Technology and Regulation

special issue: security in the digital age

Redefining Digital Sovereignty: Infrastructural Dependence, Epistemic Asymmetry, and Governance Challenges in the Age of Big Tech

Author(s)	Chee Hae Chung
Contact	chung382@purdue.edu
Affiliation(s)	Chee Hae Chung is a Postdoctoral Research Associate at the Governance and Responsible AI Lab (GRAIL) and the Computational Social Science (CSS) Lab at Purdue University
Keywords	digital sovereignty, cybersecurity governance, infrastructural dependency, epistemic asymmetry, algorithmic governance, big tech, public-private interdependence, European Union, Korea, GDPR, AI Act
Published	Published: 31 Mar 2026
Citation	Chee Hae Chung, Redefining Digital Sovereignty: Infrastructural Dependence, Epistemic Asymmetry, and Governance Challenges in the Age of Big Tech, Technology and Regulation, 2026, 57-70 • 10.71265/q0527965 • ISSN: 2666-139X

Abstract

This article examines how digital sovereignty is being structurally reconfigured through the privatization of cybersecurity governance. As governments increasingly depend on transnational technology firms for core security functions such as threat detection and cloud infrastructure, they face new constraints in defining, overseeing, and enforcing public authority. The paper develops a framework of three structural dilemmas: infrastructural dependency, epistemic asymmetry, and governance capacity gaps, to analyze how state sovereignty is reshaped through socio-technical entanglements. Through comparative case studies of AWS Sovereign Cloud (European Union), Project Maven (United States), and LG CNS Smart Surveillance (Korea), it shows how critical decisions about risk, classification, and control are embedded in proprietary systems. Reconceptualizing sovereignty as governance capacity rather than exclusive control, the article contributes to emerging debates on algorithmic governance, platform power, and digital constitutionalism. It argues that reclaiming digital sovereignty requires institutional architectures that embed public oversight within the infrastructures and epistemologies of security.

1. Introduction

Cybersecurity governance today is entangled with complex relationships between state institutions and transnational technology firms. Platforms such as Amazon, Microsoft, Google, and Palantir are no longer

external vendors; they are embedded in the operational core of public security systems, including cloud infrastructure, threat modeling, and data analytics.[1] This integration challenges foundational assumptions about sovereignty, jurisdiction, and the public-private divide in security governance.

Cybersecurity is a strategic domain where these tensions are especially visible. As public functions are digitized, ranging from biometric border control to AI-assisted threat detection, states become dependent on systems they did not build and often cannot fully audit.[2] The ability to govern these infrastructures increasingly depends on private actors' willingness to disclose, cooperate, or comply. This raises critical concerns over who gets to define threats, assess risks, and allocate protective resources.[3] In this article, 'threat detection' refers not to conventional IT systems defense, but to algorithmic classification of public security threats in domains such as predictive policing, border surveillance, and military intelligence.

This article examines how such structural dependencies reshape digital sovereignty. It argues that the increasing reliance on private platforms creates three interconnected dilemmas for states: infrastructural dependency, epistemic asymmetry, and regulatory capacity constraints. These dilemmas reveal that public authority is constrained not only by policy gaps or international competition, but also by the design, ownership, and control of the infrastructures through which security is defined and enacted.

To analyze these governance dilemmas, this article develops a framework that links material infrastructures with knowledge regimes and institutional authority. Drawing from work in platform studies, regulatory theory, and digital sovereignty, it conceptualizes security governance as a field shaped by private classification systems, opaque infrastructures, and uneven capacity to intervene in algorithmic operations.[4] This approach shifts focus from legal frameworks alone to the embedded arrangements through which governance is actually performed.

The argument unfolds through three empirical case studies: Amazon's Sovereign Cloud, Google's Project Maven, and LG CNS's deployment of public artificial intelligence (AI) systems in Korea. These cases illustrate how states confront dependencies that are technical, institutional, and epistemic in nature. Each exposes how key decisions about public safety, risk prioritization, and resource allocation are shaped by corporate infrastructures and proprietary classification systems.[5]

Rather than viewing sovereignty as exclusive control, this article redefines it as a form of governance capacity, specifically, the ability to configure infrastructures, interpret risks, and enforce oversight over digital systems used for public ends. It contributes to an emerging literature that links platform power with epistemic governance and legal legitimacy in the age of AI and security platforms.[6]

The article proceeds as follows. Section 2 outlines the structural dilemmas that shape cybersecurity governance, including infrastructural dependency, epistemic asymmetry, and governance capacity gaps, offering a conceptual framework for analyzing digital sovereignty in practice. Section 3 applies this

1. Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State* (Macmillan 2014); Freddy Dezeure, Lokke Moerel and George Webster, 'Digital Sovereignty Is Impossible Without Big Tech' (2024) 48 *Atlantisch Perspectief* 30; Hongfei Gu, 'Data, Big Tech, and the New Concept of Sovereignty' (2024) 29 *Journal of Chinese Political Science* 591.
2. Kate Crawford and Ryan Calo, 'There Is a Blind Spot in AI Research' (2016) 538 Nature 311; Matthias Monroy, 'Europol Uses Palantir' (*Matthias Monroy*, 11 June 2020) https://digit.site36.net/2020/06/11/europol-uses-palantir/ accessed 15 May 2025.
3. Luciano Floridi, 'The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU' (2020) 33 *Philosophy & Technology* 369; Paul Timmers, 'Ethics of AI and Cybersecurity When Sovereignty Is at Stake' (2019) 29 *Minds and Machines* 635; Norma Möllers, 'Making Digital Territory: Cybersecurity, Techno-Nationalism, and the Moral Boundaries of the State' (2021) 46 *Science, Technology, & Human Values* 112.
4. Samuele Fratini, 'The Sociotechnical Politics of Digital Sovereignty: Frictional Infrastructures and the Alignment of Privacy and Geopolitics' (2025) SSRN https://papers.ssrn.com/sol3/papers.cfm?abstractid=5192550 accessed 15 May 2025; Huw Roberts, 'Digital Sovereignty and Artificial Intelligence: A Normative Approach' (2024) 26 *Ethics and Information Technology* 70.
5. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs 2019); Simona Ramos and Joshua Ellul, 'Blockchain for Artificial Intelligence (AI): Enhancing Compliance with the EU AI Act through Distributed Ledger Technology. A Cybersecurity Perspective' (2024) 5 *International Cybersecurity Law Review* 1.
6. Elettra Bietti, 'Consent as a Free Pass: Platform Power and the Limits of the Informational Turn' (2019) 40 *Pace Law Review* 310; Nikolas Guggenberger, 'Consent as Friction' (2025) 66 *Boston College Law Review* 353; Maximilian Mayer and Philip J Nock, 'Digital Fragmentations, Technological Sovereignty and New Perspectives on the Global Digital Political Economy' (2025) 4 *Global Political Economy* 2.

framework to three empirical case studies: predictive policing in the United States (US), sovereign cloud infrastructure in the European Union (EU), and smart surveillance systems in the Republic of Korea (Korea). Section 4 draws out the theoretical and policy implications of these cases, arguing for a reconceptualization of sovereignty as institutional and epistemic capacity rather than territorial control. Section 5 concludes by reframing digital sovereignty as a challenge of infrastructural stewardship in conditions of interdependence.

By situating cybersecurity governance within a broader political economy of platform dependence, this article offers a new perspective on how states can regain capacity in an environment where they increasingly govern through systems they do not control.

2. Defining Cybersecurity Governance and Digital Sovereignty in the Age of Privatized Cybersecurity

As cybersecurity threats intensify and digital infrastructures become essential to public life, governments face profound challenges in asserting legal authority over increasingly privatized domains. Traditional conceptions of state sovereignty, premised on territorial jurisdiction and institutional control, are no longer adequate in a context where transnational technology firms design, own, and operate the systems through which digital governance occurs. This section integrates theoretical insights from both cybersecurity governance and digital sovereignty literature to examine how structural conditions—rather than normative ambitions—shape a state's capacity to act.

Digital sovereignty is not simply a matter of regulatory will. It depends on the institutional, technical, and epistemic capacities that allow governments to govern digital infrastructures, secure sensitive data, and oversee algorithmic systems. These capacities are increasingly constrained by public reliance on private infrastructures, asymmetries in technical expertise, and gaps between regulatory frameworks and their enforcement.

2.1 Research Framework: Structural Dilemmas and the Conditions of Digital Sovereignty

The foundational assumption of state sovereignty is that governments possess the capacity to define and enforce rules within their jurisdictions. In the digital domain, however, this assumption is increasingly difficult to sustain. Cybersecurity governance operates through globally distributed infrastructures and algorithmic systems, many of which are designed, maintained, and controlled by private technology firms. These firms are not simply service providers. They shape how data is collected, how risks are classified, and how security responses are executed. The result is a fragmented governance environment in which states often lack the infrastructural control, technical insight, or institutional leverage needed to govern effectively.

Digital sovereignty, in this context, refers to a state's ability to define, implement, and enforce political and legal decisions over digital systems, platforms, and data infrastructures.[7] It encompasses not only jurisdictional authority, but also the material and epistemic conditions necessary to exercise that authority. This includes securing critical infrastructures, overseeing algorithmic decision-making, and holding private actors accountable to democratic norms and constitutional principles.

Recent scholarship highlights that digital sovereignty is not a unitary concept, but a contested one that applies across multiple levels. The term can refer to the sovereignty of individuals (e.g., autonomy over personal data and online identity), the autonomy of organizations (such as public agencies or corporations), and the strategic sovereignty of states (i.e., the capacity to exert political and legal authority over digital

7. ENISA, 'Cybersecurity Research Directions for the EU's Digital Strategic Autonomy' (*European Union Agency for Cybersecurity (ENISA)*) (2025) https://www.enisa.europa.eu/publications/cybersecurity-research-directions-for-the-eu2019s-digital-strategic-autonomy accessed 7 November 2025; Johan David Michels, Ian Walden and Christopher Millard, 'Storm Clouds Are Building: Surveillance, Sovereignty, and State Interests (February 03, 2025)' (2025) SSRN https://dx.doi.org/10.2139/ssrn.5159829 accessed 7 November 2025.

systems).[8] The boundaries between these levels are often blurred, particularly in governance domains such as cybersecurity, where infrastructural and epistemic power is exercised through hybrid public-private arrangements.[9] While this article acknowledges the relevance of all three layers, it explicitly adopts a state-level perspective, focusing on how public institutions seek to govern critical digital infrastructures amid growing dependencies on private platforms. Individual rights and organizational autonomy are treated as consequential factors, particularly in relation to consent, privacy, and public accountability, but they are analyzed primarily as dimensions that condition or constrain the exercise of state sovereignty. This clarifies the article's focus and anchors its empirical and theoretical contributions in debates about public authority, infrastructure, and institutional design in cybersecurity governance.

Sovereignty in practice is increasingly shaped by three interrelated constraints:

- **Infrastructural dependency**: Public institutions rely on private firms for core governance functions, from cloud computing and identity verification to satellite communications and AI-based surveillance.
- **Epistemic asymmetry**: Technical knowledge, risk classification, and operational control are concentrated within corporations, leaving public regulators with limited capacity to audit or interpret complex systems.
- **Governance capacity gaps**: Even where legal frameworks exist, public institutions often lack the expertise, resources, and institutional integration necessary to enforce them meaningfully.

These are not simply implementation issues, but they are structural features of the current cybersecurity landscape. Addressing them requires a shift in how digital sovereignty is conceptualized. Rather than viewing sovereignty as a matter of exclusive control, it must be understood as a relational condition, one that depends on the ability to shape infrastructures, access and contest knowledge, and operationalize governance at scale.

Furthermore, these dilemmas are analytically distinct but structurally intertwined. Infrastructural dependency deepens epistemic asymmetry by limiting state access to data and tools. Epistemic asymmetry in turn exacerbates governance gaps by eroding the ability to regulate what cannot be understood. Together, they constrain the ability of governments to enact meaningful digital sovereignty, no matter the strength of their legal mandates. This framework offers a conceptual map for diagnosing sovereignty not as a binary possession, but as a variable capacity shaped by institutional configurations and socio-technical dependencies. This approach resonates with prior work that reconceptualizes AI governance as a negotiation of institutional legitimacy and societal expectations, reframing digital sovereignty as part of a broader rethinking of the social contract itself.[10] The following sections develop each dilemma in greater depth.

2.2 Infrastructural Dependency and the Fragmentation of State Authority

Infrastructural dependency refers to the structural reliance of public institutions on privately owned and managed digital infrastructures for the performance of essential governance functions. These infrastructures include cloud platforms, biometric identification systems, data hosting services, telecommunications networks, and AI-based analytical tools.[11] Transnational technology firms such as Amazon Web Services, Microsoft Azure, and Google Cloud increasingly serve as critical infrastructure providers for public-sector operations, including public health, law enforcement, judicial administration, and national defense.[12] Governments have become structurally embedded in private technological systems, where backend infrastructures are operated, maintained, and secured by corporate actors whose services are indispensable due to technological specialization, economies of scale, and global reach.[13]

8. Johan David Michels, Ian Walden and Christopher Millard, 'Storm Clouds Are Building: Surveillance, Sovereignty, and State Interests' (*Social Science Research Network*, 3 February 2025) https://papers.ssrn.com/abstract=5159829 accessed 7 November 2025; ENISA (n 7).
9. Floridi (n 3); Laura DeNardis, *The Global War for Internet Governance* (Yale University Press 2014).
10. Chee Hae Chung and Daniel Stuart Schiff, 'AI and the Social Contract' (2025) 8 *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society (AIES)* 615.
11. DeNardis (n 9); Michael Kwet, 'Digital Colonialism: US Empire and the New Imperialism in the Global South' (2019) 60 *Race & Class* 3.
12. Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020).
13. Ronald J Deibert, *Reset: Reclaiming the Internet for Civil Society* (House of Anansi 2020); Jean-Christophe Plantin and others, 'Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook' (2018) 20 *New Media & Society* 293.

This dilemma is rooted in the concept of infrastructural power, which traditionally referred to a state's capacity to implement decisions and project authority through the physical and institutional infrastructures that connect it with its population[14]. In the digital era, however, this power has partially shifted to private entities that design, own, and operate the infrastructures through which communication, data processing, and digital governance now occur. These infrastructures are characterized as a new terrain of governance, emphasizing that control over digital infrastructure increasingly translates into control over the terms and conditions of social and political interaction.[15]

In this setting, the modern state no longer exercises unmediated authority over its own security-critical infrastructure. Rather, it operates within technical ecosystems shaped by platform standards, intellectual property regimes, proprietary APIs, and the global logistics of data hosting and transmission. Many of these infrastructures are controlled by a small group of dominant technology firms whose services are entrenched through economies of scale, vendor lock-in, and jurisdictional complexity.[16] As a result, state sovereignty becomes conditional on access to, or compliance with, corporate standards and contractual terms.

This dependency introduces specific cybersecurity vulnerabilities. For instance, when public agencies rely on cloud-hosted services to store sensitive citizen data or execute security functions, they may not control the hardware, encryption standards, or backup protocols involved. Legal mandates for data protection or system redundancy may exist on paper, but enforcement is weakened when data centers are extraterritorial or operated under non-transparent contractual clauses. Moreover, public institutions may lack alternatives due to procurement constraints, legacy system dependencies, or the lack of in-house capacity to manage secure digital infrastructures.

This situation also undermines the performative and symbolic dimensions of state sovereignty. When citizens access government services through commercial identity providers, or when national cybersecurity responses rely on corporate dashboards and analytics, the locus of control, and the perception of legitimate authority, shifts away from the state. These dynamics are especially visible in contexts like public health infrastructure, smart city development, and border surveillance, where policy implementation is mediated through hybrid public-private infrastructures.

Thus, infrastructural dependency fragments state authority across jurisdictional and institutional boundaries. It creates a systemic condition in which sovereignty is no longer a matter of legislative competence or enforcement capacity alone, but a function of infrastructural positioning. This challenges conventional approaches to cybersecurity governance, which often assume that states can unilaterally impose and enforce rules over their digital domains. It calls instead for a reconceptualization of sovereignty as relational and infrastructurally embedded, conditioned by access to, and control over, the technical substrates through which public authority is enacted.

2.3 Epistemic Asymmetry and the Privatization of Risk Knowledge

Epistemic asymmetry refers to the structural imbalance in knowledge production, technical capability, and interpretive authority between public institutions and private technology firms in cybersecurity governance. This asymmetry is not simply a question of expertise disparity but a condition in which the ability to define threats, design responses, and evaluate risks is disproportionately held by private actors. These firms do not merely supply technical tools; they shape the underlying epistemologies that govern how cybersecurity is conceptualized and practiced.[17]

14. Michael Mann, 'The Autonomous Power of the State: Its Origins, Mechanisms and Results' (1984) 25 *European Journal of Sociology* 185.
15. DeNardis (n 9).
16. Julie E Cohen, *Between Truth and Power* (Oxford University Press 2019); Kwet (n 10).
17. Gil Eyal, *The Crisis of Expertise* (Polity Press 2019); Claudio M Radaelli, 'The Role of Knowledge in the Policy Process' (1995) 2 *Journal of European Public Policy* 159.

This concept draws on the broader literature on epistemic governance, which highlights the increasing role of expert knowledge in shaping regulatory regimes, particularly in domains governed by technical uncertainty and rapid innovation.[18] In cybersecurity, epistemic authority involves constructing threat models, establishing classification systems, designing mitigation protocols, and determining harm thresholds. These tasks are often performed through proprietary systems developed by firms with privileged access to large-scale datasets, computational infrastructures, and technical labor.

Governments face a widening gap in this space. They are frequently dependent on private sector tools, especially AI-driven threat detection platforms, without having the internal capacity to fully understand, audit, or govern them. This gap is exacerbated by the accelerating pace of technological development, which outstrips the ability of public institutions to recruit and retain personnel with adequate expertise or to update regulatory frameworks in real time.[19] As cybersecurity threats evolve, states often find themselves as passive recipients of risk definitions created by the private sector, unable to independently assess their validity or implications.

This imbalance also reshapes fundamental regulatory concepts. Consider the example of consent, a core legal requirement under frameworks like the General Data Protection Regulation (GDPR). In principle, consent provides individuals with agency over their data and establishes the legitimacy of processing practices. However, in practice, what counts as "informed" or "freely given" consent is determined through interface design, data architecture, and operational processes defined by platform providers. These are not neutral or transparent mechanisms, but strategic choices embedded in commercial objectives.[20] The state, while nominally responsible for protecting fundamental rights, often lacks the technical insight or access required to interrogate how consent is implemented in practice.

This delegation of epistemic authority extends beyond privacy regulation into the domain of national security and public safety. In predictive policing and AI-based threat classification systems, private firms are contracted to provide the models that determine what behavior is deemed suspicious or which individuals are categorized as high risk. These determinations are shaped by algorithms trained on proprietary data, often protected by intellectual property rights and trade secrecy laws. Public agencies using these tools may lack visibility into the training datasets, model logic, or error rates, and they frequently lack the legal leverage or technical skill to demand such transparency.[21]

As a result, the state becomes epistemically dependent on corporate knowledge regimes. It can neither validate nor challenge the assumptions embedded in the systems it uses to govern. This undermines not only the technical soundness of public cybersecurity practices but also their democratic legitimacy. If the knowledge used to classify threats or determine risk is inaccessible to oversight, the accountability mechanisms that underpin constitutional governance erode.

Digital sovereignty in this context requires more than formal legal competence. It depends on epistemic sovereignty: the ability to produce, access, and contest the knowledge used to define and regulate digital threats. This calls for systemic investment in public-sector technical infrastructure, inter-institutional knowledge sharing, and open epistemic architectures that reduce reliance on proprietary corporate frameworks. Without addressing this asymmetry, legal authority risks becoming symbolic, with real governance power remaining in the hands of those who control the tools, data, and definitions of cybersecurity itself.

18. Eyal (n 17).
19. Chee Hae Chung, 'AI and the Rule and Role of Law: Reshaping Legal Regulatory Frameworks to Address Emerging Challenges' (2025) *Proceedings of the IEEE International Symposium on Ethics in Engineering, Science, and Technology (ETHICS)* 1.
20. Ari Ezra Waldman, *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power* (Cambridge University Press 2021); Theodore Christakis, 'European Digital Sovereignty, Data Protection, and the Push toward Data Localization', *Data Sovereignty: From the Digital Silk Road to the Return of the State* (Oxford University Press 2023).
21. Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).

2.4 Governance Capacity Gaps and the Limits of Legal Frameworks

This section analyzes how limitations in institutional capacity undermine efforts to achieve digital sovereignty through cybersecurity regulation. It focuses on the EU and Korea, two jurisdictions that have positioned themselves as global leaders in digital governance, but that continue to face persistent challenges in translating legal frameworks into operational authority. The EU's supranational legal system and Korea's centralized governance model offer contrasting institutional architectures, allowing for comparative insight into how governance capacity gaps manifest under different regulatory regimes.[22] Korea was selected not only for its strong digital infrastructure and early adoption of a national AI Basic Act, but also for its distinct geopolitical and legal-cultural context, which offers a meaningful counterpoint to the EU's rights-based regulatory model.

These governance capacity gaps refer to the structural mismatch between the normative ambitions of legal frameworks, particularly in anticipating, managing, and mitigating digital threats, and the institutional capabilities of states to realize those ambitions. This includes limitations in technical expertise, regulatory coordination, and enforcement mechanisms across public agencies. When such gaps persist, even sophisticated regulatory tools fail to deliver effective cybersecurity governance or to reinforce digital sovereignty.[23]

The EU's regulatory landscape offers multiple examples of this tension. The GDPR, enacted in 2018, introduced a risk-based, lifecycle-oriented approach to data protection. It includes Data Protection Impact Assessments (Articles 35–36), mandates for privacy by design and by default (Article 25), and establishes accountability requirements for data controllers (Articles 5(2), 24, 30). While these mechanisms represent a shift toward proactive regulation, their practical enforcement has proven difficult. The "one-stop-shop" mechanism, designed to centralize enforcement for cross-border cases, often leads to bottlenecks, particularly in Member States like Ireland, where many tech firms are headquartered but where enforcement capacity is limited.[24] This has raised concerns about under-enforcement and regulatory capture, which threaten the EU's strategic objectives in asserting digital sovereignty. Formal regulatory tools can obscure deeper structural imbalances when legal compliance is internalized through corporate architecture that resists public scrutiny.[25]

The EU AI Act, officially adopted in 2024, extends this model into the AI domain. It establishes a risk-tiered framework that prohibits certain harmful applications, imposes transparency and documentation duties on high-risk systems, and requires conformity assessments and post-market monitoring. However, the Act delegates enforcement to national supervisory authorities, many of which face asymmetrical resource allocation and lack technical capacity to oversee complex AI systems effectively. This decentralization risks undermining the coherence of EU-wide governance, particularly in the face of fast-evolving AI deployment across sectors.[26]

Additional regulatory frameworks attempt to close this enforcement gap by targeting infrastructure and operational resilience. The Digital Operational Resilience Act (DORA), adopted as Regulation (EU) 2022/2554, focuses on financial services. It mandates cybersecurity testing, incident reporting, third-party risk management, and grants national authorities powers to audit cloud service providers (Articles 26–39).[27] The Network and Information Systems Directive 2 (NIS2 Directive), which replaces the original NIS Directive of 2016, significantly broadens the regulatory perimeter. NIS2 covers essential and important entities across sectors such as energy, healthcare, and digital infrastructure. It mandates cybersecurity risk management

22. Michels, Walden and Millard (n 7); ENISA (n 7).
23. Robert Baldwin, Martin Cave and Martin Lodge, *Understanding Regulation: Theory, Strategy, and Practice* (Oxford University Press 2011).
24. Christopher Kuner and others, 'The EU General Data Protection Regulation: A Commentary/Update of Selected Articles' (*Social Science Research Network*, 4 May 2021) https://papers.ssrn.com/abstract=3839645 accessed 30 July 2025; Bradford (n 12).
25. Ari Ezra Waldman, 'Privacy Law's False Promise' (2019) 97 *Washington University Law Review* 773.
26. Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act — Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach' (2021) 22 *Computer Law Review International* 97.
27. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 2022 (Regulation (EU) 2022/2554).

(Article 21), incident reporting (Articles 23–30), and internal governance mechanisms, including board-level accountability. Unlike the first NIS Directive, which suffered from inconsistent transposition among Member States, NIS2 introduces harmonized minimum requirements and stronger supervisory measures.[28] Yet, regulatory ambition often collides with infrastructural realities, where private firms retain decisive control over the systems that regulators are meant to oversee.[29]

Despite these legal advances, institutional asymmetries persist. The implementation of DORA and NIS2 relies heavily on national agencies with varying levels of readiness and expertise. This limits the EU's ability to act uniformly and undermines the *ex-ante* character of these regulations, especially in areas where strategic infrastructure is controlled by global technology firms.[30]

Korea presents a different but equally illustrative case. The AI Basic Act, passed in 2024, seeks to establish a centralized framework for AI governance. It mandates ethical impact assessments, algorithmic transparency, and human oversight in high-risk domains. Unlike the EU's fragmented enforcement model, the Act assigns primary regulatory authority to the Ministry of Science and ICT, with the goal of centralizing oversight and coordinating AI-related policy across sectors.[31]

However, the implementation of this framework remains heavily dependent on voluntary compliance and self-regulation by dominant domestic tech firms like Naver and Kakao, both of which play significant roles in developing foundational AI infrastructure in Korea.[32] The state's reliance on these firms for technical expertise and infrastructure provision introduces potential conflicts of interest and weakens the autonomy of regulatory decision-making.

Moreover, similar to the EU, Korea faces challenges in recruiting and retaining AI and cybersecurity specialists within public institutions. This has created asymmetries in technical competence between regulators and private firms, contributing to a governance environment in which policy often trails behind technological development.[33] As a result, enforcement is reactive, and policy interventions are limited to surface-level risk management rather than substantive intervention in design or deployment practices.

This dilemma is closely interwoven with the other structural dilemmas presented in this section. Infrastructural dependency shapes the state's limited capacity to regulate, as governments must often operate within privately controlled technical systems. Epistemic asymmetry further exacerbates these constraints by limiting the state's interpretive authority and its ability to contest private definitions of risk and harm. Governance capacity gaps, in turn, reinforce these dependencies by eroding the institutional base from which sovereign interventions might be launched.

In this sense, the dilemma of governance capacity is not only a question of institutional weakness but also a systemic feature of a digital ecosystem where private actors hold the infrastructural and epistemic levers of control. Addressing this dilemma requires more than institutional reform or additional regulation. It demands a reconfiguration of the public-private relationship in cybersecurity governance, wherein public institutions are equipped not only with formal legal authority but also with the material, technical, and organizational capacities necessary to exercise meaningful digital sovereignty.

28. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) 2022; ENISA (n 7).
29. Johan David Michels and Ian Walden, 'Cybersecurity, Cloud, and Critical Infrastructure', *Cloud Computing Law* (Oxford University Press 2021).
30. Christakis (n 20).
31. Do Hyun Park, Eunjung Cho and Yong Lim, 'A Tough Balancing Act – The Evolving AI Governance in Korea' (2024) 18 *East Asian Science, Technology and Society* 135.
32. Junhwan Mun, 'Analysis of the Present and Future of the Korea Online Platform Regulation Using Latent Dirichlet Allocation' (2024) 29 *Global Business & Finance Review* 16.
33. Jongheon Kim, 'Defining Risk in AI Legislation: Perspectives and Implications in the Korean Context' (2024) 10 *Communication Research and Practice* 316.

2.5 Structural Dilemmas and the Reconfiguration of Sovereignty

The structural dilemmas outlined in this section collectively illuminate the shifting landscape of authority within cybersecurity governance. Each represents a distinct yet interconnected limitation on how states can exercise digital sovereignty in environments where key governance functions are no longer under exclusive public control. Infrastructural dependency erodes operational autonomy, epistemic asymmetry displaces interpretive authority, and governance capacity gaps weaken enforcement. These dilemmas interact, forming a feedback loop that limits the ability of states to assert control over digital systems and security.

Together, these structural dilemmas constitute a conceptual framework for analyzing digital sovereignty in cybersecurity governance. This framework moves beyond legal formalism to diagnose the material and institutional conditions under which sovereignty is fragmented, co-opted, or displaced. It situates cybersecurity governance within a broader context of infrastructural politics, epistemic authority, and regulatory design, offering a lens through which the limitations and possibilities of public authority in the digital domain can be critically assessed.

This framework allows us to reconceptualize digital sovereignty not as a binary attribute possessed or lost, but as a contested and distributed condition shaped by socio-technical configurations and institutional dynamics. It also helps identify the blind spots in current legal frameworks that fail to account for the structural entanglements between states and corporations in cybersecurity governance. The next section operationalizes this framework through three empirical case studies: (1) the deployment of AI in predictive policing systems, (2) public sector use of corporate cloud services, and (3) the strategic use of satellite internet infrastructure. Each case illustrates how infrastructural dependency, epistemic asymmetry, and governance capacity gaps constrain the exercise of digital sovereignty within contemporary cybersecurity governance.

3. Empirical Investigations into Sovereignty under Cybersecurity Interdependence

This section applies the conceptual framework developed in the Section 2 to three case studies, each of which illustrates how digital sovereignty is structurally constrained by the presence of private actors in cybersecurity governance. These cases are selected for their strategic relevance, diversity of jurisdictional and institutional contexts, and the ways in which they represent specific dilemmas discussed earlier. Rather than serving as general examples, each case offers a detailed empirical instance where state authority is entangled with private infrastructures in ways that raise fundamental questions about digital sovereignty.

The three cases are:

- **Amazon Web Services (AWS) Sovereign Cloud (EU):** A case that foregrounds infrastructural dependency and legal ambiguity, revealing tensions between regulatory rhetoric and operational control.
- **Project Maven (United States):** An example of how the classification of threats is outsourced to private actors, illustrating epistemic asymmetry and governance capacity gaps.
- **LG CNS Smart Surveillance (Korea):** A case of public-private infrastructural integration that demonstrates how legal frameworks struggle to keep pace with private-sector dominance in surveillance technology.

These cases were selected not because they represent all possible configurations of sovereignty erosion, but because they highlight different modes of entanglement between legal authority, technical infrastructure, and private power. Each case contributes to a layered understanding of how cybersecurity governance is increasingly shaped by actors, tools, and systems beyond the direct control of the state.

3.1 AWS Sovereign Cloud and the Illusion of Infrastructural Control

AWS launched its Sovereign Cloud initiative in the EU to address growing concerns about foreign control over critical data infrastructure. The concept promised localized data processing, enhanced transparency, and compliance with EU data protection laws, particularly GDPR. However, AWS remains a U.S.-based company subject to the extraterritorial reach of the U.S. Clarifying Lawful Overseas Use of Data Act (CLOUD Act), which allows American authorities to request access to data stored overseas by U.S. tech firms.

This case is a clear instance of infrastructural dependency. Despite hosting data within the EU, operational control, software updates, and technical support remain tied to a foreign entity. The ability of European regulators to enforce jurisdiction is fundamentally limited when the technical and organizational layers of infrastructure remain external to their authority.[34] The legal infrastructure may be European, but the material and operational infrastructure remains American.

The European Commission and national governments have sought to address this vulnerability through various mechanisms. The NIS2 Directive imposes obligations on essential and important entities to adopt cybersecurity risk management frameworks and report incidents. The DORA Regulation establishes direct oversight powers for regulators in the financial sector to audit critical ICT service providers. Meanwhile, the GAIA-X project was launched as a federated cloud infrastructure designed to secure digital sovereignty by enabling European firms and institutions to build interoperable services based on common standards.[35]

However, the slow progress and limited commercial uptake of GAIA-X reveal the difficulties of building sovereign infrastructure in a market dominated by incumbent actors. Sovereignty here becomes more rhetorical than operational. Without ownership of technical architectures and administrative control over systems, legal assertions of autonomy risk becoming symbolic gestures rather than effective safeguards.

3.2 Project Maven and the Reconfiguration of Threat Epistemology

Project Maven was initiated in 2017 by the U.S. Department of Defense to integrate AI into military operations, particularly in analyzing drone surveillance footage. The project's core function was to enable automatic detection and classification of objects and individuals from video streams captured by unmanned aerial vehicles. To develop this technology, the Pentagon partnered with Google, leveraging the company's machine learning capabilities through its TensorFlow framework. Though Google later withdrew from the project following internal protests, Project Maven continued with other vendors, including Palantir and Anduril.

This case exemplifies the dilemma of epistemic asymmetry. The state's traditional monopoly over security knowledge, particularly the identification of threats, was partially outsourced to a private actor. What was once a military intelligence function became a technical process managed through proprietary algorithms and datasets, inaccessible to democratic scrutiny or legal contestation.[36] Decisions over what constitutes a valid target or suspicious activity were encoded into machine-learning models developed with limited public oversight, raising concerns about algorithmic accountability and delegated judgment.[37]

Moreover, the project reveals a clear governance capacity gap. Public institutions lacked the technical capacity to build such systems independently or to audit their internal decision logic. The reliance on black-box technologies limits the legal system's ability to attribute responsibility and foresee harm. In a military context, this raises serious questions about proportionality, accountability, and compliance with international humanitarian law.[38]

Project Maven matters theoretically because it reveals how sovereignty is not only territorial or legal but also epistemic. When the knowledge required to define threats is embedded in private software, the state loses its ability to act autonomously even while retaining formal jurisdiction. The delegation of sense-making to private platforms represents a structural transformation in how security is governed and who gets to define its parameters.

34. Bradford (n 12); Kuner and others (n 24).
35. Michels and Walden (n 29).
36. Louise Amoore, *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others* (Duke University Press 2020); Pasquale (n 21).
37. Kate Crawford, *The Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence* (Yale University Press, 2021).
38. Shermon Cruz and Nicole Parreno-Moura, 'Exploring Pathways of Smart City Futures: Insights from Engaged Foresight' in Roberto Poli (ed) *Handbook of Futures Studies* (Edward Elgar Publishing 2024).

3.3 LG CNS and Smart Surveillance in Korea

LG CNS, a major IT subsidiary of the LG Group, plays a central role in Korea's national smart city initiatives. Under programs such as U-Safety, Smart City Seoul, and Safe City Busan, LG CNS provides integrated platforms that connect CCTVs, facial recognition systems, behavioral analytics tools, and emergency dispatch systems.[39] These infrastructures are deployed in collaboration with local and central government agencies, aimed at improving crime prevention, traffic management, and public safety.

Unlike in the European context, where regulatory oversight of private actors in public infrastructure remains fragmented but institutionally developed, Korea's model is one of public-private fusion. Although legal frameworks such as the Personal Information Protection Act (PIPA) and the recently enacted AI Basic Act exist, they provide broad principles without enforceable mechanisms for algorithmic transparency or real-time oversight of automated surveillance.

This case illustrates the dilemmas of both infrastructural dependency and governance capacity gaps. First, municipalities are structurally reliant on LG CNS not only for hardware and software, but also for ongoing maintenance, system upgrades, and algorithmic decision-making. Without access to technical documentation or the ability to independently operate the systems, the state's capacity to exercise sovereignty over surveillance decisions is compromised.

Second, the legal oversight mechanisms are weak or underdeveloped. The Korea Communications Commission and Personal Information Protection Commission are tasked with overseeing compliance, but their regulatory reach does not extend into the algorithmic core of AI-driven systems.[40] This is particularly problematic given the absence of independent auditing requirements or technical benchmarks for accuracy, fairness, or bias.

Theoretically, this case highlights the fusion of innovation policy with security governance, where the promotion of national competitiveness in AI development indirectly enables private firms to shape the epistemology and infrastructure of public safety. Sovereignty becomes a shared endeavor, in which private actors hold *de facto* power over governance functions that are formally retained by the state.

3.4 Sovereignty Reconfigured: Insights from Comparative Cases

Taken together, the three cases demonstrate that digital sovereignty in cybersecurity governance is not just being eroded but structurally transformed. Each of the three dilemmas reveals a different dimension through which state sovereignty is reconfigured in the digital age. The traditional Westphalian conception of sovereignty assumes that states exercise supreme authority within their territory, underpinned by control over coercive, informational, and legal means. However, in cybersecurity governance, these prerogatives are increasingly mediated by private infrastructures that transcend territorial borders. Digital networks and algorithmic systems have created post-territorial forms of authority, where technical control rather than formal jurisdiction determines power.[41]

These case studies demonstrate that digital sovereignty in cybersecurity governance is structurally conditioned by technical architectures, knowledge asymmetries, and institutional constraints. What differentiates these dilemmas from previous public-private governance challenges is their embeddedness in critical digital infrastructure. States are no longer simply contracting private services; they are increasingly dependent on opaque systems that operate beyond their control, understanding, or ability to replicate. This

39. David Rogers, '"Smart" City in South Korea to Monitor Residents' Health' (*Global Construction Review*, 20 May 2022) https://www.globalconstructionreview.com/smart-city-in-south-korea-to-monitor-residents-health/ accessed 7 November 2025; Su-hyun Song, '[ASEAN-Korea Summit] LG CNS Taking Lead in Korea's Smart City Projects' *The Korea Herald* (25 November 2019) https://www.koreaherald.com/article/2164447 accessed 7 November 2025; Hyun-joon Na and Minu Kim, 'LG CNS Selected as Preferred Bidder for $4.23 Bn Busan Smart City Project' (*Busan Metropolitan City*, 19 May 2022) https://www.investkorea.org/bsn-en/bbs/i-1464/detail.do?ntt_sn=491200 accessed 7 November 2025.

40. Kim & Chang, 'The Korea Communications Commission Issues the Guidelines on the Protection of Users of Generative AI Services' (*Kim & Chang*, 7 March 2025) https://www.kimchang.com/en/insights/detail.kc?sch_section=4&idx=31605 accessed 7 November 2025; Thibault Schrepel, 'The New AI Regulation in Korea: Problems of Jurisdictional Overlaps' [2025] Network Law Review.

41. Laura DeNardis, *The Internet in Everything* (Yale University Press 2020).

condition challenges traditional concepts of sovereignty as the capacity to decide and act independently within one's jurisdiction. As cybersecurity threats become more dynamic, cross-border, and algorithmically mediated, the governance of digital security is no longer solely a question of regulatory design. It is a question of whether states can access, audit, and influence the infrastructures through which security is defined and delivered.

4. Reclaiming Digital Sovereignty: Theoretical and Policy Implications

4.1 Theoretical Implications: From Control to Capacity

The central theoretical implication of this study is that sovereignty in the digital age must be understood as capacity rather than control. Traditional sovereignty depends on the state's ability to decide, enforce, and monopolize legitimate power within its territory. In cybersecurity, however, control is distributed across transnational infrastructures owned and managed by private actors. What matters is not whether the state can exclude these actors, but whether it can shape, audit, and govern the dependencies that bind it to them.

This shift entails three conceptual developments:

From Territorial to Infrastructural Sovereignty: Sovereignty now resides in control over the technical architectures that underpin communication, data storage, and computation. Control over infrastructure constitutes a new vector of geopolitical influence. For policymakers, this means that strategies of national security must be inseparable from strategies of infrastructure development and standard-setting.

From Legal Jurisdiction to Epistemic Access: The legitimacy of state authority increasingly depends on epistemic capacity, including the ability to interpret, validate, and contest algorithmic decisions. This requires new institutions for algorithmic literacy within government and judicial systems. Without such epistemic access, sovereignty risks becoming performative rather than operative.

From Sovereignty as Autonomy to Sovereignty as Stewardship: Because interdependence is unavoidable, sovereignty must be reconceptualized as the stewardship of dependencies, the ability to ensure that the systems upon which the state relies remain aligned with public values of accountability, transparency, and security. This reframing directs policy away from isolationist ambitions toward governance architectures that embed public oversight within interdependent systems.

4.2 Practical Implications: Governing Dependencies

Translating these theoretical insights into policy requires moving beyond risk-based compliance toward institutionalized mechanisms of infrastructural governance. The following directions are not abstract recommendations but policy pathways that could realistically inform legislative or administrative action.

Infrastructural Investment and Strategic Autonomy: Policymakers should treat digital infrastructure as a domain of public investment, akin to energy or transport. Initiatives like the EU's *Chips Act* and Korea's *Digital New Deal* point in this direction but remain primarily economic. To advance sovereignty, such programs must explicitly link industrial policy with security governance. Public-private consortia for cloud sovereignty, joint research centers for secure AI systems, and sovereign communication networks could reduce critical dependencies while maintaining interoperability.

Institutionalizing Epistemic Oversight: Regulators need technical capacity to interrogate algorithmic systems used in cybersecurity and critical infrastructure. This can be achieved through:

- **Algorithmic auditing authorities** embedded within national cybersecurity agencies, with statutory powers to demand documentation, test model behavior, and publish independent assessments.
- **Public registries of algorithms** deployed in security and administrative contexts, modeled on the transparency requirements in the EU's AI Act but extended to cover private-public systems.
- Such measures would operationalize epistemic sovereignty without requiring full technological self-sufficiency.

Embedding Accountability in Procurement and Contracting: Much of state dependence on private actors originates in procurement. Governments can reclaim partial sovereignty by redesigning procurement contracts to include: Source-code escrow clauses ensuring public access in emergencies; Obligations for interoperability and data portability; and Mandated participation in joint security audits. These contractual instruments convert market relationships into sites of governance, aligning private incentives with public accountability.

Building Cross-Sectoral Capacity and Expertise: Sovereignty is exercised through institutions capable of understanding and responding to technological complexity. States should establish interdisciplinary digital governance units that combine legal, technical, and policy expertise, similar to the EU AI Office or Korea's AI Safety Institute. Partnerships with universities and civil society organizations can further enhance the epistemic resilience of public institutions, ensuring that expertise remains distributed yet accountable.

Enhancing Transnational and Regional Coordination: Cybersecurity threats and infrastructural dependencies are inherently transnational. Effective sovereignty thus requires cooperative mechanisms of shared governance rather than unilateral control. Regional frameworks, such as the EU-Korea Digital Partnership and the OECD's Global Forum on Technology, can serve as platforms for mutual capacity-building, coordinated audits, and the exchange of best practices. Such collaboration moves sovereignty from a defensive posture to a collective governance function grounded in shared standards.

4.3 Policy Integration: From Normative Assertion to Operational Design

The core policy challenge is integration: aligning normative goals of sovereignty with operational realities of interdependence. Policymakers can advance this integration through three strategies.

Design-Based Regulation: Regulatory goals should be embedded directly into system design. Concepts such as *security-by-design* and *accountability-by-architecture* translate legal values into technical requirements, ensuring that sovereignty principles are realized within infrastructures themselves.

Adaptive Governance: Given the pace of technological change, static legal instruments are insufficient. States should establish adaptive review mechanisms that periodically reassess dependencies, update risk classifications, and adjust oversight protocols. This continuous process of recalibration constitutes a practical expression of sovereign capacity.

Public Value Benchmarking: Sovereignty should be evaluated not solely in terms of control but by the system's ability to preserve public values such as privacy, accountability, and resilience. Governments can implement *sovereignty impact assessments* analogous to data protection impact assessments, requiring agencies to evaluate how reliance on private infrastructures affects public authority.

For policymakers, the central lesson of this analysis is that sovereignty in the digital age is a function of institutional design rather than territorial control. The challenge is not to reclaim absolute authority, but to embed public oversight within interdependent systems. Sovereignty must be enacted through infrastructures—via protocols, standards, and governance mechanisms that enable public institutions to access, audit, and influence the digital architectures on which they depend. This reframing presents sovereignty as networked, relational, and infrastructural: it is realized not through isolation, but through the capacity to shape and steward dependencies in alignment with democratic values. The future of governance depends on institutional co-design, where sovereignty is exercised through the ongoing configuration of the systems that bind them together.

4.4 Reconstituting Sovereignty in the Age of Digital Interdependence

This study has examined how the rise of private, transnational technology corporations is transforming the foundations of cybersecurity governance and, by extension, the modern state's claim to sovereignty. Through the analytical lens of three structural dilemmas, including infrastructural dependency, epistemic asymmetry, and governance capacity erosion, it has shown that state authority is increasingly mediated through privately owned systems that define, secure, and regulate the digital domain.

The three comparative cases - AWS Sovereign Cloud in the EU, Project Maven in the U.S., and LG CNS Smart Surveillance in Korea - demonstrate that this transformation is neither accidental nor sector-specific. It reflects a broader structural shift in which the capacity to govern depends less on territorial control and more on access to, and stewardship of, technological infrastructures. The theoretical contribution of the paper lies in reframing sovereignty as capacity, the institutional and epistemic ability to govern interdependence, rather than as exclusive command.

Three conceptual implications emerge from this analysis. First, sovereignty has become infrastructural: control over the physical and logical architectures of cyberspace determines the reach of public authority. Second, it has become epistemic: the ability to interpret algorithmic systems and data flows defines who can legitimately act and decide in digital governance. Third, sovereignty has become relational: it is enacted through interdependence, not despite it. These dimensions together constitute what may be called a *sovereignty of design*, the embedding of public values within the infrastructures and standards that organize digital life.

This reconceptualization challenges state-centric models of international law and security studies, which assume that authority can be asserted through formal jurisdiction. It also extends debates in technology governance by linking questions of AI accountability, cybersecurity, and platform power to the enduring problem of political legitimacy.

The persistence of infrastructural and epistemic dependency does not imply the erosion of sovereignty but signals its reconstitution. Rather than seeking to insulate state power from technological systems, the task is to govern through those systems in ways that align with democratic principles of transparency, accountability, and justice.

Reclaiming digital sovereignty is therefore not a project of restoration but of construction. It demands that policymakers, technologists, and legal scholars collaborate to design governance systems capable of both leveraging and constraining private power. The question is no longer how to protect sovereignty from technology, but how to govern through technology in ways that preserve public purpose. By reframing sovereignty as the capacity to govern interdependence, this paper contributes to a growing body of work that seeks to anchor political legitimacy in the infrastructures of the digital age. In doing so, it calls for a new social contract, one in which the technical architectures of cybersecurity are recognized as constitutional foundations of modern governance itself.

5. Acknowledgements

The author gratefully acknowledges the anonymous reviewers and the editorial team for their thorough evaluation of the manuscript and for offering substantive, well-considered critiques. Their input greatly strengthened the clarity, coherence, and overall contribution of this study.

The author also extends sincere gratitude to Professors Bryce Jensen Dietrich, Daniel Stuart Schiff, and Kaylyn Jackson Schiff for their unwavering support, guidance, and encouragement throughout the development of this project. The author further appreciates the valuable feedback and thoughtful comments received during the *Security, Digital Infrastructure & Fundamental Rights Workshop* (Rotterdam, 2025), which meaningfully enhanced the clarity and direction of this work.