e-Bangi Faculty of Social Sciences and Humanities Universiti Kebangsaan Malaysia
Journal of Social Sciences and Humanities

eISSN: 1823-884x

Volume 23, Issue 1, DOI: https://doi.org/10.17576/ebangi.2026.2301.08

Article

Social Media as a National Security Threat: Roles, Limits, and Opportunities for the Malaysian Armed Forces (MAF)

Amarmuazam Usmani Othman, Marina Abdul Majid & Ahmad Rizal Mohd Yusof

Faculty of Social Sciences & Humanities, Universiti Kebangsaan Malaysia, 43600, Bangi, Selangor, Malaysia

*Corresponding Author: p105897@siswa.ukm.edu.my

Received: 11 September 2025 / Accepted: 23 January 2026

Abstract: The advent of social media has transformed communication and information dissemination, posing significant risks to national security. This study examines the social media threat to Malaysia's cyber security and the role of the Malaysian Armed Forces (MAF) in maintaining national security. Disinformation involves the intentional spread of false information while misinformation refers to the unintentional dissemination of incorrect information. In Malaysia, such campaigns have been particularly influential during political events like the 2018 General Election. Social media platforms are also used by extremist groups to radicalise and recruit individuals. The MAF play a crucial role in mitigating these threats through advanced cyber defence capabilities, collaboration with government agencies, and public awareness initiatives. However, several research gaps remain, including the need for MAF to contribute to national cyber security. This study employs a qualitative method, using interviews with representatives from Malaysian ministries, agencies, and experts to analyse current cybersecurity threats and the role of the MAF in safeguarding national security. The findings underscore the importance of a proactive and collaborative approach, leveraging advanced technologies, enhancing inter-agency cooperation, and promoting public awareness to effectively mitigate social media threats. By implementing these strategies, the MAF can play a pivotal role in protecting Malaysia's national security in the digital age.

Keywords: Social media; Malaysian Armed Forces; National security; extremism; misinformation and disinformation

Introduction

The advent of social media has transformed communication, social interaction, and information dissemination on an unprecedented scale. While these platforms offer significant benefits, they also present substantial risks to national security. Baldwin (1997) defined security as a condition in which the probability of damage to important values is low, a definition applicable to national security as well as to other actors. Social media platforms have become fertile ground for cyber threats due to their widespread use and the vast amounts of personal and sensitive information shared by users. These threats can be categorised into several types, including misinformation and disinformation campaigns, and radicalisation. Disinformation refers to the deliberate spread of false information to deceive and manipulate public perception (Fallis, 2015). Misinformation involves the unintentional dissemination of incorrect information (Wardle & Derakhshan, 2017). Social media platforms are extensively exploited by extremist groups to radicalise and recruit individuals through the dissemination of radical ideologies (Arpinar et al., 2016; Conway et al., 2019). Malaysian authorities have documented multiple cases where these platforms were used to propagate extremist

views and recruit members for terrorist organisations (Ismail et al., 2022). The anonymity and broad reach of social media make it an effective tool for radicalisation, posing a direct threat to national security by fostering domestic extremism and terrorism (Awan, 2017).

Malaysia has implemented various measures to counteract social media threats, including legislative frameworks, public awareness campaigns, and cyber security initiatives (Tan, 2024). Malaysia has enacted several laws to combat cyber threats, including the Communications and Multimedia Act 1998 (CMA 1998) and the Computer Crimes Act 1997. Section 233(1)(a) of the CMA 1998 criminalises the improper use of network facilities or services, while Section 505(b) of the Penal Code (Act 574, 1936) deals with statements related to public mischief. While these laws provide a legal basis for addressing cyber threats, their enforcement has been inconsistent, and there are concerns about their adequacy in addressing the rapidly evolving nature of social media threats (Daud, 2020). Government actions to regulate and monitor social media platforms in the name of maintaining public order potentially violate individual privacy through content surveillance and personal data collection, simultaneously creating a chilling effect of self-censorship that restricts the freedom of speech, a fundamental human right guaranteed by the Federal Constitution in Article 10 (Federal Constitution of Malaysia, art 10).

The Malaysian Armed Forces (MAF) can play a pivotal role in mitigating social media threats to protect national cyber security. The threats posed by social media to Malaysia's national cyber security are complex and multifaceted. To effectively mitigate these threats, the MAF can adopt a proactive and collaborative approach, by leveraging advanced technologies, enhancing inter-agency cooperation, and promoting public awareness. This study examines the social media threat to Malaysia's cyber security and the role of the MAF in maintaining national security. This qualitative study draws on interviews with representatives from government agencies, the military, and subject matter experts. The analysis is grounded in Securitisation theory from the Copenhagen School (Buzan et al., 1998), which examines how issues are constructed as existential threats requiring exceptional responses beyond ordinary policy tools. The central research puzzle addresses the tension between pressures to militarise the information space in response to perceived social media threats and the imperative to preserve civilian privacy over information control and protect fundamental rights in democratic societies.

This study has three primary objectives. First, it seeks to analyse the nature and scope of social media threats facing Malaysia, including misinformation and disinformation campaigns as well as radicalisation efforts conducted through digital platforms. Second, the study evaluates the current role, capabilities, and limitations of the MAF in countering these threats, with particular attention to the legal frameworks governing military involvement and the dynamics of civil-military cooperation in cybersecurity matters. Third, this study aims to identify opportunities for enhancing the MAF's contribution to national cybersecurity while respecting appropriate boundaries between military and civilian responsibilities in democratic governance. Through these objectives, this study contributes to understanding how military institutions can effectively support national cybersecurity without compromising democratic principles and civil liberties.

Misinformation and Disinformation Campaigns

Misinformation and disinformation campaigns are deliberate efforts to spread false or misleading information to manipulate public opinion, create societal discord, and destabilise political systems (Allcott & Gentzkow, 2017; Wardle & Derakhshan, 2017). In Malaysia, such campaigns have been particularly influential, leveraging the vast reach of social media to amplify divisive content. During the 2018 General Election, numerous instances of fake news and manipulated information were disseminated through social media to influence voter behaviour and outcomes (Seman et al., 2019; Tapsell, 2018). These campaigns often involved fake news websites and coordinated efforts on platforms such as Facebook and WhatsApp (Johns, 2020).

Disinformation campaigns can destabilise the political landscape by eroding trust in democratic processes and institutions (Lim, 2017). The proliferation of false information erodes the public trust in the media and government institutions. When people are repeatedly exposed to conflicting information, their trust in official sources diminishes (Lazer et al., 2018). In Malaysia's multi-ethnic and multi-religious society, false

information that targets specific groups can inflame ethnic and religious sentiments, leading to conflict and violence (Nor & Gale, 2021).

Securitising Social Media Threats: Comparative Perspectives

Beyond Malaysia, a growing body of work uses Securitisation theory to analyse how governments and other actors frame social media-driven disinformation and cyber-enabled information operations as existential security threats that justify extraordinary measures. In Canada, Jackson (2024) shows how the federal government portrays Russian state disinformation—circulated through social media platforms—as a threat to both national security and democratic integrity. Using the Copenhagen School framework, she argues that Canadian officials engage in "pervasive rhetorical securitisation" by repeatedly describing foreign disinformation as an urgent danger in need of exceptional responses, while policy actions remain partial and fragmented. In Australia, Elzinga (2025) finds that media discourse frequently constructs cyber threats including data breaches, foreign cyber espionage and attacks on critical infrastructure as existential dangers to the Australian nation, economy and even "Australian families," thereby broadening the referent objects beyond the state. War-like metaphors (e.g., "cyber battlefield", "digital warfront") are used to legitimise stronger surveillance powers and platform regulation.

Wibowo et al. (2024) apply Securitisation theory to examine how the Indonesian government frames cyber threats. Their study shows that the Ministry of Defence acts as a key securitising actor, presenting cyber-attacks—often routed through social media, malware and hacking—as non-traditional security threats that can disrupt government operations and critical infrastructure. The response involves establishing a Cyber Operation Centree (COC), forming a military "cyber army" and promoting a doctrine of cyber defence that explicitly links military involvement in cyberspace to the protection of national sovereignty. This case is particularly relevant for Malaysia as it demonstrates how an armed force in a neighbouring Southeast Asian country is officially integrated into the state's cyber defence architecture. Cudjoe's (2025) comparative case study of Estonia and Iceland shows how cybersecurity technologies and advanced digital infrastructures become tools of small-state securitisation. At the broader level, Budhathoki (2025) argues that countries such as Nepal face multi-dimensional non-traditional security threats including cyber threats, emphasising the need for comprehensive strategies. Similarly, Bhandari and Gyawali (2020) underline how resource constraints and institutional fragmentation in developing countries complicate efforts to build effective cyber frameworks—challenges also relevant to Malaysia.

Radicalisation and Recruitment

Social media platforms are used by extremist groups to disseminate propaganda, create echo chambers, and engage in direct communication with potential recruits (Conway, 2017). The algorithms used by platforms such as Facebook, YouTube, and Twitter can inadvertently amplify extremist content by promoting highly engaging material, which often includes sensational or provocative content (Klausen, 2015). In Malaysia, young people are particularly vulnerable to online radicalisation. Factors such as unemployment, social alienation, and identity crises make them more susceptible to extremist messaging (Mikhael & Norman, 2018). The radicalisation and recruitment of individuals through social media have direct implications for national security. Malaysia has witnessed several cases where individuals radicalised online have engaged in or attempted to engage in terrorist activities (Hoffman, 2017). The global reach of social media allows Malaysian extremists to connect with international terrorist organisations. The multi-ethnic and multi-religious composition of Malaysian society makes it a target for extremist groups aiming to incite discord and violence (Jaafar et al., 2020).

MAF's Role in Safeguarding National Security

The MAF has developed a comprehensive strategic framework to address cyber security challenges. This framework includes the establishment of dedicated cyber units, the development of cyber defence capabilities, and collaboration with national and international partners (Sabtu & Mohamad, 2020). The MAF's cyber strategy is aligned with the Malaysia Cyber Security Strategy 2020-2024 (Malaysia Cyber Security Strategy

2020-2024, 2019). The MAF has invested in building robust cyber defence capabilities to protect the nation's cyber infrastructure, including advanced threat detection and response systems, cyber intelligence, and cyber resilience measures (Ibrahim et al., 2019). The operational role of the MAF in cyber security involves both defensive and offensive operations (Harib, Sarijan & Hussin, 2017). The MAF works closely with other government agencies, such as the Malaysian Communications and Multimedia Commission (MCMC) and the National Cyber Security Agency (NACSA), to coordinate efforts and share intelligence (Jalal et al., 2022; Rahim et al., 2024). International cooperation through the Association of Southeast Asian Nations (ASEAN) framework helps Malaysia address emerging cyber threats (Othman, 2018). While existing literature provides a comprehensive understanding, several gaps remain regarding MAF operations in countering disinformation and the effectiveness of inter-agency cooperation.

Securitisation Theory

Figure 1 below depicts how Securitisation theory is relevant to this study with regard to how cyber security in Malaysia is "securitised" as a non-traditional security issue by applying the said theory to social media driven threats and the state's responses. Securitisation theory is strongly influenced by the speech-act. This theory offers a distinctive understanding of security and power whereby: "security" is not treated as an objective condition but as the outcome of a particular social process (Williams, 2003, p. 513). Instead of assuming that threats simply exist "out there", the Copenhagen School scholars argue that security is created while speaking: security becomes a specific speech act that can succeed only under certain conditions, namely when a securitising actor uses the rhetoric of an existential threat and thereby produces significant political effects (Buzan et al., 1998, p. 25).

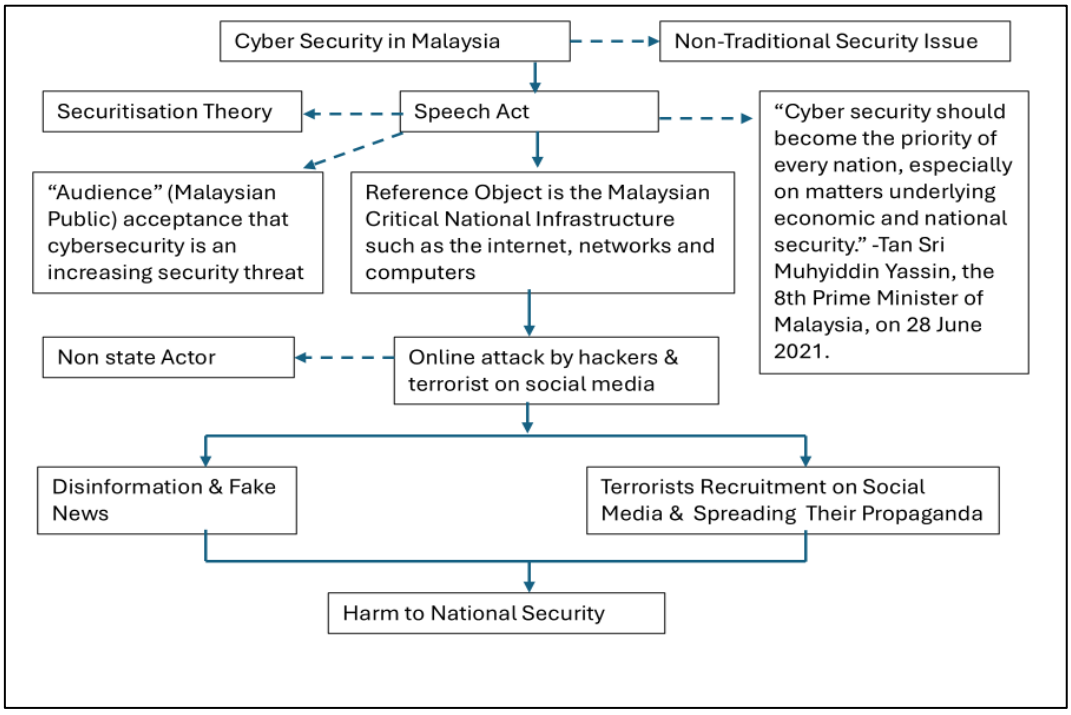

Figure 1. Elements of securitisation theory
Source: Author (2026)

In this view, securitisation is a process in which an actor declares a particular problem as dynamic or perceives an actor to be a threat to a specific referent object whereby in the Malaysian context these refer to networks and Critical National Information Infrastructure (CNII). Thus, this promotes the said phenomenon onto the security agenda (Buzan et al., 1998, p. 31; Wæver, 2004). The process of securitising a particular issue does not undergo a democratic process of governance such as obtaining parliament consent through a 2/3's majority to pass a policy but emergency measures can be justified and implemented by bypassing the

democratic process (Buzan et al., 1998, p. 24; Floyd, 2011). Emergency measures and the sense of urgency attached to a particular issue are therefore distinctive features of securitisation (Floyd, 2011, pp. 427-439).

Within this framework, cyberspace and social media can be "securitised" just like the military, economic or societal sectors. Any sector, including the cyber domain, can be securitised when an issue is presented as an existential threat that requires an exceptional action beyond ordinary policy tools (Buzan et al., 1998). The number of studies that apply Securitisation theory to cyberspace is steadily growing, reflecting the perception that threats emanating from unknown and often unknowable non-state actors such as anonymous hackers, troll farms, extremist cells have transformed how security theorists and practitioners imagine future conflict (Coker, 2009, p. ix). Since securitisation is always socially constructed, whether an issue is viewed as a security threat depends on who interprets and frames it, the social capital of the actors involved, and the broader security culture in which audiences judge those claims (Mutimer, 1997; Williams, 2003).

Methodology

This research employs a qualitative approach using purposive expert sampling in determining key individual for the interviews which include:

Table 1. Representatives from Malaysian ministries, agencies, and the industry being interviewed

No	Name	Date of Interview
1.	Officer A, Defence Cyber and Electromagnetic Division, Ministry of Defence, Kuala Lumpur.	22 June 2022, Kuala Lumpur
2.	Officer C, National Security Committee, Prime Minister Department, Putrajaya.	14 July 2022, Putrajaya
3.	Officer H, Media and Information Warfare Centre, Universiti Teknologi MARA, Shah Alam.	16 August 2022, Shah Alam
4.	Officer I, System Consultancy Services (SCS), Kuala Lumpur	24 August 2022, Kuala Lumpur
5.	Officer K, Anti-Terrorist Cell, Malaysian Defence Intelligence Organisation, Ministry of Defence, Kuala Lumpur	30 August 2023, Kuala Lumpur

Source: Author (2025)

This sample size is justified by the principle of information power (Malterud et al., 2016), whereby fewer participants are required when informants possess high levels of specialised expertise, and the study has a narrow, well-defined focus. Theoretical saturation by expertise domain was achieved, as each informant represented a distinct sector critical to understanding the MAF's role in cybersecurity. All interviews were conducted face to face. Semi-structured interviews were conducted between June 2022 and August 2023, with each interview lasting 60–90 minutes. Interviews were conducted in-person at the participants' offices to facilitate confidential discussion of sensitive security topics. Interview guide themes included: (1) perceived social media threats to national security; (2) MAF's current and potential cyber defence roles; (3) inter-agency coordination mechanisms; (4) legal and ethical boundaries; and (5) capacity-building requirements. With participants' informed consent, interviews were audio-recorded and transcribed verbatim. Interviews were conducted in Bahasa Malaysia; key quotations used in this article were translated into english by the primary researcher.

Secondary data from government policy documents, academic journals, and cybersecurity reports were systematically reviewed and triangulated with interview data. Primary data were analysed using a hybrid deductive–inductive thematic approach. Deductive codes were derived from the theoretical framework (securitisation, comprehensive security, civil–military relations), generating a priori codes such as "threat construction," "sector boundaries," and "civilian oversight." The deductive codes were derived from Securitisation theory (Buzan et al., 1998) which include threat construction, speech acts, referent objects, and emergency measures. Inductive codes emerged from close reading of transcripts, capturing themes such as "resource constraints," "inter-agency trust deficits," and "talent retention challenges." One of the inductive

codes is derived from the statement concerning resource constraints by Officer A on the limited budget allocation for cyber units. Talent retention challenges are derived from Officer A's statement on brain drain whereby government officers move to the private sector because the latter pays much better with a 40-60% salary gap. Inter-agency trust deficits are derived from Officer C's statement on institutional rivalries that impedes information sharing. The participants were chosen because of the official position they hold and importance to security. The interviews conducted had obtained the ethics clearance from the ethics committee in the National University of Malaysia (UKM).

Trustworthiness was established through multiple strategies. Credibility was enhanced through data triangulation, comparing interview accounts with policy documents (e.g., Malaysia Cyber Security Strategy 2020–2024) and publicly available threat assessments. Dependability was maintained through an audit trail documenting sampling decisions, interview protocols, coding iterations, and analytical memos. Confirmability was pursued through reflexive memo, wherein the researcher documented positionality as a Malaysian national with prior exposure to defence discourse, acknowledging potential insider bias favouring military perspectives. Transferability is supported through thick description of the Malaysian policy context, enabling readers to assess applicability to other Southeast Asian states with similar civil–military configurations.

This study has several limitations. First, the small sample (N=5) reflects the challenge of accessing elite informants in sensitive security domains; findings capture expert perspectives but may not represent the full range of institutional views. Second, elite interviews are susceptible to organisational self-presentation bias, whereby informants may emphasise successes and downplay inter-agency tensions. Third, restricted access to classified operational practices limits the study's ability to evaluate MAF cyber capabilities in depth. Fourth, the time-bounded data collection (2022–2023) captures a specific policy moment; subsequent legislative changes or organisational reforms may alter the civil–military dynamics examined here. Future research should employ mixed methods, incorporating surveys of mid-level personnel and longitudinal case studies to track policy evolution.

The Findings and Discussion

Figure 2 is the theoretical framework regarding how cyber security in Malaysia is "securitised" as a non-traditional security issue by applying the Copenhagen School Securitisation theory to social-media driven threats and the state's responses. The primary data strongly corroborates the Securitisation theory framework from the Copenhagen School (Buzan et al., 1998). Interview findings demonstrate that Malaysian officials engage in classic securitising moves, constructing social media threats as existential dangers requiring exceptional responses. Officer I (Personal communication, August 24, 2022) indicated that Malaysia has not been significantly tested by crises, making it difficult to gauge the full impact of cyber-attacks on the country. Insurgencies experienced by Malaysia have only involved small groups of people. Similarly, crises like Al-Ma'unah and Lahad Datu had limited impact. Officer A (Personal communication, June 22, 2022) stated that the effects of cyber-attacks in Estonia, Georgia, and more recently in Ukraine can serve as indicators of how Malaysia might fare if attacked through cyber means. This reference mirrors Cudjoe's (2025) comparative analysis of small-state securitisation, particularly Estonia's experience following the 2007 cyber-attacks.

The securitising move is exemplified by Prime Minister Muhyiddin Yassin's speech at the Cyber Defence and Security Exhibition and Conference 2021 (CYDES, 2021), declaring that "cyber security should become the priority of every nation, especially on matters underlying economic and national security" (Bernama, 2021). In securitisation terms, this is a classic securitising move whereby political leaders and security elites declare that cyber threats particularly those emerging from social media constitute existential dangers to the Malaysian state and society. By labelling social media-related problems (fake news, online extremism, cyber-attacks) as security issues, these actors effectively "promote" them from the realm of ordinary political debate to the realm of national security (Wæver, 2004). The declared referent object is Malaysia's CNII including internet backbones, government networks, financial systems, and defence communications whose disruption could paralyse essential services and undermine sovereignty (Ibrahim et al., 2019; Sabtu & Mohamad, 2020). Officer C's observation that "continuous cyber-attacks, especially perception attacks, will erode people's confidence in the government" (Personal communication, July 14,

2022) directly aligns with Jackson's (2024) findings from Canada, where officials similarly frame disinformation as threats to democratic integrity.

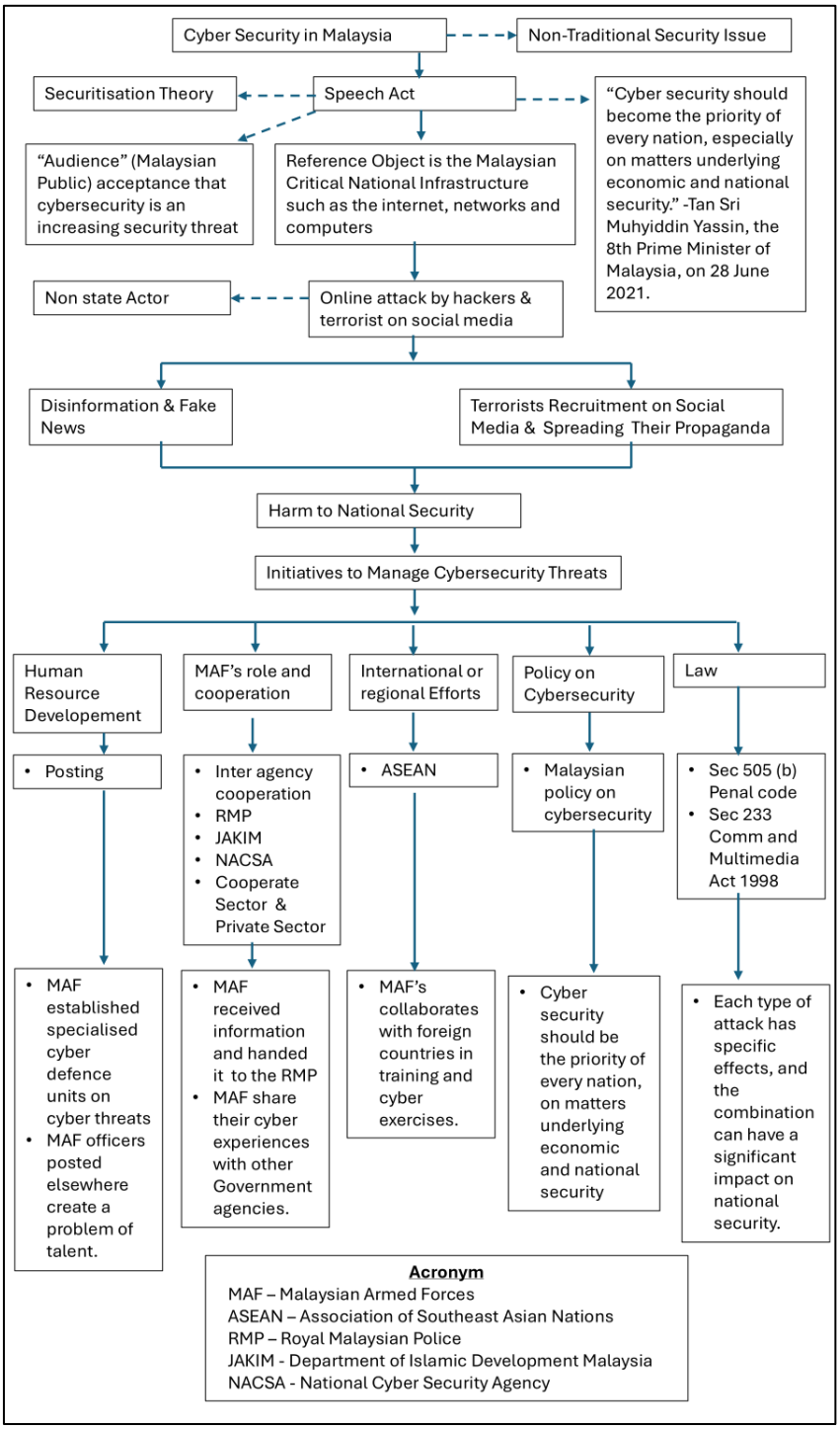

Figure 2. The framework analysis

Officer H (Personal communication, August 9, 2022) and Officer E (Personal communication, June 30, 2022) identified extremist ideology as the most significant threat. This was evident when people were exposed to extremist ideologies such as the Islamic State (IS). However, the Royal Malaysia Police (RMP), the Ministry of Home Affairs (MHA), and other agencies acted swiftly, tightening surveillance and containing this ideology. Malaysia has experienced threats from extremist groups, including the 2016 Puchong hand bomb attack orchestrated by Islamic extremists (Hassan & Ismail, 2016). This attack was undetected by the

RMP and caused public injury. Malaysians have also been detected fighting in Syria, recruited through the Internet. The identification of extremist ideology as the most significant threat strongly aligns with scholarly consensus on social media radicalisation (Arpina et al., 2016; Conway, Scrivens & Macnair, 2019). Officer E's concern that "the spread of extremist ideology can destroy this multiethnic country" directly echoes Jaafar et al. (2020) analysis of religious extremism in Malaysia's diverse society.

Officer C (Personal communication, July 14, 2022) stated that continuous cyber-attacks, especially perception attacks, will erode people's confidence in the government. Political-related attack issues will lead to public non-support for the government, undermining the unity between the people and the government. Three changes of government in one term after the Fourteenth General Election (GE14) in 2018 have made investors uncertain about investing in this country (Bernama, 2022). Officer C's assertion corroborates documentation of disinformation during the 2018 General Election (Seman et al., 2019; Tapsell, 2018). Officer H (Personal communication, August 16, 2022) observed that prolonged crises of trust will lead to changes in government, as experienced after GE14. Inflation and global economic crises cannot be accepted by the people because they have come to believe that the ruling government is incompetent. The main problem for governments worldwide today is the need to ensure continued public support, as social media is highly effective in spreading propaganda. Officer C and Officer A both highlighted how cyber-attacks targeting political institutions or social media can influence public opinion, cause societal division, and affect the democratic process echoing Vosough et al. (2018) findings on the rapid spread of false information.

Officer K (Personal communication, August 30, 2023) described how Task Force Perisai Wira, established on November 17, 2014, monitors, detects, and rehabilitates MAF members involved in extremism. This task force has been successful in identifying and rehabilitating MAF members engaged in terrorist and extremist activities. One of the major achievements of the MAF Anti-Terrorism Cell for the country was thwarting an attempted suicide bombing in Cheras in 2022. The MAF Anti-Terrorism unit received this information and handed it to the RMP. The RMP took the necessary steps and successfully foiled the suicide bombing attempt. The MAF Anti-Terrorism Cell represents MAF on the National Terrorism Control Committee, providing various inputs and suggestions to address the issues of terrorism and extremism. This exemplifies the collaborative approach advocated by Sabtu and Mohamad (2020) and the Malaysia Cyber Security Strategy 2020-2024, and demonstrates institutional parallels with Indonesia's Cyber Operation Centre (Wibowo et al., 2024), suggesting a broader regional pattern of military involvement in non-traditional security domains.

According to Officer K, MAF shares experiences in rehabilitation and deradicalisation of terrorists and extremists. Training and cooperation with external parties regarding rehabilitation and deradicalisation are shared with government agencies such as the Prison Department and the Department of Islamic Development Malaysia (JAKIM). The MAF Anti-Terrorism Cell has trained several government agencies, including JAKIM, in the field of counterterrorism and extremism. Train-the-Trainer courses have been provided to other government agencies to ensure they can confront extremists. Officer A and Officer K stated that MAF collaborates with foreign countries in training and cyber exercises, gaining expertise and knowledge to face cyber threats. MAF shares their cyber experiences with other government agencies. International cooperation operates through multilateral ASEAN frameworks: the ASEAN Defence Ministers' Meeting (ADMM) and ADMM-Plus provide formal channels for cyber confidence-building measures, including tabletop exercises simulating cross-border disinformation campaigns (Tay, 2023). The ASEAN Computer Emergency Response Team (CERT) network enables technical-level information sharing on malware signatures and threat actor tactics (Gatra, 2024). Malaysia benefits from platforms such as the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) (Kenny, 2021).

According to Officer A (Personal communication, June 22, 2022), Malaysia faces acute talent retention challenges in cybersecurity. Private-sector salaries often exceed public-sector wages by 40-60 percent, leading to brain drain from military and law enforcement cyber units. "Posting" on a rotational basis among cyber specialists to other appointments affects cybersecurity readiness due to loss of trained personnel. Inter-agency rivalries between the RMP, MCMC, and MAF can impede information-sharing, as institutional cultures and legal mandates diverge. Like any developing country, Malaysia faces challenges related to limited resources

and technical expertise, which hinder the development of effective cybersecurity frameworks (Budhathoki, 2025; Bhandari & Gyawali, 2020). It is essential for Malaysia to invest in capacity building, foster collaboration with international cybersecurity organisations, and implement comprehensive strategies that align with global best practices.

Rather than proposing wholesale restructuring, incremental confidence-building measures are recommended which include: (1) Joint Security Operations Centre (SOC) exercises conducted quarterly to harmonise incident response protocols; (2) establishment of Joint Intelligence and Operations Centres (JIOCs) with embedded liaisons from each agency for real-time coordination; and (3) temporary secondment programmes allowing MAF cyber personnel to rotate through MCMC and RMP units, as well as building interpersonal trust and mutual understanding of operational constraints. These modest steps can yield cumulative improvements in inter-agency coordination without requiring major legislative or budgetary reforms. MAF's role in international cooperation should emphasise multilateral confidence-building by participating in ADMM cyber exercises, contributing threat intelligence to ASEAN CERTs, and hosting regional workshops rather than positioning Malaysia as a unilateral actor. This approach balances sovereignty concerns with collective security benefits while reinforcing ASEAN centrality in regional security architecture.

Conclusion

Social media poses significant threats to Malaysia's national cybersecurity through the spread of misinformation, data breaches, and radicalisation. Securitisation theory provides a comprehensive framework for understanding these threats and the necessary countermeasures. The military plays a vital role in protecting cybersecurity by enhancing cyber defence capabilities, engaging in information warfare, fostering public-private partnerships, providing cybersecurity training, developing cyber policies, enhancing intelligence operations, building cyber resilience, and advocating for legislative reforms. By adopting these strategies, Malaysia can effectively mitigate the risks associated with social media and safeguard its national security.

This study makes several significant contributions to both academic scholarship and practical policy formulation. Firstly, this study makes a particularly important contribution to the area of security studies by applying Securitisation theory to the digital domain within a non-Western context, specifically applying this theory to Malaysia that faces various forms of cyberthreats. This fills a critical gap in the existing literature, which has predominantly focused on Western cases. The research demonstrates that security is not an objective condition but rather the outcome of a specific social process.

Secondly, this study can contribute to policy reform in amplifying the role that the MAF can play in integrating its cyber capabilities to protect Malaysia’s national security architecture given the success of its specialised units such as Task Force Perisai Wira and the MAF Anti-Terrorism Cell, in thwarting a planned suicide bombing in Cheras in 2022. At the implementation level to combat terrorism and deradicalisation, the involvement of Perisai Wira Task Force from the MAF should be mobilised within the Standard Operation Procedure (SOP) because of its expertise in this aspect. In conclusion, MAF plays a pivotal role in protecting the nation from social media threats. By integrating cyber intelligence, fostering public-private partnerships, and enhancing legislative frameworks, Malaysia can strengthen its national security in the digital era. Proactive and multi-dimensional approaches are essential to safeguard the nation's sovereignty, stability, and public safety in the face of evolving cyber threats.

Acknowledgement: *The authors would like to thank all the informants who have made valuable contributions to this research, as well as the reviewer for providing constructive comments in improving this article.*

Conflicts of Interest: *The authors declare no conflict of interest.*

References

Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of Economic Perspectives, 31*(2), 211-236. https://doi.org/10.1257/jep.31.2.211

Arpinar, I., Kursuncu, U., & Achilov, D. (2016). Social Media Analytics to Identify and Counter Islamist Extremism: Systematic Detection, Evaluation, and Challenging of Extremist Narratives Online. *2016 International Conference on Collaboration Technologies and Systems (CTS)*, 611-612. https://doi.org/10.1109/CTS.2016.0113

Awan, I. (2017). Cyber-extremism: Isis and the power of social media. *Society*, *54*(2), 138–149. https://doi.org/10.1007/s12115-017-0114-0

Baldwin, D. A. (1997). The concept of security. *Review of International Studies, 23*(1), 5–26. https://doi.org/10.1017/S0260210597000053

Bernama. (2021, June 28). *Cyber security complements efforts to accelerate economic growth – PM Muhyiddin*. Bernama. https://www.bernama.com/en/news.php?id=1976434

Bernama. (2022, October 10). *Three PMs in one parliamentary term, Malaysia makes its own history*. Bernama. https://www.bernama.com/en/news.php?id=2127958

Bhandari, D., & Gyawali, N. (2020). COVID-19 and Public health infrastructure in Nepal. *Health Policy and Planning*, 35(6), 686-693. https://doi.org.10.3126/unityj.v6i1.75629

Budhathoki, I. (2025). Multi-dimensional strategy for combating non-traditional security threats in Nepal. *Unity Journal*, *6*(1), 202–215. https://doi.org/10.3126/unityj.v6i1.75629

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Coker, C. (2009). *War in an age of risk*. Polity Press.

Communications and Multimedia Act 1998 (Malaysia).

Computer Crimes Act 1997 (Malaysia).

Conway, M. (2017). Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research. *Studies in Conflict & Terrorism, 40*(1), 77-98. https://doi.org/10.1080/1057610X.2016.1157408

Conway, M., Scrivens, R., & Macnair, L. (2019). *Right-wing extremists' persistent online presence: History and contemporary trends*. International Centre for Counter-Terrorism. http://www.jstor.org/stable/resrep19623

Cudjoe, D. (2025). *Cybersecurity technology as a tool for small-state securitization: A comparative case study of Estonia and Iceland* (Master's thesis). University of Iceland. https://skemman.is/bitstream/1946/49951/1/Final%20Thesis%20-%20Daniel%20Cudjoe.pdf

Daud, M. (2020). Fake News in the Malaysian 14th General Election: Shall the Net Be Free Forever? *IIUM Law Journal, 28*(S1), 587-615. https://doi.org/10.31436/IIUMLJ.V28I(S1).587

Elzinga, A. (2025). *Securitization of cyber threats: A Foucauldian discourse analysis of cyber news articles in "The Australian" between 2023 and 2024* [Master's thesis, Leiden University]. https://hdl.handle.net/1887/4210790

Fallis, D. (2015). What is disinformation? *Library Trends*, *63*(3), 401–426. https://doi.org/10.1353/lib.2015.0014

Federal Constitution (Malaysia). (1957, rev. 2010). https://www.agc.gov.my

Floyd, R. (2011). Can securitization theory be used in normative analysis? Towards a just securitization theory. *Security Dialogue, 42*(4–5), 427–439. https://doi.org/10.1177/0967010611418712

Gatra, S. (2024). ASEAN's Cyber Initiatives: A Select List. *Centre for Strategic and International Studies (CSIS)*. https://www.csis.org/blogs/strategic-technologies-blog/aseans-cyber-initiatives-select-list

Harib, A., Sarijan, S., & Hussin, N. (2017). Information Security Challenges: A Malaysian Context. *International Journal of Academic Research in Business and Social Sciences, 7*(9), 397-403. https://doi.org/10.6007/IJARBSS/V7-I9/3335

Hassan, A., & Ismail, B. (2016, July 1). Puchong bar blast linked to ISIS. *New Straits Times Online*. https://www.nst.com.my/news/crime-courts/puchong-bar-blast-linked-isis

Hoffman, B. (2017). *Inside terrorism* (3rd ed.). Columbia University Press.

Ibrahim, A., Mahmud, N., Isnin, N., Hazelbella Dillah, D., & Nurfauziah Fauz Dillah, D. (2019). Cyber warfare impact to national security - Malaysia experiences. *KnE Social Sciences, 3*(22), 206–224. https://doi.org/10.18502/kss.v3i22.5052

Ismail, N., Jawhar, J., Yusof, D., Ismail, A., & Akhtar, R. (2022). Understanding Malaysian youth's social media practices and their attitude towards violent extremism. *Intellectual Discourse, 30*(1), 187-213. https://doi.org/10.31436/id.v30i1.1855

Jaafar, M., Akhmetova, E., & Aminudin, R. (2020). The factors contributing to the rise of religious extremism in Malaysia. *Jurnal Islam dan Masyarakat Kontemporari, 21*(2), 16-27. https://doi.org/10.37231/JIMK.2020.21.2.482

Jackson, N. J. (2024). The securitisation of foreign disinformation. *Security and Defence Quarterly, 46*(2), 118–138. https://doi.org/10.35467/sdq/190799

Jalal, B., Suparman, M., Basiron, M., & Jamsari, E. (2022). OP BENTENG: Media planning by the National Task Force of Malaysia in creating people awareness in eradicating crime. *International Journal of Advanced Research, 10*(10), 809-816. https://doi.org/10.21474/ijar01/15571

Johns, A. (2020). 'This will be the WhatsApp election': Crypto-publics and digital citizenship in Malaysia's GE14 election. *First Monday, 25*(12). https://doi.org/10.5210/fm.v25i12.10381

Kenny, C. (2021, October 5). ASEAN-S'pore centre for training national cyber-security teams opens new campus. *The Straits Times*. https://www.straitstimes.com/tech/tech-news/asean-spore-centre-for-training-national-cyber-security-teams-opens-new-campus

Klausen, J. (2015). Tweeting the Jihad: Social media networks of Western foreign fighters in Syria and Iraq. *Studies in Conflict & Terrorism*, *38*(1), 1–22. https://doi.org/10.1080/1057610X.2014.974948

Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., Metzger, M. J., Nyhan, B., Pennycook, G., Rothschild, D., Schudson, M., Sloman, S. A., Sunstein, C. R., Thorson, E. A., Watts, D. J., & Zittrain, J. L. (2018). The science of fake news. *Science, 359*(6380), 1094-1096. https://doi.org/10.1126/science.aao2998

Lim, M. (2017). Freedom to hate: Social media, algorithmic enclaves, and the rise of tribal nationalism in Indonesia. *Critical Asian Studies, 49*(3), 411-427. https://doi.org/10.1080/14672715.2017.1341188

Malaysia Cyber Security Strategy 2020-2024. (2019). Government of Malaysia.

Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample size in qualitative interview studies: Guided by information power. *Qualitative Health Research, 26*(13), 1753-1760. https://doi.org/10.1177/1049732316665344

Mikhael, D., & Norman, J. (2018). Refugee youth, unemployment and extremism: Countering the myth. *Forced Migration Review, 57*, 57–58. https://www.fmreview.org/syria2018/mikhael-norman

Mutimer, D. (1997). Reimagining security: The metaphors of proliferation. In K. Krause & M. C. Williams (Eds.), *Critical security studies: Concepts and cases* (pp. 187–213). UCL Press.

Nor, M., & Gale, P. (2021). Growing fear of Islamisation: Representation of online media in Malaysia. *Journal of Muslim Minority Affairs, 41*(1), 17-33. https://doi.org/10.1080/13602004.2021.1903161

Othman, Z. (2018). Jaringan komunikasi dan media: Satu analisis dari perspektif keselamatan insan. *Jurnal Komunikasi: Malaysian Journal of Communication, 34*(3). https://doi.org/10.17576/JKMJC

Penal Code (Malaysia). https://www.agc.gov.my

Rahim, S. S. I., Mohd Huda, M. I., Sa'ad, S., & Moorthy, R. (2024). Cyber security crisis/threat: Analysis of Malaysia National Security Council (NSC) involvement through the perceptions of government, private and people based on the 3P Model. *e-Bangi: Journal of Social Sciences and Humanities, 21*(2), 191-201. http://ejournal.ukm.my/ebangi

Sabtu, S., & Mohamad, K. (2020). Critical information infrastructure protection framework development: Preliminary findings from the Malaysian public sector. *2020 8th International Conference on Information Technology and Multimedia (ICIMU)*, 1-6. https://doi.org/10.1109/ICIMU49871.2020.9263397

Seman, R., Laidey, N., & Ali, R. (2019). Netizens' political engagement in Malaysia: Impact of Anti Fake News Act 2018. *Jurnal Pengajian Media Malaysia, 21*(1), 103-116. https://doi.org/10.22452/jpmm.vol21no1.6

Tan, J. J. (2024). Social media political information use and political participation of the next generation. *e-Bangi: Journal of Social Sciences and Humanities, 21*(1), 198-211. https://doi.org/10.17576/ebangi.2024.2101.17

Tapsell, R. (2018). The smartphone as the 'weapon of the weak': Assessing the role of communication technologies in Malaysia's regime change. *Journal of Current Southeast Asian Affairs, 37*(3), 9-29. https://doi.org/10.1177/186810341803700302

Tay, K. L. (2023). *ASEAN cyber-security cooperation: Towards a regional emergency-response framework.* The International Institute for Strategic Studies.

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science, 359*(6380), 1146–1151. https://doi.org/10.1126/science.aap9559

Wæver, O. (2004). Discursive approaches. In A. Wiener & T. Diez (Eds.), *European integration theory* (pp. 197–215). Oxford University Press.

Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy making* (Report No. DGI(2017)09). Council of Europe.

Wibowo, S. E., Hartono, A., Kiswanto, H., Primawanti, H., Louerens, J. T. A., & Torang, J. (2024). Securitization of cyber threats to the Indonesian government: A study of cyber defense strategy. *Global Political Studies Journal, 8*(2), 97–108. https://doi.org/10.34010/gpsjournal.v8i2.13817

Williams, M. C. (2003). Words, images, enemies: Securitization and international politics. *International Studies Quarterly, 47*(4), 511–531. https://doi.org/10.1111/j.0020-8833.2003.00277