

STATE-CENTRIC NARRATIVES AND MULTILINGUAL DISPARITIES IN CYBERCRIME REPORTING: A CONTENT ANALYSIS OF MALAYSIAN DIGITAL NEWS

POH LING TAN

School of Media and Communication Studies, Sunway University
E-mail: pohlingt@sunway.edu.my

Abstract

This study explores how Malaysian online news media construct narratives around cybercrime and digital safety, offering insights relevant to cybersecurity communication and public awareness. Using a quantitative content analysis of 927 articles published between 2022 and 2024 across English, Chinese, and Malay-language outlets, the research applies framing theory to examine news frames, tone, and cited sources. Results reveal that English-language publications dominated approximately 72% of total cybercrime coverage, contributing more than two-thirds of all articles, with Chinese and Malay outlets providing significantly fewer reports. Across all three languages, thematic framing overwhelmingly predominates, comprising the vast majority of coverage, while episodic framing remains marginal. The most frequently employed themes focus on prevention and intervention measures, followed by reports on the prevalence of cybercrime and legal proceedings, whereas narratives emphasising personal harm, victim impact, or everyday digital risks receive comparatively limited attention. Official sources - including ministries, enforcement agencies, and cybersecurity authorities - were cited most frequently, whereas victim perspectives, NGOs, and the public were underrepresented. Coverage emphasized prevention and intervention strategies, prevalence data, and legal responses, while narratives highlighting personal impact and online risks were comparatively rare. These findings indicate that Malaysian news media privilege authoritative voices and adopt a solutions-oriented agenda, which shapes public understanding of cyber threats and digital safety. The study contributes to framing theory and offers implications for journalists, cybersecurity practitioners, and policymakers seeking to promote balanced reporting, inclusive risk communication, and effective digital literacy campaigns.

Keywords: Cybercrime, Cybersecurity communication, Digital safety, Framing theory, Online news.

1. Introduction

The proliferation of Internet usage has led to an associated rise in the occurrence of cybercrime and the associated concern surrounding it, as discussed by Lee and Kim [1]. Digitisation provides new avenues for criminal activities and reinforced the strategies used by criminals in the physical world [2-4]. Cybercrime is one of the fastest-growing categories of crime, which is predicted to cost globally USD\$10.5 trillion by 2025 [5]. Furthermore, the global occurrence of the COVID-19 pandemic has led to an increase in online sales, remote work, and cyberattacks [6]. While these statistics highlight the scale and urgency of cybercrime as a societal problem, they do not, on their own, explain how the public comes to understand digital risks, prevention strategies, or responsibility for cyber safety. In Malaysia, a local daily news report indicates that the incidence of online crime increased by 23% in 2023 compared to 2022, with 19,224 cases recorded in 2023 compared to 15,659 cases in the same period in 2022 [7].

Cybercrime is defined as a wide range of criminal activities that utilise technology to target either computers (cyber-dependent crimes like hacking) or individuals (cyber-enabled crimes like cyberstalking or cyber fraud and scam) [5, 8]. The pervasive incorporation of the internet into several facets of daily life has established connectedness as a fundamental attribute of current society [1, 9]. Nevertheless, the same features that have contributed to the internet's breakthrough have also enabled the rise of novel forms of illegal behaviour, commonly referred to as cybercrimes, as noted by Nobanee et al. [10].

In addition to the financial implications, cyber-enabled crimes such as cyberstalking can also lead to the psychological, mental health, and even physical harm [11]. At this point, the role of mass media becomes crucial. The significant financial and non-financial losses imposed by cybercrime on society illustrate the need for a fundamental understanding of the issue to safeguard individuals and organisations against a variety of cyber threats. Therefore, the media has played a vital role in raising public awareness, a role that has been recognised as thought-provoking [12, 13]. This is because the media plays an important role in affecting public opinion and is a significant information source about current events. The media frames a message as one of the communication strategies to shape perceptions, attitudes, and judgments [14, 15]. In the Malaysian context, where online news operates within a multilingual media ecosystem, the way cybercrime is framed has important implications for public understanding of digital safety across different linguistic and cultural communities.

Despite the varying prevalence rates reported on cybercrime, the frequency of this issue continues to be sufficiently high to warrant concern, thereby affecting the effectiveness of national digital safety and cybersecurity initiatives. Therefore, cybercrime is a critical phenomenon to research as victims of online fraud may experience not only financial consequences but also significant psychological effects such as individual vulnerabilities and aftermath of cybercrime on mental health [16, 17].

Despite the growing body of international research on cybercrime reporting and media framing, a clear research gap remains within the Malaysian context. Existing studies on Malaysian media have largely focused on cybersecurity, without systematically examining how cybercrime is framed in news discourse. It remains a notable gap in studies specifically addressing how the media reports on

cybercrime. The media, as a powerful conduit of information, plays a crucial role in influencing public attitudes and behaviours.

More importantly, previous research has not sufficiently addressed the intersection between cyber-safety communication and multilingual media framing. This gap is particularly significant given Malaysia's multilingual media landscape, where English-, Chinese-, and Malay-language news outlets coexist and cater to distinct yet overlapping publics. Through the lenses of various framing techniques, media outlets can emphasise certain aspects of cybercrime, thereby shaping the narrative and, ultimately, public perception. Without a comparative, cross-linguistic analysis of framing patterns, it remains unclear whether cybercrime reporting promotes a balanced understanding of digital risks and personal vulnerability, or whether it predominantly privileges institutional perspectives and solutions-oriented narratives at the expense of individual lived experiences and public agency.

Accordingly, this study addresses this gap by systematically analysing how cybercrime and digital safety are framed in Malaysian online news media across English-, Chinese-, and Malay-language outlets. By applying framing theory to examine dominant themes, framing styles, and sourcing patterns from 2022 to 2024, the study seeks to advance understanding of cybersecurity communication within multilingual media systems and to illuminate how news framing may shape public perceptions of cybercrime and digital safety in Malaysia.

2. Literature Review

2.1. Cybercrime in Malaysia

According to Malaysia Computer Emergency Response Team (My CERT), cybercrime is classified into 9 classifications: (1) intrusion attempt, (2) spam, (3) fraud, (4) denial of service, (5) intrusion, (6) vulnerabilities report, (7) cyber harassment, (8) malicious codes, and (9) content related offences.

Cybercrime such as online scams have also shown a worrying trend, with fraud cases in Malaysia having doubled from 17,668 cases in 2019 to 34,495 cases in 2023 [18]. Recent statistics from the Malaysian Communications and Multimedia Commission (MCMC) reveal that over the past three years, cyberbullying has slightly surpassed online scams, with 9,483 reports of cyberbullying compared to 9,321 complaints about online scams [19]. In addition to that, based on the recent statistics on commercial crime, a total of 23,447 cases were recorded between Jan 1, 2024, and Oct 13, 2024, involving RM1.97bil in losses [20].

Studies pinpoint rapid digital adoption and fragmented, outdated legislation as root causes; they urge comprehensive reform to match cybercriminal sophistication [21, 22]. Current laws include the Computer Crimes Act (1997), Communications and Multimedia Act (1998), Personal Data Protection Act (2010), etc., which experts critique as fragmented and insufficient.

2.2. Online media in Malaysia

Digital News Report 2019 by Reuters Institute for the Study of Journalism which showed that 86% of internet users in Malaysia chose online and social networking sites as their source of latest information and news over established mainstream media [23]. This trend continued into three years by 2021, digital and social sources reached 88%,

with a concurrent decline in television (from 57% to 55%) and print (from 45% to 24%). Oeldorf-Hirsch and Srinivasan [24] highlighted a related shift in news consumption habits, busy lifestyles and the acceleration of information dissemination through mobile devices have made push notifications and mobile-first news formats increasingly dominant. Users now routinely rely on smartphone alerts to stay abreast of the latest updates, often foregoing traditional media formats.

Malaysia's multilingual environment supports news content in Malay, English, and Chinese, catering to its diverse ethnic population. Media outlets such as The Star, Free Malaysia Today, Malaysiakini serve as cross-ethnic platforms, reaching readers from all major racial communities. This linguistic diversity, combined with high internet and mobile penetration, ensures that digital news travels swiftly across language groups.

2.3. Framing theory

This study drew upon framing theory as the theoretical foundation. Framing refers to the process of selecting and presenting news messages that are tailored to resonate with the targeted audience, Scheufele and Iyengar [25]. Framing comes from cultural norms, journalistic decision rules, and the interaction of developments of the real world with proficient efforts of competing elites for managing the news [26, 27]. Other definitions of framing include "the process of highlighting certain aspects of reality while obscuring others, potentially leading to different reactions" [28] and "the selection of a limited number of thematically related attributes for inclusion in the media agenda when discussing a particular object" [29]. Different framing patterns can portray the same event in varied ways [25, 30]. Consequently, the way a news article is presented can shape how the audience perceives the issue.

In this particular process, journalists normally pick some aspects of reality, tone, focus, language, integration of various evidence, and values [30, 31]. Frames describe the attributes of news, residing within specific elements of the news narrative that shape how events are perceived and understood. The construction and embodiment of news frames are achieved through the use of concepts, keywords, visual images, metaphors, and symbols embedded within the narrative [32]. The use of framing in news stories involves the selection of specific attributes related to particular issues, thereby shaping a narrative to make certain aspects more prominent than others [25, 33, 34]. Frames enhance the apparent ideas used to evaluate the different topics or events that are happening. Framing is influenced by cultural norms, journalistic decision-making rules, and the interaction of real-world developments with the strategic efforts of competing elites to manage the news [27, 35].

Chong and Druckman [36] discovered that communication researchers commonly employ the term "frame" in two distinct ways. A media frame encompasses the linguistic and visual elements, as well as the style in which information is presented, that a media source use to communicate about a particular problem or event to its audiences or readers. The selected frame exposes the aspects that the media outlet considers significant to the current subject. Scheufele and Tewksbury [29] considered this framing approach to be a construct at the macro level. At a macro level, the term "framing" refers to the methods of presenting that journalists and other communicators employ to convey information in a manner that aligns with the preexisting mental frameworks of their audience. Indeed, framing is an essential instrument utilized by journalists to simplify the intricacy of

a matter, taking into account the limitations imposed by their particular media platforms in terms of available space and broadcasting time. Zillman et al. [37] recognised that framing is considered a pivotal practice in journalism. It is noted that choosing a frame for a story would be the most consequential decision that journalists make. The current study drew upon the notion of framing as a macro level construct to analyse the coverage of cybercrime by the media.

3. Methods

3.1. Materials and methods

This study was based on a content analysis of 927 online news articles on cybercrime collected between 1 January 2022 and 31 December 2024. The articles were retrieved from the online archives of 20 mainstream media outlets which include English, Chinese, and Malay languages. While all 20 outlets were monitored, only 16 media outlet published articles on cybercrime during the study period. English-language contributors included The Star, New Straits Times, Malay Mail, The Borneo Post, The Sun, The Sun Daily, Bernama, and Astro Awani. Chinese-language outlets comprised Sin Chew Daily, China Press, Nanyang Siang Pau, Oriental Daily News, and Kwong Wah Yit Poh. Malay-language outlets included Harian Metro, Berita Harian, and Sinar Harian. The initial pool of 20 outlets was identified based on three criteria: (1) national-level reach and audience visibility, (2) consistent online publication during the study period (2022-2024), and (3) representation across Malaysia's major language spheres - English, Chinese, and Malay. These outlets include mainstream legacy media organisations and prominent digital-native platforms that play a central role in shaping public discourse.

Although 20 outlets were initially identified, only 16 published cybercrime-related content that met the study's inclusion criteria during the sampling period. Outlets without relevant coverage were excluded from the final analysis. The unit of analysis was the individual article, encompassing straight news, editorials, columns, and letters. This multilingual and multi-outlet approach ensured both breadth of coverage and diversity in language, enabling the researchers to identify and explain intrinsic patterns statistically while capturing contextual nuances of media framing [38, 39].

3.2. Sampling and data collection

This study investigated the reporting of cybercrime in Malaysian online news media over a three-year period, from 1 January 2022 to 31 December 2024. News articles were collected from the online archives of 20 mainstream outlets spanning three language groups: English, Chinese, and Malay. English-language publications included The Star, New Straits Times, Malay Mail, The Borneo Post, The Sun, Astro Awani, and Bernama. Chinese-language publications comprised Sin Chew Daily, China Press, Nanyang Siang Pau, Oriental Daily, and Kwong Wah Yit Poh. Malay-language publications included Harian Metro, Berita Harian, and Sinar Harian. Articles were retrieved from the online archives of the selected news outlets using the primary search term "*cybercrime*." While terms such as "*scam*," "*fraud*," and "*phishing*" are commonly used in Malaysian news reporting, the use of "*cybercrime*" as the core search term was a deliberate methodological decision. This term functions as an umbrella concept that encompasses a wide range of digitally mediated offences, including online scams, identity theft, phishing, and cyber fraud.

During the screening process, articles retrieved using “*cybercrime*” were further examined to ensure that coverage of scams, fraud, and phishing incidents linked to digital platforms was included in the dataset. This strategy prioritised conceptual consistency and analytical coherence, while minimising the risk of over-inclusion of offline or non-digital crime reports that may arise from broader search terms. The unit of analysis was the individual article, which encompassed straight news reports, editorials, columns, and letters. This multilingual and multi-outlet sampling strategy ensured a comprehensive representation of Malaysia’s diverse media landscape, resulting in a total of 927 articles analysed.

3.3. Intercoder reliability and data analysis

An intercoder reliability test was conducted to ensure consistency in the coding process. Two trained coders independently analysed 15% of the dataset ($n = 140$ articles), randomly selected from the three-year sample (2022–2024). The coders were trained using a detailed codebook that defined variables such as article type, news source, framing (episodic vs. thematic), and dominant themes. To minimize subjectivity in categorizing content, both coders cross-checked each other’s decisions during the pilot phase. Holsti’s [40] presented agreement index was employed to statistically verify the level of agreement. Reconciliation procedures were undertaken when low agreement values emerged, and coding was only allowed to proceed once all indexes achieved the accepted reliability threshold of 0.7 or above. This process ensured that the subsequent data analysis was conducted on a reliable and validated coding framework.

3.4. Coding scheme

A structured coding scheme was developed to systematically analyse each article. The unit of analysis was the individual news article. Each article was coded based on the following dimensions: (1) Basic Descriptive Information: publication name, year of publication, language category (English, Chinese, or Malay), and article type (news report, editorial, column, or opinion piece). (2) Dominant Theme: articles were coded according to their primary focus, including (a) prevention and intervention measures, (b) prevalence and trends of cybercrime, (c) legal proceedings and enforcement actions, (d) personal or societal harm, and (e) internet and digital risks. (3) Framing Style: framing was coded as episodic, thematic, or mixed, following established framing typologies.

Episodic framing focused on individual cases or events, while thematic framing contextualised cybercrime within broader social, institutional, or policy frameworks. (4) Sources Cited: the primary sources quoted or referenced in each article were identified and categorised (e.g., government agencies, law enforcement, cybersecurity experts, private sector representatives, victims, or members of the public). (5) Tone of Coverage: articles were coded as neutral, alarmist, or reassurance-oriented based on the overall narrative emphasis and language used.

4. Results and Discussion

Table 1 presents the number and types of cybercrime-related articles published in three languages—English, Chinese, and Malay from 2022 to 2024. A total of 927 articles were published during this period: 2022 ($N = 232$), 2023 ($N = 414$), and 2024 ($N = 281$). The majority of these articles were in the form of straight news ($N = 851$),

followed by editorials (N = 47) and columns or letters (N = 29). Straight news articles peaked in 2023 (N = 393), whereas editorial pieces were most numerous in 2022 (N = 27). Columns and letters were most frequently published in 2023 as well (N = 14). English-language publications consistently dominated coverage across all three years, 2022: (N = 203); 2023: (N = 339); 2024: (N = 231). This was followed by Chinese-language publications (2022: N = 10, 2023: N = 47, 2024: N = 63) and Malay-language publications (2022: N = 19, 2023: N = 28, 2024: N = 3).

Table 1. Types of articles on cybercrime published in the years 2022, 2023, and 2024.

Year	2022			2023			2024		
Items	ENG	CHI	MAL	ENG	CHI	MAL	ENG	CHI	MAL
Straight news	175	8	18	320	45	28	208	60	3
Editorial	24	2	1	5	2	0	13	2	0
Columns/Letters	4	0	0	14	0	0	10	1	0
Total	203	10	19	339	47	28	231	63	3

ENG = English, CHI = Chinese, MAL = Malay

Table 2 shows the number of cybercrime-related articles published by various news outlets in English, Chinese, and Malay between 2022 and 2024. A total of 927 articles were published across 20 media outlets, with the highest output recorded in 2023 (N = 414), followed by 2024 (N = 297), and 2022 (N = 232).

Table 2. Publications on cybercrime published in the years 2022, 2023, and 2024.

Year	2022			2023			2024		
Publications	ENG	CHI	MAL	ENG	CHI	MAL	ENG	CHI	MAL
Astro Awani	7	0	0	8	0	4	0	0	0
Bernama	21	0	2	61	0	1	0	0	0
Berita Harian	0	0	8	0	0	7	0	0	2
China Press	0	1	0	0	21	0	0	0	0
Nanyang Siang Pau	0	2	0	0	8	0	0	0	0
Harian Metro	0	0	5	1	0	7	0	0	1
Sin Chew Daily	0	1	0	0	6	0	0	63	0
Kwong Wah Yit Poh Press	0	1	0	0	1	0	0	0	0
Malay Mail	20	0	0	28	0	1	0	0	0
New Straits Times	40	0	0	56	0	0	49	0	0
Oriental Daily News	1	5	0	0	11	0	0	0	0
Sinar Harian	0	0	4	1	0	5	0	0	0
The Borneo Post	14	0	0	25	0	0	73	0	0
The Star	88	0	0	109	0	0	79	0	0
The Sun	12	0	0	49	0	3	29	0	0
The Sun Daily	0	0	0	1	0	0	1	0	0

English-language publications accounted for the majority of coverage across all years. Notably, The Star published the highest number of English articles overall (N = 276), with 88 in 2022, 109 in 2023, and 79 in 2024. This was followed by New Straits Times (N = 145), which published 40, 56, and 49 English-language articles respectively

across the three years. Other notable English-language article contributors include The Borneo Post (N = 112), The Sun (N = 90), Bernama (N = 82), Malay Mail (N = 48), and The Sun Daily (N = 2). Among the Chinese-language newspapers, Sin Chew Daily showed a marked increase in cybercrime coverage in 2024 (N = 63) from 2022 (N = 1) and 2023 (N = 6). China Press also contribute significantly in 2023 with 21 articles, followed by Nanyang Siang Pau with 8 articles. Oriental Daily News demonstrated relatively steady output in 2022 (N = 5) and 2023 (N = 11).

However, Malay-language publications showed limited engagement overall. Berita Harian and Harian Metro were the most active in this category, although their output were minimal. Berita Harian (N = 17) published 8 articles in 2022, 7 in 2023, and 2 in 2024; while Harian Metro (N = 13) produce 5 articles in 2022, 7 in 2023, and 1 in 2024. This was followed by Sinar Harian (N = 9), with 4 in 2022, and 5 in 2023. Other Malay-language contributions were negligible, with several outlets such as Bernama and Malay Mail showing occasional entries. Overall, English-language outlets contributed the majority of cybercrime-related coverage throughout the study period, followed by Chinese-language outlets, while Malay-language outlets exhibited minimal and declining engagement. Several Malay-language platforms, including Berita RTM and Rama Rama, did not publish any cybercrime-related articles that met the inclusion criteria between 2022 and 2024. This pattern highlights a marked imbalance in multilingual news attention rather than random variation at the outlet level.

Table 3 summarizes the sources cited in cybercrime-related news articles from 2022 to 2024, categorized by language. The five primary categories of sources included ministries or government agencies, the general public, experts and professionals, telecommunication or information technology (IT) companies, and non-governmental organizations (NGOs) and activists.

Table 3. News sources on cybercrime published in the years 2022, 2023, and 2024.

Year	2022			2023			2024		
Items	ENG	CHI	MAL	ENG	CHI	MAL	ENG	CHI	MAL
Ministries or government agencies	127	7	17	254	35	26	155	56	3
General public	2	2	0	5	2	0	10	2	0
Experts and professionals	26	0	0	50	9	0	42	2	0
Telecommunication (telecom) or information technology (IT) companies	48	1	1	30	1	1	13	2	0
Non-governmental organizations (NGOs) and activists	0	0	1	0	0	1	11	1	0

Across all years and languages, ministries or government agencies were the most frequently cited sources comprising the majority of attributions in the dataset.

In English-language articles, citations to ministries or government agencies peaked in 2023 (N = 254), followed by 2022 (N = 127), and 2024 (N = 155). Chinese and Malay-language articles followed a similar trend, although at much lower frequencies (Chinese: 2022 (N = 7); 2023 (N = 35); 2024 (N = 56), Malay: (2022 (N = 17); 2023 (N = 26); 2024 (N = 3)).

Experts and professionals were the second most cited group in English-language articles, particularly in 2023 (N = 50) and 2024 (N = 42), with fewer mentions in 2022 (N = 26). Chinese sources showed minimal engagement with this group (N = 9 in 2023; N = 2 in 2024), while Malay-language articles did not reference experts at all during the study period.

Telecommunication or IT companies were also a notable source, especially in 2022 (N = 48). However, citations decreased over time, 2023 (N = 30) and 2024 (N = 13). Citations in Chinese and Malay articles remained minimal throughout all years. The general public was rarely cited, appearing in a small number of English and Chinese articles. Most notably in 2024 (English: N = 10; Chinese: N = 2), followed by 2022 (English: N = 2; Chinese: N = 2) and 2023 (English: N = 5; Chinese: N = 2). Similarly, NGOs and activists were largely absent from coverage except for a modest increase in 2024 (English: N = 11; Chinese: N = 1), followed by 2022 and 2023 with only one citation in Malay article.

Table 4 shows the distribution of cybercrime news articles from 2022 to 2024 categorized by topics and language. The five primary themes identified include prevention and intervention strategies, prevalence of cybercrime, harmful impact of cybercrime, risks of the Internet and court case or laws related to cybercrime.

Table 4. News categories on cybercrime published in the years 2022, 2023, and 2024.

Year	2022			2023			2024		
Items	ENG	CHI	MAL	ENG	CHI	MAL	ENG	CHI	MAL
Prevention and intervention strategies	87	2	8	168	16	7	100	26	3
Prevalence of cybercrime	35	2	7	40	9	7	58	15	0
Harmful impact of cybercrime	9	0	1	14	7	1	10	0	0
Risks of the Internet	11	0	1	13	3	1	10	1	0
Court case or laws related to cybercrime	61	6	2	104	12	12	53	21	0

Across all years, prevention and intervention strategies were the most frequently reported theme, particularly in English-language news peaked in 2023 (N = 168), followed by 2022 (N = 87), and 2024 (N = 100). Chinese-language articles on this topic also increased over time from 2 articles in 2022 to 26 articles in 2024, while Malay-language coverage was opposed (2022: N = 8, 2023: N = 7, 2024: N = 3).

The prevalence of cybercrime was the second most reported topic, with a gradual increase in English-language articles (2022: N = 35, 2023: N = 40, 2024: N = 58). Chinese-language reporting also rose from 2 articles in 2022 to 15 articles

in 2024, while Malay articles remained relatively stable in 2022 (N = 7) and 2023 (N = 7), but dropped to zero in 2024.

Court case or laws related to cybercrime were the third most reported topic overall, especially in English-language reporting. This topic saw a surge in 2023 (N = 104), followed by 2022 (N = 61) and 2024 (N = 53). Chinese coverage of court cases also rose steadily from 2022 (N = 6) to 2024 (N = 21), whereas Malay-language coverage of this topic remained relatively low, with a slight increase from 2022 (N = 2) to 2023 (N = 12) before dropping to zero in 2024.

Furthermore, the harmful impact of cybercrime and risks of the Internet were less frequently covered overall. In English-language articles, coverage of harmful impacts rose from 2022 (N = 9) to 2023 (N = 14) but slightly declined in 2024 (N = 10). Articles about risks of the Internet followed a similar pattern, with moderate coverage across all three years, which ranging between 10 and 13 articles (2022: N = 11, 2023: N = 13, 2024: N = 10). These two themes revived minimal attention in Chinese and Malay media.

Table 5 presents the use of episodic, thematic, and combined episodic and thematic framing in news coverage of cybercrime across English, Chinese, and Malay-language publications from 2022 to 2024. Across all years, thematic framing was the most dominant approach.

Table 5. Attribution of responsibility on cybercrime published in the years 2022, 2023, and 2024.

Year	2022			2023			2024		
Items	ENG	CHI	MAL	ENG	CHI	MAL	ENG	CHI	MAL
Episodic framing	6	2	0	13	3	0	16	4	0
Thematic framing	169	6	19	281	42	27	203	57	3
Episodic and thematic framing	28	2	0	45	2	1	12	2	0

In 2022, 194 of the 232 total articles employed thematic framing (English: N = 169, Chinese: N = 6, Malay: N = 19). This trend persisted in 2023, with thematic framing rising further to 350 articles, with English (N = 281), Chinese (N = 42), and Malay (N = 27). In 2024, while the total number of articles declined, thematic framing remained the most frequent (N = 263), with English (N = 203), Chinese (N = 57), and Malay (N = 3).

In contrast, episodic framing was used far less frequently. In 2022, episodic framing was employed in English (N = 6) and Chinese (N = 2), with no Malay articles. This pattern continued in 2023 with English (N = 13), Chinese (N = 3), and Malay (N = 0); and in 2024 with English (N = 16), Chinese (N = 4), and again Malay (N = 0).

The use of episodic and thematic framing was also limited. English-language articles that employed episodic and thematic framing accounted for the majority, increasing from 28 articles in 2022 to 45 articles in 2023, before dropping to 12 articles in 2024. Chinese articles use this approach minimally (2 articles each year), and Malay articles featured it only once in 2023.

4.1. Language and format of coverage

This content analysis reveals that Malaysia's cybercrime news coverage is overwhelmingly dominated by English-language outlets. English portals accounted for 72% of all articles, whereas Chinese-language media contributed far fewer. One of the most salient findings of this study is the relative absence—or “silence”—of cybercrime reporting within Malay-language online news media. In practice, English news sites such as The Star, Malay Mail produced almost all reporting on cybercrime, whereas Malay-language titles published very little. Notably, the vast majority of these articles appeared as straight news reports with very few editorials or opinion pieces. This pattern is analytically significant and extends beyond a descriptive observation of low article counts. However, it should not be interpreted simplistically as evidence of a digital literacy deficit among Malay-language readers. Rather, the silence is more plausibly understood as a reflection of structural and editorial dynamics within the Malaysian media system.

Prior analyses of Malaysian media showed a similar pattern of English-language news dominance in specialized news coverage. For example, Abdullah and Ling [14] reported that English portals “published the highest rate” of heritage news, with most stories appearing as straight news. In sum, coverage of cybercrime has been concentrated in the English-language press and presented mainly as hard news, with minimal attention from Malay-language media and little variation in format. This imbalance has important implications for digital safety communication. When cybercrime reporting is concentrated within English-language media, awareness-building and preventive messaging may not be equitably distributed across linguistic communities. Consequently, the issue lies not in audience capability, but in uneven media mediation of digital risk, which may shape how different publics perceive responsibility, vulnerability, and appropriate responses to cyber threats.

4.2. Framing of cybercrime news

A striking finding is that thematic framing overwhelmingly dominated the news coverage, with episodic (case-based) framing almost absent. Nearly all articles were framed in broader societal or policy terms, emphasizing trends, causes, or solutions (a “wide-angle” perspective) rather than focusing on individual incidents. This pattern is remarkable given that Iyengar [41] suggested that news generally favours episodic frames focused on discrete events. In contrast, this analysis is consistent with Wen et al. [42], shows a clear inversion: thematic frames prevail, focusing on systemic issues and prevention strategies.

Thematic frames tend to highlight structural factors and collective responsibility rather than personal anecdotes. In effect, cybercrime is treated primarily as a social or policy problem to be managed, not merely as an individual's misfortune. The near-total absence of episodic stories and the related absence of personal victim voices, suggests that media narrative emphasizes official context over individual experiences. In other words, public events like policy initiatives or legislative changes are reported with context, whereas victims' experiences and specific case details receive little attention. This pattern is consistent with international findings showing that cybersecurity awareness is shaped less by individual capability and more by uneven exposure to mediated information and institutional communication structures, as evidenced in large-scale studies from other developing contexts [43, 44].

These patterns closely mirror findings in prior framing research, where prevention frames dominate coverage of cyberbullying and cybercrime [42, 45], reinforcing a consistent focus on institutional and collective solutions. As a result, cybercrime is framed less as an experiential or victim-centred social issue and more as a governance and management problem, addressed through prevention strategies, advisories, and institutional countermeasures.

4.3. Sources in cybercrime reporting

The news sources used in cybercrime articles were heavily skewed toward official, governmental voices. Ministries, law-enforcement, and other agencies were by far the most common sources cited, with virtually no reliance on citizens, NGOs, or independent experts. This mirrors a well-known tendency in crime reporting: media often depend on information “fed” by police and other authorities. As Amzat et al. [46] observed, “crime stories fed to the papers by official sources appear more in the papers than stories from other sources”.

In the dataset, journalists overwhelmingly quoted government or police representatives, while public or community voices were nearly non-existent. Such sourcing bias reinforces an official perspective on cybercrime and likely marginalizes dissenting or personal viewpoints. It also means that coverage tends to present cybercrime in terms dictated by authorities, for example focusing on law enforcement efforts and official statistics. In sum, the coverage’s source profile is very narrow and top-down, reflecting the gatekeeping role of institutions in crime news [14, 46].

4.4. Dominant themes in coverage

The dominant news themes further underscore an official, solutions-oriented agenda. In nearly every year, articles about cybercrime were most often categorized under prevention and intervention strategies such as reporting on how to avoid scams, issuing security advisories, and describing new countermeasures. Coverage of cybercrime prevalence (trends, data on incidence) and of legal or court cases also featured prominently. By contrast, stories framed around personal impact (victims harm) or the “risk of internet use” were far fewer.

These thematic patterns align closely with prior framing studies. For instance, Yang [45] identified “prevention and intervention strategies” as the dominant frame in Malaysian cyberbullying news, reflecting a similar emphasis on prevention. Similarly, Wen et al. [42] reported that Malaysian cybercrime articles “focus on prevention and intervention”.

4.5. Theoretical implications of cybercrime framing

From a theoretical standpoint, these findings extend framing theory by revealing how structural bias in news production reinforces thematic framing in a non-Western media system, contrary to Iyengar’s [41] observation that news coverage typically privileges episodic frames. Thematic framing positions cybercrime as a structural and policy-driven issue, shifting responsibility attribution from individuals to institutions and reinforcing collective rather than individual solutions. This suggests that framing choices are not only editorial decisions but are deeply embedded in structural dependencies on official sources and state-aligned expertise. In the Malaysian context, this aligns with a state-

centric discourse where government and regulatory voices play a defining role in narrative construction [47]. This contributes to framing scholarship by providing non-Western evidence of how political culture and media systems influence frame selection, thereby enriching global discussions on media power, agenda-setting, and digital risk communication.

4.6. Practical implications

Practically, the study offers several implications for media practitioners, policymakers, and civil society for the need for structural and technological interventions in newsroom practices. For journalists, reducing over-reliance on official sources requires proactive strategies, including integrating cybersecurity experts, digital forensics specialists, and civil society organisations into routine reporting workflows. Technological integration—such as automated scam alerts, AI-assisted threat monitoring tools, and expert databases—can support journalists in identifying emerging cybercrime trends beyond official press releases, particularly in Malay-language media where reporting gaps are more evident.

For policymakers and cybersecurity agencies, the strong presence of prevention frames represents an opportunity to leverage media as a strategic partner in embedding long-term digital literacy and cyber hygiene practices [48]. Civil society groups can also advocate for greater inclusion of community voices to counterbalance state-centric narratives and empower citizens as active participants in cybersecurity governance.

4.7. Limitations and future research

This study's quantitative content analysis approach effectively identifies frame, tone, and source patterns but is limited in its ability to uncover deeper interpretive meanings. Despite established intercoder reliability, some level of coder subjectivity cannot be ruled out. Moreover, the dominance of official sources may partly reflect structural biases in crime reporting rather than the full spectrum of perspectives. Future research should expand the dataset to include additional media outlets, languages, and formats, and adopt mixed-method designs to capture more nuanced insights. Additionally, as the study focused exclusively on online news, it does not account for television, radio, or social media narratives, which may differ significantly [49]. Longitudinal analyses are also recommended to track changes in framing practices, source diversity, and thematic priorities over time.

5. Conclusions

This study examined how cybercrime and digital safety were framed in Malaysian online news media between 2022 and 2024 across English-, Chinese-, and Malay-language outlets. The findings revealed a strong dominance of English-language coverage, extensive reliance on government and institutional sources, and a clear preference for thematic framing. Prevention and intervention strategies emerged as the most frequently reported themes, while victim-centred perspectives and internet-related risks received comparatively limited attention. These findings suggest that Malaysian cybercrime reporting is largely shaped by institutional narratives and solutions-oriented approaches, highlighting the need for more balanced and inclusive

coverage that incorporates diverse voices and perspectives in digital risk communication.

Abbreviations

IT	Telecommunication or information technology
MCMC	Malaysian Communications and Multimedia Commission
My CERT	Malaysia Computer Emergency Response Team
NGOs	Non-governmental organizations

References

1. Lee, C.S.; and Kim, J.H. (2023). How victims perceive fear of cybercrime: Importance of informed risk. *Criminal Justice Studies*, 36(3), 206-227.
2. Maimon, D.; and Louderback, E.R. (2019). Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology*, 2(1), 191-216.
3. Moule Jr., R.K.; Pyrooz, D.C.; and Decker, S.H. (2013). From 'what the F#@% is a Facebook?' to 'who doesn't use Facebook?': The role of criminal lifestyles in the adoption and use of the Internet. *Social Science Research*, 42(6), 1411-1421.
4. Roks, R.A.; Leukfeldt, E.R.; and Densley, J.A. (2021). The hybridization of street offending in the Netherlands. *The British Journal of Criminology*, 61(4), 926-945.
5. Ozaşçılar, M.; Çalici, C.; and Vakhitova, Z. (2024). Examining cybercrime victimisation among Turkish women using routine activity theory. *Crime Prevention and Community Safety*, 26, 112-128.
6. Smaili, N.; Radu, C.; and Khalili, A. (2022). Board effectiveness and cybersecurity disclosure. *Journal of Management and Governance*, 27(4), 1049-1071.
7. The Star. (2023). Police stats show online crime up 23% this year, total RM687mil lost. The Star. Retrieved November 14, 2023, from <https://www.thestar.com.my/news/nation/2023/11/14/police-stats-show-online-crime-up-23-this-year-total-rm687mil-lost>
8. Pyne, B.K. (2020). *Define cybercrime*. In Holt, T.; and Bossler, A. (Eds.). *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Palgrave Macmillan, Cham.
9. Leukfeldt, E.R.; Lavorgna, A.; and Kleemans, E.R. (2017). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research*, 23(3), 287-300.
10. Nobanee, H.; Alodat, A.; Bajodah, R.; Al-Ali, M.; and Al Darmaki, A. (2023). Bibliometric analysis of cybercrime and cybersecurity risks literature. *Journal of Financial Crime*, 30(6), 1736-1754.
11. Vakhitova, Z.I.; Alston-Knox, C.L.; Reeves, E.; and Mawby, R.I. (2022). Explaining victim impact from cyber abuse: An exploratory mixed methods analysis. *Deviant Behavior*, 43(10), 1153-1172.

12. Govender, N.; Rawjee, V.; and Govender, J. (2014). Magazines' representation of women and its influence on identity construction: A South African perspective. *Mediterranean Journal of Social Sciences*, 5(20), 2278-2283.
13. Weishaar, H.; Dorfman, L.; Freudenberg, N.; Hawkins, B.; Smith, K.; Razum, O.; and Hilton, S. (2016). Why media representations of corporations matter for public health policy: a scoping review. *BMC Public Health*, 16(1), 899.
14. Abdullah, K.; and Ling, T.P. (2023). Framing Malaysia heritage through the lens of online media. *International Journal of Academic Research in Business and Social Sciences*, 13(15), 233-244.
15. Abdullah, K.; Ling, T.P.; and Rahman, A.A. (2021). Framing for the heritage conservation in Malaysia. *International Journal of Academic Research in Business and Social Sciences*, 11(11), 1273-1292.
16. Monteith, S.; Bauer, M.; Alda, M.; Geddes, J.; Whybrow, P.C.; and Glenn, T. (2021). Increasing cybercrime since the pandemic: Concerns for psychiatry. *Current Psychiatry Reports*, 23(4), 18.
17. Whitty, M. T.; and Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims-both financial and non-financial. *Criminology & Criminal Justice*, 16(2), 176-194.
18. New Straits Times. (2024). Malaysia faces cybercrime surge, Fahmi wants stronger online security. New Straits Times. Retrieved April 30, 2026, from <https://www.nst.com.my/news/nation/2024/07/1080859/updated-malaysia-faces-cybercrime-surge-fahmi-wants-stronger-online>
19. The Sun Malaysia. (2024). Cyberbullying tops cybercrime reports in Malaysia with over 9k complaints. The Sun Daily. Retrieved April 30, 2026, from <https://thesun.my/news/malaysia-news/cyberbullying-tops-cybercrime-reports-in-malaysia-with-over-9k-complaints-bd12772773/>
20. The Star. (2024). Nearly RM2bil lost to commercial crime so far this year, says Bukit Aman. The Star. Retrieved April 30, 2026, from <https://www.thestar.com.my/news/nation/2024/10/18/nearly-rm2bil-lost-to-commercial-crime-so-far-this-year-says-bukit-aman>
21. Khan, S.; Saleh, T.; Dorasamy, M.; Khan, N.; Leng, O.T.S.; and Vergara, R.G. (2022). A systematic literature review on cybercrime legislation. *F1000Research*, 11, 971.
22. Tan, S.-W.; Ng, K.-W.; Khan, S.; and Tan, O.S.L. (2022). Data-centric analysis to combat cybercrime in Malaysia. *Proceedings of the International Conference on Law and Digitalization (ICLD 2022)*. Springer Nature, 707, 61-73.
23. Newman, N.; Fletcher, R.; Kalogeropoulos, A.; and Nielsen, R.K. (2019). Digital news report 2019. *Reuters Institute for the Study of Journalism*.
24. Oeldorf-Hirsch, A.; and Srinivasan, P. (2022). An unavoidable convenience: How post-millennials engage with the news that finds them on social and mobile media. *Journalism*, 23(9), 1939-1954.
25. Scheufele, D.A.; and Iyengar, S. (2014). The state of framing research: A call for new directions. In Kenski, K.; and Jamieson, K. H. (Eds.), *The Oxford Handbook of Political Communication*. Oxford Handbooks, Oxford University Press.
26. Cheregi, B.F. (2015). The media construction of anti-immigration positions: The discourse on the Romanian immigrants in the British press. *Revista Română de Sociologie*, 26(3/4), 279-294.

27. Entman, R.M. (2010). Media framing biases and political power: Explaining slant in news of Campaign 2008. *Journalism*, 11(4), 389-408.
28. Griffin, E.A.; Ledbetter, A.; and Sparks, G. (2003). *A first look at communication theory*. McGraw-Hill.
29. Scheufele, D.A.; and Tewksbury, D. (2007). Framing, agenda setting, and priming: the evolution of three media effects models. *Journal of Communication*, 57(1), 9-20.
30. An, S.-K.; and Gower, K.K. (2009). How do the news media frame crises? A content analysis of crisis news coverage. *Public Relations Review*, 35(2), 107-112.
31. Iyengar, S. (1987). Television news and citizens' explanations of national affairs. *American Political Science Review*, 81(3), 815-831.
32. Entman, R.M. (1991). Symposium framing US coverage of international news: contrasts in narratives of the KAL and Iran Air incidents. *Journal of Communication*, 41(4), 6-27.
33. Demuyakor, J.; Avenyo, S.J.; and Amankwah, A.S. (2024). COVID-19 vaccines and vaccinations coverage on news portals: Framing, tone, and source analysis. *Communication and the Public*, 9(2), 143-160.
34. Gabore, S.M. (2020). Western and Chinese media representation of Africa in COVID-19 news coverage. *Asian Journal of Communication*, 30(5), 299-316.
35. Eze, V.C.; and Elegbe, O. (2018). Trends in media framing of China's engagement in Africa and other parts of the world. *Journal of Pan African Studies*, 11(2), 92-103.
36. Chong, D.; and Druckman, J.N. (2007). A theory of framing and opinion formation in competitive elite environments. *Journal of Communication*, 57(1), 99-118.
37. Zillmann, D.; Chen, L.; Knobloch, S.; and Callison, C. (2004). Effects of lead framing on selective exposure to Internet news reports. *Communication Research*, 31(1), 58-81.
38. Barbosa, L.S.; Marshall, W.; Streipert, S.; Albantakis, L.; and Tononi, G. (2020). A measure for intrinsic information. *Scientific Reports*, 10(1), 18803.
39. Sutton, J.; and Austin, Z. (2015). Qualitative research: data collection, analysis, and management. *The Canadian Journal of Hospital Pharmacy*, 68(3), 226-231.
40. Holsti, O.R. (1969). *Content analysis for the social sciences and humanities*. Addison-Wesley.
41. Iyengar, S. (1994). *Is anyone responsible? How television frames political issues*. University of Chicago Press.
42. Wen, S.J.; Kun, S.; and Ling, T.P. (2025). Media frames and cybercrime: Understanding Malaysian online news coverage. *SEARCH Journal of Media and Communication Research*, 17(4), 71-86.
43. Ahamed, B.; Polas, M.R.H.; Kabir, A I.; Sohel-Uz-Zaman, A.S.M.; Fahad, A.A.; Chowdhury, S.; and Rani Dey, M. (2024). Empowering students for cybersecurity awareness management in the emerging digital era: The role of cybersecurity attitude in the 4.0 industrial revolution era. *SAGE Open*, 14(1).
44. Singh, S.; and Singh, S. (2025). Perceptions of Indian students towards bullying; intervention through Bullying Intervention Module (BIM). *SAGE Open*, 15(1). 21582440241305199.

45. Yang, L.F. (2020). Media reporting of cyberbullying: A framing analysis of The Star. *Journal of Asian Pacific Communication*, 30(1-2), 290-309.
46. Amzat, J.; Julius, A.A.; and Akanji, O.R. (2007). The print media and crime: values and issues. *International Journal of Criminal Justice Sciences*, 2(1).
47. Brik, A.B. (2025). Controlled neo-corporatism in disability policy: hybrid governance and institutional resilience in rentier states. *Policy Studies*, 1-33.
48. Hazarika, H.J. (2025). Impact of cybersecurity breaches on social media: A case study on undergraduate students. *Alexandria*.
49. Kozman, C.; and Mellado, C. (2025). Mapping journalistic role performance across five Arab countries. *Journalism & Mass Communication Quarterly*, 102(3), 722-749.