underestimations, for example, regarding non-EU clouds and licensing risks.

The project organized several public events and workshops, including a kick-off discussion at IMAGINE 2023, two workshops with FFG project participants, an indicators workshop, and a closing event at IMAGINE 2025. These formats served to refine the concept of technological sovereignty, incorporate project perspectives, evaluate experiences with the indicators, and discuss Austria's role in the European sovereignty discourse.

In addition, the development and use of the terms strategic autonomy, resilience, and economic security in the EU, the legal and political foundations, and the special significance of AI and quantum technologies as key strategic technologies for Europe were examined. The report shows that, despite a strong research base in quantum technology

and a comprehensive AI regulatory framework, the EU lags significantly behind the US and China in terms of infrastructure, investment, and market power.

Recommendations: Strategic Autonomy as a Guiding Political Principle
The EU and Austria should explicitly enshrine strategic autonomy as a central prerequisite for sovereignty and viability in a world characterized by crises, geopolitical tensions, and technological upheavals. Policy should be proactive, decisive, coherent, win-win, and realistic, aligning all relevant instruments—from regulation and investment to foreign and security policy—with this goal.

Quantum Technologies
Austria should develop a national quantum action plan with clear cooperation frameworks, investment priorities, and technological focus areas, and actively participate in shaping an EU-wide quantum agenda. It is recommended that the quantum ecosystem be differentiated into security-critical components under national control, areas of European sovereignty, and fields of global cooperation (e.g., within the framework of the UN), and prioritized accordingly.

Artificial Intelligence
Based on the AI strategy “AI Mission Austria 2030,” implementation and scaling are to be accelerated, with a focus on AI adoption by SMEs, integration of strategic autonomy risk analyses, and close alignment with EU objectives. Substantial national and European funding for AI transformation, active participation in shaping European data spaces and global data standards, and practical, innovation-friendly, value-based AI regulation in line with digital humanism are recommended.

FTI Funding Practices and Indicators
Calls for proposals should define clear, binding sovereignty objectives; dependencies must be systematically recorded as part of risk management, in particular licensing models, cloud dependencies, and data access. Multi-year thematic calls are proposed to ensure continuity, along with stricter sovereignty requirements for higher TRL levels and KET projects, simple, project-related metrics focusing on the usage phase, and, where appropriate, clearly defined monitoring of dependencies throughout the project.

Einführung

Übersicht über das Projekt und Technologiesouveränität

Technologiesouveränität lässt sich als die Fähigkeit definieren, jene Technologien ohne einseitige strukturelle Abhängigkeit zu entwickeln oder zu beziehen, die als kritisch für Wohlfahrt, Wettbewerbsfähigkeit und Handlungsfähigkeit angesehen werden. Dabei bedeutet Souveränität nicht Autarkie oder vollständige Autonomie, sondern jene Selbstbestimmung, die den eigenen Ansprüchen genügt. Dieser Endbericht beschreibt die Aktivitäten und erbrachten Leistungen im Rahmen des Projekts „Technologiesouveränität im europäischen Kontext“ vom März 2023 bis Februar 2026.

Die gemäß Ausschreibung zu erbringenden Leistungen im Projekt waren

(i) sechs interaktive Veranstaltungsformate
(ii) eine inhaltliche Aufbereitung des Themas
(iii) die Erstellung einer Vorlage zur (Selbst-)Einschätzung der Technologiesouveränität von F&E-Projekten inkl. Indikatoren, sowie
(iv) ein Endbericht.

Diese Projektziele wurden in vollem Umfang erreicht. In Abweichung vom ursprünglichen Projektplan wurde die Arbeit an den Indikatoren zur Technologiesouveränität in FTI-Projekten vorgezogen. Diese Änderung erfolgte mit dem Ziel, Erfahrungen mit den Indikatoren in Ausschreibungen der FFG zu sammeln.

Begriffliche Klärung

Anlässe für die Forderung nach verbesserter europäischer Technologiesouveränität gab es zuletzt viele. Sie reichen von Fällen der versuchten Wahlbeeinflussung durch internationale Akteure über die Diskurskontrolle in online Netzwerken bis zur Störung von Lieferketten und der Verknappung für die Technologieproduktion wichtiger Komponenten und Rohstoffe. Auch Coronakrise und Ukrainekrieg haben die europäische Abhängigkeit von internationalen Technologieplattformen und IT-Konzernen verdeutlicht, z.B. in der

Gestaltung von Corona-Tracing Apps (Kuipers 2020) oder von Virenschutzsoftware. Aus diesem Grund hat die Diskussion zum Thema Technologiesouveränität und insbesondere zur digitalen Souveränität in der europäischen Debatte stark an Bedeutung gewonnen. Allerdings bedarf der Begriff der Souveränität auch einiger Klärung. Ursprünglich war damit bloß staatliche Souveränität verbunden, d.h. die Unabhängigkeit eines Souveräns von anderen. Damit war das Konzept stark mit Territorialität verbunden und mutet schon aus diesem Grund im Digitalen fallweise etwas paradox an. Der Begriff kann aber auch auf individueller Ebene als „Eigentum an sich selbst" verstanden werden, d.h. als Hoheit über sich selbst, z.B. am Körper, an Entscheidungen oder an den eigenen Daten. Zuletzt tauchen sowohl Souveränität als auch strategische Autonomie vermehrt in den europäischen Debatten über die eigene Entscheidungsfähigkeit und in geopolitischen und militärischen Diskursen auf.

Technologiesouveränität kann in verschiedene Teilaspekte gegliedert werden, was vor allem aus F&E-Sicht nützlich ist (vgl. Edler et al. 2020):

- Wissenssouveränität: Zugang zu Informationen (Anwendung, Nutzung, Betrieb von Digitaltechnologien), Fähigkeit zur Bewertung, Verfügbarkeit von Expert:innen
- Forschungssouveränität: Entscheidungsfreiheit über Forschungsgegenstand, Zugang zu Ressourcen (Rohstoffe, Anlagen, Daten, Algorithmen, Softwarewerkzeugen, Hochleistungsrechner etc.), internationaler Austausch und Zusammenarbeit
- Entwicklungssouveränität: Freiheit in der Gestaltung von Produkten und Diensten, Zugang zu Ressourcen (z.B. Prototypen, Schnittstellen, Software, Hardware, Werkzeuge und Bibliotheken), Verfügbarkeit von Kenntnissen, Anpassung an eigene Anforderungen
- Produktionssouveränität: Zugang zu Ressourcen für die Fertigung (z.B. Rohstoffe, Komponenten, Werkzeuge, Anlagen)
- Betriebssouveränität: Freiheit, den Betrieb von Systemen nach eigenem Gutdünken zu gestalten, Zugang zu Ressourcen und Fähigkeiten, Überprüfbarkeit und Bewertbarkeit
- Nutzungssouveränität: Freiheit in der Nutzung (z.B. auch von Ergebnissen), Rechtssicherheit
- Transparenzsouveränität: Möglichkeit der Überprüfung und Korrektur (z.B. von Systemen), Nachvollziehbarkeit
- Datensouveränität: Informationsrechte über Daten und ihre Verwendung, Verfügungs- und Nutzungsmöglichkeiten an Daten inklusive Wertschöpfungsmöglichkeit, Ausschließungsrechte der Datennutzung für Dritte

- Plattformsouveränität: Möglichkeit digitale Handels-, Kommunikations- oder Dienste-Plattformen zu schaffen, zu nutzen und zu regulieren

Vorschlag Indikatoren

Der im Folgenden beschriebe Vorschlag zur Selbstbestimmung der Beiträge eines FTI-Projekts zur Technologiesouveränität wurde anhand von Beiträgen aus der Literatur sowie als Ergebnis von Diskussionen mit Forschungsprojektteilnehmenden erarbeitet. Die Indikatoren werden über Leitfragen ermittelt. Diese sollen von den Projekteinreichenden in einem Formular erfasst werden, um so einerseits eigene Beiträge der Projekte zur Technologiesouveränität, aber auch wichtige Abhängigkeiten des Projekts oder der Ergebnisse zu erfassen. Diese Leitfragen sind:

- Was sind die jeweils 3 wichtigsten (kritischen) technologischen Abhängigkeiten ihres Projekts in Bezug auf die hier angeführten Kategorien?
  - Hardware, Software, Daten
  - (F&E-)Infrastruktur
  - Wissen, rechtliche und organisatorische Abh.
- Gibt es für die angegebenen Abhängigkeiten Ersatztechnologien, alternative Bezugsquellen, Frühwarnmöglichkeiten oder Möglichkeiten der Verlängerung des Einsatzes älterer Systeme?
- Welche (externen) Abhängigkeiten bestehen bei der Nutzung des Projektergebnisses?
- Wie kann die Technologieabhängigkeit bei der Ergebnisnutzung reduziert werden?

Eine weitere Leitfrage dient der Erfassung des Beitrags des Projekts zu Schlüsseltechnologien (Key Enabling Technologies, KETs):

- Welcher Beitrag erfolgt für KETs und strategisch wichtige Technologien: neue Abhängigkeit oder reduzierte Abhängigkeit?

Damit ergibt sich das folgende Schema:

- Forschung und Technologieentwicklung
  - Abhängigkeiten
    - HW, SW, Daten
    - Infrastruktur
    - Wissen, rechtliche, organisatorische Abh.

  - Mitigation
    - Monitoring, Vorwarnung
    - Ersatztechnologie, alternative Quellen, Einsatzverlängerung
    - Organisatorische Maßnahmen, Partnerschaften
- Betrieb/Nutzung
  - Abhängigkeit
    - HW, SW, Daten
    - Infrastruktur
    - Wissen, rechtliche, organisatorische Abh.
    - IPR, Verträge, Terms of Use
  - Mitigation
    - Monitoring, Vorwarnung
    - Ersatztechnologie, alternative Quellen, Einsatzverlängerung
    - Organisatorische Maßnahmen, Partnerschaften

Der Test dieser Leitfragen in zwei FFG-Ausschreibungen führte zur Identifikation wichtiger Abhängigkeiten der Projekte. Genannt wurden u.a. KI-Komponenten, Daten, Abhängigkeiten von Spezialsoftware (etwa im Bereich Echtzeitsysteme), von Cloud-Services, aber auch Wissensabhängigkeiten von speziellen Expert:innen bei undokumentiertem Knowhow uvm.

Insgesamt wurden die Leitfragen und Kategorien von Abhängigkeiten sowie Mitigationsstrategien gut verstanden und zufriedenstellend beantwortet und erschienen handhabbar. Manchmal fehlte ein Grund für kritische Abhängigkeiten (z. B. von wem, welchem Land, einzelne Quelle usw.) Einige Projekte haben der Liste der Kategorien organisatorische und rechtliche Abhängigkeiten hinzugefügt. Die benutzte Unterscheidung zwischen Projektphase, Bereitstellung bzw. Nutzung ist relevant und sollte beibehalten werden. Probleme mit nicht-EU Cloud-Anbietern (Datenschutz, DSGVO usw.) wurden tendenziell unterschätzt.

Die Strategien zur Risikominimierung reichten von technischen über organisatorische Ansätze bis hin zu Aus- und Weiterbildungsmaßnahmen und erweiterten Partnerschaften. Erwartungsgemäß stellten offene Standards, die Erweiterung älterer Systeme und der Rückgriff auf Standardprodukte wichtige Strategien zur Verbesserung der Technologiesouveränität dar. Teilweise wurden auch redundante Systeme, aktive Auseinandersetzung mit Regularien und neue Partnerschaften mit lokalen Herstellern oder Universitäten erwähnt.

Veranstaltungen

Die Veranstaltungen dienten einerseits dem Ziel, das Thema Technologiesouveränität in einer breiteren Öffentlichkeit – aber auch innerhalb des FTI-Umfelds – zu verankern bzw. Maßnahmen sowie die vorgeschlagenen Indikatoren zu diskutieren. Folgende Veranstaltungen wurden durchgeführt:

- Eine interaktive Veranstaltung für eine breitere Öffentlichkeit im Rahmen der IMAGINE am 15.6.2023
- Ein Workshop mit Teilnehmenden an FTI-Förderprojekten am 9.10. 2023
- Ein Workshop mit Teilnehmenden an FTI-Förderprojekten am 6.11.2023
- Workshop 4.9. 2024 im BMIMI
    - Auswertung der Abhängigkeitsanalyse aus der Ausschreibung
    - Vorschlag für ein Indikatorschema
- Workshop „Technologiesouveränität im Europäischen Kontext“ am 8.4.2025. Dieser widmete sich folgenden Themen:
    - Technologiesouveränität im Europäischen Kontext: Zum Stand der aktuellen Debatte und der Beitrag Österreichs
    - Schwerpunktfelder KI und Quantentechnologie
    - Technologiesouveränität in FTI-Projekten: Indikatoren und Rahmenbedingungen
- Eine öffentliche Abschlussveranstaltung im Rahmen der IMAGINE 2025.

Öffentliche Auftaktveranstaltung

Die erste öffentliche Veranstaltung wurde im Rahmen der IMAGINE am 15.6.2023 organisiert. Unter dem Programmpunkt „Paralleles Denken II“ fand eine Paneldiskussion von Expert:innen aus Forschung und Entwicklung sowie aus der strategischen Landesverteidigung unter Einbindung des Publikums statt.

Hauptziel der Diskussion war es, unterschiedliche Facetten des Begriffs „Technologiesouveränität“ mit einer breiteren Bevölkerung zu erläutern. Neben den Expert:innenmeinungen wurden auch Interpretationen des Begriffs vom Publikum gesammelt und diskutiert. Es fand eine angeregte Diskussion statt, wobei sowohl die Sicht

der angewandten Forschung als auch die verteidigungspolitischen Aspekte auf großes Interesse bei den Anwesenden stießen.

Workshops mit FTI-Projekten

Es wurden zwei Workshops mit Projektteilnehmenden von FFG-geförderten Projekten durchgeführt. Gemeinsames Ziel der beiden Workshops war es, den Begriff der technologischen Souveränität zu beleuchten. Der Schwerpunkt lag dabei auf der Betrachtung aus der Sicht geförderter Projekte in Programmen der FFG. Die einzelnen Projekte stellten sich kurz vor und präsentierten eigene Interpretationen bzw. Aspekte der Technologiesouveränität aus Projektsicht. Einige Projekte haben bei dieser Gelegenheit auch eigene Anregungen für die Aufnahme von Souveränitätsaspekten als zukünftige Förderprogrammelemente gegeben.

Die behandelten Themen im ersten Workshop waren überraschend breit. Sie reichten von internationaler Regulierung über Meinungssouveränität und Bildung bis zu AI in der Medizin, Energiesouveränität, Datensouveränität, Nachhaltigkeit und Mikroelektronik bis zu Vorschlägen für weitere Förderungen in Österreich. Es hat sich klar gezeigt, dass Technologiesouveränität für viele Unternehmen, aber auch für Forschende, ein wichtiges Thema darstellt, das bisher unzureichend diskutiert wurde. Die Abgrenzung gegenüber bzw. die Zusammenarbeit mit anderen europäischen Ländern und den Aktivitäten der Union wurde insgesamt als besonders wichtig erachtet. Zwar kann Österreich wichtige Beiträge liefern, aber nur Europa als Ganzes kann wesentliche Schritte zur gemeinsamen Technologiesouveränität setzen.

Der zweite Workshop widmete sich spezifischen Fragen der technologischen Souveränität. Diskutiert wurde u.a. über Technologieplattformen und die sich daraus ergebenden Abhängigkeiten, Portabilität von Programmen und Daten, Elektronik, Energie (Effizienz) uvm. Es wurde diskutiert, dass Europa noch immer eine hohe Wissenssouveränität besitzt, Produktion und auch Services (Plattformen) jedoch oft außerhalb Europas angesiedelt sind. Es wurde u.a. vorgeschlagen, dass sich Österreich auf die spezifischen Stärkefelder konzentriert. Auch eine genaue Zielvorstellung ist zu entwickeln, das bedeutet zum Beispiel gegen welche Art von Turbulenz man sich absichern möchte oder auch welche Art von Abhängigkeit eher zu akzeptieren sein wird. Technologie kann als Querschnittsthema gesehen werden und mit gezielten Ausschreibungen gut adressiert werden.

Einschätzung der Technologiesouveränität in FTI-Projekten

Die Ergebnisse und Erfahrungen mit der Selbsteinschätzung der Technologiesouveränität aus den Einreichungen zur Ausschreibung wurden in einem Workshop diskutiert. Im Workshop wurde betont, dass eine präzise Zielbestimmung für Technologiesouveränität in F&E-Projekten entscheidend ist. Projekte benötigen klare Vorgaben, welche Abhängigkeiten relevant sind und welche Souveränitätsziele erreicht werden sollen. Abhängigkeiten werden dabei zunehmend als Risiken verstanden, die auch im Rahmen des Risikomanagements abgebildet werden können. Diskutiert wurde, inwiefern Standardsoftware und -hardware als vernachlässigbare oder relevante Abhängigkeiten gelten, da sie in vielen Projekten unvermeidlich, in manchen jedoch kritisch sind.

Besonders hervorgehoben wurde die Lizenzproblematik in der Nutzungsphase: Lizenzkosten, Änderungen von Lizenzbedingungen und Mietmodelle können die Nachnutzbarkeit erheblich gefährden – auch innerhalb Europas. Aufgrund digitaler Geschäftsmodelle steigt diese Abhängigkeit weiter an. Als Gegenmaßnahme wurde Portabilität diskutiert, die jedoch häufig zusätzliche Kosten verursacht. Auch die Weiterentwicklung bestehender Prototypen zur Reduktion von Abhängigkeiten ist finanziell schwierig.

Ein zentrales Problem ist der Mangel an Kontinuität zwischen Projekten, obwohl gerade langfristig stabile Umgebungen und Kompatibilitäten wichtig wären. Vorgeschlagen wurde daher, Technologiesouveränität über mehrjährige, thematisch fokussierte Calls zu fördern. Zudem wurde betont, dass in frühen F&E-Phasen Abhängigkeiten eher akzeptabel sind, während mit steigenden TRLs mehr Augenmerk auf Abhängigkeitsanalysen gelegt werden sollte.

Die getesteten Indikatoren wurden grundsätzlich als gut verständlich bewertet. Es fehlen jedoch projektbezogene Metriken, während nationale Ansätze in der Literatur existieren. Für Projekte in Key Enabling Technologies (KETs) könnten höhere Souveränitätsanforderungen sinnvoll sein. Auch die Frage, ob Abhängigkeiten während

des Projektverlaufs berichtet werden sollen, wurde diskutiert. Voraussetzung für jede Form von Monitoring ist aber eine klare Definition des Zwecks und der erwarteten Maßnahmen.

Große Bedeutung wird der Verfügbarkeit von Daten zugeschrieben, da oft auf internationale Quellen zurückgegriffen werden muss. Österreich sollte hier stärker in Datenbereitstellung und -zugang investieren. Abschließend wurde betont, dass die Indikatoren relevant sind, aber einfach beantwortbar sein sollten und die Nutzungsphase stärker gewichtet werden müsse. Entscheidend ist eine klare Kommunikation der politischen Erwartungen.

Zentrale Empfehlungen

- Klare und verbindliche Zieldefinition für Technologiesouveränität in Ausschreibungen
- Abhängigkeiten als Teil des Risikomanagements erfassen, nicht nur in Indikatoren
- Lizenzen und Software-Mietmodelle als kritische Abhängigkeiten systematisch berücksichtigen
- Portabilität fördern, inklusive Finanzierung zusätzlicher Entwicklungsaufwände
- Kontinuität über mehrere Projekte sicherstellen, z.B. durch thematische Multi-Projekt-Calls
- Für höhere TRLs strengere Souveränitätsanforderungen formulieren
- Entwicklung projektbezogener Metriken zur Technologiesouveränität vorantreiben
- Für KET-Projekte höhere Souveränitätsziele bzw. keine Einführung neuer Abhängigkeiten vorsehen
- Mögliches Monitoring von Abhängigkeiten während des Projektverlaufs – aber nur bei klar definiertem Zweck
- Datenverfügbarkeit in Österreich verbessern, um Abhängigkeiten von internationalen Quellen zu reduzieren
- Indikatoren einfach handhabbar machen und den Fokus stärker auf die Nutzungsphase legen.

Workshop Technologiesouveränität im EU-Kontext

Ein Workshop zum Thema der Indikatoren mit Bezug auf die Technologiesouveränität im Europäischen Kontext“ fand am 8.4.2025 im BMIMI statt. Dieser widmete sich folgenden Themen:

- Technologiesouveränität im Europäischen Kontext: Zum Stand der aktuellen Debatte und der Beitrag Österreichs
- Schwerpunktfelder KI und Quantentechnologie
- Technologiesouveränität in FTI-Projekten: Indikatoren und Rahmenbedingungen

Der Workshop diente der Präsentation und Diskussion der Empfehlungen zu möglichen österreichischen Beiträgen zur europäischen Souveränität (siehe unten). Diese Empfehlungen wurden von den Workshop-Teilnehmenden positiv aufgenommen.

Abschlussveranstaltung im Rahmen der IMAGINE 2025

Ein multidisziplinäres Panel diskutierte im Rahmen der IMAGINE 2025 verschiedene Aspekte der digitalen Souveränität, vor allem die rechtlichen, technischen, wirtschaftlichen und gesellschaftlichen Dimensionen. Souveränität wurde im Lauf der Diskussion als praktische Kontrolle, Resilienz und legitime Autorität im Einklang mit lokalen Werten und Gesetzen (z. B. DSGVO) definiert. Sie kann durch diversifizierte Abhängigkeiten, transparente Lieferketten, durchsetzbare internationale Verträge und die Akzeptanz durch die Öffentlichkeit erreicht werden. Im Mittelpunkt der Debatte standen die Grenzen der territorialen Kontrolle über globale Daten und Plattformen, die Rolle der EU im Vergleich zu nationalen Akteuren, partizipative Ethik (einschließlich der Einbeziehung junger Menschen) und die Umwandlung technologischer Stärken in wirtschaftliche und politische Macht.

Die Expert:innen debattierten auch konkrete Lösungsansätze. Dazu gehörten eine Governance in Verbindung mit Allianzen (z.B. strategischen Technologiepartnern), offene Wissens- und Haftungsstandards, nationale digitale Infrastrukturen und Vorbildprojekte, wertorientierte Beschaffung sowie Innovationsumgebungen zur Beschleunigung der Implementierung. (Siehe hierzu auch die abschließenden Empfehlungen weiter unten.)

Europäische Souveränität und Österreichs Beitrag[1]

Auf europäischer Ebene hat sich der Diskurs zuletzt verstärkt dem Begriff der strategischen Autonomie zugewandt. Mit strategischer Autonomie ist die Fähigkeit gemeint, über jene Kapazitäten und Kontrolle zu verfügen, die es einem Staat oder der EU als ganze ermöglichen, in zentralen Fragen von Wirtschaft, Gesellschaft und Demokratie eigenständig über die eigene Zukunft zu entscheiden und zu handeln. Sie dient damit der Verteidigung und Stärkung staatlicher Souveränität. Strategische Autonomie bedeutet, wie bereits erwähnt, nicht Autarkie oder völlige Selbstversorgung, sondern ein aktives Management von Risiken, der Aufbau widerstandsfähiger Interdependenzen sowie strategische Partnerschaften und Multilateralismus, damit externe Abhängigkeiten nicht zu Souveränitätsrisiken werden. Die EU steht vor einer existenziellen Wettbewerbs- und Sicherheitskrise. Die Stärkung der strategischen Autonomie ist – insbesondere bei digitalen Schlüsseltechnologien wie Quantentechnologie und KI – für EU und Österreich essenziell und dringend.

Begriff und Entwicklung der strategischen Autonomie

Zunächst ist das Verhältnis von Souveränität, Resilienz, wirtschaftlicher Sicherheit und strategischer Autonomie zu klären. Souveränität wird in grundlegende (Macht), territoriale (physische und digitale Vermögenswerte) und institutionelle (Organisation von Wirtschaft, Gesellschaft und Demokratie) Dimensionen unterteilt und beruht auf innerer wie äußerer Legitimität. Strategische Autonomie wird als Mittel zur Verwirklichung von Souveränität verstanden: Sie ist die messbare Fähigkeit, in für die Zukunft eines Landes oder der EU wesentlichen Bereichen zu wissen (Fähigkeiten), zu produzieren bzw. zu handeln (Kapazitäten) und zu entscheiden (Kontrolle). Resilienz ist die Fähigkeit, Schocks zu verkraften und sich davon zu erholen, während wirtschaftliche Sicherheit auf den Abbau riskanter Abhängigkeiten, den Aufbau eigener Kapazitäten und deren Ergänzung durch vertrauenswürdige Partnerschaften zielt. Resilienz ist damit eine notwendige, aber nicht hinreichende Bedingung für wirtschaftliche Sicherheit; wirtschaftliche Sicherheit

[1] Siehe für Details zu diesem Abschnitt die im Anhang angefügte Arbeit von Paul Timmers.

wiederum ist eine notwendige, aber nicht hinreichende Bedingung für strategische Autonomie, die auch nationale Sicherheit und demokratische Werte umfasst. Strategische Autonomie kann über vier Hauptstrategien verfolgt werden: Autarkie (realistisch nur für sehr große Mächte), Risikomanagement, strategische Partnerschaften mit Gleichgesinnten sowie weitergehende globale Kooperation jenseits eines engen Souveränitätsverständnisses.

Die Entwicklung des Begriffs in der EU erfolgte von einem primär militärischen Konzept (vor allem in Frankreich seit dem Zweiten Weltkrieg) hin zu einer breiten wirtschafts- und technologiepolitischen Agenda. Ab 2016 gewann der Begriff unter Präsident Macron, vor dem Hintergrund der Abhängigkeit von US- und chinesischen Tech-Konzernen, der Snowden-Enthüllungen und wachsender Sorgen über Cyber-Spionage, in der EU-Debatte an Gewicht. Viele Mitgliedstaaten standen Begriffen wie „Souveränität" und „strategische Autonomie" zunächst skeptisch gegenüber und sahen darin Protektionismus oder „Colbertismus", woraus der weichere Begriff der „offenen strategischen Autonomie" entstand, der Multilateralismus und regelbasierte Kooperation betont, zugleich aber die Fähigkeit zum eigenständigen Handeln bewahren will.

Eine Reihe von Krisen trieb die Agenda voran: US-Druck in der 5G-Sicherheitsfrage, die COVID-19-Pandemie und Lieferkettenstörungen, Russlands Invasion in der Ukraine sowie die verschärfte Rivalität zwischen USA und China. Diese Entwicklungen hoben Resilienz und wirtschaftliche Sicherheit auf die politische Spitzenagenda und führten dazu, dass die EU kritische Rohstoffe, Energie und „kritische Technologien" identifizierte, die „gefördert, geschützt und mit Partnern entwickelt" werden sollen. Der politische Widerstand gegen „europäische Souveränität" habe dabei abgenommen: Wurde Junckers „Stunde der europäischen Souveränität" 2018 stark kritisiert,[2] sei die Prag-Rede von Scholz 2022,[3] die sich ausführlich auf europäische Souveränität stützte, weitgehend positiv aufgenommen worden. Wichtige Entwicklungen sind u.a. die zweite Trump-Präsidentschaft mit transaktionaler, ökonomisch koerziver „America-First"-Politik in enger Verbindung mit US-Big-Tech, zunehmende chinesische Selbstbehauptung, mögliche künftige Konflikte (Taiwan, weitere russische Aggression) sowie innereuropäische Risiken durch illiberale, autoritäre Regierungen. Zusammen mit der schwachen Wettbewerbs- und Innovationslage machen dies strategische Autonomie zu einer zentralen Überlebensfrage für die EU.

[2] J.-C. Juncker, Rede zur Lage der Union, 12.9.2018, EU-Parlament, Straßburg.
[3] O. Scholz, Rede „Europa ist unsere Zukunft", 29.8.2022, Karls Universität, Prag.

EU-Recht, Politik und digitale Technologien

Rechtlich gibt es in der EU keine formale Definition von „strategischer Autonomie“, obwohl der Begriff in Politik- und Rechtsdokumenten immer häufiger auftaucht. Es gibt Beispiele aus der Raumfahrtpolitik, Cybersicherheitsstrategien, Horizon Europe und der Resilienz-Gesetzgebung, in denen der Begriff in unterschiedlichen Formulierungen mit „technologischer Souveränität“, Wettbewerbsfähigkeit oder „offener strategischer Autonomie“ verbunden wird. Auffällig ist, dass weder das KI-Gesetz (AI Act) noch der koordinierte KI-Aktionsplan ausdrücklich auf strategische Autonomie oder Souveränität Bezug nehmen. Dies kann als eine verpasste Chance gesehen werden, die Verbindung zwischen KI und Autonomie klar herauszustellen.

Im Bereich der digitalen Technologien war zuletzt häufig von einen mehrschichtigen „Stack“ (von Hardware und Infrastruktur über Plattformen und Daten bis hin zu Anwendungen) die Rede. Europa ist mit Ausnahme des Netzbereichs in den meisten Schichten relativ schwach aufgestellt. Da digitale Technologien jedoch kritische Infrastrukturen, wirtschaftliche Aktivitäten und Sicherheit durchdringen, sind sie zum zentralen Schauplatz strategischer Autonomie geworden. Unter den vielen relevanten Technologien stechen aber Quantentechnologie und Künstliche Intelligenz als für die EU insgesamt und für Österreich besonders relevant hervor.

Quantentechnologien und europäische Autonomie

Quantentechnologien – Sensorik, Kommunikation, Computing und Post-Quanten-Kryptografie – werden in EU-Erklärungen explizit als strategisch wichtig für die europäische Souveränität bezeichnet. Die 2023 von 26 Mitgliedstaaten, darunter Österreich, unterzeichnete Europäische Erklärung zu Quantentechnologien hebt hervor, dass der wirtschaftliche und strategische Wert von Quanten sie zu einer Priorität für die Souveränität der EU macht.

Bei den öffentlichen Investitionen liegt die EU laut Studie hinter China an zweiter Stelle; wesentliche Programme laufen in Frankreich, Deutschland, im Rahmen der EU-Quantum-Flagship-Initiative und in den Niederlanden, während Österreich mit rund 107 Mio. Euro deutlich weniger investiert als etwa die Niederlande mit 965 Mio. Euro. Europa verfügt über eine starke wissenschaftliche Basis, etwa durch österreichische Beiträge (z.B. Zeilingers Arbeiten), die die Quantenkommunikation geprägt haben, doch

bei der praktischen Umsetzung führe China, etwa mit einer 2.032 km langen QKD-Glasfaserstrecke zwischen Peking und Shanghai. EU-Initiativen wie die European Quantum Communication Infrastructure (EuroQCI) und ihre Einbindung in das Satellitenprogramm IRIS2 sollen sichere Quantenkommunikationskapazitäten aufbauen, die insbesondere für Regierungs- und kritische Infrastrukturkommunikation zentral sind.

Die Einführung von Post-Quanten-Kryptografie in Europa drängt, weil künftige Quantencomputer weit verbreitete heutige Verschlüsselungsverfahren brechen können und bereits heute abgegriffene Daten später entschlüsselt werden könnten. Das US-Normungsinstitut NIST habe bereits mehrere PQC-Standards verabschiedet und zeige damit, wie Früheinsteiger globale Standards und Ökosysteme prägen. Trotz beachtlicher europäischer Forschungsinvestitionen und Industrieinitiativen wie dem 167 Mitglieder starken Quantum Industry Consortium leidet die EU an einer schwachen Verzahnung von Forschung und Markteinführung, fragmentierter Nachfrage, fehlender gemeinsamer Vision für Quantencomputing bis 2030 und an einer mangelnden Strategie zur Verhinderung interner Marktfragmentierung bei Quantenprodukten und -diensten. Abhängigkeiten von kritischen Materialien und Präzisionskomponenten sind zusätzliche strategische Schwachstellen, und die EU habe bislang keine klare internationale Position formuliert, obwohl die UNO 2025 zum „International Year of Quantum Science and Technology“ erklärt hat.

Europa sollte daher bei sicherheitskritischen Quantenkomponenten (etwa bestimmten QKD-Systemen und sicheren Quanten-Hardwaremodulen) exklusive Kontrolle anstreben, während in anderen Feldern gegenseitige Interdependenzen und offene Zusammenarbeit mit gleichgesinnten Partnern (z.B. Großbritannien, Schweiz) sinnvoll sind. Globale Quantengovernance, etwa auf UN-Ebene, sei eine Chance, europäische strategische Interessen mit gemeinwohlorientierten Zielen zu verbinden.

Künstliche Intelligenz und Verwundbarkeit der EU

Auch wenn die EU-Politik zum Thema KI selten den Begriff Souveränität verwendet, bestehen weitreichende Implikationen für die strategische Autonomie, da KI wirtschaftliche Macht, Sicherheitsfähigkeiten und gesellschaftliche Ordnungsmodelle stark prägen wird. Formal verfügt die EU über einen beeindruckenden Rahmen: die KI-Regulierung, einen koordinierten KI-Aktionsplan, umfangreiche Investitionen in Supercomputing-Infrastruktur für KI, Initiativen wie „AI-Fabriken“, eine „AI Kontinent

Initiative“ sowie Daten- und KI-Strategien. Sie besitzt zudem regulatorische Stärke im Datenbereich (Data Act, Data Governance Act), baut Gemeinsame Europäische Datenräume und industrielle Datenökosysteme wie Catena-X auf und fördert industrielle Digitale Zwillinge, etwa bei Verbund in Österreich im Bereich Wasserkraft.

Die Investitionszahlen und Marktstrukturen offenbaren jedoch eine gravierende strategische Schwäche. 2023 beliefen sich private KI-Investitionen in den USA auf rund 62,5 Mrd. Euro, in China auf 7,3 Mrd. Euro und in der EU plus Großbritannien zusammen auf nur 9 Mrd. Euro. Der globale KI-Markt soll stark wachsen, doch die wesentlichen Akteure sind eine Handvoll großer US-Konzerne (OpenAI, Microsoft, Google, Meta, Apple, Nvidia, xAI), von denen viele eine durchgängige Kontrolle der KI-Wertschöpfungskette anstreben – von Chips und Rechenzentren über Cloud und Netze bis hin zu Endnutzer-Applikationen. Europa hat einige bemerkenswerte KI-Start-ups (z.B. Mistral, Aleph Alpha) und akademisches Talent, verfügt aber kaum über skalengleiche Akteure in der Generativen KI und liegt bei Infrastruktur, Investitionen, Patenten, KI-Nutzung und Talentbindung deutlich zurück.

Nur etwa 8% der EU-Unternehmen setzten bislang KI ein, und die EU erlebt einen erheblichen Brain-Drain von KI-Promovierten in die USA, was die künftige Leistungsfähigkeit schwächt – auch wenn es fallweise jüngst wieder Gegenbewegungen gab. Gleichzeitig agieren andere Mächte aggressiv: In den USA wurden zu Beginn der zweiten Trump-Amtszeit massive KI-Infrastrukturinvestitionen angekündigt und Aktivitäten zur Regulierung von KI-Risiken durch die Aufhebung von Bidens KI-Erlass zurückgefahren, während China bei Generativer KI zügige Fortschritte mit leistungsfähigen und kosteneffizienten Modellen verzeichne. Ohne souveränitätspolitische Perspektive läuft Europa Gefahr, in der KI zum „Sitting Duck“ zu werden: Die wirtschaftliche Transformation würde anderswo gestaltet, sodass die EU Abhängigkeit von fremden Regierungen und Tech-Konzernen bei Kerninfrastrukturen und KI-Anwendungen hinnehmen müsste.

Diese Abhängigkeit ist geeignet, nicht nur die Wettbewerbsfähigkeit zu schwächen, sondern gefährdet auch die Fähigkeit Europas, eigene Werte – Demokratie, Grundrechte, aufklärerische Prinzipien und „Digital Humanism“ – in der KI-Praxis zu verankern. Wenn Architektur, Plattformen und Spielregeln der KI in Washington, Silicon Valley oder Peking definiert werden, droht der praktische Einfluss von Instrumenten wie dem KI-Gesetz und ethischen Rahmenwerken etwa der UNESCO zu sinken.

Gesamtfazit und politische Leitprinzipien

Die EU steht vor einer existenziellen Krise, die durch disruptive Geopolitik (Kriege, Sanktionen, Handelskriege, Abhängigkeit von militärischer Durchsetzungsmacht), technologische Umbrüche (KI, Quanten, Satellitensysteme), der Erosion von Multilateralismus und Völkerrecht sowie innerem demokratischen Rückbau geprägt ist. Zur Bewältigung ist ein Schwenk in der EU von reaktiver Krisenpolitik zu proaktiver, chancenorientierter strategischer Autonomie nötig, insbesondere in Schlüsseltechnologien. Fünf Leitprinzipien sollten EU- und nationale Politik steuern:

- Antizipativ und proaktiv: Politik soll technologische und geopolitische Verschiebungen antizipieren, bzw. rechtzeitig erkennen, statt verspätet zu reagieren und dabei technologie-, geopolitik- und gesellschaftssensibel sein.
- Entschlossen und schnell: Angesichts der Geschwindigkeit globaler Rivalen braucht es politische Führung und zügige Entscheidungen sowie Umsetzung.
- Umfassend und kohärent: Alle Instrumente – Regulierung, Investitionen, Handel, Arbeitsmarkt-, Industrie-, Innen- und Außenpolitik – müssen konsistent auf die Ziele strategischer Autonomie ausgerichtet werden.
- Win-win-orientiert und interdependent: Gegenseitige, vorteilhafte Interdependenzen mit Partnern sollen gemeinsame Werte und Interessen stärken und die Weaponisierung von Abhängigkeiten erschweren.
- Realistisch und flexibel: Die EU kann nicht in allen Technologien führen; sie muss priorisieren und wertorientierte Ambitionen mit pragmatischen Kompromissen verbinden.

EU- und nationale Souveränität sind kein Nullsummenspiel sind: Geteilte und gebündelte Souveränität könne einen dreifachen „Gewinn“ erzeugen – mehr nationale Resilienz gegenüber globalen Herausforderungen, EU-weite souveräne Vermögenswerte (z.B. .eu-Domain) und größere externe Legitimität durch gemeinsame Fähigkeiten.

Empfehlungen für EU und Österreich

Die folgenden Empfehlungen betreffen sowohl die strategische Autonomie im Allgemeinen als auch speziell Quantentechnologie und KI, mit Augenmerk auf Österreichs Rolle in der Union.

Zur strategischen Autonomie insgesamt ist zu empfehlen, dass EU und Österreich die Stärkung strategischer Autonomie explizit als für Souveränität und Überleben zentral anerkennen. Sie sollten ihre Bereitschaft zur Zusammenarbeit mit allen Akteuren betonen, die das Recht der EU respektieren, eigenständig zu entscheiden und zu handeln, und Wettbewerbsfähigkeit sowie Sicherheit im Einklang mit der EU-Agenda 2025–2029 und den Berichten von Draghi, Letta und Niinistö priorisieren.

Im Bereich der Quantentechnologien verfügt Österreich zwar über starke wissenschaftliche Grundlagen, aber als kleiner Akteur hat es nur begrenzte Investitions- und politische Hebel. Zu empfehlen ist daher:

- Ausarbeitung eines nationalen Quantenaktionsplans mit klaren Kooperationsrahmen, Investitionsschwerpunkten und technologischen Fokusfeldern.
- Aktive Mitgestaltung der kommenden EU-Quantum-Agenda und Eintreten für eine Bündelung und Skalierung nationaler und industrieller Initiativen auf europäischer Ebene.
- Klärung, welche Teile des Quantenökosystems (a) in die nationale Souveränität (wegen Kernsicherheitsinteressen), (b) in EU-Souveränität (mit dreifachem Gewinn) und (c) in globale Kooperation (z.B. Beiträge zum UN-Jahr der Quantenwissenschaft) fallen.

Für Künstliche Intelligenz liefert die österreichische KI-Strategie (AI Mission Austria 2030) eine solide Grundlage, weitere Maßnahmen und deren Beschleunigung sind aber wichtig:

- Beschleunigte und vertiefte nationale KI-Umsetzungspläne mit starkem Fokus auf KMU-Adoption, unter Rückgriff auf Best Practices früher KI-Anwender (z.B. Finnland, USA, China) und expliziter Integration einer strategischen-Autonomie-Risikoanalyse, um österreichische Maßnahmen mit EU-Zielen zu verknüpfen.
- Bereitstellung nationaler und EU-Mittel für die KI-Transformation, verstanden als Investition, die sich durch höhere Produktivität amortisiert (McKinsey 2023, Park et al. 2026).

- Aktive Mitwirkung am Aufbau europäischer Datenräume und -dienste in für Österreich besonders relevanten Sektoren wie Energie, Umwelt und industrielle IoT-Anwendungen.
- Teilnahme an internationaler Kooperation zu KI-Anwendungen in diesen Bereichen und Förderung entsprechender Datenstandards auf globaler Ebene.
- Fortführung der Mitwirkung an praxisnaher, innovationsfreundlicher EU-Gesetzgebung für wertbasierte KI, die sich am digitalen Humanismus orientiert mit Schwerpunkt auf österreichischen Prioritätssektoren.

EU und Österreich können, wenn strategische Autonomie als Leitkonzept verinnerlicht wird und Quanten-, KI- und Wirtschaftspolitik darauf ausgerichtet werden, den Übergang von Verwundbarkeit zu einer Position schaffen, in der Kooperation statt Abhängigkeit ihre Rolle in einer fragmentierten und konfliktreichen Welt prägt.

Literaturverzeichnis

Edler, J. et al.: Technologiesouveränität: Von der Forderung zum Konzept. Karlsruhe: Fraunhofer ISI, 2020.

Kuipers, T.: The politics of contract tracing apps: how Apple and Google distance themselves from politics while building a global infrastructure of contact tracing. In: STS Vienna University, zuletzt zugegriffen 9.2.2002 https://blog.sts.univie.ac.at/2020/07/15/the-politics-of-contact-tracing-apps/

Park, G., Kang, S., Yi, S., Kim J.: Diverse impacts of AI investments on productivity gains: Effects of industry and innovation characteristics. In: Technolgical Forecasting and Social Change, Vol. 224, 124471, 2026.

McKinsey: The economic potential of generative AI, Report, 2023
zuletzt zugegriffen im März 2026
https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier#/

Abkürzungen

Abk.	Abkürzung
AIM AT 2030	Österreichische KI-Strategie
Art.	Artikel
BGBl.	Bundesgesetzblatt
F&E	Forschung und Entwicklung
FTI	Forschung, Technologie und Innovation
FFG	Forschungsförderungsgesellschaft
HW	Hardware
IPR	Geistige Eigentumsrechte (engl.: intellectual property rights)
KET	Schlüsseltechnologie (engl.: key enabling technology)
QKD	Quantenschlüsselverteilung (engl.: quantum key distribution)
SW	Software
TRL	Technology Readiness Level
usw. uvm.	und so weiter, und verschiedene mehr

Annex

Strategic autonomy and the EU with specific focus on AI and Quantum

Paul Timmers

January 2025

About the author

Prof Dr Paul Timmers is research associate at the University of Oxford, Oxford Internet Institute, professor at KU Leuven and European University Cyprus and the University of Rijeka (visiting), senior advisor EPC Brussels, President of the Supervisory Board Estonian eGovernance Academy, member of the EU Cyber Direct Advisory Board, research fellow of CERRE, CEO of iivii, and partner of WeltWert® consultancy. Previously, he was Director at the European Commission/DG CONNECT where has held responsibility for legislation and funding programmes for cybersecurity, e-ID, digital privacy, digital health, smart cities, and e-government. He was also a cabinet member of European Commissioner Liikanen. He worked as manager of a software department in a large ICT company and co-founded an ICT start-up. He holds a physics PhD from Radboud University (Nijmegen, NL), MBA from Warwick University (UK), EU fellowship at UNC Chapel Hill (USA), and a cybersecurity qualification from Harvard. His main interests are digital policy, geopolitics, and Europe. He frequently publishes and speaks on digital developments, technology and sovereignty, cybersecurity, industrial policy, and sectoral policies such as digital health and is regularly advising governments and think tanks.

Defining and clarifying strategic autonomy

Strategic autonomy is not uniquely defined, neither in policy and law nor in academic literature. An operational definition is:

[1] Strategic autonomy consists of the capabilities, capacities, and control (3C) to defend and strengthen sovereignty.

Loosely, strategic autonomy is a means to realise sovereignty. It consists of what one knows, how much agency one has, and how much say one has over this knowledge and agency. This ability includes decision power regarding the country, that is, it is contributes to sovereignty. Here we talk of sovereignty of the state or an alliance of countries such as the EU, rather than sovereignty of a person (individual sovereignty)[4]. Capabilities (what we know), capacities (how much we can produce), and control (how many decisions are ours) can all be measured and assessed even if this make include subjective judgment. We can do such measurement also in a specific domain such as energy, digital, raw materials, etc. We then would use terms such as energy strategy autonomy, health strategic autonomy, digital strategic autonomy, technological strategic autonomy, etc.

The concept of strategic autonomy developed from the defence sector, where, indeed, it is expressed in terms of military capacities and capabilities. Obviously, the military and ministries of defence are explicitly tasked to defend the sovereignty of the country. In academic and policy literature there is a lot of confusion as well as disagreement about the meaning of the term 'sovereignty'. (Bickerton et al., 2022) define sovereignty in terms of three 'assets' that need to be governed: power, which is called foundational sovereignty; physical and digital assets which are called territorial sovereignty; and the institutional organization of economy, society, and democracy, which is called institutional sovereignty.

Sovereignty also requires internal and external legitimacy (Biersteker, 2012). Internal legitimacy is acceptance of the authority of the government by the citizens and the recognition of citizens by the state. External legitimacy is the acceptance of the state by foreign countries. Sovereignty is both a socially and technologically constructed reality in the digital age (Timmers, 2022).

[4] (Floridi, 2020) defines individual sovereignty or self-sovereignty as 'self- ownership, especially over one's own body, choices, and data'.

Strategic autonomy is often confused with sovereignty. For instance, we see the term 'digital sovereignty' where the author actually talks about digital strategic autonomy in the meaning above. (Tocci, 2021) clearly distinguishes sovereignty and strategic autonomy and adds that autonomy is a prerequisite for sovereignty. She also distinguishes the internal and external dimensions of sovereignty. Can we avoid using a nebulous notion like sovereignty? The reason we use it is partly historic and custom, namely the term sovereignty has much older roots (going back as far Bodin in 1529)[5] and partly political as sovereignty is a politically charged term, in other words a rather technocratic definition such as [1] can still be mobilised for giving a political message. A definition equivalent to [1] that avoids the notion of sovereignty, building on (Moerel & Timmers, 2021), is:

[2] Strategic autonomy is the ability to decide and act on essential aspects of the future in the economy, society, and democracy as a country.

Let's also mention some other definitions:

- Digital sovereignty according to (Floridi, 2020) is: 'control of data, software, standards and protocols, processes, hardware, services, and infrastructures, in short, for the control of the digital'
- The European Parliament Research Service (EPRS, 2020) says that digital sovereignty is: 'the ability to act independently in the digital world'
- The World Economic Forum (WEF, 2025) has a definition similar to Floridi's adding: 'digital sovereignty goes beyond regulation to include fostering entrepreneurship and funding innovation'.

Evolving from the definition in defence and in line with the general direction of definitions as above we then use definition [1] above: strategic autonomy consists of the capabilities, capacities, and control (3C) to defend and strengthen sovereignty. Sometimes a misunderstanding is that strategic autonomy implies autarky or self-sufficiency. This would then be the road to protectionism (which is likely seen as an evil). However, strategic autonomy can perfectly well to together with dependency on other countries and partnerships as long as the other side does not pose a sovereignty threat. Moreover, mutual dependencies, or interdependency, can keep in check tendencies to threaten the sovereignty of the other.

[5] For a short history of the term sovereignty see for instance (Timmers, 2023).

Strategic autonomy is also not an absolute notion. A degree of risk to sovereignty realistically exists for most countries. Risk management can even be a strategic autonomy strategy. However, it would be naïve to trust that interdependencies are balanced, guaranteed to be effective, or last forever. Russia swallowed the pain of its dependencies on the West when sanctions were imposed. It managed to bypass them while keeping the West dependent on its gas. China retaliated on US export controls for advanced chips by restricting exports of germanium and gallium, inflicting pain to the US (and Europe). These export controls also spurred China to accelerate domestic innovation in order to substitute imports. US industrial policy such as the Inflation Reduction Act lures away European manufacturers, eroding jobs and its competitiveness of its long-term partner Europe. This is further being reinforced by President Trump's America First policy.

Strategic autonomy, then, can be achieved in four ways: next to the less likely autarky (at best possible for the US and China), these include risk management, strategic partnerships with likeminded countries, and global collaboration which surpasses a narrow focus on sovereignty. Both strategic partnerships and global collaboration require a commitment to multilateralism.

Any domain of economy or society that is essential for sovereignty falls under the remit of strategic autonomy, from defence to media and education, from critical infrastructures in energy, water and telecommunications to the production of essential medicines and daily food. Generally then, 'bowling alone' is not feasible and cooperation with others is essential. As a counterpart then, such cooperation should be sufficiently effective and reliable and if it is institutionalised such as by bilateral or multilateral agreement, such agreement should have sufficient mandate.

Multilateralism comes naturally to the EU and its member states, as it is a defining feature of the EU, cast in stone by the Treaties. For other countries, multilateralism is at best an instrument to be used for national security or economic security and competitiveness (Haar, 2024). However, the EU Treaties do not give a strong multilateral mandate to the EU in all domains mentioned above: the EU has limited mandate to act in the fields of defence[6], media, education, critical infrastructures, and public health. Nevertheless, if there are cross-border effects the EU can act with the force of hard law, such as when the

[6] The domain of national security is explicitly excluded from the EU mandate as the Treaty on the European Union (TEU), Article 4(2) states: "The Union […] shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State."

internal market would be at risk for instance because of cyber-attacks on critical infrastructures (cf. the EU's Network and Information Security Directive) or when EU-wide internal security is at risk (cf. the EU's Counter-terrorism Directive).

Do national and EU sovereignty add up in a zero-sum? This is not the case, even if often put forward. The EU Treaties are all about pooled, shared and transferred sovereignty. Pooled and shared sovereignty can be a win-win and even a triple win. Why? First, most EU countries are too small to protect themselves on their own against global challenges such as pandemics, climate change, cyberattacks or trade wars. By collaboration in the EU each of them wins in their national sovereignty. Indeed, EU countries have shown to constructively collaborate in this spirit within the current EU policy such as for cybersecurity or fighting the pandemic. Second, European sovereignty (in the sense of the 'assets' mentioned before already exists in certain domains. For instance, the.eu domain name represents a truly European sovereign asset, owned by all EU countries and citizens, yet not in any way going at the expense of national domain names. That is then a second 'win': sovereign assets that are truly European. Third, as stated sovereignty requires both internal and external legitimacy. An EU with strong capabilities, capacities and assets will be a more respected and credible party internationally and thereby gain external legitimacy. This is another win in terms of sovereignty.

Resilience, Economic Security, Strategic Autonomy

Next to strategic autonomy we often find the notions of resilience and economic security. Resilience is defined in the EU Critical Entities Resilience Directive as "a critical entity's ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident" (EU, 2022). A wider definition of resilience is 'the capacity to deal with change and continue to develop', which originates in social-ecological thinking (Stockholm Resilience Centre, 2020).

In itself then, resilience does not imply reduced dependencies. This, however, is a central idea in economic security. As a political rather than legal or technical concept it can be described as a combination of reducing dependencies that create risks for shorter-term resilience or for longer-term autonomy, promoting own economic capacities and capabilities, and complementing these by trustworthy international partnerships.

Resilience is therefore a necessary but not sufficient condition for economic security. Economic security in turn focuses on economic matters but does not comprise national

security directly, nor the protection of democracy and values. These are, however, all part of sovereignty, and therefore addressed by strategic autonomy. We can conclude that economic security is a necessary but not sufficient condition for strategic autonomy. The relationship between the three concepts of resilience, economic security and strategic autonomy then is that resilience is a subset of economic security and both lie within the field of strategic autonomy.

Evolution of strategic autonomy thinking in the EU

The thinking on strategic autonomy has much evolved in the EU over the past years. A short history is as follows. Sovereignty was of course the central element since the start of European collaboration with the Treaty of Rome in 1957. Remarkably, however, the EU Treaties[7] do not mention sovereignty[8]. Strategic autonomy on the contrary was not a notion in EU political discourse, until recently. The exception in this respect was France where strategic autonomy has been linked to military power at least since World War II[9]. After the war and with the trend towards post-colonialism, France still wanted to be able defend its interests wherever necessary in the world, that is, have the capacity of a 'frappe de force'. At the same time, this was influenced by technological development, Namely, France also wanted to have the atomic bomb and correspondingly developed nuclear capability for both military and civil use - that is, it developed nuclear strategic autonomy, which increased its military and energy autonomy.

Winding forward, the notion of strategic autonomy was given wider visibility in 2016 by President Macron, who outlined that both in the military and in the economic domain Europe needed to develop more strategic autonomy – and France thereby too. French minister of Economic Collomb argued in favour of 'Franco European strategic autonomy' (Timmers, 2019). At the time, France also got increasingly worried about the dependency on foreign big tech. A few years earlier, allies of the US got rocked by the Snowden revelations that exposed the extent of US infiltration of the digital word, and which included spying on friends. However, also increasingly Chinese infiltration and cyber-espionage, become a concern, exacerbated by worries about Chinese intentions to export

[7] There are two EU Treaties: The Treaty on the European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU).

[8] Strictly speaking, the EU Treaties make two references to sovereignty, but these are no longer applicable as they concern UK sovereignty over two military bases in Cyprus.

[9] Immediately after World Wat II the term strategic autonomy was only used by France and by India, the latter expressing with this its positioning as being independent from Washington, Moscow, and Beijing, fitting with its prominent role in the league of independent nations, the G77.

its authoritarian model and win-over the world. For some countries like Germany these ‘early days’ of strategic autonomy thinking were rather limited to the military domain. The threatening tone of the first Trump Presidency as regards NATO contributions especially worried Bundeskanzler Merkel.

From 2017 onwards signals of geopolitical, big tech and technological threats grew ever stronger. The European Commission formulated more explicitly the need for increased autonomy, be with the main focus on economy and society (in line with the limited EC mandate in military and defence matters). Notably in ‘digital’ and ‘space’ this was expressed. For instance, the 2017 policy on cybersecurity referred to the broader challenge of strategic autonomy for economic and society. EC and European External Action Service (EEAS) also took a firmer position with the 2019 EU-China strategy, labelling– China as partner, competitor, and systemic rival (EC and EEAS, 2019). Member States and public opinion showed, however, a more divided picture. Several member states felt uneasy with the perceived protectionist undertones in the strategic autonomy and sovereignty debate. They also suspected an agenda of Colbertism to promote national (read: French) champions. Others still stuck to the ideology of globalisation and neoliberalism, rejecting a move towards greater state influence on the economy. For instance, the term ‘industrial policy’ remained for many a taboo. A group of member states promoted the notion of ‘open strategic autonomy’ which got also some traction at European level (see the following textbox).

The sovereignty debate got a backlash too. EC President Juncker’s 2018 State of the Union was titled ‘The hour of European sovereignty’. However, he got heavily criticised in the press. It was not done to talk of European sovereignty, and certainly not done for the European Commission.

In the technological field, strategic autonomy manifested itself in 5G security. This became an issue under US pressure to remove Chinese equipment from telecom networks. A remarkable and paradoxical situation then arose: on the one hand member states willingly sat together with the EC to develop a common approach to 5G security, despite the fact that the concerns mostly touched upon national security, that is, outside the EU’s mandate. Member states relied on EC brinkmanship in this matter. Then, however, only a soft legal instrument resulted (the 2019 5G Security Recommendation which called to assess technical and political risks, read: control by the Chinese government). The result was not only soft because of the limited EU mandate but also only softly implemented: notably Germany and Spain kept in place and continued to buy Huawei equipment.

Open Strategic Autonomy

The European Commission described open strategic autonomy in the 2021 Trade Policy Review: "Open strategic autonomy emphasises the EU's ability to make its own choices and shape the world around it through leadership and engagement, reflecting its strategic interests and values. It reflects the EU's fundamental belief that addressing today's challenges requires more rather than less global cooperation. […] It encompasses: […] assertiveness and rules-based cooperation to showcase the EU's preference for international cooperation and dialogue, but also its readiness to combat unfair practices and use autonomous tools to pursue its interests where needed." (EC, 2021).

- Open strategic autonomy means "acting together wherever possible, acting alone wherever necessary" (Aspen Institute Germany, 2021).
- EU R&I's Horizon Europe programme refers to 'promote the Union's strategic autonomy while preserving an open economy' (EU, 2021).
- The European Commission's Joint Research Centre (JRC): 'The addition of 'open' [in open strategic autonomy] stresses that the EU aims for multilateral cooperation wherever possible and appropriate' (Kroll, 2024).

The soft approach to strategic autonomy changed in 2020 with the first major disruptions of the early 2020's: the COVID pandemic. This exposed Europe's vulnerability in supply chains for personal protection equipment and medicines and, soon after, also for all kind of raw materials and components in particular semiconductors. The word 'resilience' then rose to the top. Next, in addition to resilience, attention was needed for rising geopolitical threats, with the 2022 invasion of Russia in Ukraine, finding China at its side, and the rising belligerent behaviour of China towards Taiwan.

Concerns on supply chain dependencies – technical, economic and political - and the increasing dependency of economy and society on new technologies and big tech moved economic security to the top-level, framed in terms such as decoupling, high fence – small yard, and derisking. In 2023 and 2024 the EU adopted a raft of measures on economic security – identifying for instance, critical raw materials, energy, and ten critical technologies, with the objective to 'promote', 'protect' and 'partner' (see textbox below). Terms such as sovereignty and strategic autonomy were no longer 'Verboten'. Indeed, Bundeskanzler Scholz' Prague speech in September 2023 got a quite different reception

than Juncker's speech 5 years before: one-third of his speech was about European sovereignty. Critics kept silent and general press nodded approval.

EU economic security objectives

- Promoting our own competitiveness by making our economy and supply chains more resilient bolstering innovation and industrial capacity, while preserving our social market economy
- Protecting ourselves from commonly identified economic security risks, by better deploying the tools we already have in place, such as on trade defence, foreign subsidies, 5G/6G security
- Partnering with countries who share our concerns on economic security as well as those who have common interests and are willing to cooperate with us to achieve the transition to a more resilient and secure economy.

Today we experience another major disruption: the second Trump Presidency, pursuing a transactional and economically coercive policy (whether this will also be militarily coercive remains to be seen although it has been alluded to by President Trump). Moreover, and not seen as explicitly as before, US economic power joins up with big tech economic power which already has created shock waves in Europe from fear for tariffs to concerns about the viability of existing EU laws to eagerness about new economic opportunities in a world with fewer rules and attractiveness of an open EU market relative to an isolationist US. This happens at the same time that there are severe concerns about lagging competitiveness, productivity growth, and innovation, internal market fragmentation, and strangling red tape. These concerns are called existential for the EU by the Draghi report and the ECB.

What about the future? Many expect further major geopolitical disruptions, such as an invasion of Taiwan by China, an attack of Russia on a NATO EU country or a stepping up of Russia's sabotage operations (also termed as a situation 'unpeace', that is below the level of war but cumulatively as damaging as war). Adding insult to injury would be geo-economic disruption, that is, when economic instruments get mobilised for geopolitical objectives, such as China squeezing off supply chains, punitive tariffs from the USA onto geopolitical allies, and the rise of BRICS and a possibly alternative global financial transaction system. Others point to technological disruptions that span civil and military

domains, such as generative AI causing massive job disruption, quantum computing exposing the core of government, and space/satellite networks bypassing national territory. Yet others point to the disruptive power when the techno-industrial complex (i.e., big tech) joins up with the great power complex (i.e., the USA, China, perhaps also India). This is these days is exemplified by the combination Elon Musk, Mark Zuckerberg and others with the Trump-led America-First political complex. Already a phenomenon with – at least superficially - similar characteristics comes from China, with the alignment of big tech (Huawei, Tencent, ByteDance, etc) and Xi Jinping's authoritarianist leadership and party apparatus.

Finally, EU internal disruption is also looming, with the take-over of several EU member states by authoritarianism with extreme right-wing, anti-liberal democracy and pro-Russia roots. Likely, this will move attention to the wider notion of strategic autonomy and sovereignty. This does not mean, however, that member states now align behind a common notion of strategic autonomy or common interpretation of EU and national sovereignty. Some member states another view on EU sovereignty and want to break down European economic collaboration ('taking back power from Brussels'), or defence collaboration (opposing the major defence challenges, namely combatting Russia's and Chinese imperialism), or EU democracy (authoritarians being against rule of law and liberal democracy).

Moreover, member states are not equally convinced that Europe faces an existential crisis. Some do not want to accept the consequences of building strong joint industrial policy and investment at EU level, seeing this as a win-lose transfer of sovereignty and budgetary commitment (the Draghi report mentions 800 billion additional p.a.[10]). Other member states are economically not or not yet in dire straits. Some even continue to have strained labour markets.

Clearly, European leaders are challenged to develop a common approach of these future challenges materialise and cause new crises. Not all hope is lost then, however. In the past years, the EU has shown remarkable leadership in crises, and even more so in areas where the EU has a limited mandate. During the pandemic, quickly the EU took the lead in public health, where is has a limited mandate, through joint vaccine procurement and by putting

[10] This figure which seems huge must be seen in perspective. This would consist of public and private money. Public money has typically a leverage factor of over 10 on private investment, that is, the public purse would have to contribute €100 billion p.a. With toughly 400 million Europeans this then amounts to an additional €200 per person per year.

in place the COVID vaccination app in just a few months (global leadership BTW, as this got recognised by over 60 countries and 1 billion people). The EU broke the taboo of shared debt by putting creating the massive Recovery and Resilience Fund. The EU acted within weeks on Russia's invasion by imposing a sequence of packages of sanctions, again in an area with limited mandate. The EU has managed – as mentioned above – to develop a joint approach in cybersecurity despite this domain being close to national security. The advantage this time is that the next crises can be foreseen and anticipated. The disadvantage is that the EU is weaker internally than before, weaker externally in the economy of the future (digital, technological) than ever before, and that Europe is more on its own than ever before.

Strategic autonomy and EU Policies

European Union law

At the time of Brexit, the UK was denied continued access to the secure communications of the Galileo satellite system, and this was justified as it would constitute 'a loss of strategic autonomy'. The justification (EC, 2018) was heavy with legal references – but without ever defining the term strategic autonomy. Indeed, there is no legal definition of strategic autonomy in EU law. At a conference of legislators in 2024 a keynote speaker from the Commission noted this lack of legal definition and wondered what the consequences could be.S

There are, nevertheless, several references to strategic autonomy in EU legislation and policy documents, while the frequency of such references has been increasing significantly since 2017. A few examples:

- In the space domain, the Space Strategy of 2016 is titled 'Reinforcing Europe's Autonomy in Accessing and Using Space in a Secure and Safe Environment') while the 2023 Regulation on Secure Connectivity talks of 'protect the security and public interest of the Union and its Member States, including through a reinforcement of the strategic autonomy of the Union, in particular in technological terms', (Cellerino, 2023; EC, 2016; EU, 2023)
- In EU cybersecurity policy, the number of references grew from one during 2013-2018 to five during 2019-2024, though not used in a consistent phrasing. Annex I

reproduces a table from (Timmers, 2025) that gives the references to strategic autonomy.

- Recent EU R&D policy, the Regulation on Horizon Europe, refers to ‘The pillar 'Innovative Europe' should […] promote the Union's strategic autonomy while preserving an open economy.’ (EU, 2021)
- For quantum technologies there is no legislation (yet), though an EU Quantum Act has been announced. In policy papers on quantum technologies the link to sovereignty and strategic autonomy is explicit, see below.
- On the contrary, the EU AI Act and the Coordinated Action Plan on AI there is no reference to sovereignty or strategic autonomy.

Digital Technologies

In digital technologies (including quantum technology) a whole stack plays a role. The position of Europe is weak in most, except networking. Several diagrammatic representations exist; a major analysis is provided by EuroStack. Using a simplified one here, building on [Timmers, Sheikh], it suggests the weight of the USA, China, EU, and others. In this chapter two cases of particular interest for both the EU and Austria are detailed.

Quantum Technologies

Quantum technologies have clearly been linked to Europe’s sovereignty. For instance, in 2023 26 Member States amongst which Austria signed the European Declaration on Quantum Technologies which states ‘The economic and strategic value of quantum technologies, now and in the future, is clear. As such, they are a high priority for the EU’s sovereignty’ (Spanish Presidency of the Council, 2023). It is still early days for quantum technologies, but commercial use is already happening for quantum sensing, quantum communications, and post-quantum cryptology.

In public sector investments in quantum technologies the EU is second to China, with the larger contributions coming from France, Germany, the EU Quantum Flagship and The Netherlands. Austria invests €107 million, which is modest compared to The Netherlands’ €965 million (see data from World Economic Forum, 2024). Private funding is also increasing, driven by the recognition that this new technology will redefine industries. In innovation and deployment of quantum communications (Quantum Key Distribution or QKD), with the scientific knowledge originating from Austria’s Nobel Prize winner

Zeilinger, China leads, operating a 2,032 km QKD ground link between Beijing and Shanghai. The EU is advancing its capabilities through initiatives like the European Quantum Communication Infrastructure (EuroQCI)[11], which will integrate with the EU's IRIS2 satellite program[12].

To address the security challenges posed by quantum computing - which can break traditional encryption - is urgent to adopt post-quantum cryptography (PQC). This is the case even if quantum computing at scale remains five to ten or perhaps even more years away. PQC is also a necessary complement to QKD[13]. The US National Institute of Standards and Technology (NIST) has already issued three PQC standards, highlighting the strategic importance of early preparedness. Even if there is a sizable and competitive EU investment in terms of research and large-scale cooperation (for instance, the 167-member Quantum Industry Consortium) there is a lack of coordination in translating research into market-ready applications. Moreover, demand-side fragmentation within the EU remains a critical barrier. There is no unified goal for quantum computing by 2030. There is as of yet no plan to smoothen access to the internal market for quantum technologies and prevent barriers and fragmentation arising. Additionally, quantum technologies development depends on critical materials and high-precision components, where Europe faces supply constraints. There is also no articulated European international position such as for the UN, who has declared 2025 as the Year of Quantum.

To strengthen Europe's position, a coordinated approach is needed that balances self-reliance with strategic partnerships. Exclusive control over quantum technologies critical to national security, such as QKD and quantum hardware secure modules, is essential, while for other areas, Europe should pursue mutual interdependencies with like-minded countries, such as the UK and Switzerland. The UN provides a platform for global collaboration to harness quantum technologies for addressing humanity's most pressing challenges[14]. Europe's leadership in this effort could align its strategic interests with broader international goals, positioning it as a key player.

[11] (European Commission, 2024)
[12] (EU Agency for the Space Programme, 2024)
[13] (Georg Serentschy, 2024; Preneel, 2024)
[14] (United Nations, 2024)

Artificial Intelligence

As noted above, policymakers did not explicitly link strategic autonomy or sovereignty to AI policy. Nevertheless, such linkages are strong be it implicit, given the emphasis on Europe's ability to compete internationally in AI and even to position the EU as a global leader in trustworthy AI as articulated in the EU AI Act and the AI Coordinated Action Plan.

At first glance the EU appears to have a impressive range of initiatives in AI. It has the world-first comprehensive AI regulation, the AI Act, based on extensive discussions on ethical AI. It is investing in supercomputing capacity for AI, in particular making this available for SMEs and has jumped from zero supercomputers in the global top 10 in 2016 to 2 in 2024. Around these the EU is setting up 'AI factories' and has announced more of these for 2025 as well as an AI Continent Initiative [Q4 2025], Apply AI Strategy and Data Union Strategy [Q3 2025].

Underpinning AI is data, and Europe may have a particular strength in both data regulation (Data Act, Data Governance Act, …) and Common European Data Spaces[15], industrial data and related initiative such as **Catena-X**[16]\. Europe is also active in digital twins, and this also happens at the company level. In Austria for instance, Verbund AG is a leader in digital twins for hydro power[17].

However, the investment and company figures tell another story about EU 'leadership' and competitive strengths. In 2023, private AI investment in the United States reached €62.5 billion, €7.3 billion in China and €9 billion across the European Union and the UK.[18] The global AI market is expected to grow from €234 billion in 2025 to $826.70bn by 2030, a compound annual growth rate (CAGR) of 27.67%[19].

Investment – notably in generative AI - is dominated by a handful of very large American players: OpenAI, Microsoft, Google, Meta, Apple, Nvidia and xAI. Several of these big tech companies are also pursuing a whole-of-stack dominance strategy, that is they invest not only in AI software or AI chips but also massively in data centres, cloud, networks, AI PCs and robotics, up to and including end-user apps ranging from chat to internet search to a wide range of AI assistants. Europe is not quite absent from this and has many AU

[15] (European Commission, n.d.)
[16] See: (*Catena-X Your Automotive Network - Homepage*, n.d.)
[17] https://itficient.com/en/success-stories/.
[18] (Maslej, et al., 2024)
[19] (Statista, n.d.)

entrepreneurs but there are only a few sizable players in generative AI such as Mistral from France and Aleph Alpha from Germany. The EU is a leader in AI regulation.

However, it is far from certain that the AI Act will have a 'Brussels effect' on AI regulations internationally. There is still uncertainty – possibly unjustified! – about the impact of the AI Act on innovation. Other countries are moving ahead at great speed in rolling out AI and AI infrastructure. In the US a massive investment starting at $100 billion and possibly expanding to $500 billion in AI infrastructure was announced in the first week of the Trump II Presidency by OpenAI, Oracle, Softbank and MGX. Already thin on legislative actions in the US, one of the first Presidential Executive Orders of Trump II was 'Removing Barriers to American Leadership in Artificial Intelligence'. It revoked President Biden's Executive Order of October 30, 2023 on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (President Trump, 2025). China shows remarkable progress in generative AI, such as DeepSeek matching the best of US LLMs at a far lower cost.

In short, Europe's current position in AI is weak. This may turn out to pose a great risk for Europe's competitiveness and security. It can be argued that this has come about because of lack of attention to strategic autonomy in AI. The EU is far outrun in investment in AI infrastructure, AI startups, patents, number of companies, AI adoption, and very likely also the number of jobs. There is a huge skills gap in AI with many companies taking still a wait-and-see attitude - only 8% of EU businesses adopt AI. Data also shows that the EU attracts only a small share of international AI talent while it loses a large share of its PhDs, especially to the US, a massive brain-drain (Anderson, 2022).

As a consequence, the EU risks being sitting duck in AI. The economic transformation is being determined elsewhere. The consequence is either further loss of competitiveness or swallowing the bitter pill, accepting foreign dependency, and releasing control of AI adoption to foreign governments and big tech companies. Another consequence is that universal values of democracy, fundamental rights and Enlightenment that form the bedrock of the EU AI Act and indeed, of the EU, and espoused by international institutions such as UNESO and movements such as Digital Humanism[20] are at risk of being ignored (UNESCO, 2021), (Vienna Manifesto on Digital Humanism – DIGHUM, 2019).

[20] Digital Humanism — TU Wien Informatics.

Conclusions and Recommendations

New approaches are needed for the EU to survive the EU existential crisis and disruptions, several of which are already happening today or have a high likelihood in the future: war, breakdown of international collaboration, international law, and international institutions, global challenges that respect no borders of climate change and cyber-crime, transactional great power re-arrangements, the winning stream of historic materialism, hugely transformative new technologies. There is but one way to deal with these: being pro-active, being focused on opportunity as much as on weaknesses. The following principles can guide concrete action:

- Anticipatory and pro-active rather than being sitting duck: policy must be able to respond and anticipate, be geopolitically aware, technology-aware, and society-aware
- Decisiveness and leadership answering the need for speed. Global rivals move fast. First-comers win. The EU level there must show political leadership.
- Comprehensiveness and consistency mobilising all policy instruments and doing so coherently, from market access regulation to investment, employment to trade, civil to defence, internal to external policies.
- Win-win and mutual interdependency with international partners, suppliers, co-developers, customers, enabling value for all from specialisation and deterring weaponisation.
- Realism and flexibility, ‘starting as realist and aspiring the better’ which implies not claiming leadership in all technologies, nurturing like-mindedness and shared values yet accepting trade-offs.

In line with these principles are the following recommendations.

Recommendation on strategic autonomy

- As Austria and EU, it is essential and existential for our sovereignty to strengthen our strategic autonomy.
- As Austria and EU, we are willing to cooperate with any company and country that respects us and supports our objective of being able to decide and act autonomously for our future.

Because this is existential and given the EU's precarious economic and security situation the priorities are competitiveness and security, in line with the pillars of the EU's 2025-2029 agenda, the Competitiveness Compass, and the Draghi/Letta/Niinisto reports.

Recommendation on quantum technologies

Austria has great assets in quantum technologies but is a small player in the European policy and investment field. In order to increase the potential benefits of these assets and to become a stronger party at the policy-making table it is recommended to pursue AT and EU strategic autonomy in quantum technologies:

- Develop a national action plan, with cooperation, investments, technology priority areas.
- Engage pro-actively with EU policymakers in anticipation of a Quantum Action Plan, and within this promote joining-up of national and industry initiatives across Europe.
- Be pro-active in defining which aspects of quantum technologies and the quantum technologies techno-industrial ecosystem belong to:
- National sovereignty because of overriding national security interests.
- EU sovereignty, promoting a triple win and addressing competitiveness and security.
- Global collaboration, especially co-shaping the UN Year of Quantum.

Recommendation on AI

Austria is well advanced in formulating a national strategy. Tis is a good basis but international competition and technological development are moving ahead relentlessly. Therefore

- Advance and accelerate the national action plan, AI Mission Austria 2030 (AIM 2030) especially as regards adoption by SMEs; copying best practices in adoption from elsewhere in Europe and the world (e.g., Finland, USA, China); taking leadership in the EU by doing an explicit strategic autonomy risk assessment to

reinforce the link to EU strategic autonomy (again with a triple win-win objective), become specific about the protection of intellectual property and FDI in AT companies.

- Foresee and include national and EU transition funding for the AI transformation, argue payback in terms of reduced social costs and enhanced productivity growth.
- Contribute actively to European initiatives to build data commons and related services, in areas of major AT interest such as energy, environment, industrial IoT.
- Engage in wide international cooperation on AI application in sectors of AT interest and pro-actively and internationally promote related data standards.
- Continue co-developing practical pro-innovation EU guidance on value-based, ethical, and digital humanism-driven AI, focusing on sectors and applications of major AT interest.

Addendum: Sovereignty and strategic autonomy in EU cyber policy

Reproduced from (Timmers, 2025).

Policy	Year	Quotes on sovereignty or strategic autonomy
Cybersecurity Strategy	2013	None
Cybersecurity Strategy	2017	Strategic autonomy (not 'open' strategic autonomy): The approach set out in this Joint Communication will make the EU better placed to face these threats. It would build greater resilience and strategic autonomy, boosting capabilities in terms of technology and skills, as well as helping to build a strong single market. Strong cyber resilience […] requires a more comprehensive, cross-policy approach to building cyber-resilience and strategic autonomy, with a strong Single Market, major advances in the EU's technological capability, and far greater numbers of skilled experts. Those Member States with more advanced cybersecurity capabilities and willing to pull them together could consider [..] to include cyber defence within the framework of a "Permanent Structured Cooperation" (PESCO). This could be underpinned by the work set out above to encourage EU industrial capacities and strategic autonomy. The EU's international cybersecurity policy is designed to address the continuously evolving challenge of promoting global cyber stability, as well as contributing to Europe's strategic autonomy in cyberspace.
Cyber Security Act	2019	None
Cybersecurity Strategy	2020	'Technological' sovereignty, interpreted as R&I, no mention of strategic autonomy: This strategy aims to ensure a global and open Internet with strong guardrails to address the risks to the security and

		fundamental rights and freedoms of people in Europe. Following the progress achieved under the previous strategies, it contains concrete proposals for deploying three principal instruments –regulatory, investment and policy instruments – to address three areas of EU action – (1) resilience, technological sovereignty and leadership, (2) building operational capacity to prevent, deter and respond, and (3) advancing a global and open cyberspace. Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres (CCCN). The CCCN should play a key role, with input from industry and academic communities, in developing the EU's technological sovereignty in cybersecurity.
NIS2 Directive	2022	None
Cyber Defence Policy	2022	Defence 'technological sovereignty': "The EU needs to take on more responsibility for its own security.[…] To succeed in this, the EU must ensure its technological and digital sovereignty in the cyber field. " and "all the EU instruments including DEP, Horizon Europe and EDF […] to increase technological sovereignty" and "space […] key asset for technological sovereignty". A technology roadmap was promised for 2023 but not yet delivered.
Cybersecurity posture	2022	Cyber and international, cyber and defence: […] investing in innovation and making better use of civilian technology is key to enhancing our technological sovereignty. Strategic Compass will enhance the EU's strategic autonomy.
State of the Union of President Von der Leyen	2020 2021 2022	None Tech sovereignty, leadership in cyber security European Sovereignty Fund (has not materialised)

	2023	European sovereignty and access to key technologies
Cyber Resilience Act	2023	None
Cyber Solidarity Act	2024	Cyber-resilience: Focus on threat cooperation. Recital 23: Cyber Hubs [..]contributing to Union's technological sovereignty, its open strategic autonomy, competitiveness and resilience and to the development of Union capabilities; Recital 30: European Cybersecurity Alert System should enhance the Union's technological sovereignty and open strategic autonomy Recital 70: (R&I) […] contributes to increasing the resilience of Member States and the open strategic autonomy of the Union, Art 2: this Regulation pursues the general objectives of reinforcing the competitive position of industry and service sectors in the Union across the digital economy, including microenterprises and small and medium-sized enterprises as well as start-ups, and of contributing to the Union's technological sovereignty and open strategic autonomy

References

Anderson, J. (2022). Europe needs high-tech talent: (Strategic Autonomy Series). FEPS. https://feps-europe.eu/publication/europe-needs-high-tech/

Bickerton, C., Brack, N., Coman, R., & Crespy, A. (2022). Conflicts of sovereignty in contemporary Europe: A framework of analysis. Comparative European Politics, 20(3), 257–274.

Biersteker, T. (2012). State, Sovereignty and Territory. In W. Carlsnaes, T. Risse, & B. A. Simmons, Handbook of International Relations. SAGE Publications Ltd.

Catena-X Your Automotive Network—Homepage. (n.d.). Retrieved 12 January 2025, from https://catena-x.net/de/

Cellerino, C. (2023). EU Space Policy and Strategic Autonomy: Tackling Legal Complexities in the Enhancement of the 'Security and Defence Dimension of the Union in Space'. European Papers - A Journal on Law and Integration, 2023 8(2), 487–501. https://doi.org/10.15166/2499-8249/669

EC. (2016). Space Strategy for Europe. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2016%3A705%3AFIN

EC. (2018, June 13). Slides on involvement in the EU's space-related activities—European Commission. https://commission.europa.eu/publications/slides-involvement-eus-space-related-activities_en

EC and EEAS. (2019, March 12). EU-China – A strategic outlook. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52019JC0005

EPRS. (2020). Digital sovereignty for Europe.

EU. (2021). Regulation (EU) 2021/695 establishing Horizon Europe – the Framework Programme for Research and Innovation,. https://eur-lex.europa.eu/eli/reg/2021/695/oj/eng

EU. (2022, December 27). EU Directive on the resilience of critical entities (CER). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557

EU. (2023). EU secure connectivity programme (2023–2027) | EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:4659993

EU Agency for the Space Programme. (2024). IRIS2 | EU Agency for the Space Programme. https://www.euspa.europa.eu/eu-space-programme/secure-satcom/iris2

European Commission. (n.d.). Common European Data Spaces | Shaping Europe's digital future. Retrieved 12 January 2025, from https://digital-strategy.ec.europa.eu/en/policies/data-spaces

European Commission. (2024, April 23). The European Quantum Communication Infrastructure (EuroQCI) Initiative | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. Philosophy & Technology, 33(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6

Georg Serentschy. (2024). Unraveling the confusion around Quantum-Safe Encryption – Serentschy Advisory Services. https://www.serentschy.com/unraveling-the-confusion-around-quantum-safe-encryption/

Haar, R. (2024). Understanding the debate in U.S. foreign policy regarding the benefits of multilateralism and China. ISA 2024.

Maslej, N., Fattorini, L., Perrault, R., Parli, V., Reuel, A., Brynjolfsson, E., Etchemendy, J., Ligett, K., Lyons, T., Manyika, J., Niebles, J. C., Shoham, Y., Wald, R., & Clark, J. (2024). AI Index Report 2024 – Artificial Intelligence Index. AI Index Steering Committee, Institute for Human-Centered AI. https://aiindex.stanford.edu/report/

Moerel, L., & Timmers, P. (2021). Reflections on Digital Sovereignty—EU Cyber Direct. Research in Focus. https://eucyberdirect.eu/research/reflections-on-digital-sovereignty

Preneel, B. (2024). The Quantum Threat and Post-Quantum Cryptography (PQC).

President Trump. (2025, January 23). Removing Barriers to American Leadership in Artificial Intelligence. The White House. https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/

Spanish Presidency of the Council. (2023, December 6). European Declaration on Quantum Technologies | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/library/european-declaration-quantum-technologies

Statista. (n.d.). Artificial Intelligence—Global [Dataset]. Retrieved 12 January 2025, from https://www.statista.com/outlook/tmo/artificial-intelligence/worldwide

Stockholm Resilience Centre. (2020, December 12). Resilience dictionary [Text]. https://www.stockholmresilience.org/research/resilience-dictionary.html

Timmers, P. (2019). CHALLENGED BY 'DIGITAL SOVEREIGNTY'. Journal of Internet Law, 23(6), 1–20. ProQuest Central.

Timmers, P. (2022). The Technological Construction of Sovereignty. In Perspectives on Digital Humanism (pp. 213–218). Springer, Cham. https://doi.org/10.1007/978-3-030-86144-5_28

Timmers, P. (2023). Sovereignty in the Digital Age. In Introduction to Digital Humanism (pp. 571–592). Springer. http://dx.doi.org/10.1007/978-3-031-45304-5_36

Timmers, P. (2025). EU Cybersecurity Policy. In The Making of a Global Digital Rulebook: Digital sovereignty and international action in the EU, Thibaut Kleiner and Andrea Garcia Rodriguez (eds). Springer.

Tocci, N. (2021, February 24). European Strategic Autonomy: What It Is, Why We Need It, How to Achieve It. IAI Istituto Affari Internazionali. https://www.iai.it/en/pubblicazioni/european-strategic-autonomy-what-it-why-we-need-it-how-achieve-it

UNESCO. (2021, November). Ethics of Artificial Intelligence | UNESCO. https://www.unesco.org/en/artificial-intelligence/recommendation-ethics

United Nations. (2024, June 7). International Year of Quantum Science and Technology. https://quantum2025.org/en/

Vienna Manifesto on Digital Humanism – DIGHUM (2019). https://dighum.ec.tuwien.ac.at/dighum-manifesto/

WEF. (2025, January 10). What is digital sovereignty and how are countries approaching it? World Economic Forum. https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/

World Economic Forum. (2024, July 3). Explainer: What is quantum technology and what are its benefits? World Economic Forum. https://www.weforum.org/agenda/2024/07/explainer-what-is-quantum-technology/