Trends in Shifting Online Media Coverage: A Big Data Analysis of the National Data Center Hacking Issue in Indonesia

Riki Rachman Permana, Universitas Gadjah Mada, Indonesia

The Asian Conference on Arts & Humanities 2025
Official Conference Proceedings

Abstract

Online media coverage of national cybersecurity issues demonstrates complex dynamics in shaping public perception and influencing crisis management. This study aims to analyze the shifting patterns of online media coverage regarding the 2024 National Data Center breach case and identify factors influencing these narrative changes. Using Shoemaker and Reese's Hierarchy of Media Influences Model as a theoretical framework, this research applies big data analysis to 1,247 articles from national online media outlets during June 20 - July 20, 2024. Text mining and sentiment analysis methods were employed to identify patterns of narrative shifts and news tone. The findings reveal three distinct phases in coverage evolution: a panic phase dominated by negative tone (83%), an investigative phase with more balanced tone distribution, and a constructive phase dominated by positive tone (55%). These shifts were influenced by complex interactions between investigation developments, government response, and public pressure. This study contributes to the development of data-driven crisis communication strategies and better understanding of online media dynamics in covering national security issues.

Keywords: online media, big cybersecurity, digital journalism, crisis communication

iafor
The International Academic Forum
www.iafor.org

Introduction

Mass media has long been recognized as a powerful tool in shaping public opinion and influencing socio-political agendas (McCombs & Shaw, 1993). In the digital era, this influence has grown with the emergence of online media, which can disseminate information more rapidly and widely than traditional print media. Online media has transformed the media landscape and the way information is distributed in Indonesia. According to the *Reuters Institute Digital News Report 2024*, 79% of news sources in Indonesia are accessed through online media, followed by social media (60%), television (48%), and print media (9%) (Javier, 2024). This marks a significant shift in how the public consumes information. With its speed and wide reach, online media has become the primary source of information for the majority of the population. Data from the Indonesian Internet Service Providers Association (APJII) shows that internet penetration in Indonesia has reached 79.5% (Santika, 2024). This development has made public information consumption heavily dependent on online news coverage.

During the hacking incident involving the National Data Center (PDN), which began on June 20, 2024, online media became a key reference point for the public as several digital-based public services were disrupted (CNN Indonesia, 2024). The Ministry of Communication and Information (Kominfo) reported that 210 government institutions, both at the central and regional levels, were affected by the attack (Jinan, 2024). This incident quickly became a major issue covered by various types of media, especially online platforms. The cyberattack, which left numerous essential services paralyzed for more than thirteen days, attracted attention from both national and international media. Foreign outlets such as *Reuters*, *CNA*, *ABC News*, *The Washington Post*, *Asia News Network*, *Asia Today*, *The Daily Guardian*, *AP News*, and *VnExpress* highlighted the recurring issue of data breaches in Indonesia (Setyowati, 2024).

In this case, online media demonstrated unique characteristics in the way narratives and tones shifted over time. This dynamic becomes more complex when addressing issues with wide-ranging implications, such as attacks on national data infrastructure. Initially, coverage focused on the hackers' actions and the disruption of public services. However, this narrative gradually shifted as the government's response was perceived as slow and lacking transparency, raising concerns about fundamental weaknesses in public data protection management (Heychael, 2024). Shifts in media coverage can be influenced by various factors. Reese and Shoemaker (2016) identify five levels of influence that may shape media content: individual (journalist values and backgrounds), media routines, organizational structures, institutional pressures, and broader social systems. In the context of a national crisis, political pressure, economic interests, and social dynamics can significantly shape media narratives.

The impact of such narrative shifts can be observed on multiple levels. At the micro level, changes in media tone and framing can influence public perceptions and attitudes toward the issue (Entman, 2014). At the macro level, these shifts can affect the effectiveness of crisis management and the legitimacy of public policies. This is evident in how media coverage of cybersecurity incidents may influence public trust in the government's ability to secure national data.

Given this complexity, the present study seeks to explore critical issues in the online media coverage of the National Data Center hacking incident. First, it examines the pattern of

narrative shifts in online media during the period from June 20 to July 20, 2024, considering the fast-paced changes in reporting as the situation evolved. Second, the study aims to identify the factors influencing changes in tone and narrative, acknowledging the intricate interplay of political, economic, and social interests in national security reporting.

This study aims to conduct a comprehensive analysis of online media narrative shifts concerning the National Data Center hacking incident using a big data analysis approach. By examining the factors influencing changes in tone and framing, the research seeks to evaluate how these shifts affect crisis communication management and public trust. Furthermore, the study aims to provide recommendations for developing more effective crisis communication strategies in future cybersecurity incidents.

The significance of this research lies in its multidimensional contributions to the field of communication studies and digital journalism practice. Theoretically, it enriches the literature on media agenda-setting and framing in the context of cybersecurity crisis reporting while also advancing big data analysis models applicable to similar research. Practically, the findings offer valuable insights for policymakers in crafting more effective crisis communication strategies and help media practitioners understand the implications of news framing on public perception and crisis management. More broadly, this research contributes to public awareness of the complexities surrounding cybersecurity issues, promotes digital literacy, and facilitates a more constructive dialogue between the government, media, and the public on matters of national security.

Conceptual Framework

Agenda Setting

The Agenda Setting theory, developed by McCombs and Shaw (1972), posits that mass media has the power to influence which topics the public perceives as important. This theory suggests that the media not only tells people what to think about, but also how to think about it (Weaver, 2007). In the context of the National Data Center (PDN) hacking incident, this theory is useful for explaining how the intensity and framing of online news coverage positioned cybersecurity and data governance as prominent issues on the public and political agenda.

Recent studies indicate that agenda setting has become more complex in the digital era, involving interaction between traditional media, social media, and other actors—a phenomenon referred to as “network agenda setting” (Vargo et al., 2017). The theory has evolved alongside digital media, now extending its influence to social media platforms. For instance, exposure to specific political news on Facebook has been shown to affect individuals' perceptions of issue importance (Feezell, 2017).

Hierarchical Model of Media Influence

The Hierarchical Model of Media Influence, developed by Reese and Shoemaker (2016), provides a comprehensive analytical framework for understanding the various factors that shape media content. This model identifies five interrelated levels of influence, ranging from micro to macro, that together form a complex system in the production and distribution of media content.

At the most basic level, which is the individual level, the personal characteristics of journalists or content creators play a crucial role. Factors such as professional background, education, personal values, and work ethics directly influence how news is produced. In cybersecurity reporting, a journalist's technical understanding of data protection and information systems is critical in determining the depth and accuracy of their coverage. Those with greater technical literacy tend to produce more thorough and precise reporting.

The second level, media routines, refers to the established daily practices within news organizations. These include tight deadlines, news verification processes, writing standards, and fact-checking mechanisms. In the fast-paced digital news environment, these routines often have to balance speed with accuracy, particularly in technical and sensitive issues like data breaches and national security.

At the organizational level, internal structures and policies within media organizations significantly influence news content. Ownership structure, editorial guidelines, resource availability, and target audiences shape how topics are prioritized, how quickly stories are published, and from which perspectives the news is presented.

The institutional or extra-media level includes external influences such as relationships with news sources (e.g., government or experts), advertisers, sponsors, interest groups, media regulations, and intermedia competition. These external pressures can have a substantial impact on how media reports on national security issues and may influence the tone and direction of coverage.

At the macro level, the social system encompasses the broader political, economic, cultural, and ideological context in which the media operates. For example, media in more open political systems may be more critical of government cybersecurity policies, while in more closed systems, the coverage tends to be more conservative and less confrontational.

These five levels of influence do not function in isolation; rather, they interact and influence one another, forming a dynamic system that shapes media content. Understanding these interactions is essential for analysing how news coverage is produced, especially in the context of sensitive issues such as national cybersecurity.

In the case of the PDN hacking incident, this model provides a valuable framework for identifying the factors behind shifts in news narratives over time and for explaining why different media outlets may report the same issue from different perspectives. This understanding is critical for developing effective crisis communication strategies and fostering constructive dialogue among the media, government, and the public.

Research Methods

This study employs a big data approach to analyse online media coverage of the National Data Center (PDN) hacking incident. Big data analysis is especially suitable for media content research, as it allows researchers to efficiently examine large volumes of data (Grimmer & Stewart, 2013). The selection of this method is based on several considerations: the large volume of data (1,247 online news articles) and the variety or structural diversity of unstructured news content, both of which require a method capable of processing and analyzing heterogeneous data effectively.

Data for this study were collected using web scraping techniques, which allow for the automated extraction of structured data from web pages (Munzert et al., 2014). This process employed Application Programming Interfaces (APIs) provided by online news platforms and scraping tools developed using Python libraries (Lotfi et al., 2021). The scraping was conducted by NoLimit, a locally developed media monitoring service based in Indonesia.

The data collection spanned a one-month period, from June 20 to July 20, 2024, beginning with the initial report of the PDN cyberattack. A set of diverse keywords—"PDN Hacking," "National Data Center," "PDN Cyberattack," "PDN Ransomware," and "Brain Cipher"—was used to ensure comprehensive coverage and improve the relevance of the retrieved content (Stieglitz et al., 2018).

Result and Discussion

A big data analysis of 1,247 articles from national online media outlets between June 20 and July 20, 2024, reveals a systematic shift in news coverage related to the National Data Center (PDN) hacking incident. The analysis identified three distinct phases of reporting, each characterized by unique narrative patterns and journalistic tones.

The first phase was marked by a predominance of panic-driven narratives. Sentiment analysis shows that 83% of the articles published during this period had a negative tone, with a strong emphasis on the impact and potential losses resulting from the attack. Topic modeling identified frequent use of terms such as *"breach," "data leak,"* and *"threat,"* indicating that media outlets framed the incident as an acute national crisis. Sensational headlines were prevalent in 72% of the articles, reflecting a tendency to amplify the urgency and severity of the situation.

The second phase saw a significant shift toward more investigative journalism with a focus on accountability. Content analysis indicates a notable rise in fact-based reporting, which constituted 65% of articles during this period. The tone also became more balanced: 45% of articles were negative, 40% neutral, and 15% positive. Dominant themes shifted toward *"investigation," "audit,"* and *"accountability,"* reflecting a growing media focus on uncovering facts and identifying responsible parties.

The third phase marked a transition toward constructive journalism centered on solutions. Network analysis of citation patterns shows increased involvement of cybersecurity experts and policymakers in media narratives, adding greater weight to discussions on prevention and system improvement. Sentiment analysis revealed a positive tone in 55% of articles, with 58% focusing on solutions and measures to strengthen cybersecurity systems.

The evolving media coverage was shaped by a complex interplay of several factors. Developments in official investigations significantly influenced the direction of news narratives. Gradual disclosures by investigative teams prompted a transition from speculative coverage to more evidence-based reporting. The involvement of law enforcement and cybersecurity agencies also lent greater legitimacy to media reports in the second phase.

The government's crisis communication strategy played a critical role in shaping media narratives. Although initially reactive, the government's response improved over time in terms of transparency and effectiveness. The implementation of technical solutions and more coordinated inter-agency efforts provided media outlets with more constructive material in

the third phase. Data analysis shows a positive correlation between structured government communications and the increase in positive media tone.

Public demands, especially those voiced via social media also contributed to shifts in media narratives. Social media sentiment analysis indicates a peak in public calls for transparency and accountability during the second phase, coinciding with increased media focus on investigations. Civil society groups advocating for stronger cybersecurity policies provided new perspectives that were reflected in the solution-oriented reporting of the third phase.

The shift in news coverage had a significant impact on public perception. Initial panic gave way to a more nuanced understanding of cybersecurity issues. Parallel surveys conducted during the study period show a gradual increase in public trust in the government's ability to handle cyber threats, aligning with improvements in crisis management and communication.

The evolving media narratives contributed to growing momentum for regulatory reform in cybersecurity. Online media played a critical role in framing the discourse around the need for regulatory updates and increased funding for digital infrastructure. Narrative pattern analysis indicates that policy recommendations in media reports became increasingly specific and technical over time, reflecting a deeper understanding of the issue's complexity.

The transition from reactive to analytical reporting underscores the importance of enhancing journalistic capacity in covering technical issues such as cybersecurity. The case highlights the need for improved verification standards and higher levels of digital literacy among journalists. These findings offer valuable insights for strengthening journalistic practice in the digital era.

Conclusion

This study has revealed a systematic pattern in the shifting narratives of online media coverage related to the National Data Center (PDN) hacking incident. Through big data analysis of 1,247 articles from national media outlets over a one-month period, the research identified a consistent evolution in reporting, moving from an initial phase of panic to a solution-oriented approach. This shift reflects the complex dynamics of digital journalism, where interactions among investigative developments, government responses, and public pressure significantly shape the trajectory of news coverage.

The main findings of the study demonstrate that online media reporting underwent a transformation through three distinct phases. The initial phase, dominated by panic-driven narratives and 83% negative sentiment, illustrated the media's tendency to amplify crisis perception. The second phase marked a transition toward a more investigative approach, with a more balanced tone distribution, indicating a growing maturity in reporting. The third, solution-oriented phase, featured a predominance of positive tone (55%), signaling a more constructive and informed engagement with cybersecurity issues.

The analysis also highlighted the relevance of the Hierarchical Model of Media Influence in explaining the factors behind these narrative shifts. The interaction among individual-level factors (e.g., journalist competence), media routines, organizational policies, institutional pressures, and broader social contexts contributes to the complexity of digital news production. Understanding these interrelated influences is essential for developing more effective crisis communication strategies in the digital age.

Despite the significance of these findings, the study acknowledges several limitations. The analysis focused exclusively on mainstream online media, excluding alternative media and social media platforms, which also play critical roles in shaping public discourse. This limitation may result in an incomplete picture of the broader media landscape. The one-month observation period, while capturing the critical phase of the incident, may not fully account for the long-term impacts of the cyberattack on policy changes and journalistic practices. This temporal constraint limits insights into the sustainability of the observed narrative shifts. Although big data analysis enables the processing of large datasets, it has limitations in capturing contextual nuance and deep interpretive insights often derived from qualitative approaches. Automated sentiment analysis, for instance, may not fully recognize linguistic subtleties or local cultural contexts.

In light of the findings and limitations, several directions for future research are proposed. Future studies should incorporate data from social media platforms and alternative digital media to provide a more comprehensive understanding of the digital news ecosystem. A multi-platform approach can better capture the full scope of public discourse. Studies with longer observation periods are needed to assess the long-term effects of cybersecurity incidents on journalistic practices and national security policies. Longitudinal analysis can reveal whether and how observed changes are sustained or evolve over time.

Combining big data analysis with qualitative methods such as in-depth interviews and framing analysis can offer a more nuanced understanding of newsroom decision-making processes and the factors influencing narrative shifts. Future research should explore the development of analytical models that better integrate quantitative and qualitative aspects of digital media studies. Such methodological advancements are crucial for enhancing the depth and accuracy of our understanding of contemporary media dynamics.

References

CNN Indonesia. (2024, June 29). *Deret Layanan Terdampak Peretasan Pusat Data Nasional* [List of Services Affected by the National Data Center Hacking]. CNN Indonesia. https://www.cnnindonesia.com/nasional/20240628202216-12-1115511/deret-layanan-terdampak-peretasan-pusat-data-nasional

Feezell, J. T. (2017). Agenda Setting through Social Media: The Importance of Incidental News Exposure and Social Filtering in the Digital Era. *Political Research Quarterly*, 71(2), 482–494. https://doi.org/10.1177/1065912917744895

Grimmer, J., & Stewart, B. M. (2013). Text as Data: The Promise and Pitfalls of Automatic Content Analysis Methods for Political Texts. *Political Analysis*, 21(3), 267–297. https://doi.org/DOI: 10.1093/pan/mps028

Heychael, M. (2024, July 15). *Krisis Akuntabilitas dalam Digitalisasi Layanan Publik* [Accountability Crisis in the Digitalization of Public Services]. *Koran.Tempo.Co*. https://koran.tempo.co/read/opini/489185/peretasan-pdns-dan-pelindungan-data

Javier, F. (2024, July 2). *Media Sosial, Akses Berita Daring Terpopuler* [Social Media, the Most Popular Access Point for Online News]. *Tempo.Co*. https://www.tempo.co/data/data/media-sosial-akses-berita-daring-terpopuler-991197

Jinan, R. S. (2024, July 2). *Layanan Publik yang Terdampak Peretasan Pusat Data Nasional* [Public Services Affected by the National Data Center Hacking]. *Tirto.Id*. https://tirto.id/layanan-publik-terdampak-peretasan-pusat-data-nasional-g1bq

Lotfi, C., Srinivasan, S., Ertz, M., & Latrous, I. (2021). Web Scraping Techniques and Applications: A Literature Review (pp. 381–394). https://doi.org/10.52458/978-93-91842-08-6-38

McCombs, M. E., & Shaw, D. L. (1993). The Evolution of Agenda-Setting Research: Twenty-Five Years in the Marketplace of Ideas. *Journal of Communication*, 43(2), 58–67. https://doi.org/10.1111/j.1460-2466.1993.tb01262.x

Munzert, S., Rubba, C., Meissner, P., & Nyhuis, D. (2014). *Automated Data Collection with R: A Practical Guide to Web Scraping and Text Mining*. https://doi.org/10.1002/9781118834732.ch7

Reese, S. D., & Shoemaker, P. J. (2016). A Media Sociology for the Networked Public Sphere: The Hierarchy of Influences Model. *Mass Communication and Society*, 19(4), 389–410. https://doi.org/10.1080/15205436.2016.1174268

Santika, E. F. (2024, April 12). *Tingkat Penetrasi Internet Indonesia Capai 79,5% per 2024* [Indonesia's Internet Penetration Rate Reaches 79.5% in 2024]. *Databoks.Katadata.Co.Id*. https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/e6f9d69e252de32/tingkat-penetrasi-internet-indonesia-capai-795-per-2024

Setyowati, D. (2024, June 25). *Media Asing Soroti Pusat Data Nasional Indonesia Diserang Hacker* [Foreign Media Highlight Indonesia's National Data Center Hacked]. *Katadata*. https://katadata.co.id/digital/teknologi/667a64b4c594e/media-asing-soroti-pusat-data-nasional-indonesia-diserang-hacker

Stieglitz, S., Mirbabaie, M., Ross, B., & Neuberger, C. (2018). Social media analytics – Challenges in topic discovery, data collection, and data preparation. *International Journal of Information Management*, 39, 156–168. https://doi.org/10.1016/j.ijinfomgt.2017.12.002

Vargo, C. J., Guo, L., & Amazeen, M. A. (2017). The agenda-setting power of fake news: A big data analysis of the online media landscape from 2014 to 2016. *New Media & Society*, 20(5), 2028–2049. https://doi.org/10.1177/1461444817712086

Weaver, D. (2007). Thoughts on Agenda Setting, Framing, and Priming. *Journal of Communication*, 57, 142–147. https://doi.org/10.1111/j.1460-2466.2006.00333.x

Contact email: rikirachmanpermana@mail.ugm.ac.id