Journal of
Law, Policy & Society

Type of the Paper (Article, Review, Research Brief, etc.)

The Necessity of Sovereign AI and the Governance of National Security Risks: A Framework Drawn from Lorenz von Stein's Theory of the State

Tzu-Yu Chiou

[1] Department of Law, Hsuan Chuang University, Hsinchu, Taiwan; jimmy1992tw@hcu.edu.tw
[2] Affiliation 2; e-mail@e-mail.com
* Correspondence: e-mail@e-mail.com

Abstract

As states increasingly depend on foreign technology providers for algorithms, computational infrastructure, and training data, "sovereign AI" has emerged as a national security priority alongside export controls and data governance. Existing scholarship, however, largely reasons at the level of industrial policy and geopolitics, leaving the state-theoretical foundations of AI infrastructure governance under-examined. This article develops a doctrinal and comparative analysis grounded in Lorenz von Stein's nineteenth-century theory of the administrative and social state, applying his account of state personality and self-preservation to computational infrastructure, and comparing Taiwan's Cyber Security Management Act and AI Action Plan with the European Union's AI Act and India's Digital Public Infrastructure initiative. Sovereign AI, reconstructed through Stein's framework, is best understood as a contemporary exercise of the administrative state's obligation to maintain social integration and self-preservation. Legal design should embed computational infrastructure, model autonomy, and data sovereignty into national security law, while guarding against techno-nationalism and surveillance concentration.

Keywords: sovereign AI; national security; Lorenz von Stein; social state; administrative state; data governance.

Received: 07/27/26
Revised: 08/20/26
Accepted: 09/01/26

1. Introduction

The rapid diffusion of generative artificial intelligence has forced states to confront an uncomfortable dependency: the algorithms, computational infrastructure, training data, and model capabilities on which their economies, militaries, and public discourse increasingly rely are, for most jurisdictions, supplied by a small number of foreign technology firms. This asymmetry has crystallized around the label "sovereign AI," a term that has moved from industry marketing into the vocabulary of semiconductor export controls, data governance statutes, and defense procurement policy within the span of only a few years (Bradford, 2023). The national-security valence of the concept is not

merely rhetorical. Deepfake-enabled disinformation and cognitive warfare, algorithmic penetration of critical infrastructure, the reliance of defense decision-support systems on foreign-trained models, and the concentration of advanced compute supply chains in the hands of a small number of firms and states have together elevated AI governance from an industrial-policy question to a core national-security concern (Buchanan, 2020).

Existing treatments of sovereign AI cluster around two registers. The first is industrial policy: subsidy design, chip export controls, and the build-out of domestic compute capacity, exemplified by initiatives ranging from the Stargate compute program in the United States to sovereign-cloud projects across Europe and the Gulf. The second is geopolitical competition, most influentially theorized by Bradford (2023) as a contest among three "digital empires"—an American market-driven model, a Chinese state-driven model, and a European rights-driven model—each seeking to extend its regulatory and infrastructural reach. Complementary work on data sovereignty (Chander & Sun, 2023) and digital sovereignty more broadly (Floridi, 2020) has enriched this picture by foregrounding questions of governance rather than production alone. What remains comparatively underdeveloped is an account pitched at the level of state theory (Staatslehre): an explanation of why, and on what constitutional basis, the state is entitled—or obligated—to intervene in the construction and governance of AI infrastructure at all, as distinct from why it might be prudent or profitable to do so.

This article addresses that gap by returning to a nineteenth-century figure whose work anticipated many of the structural questions now facing digital governance: the German administrative-law scholar and social theorist Lorenz von Stein (1815–1890). Stein's Verwaltungslehre and his theory of the Sozialstaat (social state) offer a framework in which the administrative state is not a passive referee of market outcomes but an active agent of social integration, charged with mediating structural tensions between capital and labor so as to preserve the organic coherence—and ultimately the freedom and survival—of the polity as a whole (Stein, 1870; Stein, 1964). Because Stein's framework was built precisely to explain state intervention in the face of a transformative material infrastructure (industrial capital) that threatened to concentrate power and destabilize social integration, it offers an unusually apt lens for a digital infrastructure—computational capacity, training data, and foundation models—that poses structurally analogous risks. This article argues that "sovereign AI" is best understood not primarily as an industrial-policy artifact or a geopolitical maneuver, but as a contemporary manifestation of the administrative state's Steinian obligation to maintain social integration and ensure its own self-preservation (Selbsterhaltung) in the digital age.

The remainder of the article proceeds in three steps. Section 2 reconstructs Stein's theory of the state, with particular attention to his concepts of state personality (Persönlichkeit) and self-preservation, and translates this framework to computational infrastructure. Section 3 applies the resulting framework to define the constitutive elements of sovereign AI and undertakes a comparative institutional analysis of Taiwan, the European Union, and India. Section 4 discusses the normative and policy implications of a Steinian legitimacy basis for sovereign AI, culminating in four concrete recommendations, before Section 5 concludes.

https://doi.org/10.3390/ eessfz62

2. Theoretical Framework: Lorenz von Stein's Theory of the State

2.1 Beyond the Night-Watchman State

Stein rejected the liberal "night-watchman" conception of the state, in which public authority is confined to maintaining order and adjudicating disputes while leaving socio-economic structure to private ordering. In his Handbuch der Verwaltungslehre and the broader Verwaltungslehre corpus, Stein instead argued that the state must actively intervene in socio-economic relations, using administrative authority to mediate the structural tension between capital and labor that industrialization had produced (Stein, 1870). Writing against the backdrop of the 1848 revolutions and his own study of French socialist movements, Stein contended that unmediated class antagonism threatened not merely the welfare of individuals but the organic integration of society as such, and that only an administratively capable state could reconcile freedom and material inequality on a sustainable basis (Stein, 1964). This is the conceptual root of what German scholarship later canonized as the Sozialstaat, or social state (Koslowski, 2014).

2.2 State Personality and Self-Preservation

Central to Stein's account is the claim that the state possesses a "personality" (Persönlichkeit) that transcends the interests of any particular class or faction. Administrative institutions are, on this view, the mechanism through which the state's personality externalizes its will toward self-preservation (Selbsterhaltung). This move gives state intervention a significance beyond economic regulation: administrative action becomes constitutionally significant as the vehicle through which the state maintains its own subjectivity and continuity against forces—whether class conflict in Stein's own time, or, as this article argues, structural digital dependency today—that would otherwise fragment or hollow it out. Stein's continuing relevance to public administration theory, including his insistence that the discipline cannot be adequately theorized without a concept of the state, has been recognized well beyond German-language scholarship (Rutgers, 1994; Koslowski & Koslowski, 2023).

2.3 Translating Stein to Digital Infrastructure

This article translates Stein's account of active state intervention for social integration into the register of digital infrastructure. As algorithms and large language models increasingly displace traditional means of production as the pivot of information distribution, public discourse formation, and even defense decision-making, allowing their complete provision by foreign private actors risks generating a new species of "digital dependency" and structural inequality, closely analogous in form—if not in origin—to the nineteenth-century capital–labor antagonism that animated Stein's own theorizing. On this reading, "sovereign AI" names the contemporary form taken by the administrative state's obligation to maintain social integration and ensure self-preservation once computational infrastructure, rather than industrial capital, has become the decisive structural variable. This reframing does not deny the industrial-policy and geopolitical dimensions of sovereign AI; rather, it supplies the constitutional and state-theoretical foundation that existing accounts (Bradford, 2023; Chander & Sun, 2023) tend to presuppose without articulating.

https://doi.org/10.3390/ eessfz62

3. Analysis: Sovereign AI as an Object of Administrative State Governance

3.1 The Constitutive Elements of Sovereign AI

Building on this Steinian foundation, sovereign AI can be disaggregated into four constitutive elements: (1) autonomous and controllable computational capacity and semiconductor supply chains; (2) training data and models grounded in domestic language, culture, and legal context; (3) technological resilience of critical infrastructure and defense applications; and (4) talent development and cross-sector governance capacity. Recent comparative work confirms that few, if any, states can achieve full-stack self-sufficiency across all four elements simultaneously, given that the AI stack spans minerals, energy, compute hardware, networks, data assets, models, and applications as a transnational whole (Bradford, 2023). This structural interdependence does not undermine the Steinian argument for state intervention; rather, it clarifies that the administrative state's task is one of managed resilience and selective autonomy across these four elements, not autarky.

3.2 The State–Society Dialectic Applied to AI Governance

Stein's state–society dialectic supplies an analytical tool for explaining how the state may legitimately intervene through administrative law to correct market failure and informational power asymmetry, and this justification extends naturally to AI governance. Concretely, this includes data-sovereignty legislation, mandatory resilience standards for critical computational infrastructure, algorithmic accountability regimes, and regulation of cross-border data flows. Stein's own observation—that administration typically precedes legislation in responding to social change—is borne out in the comparative record examined below: in each jurisdiction, administrative agencies and executive strategies preceded, and in places continue to substitute for, comprehensive statutory frameworks governing AI infrastructure.

3.3 Comparative Institutional Analysis

The three jurisdictions examined below were selected because they instantiate three analytically distinct institutional responses to the same underlying Steinian problem—how the administrative state discharges its obligation of self-preservation and social integration under conditions of computational dependency—while holding constant three comparative criteria: (i) the statutory or constitutional basis invoked for intervention, (ii) the administrative actor or actors principally responsible for its exercise, and (iii) the treatment of defense and national-security applications within the resulting framework. Taiwan represents administrative anticipation in the absence of comprehensive AI-specific legislation; the European Union represents comprehensive legislative codification; and India represents sovereignty pursued through direct public-infrastructure provision rather than market regulation. Holding these criteria constant across three otherwise dissimilar polities—a small East Asian democracy facing acute external security pressure, a supranational rights-oriented regulatory union, and a large developing democracy—allows the analysis to isolate the recurring Steinian pattern of administration preceding legislation from the idiosyncrasies of any single jurisdiction's politics.

Taiwan illustrates the administrative-anticipation pattern with particular clarity. Its Cyber Security Management Act, in force since January 2019, empowers competent authorities to designate "critical infrastructure providers" across nine sectors—energy, water, communications, transportation, finance, emergency and medical services, government agencies, science and industrial parks, and food—and to impose cybersecurity maintenance plans and periodic audits on them. This statutory infrastructure has since been layered with executive strategy rather than fresh legislation:

the National Science and Technology Council's AI Action Plan 2.0 (2023–2026) commits recurring funding toward trustworthy AI development, an AI product and system evaluation centre, and explicit alignment with the EU AI Act and OECD AI principles, while the Ministry of Digital Affairs' Seventh Phase National Cyber Security Development Program (2025–2028) adds AI-assisted active defense and AI-application pillars to critical-infrastructure resilience. The result is a governance architecture built substantially through administrative coordination among the National Security Council, the National Science and Technology Council, and the Ministry of Digital Affairs, rather than through a single comprehensive AI statute—precisely the pattern of administration preceding legislation that Stein identified.

The European Union, by contrast, has pursued comprehensive legislative codification through Regulation (EU) 2024/1689 (the AI Act), which entered into force on 1 August 2024 and adopts a risk-tiered framework in which AI systems used in the management and operation of critical infrastructure are classified as high-risk and subjected to conformity assessment, registration, and human-oversight obligations, with obligations phasing in through 2026 and 2027. Notably, the AI Act's exclusion of AI systems used exclusively for military, defense, or national-security purposes leaves a Steinian gap: the very domain in which sovereign-AI anxieties are most acute—defense decision-support and national-security infrastructure—sits formally outside the Union's flagship AI statute, leaving self-preservation functions to be addressed, if at all, through member-state competence and separate instruments.

India offers a third model, building sovereignty through public infrastructure provision rather than through market regulation alone. Its Digital Public Infrastructure approach—extending the interoperable, state-backed digital identity and payments rails pioneered by Aadhaar and the Unified Payments Interface into the AI domain—combines data-localization requirements with public investment in shared digital rails, reflecting what commentators have described as a distinctively state-driven route to digital sovereignty positioned between the American market-driven and Chinese state-driven models (Bradford, 2023; Chander & Sun, 2023). Read together, the three jurisdictions confirm Stein's observation that administrative innovation—designation regimes, evaluation centres, coordination programs, and public digital rails—tends to run ahead of, and in Taiwan's and India's cases substantially substitute for, comprehensive statutory codification of AI infrastructure governance.

3.4 Alternative Perspectives: Testing the Steinian Account Against Its Rivals

A Steinian account of sovereign AI invites at least three serious rivals, each of which must be addressed rather than assumed away. The first is a Schmittian or exceptionalist reading of the very carve-outs this article treats as a Steinian gap: on this view, the EU AI Act's exclusion of defense and national-security applications is not an oversight to be closed but a deliberate recognition that sovereign decision in matters of existential security belongs to a logic of the exception that ordinary administrative law—Steinian or otherwise—cannot and should not domesticate. Against this objection, the Steinian framework's comparative advantage is that it locates self-preservation within, rather than outside, ordinary administrative competence: it treats computational-infrastructure governance as continuous administrative practice rather than as a standing invitation to emergency powers, and thereby supplies a legal-design vocabulary—audits, designation regimes, coordination mandates—that the exceptionalist account, by definition, cannot.

A second rival is the existing digital-sovereignty literature itself (Floridi, 2020; Chander & Sun, 2023), which already supplies a normative vocabulary of control over data, infrastructure, and algorithms without requiring Stein's apparatus of state personality. This article's contribution is not to displace that literature but to supply it

with a constitutional foundation it tends to presuppose: digital-sovereignty scholarship explains what states are doing and, often, what they should do, but rarely explains why the state—as opposed to markets, international institutions, or civil society—is the legitimate site of that authority in the first instance. Stein's theory of state personality and self-preservation answers precisely that prior question, and in doing so distinguishes normatively defensible sovereign-AI policy from the techno-nationalist and protectionist variants that digital-sovereignty rhetoric can otherwise be used to legitimate.

A third and more skeptical rival is a public-choice account that treats appeals to state "self-preservation" as rhetorical cover for rent-seeking and industrial protectionism—the concern that Steinian language simply dresses up subsidy politics in constitutional clothing. This article does not dismiss that risk; Section 4.3 below treats the concentration of administrative power as a standing danger inherent in, rather than external to, the Steinian framework itself. What the public-choice critique cannot supply on its own, however, is a normative account of when computational-infrastructure intervention is legitimate rather than merely rent-seeking; the Steinian criterion—intervention justified by social integration and self-preservation rather than sectoral advantage—offers exactly the limiting principle that a purely public-choice analysis lacks.

4. Discussion: Policy and Normative Implications

4.1 A Legitimacy Basis Beyond Industrial Competitiveness and Geopolitics

This article argues that the legitimacy of sovereign AI policy should not rest solely on industrial competitiveness or geopolitical rivalry, but on a Steinian conception of the state's fundamental obligation to maintain social integration and ensure its own self-preservation. Grounding sovereign AI in this obligation allows legal design to reconcile efficiency with legitimacy, and helps distinguish genuine national-security governance from industrial subsidy dressed in security rhetoric or techno-nationalist posturing.

4.2 Recommendations

First, national-security legislation should explicitly incorporate computational infrastructure, model autonomy, and data sovereignty as constitutive elements of national security, coupled with cross-sector coordination mechanisms spanning national security, economic, digital development, and defense authorities—extending Taiwan's existing critical-infrastructure designation logic under the Cyber Security Management Act to computational and model-level dependencies that current law does not yet reach.

Second, echoing Stein's principle of preventive administrative intervention, data-governance legislation should impose localization, auditability, and transparency obligations on foreign AI service providers before harms materialize, rather than only after critical infrastructure has been compromised—an approach partly reflected in the EU AI Act's ex ante conformity-assessment regime for high-risk systems, but presently undercut by that regime's exclusion of defense and national-security applications.

Third, in keeping with the social state's concern for structural stratification, sovereign AI policy design should integrate digital-divide and labor-market-disruption concerns directly into the policy, rather than treating them as externalities, so that the pursuit of technological sovereignty does not itself become a new vector of power concentration or a pretext for expanded surveillance.

Fourth, academic and legislative discourse should revive Stein's state theory as a bridge connecting classical administrative theory to emerging digital-governance questions, thereby offering small and medium-sized East Asian democracies—Taiwan foremost among them—a normative vocabulary for sovereign AI that is distinct from, and not reducible to, the dominant United States–China binary.

https://doi.org/10.3390/ eessfz62

4.3 Limits: Avoiding Techno-Nationalism and Surveillance Concentration

A Steinian framework carries its own risk, which Stein himself would have recognized: an administrative state empowered to intervene in computational infrastructure for the sake of self-preservation can just as easily concentrate power domestically as resist dependency externally. Recent comparative assessments caution that full-stack AI sovereignty is structurally infeasible for almost any country, given concentrated choke points across minerals, energy, compute, networks, data, and talent across the AI stack, and that pursuing it regardless can produce protectionism, market fragmentation, and stranded public investment rather than genuine resilience. The more defensible posture, consistent with Stein's own emphasis on mediating rather than eliminating structural tension, is one of managed interdependence: selective, audited, and rights-respecting intervention rather than autarkic ambition.

5. Conclusions

By reinterpreting Lorenz von Stein's nineteenth-century theory of the state for a digital age, this article has sought to supply sovereign AI discourse with a legitimacy basis that existing industrial-policy and geopolitical accounts leave underexamined. Read through Stein, sovereign AI is neither a subsidy program nor a nationalist slogan, but a contemporary expression of the administrative state's constitutional obligation to preserve social integration and its own continuity amid a structural transformation as consequential, for the digital age, as industrialization was for Stein's own. This reframing offers Taiwan and other small and medium-sized democracies a theoretical resource for AI-era national-security governance that neither collapses into the United States–China binary nor abandons the state's obligation to mediate, rather than merely regulate, the structural risks of computational dependency. It also invites renewed engagement, within public-law scholarship, with Stein's continuing relevance—opening a research pathway that connects nineteenth-century administrative theory with twenty-first-century digital governance.

Author Contributions: Conceptualization, methodology, investigation, writing—original draft preparation, and writing—review and editing, T.-Y.C. The author has read and agreed to the published version of the manuscript.

References

Bradford, A. (2020). The Brussels effect: How the European Union rules the world. Oxford University Press.

Bradford, A. (2023). Digital empires: The global battle to regulate technology. Oxford University Press.

Buchanan, B. (2020). The AI triad and what it means for national security strategy. Center for Security and Emerging Technology, Georgetown University.

Chander, A., & Sun, H. (2023). Data sovereignty: From the digital silk road to the return of the state. Oxford University Press.

Cyber Security Management Act. (2018, amended). Laws & Regulations Database of the Republic of China (Taiwan). https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=A0030297

European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union.

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.

Koslowski, S. (2014). Lorenz von Stein und der Sozialstaat. Nomos.

Koslowski, S., & Koslowski, A. (2023). Stein, Lorenz von. In M. Sellers & S. Kirste (Eds.), Encyclopedia of the philosophy of law and social philosophy. Springer. https://doi.org/10.1007/978-94-007-6519-1_651

Ministry of Digital Affairs, Taiwan. (2025). Seventh phase national cyber security development program (2025–2028). Administration for Cyber Security.

National Science and Technology Council, Taiwan. (2023). Taiwan AI action plan 2.0 (2023–2026).
Rutgers, M. R. (1994). Can the study of public administration do without a concept of the state? Reflections on the work of Lorenz Von Stein. Administration & Society, 26, 395–412.
Stein, L. von. (1870). Handbuch der Verwaltungslehre und des Verwaltungsrechts. Cotta.
Stein, L. von. (1964). The history of the social movement in France, 1789–1850 (K. Mengelberg, Trans. & Ed.). Bedminster Press. (Original work published 1850).