

Hoaxes, Counter-Information, and the Unequal Governance of Public Information in the Technoculture Era

Eko Setiawan^{1*}, Rachmah Ida², Irfan Wahyudi³

^{1,2,3} Universitas Airlangga

Jl. Dharmawangsa Dalam, Airlangga, Kec. Gubeng, Surabaya, Jawa Timur 60286

*Email Corresponding: ekopangkapi@gmail.com

Article History:

Received: 15/01/2025

Revised: 27/07/2026

Accepted: 27/07/2026

Published: 18/08/2026

Keywords:

Counter-Information

Counterculture

Data breach

Hyper-Information Society

Technoculture.

Abstract: The labeling of hoaxes by state authorities over data breach claims does not merely serve as an informational correction; it operates as a mechanism for regulating epistemic authority in the digital space. This article analyzes how hoax formation and the circulation of counter-information on social media function as expressions of digital counterculture within the frameworks of technoculture and the Social Construction of Technology (SCOT), and how these dynamics reflect unequal governance of public information in Indonesia. This study employs a qualitative approach with a case study design and discourse analysis. Data were collected purposively from social media content, digital news coverage, official government statements, and interviews with personnel from the National Police Cyber Unit (Siber Polri), the National Cyber and Crypto Agency (BSSN), and the Ministry of Communication and Information (Kominfo) as state actors, as well as white hacker and black hacker communities. Analysis proceeded through data reduction, thematic coding, narrative categorization, discourse analysis, and theory-driven interpretation using technoculture and SCOT, validated through source triangulation. Findings indicate that hoax labeling serves a dual function as an instrument of epistemic control; counter-information emerges in response to a crisis of public trust and unequal information access; and interpretative flexibility among state actors, media, cyber communities, and the digital public explains how the meaning of data breaches is contested. These dynamics signal a transition from network society to hyper-information society, a condition in which information overload and the illusion of truth effect blur the boundaries between official information, hoaxes, and counter-information.

1. Introduction

The acceleration of information circulation in digital spaces has blurred the boundaries between official information, citizen-generated content, *hoaxes*, and counter-narratives. In Indonesia, the rapid growth of *social media* as a channel for producing and distributing information has repositioned the state from the sole authority on public information to one actor among many in an increasingly fragmented information ecosystem. This shift affects not only the quality of circulating information but also how epistemic authority is contested in digital spaces (Bollmer, 2018; Castells, 2011).

This article argues that state authorities' labeling of *hoaxes* is not always a neutral act of informational correction. In public information governance, the *hoax* label can serve a dual function: protecting the public from false information while also regulating epistemic authority in ways that marginalize alternative narratives. The concern of this article is therefore not simply about the factual accuracy of a given piece of information, but about who holds the power to determine the boundary between legitimate and illegitimate information in the digital sphere.

The case of Bjorka in 2022 provides a relevant empirical entry point for examining these dynamics. When this anonymous actor claimed to have leaked government data and shared it via Telegram and Twitter, Kominfo and BSSN responded with official denials and *hoax* labels. Meanwhile, cyber communities, independent journalists, and the digital public questioned the credibility of the government's clarifications. The collision between data breach claims, state denials, mainstream media coverage, and community interpretations reveals that the information contest in this case was not merely a technical dispute over data validity, but a broader struggle over meaning and epistemic authority in digital space.

To analyze these dynamics, this article draws on two analytical frameworks. The first is the technoculture perspective, which positions digital technology not as a neutral communication tool but as a socio-cultural space where power relations, values, and resistance are negotiated (Penley & Ross, 1991; D. B. Shaw, 2008). The second is the *Social Construction of Technology* (SCOT), developed by Bijker and Pinch (1987), which holds that the meaning of a technological artifact, including digital information, is shaped through *interpretative flexibility* among *relevant social groups*, rather than standing as an objective and fixed category. Within this framework, the meaning of *hoaxes* and data breaches is understood as the product of social processes involving negotiation, conflict, and *closure* among competing social groups.

Prior scholarship on *hoaxes* and disinformation in Indonesia has contributed significantly to mapping patterns of false content dissemination on *social media* (Juditha, 2018), describing *post-truth* conditions in digital media ecologies (Cosentino, 2020; Pane, 2018) and analyzing how media hyperreality shapes public perception during crises (Ehsen & Alam, 2021; Wirman & Sari, 2020). International studies have also examined opinion manipulation and *agenda setting* in *fake news* proliferation (Basu, 2021; Bharali & Goswami, 2018). However, these studies have largely treated *hoaxes* as a problem of informational validity and have not systematically examined how narratives labeled as *hoaxes* can operate as *counter-information*, that is, as counter-narratives that respond to unequal access to information and a crisis of trust in state institutions.

This article addresses three specific gaps in the existing literature. Prior studies tend to treat *hoax* research, public information governance, and digital resistance as separate fields of inquiry. Furthermore, limited scholarship explicitly reads *counter-information* as a form of digital *counterculture* within the frameworks of *technoculture* and SCOT. Beyond that, the dynamics of Indonesia's transition from a *network society* to a *hyper-information society*, characterized by information overload, a crisis of verification, and the dominance of the *illusion of truth effect*, have not been analyzed in an integrated manner alongside the contestation of meaning in digital spaces. This study aims to analyze how the formation of *hoaxes* and the circulation of *counter-information* on social media can be understood as a form of digital *counterculture* through the perspectives of *technoculture* and SCOT, and to examine how such dynamics contribute to the emergence of a *hyper-information society* in the Indonesian context.

2. Literature Review

Hoax, Disinformation, and the Crisis of Truth in Digital Culture

Studies of *hoaxes* and disinformation generally begin by distinguishing three categories of information disorder: misinformation, understood as false information disseminated without intent to mislead; disinformation, understood as false information disseminated deliberately; and mal-information, understood as fact-based information used to harm particular parties. This distinction is conceptually relevant. However, in public information governance, these categories cannot always be applied neatly because labeling information itself involves judgments shaped by authority, interests, and power relations.

The production and spread of *hoax* content on Indonesian social media depend heavily on social

networks formed around shared purposes between senders and receivers, as well as on emotional factors that make the public receptive to unverified information (Juditha, 2018). Fake news is often produced with clear intent to manipulate public opinion through framing and agenda-setting mechanisms, rather than reflecting random informational error (Bharali & Goswami, 2018). Furthermore, in Indonesia's digital media ecology, emotionally packaged content is often perceived as more credible than official information, reflecting a deeper crisis of trust in state institutions (Pane, 2018). While these studies make important contributions to mapping patterns of hoax dissemination, they uniformly treat hoaxes as a problem of informational validity, opinion manipulation, or media literacy, without examining how the hoax label itself can function as an instrument for regulating epistemic authority within the power relations between the state and the digital public.

Counter-Information as Digital Counterculture

Counter-information must be distinguished conceptually from both disinformation and *hoaxes*. While disinformation is driven by an intent to deceive, *counter-information* emerges from conditions of public distrust toward official narratives and unequal access to information regarded as significant. In this sense, *counter-information* operates as a counter-narrative that challenges the epistemic monopoly of the state, mainstream media, or other authoritative institutions (Basu, 2021). It is not simply a factual rebuttal, but a declaration that certain groups do not recognize the legitimacy of those who currently hold the authority to define truth.

The relationship between counter-information and counterculture becomes analytically meaningful when such counter-narratives are no longer individual acts of dissent but are organized into recurring digital cultural practices that deploy anonymity, satire, and virality as tools of resistance. Media produces simulations and hyperreality that lose connection with verifiable facts, such that narratives that originally function as critical responses to power can slide into misleading constructions of reality (Ehsen & Alam, 2021). This condition illustrates the inherent ambivalence of counter-information: it can constitute a legitimate critique of power, while also risking a slide into disinformation when it lacks sufficient basis in verifiable evidence (Wirman & Sari, 2020). Nevertheless, none of these studies systematically reads counter-information as a form of digital counterculture operating within a technoculture framework, leaving the cultural and resistive dimensions of counter-narratives analytically underexamined in the existing literature.

Technoculture and SCOT as an Integrative Framework

The *technoculture* perspective holds that digital technology is not a neutral communication tool but a socio-cultural space shaped by layered values, interests, power, and cultural practices (D. B. Shaw, 2008). Within this framework, social media platforms are not mere technical infrastructure but arenas where cultural values, political interests, and social resistance are mutually negotiated. Technoculture constitutes a complex matrix of technology, politics, and culture, in which technology is not merely a tool but also a medium that shapes and regulates social interaction and the production of meaning (Penley & Ross, 1991). Within this framework, resistance to dominant culture mediated by technology cannot be understood solely through the lens of informational content, but must be read as a cultural practice rooted in broader power relations.

The *Social Construction of Technology* (SCOT), developed by Pinch and Bijker (1984), complements this perspective by providing a mechanistic explanation of how the meaning of a technological artifact or digital information is socially constructed. The concept of *interpretative flexibility* explains why a single event or piece of information can be read in fundamentally different ways by different social groups: the

state may read a data breach as a national security threat, a cyber community may read it as evidence of inadequate data protection, mainstream media may frame it as a governance crisis, while the digital public may receive it as validation of their existing distrust of the government (T. J. Pinch & Bijker, 1984). The concept of *closure and stabilization* then describes one group's effort to end the contest over meaning and fix one interpretation as authoritative truth. In open digital ecosystems, state-driven *closure* frequently fails because counter-narratives continue to be reproduced and circulated independently of any single distribution channel. Prior studies on *hoaxes* in Indonesia have not used the SCOT framework to read the social construction of meaning around *hoaxes* and data breaches, so the dynamics of *interpretative flexibility* among relevant social groups have never been systematically analyzed in this context.

From Network Society to Hyper-Information Society

The network society is characterized by connectivity that transcends geographical and institutional boundaries, enabling mass participation and information distribution (Castells, 2011). However, these conditions do not invariably produce emancipatory outcomes. Digital culture not only expands access but also complicates how individuals and communities negotiate identity, trust, and truth in increasingly complex informational environments (Bollmer, 2018). Within the network society, the echo chamber effects generated by platform algorithms push individuals toward continuous engagement with information consistent with their existing beliefs, progressively weakening critical reflection on circulating information (Castells, 2011).

When information volume exceeds the public's capacity to verify it, the network society can transition into what this article terms a hyper-information society. In this condition, information is not only abundant but also mutually contradictory, hard to verify, and often evaluated based on repetition and emotional proximity rather than factual accuracy. This mechanism has been identified as the illusion of truth effect: the tendency to assess a claim as true not because it has been verified, but because it has been frequently repeated and is consistent with pre-existing beliefs (Cosentino, 2020). Prior studies have touched on the crisis of verification and the deliberate manipulation of public opinion through framing and agenda setting (Bharali & Goswami, 2018; Juditha, 2018), as well as the weak digital literacy that allows emotionally packaged content to be perceived as more credible than official information (Pane, 2018), but none of them explicitly connect these dynamics to the concept of a transition from network society to hyper-information society, nor do they examine this transition in relation to the contestation of meaning among the state, media, cyber communities, and the digital public in Indonesia.

Synthesis and Research Gap

Prior journal studies consistently treat *hoaxes* as a problem of information manipulation, hyperreality, or media literacy. None of these studies systematically reads *counter-information* as a form of digital *counterculture* operating within the frameworks of *technoculture* and SCOT, nor do they connect these dynamics to the emergence of a *hyper-information society* in the Indonesian context. These studies also tend to treat *hoax* research, public information governance, and digital resistance as separate fields of inquiry, obscuring how the three mutually constitute one another within a single integrated digital information ecosystem.

This article addresses three specific gaps in the existing literature. First, prior studies have not adequately explained how *hoaxes* and *counter-information* are socially constructed through power relations among the state, media, cyber communities, and the digital public, continuing instead to treat them as matters of informational validity. Second, *counter-information* has not been systematically read as a form of digital *counterculture* operating within a *technoculture* framework, leaving its cultural and

resistive dimensions underanalyzed. Third, the dynamics of Indonesia's transition from a *network society* to a *hyper-information society* have not been examined in an integrated manner alongside the contestation of meaning in digital spaces. This article fills these three gaps by combining *technoculture* and SCOT into an integrative analytical framework for reading *hoax* formation and the circulation of *counter-information* as digital *counterculture*, while also explaining the conditions for a *hyper-information society* emerging in the Indonesian context.

3. Research Methods

This study applies a qualitative approach with a case study design [Creswell & Poth \(2018\)](#), to examine in depth the dynamics of hoaxes, counter-information, and epistemic resistance within Indonesia's digital public sphere. The study collected research data using purposive sampling [Patton \(2015\)](#), drawing on both digital and field sources. Digital data came from social media activity on Twitter (now X), digital news coverage, and official press releases from relevant government agencies. Meanwhile, field data were obtained through interviews with representatives from the Ministry of Communication and Information Technology (Kominfo), the National Cyber and Crypto Agency (BSSN), and the National Police Cyber Unit (Siber Polri) as state representatives, alongside informants from both white-hat and black-hat hacker communities to capture the exclusive perspectives of independent cyber actors.

This research follows a discourse analysis and thematic coding structure [Braun & Clarke \(2006\)](#), carried out in five systematic stages: data reduction, thematic analysis to identify main patterns, narrative categorization, discourse analysis, and theory-driven interpretation ([Miles et al., 2014](#)). The theoretical frameworks of technoculture [D. B. Shaw \(2008\)](#), and the Social Construction of Technology [T. J. Pinch & Bijker \(2021\)](#), were integrated as analytical instruments to dissect the contestation of meaning and interpretative flexibility among relevant social groups. To ensure the validity, reliability, and trustworthiness of the research findings, we conducted data validation through source triangulation by cross-referencing and comparing findings from official government documents, digital activity data on social media, and in-depth interview transcripts from the various informant groups.

4. Results and Discussion

Dominance of Official Narratives and the Delegitimization of Alternative Information

We live in a time when information moves rapidly across digital networks, creating a highly volatile environment for public discourse ([Castells, 2011](#)). In this digital age, the massive influx of information has triggered a crisis of verification, where traditional methods of testing the truth are no longer effective. The algorithmic architecture of digital platforms exacerbates this situation by creating "echo chambers" that limit users' exposure only to content that confirms their preexisting beliefs ([Del Vicario et al., 2016](#)). Reliance on this algorithmically customized content delivery worsens information fragmentation, where limited exposure to diverse perspectives gradually distorts public discourse and narrows individual worldviews. This crisis is also shaped by the psychology of information dissemination. Often, false information spreads not to convey facts, but as a form of "affective networking" or an identity signal that signals the sender's values and norms to their social group ([Bailey & Hsieh-Yee, 2019](#)). The drive to build such solidarity frequently overrides concerns for factual accuracy.

Often, this digital information spreads too quickly for state authorities and traditional gatekeepers to verify its accuracy before it reaches a mass audience ([Vosoughi et al., 2018](#)). Consequently, to manage inherent risks and maintain public order, state actors constantly seek ways to firmly assert their authority

over what is considered true. One primary method is rapidly classifying unfavorable, critical, or unverified information as “hoaxes” (Tandoc et al., 2018). This study highlights that labeling information as a hoax is often less about objective factual accuracy and more about strategically controlling public perception and determining which epistemic sources are deemed legitimate and trustworthy (Sudibyo, 2021). By weaponizing terms like “hoax” or “fake news”, governments can effectively contain alternative narratives and limit the boundaries of acceptable public discourse (Lazer et al., 2017). This dynamic is further illuminated by recent critiques of the “polarisation narrative.” Authorities often weaponize the discourse of polarization to simplify complex political grievances, framing dissenting or alternative voices as irrational “extremes” (Roch et al., 2026). By doing so, state actors justify a return to post-political technocratic management to “restore order,” effectively using the perceived threat of polarization to neutralize legitimate political contestation and reassert centralized control over the truth (Roch et al., 2026). Extreme polarization resulting from this information fragmentation ultimately creates a severe challenge known as the “backfire effect.” In this scenario, attempts by authorities or experts to correct facts can make groups who already believe the hoax more defensive and more likely to consume conspiratorial content (Zollo et al., 2017).

In Indonesia, the government’s response to the digital interventions of the hacker known as Bjorka in 2022 exemplifies this dynamic of narrative dominance (Llewellyn, 2022). A systemic crisis of trust in state institutions makes the public more susceptible to absorbing unverified counter-information, thereby worsening the polarization of truth in the public sphere (Ong & Tapsell, 2022). When Bjorka claimed to have breached and publicized sensitive government data—ranging from SIM card registrations to the personal details of public officials—state agencies rapidly dismissed the claims as invalid or mere hoaxes (Bisnis.com, 2022; CNN Indonesia, 2022). Through coordinated press briefings and official social media channels, the state positioned itself as the sole legitimate arbiter of truth regarding digital security. While governments legitimately worry about the proliferation of false information and its potential destabilizing impact on national security, unilaterally labeling claims as false without transparent public discussion creates a significant democratic problem. This approach systematically excludes independent researchers, cybersecurity communities, and public interest groups from participating in the verification process (Badan Siber dan Sandi Negara, 2025; Komunitas Etis Keamanan Siber, 2025).

Mainstream media further amplifies this institutional dominance by relying heavily on official sources. In the Bjorka case, media outlets extensively reported the state’s denials while largely marginalizing independent security experts who provided alternative insights into the severity of the data breach (Voice of Indonesia (Corporate Author), 2022). This over-reliance creates a dominant narrative that suppresses alternative viewpoints and hinders citizen-led, critical inquiry. The Social Construction of Technology (SCOT) framework is highly relevant here, demonstrating that the meaning and societal impact of technology—including leaked digital information—are shaped by negotiations among different social groups, a concept known as interpretive flexibility (T. Pinch & Bijker, 1984). When the state exerts excessive control over narrative classification to protect its institutional reputation, it curtails this flexibility. To maintain both public trust and participatory legitimacy, the state must navigate information containment cautiously, moving away from unilateral hoax labeling and instead embracing communicative rationality and epistemic pluralism within the digital public sphere (Habermas, 1989; Hardiman, 1993).

Counter-Information as an Expression of Epistemic Resistance

In today’s interconnected digital landscape, the democratization of information creation allows non-

traditional and marginalized actors to significantly influence public discourse (Jenkins et al., 2015). In this context, counter-information does more than express a differing opinion from official state narratives; it serves as a robust mechanism to directly challenge dominant structures of knowledge and institutional authority (Tapsell, 2021). It is crucial to distinguish between malicious disinformation, which is deliberately spread to deceive or cause harm, and genuine counter-information.

Not all actors claiming to provide alternative narratives contribute positively to democratic discourse. Recent scholarship warns against the emergence of “regressive” alternative media that co-opt the “alternative” label to spread disinformation and defend systemic inequalities (Cazzamatta, 2025). Unlike progressive counter-publics that seek to democratize information and represent marginalized voices, these regressive and defensive publics maintain a tenuous relationship with the truth and actively disrupt the democratic public sphere (Cazzamatta, 2025). Counter-information, in its legitimate democratic form, typically emerges in environments where citizens feel structurally marginalized, lack access to official data, or perceive existing institutions as lacking in transparency and accountability.

Media literacy provides a strong cognitive foundation because it increases user control over information processing, encourages critical engagement, and supports the deliberate evaluation of diverse content amid the rapid flow of visual information (Jones-Jang et al., 2021). Interestingly, recent empirical findings indicate that high levels of media literacy do not necessarily reduce users’ perceptions of the threat of information fragmentation; instead, media literacy actually sharpens individuals’ critical awareness of content silos, algorithmic recommendation biases, and detrimental selective exposure patterns. To address this information disorder and effectively distinguish between malicious disinformation and legitimate counter-information, comprehensive digital literacy policies are crucial. Contemporary digital literacy focuses on using devices, but it must also develop information literacy—the cognitive capacity to critically evaluate sources and process information deeply (Jones-Jang et al., 2021).

This form of counter-information represents a concerted attempt by individuals or digital communities to reclaim agency over the interpretation of events and facts that are traditionally monopolized by powerful state or corporate entities (Lim, 2018). For these voices, producing and disseminating counter-narratives is a vital tool for democratic participation and a form of digital resistance against informational hegemony (Treré, 2018). Therefore, reactive government policies—such as merely labeling information as hoaxes downstream—will not be effective (Juditha, 2018). The state needs a “pre-bunking” approach that equips the public with a critical analytical framework before exposure to hoaxes and supports multi-dimensional literacy initiatives that integrate cognitive, emotional, and social support (Bailey & Hsieh-Yee, 2019).

The 2022 case of Bjorka in Indonesia provides a compelling illustration of this phenomenon. By systematically breaching government databases and disseminating secret documents via platforms like Telegram and Twitter, Bjorka actively challenged the state’s prevailing narrative on the robustness of its cybersecurity infrastructure (Intan Rakhmayanti Dewi (CNBC Indonesia), 2022; Kakak Indra Purnama, 2022). While authorities predictably condemned these actions as illegal breaches and quickly dismissed the associated claims as hoaxes Agus Tri Haryanto (2022), Bjorka’s interventions successfully catalyzed widespread, critical public discourse regarding state accountability and the vulnerability of personal data. Rather than simple criminality, these actions can be analytically interpreted as a profound form of epistemic resistance and digital disobedience, protesting a bureaucratic system that often stifles transparency and dismisses alternative public inquiries (Komunitas Underground Hacker, 2025; Romagna & Leukfeldt, 2024).

Viewed through the lens of the SCOT framework, these digital actions’ meaning is continuously

negotiated and contested among different social groups (Bijker, 1995). Hackers, independent journalists, and digital activists are relevant social groups that assign new, critical meanings to technological tools and information-dissemination networks (Coleman, 2014; Rayner, 2018). SCOT's core principle of interpretive flexibility helps explain why state actors uniformly view data leaks as severe national security threats, while online communities may simultaneously see them as necessary, democratic checks on unchecked institutional power (T. J. Pinch & Bijker, 2021).

Furthermore, the technoculture perspective emphasizes that digital technology is never neutral; it is deeply intertwined with cultural values, political interests, and systemic power dynamics (Penley & Ross, n.d.; D. B. Shaw, 2008). The internet functions as a highly contested space where counter-narratives consistently challenge hegemonic truths. However, while counter-information can effectively foster critical inquiry and expose systemic flaws, navigating this complex digital age requires more than just adversarial resistance. Drawing on both SCOT and technocultural perspectives, it becomes clear that society needs robust, participatory information governance frameworks—policies that secure digital infrastructure while explicitly integrating the diverse, citizen-led realities that shape modern public life. Ultimately, policymakers and digital platform providers must collaborate to promote the transparency of algorithmic recommendation systems, empowering the public to proactively diversify their media exposure and build democratic resilience in the digital age (Castells, 2011; Tréré, 2018).

Technoculture and the Inequality of Information Spaces

Digital technologies have become deeply embedded in contemporary social, political, and informational life, shaping not only communication practices but also power distribution within digital environments. From a technocultural perspective, technologies should not be understood as neutral communication tools; rather, they are socio-technical systems shaped by cultural values, institutional interests, and political structures (D. T. Shaw, 2008). Crucially, this analysis demonstrates how digital platforms have become central infrastructures through which information is produced, circulated, and evaluated within contemporary society.

Although digital media have expanded opportunities for participation and content creation, access to visibility, influence, and agenda-setting power remains uneven. The platformization of communication has strengthened the role of digital infrastructures, algorithms, and content moderation systems in regulating information flows, shaping which voices are amplified and which are marginalized in public discourse (Gillespie, 2018; Helmond, 2015). Consequently, contemporary information ecosystems are characterized not only by technological connectivity but also by persistent asymmetries of power that shape the production, circulation, and legitimacy of information in digital society (Nick & Ulises, 2019).

Digital platforms occupy a paradoxical position within contemporary information ecosystems. On the one hand, they expand opportunities for individuals and communities to create, distribute, and access information without relying on traditional institutional gatekeepers. On the other hand, the architecture of digital platforms, including algorithmic curation, content moderation, and platform governance mechanisms, can privilege certain actors while constraining the visibility of others (Gillespie, 2018; Helmond, 2015).

This situation creates unequal information spaces in which institutional actors, including state agencies and mainstream media organizations, often possess greater capacity to shape public narratives than ordinary citizens. As a result, official accounts tend to receive broader visibility and legitimacy, whereas alternative perspectives are more likely to be marginalized, contested, or dismissed. This shows that democratizing information production does not necessarily eliminate existing power asymmetries;

instead, digital platforms may reproduce and even reinforce inequalities in how knowledge circulates and is recognized in public discourse ([Helmond, 2015](#)).

The unequal distribution of informational power is especially visible in the Indonesian context, particularly during periods of controversy over data security and public accountability. In such highly contested settings, state institutions often seek to reassert control over public discourse by framing alternative information as misinformation or hoaxes. The 2022 Bjorka data breach controversy illustrates this dynamic. After the disclosure of alleged government and public data leaks, official responses from state agencies focused primarily on questioning the claims' validity and mitigating public concern.

Mainstream media coverage often relied on official statements, while alternative interpretations from independent cybersecurity experts received comparatively less visibility. Viewed through a technocultural lens, this empirical pattern highlights how institutional actors possess greater capacity to shape the circulation and legitimacy of information within digital spaces. Although such responses may be justified as efforts to maintain public order and cybersecurity, they also reinforce existing asymmetries in informational authority by privileging official narratives over competing interpretations. Consequently, digital security governance becomes intertwined with broader struggles over knowledge, credibility, and the power to define what counts as legitimate public information ([Merylina, 2017](#)).

This dynamic can be understood through the concept of institutional gatekeeping, whereby media organizations rely heavily on official sources when reporting sensitive political and security-related issues. Rather than functioning solely as neutral channels of information, media institutions play a key role in determining which actors, perspectives, and narratives gain legitimacy in public discourse ([Gillespie, 2018](#)).

The findings suggest that such gatekeeping practices may inadvertently reinforce the dominance of institutional viewpoints by prioritizing official accounts over alternative interpretations. Consequently, citizens, independent experts, and civil society actors often face greater challenges in influencing how public issues are framed and understood. From a technocultural perspective, this process contributes to the unequal distribution of communicative power, where access to visibility and credibility is shaped not only by the quality of information but also by the institutional authority of those who produce and disseminate it. This pattern reflects what is conceptualized as symbolic power, in which institutional actors have greater authority to define legitimate knowledge and shape public understanding of contested issues ([Barsky, 1991](#)).

Beyond institutional gatekeeping, algorithmic governance represents another mechanism through which information inequality is reproduced within digital environments. This study's findings indicate that algorithmic recommendation systems, engagement-driven metrics, and content moderation practices play a significant role in determining which narratives gain visibility within digital spaces. As a result, platforms often prioritize information that generates high interaction over content that promotes critical reflection or substantive public discussion.

Moreover, platform governance mechanisms may disproportionately disadvantage perspectives that challenge dominant institutional narratives, thereby limiting the diversity of viewpoints available in public discourse. From a technocultural perspective, these dynamics show that participation alone does not guarantee equal influence, as platform architectures and broader power relations shape the visibility and legitimacy of information within digital communication systems ([Helmond, 2015](#)).

Furthermore, the investigation underscores that unequal information spaces cannot be understood solely as a matter of individual access to digital technologies. Rather, broader institutional and infrastructural arrangements shape them by influencing how information is produced, circulated, and

legitimized within digital environments. From this perspective, information inequality reflects not only disparities in access but also differences in opportunities to shape public knowledge (Arne et al., 2019). Consequently, the concentration of informational authority among a limited number of actors may constrain the plurality of perspectives necessary for informed public deliberation, thereby limiting the inclusiveness of digital public spheres (Fraser, 1990).

Taken together, these findings demonstrate that technology and culture are deeply intertwined in shaping contemporary information environments. While digital technologies appear to expand access to information and participation, the capacity to influence what is recognized as credible knowledge remains unevenly distributed. This study finds that informational authority is shaped not only by state institutions but also by platform operators, media organizations, and other actors with greater influence over the production, circulation, and legitimization of information. From a technocultural perspective, information inequality emerges not merely from differences in technological access, but from unequal capacities to shape visibility, credibility, and public understanding within digital communication systems. Consequently, digital platforms function not only as channels for information exchange but also as arenas where power, knowledge, and legitimacy are continuously negotiated.

Crisis of Verification and the Fragmentation of Truth

The crisis of verification in the Bjorka case did not emerge merely because of the abundance of information circulating on social media. Rather, it was shaped by the fragmentation of authority over who has the legitimacy to determine the truth status of information. The thematic analysis of official statements, media coverage, digital conversations, and interviews with cyber communities shows that verification did not operate as a linear process from claim to clarification. Instead, verification became an arena of meaning contestation among the state, media, cyber communities, and digital publics. In this arena, information claiming to involve data breaches was not automatically accepted as factual, yet it was also not fully settled when official authorities labeled it a hoax. This situation suggests the central issue was not only the information's validity, but also who the public trusted to define it.

At the state level, responses to data breach claims tended to stabilize meaning through official clarification, *hoax* labeling, and cybersecurity framing. Kominfo, BSSN, and Siber Polri emphasized that some circulating claims could not be understood as new data breaches or did not meet official verification standards. Within the framework of SCOT, this response can be read as a form of *closure and stabilization*, namely an attempt by dominant groups to close interpretative space and establish a meaning considered legitimate (T. Pinch & Bijker, 1984). However, this process of *closure* was not fully successful because digital publics and cyber communities continued to question the transparency of the technical evidence used by state institutions. When clarification was not accompanied by accessible or independently verifiable audits, parts of the public could perceive hoax labeling as a strategy of narrative control.

Cyber communities became important actors in demonstrating that digital verification is no longer monopolized by state institutions. Interviews with *white hacker* communities indicate skepticism in two directions: toward Bjorka's claims, which were not necessarily entirely new or valid, and toward the state's response, which was perceived as too quick to label information without open forensic evidence. This position reveals an important ambivalence: *counter-information* cannot be assumed true, but it also cannot be immediately dismissed as false. It operates as an alternative interpretation that emerges when official verification mechanisms are perceived as insufficiently convincing. Studies on misinformation need to be cautious not to equate all contested information with public misbelief (Altay et al., 2023). In this context, the issue is not only whether the public believes a particular claim, but why the public feels the need to seek verification beyond the state.

This interpretative plurality demonstrates the relevance of *interpretative flexibility* in SCOT. Different social groups can interpret the same data breach claim differently. For the state, such claims are positioned as threats to cybersecurity and informational order. For the media, they become public events with high news value. For cyber communities, they may be read as indicators of weak data governance and the need for technical audits. For parts of the digital public, they are perceived as symbols of the state's failure to protect citizens' data. These differences show that digital truth does not appear as a single category, but is constructed through social relations, institutional interests, technical capacity, and public experience.

Mainstream media also contributed to this fragmentation because of its ambivalent position. On the one hand, the media circulated official clarification and expanded the reach of institutional narratives. On the other hand, media institutions operate within an attention economy that tends to highlight the sensational aspects of data breach claims. As a result, the public often encounters two layers of reality: headlines that create a sense of crisis and articles that contain denials or official clarification. The gap between audience expectations and journalistic practices can weaken the media's position as an epistemic institution (Núñez-Mussa et al., 2025). In the Bjorka case, the media did not merely function as an information channel, but also as an arena that contributed to uncertainty over what should be understood as official information, *hoax*, or *counter-information*.

The fragmentation of truth intensified as information moved through digital spaces that were neither fully public nor fully private. Telegram, digital forums, chat groups, and X allowed information to move rapidly from technical spaces to popular public arenas. The concept of *meso news-spaces* explains how news-related communication can occur between private and public domains, including community channels, group conversations, and semi-closed platforms (Kligler-Vilenchik & Tenenboim, 2024). In such spaces, information gains credibility not only through technical evidence but also because it circulates through trusted networks. Information disorder can also be organized through links, keywords, and search patterns that direct the public toward particular information ecosystems (Rödl & Haider, 2025). Thus, the crisis of verification occurs not only when the public receives information, but also when the public searches for, compares, and interprets it.

Social media prolongs narratives through repetition, memes, satire, comments, and recirculation. Information that is repeated, easy to understand, and aligned with the public's emotional experience tends to resonate more quickly than formal, procedural clarification. This is where the *illusion of truth effect* operates: information that appears repeatedly may seem more credible, even when it lacks a strong evidentiary basis. Digital media can intensify affective polarization because users do not merely consume information; they also evaluate it based on its proximity to their identity, emotions, and social position (Törnberg, 2022). In the Bjorka case, memes and satire were not merely forms of entertainment; they became cultural mechanisms through which counter-narratives continued to circulate in the digital public sphere.

The crisis of verification was also closely linked to declining public trust in institutions. When the state provides clarification without technical evidence the public considers adequate, some users interpret it as defensive. Public trust is shaped not only by the content of clarification, but also by institutional reputation, consistency of communication, and openness of verification procedures. Trust in institutions plays a crucial role in whether the public accepts or rejects official information (Štětka et al., 2025). In this context, the *hoax* label has a dual function: it may protect the public from inaccurate information, but it may also be perceived as an instrument of control when used without transparency and clear accountability mechanisms.

From a technocultural perspective, this case shows that digital technology is not a neutral tool for transmitting information. Digital platforms, algorithms, semi-closed channels, and mainstream media form a communication ecology in which power, affect, and knowledge are produced simultaneously. Certain

digital environments may give rise to alternative knowledge authorities, including through practices of independent searching and the production of *alternative facts* (Marwick & Partin, 2024). In the Bjorka case, such alternative authority was not always grounded in solid evidence, but gained legitimacy because it emerged in a context of distrust toward institutions. This is the central ambivalence of *counter-information*: it can open space for criticism against institutional opacity, but it can also deepen the crisis of verification when it circulates without sufficient evidentiary grounding.

Thus, the crisis of verification in the Bjorka case marks a shift from network society toward a *hyper-information society*. In a network society, connectivity enables information to circulate widely. In a *hyper-information society*, however, the central problem is no longer the lack of access to information, but the overflow of contradictory information that is difficult to verify and produced by competing authorities. Truth no longer moves in a single direction from institutions to citizens; it is contested through interactions among the state, media, cyber communities, digital platforms, and the public. Therefore, the crisis of verification in Indonesia's digital society cannot be reduced to the problem of individual literacy. It is also a problem of *digital governance*: how the state builds transparent verification mechanisms, how the media maintains epistemic accountability, how cyber communities are involved in verification, and how the public is given space to critically assess information without being trapped in the fragmentation of truth.

Digital Literacy as a Policy Solution to Information Disorder

Digital literacy in the Bjorka case cannot be reduced to the individual ability to use digital devices or to identify true and false information in a simple way. The previous analysis shows that the verification crisis emerged from the interaction between *hoax* labeling, official clarification, public skepticism, and the reproduction of narratives across social media. For this reason, *digital literacy* needs to be understood as a public policy instrument that strengthens verification capacity, institutional transparency, and civic participation. Asking citizens to be "more careful" online is not enough. A more substantive approach requires the public to read sources critically, understand context, assess motives, recognize algorithmic influence, and identify power relations behind the circulation of information. This view is consistent with the argument that online information literacy should be treated as a structural issue rather than merely an individual skill (McGrew & Kohnen, 2024).

In the Bjorka case, the central problem was not simply that the public lacked the ability to distinguish accurate information from misleading claims. The deeper issue was the weakening of public trust in information authorities. When the state labeled data-breach claims a *hoax*, parts of the digital public did not automatically accept that clarification because the verification process was perceived as insufficiently transparent. At the same time, cyber communities did not necessarily treat Bjorka's claims as technically valid; instead, they demanded forensic evidence, independent audits, and greater openness in data verification. This situation shows that digital literacy must move toward *critical digital literacy*, which enables citizens to assess information critically without depending entirely on a single authority. Critical literacy also helps citizens understand that digital information is always embedded in social, political, and technological contexts (Polizzi, 2025).

As a policy approach, digital literacy must also help the public distinguish between *hoaxes*, disinformation, and *counter-information*. In this article, *hoax* refers to misleading information or information without sufficient factual grounding, while disinformation refers to intentionally manipulated information. *Counter-information*, however, may emerge as an alternative narrative that challenges official information, especially when the public perceives unequal access to information or limited institutional transparency. This does not mean that *counter-information* should be accepted as truth. It must still be examined through data, transparent methods, and verifiable evidence. This distinction

matters because studies of misinformation often face conceptual problems when they treat all contested information as false (Altay et al., 2023).

The empirical findings show that the state has already developed mechanisms for managing problematic information. Kominfo relies on a layered validation standard involving official sources, mainstream media, and fact-checking channels, while BSSN conducts early detection, verifies content, and recommends action against information considered misleading. BSSN also places digital literacy as a preventive pillar. However, these mechanisms still tend to operate top-down. When the public only receives the final label of *hoax* without access to the verification process behind it, such policy may be interpreted as a closure of meaning rather than an accountable clarification. For this reason, information regulation must pay careful attention to rights, accountability, and freedom of expression so that the governance of misinformation does not become a mechanism for restricting legitimate criticism (Davis & Molitorisz, 2024).

The limitations of a top-down approach are also visible in the state's difficulty in keeping pace with the speed of digital circulation. BSSN acknowledges that verification can be constrained by limited access to affected systems and coordination problems among institutions, while public opinion may already be formed through social media. Under these conditions, *digital literacy* cannot rest solely with individuals. It must become part of *digital governance*, understood as an information governance framework involving multiple actors. The state needs to work with media institutions, cyber communities, academics, civil society organizations, and digital platforms to build a trusted verification ecosystem. Effective media literacy provision requires institutional coordination, sufficient resources, and collaboration with civil society organizations, rather than temporary public campaigns (Polizzi, 2025).

In this context, *participatory verification* becomes essential. The Bjorka case shows that cyber communities have a role that cannot be ignored, particularly when they demand technical evidence, digital audits, and clarification that can be independently tested. This does not mean that cyber communities are always correct. Rather, it indicates the need to open verification processes to actors with technical competence and relative independence. The state can develop public clarification channels through which citizens, journalists, academics, and cyber communities can raise questions, test claims, and obtain technical explanations in accessible language. Such mechanisms may reduce the gap between institutional verification and public perception, while also strengthening trust in information governance.

Media and digital platforms must also be treated as part of digital literacy policy. In the Bjorka case, mainstream media did not merely transmit state clarification; it also shaped public perception through headlines, framing, and issue emphasis. Meanwhile, conversations on Telegram, X, digital groups, and semi-closed spaces accelerated the circulation of narratives that had not yet been fully verified. These spaces show that news-related communication no longer takes place only in open public domains, but also in spaces located between public and private communication, or what has been described as *meso news-spaces* (Kligler-Vilenchik & Tenenboim, 2024). Therefore, digital literacy must include the capacity to understand how media, platforms, algorithms, and social networks shape information visibility. Without this dimension, literacy risks becoming a moral appeal to citizens while leaving the structure of information distribution untouched.

Digital literacy must also be connected to the crisis of institutional trust. When state clarification is perceived as slow, defensive, or insufficiently transparent, the public becomes more vulnerable to alternative narratives that resonate with their emotional experience. In such a situation, digital literacy cannot function effectively without reforms in public communication and institutional openness. Trust in institutions plays a key role in whether the public accepts or rejects official information (Štětka et al., 2025). Thus, digital literacy programs should be accompanied by public communication audits, data transparency, and accountable verification procedures. Citizens need to be trained to examine

information, but institutions must also provide information that can be examined.

In a *hyper-information society*, digital literacy should also focus on slowing information consumption and strengthening verification habits. Information often moves faster than institutions can examine, explain, or correct it. Repetition, virality, *echo chambers*, and the *illusion of truth effect* make frequently repeated information appear more convincing than official clarification that arrives later. For this reason, digital literacy policy should encourage citizens not only to respond quickly to viral information, but also to pause, compare sources, read context, and recognize possible manipulation. Digital literacy oriented toward critical citizenship can strengthen public participation in digital spaces without weakening citizens' capacity for reflection (Costa & Oliver, 2026).

This finding implies that Indonesia's digital literacy agenda should shift from an educational campaign model to a stronger institutional approach to public information governance. First, digital literacy curricula should include understanding algorithms, verifying sources, recognizing digital rights, and distinguishing data-based criticism from misleading information. Second, the state needs to build mechanisms for *participatory verification* through open audits, public clarification channels, and collaboration with cyber communities and academics. Third, media institutions should strengthen epistemic accountability so that news coverage does not intensify uncertainty through sensationalism. Fourth, digital platforms should be encouraged to be more transparent in moderation, recommendation, and content distribution. Fifth, policies addressing *information disorder* must continue to protect freedom of expression so that *hoax* labeling is not used to restrict legitimate criticism. Digital literacy, therefore, is not a single solution. It is part of a broader reform of *digital governance*: a more transparent, participatory, and accountable system for governing public information in the digital age.

5. Conclusion

This study examined how hoax formation and the circulation of counter-information on social media operate as forms of digital counterculture within the frameworks of technoculture and the Social Construction of Technology (SCOT), and how these dynamics shape the emergence of a hyper-information society in Indonesia. The findings indicate that hoax labeling is not merely a mechanism for correcting false information but also functions as a practice of regulating epistemic authority within digital public spaces. The analysis reveals that counter-information emerges from unequal access to information, declining public trust in institutions, and contestation over who has the legitimacy to define truth. Through the Bjorka case, the study demonstrates that state institutions, media organizations, cyber communities, and digital publics construct competing interpretations of the same information, reflecting the interpretative flexibility emphasized by SCOT. These competing interpretations contribute to a crisis of verification in which people assess information not only by factual accuracy but also by trust, repetition, emotional resonance, and networked circulation. The study further shows that digital platforms simultaneously expand opportunities for participation while reproducing inequalities in visibility, legitimacy, and informational influence. As a result, Indonesia's transition toward a hyper-information society is characterized by information abundance, fragmented authority, and ongoing struggles over meaning and credibility. Therefore, strengthening participatory information governance, transparent verification mechanisms, institutional accountability, and critical digital literacy is essential to support a more democratic, inclusive, and trustworthy digital information ecosystem.

6. Recommendations

Based on the findings, public information and cybersecurity authorities in Indonesia should replace unilateral hoax labeling with transparent, evidence-based, and participatory verification mechanisms. In responding to alleged data breaches, official clarifications should disclose the verification criteria, the non-sensitive technical evidence supporting institutional conclusions, the degree of uncertainty involved, and accessible procedures for correction or independent review. Verification processes should involve cybersecurity experts, academics, journalists, civil society organizations, and relevant digital communities to strengthen institutional accountability without compromising data security. Media organizations should diversify their sources and avoid sensational framing, while digital platforms should increase transparency regarding content moderation and algorithmic recommendation systems. Digital literacy policies should also move beyond temporary awareness campaigns by strengthening citizens' abilities to verify sources, understand algorithmic influence, recognize digital rights, and distinguish evidence-based criticism from hoaxes and deliberate disinformation. Given the qualitative, single-case nature of this study, future research should conduct comparative and longitudinal analyses of data breach controversies across institutions and digital platforms. Subsequent studies should also empirically examine the concept of hyper-information society and evaluate whether participatory verification mechanisms can effectively improve public trust, reduce information inequality, and protect legitimate criticism in digital public spaces.

7. References

- Agus Tri Haryanto. (2022). *BSSN Akui Ada Data Valid Dibocorkan Bjorka*. DetikNet.
- Altay, S., Berriche, M., & Acerbi, A. (2023). Misinformation on Misinformation: Conceptual and Methodological Challenges. *Social Media + Society*, 9(1). <https://doi.org/10.1177/20563051221150412>
- Arne, H., Karin, W.-J., & Lina, D. (2019). *Digital Citizenship in a Datafied Society*. Polity Press. <https://doi.org/10.33137/ijidi.v4i2.33335>
- Badan Siber dan Sandi Negara. (2025). *Laporan Keamanan Siber*.
- Bailey, T. C., & Hsieh-Yee, I. (2019). Combating the Sharing of False Information: History, Framework, and Literacy Strategies. *Internet Reference Services Quarterly*, 24(1–2), 9–30. <https://doi.org/10.1080/10875301.2020.1863286>
- Barsky, R. F. (1991). *Language and Symbolic Power*. Harvard University Press. <https://doi.org/10.1215/00267929-52-4-466>
- Basu, S. (2021). Social Reality or Digital Hyperreality: Mapping the “Cyborgian” Present. In *Changing Paradigm in New Media* (pp. 76–89). Nitya Publication.
- Bharali, B., & Goswami, A. L. (2018). Fake news: credibility, cultivation syndrome and the new age media. *Media Watch*, 9(1), 118–130.
- Bijker, W. E. (1995). *Of Bicycles, Bakelites, and Bulbs: Toward a Theory of Sociotechnical Change*. MIT Press.
- Bisnis.com. (2022). *Mahfud MD Klaim Bjorka Tak Mampu Bobol Rahasia Negara*. Bisnis.Com.

- Bollmer, G. D. (2018). *Theorizing digital cultures*. SAGE Publications Ltd.
- Castells, M. (2011). *The Rise of the Network Society* (2nd ed.). Wiley-Blackwell.
- Cazzamatta, R. (2025). Regressive 'alternative' media and their role in disrupting the public spheres in Europe and Latin America. *Publizistik*, 70(1–2), 205–234. <https://doi.org/10.1007/s11616-025-00892-9>
- CNN Indonesia. (2022). *1,3 Miliar Data SIM Card Diduga Bocor di Forum Gelap, Kominfo Bantah*. CNN Indonesia.
- Coleman, G. (2014). *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. Verso Books.
- Cosentino, G. (2020). *Social Media and the Post-Truth World Order: The Global Dynamics of Disinformation*. Palgrave Macmillan.
- Costa, C., & Oliver, M. (2026). Young people and digital literacy learning: co-producing critical citizenship practices. *Pedagogy, Culture & Society*, 34(4), 913–932. <https://doi.org/10.1080/14681366.2025.2593611>
- Creswell, J. W., & Poth, C. N. (2018). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches* (4th ed.). SAGE Publications.
- Davis, M., & Molitorisz, S. (2024). Promoting rights and accountability in the regulation of misinformation. *Australian Journal of Human Rights*, 30(2), 251–278. <https://doi.org/10.1080/1323238X.2025.2466862>
- Del Vicario, M., Bessi, A., Zollo, F., Petroni, F., Scala, A., Caldarelli, G., Stanley, H. E., & Quattrociocchi, W. (2016). The spreading of misinformation online. *Proceedings of the National Academy of Sciences*, 113(3), 554–559. <https://doi.org/10.1073/pnas.1517441113>
- Ehsen, S., & Alam, S. (2021). The influence of digital media on political participation: A study on youth in Pakistan. *Global Media Journal*, 19(36), 1–10.
- Fraser, N. (1990). *Rethinking the public sphere: A contribution to the critique of actually existing democracy*. <https://doi.org/https://doi.org/10.2307/466240>
- Gillespie, T. (2018a). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. Yale University Press. <https://doi.org/10.12987/9780300235029>
- Gillespie, T. (2018b). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. Yale University Press. <https://doi.org/10.12987/9780300235029>
- Habermas, J. (1989). *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*. MIT Press.
- Hardiman, F. B. (1993). *Menuju Masyarakat Komunikatif: Ilmu, Masyarakat, Postmodernisme, dan*

Tantangan Generasi. Kanisius.

- Helmond, A. (2015a). *The Platformization of the Web: Making Web Data Platform Ready*. <https://doi.org/10.1177/2056305115603080>
- Helmond, A. (2015b). *The Platformization of the Web: Making Web Data Platform Ready*. <https://doi.org/10.1177/2056305115603080>
- Intan Rakhmayanti Dewi (CNBC Indonesia). (2022). *Bikin Heboh RI, Data Apa Saja yang Dibocorkan Hacker Bjorka?* CNBC Indonesia.
- Jenkins, H., Ito, M., & boyd, danah. (2015). *Participatory Culture in a Networked Era: A Conversation on Youth, Learning, Commerce, and Politics*. Polity Press.
- Jones-Jang, S. M., Mortensen, T., & Liu, J. (2021). Does Media Literacy Help Identification of Fake News? Information Literacy Helps, but Other Literacies Don't. *American Behavioral Scientist*, 65(2), 371–388. <https://doi.org/10.1177/0002764219869406>
- Juditha, C. (2018a). Hoax Communication Interactivity in Social Media and Anticipation (Interaksi Komunikasi Hoax di Media Sosial serta Antisipasinya). *Journal Pekommas*, 3(1), 31. <https://doi.org/10.30818/jpkm.2018.2030104>
- Juditha, C. (2018b). Interaksi Komunikasi Hoax di Media Sosial serta Antisipasinya. *Jurnal Pekommas*, 3(1), 31–44.
- Kakak Indra Purnama. (2022). *Inilah Deretan Aksi Peretasan yang Dilakukan Hacker Bjorka*. Tempo.Co.
- Kligler-Vilenchik, N., & Tenenboim, O. (2024). Meso News-Spaces and Beyond: News-Related Communication Occurring Between the Public and Private Domains. *Digital Journalism*, 12(5), 565–573. <https://doi.org/10.1080/21670811.2024.2345201>
- Komunitas Etis Keamanan Siber. (2025). *Wawancara Komunitas Etis Keamanan Siber*.
- Komunitas Underground Hacker. (2025). *Wawancara Komunitas Underground Hacker*.
- Lazer, D., Baum, M., Grinberg, N., Friedlan, L., Joseph, K., Hobbs, W., & Mattson, C. (2017). *Combating Fake News: An Agenda for Research and Action*.
- Lim, M. (2018). Roots, Routes, and Routers: Communications and Media of Contemporary Social Movements. *Journalism and Communication Monographs*, 20(2), 92–136. <https://doi.org/10.1177/1522637918770419>
- Llewellyn, A. (2022). *Who is 'Bjorka', the hacker taunting Indonesia's government?* Al Jazeera.
- Marwick, A. E., & Partin, W. C. (2024). Constructing alternative facts: Populist expertise and the QAnon conspiracy. *New Media & Society*, 26(5), 2535–2555. <https://doi.org/10.1177/14614448221090201>
- McGrew, S., & Kohnen, A. M. (2024). Tackling misinformation through online information literacy: Structural and contextual considerations. *Journal of Research on Technology in Education*, 56(1),

1–6.

- Merylina, L. (2017). *Freedom to hate: Social media, algorithmic enclaves, and the rise of tribal nationalism in Indonesia*. <https://doi.org/https://doi.org/10.1080/14672715.2017.1341188>
- Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative Data Analysis: A Methods Sourcebook* (3rd ed.). SAGE Publications.
- Nick, C., & Ulises, A. M. (2019). *The Costs of Connection How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford University Press. <https://doi.org/10.1515/9781503609754>
- Núñez-Mussa, E., Riquelme, A., Valenzuela, S., Aldana, V., Padilla, F., Bassi, R., Campos, S., Providel, E., & Mendoza, M. (2025). The Threat of Misinformation on Journalism's Epistemology: Exploring the Gap between Journalist's and Audience's Expectations when Facing Fake Content. *Digital Journalism*, 13(3), 478–499. <https://doi.org/10.1080/21670811.2024.2320249>
- Ong, J. C., & Tapsell, R. (2022). Demystifying disinformation shadow economies: fake news work models in Indonesia and the Philippines. *Asian Journal of Communication*, 32(3), 251–267. <https://doi.org/10.1080/01292986.2021.1971270>
- Pane, M. D. (2018). Hyperreality of Law Between Hoax and Enforcement of Law No. 19 Year 2016: An Actualization of Technology Shift Law Perspective. *International Conference on Business, Economic, Social Science and Humanities (ICOBEST 2018)*, 13–15.
- Penley, C., & Ross, A. (1991). *Technoculture*. University of Minnesota Press.
- Pinch, T., & Bijker, W. E. (1984). The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other. *Social Studies of Science*. <https://doi.org/10.1177/030631284014003004>
- Pinch, T. J., & Bijker, W. E. (1984). The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other. *Social Studies of Science*, 14(3), 399–441.
- Pinch, T. J., & Bijker, W. E. (2021). The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other. *Social Studies of Science*, 14(3), 399–441.
- Polizzi, G. (2025). Digital literacy and strategic (dis)engagement: examining how functional and critical digital literacy shapes participation. *Information, Communication & Society*, 28(14), 2483–2502.
- Rayner, T. (2018). *Hacker Culture and the New Rules of Innovation*. Routledge.
- Roch, J., Balinhas, D., & Mondon, A. (2026). A critique of the polarisation narrative: expanding the limits of democracy, parties and political participation. *Contemporary Political Theory*, 25(1), 5. <https://doi.org/10.1057/s41296-025-00779-4>
- Rödl, M., & Haider, J. (2025). 'Google this!' How performative links and search engines organise

- information disorders in a climate obstruction network. *Information, Communication & Society*, 28(14), 2462–2482.
- Romagna, M., & Leukfeldt, R. E. (2024). Becoming a hacktivist. Examining the motivations and the processes that prompt an individual to engage in hacktivism. *Journal of Crime and Justice*, 47(4), 511–529. <https://doi.org/10.1080/0735648X.2023.2216189>
- Shaw, D. B. (2008). *Technoculture: The Key Concepts*. Berg Publishers.
- Štětka, V., Brandao, F., Mihelj, S., Tóth, F., Hallin, D., Rothberg, D., Ferracioli, P., & Klimkiewicz, B. (2025). Have people 'had enough of experts'? The impact of populism and pandemic misinformation on institutional trust in comparative perspective. *Information, Communication & Society*, 28(6), 1039–1060. <https://doi.org/10.1080/1369118X.2024.2413121>
- Sudibyo, A. (2021). *Tarung Digital: Propaganda Komputasional di Berbagai Negara*. Kepustakaan Populer Gramedia (KPG).
- Tandoc, E. C., Lim, Z. W., & Ling, R. (2018). Defining "Fake News." *Digital Journalism*, 6(2), 137–153. <https://doi.org/10.1080/21670811.2017.1360143>
- Tapsell, R. (2021). Disinformation and Cultural Practice in Southeast Asia. In *Disinformation and Fake News* (pp. 91–101). Springer Singapore. https://doi.org/10.1007/978-981-15-5876-4_7
- Törnberg, P. (2022). How digital media drive affective polarization through partisan sorting. *Proceedings of the National Academy of Sciences*, 119(42). <https://doi.org/10.1073/pnas.2207159119>
- Treré, E. (2018). *Hybrid Media Activism*. Routledge. <https://doi.org/10.4324/9781315438177>
- Voice of Indonesia (Corporate Author). (2022). *Ternyata Begini Cara Hacker Bjorka Sulit Dilacak Pemerintah*. Voice of Indonesia (VOI).
- Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380), 1146–1151. <https://doi.org/10.1126/science.aap9559>
- Wirman, W., & Sari, G. G. (2020). Hiperealitas Media pada Pemilihan Umum Indonesia Tahun 2019. *Communicology: Jurnal Ilmu Komunikasi*, 8(1), 84–94.
- Zollo, F., Bessi, A., Del Vicario, M., Scala, A., Caldarelli, G., Shekhtman, L., Havlin, S., & Quattrociocchi, W. (2017). Debunking in a world of tribes. *PLOS ONE*, 12(7), e0181821. <https://doi.org/10.1371/journal.pone.0181821>