International Journal of New Political Economy 7(2): 67-96, 2026

Research Article

Digitalising the Global Economy and the Future of State Sovereignty: Towards a Theory of Multi-layered Networked Sovereignty

Fariborz Arghavani Pirsalami*[1], Farzin Nejati[2], Mohammad Sadegh Mahmoudi[3]

ARTICLE INFO

Article history:

Date of submission: 31 December 2025

Date of revise: 06 June 2026

Date of acceptance: 16 June 2026

JEL Classification:

F52; O33; O38; L86; K24; D85.

Keywords:

Digital economy; State sovereignty; Multi-layered networked sovereignty; Fourth Industrial Revolution; International politics.

ABSTRACT

This article examines how the digitalisation of the global economy, particularly within the Fourth Industrial Revolution, reshapes the meaning and exercise of state sovereignty in international politics. It asks how sovereign authority is reorganised through digital infrastructures, cross-border data flows, platform governance, cloud systems, technical standards, and transnational regulatory networks. The article adopts a qualitative, conceptual, and descriptive-analytical approach informed by network theory, and synthesises debates on digital sovereignty, infrastructural power, platform authority, data governance, fiscal sovereignty, digital taxation, and networked interdependence. It argues that digitalisation neither eliminates sovereignty nor leaves its classical territorial model intact. Rather, sovereignty is reassembled as a multi-layered networked capacity operating across infrastructural, rules-and-institutions, and legitimacy layers. The analysis shows that digitalisation can strengthen state capacity through regulation, public service delivery, cybersecurity, taxation, and infrastructure-building, while deepening dependence on private platforms, foreign cloud providers, external standards, payment infrastructures, and cross-border data regimes. Effective sovereignty in the digital economy therefore depends on states' ability to secure critical infrastructures, shape rules and standards, manage platform power, diversify strategic dependencies, and sustain legitimacy across domestic and international arenas while preserving accountability and rights in digital governance.

1. Associate Professor, Department of Political Sciences, Faculty of Law and Political Sciences, Shiraz University, Shiraz, Iran.
2. Ph.D Candidate in Political Sciences, Department of Political Sciences, Faculty of Law and Political Sciences, Shiraz University, Shiraz, Iran.
3. Ph.D Candidate in Political Sciences, Department of Political Sciences, Faculty of Law and Political Sciences, Shiraz University, Shiraz, Iran.
*** Corresponding Author Email Address**: farghavani@shirazu.ac.ir
DOI: https://doi.org/10.48308/jep.2026.243112.1261
Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

State sovereignty remains a foundational principle of the modern international order, linking territorial authority, legal jurisdiction, political autonomy, and recognition within a system of states (Biersteker & Weber, 1996:21; Krasner, 1999:3; Sassen, 2006:5). Classically, sovereignty was associated with the capacity of state institutions to legislate, provide security, govern populations, regulate economic life, and exercise authority within territorially bounded space. The digital economy has not abolished this foundation, but it has altered the conditions under which it operates. During the Fourth Industrial Revolution, production, trade, finance, communication, and public services have become increasingly dependent on data-intensive systems, digital platforms, cloud infrastructures, and technical standards that frequently operate across borders (Schwab, 2017:10; World Bank, 2016:3, 11; UNCTAD, 2019:1; UNCTAD, 2024:4). Data may be transferred, stored, and processed across jurisdictions; payment systems and cloud services may rely on infrastructures beyond direct national control; and platforms increasingly shape access, visibility, interaction, and exchange through private rules, algorithms, and technical architectures (DeNardis, 2014:2; Pohle & Thiel, 2020:3; Musiani, 2022:788). The problem, therefore, is not simply whether sovereignty is weakening. The more important issue is how, where, and through which infrastructures sovereignty is exercised, and which elements of sovereign authority are being reconfigured. The Fourth Industrial Revolution is not merely a collection of discrete technologies. Artificial intelligence, the Internet of Things, cloud computing, blockchain, and advanced data infrastructures interact to reshape production, exchange, administration, and governance. Power is often concentrated in network nodes and chokepoints through which data, transactions, standards, and access are organised. Actors that control these nodes can shape users, firms, and governments even without formal sovereign authority.

Recent scholarship has examined digital sovereignty, platform governance, infrastructure politics, and the geopolitical use of interdependence (Gorwa,

2024:3). Yet these debates often remain dispersed across separate literatures. What remains insufficiently developed is an integrated International Relations account of how sovereignty is reconfigured across the infrastructural, regulatory, and legitimacy dimensions of the global digital economy. The article's central question is therefore: how does the digitalisation of the global economy, within the Fourth Industrial Revolution, redefine the meaning of sovereignty and how sovereignty is exercised in international politics? The article argues that digitalisation signifies neither the "death" of sovereignty nor the unaltered persistence of its classical model. It reassembles sovereignty as a multi-layered networked capacity. Territorial sovereignty remains formally central, but its effective exercise increasingly depends on the state's ability to govern digital infrastructures, regulate network chokepoints, participate in standards and data regimes, and connect domestic regulation to international arrangements. Sovereignty is therefore treated not only as a legal principle, but also as an effective capacity involving territorial control, infrastructural authority, state-citizen relations, taxation, rule-making, legal enforcement, and international influence. The article's contribution is to bring these dimensions together in a framework useful for International Relations and relevant to debates on digital policy, institutional resilience, and technological dependence.

Methodologically, the article adopts a qualitative, conceptual, and descriptive-analytical approach. It uses network theory to examine how authority and dependence are structured among states, firms, platforms, technical bodies, international institutions, and users. This lens identifies the positions and chokepoints through which influence is exercised (Kahler, 2009:1–3). A state may formally possess sovereignty while lacking effective control over crucial infrastructures, standards, platforms, or data flows. Conversely, it may strengthen effective sovereignty by influencing key nodes, building resilient infrastructures, shaping standards, and linking domestic regulation to international regimes.

The article proceeds as follows. Section 2 integrates the literature review and theoretical grounding, situating the argument in relation to digital

sovereignty, infrastructure power, platform authority, data governance, and networked interdependence. Section 3 explains the research methodology. Section 4 analyses the digital economy and the Fourth Industrial Revolution as the structural context, then examines their implications for territory, infrastructure, population, legitimacy, platforms, and multi-layered networked sovereignty. The final section concludes with policy recommendations..

2. Literature Review

2.1. Digitalisation, Digital Sovereignty, and the Transformation of State Authority

digital change belongs to a separate technological sector. Digitalisation increasingly reorganises production, exchange, labour relations, financial transactions, public services, and the boundary between domestic and global markets. Studies of the digital economy and the Fourth Industrial Revolution show that platforms, cloud services, artificial intelligence, blockchain, data infrastructures, and digitally mediated value chains have become central to contemporary economic life (Jahangard, 2021; Ameli & Haji-Jafari, 2020; Schwab, 2017; World Bank, 2016; UNCTAD, 2019, 2024). Their importance for this article lies in the fact that they treat digitalisation as a structural transformation rather than as a narrow technical development. Economic activity, public administration, communication, and market coordination are increasingly organised through data-intensive and networked systems. The difficulty, however, is that much of this literature approaches digitalisation through productivity, innovation, industrial policy, institutional adaptation, or development. It establishes the scale and depth of digital transformation, but it often treats sovereignty only indirectly. For International Relations, the central issue is not merely that economic activity has become digital. The more important question is how the infrastructures, rules, platforms, and standards enabling this activity alter the conditions under which sovereign authority is exercised. Digitalisation matters politically because many of the systems through which states govern, tax, communicate, regulate, and provide services are no longer fully contained within territorial borders.

Debates on digital sovereignty address this problem more directly. They examine data localisation, cloud dependency, cybersecurity, internet governance, technical standards, jurisdictional conflict, and the political consequences of cross-border data flows (Pohle & Thiel, 2020; Taylor, 2020; Musiani, 2022; Pohle & Santaniello, 2024). This scholarship usefully shows that digital sovereignty is not a settled concept. In some contexts, it refers to strategic autonomy and infrastructural control; in others, it is linked to privacy, democratic accountability, data protection, individual rights, or resistance to external technological dependence (Jiang & Belli, 2025). It also corrects the simplistic assumption that digitalisation necessarily weakens the state. States continue to legislate, regulate, invest, build digital capacity, and negotiate international rules. Yet their authority is increasingly conditioned by infrastructures and technical systems that are transnational, privately governed, or institutionally dispersed.

For the purposes of this article, the crucial limitation of existing digital sovereignty debates is that they often remain attached to policy discourse, regional strategy, or specific regulatory problems. They do not always integrate the territorial, infrastructural, regulatory, fiscal, and legitimacy-based dimensions of sovereignty into a single analytical account. This article therefore builds on the digital sovereignty literature while shifting the emphasis from sovereignty as a policy aspiration to sovereignty as an effective and relational capacity under digital-economic conditions.

2.2. Infrastructure, Platform Power, and the Political Economy of Data

A second body of scholarship is concerned with infrastructure, platform power, and the political economy of data. Work on internet governance has shown that apparently technical arrangements—domain names, IP addresses, protocols, standards, undersea cables, data centres, cloud systems, and access platforms—are also sites of political authority and contestation (DeNardis, 2014; Musiani, 2022). These arrangements shape who can connect, who can regulate, who can extract value, who can monitor flows, and who can interrupt

access. The significance of this literature is that it locates power not only in formal institutions or legal jurisdiction, but also in the technical architectures and infrastructural arrangements through which digital life is organised. This infrastructural perspective is important for sovereignty because it reveals a practical gap between formal authority and operational control. A state may legislate within its territory while depending on foreign cloud systems, private platforms, external standards, payment infrastructures, or cross-border data regimes. Conversely, a state may strengthen its effective sovereignty by securing critical infrastructures, diversifying dependencies, shaping standards, and linking domestic regulation to wider international arrangements. The issue is therefore not whether territorial sovereignty disappears, but whether territorial authority can still be exercised effectively when the infrastructures of economic and social life are networked across jurisdictions.

Platform studies develop this problem from the side of private authority. Research on surveillance capitalism and platform society shows that large digital platforms are not merely intermediaries between producers and consumers. They shape visibility, access, behavioural prediction, content moderation, market participation, and the conditions under which citizens and firms engage in social, economic, and political life (Zuboff, 2019; van Dijck et al., 2018). Recent work on platform regulation further demonstrates that states increasingly seek to discipline, incorporate, or regulate private platform governance, particularly in relation to disinformation, online harms, electoral integrity, market power, algorithmic transparency, and content moderation (Bietti, 2023; Gorwa, 2024; Afina et al., 2024; Kausche & Weiss, 2025). In security-related domains, governments may also depend on technology firms that control critical data, communication channels, and technical capacities (Chachko, 2021). This literature is directly relevant to sovereignty because it shows that public authority and private power increasingly overlap. Platform firms may make decisions with public consequences, while states often require platform cooperation to regulate markets, protect security, tax value, manage information disorder, or preserve public-order functions. Nevertheless, platform

scholarship usually approaches these issues through capitalism, regulation, rights, content governance, or security. It does not always place platform power within a broader International Relations account of state sovereignty.

A third strand links digitalisation to taxation, inequality, and global political economy. Digital business models based on intangible assets, cross-border services, and platform-mediated value creation place pressure on traditional instruments of taxation and fiscal regulation (European Parliament, 2021; OECD, 2021). Studies of data localisation and digital trade show that attempts to restore territorial control over data may increase resilience and regulatory leverage, but can also raise costs, fragment networks, and reduce innovation if pursued defensively (Aaronson, 2019; Taylor, 2020; Sheppard et al., 2021). Critical political economy approaches add that the digital economy may reproduce unequal centre–periphery relations: data, attention, labour, minerals, and environmental burdens may be widely distributed, while value capture remains concentrated in a limited number of technological hubs (UNCTAD, 2019, 2024; Couldry & Mejias, 2019). These debates clarify the fiscal, developmental, and distributional stakes of digitalisation, but they too remain only partially integrated into IR debates on authority, jurisdiction, and sovereignty.

2.3. Theoretical Grounding: Network Theory and Multi-layered Networked Sovereignty

The theoretical grounding of this article begins with a distinction between sovereignty as formal status and sovereignty as effective capacity. In its formal sense, sovereignty refers to territorial authority, jurisdiction, autonomy, and recognition within an international system of states. This dimension remains indispensable. Digitalisation does not dissolve the legal and territorial foundations of sovereign authority. Yet sovereignty has never been reducible to legal title alone. It must also be made practical through administrative reach, infrastructural control, fiscal capacity, rule-making authority, security provision, and public legitimacy. The question addressed here is whether they can exercise sovereignty effectively when data storage,

payment systems, standards, communication channels, and platform-mediated relations are organised through transnational digital networks. This point draws on a wider tradition that treats state power as more than command. Mann's distinction between despotic and infrastructural power is useful because it shifts attention from the formal authority of the state to its capacity to implement decisions across social and territorial space (Mann, 1984:186). The digital economy changes the infrastructures through which that capacity is exercised. Governance increasingly depends not only on bureaucratic institutions, taxation systems, and communication networks, but also on cloud services, data centres, digital identity systems, cybersecurity architectures, payment infrastructures, and technical standards. Infrastructure theory reinforces this claim. Infrastructures are not passive background systems; they organise circulation, enable exchange, create dependence, and structure political possibility (Larkin, 2013:327). In the digital economy, cables, cloud platforms, app stores, protocols, data centres, and payment systems therefore become political sites as well as technical systems.

Network theory provides the second pillar of the framework. Its relevance is not simply that the digital economy contains networks. Its deeper value is that it explains how power, dependence, and vulnerability are produced by position within relational structures. States, firms, platforms, infrastructure providers, technical bodies, international organisations, and users may be understood as nodes whose influence depends on ties, centrality, substitutability, and control over chokepoints (Wasserman & Faust, 1994:18; Borgatti & Halgin, 2011:1168). Interdependence, in this sense, is not necessarily symmetrical or benign. Keohane and Nye's distinction between sensitivity and vulnerability remains important because it shows that connectedness becomes politically consequential when actors cannot easily escape or substitute the networks on which they depend (Keohane & Nye, 1977:19). Later work on networked politics and weaponised interdependence develops this logic by showing how central positions in financial, informational, and infrastructural networks can generate surveillance,

coercive leverage, and strategic advantage (Kahler, 2009, p. 10; Farrell & Newman, 2019: 45, 68).

A third element concerns rules. Digital authority is not produced by infrastructure alone; it is also organised through law, standards, platform terms of service, algorithmic governance, tax rules, cybersecurity norms, data-protection regimes, and international agreements. Cohen's account of informational capitalism is useful here because it shows that information economies are legally and institutionally constructed rather than naturally given (Cohen, 2019). For this article, the implication is direct: effective sovereignty depends not only on control over territory or data location, but also on the capacity to shape the legal and technical rules through which digital markets and infrastructures operate. On this basis, the article defines multi-layered networked sovereignty as the effective exercise of sovereign authority across three interdependent layers. The infrastructural layer includes cables, data centres, cloud systems, payment networks, digital identity systems, platforms, protocols, and technical standards. The rules-and-institutions layer includes domestic regulation, platform rules, algorithmic governance, tax arrangements, cybersecurity norms, data-protection regimes, technical standards, and international agreements. The legitimacy layer concerns whether citizens, firms, and social groups regard digital authority as accountable, secure, rights-protecting, transparent, effective, and politically acceptable.

The concept is therefore neither a claim about the death of the state nor a simple restatement of state resilience. States remain formally central, but some practical capacities through which sovereignty is exercised are mediated by public, private, technical, and transnational actors. A state may retain legal sovereignty while depending on foreign cloud providers, platform ecosystems, payment infrastructures, external standards, or cross-border data regimes. Conversely, it may strengthen effective sovereignty by securing critical infrastructures, diversifying dependencies, shaping standards, regulating platforms, and sustaining legitimacy. The theoretical task is to examine where authority is located, which dependencies matter, who controls

relevant chokepoints, how rules are made, and whether the exercise of digital authority remains legitimate under networked conditions.

2.4. Research Gap and Contribution of the Present Article

Taken together, the existing literatures provide important insights, but they remain fragmented across fields and levels of analysis. The digital economy literature clarifies structural transformation but often treats sovereignty only indirectly. Digital sovereignty debates examine autonomy, data governance, and infrastructure, but frequently remain tied to policy discourse or regional strategy. Platform studies illuminate private authority, but do not always connect it to a broader theory of sovereign capacity. Political economy approaches reveal fiscal, developmental, and centre–periphery inequalities, but they are not always integrated into IR debates on authority and jurisdiction. Network theory explains relational power, yet it is often used to analyse interdependence or infrastructure rather than to reconstruct sovereignty itself.

The research gap, therefore, is not the absence of relevant scholarship. It is the absence of an integrated International Relations framework capable of explaining how sovereignty is being reassembled across infrastructure, rules and institutions, and legitimacy in the global digital economy. This article addresses that gap by developing the concept of multi-layered networked sovereignty. Conceptually, it moves beyond the binary claim that digitalisation either destroys sovereignty or leaves it intact. Analytically, it explains how sovereign authority is exercised through networked relations among states, platforms, technical bodies, infrastructures, firms, citizens, and international regimes. Prospectively, it uses scenario planning to identify plausible trajectories through which this reconfigured sovereignty may develop over the next 10–15 years.

The article's contribution is threefold. First, it reframes sovereignty as a layered and relational capacity rather than a purely territorial attribute or a disappearing legal fiction. Second, it links digital sovereignty, infrastructure politics, platform power, fiscal sovereignty, and networked interdependence

within a single analytical vocabulary. Third, it offers a scenario-based account of how different configurations of infrastructure, rules, and legitimacy may shape the future of state sovereignty in the digital economy.

3. Methodology and Data

This article adopts a qualitative, conceptual, and descriptive-analytical methodology. Its purpose is to develop an analytical framework for explaining how state sovereignty is reconfigured under conditions of digital interdependence. Such a design is appropriate for a study whose central task is conceptual clarification, theoretical synthesis, and the specification of relations among concepts that are discussed across several literatures but are not always brought into direct conversation (Gilson & Goldberg, 2015:130; Jaakkola, 2020:18–26).

The analysis proceeds in four connected stages. First, the article undertakes an integrative and theoretically guided review of scholarship on digital sovereignty, platform governance, internet infrastructure, data governance, digital taxation, political economy, and networked interdependence. The review is not presented as a systematic or bibliometric review. It synthesises conceptually relevant literatures in order to clarify how they speak to a common problem: the changing conditions under which sovereign authority is exercised in the global digital economy. This use of literature review is suitable where the aim is to build an organising framework for a dispersed conceptual field rather than to aggregate empirical results (Snyder, 2019: 334).

Second, the article uses network theory as its principal analytical lens. States, platforms, firms, technical bodies, infrastructures, international organisations, and users are treated as actors positioned within overlapping digital-economic networks. Their relations are examined in terms of dependence, access, control, standard-setting, regulatory capacity, and vulnerability. Concepts such as centrality, connectivity, and chokepoints are not used as formal network metrics in this article. They operate as analytical categories for identifying where authority and dependence are concentrated

(Borgatti & Halgin:1168). This is particularly relevant because power in the digital economy often derives from control over infrastructural hubs and network bottlenecks, not only from formal jurisdiction over territory (Farrell & Newman, 2019: 44).

Third, the article reconstructs sovereignty across three analytical layers: infrastructure, rules-and-institutions, and legitimacy. This layered structure makes it possible to distinguish formal sovereignty from effective sovereignty. A state may retain legal authority while depending on foreign cloud providers, private platforms, external standards, payment infrastructures, or transnational data regimes. Conversely, it may strengthen effective sovereignty by securing critical infrastructures, shaping rules, diversifying dependencies, and sustaining public legitimacy. These layers are not treated as isolated variables, but as interdependent dimensions through which sovereignty is exercised under networked conditions.

Fourth, the article uses qualitative scenario planning to explore plausible trajectories over a 10–15-year horizon. The scenarios are not predictions and do not assign statistical probabilities. They are analytical exercises designed to clarify how different configurations of infrastructural dependence, regulatory capacity, platform power, geopolitical rivalry, state capacity, and legitimacy may shape the future exercise of sovereignty. Scenario planning is appropriate here because it is most useful under conditions of uncertainty, where the purpose is to examine plausible alternatives rather than forecast a single outcome (Amer et al., 2013: 23; Bradfield et al., 2005: 795; Cordova-Pozo & Rouwette, 2023, Article 103153). The article therefore uses conservative causal language. It does not claim that digitalisation produces one necessary sovereign outcome. Instead, it identifies the conditions under which digitalisation may strengthen, constrain, redistribute, or affect the legitimacy of practical capacities associated with sovereignty in the global digital economy.

4. Results and Discusion

This section examines how digitalisation reconfigures the effective exercise of state sovereignty. Since the article is conceptual rather than statistical, the results presented here are analytical findings derived from the literature, the theoretical framework, and the scenario-building logic developed above. It then analyses sovereignty through infrastructure, data flows, legitimacy, platform power, and multi-layered networked sovereignty.

To analyse the implications of the digitalisation of the global economy, it is first necessary to clarify the relationship between the "digital economy" and the "Fourth Industrial Revolution" (4IR). The 4IR refers to a phase of technological change in which physical, digital, and biological systems increasingly intersect. Artificial intelligence, the Internet of Things, blockchain, additive manufacturing, and advanced data infrastructures do not operate as isolated technologies; they form interconnected systems that reshape production, exchange, and governance. Schwab describes this transformation as a step-change enabled by ubiquitous connectivity, cheap sensors, and expanded computing power, whose "scale, scope, and complexity" distinguish it from earlier industrial transformations (Schwab, 2017:13). Against this background, the digital economy can be understood as the portion of economic activity that depends directly on digital infrastructures, data, platforms, cloud services, and data-intensive infrastructures, as well as sectors reorganised through digital integration. Banking, retail, manufacturing, logistics, public administration, and communication increasingly rely on data processing, algorithms, and network connectivity. Estimates cited in policy discussions suggest that digital-economy activities already represented a substantial share of global output by the mid-2010s. The precise figure is less important than the structural implication: the digital economy is no longer peripheral to global value creation (World Bank, 2016; World Economic Forum, 2016). This transformation is uneven. Internet access, firm-level digital adoption, cloud capacity, platform markets, and the market capitalisation of leading digital

firms remain highly concentrated. UNCTAD reports that digital advances have generated substantial wealth, but that this wealth is highly concentrated in a limited number of countries, companies, and individuals (UNCTAD, 2019). Many developing economies continue to face weak digital infrastructure and limited firm-level adoption (Cusolito et al., 2020:3). Connectivity has also expanded rapidly, with internet use, smartphones, connected devices, and digital transactions growing at considerable speed (UNCTAD, 2024). These trends matter for sovereignty because they point not only to digital expansion, but also to uneven control over the infrastructures and platforms through which economic and political life is increasingly mediated.

A further dimension is material and environmental. The digital economy depends on minerals, energy-intensive data centres, hardware supply chains, and electronic waste systems. UNCTAD notes that digital technologies and infrastructures depend heavily on raw materials, while data centres, ICT networks, device production, and digital waste place growing pressure on the environment (UNCTAD, 2024). Digitalisation may therefore generate opportunities for some resource-rich states, but it can also reproduce unequal ecological and economic relations. These patterns—technological acceleration, infrastructural concentration, uneven participation, and material dependency—frame the central question of this article: how does the digital economy reconfigure sovereignty within International Relations?

a. Dimensions of the Digital Economy and Its Implications for State Sovereignty

The digital economy is not simply a cluster of new industries. It has become an infrastructural layer of economic and social organisation, superimposed on national economies and increasingly relevant to how sovereignty is exercised. Cables, data centres, cloud services, platforms, payment systems, and technical standards connect domestic activity to transnational networks that are frequently owned, governed, or mediated by private actors. The central question for states is therefore no longer only what occurs within their

territorial borders, but how much authority they can exercise over data flows, platform rules, and infrastructures that organise economic and social life across borders (Musiani, 2022:785). This section examines two dimensions of that problem: first, the relationship between territory, infrastructure, and data flows; and second, the connection between population, legitimacy, and the political economy of platforms.

b. Territory, Infrastructure, and Sovereignty over Data Flows

In classical International Relations, sovereignty is anchored in territory and geographical borders. The digital economy does not abolish that territorial foundation. Rather, it adds a networked spatial layer in which authority, dependence, and control do not fully coincide with physical borders. Territory remains indispensable because cables, data centres, energy systems, ports, rare minerals, and legal jurisdictions are still geographically located. What changes is that territorial sovereignty increasingly depends on the capacity to secure the interfaces through which domestic territory is connected to global data, cloud, payment, and communication networks (Castells, 2010:459; Musiani, 2022:785). This is why digital sovereignty is often debated through questions of infrastructure and data flows. Financial data, social media, cloud services, and payment systems may be used within one country while depending on infrastructures, firms, or standards located elsewhere. One response has been the expansion of data localisation policies, especially in sectors such as finance, health, and critical infrastructure (Taylor, 2020:1-2; Wu, 2021:4). Supporters argue that such policies can strengthen jurisdictional control, protect sensitive data, and reduce exposure to sanctions, cyber-attacks, or service disruption. Critics warn that localisation can increase costs, fragment the internet, reduce innovation, and weaken the benefits of global connectivity. The deeper issue is not localisation itself, but infrastructural dependence. When a small number of firms control cloud services, search engines, mobile operating systems, app ecosystems, and payment platforms, private decisions can acquire public consequences. Changes in privacy rules,

suspension of services, compliance with foreign sanctions, or interruptions in platform access can affect a state's ability to reach citizens, regulate markets, or maintain access to global economic networks. For this reason, digital sovereignty cannot be reduced to closing digital borders. It concerns the ability to shape, secure, and diversify key infrastructural nodes while remaining connected to wider digital systems. Different states respond to this problem in different ways. Some invest in national data centres, domestic fibre-optic networks, public cloud capacities, or state-backed digital infrastructures to secure minimum operational autonomy in moments of crisis (Bietti, 2023:5; Kaul et al., 2003:3). Others place greater emphasis on open data flows, interoperability, and active participation in international regimes for responsible data governance (Aaronson, 2019:6). The strongest strategies are likely to combine these elements: protecting critical infrastructures and sensitive data while avoiding forms of digital closure that produce technological isolation or long-term economic marginalisation.

c. Population, Legitimacy, and the Political Economy of Platforms

The second dimension concerns the relationship between the state, citizens, and platforms. In the digital economy, everyday life is increasingly converted into data. Interactions, purchases, movements, communications, and media use are recorded, processed, and analysed. This data is a source of value for private platforms, but it also enables states to deliver public services, target subsidies, manage risks, and design more responsive policies (Törnberg, 2023:1). Digital public administration can therefore strengthen state capacity. E-government, digital identity systems, electronic payments, and online services may make the state more visible and more efficient in citizens' daily lives. Yet the same processes raise questions of legitimacy. When digital systems are unstable, exclusionary, insecure, or opaque, they can erode trust rather than reinforce it. When they expand surveillance without accountability, they may strengthen administrative reach while weakening political legitimacy. The legitimacy of digital sovereignty therefore depends not only on technical

capacity, but also on rights protection, transparency, inclusion, security, and public accountability. Platforms complicate this relationship further. Social media, search engines, app stores, and other digital intermediaries increasingly function as social and economic infrastructure. They establish rules for access, visibility, privacy, content moderation, and market participation. As recent work on platform regulation shows, states can no longer treat these private rules as external to public authority. They increasingly seek to regulate platforms through competition law, online safety rules, data protection regimes, algorithmic transparency requirements, and measures addressing disinformation, electoral integrity, and online harms.The challenge also has a fiscal and security dimension. Digital business models based on intangible assets, cross-border services, and platform-mediated value creation are difficult to tax through traditional instruments, making fiscal sovereignty a central issue in global digital governance (European Parliament, 2021: 1–4; OECD, 2019). In security-related domains, governments may also depend on platforms for data, communication infrastructures, and technical cooperation in areas such as foreign interference, violent extremism, and crisis response (Chachko, 2021:60). These relationships blur the line between public sovereignty and private power. Overall, the digital economy produces an ambivalent transformation of population and legitimacy. Digital tools can improve public service delivery, broaden participation, and support data-driven policymaking. At the same time, platform concentration, opaque algorithmic governance, weak privacy protection, and fiscal dependency can constrain state authority and undermine public trust. State sovereignty in this domain is therefore no longer exercised solely through public law and bureaucracy. It is negotiated through interactions among states, platforms, firms, citizens, and transnational regulatory regimes.

d. Networked Sovereignty in the Digital Economy: From Description to Explanation

The preceding sections have shown how the digital economy and the Fourth Industrial Revolution reshape sovereignty across territory, infrastructure,

population, taxation, legitimacy, and platform governance. The key question is what these shifts mean when considered together. They do not show a simple weakening of the state, nor a straightforward return of sovereign control. They point instead to a reconfiguration of sovereignty through networked relations among states, firms, platforms, infrastructures, technical bodies, and international regimes. Network theory helps move the analysis from description to explanation. Castells' account of the network society shows how power in the information age is organised through flows of information, capital, and symbols across flexible networks rather than solely through fixed territorial hierarchies (Castells, 2010:19). This does not make territory irrelevant. It shows that territorial authority is increasingly mediated by the state's position within wider networks of data, infrastructure, finance, standards, and communication. A similar insight appears in the International Relations literature on networked politics. Kahler argues that networks are not merely metaphors for interdependence; they can enable, constrain, and sometimes constitute collective forms of power (Kahler, 2009:1). From this perspective, sovereignty is exercised through relations with other states, firms, international organisations, technical bodies, and civil-society actors, not only through domestic law or border control. In the digital economy, this relational dimension becomes especially important because authority is often embedded in platforms, standards, protocols, data centres, payment systems, and access infrastructures.

DeNardis' work on internet governance illustrates this point clearly. Domain names, IP addresses, technical standards, cables, and access platforms are not politically neutral technical arrangements. They structure who can connect, who can regulate, who can extract value, and who can interrupt access. Power is therefore partly built into technical architectures and institutional arrangements, even when formal sovereignty remains attributed to states (DeNardis, 2014:2). The implication is that some practical capacities associated with sovereignty are increasingly exercised through points of control within networks. The digital economy therefore transforms sovereignty into a multi-layered and networked form. The state remains a

decisive actor, but its authority is exercised in environments shaped by private infrastructures, technical bodies, platform governance, and transnational regulatory arrangements. The next section uses scenario planning not to forecast a single future (Schoemaker, 1995:25), but to examine plausible trajectories through which infrastructural dependence, regulatory capacity, platform power, geopolitical rivalry, and legitimacy may shape the future exercise of sovereignty.

e. Plausible Scenarios for the Relationship Between the Digital Economy and State Sovereignty

Scenario planning is used here to examine alternative trajectories, not to predict a single future. A scenario is treated as a disciplined construction of a plausible future based on current trends, key uncertainties, and interacting drivers; its value is to test assumptions, reveal vulnerabilities, and clarify the implications of different policy choices (Schoemaker, 1995:25; Amer et al., 2013:23; Bradfield et al., 2005:797). The scenarios are constructed through qualitative scenario-building rather than statistical modelling. They derive from three drivers identified above: expanding cross-border data flows and platform-based activity; growing state dependence on digital infrastructures and private technological intermediaries; and the politicisation of data, standards, cybersecurity, and digital regulation. They are constrained by institutional inertia, geopolitical fragmentation, and the financial, technical, and administrative costs of digital autonomy. The 10–15-year horizon is long enough for infrastructural investment, regulation, and platform strategies to have observable effects, but short enough to avoid distant technological speculation. The plausibility labels are therefore heuristic judgements, not empirical probabilities; they indicate how strongly each trajectory follows from these drivers and constraints across the infrastructural, regulatory, and legitimacy layers of networked sovereignty.

A. Continuity with gradual change (High plausibility).

Under this trajectory, existing trends continue at broadly their current pace. States expand digital capacity through infrastructure investment, e-government, and data regulation, while major platforms remain central to economic and informational networks. Cross-border data rules develop incrementally, without a sudden institutional breakthrough. Multi-layered networked sovereignty therefore consolidates gradually: states, firms, and transnational institutions all operate across the infrastructural and regulatory layers, but no actor decisively controls the arrangement. Given institutional inertia and recent regulatory patterns, this scenario has high plausibility over a 10–15-year horizon.

B. Erosion of state sovereignty in favour of non-state actors (Medium plausibility).

In this scenario, platforms and private networks gain influence over access, standard-setting, and content management. Recommender systems, proprietary rules, and corporate standards shape information exposure and may affect public opinion. States remain active, but often respond after private governance has structured the field. Traditional legal mechanisms are only partly effective against global data flows, cloud services, and platform-mediated markets. The main risk is a legitimacy gap, as consequential decisions occur in settings with limited democratic oversight. Because platform power also faces regulation, public scrutiny, and geopolitical contestation, this scenario is assigned medium plausibility.

C. Strengthening state sovereignty through technology (Medium-low plausibility).

This scenario develops the state-centred side of the argument. States adopt longer-term strategies for digital capacity through domestic infrastructure, national platforms, regulatory coordination, technology diplomacy, and stronger public data governance. National data centres, stricter rules for

sensitive cross-border data, personal data protection, and unified digital identity systems may increase state leverage over technology firms and better protect citizens' rights. The risks are clear: stronger state capacity may also enable surveillance, administrative overreach, and a narrower digital public sphere. Given current trends, this scenario is plausible but less likely than gradual continuity or partial platform dominance; it is therefore assigned medium-low plausibility.

D. A new global order centred on digital networks (Low plausibility).
This scenario shifts attention to transnational institutionalization. New or strengthened arrangements emerge around data flows, artificial intelligence, cybersecurity, digital competition, and technical standards. Some functions associated with national sovereignty are pooled or coordinated through multi-level regimes involving states, firms, technical bodies, and civil society. Cyberattacks, AI-related risks, and supply-chain disruption create incentives for cooperation, but geopolitical rivalry, regulatory divergence, and uneven capacity limit global coordination. The scenario therefore has low plausibility as a comprehensive order, though narrower forms of institutionalization remain possible.

E. The development of digitally autonomous states (Low plausibility).
This scenario centres on digital self-reliance. Some states, especially major powers or technologically capable regional actors, seek greater control across cables, satellites, cloud infrastructure, software, standards, chips, and strategic hardware. Digital independence becomes a visible component of sovereignty and may appeal to states exposed to sanctions, insecure supply chains, or geopolitical pressure. The likely outcome is selective autonomy by a limited number of powerful actors, alongside technology-based blocs and sharper global divisions. Because of cost, complexity, and interdependence, this scenario has low plausibility as a general model, though it remains realistic for a few key players.

Table 1. Plausible Scenarios

Code	Scenario title	Overall future picture	Status of state sovereignty	Dominant actors in the network	Main risks	Main opportunities	Estimated likelihood
A	Gradual continuity	Incremental change; steady rule evolution; platforms remain central.	Multi-layered networked sovereignty consolidates slowly.	States; major platforms; transnational regimes.	Regulatory lag; dependence on external nodes; uneven capacity.	Policy learning; gradual capacity-building; stable co-regulation.	High plausibility
B	Platform dominance	Platforms shape access, standards, and content governance; states react.	Weaker effective sovereignty in key digital layers.	Major platforms; private standard-setters; cloud/payment gatekeepers.	Legitimacy gap; privacy harms; concentrated platform power.	Rapid innovation; scalable services; cross-border connectivity.	Medium plausibility
C	Sovereignty strengthened through technology	Active state strategy; domestic infrastructures; smart regulation.	Stronger steering capacity; states become network gatekeepers.	States; regulators/security agencies; selected national champions.	Excessive surveillance; state monopolisation; restricted public sphere.	Greater resilience; reduced dependency; clearer accountability.	Medium-low plausibility
D	New global order centred on data and digital standards	New regimes for data/AI/cyber; multi-stakeholder rule-making grows.	Partial pooling of functions into transnational, multi-level regimes.	States; IOs; technical bodies; platforms; civil society.	Rule capture; slow consensus; enforcement gaps; uneven voice.	Harmonised standards; reduced systemic risk; predictability.	Low plausibility
E	Digitally autonomous states	Digital self-reliance by a few; stronger blocs; more fragmentation.	Strong sovereignty for some; wider centre–periphery divides.	Major powers; aligned blocs; reduced open-regime influence.	High costs; duplication; bloc formation; exclusion of smaller states.	Supply-chain security; sanction resilience; bargaining leverage.	Low plausibility

Source: Authors' compilation

The plausibility weights are analytical judgements, not statistical measurements. Gradual continuity is closest to current trends and institutional inertia. Platform dominance has considerable weight, but regulatory pressure, public scrutiny, and geopolitical contestation make complete private predominance less likely. State-led strengthening is feasible where fiscal, administrative, and technical capacity exist; global institutionalization is limited by rivalry and fragmentation; and digital autonomy is strategically attractive but costly and viable mainly for a small group of states. The scenarios therefore clarify three questions: who controls key infrastructures, who writes and enforces digital rules, and how legitimacy is maintained in systems mediated by platforms and data flows.

Theoretical and Practical Implications of the Scenarios for Understanding Networked Sovereignty

Considered together, the scenarios do not describe either the "decline" or the "return" of sovereignty. They point to displacement and recombination: the state may gain authority in some layers, such as data regulation or critical infrastructure, while private actors or transnational institutions become more prominent in others. This is consistent with "networked politics", in which power is distributed across nodes and ties and states must consolidate their position within networks to exercise sovereignty effectively (Kahler, 2009:7). Theoretically, sovereignty in the digital economy is best understood as multi-dimensional and networked. Territorially, the state remains central to physical security and infrastructural protection; in the data layer, it must negotiate regulatory settlements with firms and technical institutions; and in the legitimacy layer, it must address privacy, platform power, and the public value of digital services (van Dijck et al., 2018; Brynjolfsson & McAfee, 2014:123, 205). Practically, the scenarios identify different policy priorities: regulatory capacity and technology diplomacy under gradual continuity; competition, platform governance, content regulation, and privacy protection under platform dominance; and domestic infrastructure and reduced sensitive

dependencies under digital autonomy. The broader implication is that sovereignty is not a scale from "strong" to "weak", but a relational capacity shaped by how states manage connections across actors and layers.

5. Conclusion and Policy Recommendations

This article has examined how the digitalisation of the global economy reconfigures the meaning and exercise of state sovereignty in international politics. Its argument is not that sovereignty has disappeared, or that the classical territorial model remains unchanged. Rather, digitalisation alters the conditions under which sovereignty becomes effective. Contemporary authority is still exercised through territory, but it also depends on data infrastructures, cloud systems, platforms, payment networks, technical standards, digital identity systems, and cross-border regulatory arrangements.

The concept of multi-layered networked sovereignty captures this transformation. Sovereignty remains formally centred on the state, yet its practical exercise increasingly depends on three interdependent layers: infrastructure, rules-and-institutions, and legitimacy. The infrastructural layer concerns the systems through which data, communication, payments, identification, public services, and market access move. The rules-and-institutions layer concerns the legal, technical, fiscal, regulatory, and platform-based arrangements that structure digital space. The legitimacy layer concerns whether citizens, firms, and social groups experience digital authority as accountable, secure, rights-protecting, transparent, effective, and politically acceptable.

The analysis has shown that digitalisation redistributes practical sovereign capacities unevenly. It can strengthen state authority through digital public services, cybersecurity, taxation, infrastructure-building, and regulatory coordination. It can also constrain authority through dependence on foreign cloud providers, private platforms, external standards, payment infrastructures, and transnational data regimes. The scenarios developed in the article reinforce this point: gradual adaptation, platform dominance, stronger

state steering, global digital governance, and selective digital autonomy represent different combinations of infrastructure, rules, and legitimacy, not a single predetermined future. Several policy implications follow. First, states should treat critical digital infrastructure as a core component of sovereignty rather than as a purely technical or commercial field. This requires mapping dependencies in cloud services, data centres, connectivity, payment systems, digital identity, cybersecurity, and platform access, and then building resilience, redundancy, and diversification without retreating into costly digital isolation. Second, digital regulation should be designed as a connected field. Platform governance, competition policy, data protection, digital taxation, cybersecurity, algorithmic accountability, and cross-border data rules jointly shape the conditions under which authority is exercised. Third, legitimacy must be treated as a condition of digital sovereignty. Opaque, exclusionary, insecure, or excessively intrusive digital systems may expand administrative reach while weakening political authority. Durable digital sovereignty therefore requires transparency, rights protection, procedural accountability, cybersecurity, inclusion, and public trust.

Finally, digital sovereignty has an external dimension. Participation in international standard-setting, data governance, digital taxation, cybersecurity norms, and platform regulation should be understood as part of foreign policy. In a networked digital economy, sovereignty is partly exercised through shaping external regimes, not merely through defending domestic jurisdiction. The article therefore contributes to International Relations by reframing sovereignty as a layered, relational, and institutionally mediated capacity under digital conditions.

Funding

This study received no financial support from any organization.

Authors' contributions

All authors had contribution in preparing this paper.

Conflicts of interest

The authors declare no conflict of interest.

References

Aaronson, S. A. (2019). *Data is different, and that's why the world needs a new approach to governing cross-border data flows*. Digital Policy, Regulation and Governance, 21(5), 441–459. https://doi.org/10.1108/DPRG-03-2019-0021

Afina, Y., Buchser, M., Krasodomski, A., Rowe, J., Sun, N., & Wilkinson, R. (2024). *Towards a global approach to digital platform regulation: Preserving openness amid the push for internet sovereignty*. Chatham House.

Ameli, S. R., & Haji Jafari, M. (2020). *Digital economy*. Tehran: SAMT. [In Persian]

Amer, M., Daim, T. U., & Jetter, A. (2013). A review of scenario planning. *Futures, 46*(1), 23–40. https://doi.org/10.1016/j.futures.2012.10.003

Biersteker, T. J., & Weber, C. (Eds.). (1996). *State sovereignty as social construct*. Cambridge University Press. https://doi.org/10.1017/CBO9780511598685

Bietti, E. (2023). A genealogy of digital platform regulation. *Geo. l. Tech. Rev.*, *7*, 1.http://dx.doi.org/10.2139/ssrn.3859487

Borgatti, S. P., & Halgin, D. S. (2011). On network theory. *Organization Science, 22*(5), 1168–1181. https://doi.org/10.1287/orsc.1100.0641

Bradfield, R., Wright, G., Burt, G., Cairns, G., & van der Heijden, K. (2005). The origins and evolution of scenario techniques in long range business planning. *Futures, 37*(8), 795–812. https://doi.org/10.1016/j.futures.2005.01.003

Brynjolfsson, E., & McAfee, A. (2014). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*. W. W. Norton & Company.

Castells, M. (2010). *The rise of the network society* (2nd ed., with a new preface). Wiley-Blackwell. https://doi.org/10.1002/9781444319514

Chachko, E. (2021). National security by platform. *Stanford Technology Law Review, 25*(1), 55–140.

Cohen, J. E. (2019). *Between truth and power: The legal constructions of informational capitalism.* Oxford University Press. https://doi.org/10.1093/oso/9780190246693.001.0001

Cordova-Pozo, K., & Rouwette, E. A. J. A. (2023). Types of scenario planning and their effectiveness: A review of reviews. Futures, 149, Article 103153. https://doi.org/10.1016/j.futures.2023.103153

Couldry, N., & Mejias, U. A. (2019). The costs of connection: How data is colonizing human life and appropriating it for capitalism. Stanford University Press. https://doi.org/10.1515/9781503609754

Cusolito, A. P., Lederman, D., & Peña, J. (2020). *The effects of digital-technology adoption on productivity and factor demand: Firm-level evidence from developing countries* (Policy Research Working Paper No. 9333). World Bank. https://doi.org/10.1596/1813-9450-9333

DeNardis, L. (2014). *The global war for internet governance*. Yale University Press. https://doi.org/10.12987/yale/9780300181357.001.0001

European Parliament. (2021). *Taxing the digital economy: New developments and the way forward* (EPRS Briefing 698761). European Parliamentary Research Service.

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security, 44*(1), 42–79. https://doi.org/10.1162/ISEC_a_00351

Gilson, L. L., & Goldberg, C. B. (2015). Editors' comment: So, what is a conceptual paper? Group & Organization Management, 40(2), 127–130. https://doi.org/10.1177/1059601115576425

Gorwa, R. (2024). *The politics of platform regulation: How governments shape online content moderation.* Oxford University Press. https://doi.org/10.1093/oso/9780197692851.001.0001

Jaakkola, E. (2020). Designing conceptual articles: Four approaches. AMS Review, 10(1–2), 18–26. https://doi.org/10.1007/s13162-020-00161-0

Jahangard, E. (2021). *Digital economy: Analyses and dynamics* (2nd ed.). Tehran: Amareh Publishing. [In Persian]

Jiang, M., & Belli, L. (Eds.). (2025). Digital sovereignty in the BRICS countries: How the Global South and emerging power alliances are reshaping digital governance. Cambridge University Press. https://doi.org/10.1017/9781009531085

Kahler, M. (Ed.). (2009). *Networked politics: Agency, power, and governance*. Cornell University Press.

Kaul, I., Conceiçao, P., Le Goulven, K., & Mendoza, R. U. (2003). Why do global public goods matter today. Providing global public goods: Managing globalization, 2-20.

Kausche, K., & Weiss, M. (2025). Platform power and regulatory capture in digital governance. *Business and Politics, 27*(2), 284–308. https://doi.org/10.1017/bap.2024.33

Keohane, R. O., & Nye, J. S., Jr. (1977). *Power and interdependence: World politics in transition*. Little, Brown.

Krasner, S. D. (1999). *Sovereignty: Organized hypocrisy*. Princeton University Press. https://doi.org/10.1515/9781400823260

Larkin, B. (2013). The politics and poetics of infrastructure. *Annual Review of Anthropology, 42*, 327–343. https://doi.org/10.1146/annurev-anthro-092412-155522

Mann, M. (1984). The autonomous power of the state: Its origins, mechanisms and results. *European Journal of Sociology / Archives Européennes de Sociologie, 25*(2), 185–213. https://doi.org/10.1017/S0003975600004239

Musiani, F. (2022). Infrastructuring digital sovereignty: A research agenda for an infrastructure-based sociology of digital self-determination practices. *Information, Communication & Society, 25*(6), 785–800. https://doi.org/10.1080/1369118X.2022.2049850

OECD. (2019). *Measuring the digital transformation: A roadmap for the future*. OECD Publishing. https://doi.org/10.1787/9789264311992-en

OECD/G20 Inclusive Framework on BEPS. (2021). Statement on a two-pillar solution to address the tax challenges arising from the digitalisation of the economy. OECD.

Pohle, J., & Santaniello, M. (2024). From multistakeholderism to digital sovereignty: Toward a new discursive order in internet governance? *Policy & Internet, 16*(4), 672–691. https://doi.org/10.1002/poi3.426

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review, 9*(4), 1–19. https://doi.org/10.14763/2020.4.1532

Sassen, S. (2006). Territory, authority, rights: From medieval to global assemblages. Princeton University Press.

Schoemaker, P. J. H. (1995). Scenario planning: A tool for strategic thinking. *Sloan Management Review, 36*(2), 25–40.

Schwab, K. (2017). *The fourth industrial revolution*. Crown Business.

Sheppard, L. R., Yayboke, E., & Ramos, C. G. (2021). *The real national security concerns over data localization*. Center for Strategic and International Studies (CSIS).

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Taylor, R. D. (2020). Data localization: The internet in the balance. *Telecommunications Policy, 44*(8), 102003. https://doi.org/10.1016/j.telpol.2020.102003

Törnberg, P. (2023). How platforms govern: Social regulation in digital capitalism. *Big Data & Society*, *10*(1). https://doi.org/10.1177/20539517231153808

UNCTAD. (2019). *Digital economy report 2019: Value creation and capture – Implications for developing countries*. United Nations.

UNCTAD. (2024). United Nations Conference on Trade and Development. (2024). *Digital economy report 2024: Shaping an environmentally sustainable and inclusive digital future*. UN Trade and Development. https://unctad.org/publication/digital-economy-report-2024

van Dijck, J., Poell, T., & de Waal, M. (2018). The platform society: Public values in a connective world. Oxford University Press. https://doi.org/10.1093/oso/9780190889760.001.0001