

**THE COMPARATIVE RHETORICAL STRATEGIES IN
INDONESIAN NEWS OF KOMINFO DATA BREACH 2024
THESIS**

By:

LUKIS HERLAMBAH SYAHPUTRA

NIM 19320218



**DEPARTMENT OF ENGLISH LITERATURE
FACULTIES OF HUMANITIES
UNIVERSITAS NEGERI MAULANA MALIK IBRAHIM
MALANG
2025**

**THE COMPARATIVE RHETORICAL STRATEGIES IN
INDONESIAN NEWS OF KOMINFO DATA BREACH 2024**

THESIS

Presented to Universitas Islam Negeri Maulana Malik Ibrahim Malang
in Partial Fulfillment of the Requirements for the Degree of Sarjana
Sastra (S.S)

By:

LUKIS HERLAMBAANG SYAHPUTRA

NIM 19320218

Advisor:

Dr. AGUS EKO CAHYONO, S.Hum., M.Pd

NIP. 198208112011011008



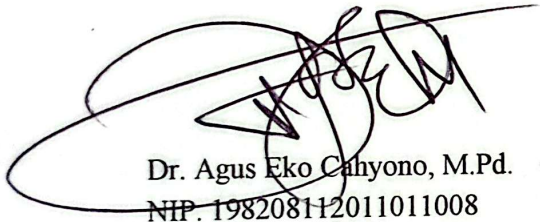
**DEPARTMENT OF ENGLISH LITERATURE
FACULTIES OF HUMANITIES
UNIVERSITAS NEGERI MAULANA MALIK IBRAHIM
MALANG
2025**

APPROVAL SHEET

This is to certify that Lukis Herlambang Syahputra's thesis entitled "**The Comparative Rhetorical Strategies In Indonesia News Of Kominfo Data Breach 2024**" has been approved for thesis examination at Faculty of Humanities, Universitas Islam Negeri Maulana Malik Ibrahim Malang, as one of the requirements for the degree of Sarjana Sastra (S.S.).

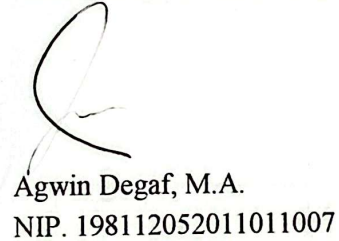
Malang, 23 September 2025

Approved by
Advisor,



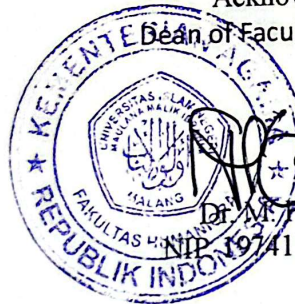

Dr. Agus Eko Cahyono, M.Pd.
NIP. 198208112011011008

Head of Department of English Literature,



Agwin Degaf, M.A.
NIP. 198112052011011007

Acknowledged by,
Dean of Faculty of Humanities,



Dr. M. Faisol, M.Ag.
NIP. 197411012003121004

STATEMENT OF AUTHORSHIP

I state that the thesis entitled “The Comparative Rhetorical Strategies in Indonesian News of Kominfo Data Breach 2024” is my original work. I do not include any materials previously written or published by another person, except those cited as references and written in the bibliography. Hereby, if there is any objection or claim, I am the only person who is responsible for that.

Malang, 23 Desember 2025
The Researcher,



Lukis Herlambang Syahputra
NIM. 19320218

LEGITIMATION SHEET

This is to certify that Lukis Herlambang Syahputra thesis entitled **The Comparative Rhetorical Strategies In Indonesia News Of Kominfo Data Breach 2024** has been approved by the Board of Examiners as one of the requirements for the degree of Sarjana Sastra (S.S.) in Department of English Literature.

Malang,
22 ~~December~~2025
Signatures

Board of Examiners

1. Dr. Lina Hanifiyah, M.Pd

NIP. 198108112014112002

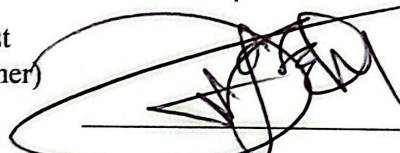
(Chair)



2. Dr. Agus Eko Cahyono, M.Pd

NIP. 198208112011011008

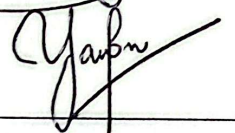
(First Examiner)



3. Dr. Yayuk Widyastuti Herawati, M.Pd

NIP. 197705032014112002

(Second Examiner)



Approved by,

Dean of Faculty of Humanities



Dr. M. Faisol, M.Ag.

NIP. 19741101200312003

MOTTO

“Being late at start, doesn’t mean everything will result in failure. Keep your focus, steady, and aim to get better result, everyone might said “it’s okay to fail at your first attempt, keep trying” that’s an okay, but will lose one of your chance. Now, what if your chance only once? Please becarful with that”

DEDICATION

I dedicate my thesis to:

My beloved parents.

My friends which helping me in struggle.

My best friend, Unggul, which helped me finish through emotional support.

ACKNOWLEDGMENTS

First and foremost, all praise and gratitude be to Allah Subhanahu wa Ta'ala for His endless mercy and blessing, which able to made this thesis entitled “ *The Comparative Rhetorical Strategies in Indonesia News of Kominfo Data Breach 2024*” Peace and blessing may be upon Prophet Muhammad صلى الله عليه وسلم, for the guidance to the bright future of Islam as have been seen now.

Secondly, I would like to express heartfelt thanks to all parties who have helped complete this thesis and a special thanks go to Dr. Agus Eko Cahyono, M.Pd., who helped me finish the thesis from the beginning until it is fully completed. Thanks for the guidance for making the thesis be completed through many questions which being asked a lot. May Allah Subhanahu wa Ta'ala will help you in each step you take in life which help people a lot not only for me, but also everyone, all people which you beloved.

I am also profoundly grateful to my beloved parents for their unwavering financial and emotional support. Thanks to all people who helped me finish the thesis from nothing, especially my close friend. Fitra which helped me a lot in many from consulting on the progress up to supporting emotionally through invitation for hanging out to drink a coffee outside, or taking sport activity like jogging and stuff that helped me to keep my body in check. Also not forgetting for my best friend from Junior High until now, Unggul, for helping me keeping my emotion being stable, for not stressing out finishing the thesis through invitation in playing games a lot and thanks for the gift of one that game we used to play, will save it for sure.

Lastly, I realize that this thesis is far from perfect. Therefore, with an open heart, I welcome constructive criticism and suggestions for future improvement. May this thesis provide some benefit and serve as a small contribution to the development of knowledge, particularly in the field of Linguistics.

Malang, 23 September.....2025



Lukis Herlambang Syahputra
NIM. 19320218

ABSTRACT

Syahputra, Lukis Herlambang (2025). *THE COMPARATIVE RHETORICAL STRATEGIES IN
INDONESIAN NEWS OF KOMINFO DATA BREACH 2024* Undergraduate Thesis.
Department of English Literature, Faculty of Humanities, Universitas Islam Negeri Maulana
Malik Ibrahim Malang. Advisor, Dr. Agus Eko Cahyono, M.Pd.

Keywords: cybersecurity, media framing, critical discourse analysis, ideological discourse,
ransomware

This study explores how Indonesian media discourse frames the 2024 ransomware attack on the Temporary National Data Center (PDNS), which disrupted over 200 public services and raised widespread concerns about state cybersecurity and public trust. Using critical discourse Analysis of CDA), the study compares news coverage from VOI News and *The Jakarta Post*, employing theoretical frameworks from Teun A. van Dijk, Norman Fairclough, Theo van Leeuwen, and Robert Entman to analyze macrostructures, microstructures, and ideological framing. The findings reveal stark contrasts in media representation: VOI News adopts a developmentalist frame that portrays the incident as an “important lesson,” emphasizing institutional learning, depersonalized responsibility, and optimism. In contrast, *The Jakarta Post* employs a crisis framing approach, highlighting systemic vulnerability, bureaucratic opacity, and the moral tension of the government's refusal to negotiate with cybercriminals. These divergent narratives illustrate how media function as ideological instruments that shape public understanding, institutional credibility, and policy discourse. While the study provides insight into media's role in constructing cybersecurity narratives, it is limited by its narrow media sample, short-term focus, and lack of audience reception data. Future research is encouraged to incorporate a wider media landscape, longitudinal data, and cross-national comparisons to deepen understanding of how digital crises are mediated in contemporary societies.

ABSTRAK

Syahputra, Lukis Herlambang (2025). *STRATEGI RETORIKA KOMPARATIF DALAM PEMBERITAAN PEMBOBOLAN DATA KOMINFO 2024 DI INDONESIA*, Undergraduate Thesis. Program studi Sastra Inggris, Fakultas Humaniora, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Advisor, Dr. Agus Eko Cahyono, M.Pd.

Keywords: *keamanan siber, pembungkahan media, analisis wacana kritis, wacana ideologis, ransomware*

Penelitian ini mengeksplorasi bagaimana wacana media Indonesia membingkai serangan ransomware tahun 2024 terhadap Pusat Data Nasional Sementara (PDNS), yang mengganggu lebih dari 200 layanan publik dan menimbulkan kekhawatiran yang meluas tentang keamanan siber negara dan kepercayaan publik. Dengan menggunakan analisis wacana kritis (CDA), penelitian ini membandingkan liputan berita dari VOI News dan The Jakarta Post, dengan menggunakan kerangka teori dari Teun A. van Dijk, Norman Fairclough, Theo van Leeuwen, dan Robert Entman untuk menganalisis struktur makro, mikro, dan pembungkahan ideologis. Temuan-temuannya mengungkapkan perbedaan yang mencolok dalam representasi media: VOI News mengadopsi bingkai developmentalis yang menggambarkan insiden tersebut sebagai “pelajaran penting”, menekankan pembelajaran institusional, tanggung jawab yang didepersonalisasi, dan optimisme. Sebaliknya, The Jakarta Post menggunakan pendekatan pembungkahan krisis, menyoroti kerentanan sistemik, ketidakjelasan birokrasi, dan ketegangan moral akibat penolakan pemerintah untuk bernegosiasi dengan penjahat siber. Narasi-narasi yang berbeda ini menggambarkan bagaimana media berfungsi sebagai instrumen ideologis yang membentuk pemahaman publik, kredibilitas institusi, dan wacana kebijakan. Meskipun penelitian ini memberikan wawasan tentang peran media dalam membangun narasi keamanan siber, penelitian ini dibatasi oleh sampel media yang sempit, fokus jangka pendek, dan kurangnya data penerimaan audiens. Penelitian di masa depan didorong untuk memasukkan lanskap media yang lebih luas, data longitudinal, dan perbandingan lintas negara untuk memperdalam pemahaman tentang bagaimana krisis digital dimediasi dalam masyarakat kontemporer.

Table of Contents

STATEMENT OF AUTHORSHIP	i
APPROVAL SHEET	ii
LEGITIMATION SHEET.....	iii
MOTTO	iv
DEDICATION	v
ACKNOWLEDGMENTS	vi
ABSTRCT	vii
ABSTRAK	viii
CHAPTER I.....	1
INTRODUCTION.....	1
A. Background of the Research.....	1
B. Research questions	5
C. Significance of the Research	6
D. Scope and Limitations.....	6
E. Definition of Key Terms	6
CHAPTER II	10
LITERATURE REVIEW	10
A. Critical Discourse Analysis	10
B. Micro and Macro structures.....	12
C. Actor representation.....	15
D. News in Discourse.....	16
E. Fairclough three-dimensional Structure	16
F. Media Framing	17
CHAPTER III.....	20
RESEARCH METHODE.....	20
A. Research Design.....	20
B. Data and Data Source	21
C. Data Collection.....	21
D. Data Analysis.....	22

CHAPTER IV	24
FINDINGS AND DISCUSSIONS	24
A. Findings	24
B. Discussion.....	75
CHAPTER V	81
CONCLUSION AND SUGGESTION	81
A. CONCLUSION	81
B. SUGGESTION	82
REFERENCES	84
APPENDIX	87

CHAPTER I

INTRODUCTION

This chapter discuss the research problem's discussion, containing background of the research, research questions, significance of the researchscope and limitation, and definition of key terms.

A. Background of the Research

In this digital age, technologies have become part of people's life in managing their daily life in such of doing job or work, asisting an individual or group of people as in company or organization owned by person or working alone whenever doing job or just taking part of some. Sometimes, can be used as a place to store an information or data from an individual or organizations that may, contain, another people's data as such information from the company of the company that contain their buyer's personal data, information, that is not publicly accessed, and a lot of them rely on this data storage because of its reliability and mobility, which can be accessed easily without managing documents (paper) that contain a lot of time. However, this dependency has led to growing concerns about cybersecurity, which plays a huge role in defending the data from being leaked or stolen by certain individuals or groups. Over the past years, concerns about cybersecurity have been an issue since a lot of cases from 2024 have already been attacked, including those involving the Indonesian government.

In recent cases in June, 2024, VOI mentioned that Indonesia government has been addressed as being victim in recent hijacking of the data in PDNS, that

shows a result of a lot of data is being leaked (VOI, 2024). The cause, Reuters mentioned that, the Windows Defender in the server is being disabled causing the ransomware to enter and lock a lot of confidential data, and demanding a ransom money for recovery (Reuters, 2024) causing a widespread of insecurity and lowering people trust over the government. But still, the government shift the blame to the public (people) instead of acknowledging systemic failure over the case instead of taking responsibility. The authorities believe that the cause is in citizen's lack of cybersecurity awareness. Thus, it raises questions about responsibility over government action in securing the national data.

This study aims to analyze how Indonesian local news presents the information and show any framing that might appear in the research about data breaches through Critical Discourse Analysis by Van Dijk (1980), Fairclough (1989), and Entman (1993). Media presentation plays a huge role in shaping public opinion and trust through framing narratives that may, manipulate, the reader of the news. Van Dijk (2015) mentioned that CDA explores how social power abuse, shows dominance, and inequality are reproduced through discourse. By analyzing the media report or presentation, this research will uncover potential biases, ideology of the news media, and what strategies used to shape public opinion about cybersecurity and government accountability.

Discourse analysis considers not only as the linguistic aspects, in this case as the aspect of the articles, but also considered as sociocognitive framework that connects language to social beliefs. News representation can create a polarization, evoke emotion, or legitimize a certain actions as example being shown by

Kompas.com in 2020 about the misinformation during the COVID-19 crisis in Indonesia (Konpas.com, 2020) that cause a confusion in public and resulting of getting distrust over the people. Through analyzing critically the media represented from the case of data leak in 2024 from VOI and The Jakarta Post, this study seeks to determine whether a manipulative strategies is being used in the analyzed news related the issue of Indonesian PDNS server being hijacked or leaked.

The Ministry of Communication and Information is responsible for formulating national policies on cybersecurity, telecommunications, and digital infrastructure, specifically for a particular server. Given its role, it should ensure transparency regarding data leaks and take responsibility if the cause is internal, rather than quickly blaming citizens for a lack of cybersecurity. This resesarch, after analyzing the linguistic strategies used in the articles then, investigate how media potrays the institution's role in handling the data breaches, and assessing whether the news coverage aligns with accountability or deflects the responsibility.

Being critical is essential in preventing misinformation and misinterpretation about the case, and it will also help to realize biased narratives from the articles. By applying Van Dijk's CDA framework and Fairclough's Three-Dimensional structure in this research, it may reveal how the news constructs the narrative about data breaches and the government's role, and help contribute to a deeper understanding of digital security concerns in Indonesia. This research also aims to understand how the media represent the subject of the current issue, in order to identify possible biased media through several news published on the same issue

from 2024 about the same matter of the Indonesian government's data being hacked, which caused disturbances from both the people and the government.

Eventhough discourse of cyber-security in Indonesia is already deeply explored, especially in the incident of Bjorka 2020 and 2024 which seen at the Macro Frame Analysis by Susanto & Dahlia (2023) and Thematic content study by Hidayat & Zarkasi (2024) reveals that there are still significant gaps in research related to the specific rhetorical mechanisms of the 2024 Kominfo data leak. Current literature often prioritizes government-centered crisis communication strategies, as analyzed by Pratama (2024), or focuses on the theme of digital literacy in general, as in the work of Lestari (2024), but these approaches often ignore the critical ideological mediation carried out by the media. Although Wibowo et al. (2023) and Fauzi & Utami (2023) have used Van Leeuwen's representation of social actors and analyzed the use of passive sentences in government denials, their findings are limited to non-comparative or single-media contexts. In addition, although Sari (2023) and Indriani (2024) discuss data sovereignty and resistance to power in broader political discourse, and Rahman (2023) applies Van Dijk's ideological square to general data leaks, there is a lack of rigorous comparison between pro-government platforms such as VOI News and critical outlets such as The Jakarta Post. This study, therefore, responds to the gap identified by the general trend in Nugraha's (2025) research by using Fairclough's three-dimensional model to reveal how contrasting rhetorical strategies in the two media specifically construct narratives of the 2024 PDNS crisis.

The current study intends to close this gap by critically analysing the ways in which media discourse use language patterns and rhetorical devices to depict social actors and create ideological meaning. This study aims to understand how language functions both structurally and functionally to uphold power and ideology in news reporting by utilizing Van Leeuwen's social actor paradigm, rhetorical analysis, and systemic functional linguistics. By providing a more integrative viewpoint that use macro-level ideological critique with micro-level textual analysis, this work advances the area of critical discourse analysis. In addition to strengthening the theoretical application of CDA in media studies, it gives academics, journalists, and critical readers the skills they need to recognize the ways in which persuasive language is used to construct narratives and influence public opinion.

B. Research questions

Previous study shows a significance research regarding the same topic related to **Critical Discourse Analysis**, this research help understanding problem deeper based on each previous study sugestion and some problems that may not being mentioned by the following research questions:

1. How have Indonesian media outlets represented Kominfo data leak case from 2024?
2. How do rhetorical chores shape the construction of blame/responsibility in public sentiment?

C. Significance of the Research

This study helps in contributing about the role of media in shaping narrative about data breach and government accountability, by analyzing the case of PDNS being hacked (locked) by ransomware that cause of the Windows Defender is being turned off (The Jakarta Post, 2025) that lead to public personal data being leaked. By analyzing the case that highlights the section on how the media use the language, media power through narrative and shape the public trust in digital society. The finding may inform the strategies for transparent communication and crisis in management by the subject of the news article.

D. Scope and Limitations

This research is focused on how the media representing the issue and the actor being presented through selected local news. This research analysing on the text used by several media to present their news by using theory from Van Dijk that talk about Discourse text (how the text is interpreted through Micro and Macro structure) and the social cognition about the current issue, also using Leeuwen, 2008 (That is focused on using social actors, and social action to understand about the relation with the current issue) to get more answer about the related issue

E. Definition of Key Terms

Researcher tend to select several key phrases to support the research in obtaining the research question answer. Several terms are:

1. Critical Discourse Analysis (CDA)

In this study, CDA refers to Norman Fairclough's three-dimensional framework used to analyze the relationship between language, ideology, and power. This analysis focuses on how news texts (description), news production (interpretation), and the broader social context of the 2024 data leak (explanation) interact to shape public perception.

2. Rhetorical Strategies

These are deliberate linguistic techniques used by VOI News and The Jakarta Post to influence, persuade, or direct the audience's attention. In this study, these strategies include word choice (lexicon), the use of passive or active sentences, and the emphasis or omission of certain details to frame the data leak incident.

3. 2024 Kominfo Data Leak

This refers to a specific cybersecurity crisis involving the Temporary National Data Center (PDNSS) in June 2024, which was the target of a Brain Cipher ransomware attack. This incident serves as the main context and data source for the news articles analyzed in this study.

4. Framing

Based on Robert Entman's theory, framing in this study is the process by which the media selects certain aspects of the reality of data leaks and makes them more prominent. This framing is categorized into two main

frameworks identified in the findings: the Development Framework (focusing on improvement) and the Crisis Framework (focusing on systemic failure).

5. Representation of Social Actors

Derived from Theo van Leeuwen's theory, this term refers to the way individuals or institutions (such as Kominfo, the government, or the community) are described in the text. This study specifically analyzes whether these actors are “included” as responsible agents or “excluded” through depersonalization to shift responsibility.

6. Agents

This term refers to the linguistic attribution of responsibility or action to social actors. In this study, agents are analyzed to determine whether the media depicts the government as an active “problem solver” or a “passive victim” of circumstances, especially in relation to shifting blame to the public.

7. VOI News

A digital news platform in Indonesia analyzed in this study. Operationally, VOI News is defined as a media representative that tends to use the Development Framework, often in line with the government's narrative of progress and recovery.

8. The Jakarta Post

A leading English-language daily newspaper in Indonesia analyzed in this study. Operationally, The Jakarta Post is defined as a critical and independent media representative that tends to use the Crisis Framework, focusing on government accountability and systemic vulnerabilities.

CHAPTER II

LITERATURE REVIEW

This chapter discuss of literature related on the main topic of the news from local news as **VOI** and **The Jakarta Post**, taking focus on problem about how media represent the news through CDA Analysis using Micro and Macro structure

A. Critical Discourse Analysis

Foucault mentioned that discourse is a methodological tool to develop a theory of relation between knowledge and form of social control (Walshaw, 2007). Critical discourse analysis is a discourse that is focused on a politic and social context that represented through text that are enacted, reproduced, legitimated, and resisted and also can be characterized as social movement of politically committed discourse Analysis of Van Dijk, 2015). Wodak (2001) assumed that Critical discourse analysis aims to investigate critically about social inequality that appears in a social context, expressed, signalled, constituted, legitimized by language use (Allagbe & Amossou, 2018)

Discourse-as text refers to the linguistics aspect of the called organization that function in building the communication aspect for each word that able to construct a sentence and its meaning. (Berkovich, 2024) in which each sentence contains a meaning that hold a specific aspect to present such as being explained in Tan Dijk about the function of the text used as power as such authority, character in a detailed view or giving information about the current situation explicitly through the use of

word. After the text being constructed, the next will be the practice to be applied. Describing the way texts are produced through various media from specific language and being combined by the other that may cause such a different in meaning, and cause some people to misinterpret some of the word through the way people speak or read that depend on the time and place which being produced. (Berkovich & Benoliel, 2024)

Fairclough (1989) identifies three components of discourse as a text, interaction, and context:

1. Description: it is the level that is concerned mainly with the formal properties of the text.
2. Interpretation: it is concerned with the relationship between the interactions with the text. The latter is seen as the end product of the process of text production and as a resource in the process of text interpretation.
3. Explanation: It deals with the relationship between social context and interaction with the social determination of the processes of production and interpretation, and their social effects.

Thus, 'Text' is part of discourse analysis which is seen as a product and not as a process. Additionally, Fairclough (1989) argues that the three elements mentioned above have different ways of analysis. In other words, the process of explanation is quite different from that of interpretation and description in the level of form. Explanation requires a micro-analysis, whereas interpretation and description are globed in the macro-analysis. To sum up, Fairclough presents three

fundamental stages in the investigation of any communicative event of CDA from the sociological and linguistic perspectives. On the other hand, Van Dijk's framework is quite different since the focus is on the cognitive aspects of the language user in a specific social context.

B. Micro and Macro structures

One of elements in discourse analysis is using micro and macrostructures to show a sign of specific phenomenon to get more detailed information about the case by analysing each element. Macrostructures are mostly used in the theme of a specific context, that contains a specific topic. As for the microstructures is used in how subject representing about the specific case that mostly used in the sentence or text

1. Macrostructures

Macrostructures are global semantics in relation to the microstructures of language, cognition, and interaction. Defining the relations between the microlevels and the macro levels in terms of various reduction rules is called macro rules (Van Dijk, 1980). Macro rules that will be adapted in this research are:

- a. **Deletion:** Remove any premises from a sequence that do not serve as interpretation conditions (such as presuppositions) for other statements in the series.

- b. **Generalization:** Replacing a sequence of statements with a proposition that is implied by each of the preceding propositions in the sequence.
- c. **Construction:** Replace a series of propositions with a statement that is implied by the joint set of the sequence's propositions

2. Microstructures

Microstructure emphasize on how the content is being presented at the linguistical level, often being used as the main material in the news used in this research is being functionally connected, relatively, with the topic and knowledge about how the publisher is being made (Van Dijk, 1980) in the higher-level statement it may appear in sequent sentence that being further classified with details that always can be seen in a news discourse. As for microstructures, are mostly found within a text or sentence that may contain a specific information that contain semantics elements based on Van Dijk (Zurstiege, 2000). in which being mentioned:

- a. Actor description (meaning) may be described members of groups or individuals, that specific or unspecific, function, role, or group name, by their action to seek about positive self-presentation and negative other-presentation

- b. Authority (argumentation) means calling a specific group or individual that has an authority to strengthen a specific information, argument, or such
- c. Burden (topos) means representing a problem in a specific case (phenomenon) in the text as a big problem to be self-evident and as sufficient reason to accept the conclusion
- d. Consensus (political strategy) is often used in issues of national importances. That is defined as claims, appearance, or will that may be seen as a vote from many people
- e. Empathy manages the speaker impression with audience that represented as the victim of a group or individuals
- f. Evidentiality, shows a fact(s) that has a sign to support a specific side of group or individuals.
- g. Examples/Illustration gives a concrete example, often in the form of short story that illustrating general point of defendant or a group in a specific situation as debating to get better information rather just telling evidence directly
- h. Fallacies, representing the fault of a specific group of people or individuals
- i. Self-glorification, representing itself or a specific group or individuals with a positive statement
- j. Polarization, shows an expression of polarized cognition and the categorial division of people ingroup and outgroup

C. Actor representation

Van Luween (2008) describes a social actor as a participant that participates or takes a role in a social practice. Social actors are mostly seen as something that interferes with “the actor’s point of view” (Button, 1991) that can be assumed as how the actors describe a phenomenon in which, in this case, about the government Ministry of Communication and Information view and about how it sees the case based on their response. Beside, the framework involves three primary semantic component that analyzed how the social actor being potraited:

1. Inclusion/Exclusion: This component discusses the basic choice of whether an actor is mentioned in the text at all [1]. Inclusion makes the actor visible, while exclusion (omission) makes them invisible, possibly to hide responsibility or generalize events.

2. Activation/Passivation: This refers to whether the actor is depicted as an active agent (performer of the action) or a passive recipient (object of the action). Active representation emphasizes agency and responsibility, while passive representation may deflect that responsibility.

3. Role Allocation: When actors are included, this component analyzes the specific social roles or identities assigned to them [1]. This involves how actors are mentioned (e.g., by name, title, or descriptive phrase) and the characteristics or actions that define their function in the discourse (e.g., “victim,” “perpetrator,” “expert,” “mother”).

D. News in Discourse

News in Discourse is related in communicating the information about the current issue or topic that being held (Van Dijk, 1988) while informing through organized structure of micro and macro in discourse as being explained in part B, that uses a specific word to describe how the thing related being informed or being seen by others as being antagonized by a specific group or justified about the action toward a specific subject about the current issue (showing a sign of bias) and shows a significance ideology used by the group of the journalist or publisher.

E. Fairclough three-dimensional Structure

In Fairclough Three-Dimensional structure framework emphasize on how the micro-level discourse work in linguistic has any relation toward the macro-level discourse in society, these three are:

1. Text

First step in three-dimensional framework CDA by Fairclough is the text. The text covers both the written and spoken inside the work (which in this research uses the online media news as the source). "Texts" may be written or oral, and oral texts may be just spoken or spoken and visual through media television, (Fairclough, 1995). The study of the linguistic structures generated during a discursive event is the text's analysis. Its foundation is first the study of grammar, coherence, semantics, vocabulary, etc. However, the processes of text production and perception that are

combined into the discourse practice must also be analysed in order to fully comprehend the text.

2. Discourse Practice

Three fundamental components of discourse practice that need to be comprehensively examined are text production, text distribution, and text consumption. The writer encodes specific ideas and beliefs (ideology) in the text during the writing process. Proceeding into that, the target audience is clearly established. The audience then decodes the meaning of the text based on their prior experiences, knowledge, and beliefs. As a result, the audience's opinions and beliefs may be influenced by the content.

3. Sociocultural Practice

The sociocultural practice is the last level of the CDA communicative event. For Fairclough (1995), "sociocultural practice" is "the social and cultural goings-on which the communicative event is a part of." On which basis analysis of what is going on within some sociocultural context is the sociocultural practice analysis. It investigates how discourses function in different field of society and also with respect to dominance and power. Discourse practice and the text need to be reconciled in order to unite for sociocultural practice.

F. Media Framing

Media framing focuses on the ways in which the media construct upon our knowledge of the issue by promoting specific aspects. Goffman (1974) first

theorized about the frames in social interaction. He described that people have access to reality through interpretative "frames," upon which they base their interpretation of occurrences. Such frames are developed based on social and cultural experiences.

In the study of the media, Goffman's theory argues that information presentation has an influence on the way audiences receive it. The media have a significant role in framing through which public knowledge of news and events is constructed.

Entman (1993) characterizes framing as the process by which media frame and highlight particular dimensions of reality in order to shape public interpretation.

Framing, Entman argues, consists of four key elements:

- 1. Identify issues** (declaring the issue)
- 2. Diagnose reasons** (declaring the reason)
- 3. Make ethical judgments** (providing ethical judgments)
- 4. Provide cures** (suggesting solutions)

Media use framing to shape public opinion and policy by selectively drawing attention to some things, deciding how audiences perceive events.

According to Güran & Özarslan (2022), Framing Theory describes communicational frames as social and cultural norms that guide discourse, relationships, and social actors' roles in political, ethical, and social contexts. The frames are dynamically negotiated and established by the users.

De Vreese, (2005) averred that Framing research is a new and dynamic field, with increasing empirical evidence giving rise to diverse results and theory building. Media framing research has emerged as a unifying discourse in communication research, yet research practiced is mixed in terms of methodology, namely issue-specific frames (topic-specific) versus generic frames (transferable across topics).

CHAPTER III

This chapter discuss on how the data will be analyzed through several steps that will be conducted. Through research design, data and data source as the main topic of the research source, data collection, and data analysis.

RESEARCH METHOD

A. Research Design

This study conducted through a descriptive qualitative approach, Critical Discourse Analysis of CDA, to analyze how Indonesian local news media describe situations related to cybersecurity issues, using the 2024 Kominfo data leak as an example. By focusing on the interpretation of text, meaning, and language patterns rather than text analysis, a descriptive qualitative approach was suitable for this study. This method helped in understanding of how language was used in news media to shape public opinion and perceptions of government responsibility. According to Fairclough (1995), language is not only a tool of communication, but also a tool for constructing social reality and reinforcing power relations. Media framing (Entman, 1993) involves selecting a certain point of the main topic, which can be an object or text, then highlightning it to support in researching the subject.

The research in this study involved analyzing news articles in several Indonesian online news media, focusing on linguistic patterns, framing habits, and ideological narratives. Based on Van Dijk's discourse structure and Fairclough's three-dimensional model, this study critically analyzed on how news being

delivered as giving a good, neutral, or bad image based on how the media presenting their news through local newspaper up-to digital like media in any website.

The qualitative strategy allows context-based analysis of how media stories evolve over time and how they can, in turn, impact public trust in digital security solutions.

B. Data and Data Source

The data which will be collected in this research are consist of linguistic units from the word, phrases, clauses, and sentences, used to deliver the news through an online news media as the data source, from VOI and The Jakarta Post. The data source obtained through news from VOI (2025, January 3). A Myriad Of Government Homeworks Facing Cyber Attacks That Are Increasingly Growing. VOI.id. Retrieved on March 12, 2025, from <https://voi.id/en/bernas/447752> and The Jakarta Post. (2024, June 25). Govt refuses to pay \$8 million after ransomware attack on national data center. The Jakarta Post. Retrieved on March 13, 2025, from <https://www.thejakartapost.com/indonesia/2024/06/25/govt-refuses-to-pay-8-million-after-ransomware-attack-on-national-data-center.html>.

C. Data Collection

In part of data collection, is an important step for researcher to obtain the necessary data which later be analyzed. In this research, researcher tend to search both the news from VOI and The Jakarta Post which has credible reputation of delivering news in recent years, then collecting the news which has the same topic as the focus int his research as Kominfo Data Breach, PDNS Ransomware,

and Cybersecurity accountability. For the first step of collecting the data, researcher tend to search both the news with the same topic. The selected articles were archived in their original digital format. This involved: a) Saving the full text and metadata (author, date of publication, URL), b) Converting the articles into a plain text format to facilitate coding and linguistic annotation. Then reading and extracting linguistic units inside the text, involving a preliminary reading to identify and extract the primary data units. These include: a) Sentences and clauses that represent the government or the public. b) Passive voice constructions used to obscure agency. c) Specific lexical choices (adjectives/nouns).

D. Data Analysis

The collected data analyzed using discourse analysis techniques, Van Dijk's (2015) model for Critical Discourse Analysis of CDA and Fairclough's (1989) three-dimensional model. Both the techniques are suitable for examining the linguistic pattern and ideological frames in news. Analysis will take place in three stages.

The first stage involves thematic analysis, by coding the news through the dominance themes as blame attribution (e.g., the focus on the subject being blamed, whether the government, the hacker, or the public), accountability and transparency (e.g., government failure or response being highlighted), and public opinion and trust (e.g., how discourse able to shape trust through cybersecurity policies which cause the issue to happen). Articles will be identified within these themes to obtain recurring patterns of discourse. The second is linguistic and

rhetorical analysis, which takes focus on the investigation of microstructures, such as sentence structure, word choice, and tone (Van Dijk, 2015), and macrostructures, such as overall themes and narratives. On the basis of Entman's (1993) theory, framing analysis will also be used to analyze how media emphasize, foreground, or marginalize information in an attempt to construct certain frames of hijacking incident. The third stage is comparative media representation analysis, in which, the study will examine how different media organizations report on the same cybersecurity issue. The comparison will determine whether some of the media reveal ideological bias by criticizing or praising the government's reaction to data security matters or focusing the subject whether it's the hacker, the government, or the public. Through the integration of the application of CDA and framing theory, this analysis is aspiring to gain a more comprehensive insight into how media language contributes to public discourse and builds ideological meaning. This comparison will reveal whether the local news demonstrate the framing regarding the matter of the data breach through criticizing the issue, or defending government about how the government handle the security's of the data. Through the use of CDA and framing theory, this analysis aims to provide a deeper understanding on how the language in media contributes in public discourse and shape opinion through the presented news.

CHAPTER IV

FINDINGS AND DISCUSSIONS

This chapter present research findings based on CDA from Van Dijk and Foucault three-dimensional Structure, Goffman Media Framing, and Van Luween Actor Representation. Each finding, then will be analyzed using the mentioned theory to obtain information regarding the research question on how media represent the subject.

A. Findings

Distrust in public may already grown larger as the issue of PDNS data being hacked and locked, causing the government shows a lack in managing the cybersecurity in the recent event as happen in June 2024. The ransomware attack gain a lot attention because of how the government handle the issue with lack of accountability and the transparency of the information of which data is being hacked or locked by the hacker (The Jakarta Post, 2024. VOI.id, 2025) as it handling over 200 public services, including the immigration and civil registration. The cyber attack causing uproar about public safety regarding the personal information that is inside of the hacked server (The Jakarta Post, 2024). Along these lines, the news plays a great roles in shaping public opinion and trust through how the media deliver the news regarding the issue, especially about the social actors, which in this case is the KOMINFO, which later be changed to KOMDIGI on October 21, 2024(The Jakarta Post, 2024) causing the preperators of the attack being concerned, along with the framing narrative.

To back-up the findings, this part take a quick look about the data and regarding the issue of PDNS being leaked that happened in June 2024. The attack cause a lot of problem from the government service to public trust and opinion about the KOMINFO handle the issue and being asked about the accountability of KOMINFO. The report stated that it has affected over 200 national-level and local government services, including immigration, licensing, and civil registration systems. It exploited the weaknesses of software from legacy applications that had poor cybersecurity controls. According to the National Cyber and Crypto Agency (BSSN), the ransomware was identified as a new form of LockBit 3.0, a well-known file encryption player. For this attack, this type of malware had previously been used to target French hospitals and critical U.S. infrastructures. The attackers demanded ransom and a decryption key worth \$8 million; however, the government did not push for negotiations consistent with its policy against ransom payments. A 2024 survey conducted by Cyberkreasi with almost 1,200 respondents in Jakarta, Surabaya, and Makassar revealed that 74 percent were unaware of the government's management of digital content related to them. In addition, 68 percent severely doubted the ability of the government to secure their information through the experience of the breach. This figure reflects the effects of the breach, which take the most evident forms of technological disruption and the resultant dissipation of public and institutional trust. No doubt it will require extensive reforms in cybersecurity, transparency, and digital rights.

1. Macrostructure Analysis

Both pieces at the macro level revolve around the same significant event: a ransomware assault that encrypted valuable government data and disrupted public services. The thematic tone and ideological position, however, are not alike.

1.1 VOI News: Cybersecurity as Institutional Homework

A. Data I

“The government still has a myriad of homework regarding cybersecurity,” the article asserts, pointing to long-standing structural deficiencies in Indonesia’s digital defense systems (VOI News, 2025).

This data was taken from VOI. (2025, January 3). A Myriad Of Government Homeworks Facing Cyber Attacks That Are Increasingly Growing. VOI.id. Retrieved on March 12, 2025, from <https://voi.id/en/bernas/447752>

B. Context of Data 1

The passage mentions the growing frequency and intensity of cyber-attacks on Indonesian government agencies in 2024, such as ransom attacks on the Temporary National Data Center (PDNS). The news information obtained through Indonesian Communication Center interview from several figure that has a control over the information. The scene is set in Indonesia, in the year 2024 with focus on cyber-attacks that have penetrated a number of governmental institutions, including the PDNS. Relevance to Research Question: This paragraph highlights Indonesian government digital infrastructure vulnerability, that has a consent on discourse structure from how the news is being built and delivered. It depicts matters of systematic response to cybersecurity, commensurate with the research's examination of

media framing and critical discourse Analysis of CDA) of national data breaches.

C. Analysis of Data 1

The article mainly shows a complaint over the length of time the system has not been ready, using the metaphor of "homework" to describe the fact that vital cybersecurity work remains to be finished. It is not hyperbolic in assigning blame, but clearly intimated bureaucrat slowdown and that real progress has not yet been made. This differs from previous VOI reporting that emphasized possibilities for change, and is also less confrontational in tone than The Jakarta Post, which has a more aggressive style. At a deeper level, the article depicts a slight movement toward institutionally critical thinking while retaining a the development of the country and the issue's perspective.

It recognizes that it is the government's function to oversee digital change but does not aim at specific individuals or organizations, which suits Van Leeuwen's (2008) institutional abstraction. The overall message is one of national advancement but indirectly urges faster reforms and increased responsibility. As Fairclough (1995) would deconstruct, the article presents some contradictory elements: it is in support of the legitimacy of institutions but also gives critique to appear credible. This balancing act, which acts as what Van Dijk (2015) calls "ideological management", giving criticisms so

that it falls into the acceptable parameters to uphold the faith of the people in the competence of the government, though it admits there are issues.

1.2 Jakarta Post: Tensions, Threats, and Government Rejections.

A. Data 2

The Jakarta Post headline reads: "Govt refuses to pay \$8 million" in response to the ransomware attack on PDNS (The Jakarta Post, accessed August 13, 2024). The Jakarta Post extracted this data source. No date. (2024, June 25). Government does not agree to pay \$8 million after ransomware attack on national data center.

Retrieved on March 13, 2025, from
<https://www.thejakartapost.com/indonesia/2024/06/25/govt-refuses-to-pay-8-million-after-ransomware-attack-on-national-data-center.html>.

B. Context of Data 2

According to the Jakarta Post news report that was acquired in March 2025, the Indonesian government rejected the \$8 million ransom after a June 2024 cyberattack in which the Pusat Data Nasional Sementara (PDNS) went offline influencing more than 200 sub-channel that contain an information needed from the main site. The article does cite, like Kominfo and BSSN, but isn't naming particular organization. This can be an aimless talk technique of organization being confidential. All of this in the midst of a setting of highlighting cyber dangers and uneasiness is displayed as a striking, policy-oriented choice, whereas at the same time raising concerns almost straight-forwardness. The Jakarta Post headline wrote in brief with risk, weighted, "Govt denies to pay \$8 million" and had no cited sources, comes from this point of view for emphasizing critical thought, risk, and

bureaucratic anonymous, which staying with its liberal democratic motivation and as the “guard dog” which secure the information related the issue. The article presents cybersecurity not as it were as a specialized issue but as a politically challenged problem, where state strength, ethical grandstanding, and open responsibility.

C. Analysis of Data 2

Jakarta Post focus on crisis-framing macrostructure, by emphasizing on stress, threat, and policy implications. With the title "Govt refuses to pay \$8 million," a degree of tension and urgency is evoked immediately. This framing approach follows Entman (1993) media-framing theory, and emphasizing the problem definition and suggesting the cause function, by emphasizing on institutional decision-making under pressure. Unlike the VOI, Jakarta Post does not name particular individuals within the government or refer to the internal debates. That kind of indirection, separating problems from personalization and enhance the vagueness perception from bureaucratic.

The absence of named actors, according to Van Leeuwen (2008), is very close to exception, a discursive practice that abbreviated agency and focuses on institutional systems, rather than human agency. The focus on confronting policies, that being reflected as “watch dogs” journalism especially in liberal democratic settings (Waisbord 2000). By stating that

the government is determined not to negotiate with cyber-terrorists, this can be framed as a morally strict, maybe even irresponsible, for a while.

The selection of a narrative framework that focuses on future consequences is in line with Entman's (2004) narrative framework, as this framework discusses the potential losses that may occur in the future as a result of choices made. Furthermore, the use of lexicon, such as “threaten,” “reject,” and “attack” illustrates the macro-ideological structure of news content according to Van Dijk (2015), in which he frames the news to insert a certain type of social cognition, in this case, fear of national cyber security. The amount of report to get rid the problem (e.g. ransom amounts such as US\$8 million) is a type of evidentiality, which enhances credibility of the fact delivered and stating as what is at stake (Cotter, 2010). It develops a crisis story within the Jakarta Post framed around risk which is not able to be moved and institutional failure. It cause in revealing of information to be transparent as possible and emphasizes structural conflict, hence adopting liberal media ideology, while also seeks to counter state authority and demand transparency (McNair, 2011).

2. Teun A. van Dijk's Macrostructure Operations

Vand Dijk Macrostructure Operation contain information on relation between the microstructure language as such language, cognition, and interaction.

2.1. Generalization

Generalization as being mentioned in Van Dijk Macrostructure Operation replacing the statemen using a preposition, which implied by preceding proposition in the sequences.

A. Data 3

1. VOI News: States that *“the government still has a myriad of homework regarding cybersecurity”* without detailing specific institutional failures or individuals involved (VOI News, 2025).

This data was taken from VOI. (2025, January 3). A Myriad Of Government Homeworks Facing Cyber Attacks That Are Increasingly Growing. VOI.id. Retrieved on March 12, 2025, from <https://voi.id/en/bernas/447752>

2. The Jakarta Post: Presents the refusal to pay ransom as a unified policy act: *“the government refused to pay the ransom demanded by the hackers”* (The Jakarta Post, 2024).

This data was taken from The Jakarta Post. (2024, June 25). Govt refuses to pay \$8 million after ransomware attack on national data center. The Jakarta Post. Retrieved on March 13, 2025, from <https://www.thejakartapost.com/indonesia/2024/06/25/govt-refuses-to-pay-8-million-after-ransomware-attack-on-national-data-center.html>

B. Context of Data 3

The discussion here focuses on how the media tends to generalize the responsibility when the news gives a report about the matter on Indonesia data breach in 2024. The information comes from VOI News (2025) and The Jakarta Post (2024), which refer to subject like “the government” without mentioning a specific agencies or officials. VOI

mentions the issue with saying that the government has a “lot of work” when it comes to cybersecurity. The Jakarta Post takes a stance by mentioning that government refused to pay the ransom. This statement appear after the issue of the ransomware attack in June 2024 targetting PDNS that cause over 200 public services going offline while the server is being attacked (The Jakarta Post, 2024). The way media media generalize the issue seems to be an intention choice. VOI uses it to emphasize the reform and development, focusing on how the cybersecurity need an improvement. While The Jakarta Post emphasize about the government decision about their action, especially in a pressured situation without getting into personal blame or complicating the government details related to the matter. Both news provides a broad information to make the issue being able to be understood easily by the people.

C. Analysis of Data 3

VOI News covered the incident in context of the ongoing institutional delay and how the subject shows a not readiness. Instead of mentioning specific failures, the report used the metaphor of “homework,” framing cybersecurity as an ongoing task. This removes the breach from its policy or technical framework and places it within the framework of long-term formation (VOI News, 2025).

The Jakarta Post generalized by highlighting policy, portraying the government's rejection as a single symbolic choice. Internal attacks or

politics were not disclosed, resulting in a clear and general picture of an uncooperative state (The Jakarta Post, 2024). The Jakarta Post generalized by focusing on policy, showing political indifference and disregard for the issue. VOI News and The Jakarta Post employ generalization when reporting the 2024 Kominfo data breach, stating "the government" without naming individuals or agencies.

This institutional generalization, used by both news media, works to flatten the complicated institutional action and disperse immediate responsibility. VOI portrays the government as one that has "homework" to do in cybersecurity, gradually reform the development of cybersecurity issue, whereas The Jakarta Post stresses the strong commitment of the government not to pay ransom, highlighting strict policy action's, which is strict, be taken under pressure. Generalization is a representational and linguistic process whereby public opinion is framed according to the ideological position of each outlet, VOI for institutional development and The Jakarta Post for institutional risk and accountability (VOI News, 2025; The Jakarta Post, 2024).

2.2 Deletions

Deletion removes any premise from consequence that do not serve as interpretation condition in the context of the news.

A. Data 4

1. VOI News: Omits citizen perspectives, technical details of the breach, or reactions from victims; focuses solely on the government's backlog of tasks (VOI News, 2025).

This data was taken from VOI. (2025, January 3). A Myriad Of Government Homeworks Facing Cyber Attacks That Are Increasingly Growing. VOI.id. Retrieved on March 12, 2025, from <https://voi.id/en/bernas/447752>

2. The Jakarta Post: Omits names of decision-makers or technical agencies like BSSN; focuses on government actions in aggregate (The Jakarta Post, 2024).

This data was taken from The Jakarta Post. (2024, June 25). Govt refuses to pay \$8 million after ransomware attack on national data center. The Jakarta Post. Retrieved on March 13, 2025, from <https://www.thejakartapost.com/indonesia/2024/06/25/govt-refuses-to-pay-8-million-after-ransomware-attack-on-national-data-center.html>

B. Context of Data 4

The discussion here focuses on how Indonesian media often leave out certain details when covering the 2024 Kominfo data breach. VOI News and The Jakarta Post act as the main subject, but they each have their own focus. VOI tends to zoom in on government responsibilities and the bigger system's flaws, while skipping over what regular folks experienced and the technical side of things. On the other hand, The Jakarta Post emphasizes how the government refused to pay ransom money but doesn't share the names of specific officials or agencies involved with the decision. These gaps in the story came up during the June 2024 ransomware attack on the Temporary National Data Center (PDNS), which really messed up public services that has an access to the server or being linked. How they choose

not to share the decision leave out shapes what people think, either by playing the word used to report the situation and keep the focuses on the technologies (like VOI does) or by making the government's bureaucrat seem secretive and mysterious (like The Jakarta Post). It kinds of shows, that each has a different point of view or bias in how they tell the story.

C. Analysis of Data 4

VOI News didn't mention the human centered focuses such as public disturbance, user impact, or public doubt. Not mentioning these factors weakens the crisis, focusing on policy backlogs rather than real failure or accountability (VOI News, 2025).

The Jakarta Post removes the individualized responsibility, thus showing accountability throughout the bureaucratic system. This removal creates uncertainty, which questions leadership and transparency (The Jakarta Post, 2024).

Both The Jakarta Post and VOI News utilize deletion to shape the 2024 Kominfo data breach in different ideological ways. VOI News, as commented by Bernas (2025) in an editorial, outline the growing number of cyberattacks and how the government is not prepared, with a "myriad of homework" to be done by them. However, the report ignores important facts such as the technical reasons behind the violations, the role of institutions such as Kominfo or BSSN, and the reaction from the public. Deletion here, serve to downplay the crisis story and divert attention from short-term

failure to long-term reform to safeguard institutional credibility (Van Leeuwen, 2008; Van Dijk, 2015).

The Jakarta Post (2024) covers the government's not paying the ransom money of a US\$8 million without attributing a specific individuals or agencies accountable for the action. By avoiding personal attribution and technical details, this story builds a narrative about bureaucratic obscurity, indirectly criticizing institutional transparency while highlighting high-risk policy actions. They both employ the subject like "the government" and passive voice to transparent the agency, yet they have a different agenda, VOI is towards maintaining institutional legitimacy, whereas The Jakarta Post pointing its watchdog status by calling for government's cybersecurity state as accountability (Van Dijk, 2015). The deletions are not merely linguistic strategy to not mention about a certain subject, but an ideological system, that in this case influencing public discourse and showing responsibility and urgency.

2.3 Construction

One of Van Dijk Macrostructure operation used in this research is Construction, in which, replacing the statement with joint set of thesequences' preposition.

A. Data 5

1. VOI News: Constructs a narrative around phrases such as "*government homework*," "*systemic vulnerabilities*," and "*need for improvement*" (VOI News, 2025).

This data was taken from VOI. (2025, January 3). A Myriad Of Government Homeworks Facing Cyber Attacks That Are Increasingly Growing. VOI.id. Retrieved on March 12, 2025, from <https://voi.id/en/bernas/447752>

2. The Jakarta Post: Constructs urgency using terms like “*refused to pay*,” “*threatened to release data*,” and “*paralyzed services*” (The Jakarta Post, 2024).

This data was taken from The Jakarta Post. (2024, June 25). Govt refuses to pay \$8 million after ransomware attack on national data center. The Jakarta Post. Retrieved on March 13, 2025, from <https://www.thejakartapost.com/indonesia/2024/06/25/govt-refuses-to-pay-8-million-after-ransomware-attack-on-national-data-center.html>

B. Context of Data 5

This section talks about how VOI News and The Jakarta Post tell the story around the 2024 Kominfo data breach, especially focusing on the language they use and how they frame things. In VOI.id Bernas's article from 2025, the statement shows the government has a lot of reason when it comes to cybersecurity, emphasizing the need to change or improve, and institutional responsibility instead of just pointing out failures. The incident is set after June 2024, right after a big ransomware attack on the Temporary National Data Center (PDNS), which messed up over 200 public services and on its linked affiliate. On the other hand, The Jakarta Post from 2024 uses more dramatic language, like saying the government “refused to pay” and describing services as “paralyzed,” to really emphasize the crisis aspect and make the situation sound important and urgent. These different approaches reflect their own perspectives: VOI leans towards a bureaucratic,

while The Jakarta Post focuses more on urgency and holding the government accountable.

C. Analysis of Data 5

VOI News builds a secretive story, that highlight the increase of improvement and government accountability. Such framing evokes consideration in the long term. It utilizes positive vagueness (e.g, "should improve infrastructure") to propose improvement but not details on previous contexts (VOI News, 2025).

The Jakarta Post constructs a crisis narrated story by focusing on the institutional choices in moments of crisis. The article uses fast wording in case of emergency (as such "should improve infrastructure") to convey the events' emphasis, underlining the stakes and implications involved (The Jakarta Post, 2024).

In VOI (2025), VOI News frames the 2024 Kominfo data breach as being within a broader institutional issue rather than a short-term crisis. With adjectives such as "a myriad of homework" and "systemic vulnerabilities," the article portrays the government as a reforming institution with increasing cyber attacks. This is a perspective that does not blame explicitly, but rather points to the ones of bureaucracy and the necessity of long-term change. This type of construction demonstrates a stance where they try to develop further through an undergoing transformation. This direction is in accord with Van Dijk's (2015) positive

self-presentation theory, in which discourse operates to defend institutional legitimacy through the emphasis on reform instead of vulnerabilities.

In contrast, The Jakarta Post (2024) constructs a more urgent and confrontational narrative using active voice and a lexical choices such as “refused to pay,” “threatened,” and “paralyzed services.” This framing emphasizes on taking action after the case happened, institutional stress, and policy risk. Unlike VOI’s abstract tone, The Jakarta Post uses concrete actions and figures the estimation or mentioned value on how much the government should pay (e.g., “US\$8 million”) to give a clear image of how much the value and encourage public awareness regarding the issue on cyber attack case. This framing is stated as the main media role characteristic of liberal democracy that constructs the incident as a demonstration of government accountability. Together, these competing local news illustrate how Indonesian media employed some rhetorical and linguistic strategies to frame the Kominfo attack as either a persistent institutional problem (VOI) or as a crisis demanding transparency and firm leadership (The Jakarta Post).

3. Microstructure Analysis

In microstructure operation, the focus is slightly different from the macrostructure, while the macrostructure contain several element from microstructure, microstructure contain an information at linguistical feature that

often being used in a news material to describe, pointing, subjecting the issue, resulting in bias to one point instead of being neutral.

3.1 Actor Representation (Van Leeuwen, 2008)

Van Leeuwen define actor representation as the point of view of the writer, which indicates how the writer sees the issue based on one point by not making a specific subject bad or the other.

A. Data 6

1. VOI News refers to “the government” without naming specific individuals or departments (VOI News, 2025).

This data was taken from VOI. (2025, January 3). A Myriad Of Government Homeworks Facing Cyber Attacks That Are Increasingly Growing. VOI.id. Retrieved on March 12, 2025, from <https://voi.id/en/bernas/447752>

2. The Jakarta Post uses generalized expressions such as “the government” or “officials” without naming individuals (The Jakarta Post, accessed August 13, 2024).

This data was taken from The Jakarta Post. (2024, June 25). Govt refuses to pay \$8 million after ransomware attack on national data center. The Jakarta Post. Retrieved on March 13, 2025, from <https://www.thejakartapost.com/indonesia/2024/06/25/govt-refuses-to-pay-8-million-after-ransomware-attack-on-national-data-center.html>

B. Context of Data 6

This part looks at how VOI News and The Jakarta Post show representing the actor/subject in their coverage of the 2024 Kominfo data breach. In the VOI Bernas report (2025), the editorial only mentions “the government” without pointing out specific agencies like Kominfo or BSSN, which gives a broad sense of who might be

responsible for the incident to happen (VOI News, 2025). The Jakarta Post (2024) stated that the government was the one who decided not to pay the US\$8 million ransom, but doesn't name any particular individuals or departments. Both articles focus on what happened after the ransomware attack on the Temporary National Data Center (PDNS) in June 2024, which disrupted public services and all of the connected branches. The way they avoid naming specific people or departments seems like aware of the situation, VOI wants to protect the reputation of institutions, while The Jakarta Post seems to emphasize the lack of transparency in government actions. This approach lines up with their different perspectives.

C. Analysis of Data 6

Van Leeuwen's (2008) social actor network model provides a framework for analyzing how discourse includes or excludes social actors, and how roles are allocated to them based on how the writer presenting the social actor. His typology identifies strategies such as inclusion/exclusion, activation/passivation, and role allocation, which are evident in the media texts analyzed. The findings will be separated by each categories below:

3.1.1 Inclusion/Exclusion

Van Leeuwen introduce the social actor representation in discourse to show how the subject being written in text, as news media by mentioning it clearly or explicitly.

A. Data 7

1. VOI News: Uses phrases such as “*the government still has a myriad of homework*”, without mentioning KOMINFO, BSSN, or any government official by name (VOI News, 2025).

This data was taken from VOI. (2025, January 3). A Myriad Of Government Homeworks Facing Cyber Attacks That Are Increasingly Growing. VOI.id. Retrieved on March 12, 2025, from <https://voi.id/en/bernas/447752>

2. The Jakarta Post: States “*the government refused to pay the ransom demanded by the hackers*”, with no attribution to specific authorities (The Jakarta Post, 2024).

This data was taken from The Jakarta Post. (2024, June 25). Govt refuses to pay \$8 million after ransomware attack on national data center. The Jakarta Post. Retrieved on March 13, 2025, from <https://www.thejakartapost.com/indonesia/2024/06/25/govt-refuses-to-pay-8-million-after-ransomware-attack-on-national-data-center.html>

B. Context of Data 7

The topic concerns how VOI News and *The Jakarta Post* use inclusion and exclusion of social actors to frame the 2024 Kominfo data breach. In the VOI Bernas article (2025), the writer refers only “the government,” omitting specific mentions of Kominfo, BSSN, or named officials involved in the response (VOI News, 2025) while The Jakarta Post (2024) states that “the government refused to pay

the ransom” without identifying the individuals or departments behind the decision. Both reports are set in the context of the June 2024 ransomware attack on the Temporary National Data Center, which disrupted hundreds of all connected services that used the main data from the PDSS. These deletion or not to mention act, reflect a discursive strategy where institutional actors are generalized to protect state legitimacy (VOI) or emphasizing on government vaguity (*The Jakarta Post*), revealing how each news use exclusion to shape public interpretation and align with its ideological stance.

C. Analysis of Data 7

Both VOI News and The Jakarta Post through a process of inclusion and exclusion of social actors in reporting the 2024 Kominfo data breach, constructing public opinion through selective representation. In its analysis of the news titled "Cybersecurity as Institutional Homework" (VOI News, 2025), VOI News used general institutional terms such as "the government" frequently, while intentionally not naming particular institutions like KOMINFO (later KOMDIGI) or BSSN. This rhetorical decision is in tune with Van Leeuwen's (2008) institutional abstraction, in which the responsibility is shared among anonymous institutions instead of being held by an agents or subject. The use of metaphors such as "a myriad of homework" along with the lack of critical attribution situates the transgression within a broader, continuing process of

digital reform and hence reduces the level crisis of the incident. This linguistic passivation illustrates Van Dijk's (2015) definition of positive self-presentation, protecting institutional credibility and creating a narrative of delayed but real progress.

In contrast, The Jakarta Post (2024) also withheld individual attribution but used this to highlight bureaucratic opacity and institutional strife. With the use of active verbs like "refused to pay" and specific numerical information (as mentioned in The Jakarta Post about how the hacker need the money to be paid for US\$8 million ransom), the newspaper highlighted the government's choice without personalized storytelling. This convention aligns with a liberal-democratic media ideology supporting institutional accountability and watchdog reporting (Waisbord, 2000). Van Dijk's (2015) ideological macrostructures are apparent in the content organization of the article in order to emphasize conflict, urgency, and policy relevance. So, while both media abstract social actors, they do so for different purposes: VOI News stifles criticism through reformist framing, while The Jakarta Post facilitates public accountability by emphasizing state uncertainty and risk. These different approaches illustrate how inclusion and exclusion are employed as ideological tools in framing national cybersecurity discourse.

3.1.2 Activation/Passivation

Van Leeuwen introduce the terms associo-semantic inventory to examine how the subject being portrayed in discourse, showing how language able to shape people interpretation about the issued topic.

A. Data 8

1. VOI News: The article states, *“the government still has many homework tasks to address cybersecurity gaps”* and *“cyberattacks are becoming increasingly massive”* (VOI News, 2025).

This data was taken from VOI. (2025, January 3). A Myriad Of Government Homeworks Facing Cyber Attacks That Are Increasingly Growing. VOI.id. Retrieved on March 12, 2025, from <https://voi.id/en/bernas/447752>

2. The Jakarta Post: Writes, *“the government refused to pay the ransom”* and *“hackers threatened to release sensitive data”* (The Jakarta Post, 2024).

This data was taken from The Jakarta Post. (2024, June 25). Govt refuses to pay \$8 million after ransomware attack on national data center. The Jakarta Post. Retrieved on March 13, 2025, from <https://www.thejakartapost.com/indonesia/2024/06/25/govt-refuses-to-pay-8-million-after-ransomware-attack-on-national-data-center.html>

B. Context of Data 8

This discussion is all about how VOI News and The Jakarta Post talk about the 2024 Kominfo data breach by choosing which social actors to mention and which to leave out. In VOI News(2025), the editorial only talks about “the government” without mentioning any official that has relation with the incident (VOI News, 2025). On the other hand, The Jakarta Post (2024) says that “the government

refused to pay the ransom,” but doesn’t name the person or departments from government responsible for that decision. Both stories are centered around the ransomware attack at the Temporary National Data Center in June 2024, which cause a lot of public service data being leaked. By leaving out certain actors, both news use different strategy. VOI tends to generalize or keep things vague to protect the government’s image, while The Jakarta Post emphasizes the opaque nature of bureaucracy. This shows how each one uses omission and selection of actors to shape how the public sees the story and to support their own perspectives or biases.

C. Analysis of Data 8

The media in Indonesia used activation and passivation rhetorical tactics to present the 2024 Kominfo data breach while developing their narratives on who was responsible and what actions were taken by various organizations. The main approach of VOI News (2025) involves passivation through the government as an entity that responds passively to overwhelming challenges. The phrase "the government still has many homework tasks to address cybersecurity gaps" uses vague description to assign responsibility without identifying specific people. The description of "increasingly massive cyberattacks" allows the state to present itself as an innocent bystander in the crisis because the focus shifts toward external threats. The passivation linguistic style fits with Van

Leeuwen's (2008) theory of passivation and helps maintain institutional credibility by highlighting duties while concealing organization responsibility. The passivated narrative from VOI promotes a slow response to change through its portrait of the breach as a natural part of state development rather than an immediate government misstep. The media ideology of development views institutional longevity as more important than holding organizations responsible for immediate failures.

The Jakarta Post (2024) takes a more confrontational stance by using active language to tell the news. Their headline, "Govt refuses to pay \$8 million," puts the government front and center as the one making the decision, showing they're active players in this situation. They also keep the verbs in the story lively, words like "refused" (by the government) and "threatened" (by hackers) pointing directly, making the story feel more urgent and intense. This approach lines up with Entman's idea of framing, which is about how the news shapes our view of problems and makes the consequences seem more dramatic. It also fits with Van Dijk's concept of how news is built to influence how we think about social issues, emphasizing urgency, responsibility, and risk. Unlike VOI, which tends to downplay the government behind the scenes, The Jakarta Post really pushes the idea that institutions are responsible, calling attention to accountability and the moral questions involved.

This way of framing fits with its role as a watchdog for democracy, challenging opacity and pushing for transparency. So, even though both outlets cover the same event, their language choices show their different priorities. VOI tends to soften its tone to protect institutions, while The Jakarta Post emphasizes governance, responsibility, and holding power to account.

3.1.3 Role Allocation

Van Leeuwen role allocation focus on specific roles (grammatical and semantic) to determine how the social actor being presented as an active or passive recipient in a given activity.

A. Data 9

1. VOI News: Phrases like “*the government has many tasks to improve its cybersecurity readiness*” position the state as a reformer with unfinished duties (VOI News, 2025).

This data was taken from VOI. (2025, January 3). A Myriad Of Government Homeworks Facing Cyber Attacks That Are Increasingly Growing. VOI.id. Retrieved on March 12, 2025, from <https://voi.id/en/bernas/447752>

2. The Jakarta Post: Writes that “*the government refused to pay US\$8 million despite ongoing service disruptions*” (The Jakarta Post, 2024).

This data was taken from The Jakarta Post. (2024, June 25). Govt refuses to pay \$8 million after ransomware attack on national data center. The Jakarta Post. Retrieved on March 13, 2025, from <https://www.thejakartapost.com/indonesia/2024/06/25/govt-refuses-to-pay-8-million-after-ransomware-attack-on-national-data-center.html>

B. Context of Data 9

This examines how VOI News and The Jakarta Post allocated roles to institutional actors in framing the 2024 Kominfo data breach, which followed a ransomware attack on the Temporary National Data Center (PDNS) that disrupted over 200 public services in June 2024. VOI News (2025) assigns the government the role of a delayed reformer, using phrases like “the government has many tasks to improve its cybersecurity readiness” to construct a narrative of obligation and institutional learning rather than immediate failure. This role allocation portrays the state as an actor, undergoing long-term development, aligning with a developmentalist ideology that emphasizes structural improvement over crisis accountability. In contrast, The Jakarta Post (2024) frames the government as a decisive leader under compulsion, especially by highlighting its refusal to pay a US\$8 million ransom. The article’s phrasing “the government refused to pay” showing that the actors has bold decision-makers facing complex moral and policy dilemmas. Both articles reflect the same setting of heightened national concern in mid-2024 but branching in rhetorical framing: VOI reinforces institutional legitimacy through patient reform, while The Jakarta Post emphasizes risk, responsibility, and institutional consequence, illustrating how role allocation functions as a critical discursive

strategy to frame agency, intent, and legitimacy (VOI News, 2025; The Jakarta Post, 2024; Van Leeuwen, 2008).

C. Analysis of Data 9

In the 2024 Kominfo data breach reporting, VOI News and The Jakarta Post used different strategies to define public perceptions of government responsibility. The Jakarta Post and VOI News differ in their characterization of the government regarding cybersecurity improvement and data breach accountability. According to VOI News (2025) the government acts as a late adopter of reforms to enhance cybersecurity while the breach does not directly result from government failure. Through its statement about government responsibilities to strengthen cybersecurity readiness VOI positions the entity as a party which maintains unfinished work rather than one that demonstrates failure. The role distribution framework resembles Van Leeuwen's (2008) concept which assigns a reformist role to the actor instead of making them responsible for negligent behavior. The government receives a student metaphor through the "homework" analogy which indicates a slow but continuous improvement approach that supports a perspective focused on building structures and capabilities rather than immediate fault. The government uses this rhetorical approach to show its ability to acquire knowledge from emergencies rather than breakdown in its obligation to safeguard public information.

The Jakarta Post for the year 2024 presented the government as an active decision-maker with moral obligations. Through its use of active constructions such as “the government refused to pay” the US\$8 million ransom, the outlet emphasizes a sense of agency and leadership under pressure. Unlike VOI’s soft reform framing, The Jakarta Post’s role allocation places the government in a high-stakes moral and policy dilemma, where refusal could be interpreted as courageous or reckless. This approach reflects a liberal-democratic framing, where state actors are expected to make bold decisions while being held accountable for their outcomes. The allocation of this assertive role is reinforced by dramatic lexical choices and omission of individual names, creating a faceless but responsible institutional body. The rhetorical effect is one of increased public security, where institutional legitimacy is not assumed but tested. Together, the two outlets represent the Kominfo breach through divergent role allocations VOI supports institutional continuity and progress, while The Jakarta Post invites civic evaluation of state leadership revealing how role assignment serves as a crucial linguistic and ideological tool in shaping media discourse on national crises.

4. Ideological Discourse Structures (Van Dijk, 2015)

Van Dijk’s (2015) framework identifies ideological structures embedded at the micro-level of discourse, particularly in how language constructs

representations of social actors, power relations, and institutional legitimacy. These ideological structures are not only reflected in what is said, but also in how it is said, including choices of grammar, modality, and lexical selection:

4.1 Description

Description describe members of the group or individuals, through their action to seek positive or negative of the self-presentation.

A. Data 10

VOI News: Describes the state as having “a myriad of government homeworks” and emphasizes the need to improve digital infrastructure without referring to specific failures or responsible individuals (VOI News, 2025).

This data was taken from VOI. (2025, January 3). A Myriad Of Government Homeworks Facing Cyber Attacks That Are Increasingly Growing. VOI.id. Retrieved on March 12, 2025, from <https://voi.id/en/bernas/447752>

The Jakarta Post: Uses terms like “demanded” and “threatened” in reference to the hackers and “refused to pay” for the government’s response (The Jakarta Post, 2024).

This data was taken from The Jakarta Post. (2024, June 25). Govt refuses to pay \$8 million after ransomware attack on national data center. The Jakarta Post. Retrieved on March 13, 2025, from <https://www.thejakartapost.com/indonesia/2024/06/25/govt-refuses-to-pay-8-million-after-ransomware-attack-on-national-data-center.html>

B. Context of Data 10

The analysis examines the description of organizational players in the 2024 Kominfo data breach by VOI News and The Jakarta Post. The editorial from VOI News in 2025 uses the term

“the government” to discuss KOMINFO (subsequently KOMDIGI) or BSSN without specifying any particular government elements which creates the perception of an anonymous state entity executing extended transformative measures. The presented image complies with an interpretation that prevents specific fault identification. The Jakarta Post in 2024 continues its policy of not mentioning names and instead uses forceful language to describe government decisions that demonstrate institutional authority and ethical judgment. Both news outlets employ actor descriptions in their post-June 2024 ransomware coverage of PDNS to control public reactions according to their strategic goals which protect institutional interests for VOI and promote government responsibility with significant judgment calls for The Jakarta Post (Van Leeuwen, 2008; VOI News, 2025; The Jakarta Post, 2024).

C. Analysis of Data 10

The 2024 Kominfo data breach analysis between VOI News and The Jakarta Post showed different rhetorical frameworks for assigning blame to organizations which affected the public perception of accountability and official standing. In their coverage of the 2024 Kominfo data breach, VOI News (2025) maintained a writing style which replaced specific agency names with the term “the government” and did not mention any official names. By referring to “the government” instead of using specific agency

names, VOI employed Van Leeuwen (2008) suppression and genericization through their linguistic approach. The absence of personalized details helps VOI present the government as a single entity facing general challenges rather than a specific leaders who missed the opportunity to stop the breach. VOI uses vague language to maintain trust in institutions while promoting a narrative of continuous improvement which supports an ideological perspective that values systematic governance over immediate responsibility.

The Jakarta Post (2024) refrains from mentioning specific individuals but demonstrates distinctive differences in its messaging style. The publication utilizes the term “the government” in its reports yet their actor portrait show more dynamic descriptions with stronger emphasis on results. The statement “the government refused to pay the ransom” places a strong moral choice onto the state which demonstrates full control while making altering decisions. The institutional determination receives a major focus through this actor description while simultaneously exposing the state to public examination because of its failure to prevent extensive negative effects from the breach. The Jakarta Post uses Van Dijk’s (2015) theoretical framework of ideological macrostructures to direct attention towards opposition and responsibility together with urgent action by emphasizing the state’s past decisions. The rhetorical strategy supports the publication’s

watchdog role according to Waisbord (2000) because it shows the state as a decision maker with major national consequences. The two media outlets express their institutional references through impersonal language usage, but their linguistic choices and ideological objectives demonstrate distinct separation: VOI uses neutral actor descriptions to safeguard institutional reputation whereas The Jakarta Post uses active institutional descriptions for democratic oversight and critical analysis.

2. Authority

Authority indicating the subject power over specific information, argument or any related to authority in a certain area, as the topic is about the media representation, it will be, then, show part of information containing subject authority.

A. Data 11

VOI News: Avoids quoting or naming individual officials; relies on abstract institutional references (VOI News, 2025).

This data was taken from VOI. (2025, January 3). A Myriad Of Government Homeworks Facing Cyber Attacks That Are Increasingly Growing. VOI.id. Retrieved on March 12, 2025, from <https://voi.id/en/bernas/447752>

The Jakarta Post: Relies on impersonal references like “officials stated” or “the government refused” (The Jakarta Post, 2024).

This data was taken from The Jakarta Post. (2024, June 25). Govt refuses to pay \$8 million after ransomware attack on national data center. The Jakarta Post. Retrieved on March 13, 2025, from <https://www.thejakartapost.com/indonesia/2024/06/25/govt-refuses-to-pay-8-million-after-ransomware-attack-on-national-data-center.html>

B. Context of Data 11

The research investigate the way VOI News and The Jakarta Post established authoritative coverage during their analysis of the 2024 Kominfo data breach. VOI News from 2025 does not directly mention KOMDIGI or BSSN or any other government entities but depends on general institutional terms like "the government" to describe systemic problems. The discussion maintains an impersonal tone which establishes a bureaucratic description of authority that avoids personal responsibility and supports an approach that views the state as capable but struggling with rising obstacles. The Jakarta Post (2024) does not disclose the names of individuals involved in their reports but assesses institutional power by focusing on state choices, including the rejection of an US\$8 million ransom, without using direct source citations. Media outlets build authority through selective information disclosure during their coverage following the June 2024 ransomware attack on Indonesia's Temporary National Data Center (PDNS); but, they demonstrate different ideological roles: VOI uses institutional language to endorse state power while The Jakarta Post uses ambiguous language to expose government opacity and encourage public doubt. (VOI News, 2025; The Jakarta Post, 2024; Van Leeuwen, 2008).

C. Analysis of Data 11

VOI News and The Jakarta Post adopted distinct methods to establish credibility when they reported the 2024 Kominfo data breach because these approaches demonstrate how institutions develop legitimacy through language. The 2025 VOI News report fails to mention specific statistics or name official government organizations like KOMDIGI and BSSN. The news outlet uses generic institutional terms to refer to “the government” and presents its information in a formal, bureaucratic manner. According to Van Leeuwen (2008), authorization by abstraction establishes authority through impersonal institutions which people accept without personal expertise or named figures. By avoiding direct quotes and named sources, the news outlet creates an unbiased perspective which presents the government as competent although it is overwhelmed by digital security issues. The language used in this approach to helps build institutional trust while promoting a media ideology which views the state as an unchanging institution in the fight against digital security threats. VOI News establishes trust through its reporting by presenting the government as a capable problem-solving entity which minimizes confusion about its abilities.

VOI News and The Jakarta Post adopted distinct methods to establish credibility when they reported the 2024 Kominfo data breach because these approaches demonstrate how institutions

develop legitimacy through language. The 2025 VOI News report fails to mention specific statistics or name official government organizations like KOMDIGI and BSSN. The news outlet uses generic institutional terms to refer to “the government” and presents its information in a formal, bureaucratic manner. According to Van Leeuwen (2008), authorization by abstraction establishes authority through impersonal institutions which people accept without personal expertise or named figures. By avoiding direct quotes and named sources, the news outlet creates an unbiased perspective which presents the government as competent although it is overwhelmed by digital security issues. The language used in this approach to journalism helps build institutional trust while promoting a media ideology which views the state as an unchanging reformist institution in the fight against digital security threats. VOI News establishes trust through its reporting by presenting the government as a capable problem-solving entity which minimizes confusion about its abilities.

3. Evidentiality

Evidentiality shows a fact that has a sign to support a specific side of the subject mentioned in the news.

A. Data 12

The Jakarta Post: States the hackers demanded a ransom of US\$8 million and reports service disruptions (The Jakarta Post, 2024).

This data was taken from The Jakarta Post. (2024, June 25). Govt refuses to pay \$8 million after ransomware attack on national data center. The Jakarta Post. Retrieved on March 13, 2025, from <https://www.thejakartapost.com/indonesia/2024/06/25/govt-refuses-to-pay-8-million-after-ransomware-attack-on-national-data-center.html>

VOI News: Omits numerical or technical specifics; emphasizes general conditions like “massive cyber threats” and “systemic vulnerabilities” (VOI News, 2025).

This data was taken from VOI. (2025, January 3). A Myriad Of Government Homeworks Facing Cyber Attacks That Are Increasingly Growing. VOI.id. Retrieved on March 12, 2025, from <https://voi.id/en/bernas/447752>

B. Context of Data 12)

This section focuses on evidentiality, or how media sources use facts, figures, and references to construct credibility and support claims in their coverage of the 2024 Kominfo data breach, following the June ransomware attack on Indonesia’s Temporary National Data Center (PDNS). VOI News uses broad generalizations such as “systemic vulnerabilities” and “massive cyber threats” without including specific details, numerical evidence, or quotes from named experts. In contrast, The Jakarta Post (2024) incorporates concrete, quantified data such as the exact ransom amount, “US\$8 million”, and the widespread service disruption caused by the attack. These evidentiary details anchor the report in specificity, enhancing its perceived objectivity and urgency. Both articles are situated within the national context of a high-profile cyberattack that raised concerns about state capacity and public data security. However, the difference in evidential strategies reflects their ideological orientations: VOI uses generalized

claims to sustain institutional credibility, while The Jakarta Post employs precise figures and outcome-based framing to encourage scrutiny and convey the gravity of the incident (VOI News, 2025; The Jakarta Post, 2024; Van Dijk, 2015).

C. Analysis of Data 12)

In their coverage of the 2024 Kominfo data breach, VOI News and The Jakarta Post employed contrasting evidential strategies that shaped how the crisis was represented. VOI News (2025) relied on vague, generalized terms such as “systemic vulnerabilities” and “massive cyber threats” without citing specific figures, technical details, or expert sources. This lack of concrete evidence served to reduce the immediacy and severity of the event, aligning with a narrative that presents the breach as part of a broader institutional learning curve. The use of abstract evidentiality supports Van Dijk’s (2015) concept of ideological vagueness, framing the state as a passive actor facing structural challenges rather than direct failure.

By contrast, The Jakarta Post (2024) employed specific evidential markers to enhance credibility and urgency, by citing the hackers’ demand of “US\$8 million” and widespread service disruption. These quantifiable details created a heightened sense of consequence and accountability, consistent with Entman’s (1993) framing of severity and risk. Though it also omitted named officials, the report’s use of factual precision supported its watchdog role, encouraging critical public evaluation of the government’s

decisions. In doing so, The Jakarta Post used evidentiality not just to inform, but to position the breach as a politically charged failure of preparedness.

4. Polarization

Expressing polarized cognition and the categorial division of people ingroup and outgroup, us vs them, by highlightning positive in us, and negative in them.

A. Data 13

The Jakarta Post: Emphasizes binary tensions government vs hackers, payment vs refusal (The Jakarta Post, 2024).

This data was taken from The Jakarta Post. (2024, June 25). Govt refuses to pay \$8 million after ransomware attack on national data center. The Jakarta Post. Retrieved on March 13, 2025, from <https://www.thejakartapost.com/indonesia/2024/06/25/govt-refuses-to-pay-8-million-after-ransomware-attack-on-national-data-center.html>

VOI News: Avoids binary oppositions and does not define a direct adversary (VOI News, 2025).

This data was taken from VOI. (2025, January 3). A Myriad Of Government Homeworks Facing Cyber Attacks That Are Increasingly Growing. VOI.id. Retrieved on March 12, 2025, from <https://voi.id/en/bernas/447752>

B. Context of Data 13

This section examines how VOI News and The Jakarta Post used polarization in framing the 2024 Kominfo data breach, following the June ransomware attack on the Temporary National Data Center (PDNS). VOI News (2025) avoids oppositions, framing the breach as a systemic issue and emphasizing the government's ongoing “homework” without positioning clear enemy, which is the hacker. This depolarized narrative supports a tone that softens crisis perception. In contrast, The Jakarta Post (2024) constructs a clear stance between state and attacker through active, conflict-driven

language such as “hackers threatened” and “government refused to pay,” highlighting moral tension and institutional pressure. These differing strategies reflect their ideological alignments. VOI seeks to preserve institutional legitimacy, while The Jakarta Post intensifies confrontation to stress accountability and state vulnerability (VOI News, 2025; The Jakarta Post, 2024; Van Dijk, 2015).

C. Analysis of Data 13

In covering the 2024 Kominfo data breach, VOI News (2025) adopts a depolarized narrative, avoiding subject of the cause between the government and the attackers. Rather than frame the event as a conflict, VOI uses abstract language like “systemic vulnerabilities” and “homework” to emphasize institutional challenges and reform. This rhetorical choice reflects Van Dijk’s (2015) concept of ideological moderation, where the absence of opposite framing serves to soften public perception and maintain trust in state institutions. The focus on long-term governance rather than immediate tension supports VOI’s stance, presenting the government as a capable but evolving actor.

Conversely, The Jakarta Post (2024) employs polarization to dramatize the event, constructing a clear opposition between hackers and the state. Phrases like “hackers threatened” and “government refused to pay” establish a structure that highlights conflict, urgency, and moral pressure. This aligns with Entman’s (1993) framing theory, where conflict enhances

narrative engagement and encourages public security. While still using institutional abstraction, the active, high-stakes language reflects The Jakarta Post's watchdog role, inviting readers to critically assess government decisions and transparency in times of crisis.

5. Empathy

Is treated as sociocognitive element that can be changed through discourse to shape social attitudes and relations, instead of using text, social cognition, or social context.

A. Data 14

Neither VOI nor TJP includes public voices or references to affected individuals (VOI News, 2025; The Jakarta Post, 2024).

This data was taken from VOI. (2025, January 3). A Myriad Of Government Homeworks Facing Cyber Attacks That Are Increasingly Growing. VOI.id. Retrieved on March 12, 2025, from <https://voi.id/en/bernas/447752>

This data was taken from The Jakarta Post. (2024, June 25). Govt refuses to pay \$8 million after ransomware attack on national data center. The Jakarta Post. Retrieved on March 13, 2025, from <https://www.thejakartapost.com/indonesia/2024/06/25/govt-refuses-to-pay-8-million-after-ransomware-attack-on-national-data-center.html>

B. Context of Data 14

This section examines how VOI News and The Jakarta Post addressed, empathy in their coverage of the 2024 Kominfo data breach. Both reports, set in the aftermath of the June ransomware attack on the PDNS, focus on institutional response while excluding citizen perspectives or emotional narratives. VOI News (2025) uses abstract terms like “systemic vulnerabilities” without mentioning affected individuals, while The Jakarta Post (2024) highlights policy decisions such as the

government's refusal to pay ransom, but similarly, avoids personal accounts. This omission reflects a top-down framing that emphasizes structural and political implications over human impact, shaping public understanding through institutional, rather than empathetic, discourse (VOI News, 2025; The Jakarta Post, 2024; Van Dijk, 2011).

C. Analysis of Data 14

Both VOI News and The Jakarta Post demonstrate a lack of empathetic framing in their coverage of the 2024 Kominfo data breach. VOI News (2025) uses abstract and institutional language like “systemic vulnerabilities” and “cybersecurity homework,” focusing on structural reform while omitting the human impact of service disruptions. This top-down approach reflects Van Dijk's (2011) concept of depersonalized discourse, where emotional connection is replaced by technical expert framing, reinforcing institutional legitimacy over citizen experience.

Similarly, The Jakarta Post (2024) emphasizes government decisions, such as the refusal to pay ransom money without including personal stories or emotional perspectives. While the article highlights national-level risks and institutional accountability, it excludes the lived realities of those affected by the breach. This omission limits public empathy and reinforces a policy-focused narrative. Both outlets, despite different tones, present the breach as a state-centered issue, using rhetorical omission of empathy to control how the crisis is perceived.

4.4 Fairclough's Three-Dimensional Model (1995)

Norman Fairclough's (1995) three-dimensional model of discourse analysis provides a comprehensive framework for understanding how discourse operates simultaneously at textual, discursive, and sociocultural levels. This model is particularly valuable in identifying how media texts reflect, reinforce, or resist dominant power structures. It consists of three interrelated dimensions: (1) textual Analysis of description), (2) discourse practice (interpretation), and (3) sociocultural practice (explanation). In analyzing the media representations of the 2024 PDNS ransomware attack, these dimensions reveal not only the linguistic construction of meaning but also how ideology and institutional authority are embedded and reproduced in the discourse.

4.4.1 Textual Analysis

Text is the first step in three-dimensional framework CDA by Leeuwen that covers written and spoken word inside the work. Focusing in linguistic structure through text analysis.

A. Data 15

VOI News: Uses neutral institutional expressions such as "systemic vulnerabilities," "massive threats," and metaphors like "homework to be completed," along with modal verbs such as "must," "need to," and "should" (VOI News, 2025).

This data was taken from VOI. (2025, January 3). A Myriad Of Government Homeworks Facing Cyber Attacks That Are Increasingly Growing. VOI.id. Retrieved on March 12, 2025, from <https://voi.id/en/bernas/447752>

The Jakarta Post: Uses active constructions such as "Government refuses to pay," "Hackers threatened," and

“Cyberattack disrupted immigration systems” (The Jakarta Post, 2024).

This data was taken from The Jakarta Post. (2024, June 25). Govt refuses to pay \$8 million after ransomware attack on national data center. The Jakarta Post. Retrieved on March 13, 2025, from <https://www.thejakartapost.com/indonesia/2024/06/25/govt-refuses-to-pay-8-million-after-ransomware-attack-on-national-data-center.html>

B. Context of Data 15

This section examines how VOI News and The Jakarta Post framed the 2024 Kominfo data breach following the June ransomware attack on the PDNS. VOI News (2025) presents the incident as part of ongoing institutional reform, using abstract terms like “government homework” without naming specific actors. In contrast, The Jakarta Post (2024) focuses on the government’s refusal to pay a US\$8 million ransom, using more direct and active language. While both address the same event, they differ in tone and emphasis. While VOI highlights reform, The Jakarta Post stresses decision-making and risk.

C. Analysis of Data 15

VOI News (2025) and The Jakarta Post (2024) represented the 2024 Kominfo data breach using distinct rhetorical strategies tied to their ideological orientations. VOI framed the incident as part of ongoing institutional “homework,” using abstract, passive language and avoiding blame. Using of general terms and absence of specific actors or emotional impact reflected on the approach, portraying the breach as a systemic issue tied to national reform, rather than a failure of governance.

In contrast, The Jakarta Post used active voice and evidential detail, such as the US\$8 million ransom to construct a more urgent, polarized narrative. While still referring to “the government” in general terms, it emphasized agency and accountability through strong action verbs like “refused” and “threatened.” This framing supports its watchdog role, inviting critical public engagement. Despite their differences, both outlets omitted empathetic language and citizen perspectives, focusing instead on institutional responses. These rhetorical patterns reveal how language was used to frame legitimacy, risk, and responsibility in shaping public understanding of the breach.

4.4.2 Discourse Practice

Discourse Practice examine the text production, text distribution, and textconsumption, that may indidcate the writer ideology from the text written.

A. Data 16

VOI News: Does not quote individual officials but reflects institutional tone and reproduces bureaucratic perspectives (VOI News, 2025).

This data was taken from VOI. (2025, January 3). A Myriad Of Government Homeworks Facing Cyber Attacks That Are Increasingly Growing. VOI.id. Retrieved on March 12, 2025, from <https://voi.id/en/bernas/447752>

The Jakarta Post: Summarizes institutional actions and omits direct quotations, but frames through interpretative commentary (The Jakarta Post, 2024).

This data was taken from The Jakarta Post. (2024, June 25). Govt refuses to pay \$8 million after ransomware attack on national data center. The Jakarta Post. Retrieved on March 13, 2025, from <https://www.thejakartapost.com/indonesia/2024/06/25/govt-refuses-to-pay-8-million-after-ransomware-attack-on-national-data-center.html>

B. Context of Data 16

This section examines how VOI News and The Jakarta Post framed the 2024 Kominfo data breach following the June ransomware attack on the PDNS. VOI News (2025) uses an institutional voice to describe the breach as a structural issue, emphasizing “systemic vulnerabilities” and avoiding blame or specific actors. In contrast, The Jakarta Post (2024) highlights the government’s refusal to pay a US\$8 million ransom, using active, conflict-oriented language. Both were published during heightened public concern but differ in tone and framing. VOI presents reflection, while The Jakarta Post stresses urgency and accountability.

C. Analysis of Data 16

VOI News (2025) framed the 2024 Kominfo data breach through abstract, reform-oriented language. By using terms like “systemic vulnerabilities” and “government homework,” VOI downplayed urgency and avoided naming specific actors, relying on passivation and exclusion to maintain a narrative of institutional growth. This rhetorical strategy aligns with its ideology, presenting the breach as part of Indonesia’s digital transformation rather than a moment of institutional failure.

In contrast, The Jakarta Post (2024) used more active and polarized language, highlighting the government’s refusal to pay the US\$8 million ransom and stressing the moral and strategic weight of that decision. Through activation, evidential detail, and conflict framing, the outlet

positioned the breach as a test of government accountability and risk management. While both reports avoided personalizing the impact, The Jakarta Post's discourse encouraged security, whereas VOI's sought to protect institutional credibility. These contrasting approaches reflect how linguistic choices shape public perception of crisis and responsibility.

4.4.3 Sociocultural Practice

It investigate how discourse function in field of society and need both, from the text and discourse practice, in order to get better understanding and obtaining information through sociocultural practice.

A. Data 17

VOI News: Frames cybersecurity issues as an evolving national responsibility, emphasizing the need to improve systems without assigning blame or moral judgment (VOI News, 2025).

This data was taken from VOI. (2025, January 3). A Myriad Of Government Homeworks Facing Cyber Attacks That Are Increasingly Growing. VOI.id. Retrieved on March 12, 2025, from <https://voi.id/en/bernas/447752>

TJP: Highlights tension, policy stakes, and ambiguity in government decision-making (The Jakarta Post, 2024).

This data was taken from The Jakarta Post. (2024, June 25). Govt refuses to pay \$8 million after ransomware attack on national data center. The Jakarta Post. Retrieved on March 13, 2025, from <https://www.thejakartapost.com/indonesia/2024/06/25/govt-refuses-to-pay-8-million-after-ransomware-attack-on-national-data-center.html>

B. Context of Data 17

This section examines how VOI News and The Jakarta Post construct meaning in their coverage of the 2024 Kominfo data leak following the June ransomware attack on the PDNS. VOI News (2025) presents the breach as part of a broader digital reform effort, using abstract

terms like “systemic vulnerabilities” and avoiding specific attribution. In contrast, The Jakarta Post (2024) highlights the government's refusal to pay a US\$8 million ransom, using active language to frame the incident as a direct confrontation. Both were published during heightened public concern but differ in tone. VOI offering institutional reflection, The Jakarta Post emphasizing urgency and decision making, providing contrasting narrative settings for discourse analysis.

C. Analysis of Data 17

VOI News (2025) constructs the Kominfo data breach through abstract language and a reform-oriented lens. The outlet avoids technical specifics and personal impact, instead using general terms like “government homework” and “cybersecurity readiness” to portray the issue as part of an ongoing institutional development process. This use of passive voice and depersonalized framing reduces urgency and deflects direct blame, aligning with the narrative that prioritizes national progress over immediate accountability.

In contrast, The Jakarta Post (2024) takes a more active and critical approach, emphasizing the government's decision to refuse the US\$8 million ransom and presenting the breach as a high-stakes policy challenge. The use of activation, evidentiality, and binary framing positions the state as a decision-maker under pressure, inviting public scrutiny. While both outlets avoid emotional storytelling, The Jakarta Post's tone fosters

accountability, whereas VOI promotes institutional stability. These contrasting strategies show how linguistic framing influences public perception of state legitimacy and responsibility during a cybersecurity crisis.

4.5 Framing Analysis of Entman

Framing, as theorized by Robert Entman (1993), involves the selection and emphasis of certain aspects of perceived reality to promote particular problem definitions, causal interpretations, moral evaluations, and treatment recommendations. The power of framing lies in its ability to structure how audiences interpret complex events. In the context of the 2024 ransomware attack on Indonesia's Temporary National Data Center (PDNS), both VOI News and The Jakarta Post deploy distinct frames that guide public perception in ideologically significant ways.

A. Data 18

VOI News (2025) – the editorial titled *Cybersecurity as Institutional Homework*:

Excerpt 1: “The government still has a myriad of homework to do in terms of cybersecurity infrastructure.”

Excerpt 2: “Systemic vulnerabilities continue to haunt our digital transformation, and the state must catch up with growing technological threats.”

These statements are analyzed for their use of abstraction, institutional generalization, and the absence of direct attribution to individuals or agencies.

These datas were taken from VOI. (2025, January 3). A Myriad Of Government Homeworks Facing Cyber Attacks That Are Increasingly

Growing. VOI.id. Retrieved on March 12, 2025, from <https://voi.id/en/bernas/447752>

From **The Jakarta Post** (August 2024) – news article reporting on the incident:

Excerpt 1: “The government refused to pay the US\$8 million ransom demanded by the hackers.”

Excerpt 2: “Hackers threatened to release sensitive data if the ransom was not paid.”

These excerpts are selected for their use of active voice, conflict framing, and clear positioning of agency between actors (government vs. hackers), as well as the inclusion of specific figures.

These selected excerpts provide the basis for analyzing how each outlet frames the incident through linguistic and ideological choices.

This data was taken from The Jakarta Post. (2024, June 25). Govt refuses to pay \$8 million after ransomware attack on national data center. The Jakarta Post. Retrieved on March 13, 2025, from <https://www.thejakartapost.com/indonesia/2024/06/25/govt-refuses-to-pay-8-million-after-ransomware-attack-on-national-data-center.html>

B. Context of Data 18

The selected data comes from news and editorial coverage of the June 2024 ransomware attack on Indonesia’s Temporary National Data Center (PDNS), which affected over 200 government services. VOI News, in a 2025 editorial, reflects on the breach as a broader policy issue within Indonesia’s digital transformation. The article adopts a collective voice, presenting the government as an abstract entity engaged in long-term institutional reform. In contrast, The Jakarta Post provides real-time news coverage published during the immediate aftermath of the attack. It emphasizes the state’s refusal to negotiate with hackers and describes the attack as a direct threat to national data security. While both discuss the same

event, they differ in tone, structure, and rhetorical emphasis one editorial, the other news reportage.

C. Analysis of Data 18

The two media outlets represent the Kominfo data breach through different significance different strategies. VOI News uses generalized language like “homework” and “systemic vulnerabilities,” along with passive voice and institutional abstraction. These linguistic patterns reflect a developmentalist framing, portraying the breach as a natural obstacle in Indonesia’s modernization. By avoiding specific actors and omitting public or emotional responses, VOI positions the government as a well-meaning institution in need of reform, not accountability. This use of rhetorical softening and omission aligns with an intent to maintain institutional legitimacy and focus public attention on future improvement rather than past failure.

In contrast, The Jakarta Post apply a more critical frame. By stating “The government refused to pay” and “Hackers threatened,” it uses activation and polarization to construct a confrontational narrative between two distinct subject. The inclusion of a specific ransom figure (US\$8 million) introduces evidentiality, increasing perceived credibility and urgency. While the article also avoids naming officials, it nonetheless emphasizes state decision-making and risk. The rhetorical strategy aligns with the outlet’s watchdog role, using factual precision and active language

to scrutinize government response. Both articles exclude empathic framing, but The Jakarta Post’s activation and risk-oriented language invite public judgment, while VOI’s abstraction escalates critique.

Table 1 Framing Functions Comparison (Adapted from Entman, 1993)

Framing Function	VOI News (2025) – <i>Cybersecurity as Institutional Homework</i>	The Jakarta Post (2024) – <i>Govt refuses to pay \$8 million ransom</i>
Defining Problems	Cybersecurity weaknesses framed as ongoing governance “homework”	Described as a national security breach with real-world consequences
Diagnose Causes	Vague causes: “systemic vulnerabilities” and digital transition challenges	Implied causes: unprepared institutions, attacker demands, and weak security
Make Moral Judgments	Avoids blame; presents state as a reformer	Suggests moral tension in government’s refusal to pay ransom
Suggest Remedies	Long-term institutional reform and policy improvement	Implied need for stronger security, transparency, and preparedness

B. Discussion

This study's findings reveal that the most dominant data type is textual discourse, specifically in the form of linguistic constructions and rhetorical strategies used in news articles from two contrasting Indonesian media outlets: VOI News and The Jakarta Post. The Analysis show that, The Jakarta Post uses a Crisis Framework that emphasizes systemic vulnerabilities. This is in line with Sari's (2023) argument, which states that The Jakarta Post often constructs a narrative of "data sovereignty" as a criticism of state policy. This study confirms Sari's observations but adds a new layer of evidence: the use of Negative Agency (Van Leeuwen, 2008). By portraying the government as "vague" or "ineffective," the media not only reports on the crisis; it rhetorically creates a space of resistance against the government's attempts to blame the public. These textual data, including key sentences such as "The government still has a myriad of homework to do in terms of cybersecurity infrastructure" (VOI News) and "The government refused to pay the US\$8 million ransom demanded by the hackers" (The Jakarta Post), are rich in ideological meaning. They are particularly valuable for applying critical discourse analysis because they demonstrate how meaning is constructed through choices in actor representation, lexical selection, and framing structures. Textual data are dominant in this research because they allow close analysis at both the micro-linguistic level (such as verb use, passivization, and abstraction) and the macro-discursive level (such as framing, narrative structure, and ideological positioning). This emphasis on language aligns with the central concerns of critical discourse analysis, especially through the lens of Van Dijk's socio-cognitive model,

Van Leeuwen's social actor representation theory, Fairclough's three-dimensional discourse model, and Entman's framing theory. Previous studies, such as Susanto & Dahlia (2023) on the Bjorka data leak, were limited to a macro framework, identifying what was said rather than how it was constructed linguistically. This study fills that gap by providing a micro-rhetorical analysis. Although Hidayat & Zarkasi (2024) claim that media narratives are heavily focused on "cybersecurity awareness," this study reveals that "awareness" is often used as a rhetorical device for agent transfer. Furthermore, this study addresses the methodological void identified in Rahman (2023) and Wibowo et al. (2023) by providing a direct comparative analysis. By comparing VOI News and The Jakarta Post side by side, this study proves that the 2024 data leak is not a singular narrative. Instead, it is a "dual reality" constructed through language: one reality focuses on government recovery and resilience, and the other focuses on systemic failure and risk. Using Fairclough's (1995) three-dimensional model, the discussion shows that the Textual Dimension (specific words used) cannot be separated from Discursive Practice (media ideology).

In contrast, the less dominant type of data in this research is non-textual content such as multimedia elements, audience reactions, or visual framing. This exclusion is methodological: the study is text-based and focuses on institutional narratives as they are constructed through language. Including social media responses, user comments, or visual images would have expanded the scope beyond what is manageable in a focused critical discourse analysis framework. While such elements are increasingly relevant in digital journalism, they are excluded here to

allow for a deep analysis of formal news discourse, which remains a primary site of ideological construction. These excluded modalities such as infographics, comment sections, or audio-visual storytelling may provide complementary insights but would require a multi-modal discourse analysis approach, which falls outside the scope of this research. Nonetheless, future studies could build on these findings by examining how the discursive strategies found in text are amplified or contested in other media formats and among audiences.

A particularly unique aspect of this research lies in its comparative approach, analyzing two ideologically distinct news outlets reporting on the same national crisis, the 2024 Kominfo data breach caused by a ransomware attack on the Temporary National Data Center (PDNS). This attack disrupted over 200 government services, yet the two outlets framed the issue in sharply contrasting ways. VOI News adopted a development-oriented, reformist tone, portraying the state as a rational but overburdened actor facing “systemic vulnerabilities” and “homework” in cybersecurity. The Jakarta Post, by contrast, used more confrontational language, emphasizing the government's active refusal to pay the ransom and the high stakes involved, thus placing the state in a position of agency, responsibility, and moral decision-making. This contrast illustrates the ideological divergence between a reformist, legitimacy-focused media outlet and a liberal-democratic, accountability-focused publication. It is rare in Indonesian media research to find such direct comparative framing of the same event with equal textual weight given to editorial commentary and news reporting. This uniqueness enables a robust application of Entman’s (1993) framing theory, which looks at how

media define problems, diagnose causes, make moral judgments, and suggest remedies.

In terms of contribution to previous research, this study fills a gap in the existing body of literature on media discourse in Indonesia, which has primarily focused on the representation of political figures or electoral issues, such as media portrayals of Joko Widodo or other public officials. Most existing studies have relied on thematic content analysis or sentiment analysis, which provide valuable surface-level insights but often miss the deeper linguistic mechanisms through which ideology operates. By using a critical discourse analysis framework that draws from Van Dijk, Van Leeuwen, Fairclough, and Entman, this research brings a new perspective to how cybersecurity is framed in national media, especially during crises involving state institutions. It reveals how seemingly neutral linguistic choices, such as using passive voice, avoiding direct attribution, or omitting emotional appeals, can serve powerful ideological functions. The study also demonstrates how different media genres (editorial vs. hard news) shape the rhetorical construction of crises, with *VOI* relying on reform metaphors and institutional abstraction, while *The Jakarta Post* emphasizes policy action and institutional tension. These findings contribute to our understanding of how media framing not only reports on reality but actively shapes the public's cognitive and emotional engagement with national crises.

The theoretical frameworks applied in this study offer a coherent lens for interpreting the discursive features of the selected texts. Van Dijk's socio-cognitive model helps unpack how language reinforces social hierarchies and mental models

of institutional legitimacy. His concepts of *positive self-presentation* and *ideological square* are especially useful in analyzing VOI News' protective stance toward government actors. Van Leeuwen's theory of social actor representation guides the analysis of how actors are included, excluded, activated, or passivated within the text, revealing, for example, how both articles avoid naming specific officials, but for different ideological reasons. Fairclough's three-dimensional model supports an integrated analysis of text, discourse practice, and social practice, providing context to the power structures influencing journalistic choices. Finally, Entman's framing theory offers a functional framework for comparing the discursive goals of the two texts defining the breach as a policy issue versus a political crisis; diagnosing failure as structural versus moral; and suggesting reform versus institutional accountability.

Despite the richness of the data, the study is not without limitations. First, the data sample is narrow, focusing only on two news outlets and two articles. While these sources were selected for their ideological contrast and textual richness, they may not fully represent the broader media discourse surrounding the Kominfo data breach. Including additional media sources such as Kompas, Tempo, CNN Indonesia, or Detik could offer a wider spectrum of ideological positioning and framing strategies. Second, the research is limited to textual data and does not engage with audience reception or visual media, which are increasingly central in digital journalism. This means the study does not capture how readers actually interpret these texts, nor does it account for how visual or multimedia cues may influence meaning. Third, the analysis is temporally limited to immediate responses

following the breach. A longitudinal study tracking how coverage evolves over weeks or months would provide further insight into how media narratives develop or shift in response to institutional actions, public reaction, or follow-up incidents.

Lastly, the absence of audience-based data such as comments, surveys, or interviews means that conclusions about media influence remain speculative. While discourse analysis can infer ideological effects, it cannot definitively measure how these frames impact public understanding or behavior. Thus, future research should consider integrating discourse analysis with reception studies to gain a fuller picture of media influence in the context of national digital security and institutional trust. Nonetheless, within the constraints of this study, the findings make a valuable contribution to the understanding of Indonesian media discourse, showing that even in the absence of overt political rhetoric, subtle language choices such as who is mentioned, how actions are described, and what perspectives are omitted play a crucial role in shaping how the public perceives national crises.

CHAPTER V

CONCLUSION AND SUGGESTION

A. CONCLUSION

This study's comparative discourse analysis of VOI News and The Jakarta Post coverage of the 2024 Kominfo data breach reveals how media framing constructs competing realities of the same cybersecurity crisis. Using CDA frameworks from Van Dijk, Van Leeuwen, Fairclough, and Entman, the research demonstrates that both news outlets engage in ideologically loaded discourse strategies that reflect their institutional alignments and editorial positions.

VOI News (2025) adopts a developmentalist and bureaucratic narrative, framing the breach as a symptom of long-term institutional "homework" rather than immediate failure. The outlet uses depersonalized language, avoids dramatization, and emphasizes the need for systematic improvement—thereby fostering trust in government capacity while avoiding overt critique. Its framing promotes institutional legitimacy through a tone of reformist optimism and passive responsibility, exemplifying Van Dijk's (2015) concept of positive self-presentation and Fairclough's (1995) idea of hegemonic discourse reproduction.

The Jakarta Post, by contrast, exercises a watchdog function, highlighting institutional opacity, crisis urgency, and policy consequence. Its reporting uses active language, evidential specificity (e.g., "US\$8 million ransom"), and exclusion of personal actors to emphasize bureaucratic accountability while dramatizing state

decisions. Through lexical urgency and confrontation framing, it constructs a macrostructure of institutional risk and strategic ambiguity, aligning with Entman's (2004) framing theory and the liberal-democratic ideals of press independence (Waisbord, 2000).

Together, the findings suggest that media discourse is not merely a descriptive account of events but a mechanism of ideological control and public influence. By emphasizing or omitting actors, causes, consequences, and solutions, both outlets reproduce power relations, reinforce or challenge institutional authority, and shape how citizens perceive state competence in the digital age.

This chapter affirms that Critical Discourse Analysis (CDA) is a powerful tool for uncovering how news texts act as sociocognitive instruments that manage public meaning. As Indonesia continues to face evolving cyber threats, understanding media's ideological role in constructing state-public relations is vital for ensuring informed democratic participation and robust digital governance.

B. SUGGESTION

While this study offers a deep comparative analysis between VOI News and The Jakarta Post, it is limited by its scope focusing exclusively on two national, English-language media outlets. This leaves out other significant sources such as regional news media, citizen journalism, television broadcasts, and social media discourse, all of which contribute to the pluralistic construction of public opinion in Indonesia.

Future research should consider:

- Expanding the media sample to include regional press (e.g., Jawa Pos, Tribun Network), broadcast outlets (e.g., Metro TV, TV One), and user-generated content.
- Incorporating multilingual discourse, especially in Bahasa Indonesia and local dialects, to capture how diverse audiences engage with national cybersecurity narratives.
- Analyzing temporal framing, observing how discourse shifts before, during, and after key events.
- Exploring multimodal CDA, integrating visual elements (e.g., images, infographics, headlines) alongside textual analysis.

Additionally, scholars should investigate how media framing influences policy development, public trust, and citizen awareness in digital risk contexts—especially as Indonesia implements new data protection regulations.

In conclusion, critical engagement with media discourse is not only relevant to communication and linguistics but increasingly essential for public policy, cybersecurity strategy, and democratic accountability in the digital era.

REFERENCES

- Anastasya, Z., & Effendi, A. (2023). Study of Critical Discourse Analysis of CDA) Teun a van Dijk in Jokowi News Sentil Minister Related to Oil Price Increase in Beritasatu. com. Britain International of Linguistics Arts and Education (BLoLAE) Journal, 5(2), 111-123.
- Badara, A., Amirudin, A., & Suardika, K. (2023). Representation of Indonesian Leaders Post Covid-19 Revealed Through On Line Media Reports by BCC Indonesia and CNN Indonesia: A Study of Critical Discourse Analysis. *International Journal of Education and Literature*, 2(3), 123-138.
- Cahyaningsih, O., & Pranoto, B. E. (2021). a Critical Discourse Analysis: the Representation of Donald Trump in the Reuters and the New York Times Towards the Issue of# Blacklivesmatter. *Linguistics and Literature Journal*, 2(2), 75-83.
- Dahunsi, T. N., & Ibiyemi, O. O. BIAS AND IDEOLOGY IN NEWSPAPERS' REPORTAGE OF HERDSMEN RELATED CRIMES IN NIGERIA.
- Das, A. K. Lexical Choice and Critical Discourse Analysis of Language Bias in Media.
- De Vreese, C. H. (2005). News framing: Theory and typology. *Information design journal+ document design*, 13(1), 51-62.
- Entman, R. M. (1993). Framing: Toward clarification of a fractured paradigm. *Journal of Communication*, 43(4), 51–58. <https://doi.org/10.1111/j.1460-2466.1993.tb01304.x>
- Fairclough, N. (2003). *Analyzing discourse: Textual analysis for social research*. London: Routledge.
- Fairclough, N. (1995). *Media discourse*. Edward Arnold.
- Fairclough, N. (1995a). *Critical discourse analysis: The critical study of language*. Harlow, UK: Longman.
- Fauzi, A., & Utami, P. (2023). The language of denial: Passive voice in government-leaning news. *Journal of Applied Linguistics and Rhetoric*, 5(2), 112–125.
- Goffman, E. (1974). *Frame analysis: An essay on the organization of experience*. Cambridge, MA: Harvard University Press.
- Güran, M. S., & Özarslan, H. (2022). Framing theory in the age of social media. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, (48), 446-457.
- Hafiane, I. A Critical Discourse Analysis of Al Jazeera English and BBC News Headlines (Doctoral dissertation, Kasdi Merbah Ouargla University).

- Hidayat, S., & Zarkasi, I. (2024). Cybersecurity awareness and media narratives: A content analysis. *Indonesian Journal of Communication Studies*, 12(1), 45–60.
- Indriani, L. (2024). Power and resistance in Indonesian digital media discourse. *Journal of Critical Discourse Studies*, 8(3), 201–218.
- Li, K., & Zhang, Q. (2022). A corpus-based study of representation of Islam and Muslims in American media: Critical Discourse Analysis Approach. *International Communication Gazette*, 84(2), 157–180.
- Nugraha, E. (2025). Comparative media rhetoric in the era of digital vulnerability. *Global Media Journal: Indonesia Edition*, 14(1), 15–32.
- Omolabi, I. (2023). A critical discourse analysis of selected print media reports on insurgency in Nigerian newspapers. *Journal of Languages, Linguistics and Literary Studies*, 3(1), 20–29.
- Pratama, A. (2024). Crisis communication strategies of Kominfo during the PDNS ransomware. *Public Relations and Crisis Management Journal*, 7(4), 310–325.
- Rahman, F. (2023). Van Dijk's ideological square in digital media reports on data leaks. *Discourse and Society Quarterly*, 9(2), 77–92.
- Rahman, M. M., & Arefin, S. (2024). A Comparative Critical Discourse Analysis of the Two News Articles from the BBC News and the Hindustan Times. *Journal of Applied Linguistics and Language Research*, 11(2), 79–97.
- Rizaldi, S. (2022). A critical discourse analysis on ideological representation of The Jakarta Post and The New York Times' Covid-19-related news (Doctoral dissertation, Universitas Islam Negeri Maulana Malik Ibrahim).
- Rubing, G., & Sandaran, S. C. (2023). A critical discourse analysis of news discourse on in the times. *International Journal of Academic Research in Business and Social Sciences*, 13(1), 968–984.
- Sari, R. (2023). The ideological construction of data sovereignty in The Jakarta Post. *International Journal of Media and Cultural Politics*, 19(1), 50–68.
- Sari, K., & Pranoto, B. E. (2021). Representation of Government Concerning the Draft of Criminal Code in The Jakarta Post: A Critical Discourse Analysis. vol, 11, 98–113.
- Susanto, B., & Dahlia, M. (2023). Framing the Bjorka data breach in national news. *Communication and Information Technology Journal*, 11(3), 140–155.
- Solove, D. J. (2011). *Nothing to hide: The false tradeoff between privacy and security*. Yale University Press.

- Tempo. (2024, June 25). PDNS decryption key offered, but hackers threaten Kominfo data release on denial. Retrieved from <https://en.tempo.co/read/1887231/pdns-decryption-key-offered-but-hackers-threaten-kominfo-data-release-on-denial>
- The Jakarta Post. (2024, June 25). Govt refuses to pay \$8 million after ransomware attack on National Data Center. Retrieved from <https://www.thejakartapost.com/indonesia/2024/06/25/govt-refuses-to-pay-8-million-after-ransomware-attack-on-national-data-center.html>
- Van Dijk, T. A. (1998). *Ideology: A multidisciplinary approach*. Sage Publications.
- Van Dijk, T. A. (2006). Discourse and manipulation. *Discourse & Society*, 17(3), 359–383. <https://doi.org/10.1177/0957926506060250>
- Van Leeuwen, T. (2008). *Discourse and practice: New tools for critical discourse analysis*. Oxford University Press.
- VOI. (2025, January 03). A Myriad Of Government Homeworks Facing Cyber Attacks That Are Increasingly Growing. VOI.id. <https://voi.id/en/bernas/447752>
- Wibowo, A., et al. (2023). Representing social actors in Indonesian cybersecurity discourse. *Humaniora Linguistics Journal*, 35(2), 160–178.
- Yunita, A. N. (2023). *CRITICAL DISCOURSE ANALYSIS IN DONALD TRUMP'S TERRORISM NATIONAL SECURITY SPEECH* (Doctoral dissertation, UIN RADEN INTAN LAMPUNG).

APPENDIX

A. The Jakarta Post

The government will not pay the US\$8 million ransom demanded by attackers responsible for the ransomware attack at two temporary National Data Center (PDN) facilities since last week that disrupted public services. The facilities were subject to a cyberattack last week, as confirmed by the National Cyber and Encryption Agency (BSSN) on Monday, resulting in the disruption of immigration services and other public services. The attackers used Brain Cipher, an update of the LockBit 3.0 ransomware, the variant reportedly used by hacker group LockBit in a similar attack last year on state-owned sharia lender Bank Syariah Indonesia (BSI). They also demanded an \$8 million ransom, according to state-owned telecommunications firm PT Telkom Indonesia. The company's subsidiary Telkomsigma operates the temporary PDN facilities in Jakarta and Surabaya, East Java. But the government "will not pay" the ransom, Communications and Information Minister Budi Arie Setiadi said at the Presidential Palace in Jakarta on Monday, as reported by Kompas.

But the minister was reluctant to reveal the identity of the hackers, asserting that more details on the latest cyberattack would be announced following the BSSN investigation. "We are still evaluating [and] are trying our best to restore [the system]," Budi added. "The important thing is that public services can resume," he continued, claiming that public data remained safe despite the disruption.

In a press briefing on Monday, the ministry said around 210 databases belonging to central government and regional administration institutions were impacted by the attack, which was first reported on Thursday. As of Monday, several agencies, including immigration offices, the Office of the Coordinating Maritime Affairs and Investment Minister and the city of Kediri in East Java, have had their access to the databases restored and have resumed public services.

B. VOI.id

The Indonesian government is still vulnerable to cyber attacks. The weak cyber security system has made a number of companies and even ministries target severe hackers to hack data. Throughout 2024, there have been at least three incidents of cyber attacks against Indonesian agencies, including ransomware incidents that attacked the Temporary National Data Center or PDNS. Based on records from the Communication and Information System Security Research Center (CISSEeC), Indonesia experienced several cyber attacks over the past year, one of which was experienced by KAI by hacker actor Stormous. In addition, the public must still remember when PDNS in Surabaya experienced paralysis last June due to a ransomware attack. As a result, it was no joke. A total of 47 services from the Ministry of Education, Research and Technology (Kemendikbudristek) were affected by the hacking of PDNS, including scholarship systems, KIP Lectures, and film licensing services. In addition, immigration is the most affected institution. Immigration services at a number of international airports, including Ngurah Rai Airport, Bali, have problems that cause a buildup of passengers. The paralysis was later discovered to have been caused by a ransomware attack from the hacker group Brain Cipher. In total there are 282 government agencies whose data is stored in the Surabaya PDNS affected by the ransomware attack.

However, the series of cyber attacks that occurred in 2024 is believed not to be the last. Head of CISSReC Pratama Persadha said cyber threats would grow in 2025 in line with technological advances and their complexity. "In 2025, of course, there will still be many cyber attacks faced by the Indonesian people," said Pratama in a statement received by VOI. The year 2025 is predicted to be a challenging year in the realm of Indonesian cyberspace. Pratama predicts there will be at least five cyber attacks that need attention from the government this year. The first is the emergence of AI Agentics. This happens because the development of artificial intelligence (AI) technology makes cyber threats more sophisticated and complex. Pratama explained, AI Agentik will emerge as a new opportunity that is of interest to everyone, and a new potential cyber threat sector. This AI agency can automate cyberattacks, reconnaissance, and exploitation so as to increase the speed and accuracy of attacks. In addition, bad AI agents can adapt in real time, break through traditional defenses and increase attack complexity," said Pratama.

The second threat that Indonesia needs to be aware of is AI-based fraud and social engineering. This artificial intelligence has the potential to increase fraud such as first aid (long-term financial fraud) and voice phishing (vishing) so that social engineering attacks are increasingly difficult to detect. "The advanced deepfake produced by AI and synthetic sounds will also allow identity theft, fraud,

and security protocol disruptions," he said. With this technology, cybercriminals can easily imitate the identities of others to commit fraud that is difficult to detect. The third is a ransomware attack that is growing with the use of AI. According to Pratama, cybercriminals will prepare post-quantum cryptography by adapting ransomware capabilities for future resilience so that attacks like this are increasingly difficult to track and overcome. Fourth, supply chain attacks will also pose a serious threat in 2025. Hackers will target open-source ecosystems and exploit code dependencies to disrupt organizations. Cloudan environment is the main target as attackers exploit weak points in the complex supply chain of clouds. "In addition, hackers will target third-party companies as entry points for attacks on large companies they are targeting," Pratama explained. Finally, Pratama predicts that cyber warfare driven by ideological or political agendas will increase following the campaign action of espionage by "Big Four" actors, namely Russia, China, Iran, and North Korea. "Cyber attacks driven by ideological or political agendas will increase, targeting critical governments, businesses and infrastructure," he added.

Facing increasingly complex cyber threats, Pratama encouraged the Indonesian government to fix a number of crucial homeworks that must be completed by 2025 in order to strengthen protection against digital infrastructure and public data. One of the priorities is the establishment of a Personal Data Protection Agency (PDP) as a concrete manifestation of the implementation of the Personal Data Protection Law. "This institution is expected to have a strong independent structure and capability to monitor compliance with regulations, handle data violations, and impose sanctions on those who violate it," Pratama explained.

In addition, the completion of Government Regulations as a derivative of the PDP Law is an important step to provide clear operational guidelines for various parties, both in the public and private sectors, in the management and protection of personal data. This regulation, according to Pratama, must include relevant technical and legal aspects, such as data security standards, incident reporting procedures, as well as dispute resolution mechanisms. The government must also accelerate the discussion of the Draft Law on Cyber Security and Resilience, which has become part of the National Legislation Program (Prolegnas). This regulation is needed to provide a more comprehensive legal framework in dealing with increasingly complex and organized cyber threats, as well as strengthening cross-sectoral coordination in overcoming cyber incidents.

In the institutional context, strengthening the functions and authorities of the National Cyber and Crypto Agency (BSSN) is urgent. The government needs to ensure that BSSN has adequate human resources, technology, and budget to carry

out its duties, including in the field of detection, response, and recovery of cyber incidents. "BSSN must also be empowered to play a central role in securing national critical infrastructure, such as energy, transportation, and telecommunications," he said. Finally, strengthening cyber security and defense within the government must be the main focus. This includes the implementation of strict cybersecurity policies in all government agencies, integration of interoperable security systems, and increasing human resource capacity through intensive training and certification in the field of cybersecurity. "This effort will be an important foundation for Indonesia in facing the challenges of the digital era and maintaining sovereignty in cyberspace," said Pratama ending.