DISCURSIVE STRATEGIES IN HACKTIVISM DISCOURSE: REVEALING IDEOLOGY IN *AL-HAKIRZ AL-MUSLIMUN'S* HACKING THREAT

Reflinaldi[1], Erizal Ilyas[2], Awliya Rahmi[3], Melisa Rezi[4], Amal Syahidin[5], Resty Syahrotul Aini[6]

[1] reflinaldi@uinib.ac.id
[1], [2], [3], [4] Universitas Islam Negeri Imam Bonjol Padang
Padang, Indonesia.
[5] Ezzitouna University
Tunis, Tunisia
[6] Universitas Islam Negeri Sunan Kalijaga Yogyakarta
Yogyakarta, Indonesia

Abstract: This study explores the underlying ideology in the hacktivism discourse of *al-hākirz al-muslimūn* (MH), a group of Muslim hackers. The objective was to uncover the discursive strategies used by MH in its cyber threats, focusing on how they construct their identity and position themselves in opposition to perceived threats. A critical qualitative design was employed to analyze three videos from the Hacker News YouTube channel, using the ideological square framework as the theoretical lens for data analysis. The results of macroanalysis show that MH used the basic strategy of emphasizing positive 'us' on 11 data (14.67%), emphasizing negative 'them' on 31 data (41.33%), and de-emphasizing positive 'them' on 33 data (44.00%). In the microanalysis dimension, the rhetorical discursive strategies found include actor description amounting to 23 data (31.08%), consensus with a total of 2 data (2.70%), evidentiality reaching 5 data (5.41%), example/illustration with a total of 7 data (9.46%), values expression reaching 14 data (18.92%), number game with a total of 4 data (5.41%), and victimization-criminalization amounting to 20 data (27.03%). The ideological analysis indicated that MH's discourse is characterized by anti-imperialism, reflecting their defense of oppressed populations and the use of hacking as a form of retribution. Additionally, anti-extremism was evident in the group's critique of actions perceived as insults to Islam, often tied to extremist ideologies. This study contributes to the understanding of hacktivism as a form of digital activism, emphasizing its role in shaping political discourse and public opinion through cyber threats. It provides insights into the ideological motivations behind hacktivism, showing how groups like MH use digital platforms to challenge global political structures. The implications of this study are significant for future research into hacktivism, particularly in exploring the broader impact of such discourse on global politics, the ethical dimensions of cyber activism, and the potential of multimodal discourse analysis to examine the interplay of textual, visual, and audiovisual elements in discourse interpretation. By applying multimodal discourse analysis, future researchers could explore how audio, visual, and color codes contribute to shaping meaning in hacktivist narratives. This study highlights the complexity of hacktivism and its potential to reshape political narratives and activism in the modern world.

Keywords: hacktivism, ideology, *al-hākirz al-muslimuñ,* ideological square, critical discourse analysis.

INTRODUCTION

Hacktivism has emerged as a form of modern digital activism, providing political intervention to specific parties as a consequence of the digital world's extensive development (Delmas, 2018; George & Leidner, 2019; Richards & Wood, 2018). In the Arab cyber landscape, this phenomenon appears through the group of hackers الهاكرز المسلمون *al-hākirz al-muslimūn* 'Muslim hackers' (hereinafter referred to as MH), which issued threats to compromise public facilities in Israel, Sweden, and Australia during early to middle of 2023 (Reflinaldi et al., 2023, 2024). The hacking threat issued by MH, communicated publicly via a YouTube channel, was driven by perceived insults to sacred Islamic symbols and the physical oppression of Muslims in various nations (News, 2023a, 2023c, 2023b). MH addressed the incidents involving the burning of the Qur'an in Sweden, the assault on worshippers at the Al-Aqsa Mosque, and the disrespectful use of Allah's name during a fashion show in Australia. MH articulated their opposition to anti-Islamic actions, extremism, and terrorism within their hacking discourse (Reflinaldi et al., 2023, 2024).

In the landscape of discourse and media studies, MH's stance against anti-Islamic actions, extremism, and terrorism can be understood through the lens of social media's role as a tool for movement. Several previous studies have highlighted the same phenomenon, including Elamin (2024); Maghfiroh and Rohma (2021); and Poole et al. (2023). These researchers demonstrated the effectiveness of strategic pro-Islamic narratives from various non-state actors communicated through multiple social media platforms in reducing Islamophobic issues. Alongside non-state actors, Ansusa Putra (2023) and Ismail (2023) highlighted Qatar as a nation that successfully promoted peaceful Islam through diverse discourses during the 2022 FIFA World Cup. Additional researchers have detailed initiatives aimed at addressing anti-Islamic narratives through diverse social media content, including Islamic education and comedy (Mansoor et al., 2021; Mashwani et al., 2022; Umar et al., 2021). The studies conducted by Bélanger et al. (2020) as well as Álvarez-Benjumea and

Winter (2020) also identified various constructive actions for countering extremism and terrorism on social media. Bélanger et al. (2020) demonstrated that counter-narratives on social media, while not significantly impactful, were effective in diminishing support for ISIS. To attain the objectives of the movement, it is essential to effectively package counter-extremism and counter-terrorism narratives on social media. Research conducted by Ganesh and Bright (2020) as well as Khan and Pratt (2022) outlined strategic communication patterns and content moderation as narrative options available to media users. Borelli (2023) indicated that counter-narratives on social media, as a form of cyber warfare, are significantly influenced by corporate entities. Borelli (2023) also concluded that social media platforms, including Facebook, YouTube, and Twitter, have effectively functioned as strategic actors in mediating these movements.

In addition to narratives and constructive actions, resistance to anti-Islam, extremism, and terrorism on social media is also found in the form of protests and demonstrations. The pattern that defines traditional digital activism initiates action through the dissemination of narratives across multiple media platforms, subsequently leading to mass mobilization in physical spaces (Abbas et al., 2022; Dumitrica & Felt, 2020; Kazkaz & Bosch, 2023). Media users employ various strategies to disseminate narratives, one of which involves embedding hashtags to stimulate discussion on the conveyed protest narratives (Abushbak & Majeed, 2020; Maryoga & El Fasha, 2022). The narrative escalation through this strategy is achieved by exchanging provocative and aggressive comments to elicit emotions and anger (Faisol & Rahmat, 2021a, 2021b). These efforts succeeded in mobilizing large-scale participants and facilitating demonstrations in multiple locations (Kabir, 2021; Tabib, 2022; Tudor & Ladjouzi, 2020).

In contrast to the aforementioned patterns of constructivism, protest, and demonstration, hacktivism executed by MH represents a distinct form. MH fails to construct narratives and implement constructive actions, nor does it effectively communicate protests or mobilize the masses. MH engages in novel activism against the

prevailing global governance and order (Alexopoulou & Pavli, 2021; Sharevski & Kessell, 2023). Researches indicate that hacktivism conducted by MH may be driven by discontent with conventional movements, opposition to structural moral violations, the pursuit of financial gain, and responses to war aggression (Alexopoulou & Pavli, 2021; Romagna & Leukfeldt, 2023; Shires, 2019; Svyrydenko & Mozgin, 2022). Hacktivism typically aims to disrupt public services and reveal sensitive information. This strategy is deemed ineffective as negotiation and constructive measures frequently fail and are subject to manipulation by authoritative tools (Bélanger et al., 2020; Ellefsen & Jämte, 2023).

The distinction between discourse structure and forms of activism serves as the foundational argument for addressing why the hacktivism discourse presented by MH is both intriguing and complex as a subject of analysis. The subsequent argument addresses the issue of ideology that remains unexamined in the aforementioned studies. Discourses resisting anti-Islam, counter-extremism, and counter-terrorism represent verbal aggressions that encompass threats and foster antagonism toward opposing parties (Qi, 2020). According to the research conducted by Etaywe (2022) as well as Etaywe and Zappavigna (2022), these discourses serve a social function by affirming ideological positions. The ideology within the discourse is discernible through the frequency of lemmas, judgmental attitudes, and the consistency in the representation of "us" and "them," which reinforce the worldview of the discourse producer (Etaywe & Zappavigna, 2022; Navarretta & Hansen, 2020; Qi, 2020).

Based on the orientation of the aforementioned studies, analysis of ideology in the MH hacktivism discourse addresses a gap in the existing literature that prior researchers have not explored. The analysis of ideology, through the mapping of the representation of

"self" and "other," is structured around two research questions. Firstly, what are the basic discursive strategies employed in MH's hacktivism discourse? Secondly, what is the role of rhetorical discursive strategies in MH's hacktivism discourse? The analysis will employ a simultaneous and integrative approach to address these two questions, utilizing the critical discourse analysis (CDA) framework, particularly the ideological square as proposed by van Dijk (van Dijk, 2006; Van Dijk, 2006b). The ideological square facilitates the revelation of ideology by distinguishing positive representation strategies for the self, referred to as "us," and negative representations for others, termed "them." The presence of protagonism and antagonism towards specific values within the discourse ultimately reinforces its ideology.

METHOD

The process of systematically addressing research questions was established by critical-qualitative construction (Alharahsheh & Pius, 2020; Aspers & Corte, 2019, 2021). The research data, consisting of videos depicting MH's threat, were extracted from the Hacker News YouTube channel (https://www.youtube.com/@HackerNewsAR/about). This channel served as a platform for sharing videos showcasing hacking actions conducted by different hacker organizations. Researchers chose three videos showcasing the MH hacking gang from various videos depicting other hacker groups worldwide. In addition to meeting the criteria for comprehensiveness and data adequacy, all MH videos were taken to obtain a complete representation of the ideology contained in their hacking discourse. The specifics of the three data source videos are presented in Table 1.

Table 1. List of Data Sources

Code	Title	Link and Publication Date
A	رسالة الهاكرز المسلمين للسويد بعد حرق القرآن الكريم	https://youtu.be/WmZqWQjfVXw
	Risālah al-hākirz al-muslimīn li al-swīd ba'd ḥarq al-qur'ān al-karīm 'Muslim hackers' messages to Sweden after the holy Qur'an burning incident'	January 29th, 2023

B	بدأ حملة الرد على أستراليا بضرب أهم المواقع الاستراتيجية الأسترالية	https://www.youtube.com/watch?v=b-2klMMOZUM
	Bad'u ḥamlah al-radd 'alā austrāliyā bi ḍarb ahamm al-mawāqi' al-istrātījiyah al-austrāliyah	
	'Beginning the campaign to retaliate against Australia by striking the most important Australian strategic sites'	March 25th, 2023
C	رد الهاكرز المسلمين على الصهاينة بعد الإعتداء على المصلين داخل المسجد الأقصى المبارك	https://youtu.be/ALAvksPfB8M
	Radd al-hākirz al-muslimīn 'alā al-ṣahāyanah ba'd al-I'tidā' 'alā al-muṣallīn dākhil al-masjid al-aqṣā al-mubārak	April 6th, 2023
	'The response of Muslim hackers to the Zionists after the attack on worshipers at the al-Aqsa mosque'	

Data collecting involved the steps of data transcription, rereading, printing, and classification. Video narration and running text correctness were prioritized in manual data transcription. Re-reading as a validation technique of transcription results involved checking transcribed words, phrases, and clauses. To strengthen the validity of the data, cross-referencing between the transcription results and subtitle videos was repeatedly carried out to yield the final data. In addition, time details in the form of minutes and seconds were also included in the presentation of sentence data to ensure that the data has been rigidly validated. Finally, the researcher printed the data for classification. Inclusion and exclusion of data in the form of words, phrases, and sentences referred to analysis features that emphasized attention to the meaning and context of the data. A data card inventory of each data point simplified data analysis after classification.

The data card's final data was reduced, presented, analyzed, interpreted, and concluded (Antonio et al., 2020; Lester et al., 2020; Mezmir, 2020; Ningi, 2022). Data reduction involved choosing data points for analysis display. At this point, the researcher validated that each data variation would be represented. After transliterating the Arabic into Latin script according to ALA-LC romanization norms, the data display step began. Next came data analysis and interpretation. Language in the data was analyzed using van Dijk's ideological square theoretical framework. The interpretation stage included explaining and comparing analytical results to previous investigations. In the last phase, the researcher confirmed the research questions and highlighted the innovative discoveries.

The data analysis was conducted using a critical discourse analysis framework by employing the ideological square model put forward by van Dijk (van Dijk, 2006; Van Dijk, 2006b). The ideological square elucidated the dichotomous depictions of oneself and others in communication, wherein the self or in-group was typically shown favorably, while individuals from the out-group were depicted unfavorably. According to Van Dijk (2006, 2006b & 2006a), the analysis stage involved a macro analysis with basic discursive strategies and a micro analysis with rhetorical discursive strategies. The data cards were used as the basis for thematic identification and classification of discursive strategies which were arranged in tabular form according to existing analysis features. The microanalysis and macroanalysis elements are shown in Table 2.

Table 2. Microanalysis and Macroanalysis Elements in the Ideological Square Model

Macro Analysis (Basic Discursive Strategies)	Micro Analysis (Rhetorical Discursive Strategies)
(1) Emphasize positive things about 'us'; (2) Emphasize negative things about 'them'; (3) De-Emphasize negative things about 'us'; and (4) De-emphasize positive things about 'them'.	(1) Actor description; (2) Authority; (3) Burden; (4) Categorization; (5) Comparison; (6) Consensus; (7) Counterfactual; (8) Disclaimer; (9) Euphemism; (10) Evidentiality; (11) Argumentation; (12) Ilustration/Example; (13) Generalization; (14) Hyperbole; (15) Implication; (16) Irony; (17) Lexicalization; (18) Metaphor; (19) National self-glorification; (20) Norm expression; (21) Number game;

(22) Polarization; (23) Populism; (24) Presupposition; and (25) Victimization.

FINDINGS AND DISCUSSION

The research findings indicate the presence of three basic discursive strategies in MH's discourse: emphasizing positive "us"; emphasizing negative "them"; and de-emphasizing positive "them." Additionally, the author identified seven rhetorical discursive strategies: actor description; consensus; evidentiality; example/illustration; values expression; number game; and victimization-criminalization. Table 3 displays the descriptive statistics for these findings.

Table 3. Descriptive Statistics of Basic and Rhetorical Discursive Strategies in MH's Hacktivism Discourse

No	Strategies	Emphasizing Positive 'Us'		Emphasizing Negative 'Them'		De-emphasizing Negative 'Us'		De-emphasizing Positive 'Them'		Total	
		N	%	N	%	N	%	N	%	N	%
1	Actor Description	4	36.36	6	19.35	0	0.00	13	39.39	23	31.08
2	Consensus	2	18.18	0	0.00	0	0.00	0	0.00	2	2.70
3	Evidentiality	0	0.00	5	16.13	0	0.00	0	0.00	5	5.41
4	Example/Illustration	2	18.18	0	0.00	0	0.00	5	15.15	7	9.46
5	Values Expression	0	0.00	12	38.71	0	0.00	2	6.06	14	18.92
6	Number Game	3	27.27	1	3.23	0	0.00	0	0.00	4	5.41
7	Victimization-Criminalization	0	0.00	7	22.58	0	0.00	13	39.39	20	27.03
	Total	11	100	31	100	0	0.0	33	100	75	100

Descriptive statistics in Table 3 prove that the dominant strategies used by MH are actor description (31.08%), victimization-criminalization (27.03%), and values expression (18.92%). This finding indicates that MH's hacking threat discourse focuses more on actor representation than action representation. Based on the actor representation strategies, these three dominant strategies are strongly interconnected. In actor description, MH emphasizes their perspective on the subjects mentioned in the discourse. This perspective is strengthened by grouping actors as criminals and victims in the victimization-criminalization strategy. Ultimately, MH justifies the positive and negative dimensions of these actors through values expression. This finding is in line with the "us" versus "them" dichotomy proposed by van Dijk as the main basis for mapping ideology in discourse.

Actor Description

Actor description is a discursive tactic to construct the image of an individual or group mentioned in the discourse. Actor description can be a depiction of the character, role, tendencies, and status of the actor in various social and political dimensions. Through this tactic, discourse producers classify actors as in-groups that tend to be represented positively and out-groups that tend to be represented negatively. This form of representation further indicates the bias of the discourse producer towards certain actors. About this concept, the actors mentioned in the MH's threat are shown in Table 4.

No	Actors	Description	Freq.	Percent.
1	'Government of Sweden' (ḥukūmah al-swīd) حكومة السويد	Anti-Islam	١	4.35%
2	'Zionist soldiers' (al-junūd al-ṣahāyanah) الجنود الصهاينة	Terrorist	١	4.35%
		Destroyer	1	4.35%
3	'Moslem' (al-muslimūn) المسلمون	Victims	5	17.39%
4	'worshipers' (al-muṣallīn) المصلين	Victims	2	8.70%
5	'Rasmus Paludan' (rāsmūs bālūdān) راسموس بالودان	Extremist	1	4.35%
		Racist	1	4.35%
6	'group of hackers' (majmuʽah hākirz) مجموعة هاكرز	Activist	1	4.35%

7	'Refugees' (*lāji'īn*) لاجئين	Victims	٢	8.70%
8	'Afghanistan' (*afghānistān*) أفغانستان	Crisis country	1	4.35%
9	'Iraq' (*'irāq*) عراق	Crisis country	1	4.35%
10	'Syria' (*sūriya*) سوريا	Crisis country	1	4.35%
11	'Australian fashion house' (*dār al-azyā' al-astrāliyah* دار الأزياء الأسترالية)	Provocateur	1	4.35%
12	'Government of Australia' (*hukūmah astrāliya* حكومة أسترالیا)	Victims	1	4.35%
13	'Moslem hackers' (*al-hākirz al-muslimūn* الهاكرز المسلمون)	Activist	3	13.05%
14	'People of Sweden' (*sha'b al-swīd* شعب السويد)	Victims	1	4.35%
Total			23	100%

Based on the description of roles and attitude tendencies, the actors in Table 4 are classified into three types: positive; neutral; and negative. Positive actors are *al-hākirz al-muslimūn* 'moslem hackers' and *majmu'ah hākirz* 'group of hackers' who are described as activists (17.40%). Neutral actors are groups and countries described as victims as well as crisis countries (56.50%). Negative actors are groups and countries that carry out various negative actions and are described as anti-Islam, terrorists, destroyers, extremists, racists, and provocateurs (26.10%). The positive actors are a manifestation of the strategy of emphasizing positive "us", neutral actors are a manifestation of the strategy of deemphasizing positive "them", and negative actors are a reflection of the strategy of emphasizing negative "them".

In their hacking threat, MH describes the actors through lexicalization techniques, namely choosing strong words to describe the actors' actions. For example, MH describes the hacker group as activists through the phrase *tuwaḥḥidu li naṣrah filasṭīn* 'unite to support Palestine'. The lexical *naṣrah* 'support' contains a positive intention which means the hacker group is an organization that is involved in fighting to defend Palestine. The same technique is also found in the description of negative actors, where HM describes the Israeli army through the phrases *i'taddū bi quswah* 'they brutally destroyed' and *i'taqalū al-miāt min al-muṣallīn* 'they arrested hundreds of worshipers'. The lexical *i'taddū* 'destroyed' and *i'taqalū* 'arrested' mean that the Israeli army is the perpetrator of violence.

Consensus

As a political strategy to build consolidation between several actors, consensus emphasizes the existence of understanding and agreement on values between one actor and another. This strategy is used by discourse producers to strengthen arguments by involving other actors in the form of individuals or organizations. The involvement of other actors aims to increase the authority and legitimacy of the discourse, as well as the bargaining position of the discourse producers toward the discourse target. In line with this concept, MH in their threats only mentioned two organizations, namely *majmu'ah hakirz* 'group of hackers' and *al-hakirz al-muslimun* 'moslem hackers', where each organization is only mentioned once. The construction of consensus in the discourse involving the two organizations can be seen in the excerpts below.

بمشاركة أكثر من أربعين مجموعة هاكرز من مختلف أنحاء العالم.

bi mushārakah akthar min arba'īn majmu'ah hākirz min mukhtalif anhā' al-'ālam. (Data C. Minutes 1:18-1:23)
'With the participation of more than forty hacker groups from around the world.'

هجمات سيبرانية من الهاكرز المسلمين على أكثر من سبعين من المواقع الاستراتيجية الأسترالية.

hajamāt sibrāniyah min al-hākirz al-muslimīn 'alā akthar min sab'īn min al-mawāqi' al istrātījiyah al-astrāliyah. (Data B. Minutes 0:56-0:58)
'Cyber-attacks by Moslem hackers on more than seventy Australian strategic sites.'

The excerpts show that MH does not build consensus with organizations, institutions, or superpowers. However, they only consolidate power with other hacker groups. *Majmu'ah hākirz* 'hacker groups' and *al-hākirz al-muslimūn* 'moslem hackers' mentioned are underground organizations whose existence is unknown to the public. Information about the organization that is

spread to the public is limited to the history of hacking actions carried out, not to the identity of the individuals involved in it. Thus, the power of political consolidation built by MH through consensus is based on the track record of these hacker organizations which may be known to have carried out actions on many targets.

The consensus strategy implemented by MH is an effort to define their identity. MH acknowledges their relationship with other groups that have the same vision, actions, and values. This strategy in the ideological square aims to emphasize positive 'us'. MH indirectly describes their self-identity as brave, untraceable, and unpredictable activists. That consensus is also a political movement, where MH also emphasizes their relations and consolidation to exert greater political pressure on their targets. The main target of the political movement is of course to influence the political decisions and policies of the Israeli, Swedish, and Australian governments.

Evidentiality

Evidentiality is a strategy of rationalizing arguments or discourse by showing valid and credible evidence. Evidentiality can be done by referring to authoritative statements or factual information that is objective and transparent. The evidentiality strategy aims to emphasize the objectivity, reliability, and credibility of the arguments mentioned in the discourse. With rationalization through evidentiality, discourse producers can construct a positive image of themselves as a source of trustworthy information. Concerning this concept, the five evidentiality strategies found in the MH's threat discourse are directed at emphasizing the negative image of the discourse target consisting of Zionist soldiers, the racist extremist Rasmus Paludan, the government of Sweden, and the Australian fashion house. Among the examples of evidentiality can be seen in the excerpts below.

<div dir="rtl">

...واعتدو بقصوة على المصلين داخل المسجد.

</div>

...wa i'taddū bi quswah 'alā al-muṣallīn dākhil al-masjid. (Data C. Minutes 0:14-0:18)
'...and brutally attacked the worshipers inside the mosque.'

<div dir="rtl">

...بحرق نسخة من القرآن الكريم.

</div>

...bi ḥarq nuskhah min al-qur'ān al-karīm. (Data A. Minutes 0:40-0:41)
'...burned a copy of the Holy Quran.'

These excerpts contain important facts about the actions that triggered the emergence of MH hacking threats to their targets. In the first excerpt, the fact is the brutal attack by Israeli soldiers (...*wa i'taddū bi quswah 'alā al-muṣallīn dākhil al-masjid* '...and brutally attacked the worshipers inside the mosque). Meanwhile, in the second excerpt, the fact is the burning of the Qur'an by Rasmus Paludan (*ḥarq nuskhah min al-qur'ān al-karīm* 'burned a copy of the Holy Qur'an). MH strengthens these facts through audiovisual evidence that is shown at the opening and background of the narrative video. The fact in the first excerpt is supported by evidence in the form of a video of the Israeli army attacking worshipers at the Al-Aqsa mosque. Meanwhile, the fact in the second excerpt is supported by visual evidence Rasmus Paludan burning the Qur'an in a public space. The evidentiality strategy applied by MH in their narrative can be seen in Figures 1 and 2.

Figure 1. Attack of Israeli soldiers in Al-Aqsa Mosque

Figure 2. Burning of the Qur'an by Rasmus Paludan

The MH's evidentiality strategy emphasizes the negative acts of "them". The display of videos of Israeli soldiers attacking people and visuals of the burning of the Qur'an represent actors who do not appreciate the values of humanity and tolerance. In the prediction of further effects, this strategy is effective in provoking Muslims in various parts of the world. The Al-Aqsa Mosque and the Qur'an are sacred and holy entities in Islam, and criminal treatment of the two entities can incur Muslim anger. This provocation effect can then become MH's capital to mobilize the masses of supporters of their hacking actions. Thus, the hacking threats they spread via the

internet can gain more legitimacy from other users.

Example/Illustration

Example/illustration is a strategy to concretize arguments or narratives conveyed in discourse. This strategy can be in the form of sketches or short stories, more complete detailed descriptions, and illustrations in audio or visual form. The example/illustration strategy aims to build emotional, persuasive, and provocative impacts. With the presentation of examples and illustrations, the discourse will become stronger and easier to understand. Based on this concept, seven example/illustration strategies were found in MH's threat discourse. These strategies are shown in the excerpt below.

أصابت المواقع الحكومية والخاصة والبنوك والموانئ والمطارات منها موقع الشرطة الأسترالية: بنك سيدني، مطار بورت ماكواري، مطار كوفي هاربور، مطار كيرنز، مطار أبوري، موقع لجنة الإنتاجية، المعهد الأسترالية للدراسات الأسرية، ميناء داروين.

aṣābat al-mawāqi' al-ḥukūmiyah wa al-khāṣṣah wa al-bunuk wa al-mawāini' wa al-maṭārāt minhā mawqi' al-shurṭah al-astrāliyah: bank sidney, maṭār pūrt mākwārī, maṭār kufī hārbūr, maṭār kīrnz, maṭār abūrī, mawqi' lajnah al-intājiyah, al-ma'had al-astrāliyah li al-dirāsāt al-usriyah, mīnā dārwīn. (Data B. Minutes 0:59-1:29)
'It affected the government and private sites, banks, ports, and airports, including the Australian Police Force website: Bank of Sydney, Port Macquarie Airport, Coffee Harbor Airport, Cairns Airport, Apuri Airport, Productivity Commission website, Australian Institute for Family Studies, Port Darwin.'

MH provides detailed descriptions and visual illustrations as a reflection of the example/illustration strategy. Detailed descriptions can be seen in the excerpts, where MH mentions the targets of their hacking operations one by one. In the first excerpt, MH mentions strategic Australian government sites related to economic activities and public services (*…al-bunuk wa al-mawāini' wa al-maṭārāt minhā mawqi' al-shurṭah al-astrāliyah: bank sidney, maṭār pūrt mākwārī, maṭār kufī hārbūr, maṭār kīrnz, maṭār abūrī, mawqi' lajnah al-intājiyah, al-ma'had al-astrāliyah li al-dirāsāt al-usriyah, mīnā dārwīn* '…banks, ports, and airports, including the Australian Police

website: Bank of Sydney, Port Macquarie Airport, Coffee Harbor Airport, Cairns Airport, Apuri Airport, Productivity Commission website, Australian Institute for Family Studies, Port Darwin).

The example/illustration strategy in visual form is found in video 3, where MH displays screen captures of the impact of the attack on the Port Macquarie Airport and Cairns Airport websites, in Australia. The visual illustration is shown in Figure 3.
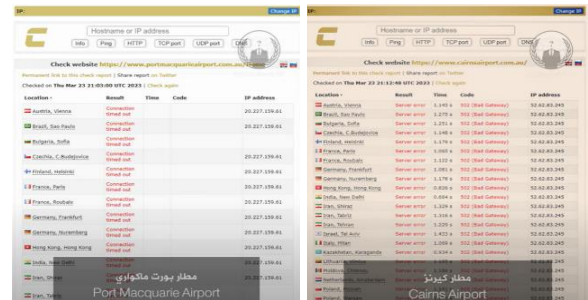

Figure 3. Hacking attack in Australia's strategic public sites

Following the purpose of the threat they spread, the example/illustration strategy in MH's discourse is effective in creating anxiety and fear in their targets. Rigid mention of hacking targets that are strategic infrastructures will automatically become a serious concern for the government. In addition, screen captures showing that the hacking action has begun will increase the panic of the targeted government. In the context of the ideological square, this strategy reflects self-identity description, activity description, and goal description. Example/illustration exposes the positive sides of MH as a discourse producer. Through this strategy, MH represents itself as a group that is brave, clever, smart, and able to put pressure on its targets.

Values Expression

As an association strategy towards certain actors, values expression aims to affirm the category of actors through the positive and negative values associated with them. Positive values will tend to be associated with "us", while negative values tend to be associated with "them". In this context, the values expressed by MH are shown in Table 5 below.

No	Values	Tendency	Freq.	Total	Percent.
1	'blessed' (*al-mubārak*) المبارك	Positive	1	2	14.29%
2	'holy' (*al-muqaddasah*) المقدسة		1		
3	'big' (*al-kabīr*) الكبير	Negative	1	12	85.71%
4	'harsh' (*qāṣ*) قاس		2		
5	'barbarism' (*hamjiyah*) همجية		1		
6	'low' (*mutadannī*) متدني		1		
7	'pseudo' (*al-zaīfah*) الزائفة		1		
8	'bad' (*al-sayyiah*) السيئة		1		
9	'vile' (*danīah*) دنيئة		1		
10	'provocative' (*mustafiz*) مستفز		2		
11	'painful' (*mu'lim*) مؤلم		1		
12	'racist' (*al-'unsurī*) العنصري		1		
	Total		14	14	100%

Their threat, namely *al-mubārak* 'blessed' and *al-muqaddasah* 'holy'. These values are not associated with any actor, but are attached to the nouns *al-masjid al-aqsā* 'al-Aqsa mosque' and *al-ard* 'land' which refers to the Palestinian territories. In contrast, MH mentions twelve negative values associated with several actors and actions. MH describes the Israeli army as having great arrogance (*kabīr*). The Swedish government is represented as an actor that is barbaric (*hamajiyah*), fake (*al-zaīfah*), lowly-civilized (*mutadannī*), bad (*sayyiah*), and vile (*danīah*). The Australian fashion house is said to have carried out provocative actions (*mustafiz*), while Rasmus Paludan is called a racist (*al-'unsurī*). Meanwhile, MH describes the hacking action as a harsh (*qāṣ*) and painful (*mu'lim*) revenge.

From the strategic discursive perspective, the data in Table 4 are oriented towards emphasizing the negative "them". Although there are some positive values, these values are not attached to the actors and are used to construct a negative image of certain actors. The actor is described as violating certain noble values so he is represented negatively. In this context, *mubārak* 'blessed' and *al-muqaddasah* 'holy' are two noble values attached to sacred monuments of Muslims. So the behavior of the Israeli army that violates the sacredness is associated with behavior with negative values. The association of the values in Table 4 with the actors explicitly mentioned in the discourse strengthens the argument about the efforts of MH to emphasize the negative side of "others".

Number Game

Number game is a strategy to increase the credibility of discourse through the mention of objective data in the form of numbers and statistics. Number games can construct an image of the discourse producer's understanding of his argument. Through the expression of numbers and statistics, the arguments will become more valid and reliable. Related to this concept, three uses of the number game strategy were found in MH's threat. These strategies can be seen in the excerpts below.

واعتقلوا المئات من المصلين.

wa i'taqalū al-miaṭ min al-muṣallīn. (Data C. Minutes 0:24-0:26)
'They arrested hundreds of worshipers.'

بمشاركة أكثر من أربعين مجموعة هاكرز من مختلف أنحاء العالم.

bi mushārakah akthar min arba'īn majmu'ah hākirz min mukhtalif anhā' al-'ālam. (Data C. Minutes 1:18-1:23)
'With the participation of more than forty hacker groups from around the world.'

هجمات سيبرانية من الهاكرز المسلمين على أكثر من سبعين من المواقع الاستراتيجية الأسترالية.

hajamaṭ sibrāniyah min al-hākirz al-muslimīn 'alā akthar min sab'īn min al-mawāqi' al istratījiyah al-astrāliyah. (Data B. Minutes 0:56-0:58)
'Cyber-attacks by Muslim hackers on more than seventy Australian strategic sites.'

MH uses a number game strategy by mentioning several numbers in the data above. The number *al-miaṭ* 'hundreds' in the first

excerpt indicates the number of worshipers attacked; *akthar min arba'īn* 'more than forty' in the second excerpt indicates the number of hacker groups; while *akthar min sab'īn* 'more than seventy' in the third excerpt indicates the number of government sites targeted for hacking. MH never mentions a definite number at all, but uses approximate phrases such as *al-miaī* 'hundreds' and *akthar min* 'more than'. On the one hand, this pattern indicates that MH does not have valid and fixed statistical data. However, on the other hand, this pattern constructs the meaning of infinite numbers that can be an effect of anxiety and fear in their target organizations or countries.

The number game in these data reflects the strategy of emphasizing positive 'us' and emphasizing negative 'them'. In the second and third excerpts, MH represents their positive image as actors who initiate and carry out hacking actions. The numbers in the second excerpt show their strength in carrying out political consolidation, with thw capability of mobilizing more than forty other hacker groups. Meanwhile, the numbers in the third excerpt also show their greatness in activism, by being able to hack more than seventy strategic Australian government sites. In contrast to the second and third excerpts, the first excerpt contains a negative image of Israeli soldiers who attacked worshipers at the al-Aqsa mosque. MH describes the soldiers as brutal actors because of the high number of victims of the attack, which reached hundreds of people.

Victimization-Criminalization

Victimization-criminalization is an important strategy that positions certain actors as victims and criminals in discourse. In their threat, MH positions Zionist soldiers, Zionists, Rasmus Paludan, Extremists, the King of Sweden, and an Australian fashion house as criminals. On the other hand, worshipers, Muslims, refugees, Afghanistan, Iraq, Syria, and the babies were positioned as victims. The distribution of victims' and criminals' status can be seen in Table 6.

No	Actors	Status	Freq.	Total	Percent.
1	'Zionist soldiers' (*al-junūd al-ṣahāyanah*) الجنود الصهاينة	Criminal	1	7	35.00%
2	'Zionist' (*al-ṣahāyanah*) الصهاينة		2		
3	'Rasmus Paludan' (*rāsmūs bālūdān*) راسموس بالودان		1		
4	'Extremist' (*al-mutaṭarrif*) المتطرف		1		
5	'King of Sweden' (*al-sulṭān al-swīdiyah*) السلطان السويدية		1		
6	'Australian Fashion House' (*dār al-azyaʾ al-astrāliyah*) دار الأزياء الأسترالية		1		
7	'Worshipers' (*al-muṣallīn*) المصلين	Victim	2	13	65.00%
8	'Moslem' (*al-muslimīn*) المسلمين		5		
9	'Refugees' (*lāji'īn*) لاجئين		2		
10	'Afghanistan' (*afghānistān*) أفغانستان		1		
11	'Iraq' (*'irāq*) عراق		1		
12	'Syria' (*sūriya*) سوريا		1		
13	'Babies' (*al-aṭfāl*) الأطفال		1		
	Total		20	20	100%

Based on the data in Table 6, MH's tendency to categorize victim-criminals based on the perspective of religiosity and humanity was found. Israel and its soldiers called *al-junūd al-ṣahāyanah* 'zionist soldiers' and *al-ṣahāyanah* 'zionist' were declared criminals for committing crimes against humanity against worshipers at the Al-Aqsa mosque in particular and Palestinians in general. Meanwhile, actors such as *rāsmūs bālūdān* 'Rasmus Paludan' *al-*

mutaṭarrif 'extremist', *al-sulṭān al-swīdiyah* King of Sweden, and *dār al-azyaʾ al-astrāliyah* 'Australian Fashion House' were declared criminals for committing religious crimes in the form of blasphemy against Islam. In the victim categorization, this perspective is emphasized by the actor *al-muslimīn* 'moslem' who is positioned as a victim of blasphemy against Islam and several other actors (*al-muṣallīn* 'the worshipers', *lāji'īn* 'refugees',

afghaฺnistaฺn 'Afghanistan, *'iraฺq* 'Iraq', *suฺriya* 'Syria', and *al-atfaฺl* 'the babies') who are positioned as victims of crimes against humanity.

The representation of actors as victims is a form of de-emphasizing positive 'them', while the representation of actors as criminals is a form of emphasizing negative 'them'. In this context, the actors who contrast as victims and criminals are not part of the in-group of MH. Actors such as *al-muṣallīn* 'worshipers', *al-muslimīn* 'moslems', *lāji'īn* 'refugees', *afghaฺnistaฺn* 'Afghanistan', *'iraฺq* 'Iraq', *suฺriya* 'Syria', and *al-atfaฺl* 'babies' are depicted neutrally. MH does not mention any positive values of these actors. MH instrumentalizes them as tools for the real discourse, namely the construction of negative images of criminal actors. In other work by van Dijk, this tactic is also called by compassion move, where discourse producers show empathy and sympathy for weak victims of the "other's" actions to escalate the brutality of the "other".

From the standpoint of basic discursive strategies, MH's hacktivism discourse is primarily characterized by de-emphasizing positive things about "them" (44.00%) and emphasizing negative things about "them" (41.33%). Yet, the data sources show that emphasizing positive things about "us" is scarce, accounting for only 14.67%. Within the two prevailing strategies, MH delineates "others" in a multitude of manifestations. De-emphasizing positive things about "them" is employed in the portrayal of third parties who serve as instruments in the construction of hacking threats. Meanwhile, emphasizing negative things about "them" is directed toward adversarial actors who are the source of resentment and the subject of cyber threats. Table 7 below provides a comprehensive breakdown of the quantity and percentage of use for each strategy.

No	Strategies	Frequency	Percentage
1	Emphasizing Positive Things about 'Us'	11	14.67
2	Emphasizing Negative Things about 'Them'	31	41.33
3	De-Emphasizing Negative Things about 'Us'	0	00.00
4	De-Emphasizing Positive Things about 'Them'	33	44.00
	Total	75	100

The dominance of *de-emphasizing positive things about "them"* (44.00%) and *emphasizing negative things about "them"* (41.33%) prove that MH's hacking threat discourse focuses more on actors outside themselves. Thus, the ideology in the discourse can be read through MH's perspective on the subjects they mention, not assumptions and glorification of themselves. The percentage of talking more about "them" than "us" can be explained by analyzing MH's position in the social structure and context. MH represents itself as an underground hacker organization that usually hides its identity. This status requires MH to talk less about themselves because it risks exposing their identities. Therefore, the hacking discourse is certain not to contain explicit representations of MH as discourse producers because that could be a clue to their true identities. In this context, MH becomes an ideological symbol, not an identified figure.

The arguments presented by Navarretta and Hansen (2020) as well as Etaywe and Zappavigna (2022) suggest that ideology can be analyzed through the word frequency and the consistency of actor representation in discourse. Consequently, the ideology within the MH hacking discourse can be effectively mapped and identified. The basic and rhetorical discursive strategies that are increasingly beneficial indicate that the ideology present in the discourse is characterized by anti-imperialism and anti-extremism. Anti-imperialism can be understood as an ideology that rejects forms of domination of certain individuals or groups over other individuals or groups, while anti-extremism is an ideology that opposes extreme ways of thinking and acting. Both ideologies serve as foundational elements that encapsulate normative and ideal values for MH in perceiving, interpreting, and reacting to their surrounding reality. In response to instances of violence against humanity and Islamic thought, MH adopts a definitive ideological stance, explicitly rejecting all manifestations of such practices.

The anti-imperialism ideology, as linked to the ideological square theory (van Dijk, 2006a, 2006b), is evident in the data that portrays the Israeli army, the Swedish government, and the Australian government in a negative light. MH employs strong diction to assert that violence against worshipers at Al-Aqsa and refugees from various Middle Eastern countries constitutes a violation of universal humanitarian values. Furthermore, anti-imperialism is evident in the neutral representation of third-party actors, including worshipers, refugees, and individuals from Afghanistan, Iraq, Syria, and infants. MH fails to articulate the positive aspects of these actors. They manipulate and politicize the circumstances of the actors to highlight the negative attributes of the threatened targets. By defending these actors, MH enhances their self-representation as adversaries of imperialism and violence against humanity.

The anti-extremism ideology is evident in the unfavorable data portraying Rasmus Paludan, the Swedish government, a fashion house in Australia, and the Australian government. MH unequivocally condemns racist and hateful actions against Islam perpetrated by Western nations. MH characterizes Rasmus Paludan's act of burning the Qur'an as an expression of extremism and racism, indicative of a deterioration in the intellectual climate of Swedish society. He similarly criticized a fashion house in Australia for showcasing women's clothing designs featuring the name "Allah" at a fashion show in Melbourne. For MH, the provocation and harassment of Islamic values represent not merely a manifestation of Islamophobia, but rather an expression of hatred. MH challenges the prevailing narrative regarding extremists commonly linked to Muslims through their discourse. MH posits that extremism can arise in any individual, including those within Western society.

From the perspective of discourse content, the results of the study strengthen several findings in previous studies. MH's hacking threat, which is characterized by the dichotomy of "us" and "them," aligns with the findings of Etaywe (2022) as well as Etaywe and Zappavigna (2022), which indicate that the grammar of othering and antagonism is framed within the narrative of the out-group as an ideological threat. The negation of "them" is articulated through justification languages that reference the ideal cultural parameters and meta-values of the discourse producers. MH rationalizes negative actors through the lens of Islamic values, humanity, freedom, and justice. MH's approach to constructing the images of these actors reinforces the findings of Etaywe (2022), which indicate that othering and antagonism function within a framework of victimization and injustice. Moral violations catalyze discourses that frame antagonism and aggressive actions as commonplace and socially acceptable.

From the perspective of style, the *language of threat*, a central phenomenon in HM threat discourse, is aligned with the *language of terror* associated with transnational terrorist groups (Qi, 2020; Reflinaldi et al., 2021). Loyalty to the in-group and concern for threats against in-group members are employed to justify violent actions and violations of norms (Etaywe, 2022; Etaywe & Zappavigna, 2022). This context positions MH's hacking threat and action as violations of norms, which are justified through the defense of oppressed neutral actors who are victims of systemic violence. MH's threat discourse parallels the substance of threats posed by terrorist groups. However, the MH threat discourse is more specific because it focuses on the construction of cyber-activism as a measured and systematic response to targets (Farmer, 2022; Richards & Wood, 2018; Romagna & Leukfeldt, 2023).

Discourse orientation, as a method of countering Islamophobia, extremism, and terrorism, reveals that the threat of MH hacking represents a unique manifestation of actions identified in various prior studies. Prior studies indicated that counter-narrative actions were primarily influenced by education, culture, and art (Elamin, 2024; Ismail, 2023; Mansoor et al., 2021; Mashwani et al., 2022; Umar et al., 2021). In contrast to these actions, MH engages in political advocacy that directly targets policymakers. Previous studies indicate that counter-narrative actions originated from grassroots movements, whereas MH hacking threats and actions were implemented from a top-down approach. MH's decision to undertake actions that directly intervene in the government can be analyzed through the lens of Islamophobia and anti-Islam sentiment prevalent in the Western

world. Islamophobia and anti-Muslim sentiments are openly promoted and legitimized by state leaders in official forums (M. H. Khan et al., 2020, 2021; R. M. Khan, 2021; Rubin, 2020; Ślusarczyk, 2021).

From the perspective of digital activism, the hacktivism discourse echoed by MH is different from various forms of digital activism that have existed before (Reflinaldi et al., 2023, 2024). MH operates within a specialized domain, wherein hacking is exclusively conducted by elite groups proficient in information and communication technology. The activism conducted by MH extends beyond conventional digital activism as demonstrated in various prior studies (George & Leidner, 2019; Richards & Wood, 2018). In the contemporary digital landscape, hacktivism executed by MH is likely to be more effective than traditional campaigns and demonstrations, which remain susceptible to suppression via negotiation, hegemony, and repressive measures (Álvarez-Benjumea & Winter, 2020; Bélanger et al., 2020). The prioritization of concerns regarding hacking over street demonstrations in numerous countries indicates that hacktivism can exert more significant and strategic political pressure than traditional mass action (Alexopoulou & Pavli, 2021; Beck, 2016; Svyrydenko & Mozgin, 2022).

CONCLUSION

This study concludes that MH employs both basic and rhetorical discursive strategies concurrently in the discourse surrounding hacking threats. The fundamental discursive strategies employed include emphasizing positive 'us', emphasizing negative 'them', and deemphasizing positive 'them'. Meanwhile, the rhetorical discursive strategies employed include actor description, consensus, evidentiality, example/illustration, values expression, game number, and victimization-criminalization. The analysis of the discursive strategies revealed that the underlying ideology in the discourse is characterized by anti-imperialism and anti-extremism. Anti-imperialism is expressed in discourses advocating for the defense of colonized populations and is enacted through hacking activities aimed at retribution. Anti-extremism is reflected in protest discourses concerning insults to Islam that are linked to extremist actions. Hacktivism, as a novel form of digital activism executed by MH, will effectively exert political pressure on the target.

This study is limited by the relatively small data corpus. This situation presents an opportunity for future researchers to conduct observations on larger datasets or, if feasible, in the form of a corpus. The threat of hacking is a prevalent issue in the digital and technological era. Consequently, it will be feasible to compile a corpus of discourse regarding the threat of hacking. This study is examined through the lens of critical discourse analysis, specifically the ideological square. The ideological square emphasizes the identification of ideology by examining the representation of "self" versus "other" or "us" versus "them" within a discourse. The phenomenon of hacking threats disseminated via YouTube can be examined through various discourse analysis frameworks. Further researchers may apply multimodal discourse analysis as a perspective. This perspective allows for a deeper examination of audio, visual, color codes, and other videographic elements about their role in discourse interpretation. The study aims to offer novel theoretical perspectives on pertinent research.

REFERENCES

Abbas, L., Fahmy, S. S., Ayad, S., Ibrahim, M., & Ali, A. H. (2022). TikTok intifada: Analyzing social media activism among youth. *Online Media and Global Communication*, *1*(2), 287–314. https://doi.org/10.1515/omgc-2022-0014

Abushbak, A. M. A., & Majeed, T. (2020). *The role of social media in mobilizing crowd protest-A case study of Palestinian anger against Israel's military measures at Al-Aqsa compound on Instagram*. *40*(10), 511–526. ssrn_id3972494_code2261782.pdf

Alexopoulou, S., & Pavli, A. (2021). 'Beneath this mask there is more than flesh, beneath this mask there is an idea': Anonymous as the (Super)heroes of the internet? *International Journal for the Semiotics of Law*, *34*(1), 237–264. https://doi.org/10.1007/s11196-019-09615-6

Alharahsheh, H. H., & Pius, A. (2020). A review of key paradigms: Positivism vsinterpretivism. *Global Academic Journal of Humanities and Social Science*, *2*(3), 39–43. DOI: 10.36348/gajhss.2020.v02i03.001

Álvarez-Benjumea, A., & Winter, F. (2020). The breakdown of antiracist norms: A natural experiment on hate speech after terrorist attacks. *Proceedings of the National Academy of Sciences of the United States of America*, *117*(37), 22800–22804. https://doi.org/10.1073/pnas.2007977117

Antonio, M. G., Schick-Makaroff, K., Doiron, J. M., Sheilds, L., White, L., & Molzahn, A. (2020). Qualitative data management and analysis within a data repository. *Western Journal of Nursing Research*, *42*(8), 640–648. https://doi.org/10.1177/0193945919881706

Aspers, P., & Corte, U. (2019). What is qualitative in qualitative research. *Qualitative Sociology*, *42*(2), 139–160. https://doi.org/10.1007/s11133-019-9413-7

Aspers, P., & Corte, U. (2021). What is qualitative in research. *Qualitative Sociology*, *44*(4), 599–608. https://doi.org/10.1007/s11133-021-09497-w

Beck, C. (2016). Web of resistance: Deleuzian digital space and hacktivism. *Journal for Cultural Research*, *20*(4), 334–349. https://doi.org/10.1080/14797585.2016.1168971

Bélanger, J. J., Nisa, C. F., Schumpe, B. M., Gurmu, T., Williams, M. J., & Putra, I. E. (2020). Do ounter-narratives reduce support for ISIS? Yes, but not for their target audience. *Frontiers in Psychology*, *11*(June/6), 1–11. https://doi.org/10.3389/fpsyg.2020.01059

Borelli, M. (2023). Social media corporations as actors of counter-terrorism. *New Media and Society*, *25*(11), 2877–2897. https://doi.org/10.1177/14614448211035121

Delmas, C. (2018). Is hacktivism the new civil disobedience?. *Raisons Politiques*, *69*(1), 63–81. https://doi.org/10.3917/rai.069.0063

Dumitrica, D., & Felt, M. (2020). Mediated grassroots collective action: Negotiating barriers of digital activism. *Information Communication and Society*, *23*(13), 1821–1837. https://doi.org/10.1080/1369118X.2019.1618891

Elamin, M. O. I. (2024). Counteracting islamophobia through strategic media narratives: A multi-case study approach. *International Journal of Religion*, *5*(10), 2733–2750. https://doi.org/10.61707/9px57616

Ellefsen, R., & Jämte, J. (2023). The causes, content and consequences of repression: A framework for analyzing protest control in the counter-extremism era. *Social Movement Studies*, *22*(4), 567–582. https://doi.org/10.1080/14742837.2022.2067140

Etaywe, A. (2022). Exploring the grammar of othering and antagonism as enacted in terrorist discourse: Verbal aggression in service of radicalisation. *Humanities and Social Sciences Communications*, *9*, Article 177 (2022). https://doi.org/10.1057/s41599-022-01178-5

Etaywe, A., & Zappavigna, M. (2022). Identity, ideology and threatening communication. *Journal of Language Aggression and Conflict*, *10*(2), 315–350. https://doi.org/10.1075/jlac.00058.eta

Faisol, Y., & Rahmat, W. (2021a). Cyberactivism in Palestinian conflict news comments on Al-Jezeera

YouTube channel: A cyberpragmatic study (Aktivisme siber dalam komentar berita konflik Palestina di kanal YouTube Al-Jazeera: Kajian siberpragmatik). *Gramatika STKIP PGRI Sumatera Barat*, *7*(2), 267–286. https://doi.org/10.22202/jg.2021.v7i2.4954

Faisol, Y., & Rahmat, W. (2021b). Negative impoliteness and reconstruction of identity: Cyberpragmatics analysis of Palestinian conflict news comments on Arab YouTube channel. *Jurnal Arbitrer*, *8*(2 SE-Articles), 168–179. https://doi.org/10.25077/ar.8.2.168-179.2021

Farmer, F. (2022). *Cybercrime vs hacktivism: Do we need a differentiated regulatory approach?* [Doctoral Thesis, University of Exeter]. University of Exeter Repository. http://hdl.handle.net/10871/129654

Ganesh, B., & Bright, J. (2020). Countering extremists on social media: Challenges for strategic communication and content moderation. *Policy and Internet*, *12*(1), 6–19. https://doi.org/10.1002/poi3.236

George, J. J., & Leidner, D. E. (2019). From clicktivism to hacktivism: Understanding digital activism. *Information and Organization*, *29*(3), Article 100249. https://doi.org/10.1016/j.infoandorg.2019.04.001

Ismail, M. O. (2023). Countering Islamophobia through sports: Qatar's initiatives during the 2022 FIFA World Cup. *International Journal of Membrane Science and Technology*, *10*(1), 1568–1578. https://doi.org/10.15379/ijmst.v10i1.2997

Kabir, S. N. (2021). The Muhammad cartoon controversy in New Zealand newspapers. *Journal of Arab & Muslim Media Research*, *14*(1), 143–156. https://doi.org/https://doi.org/10.1386/jammr_00028_1

Kazkaz, L., & Bosch, M. D. (2023). Islamic caricature controversy from Jyllands-Posten to Charlie Hebdo from the perspective of Arab opinion leaders. *Religions*, *14*(7), 864. https://doi.org/10.3390/rel14070864

Khan, M. H., Adnan, H. M., Kaur, S., Qazalbash, F., & Ismail, I. N. (2020). A critical discourse analysis of anti-Muslim rhetoric in Donald Trump's historic 2016 AIPAC policy speech. *Journal of Muslim Minority Affairs*, *40*(4), 543–558. https://doi.org/10.1080/13602004.2020.1828507

Khan, M. H., Qazalbash, F., Adnan, H. M., Yaqin, L. N., & Khuhro, R. A. (2021). Trump and Muslims: A critical discourse analysis of Islamophobic rhetoric in Donald Trump's selected tweets. *Sage Open*, *11*(1). https://doi.org/10.1177/21582440211004172

Khan, M. K., & Pratt, C. B. (2022). Strategic communications: The Pakistan military's use of social media against terrorism. *Media, War and Conflict*, *15*(4), 450–485. https://doi.org/10.1177/1750635220972127

Khan, R. M. (2021). Race, coloniality and the post 9/11 counter-discourse: Critical Terrorism Studies and the reproduction of the Islam-Terrorism discourse. *Critical Studies on Terrorism*, *14*(4), 498–501. https://doi.org/10.1080/17539153.2021.1983112

Lester, J. N., Cho, Y., & Lochmiller, C. R. (2020). Learning to do qualitative data analysis: A starting point. *Human Resource Development Review*, *19*(1), 94–106. https://doi.org/10.1177/1534484320903890

Maghfiroh, S. L., & Rohma, S. (2021). Optimization of social media as a counter to Islamophobia in Australia. *Kanal: Jurnal Ilmu Komunikasi*, *9*(2), 44–49. https://doi.org/10.21070/kanal.v9i2.1196

Mansoor, M., Ishaque, W., & Mukhtar, M. (2021). American Muslim comedians use of humour as a persuasive agent to counter Islamophobia. *Annals of Social Sciences and Perspective*, *2*(2), 361–372. https://doi.org/10.52700/assap.v2i2.129

Maryoga, Y. T., & El Fasha, I. Y. (2022). Analysis protection of the right to freedom of religion in prohibition of worship at Al Aqsa Mosque by Israeli police to Palestinians. *Contemporary Issues on Interfaith Law and Society*, *1*(1), 59–76. https://doi.org/10.15294/ciils.v1i1.56713

Mashwani, H. F., Ejaz, T., Iqbal, S., Aleem, A., Mahmood, N., & Ali, A. (2022). Strategic teachings of Islam and counter mechanism to prevent Islamophobia in contemporary scenario. *Journal of Positive School Psychology*, *6*(7), 2393–2400. https://mail.journalppw.com/index.php/jpsp/article/view/11775/7619

Mezmir, E. A. (2020). Qualitative data analysis: An overview of data reduction, data display and interpretation. *Research on Humanities and Social Sciences*, *10*(21), 15–27. https://doi.org/10.7176/rhss/10-21-02

Navarretta, C., & Hansen, D. H. (2020). Identifying parties in manifestos and parliament speeches. *Proceedings of ParlaCLARIN II Workshop*, 51–57. https://aclanthology.org/2020.parlaclarin-1.10.pdf

News, H. (2023a). *Bada'a ḥamlah al-radd 'alā austrāliyā bi ḍarb ahamm al-mawāqi' al-istrātījiyah al-austrāliyah*.

Hacker News. (2023, March 25). بدأ حملة الرد على أستراليا بضرب أهم المواقع الاستراتيجية الأسترالية [Video]. YouTube. https://youtu.be/b-2klMMOZUM?si=7bK24IK1Lwz0CsCG

News, H. (2023b). *Radd al-hākirz al-muslimīn 'alā al-ṣahāyanah ba'd al-I'tidā' 'alā al-muṣallīn dākhil al-masjid al-aqṣā al-mubārak*.Hacker News. (2023, April 6). رد الهاكرز المسلمين على الصهاينة بعد الإعتداء على المصلين داخل المسجد الأقصى المبارك [Video]. YouTube. https://youtu.be/ALAvksPfB8M?si=ien7G3vN4_XfxY9K

News, H. (2023c). *Risālah al-hākirz al-muslimīn li al-swīd ba'd ḥarq al-qur'ān al-karīm*.

Hacker News. (2023, January 9). رسالة الهاكرز المسلمين للسويد بعد حرق القرآن الكريم [Video]. YouTube. https://youtu.be/WmZqWQjfVXw?si=XzzIVRXLwtMLYM7E

Ningi, A. I. (2022). Data presentation in qualitative research: The outcomes of the pattern of ideas with the raw data. *International Journal of Qualitative Research*, *1*(3), 196–200. https://doi.org/10.47540/ijqr.v1i3.448

Poole, E., De Quincey, E., Giraud, E., & Richardson, J. (2023). Tracing media solidarities with Muslims: Contesting Islamophobia on Twitter. *AoIR Selected Papers of Internet Research*. https://doi.org/10.5210/spir.v2023i0.13480

Putra, D. I. A. (2023). Representing the belief of Muslims: Role and actions of Qatar to encounter Islamophobia during 2022 World Cup. *Journal of Islamic Thought and Civilization*, *13*(1), 14–33. https://doi.org/10.32350/jitc.131.02

Qi, Y. (2020). The language of terror: Exploring speech acts in official English-language ISIS videos, 2014-2017. *Small Wars and Insurgencies*, *31*(6), 1196–1241. https://doi.org/10.1080/09592318.2020.1775055

Reflinaldi, R., Rahman, B. A., Rahmi, A., & Rezi, M. (2023). Hacking threat in Arab cyberspace: How al-Hākirz al-Muslimūn construct narratives against Zionists and anti-Islamists. *Arabiyatuna:*

Jurnal Bahasa Arab, *7*(2 November), 457-478. https://doi.org/10.29240/jba.v7i2.8156

Reflinaldi, R., Rahmi, A., Rezi, M., & Syahidin, A. (2024). Hacking threat in Arab cyberspace: Appraisal analysis on Al-Hakirz Al-Muslimun's hacktivism narratives. *Journal of Languages and Language Teaching*, *12*(1), 353-365. https://doi.org/10.33394/jollt.v12i1.9671

Reflinaldi, R., Sawirman, S., & Usman, F. (2021). Dā'ish vs Tanẓīm Al-Dawlah: Break analysis of the names of ISIS in Arab mass media. *Jurnal Arbitrer*, *8*(2), 157-167. https://doi.org/10.25077/ar.8.2.157-167.2021

Richards, I., & Wood, M. A. (2018). Hacktivists against terrorism: A cultural criminological analysis of anonymous' anti- IS campaigns. *International Journal of Cyber Criminology*, *12*(1), 187–205. https://doi.org/10.5281/zenodo.1467895

Romagna, M., & Leukfeldt, R. E. (2023). Becoming a hacktivist. Examining the motivations and the processes that prompt an individual to engage in hacktivism. *Journal of Crime and Justice*, *47(4)*,511-529. https://doi.org/10.1080/0735648X.2023.2216189

Rubin, G. (2020). Donald Trump, Twitter, and Islamophobia: The end of dignity in presidential rhetoric about terrorism. In *Presidential Rhetoric on Terrorism under Bush, Obama and Trump*, (pp. 105–128). https://doi.org/10.1007/978-3-030-30167-5_4

Sharevski, F., & Kessell, B. (2023). Fight fire with fire: Hacktivists' take on social media misinformation. *Proceedings of the 19th Symposium on Usable Privacy and Security, SOUPS 2023*, 19–36. https://www.usenix.org/system/files/soups2023-sharevski.pdf

Shires, J. (2019). Hack-and-leak operations: Intrusion and influence in the gulf. *Journal of Cyber Policy*, *4*(2), 235–256. https://doi.org/10.1080/23738871.2019.1636108

Ślusarczyk, P. (2021). Language in the service of ideological and political struggle. Instrumentalization of the term Islamophobia. *Christianity World • Politics*, *25*, 68–91. [source not found]

Svyrydenko, D., & Mozgin, W. (2022). Hacktivism of the anonymous group as a fighting tool in the context of Russia's war against Ukraine. *Future Human Image*, *17*(January 2022), 39-46. https://doi.org/10.29202/fhi/17/6

Tabib, M. T. S. (2022). *The Rise of Neo-Fascist Populism and Islamophobia in the West*. [Master's Thesis, Portland State University]. PDXScholar. https://doi.org/10.15760/etd.7899

Tudor, M. A., & Ladjouzi, F. (2020). Information literacy practices of young internet users related to the production of religious content: 2019 Algerian protests case. *Journal of African Media Studies*, *12*(2), 97–122. https://doi.org/10.1386/jams_00014_1

Umar, M., Abbasi, R., National, S., & Languages, M. (2021). The innovative role of the Islamic world to counter the phenomenon of western "Islamophobia" during the post-corona era. *İlköğretim Online*, *20*(3), 325–340. https://doi.org/10.17051/ilkonline.2021.03.32

van Dijk, T. A. (2006). Ideology and discourse analysis. *Journal of Political Ideologies*, *11*(2), 115–140. https://doi.org/10.1080/13569310600687908

van Dijk, T. A. (2006a). Discourse, context and cognition. *Discourse Studies*, *8*(1), 159–177. https://doi.org/10.1177/1461445606059565

van Dijk, T. A. (2006b). Discourse and manipulation. *Discourse and Society*, *17*(3), 359–383.