Online at www.e-iph.co.uk

Indexed in Clarivate Analytics WoS, and ScienceOPEN

E-B Environment - Behaviour Proceedings Journal

KICSS2024

Kedah International Conference on Social Sciences:

https://kicss2024.wixsite.com/kicss2024

e-IPH e-International Publishing House Ltd., United Kingdom

iCSSP2024: International Conference on Social Science & Public Policy

Virtual Conference, 23 & 24 October 2024

Organised by: Universiti Teknologi MARA, Kedah, Malaysia

Cybertrooper Politics in Malaysia: Definitions, threats, and control mechanisms

Norhafiza Mohd Hed*, Rahimah Wahid, Nafisah Ilham Hussin, Sakinah Salleh

**Corresponding author*

Faculty of Human Sciences,
Universiti Pendidikan Sultan Idris, 35900 Tanjung Malim, Perak

norhafiza@fsk.upsi.edu.my, rahimah.wahid@fsk.upsi.edu.my, sakinah.salleh@fsk.upsi.edu.my, nafisah@fsk.upsi.edu.my
Tel: +6012-3582021

Abstract

This study explores the definitions, threats, and mechanisms for controlling cybertrooper movements in Malaysia, focusing on their impacts on national security. Using a qualitative approach through semi-structured interviews with 10 informants, the findings show that cybertroopers act as intermediaries contracted to shape public opinion on social media platforms. While cybertrooper movements pose a moderate threat to political stability, they do not significantly risk national security. Effective control mechanisms identified include cyber surveillance, filtering, and cybersecurity education. These findings aim to assist the government in formulating a practical guideline for regulating and managing cybertrooper activities in Malaysia.

Keywords: cybertroopers; politics; Malaysia; movement.

DOI: https://doi.org/10.21834/e-bpj.v10iSI30.6890

1.0 Introduction

The widespread use of cyber media has contributed to the growth and evolution of cybertrooper movements in Malaysia. Although research on cybertroopers is expanding, most studies focus primarily on the roles and platforms used by political cybertroopers to carry out their activities (Hopkins, 2014; Tapsell, 2013; Mastura, Siti Zobidah & Krauss, 2020). While some scholars have attempted to define cybertroopers in the Malaysian context, these definitions remain limited in scope. For example, Hopkins (2014) defines cybertroopers as bloggers, tweeters, or users who comment on and respond to online posts, whereas Tapsell (2013) describes them as individuals hired by political actors, whether from the government or opposition, to defame opponents through social media campaigns. However, these definitions often lack empirical grounding, causing the term 'cybertroopers' to be misused or conflated with netizens, keyboard warriors, or general social media critics. Several scholars have raised concerns about the potentially harmful influence of cybertroopers, particularly concerning national security. For instance, the dissemination of false or inflammatory information by cybertroopers during politically sensitive periods, such as elections, may disrupt social cohesion and incite public unrest (Mohd Azlim, 2019, November 11). In response, the government has introduced various legal measures to mitigate such risks, including the Anti-Fake News Act 2018, the Communications and Multimedia Act (CMA) 1998, Section 233 (1), the Sedition Act 1948, the Official Secrets Act 1972, and the Security Offenses (Special Measures) Act 2012, or SOSMA. Despite these efforts, enforcement appears insufficient in curbing the rising influence of cybertroopers, as their numbers continue to grow (Leong, 2015). This study argues that Malaysia's current legal and social frameworks

eISSN: 2398-4287 © 2025. The Authors. Published for AMER by e-International Publishing House, Ltd., UK. This is an open access article under the CC BY-NC-ND license (http://c5eativecommons.org/licenses/by-nc-nd/4.0/). Peer–review under responsibility of AMER (Association of Malaysian Environment-Behaviour Researchers
DOI: https://doi.org/10.21834/e-bpj.v10iSI30.6890

are inadequate to address the evolving threat of cybertrooper activities. Therefore, based on qualitative interviews, it provides empirical insights into their definition, perceived threats, and current control efforts, aiming to develop a guideline for the government to manage cybertroopers' movements and enhance public awareness.

2.0 Literature Review

The study of cybertroopers in Malaysia has evolved alongside the country's dynamic digital political landscape. Early research primarily focused on their roles during the election periods, highlighting their influence on political discourse and public opinions. Johns and Cheong (2019) examine the BERSIH movement between 2011 and 2016, noting the involvement of cybertroopers in disseminating political propaganda to create public uncertainty. Similarly, Tiung, Rizal Zamani, and Rafiq (2019) discuss the emergence of cybertroopers in the late 1990s as alternative channels for political communication, emphasizing their role in spreading fake news during the 2018 general election.

Recent studies have expanded the scope by analyzing the tactics employed by cybertroopers and their impact on Malaysia's digital public sphere. For example, Leong and Loh (2024) identify two main strategies for cybertroopers' activities, which are: launching attacks and counter-narratives against the opposition; and projecting strong public support for the government. As such, the digital warfare among political alliances has fueled national instability and heightened tensions, particularly through the exploitation of racial and religious sentiments. Tapsell (2023), on the other hand, finds that the professionalization of social media campaigning in Malaysia's 2022 General Election (GE15) highlights the use of live streaming and video content by cybertroopers to incite and polarize public opinion. This study emphasizes that while new platforms like TikTok have emerged as influential conduits for campaign messages, they have also become arenas for disinformation and hate speech. Similarly, Munira (2024) highlights how political parties deployed cybertroopers during GE15 to disseminate disinformation, discredit opponents, and shape public opinion online. She describes cybertroopers, or "cytros," as organized groups of trolls (whether paid or volunteer) who are strategically mobilized to influence political narratives through the use of conspiracy theories and hate speech. Such tactics, however, pose a significant threat to democratic processes. Additionally, Nurul and Norhafiza (2023) define cybertroopers as paid intermediaries who serve as agents between political leaders and the public, spreading content on social media to shape public opinion. Their study outlines several key typologies of cybertroopers, including systematically organized groups that use fake accounts to hide their identities, accept financial compensation, and manipulate online news content. However, their research does not specifically examine the threats posed by cybertrooper activities or the mechanisms used to control them.

Previous studies have offered a preliminary understanding of cybertroopers, contributing to a general conceptual foundation for researchers. However, there remains a lack of empirical research that comprehensively examines their definition, associated threats, and control mechanisms within the Malaysian context—gaps that this study seeks to address.

3.0 Methodology

This study employs a qualitative research design, utilizing in-depth interviews as the primary methodological approach. In-depth interview research was chosen as it allows for an in-depth examination of cybertrooper politics in Malaysia, an analysis of the definition, threat, and the formulation of control mechanisms for the Malaysian government. Given the multifaceted nature of the issue, 10 key informants, including politicians, academicians, cybertroopers, and political activists, were purposively selected and interviewed. Semi-structured interviews were conducted face-to-face and online, lasting between 45 to 90 minutes. The semi-structured interviews included predetermined questions on various topics developed by the researcher. While prepared questions were used, each interview allowed for flexibility to incorporate new questions arising from the interviewee's responses (Flick, 2007). All interviews were recorded with permission and transcribed for analysis. Thematic analysis was then applied to identify key patterns and themes related to the definition, threats, and control of cybertrooper activities in Malaysia.

4.0 Findings

4.1 Definition of the Cybertrooper Politics

The term "cybertroopers" is said to have originated in Malaysia, referring to cyber soldiers who are paid to spread political propaganda online (Nurul & Norhafiza, 2023). However, according to Bradshaw & Howard (2017), this term has long been used in other countries and encompasses a broader concept, including political bots and political sock puppets. Therefore, based on the framework of political astroturfing, this study will define the term "political cybertroopers" through empirical evidence from interviews. The interview findings revealed that the majority (8 out of 10) of informants agreed that the term "political cybertroopers" can be defined as individuals or groups paid by political actors to disseminate information and spread political propaganda. According to Informant 2,

> "Cybertroopers refer to activists who are paid to spread propaganda, ideology, or beliefs on the internet, particularly on social media. Cybertroopers are created to spread propaganda, such as disseminating information for marketing purposes. There are also cybertroopers created for specific reasons. They are paid and use fake accounts as well as pure accounts." (Informant 2)

Based on the definition above, three main elements can be summarized regarding cybertroopers: paid activists, spreading propaganda, and existing for a specific purpose or agenda. Additionally, some view cybertroopers as a planned and organized movement that creates its narrative to raise public awareness about the political scenario in Malaysia, as argued by Informant 5,

> "Troopers are like an army. To use that definition, what is a Trooper and an army? You must first understand the structure; they have commands, and they have discipline. So, to qualify someone as a cybertrooper, they must meet the criteria of a real army. So, what other criteria do armies have? You must have a group, you must have leaders, structure, discipline, self-soldiers, and a clear line of command. For cybertroopers, they must also have these; they must have troopers, and they must have soldiers. Since they operate in cyberspace, once they have 10 accounts, they have 10 cyberspace soldiers, and the instructions given will reach them, and they will execute them as any army would. Cybertroopers have one purpose: to attack others or to defend themselves, so I think this fits the definition of cybertroopers." (Informant 5)

According to Informant 5, cybertroopers are an organized movement similar to a military formation, where they have a leader who provides clear instructions. Moreover, Informant 1 emphasized that cybertroopers are propaganda agents who create political narratives to attract public attention. At the same time, they also manipulate issues to make them viral or gain high popularity. This argument aligns with the view of Informant 6, who stated:

> "Cybertroopers are people paid to attack a particular issue. Cybertroopers are a group from a paid organization given a specific goal, method, and modus operandi to attack a particular issue. Cybertroopers have a narrative and goal to divert people's attention." (Informant 6)

Based on Informant 6's views, it can be understood that political cybertroopers have a pre-planned modus operandi, either to build a narrative or to emphasize an issue to influence public thinking. However, according to Informant 7, "Cybertroopers are political cyber soldiers formed to damage or tarnish the image of certain parties or leaders with the intent to bring them down."

From the definitions provided by the informants above, several key elements related to cybertroopers in Malaysia are emphasized. First, cybertroopers are activists, movements, or agents, whether individuals or groups, paid by political actors using fake accounts and identities. These cybertroopers are organized, systematic, and have a structured modus operandi with specific objectives. These objectives can manifest in two forms: positive goals, such as sharing information or building narratives to raise public awareness and attention towards current political issues and scenarios occurring domestically and abroad. However, on the other hand, cybertroopers tend to have negative goals, such as spreading propaganda, provoking issues, and sharing false information to bring down specific individuals or parties. Furthermore, cybertroopers can also threaten national security when they start playing on racial sentiments or discussing sensitive issues that can disrupt societal harmony.

4.2 Threats of Political Cybertroopers to National Security

Findings from interviews show that the majority of informants found that cybertrooper movements pose a threat to the country if not properly controlled. Six out of 10 informants agreed that these movements indeed pose a threat to national security. Among the groups supporting this view were academics, politicians, and policymakers from the Malaysian Communications and Multimedia Commission (MCMC). According to Informant 1, cybertroopers can threaten national security because the statements they issue on social media can confuse the public and cause unrest. Specifically, they concluded, “Yes, of course, they threaten national security because, as I mentioned earlier, they are created to find faults, bring down opponents, and make statements that can cause chaos in the country.” This argument is supported by Informant 3, who stated:

> “Yes, because if we don’t curb them, if we allow them and don’t provide our citizens with the necessary awareness, education, or exposure, their lack of understanding about this information will destroy them. Things that don’t exist are said to exist, and things that exist are misrepresented. They don’t speak based on facts or a system or structure; instead, they follow whoever pays them.”

Informant 3's statement indicates that the lack of strict government control could lead to the collapse of the country's political system and institutional structure. Additionally, the absence of proper education and awareness among the public would tarnish digital information and reduce public trust in political institutions. This is because most online messages spread by cybertroopers involve propaganda, either pro-government or pro-opposition.

Moreover, the interview results show that the emergence of cybertroopers can pose a serious threat to national security. According to Informant 4, the issues touched upon by cybertroopers are not limited to sensitive topics like ethnicity and religion but also include current issues related to the present situation, which become their messaging agenda on social media.

“Yes, all of this threatens our national security. Issues related to race and religion are often used as political capital, but when you talk about religion or race, people no longer care because these are common issues played by politicians. But current stories, like issues about citizen assistance or vaccines, are hot topics right now that draw their attention. Their statements about these issues can cause chaos; just because someone is anti-vaccine, they want to make all anti-vaxxers follow them.” (Informant 4).

In conclusion, the interviews from the first group indicate that the presence of cybertroopers in the country can threaten national security. Although it may not be considered a serious threat, given Malaysia’s background as a multi-ethnic and multi-religious country, it can disrupt public order. Among the threats mentioned by the informants is the spread of inaccurate or slanderous news, which could cause chaos in the country. Additionally, issues touching on ethnic sensitivities are often provoked by cybertroopers, potentially leading

to racial divisions in Malaysia. There is concern that prolonged racial provocation could reignite events like those of May 13. Furthermore, the most dangerous situation could occur if cybertroopers leak state secrets to outsiders and expose them to enemies, because these individuals will do anything as long as they are paid to do so. Therefore, cybertroopers must adhere to certain ethics or regulations to ensure that their agenda does not deviate from its primary purpose.

4.3 Mechanisms to Control the Cybertrooper Politics

Many mechanisms can be used to control cybertrooper politics. First, the government must ensure that the public uses mass media wisely and ethically, and, most importantly, knows how to differentiate whether the news presented on social media is true or not. According to Informant 1, the government needs to review existing laws and regulations. He stated, "From the enforcement perspective, from the government officials' perspective, what they need to do is tighten the existing laws, review the current laws such as the Communications Act, and the Defamation Act, and further strengthen those laws."

The laws in place today are good, but their enforcement remains weak, as the spread of fake news and misinformation is still rampant and increasingly critical, affecting political institutions. Therefore, these laws need to be empowered and further strengthened to prevent the spread of false news on social media. Additionally, Informant 2 mentioned that "...the importance of awareness advocacy programs, especially social media advocacy, is highly needed in this country." Awareness campaigns are crucial to educating the public about the misuse of social media, the exposure of personal information and data on social media, and misconduct on social media. In developed countries, advocacy and awareness campaigns are numerous and frequently conducted.

Additionally, the majority of informants (7 out of 10) agreed that cybersecurity education is crucial for all segments of society. This was expressed by Informants 7 and 9, who said, "Another step, in my opinion, is cyber education. Educate the public from a young age. Don't just talk about this and that. Everyone needs to work together in educating society. Start educating them from a young age." Informant 7 also echoed this sentiment, stating, "The aspect of education is important and needs to be introduced early to children, especially the younger generation, about ethics, manners, and proper language when using digital technology." Therefore, Malaysia should take proactive steps, in line with developed countries, to introduce formal and informal cybersecurity education at every level of the education system. Higher education institutions are also encouraged to offer undergraduate and postgraduate programs in cybersecurity.

5.0 Discussion

Based on informant input, this study defines cybertroopers as individuals or groups, referred to as a movement or agents, paid by political actors to use fake accounts and identities to disseminate information, spread propaganda, construct narratives, or provoke controversy to discredit specific individuals or political parties. While the presence of cybertroopers in Malaysia is not new, this study aligns their definition with the concept of political astroturfing as discussed by Kovic et al. (2018), Schoch et al. (2022), and Walker (2014). This alignment is based on five core elements: (1) the use of online platforms; (2) funding by political actors; (3) manipulation of public opinion through fabricated or deceptive content; (4) the use of multiple, false identities; and (5) a top-down structure driven by political interests.

Interview findings reveal that most informants perceive cybertroopers as a moderate threat, particularly in destabilizing political alliances and public trust through the strategic use of divisive issues. However, if left unregulated, especially when exploiting race, religion, and royalty (3R) issues, the movement could escalate into a serious threat to national unity and even invite foreign interference. Informants widely agreed that cyber surveillance and content filtering, enforced under existing laws, are necessary to curb the potential threats posed by cybertroopers. These mechanisms are particularly important in today's digital age, where cyberspace is a primary source of political information, especially for youth. Effective regulation of cyber activities is therefore essential to prevent misuse and promote societal harmony.

However, some informants, particularly cybertroopers and political activists, pointed out challenges in enforcing these controls. Because cybertroopers are often backed by political actors with vested interests, enforcement of laws may be biased or inconsistent. Additionally, the use of fake identities makes it difficult for authorities to track and regulate these individuals effectively. From a governmental standpoint, direct surveillance and filtering are seen as potential infringements on human rights. Nonetheless, the Malaysian Communications and Multimedia Commission (MCMC) continues to address offenses under current laws and collaborates with law enforcement to identify individuals spreading harmful content. In conclusion, while cyber surveillance and filtering are effective tools to control political cybertrooper activity, their enforcement must be transparent and impartial. Furthermore, public education in digital ethics and cybersecurity is essential. A coordinated effort among government agencies, NGOs, and educational institutions is needed to foster greater digital literacy and responsible online behavior through awareness campaigns and formal or informal educational initiatives.

6.0 Conclusion and Recommendation

Overall, the findings conclude that the lack of a clear definition of cybertroopers has led to this movement being consistently viewed negatively, with the public often assuming that cybertroopers are the same as keyboard warriors and netizens. Through this study, the concept of cybertroopers has been detailed, including their typologies and the objectives of their formation. Therefore, the government and non-governmental organizations must play a crucial role in providing cybersecurity education to the public so that they better understand the clear definition and importance of cybertroopers. The failure to provide in-depth knowledge about cybertrooper

movements can threaten national security through the spread of false information that could disrupt societal sensitivities. The implications of this study suggest that the lack of formal and informal education regarding cybertroopers makes youth more susceptible to being influenced by false information, political campaigns, and provocations spread by cybertroopers, which could, in turn, destabilize the political landscape. While this study provides valuable insights into cyber trooper politics in Malaysia, a limitation must be acknowledged: the reliance on one method of data collection may have constrained the depth of analysis and been subject to informants' bias. To address the limitations identified in this study, future research could adopt a mixed-methods approach, combining document analysis with primary data collection methods such as surveys or interviews. This would allow for a more comprehensive understanding of the cybertroopers' politics in Malaysia. Building on the findings of this study, future research could explore additional dimensions of the cybertrooper's politics in Malaysia, such as its effectiveness, weaknesses, and comparative studies across different geographical contexts and socio-economic settings.

Acknowledgments

This article is part of research funded by the Ministry of Higher Education Malaysia (MOHE) through the Fundamental Research Grant Scheme FRGS/1/2020/ SS0/UPSI/02/07 (Code: 2020-0226-106-102) and supported by the Sultan Idris Education University Malaysia, to whom we are grateful.

Paper Contribution to Related Field of Study

The study significantly advances the understanding of cybertrooper activities in Malaysia, offering valuable insights for scholars, policymakers, and practitioners in political communication, cybersecurity, and public policy.

References

Bradshaw, S.,& Howard, P. (2017). *Troops, Trolls, and Troublemakers: A global Inventory of Organised Social Media Manipulation.* Oxon: University of Oxford Press.

Flick, U. (2007). *Designing Qualitative Research*. New York: Sage Publications Ltd.

Hopkins, J. (2014). Cybertroopers and Tea Parties: Government Use of the Internet in Malaysia. *Asian Journal of Communication, 24* (1), 5-24. https://doi.org/10.1080/01292986.2013.851721.

Johns. A & Cheong. N. (2019). *Feeling the Chill: Bersih 2.0, State Censorship, and "Networked Affect" on Malaysian Social Media 2012–2018. Social media +Society*, *5*(2). https://doi.org/10.1177/2056305118821801

Kovic, M., Rauchfleisch, A., Sele, M., & Caspar, C. (2018). Digital Astroturfing in Politics: Definition, Typology and Countermeasures. *Studies in Communication Sciences, 18* (1), 69-85. https://doi.org/10.24434/j.scoms.2018.01.005

Lee, C. A. L., & Kerr, E. (2020). Trolls at the Polls: What Cyberharassment, Online Political Activism, and Baiting Algorithms Can Show Us About the Rise and Fall of Pakatan Harapan. *First Monday, 25*(6). https://doi.org/10.5210/fm.v25i6.10704.

Leong, P. (2015). Political Communication in Malaysia: A Study on the Use of New Media in Politics. *Journal of eDemocracy, 7*(1), 46-71. https://doi.org/10.29379/jedem.v7i1.372

Leong, P.P. Y., & Loh, B. Y. H. (2024). State-sponsored Disinformation through Digital Media in Malaysia. In Echeverria, M., Santamaria, S. G., & Hallin, D. C. *State-Sponsored Disinformation Around the Globe: How Politicians Deceive their Citizens.* New York: Routledge.

Mastura, M., Siti Zobidah, O., & Krauss, S.E. (2020). Is Citizen Journalism to Keyboard Warriors and Cybertroopers? An Exploration and Meaning from Citizen Journalist Experience*. International Journal of Academic Research in Business and Social Sciences*, 10(6), 813–830. https://doi.org/10.6007/IJARBSS/v10-i6/7376

Mohd Azlim, Z. (2019, November 11). Perselisihan kaum, agama, Ahli politik dan media sosial jadi punca. *Sinar Harian.* https://www.google.com.my/amp/s/www.sinarharian.com.my/ampArticle/56621.

Munira, M. (2024). *When opposition is extremism: The dangers of oversecuritisation and online vigilantism*. International Centre for Counter-Terrorism.

Nurul, I., & Norhafiza, M. H. (2023). Definisi dan Tipologi Istilah Politik Laskar Siber di Malaysia. *Jurnal Komunikasi; Malaysian Journal of Communication*, 39(3), 81-100.

Schoch, D., Keller, F.B., Stier, S.,& Yang, J. (2022). Coordination Patterns Reveal Online Political Astroturfing across the World. *Scientific Report*s, 12, 4572. https://doi.org/10.1038/s41598-022-08404-9.

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

Tapsell, R. (2023). Social Media and Malaysia's 2022 Election: The Growth and Impact of Video Campaigning. *Pacific Affairs,* 96(2), 303-322. https://doi.org/10.5509/2023962303

Tiung, L.K., Rizal Zamani, I., & Rafiq, I. (2019). Propaganda dan disinformasi: Politik persepsi dalam Pilihan Raya Umum ke-14 (PRU14) Malaysia. *Jurnal Kinabalu Edisi Khas*, 171-198. https://doi.org/10.51200/ejk.vi.1648

Walker, E. T. (2014). *Grassroots for hire: Public affairs consultants in American democracy*. Cambridge: Cambridge University Press.