Framing Analysis of the Hacking of Bank Syariah Indonesia by LockBit Ransomware on Republika.co.id and Idntimes.com
[Analisis Framing Berita Peretasan Bank Syariah Indonesia oleh Ransomware LockBit pada Republika.co.id dan Idntimes.com]

Indah Nurjanah[1)], Didik Hariyanto[*2)]

[1)] Program Studi Ilmu Komunikasi, Universitas Muhammadiyah Sidoarjo, Indonesia
[2)] Program Studi Ilmu Komunikasi, Universitas Muhammadiyah Sidoarjo, Indonesia
*Email Penulis Korespondensi: didikhariyanto@umsida.ac.id

Abstract. *This research aims to analyze the framing of news by Republika.co.id and Idntimes.com regarding the phenomenon of hacking Bank Syariah Indonesia by LockBit 3.0 Ransomware. This research was conducted because the hacking issue of Bank Syariah Indonesia became the major topic of public interest and impacted the perceived security of data and funds. The sensitive issue of security hacking certainly has economic relevance for both the public and investors of Bank Syariah Indonesia. The research method used is a qualitative approach with Robert N. Entman's framing analysis model, which has four major elements to interpret the news: define problem, diagnose causes, make moral judgement, and treatment recommendation. The result showed that Republika.co.id sharply criticized Bank Syariah Indonesia in its reporting, but did not emphasize the ransom demand made by LockBit. The criticism in its reporting humanistically and in favor of the community. Meanwhile, Idntimes.com attempted to downplay the inevitability of cyberattacks in the IT world, and framed the news of Bank Syariah Indonesia hacking by LockBit by playing on public emotions using clickbait, rather than highlighting the mitigation steps taken by Bank Syariah Indonesia.*

Keywords *- Framing Analysis; Robert N. Entman; Hacking; LockBit; Bank Syariah Indonesia*

I. INTRODUCTION

The media play a crucial role in shaping reality by constructing and presenting facts and data related to an event. Event are not *'taken for granted'*; rather, journalists and the media actively shape, present, and interpret reality for the public [1]. By employing framing techniques, journalists shape and construct facts to align with their categories and ideals [2]. The media is not merely a passive channel but actively shapes reality, incorporating gits own viewpoints, prejudices, and partisanship [3]. Because the media is frequently influenced by its ownership in reporting, it functions as an ideological tool that supports the dominance of the capitalist class. This influence often reduces people to mere consumers and persuades those in power to favor market interests through ownership and the materials they publish [4]. The inclusion of these capitalist elements compels the media to prioritize market considerations in pursuit of profit, whether from content sales or advertising revenue [5]. This shift has a detrimental effect on the core principles of journalism, as the media prioritizes profit over the pursuit and presentation of the truth to its audience [6].

In the reporting of the LockBit 3.0 Ransomware attack on Bank Syariah Indonesia, the narrative is shaped by media ownership and interests, leading to the construction of the story from various perspectives. The Ransomware attack on Bank Syariah Indonesia was initially suspected to have occurred prior to the disruption of mobile banking services on May 8, 2023, resulting in the theft and dissemination of approximately 15 million customer and employee records on dark web sites. The attack was first reported by the X's social media account @darktraces_int on May 13, 2023, which identified LockBit as the perpetrator behind the system disruption at Bank Syariah Indonesia. LockBit claimed to have stolen 15 million customer records, employee information, and 1.5 TB of internal data.

Additionally, LockBit proposed negotiations for the ransom of the stolen and encrypted customer data, demanding 295.619.469.026 IDR, with a deadline of May 16, 2023, for Bank Syariah Indonesia. However, the negotiation process was unsuccessful, leading to the stolen data being disseminated on dark web site, and Bank Syariah Indonesia suffered significant financial losses.

The reporting of this incident varied significantly across different media outlets, influenced by their ownership structures and underlying interests. Some outlets emphasized the technical aspects of the ransomware attack, framing it as a cybersecurity failure, while others highlighted the potential implications for customer trust and data privacy. The media outlets that reported on the issue included Republika.co.id and Idntimes.com, each presenting the news from different perspectives and with varying interests. Republika.co.id, one of the oldest news chanel in Indonesia, was established on August 17, 1992, by the Indonesian Muslim Scholars Association through the Abdi Bangsa Foundation [2]. Idntimes.com, in contrast, is relatively young media outlet, founded by Winston Utomo and William Utomo in 2014 in Surabaya. It aims to cater to the voices of Millennials and Gen Z [7].

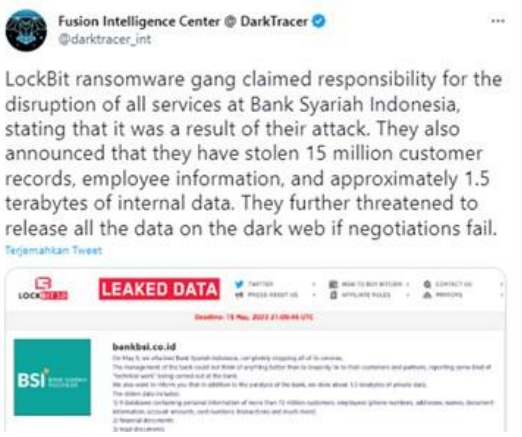

Figure 1. LockBit's Claim on the Bank Syariah Indonesia Data Theft
Source: Screenshot from the X account @darktracer_int (now @ stealthmole_int)
URL: https://x.com/stealthmole_int/status/1657156728893632512

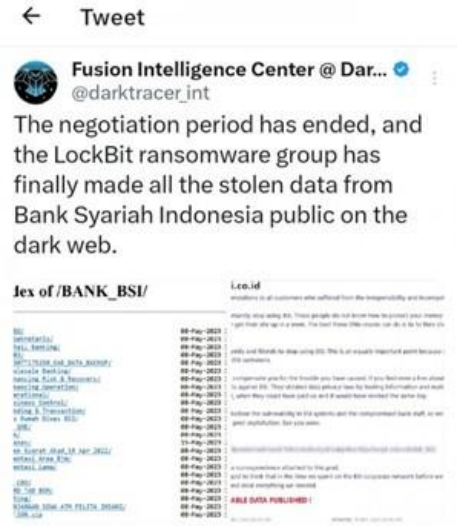

Figure 2. LockBit Disseminated Bank Syariah Indonesia's Data on the Dark Web Site
Source: Screenshot from the X account @darktracer_int (now @ stealthmole_int)
URL: https://x.com/stealthmole_int/status/1657156728893632512

In the context of uncertainty surrounding the LockBit hack of Bank Syariah Indonesia, the public's demand for information on the situation increased sharply, leading to intensive coverage from various media outlets. This heightened demand stems from the fact that the public's understanding of such crises is largely shaped by the information provided by the mass media [8]. The public's reliance on information has endowed the media with significant power. In the media industry, there is a concept known as *'blessing in disguise'*, which refers to the idea that a disaster serves as a continuous source of high-quality of news content [8].

Previous studies, such as those by Gulo et al. [9], and Yurita et al. [10], primarily discuss cybercrime in the form of phishing from technical perspectives and in relation to applicable legal regulations, without examining the role of the media in reporting and framing cybercrime. In contrast, research by Michael & Susilo [11], focuses on financial literacy campaigns as a preventive measure for securing digital banking against cybercrime, yet does not address how mass media frames and presents information on actual cyberattacks targeting banking institutions, not their impact on public perception. Furthermore, studies by Hariyanto & Prituesdina [2], and Ridha Risma Yunita et al. [12], while demonstrating how media framing can shape public perception on sensitive issues, remain limited to political topics rather than cyber threats, which are increasingly relevant in today's media landscape.

This study addresses the gap by analyzing the framing of mass media coverage of the LockBit ransomware attack, one of the major cybercrime organizations targeting national banking institutions in Indonesia, such as Bank Syariah Indonesia. The research investigates how credible mass media outlets, such as Republika.co.id and Idntimes.com, influenced by differing media ownership and ideologies, shape narratives and interpretation of cybercrime in the

banking sector, potentially affecting public understanding of digital security issues. The purpose of this research is to analyze the news framing employed by Republika.co.id and Idntimes.com concerning the LockBit 3.0 Ransomware attack on Bank Syariah Indonesia, to determine whether these media outlets support, downplay, or discredit the issue. The study is significant as it focuses on the vulnerabilities in the digital security systems of banks in Indonesia and their impact on the economic sector. It offers a new perspective on how mainstream media addresses cybersecurity issues, which are increasingly relevant in the digital age, particularly concerning financial institution that have broad societal implications.

By analyzing how the media framed the news regarding the ransomware attack, this research aims to enhance public understanding of the dynamics of information surrounding cyber threats and the media's influence on the formation of public perception. This, in turn, cans foster a stronger dialogue between the public, the media, and the other stakeholders, such as the government and the financial institution, encouraging the public to respond more critically to the information conveyed by the media. By recognizing the potential framing, the public will be better equipped to make informed and wise decisions regarding digital security.

Robert N. Entman's Framing

Framing, as defined by Robert N. Entman, is a technique employed by journalists to select a particular perspective when reporting news. This chosen perspective influences which facts are highlighted or omitted and shapes the overall direction of the news narrative [1]. Framing is an integral aspect of journalistic practice, embedded in the editorial process of news production. This includes the strategies used for processing and presenting news [3]. Essentially, the facts presented in news reports are a product of reality construction [13]. Framing provides insight into how the media interprets and portrays events, shaping news interpretation aligned with their interests [14]. Through framing, the media constructs a version of reality that influences the audience's perception, leading them to interpret phenomena based on the media's perspective [15]. From a constructionist perspective, the audience is not merely a passive recipient but actively constructs information using their own frameworks. In this context, public opinion, attitudes, and behavior can be influenced by mass media in alignment with the communicator's objectives in disseminating information [16]. The more attention the media devoted to an issue, the greater the attention it receives from the public [17].

Robert N. Entman is a key figure in the development of framing analysis within media studies. According to Entman, framing involves of two main aspects: the selection of issues and the highlighting of specific aspects [12]. The media selects and emphasizes certain issues through various strategies, including repetition, headline placement, graphics, labels, generalization, and simplification. Robert N. Entman's framing analysis model consists of four components: (1) Define Problem: This component highlights an issue as a problem; (2) diagnose causes: This component identifies the causes of the problem; (3) Make Moral Judgement: This component presents moral values that frame the issue; (4) Treatment Recommendation: this component offers solutions or resolutions proposed by journalists [18].

LockBit Ransomware

LockBit is a cybercriminal group that utilizes malicious software to encrypt victim's data, thereby disrupting their access to it. They demand a ransom to ensure that the data is not released or further disseminated on the dark web sites [19]. Ransomware, on the other hand, is a type of malicious software designed to lock files on a system by restricting user access to the targeted computer [20]. The purpose of the LockBit attack is to demand a ransom from the victim after successfully encrypting the data on their device. The data will be decrypted and restored to the victim only upon payment of the requested ransom [21]. Typically, ransoms are demanded in the form of cryptocurrencies due to their anonymity and difficulty in tracing [22].

LockBit typically targets government agencies, organizations, companies, and major banks across various countries [23]. The banking sector, which increasingly relies on fintech for its operations, is particularly vulnerable to security breaches, with a risk level 300 times higher that of other industries [24]. By 2023, the number of LockBit Ransomware victims in the banking and finance sector had increased from 9 to 19, highlighting the appeal of sensitive data and intellectual property to cybercriminals [25]. Additionally, cybercrime groups target the economic for reasons such as access to personal data, financial gain, exploitation of connected financial infrastructure, as well as prestige and political objective. Other sectors, such as telecommunications, energy, and electricity, are also vulnerable to hacking due to their designation as Vital Information Infrastructures (VII) [26]. Some of the companies worldwide that have been victims of LockBit attacks include SpaceX, Bangkok Airways, Royal Mail, Thales Group, Bank Sentral Bangladesh, as Bank Syariah Indonesia in Indonesia.

Bank Syariah Indonesia

Bank Syariah Indonesia is one of the Badan Usaha Milik Negara (BUMN) and an Islamic bank established from the merger of BRI Syariah, BNI Syariah, and Bank Syariah Mandiri, adhering to Islamic sharia principles [27].

Mudharabah is a profit-sharing system employed by Bank Syariah Indonesia, where financial institutions and customers share profits and losses. In this system, losses are shared between the capital provider and the business operators, provided the losses are not a result of negligence or misconduct by the business operators. Additionally, Islamic banks do not charge interest on loans, as interest (*riba*) is prohibited under Islamic sharia principles [28]. Because Islamic banks are not only concerned on meeting financial needs, but also responsible for organizing, managing, and ensuring that all their business activities comply with Islamic sharia provisions [29].

In the context of cyber hacking, Bank Syariah Indonesia has implemented a digital banking system through mobile banking applications for transactions and other services. However, this system creates numerous entries points that hacker can exploit to access the operational targets. Potential vulnerabilities include phishing, social engineering, downloading files containing exploits, and the connection of USB or external storage devices to the server [26]. These factors are believed to be among the initial triggers for the LockBit Ransomware attack on Bank Syariah Indonesia.

II. METHOD

In describing the research results through the selection and emphasis of specific aspects of media coverage, a qualitative approach using a constructivist paradigm is required. The qualitative approach was selected because it enables the interpretation and description of data not only at a surface level, but also by exploring the deeper meanings of content that are not immediately apparent [30]. The media text analysis method employs Robert N. Entman's framing analysis model, focusing on several aspects: customers protection, disaster impact and mitigation, and security system recovery. Entman's framing analysis utilizes four key elements to interpret the news: (1) define problem, (2) diagnose causes, (3) make moral judgement, (4) treatment recommendation.

Robert N. Entman's framing analysis model was chosen for this study due to its significant advantages in discourse and content studies, particularly in relation to public issues. The hacking of Bank Syariah Indonesia by LockBit ransomware, as reported by mass media, such as Republika.co.id and Idntimes.com, represents a public issue that requires an in-depth analytical approach to understand how the media frames the information. Therefore, Robert N. Entman's analytical model is relevant for exploring the perspectives and biases in news coverage related to this issue.

In this case Robert N. Entman's framing analysis offers several advantages. First, this model provides a systematic and clear structure for analysis, allowing for a more comprehensive understanding of how the media frames news related to an issue and influences public perception. Second, Entman's model emphasizes issue selection and the prominence of aspects, which allows for the examination of the context behind the framing of issues, in contrast to other models that focus more on the structural aspects of the text. Third, the model's incorporation of moral judgments enables the exploration of relevant social values in the context of public policy, which play a role in framing issues and can influence the responses of the public and policymakers. Fourth, the flexibility of applying this method across various media contexts allows for customization according to the specific need of the research. Overall, Robert N. Entman's framing analysis offers a comprehensive understanding of how issues are framed by the media and their subsequent impact on public perception and policy decisions.

The primary data for this study comprises the coverage of the Bank Syariah Indonesia hacking case by LockBit 3.0 Ransomware on Republika.co.id and Idntimes.com during the period from May 1 to May 31, 2023. This dataset includes a total of 10 news articles: 5 from Republika.co.id and 5 from Idntimes.com, as listed below:

Table 1. News Summary of Republika.co.id and Idntimes.com

News Titles from Republika.co.id	Publication Date	News Titles from Idntimes.com	Publication Date
BSI Disruption, MUI Deputy Chairman Urges BSI to Address Cyberattacks Seriously [31]	May 11, 2023	BSI Mobile Banking Error, Erick Thohir Admits Cyberattack [32]	May 10, 2023
BSI Services Disrupted, LockBit Ransomware Claims Responsibility [33]	May 11, 2023	Inspector General of Ministry of Religious Affairs Mentions Hajj Cost Repayment Affected by BSI System Error [34]	May 11, 2023
If Exposed to Ransomware, BSI Protection Considered Highly Vulnerable [35]	May 13, 2023	LockBit Hacker Group Claims to Have Leaked Customer Data, BSI Responds [36]	May 16, 2023

Customer Data Leaked, BSI Shares Immediately ARB [37]	May 16, 2023	Bareskrim and BSSN Investigate Alleged Hacking of BSI Services [38]	May 19, 2023
BSI Strengthens Synergy with BSSN to Address Suspected Cyberattacks [39]	May 26, 2023	Due to Service Error, Two BSI Directors Removed! [40]	May 23, 2023

Source: Primary Research Data, 2023

While the secondary data used includes: (1) books containing material on online journalism, media construction, framing theory and analysis, research methodology; and (2) national and international reference journals relevant to the research being conducted.

This study employed the Miles and Huberman model as the technique for data analysis. The model involves three key stages: reducing data, displaying data, and drawing conclusions followed by validation [41]. This analysis focuses on identifying the key components in the news text used to frame an issue and involves analyzing the narrative structure and language used by the media. The data validity technique used is source triangulation, which is done by examining data obtained from multiple source [42]. In source triangulation, the researcher compares the frames emerging in the 10 news articles from the two media outlets, Republika.co.id and Idntimes.com, during a specific period to ensure consistency and reliability of the analysis result. This approach helps identify biases and differing perspective in the coverage of the same issue, thus providing a more comprehensive understanding of how media frames the issue and identifies differences and similarities in the narratives presented.

In addition, the credibility of the media used is crucial for ensuring the validity of the data. Republika.co.id and Idntimes.com are media outlets recognized by the Press Council and adhere to clear journalistic standards, making the data obtained from these sources more reliable and valid for framing the issue. However, to ensure the validity od the result, the researcher also pays attention to the diversity of perspectives present in both media and examines whether there is any potential bias that may affect the framing of the coverage. Thus, the framing analysis conducted will provide an objective view of how the hacking of Bank Syariah Indonesia was framing in the coverage by these media outlets.

III. FINDINGS AND DISCUSSION

A. News Framing Analysis of Expert Statements on the Bank Syariah Indonesia Cyber Attack

Table 2. Framing Result

Element Framing	**Republika.co.id News "If Exposed to Ransomware, BSI Protection Considered Highly Vulnerable"**	**Idntimes.com News "BSI Mobile Banking Error, Erick Thohir Admits Cyberattack"**
Define Problem	Expert Assesses BSI's security system as highly vulnerable	BSI system disruption for several days, customers express complaints
Diagnose Causes	Cyberattack on BSI mobile user account	A three-point cyberattack occurred
Make Moral Judgement	Abimanyu criticized and highlighted vendor cooperation for system weaknesses	- Erick Thohir admits the hacking issue and views it as an inevitable aspects of the IT world - Gunawan reports that BSI services have been restored since Tuesday
Treatment Recommendation	No treatment recommendation provided	Erick Thohir's statement on the need for BSI to strengthen its IT system

Source: Research Findings, 2024

Both Republika.co.id and Idntimes.com reported on the statements of technical and economic expert regarding the hacking incident at Bank Syariah Indonesia. Republika.co.id strongly criticized the bank's security system, expressing disappointment with the consultants and developers involved with Bank Syariah Indonesia. Republika.co.id noted that Bank Syariah Indonesia had failed to collaborate with vendors for system repair, maintenance, improvement and

development system, proving that there is a void in their roles and responsibilities. This framing is further reinforced by a statement from IT expert, Abhimanyu Wachjoewidajat:

*"Then, **what is the purpose** of having consultants, application developers, and other vendors who have been supporting BSI" he asked.*

Republika.co.id emphasizes the description of technical problems and critiques of system security without offering concrete solutions, thereby creating the impression that the issue is still under evaluation. On the other hand, Idntimes.com highlights the technical disruptions affecting Bank Syariah Indonesia's services, and the responsibilities the company should assume. Idntimes.com attempts to downplay the issue by portraying the cyberattack as a common occurrence in the IT field, through the statement by Erick Thohir:

*"We have to. During a meeting yesterday, the President Director of BSI actually met with me three days ago, and one of the topics discussed was related to IT issue. He brought up the matter, and then suddenly, this incident occurred. **Well, that's how it is**," said Erick.*

Idntimes.com framed the solution through Erick Thohir's recommendation that Bank Syariah Indonesia strengthen its IT security system, although Idntimes.com did not provide a comprehensive moral evaluation of the issue.

B. News Framing Analysis of the Impact of Cyberattack on Bank Syariah Indonesia's Banking Services

Table 3. Framing Result

Element Framing	**Republika.co.id News "BSI Disruption, MUI Deputy Chairman Urges BSI to Address Cyberattacks Seriously"**	**Idntimes.com News "Inspector General of Ministry of Religious Affairs Mentions Hajj Cost Repayment Affected by BSI System Error"**
Define Problem	Anwar Abbas's statement, BSI services experience problems	Faisal's statement, hajj cost repayment hampered
Diagnose Causes	Many customers have reported inaccessibility issues with BSI services	Constraints of the BSI system
Make Moral Judgement	BSI Director apologizes to customers regarding service constraints	Hery confirm that system constraints due to suspected cyberattacks and states that banking services were restored on Thursday (May 11, 2023)
Treatment Recommendation	- Anwar Abbas urged the public to avoid actions that could harm both parties and called on BSI to address cyberattacks with seriousness - Hery's statement, system normalization efforts are focused on data security and protection of customer funds	The head of the regional office of the ministry of religion affairs will address payment issues for pilgrims

Source: Research Findings, 2024

The public is consistently interested in various aspects of a disaster, including its causes, victims, losses, impacts, and mitigation strategies [8]. Republika.co.id and Idntimes.com highlighted the societal impact of the cyberattack on Bank Syariah Indonesia. The issues selected and the experts chosen by each media outlet reflect their relevance to community interests. Republika.co.id captures the community's emotional response, specifically the disappointment over losses resulting from the disruption of Bank Syariah Indonesia's services, through the statement by Anwar Abbas. Additionally, Republika.co.id emphasizes moral judgment and accountability, through the statement by Hery Gunardi:

*"On behalf of Bank Syariah Indonesia, **we apologize for the inconvenience** caused to customers due to issues accessing BSI services on May 8, 2023. We have undertaken measures to restore Bank Syariah Indonesia's services, with the primary priority on ensuring the safety of customer funds and data," said Hery in a press statement in Jakarta.*

In this case, Republika.co.id's reporting is influenced by public sentiment. In contrast, Idntimes.com framed a technical solution addressing the obstacles to Hajj fee payments caused by disruptions in Bank Syariah Indonesia's services due to cyberattacks, reinforced by statement of Inspector General of the Ministry of Religion, Faisal. A similar news pattern is evident in the reports "Inspector General of Ministry of Religious Affairs Mentions Hajj Cost

Repayment Affected by BSI System Error" and "BSI Mobile Banking Error, Erick Thohir Admits Cyberattack". Both news emphasized the gradual recovery of Bank Syariah Indonesia's banking system, as follows:

Previously reported, PT Bank Syariah Indonesia Tbk (BSI) ***has restored its banking services to normal*** *as of today, Thursday (May 11, 2023).* (News titled "Inspector General of Ministry of Religious Affairs Mentions Hajj Cost Repaymen Affected by BSI System Error")

Previously, BSI Corporate Secretary Gunawan Arief Hartoyo stated that interbank transaction services ***have been available*** *to all customers since Tuesday, (May 9, 2023).* (News titled "BSI Mobile Banking Error, Erick Thohir Admits Cyberattack")

Idntimes.com aims to shape public opinion that the failure of Bank Syariah Indonesia system can be resolved, enabling the public to once again access banking services safely.

C. News Framing Analysis of LockBit Ransomware's Claim of Hacking Bank Syariah Indonesia

Table 4. Framing Result

Element Framing	**Republika.co.id News "BSI Services Disrupted, LockBit Ransomware Claims Responsibility"**	**Idntimes.com News "LockBit Hacker Group Claims to Have Leaked Customer Data, BSI Responds"**
Define Problem	BSI system disruption has resulted in customers being unable to access banking services	LockBit claims to have leaked BSI customer data
Diagnose Causes	Cyberattack by LockBit	BSI system failed to protect customer data and refusal to pay the ransom resulted in customer data being disseminated on the dark web
Make Moral Judgement	Hery confirms the cyberattack but denies the issue of a ransom demand	LockBit statement, BSI failed to protect customer data. Gunawan statement, cyberattack are in inevitable part of the IT world
Treatment Recommendation	Pratama Persadha stated that BSI must conduct audits and digital forensics, and be transparent with the public	BSI will audit, mitigate, and restore its system

Source: Research Findings, 2024

Both media outlets provided a comprehensive chronology of the LockBit Ransomware attack on Bank Syariah Indonesia. Both framed LockBit's claim of responsibility for the failure of Bank Syariah Indonesia as a result of the system disruption. However, Republika.co.id emphasized Bank Syariah Indonesia's response, which denied the ransom threat allegedly made by LockBit, as reinforced by statement from Hery:

"We found indications of a cyberattack. We temporarily switched off the system to ensure its safety, ***but no ransom demand was made****," he stated.*

Idntimes.com, on other hand, framed Bank Syariah Indonesia's refusal to pay the ransom demanded by LockBit as a failure to secure the data, and emphasizing the bank's perceived disregard for customer security, as reinforced by statement from LockBit:

"They have violated data privacy laws by leaking information and making you wait and worry while 'technical work takes place'. ***In reality, they (BSI) could have paid us (LockBit)****, and everything would have been operational again the same day," LockBit stated.*

In this report, Idntimes.com once again framed the downplaying of the LockBit hacking incident, similarly to how it did in the article "BSI Mobile Banking Error, Erick Thohir Admits Cyberattack", through Gunawan's statement:

*"****This is a necessity*** *due to the increasing reliance on IT in business. Therefore, it is important for us as business people to increase vigilance and strengthen collaboration with the government, regulators, and the general public to prevent the growth of cybercrime," stated Gunawan*.

In contrast, Republika.co.id, in the article "BSI Services Disrupted, LockBit Ransomware Claims Responsibility", frames the criticism from IT experts by highlighting that the cyberattack is perceived as a preventable error.

*"It is true **that an error must have occurred**, leading to the system disruption, but we should give the system organizers time to recover and make repairs," he said.*

D. News Framing Analysis of Synergizes Bank Syariah Indonesia with BSSN on Cyberattack

Table 5. Framing Result

Element Framing	Republika.co.id News "BSI Strengthens Synergy with BSSN to Address Suspected Cyberattacks"	Idntimes.com News "Bareskrim and BSSN Investigate Alleged Hacking of BSI Services"
Define Problem	BSI synergizes with BSSN to take preventive measures to strengthen the protection system	Bareskrim and BSSN collaborated on the investigation, mitigation, and recovery of the Bank Syariah Indonesia system
Diagnose Causes	The occurrence of the LockBit cyberattack	BSI system constraints
Make Moral Judgement	BSI statement, customers are the company's top priority and commitment to strengthen corporate cyber defense and security	- BSI has not submitted a report - Hary statement, cyberattacks require further evidence, but customer data dan funds remain secure
Treatment Recommendation	BSI and BSSN will conduct joint assessments, audit, and mitigations	The investigation continues without a report from BSI

Source: Research Findings, 2024

Both media framed Bank Syariah Indonesia's responsible approach to protecting customer data and funds. Republika.co.id emphasizes Bank Syariah Indonesia's positive response by highlighting its collaboration with BSSN to safeguard customer security. This narrative is reinforced by Hery Gunardi's meeting with BSSN Head Hinda Siburian on Tuesday, May 16, 2023, which focused on coordinating efforts to prevent future attacks and strengthen the banking data protection system, as follows:

***BSSN and BSI have also agreed** to implement joint measures to enhance the security and resilience of BSI's system, as well as to manage the aftermath of IT disruptions affecting BSI's operations.*

Meanwhile, Idntimes.com highlighted the negative response of Bank Syariah Indonesia for not reporting to Bareskrim Polri regarding disaster mitigation, suggesting a lack of alignment with the collaboration between Bareskrim Polri and BSSN. Nonetheless, Idntimes.com included information about how Bareskrim Polri and BSSN continued their investigation and mitigation efforts despite the absence of a report from Bank Syariah Indonesia, as reinforced by the statement from the source:

*Adi explained that the **investigation was continued despite the Bareskrim Polri not having received a report** regarding the alleged hacking incident involving BSI. He also stated that BSI would submit a report soon.*

E. News Framing Analysis of the Impact of Cyberattacks on Bank Syariah Indonesia

Table 6. Framing Result

Element Framing	Republika.co.id News "Customer Data Leaked, BSI Shares Immediately ARB"	Idntimes.com News "Due to Service Error, Two BSI Directors Removed!"
Define Problem	BSI shared dropped into the red zone, reaching the Auto Rejection Lower limit	BSI reshuffles its board, removal two directors
Diagnose Causes	The occurrence of customer data leaks as a result of cyberattack	Idntimes.com did not provide the reason for the removal
Make Moral Judgement	- Nico stated that investors are beginning to lose confidence - There has been no confirmation yet from BSI regarding the stock drop	Hery's statement indicate that the removal of two BSI directors was carried out honorably

Treatment Recommendation	Nico urges BSI to be more responsive to these issues	The RUPST appointed Saladin D. Effendi as the new Director of Information Technology and Grandhis Helmi H. as the new Directors of Risk Manajemen

Source: Research Findings, 2024

The cyberattack on Bank Syariah Indonesia undoubtedly triggered internal turmoil, including negative sentiment from various stakeholders and a loss of investor confidence. In this context, Republika.co.id criticized Bank Syariah Indonesia's handling of the cyberattacks, highlighting the sensitive banking security is of significant economic relevance to investor confidence. This perspective is substantiated by Nico's statement as an economic expert:

*"This is certainly a concern because **banking discussions inherently involve trust**," stated Associate Director of Research and Investment Pilarmas Investindo Sekuritas Maximilianus Nico Demus, to Republika on Tuesday (May 16, 2023).*

Idntimes.com, on other hand, reported on the removal of two directors at Bank Syariah Indonesia following the cyberattack. Although the specific reasons for their removal were not explicitly detailed, Idntimes.com attributed this action to the impact of the cyberattack. This attribution is suggested by the headline with a negative tone, emphasized by the exclamation mark: "Due to Service Error, Two BSI Directors Removed!". Additionally, the two removed directors—the Director of Information Technology and the Director of Risk Management—were responsible for key areas affected by the LockBit hacking, which reinforced this assumption, as demonstrated by the following news text:

*President Director of BSI, Hery Gunardi, stated that **the RUPST had honorably removed Achmad Syafii from his position as Director of Information Technology and Tiwul Widyastuti from her position as Director of Risk Management**.*

In the same headline, Idntimes.com also reported on Bank Syariah Indonesia's cash dividend distribution in 2022, presenting a contrast to the negative news of the directors' removal. This duality of information creates the impression that Idntimes.com is steering public opinion towards the view that Bank Syariah Indonesia remains stable despite the cyberattack and changes in company leadership.

F. Issue selection

Issue selection pertains to the choice of facts that journalists decide to highlight. Journalists focus on specific aspects of an issue while potentially overlooking other relevant facets [43]. In the coverage provided by Republika.co.id and Idntimes.com, issues such as claims of cyberattacks, the LockBit threat, the tangible impact of these attacks, and Bank Syariah Indonesia's mitigation measures were framed with an emphasis on the security of customer data and funds.

Regarding the ransom demands from LockBit, Republika.co.id framed Bank Syariah Indonesia's denial, supported by Gunawan A. Hartoyo's statement in the article "BSI Services Disrupted, LockBit Ransomware Claims Responsibility". In contrast, Idntimes.com addressed the issue by highlighting Bank Syariah Indonesia's lack of responsiveness, which allegedly contributed to the dissemination of customer data on dark web sites.

The selection of facts related to the mitigation of Bank Syariah Indonesia's banking system is consistently framed by both Republika.co.id and Idntimes.com, with these issues frequently appearing in each headline. In terms of moral judgment, Republika.co.id repeatedly highlighted Hery Gunardi's apology in the articles "BSI Disruption, MUI Deputy Chairman Urges BSI to Address Cyberattacks Seriously" and "BSI Services Disrupted, LockBit Ransomware Claims Responsibility".

On other hand, Idntimes.com consistently framed the issue of cyber hacking in manner that downplays its severity. This includes emphasizing the inevitability of hacking in the IT world and the periodic restoration of Bank Syariah Indonesia's system, as seen in the articles "BSI Mobile Banking Error, Erick Thohir Admits Cyberattack", "LockBit Hacker Group Claims to Have Leaked Customer Data, BSI Responds", and "Inspector General of Ministry of Religious Affairs Mentions Hajj Cost Repayment Affected by BSI System Error".

G. Aspects Prominence

Salience is closely tied to how facts are presented in writing. It refers to making information more noticeable and memorable for the audience [44]. This process involves the use of words, sentences, images, and visuals in the reporting [43]. An analysis of 10 news articles from Republika.co.id and Idntimes.com reveals that the diction used in the headlines is framed with negative connotations. For instance, Republika.co.id features headline such as "BSI **Disruption**, MUI Deputy Chairman Urges BSI to Address **Cyberattacks** Seriously", "If **Exposed** to Ransomware, BSI Protection Considered **Highly Vulnerable**", and "Customer **Data Leaked**, BSI Shares Immediately ARB". Similarly, Idntimes.com includes headline like "BSI Mobile Banking **Error**, Erick Thohir Admits **Cyberattack**",

"LockBit Hacker Group Claims to Have **Leaked Customer Data**, BSI Responds", and "Due to **Service Error**, Two BSI Directors **Removed!**".

In addition, negative phrasing was also identified in the news text of Republika.co.id and Idntimes.com regarding the hacking of Bank Syariah Indonesia. For example:

> *LockBit, which claimed responsibility for **attacking BSI's IT system, disseminated encrypted customer data on the dark web** through Twitter posts.* (Republika.co.id article, "Customer Data Leaked, BSI Shares Immediately ARB")
>
> *"They also announced that they had **stolen 15 million customer record, employee information, and approximately 1.5 terabytes of internal data**. They claimed they would **release the data on the dark web if negotiations fail**," tweeted @darktracer.* (Republika.co.id article, "If Exposed to Ransomware, BSI Protection Considered Highly Vulnerable")
>
> *"They have **violated data privacy laws by leaking information** and **causing customers to wait and worry** while 'technical work is in progress'. At that time, they (BSI) could have paid us (LockBit), and the system would have been operational again on the same day," wrote LockBit.* (Idntimes.com article, "LockBit Hacker Group Claims to Have Leaked Customer Data, BSI Responds")

Both media focus on the hacking of Bank Syariah Indonesia primarily from a technical perspective, highlighting terms such as temporary switch off, audit, digital forensics, IDS/IPS firewall system, three-point attacks, among others. Republika.co.id also addresses the hacking issue from an economic perspective, supported by financial data in the article "Customer Data Leaked, BSI Shares Immediately ARB". Interestingly, Idntimes.com highlighted the negative issues in the news article titles "Due to Service Errors, Two BSI Directors Removed!" by employing clickbait to accentuate the issue and shape public opinion to blame the two directors as the cause of the service errors at Bank Syariah Indonesia, despite the absence of concrete reasons for their dismissal in the news content. Clickbait is a news strategy designed with hyperbolic and sensationalized thumbnails and hyperlinks to attract attention and encourage reader clicks, thereby increasing online news traffic [45]. While clickbait can make news headlines more engaging, the content often fails to align with reality, making it a tool for generating rumors and disinformation [46].

Republika.co.id and Idntimes.com did not approach the hacking of Bank Syariah Indonesia from a political perspective, despite the bank being part of Badan Usaha Milik Negara (BUMN). However, Idntimes.com featured BUMN Minister Erick Thohir as a political figure, which served to downplay the significance of the hacking issue. In contrast, Republika.co.id relied on sources more relevant to the technical and economic aspects, such as Abimanyu Wachjoewidajat, Pratama Persadha and Maximilianus Nico Demus.

These findings can provide valuable insights to media managers regarding the importance of objectivity in reporting, particularly on the crucial issue of cybercrime, and encourage the enhancement of ethical standards and accuracy in news coverage. Additionally, the results of this study can serve as a reference for policymakers, including media organization, government agencies, and financial institutions, in formulating more affective policies or communication strategies to disseminate information about cyber threats to the public, ensuring that the public receives transparent and reliable information. This expected to contribute to the improvement of digital literacy and help protect the public from potential cybersecurity risks.

IV. CONCLUSION

The result indicate that Republika.co.id offered sharp criticism of Bank Syariah Indonesia, focusing on both technical and economic aspects related to the LockBit cyber hacking incident. However, the criticism remained humanistic and community-oriented by emphasizing facts concerning mitigation efforts, recovery measures, and guarantees for customer security, despite not focusing on the ransom demand made by LockBit. This perspective was reinforced by statements from sources such as Abimanyu Wachjoewidajat, Anwar Abbas, Pratama Persadha, and Maximilianus Nico Demus. On other hand, Idntimes.com emphasizes the downplaying of the hacking issue by framing the news around the regular recovery of the banking system, supported by report of dividend distribution and statements from sources such as Erick Thohir and Hery Gunardi. However, Idntimes.com appears to employ clickbait tactics to boost its news traffic, rather than focusing on the mitigation efforts undertaken by Bank Syariah Indonesia. This suggests that its news framing is influenced by media interests.

This study has certain limitations, one of which is the restricted use of agenda-setting analysis as applied to Republika.co.id and Idntimes.com. consequently, the research does not provide an in-depth explanation of the agenda-setting context underlying the framing by these two media outlets. Future studies are recommended to enhance this research by delving further into the agenda-setting foundations of the framing employed by Republika.co.id and Idntimes.com in reporting on the Bank Syariah Indonesia hack, utilizing agenda-setting theory and advanced analytical techniques.

ACKNOWLEDGMENT

Deepest gratitude is expressed to God for providing strength and guidance throughout this journey. A special thank you is extended to the researcher for the persistence and commitment to completing this study despite various challenges. Appreciation is also given to the parents for their unwavering emotional and financial support, to the supervisor for his time and advice during the whole undertaking, to the elder sister and psychiatrist for ensuring the researcher's health, and to friends for their help along the way.

REFERENCES

[1] Eriyanto, *Analisis Framing: Konstruksi, Ideologi, dan Politik Media*. Yogyakarta: LKiS, 2002. [Online]. Available: https://books.google.co.id/books?id=wGwj0CPSjlQC

[2] D. Hariyanto and F. Prituesdina, "Analisis Framing Berita Kasus Ahok dalam Polemik Surat Al-Maidah pada Kompas.com dan Republika.co.id," *J. Ilmu Komun. MEDIAKOM*, vol. 2, no. 1, pp. 74–88, 2018, doi: https://doi.org/10.32528/mdk.v2i1.1837.

[3] M. Aslam, "Analisis Sikap dan Posisi Tribun Timur dalam Wacana Polemik Kasus KPK Vs Polri," *J. Communio J. Jur. Ilmu Komun.*, vol. 10. No. 1, no. 1, pp. 107–122, 2021, doi: https://doi.org/10.35508/jikom.v10i1.3677.

[4] A. Sudibyo, *Ekonomi Politik Media Penyiaran*. Yogyakarta: LKiS, 2004. [Online]. Available: https://books.google.co.id/books?id=4AIdDg2uBccC

[5] I. Hamad, *Konstruksi Realitas Politik dalam Media Massa: Sebuah Studi Critical Discourse Analysis Terhadap Berita-berita Politik*. Jakarta: Granit, 2004. [Online]. Available: https://books.google.co.id/books?id=BkEB7gJQMLQC

[6] M. N. Fakhruzzaman, S. Z. Jannah, R. A. Ningrum, and I. Fahmiyah, "Flagging clickbait in Indonesian online news websites using fine-tuned transformers," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 3, pp. 2921–2930, 2023, doi: 10.11591/ijece.v13i3.pp2921-2930.

[7] IDNTimes, "Profil Winston Utomo, Kisah Inspiratif di Balik Kesuksesan IDN Media," *IDN Times*, 2022. https://www.idntimes.com/news/indonesia/syifa-putri-naomi/inspiratif-kegigihan-winston-utomo-di-balik-kesuksesan-idn-media

[8] R. Simatupang, "Analisis Framing Pemberitaan Kompas.Com Tentang Covid-19 Di DKI Jakarta," *J. Pustaka Komun.*, vol. 4, no. 1, pp. 39–52, 2021, doi: 10.32509/pustakom.v4i1.1315.

[9] A. S. Gulo, S. Lasmadi, and K. Nawawi, "Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik," *PAMPAS J. Crim. Law*, vol. 1, no. 2, pp. 68–81, 2021, doi: 10.22437/pampas.v1i2.9574.

[10] I. Yurita, M. Kevin Ramadhan, M. Candra, and U. Muhammadiyah Kotabumi, "Pengaruh Kemajuan Teknologi Terhadap Perkembangan Tindak Pidana Cybercrime," *J. Huk. Leg.*, pp. 144–155, 2023, doi: https://doi.org/10.47637/legalita.v5i2.995.

[11] Michael and D. Susilo, "The Effect Of The #AwasModus Campaign At @bankbca Tiktok On Community Financial Literacy," *J. Media dan Komun.*, vol. 4, no. 1, pp. 18–32, 2023, doi: 10.20473/medkom.v4i1.47194.

[12] R. R. Y. Ridha risma yunita, S. T. Suanti tunggala, and K. A. S. Ken amasita, "Framing analysis on Luwuk Post on the news of regional head election campaign (Pilkada) Banggai Regency in 2020," *Commicast*, vol. 3, no. 3, pp. 221–236, 2022, doi: 10.12928/commicast.v3i2.5959.

[13] G. Sitohan, "Humanitarian news frame in Harian Republika and Kompas on Wamena ferugees (framing analysis on Republika news and Kompas edition 24 – 30 September 2019 on the tragedy of the riots in Wamena)," *Commicast*, vol. 2, no. 2, p. 98, 2021, doi: 10.12928/commicast.v2i2.3351.

[14] H. M. Syam, N. Anisah, R. Saleh, and M. A. Lingga, "Ideology and media framing: Stigmatisation of LGBT in media coverage in Indonesia," *J. Komun. Malaysian J. Commun.*, vol. 37, no. 1, pp. 59–73, 2021, doi: 10.17576/JKMJC-2021-3701-04.

[15] S. S. Yanuar Rahmadan, "A Framing Analysis of Indonesian Newspaper Coverage on the Issue of Palm Oil Discrimination Between Indonesia and the European Union," *J. Int. Stud.*, vol. 17, pp. 27–52, 2021, doi: https://doi.org/10.32890/jis2021.17.2.

[16] D. Hariyanto, *Buku Ajar Pengantar Ilmu Komunikasi*. Sidoarjo: Umsida Press, 2021. doi: https://doi.org/10.21070/2021/978-623-6081-32-7.

[17] R. West and L. H. Turner, *Pengantar Teori Komunikasi: Analisis dan Aplikasi Buku 2*. Jakarta: Salemba Humanika, 2017.

[18] D. Hariyanto and A. D. Kharina, "Pemberitaan Pidato Pribumi Anies Baswedan Pada Media Indonesia.Com dan Okezone.Com," *Kanal J. Ilmu Komun.*, vol. 7, no. 1, pp. 10–16, 2018, doi: 10.21070/kanal.v.

[19] N. Maulana, T. Laurens, H. A. Faiz, and T. Patrianti, "Manajemen Krisis PT. BSI Tbk Pasca Peretasan Data

Nasabah," *Innov. J. Soc. Sci. Res.*, vol. 4, no. 1, pp. 8244–8258, 2024, doi: https://doi.org/10.31004/innovative.v4i1.8620.
[20] S. Enomoto, H. Kuzuno, H. Yamada, Y. Shiraishi, and M. Morii, "Early mitigation of CPU-optimized ransomware using monitoring encryption instructions," *Int. J. Inf. Secur.*, vol. 23, pp. 3393–3413, 2024, doi: 10.1007/s10207-024-00892-2.
[21] L. A. I. W. Sin and M. F. Zolkipli, "Evolution of Ransomware Tactics and Defenses," *Borneo Int. J. EISSN 2636-9626*, vol. 7, no. 3, pp. 11–25, 2024, [Online]. Available: https://majmuah.com/journal/index.php/bij/article/view/647
[22] M. Aggarwal, "Ransomware Attack: An Evolving Targeted Threat," *2023 14th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2023*, pp. 1–7, 2023, doi: 10.1109/ICCCNT56998.2023.10308249.
[23] Kompas, "Mengenal Ransomware LockBit 3.0 yang Diduga Serang BSI dan Cara Kerjanya," *Kompas.com*, 2023. https://tekno.kompas.com/read/2023/05/15/12450037/mengenal-ransomware-lockbit-30-yang-diduga-serang-bsi-dan-cara-kerjanya (accessed Jun. 25, 2024).
[24] K. Najaf, M. I. Mostafiz, and R. Najaf, "Fintech firms and banks sustainability: Why cybersecurity risk matters?," *Int. J. Financ. Eng.*, vol. 08, no. 02, p. 2150019, 2021, doi: 10.1142/s2424786321500195.
[25] Republika, "LockBit Klaim Serang BSI, Siapa Saja yang Pernah Jadi Korban?," *News Republika*, 2023. https://news.republika.co.id/berita/rukuyj425/lockbit-klaim-serang-bsi-siapa-saja-yang-pernah-jadi-korban
[26] Tirto, "Serangan Ransomware & Upaya Perbankan Minimalisasi Ancaman Siber," *Tirto*, 2023. https://tirto.id/serangan-ransomware-upaya-perbankan-minimalisasi-ancaman-siber
[27] A. Ulfa, "Dampak Penggabungan Tiga Bank Syariah di Indonesia," *J. Ilm. Ekon. Islam*, vol. 7, no. 2, pp. 1101–1106, 2021, doi: 10.29040/jiei.v7i2.2680.
[28] H. Irawan, I. Dianita, and A. D. Salsabila Mulya, "Peran Bank Syariah Indonesia Dalam Pembangunan Ekonomi Nasional," *J. Asy-Syarikah J. Lemb. Keuangan, Ekon. dan Bisnis Islam*, vol. 3, no. 2, pp. 147–158, 2021, doi: 10.47435/asy-syarikah.v3i2.686.
[29] Mohammad Yusuf and Reza Nurul Ichsan, "Analysis of Banking Performance in The Aftermath of The Merger of Bank Syariah Indonesia in Covid 19," *Int. J. Sci. Technol. Manag.*, vol. 2, no. 2, pp. 472–478, 2021, doi: 10.46729/ijstm.v2i2.182.
[30] B. M. Lindgren, B. Lundman, and U. H. Graneheim, "Abstraction and interpretation during the qualitative content analysis process," *Int. J. Nurs. Stud.*, vol. 108, p. 103632, 2020, doi: 10.1016/j.ijnurstu.2020.103632.
[31] Republika, "BSI Gangguan, Waketum MUI Minta BSI Serius Hadapi Serangan Siber," *Sharia Republika*, 2023. https://sharia.republika.co.id/berita/ruhbb2370/bsi-gangguan-waketum-mui-minta-bsi-serius-hadapi-serangan-siber (accessed Mar. 20, 2024).
[32] IDNTimes, "Mobile Banking BSI Eror, Erick Thohir Akui Ada Serangan Siber," *IDN Times*, 2023. https://www.idntimes.com/business/finance/vadhia-lidyana-1/mobile-banking-bsi-eror-erick-thohir-akui-ada-serangan-siber (accessed Mar. 25, 2024).
[33] Republika, "Layanan BSI Diganggu, LockBit Ransomware Klaim Bertanggung Jawab," *Sharia Republika*, 2023. https://sharia.republika.co.id/berita/ruknti377/layanan-bsi-diganggu-lockbit-ransomware-klaim-bertanggung-jawab (accessed Mar. 20, 2024).
[34] IDNTimes, "Irjen Kemenag Sebut Pelunasan Biaya Haji Terdampak Sistem BSI Eror," *IDN Times*, 2023. https://www.idntimes.com/news/indonesia/muhammad-ilman-nafian-2/irjen-kemenag-sebut-pelunasan-biaya-haji-terdampak-sistem-bsi-eror (accessed Mar. 25, 2024).
[35] Republika, "Bila Terkena Ransomware, Proteksi BSI Dinilai Sangat Rentan," *Sharia Republika*, 2023. https://sharia.republika.co.id/berita/rukwil457/bila-terkena-ransomware-proteksi-bsi-dinilai-sangat-rentan (accessed Mar. 20, 2024).
[36] IDNTimes, "Kelompok Hacker LockBit Klaim Sebar Data Nasabah, BSI Buka Suara," *IDN Times*, 2023. https://www.idntimes.com/business/finance/vadhia-lidyana-1/kelompok-hacker-lockbit-klaim-sebar-data-nasabah-bsi-buka-suara (accessed Mar. 20, 2024).
[37] Republika, "Data Nasabah Bocor, Saham BSI Langsung ARB," *Sharia Republika*, 2023. https://sharia.republika.co.id/berita/ruqi9p457/data-nasabah-bocor-saham-bsi-langsung-arb (accessed Mar. 20, 2024).
[38] IDNTimes, "Bareskrim dan BSSN Gelar Penyelidikan Dugaan Peretasan Layanan BSI," *IDN Times*, 2023. https://www.idntimes.com/news/indonesia/irfanfathurohman/bareskrim-dan-bssn-gelar-penyelidikan-dugaan-peretasan-layanan-bsi (accessed Mar. 25, 2024).
[39] Republika, "BSI Perkuat Sinergi dengan BSSN Tangani Dugaan Serangan Siber," *News Republika*, 2023. https://news.republika.co.id/berita/rur8h9451/bsi-perkuat-sinergi-dengan-bssn-tangani-dugaan-serangan-siber (accessed Mar. 20, 2024).
[40] IDNTimes, "Imbas Layanan Error, Dua Direktur BSI Dicopot!," *IDN Times*, 2023. https://www.idntimes.com/business/economy/ridwan-aji-pitoko-1/imbas-layanan-error-dua-direktur-bsi-

dicopot (accessed Mar. 25, 2024).
[41] T. Santoso, *Metodologi Penelitian Kualitatif*. Surabaya: Pustaka Saga, 2022. [Online]. Available: https://repository.petra.ac.id/id/eprint/19963
[42] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif Dan R&D*. Bandung: Alfabeta, 2013. [Online]. Available: https://www.academia.edu/118903676/Metode_Penelitian_Kuantitatif_Kualitatif_dan_R_and_D_Prof_Sugiono
[43] Eriyanto, *Analisis Framing: Konstruksi, Ideologi, dan Politik Media*. Yogyakarta: LKiS, 2012. [Online]. Available: https://books.google.co.id/books?id=wGwj0CPSjlQC
[44] A. Sobur, *Analisis Teks Media: Suatu Pengantar Untuk Analisis Wacana, Analisis Semiotik, dan Analisis Framing*. Bandung: PT Remaja Rosdakarya, 2006.
[45] R. K. Mundotiya and N. Yadav, "Forward Context-Aware Clickbait Tweet Identification System," *Int. J. Ambient Comput. Intell.*, vol. 12, no. 2, pp. 21–32, 2021, doi: 10.4018/IJACI.2021040102.
[46] X. Li, J. Zhou, H. Xiang, and J. Cao, "Attention Grabbing through Forward Reference: An ERP Study on Clickbait and Top News Stories," *Int. J. Hum. Comput. Interact.*, vol. 40, no. 11, pp. 3014–3029, 2024, doi: 10.1080/10447318.2022.2158262.

Conflict of Interest Statement:
The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.