Research Journal in Advanced Humanities

RJAH

https://doi.org/10.58256/hprs3b27

Open Access

Check for updates

RESEARCH ARTICLE Section: *Digital Humanities*

Digital sovereignty in the Global South: Indonesia's cyber governance between global power and national autonomy

Dharma Pongrekun [1]*, Arfin Sudirman[1], Widya Setiabudi[1] & Arry Bainus[1]

[1]Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Padjadjaran, Bandung

*Correspondence: poldharmapongrekun@gmail.com

ABSTRACT

Indonesia's national cybersecurity policy is confronting a critical challenge amid an increasingly hegemonic global digital architecture and intensifying geopolitical competition. In this context, states are often compelled to adopt international regulatory standards that may undermine national data sovereignty. This article examines how Indonesia can formulate a sovereign cybersecurity policy within an asymmetric global digital governance structure characterized by technological dependency and the dominance of global actors that limit national policy autonomy. Employing a qualitative–interpretive approach with a strategic policy analysis design, the study reveals that global digital governance reproduces structural power asymmetries between advanced economies as technology producers and developing countries as technology consumers and regulatory subjects. These asymmetries facilitate new forms of digital penetration through algorithmic control, infrastructure dependency, and the expanding influence of transnational technology corporations, thereby threatening not only technical security but also data sovereignty and epistemic independence. This article introduces OGDS (One Gate Data System) as an integrated policy framework that synthesizes governance, resilience, ethics, and diplomacy. By reframing digital self-reliance as a political and normative project, OGDS positions Indonesia not merely as a passive adopter of global standards but as a potential architect of a sovereign and ethical digital order grounded in the values of Pancasila.

KEYWORDS: cybersecurity, data sovereignty, diplomacy, One Gate Data System, technological dependency

Research Journal in Advanced Humanities

Volume 7, Issue 1, 2026

ISSN: 2708-5945 (Print)

ISSN: 2708-5953 (Online)

ARTICLE HISTORY

Submitted: 01 **January 2026**

Accepted: 09 **February 2026**

Published: 14 **March 2026**

HOW TO CITE

Pongrekun, D., Sudirman, A., Setiabudi, W., & Bainus, A. (2026). Digital sovereignty in the Global South: Indonesia's cyber governance between global power and national autonomy. *Research Journal in Advanced Humanities*, 7(1). https://doi.org/10.58256/hprs3b27

Published in Nairobi, Kenya by Royallite Global, an imprint of Royallite Publishers Limited

1. Introduction

1.1. Background

The rapid advancement of digital technology has brought profound transformations to global governance, reshaping not only economic and communication systems but also the ways in which states construct power, regulate societies, and safeguard national sovereignty. In this context, cybersecurity has emerged as a strategic issue that can no longer be treated as peripheral, particularly for developing countries such as Indonesia, which possesses one of the largest digital populations in the world while remaining structurally dependent on global technological infrastructure and services.

Digital transformation has fundamentally altered the architecture of global governance by introducing cyberspace as a new strategic domain in which control over data, digital infrastructure, and information architecture is directly intertwined with national security interests and a state's geopolitical positioning. Cybersecurity, therefore, should no longer be understood merely as a technical matter of network protection, but as a multidimensional issue encompassing political, economic, and ethical dimensions that ultimately shape a state's capacity to maintain sovereignty in the digital era.

Contemporary literature indicates that global cybersecurity policy remains largely dominated by technocratic and normative approaches oriented toward system stability, risk management, and the harmonization of international standards. Numerous studies highlight the influential role of global actors (both advanced states and major technology corporations) in shaping digital governance architectures through technical standards, cross-border data flow regimes, and global digital platforms. However, much of this scholarship tends to position developing countries as passive policy adopters rather than as sovereign actors with strategic agency to define their own digital policy trajectories. As a result, critical dimensions such as structural dependency, technological hegemony, and the epistemic implications of global cyber governance are often marginalized in policy analysis. Within the Indonesian context, these challenges become increasingly salient. As one of the world's largest digital societies, Indonesia stands at a strategic crossroads between two competing imperatives. On the one hand, there is mounting pressure to integrate with global cybersecurity regulations and protocols largely formulated by dominant technological powers. On the other hand, there is an urgent need to protect and strengthen national data sovereignty as the foundation of an autonomous cybersecurity framework. This tension is evident in debates surrounding cross-border data storage, the dominance of foreign digital platforms, and the rising intensity of transnational cyber threats that continuously test the state's capacity to adopt firm and sovereign policy positions.

Although various national policies signal the government's efforts to establish a framework for digital and cybersecurity governance, existing policy studies reveal that these regulations remain fragmented, sectoral, and largely reactive. They have yet to coalesce into a coherent long-term strategic vision that places data sovereignty at the core of national security. In this sense, a clear policy gap persists between the aspiration for sovereign cybersecurity and the reality of a fragmented regulatory architecture that remains vulnerable to global normative pressures.

Moreover, contemporary cybersecurity challenges extend beyond technical considerations to encompass geopolitical and epistemic dimensions. Digital infiltration through algorithms, platform architectures, and control over information flows has generated new forms of power that operate in latent and non-territorial ways. Under such conditions, cybersecurity concerns not only system protection but also contestation over who controls knowledge production, technological standards, and value orientations within digital spaces. Despite its strategic importance, this epistemic dimension remains relatively underexplored in Indonesian cybersecurity policy literature.

Addressing this gap, this article situates itself within the framework of critical cybersecurity studies by integrating perspectives from dependency theory and techno-hegemony. It examines Indonesia's cybersecurity policy as part of an asymmetric global digital power structure, moving beyond conventional technical or legal-formal analyses. Specifically, the article interrogates how technological dependency, the dominance of global standards, and digital power relations shape national cybersecurity policy dilemmas.

The primary novelty of this study lies in the formulation of the One Gate Data System (OGDS) as a strategic policy concept. Rather than serving as an analytical tool, OGDS is positioned as an integrated policy solution designed to address the intertwined challenges of data sovereignty and national cybersecurity. Through

this approach, cybersecurity is conceptualized as a national project that integrates public policy, digital civility, and geopolitical strategy, grounded in Indonesia's foundational normative values.

Against an increasingly hegemonic and fragmented global digital landscape, this study offers a space for critical reflection as well as an alternative policy pathway toward sovereign, just, and ethical digital governance. Accordingly, the article contributes not only to the enrichment of academic discourse on cybersecurity and data sovereignty in developing countries, but also provides a policy framework with practical relevance for the formulation of Indonesia's National Cybersecurity Policy.

1.2. Problem Statement

Building on the foregoing background, the central problem addressed in this article concerns how Indonesia can formulate a national cybersecurity policy capable of safeguarding data sovereignty within a hegemonic and asymmetrical global digital governance structure. This challenge extends beyond the state's technical capacity to protect critical infrastructure and vital information systems, encompassing broader issues of technological dependency, pressures arising from global standards, and the ethical as well as epistemic implications of dominance by global digital actors.

More specifically, this article interrogates the extent to which Indonesia's existing national cybersecurity policy framework remains confined within a logic of adaptation to global norms and governance architectures. Such a condition potentially constrains the country's policy space to exercise sovereign control over data, information, and knowledge. Concurrently, the article raises a fundamental question regarding how cybersecurity policy can be designed not merely as a technocratic instrument, but as a political and ethical national project—one that strengthens epistemic resilience, advances digital autonomy, and enhances Indonesia's geopolitical positioning within the global cyber landscape.

2. Literature Review and Theoretical Framework

In examining the dilemmas of Indonesia's national cybersecurity policy amid global pressures and the demand for data sovereignty, a conceptual foundation is required that can adequately explain global power relations, technological dependency, and the position of developing countries within the international digital landscape. This article employs three complementary analytical approaches as its theoretical framework: dependency theory, techno-hegemony, and digital sovereignty, each supported by recent empirical and policy-oriented literature (Fernández Franco, Graña, & Rikap, 2024; Pohle & Thiel, 2020; UNCTAD, 2021).

2.1. Dependency Theory in the Digital Context

Dependency theory emphasizes that structural inequalities between countries are not merely the result of domestic shortcomings, but are produced through asymmetrical international relations (Cardoso & Faletto, classic formulation; with contemporary digital applications elaborated in recent studies). In the digital domain, dependency materializes when domestic actors rely heavily on infrastructure, cloud services, and computational tools controlled by multinational corporations, a condition that positions developing countries in a subordinate role with respect to data control and technological capabilities (Fernández Franco et al., 2024; UNCTAD, 2021). Recent empirical case studies, such as analyses of regional platforms like *Mercado Libre* in the e-commerce sector, demonstrate how even regionally dominant actors remain embedded in algorithms, cloud computing infrastructures, and services provided by Big Tech firms. This dynamic reinforces structurally embedded patterns of digital dependency (Fernández Franco et al., 2024). Consequently, dependency theory provides a critical lens for analyzing how technical and institutional dependencies constrain national policy space and limit the realization of data sovereignty (UNCTAD, 2021).

2.2. Techno-Hegemony and Control over Digital Architecture

The second approach highlights how power in the digital realm is increasingly exercised through the governance of technical standards, protocols, platforms, and algorithms, rather than solely through traditional military or economic means. Literature on platform power and surveillance capitalism elucidates how dominant digital actors (Big Tech) construct normative and technical infrastructures that shape user behavior as well as state regulatory decisions (Zuboff, 2019; Couldry & Mejias, 2019).

Policy-oriented analyses further reveal that norms governing cross-border data flows and interoperability standards are often formulated within arenas dominated by powerful actors. This process produces what can be conceptualized as techno-hegemony, a form of dominance exercised through soft technical infrastructures and normative narratives (DeNardis, 2014; Bradshaw, Millard, & Walden, 2022). The techno-hegemony framework thus helps explain why ostensibly technical national policies are frequently conditioned by broader global power structures, thereby necessitating counter-hegemonic strategies at both the domestic policy level and within digital diplomacy.

In this article, the techno-hegemony framework is applied to examine global power dynamics shaping Indonesia's digital policy environment, including the geopolitical roles played by major powers such as the United States and China in defining the trajectory of global technological development.

2.3. Digital Sovereignty as a Policy Framework

The concept of digital sovereignty emphasizes a state's capacity to regulate and protect its data and digital infrastructure from external intervention (Pohle & Thiel, 2020). International policy reports and academic studies underscore the persistent tension between the economic imperative for cross-border data flows and the need for states to maintain legal control over citizens' data and critical digital infrastructure (UNCTAD, 2021; OECD, 2022).

Digital sovereignty extends beyond narrowly technical measures (such as data localization) to encompass legal structures, governance arrangements, ethical principles governing technology use, and institutional capacities required for long-term digital defense (Pohle & Thiel, 2020; OECD, 2022). In the Indonesian context, empirical studies and national policy assessments indicate that despite notable regulatory progress, structural challenges including infrastructure dependency and institutional fragmentation, continue to impede the operationalization of digital sovereignty (UNCTAD, 2021).

Taken together, these three theoretical approaches (dependency theory, techno-hegemony, and digital sovereignty) offer a comprehensive framework for understanding the complexity of cybersecurity policy dilemmas in developing countries. Specifically, they illuminate: (1) the structural relations that generate technological dependency; (2) the ways in which power is reconstituted through technical infrastructures; and (3) the imperative for states to formulate policy strategies that preserve political, legal, and ethical control over digital spaces.

3. Methodology

This study adopts a qualitative–interpretative approach with a strategic policy analysis design that is analytical and conceptual in nature. The primary objective of this approach is to develop an in-depth understanding of the direction, dilemmas, and policy orientations of Indonesia's national cybersecurity strategy as it confronts global agenda pressures while seeking to preserve national data sovereignty. Rather than measuring variables quantitatively, the study focuses on interpreting policy meaning, power relations, and strategic orientations embedded in cybersecurity governance.

The analysis is conducted through the triangulation of three main dimensions. First, the normative dimension, which examines national regulatory frameworks and cybersecurity-related policies. Second, the theoretical dimension, which draws upon dependency theory and the techno-hegemony framework to interpret structural and power-based dynamics. Third, the digital geopolitical dimension, which situates Indonesia's cybersecurity policy within broader global power relations shaping contemporary cyber governance.

The study relies exclusively on secondary data, including national policy documents, statutory regulations, strategic reports issued by government institutions, as well as peer-reviewed academic publications and reports from international organizations. All data are subjected to critical thematic analysis to identify patterns of structural dependency, global normative pressures, and their implications for Indonesia's national policy space. Based on the findings derived from this analytical process, the article formulates the One Gate Data System (OGDS) as a conceptual policy model designed to address the intertwined challenges of data sovereignty and national cybersecurity. OGDS is not positioned as a methodological instrument, but as a strategic policy construct emerging from critical analysis of existing governance limitations.

Accordingly, this methodological framework conceptualizes cybersecurity not merely as a technical or

administrative concern, but as a political, ethical, and strategic issue that demands policy formulation grounded in national values, digital autonomy, and Indonesia's core national interests amid ongoing global digital transformation.

4. Discussion

4.1. National Cybersecurity Policy Dilemmas amid Global Dependency

Indonesia's national cybersecurity policy occupies a fundamentally dilemmatic position between two competing imperatives: global demands for open connectivity and national imperatives to preserve digital sovereignty. Within a global environment dominated by Western and Eastern technological architectures, Indonesia confronts a classic paradox identified by dependency theory—namely, that modernization efforts may inadvertently deepen structural dependence on external actors (Fernández Franco, Graña, & Rikap, 2024). This paradox has now materialized in the digital realm, where access to critical infrastructure, algorithms, and large-scale computational resources such as cloud computing is controlled by a limited number of multinational corporations, including Amazon, Microsoft, Google, Alibaba, and Huawei. Such dependency is not merely economic in nature, but also epistemic, shaping how knowledge, values, and digital policy norms are formulated.

From a political economy perspective, digital dependency is rooted in global structures that position developing countries at the periphery of technological value chains. Countries such as Indonesia function primarily as consumers of innovations and systems developed in global technological centers, thereby constraining domestic policy space through licensing regimes, patent ownership, and global regulatory frameworks that are often formulated with limited participation from the Global South (UNCTAD, 2021). These asymmetries render national digital transformation only partially autonomous, as initiatives aimed at data sovereignty must be continuously negotiated with the commercial and security interests of external actors.

In the realm of public policy, this dilemma manifests along two parallel trajectories. First, there is strong pressure to adopt international best practices in order to attract investment and accelerate digital transformation. Second, there is growing awareness of the risks associated with foreign control over strategic infrastructure, which may undermine national security. Indonesia's Law No. 27 of 2022 on Personal Data Protection, for instance, affirms the state's authority over citizens' data; yet its implementation remains heavily dependent on foreign technology providers that dominate cloud storage architectures and data analytics platforms. This situation illustrates a clear policy contradiction: legal sovereignty is asserted, while technological dependency persists.

Digital dependency also carries significant social and epistemic dimensions. Zuboff (2019) conceptualizes this condition as *surveillance capitalism*, a form of capitalism based on the extraction of behavioral data for commercial and political purposes. In the Indonesian context, reliance on global social media platforms places public information flows under the control of opaque algorithms operating beyond national jurisdiction. This weakens the state's capacity to safeguard the public information sphere from manipulation and digital disinformation, which have emerged as strategic threats to political sovereignty. As emphasized by Couldry and Mejias (2019), digital dependency is therefore not merely a matter of hardware or software, but fundamentally concerns control over public consciousness and the circulation of knowledge.

Comparative experiences further illuminate this dilemma. India, through its *Digital India* initiative, has pursued strict data localization policies to ensure that citizens' data are stored domestically (OECD, 2022). However, these measures have generated tensions with major U.S.-based technology firms, which perceive such policies as trade barriers. Brazil has faced similar challenges in strengthening the *Marco Civil da Internet*, a regulatory framework affirming digital rights, while remaining dependent on foreign platform providers for implementation. Vietnam, meanwhile, has developed extensive domestic systems of digital control and censorship to secure its cyberspace, a strategy that has drawn criticism for undermining civil liberties. Indonesia occupies an intermediate position among these approaches, seeking to enforce data sovereignty without disengaging from the global digital economy. This comparative landscape underscores the difficulty of balancing security and openness within a system still reliant on external infrastructure.

Furthermore, digital dependency is reinforced through policy transfer processes, whereby developing countries adopt digital policy norms, standards, and instruments promoted by international organizations such as the OECD, the G20, and the World Economic Forum. As argued by Bradshaw, Millard, and Walden

(2022), such transfers often consolidate the normative hegemony of advanced economies, as "global standards" tend to reflect the interests of dominant corporations and technological centers. Consequently, when Indonesia formulates its national cybersecurity strategy by referencing frameworks such as the OECD Digital Security Recommendations or regional cybersecurity cooperation initiatives, it simultaneously contributes to the reproduction of dependency structures. Within the techno-hegemony framework, this constitutes a form of consensual power, power that is voluntarily accepted because it is framed as global rationality (DeNardis, 2014).

Digital dependency also introduces new diplomatic challenges. At the global level, rivalry between the United States and China over control of 5G infrastructure, artificial intelligence, and cloud computing places developing countries in precarious bargaining positions. Indonesia, which seeks to engage both sides, must navigate carefully to avoid becoming trapped in a form of digital bipolarity that could undermine long-term technological autonomy. The emerging discourse on *digital non-alignment* within Indonesia's foreign policy can thus be understood as a pragmatic strategy to preserve political flexibility in technological affairs without aligning exclusively with any single power bloc (Nye, 2021).

At the same time, technological dependency may be interpreted as a transitional phase toward national capacity building. This perspective resonates with the concept of *technological learning* in development theory, which emphasizes that the adoption of foreign technologies can serve as a foundation for domestic innovation when accompanied by deliberate strategies of knowledge transfer and capability development (UNCTAD, 2021). Realizing this potential, however, requires public policies that explicitly link cybersecurity with human capital development, research investment, and national industrial strategies. Absent such integration, cybersecurity policy risks remaining reactive (focused on responding to threats) rather than proactive in building digital sovereignty.

Accordingly, the dilemma of national cybersecurity policy cannot be reduced to technical or institutional issues alone. It reflects a deeper structural contradiction between the logic of global markets and the logic of state sovereignty. High levels of digital dependency erode domestic policy space—the autonomy required to formulate strategies aligned with national priorities. Thus, Indonesia's core challenge lies not only in regulating data, but in redefining its power relations within the global digital order. This necessitates a strategic shift that moves beyond technical security toward a broader political-economic repositioning of Indonesia within the global cyber architecture, an agenda that will be further elaborated in the subsequent discussion on global agenda pressures and data sovereignty.

4.2. Global Agenda Pressures and Cyber Governance Standards

Over the past decade, the architecture of global digital governance has expanded rapidly, driven by growing demands for data interoperability, the strengthening of cross-border cybersecurity, and the harmonization of technical standards to support the integration of the global digital economy. Beneath this trend toward harmonization, however, lies a pronounced imbalance of power between advanced economies (acting as technology producers and standard-setters) and developing countries, which are more frequently positioned as technology consumers and objects of international regulation (UNCTAD, 2021).

Indonesia, like many countries in the Global South, does not occupy a symmetrical position within this configuration. As has been argued in this study, the global digital architecture remains largely dominated by entities such as the Internet Corporation for Assigned Names and Numbers (ICANN), along with major technology corporations based primarily in the United States and China, which exercise significant control over core infrastructure, internet protocols, and dominant digital platforms (Manuel Castells, 2001; Ronald Deibert, 2009). This structural asymmetry generates conditions in which global norms and standards do not necessarily reflect the sovereignty aspirations of developing states, but instead embody the political–economic interests of countries with superior technological power.

4.2.1. Technological Hegemony and Global Policy Transfer

Within the framework of techno-hegemony, as elaborated by DeNardis (2014) and Pohle and Thiel (2020), digital dominance operates not only through control over infrastructure but also through the establishment of ostensibly neutral global standards and narratives. International forums such as the G20, the Organisation

for Economic Co-operation and Development, and the World Economic Forum actively promote global digital governance principles, including cross-border data flows, an open internet, and digital trade facilitation. Although framed in the language of liberalization and collaboration, many of these principles originate from ideological frameworks that prioritize market openness and economic efficiency, while neglecting structural inequalities in technological access, institutional capacity, and the protection of domestic data (Bradshaw, Millard, & Walden, 2022).

This process exemplifies policy transfer, defined as the diffusion and adoption of policies and standards from one political system to another on the assumption that they represent universal best practices, despite their frequent misalignment with national contexts (Dolowitz & Marsh, 2000). In the Indonesian case, normative pressures to adopt regulatory models such as the European Union's General Data Protection Regulation (GDPR) and the OECD's *Data Free Flow with Trust* principle generate a strategic dilemma between global data openness and the protection of national digital sovereignty.

The metaphor of "data as the new oil," popularized by The Economist (2017), has become emblematic of the digital economy paradigm that positions data as the primary resource of contemporary global capitalism. However, as critically argued by Zuboff (2019), this metaphor obscures the reality that not all countries possess the infrastructural, legal, or technical capacities required to "extract" and process data independently. Consequently, developing countries are often reduced to providers of raw data derived from user activity, while economic value creation and knowledge accumulation remain concentrated within global technological centers.

4.2.2. Global Norms and Regulatory Asymmetries

Reports by the United Nations Conference on Trade and Development (2021) underscore that the dominance of large technology corporations has produced a global digital landscape that is far from neutral. Data governance and cybersecurity policies in many developing countries are increasingly shaped to accommodate the interests of transnational corporations through mechanisms such as bilateral digital trade agreements, pressures exerted within multilateral forums, and cross-border technical regulations.

Indonesia has experienced such pressures directly in various international negotiations, including the Indo-Pacific Economic Framework and the ASEAN *Digital Economy Framework Agreement* (Digital Economy Framework Agreement), both of which emphasize the principle of *data free flow with trust*. The accompanying discourse of "trust" is frequently deployed to justify the relaxation of data jurisdiction boundaries and to constrain national data localization policies. Bradshaw et al. (2022) caution that, in the absence of robust domestic safeguards, such provisions may facilitate the extraction of strategic data by foreign entities and weaken state authority over the regulation of citizens' information.

When global standards are defined by a limited number of states and corporations, developing countries encounter a new form of digital colonialism, characterized by algorithmic control and protocol dominance that compels compliance without meaningful bargaining power (Couldry & Mejias, 2019). From the perspective of dependency theory, this phenomenon represents the reproduction of long-standing dependency structures in a new guise: a transition from commodity-based dependency to digital dependency (Fernández Franco, Graña, & Rikap, 2024).

4.2.3. National Capacity Constraints and Implementation Challenges

Pressures to comply with global standards are not always matched by adequate domestic institutional readiness. Reports by the Badan Siber dan Sandi Negara (BSSN, 2023) document a significant gap between the complexity of global regulatory frameworks and the capacity of national institutions to translate them into operational policies. Limitations in human resources, cybersecurity infrastructure, and inter-agency coordination weaken Indonesia's position in responding to rapidly evolving global norms.

At the same time, Indonesia's engagement in international digital forums tends to be reactive rather than proactive. The country is more often positioned as a policy taker, adopting standards formulated elsewhere, rather than as a policy shaper capable of producing norms aligned with domestic contexts. This condition reflects an epistemic gap in global digital policy-making processes, in which the voices of developing countries frequently lack the same level of legitimacy as those of actors from global technological centers (DeNardis, 2020).

Such imbalances are also evident in cybersecurity certification systems, encryption standards, and digital intelligence cooperation mechanisms, which remain largely controlled by technologically advanced states. As a result, countries like Indonesia are frequently relegated to the role of standard implementers with limited negotiating space. Within the techno-hegemony framework, this form of dominance produces normative dependency, whereby developing states are compelled not only to adopt external technologies, but also to internalize the policy rationalities and cognitive frameworks of advanced economies (Pohle & Thiel, 2020).

4.2.4. Technological Geopolitics and the Challenge of the "Splinternet"

Another dimension of global pressure arises from the increasing fragmentation of international cyber governance driven by geopolitical rivalry between the United States and China. This competition has generated two major poles in global digital infrastructure and regulatory models, a phenomenon commonly described as the splinternet (Mahoney, 2022). The United States promotes a governance model emphasizing information freedom and private sector ownership, whereas China prioritizes state control and national security through regulatory instruments such as its Cybersecurity Law and Data Security Law.

Indonesia, as a middle power in the Indo-Pacific region, occupies a particularly difficult position. On the one hand, it must maintain economic and technological cooperation with both blocs; on the other, continued dependence on foreign infrastructure and technologies risks eroding long-term strategic autonomy. Controversies surrounding the deployment of 5G infrastructure (particularly those involving Huawei) illustrate this dilemma in concrete terms. As noted by Nye (2021), competition for *soft power* in the digital domain has transformed technology into a central arena of geopolitical influence.

In this context, Indonesia's national cybersecurity policy cannot be understood solely as a response to technical threats. It must also be interpreted as an integral component of foreign policy strategy. Indonesian digital diplomacy is therefore required to perform a dual function: sustaining engagement in global cyber governance while preserving the principle of data sovereignty, and simultaneously advancing a digital non-alignment agenda to avoid entrapment in geopolitical polarization. Such an approach represents a form of counter-hegemonic digital policy, positioning Indonesia as an independent actor amid competing centers of global technological power.

4.2.5. Toward Sovereign Digital Diplomacy

Under these conditions, Indonesia requires a firm digital diplomacy strategy grounded in the principles of global information justice. Digital diplomacy should not be viewed merely as a technical instrument, but as a mechanism for contesting hegemonic and extractive global structures (Deibert, 2020). As a middle power in the Indo-Pacific, Indonesia possesses strategic capital to advocate for digital governance norms that are more equitable, participatory, and reflective of the interests of developing countries.

Concrete initiatives, such as promoting an ASEAN Digital Governance Charter, strengthening regional data governance frameworks, and establishing a national cyber diplomacy academy, could serve as strategic pathways toward a more active role in global forums. By enhancing technical, institutional, and epistemic capacities in digital diplomacy, Indonesia can transition from a policy follower to a norm entrepreneur, contributing to the creation of new norms that balance openness with sovereignty.

Accordingly, pressures on national cybersecurity policy do not stem solely from cyber threats or digital disinformation, but also from a global architecture that dictates how digital standards and norms are produced. Without strengthening bargaining power and institutional capacity, Indonesia risks becoming a passive follower within an increasingly consolidated and asymmetrical global digital power structure. National cybersecurity policy must therefore be positioned as an integral element of foreign policy and a broader digital autonomy strategy—one oriented toward sovereignty, justice, and long-term security.

4.3. Digital Infiltration and Threats to Cyber Sovereignty

Digital infiltration constitutes one of the most latent dimensions of contemporary cybersecurity landscapes. Unlike conventional cyber threats (such as malware attacks, hacking incidents, or denial-of-service operations) digital infiltration operates through subtler and more systemic mechanisms, namely algorithms, platform architectures, and data control structures that shape how information is produced, distributed, and received by

society. In this context, threats to cyber sovereignty do not manifest solely as technical vulnerabilities, but also as epistemic infiltration, the domination of knowledge, public consciousness, and perception that ultimately influences policy direction and collective social behavior (Zuboff, 2019; Couldry & Mejias, 2019).

4.3.1. Algorithmic Colonialism and Informational Inequality

The digital era has ushered in a new form of colonialism that no longer relies on physical domination, but rather on control over data flows and algorithmic systems. Couldry and Mejias (2019) conceptualize this phenomenon as data colonialism, a process through which human data are extracted and transformed into economic and political resources. Within this model, users are no longer merely consumers; they become unwitting "data laborers," continuously contributing behavioral patterns, preferences, and social interactions that fuel global platform capitalism.

In the Indonesian context, algorithmic colonialism is evident in the ways global digital platforms shape public information consumption. Recommendation algorithms governed by commercial logics not only determine content visibility but also generate structural biases in the formation of public opinion. When local content and data must operate within ecosystems defined by global algorithmic architectures, the state's capacity to regulate data flows and public narratives becomes increasingly constrained. This condition signals an erosion of national data sovereignty, wherein control over digital space is exercised not through territorial domination, but through asymmetric platform governance mechanisms embedded in the global digital economy (Sutrisno & Nugroho, 2020).

This dynamic illustrates how techno-hegemony operates at cultural and ideological levels. As argued by Antonio Gramsci (1971), hegemony is not merely coercive domination, but the capacity to shape social consensus through control over meaning. In the digital context, global technology corporations have successfully constructed new consensuses around values such as "connectivity," "efficiency," and "innovation," which obscure underlying logics of data accumulation and control (Pohle & Thiel, 2020). Consequently, global societies—including Indonesia—become participants in hegemonic systems that voluntarily reproduce digital dependency.

4.3.2. Information Manipulation and Threats to Political Sovereignty

Digital infiltration also operates within the political sphere, particularly through disinformation and algorithmic manipulation that undermine democratic processes. Deibert's study in *Reset* (2020) demonstrates that global digital spaces have evolved into new arenas of information warfare, where the boundaries between public opinion and propaganda are increasingly blurred. Control over social media platforms enables transnational actors to influence domestic political discourse through digital campaigns, bot networks, and data-driven micro-targeting.

Indonesia has experienced several major incidents that underscore the severity of these threats. Large-scale data breaches involving e-commerce platforms and public institutions reveal persistent weaknesses in national data protection systems. More critically, the emergence of cyber troops and coordinated disinformation campaigns during electoral periods illustrates how algorithms can be weaponized to polarize public opinion. From the perspective of surveillance capitalism (Zuboff, 2019), control over behavioral data enables the prediction and steering of political decision-making. When such instruments are controlled by foreign corporations or states, the risks extend beyond individual privacy to encompass the very sovereignty of democratic governance. Similar dynamics have been observed globally. The Cambridge Analytica scandal serves as a paradigmatic example of how personal data can be exploited for cross-border political manipulation. In many Global South contexts, dependence on foreign platforms deprives states of access to algorithmic systems and control over information distribution. DeNardis (2020) describes this condition as information asymmetry, a structural imbalance in data ownership and governance that undermines political legitimacy and erodes public trust in state institutions.

4.3.3. Epistemic Security and Threats to National Identity

Digital infiltration is not solely a cybersecurity issue; it also penetrates epistemic and cultural dimensions. When a nation's information systems and digital media ecosystems are controlled by foreign infrastructure, the direction of knowledge production and collective imagination is inevitably affected. Ronald Deibert (2009)

emphasizes that power in the digital age is fundamentally power over information flows. States that lack control over these flows risk losing their capacity to define truth within their own public spheres.

In the Indonesian context, the risk of losing epistemic sovereignty is becoming increasingly tangible, particularly as public digital literacy remains uneven and information consumption is dominated by foreign platforms. This pattern threatens not only information security, but also fosters cultural dependency, whereby narratives, lifestyles, and worldviews are progressively shaped by global media ecosystems. As algorithms become the primary curators of social experience, national public spaces risk fragmentation and the erosion of local moral authority.

These dynamics underscore the importance of linking cybersecurity policy with cultural and educational strategies. Digital literacy should not be understood merely as the technical ability to use devices, but as critical awareness of how algorithms operate, how data economies function, and how technological hegemony is reproduced. Only through such epistemic awareness can citizens act as active subjects in digital spaces, rather than passive objects of global information flows (Luciano Floridi, 2013).

4.3.4. Infiltration through Strategic Infrastructure and Technologies

Another form of digital infiltration emerges through dependence on strategic technological infrastructure, including telecommunications networks, cloud computing systems, data management software, and national cyber defense architectures. When core technology providers are foreign-based, each infrastructural layer becomes a potential entry point for external control. The United Nations Conference on Trade and Development (UNCTAD, 2021) reports that more than 80 percent of global data are managed by a small number of corporations headquartered in the United States and China. This dominance is not merely economic, but deeply geopolitical.

Cases of large-scale data breaches in Indonesia's public sector reveal that many government systems continue to rely heavily on foreign technologies, encompassing hardware, software, and cloud-based services. Such reliance amplifies supply chain vulnerabilities, whereby security flaws within external vendors can be exploited for intelligence gathering or digital sabotage (Organisation for Economic Co-operation and Development, 2022). From a national security perspective, this constitutes one of the most strategic forms of infiltration, precisely because it is structural, systemic, and difficult to detect.

As noted by Mahoney (2022), technological rivalry between the United States and China has generated new geopolitical pressures for developing countries. Technological choices are no longer purely economic decisions; they are inherently political. Under such conditions, Indonesia must carefully navigate between the imperatives of global integration and the urgency of digital self-reliance.

4.3.5. Toward Epistemic Resilience and Digital Self-Reliance

In confronting digital infiltration that operates through algorithms, platform architectures, and control over data flows, Indonesia's cybersecurity policy must shift from a reactive paradigm toward one centered on epistemic resilience and autonomy. This shift affirms that cybersecurity cannot be reduced to technical protection of networks and systems alone, but must encompass the capacity of the state and society to control knowledge, meaning, and value orientations within digital spaces. Epistemic autonomy requires strengthening national capacities to understand, interpret, and govern data as a strategic resource that shapes policy direction, collective identity, and state sovereignty.

Within this framework, the One Gate Data System (OGDS) is positioned as a strategic policy concept emerging from a systemic reading of digital dependency and global power relations. OGDS functions as an integrated governance architecture that brings together technical control, institutional coordination, regulatory authority, and ethical orientation within a single national framework. Through OGDS, data governance is firmly placed under national jurisdiction and capacity, ensuring that knowledge production, decision-making processes, and the protection of public interests do not depend on infrastructure, algorithms, or interpretive frameworks controlled by external actors.

Experiences from countries such as Estonia and South Korea demonstrate that digital sovereignty can be achieved through long-term investment in research, robust legal architectures, and the empowerment of citizens as active participants in digital spaces. However, rather than imitating these models wholesale, Indonesia must

develop an approach rooted in its own values and socio-political context. Principles such as digital "gotong royong", collective ethics, and data solidarity constitute essential foundations for building sustainable epistemic resilience. Digital infiltration can only be effectively countered when society collectively recognizes that data are not merely economic commodities, but integral components of national sovereignty and the future of Indonesia's digital democracy.

4.4. Strategies for Digital Autonomy and the Ethics of Cyber Policy

In confronting the complexity of threats and pressures embedded within global cybersecurity governance, Indonesia must develop policy strategies that extend beyond reactive and technocratic responses toward approaches that are reflective, sovereign, and grounded in humanistic values and digital civility. Such strategies position digital sovereignty at the core of national development in the era of digital transformation. Within this context, digital autonomy should not be understood merely as technical capability or the availability of domestic technologies, but rather as the state's capacity to regulate, secure, and interpret digital space in accordance with principles of sovereignty, justice, and public ethics (Zuboff, 2019; Luciano Floridi, 2013).

This article proposes the One Gate Data System (OGDS) as a conceptual model for national cybersecurity policy oriented around four interrelated dimensions: governance, resilience, ethics, and diplomacy. Through OGDS, Indonesia's digital policy direction is envisioned not only as a mechanism for withstanding global pressures, but also as a means of actively shaping a just and ethical digital order. The model underscores that digital sovereignty emerges from the synergy between institutional strength, technological capability, and the nation's value orientation.

4.4.1. Infrastructure Autonomy and Structural Resilience

The first pillar of a digital autonomy strategy is the development of national digital infrastructure independence. This entails not merely the physical availability of data centers or locally sourced technologies, but comprehensive control over the national digital value chain—from data governance to cybersecurity protection. Infrastructure autonomy requires that all strategic digital activities remain fully subject to national legal jurisdiction and domestic protection mechanisms.

Government policy initiatives, particularly Presidential Regulation No. 95 of 2018 on the Electronic-Based Government System (SPBE) and its integration into the 2020–2024 National Medium-Term Development Plan (RPJMN), represent important initial steps toward the establishment of a National Data Center (NDC). However, as noted by Gultom (2017), the construction of an NDC will only be substantively meaningful if accompanied by firm policy safeguards restricting the use of foreign cloud services by state institutions. Absent such safeguards, the NDC risks becoming a fragile symbol of digital sovereignty—formally national in designation, yet structurally dependent on global infrastructure providers.

Within the OGDS framework, digital infrastructure development must be strategy-oriented rather than project-oriented. This implies that the NDC and SPBE systems should be embedded within a National Digital Resilience Policy that integrates defense, economic, and technology diplomacy considerations. Such an approach aligns with the conception of digital sovereignty advanced by Pohle and Thiel (2020), who argue that technological control should be understood as a form of political and epistemic autonomy, not merely technical competence.

Moreover, Ronald Deibert (2020) emphasizes the importance of cross-sectoral coordination in maintaining the integrity of information governance. In Indonesia, institutional fragmentation, where entities such as the Badan Siber dan Sandi Negara (BSSN), the Ministry of Communication and Information Technology, and the defense sector operate within largely sectoral mandates, has diminished the overall effectiveness of cybersecurity policy. Consequently, infrastructure autonomy cannot be achieved without establishing a National Cybersecurity Governance Framework: an integrated, cross-agency and cross-sectoral governance structure grounded in whole-of-government and whole-of-society principles, as recommended by the International Telecommunication Union (2020) and the Organisation for Economic Co-operation and Development (2022).

4.4.2. An Integrated and Sustainable Cyber Policy Architecture

The second strategic pillar involves constructing an integrated and sustainable national cyber policy architecture.

To date, Indonesia's cybersecurity policies continue to operate within overlapping sectoral domains, with no single institution serving as the primary coordinating nexus between national security, digital transformation, and public data governance.

As Deibert (2009) cautions, power in the digital age no longer manifests through physical monopolies, but through control over information flows and normative frameworks. Accordingly, cross-agency coordination must ensure unity of strategic direction, recognizing that cybersecurity is not merely a protective function, but an instrument for shaping a digital ecosystem that is resilient, transparent, and sovereign.

In this regard, Indonesia must designate a national cyber authority that extends beyond operational responsibilities (such as those currently held by BSSN) to include cross-policy strategic formulation. This authority should be capable of linking digital security with economic development, social policy, and geopolitical considerations. As illustrated by United Nations Conference on Trade and Development (2021), countries that successfully balance cybersecurity with digital development are those that combine multi-stakeholder governance with a firm commitment to national sovereignty.

Such an integrated policy architecture would significantly strengthen Indonesia's position in responding to external pressures. A coherent and unified policy framework enables the state to engage in international negotiations based on clearly articulated national interests, rather than merely adapting to global standards shaped by dominant powers (Bradshaw et al., 2022).

4.4.3. Cyber Policy Ethics and Technological Civility

The third strategic pillar is to ensure that all cybersecurity policies are grounded in digital ethics and technological civility. Cyber policy ethics must not remain merely normative or declarative; rather, they should function as a substantive foundation for maintaining a balance between state security and the civil rights of digital citizens. Manuel Castells (2001) argues that digital space should serve as an arena for democracy and participation, rather than as an instrument of control that restricts information freedom. In the Indonesian context, this requires rejecting two extremes: on the one hand, a surveillance state that disregards privacy rights; on the other, digital anarchy characterized by the absence of regulation and accountability.

Through the framework of the *ethics of information*, Luciano Floridi (2013) emphasizes that information ethics constitutes a moral responsibility toward human beings as "informational subjects." This principle becomes increasingly vital amid the growing power of algorithmic governance and the exploitative dynamics of the global data economy (Zuboff, 2019). Accordingly, national cybersecurity policy must institutionalize algorithmic transparency, ensure the accountability of digital oversight bodies, and safeguard rights to privacy as well as meaningful public participation in technology policymaking.

In this sense, cyber policy ethics do not merely enhance security; they uphold human dignity and information justice. Ethics thus function as the moral compass of the national digital architecture—guiding policy choices to remain aligned with human values rather than subordinated to market logic or geopolitical interests.

4.4.4. Strengthening Human Capital and Public Digital Literacy

Digital autonomy can only be achieved when supported by knowledgeable and ethically grounded human actors. The Organisation for Economic Co-operation and Development (2022) notes that a country's cyber resilience is determined not solely by technological sophistication, but by the capacity of its human and institutional resources.

Consequently, strengthening national cybersecurity human capital must become a top priority. Educational programs, professional certification, and specialized training in cybersecurity should be expanded with a deliberate emphasis on three dimensions of competence: technical expertise, ethical reasoning, and geopolitical awareness. This approach is essential to ensure that Indonesia's cybersecurity workforce evolves beyond operational roles to become architects and custodians of digital sovereignty.

In parallel, public digital literacy must be positioned as a component of national non-military defense. In the context of algorithmic infiltration and information manipulation (Deibert, 2020; Couldry & Mejias, 2019), citizens must be equipped with critical capacities to assess information sources, recognize algorithmic bias, and understand data politics. Ethically grounded digital literacy plays a crucial role in strengthening

societal resilience against forms of digital colonialism that operate at cultural and epistemic levels—particularly by enhancing public awareness of power relations embedded in asymmetrical data governance and the global digital economy (Sutrisno & Nugroho, 2020).

4.4.5. Digital Diplomacy and Global South Coalitions

The final strategic pillar involves strengthening digital diplomacy as an instrument of foreign policy aimed at advancing principles of digital non-alignment, data justice, and algorithmic accountability.

Ronald Deibert (2009) emphasizes that digital diplomacy is not merely diplomacy about technology, but diplomacy about values, specifically, who controls data, who has the right to access it, and for what purposes data are used. Indonesia's position as a middle power in the Indo-Pacific should therefore be leveraged to build coalitions among Global South countries advocating for fair and sovereign digital governance (United Nations Conference on Trade and Development, 2021).

Within forums such as the G20, ASEAN, and the Indo-Pacific Economic Framework, Indonesia can actively promote the principle of digital non-alignment, an independent stance in shaping digital policy without subordination to any technological bloc. In this context, digital diplomacy functions not only to safeguard national interests, but also to expand global solidarity around data sovereignty and algorithmic justice.

Through this approach, digital diplomacy becomes an extension of national cyber sovereignty on the global stage. It integrates security, justice, and human values into a unified national defense strategy suited to the challenges of the digital era.

5. Conclusion

Global dynamics in cyber governance have drawn states into new forms of dependency on infrastructure, standards, and technological architectures controlled by major world powers. Within this context, Indonesia faces a strategic dilemma between the need to participate in the global digital ecosystem and the obligation to safeguard its own data sovereignty. This study demonstrates that national cybersecurity policy cannot be understood merely as a technical matter, but rather as a reflection of asymmetrical global power structures embedded within contemporary digital governance.

Through the analytical lenses of dependency theory and techno-hegemony, the findings reveal that Indonesia's digital dependency constitutes part of a broader political–economic architecture that positions developing countries primarily as consumers within global technological systems. This condition necessitates a paradigmatic shift: from digital adaptation toward digital sovereignty. In practical terms, cybersecurity policy must move beyond passive compliance with international standards and pressures, toward the construction of an autonomous framework rooted in national values, strategic interests, and ethical commitments to humanity. Within this framework, the One Gate Data System (OGDS) is advanced as a policy concept designed to strengthen national digital sovereignty. OGDS conceptualizes digital sovereignty as the outcome of synergy among four core pillars: governance, resilience, ethics, and diplomacy. The governance pillar emphasizes coordinated, cross-institutional data and cybersecurity management; resilience highlights the necessity of robust infrastructure and human capital; ethics ensures that digital policy is grounded in justice and human dignity; and diplomacy extends the struggle for data sovereignty into the global arena through equitable and cooperative engagement.

The OGDS approach also marks a fundamental reorientation in how cybersecurity is conceptualized: from a narrow defense paradigm toward one centered on epistemic and moral resilience. Cybersecurity is thus understood not only as the protection of digital infrastructure, but also as the safeguarding of informational integrity, freedom of thought, and national knowledge autonomy. Within this perspective, digital space must be treated as an infosphere governed ethically, where human beings are recognized as primary subjects rather than mere data sources to be extracted and exploited.

The policy implications of these findings suggest that efforts to strengthen Indonesia's digital sovereignty will only be effective if anchored in a clear political vision that recognizes data and technology as integral components of national sovereignty. Accordingly, national digital strategies must be situated within a broader framework encompassing national defense, equitable economic development, and the cultivation of public civility in digital spaces.

At the global level, Indonesia is called upon to assume a more active role in building coalitions among

Global South countries to advocate for inclusive and non-hegemonic cyber governance. The principle of digital non-alignment offers a strategic middle path for developing states to resist regulatory and technological domination by major powers, while remaining constructively engaged in global digital development. Indonesia's position as a middle power in the Indo-Pacific region provides strategic capital to lead value-based diplomacy on issues of data sovereignty, algorithmic justice, and regional cybersecurity.

Ultimately, Indonesia's digital sovereignty should not be interpreted as a form of isolationism, but as a long-term national project aimed at preserving independence in the digital age. Amid an increasingly hegemonic and dynamic global architecture, Indonesia is challenged to become the architect of its own future, developing technologies that serve humanity, governing digital spaces that are just and sovereign, and ensuring that every innovation is guided by ethical awareness and moral responsibility toward both the nation and a more equitable global order.

References

Badan Siber dan Sandi Negara (BSSN). (2023). *Laporan Tahunan Keamanan Siber Nasional 2022–2023*. Jakarta: BSSN.

Bradshaw, S., Millard, C., & Walden, I. (2022). *Cross-Border Data Flows: The Regulation of Data Exports from the EU and Beyond*. Oxford Internet Institute. https://www.oii.ox.ac.uk/publications/.

Castells, M. (2001). *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford University Press.

Couldry, N., & Mejias, U. A. (2019). *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford University Press.

Deibert, R. (2009). *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. MIT Press.

DeNardis, L. (2014). *The Global War for Internet Governance*. Yale University Press.

DeNardis, L. (2020). *The Internet in Everything: Freedom and Security in a World with No Off Switch*. Yale University Press.

Dolowitz, D. P., & Marsh, D. (2000). Learning from Abroad: The Role of Policy Transfer in Contemporary Policy-Making. *Governance, 13*(1), 5–23. https://doi.org/10.1111/0952-1895.00121

Fernández Franco, S., Graña, J. M., & Rikap, C. (2024). Dependency in the digital age? The experience of Mercado Libre in Latin America. *Development and Change, 55*(3), 429–464. https://doi.org/10.1111/dech.12839

Floridi, L. (2013). *The Ethics of Information*. Oxford University Press.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2021). *Evaluasi SPBE dan Rencana Pusat Data Nasional*. Jakarta: Kominfo.

Mahoney, J. G. (2022). China's Rise as an Advanced Technological Society and the Rise of Digital Orientalism. *Journal of Chinese Political Science, 27*(4), 687–705. https://doi.org/10.1007/s11366-022-09811-6

Microsoft. (2022). *Digital Defense Report 2022*. https://www.microsoft.com/en- us/security/business/microsoft-digital-defense-report

Morozov, E. (2011). *The Net Delusion: The Dark Side of Internet Freedom*. PublicAffairs.

Nye, J. S. (2021). *Soft Power and Great Power Competition in the Digital Age*. Foreign Affairs. https://www.foreignaffairs.com/articles/2021-02-12/soft-power-and-great-power- competition-digital-age

OECD.(2022). *Cybersecurity and the Human Factor.* OECD Publishing. https://www.oecd.org/digital/ (laporan).

Peraturan Presiden Republik Indonesia Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital.

Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE).

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

Sutrisno, A., & Nugroho, Y. (2020). Kedaulatan data dalam tata kelola ekonomi digital di Indonesia. *Jurnal Ilmu Sosial dan Ilmu Politik*, **24**(1), 1–15. https://doi.org/10.22146/jsp.50760

The Economist. (2017, May 6). *The world's most valuable resource is no longer oil, but data*. Retrieved from https://www.economist.com

UNCTAD. (2021). *Digital Economy Report 2021: Cross-Border Data Flows and Development*. United Nations Conference on Trade and Development. https://unctad.org/system/files/official-document/der2021_en.pdf

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.