IMPACTIA

Article

Bending the Bulwarks of Digital Sovereignty: Evaluating Cyber-Security Technologies, Cultural Resistance, and State Power in Indonesia

Neng Yayu Wandira [1,†*], Aryo De Wibowo Muhammad Sidik [1]

[1] Universitas Nusa Putra; neng.yayu.wandira@nusaputra.ac.id
* Correspondence: neng.yayu.wandira@nusaputra.ac.id
† Current address: Universitas Nusa Putra.
‡ These authors contributed equally to this work.

Abstract: As digital transformation accelerates, post-colonial nation-states increasingly seek to construct regulatory and technological cyber-boundaries through which national authority can be asserted in digital space. This study evaluates the complex interplay among state power, cyber-security technologies, and cultural resistance in Indonesia's pursuit of digital sovereignty. Employing a qualitative case-study design that combines critical policy analysis with socio-technical framework mapping, the study examines national cyber-governance instruments, including Private Electronic System Operator (*Penyelenggara Sistem Elektronik*, PSE) regulations, personal data protection frameworks, national cyber-security strategies, network-level filtering mechanisms, and centralized digital infrastructures, alongside grassroots forms of digital resistance. The findings indicate that although the Indonesian state has substantially expanded its regulatory and technological capacity to govern digital space, the resulting sovereign control remains contingent and contested. State-imposed digital boundaries are continuously negotiated through digital activism, circumvention practices, decentralized communication channels, and culturally embedded forms of online participation. Moreover, persistent dependence on transnational platforms, foreign technological infrastructures, and external technology vendors constrains the achievement of full technological autonomy. This study therefore conceptualizes digital sovereignty not as a static state-controlled fortress, but as a continuously negotiated socio-technical field in which state authority is reshaped by technological dependencies and societal resistance. The findings suggest that sustainable cyber-governance in emerging democracies requires participatory, rights-sensitive, and socio-technically aligned approaches rather than an exclusive reliance on centralized regulatory control.

Keywords: Digital Sovereignty; Cyber-Security Technologies; Cultural Resistance; State Power; Indonesia; Cyber-Governance; Socio-Technical Systems

Citation: Neng Yayu Wandira, Aryo De Wibowo Muhammad Sidik. Bending the Bulwarks of Digital Sovereignty: Evaluating Cyber-Security Technologies, Cultural Resistance, and State Power in Indonesia. *IMPACTIA* **2024**, *1*, 0. https://doi.org/

Received:
Accepted:
Published:

1. Introduction

The contemporary Internet, once widely imagined as a borderless global communication infrastructure, has increasingly become an arena of geopolitical fragmentation, regulatory intervention, and renewed assertions of territorial authority. Governments across different political systems are attempting to extend conventional concepts of sovereignty into digital environments by regulating platforms, controlling data flows, securing critical information infrastructures, and shaping the technological architectures through which citizens communicate. These developments have contributed to the emergence of concepts such as "digital sovereignty", "data sovereignty", and "cyber sovereignty", each reflecting different dimensions of state efforts to regain strategic control over increasingly transnational digital ecosystems [1,2]. These dynamics are particularly significant in post-colonial and Global South contexts, where digital transformation frequently occurs through technological infrastructures that are only partially controlled by domestic institutions.

Governments seeking greater national autonomy must simultaneously confront foreign platform dominance, imported hardware and software, transnational cloud infrastructures, cyber-security threats, cross-border data flows, and domestic demands for political openness. Digital sovereignty in such environments therefore cannot be understood solely as a matter of legal jurisdiction or technological capacity. Rather, it represents a socio-technical process in which regulatory authority, technological infrastructure, economic dependency, institutional capacity, and social practices interact continuously. Indonesia provides a particularly important case for examining these tensions. With more than 221 million Internet users recorded in 2024 and an Internet penetration rate of approximately 79.5%, Indonesia possesses one of the world's largest digitally connected populations [3]. The country's expanding digital economy has been accompanied by increasingly extensive state efforts to regulate electronic systems, digital platforms, personal data, cyber-security, and online content. Among the important elements of this regulatory architecture are the rules governing Private Electronic System Operators (*Penyelenggara Sistem Elektronik Lingkup Privat*, PSE), Indonesia's personal data protection regime, and the development of a national cyber-security strategy [4–7]. Under the PSE framework, private electronic system operators serving users in Indonesia are subject to registration and regulatory obligations, while the government possesses mechanisms for requesting the removal of prohibited electronic information and, under specified circumstances, restricting access to non-compliant systems [4,5]. The enactment of Law No. 27 of 2022 concerning Personal Data Protection further expanded Indonesia's legal framework by regulating the rights of data subjects as well as the obligations of data controllers and processors [6]. In parallel, Presidential Regulation No. 47 of 2023 established a National Cyber Security Strategy and Cyber Crisis Management framework, providing a broader strategic basis for coordinating national cyber-security governance [7]. Taken together, these developments illustrate an increasingly institutionalized state project for governing Indonesian digital space. Yet the expansion of formal regulatory authority does not necessarily produce complete sovereign control. Indonesia's digital ecosystem remains deeply interconnected with transnational platforms, global cloud services, imported network technologies, international technical standards, and foreign technology vendors. Consequently, efforts to strengthen national technological autonomy coexist with structural dependencies that potentially constrain the state's capacity to construct fully autonomous digital borders. At the same time, state-centered governance encounters a highly dynamic domestic Internet culture. Indonesian digital society has developed through decentralized online communities, participatory social media practices, peer-to-peer information exchange, civic activism, and informal modes of technological adaptation. Users may respond to restrictions through Virtual Private Networks (VPNs), proxy services, encrypted or decentralized communication platforms, alternative accounts, coded language, platform migration, and other forms of technical or discursive circumvention. These practices demonstrate that digital governance is not implemented upon a passive technological population. Rather, citizens and online communities actively interpret, negotiate, adapt to, and sometimes resist regulatory and technological interventions. The resulting tension constitutes the central analytical concern of this study. The Indonesian state seeks to construct regulatory and technological "bulwarks" capable of securing its digital domain, yet these boundaries remain permeable because they operate within a transnational technological infrastructure and a socially adaptive digital environment. The concept of "bending" employed in this article therefore refers to the processes through which formally imposed digital boundaries are modified, circumvented, renegotiated, or reinterpreted through the interaction of state institutions, technological systems, economic dependencies, and cultural practices.

1.1. Problem Statement and Research Gap

Existing scholarship on digital sovereignty has generated important theoretical insights into the increasing fragmentation of the global Internet, platform regulation, data governance, technological autonomy, and the reassertion of state authority in cyberspace [1,2,8].

However, a substantial portion of this literature remains centered on technologically powerful geopolitical actors, particularly the United States, China, Russia, and the European Union. Such perspectives are insufficient for explaining digital sovereignty in post-colonial democracies in the Global South. In these contexts, sovereign authority frequently operates under conditions of institutional hybridity, uneven technological capacity, infrastructural dependence, regulatory contestation, and extensive reliance on transnational digital corporations. The ability of a government to enact legislation therefore does not necessarily correspond to an equivalent ability to exercise technological control. A second limitation concerns the tendency to conceptualize digital sovereignty primarily through state institutions. Regulatory instruments, cyber-security agencies, data localization policies, platform obligations, and technical filtering systems are frequently treated as the principal units of analysis. Such approaches risk positioning citizens as passive subjects of governance while underestimating the capacity of digital communities to adapt to, negotiate, or circumvent technological restrictions. A third gap emerges from overly binary interpretations of cyber governance. Digital sovereignty is often implicitly evaluated as either successful sovereign control or failed state censorship. This binary distinction obscures intermediate and continuously changing configurations in which state authority may be simultaneously strengthened in one technological layer and weakened in another. This study addresses these limitations by conceptualizing digital sovereignty as a *negotiated socio-technical assemblage*. Rather than asking exclusively whether the Indonesian state possesses digital sovereignty, the study investigates how sovereignty is continuously produced, challenged, and transformed through interactions among regulatory authority, cyber-security technologies, infrastructural dependencies, and culturally embedded digital practices. Accordingly, the principal research gap addressed by this study concerns the limited understanding of how *state power, cyber-security technologies, and grassroots cultural resistance mutually constitute and reshape digital sovereignty within a Global South democratic context*.

1.2. Research Questions

To address this research gap, the study is guided by three research questions:

RQ1: How does the Indonesian state conceptualize and operationalize digital sovereignty through legal-regulatory frameworks, institutional arrangements, and cyber-security infrastructures?

RQ2: In what ways do grassroots socio-cultural practices, digital activism, and informal technological workarounds negotiate, circumvent, or reshape state-imposed digital boundaries?

RQ3: What structural, institutional, and technological limitations constrain the Indonesian state's capacity to maintain autonomous digital borders within a globally interconnected technological ecosystem?

1.3. Theoretical Framework and Conceptual Synthesis

This study integrates three complementary theoretical traditions: Science and Technology Studies (STS), the critical political economy of communication, and post-colonial approaches to state power. The combination enables digital sovereignty to be examined not only as a legal doctrine or cyber-security strategy, but also as a socio-technical configuration shaped by interactions among institutions, infrastructures, markets, technologies, and everyday social practices. From an STS perspective, technological systems are understood as socially embedded arrangements rather than politically neutral instruments. Algorithms, filtering systems, servers, cloud infrastructures, identification mechanisms, and network protocols acquire political significance through the institutions and practices in which they are embedded [9,10]. Cyber-security infrastructure can therefore enable state authority while simultaneously generating technical constraints, dependencies, and opportunities for circumvention. The critical political economy perspective extends this analysis by examining ownership, economic dependency, platform concentration, and asymmetrical control over digital infrastructures. Indonesia's pursuit of technological autonomy occurs

within a global digital economy in which crucial layers of cloud computing, operating systems, semiconductor production, social media platforms, and cyber-security services remain dominated by transnational corporations. Sovereignty must consequently be assessed not only through formal governmental authority but also through the distribution of technological and economic capabilities. Post-colonial perspectives further illuminate how technological dependency intersects with historical patterns of unequal political and economic power. From this perspective, attempts by Global South states to establish digital sovereignty may represent legitimate efforts to reduce external dependency while simultaneously creating new mechanisms of domestic surveillance and political control. Digital sovereignty therefore contains an inherent duality: it may function both as a strategy of autonomy from external domination and as an instrument through which governmental authority is consolidated internally. Bringing these perspectives together, this study employs the concept of a *socio-technical assemblage* to examine digital sovereignty as an interaction among three analytical dimensions: state power and legal infrastructure, cyber-security technologies, and cultural resistance.

Table 1. Conceptual Framework for Evaluating Digital Sovereignty in Indonesia

Analytical Dimension	**State Power and Legal Infrastructure**	**Cyber-Security Technologies**	**Cultural Resistance and Grassroots Response**
Core Mechanisms	PSE regulation, personal data governance, cyber-security strategy, platform obligations, content governance, and institutional coordination.	Network filtering, traffic inspection, centralized digital infrastructure, threat-monitoring systems, data centers, and cyber-security architectures.	VPN and proxy use, encrypted or decentralized communication, coded language, platform migration, digital activism, and algorithmic or technical circumvention.
Sovereign Intent / Social Response	Expansion of jurisdiction, regulatory oversight, platform accountability, and control over nationally relevant digital activities.	Strengthening of threat detection, infrastructural visibility, content restriction, and technical enforcement capacity.	Negotiation of digital boundaries, preservation of communicative autonomy, circumvention of restrictions, and creation of alternative digital spaces.
Structural Vulnerabilities	Institutional fragmentation, regulatory contestation, implementation gaps, legitimacy concerns, and tensions with fundamental rights.	Dependence on foreign hardware, software, cloud infrastructure, vendors, and international technical standards.	Exposure to legal sanctions, surveillance, platform moderation, technological exclusion, and unequal access to circumvention tools.

The framework does not assume that these dimensions operate independently. Instead, the study focuses on their interaction. Regulatory decisions can shape technological architecture; technological architecture can generate new opportunities for control or circumvention; grassroots adaptations can prompt regulatory responses; and external infrastructural dependencies can constrain the state's capacity to implement sovereign objectives. Digital sovereignty is therefore conceptualized as an evolving outcome of continuous socio-technical negotiation.

1.4. Significance and Contributions of the Study

This study makes three principal contributions. First, at the theoretical level, it extends digital sovereignty scholarship beyond predominantly Western-, Chinese-, and Russian-centered models by developing a socio-technical interpretation applicable to a major Global South democracy. The concept of *bending the bulwarks* emphasizes that digital boundaries are neither absolute nor technologically fixed; instead, they are repeatedly reconstructed through interactions among state institutions, technical infrastructures, global economic dependencies, and social actors. Second, at the methodological level, the study combines critical policy analysis with socio-technical infrastructure mapping and qualitative examination of digital resistance. This approach permits regulatory texts, institutional arrangements, technical systems, and grassroots practices to be analyzed within a single conceptual framework rather than as separate domains. Third, at the practical level, the study provides insights relevant to policymakers, cyber-security institutions, civil society organizations, and technology practitioners. It argues that cyber-governance strategies must reconcile legitimate objectives of national security and technological autonomy with privacy, freedom of expression, institutional accountability, technological openness, and meaningful public participation. The remainder of the paper is structured as follows. Section 2 reviews the literature concerning digital sovereignty, cyber governance, socio-technical state power, and digital resistance. Section 3 describes the qualitative case-study methodology, critical policy analysis, data-selection strategy, and socio-technical mapping procedure. Section 4 evaluates the regulatory, institutional, and technological architecture through which the Indonesian state seeks to operationalize digital sovereignty. Section 5 examines patterns of cultural resistance, digital activism, and technical circumvention. Section 6 integrates these findings and discusses their implications for theories of state power and digital sovereignty in Global South democracies. Finally, Section 7 presents the conclusions, limitations, and policy recommendations.

2. Research Methodology

To investigate how state-imposed cyber-security architectures, legal-regulatory frameworks, and grassroots cultural practices interact in shaping digital sovereignty in Indonesia, this study adopts a qualitative, multi-method, and socio-technical research design. Digital sovereignty in a post-colonial Global South democracy cannot be adequately examined solely through statutory analysis or technical evaluation because state authority is exercised simultaneously through legal mandates, institutional arrangements, network infrastructures, platform governance, and everyday digital practices.

Accordingly, the methodological framework integrates four complementary approaches: (1) Critical Policy Analysis (CPA), (2) OSINT-based technical architecture and infrastructure mapping, (3) qualitative digital ethnography, and (4) semi-structured Key Informant Interviews (KIIs). These methods were applied as mutually reinforcing empirical streams rather than as independent analytical procedures. The resulting triangulation enabled systematic comparison between the state's normative intentions, its observable technological capacity, and the ways in which citizens and digital communities negotiate or circumvent state-imposed digital boundaries.

The unit of analysis was therefore not a single law, institution, technological system, or activist community, but the broader *socio-technical assemblage* through which digital sovereignty is continuously constructed, implemented, contested, and reconfigured.

2.1. Research Philosophy and Overall Design

This research is situated within a critical interpretivist paradigm informed by Science and Technology Studies (STS), critical political economy, and socio-technical systems thinking. From this perspective, digital sovereignty is conceptualized not as a fixed condition achieved through legislation or infrastructure alone, but as an evolving configuration of institutions, technologies, political interests, economic dependencies, and social practices.

The critical interpretivist orientation is particularly appropriate because the study seeks to examine both the formal meanings attributed to digital sovereignty by state institutions and the alternative meanings produced through technological practices and citizen responses. Legal provisions, policy documents, filtering infrastructures, cloud architectures, and circumvention practices are therefore treated as politically situated components of a broader socio-technical system.

Technology is consequently not conceptualized as a passive instrument fully controlled by governmental actors. Nor is it understood as a politically neutral resource available equally to all social groups. Instead, technological infrastructure is treated as an arena in which political authority, technical constraints, economic interests, and citizen agency intersect.

The overall research process was organized into three principal empirical phases corresponding to three dimensions of the analytical framework: state intent, technological capacity, and socio-cultural response. Table 2 summarizes the research design.

Table 2. Research Phases, Empirical Sources, and Analytical Objectives

Research Phase	Primary Method	Target Empirical Corpus	Analytical Objective
Phase 1: Legal and Institutional Analysis	Critical Policy Analysis and legal-document interpretation	PSTE and PSE regulations, ITE Law, Personal Data Protection Law, presidential regulations, ministerial regulations, BSSN publications, policy statements, and institutional documents.	Identify the state's normative conception of digital sovereignty, regulatory instruments, enforcement mechanisms, institutional responsibilities, and formally constructed digital boundaries.
Phase 2: Technical and Infrastructure Mapping	OSINT-based technical architecture mapping and infrastructure assessment	Public data-center documentation, procurement records, network-routing information, DNS filtering infrastructure, publicly documented filtering technologies, cloud architectures, and vendor relationships.	Evaluate observable state technological capacity, centralization points, infrastructural dependencies, implementation constraints, and potential vulnerabilities within the cyber-governance architecture.
Phase 3: Socio-Cultural Resistance Analysis	Digital ethnography and semi-structured Key Informant Interviews	Public digital discussions, digital-rights communities, technology practitioners, civil society organizations, activists, developers, and users familiar with circumvention practices.	Identify patterns of digital adaptation, circumvention, discursive resistance, technological workarounds, and broader negotiations of state-imposed digital boundaries.

This three-phase structure allowed the study to compare what the state *intends to regulate*, what its technological infrastructure can *operationally enforce*, and how citizens and digital communities *respond in practice*. Rather than treating discrepancies among these

dimensions as methodological noise, the study considered them central empirical evidence of negotiated digital sovereignty.

2.2. Data Collection Protocols and Empirical Corpus

Data collection was conducted over an 18-month period spanning 2024–2026. Primary and secondary evidence was systematically assembled across four interconnected empirical streams: (1) legal and policy documentation, (2) technical and infrastructure data, (3) semi-structured interviews, and (4) public digital ethnographic observations.

The collection strategy followed the principle of methodological triangulation. No major conclusion regarding state capacity, technological implementation, or cultural resistance was derived from a single type of evidence where corroborating sources were available. Official claims were compared with technical documentation and civil society assessments, while interview findings were evaluated alongside documentary and observational evidence.

2.2.1. Document Corpus and Policy Archive

The first empirical stream consisted of a structured archive of Indonesian legal, regulatory, strategic, and institutional documents related to electronic systems, cyber-security, online content governance, data protection, and digital infrastructure.

The core legal corpus included, among other materials:

- Government Regulation No. 71 of 2019 concerning the Operation of Electronic Systems and Transactions (*Penyelenggaraan Sistem dan Transaksi Elektronik*, PSTE);
- Minister of Communication and Informatics Regulation No. 5 of 2020 concerning Private Electronic System Operators (*Penyelenggara Sistem Elektronik Lingkup Privat*, PSE);
- Minister of Communication and Informatics Regulation No. 10 of 2021 amending Regulation No. 5 of 2020;
- Law No. 27 of 2022 concerning Personal Data Protection (*Perlindungan Data Pribadi*, PDP);
- Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law);
- Presidential regulations and strategic documents related to national cyber-security governance; and
- publicly available strategic publications, policy documents, and institutional materials issued by the National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara*, BSSN) and relevant ministries.

To avoid reproducing state narratives uncritically, the official policy corpus was supplemented with secondary policy analysis produced by Indonesian civil society organizations and digital-rights institutions, including SAFEnet and ELSAM, as well as reports from international organizations monitoring Internet freedom, privacy, platform regulation, cyber-security, and digital rights.

Documents were selected using three principal inclusion criteria: direct relevance to the governance of Indonesian digital space; substantive discussion of cyber-security, electronic systems, personal data, content control, or digital infrastructure; and sufficient institutional or evidentiary credibility for scholarly analysis.

The policy corpus was analyzed not only to identify formal legal requirements but also to examine recurring justificatory discourses, particularly those concerning national security, public order, technological autonomy, data protection, platform accountability, economic sovereignty, and state responsibility for cyberspace.

2.2.2. Technical Architecture and Infrastructure Mapping

The second empirical stream examined the technological infrastructures through which regulatory objectives could potentially be translated into operational control. Because this study did not involve privileged administrative access to classified or internally

restricted government systems, the technical component is more accurately characterized as *OSINT-based infrastructure mapping* rather than a direct systems audit.

Technical evidence was compiled from publicly accessible sources, including:

- government procurement documentation;
- publicly released technical specifications;
- official documentation concerning national and governmental data-center initiatives;
- Internet routing and autonomous-system information;
- Domain Name System (DNS) filtering and blocking mechanisms;
- public documentation concerning Trust+Positif and subsequent content-governance infrastructures;
- publicly disclosed cloud and data-center architectures;
- technical documentation produced by Internet service providers and infrastructure operators;
- vendor documentation and procurement disclosures; and
- credible technical investigations and open-source intelligence concerning network-level content filtering.

Particular attention was directed toward the architecture of national data infrastructure, including the *Pusat Data Nasional* (PDN), centralized and distributed points of network control, DNS-based filtering mechanisms, cloud-service dependency, and publicly documented or credibly reported deployment of automated content-filtering technologies.

Claims regarding Deep Packet Inspection (DPI) were treated with particular methodological caution. The analysis distinguished among:

1. **Documented deployment**, where implementation was explicitly supported by official technical documents, procurement records, or verifiable infrastructure evidence;
2. **Reported deployment**, where implementation was identified through credible technical investigations or independent reporting but could not be directly verified through official system documentation; and
3. **Inferred technical capability**, where observable network behavior was consistent with particular filtering architectures but insufficient to establish the specific technology or vendor responsible.

This evidentiary distinction was introduced to prevent speculative attribution of surveillance or filtering capabilities to state institutions where publicly available evidence remained incomplete.

The technical mapping process subsequently classified infrastructure according to four analytical layers:

1. **Physical Infrastructure Layer:** data centers, physical network infrastructure, hardware systems, and hosting environments;
2. **Network and Transport Layer:** Internet routing, DNS infrastructure, traffic-management systems, and network-level filtering mechanisms;
3. **Application and Platform Layer:** cloud services, digital platforms, electronic systems, and application-level governance mechanisms; and
4. **Content and Information Layer:** content restrictions, keyword-based interventions, platform takedown mechanisms, and user-facing information controls.

Mapping these layers made it possible to identify where state control was relatively centralized, where authority depended on cooperation from private intermediaries, and where technical dependencies limited autonomous enforcement.

2.2.3. Key Informant Interviews

The third empirical stream consisted of in-depth semi-structured Key Informant Interviews (KIIs). Participants were recruited using a combination of purposive and snowball sampling in order to obtain perspectives from actors occupying different positions within Indonesia's digital-governance ecosystem.

A total of 28 informants were distributed across four stakeholder categories, as summarized in Table 3.

Table 3. Key Informant Interview Participant Categories

Stakeholder Category	Code Series	N	Selection Criteria and Professional Profile
State Regulators and Policy Experts	REG-01–REG-06	6	Government officials, legal and policy specialists, or individuals with professional expertise concerning Indonesian digital regulation, cyber-security policy, or legislative processes.
Cyber-Security Technologists and Industry Engineers	ENG-01–ENG-08	8	Network engineers, cyber-security professionals, cloud architects, infrastructure specialists, consultants, and professionals with experience in Internet service provision or enterprise digital infrastructure.
Civil Society Organizations and Legal Advocates	CSO-01–CSO-07	7	Digital-rights advocates, legal practitioners, civil society researchers, human-rights specialists, and policy analysts concerned with privacy, freedom of expression, Internet governance, or related issues.
Grassroots Activists and Technology Communities	ACT-01–ACT-07	7	Independent developers, digital-community organizers, privacy-oriented technology users, online activists, and individuals familiar with technical or cultural circumvention practices.
Total		**28**	

Purposive sampling was initially used to identify individuals possessing direct professional, institutional, or experiential knowledge relevant to one or more dimensions of the research questions. Snowball sampling was subsequently employed to identify additional informants whose technical expertise or community involvement might otherwise have remained inaccessible through formal recruitment channels.

The interviews followed a semi-structured protocol organized around four thematic domains:

1. perceptions and definitions of Indonesian digital sovereignty;
2. interpretations of the state's legal and institutional cyber-governance framework;
3. assessments of technical capability, infrastructural dependency, and operational constraints; and
4. experiences or observations concerning digital resistance, adaptation, circumvention, and regulatory negotiation.

The semi-structured format allowed consistent comparison across stakeholder categories while preserving sufficient flexibility for participants to elaborate on institution-specific experiences, technical details, and contextual interpretations.

Where participants discussed potentially sensitive technical or political practices, interview questions focused on analytical interpretation and personal experience rather than requesting operational instructions for bypassing security systems or identifying individual actors engaged in legally sensitive activities.

2.2.4. Digital Ethnography and Online Fieldwork

The fourth empirical stream consisted of qualitative digital ethnography conducted in publicly accessible online environments in which state regulation, content restriction, technical adaptation, and digital-rights discourse were openly discussed.

Observation sites included selected public discussions and communities on X (formerly Twitter), Reddit, publicly accessible technology forums, open-source GitHub repositories, public Telegram channels, and other openly available Indonesian digital-community spaces relevant to cyber governance and Internet restriction.

The ethnographic component focused on observable discourse and practices concerning:

- public reactions to website or platform blocking;
- discussions concerning Virtual Private Networks (VPNs), alternative DNS configurations, and other publicly documented circumvention technologies;
- migration between digital platforms following regulatory or moderation interventions;
- the circulation of publicly available technical knowledge concerning Internet access and privacy;
- digital-rights campaigning and online collective action;
- linguistic adaptation and coded communication;
- *bahasa plesetan*, altered spellings, euphemisms, memes, and other forms of discursive obfuscation; and
- public narratives concerning censorship, surveillance, platform governance, and technological autonomy.

The objective was not to evaluate the technical effectiveness of individual circumvention tools, but to understand the social meanings associated with their use and the ways in which technical adaptation becomes embedded within broader cultural practices of negotiation and resistance.

The analysis therefore differentiated between *technical circumvention*, referring to technological modification of access pathways, and *discursive circumvention*, referring to linguistic, symbolic, and communicative practices designed to reduce visibility to automated or socially enforced content controls.

No researcher joined closed or password-protected communities through deceptive identities, obtained unauthorized access to private communications, or conducted covert surveillance of private individuals. Only material reasonably understood to be publicly accessible was included in the ethnographic observational corpus.

2.3. Data Analysis and Synthesis Framework

The qualitative corpus was managed and coded using NVivo 14. Analysis followed an iterative multi-layered strategy combining deductive and inductive coding. Deductive categories were initially derived from the conceptual framework and research questions, while additional codes were developed inductively as recurring themes emerged from documents, interviews, and ethnographic observations.

The analytical process consisted of four stages: policy deconstruction, technical architecture assessment, resistance mapping, and cross-stream triangulated synthesis.

2.3.1. Stage 1: Policy Deconstruction and Structural Coding

The first analytical stage applied structural and thematic coding to legislation, government regulations, institutional publications, policy statements, and relevant civil society documents.

Initial coding categories included:

- sovereignty and national jurisdiction;
- cyber-security and national security;
- public order and prohibited content;
- personal data governance;

- electronic-system registration;
- platform and intermediary obligations;
- administrative and access-related sanctions;
- technological autonomy;
- institutional authority and coordination;
- rights protection; and
- legal ambiguity and discretionary enforcement.

The objective was to reconstruct the state's normative model of digital sovereignty and identify the legal mechanisms through which that model is intended to become operational.

Where relevant, legal-policy claims were compared with internationally recognized principles concerning privacy, freedom of expression, necessity, proportionality, transparency, and procedural accountability. Such comparisons were used analytically rather than as a substitute for formal constitutional or doctrinal legal review.

2.3.2. Stage 2: Technical Architecture Assessment

The second stage organized technical evidence according to the layered infrastructure framework described above. The analysis examined the relationship between regulatory authority and the technical architectures available to implement that authority.

Technical coding dimensions included:

- infrastructure ownership;
- hardware and software provenance;
- domestic versus foreign vendor dependency;
- cloud-service dependency;
- DNS governance;
- Internet routing architecture;
- filtering and blocking points;
- centralized versus distributed control;
- interoperability constraints;
- technical bottlenecks;
- redundancy and resilience; and
- dependence on transnational technical standards or service providers.

The purpose of this stage was not to conduct penetration testing or vulnerability exploitation. Rather, it sought to determine how observable infrastructure either enabled or constrained the state's declared cyber-sovereignty objectives.

2.3.3. Stage 3: Inductive Coding of Cultural Resistance

Interview transcripts and digital ethnographic field notes were subsequently subjected to inductive thematic coding. Open codes were progressively grouped into broader conceptual categories describing recurrent forms of digital adaptation and resistance.

Emergent analytical themes included:

- tactical technological workarounds;
- informal technological literacy;
- VPN and alternative-access practices;
- platform migration;
- algorithmic and linguistic evasion;
- coded political expression;
- networked digital activism;
- privacy-oriented practices;
- normalization of circumvention;
- regulatory fatigue;
- perceived surveillance; and
- cultural counter-hegemonic practices.

Coding did not assume that all circumvention constituted deliberate political resistance. Particular attention was paid to participant motivations in order to distinguish explicitly political activism from convenience-driven adaptation, privacy-seeking behavior, commercial practices, entertainment access, or everyday technical problem solving.

This distinction prevented the analytical framework from automatically politicizing all forms of technological workaround behavior.

2.3.4. Stage 4: Cross-Stream Triangulation and Theoretical Synthesis

The final stage cross-referenced findings from the policy corpus, infrastructure mapping, interviews, and digital ethnography. A triangulation matrix was developed around the three research questions to identify areas of convergence, contradiction, and implementation gaps.

Three relationships were particularly examined:

1. whether formal regulatory authority corresponded with observable technological enforcement capacity;
2. whether technological control mechanisms generated predictable forms of social adaptation or circumvention; and
3. whether infrastructural and vendor dependencies limited the state's capacity to achieve its stated objectives of technological autonomy.

Contradictory evidence was retained rather than eliminated. For example, where institutional documents described a centralized governance capability but technical or interview evidence indicated fragmented implementation, the discrepancy itself was treated as an analytically significant finding.

The synthesis ultimately sought to develop an empirically grounded model of *negotiated digital sovereignty*, in which sovereign authority emerges as the provisional result of interactions among regulatory ambition, technological capability, infrastructural dependency, and citizen agency.

Table 4 summarizes the four analytical stages.

Table 4. Data Analysis and Synthesis Framework

Analytical Stage	Primary Method / Tool	Coding Scheme / Dimension	Target Output
Stage 1: Policy Deconstruction	Critical Policy Analysis and thematic coding using NVivo 14	Sovereignty framing, national security, legal ambiguity, institutional authority, enforcement mandates, sanctions, platform obligations, and rights safeguards.	Taxonomy of legal-regulatory mechanisms and reconstruction of state sovereign intent.
Stage 2: Technical Assessment	Layered socio-technical infrastructure mapping	Infrastructure ownership, vendor origins, DNS governance, network filtering points, cloud dependencies, routing architecture, and centralized versus distributed control.	Structural map of state digital-control capacity, infrastructural dependencies, and implementation constraints.
Stage 3: Resistance Mapping	Inductive thematic coding of interviews and ethnographic observations	VPN and alternative-access practices, platform migration, linguistic adaptation, digital activism, technological literacy, coded communication, and circumvention practices.	Typology of technical, cultural, and discursive responses to state-imposed digital boundaries.
Stage 4: Synthesis and Theory Construction	Cross-data triangulation and STS-informed interpretation	Co-construction, implementation gaps, technological dependency, adaptation, contestation, and shifting state–society boundaries.	Integrated theoretical model of negotiated digital sovereignty in a Global South democratic context.

2.4. Research Trustworthiness

The credibility and analytical rigor of the study were strengthened through multiple qualitative validation procedures.

First, **source triangulation** was employed by comparing information obtained from government documents, technical documentation, civil society publications, interview participants, and public digital observations. Claims supported only by a single source were treated cautiously and were not generalized without corroborating evidence.

Second, **methodological triangulation** was achieved by integrating policy analysis, technical architecture mapping, interviews, and digital ethnography. This allowed institutional narratives to be compared against both observable infrastructure and lived digital practices.

Third, the study maintained an **analytical audit trail** documenting data-selection decisions, coding revisions, category development, and the relationship between empirical evidence and higher-order theoretical interpretations.

Fourth, **negative-case analysis** was applied to identify evidence that contradicted emerging explanations. Cases in which state regulation appeared effective, citizen resistance was limited, or technological dependencies were less significant than anticipated were retained in the analytical process to reduce confirmation bias.

Fifth, selected interpretations derived from interview data were subjected to **member checking** where feasible, particularly with informants possessing specialist knowledge of digital policy, civil society advocacy, or technical infrastructure. Member checking was used to test factual interpretation and contextual accuracy rather than to require participants to endorse the study's theoretical conclusions.

Finally, thick contextual description was employed throughout the analysis to enable readers to assess the transferability of findings beyond the Indonesian case.

2.5. Research Ethics and Risk Mitigation

The politically and technologically sensitive nature of research on cyber-security governance, content restriction, digital activism, and surveillance required enhanced attention to participant protection and data security.

2.5.1. Informed Consent and Participant Anonymity

All interview participants were provided with information concerning the purpose of the research, the voluntary nature of participation, the intended use of collected information, and their right to decline questions or withdraw from participation subject to the conditions communicated during recruitment.

Consent was obtained prior to substantive interviewing. Where written documentation could itself create unnecessary identification risks, digitally recorded verbal consent was used where permitted by the applicable research ethics protocol.

Personal identifiers were removed from analytical records. Participants were assigned alphanumeric identifiers corresponding to stakeholder categories, including REG, ENG, CSO, and ACT codes. Quotations and contextual information were reviewed to minimize the risk of deductive identification, particularly for participants occupying specialized professional positions.

2.5.2. Sensitive Information and Data Minimization

The study followed a data-minimization principle. Information unnecessary for answering the research questions was not systematically collected. Researchers did not request passwords, authentication credentials, private network configurations, unpublished security vulnerabilities, operational access to restricted systems, or personally identifying information concerning individuals engaged in digital circumvention.

Where interviews generated unexpectedly sensitive operational details, such information was excluded, generalized, or redacted when its disclosure could reasonably increase legal, professional, or cyber-security risks.

2.5.3. Data Security

Interview recordings, transcripts, field notes, and research metadata containing potentially sensitive information were stored in encrypted research environments with access restricted to authorized members of the research team.

Sensitive raw data were separated from anonymized analytical datasets wherever practicable. Identifying information was maintained separately from coded transcripts, and dissemination materials used anonymized or aggregated evidence.

Where offline encrypted storage was used for particularly sensitive material, external cloud synchronization of unredacted raw interview data was avoided.

2.5.4. Ethical Digital Ethnography

Digital ethnography was restricted to information available in publicly accessible online spaces. The study did not employ deceptive identities to enter private communities, circumvent access controls, or monitor closed interpersonal communication.

Although public accessibility informed data selection, public availability was not treated as equivalent to unrestricted ethical usability. Direct quotation of potentially identifiable social-media users was minimized when verbatim text could facilitate reverse

identification through search engines. Where the identity of an ordinary user was not analytically necessary, material was paraphrased or reported in aggregated thematic form.

Greater latitude was applied to statements intentionally made in an official or clearly public professional capacity by government institutions, organizations, public officials, and established advocacy groups.

2.5.5. Researcher and Participant Risk Mitigation

Because discussion of digital censorship, state surveillance, cyber-security infrastructure, or circumvention practices can create political, legal, or professional sensitivities, interview protocols avoided questions that would require participants to disclose unlawful conduct or operational information unrelated to the research objectives.

The study focused on governance structures, perceptions, technological architectures, and observable socio-cultural practices rather than identifying individual actors engaged in controversial digital activities.

These safeguards were designed to reduce participant exposure while preserving the analytical capacity to examine contested processes of digital governance and resistance.

2.6. Methodological Scope and Limitations

Several methodological limitations should be acknowledged.

First, because the technical assessment relied primarily on publicly accessible evidence, it cannot provide comprehensive visibility into classified, proprietary, or otherwise non-public governmental cyber-security systems. The infrastructure maps presented in this study should therefore be interpreted as reconstructions of the *observable digital-governance architecture*, rather than exhaustive representations of all state cyber capabilities.

Second, digital ethnographic observation disproportionately captures users who publicly discuss governance, censorship, privacy, or circumvention. Such users may possess higher levels of technical literacy or political engagement than the general Indonesian Internet population. Consequently, identified resistance practices should not automatically be interpreted as nationally representative behavioral patterns.

Third, purposive and snowball interview sampling prioritizes information-rich participants rather than statistical representativeness. The purpose of the 28 interviews is therefore analytical depth and stakeholder comparison rather than population-level generalization.

Fourth, the rapidly changing nature of cyber-security technology and digital regulation means that infrastructure configurations, platform practices, regulatory implementation, and citizen circumvention techniques may evolve during or after the research period. The findings consequently represent a temporally bounded interpretation of Indonesia's digital-sovereignty ecosystem.

These limitations do not invalidate the qualitative design but define the scope within which claims of technological capacity, cultural resistance, and negotiated sovereignty are interpreted.

3. Results

The empirical findings reveal that digital sovereignty in Indonesia operates less as a rigid state enclosure than as a continuously contested socio-technical configuration. Across the legal-policy corpus, technical infrastructure mapping, interview data, and digital ethnographic observations, three recurring patterns emerged. First, the state has substantially expanded its formal regulatory capacity to impose jurisdiction over platforms, electronic systems, online content, and personal data. Second, the operational translation of this authority into technological control remains uneven and constrained by infrastructural fragmentation, implementation gaps, and dependence on transnational technologies. Third, citizens, technology communities, and civil society actors continuously adapt to regulatory interventions through technical circumvention, platform migration, linguistic innovation, and collective digital mobilization.

The central empirical pattern can therefore be characterized as a persistent divergence among *regulatory intent*, *technical capability*, and *social practice*. State institutions construct regulatory and technological "bulwarks" intended to establish authority over Indonesian digital space; however, these boundaries remain permeable and are repeatedly modified by technological limitations, economic pressures, infrastructural dependencies, and user adaptation.

Rather than demonstrating either complete state control or complete state failure, the results indicate an intermediate condition of *negotiated digital sovereignty*, in which the effective boundaries of state power are repeatedly produced through interaction among legal rules, technological architectures, private intermediaries, and digitally networked communities.

3.1. The Regulatory Bulwarks: Institutionalizing State Authority

The first major finding concerns the progressive institutionalization of state authority over digital space. Critical policy analysis identified three particularly significant components of the contemporary regulatory architecture: Minister of Communication and Informatics Regulation No. 5 of 2020 concerning Private Electronic System Operators and its amendment through Regulation No. 10 of 2021; Law No. 27 of 2022 concerning Personal Data Protection; and Law No. 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law [4–6,11].

Although these instruments address different regulatory domains, collectively they reflect an expansion of state jurisdiction over platforms, electronic information, personal data processing, and digitally mediated activities. This represents a broader shift from a policy orientation primarily concerned with connectivity and network expansion toward one in which platform accountability, data governance, content control, and cyber-security have become increasingly central.

3.1.1. PSE Registration as Jurisdictional Infrastructure

Ministerial Regulation No. 5 of 2020 constitutes one of the clearest examples of this regulatory transformation. The regulation requires qualifying domestic and foreign Private Electronic System Operators (*Penyelenggara Sistem Elektronik Lingkup Privat*, PSE) operating within the Indonesian jurisdictional framework to comply with registration and governance requirements [4].

The regulation is significant not only because of the registration obligation itself, but because registration is embedded within a broader system of platform accountability and content enforcement. Private PSEs may be ordered to remove prohibited electronic information or documents. For ordinary requests, removal is required within a maximum period of 24 hours following receipt of an official order, while requests legally categorized as urgent are subject to a maximum four-hour response period [4].

Urgent requests under the regulation include content related to terrorism, child pornography, and content categorized as causing public unrest or disturbing public order. Failure to comply with applicable obligations may ultimately result in access restriction against the relevant electronic system through Internet service providers [4].

From the perspective of state sovereignty, this arrangement effectively transforms platform registration into a form of jurisdictional infrastructure. Registration establishes a regulatory relationship through which the Indonesian government can require foreign and domestic platforms to respond to national legal and administrative orders.

Interview data from the regulatory stakeholder group reflected this interpretation. Participants REG-02 and REG-04 consistently framed PSE regulation primarily as a mechanism for establishing jurisdiction over transnational technology corporations rather than as a censorship instrument. REG-02 stated:

> "For over two decades, foreign technology companies operated in Indonesia while many of their most important governance decisions were still determined outside Indonesia.

> PSE registration is intended to establish that services operating in Indonesian digital space must also respond to Indonesian law" [REG-02].

This interpretation demonstrates the sovereignty-oriented logic underlying the regulatory framework: control is pursued not necessarily through domestic ownership of platforms, but by extending national administrative jurisdiction over transnational services.

However, interviews with civil society participants produced a markedly different interpretation. CSO-01 and CSO-04 emphasized that broad categories of prohibited information, particularly concepts related to public unrest and public order, could produce significant discretionary space for executive interpretation. From this perspective, the combination of mandatory registration, rapid takedown requirements, subscriber-information obligations, and access blocking creates a regulatory architecture whose effect depends heavily on institutional safeguards and implementation practices.

The tension between these interpretations—jurisdictional sovereignty on the one hand and discretionary content governance on the other—constitutes the first major form of contested digital sovereignty identified in the data.

3.1.2. The 2022 PSE Blocking Episode as an Empirical Stress Test

The enforcement of PSE registration requirements in July 2022 provided an important empirical test of this regulatory architecture. Following the registration deadline, access was restricted to several digital services that had not completed registration, including PayPal, Yahoo, Steam, Dota 2, Counter-Strike, and Epic Games [12].

The blocking demonstrated that PSE registration was not merely symbolic: the government possessed both the legal authority and intermediary cooperation necessary to make major transnational services temporarily inaccessible from Indonesian networks.

At the same time, the episode exposed the socio-economic limits of rigid enforcement. Public criticism rapidly intensified, with the hashtag *#BlokirKominfo* circulating widely and users emphasizing the consequences of blocking services used for digital payments, gaming, freelancing, and other economic activities [12].

PayPal became particularly significant because users relied on the service to access funds associated with international transactions. The government subsequently reopened access temporarily to enable users to withdraw or transfer funds [13]. After registration and communication between affected firms and the government, several services were normalized and became accessible again.

This episode illustrates what this study conceptualizes as the first observable *bending effect*. The formal legal rule was enforceable, but its practical implementation generated economic and social consequences sufficiently significant to produce rapid administrative adjustment.

The outcome was therefore neither straightforward regulatory victory nor regulatory failure. Instead, state authority remained effective but was recalibrated through interaction with platform compliance, economic dependency, and public resistance.

3.1.3. Personal Data Protection and the Limits of Data Sovereignty

The Personal Data Protection Law (Law No. 27 of 2022) introduced a second important layer of digital sovereignty by establishing comprehensive obligations for personal data controllers and processors and strengthening the rights of data subjects [6].

Importantly, the empirical analysis does not support interpreting the PDP Law as a blanket requirement that all Indonesian private-sector personal data must be physically localized within Indonesian territory. Instead, Article 56 establishes conditions governing cross-border personal data transfers, including requirements concerning the level of protection in the recipient jurisdiction, adequate and binding safeguards, and, under specified circumstances, consent from the data subject [6].

The sovereignty dimension of the PDP framework therefore lies principally in extending Indonesian legal protections and accountability requirements across data-processing relationships rather than simply territorializing all data storage.

Nevertheless, implementation revealed an institutional gap. The PDP Law mandates a dedicated personal data protection authority; however, during the study period the establishment of the authority remained incomplete. By 2026, governmental statements continued to describe the institution as being in the process of establishment [14].

This produced a recurring pattern found elsewhere in the study: formal regulatory ambition developed more rapidly than institutional enforcement capacity.

3.1.4. The ITE Law and the Regulation of Digital Expression

The third component of the regulatory architecture is the Electronic Information and Transactions Law and its subsequent amendments, including Law No. 1 of 2024 [11]. Unlike the PSE framework, which primarily structures relations between the state and electronic system operators, the ITE framework directly affects individual and organizational conduct within digital environments.

Interview participants from the civil society group consistently identified the ITE framework as one of the primary legal sources shaping perceptions of digital expression and regulatory risk. Several participants emphasized that the practical effect of digital law cannot be assessed exclusively through the number of prosecutions or formal sanctions. Anticipatory behavior—including self-censorship, deletion of content, migration toward closed communication channels, and avoidance of particular political expressions—also constitutes a significant governance outcome.

Table 5 summarizes the primary regulatory findings.

Table 5. Regulatory Architecture and Empirical Tensions in Indonesian Digital Sovereignty

Legal Framework	Key Regulatory Mechanism	Sovereignty Function	Observed Tension
Permenkominfo No. 5/2020 and No. 10/2021	PSE registration, platform obligations, subscriber-information requirements, rapid content-removal procedures, and access blocking for specified non-compliance.	Extension of Indonesian jurisdiction over domestic and transnational electronic system operators.	Public backlash, economic disruption, dependence on intermediary compliance, and concern regarding broad categories of prohibited content.
Law No. 27/2022 (PDP)	Data-subject rights, controller and processor obligations, cross-border transfer safeguards, breach-related responsibilities, and supervisory framework.	Extension of Indonesian legal protection and accountability across personal data-processing relationships.	Delayed supervisory institutionalization and continuing implementation gaps despite the expiration of the statutory transition period.
Law No. 1/2024 (ITE Amendment)	Revision of rules concerning prohibited electronic information, digital conduct, criminal liability, and state authority in electronic environments.	Maintenance of public order and legal accountability within digitally mediated communication.	Continuing concern regarding legal ambiguity, chilling effects, and the proportionality of enforcement against expression.

3.2. The Cyber-Security Apparatus and Technological Infrastructure

The second major finding concerns the technological mechanisms through which formal regulatory authority is translated into observable control over digital information flows. The infrastructure mapping revealed a multi-layered architecture involving government

institutions, Internet service providers, electronic system operators, content-monitoring systems, national data infrastructure, and private technology vendors.

Three components were particularly visible in the empirical corpus: automated content identification, DNS- and domain-based filtering, and network-level traffic-management capabilities.

3.2.1. Automated Content Identification and Blocklist Governance

Indonesia's content-control infrastructure has historically relied on centralized lists of prohibited or negatively classified domains combined with obligations imposed upon Internet service providers. The Trust+Positif framework formally required ISPs to restrict access to listed sites and maintain updated blocking information [15].

The introduction of the Ministry's AIS crawling system expanded this governance model from a predominantly report-driven structure toward a more proactive content-discovery model. Official descriptions characterize AIS as an automated crawling system used to identify potentially problematic online content for subsequent verification by human personnel [16].

This distinction is analytically important. AIS does not itself constitute a universal packet-interception system. Rather, it operates primarily at the content-discovery and classification stage. Once content is identified and verified, restriction can subsequently occur through platform takedown requests, domain blocking, or ISP-level access controls.

The technical architecture therefore separates at least three processes:

1. **Discovery**, in which automated systems or human reports identify potentially prohibited content;
2. **Classification and Verification**, in which content is evaluated against regulatory categories; and
3. **Enforcement**, in which platforms or network intermediaries are instructed to remove, restrict, or block access to the relevant resource.

This structure demonstrates that algorithmic monitoring and network blocking are related but technically distinct components of the cyber-governance apparatus.

3.2.2. DNS-Based Blocking and Its Technical Limits

The clearest independently documented network-level filtering technique identified in the empirical corpus is DNS interference. Independent network measurements have documented DNS hijacking among Indonesian networks, although implementation has varied across providers and over time [17].

DNS-based filtering offers the state several administrative advantages. It is comparatively inexpensive, can be implemented by Internet service providers without redesigning the broader Internet routing architecture, and can restrict access to large numbers of listed domains.

However, it also creates significant technical limitations. DNS control operates at the name-resolution layer rather than directly eliminating the underlying content from the global Internet. Consequently, the effectiveness of such filtering depends partly on whether users continue to rely upon ISP-controlled name-resolution pathways.

Interviewed engineers repeatedly described this architecture as administratively scalable but technically porous. ENG-05 characterized DNS blocking as a "compliance layer rather than an impermeable border", because the target resource generally remains accessible outside the controlled resolution pathway.

This finding is consistent with the broader socio-technical argument of the study: the state may control a particular infrastructural gateway without controlling the underlying global resource.

3.2.3. Beyond DNS Filtering: Middleboxes, Traffic Management, and the Evidentiary Limits of DPI Claims

A more complex finding concerns Deep Packet Inspection (DPI), Server Name Indication (SNI) filtering, protocol classification, and bandwidth management.

The interview corpus contained repeated references from network engineers to middlebox technologies capable of traffic classification, protocol differentiation, and bandwidth management. Historical independent research has also identified commercial traffic-management appliances within Indonesian networks, demonstrating that sophisticated middlebox capability has existed within parts of the country's network infrastructure [18].

However, the OSINT-based technical assessment did *not* identify sufficient publicly verifiable evidence to conclude that Indonesia operates a single, standardized, nationwide DPI censorship architecture comparable to the highly centralized filtering systems documented in some other jurisdictions.

This distinction is important. Evidence of traffic-management appliances, SNI-sensitive interference, or protocol-level throttling does not by itself establish the existence of a unified national DPI system. Accordingly, the findings classify such capabilities as *network-level traffic management and middlebox capacity*, with individual implementation claims evaluated according to the evidentiary categories established in Section 2.2.2.

The resulting technical hierarchy is summarized in Table 6.

Table 6. Observed and Potential Network Control Mechanisms

Mechanism	Infrastructure Layer	Control Capability	Principal Limitation
DNS interference / redirection	DNS / Application	Prevents or redirects conventional domain resolution through participating ISP resolvers.	Does not remove underlying content and may be less effective when users employ alternative encrypted or external resolution pathways.
IP address blocking	Network	Prevents connections to specified destination addresses or address ranges.	Shared hosting and cloud infrastructure create substantial risks of over-blocking and collateral disruption.
SNI-sensitive filtering	TLS handshake / Transport	Can identify the requested hostname when relevant handshake metadata remains observable.	Effectiveness is reduced when hostname information is encrypted or when services share infrastructure in ways that complicate precise blocking.
Application / protocol classification	Transport / Application	Allows network operators to identify traffic categories and apply differential management policies.	Encrypted and rapidly evolving protocols complicate reliable classification and increase false-positive risks.
Bandwidth throttling	Network / Transport	Reduces capacity available to selected traffic classes, applications, or geographic areas.	Can generate extensive collateral effects and disrupt economically or socially important services.
Platform-level takedown	Application / Content	Removes or restricts specific content through cooperation from an electronic system operator.	Depends upon platform identification, platform compliance, jurisdiction, and the availability of replicated content.

3.2.4. Bandwidth Restrictions and the Politics of Network Control

The empirical corpus also identified bandwidth restriction as an important precedent in Indonesian Internet governance. During unrest in Papua and West Papua in 2019, authorities restricted Internet speeds and subsequently imposed broader access limitations, officially justified as measures intended to limit the spread of misinformation [19].

The episode demonstrates that Indonesian state capacity extends beyond domain-level filtering to temporary control over broader connectivity. However, the subsequent legal challenge also revealed institutional contestation over the legitimacy of such measures. The Jakarta State Administrative Court later ruled that the 2019 shutdown and throttling measures were unlawful [20].

From the perspective of this study, this episode illustrates another form of negotiated sovereignty: technical capability enabled intervention, while judicial and civil society institutions subsequently contested the manner in which that capability had been exercised.

3.3. Structural Dependencies and Vulnerabilities of the Sovereign Infrastructure

The third major empirical finding is that Indonesia's pursuit of digital sovereignty is constrained by the transnational character of the technological systems upon which state digital governance itself depends.

Across procurement documents and engineering interviews, the technical mapping identified recurrent dependence on foreign-proprietary components at multiple layers of the digital stack, including network appliances, virtualization technologies, cloud infrastructure, enterprise software, cyber-security products, operating systems, and vendor-maintained security updates.

This does not imply that Indonesia possesses no domestic technological capacity. Rather, the findings demonstrate an asymmetry between *administrative sovereignty* and *technological autonomy*. The state can regulate the use of technologies within Indonesian jurisdiction even when it cannot independently design, manufacture, maintain, or replace all of the technologies through which such regulation is implemented.

3.3.1. Foreign Vendor Dependency and Technological Autonomy

Engineering participants repeatedly emphasized this distinction. ENG-01 summarized the problem as follows:

> "We speak about cyber sovereignty, but many of the critical hardware and software layers still depend on external vendors. We may control the policy and the configuration, but patches, threat signatures, firmware, licensing, and major upgrades can remain dependent on companies outside Indonesia. That is sovereignty at the administrative layer, but not necessarily technological autonomy" [ENG-01].

Procurement mapping supported the broader substance of this observation by identifying the continued use of foreign-origin or foreign-controlled proprietary technologies within parts of the state and commercial cyber-security ecosystem.

The significance of this dependence is not that foreign technologies are inherently insecure. Rather, dependence becomes a sovereignty issue when critical functions cannot be maintained, independently inspected, replaced, or rapidly recovered without continued access to external intellectual property, vendor support, licensing, supply chains, or technical expertise.

Digital sovereignty, viewed through this lens, therefore becomes a question of *strategic dependency management* rather than technological isolation.

3.3.2. The 2024 PDNS Ransomware Incident as a Test of Centralized Sovereignty

The June 2024 ransomware attack against the Temporary National Data Center 2 (*Pusat Data Nasional Sementara*, PDNS 2) in Surabaya constituted the most significant empirical case of infrastructure fragility identified during the study period.

The attack disrupted multiple public services, including immigration and airport-related services. Indonesian authorities attributed the incident to ransomware associated with the LockBit 3.0 family and subsequently identified as Brain Cipher [21,22].

Government statements subsequently indicated that more than 230 public agencies had been affected and that approximately 98% of government data stored within one of the compromised data-center environments had not been backed up [22].

The PDNS incident is significant for this study because it exposed a contradiction at the core of centralized digital sovereignty. Consolidating public-sector data infrastructure can enhance administrative coordination, standardization, and national control; however, concentration also increases systemic consequences when redundancy, segmentation, recovery procedures, and backup governance are inadequate.

Three vulnerabilities were particularly evident.

Centralization Without Adequate Resilience.

The incident demonstrated that centralized national infrastructure can become a concentration point for systemic risk. Centralization itself was not the sole cause of the crisis, but insufficient backup adoption and disaster-recovery readiness magnified the consequences of the attack.

Governance and Backup Failure.

Public reporting following the attack indicated that backup capacity existed but had not been uniformly utilized by participating government agencies. This reveals a governance problem in which technical capability and organizational implementation were misaligned.

The existence of a backup facility therefore did not automatically translate into resilient sovereign infrastructure.

Dependence on Complex Proprietary Technology Stacks.

The broader technical mapping further demonstrated that centralized government cloud environments depend upon multi-layered hardware, virtualization, software, and security ecosystems that are rarely produced entirely within a single national technological system.

The sovereignty challenge is consequently not simply where data are physically stored, but whether the state possesses sufficient technical, organizational, and supply-chain capacity to secure, maintain, recover, and independently govern the infrastructures on which those data depend.

Table 7 summarizes these findings.

Table 7. Sovereign Ambition and Operational Vulnerability

Dimension	**Sovereign Objective**	**Observed Operational Reality**	**Socio-Technical Consequence**
National data infrastructure	Consolidated, nationally governed infrastructure for public-sector information systems.	Concentration of services increases systemic exposure when backup, segmentation, and recovery practices are inconsistent.	Large-scale service disruption can propagate across multiple government institutions following a single infrastructure incident.
Technological autonomy	Greater domestic control over security-critical digital infrastructure.	Continued reliance on globally produced hardware, software, cloud, and cyber-security ecosystems.	Administrative control coexists with technological and supply-chain dependency.
Threat detection and incident response	Coordinated national cyber-security monitoring and response capacity.	Different levels of cyber-security maturity across ministries, agencies, operators, and service providers.	Response effectiveness depends on organizational coordination rather than central policy alone.
Data protection	National legal framework designed to protect personal data and establish accountability.	Regulatory framework developed faster than the dedicated supervisory institution responsible for comprehensive enforcement.	Normative sovereignty is stronger than institutional enforcement capacity.

3.4. Grassroots Cultural Resistance and Everyday Digital Adaptation

The fourth major finding concerns the capacity of users and digital communities to adapt to state-imposed digital restrictions. Across ethnographic observations and interviews with ACT and CSO participants, resistance rarely appeared as a single organized anti-state movement. Instead, it consisted of a continuum ranging from everyday convenience-driven workarounds to explicitly political forms of digital activism.

This distinction is important because technical circumvention does not automatically constitute political resistance. Some users adopted alternative connectivity tools to access entertainment or commercial services; others sought privacy or reliability; and others explicitly interpreted circumvention as resistance to state control.

Nevertheless, when aggregated across large digital communities, these practices collectively reduce the practical impermeability of centrally imposed digital boundaries.

3.4.1. Diffusion of Circumvention Practices

The 2022 PSE blocking episode demonstrated how rapidly knowledge of circumvention techniques could diffuse through Indonesian digital networks. Ethnographic observations recorded extensive public discussion concerning VPN services, alternative DNS mechanisms, proxy technologies, browser-level privacy features, and other mechanisms capable of altering conventional access pathways.

Rather than remaining confined to highly specialized cyber-security communities, circumvention knowledge circulated through mainstream social platforms, messaging applications, technology forums, video tutorials, and peer-to-peer explanations.

ACT-02 described this process as follows:

> "Blocking a popular service does not necessarily mean people stop using it. Very often, the first consequence is that people begin asking how the block works. Someone explains VPNs, someone explains DNS, and suddenly a technical subject that was previously limited to technology communities becomes ordinary public knowledge" [ACT-02].

This finding suggests that restriction can produce an unintended educational effect. Enforcement may reduce access for users with limited technological knowledge, while simultaneously encouraging a subset of users to acquire new technical literacy.

The empirical evidence does not establish that all Indonesian users adopted circumvention technologies. Rather, it demonstrates that regulatory interventions can accelerate the *social diffusion of circumvention knowledge*.

3.4.2. A Typology of Technical and Cultural Adaptation

Four broad modes of adaptation emerged from the ethnographic and interview corpus.

Table 8. Typology of Grassroots Responses to Digital Control

Resistance Mode	Observed Practice	Targeted Governance Mechanism	Primary Diffusion Environment
Network-path adaptation	VPNs, encrypted or alternative DNS services, proxy systems, privacy-oriented routing, and related access technologies.	DNS blocking, IP restrictions, geographically differentiated access, and selected network controls.	Technology communities, mainstream social media, video tutorials, messaging groups, and peer networks.
Platform adaptation	Migration between platforms, mirror sites, alternative accounts, decentralized communication services, and content replication.	Platform-level takedowns, account restrictions, and domain blocking.	Activist networks, creator communities, independent media, and public social platforms.
Linguistic adaptation	Intentional spelling changes, wordplay, euphemism, satire, images containing text, memes, coded references, and multilingual substitutions.	Keyword-based discovery, automated moderation, social monitoring, and perceived algorithmic visibility.	Social-media posts, comment sections, political discussions, and meme communities.
Collective digital advocacy	Hashtag campaigns, public criticism, digital-rights advocacy, petitions, platform-focused protest, and coordinated information dissemination.	Regulatory legitimacy, enforcement decisions, and public narratives supporting restrictive policy.	Civil society networks, social media, professional communities, independent media, and digitally networked economic groups.

These practices demonstrate that resistance operates across the same layers through which state power is exercised. Network-level intervention produces network-level adaptation; platform restrictions generate platform migration; content monitoring encourages discursive transformation; and regulatory enforcement generates public political mobilization.

3.4.3. Algorithmic Evasion and *Bahasa Plesetan*

One of the most distinctive findings concerned linguistic adaptation. Indonesian digital discourse frequently incorporates humor, abbreviations, multilingual slang, phonetic substitution, visual symbolism, satire, memes, and *bahasa plesetan*—forms of wordplay in which familiar expressions are intentionally modified while remaining interpretable to culturally situated audiences.

Participants reported that these practices sometimes become strategically significant when users perceive particular terms as likely to attract algorithmic moderation, automated crawling, platform restrictions, or unwanted visibility.

Observed examples included intentionally altered spellings, substitution of characters with numbers or symbols, phonetic variations, use of regional-language vocabulary, image-based text, indirect references to political actors, and continuously changing euphemisms.

CSO-03 described the phenomenon as follows:

> "Indonesian online political language changes extremely quickly. It is ironic, slang-heavy, multilingual, and full of wordplay. Once one term becomes too visible, communities

> often create another variation. The meaning remains understandable to people inside the conversation even when the vocabulary changes" [CSO-03].

The study does not claim that every such linguistic transformation successfully defeats automated content-classification systems. Nor did the research directly benchmark AIS or platform machine-learning accuracy against these linguistic forms.

Rather, the empirical significance lies in the *perception and social practice of algorithmic evasion*: users actively modify language because they understand digital communication as taking place within environments where visibility is partly algorithmically mediated.

This finding transforms cultural resistance from a purely political concept into a socio-technical practice. Language itself becomes part of the negotiation over machine-readable sovereignty.

3.4.4. Collective Campaigning and Digital Counter-Hegemony

Resistance also occurred through organized public mobilization. The *#BlokirKominfo* campaign following the July 2022 PSE enforcement episode illustrates how regulatory controversy can connect otherwise heterogeneous communities.

Public criticism involved digital-rights advocates, gamers, freelance workers, technology professionals, content creators, and ordinary users concerned about access to international digital services. Their motivations were not identical: some objected to potential censorship, others to economic disruption, and others to what they perceived as technically ineffective regulation.

The significance of the campaign therefore lies in its coalition structure. Regulatory enforcement created a temporary convergence between rights-oriented political criticism and economically motivated technological opposition.

Digital ethnographic observations further identified coordinated criticism directed toward government social-media channels, public-facing digital services, and online discussions concerning the technical competence and legitimacy of the regulatory regime.

The resulting public discourse challenged the state's exclusive authority to define what constituted legitimate digital sovereignty. Whereas official narratives emphasized jurisdiction, security, and platform responsibility, counter-narratives emphasized access, livelihood, technical competence, freedom of expression, and the social costs of centralized control.

3.5. The "Bending" Effect: Negotiated Digital Sovereignty in Practice

The final cross-stream synthesis demonstrates that the interaction of regulatory authority, technical capacity, infrastructural dependency, and social adaptation produces what this study terms the *bending effect*.

A digital bulwark is "bent" when a formally asserted boundary remains legally intact but its practical operation is modified by technological, economic, institutional, or social pressures.

Four recurring forms of bending were identified.

3.5.1. Administrative Recalibration

The first form occurs when technically enforceable regulatory decisions produce consequences that require administrative modification.

The temporary restoration of PayPal following the 2022 PSE blocking episode provides the clearest example. The state did not abandon the registration requirement. Instead, implementation was temporarily modified because rigid enforcement created consequences for users requiring access to funds [13].

The sovereign rule therefore persisted while the enforcement pathway was recalibrated.

3.5.2. Technological Porosity

The second form concerns restrictions that remain legally valid but are technologically permeable. DNS restrictions illustrate this condition particularly clearly. The state can require participating intermediaries to block listed domains, yet the global resource itself remains outside the filtering layer.

This produces a distinction between *formal inaccessibility* and *practical inaccessibility*. A resource may be officially blocked while remaining accessible to users employing alternative access pathways.

Digital sovereignty therefore varies across users according to technical literacy, infrastructure, economic resources, and knowledge of alternative technologies.

3.5.3. Institutional Lag

The third form of bending occurs when legislation creates formal authority that institutional structures cannot immediately operationalize.

The PDP framework exemplifies this condition. The legal regime created comprehensive obligations and mandated a dedicated supervisory institution, yet the authority remained under development during the study period [6,14].

In this case, sovereignty is legally articulated but institutionally incomplete.

3.5.4. Infrastructural Dependency

The fourth form occurs when a state can exercise regulatory authority over systems whose underlying technological production and maintenance remain transnational.

Foreign-proprietary infrastructure does not eliminate sovereignty, but it conditions the forms sovereignty can take. States may determine policy objectives while remaining dependent on external vendors, technical standards, global cloud architectures, semiconductor supply chains, software ecosystems, and international network interconnection.

The resulting condition is better described as *interdependent sovereignty* than complete technological autonomy.

3.5.5. Integrated Empirical Model

Table 9 summarizes how the four dimensions interacted across the empirical cases.

Table 9. Empirical Manifestations of the Bending Effect

Sovereign Domain	Initial State Assertion	Friction Mechanism	Negotiated Outcome
Platform regulation	Mandatory registration and potential access blocking for non-compliant electronic system operators.	Economic disruption, user backlash, dependence on global platforms, and platform negotiation.	Temporary restoration, normalization following registration, and pragmatic enforcement adjustment.
Content governance	Central identification and restriction of prohibited online content through platform requests and network-level blocking.	Alternative access technologies, replicated content, platform migration, and linguistic adaptation.	Persistent but porous content boundaries requiring continuous enforcement rather than one-time exclusion.
Personal data governance	Comprehensive national legal framework establishing data-subject rights and controller obligations.	Institutional implementation lag and delayed establishment of the dedicated supervisory authority.	Strong normative framework combined with incomplete institutional enforcement capacity.
Public-sector data infrastructure	Centralized nationally governed data-center infrastructure intended to strengthen control and efficiency.	Cyber-security failures, insufficient backup adoption, organizational fragmentation, and systemic concentration risk.	Greater emphasis on resilience, backup governance, audit, and recovery rather than centralization alone.
Technological autonomy	National aspiration for stronger domestic control over cyber-security and digital infrastructure.	Dependence on foreign-proprietary hardware, software, cloud ecosystems, and global technical standards.	Sovereignty becomes a strategy of dependency management rather than complete technological independence.
Citizen communication	Legal and technical governance of digital expression and access.	Circumvention, platform migration, satire, *bahasa plesetan*, and digitally networked advocacy.	Digital boundaries are continuously renegotiated through user adaptation and cultural innovation.

3.6. Synthesis of Findings

Taken together, the findings answer the three research questions by demonstrating that Indonesian digital sovereignty is neither absent nor absolute.

Regarding **RQ1**, the state operationalizes digital sovereignty through an increasingly dense combination of platform-registration requirements, electronic information regulation, personal data governance, access-restriction mechanisms, automated content identification, ISP obligations, national cyber-security institutions, and centralized public digital infrastructure. These mechanisms substantially increase the state's capacity to project jurisdiction into digital environments.

Regarding **RQ2**, grassroots responses reshape these boundaries through multiple forms of technical and cultural adaptation. VPNs and alternative network pathways alter how restrictions are experienced; platform migration reduces dependency upon individual services; digital-rights mobilization contests regulatory legitimacy; and linguistic practices such as satire, coded expression, and *bahasa plesetan* modify the relationship between human communication and algorithmic monitoring.

Regarding **RQ3**, state digital authority is constrained by three primary structural factors: the transnational architecture of the Internet, dependency upon globally produced technological systems, and uneven institutional capacity to translate regulatory ambition into secure and resilient infrastructure. The PDNS ransomware incident demonstrated particularly clearly that territorial control over infrastructure does not automatically produce cyber-security resilience.

The empirical evidence therefore supports a model of *negotiated digital sovereignty*. In this model, sovereignty does not disappear simply because citizens can circumvent a block, nor is sovereignty complete merely because the government possesses the legal authority to impose one. Effective digital sovereignty is continuously produced through interactions among law, code, infrastructure, markets, institutions, and culture.

The metaphor of "bending the bulwarks" captures this dynamic. Indonesia's digital boundaries possess sufficient regulatory and technological strength to influence platform behavior, constrain access, and reorganize digital governance. Yet they remain sufficiently porous that technological adaptation, public resistance, infrastructural failure, economic dependency, and global interconnection repeatedly alter how those boundaries function in practice.

Digital sovereignty in Indonesia is therefore best understood not as a completed fortress, but as a contested and continuously reconstructed socio-technical boundary.

4. Discussion

The empirical findings presented in Section 3 demonstrate that digital sovereignty in Indonesia cannot be adequately conceptualized as the construction of an impermeable, state-controlled digital territory. Instead, the Indonesian case reveals a more complex configuration characterized by regulatory expansion, infrastructural dependency, technical porosity, institutional unevenness, and continuous negotiation between state and non-state actors.

This finding complicates conventional understandings of cyber sovereignty that equate sovereign capacity with the ability of a state to construct technically enforceable digital borders. In Indonesia, the expansion of legal jurisdiction does not automatically generate equivalent technological autonomy, while technological control does not necessarily produce stable social compliance. Regulatory intervention instead generates responses from platforms, infrastructure providers, civil society organizations, technology communities, and individual users, each of which can alter how formally established digital boundaries function in practice.

The Indonesian case therefore suggests that digital sovereignty should be treated as a relational and socio-technical condition rather than a binary state of either sovereign control or sovereign failure. The capacity to regulate digital platforms, restrict content, govern personal data, or centralize public infrastructure constitutes only one dimension of sovereignty. Effective sovereign power additionally depends upon institutional legitimacy, infrastructural resilience, technological autonomy, intermediary cooperation, economic interdependence, and the adaptive behavior of citizens.

The discussion develops this argument through four theoretical implications: (1) the transition from digital enclosure toward negotiated sovereignty in Global South contexts; (2) the sovereignty–security paradox produced by excessive centralization; (3) the emergence of everyday digital adaptation as informal socio-technical infrastructure; and (4) the policy tension between sovereign regulation and an open, interoperable Internet.

4.1. Rethinking Digital Sovereignty in the Global South: From Enclosure to Negotiated Control

Scholarship on cyber and digital sovereignty has frequently examined highly state-centric models of Internet governance, particularly those associated with China and Russia [2]. These cases demonstrate how states may combine legal authority, infrastructural intervention, platform governance, data regulation, domestic technology policy, and national-security discourse to strengthen control over digital environments.

However, directly applying such models to Indonesia risks obscuring substantial differences in political economy, technological capacity, platform ecosystems, civil society organization, and institutional structure.

China, for example, has combined extensive information-control capabilities with the long-term development of a large domestic platform ecosystem and increasingly sophisticated national technological capacity [2]. Russia has pursued a different but related process of "sovereignization" aimed at increasing the state's technical and legal capacity to govern the RuNet and reduce selected external dependencies [2].

Indonesia exhibits neither configuration in equivalent form.

The findings instead indicate a model of *negotiated digital sovereignty*. The Indonesian state possesses substantial legal and administrative capacity to impose obligations upon electronic system operators, request content removal, regulate personal data, coordinate cyber-security institutions, and require intermediary participation in access restrictions. Yet these capabilities coexist with extensive reliance on global platforms, transnational cloud infrastructures, internationally produced cyber-security technologies, global payment systems, and interconnected Internet architectures.

This produces a fundamental constraint on sovereign enforcement. Blocking or restricting a globally important digital service does not affect only the targeted corporation. It can simultaneously affect Indonesian consumers, freelance workers, software developers, creative industries, businesses, and other actors whose economic activities depend upon that infrastructure.

The 2022 PSE enforcement episode illustrates this condition particularly clearly. The state was technically and legally capable of restricting access to unregistered services, but the economic and social consequences of doing so generated immediate pressures for administrative adjustment. As demonstrated in Section 3.5, sovereignty was therefore exercised, but its implementation was subsequently recalibrated.

This differs from the idea of sovereignty as complete enclosure. Indonesian sovereign authority operates within an environment whose economic value depends substantially upon maintaining connectivity with the very transnational platforms and infrastructures over which the state seeks greater jurisdiction.

Table 10 provides an analytical comparison. The categories should be interpreted as ideal types rather than exhaustive descriptions of any individual country.

Table 10. Ideal-Typical Comparison of State-Centric Digital Sovereignty and the Indonesian Negotiated Model

Analytical Dimension	High-Control Sovereignization Model	Indonesian Negotiated Sovereignty	Theoretical Implication
Platform ecosystem	Greater capacity to sustain domestic platform alternatives or impose extensive national control over platform access.	Substantial economic and social dependence on globally interconnected platforms and services.	Blocking decisions impose domestic costs and strengthen incentives for regulatory negotiation.
Regulatory capacity	Dense legal and administrative mechanisms combined with sustained state-centric enforcement.	Expanding legal jurisdiction combined with uneven implementation and intermediary dependence.	Legal sovereignty can exceed operational sovereignty.
Technical capacity	Greater institutionalized capacity for centralized network intervention and systematic information control.	Mixed filtering, intermediary cooperation, content-removal procedures, and heterogeneous network-level controls.	Sovereignty varies across technical layers rather than operating as a single integrated barrier.
Technological autonomy	Strategic efforts to develop domestic technologies, infrastructures, platforms, or standards capable of reducing selected external dependencies.	Persistent reliance on foreign-origin hardware, software, cloud, platforms, security products, and global technical ecosystems.	Administrative sovereignty can coexist with substantial technological dependency.
Civil society environment	Public circumvention and political opposition may face stronger institutional constraints, although circumvention remains present.	Relatively visible civil society contestation, public campaigns, legal challenges, technological adaptation, and digital-rights advocacy.	State power is continuously subjected to social and institutional counter-pressure.
Sovereign outcome	Greater potential for sustained information enclosure, although never technically absolute.	Porous, selective, adaptive, and continuously renegotiated digital boundaries.	Digital sovereignty is more accurately conceptualized as a process than an achieved condition.

The comparison suggests that digital sovereignty should not be understood along a single continuum ranging from "weak" to "strong". A state may simultaneously possess strong legal jurisdiction, moderate network-control capacity, limited technological autonomy, high dependence on foreign platforms, and substantial domestic political contestation.

Digital sovereignty is therefore multidimensional.

The Indonesian case further demonstrates that the state is not the only actor capable of shaping sovereign outcomes. Transnational corporations can alter policy feasibility through market power; Internet service providers operationalize or constrain network-level enforcement; courts can challenge executive actions; civil society organizations can contest regulatory legitimacy; and users can technologically adapt to restrictions.

Consequently, sovereignty in digitally interconnected societies is relational. State power remains important, but its effective scope is produced through interactions with other actors possessing infrastructural, economic, legal, or cultural resources.

This study therefore defines *negotiated digital sovereignty* as:

> A condition in which the state's formal authority to regulate digital territory is continuously translated, constrained, and reconfigured through interactions among technological infrastructures, economic dependencies, intermediaries, institutional checks, and adaptive social practices.

This conceptualization moves the analytical question away from whether Indonesia "has" or "does not have" digital sovereignty. The more productive question becomes: *which dimensions of sovereignty can the state exercise, through which technological layers, under what institutional conditions, and with what forms of resistance or dependency?*

4.2. The Sovereignty–Security Paradox: Centralization, Control, and Resilience

A second theoretical contribution concerns the relationship between administrative centralization and cyber-security resilience.

Digital sovereignty discourse frequently associates national control with the consolidation of critical information systems, government data, institutional authority, and strategic cyber-security capabilities. From an administrative perspective, centralization can offer significant advantages. It can facilitate standardization, reduce duplication, improve visibility, simplify coordination, and enable common security requirements to be imposed across previously fragmented institutions.

However, the findings indicate that centralization and security are not equivalent.

The 2024 PDNS ransomware incident provides an important empirical demonstration of this distinction. As discussed in Section 2.2.2, the incident did not merely represent a conventional cyber-security failure. It exposed a broader mismatch among infrastructural consolidation, organizational responsibility, backup practices, and disaster-recovery capacity.

The central theoretical problem can be represented as follows:

$$\text{Administrative Centralization} \neq \text{Cyber-Security Resilience} \tag{1}$$

Centralization can improve administrative legibility and coordination, but without appropriate redundancy and institutional security maturity it can simultaneously increase the consequences of failure.

This produces what this study terms the *sovereignty–security paradox*: measures intended to strengthen sovereign control can weaken practical sovereignty when centralized infrastructure becomes more consequential than the state's capacity to defend and recover it.

A more useful model of sovereign cyber-security is therefore:

$$\text{Digital Resilience} = f(R, B, S, I, C, G) \tag{2}$$

where:

- R = infrastructure redundancy;
- B = reliable backup and restoration capacity;
- S = segmentation and security architecture;
- I = incident detection and response capability;
- C = institutional cyber-security competence; and
- G = governance, accountability, and coordination.

Under this formulation, the physical location or governmental ownership of infrastructure represents only one component of sovereign resilience.

This distinction has important implications for the concept of data sovereignty. Keeping state-controlled information within nationally governed infrastructure may increase

jurisdictional control, but territorial control does not automatically guarantee confidentiality, integrity, availability, or recoverability.

A server may be physically located within Indonesia while depending upon foreign firmware, internationally developed virtualization technologies, externally maintained software libraries, imported network hardware, or vendor-controlled security updates. Conversely, infrastructure incorporating foreign technologies may still be governed through strong contractual, security, audit, interoperability, and redundancy requirements.

Thus, the relevant sovereignty question is not simply:

> "Where is the infrastructure located"?

but rather:

> "Who can govern, inspect, maintain, secure, replace, recover, and ultimately exercise effective control over the infrastructure throughout its operational lifecycle"?

This perspective reframes technological sovereignty away from technological autarky. Complete independence from global technological supply chains is neither empirically realistic nor necessarily desirable for an interconnected digital economy.

Instead, digital sovereignty requires the management of *critical dependencies*. Strategic autonomy is strengthened when the state can identify external dependencies, diversify suppliers, establish interoperability requirements, maintain exit strategies, preserve technical knowledge domestically, test recovery procedures, and prevent individual vendors or infrastructure nodes from becoming irreplaceable.

The PDNS incident therefore reveals a broader theoretical lesson: sovereignty without resilience is fragile. Centralized administrative visibility can strengthen state control while simultaneously increasing systemic vulnerability if resilience does not develop at a comparable pace.

4.3. Cultural Resistance as Everyday Digital Infrastructure

The third major contribution concerns the role of everyday citizen practices in reshaping state digital authority.

Conventional studies of digital activism frequently emphasize highly visible political activities: hashtag campaigns, online petitions, investigative journalism, organized protest, and social movements. These remain important in Indonesia, as illustrated by the #*BlokirKominfo* episode.

However, the findings reveal a second, less formally organized layer of adaptation. Users respond to digital restrictions through routine technical and communicative practices that may not initially appear political: changing network settings, adopting alternative communication services, replicating information, migrating between platforms, modifying vocabulary, distributing technical knowledge, or helping peers restore access.

These practices can be interpreted through James C. Scott's concept of *everyday resistance* and Asef Bayat's concept of the *quiet encroachment of the ordinary* [23,24].

Scott's framework emphasizes forms of resistance that do not necessarily depend upon organized confrontation with authority. Small-scale acts of evasion, non-compliance, adaptation, and circumvention can cumulatively reduce the effectiveness of top-down control.

Bayat similarly directs attention toward the political significance of dispersed practices through which ordinary actors incrementally reshape the environments governing everyday life.

Applied to Indonesian cyberspace, these perspectives suggest that technical circumvention should not be reduced to a purely instrumental response to blocked websites. Repeated and socially transmitted adaptation can produce an alternative layer of digital infrastructure.

This study therefore introduces the concept of *everyday digital infrastructure* to describe:

The decentralized accumulation of technical knowledge, communication practices, alternative access pathways, cultural codes, and peer-support networks through which users maintain digital connectivity under changing conditions of platform and state control.

4.3.1. Technical Normalization and the Social Diffusion of Cyber Knowledge

One important mechanism is the normalization of technologies previously associated with technically experienced users.

VPN services, alternative DNS mechanisms, encrypted communication systems, privacy-oriented browser functions, and related technologies become socially significant when knowledge of them moves beyond specialist communities.

The findings from the 2022 blocking episode indicate that regulatory intervention can create precisely such a diffusion mechanism. Restrictions generate questions about why a service is unavailable; these questions generate explanations of the technical mechanism; explanations subsequently generate peer-to-peer transmission of circumvention knowledge.

The process can be represented conceptually as:

$$\begin{aligned}\text{Restriction} &\rightarrow \text{Technical Curiosity} \rightarrow \text{Knowledge Diffusion} \\ &\rightarrow \text{User Adaptation} \rightarrow \text{Reduced Marginal Effectiveness of Restriction}\end{aligned} \tag{3}$$

This does not mean that censorship invariably increases digital literacy, nor that every user possesses equal capacity to circumvent restrictions. Digital inequalities remain important. Technical knowledge, device capability, economic resources, age, education, geography, and access to trusted information all affect the ability to adapt.

Nevertheless, the empirical pattern indicates an unintended consequence of repeated network restrictions: interventions intended to increase state control may simultaneously increase public awareness of the technical architecture through which that control operates.

4.3.2. Linguistic Subversion and Machine-Readable Sovereignty

The role of *bahasa plesetan* and other forms of linguistic adaptation introduces another theoretical dimension.

Automated governance systems depend upon making human behavior technically legible. Keyword detection, content classifiers, pattern recognition, recommendation algorithms, and automated moderation all require social communication to be translated into machine-readable categories.

Human language, however, is unstable.

Indonesian online discourse incorporates Indonesian, regional languages, English, abbreviations, phonetic transformations, memes, visual references, sarcasm, cultural symbolism, and rapidly changing slang. This creates a persistent interpretive asymmetry between formal classification systems and cultural communication.

When users intentionally exploit this asymmetry, linguistic adaptation becomes a form of *algorithmic negotiation*.

The important finding is not that wordplay makes automated classification universally ineffective. Contemporary machine-learning systems are capable of contextual analysis substantially more sophisticated than simple keyword matching.

Rather, the problem is dynamic adaptation. Classification systems operate against linguistic environments whose participants can observe moderation outcomes and subsequently change their communication strategies.

This creates an iterative relationship:

$$\text{Classification} \rightarrow \text{User Adaptation} \rightarrow \text{Classifier Adjustment} \rightarrow \text{New Adaptation} \tag{4}$$

Digital sovereignty at the content layer therefore cannot be finalized through a static dictionary of prohibited expressions. It requires continuous interpretive labor, and the greater the semantic ambiguity of regulated categories, the greater the potential tension between automated enforcement and contextual human communication.

4.3.3. From Everyday Adaptation to Digital Counter-Hegemony

Everyday adaptation becomes more explicitly political when individual practices converge into collective narratives concerning legitimate digital governance.

The *#BlokirKominfo* controversy demonstrated such a transition. Technical criticism of blocking mechanisms combined with economic grievances, digital-rights concerns, criticism of institutional competence, and broader questions regarding the appropriate boundaries of state authority.

The resulting coalition did not require ideological uniformity.

A digital-rights organization could oppose regulation because of freedom-of-expression concerns; a freelancer because of access to international payments; a gamer because of access to a platform; a developer because of dependency upon global digital infrastructure; and a cyber-security professional because of perceived technical shortcomings.

Different grievances could therefore converge upon a common challenge to the legitimacy or proportionality of regulatory enforcement.

Table 11 connects these empirical practices to broader theoretical concepts.

Table 11. Everyday Resistance and Informal Digital Infrastructure

Theoretical Concept	Conventional Interpretation	Application to Indonesian Digital Space	Implication for Sovereign Control
Everyday resistance	Dispersed, low-visibility forms of evasion and non-compliance outside formal political mobilization.	Routine circumvention, platform migration, alternative connectivity, information replication, and informal technical assistance.	Reduces the practical effectiveness of restrictions without requiring direct confrontation with state institutions.
Quiet encroachment	Cumulative everyday practices through which ordinary actors expand practical autonomy.	Normalization and social diffusion of privacy, alternative-access, and decentralized communication practices.	Creates user practices that become increasingly difficult to govern solely through formal prohibitions.
Informal infrastructure	Systems constructed outside formal state planning to address everyday functional needs.	Peer-distributed technical knowledge, alternative digital channels, mirrored information, community troubleshooting, and decentralized communication.	Creates parallel pathways through which connectivity can persist despite centralized intervention.
Algorithmic negotiation	Adaptive interaction between classification systems and users responding to machine-mediated governance.	Wordplay, coded language, memes, visual communication, multilingual substitution, and changing digital vocabulary.	Increases the interpretive and administrative cost of automated content governance.
Digital counter-hegemony	Collective production of alternative narratives challenging dominant definitions of legitimate governance.	Hashtag campaigns, digital-rights advocacy, technical criticism, economic grievances, and public scrutiny of regulatory institutions.	Challenges the state's ability to define digital sovereignty exclusively through security and administrative control.

The broader implication is that digital resistance should not be interpreted solely through dramatic events such as Internet shutdowns or coordinated political campaigns. The durability of digital autonomy may instead depend substantially upon the accumulated technical and cultural capabilities of ordinary users.

4.4. Digital Sovereignty and the Fragmentation of the Global Internet

The Indonesian case also contributes to broader debates concerning Internet fragmentation, frequently described as the emergence of a "splinternet". Scholarship increasingly recognizes that contemporary Internet governance is characterized not simply by a choice between a global Internet and completely isolated national networks, but by varying forms of fragmentation, regulatory divergence, platform segmentation, and hybridization [2].

Indonesia illustrates this intermediate condition particularly clearly.

The country has not constructed a separate national Internet disconnected from global infrastructure. Instead, fragmentation occurs selectively through platform registration, access restrictions, content-removal requirements, data-governance rules, temporary connectivity restrictions, and intermediary obligations.

Such measures produce what may be described as *jurisdictional fragmentation*: users remain connected to the global Internet, but the services, content, legal obligations, and access conditions they experience differ according to national regulatory boundaries.

This form of fragmentation can serve legitimate objectives. States have valid interests in cyber-security, consumer protection, law enforcement, child protection, data privacy, taxation, market accountability, and protection of critical infrastructure.

The policy problem is therefore not whether states should regulate digital environments.

The more consequential question is how regulatory objectives can be achieved without unnecessarily undermining interoperability, proportionality, security, economic opportunity, and fundamental rights.

The findings reveal three particularly important trade-offs.

4.4.1. Jurisdiction versus Interoperability

Requiring global platforms to comply with Indonesian law can strengthen accountability. Yet regulatory requirements that become technically incompatible with global systems or impose disproportionate obligations may create incentives for service withdrawal, fragmented functionality, or reduced investment.

Digital sovereignty therefore benefits from regulatory interoperability wherever national security or fundamental legal differences do not require divergence.

4.4.2. Content Control versus Cyber-Security Investment

The findings also highlight an allocation problem.

Content governance and cyber-security are frequently grouped under the broad category of digital security, but they address fundamentally different threats. Detecting politically or socially prohibited information does not substitute for maintaining backups, patching vulnerable infrastructure, segmenting networks, protecting administrative credentials, conducting independent security testing, or rehearsing disaster recovery.

The PDNS case demonstrates why this distinction matters.

A state may possess increasingly sophisticated capacity to govern digital content while remaining vulnerable to conventional cyber-security failures affecting critical public infrastructure.

Sovereign capacity should therefore be evaluated partly according to whether resources devoted to cyber governance improve the confidentiality, integrity, availability, and recoverability of critical national systems.

4.4.3. Administrative Efficiency versus Procedural Legitimacy

Rapid executive takedown mechanisms can respond quickly to harmful digital content. However, speed can also reduce opportunities for independent review, procedural contestation, transparency, and proportionality assessment.

This creates a governance trade-off between administrative responsiveness and procedural legitimacy.

The findings suggest that sustainable digital sovereignty requires both. A regulatory system perceived as technically capable but procedurally arbitrary may increase avoidance, resistance, and distrust. Conversely, a highly deliberative system incapable of responding rapidly to genuine cyber threats may fail to protect users and infrastructure.

The relevant policy objective is therefore not maximal state control, but *legitimate and resilient regulatory capacity*.

4.5. Policy Implications: From Control-Oriented Sovereignty to Resilient Digital Governance

The results suggest that Indonesia does not need to abandon the pursuit of digital sovereignty. Rather, the meaning of sovereignty should shift from an emphasis on centralized control toward a broader model combining jurisdiction, technological resilience, institutional accountability, strategic autonomy, and public legitimacy.

Four policy implications follow from the analysis.

4.5.1. Strengthening Independent and Procedural Oversight

Content-removal and platform-restriction mechanisms should incorporate stronger safeguards capable of distinguishing clearly unlawful or immediately harmful material from contested political, journalistic, cultural, or public-interest expression.

Depending upon the severity and urgency of the measure, safeguards may include transparent legal criteria, documented justification, notice procedures, meaningful opportunities for appeal, independent review, and judicial authorization or subsequent judicial scrutiny where significant restrictions on rights are involved.

The objective is not to eliminate executive capacity to respond to urgent threats, but to reduce discretionary overreach and strengthen institutional legitimacy.

4.5.2. Prioritizing Infrastructure Resilience

Cyber-security investment should place greater emphasis on resilience of critical public infrastructure.

Priority areas include:

- mandatory and routinely tested backup procedures;
- geographically and logically separated recovery environments;
- network segmentation;
- vulnerability and patch management;
- identity and privileged-access management;
- independent security assessment;
- coordinated vulnerability disclosure mechanisms;
- incident-response exercises;
- cyber-security capacity development for public institutions; and
- measurable recovery-time and recovery-point objectives for critical services.

These capabilities strengthen sovereignty because they increase the state's ability to maintain essential functions under adverse conditions.

4.5.3. Replacing Autarky with Strategic Technological Autonomy

Reducing dependency on external technologies should not be interpreted as requiring the elimination of foreign technology.

A more feasible strategy involves identifying *critical dependencies* and ensuring that no single external dependency can unreasonably compromise national continuity.

Relevant measures include:

- supplier diversification;
- interoperability and portability requirements;
- transparent procurement standards;
- domestic technical capacity development;
- source-code or security review requirements where appropriate;
- contractual exit and continuity provisions;
- local incident-response competence;
- support for domestic open-source ecosystems; and
- investment in strategically important national research and development.

This approach transforms digital sovereignty from technological isolation into the capacity to make meaningful technological choices.

4.5.4. Institutionalizing Multi-Stakeholder Governance

The findings further indicate that government agencies do not possess all of the knowledge required for effective digital governance.

Internet service providers understand network architecture; civil society organizations identify rights-related consequences; security researchers discover technical vulnerabilities; universities contribute independent analysis; businesses understand economic dependencies; and digital communities observe practical circumvention and user behavior.

Cyber-governance frameworks should therefore provide structured mechanisms through which these groups participate in regulatory design and evaluation.

A multi-stakeholder model does not require the state to surrender regulatory authority. Rather, it increases the informational quality, technical feasibility, and societal legitimacy of state decision-making.

4.6. Theoretical Synthesis: The Negotiated Digital Sovereignty Model

Drawing together the empirical and theoretical findings, this study proposes an integrated model of *negotiated digital sovereignty*.

The model treats effective sovereign capacity (S_{eff}) as dependent upon five interacting dimensions:

$$S_{\text{eff}} = f(L, T, I, A, R) \tag{5}$$

where:

- L = legal and regulatory authority;
- T = technological and infrastructural capacity;
- I = institutional competence and implementation capacity;
- A = technological autonomy and management of external dependency; and
- R = social legitimacy, resistance, and adaptive user response.

The model differs from state-centric interpretations because increases in one dimension do not necessarily produce proportional increases in effective sovereignty.

For example:

- stronger legal authority without technical capacity produces *symbolic or weakly enforceable sovereignty*;
- stronger technical control without institutional legitimacy produces *contested sovereignty*;
- centralized infrastructure without resilience produces *fragile sovereignty*;
- national regulation built upon irreplaceable foreign technological dependencies produces *dependent sovereignty*; and
- extensive state restrictions combined with widespread citizen adaptation produce *porous sovereignty*.

Indonesia exhibits elements of each condition.

The concept of *bending* therefore describes the mechanism through which these dimensions interact. State authority establishes an intended digital boundary, but that boundary changes when it encounters technological architecture, economic dependency, institutional limitations, private intermediaries, legal contestation, and citizen adaptation.

This can be represented as:

$$B_{t+1} = B_t + S_t - (F_t + D_t + R_t) \tag{6}$$

where B_t represents the state's intended digital boundary at a given time, S_t represents additional regulatory or technological state intervention, F_t represents technical and institutional friction, D_t represents external dependency, and R_t represents social resistance and adaptation.

Equation 6 is conceptual rather than predictive. Its purpose is to illustrate that formally imposed digital boundaries are continuously modified through countervailing sociotechnical forces.

Accordingly, the Indonesian case challenges both technological determinism and state determinism. Technology does not automatically produce political control, and legal authority does not automatically determine technological outcomes. Equally, grassroots adaptation does not eliminate state power.

Instead, law, infrastructure, institutions, markets, technologies, and culture co-produce the practical boundaries of Indonesian cyberspace.

4.7. Study Limitations and Future Research Directions

Several limitations define the scope of the conclusions presented in this study.

First, digital governance infrastructures evolve rapidly. Filtering mechanisms, encryption standards, browser capabilities, platform moderation architectures, circumvention technologies, and Internet service provider configurations can change significantly within relatively short periods. Technical observations should therefore be interpreted as temporally bounded rather than permanent descriptions of Indonesian network architecture.

Second, the study relied primarily upon publicly observable infrastructure evidence and interviews rather than privileged access to internal state cyber-security systems. Consequently, the research cannot establish a complete inventory of government network-monitoring, threat-intelligence, or classified cyber-security capabilities.

Third, the technical component reconstructed observable architecture through OSINT-based evidence rather than active penetration testing or direct auditing of restricted government systems. This methodological constraint was necessary for both ethical and practical reasons, but limits claims concerning internal configuration, vendor-specific implementation, and classified capabilities.

Fourth, the interview sample was designed for analytical diversity rather than statistical representativeness. The perspectives of regulators, engineers, civil society actors, and activists provide important explanatory depth but cannot be interpreted as population-level estimates of Indonesian public opinion.

Fifth, public digital ethnography is more likely to capture technologically engaged and politically expressive users than individuals with limited technical participation. Circumvention and resistance identified in this study should therefore be interpreted as observable repertoires of action rather than universally adopted practices.

Future research should develop the present analysis in at least four directions.

First, comparative research should examine whether negotiated digital sovereignty also characterizes other Southeast Asian states. Comparative studies involving Indonesia, Malaysia, Thailand, Vietnam, and the Philippines could identify how differences in political institutions, domestic technological capacity, civil society organization, and platform dependence affect sovereign outcomes.

Second, future research should incorporate longitudinal and ethically designed network measurements to examine changes in DNS interference, routing behavior, service reachability, latency, throttling, and other observable forms of network intervention across regions and Internet service providers. Such measurement should distinguish demonstrable technical behavior from assumptions regarding the specific equipment or institutional actor responsible.

Third, longitudinal policy research should examine the institutionalization and practical enforcement of Indonesia's personal data protection framework, including the eventual establishment, independence, authority, enforcement practices, and accountability mechanisms of the institution responsible for personal data protection.

Fourth, future studies should investigate inequality in circumvention capacity. The ability to maintain access under conditions of restriction is unlikely to be evenly distributed across geography, income, education, age, device ownership, gender, disability, and technological literacy. Digital circumvention may therefore create a secondary form of inequality in

which technically sophisticated users experience significantly more porous digital borders than less technologically capable populations.

4.8. Discussion Summary

The discussion demonstrates that Indonesia's pursuit of digital sovereignty cannot be adequately understood through the metaphor of a completed digital fortress. The state has clearly expanded its capacity to regulate platforms, govern electronic information, intervene in network access, protect personal data, and centralize critical digital infrastructure. These developments represent substantive sovereign power rather than merely symbolic policy.

Yet this power remains conditional.

Regulation is constrained by economic interdependence; centralized infrastructure is constrained by cyber-security resilience; technological autonomy is constrained by global supply chains; content governance is constrained by linguistic and technical adaptation; and executive authority is constrained by public legitimacy, legal institutions, and civil society mobilization.

The Indonesian case therefore demonstrates that digital sovereignty is simultaneously *real, partial, contested, and dynamic*.

The central theoretical contribution of this study is accordingly not the claim that Indonesian digital sovereignty has failed. Rather, it is that sovereignty itself is continuously negotiated. Its practical boundaries emerge from the interaction between state authority and the technological and social environment through which that authority must operate.

The "bulwarks" of sovereignty are consequently neither absent nor unbreakable. They bend.

This bending is not merely evidence of state weakness. It is the normal political condition of sovereignty within an interconnected socio-technical system in which no single actor—state, corporation, infrastructure provider, or citizen network—possesses complete control over the architecture of digital life.

5. Conclusion

This study examined how legal authority, cyber-security technologies, infrastructural dependencies, and grassroots digital practices interact in shaping digital sovereignty in Indonesia. The findings demonstrate that Indonesian digital sovereignty is neither an absent political aspiration nor a completed system of state control. Rather, it operates as a structurally porous and continuously contested process of *negotiated digital sovereignty*.

Regarding the first research question, the Indonesian state has substantially expanded its capacity to project authority into digital environments through regulatory instruments such as Minister of Communication and Informatics Regulation No. 5 of 2020 and its amendment, the Personal Data Protection Law, the amended Electronic Information and Transactions Law, platform-registration requirements, content-removal procedures, ISP-level access restrictions, national cyber-security institutions, and increasingly centralized public digital infrastructure. These developments demonstrate that digital sovereignty has become an institutionalized component of contemporary Indonesian governance rather than merely a rhetorical policy objective.

However, the findings concerning the second and third research questions demonstrate that formal regulatory authority does not translate automatically into comprehensive technological control. Indonesia's digital-governance architecture remains constrained by the globally interconnected structure of the Internet, uneven institutional implementation, dependence on transnational platforms and foreign-origin technological ecosystems, and limitations in the resilience of critical public infrastructure. The 2024 ransomware attack against the Temporary National Data Center (PDNS 2) illustrated this contradiction particularly clearly: greater administrative centralization did not necessarily produce greater cyber-security resilience.

Network-level control mechanisms similarly remain technically contingent. DNS interference and other forms of intermediary-based restriction can limit conventional access

to targeted digital resources, while more sophisticated network-management technologies may increase the state's ability to classify or manage traffic. Yet these mechanisms do not create an impermeable national digital border. Their effectiveness varies across infrastructure providers, technological layers, implementation contexts, and user capabilities.

At the societal level, the findings demonstrate that Indonesian Internet users are not passive recipients of digital regulation. Technical circumvention, alternative access pathways, platform migration, privacy-oriented technologies, digital-rights advocacy, and culturally embedded communicative practices provide multiple mechanisms through which state-imposed digital boundaries are negotiated in everyday life. Linguistic adaptation, including *bahasa plesetan*, satire, coded expression, and rapidly changing online vocabulary, further illustrates how culturally situated communication complicates attempts to translate social discourse into stable machine-readable categories.

Importantly, the study does not suggest that all such practices constitute organized political resistance or that circumvention eliminates state power. Instead, the cumulative effect of technological and cultural adaptation is to make sovereign control conditional, differentiated, and costly to maintain. Restrictions that are legally enforceable may remain technically porous, while technically effective interventions may generate economic, institutional, or political pressures that encourage subsequent recalibration.

The principal theoretical contribution of this study is therefore the concept of *negotiated digital sovereignty*. This perspective challenges binary interpretations that classify states as either digitally sovereign or technologically dependent. Effective digital sovereignty instead emerges from the interaction of at least five dimensions: legal authority, technological capacity, institutional competence, management of external technological dependency, and societal legitimacy and adaptation. Strength in one dimension cannot fully compensate for weakness in another.

The metaphor of *bending the bulwarks* captures this condition. Indonesia has constructed meaningful legal and technological boundaries around its digital environment, but these boundaries continually bend under the pressures of global technological interdependence, infrastructure vulnerability, economic necessity, intermediary power, institutional contestation, and citizen adaptation. The resulting digital order is therefore neither fully open nor fully enclosed, but continuously reconstructed through socio-technical negotiation.

These findings have several implications for Indonesian cyber-governance. First, strengthening digital sovereignty requires moving beyond an emphasis on access restriction and administrative control toward the resilience of critical national infrastructure. Reliable backup systems, redundancy, network segmentation, vulnerability management, incident-response capability, and institutional cyber-security competence are fundamental components of meaningful sovereign capacity.

Second, technological sovereignty should be understood as *strategic autonomy* rather than technological isolation. Indonesia's objective should not necessarily be to eliminate foreign technologies, but to reduce critical single-vendor dependencies, strengthen domestic technical expertise, improve interoperability, diversify strategic suppliers, and ensure that essential systems can be independently maintained, audited, recovered, or replaced.

Third, regulatory legitimacy requires stronger procedural safeguards. Platform restrictions, content-removal mechanisms, and other forms of digital intervention should be accompanied by transparent legal standards, proportionality assessments, meaningful opportunities for appeal, independent oversight, and appropriate judicial review where fundamental rights are substantially affected.

Fourth, sustainable digital governance requires institutionalized multi-stakeholder participation. Civil society organizations, universities, cyber-security researchers, technology companies, Internet service providers, independent technical communities, and affected user groups possess forms of expertise that cannot be reproduced entirely within centralized administrative institutions. Their participation can strengthen both the technical quality and democratic legitimacy of digital policy.

For Global South democracies more broadly, the Indonesian experience demonstrates that digital sovereignty cannot be sustainably constructed through top-down technological enclosure alone. States operating within globally interconnected digital economies must simultaneously manage national-security concerns, foreign technological dependencies, economic integration, citizen rights, cyber-security resilience, and socially adaptive digital cultures.

Consequently, the central policy challenge is not how to construct an impermeable digital fortress. Such a goal is both technically unrealistic and economically costly within an interconnected Internet ecosystem. The more sustainable objective is to develop a digital-governance framework capable of exercising legitimate national authority while remaining resilient, accountable, interoperable, and responsive to the society it governs.

Indonesia's experience ultimately demonstrates that sovereignty in cyberspace is not a finished technological condition. It is an ongoing political and socio-technical process. The state's digital bulwarks exist, but their boundaries are continuously negotiated, contested, and reshaped. In this sense, the most durable form of digital sovereignty may not be the capacity to prevent those bulwarks from bending, but the institutional capacity to govern responsibly and resiliently as they inevitably do.

References

1. Pohle, J.; Thiel, T. Digital Sovereignty. *Internet Policy Review* **2020**, *9*. https://doi.org/10.14763/2020.4.1532
2. Mueller, M.L. *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*; Polity Press: Cambridge, UK, 2017.
3. Asosiasi Penyelenggara Jasa Internet Indonesia. Pengguna Internet Indonesia Tembus 221 Juta Orang. 2024. Available online: https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang (accessed on 17 August 2026).
4. Ministry of Communication and Informatics of the Republic of Indonesia. Regulation Number 5 of 2020 concerning Private Electronic System Operators; Jakarta, Indonesia, 2020.
5. Ministry of Communication and Informatics of the Republic of Indonesia. Regulation Number 10 of 2021 concerning the Amendment to Regulation Number 5 of 2020 on Private Electronic System Operators; Jakarta, Indonesia, 2021.
6. Republic of Indonesia. Law Number 27 of 2022 concerning Personal Data Protection; Jakarta, Indonesia, 2022.
7. Republic of Indonesia. Presidential Regulation Number 47 of 2023 concerning the National Cyber Security Strategy and Cyber Crisis Management; Jakarta, Indonesia, 2023.
8. Gillespie, T. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*; Yale University Press: New Haven, CT, USA, 2018.
9. Latour, B. *Reassembling the Social: An Introduction to Actor-Network-Theory*; Oxford University Press: Oxford, UK, 2005.
10. Bijker, W.E.; Hughes, T.P.; Pinch, T.J., Eds. *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*; MIT Press: Cambridge, MA, USA, 1987.
11. Republic of Indonesia. Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions; Jakarta, Indonesia, 2024.
12. Reuters. Indonesia Blocks Yahoo, PayPal, Gaming Websites over Licence Breaches. 30 July 2022.
13. Reuters. Indonesia Opens Temporary Access to PayPal after Blocking Sparks Backlash. 31 July 2022.
14. Antara News. Indonesia to Establish Independent Personal Data Protection Agency. 4 February 2026. Available online: https://en.antaranews.com/news/402914/indonesia-to-establish-independent-personal-data-protection-agency (accessed on 17 August 2026).
15. Ministry of Communication and Informatics of the Republic of Indonesia. Regulation Number 19 of 2014 concerning the Handling of Internet Sites Containing Negative Content; Jakarta, Indonesia, 2014.
16. Ministry of Communication and Informatics of the Republic of Indonesia. AIS Internet Content Crawling System; Jakarta, Indonesia, 2018.
17. Open Observatory of Network Interference. No Access: LGBTIQ Website Censorship in Six Countries. 31 August 2021. Available online: https://ooni.org/post/2021-no-access-lgbtiq-website-censorship-six-countries/ (accessed on 17 August 2026).
18. Citizen Lab. Planet Blue Coat: Mapping Global Censorship and Surveillance Tools. 15 January 2013. Available online: https://citizenlab.ca/research/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/ (accessed on 17 August 2026).
19. Reuters. Rights Group, Journalists Press Indonesian Government to Lift Internet Curb in Restive Papua. 23 August 2019.
20. Amnesty International Indonesia. Court Ruling on Internet Blackout Is a Rare Victory for Freedom of Expression in Papua. 3 June 2020. Available online: https://www.amnesty.id/kabar-terbaru/siaran-pers/court-ruling-on-internet-blackout-is-a-rare-victory-for-freedom-of-expression-in-papua/06/2020/ (accessed on 17 August 2026).
21. Antara News. Disruption at National Data Center Caused by Brain Cipher Ransomware. 24 June 2024. Available online: https://en.antaranews.com/news/316773/disruption-at-national-data-center-caused-by-brain-cipher-ransomware (accessed on 17 August 2026).
22. Reuters. Indonesia, Suffering from a Ransomware Attack, Discovers It Has No Backups. 3 July 2024.

23. Scott, J.C. *Weapons of the Weak: Everyday Forms of Peasant Resistance*; Yale University Press: New Haven, CT, USA, 1985.
24. Bayat, A. *Life as Politics: How Ordinary People Change the Middle East*, 2nd ed.; Stanford University Press: Stanford, CA, USA, 2013.