Journal of Contemporary Local Politics, 4 (2) December 2025, 231-246
ISSN: 2830-6120 (Online)
Available Online at https://journal.ppishk.org/index.php/jclp

Political Dynamics of Cybersecurity Policy in Indonesia: A Governmentality Analysis under Joko Widodo's Administration (2014-2024)

Anggi Anggraeni Kusumoningtyas[1], Syarkawi[2]
[1]Department of Government Studies, Universitas Pamulang, Indonesia
[2]Department of Public Administration, Universitas Pamulang, Indonesia
Corresponding author: anggi.anggraeni@unpam.ac.id

Received: 06 November 2025; Revised: 16 November 2025; Accepted: 31 December 2025

ABSTRACT - This article examines Indonesia's cybersecurity policy during the Joko Widodo administration (2014–2024) through the lens of Michel Foucault's concept of governmentality. As cyberspace has increasingly been constructed as a strategic domain of governance, the Indonesian state has framed cyber threats as risks to national security, digital sovereignty, and political stability. This framing has justified the expansion of regulatory authority, institutional consolidation, and digital surveillance practices. Using a qualitative document analysis approach, this study analyzes cybersecurity-related laws, presidential regulations, national cybersecurity strategies, and official reports issued by state institutions, particularly the National Cyber and Crypto Agency. The findings demonstrate that cybersecurity policy in Indonesia functions not merely as a technical mechanism to protect digital infrastructure, but also as a political technology of governance. Through the production of threat discourses, the deployment of governing technologies, and the shaping of digital subjectivities, cybersecurity policy operates as a form of population management that encourages self-regulation and compliance among citizens. Drawing on governmentality theory, this article argues that cybersecurity governance reflects broader state strategies to regulate conduct in the digital sphere rather than simply respond to technical risks. The study contributes to debates on digital governance and local politics by highlighting how cybersecurity policy in a democratic developing country simultaneously enhances state capacity while generating tensions with democratic accountability, civil liberties, and digital rights.

Keywords: *Cybersecurity, Governmentality, Digital Governance, State Power, Political Dynamics*

Copyright © 2025 by the Authors. Published by the Pusat Penelitian Ilmu Sosial dan Humaniora Kontemporer, Indonesia. This is an open access article distributed under the terms of the CC BY-SA Licence (https://creativecommons.org/licenses/by-sa/4.0).

How to Cite: Kusumoningtyas, A. A., & Syarkawi, S. (2025). Political Dynamics of Cybersecurity Policy in Indonesia: A Governmentality Analysis under Joko Widodo's Administration (2014-2024). *Journal of Contemporary Local Politics, 4*(2), 231-246. https://doi.org/10.46507/jclp.v4i2.800

Permalink/DOI: https://doi.org/10.46507/jclp.v4i2.800

Introduction

The rapid expansion of information and communication technologies over the past two decades has fundamentally transformed the nature of governance, political authority, and security practices (Bilan et al., 2023; Hilbert, 2014; Liu & Yuan, 2015). Cyberspace has evolved from a technical infrastructure facilitating communication into a strategic political domain in which states exercise power, regulate behavior, and manage populations. As digital technologies increasingly mediate social, economic, and political interactions, cybersecurity has become a central concern within national and local governance agendas. Governments across the world now perceive cyberspace as both an opportunity for development and a source of vulnerability that requires continuous intervention (Cavelty, 2007; Shi & Feng, 2024)

Within this governance framework, cybersecurity is no longer treated solely as a technical issue related to network protection or data integrity. Instead, it has become deeply embedded in political discourses of national security, sovereignty, and public order. International organizations such as the International Telecommunication Union (ITU) define cybersecurity as a set of practices and policies designed to protect digital systems, networks, and data from disruption and misuse. However, such definitions often obscure the political dimensions of cybersecurity, particularly the ways in which security narratives are mobilized to legitimize expanded state authority and surveillance over digital life (Cavelty & Wenger, 2020; Foucault, 2009)

Indonesia represents a particularly significant case within this global transformation. As one of the largest digital societies in Southeast Asia, Indonesia has experienced rapid growth in internet penetration, digital platforms, and online political participation. At the same time, the country has faced a sharp increase in cyber threats, including data breaches, ransomware attacks, cyber fraud, and online disinformation campaigns. Official reports from the National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara,* BSSN) indicate hundreds of millions of cyber anomalies annually, affecting both public institutions and private actors. These developments have positioned cybersecurity as a priority issue within Indonesia's national and local political agenda.

During the administration of President Joko Widodo (2014–2024), cybersecurity governance in Indonesia underwent significant institutional and regulatory expansion. The establishment of the National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara*, BSSN) in 2017 marked a turning point toward centralized cybersecurity coordination under executive authority. This period also witnessed the formulation of national cybersecurity strategies, the strengthening of digital monitoring capacities, and the increasing use of regulatory instruments to govern online platforms and digital behavior. While these measures have often been justified as necessary for protecting national security and maintaining digital sovereignty, scholars have noted that expanding digital governance mechanisms in Indonesia has also generated debates regarding their implications for democratic governance, freedom of expression, and the regulation of online political communication

The direction of cybersecurity policy during the Joko Widodo administration cannot be separated from broader national and local political dynamics. At the national level, the government faced increasing political pressure to maintain stability in the digital sphere, particularly in the context of rising online political mobilization, electoral competition, and the proliferation of digital disinformation. Events such as the 2019 presidential election and the

growing influence of social media in shaping political narratives heightened state concerns regarding information security and political order. At the same time, local governments became increasingly dependent on national digital infrastructures and regulatory frameworks to manage digital governance, ranging from public service platforms to regional information systems. This dynamic reinforced the central government's role in setting cybersecurity priorities while local actors operated within nationally defined digital security regimes. Consequently, cybersecurity governance evolved not only as a response to technological threats but also as a political strategy aimed at managing digital political participation, maintaining administrative control, and stabilizing governance across different levels of the state.

Existing studies on cybersecurity in Indonesia have predominantly emphasized technical capacity building, regulatory frameworks, and institutional arrangements, particularly through analyses of national cybersecurity strategies, legal instruments, and state coordination mechanisms (Canton, 2021). These works provide valuable insights into policy design and implementation, especially in relation to infrastructure protection and regulatory compliance. However, they generally approach cybersecurity as a technical or administrative response to external threats, rather than as a political practice embedded in broader relations of power. Consequently, the ways in which cybersecurity governance reshapes state–society relations, legitimizes surveillance, and produces new forms of political control remain relatively underexplored. Limited attention has been paid to how cybersecurity policies function as governing technologies that mediate political participation and democratic accountability at both national and local levels, particularly in developing democratic contexts (Cavelty & Wenger, 2020)

To address this gap, this article adopts a critical political perspective by employing Michel Foucault's concept of governmentality. Governmentality refers to the rationalities, techniques, and practices through which states seek to govern populations by shaping conduct rather than relying exclusively on coercive force. (Foucault, 2009) From this perspective, modern governance operates through the production of knowledge, norms, and administrative technologies that encourage individuals to regulate themselves in accordance with state objectives. Scholars such as Dean, (2010) and Rose & Miller (2017) emphasize that governmentality is particularly relevant for analyzing contemporary forms of governance that rely on surveillance, data, and normalization.

Applying governmentality to cybersecurity allows for a deeper understanding of how security policies function as political technologies. Rather than viewing cybersecurity solely as protection against digital threats, a governmentality approach highlights how threat discourses construct cyberspace as a domain of risk, thereby legitimizing exceptional forms of intervention. It also draws attention to the technologies of government, such as regulatory frameworks, surveillance systems, and digital classification mechanisms, that translate security rationalities into everyday governance practices. Furthermore, it reveals processes of subjectification through which citizens are shaped as "responsible" digital subjects who internalize security norms and participate in self-regulation (Dean, 2010)

While governmentality has been widely applied in studies of public administration, social policy, and surveillance, its application to cybersecurity governance in developing democratic contexts remains limited. Most existing governmentality-based studies focus on Western liberal democracies or authoritarian regimes, leaving a gap in understanding how cybersecurity governance operates in hybrid or developing democratic settings. Indonesia's political context, characterized by democratic institutions alongside strong executive power, offers a valuable case

for examining how cybersecurity policies mediate tensions between security imperatives and democratic accountability.

The scientific novelty of this article lies in its application of governmentality to Indonesia's cybersecurity policy during the Joko Widodo administration, with a specific focus on its implications for governance and local political dynamics. By analyzing cybersecurity policy as a form of governmentality, this study moves beyond technical and legal analyses to reveal how state power is exercised through digital security narratives, institutional arrangements, and citizen subject formation. This approach contributes to the literature on contemporary local politics by situating cybersecurity governance within broader debates on state power, democracy, and digital control.

Accordingly, this article addresses the following research problem: how does the Indonesian state exercise governmentality through cybersecurity policy during the Joko Widodo administration (2014–2024)? More specifically, how are cyber threats framed to justify state intervention, what governing technologies are deployed to manage digital risks, and how are citizens constituted as digital subjects within cybersecurity governance? In addressing these questions, the analysis also examines the power relations and political contestations that shape the formulation of cybersecurity policies in Indonesia, including the interactions between executive institutions, security agencies, regulatory authorities, digital platform companies, and civil society actors. Cybersecurity governance does not emerge in a politically neutral environment; rather, it is shaped by competing interests over authority, information control, and the management of digital political participation. By answering these questions, the article aims to contribute to a more critical understanding of cybersecurity as a political project with significant consequences for democratic governance and civil liberties in Indonesia.

Method

This study employs a qualitative research design with document analysis as its primary methodological approach. Qualitative document analysis is particularly suitable for examining cybersecurity policy because policy practices in this domain are largely articulated through formal texts, institutional strategies, legal frameworks, and official discourses rather than measurable behavioral outcomes. As cybersecurity governance is constructed and legitimized through policy documents, institutional reports, and regulatory instruments, analyzing these materials enables a systematic examination of how state power is articulated and exercised within digital governance structures. Document analysis is widely recognized as an effective qualitative method for interpreting policy narratives, institutional practices, and governance discourses within contemporary political research (Cresswell & Cheryl, 2017; Liang, 2019)

The primary data sources consist of official Indonesian government documents related to cybersecurity policy issued during the Joko Widodo administration (2014–2024). These include cybersecurity-related legislation, presidential regulations, national cybersecurity strategies, and official reports published by state institutions, particularly the National Cyber and Crypto Agency (Badan Siber dan Sandi Negara, BSSN). These documents were selected because they represent authoritative articulations of state rationalities, institutional priorities, and governing practices in cyberspace. In addition, the study draws on policy statements and strategic documents produced by the Ministry of Communication and Information Technology, as well as publicly available reports addressing cyber incidents and digital governance.

To contextualize and critically assess state-produced documents, secondary sources were also utilized. These include peer-reviewed academic journal articles, books on cybersecurity governance and political theory, and reports published by international organizations such as the International Telecommunication Union (ITU) and human rights organizations. These sources provide comparative perspectives and analytical frameworks that help situate Indonesia's cybersecurity policy within broader debates on security, governance, and democracy (Camini, 2022; Cavelty, 2007).

First, governmental rationality, which is the logic and justification used by the state to define cybersecurity as a matter of national security, digital sovereignty, and public order. This dimension highlights how cyber threats are discursively constructed to legitimize state intervention in the digital space. Second, government technology, which refers to a set of institutional, legal, and technical mechanisms used to implement cybersecurity governance. This includes regulatory frameworks, institutional arrangements such as the establishment of the National Cyber and Crypto Agency (BSSN), surveillance systems, data classification practices, and content moderation mechanisms. Through an analysis of these technologies, we can understand how abstract security rationalities are translated into concrete governance practices (Dean, 2010). Third, the process of subjectivation, which is the process of forming individuals as digital subjects in the cybersecurity regime. In this dimension, citizens are not positioned solely as objects of surveillance, but also as actors who are encouraged to internalize security norms through digital literacy programs, cybersecurity awareness campaigns, and regulatory compliance mechanisms, thereby encouraging self-regulatory practices that are in line with national security objectives.

Data analysis was conducted through a systematic examination of policy documents and institutional reports relevant to Indonesia's cybersecurity governance. Documents were first read to identify recurring themes related to threat framing, institutional authority, surveillance practices, and citizen responsibility. These themes were then interpreted through the governmentality framework to reveal underlying power relations and governing logics. Rather than seeking causal explanations, the analysis emphasizes interpretation and critical understanding of how cybersecurity policy functions as a mode of governance.

Result and Discussion

Cyber Threat Framing and Governing Rationalities

The findings indicate that Indonesia's cybersecurity policy is driven by a dominant security rationality that frames cyberspace as a vulnerable and contested domain requiring strong and centralized state intervention. Official policy documents, presidential statements, and national cybersecurity strategies consistently construct cyber threats as risks to national sovereignty, economic stability, and public order. This framing transforms cybersecurity from a technical concern into an existential security issue, thereby legitimizing exceptional measures and expanded state authority (Foucault, 2009; Hampson et al., 1998)

During the Joko Widodo administration, the discourse of *digital sovereignty* became increasingly prominent. Cyber threats were portrayed not only as criminal or technical disruptions but also as strategic challenges that could undermine state authority and national unity. This narrative was reinforced by references to large-scale cyber incidents, such as data breaches affecting public institutions and private platforms, as well as the growing threat of

cyber-enabled disinformation during electoral periods. By emphasizing the scale and urgency of these threats, the state constructed a sense of permanent digital insecurity that justified continuous intervention in cyberspace.

From a governmentality perspective, this threat framing functions as a governing rationality that shapes how cybersecurity problems are understood and addressed. Rather than treating cyber incidents as isolated events, policy discourse presents them as systemic risks requiring centralized coordination and surveillance. This rationality enables the state to expand its role in regulating digital infrastructure, online content, and user behavior, while marginalizing alternative approaches that emphasize decentralization or civil society participation (Dean, 2010)

Beyond rhetorical framing, the production of digital insecurity is reinforced through statistical narratives and risk quantification. Annual reports issued by the National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara*, BSSN) consistently present figures reaching hundreds of millions of cyber anomalies, thereby constructing an image of cyberspace as a domain of constant emergency. In contemporary governance, numbers function not merely as descriptive indicators but as technologies of truth that shape political perception and legitimize intervention (Hollanek, 2021). The quantification of cyber threats transforms abstract risks into measurable and governable objects, enabling policymakers to frame cybersecurity as an urgent and technical necessity rather than a contested political choice.

Recent scholarship on cybersecurity governance emphasizes that states increasingly deploy risk-based rationalities to justify regulatory expansion (Cavelty & Wenger, 2020; Fuster & Jasmontaite, 2020). In Indonesia, this logic manifests through the institutional strengthening of BSSN and the consolidation of cybersecurity authority under executive control. By framing cyber threats as transnational and unpredictable, the state positions centralized coordination as the only viable solution. This reinforces a technocratic mode of governance in which expertise, intelligence, and surveillance capacity become central to political authority. Such developments align with broader global trends in digital governance, where cybersecurity has become a key domain through which states reassert sovereignty in the digital age (Farrell & Newman, 2019)

The institutional transformation from the National Crypto Agency (*Lembaga Sandi Negara, Lemsaneg*) into the National Cyber and Crypto Agency (BSSN) also reflects broader political dynamics within Indonesia's executive governance structure. Established through Presidential Regulation No. 53 of 2017 and placed directly under the authority of the President, BSSN represents more than a bureaucratic reorganization aimed at improving administrative efficiency. Rather, the institutional redesign consolidated cybersecurity authority within the executive branch, strengthening presidential control over strategic digital infrastructures and information governance. Scholars have noted that in contemporary political systems, the expansion of executive authority through security institutions is often associated with processes of executive aggrandizement, where executive actors gradually increase their power by centralizing control over key governance domains (Bermeo, 2016). In the Indonesian context, the elevation of BSSN to a presidential-level agency can be interpreted as part of a broader pattern in which the executive branch strengthens its capacity to regulate digital spaces, monitor information flows, and manage political stability in an increasingly networked society. Consequently, cybersecurity governance becomes not only a technical response to digital threats but also a political instrument through which the state consolidates authority over the rapidly expanding digital public sphere.

The concept of digital sovereignty plays a particularly significant role in shaping Indonesia's cybersecurity rationality. Digital sovereignty is frequently invoked to justify regulatory intervention in digital platforms, data localization policies, and content moderation practices. While sovereignty traditionally refers to territorial authority, in the digital context it is rearticulated as control over data flows, infrastructure, and digital platforms (Steinbach, 2024). In Indonesia, this discourse supports state efforts to regulate foreign technology companies and enhance domestic cybersecurity capabilities. However, from a governmentality perspective, sovereignty discourse also functions as a normative justification for expanded monitoring and data governance, positioning state control as synonymous with national protection.

Importantly, cybersecurity threat framing is intertwined with electoral politics and information governance. The increasing concern over online disinformation, cyber propaganda, and foreign interference has reinforced narratives of digital vulnerability. Studies show that governments worldwide have expanded digital surveillance and content regulation in response to perceived information threats (Bradshaw & Howard, 2018; Gorwa, 2019). In Indonesia, regulatory interventions aimed at combating disinformation during electoral periods reflect a similar pattern, where the protection of democratic processes is invoked to justify enhanced monitoring of digital platforms. While such measures may aim to safeguard electoral integrity, they also blur the boundary between security management and political control.

From the perspective of governmentality, the production of cyber threats is inseparable from the production of governable subjects. Risk discourse encourages citizens and institutions to perceive themselves as potential targets of cyber insecurity, thereby fostering compliance with security-oriented policies. This aligns with contemporary analyses of digital governance, which argue that cybersecurity operates through anticipatory logics that manage uncertain futures (Hollanek, 2021). By invoking hypothetical risks such as data breaches, infrastructure sabotage, electoral manipulation, the state normalizes preventive intervention as rational and necessary.

Furthermore, the institutionalization of cybersecurity governance reflects a shift from reactive crisis management to permanent preparedness. Scholars have noted that modern security governance increasingly relies on preparedness and resilience as governing principles (Chandler, 2019).In Indonesia, cybersecurity strategies emphasize resilience, digital literacy, and national preparedness against cyber threats. While resilience discourse appears empowering, it also redistributes responsibility onto citizens and institutions, encouraging them to internalize security norms. This diffusion of responsibility strengthens the reach of cybersecurity governance beyond formal institutions and into everyday digital practices.

The dominance of security rationality in cybersecurity governance also shapes inter-agency relations and policy hierarchies. Centralization under BSSN enhances coordination but simultaneously reinforces executive dominance in digital policymaking. This development mirrors global debates about the securitization of cyberspace, where security institutions gain increased influence over regulatory domains traditionally associated with civilian governance (Cavelty, 2018). As cybersecurity becomes institutionalized as a national security priority, policy debates increasingly prioritize technical expertise and threat intelligence over democratic deliberation.

Moreover, the framing of cybersecurity as an existential issue limits alternative policy imaginaries. When cyberspace is constructed as a domain of constant threat, policy solutions emphasizing rights-based digital governance, decentralized oversight, or civil society participation appear secondary or even risky. Governmentality theory helps explain this dynamic: security

discourse narrows the field of possible action by presenting certain interventions as self-evident and unavoidable. In this sense, cybersecurity governance does not merely respond to threats but actively shapes the political conditions under which digital policy is debated and implemented.

Taken together, the analysis demonstrates that cyber threat framing in Indonesia operates as a central governing rationality that legitimizes institutional consolidation, regulatory expansion, and surveillance normalization. By mobilizing discourses of sovereignty, resilience, and digital vulnerability, the state constructs cybersecurity as a domain requiring continuous oversight and centralized control. While such measures enhance national capacity to address cyber risks, they also reconfigure power relations in the digital sphere. Cybersecurity governance thus emerges not only as a protective strategy but as a modality of rule that organizes authority, knowledge, and citizen conduct in contemporary Indonesia.

Institutionalization and Technologies of Government

The security rationality described above is operationalized through a range of governing technologies, particularly institutional arrangements and regulatory frameworks. One of the most significant developments during the Joko Widodo administration was the establishment of the National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara,* BSSN) in 2017. BSSN functions as the central coordinating body for cybersecurity governance, consolidating authority that was previously fragmented across multiple ministries and agencies.

The creation of BSSN reflects a broader trend toward centralized executive control over cybersecurity policy. Through BSSN, the state exercises oversight over cyber threat detection, incident response, and national cybersecurity strategy. This institutional consolidation enhances the state's capacity to monitor digital activities and respond to perceived threats, but it also reduces transparency and limits external oversight, particularly from local governments and civil society actors.

To illustrate the expansion of cybersecurity governance, Table 1 summarizes key institutions and their roles within Indonesia's cybersecurity policy framework.

Table 1. Key Institutions in Indonesia's Cybersecurity Governance

Institution	Primary Role in Cybersecurity Governance	Political Implications
National Cyber and Crypto Agency (BSSN)	National coordination of cybersecurity, threat detection, incident response	Centralization of authority under executive power
Ministry of Communication and Information Technology (Kominfo)	Regulation of digital platforms, content moderation, internet governance	Control over online discourse and information flows
National Police (Polri)	Law enforcement related to cybercrime	Criminalization of digital behavior
State Intelligence Agency (BIN)	Cyber intelligence and threat assessment	Expansion of surveillance capabilities

Source: Processed from official government documents (2017–2024)

In addition to institutional consolidation, cybersecurity governance relies heavily on regulatory technologies. Laws on electronic information, data protection, and national cybersecurity strategies provide legal justifications for surveillance, data collection, and content

regulation. These regulatory instruments function as technologies of government that translate abstract security rationalities into concrete practices of control (Rose & Miller, 2017).

Cyber Incident Trends as a Basis for Governance Expansion

Official data on cyber incidents plays a crucial role in reinforcing security rationalities. Reports published by BSSN consistently highlight the growing scale and complexity of cyber threats, thereby legitimizing further policy intervention. Table 2 presents a summary of reported cyber incidents in Indonesia over selected years during the Joko Widodo administration.

Table 2. Reported Cyber Incidents in Indonesia (Selected Years)

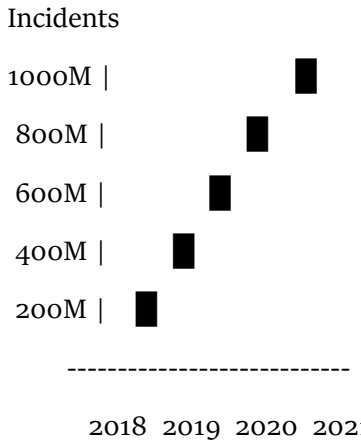
Year	Estimated Cyber Incidents	Dominant Threat Types
2018	~232 million	Malware, phishing
2020	~495 million	Data breaches, ransomware
2022	~976 million	Malware, phishing, APTs

Source: BSSN Annual Cybersecurity Reports (2018–2022)

The data presented in Table 2 illustrate a significant increase in reported cyber incidents in Indonesia over recent years, rising from approximately 232 million anomalies in 2018 to nearly one billion incidents by 2022 according to official reports from the National Cyber and Crypto Agency (BSSN). While these figures are frequently interpreted as evidence of escalating digital threats, their political relevance becomes clearer when viewed in relation to key political moments in Indonesia's recent history. For instance, the rise in cyber incidents between 2018 and 2020 coincided with the highly polarized 2019 presidential election, a period marked by intense online political mobilization, disinformation campaigns, and digital propaganda across social media platforms (Lim, 2017). During this period, government officials repeatedly emphasized the risks posed by cyber threats and online misinformation as justification for strengthening regulatory oversight and digital monitoring mechanisms. Similarly, the continued increase in cyber anomalies reported in the early 2020s emerged alongside preparations for the 2024 electoral cycle, when concerns about foreign interference, coordinated disinformation networks, and digital manipulation again became central to national security discourse.

From a governmentality perspective, the political significance of these statistics lies not only in their empirical representation of cyber risks but also in how they are mobilized to shape governance practices. Numerical indicators of cyber incidents function as instruments that frame cyberspace as a domain of persistent insecurity requiring constant state intervention. As Amoore, (2020) argues, statistical risk representations often operate as "technologies of truth" that render uncertain threats visible and governable, thereby legitimizing anticipatory regulatory responses. In the Indonesian context, the repeated presentation of large-scale cyber anomaly figures by BSSN contributes to constructing a narrative of permanent digital vulnerability. This narrative supports the expansion of regulatory instruments, surveillance infrastructures, and centralized cybersecurity coordination. Consequently, the statistical reporting of cyber incidents not only informs policy but also plays a performative role in sustaining a governance logic in which continuous monitoring and regulatory intervention are framed as necessary safeguards for political stability and national security (Hollanek, 2021). A simplified representation of the upward trend in reported cyber incidents is shown in Figure 1.

Figure 1. Trend of Reported Cyber Incidents in Indonesia (2018–2022)



Source: Compiled from BSSN reports

The visualization highlights how the continuous rise in reported incidents reinforces a narrative of escalating digital insecurity. This narrative supports the normalization of surveillance and regulatory intervention as necessary and unavoidable responses to cyber threats.

From a governmentality perspective, institutions such as BSSN are not merely administrative bodies but sites where knowledge, expertise, and authority converge to render cyberspace governable. Governmentality operates through institutional infrastructures that produce standardized procedures, risk classifications, and reporting mechanisms (Dean, 2010). In Indonesia, BSSN institutionalizes cybersecurity as a permanent domain of state intervention, embedding digital risk management within national bureaucratic structures. This reflects what contemporary scholarship describes as the bureaucratization of digital security, where technical expertise becomes a central source of political authority (Cavelty & Wenger, 2020)

The centralization of cybersecurity governance under BSSN also mirrors global patterns in which states strengthen executive coordination in response to perceived digital threats. Research on cybersecurity governance suggests that national cybersecurity agencies often emerge as hybrid institutions combining intelligence, military, and civilian regulatory functions . Such hybridization blurs the boundaries between security policy and civil governance, expanding the reach of national security logic into areas traditionally associated with civilian administration. In Indonesia, this hybrid structure enhances rapid response capabilities but simultaneously consolidates power within executive networks, potentially limiting parliamentary scrutiny and multi-stakeholder participation.

Regulatory frameworks further operationalize cybersecurity rationalities. The Electronic Information and Transactions Law, data protection legislation, and derivative regulations empower the state to regulate online content, mandate platform compliance, and impose sanctions for digital violations. These laws function as normative infrastructures that shape the conduct of digital actors, from technology companies to individual users. Scholars argue that contemporary digital regulation increasingly relies on platform governance mechanisms, where states delegate certain regulatory responsibilities to private intermediaries while retaining oversight authority (Gorwa, 2019; Suzor, 2019). In Indonesia, platform regulation through Kominfo illustrates how state authority extends indirectly into digital ecosystems by compelling intermediaries to enforce state-defined standards.

The deployment of regulatory technologies is closely linked to the concept of digital sovereignty. As discussed earlier, digital sovereignty redefines traditional notions of territorial control by emphasizing authority over data, infrastructure, and information flows (Steinbach, 2024). In practice, data localization policies, platform registration requirements, and cybersecurity certification regimes strengthen state capacity to control digital infrastructures within national borders. While these measures are justified as necessary for national resilience, they also enhance state leverage over digital actors and increase the regulatory burden on private sector entities.

Institutionalization also transforms cybersecurity governance from reactive crisis management into a proactive regime of anticipation and preparedness. Contemporary security governance increasingly relies on anticipatory logics that seek to preempt threats before they materialize (Hollanek, 2021). In Indonesia, cybersecurity strategy documents emphasize resilience, early detection systems, and predictive monitoring technologies. Such anticipatory governance reflects a shift from responding to incidents toward managing potential futures, where hypothetical threats justify continuous surveillance and risk assessment.

Moreover, the integration of cybersecurity into broader digital transformation agendas reflects the normalization of security within development policy. As Indonesia advances digital economy initiatives, cybersecurity becomes embedded in economic governance frameworks, linking digital growth with risk management. This integration illustrates what scholars describe as the securitization of development, where economic modernization is intertwined with security rationalities (Christou, 2016). In this context, cybersecurity governance does not merely protect infrastructure but structures the very conditions under which digital development unfolds.

The political implications of these institutional arrangements extend beyond administrative efficiency. By consolidating cybersecurity authority under executive agencies, the state restructures power relations within the digital domain. Executive-led cybersecurity governance may enhance coordination but risks marginalizing legislative oversight and civil society participation. As Farrell & Newman, 2019 argue in their concept of “weaponized interdependence,” control over network infrastructures provides states with new instruments of geopolitical and domestic leverage. While Indonesia’s cybersecurity policies are primarily framed as defensive, their institutional architecture creates capacities that could potentially be mobilized for broader regulatory control.

Additionally, regulatory expansion affects subnational governance dynamics. Local governments increasingly rely on national cybersecurity directives and centralized digital infrastructures. This dependency reinforces hierarchical governance patterns, where local actors operate within nationally defined security frameworks. Consequently, cybersecurity governance contributes to the reconfiguration of center–local relations, embedding digital security within centralized administrative hierarchies.

From a governmentality perspective, these institutional and regulatory developments illustrate how power operates through administrative normalization rather than overt coercion. Institutions produce standards, protocols, and classifications that shape acceptable digital conduct. Regulatory frameworks create compliance obligations that structure user behavior and corporate practices. Together, they form an integrated apparatus of digital governance that organizes cyberspace as a domain of calculable risk and regulated activity.

At the same time, the expansion of governing technologies generates tensions with democratic accountability. The concentration of cybersecurity authority within executive institutions may limit transparency and reduce opportunities for public deliberation. Recent studies emphasize the importance of multi-stakeholder governance in maintaining democratic legitimacy in digital policy domains (Cavelty & Wenger, 2020; Gorwa, 2019). However, security rationalities often prioritize efficiency and secrecy over participatory processes. In Indonesia, the balance between national security imperatives and democratic oversight remains a critical issue in evaluating the long-term trajectory of cybersecurity governance.

Taken together, the institutionalization of cybersecurity in Indonesia demonstrates how governing technologies translate abstract security rationalities into concrete administrative structures and regulatory instruments. Institutions such as BSSN embody centralized authority, regulatory frameworks extend state oversight into digital ecosystems, and anticipatory risk management embeds security into everyday governance practices. Through these mechanisms, cybersecurity governance emerges as a structured apparatus of rule that shapes digital infrastructures, organizational behavior, and citizen conduct. Rather than functioning solely as a protective measure, institutionalized cybersecurity governance constitutes a key modality through which the Indonesian state reorganizes authority and power in the digital age.

Digital Subject Formation and Self-Regulation

Beyond institutional arrangements and regulatory instruments, Indonesia's cybersecurity governance also operates through processes of digital subject formation. The findings show that cybersecurity policy during the Joko Widodo administration actively constructs citizens as *digital subjects* who are simultaneously protected, monitored, and disciplined. This process reflects a broader shift in governance from direct coercion toward indirect forms of control that rely on normalization, responsibility, and self-regulation .

Drawing on Kusumoningtyas's analysis of cyber surveillance as a national security instrument, cybersecurity governance in Indonesia encourages citizens to internalize security norms by framing surveillance as both necessary and legitimate in democratic contexts. Kusumoningtyas, (2023) argues that while cyber surveillance is often justified as a means of protecting national security, its expansion tends to blur the boundaries between protection and control, particularly when transparency and accountability mechanisms remain limited. In this sense, cybersecurity policy does not merely regulate digital infrastructures but also reshapes how citizens understand their roles and responsibilities in digital space.

Public campaigns on digital literacy, cybersecurity awareness, and "responsible internet use" function as key mechanisms of subjectification. These initiatives promote the idea that citizens must actively participate in maintaining cybersecurity by monitoring their own online behavior, avoiding prohibited content, and complying with digital regulations. Such governance strategies place significant responsibility on individuals while simultaneously normalizing state surveillance as an unavoidable aspect of digital life, positioning citizens as both potential risks and partners in cybersecurity governance (Kusumoningtyas & Puspitasari, 2020)

From a governmentality perspective, this emphasis on self-regulation illustrates how power operates through the internalization of norms rather than through overt repression. Individuals are encouraged to discipline themselves in accordance with state-defined security objectives, reducing the need for visible coercive intervention . However, as Kusumoningtyas,

(2023) highlights in her comparative study on cyber surveillance and democracy, this model of governance carries democratic risks when surveillance practices are not accompanied by robust legal safeguards and public oversight.

Moreover, the construction of digital subjects through cybersecurity policy has important implications for democratic participation and freedom of expression. When citizens perceive digital surveillance as a normal and necessary condition of security, critical engagement with state power may be diminished. Kusumoningtyas's work demonstrates that the normalization of surveillance can lead to a chilling effect on online political expression, particularly in contexts where legal ambiguities and broad security mandates persist .

In this context, digital subject formation becomes a central mechanism through which cybersecurity governance reshapes state–society relations. Rather than acting solely as rights-bearing citizens, individuals are increasingly governed as data subjects whose behaviors are continuously assessed and regulated. This process aligns with broader critiques of digital governance that emphasize how security-driven policies risk prioritizing control over democratic accountability (Zuboff, 2023)

Taken together, these findings indicate that cybersecurity policy in Indonesia functions as a technology of subjectification that encourages self-regulation while legitimizing expanded state surveillance. By drawing on Kusumoningtyas's empirical and normative insights, this study demonstrates that digital subject formation is not a peripheral outcome of cybersecurity governance but a core political process with lasting implications for democracy and civil liberties.

Democratic Implications and Local Political Dynamics

The expansion of cybersecurity governance in Indonesia has significant implications for democratic governance and local political dynamics. Practices such as content blocking, internet shutdowns, and the expansion of surveillance authorities illustrate how security-oriented policies can come into tension with democratic principles, particularly freedom of expression and access to information. Several high-profile cases, including temporary internet restrictions during periods of political unrest, demonstrate how cybersecurity measures may be deployed to manage dissent and control information flows at the local level. These interventions are often justified as necessary to maintain public order and national security, yet they simultaneously restrict civic space and democratic participation .

From a governmentality perspective, such practices reveal that cybersecurity policy is inherently political rather than merely technical. Security operates as a governing logic that defines acceptable and unacceptable forms of digital behavior, determines who can speak, and regulates what information is allowed to circulate in the public sphere. Through this logic, the state does not simply respond to threats but actively produces categories of risk and deviance that legitimize intervention. Cybersecurity governance thus functions as a mechanism for shaping political conduct and managing populations in digital spaces.

These dynamics are particularly visible at the local political level, where cybersecurity measures intersect with local governance, elections, and social mobilization. Local governments and security agencies often act as intermediaries in implementing national cybersecurity directives, translating abstract security rationalities into concrete actions such as content moderation, monitoring online activism, or restricting internet access in specific regions. As a result, cybersecurity governance reshapes local power relations by strengthening the role of

security institutions while limiting the capacity of local civil society actors to engage freely in digital political activities.

Moreover, the normalization of cybersecurity interventions has long-term consequences for democratic accountability. When extraordinary measures such as surveillance and internet shutdowns become routine responses to political tension, they risk being perceived as normal and necessary aspects of governance. This normalization reduces public scrutiny and weakens demands for transparency and oversight. In this context, citizens may become accustomed to restricted digital freedoms, leading to a gradual erosion of democratic norms and expectations regarding state accountability.

Taken together, these findings demonstrate that cybersecurity policy in Indonesia functions as a form of governmentality that integrates threat framing, governing technologies, and processes of subjectification. The framing of cyber threats legitimizes expanded state authority, institutional and regulatory technologies operationalize control, and digital subject formation ensures the internalization of security norms among citizens. While these mechanisms enhance the state's capacity to manage digital risks, they simultaneously generate persistent tensions with democratic accountability, civil liberties, and the quality of local political participation. Understanding these tensions is essential for evaluating cybersecurity governance not only as a security strategy, but also as a transformative force in contemporary democratic politics.

Conclusion

This article has demonstrated that cybersecurity policy in Indonesia during the Joko Widodo administration (2014–2024) operates as a form of governmentality through which the state governs cyberspace, digital conduct, and political participation. By moving beyond technical and legal perspectives, the analysis reveals cybersecurity as a political project embedded in broader strategies of state power, rather than a neutral response to digital threats.

Drawing on Michel Foucault's concept of governmentality, this study shows that cybersecurity governance in Indonesia is structured around three interrelated mechanisms. First, cyber threats are discursively framed as risks to national sovereignty, public order, and political stability. This framing produces a persistent sense of digital insecurity that legitimizes exceptional forms of state intervention. Second, these security rationalities are translated into practice through governing technologies, including institutional consolidation under the National Cyber and Crypto Agency (BSSN), regulatory frameworks, surveillance systems, and content moderation mechanisms. Third, cybersecurity governance operates through processes of subjectification, whereby citizens are constructed as digital subjects who internalize security norms and participate in self-regulation.

The findings highlight a central tension within Indonesia's cybersecurity policy. On the one hand, enhanced cybersecurity governance contributes to the protection of digital infrastructure and the management of cyber risks in an increasingly digital society. On the other hand, the expansion of surveillance, content control, and regulatory authority raises significant concerns regarding democratic accountability, freedom of expression, and the protection of privacy. From a governmentality perspective, these tensions are not accidental but are inherent to security-oriented governance, which prioritizes risk management and order over pluralism and contestation.

This study contributes to the literature on contemporary local politics by situating cybersecurity policy within debates on governance, power, and democracy in a developing democratic context. By applying a governmentality framework, the article provides a critical lens for understanding how digital security policies reshape state–society relations and influence local political dynamics. It also extends the application of governmentality beyond Western contexts, demonstrating its relevance for analyzing cybersecurity governance in Southeast Asia.

In practical terms, the findings suggest the need for greater transparency, oversight, and public participation in the formulation and implementation of cybersecurity policy. Strengthening democratic safeguards and accountability mechanisms is essential to ensure that cybersecurity governance does not evolve into a normalized form of digital control. Future research could explore comparative cases across different political systems or examine how local actors, civil society organizations, and digital communities negotiate and resist cybersecurity governance in everyday practice.

References

Bermeo, N. (2016). On democratic backsliding. *Journal of Democracy*, *27*(1), 5–19. https://doi.org/10.1353/jod.2016.0012

Bilan, Y., Oliinyk, O., Mishchuk, H., & Skare, M. (2023). Impact of information and communications technology on the development and use of knowledge. *Technological Forecasting and Social Change*, *191*, 122519. https://doi.org/10.1016/j.techfore.2023.122519

Bradshaw, S., & Howard, P. N. (2018). Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation. *Computational Propaganda Research Project*, *1*(3), 26pp. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf

Camini, A. (2022). Resenha: "Do Morals Matter? Presidents and foreign policy from FDR to Trump." In *Conjuntura internacional* (Vol. 18, Issue 2). Oxford University Press. https://doi.org/10.5752/p.1809-6182.2021v18n2p2-3

Canton, H. (2021). International telecommunication union—ITU. In *The Europa directory of international organizations 2021* (pp. 355–358). Routledge.

Cavelty, M. D. (2007). Cyber-Security and Threat Politics: US Efforts to Secure the Information Age. In *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. Routledge. https://doi.org/10.4324/9780203937419

Cavelty, M. D. (2018). Cybersecurity research meets science and technology studies. *Politics and Governance*, *6*(2), 22–30. https://doi.org/10.17645/pag.v6i2.1385

Cavelty, M. D., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

Chandler, D. (2019). Resilience and the end(s) of the politics of adaptation. *Resilience*, *7*(3), 1–10. https://doi.org/10.1080/21693293.2019.1605660

Christou, G. (2016). Cybersecurity in the European Union Resilience and Adaptability in Governance Policy. In *New Security Challenges* (pp. 1–222). Taylor & Francis. https://doi.org/10.1080/09662839.2016.1160892

Cresswell, J. W., & Cheryl, P. N. (2017). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. Sage publications. https://keithrkenney.files.wordpress.com/2012/02/creswellcritique.pdf

Dean, M. M. (2010). Governmentality: power and rule in modern society. *Choice Reviews Online*, *47*(11), 47-6521-47–6521. https://doi.org/10.5860/choice.47-6521

Farrell, H., & Newman, A. L. (2019). Weaponized Interdependence How Global Economic Networks Shape State Coercion. *International Security*, *44*(1), 42–79.

https://doi.org/10.1162/ISEC_a_00351
Foucault, M. (2009). *Security, Territory, Population* (M. Senellart, F. Ewald, & A. Fontana (eds.)). Palgrave Macmillan UK. https://doi.org/10.1057/9780230245075
Fuster, G. G., & Jasmontaite, L. (2020). Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights. In M. Christen, B. Gordijn, & M. Loi (Eds.), *The Ethics of Cybersecurity* (pp. 97–115). Springer International Publishing. https://doi.org/10.1007/978-3-030-29053-5_5
Gorwa, R. (2019). What is platform governance? *Information Communication and Society*, *22*(6), 854–871. https://doi.org/10.1080/1369118X.2019.1573914
Hampson, F. O., Buzan, B., Waever, O., & Wilde, J. de. (1998). Security: A New Framework for Analysis. In *International Journal* (Vol. 53, Issue 4). Lynne Rienner Publishers. https://doi.org/10.2307/40203739
Hilbert, M. (2014). How much of the global information and communication explosion is driven by more, and how much by better technology. *Journal of the Association for Information Science and Technology*, *65*(4), 856–861. https://doi.org/10.1002/asi.23031
Hollanek, T. (2021). Cloud Ethics: Algorithms and the Attributes of Ourselves and Others. In *Design Issues* (Vol. 37, Issue 4). Duke University Press. https://doi.org/10.1162/desi_r_00662
Kusumoningtyas, A. A. (2023). Nexus Pengawasan Siber Sebagai Instrumen Keamanan Nasional Dan Relevansinya Dengan Demokrasi: Perbandingan Beberapa Negara. *Jurnal Adhikari*, *2*(3), 416–433. https://doi.org/10.53968/ja.v2i3.80
Kusumoningtyas, A. A., & Puspitasari, P. (2020). Dilema Hak Perlindungan Data Pribadi Dan Pengawasan Siber: Tantangan Di Masa Depan. *Jurnal Legislasi Indonesia*, *17*(2), 234–250. https://doi.org/10.54629/jli.v17i2.706
Liang, J. (2019). Qualitative research methods: collecting evidence, crafting analysis, communicating impact: by S. J. Tracy, West Sussex, UK, John Wiley & Sons, Ltd. 368 pp., $115.50 (hardback), ISBN: 978-1-4051-9202-3. In *Communication Research and Practice* (Vol. 5, pp. 1–2). Taylor & Francis.
Lim, M. (2017). Freedom to hate: social media, algorithmic enclaves, and the rise of tribal nationalism in Indonesia. *Critical Asian Studies*, *49*(3), 411–427. https://doi.org/10.1080/14672715.2017.1341188
Liu, S. M., & Yuan, Q. (2015). The Evolution of Information and Communication Technology in Public Administration. *Public Administration and Development*, *35*(2), 140–151. https://doi.org/10.1002/pad.1717
Rose, N., & Miller, P. (2017). Political power beyond the state: Problematics of government. In *Foucault and law* (pp. 191–224). Routledge. https://doi.org/https://doi.org/10.2307/591464
Shi, J., & Feng, G. (2024). Do moral matters?: Presidents and Foreign policy from FDR to Trump Do moral matters?: Presidents and Foreign policy from FDR to Trump , by Joseph S. Nye, Oxford University. *Critical Policy Studies*, *18*, 1–3. https://doi.org/10.1080/19460171.2024.2340660
Steinbach, A. (2024). Digital sovereignty. *List Forum Fur Wirtschafts- Und Finanzpolitik*, *50*(1–2), 51–74. https://doi.org/10.1007/s41025-023-00252-3
Suzor, N. P. (2019). *Lawless: The secret rules that govern our digital lives*. Cambridge University Press. https://doi.org/https://doi.org/10.1017/9781108666428
Zuboff, S. (2023). The Age of Surveillance Capitalism. In *Social Theory Re-Wired* (pp. 203–213). Routledge. https://doi.org/10.4324/9781003320609-27