When Opposition is Extremism

The Dangers of Oversecuritisation and Online Vigilantism

Munira Mustaffa

International Centre for Counter-Terrorism

When Opposition is Extremism

The Dangers of Oversecuritisation and Online Vigilantism

Munira Mustaffa

ICCT Policy Brief
February 2024

International Centre for Counter-Terrorism

About ICCT

The International Centre for Counter-Terrorism (ICCT) is an independent think and do tank providing multidisciplinary policy advice and practical, solution-oriented implementation support on prevention and the rule of law, two vital pillars of effective counter-terrorism.

ICCT's work focuses on themes at the intersection of countering violent extremism and criminal justice sector responses, as well as human rights-related aspects of counter-terrorism. The major project areas concern countering violent extremism, rule of law, foreign fighters, country and regional analysis, rehabilitation, civil society engagement and victims' voices.

Functioning as a nucleus within the international counter-terrorism network, ICCT connects experts, policymakers, civil society actors and practitioners from different fields by providing a platform for productive collaboration, practical analysis, and exchange of experiences and expertise, with the ultimate aim of identifying innovative and comprehensive approaches to preventing and countering terrorism.

Licensing and Distribution

ICCT Policy Brief
February 2024
DOI: 10.19165/2024.3834
ISSN: 2468-0486

Contents

Abstract

The policy brief makes the case that policymakers and practitioners need to consider who the state defines as 'extremists.' In the West, terrorism and violent extremism are seen as the most radical expressions of anti-government resistance. Things, however, look different in the Global South where some governments effectively foster extremists of their own while targeting legitimate and often nonviolent opposition. Echoes of such an approach are also present in Europe where certain (semi-) authoritarian governments securitise their responses to political dissent while seemingly drawing inspiration from more autocratic regimes outside this continent. Thus, in their case, an attempt to counter real or imagined extremism could consequently and likewise lead them to foster extremists of their own.

This policy brief will focus on the case of Malaysia, where cyber troopers, or cytros, i.e., groups of coordinated trolling individuals (either paid or voluntary), are deployed for political messaging or conduct online malign influence operations to manipulate and manage the public opinion on domestic political issues. The red-ragging tactic brands individuals or groups as communists or terrorists to justify coercive actions against them or creates some green scares that could focus on individuals who allegedly belong to the Islamist extremist milieu. Ironically, these strategies, which seem to target extremists, nurture a peculiar brand of pro-government extremism themselves. Using Malaysia as a case study, this policy brief hopes to demonstrate how the ethnonationalist political actors and their agents use polarising hate speech, the weaponisation of conspiracy theories, and religious supremacy as a criterion for belonging to manage democratic constituents by exploiting existing sociopolitical divisions.

Keywords: extremism, vigilantism, digilantism, sedition, incitement, surveillant assemblage, networked authoritarianism

Introduction

Following Russia's interference activities in the 2016 US presidential election (when Russia intervened to support Donald J. Trump's campaign and seriously undermined that of Hillary Clinton), along with COVID-19 conspiracy theories that flourished during the pandemic, disinformation and influence operations were identified as an emerging challenge by various individuals and entities, including government agencies such as the Special Counsel's Office[1], journalists and the researchers.[2] However, due to the US experience, malign influence operations are often viewed as a foreign interference issue, while they can be utilised by political party actors to influence their own democratic constituents. This policy brief focuses on the malign influence operations, specifically disinformation.

Misinformation and disinformation are often used interchangeably and conflated with each other but it is crucial to delineate their differences, especially when considering intent. Misinformation is generally understood as the unintentional sharing of falsehoods. In contrast, disinformation is the deliberate spread of falsehoods with the aim of deceiving the audience or consumers of information for political or financial goals.[3] Disinformation is a powerful communication strategy with the potential to significantly impact a target population by influencing their opinion and decision-making. When orchestrated effectively by a network of organised actors, whether state-sponsored or non-state individuals or entities, disinformation campaigns have the capacity to manipulate the political sentiments of the target audience, ultimately serving strategic and geopolitical objectives. In this context, disinformation functions as a tool of influence, allowing its orchestrators to shape narratives, sow confusion, and achieve specific outcomes that subvert democracy. The proliferation of social media has facilitated the diffusion of disinformation and those who manufacture it.

This is where social media has increasingly become instrumental for public messaging for a wide variety of actors, not just for non-state actors, but from heads of state to political players to armed groups. Public institutions and governments have normalised the use of social media to engage with citizens and encourage their participation in government processes.[4] However, authoritarian and semi-democratic authoritarian states have a well-documented history keeping under control media freedom and employing censorship laws in place of violence to regulate critical political reporting.[5] The proliferation of social media channels has ushered in a new era where media, journalism, and reporting are democratised, giving individuals unprecedented access to platforms that allow them to circumvent censorships to report events, express grievances related to social injustice, and even expose instances of war crimes. Simultaneously, the advent of social media has transformed the landscape of propaganda, image-building, and the audience engagement, expanding the capabilities of disinformation operators in these domains.[6] The online ecosystem has emerged as a significant challenge for authoritarian regimes, compelling them to grapple with the intricacies of public sentiment, opposition management, and the high suppression of dissent in an environment where information flows more freely than ever before.

1 Special Counsel's Office, "Report on the Investigation into Russian Interference in the 2016 Presidential Election," n.d.
2 Samantha Bradshaw, "Influence Operations and Disinformation on Social Media," Centre for International Governance Innovation, November 23, 2020, https://www.cigionline.org/articles/influence-operations-and-disinformation-social-media/.
3 Andrew M. Guess and Benjamin A. Lyons, "Misinformation, Disinformation, and Online Propaganda," in Social Media and Democracy: The State of the Field, Prospects for Reform (Cambridge University Press, 2020), 10–33.
4 Sara Hofmann et al., "What Makes Local Governments' Online Communications Successful? Insights from a Multi-Method Analysis of Facebook," Government Information Quarterly 30, no. 4 (October 2013): 387–96, https://doi.org/10.1016/j.giq.2013.05.013.
5 Mikal Hem, "Evading the Censors: Critical Journalism in Authoritarian States," Reuters Institute for the Study of Journalism (Reuters Institute Fellowship Paper University of Oxford, n.d.), https://reutersinstitute.politics.ox.ac.uk/our-research/evading-censors-critical-journalism-authoritarian-states.
6 Bulovsky, Andrew. "Authoritarian Communication on Social Media: The Relationship between Democracy and Leaders' Digital Communicative Practices." International Communication Gazette 81, no. 1 (April 5, 2018): 20–45. https://doi.org/10.1177/1748048518767798.

Before the advent of social media, media bias was a potent instrument for shaping the most traditional news narratives. The evolution of digital communication has compelled authoritarian and semi-democratic states to adapt to the transformations and develop strategies to effectively manage public discourse and curtail potential resistance arising from dissent. The term "networked authoritarianism," coined by Mackinnon was epitomised by China's approach, in which the government embraces the internet's technological advancements while simultaneously exerting close surveillance of its citizens and censoring and manipulating online conversations to make it exceptionally challenging for opposition movements to organise effectively. [7]

Similarly, Russia's autocratic political elites employ a surveillance assemblage which is comprised of state-recruited vigilant citizens to monitor online speech and identify dissent.[8] This surveillance assemblage is a crucial component of Russia's strategy to maintain control over the digital sphere. In Venezuela, the Maduro government employed coordinated online trolls known to as "tropas" as a tool to manipulate narratives. These tropas are engaged in disseminating propaganda, and distorting public perception, part of a broader strategy to control and influence online discourse.[9] Such issues present significant challenges for the public, particularly in their search for free access to information and making informed electoral decisions.

The concept of counter-narratives in the strategic communications lexicon gained prominence during the Global War on Terror (GWOT) as a soft approach by the government to counter online propaganda from groups such as al-Qaeda and the Islamic State (IS), but it is not new.[10] While the effectiveness of online counter-narratives in countering extremist and terrorist propaganda remains a subject of debate, they are a standard tool in the strategic communication arsenal of state actors.[11] The idea behind counter-narratives can be attributed to the British counter-insurgency campaign during the Malayan Emergency between 1948 and 1960. Sir Gerald Templer's coined the phrase 'winning hearts and minds' to encapsulate the concept of winning popular support against the Communist insurgency.[12] But recently declassified documents concerning the Batang Kali massacre in Malaya not only contradict this slogan but also expose the fact that it was an exaggeration of British counter-insurgency achievements to conceal the use of brutal force against unarmed civilians.[13]

In the present context, counter-narratives are employed to neutralise divergent perspectives. To make censorship effective, these strategies require the use of counter-narratives or competing narratives.[14] This is accomplished by leveraging "online commentators" or "social influencers" to manipulate online discourse and conduct digital astro-turfing to neutralise unfavourable opinions, steer narratives, defend party policies, and impact news reporting.[15] Strategies like

7 Rebecca Mackinnon, "Liberation Technology: China's 'Networked Authoritarianism,'" Journal of Democracy 22, no. 2 (April 2011): 32–46.
8 Rashid Gabdulhakov, "(Con)Trolling the Web: Social Media User Arrests, State-Supported Vigilantism and Citizen Counter-Forces in Russia," Global Crime 21, no. 3–4 (February 19, 2020): 283–305, https://doi.org/10.1080/17440572.2020.1719836.
9 Advox. "Unfreedom Monitor Report: Venezuela Country Report." Global Voices. The Unfreedom Monitor, May 25, 2023. https://globalvoices.org/2023/05/25/unfreedom-monitor-report-venezuela/
10 Christian Leuprecht et al., "Narrative and Counter-Narratives Strategy," Perspectives on Terrorism 3, no. 2 (2009): 25–35. https://www.universiteitleiden.nl/binaries/content/assets/customsites/perspectives-on-terrorism/2009/issue-2/winning-the-battle-but-losing-the-war-narrative-and-counter-narratives-strategy---christian-leuprecht-todd-hataley-sophia-moskalenko-clark-mccauley.pdf.
11 Winterbotham, Emily, and Eric Rosand. "Do Counter-Narratives Actually Reduce Violent Extremism?" Brookings, March 20, 2019. https://www.brookings.edu/articles/do-counter-narratives-actually-reduce-violent-extremism/
12 Maley, William. "Terrorism, Diplomacy, and State Communications." ICCT Research Paper, 2018. https://www.icct.nl/sites/default/files/import/publication/ICCT-Maley-Terrorism-Diplomacy-and-State-Communications-March2018-1.pdf
13 Paul Dixon, "'Hearts and Minds'? British Counter-Insurgency from Malaya to Iraq," Journal of Strategic Studies, June 1, 2009. See also Kevin Doyle, "Batang Kali: A British Massacre in Colonial Malaya and a Fight for Justice," Al Jazeera, December 11, 2023. https://www.aljazeera.com/news/longform/2023/12/11/batang-kali-a-british-massacre-in-colonial-malaya-and-a-fight-for-justice
14 Nicholas Cheong, "Disinformation as a Response to the 'Opposition Playground' in Malaysia," in From Grassroots Activism to Disinformation: Social Media in Southeast Asia, ed. Aim Sinpeng and Ross Tapsell (ISEAS-Yusof Ishak Institute, 2020), 63–85.
15 "Digital astroturfing" refers to the deceitful practice of orchestrating political campaigns to manufacture the presence or appearance of organic and/or grassroots support online, whereas in fact they are sponsored and inauthentic. See Marko Kovic, Adrian Rauchfleisch, Marc Sele, and Christian Caspar. 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.

"red-tagging," as known in the Philippines, are crucial for discrediting the opposition by labelling them as the extremists, terrorists, or even traitors.[16] This is a worrying development because the employment of online influence tactics poses a significant threat to democratic processes, media integrity, and social cohesion. This policy brief focuses on Malaysia's experience with surveillance assemblage and digital vigilantism, highlighting a top-down approach to counter what the state defines 'extremists' and how it utilises the concept of extremism. The policy brief aims to highlight that policymakers and practitioners should assess how the state defines 'extremists' and utilises the idea of extremism. This will be accomplished while showcasing the term "vigilantism," understood here as a sub-genre of extremism. The focus will be on its online manifestation in the form of "digital vigilantism", which will allow for a more nuanced understanding of how extremist narratives, deployed by state actors, fuel polarisation, both in online and offline contexts. This policy brief offers recommendations on how to tackle the issue.

Key Concepts and Definitions

Extremism involves the advocacy of a supremacist ideology which asserts the superiority and dominance of an identity-based in-group over all out-groups.[17] Ideological supremacy could manifest itself through violence and the targeting of hate toward groups based on their identity.[18] The process can be part of a more gradual social or political initiative aimed at undermining human rights, democratic institutions, and civic culture. In this policy brief, extremism is characterised as a product of the *us versus them* mentality, often intensified by the belief that the success or survival of an in-group (us) is intrinsically related to hostile actions against another (them).[19] One aspect of extremism that needs more attention is vigilantism. Although vigilantism has become increasingly linked to far right political beliefs and xenophobia, many still view the practice as a violent act isolated from state involvement. Conceptualising what vigilantism may mean in this context and how extremism can manifest itself in pro-establishment vigilantism could help explain the phenomenon of "cyber troopers" in the context of Malaysia's digital ecosystem later in this brief. Moncada defines vigilantism as ''the collective use or threat of the extra-legal violence in response to an alleged criminal act.''[20] This definition underscores that vigilantism is a response to perceived criminality that falls beyond the scope of conventional legal procedures. Loveluck further elaborates that vigilantism represents a form of collective power to either establish or reinstate order through direct, often punitive actions, which blatantly challenge and defy the conventional legal and institutional frameworks.[21] JM Berger adds another dimension to this debate by illustrating that extremism can assume a veneer of legality, particularly when an extremist majoritarian faction controls the government.[22] This point underscores the complexity of extremism and vigilantism, highlighting how they can be perceived differently depending on who wields power and how they manipulate legal structures to their advantage.

This policy brief also builds upon Loveluck's perspective on digital vigilantism, also known as the digitalantism, which refers to online actions as a direct response to perceived violations of the institutionalised norms.[23] It resonates with Donald Black's perspective on the law as an instrument

16 "Red-tagging" refers to the branding of individuals or organisations as communists, terrorists, or in Malaysia's case, Zionist-sympathisers.
17 Isabel Jones, Jakob Guhl, and Moustafa Ayad, "Young Guns: Understanding a New Generation of Extremist Radicalization in the US," ISD (Institute for Strategic Dialogue, August 29, 2023), https://www.isdglobal.org/isd-publications/young-guns-understandings-a-new-generation-of-extremist-radicalization-in-the-us/.
18 Ibid.
19 J. M. Berger, Extremism (MIT Press, 2018).
20 Eduardo Moncada, "Varieties of Vigilantism: Conceptual Discord, Meaning and Strategies," Global Crime 18, no. 4 (September 14, 2017): 403–23, https://doi.org/10.1080/17440572.2017.1374183.
21 Benjamin Loveluck, "The Many Shades of Digital Vigilantism. A Typology of Online Self-Justice," Global Crime 21, no. 3–4 (June 4, 2019): 213–41, https://doi.org/10.1080/17440572.2019.1614444.
22 J.M. Berger, "Lawful Extremism: Extremist ideology and the Dred Scott decision." Center on Terrorism, Extremism and Counterterrorism, Middlebury Institute of International Studies. Occasional paper. November 2023.
23 Loveluck, 2019. See also Les Johnston, "What Is Vigilantism?," British Journal of Criminology 36, no. 2 (January 1, 1996): 220–36, https://doi.org/10.1093/oxfordjournals.bjc.a014083 for his discussion on vigilantism.

of government social control. Black's framework distinguishes between legal and societal norms and emphasises the role of social control in shaping our understanding of deviant behaviours.[24] In practice, vigilantism often emerges in response to perceived deviations from social norms or breaches of the social contract, particularly when authorities fail to address these transgressions effectively. Understanding vigilantism requires us to delve into the intricate dynamics between the state and society, especially in cases where state failure contributes to the phenomenon.[25]

The Effects of Disinformation

While disinformation is widely acknowledged for its ability to shape opinions and to influence behaviour, its capacity extends beyond manipulation. Disinformation can serve as a tool for astroturfing, orchestrating the creation of artificial support to manufacture consent. This often-underappreciated facet of disinformation holds paramount significance in understanding its multifaceted impact on society. Astroturfing goes beyond deceiving individuals; it actively undermines the authenticity of public discourse and democratic processes. This manipulation tactic not only distorts the narrative but also poses a substantial threat to the foundations of trust within institutions and the integrity of civic engagement. More crucially, if the number of astroturfers is high enough, it can generate the illusion of social visibility, which is then leveraged to construct the illusion of organic intervention and support from the perceived majority that leads to policing the discourse space with weaponised narratives.[26] This is arguably a form of subversive campaign.[27] This phenomenon highlights the ability of hate groups to manipulate social media to foster and amplify extremist ideologies with potential real-world consequences. In India, for instance, groups like the Bhartiya Gau Raksha Dal (BGRD) vigilantes or Gau Rakshaks (cow protectors) for short, who are dedicated to protecting cows from slaughter because of the divinity of the animal in Hindu belief, use social media to target individuals suspected of cow slaughter, leading to violent attacks.[28] Similarly, Ma Ba Tha's anti-Rohingya propaganda in Myanmar illustrates how such groups leverage social media to incite and legitimise state-sanctioned violence - a catalyst for the 2017 genocide in the Rakhine State.[29]

Individuals affiliated with the Myanmar military junta and radical Buddhist nationalist groups' who were active on Facebook were instrumental in cultivating a hostile environment that not only condones but also advocates for atrocities against targeted groups.[30] The algorithmic design of Facebook, which can foster hate-filled echo chambers, played a pivotal role in desensitising the audience to the ongoing persecution.[31] Compounding the issue, Facebook's prevailing content moderation practises, often favouring the ruling government for operational reasons, neglected the broader impact of censorship on vulnerable communities. In another example, following Elon Musk's Twitter acquisition in April 2022, the platform experienced a significant increase in harmful content such as hate speech, extremist views, and propagation of misinformation and disinformation.[32] Musk's free speech absolutism emboldened right-wing extremists on X (formerly known as Twitter). Adding to the turmoil, Musk's decision to remove headlines from shared news articles on the platform worsened the disinformation problem. The impact was particularly pronounced after the October 7 attack by Hamas and Israel's retaliatory strikes on

24 Donald Black, The Behavior of Law: Special Edition (Emerald Group Publishing, 2010).
25 Tore Bjørgo and Miroslav Mareš, Vigilantism against Migrants and Minorities (Routledge, 2019).
26 Daniel Trottier, "Digital Vigilantism as Weaponisation of Visibility," Philosophy & Technology 30, no. 1 (April 2016): 55–72. https://link.springer.com/article/10.1007/s13347-016-0216-4
27 Andreas Krieg, Subversion: The Strategic Weaponization of Narratives (Georgetown University Press, 2023).
28 Megan Ward, "Walls and Cows: Social Media, Vigilante Vantage, and Political Discourse." Social Media + Society 6, no. 2 (April 2020): 205630512092851. https://doi.org/10.1177/2056305120928513
29 Eleanor Albert, "The Rohingya Crisis," Council on Foreign Relations, June 17, 2015, https://www.cfr.org/backgrounder/rohingya-crisis.
30 Fortifyrights. "'They Gave Them Long Swords.'" Fortify Rights, July 19, 2018. https://www.fortifyrights.org/mly-inv-rep-2018-07-19/.
31 Amnesty International. "Myanmar: Facebook's Systems Promoted Violence against Rohingya; Meta Owes Reparations – New Report," September 29, 2022. https://www.amnesty.org/en/latest/news/2022/09/myanmar-facebooks-systems-promoted-violence-against-rohingya-meta-owes-reparations-new-report/.
32 Joy Anyanwu and Rashawn Ray, "Why Is Elon Musk's Twitter Takeover Increasing Hate Speech?," Brookings, November 23, 2022, https://www.brookings.edu/articles/why-is-elon-musks-twitter-takeover-increasing-hate-speech/.

Gaza.

The dissemination of fake and manipulated graphic visuals, along with "fish-wrapped" photos repurposed from Syria's civil war in 2011 falsely presented as from Palestine on X, resulted in heightened confusion and polarisation.[33] This was further exacerbated by conflicting statements by government officials. The polluted information ecosystem on X not only severely undermined trust in mainstream media, but also fuelled vigilante activities, including hate crimes in the US against Jews and Muslims. Tragically, this escalation culminated in the tragic stabbing of six-year-old Wadea Al-Fayoume, on October 14 2023, in Plainfield, Illinois.[34]

The Future of Information Warfare and Digital Vigilantism

Digital vigilantism has emerged as a means for actors to exhibit their capacity for violence, leveraging the anonymity provided by digital platforms without requiring offline physical actions. In some instances, especially in nations with precarious democracies, individuals might even align themselves with the state's interests for self-preservation. Incentives are created to authorise and empower private citizens, supported by the state or state-aligned entities, to engage in coordinated or networked responses as directed. This conveniently provides a substantial level of plausible deniability insulating the involvement of the political establishment. Social networks have become a valuable tool for political campaigns because they allow political players to reach a large audience quickly and effectively. More specifically, social media manipulation has become an integral part of information wars and election rigging and poses the potential to undermine the integrity of elections and earn its instigators an electoral advantage. Political vigilantism, or footsoldiering (a phenomenon that seems particularly linked to the electoral experiences of the global South, where political parties mobilise their members and grassroots supporters as part of their political messaging) is seen as an evolving problem, but again, its origins are hardly new. The concept of 'footsoldiering' can be traced to Ghana's electoral politics in the 1980s and 1990s, which involved the informal recruitment of campaign personnel or messengers tasked with disseminating party information to grassroots communities.[35] Comparatively a more modern digital version of Ghana's 'footsoldiers' would be Malaysia's cyber troopers.

Cyber troopers, often referred to as "cytros", are a sub-category of (digital) vigilantes who play an active role in shaping public discourse related to domestic politics in Malaysia.[36] These individuals are often involved in campaigning for specific political parties while simultaneously disparaging their rivals, whether paid or otherwise. These political influence efforts are commonly referred to as "black ops," an epithet that might have been inspired by a *Washington Post* article discussing the "black operations" of political trolls in the Philippines.[37] Given their vigilant tendencies and hostile targeting behaviour to counter opposing views, cyber troopers can be considered the surveillant assemblage of Malaysia's political machinery. The landscape of digital campaigns in Malaysia vividly illustrates how ordinary citizens can mobilise themselves as cyber vigilantes to further the goals or ambitions of whichever political entity or personality suits them. This

33 Matt O'Brien and Frank Bajak, "Misinformation about the Israel-Hamas War Is Flourishing on X," AP News, October 10, 2023. https://www.brookings.edu/articles/why-is-elon-musks-twitter-takeover-increasing-hate-speech/

34 Mike Wendling, "Wadea Al-Fayoume: Last Words of Knifed US Muslim Boy Were 'Mom, I'm Fine,'" BBC News, October 17, 2023. https://apnews.com/article/twitter-x-hamas-israel-war-elon-musk-misinformation-5e344fc9134741d4f5dc17ed04262940

35 Kwesi Aning and Emma Birikorang, "Negotiating Populism and Populist Politics in Ghana, 1949-2012," in Managing Election-Related Violence for Democratic Stability in Ghana, ed. Kwesi Aning and Kwaku Danso (Friedrich Ebert Stiftung, 2012), 61–96. https://www.bbc.com/news/world-us-canada-67085553

36 Loh, Benjamin Y. H., and Sarah Ali. "Increased Cybertrooper Activity in Malaysia's State Elections and Increased Voter Apathy on Social Media." Fulcrum. ISEAS – Yusof Ishak Institute, August 18, 2023. https://fulcrum.sg/increased-cybertrooper-activity-in-malaysias-state-elections-and-increased-voter-apathy-on-social-media/.

37 Mahtani, Shibani, and Regine Cabato. "Why Crafty Internet Trolls in the Philippines May Be Coming to a Website near You." The Washington Post, July 26, 2019. https://www.washingtonpost.com/world/asia_pacific/why-crafty-internet-trolls-in-the-philippines-may-be-coming-to-a-website-near-you/2019/07/25/c5d42ee2-5c53-11e9-98d4-844088d135f2_story.html.

extension of the ruling party's objectives manifests itself in various ways, including intimidation tactics, coercive behaviour, and punitive responses involving lawfare.

Cybertrooper's digilantism involves various coercive tactics to exploit divisive social or political fault lines. This includes employing hate speech against minority groups, the dissemination of falsehoods and disinformation to smear and discredit opponents, leading to phenomena like red-tagging and green scare. These methods are designed to validate political party policies, justify prevailing systemic discrimination, and weaponise conspiracy theories as integral elements of their influence strategies while asserting their authority and belonging.[38] The overarching objective is to stifle dissent, coercing the public to endorse the party or weaken them enough to comply with establishment policies, under the threat of being securitised as a potential threat.

Surveillance Assemblage and Digital Vigilantes

In Malaysia's experience, cyber troopers are deployed to infiltrate and manipulate political conversation online on behalf of their principal, which may include political parties that fund them.[39] Their value lies in the potential for plausible deniability, and they can be categorised as either paid agents or volunteers (who are likely to be grassroots supporters or loyalists). Paid cyber troopers typically operate within a centralised command structure, while volunteers are likely to be dispersed and decentralised. While their motivations may not be exclusively ideological, financial incentives can play a significant role. Cyber trooper activities tend to intensify during election periods, with their primary objective being to influence voters.[40] However, their scope of activities can occasionally extend beyond election interference.

Malaysia's political landscape increasingly relies on these malign operations, employing diverse tactics, techniques, and procedures (TTPs).[41] Cyber troopers often exploit legal frameworks, particularly the 1948 Sedition Act, to quell dissent and brand legitimate criticisms as violations of race, religion, and royal institutions, known as 3R in Malaysia.[42] They engage in hyper-partisan content amplification, gaslighting, dissent suppression, and reality distortion, all to achieve specific political goals. [43] A key tactic is "red-tagging," labelling critics or oppositions as communists or extremists to undermine their credibility and justify potential punitive measures against them. "Green scare" is often employed in tandem with red-tagging to amplify fears that Malaysia of Malaysia falling under Islamist opposition. This tactic stems from anxieties about the perceived "green wave" effect associated with the electoral impact of the Malaysian Islamic Party (PAS) in the period surrounding the 15th General Election in November 2022.[44] This even involved manufacturing an unsubstantiated link between PAS and the Islamic State.[45]

Online nationalist and reactionary right-wing vigilantes in Malaysia are increasingly emboldened

38 Munira Mustaffa, "Rage Clicks, Hatebomb and the New World Order: How Hard-Right Politics and Conspiracy Theories Overlapped to Undermine Malaysia's Elections," GNET, December 14, 2022, https://gnet-research.org/2022/12/14/rage-clicks-hatebomb-and-the-new-world-order-how-hard-right-politics-and-conspiracy-theories-overlapped-to-undermine-malaysias-elections/.
39 Julian Hopkins, "Cyber troopers and Tea Parties: Government Use of the Internet in Malaysia," Asian Journal of Communication, January 2, 2014.
40 Peter Guest, "Malaysia Elections: The inside Story of Malaysia's Prolific Election Fixer," WIRED UK, May 9, 2018. https://www.wired.co.uk/article/election-malaysia-2018-general-fake-news-day-2008-syarul-ema
41 Pauline Pooi Yin Leong, "Digital Mediatization and the Sharpening of Malaysian Political Contests," in Digital Mediatization and the Sharpening of Malaysian Political Contests (ISEAS–Yusof Ishak Institute Singapore, 2021), VII–XXXVIII, http://dx.doi.org/10.1355/9789814951883-002.
42 Refworld, "Malaysia: Federal Constitution," Refworld (UNHCR, August 31, 1957), https://www.refworld.org/docid/3ae6b5e40.html.
43 Benjamin Y. H. Loh and Sarah Ali, "Increased Cybertrooper Activity in Malaysia's State Elections and Increased Voter Apathy on Social Media," Fulcrum (ISEAS – Yusof Ishak Institute, August 18, 2023), https://fulcrum.sg/increased-cybertrooper-activity-in-malaysias-state-elections-and-increased-voter-apathy-on-social-media/.
44 Kai Ostwald and Steven Oliver, "2023/87 'Continuity and Change: The Limits of Malaysia's Green Wave from a Four Arenas Perspective' by Kai Ostwald and Steven Oliver," October 27, 2023, https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2023-87-continuity-and-change-the-limits-of-malaysias-green-wave-from-a-four-arenas-perspective-by-kai-ostwald-and-steven-oliver/.
45 Munira Mustaffa, "The Deep Dive: Al Malaka Media Center," Chasseur Group, March 16, 2023, https://deepdive.chasseur.group/al-malaka-media-center/.

in employing similar strategies to promote a uniform national identity while actively opposing cultural and ethnic diversity. These groups, frequently engaged in incendiary hate speech and organised online harassment campaigns against minorities, rarely face significant repercussions. This impunity is partly due to the protection afforded by their status as Malay Muslims, the dominant majority in the country. This is compounded by a general lack of political will to confront these issues, driven by a fear of alienating Malay majority voters. This is why these vigilantes are instrumentalised to entrench views instead of defending the status quo.

While not all members of these groups share the same political views, a substantial number align with the nationalist ideology known as "Ketuanan Melayu" (Malay supremacy).[46] They are fuelled by the fear of a localised "Great Replacement" – a deep-seated anxiety that originates from the era of colonial British policies. This fear revolves around the concern that non-Malays might attempt a coup to usurp political power from the Malays, with the ultimate goal of commandeering national assets for their communal benefit. This anxiety is deeply rooted in Malaysia's colonial history, during which there was a perceived loss of sovereignty and control over their homeland. This historical context continues to influence the current political and social landscape in Malaysia.

Key Takeaway: Rethinking Extremism

While terrorism is usually understood to mean nonstate political violence directed primarily against state authority, the term "extremism" presents an even greater challenge when it comes to a universally applicable definition due to its inherent ambiguity and its relationship to terrorism, with which it is often considered synonymous. This ambiguity becomes an enabler for different interpretations and makes the term vulnerable to misuse for political or ideological purposes. The lack of clear criteria for applying the term can lead to subjective judgments rather than objective assessments and allow for the exclusion or discrediting of groups or individuals. Extremism research to date, particularly in the global North, generally recognises anti-state and anti-government extremism (ASAGE) but is reluctant to acknowledge that extremism can also take pro-government and pro-establishment forms. This unwillingness can be attributed to the delimitation of partisan politics and different experiences with statehood, with institutional strength being an essential component of effective P/CVE efforts, a shortcoming in many developing countries. For this reason, defining what constitutes 'government' as part of the P/CVE framework should be a necessary exercise. Granted, the issue is fraught with complexity, particularly in autocratic states with eroding democracy where the partisan aspect of government is central, calibrated by gerrymandering, and a weak electoral body.

The line between government and partisan interests can blur if not disappear altogether. Autocratic and authoritarian regimes often manipulate state institutions, including law enforcement and the judiciary, to advance their political agendas. As democratic principles wane, state power tends to concentrate within the ruling party or under the control of a single leader. This concentration of power often results in institutional fragility and an atmosphere of hyper-securitisation, with those in power viewing any form of dissent or deviation from the established order as a substantial threat. The ruling elites are particularly sensitive to actions or expressions that challenge their authority or diverge from accepted norms.

In such an environment where the ruling party or faction prioritises its own interests over the welfare of the nation, issues related to extremism and vigilantism can become deeply intertwined with partisan politics. This alignment can extend to even include violent far right actors who may seek protection or support from the government, further complicating efforts to effectively counter extremism and address vigilantism. Understanding these complicated dynamics is critical to developing strategies to counter these threats. This requires a comprehensive understanding

46 Munira Mustaffa, "Radical Right Activities in Nusantara's Digital Landscape: A Snapshot," GNET, April 19, 2022. https://www.wired.co.uk/article/election-malaysia-2018-general-fake-news-day-2008-syarul-ema

of the broader political landscape in which these actors operate.

Policy Recommendations

The prevailing policy recommendation for addressing information consumption issues is the implementation of digital literacy programmes. However, a key challenge associated with this approach lies in the assumption that members of society share common values and goals. This fallacy underscores the complexity of the problem, as individuals often prioritise information that aligns with their confirmation bias rather than factual accuracy. Weaponised narratives capitalise on this phenomenon, exploiting individuals' tendency to prioritise confirmation bias over factual accuracy. Given the intricate challenges within this landscape, a multifaceted approach is not only necessary but must also encompass government participation, collaboration with tech companies, and the engagement of a more autonomous civil society. The process of content takedown should mandate transparency, particularly in cases involving criticism or dissent, and it should allow for mechanisms to challenge censorship should be permitted. Moreover, tech companies should assume responsibility for cultivating a less hostile environment on social media platforms by discontinuing incentives for those who profit from rage-farming or hate-baiting, and they should be more responsive to reports of malicious behaviour.

In addition, policymakers should explore measures to discourage social media companies from facilitating cyber social ills and review how they address malicious actors or harmful content online. This effort necessitates a more holistic moderation approach, emphasising the importance of strengthened collaboration with grassroots civil society organisations and community leaders, particularly those who are marginalised or at risk that can benefit from digital resilience initiatives. Above all, it is crucial for this multi-stakeholder approach to be guided by shared humanitarian values to mitigate the risk of legal mechanisms being abused.

Bibliography

Advox. "Unfreedom Monitor Report: Venezuela Country Report." Global Voices. *The Unfreedom Monitor,* May 25, 2023. https://globalvoices.org/2023/05/25/unfreedom-monitor-report-venezuela/

Albert, Eleanor. "The Rohingya Crisis." *Council on Foreign Relations,* June 17, 2015. https://www.cfr.org/backgrounder/rohingya-crisis

Amnesty International. "Myanmar: Facebook's Systems Promoted Violence against Rohingya; Meta Owes Reparations – New Report," September 29, 2022. https://www.amnesty.org/en/latest/news/2022/09/myanmar-facebooks-systems-promoted-violence-against-rohingya-meta-owes-reparations-new-report/

Aning, Kwesi, and Emma Birikorang. "Negotiating Populism and Populist Politics in Ghana, 1949-2012." In *Managing Election-Related Violence for Democratic Stability in Ghana*, edited by Kwesi Aning and Kwaku Danso, 61–96. Friedrich Ebert Stiftung, 2012. https://library.fes.de/pdf-files/bueros/ghana/11294.pdf.

Anyanwu, Joy, and Rashawn Ray. "Why Is Elon Musk's Twitter Takeover Increasing Hate Speech?" *Brookings*, November 23, 2022. https://www.brookings.edu/articles/why-is-elon-musks-twitter-takeover-increasing-hate-speech/.

Bateson, Regina. "The Politics of Vigilantism." *Comparative Political Studies* 54, no. 6 (September 21, 2020): 923–55. https://doi.org/10.1177/0010414020957692.

Berger, J. M. *Extremism*. MIT Press, 2018.

Berger, J.M., "Lawful Extremism: Extremist ideology and the Dred Scott decision." *Center on Terrorism, Extremism and Counterterrorism, Middlebury Institute of International Studies.* Occasional paper. November 2023.

Bjørgo, Tore, and Miroslav Mareš. *Vigilantism against Migrants and Minorities*. Routledge, 2019.

Black, Donald. *The Behavior of Law: Special Edition*. Emerald Group Publishing, 2010.

Bradshaw, Samantha. "Influence Operations and Disinformation on Social Media." Centre for International Governance Innovation, November 23, 2020. https://www.cigionline.org/articles/influence-operations-and-disinformation-social-media/

Bulovsky, Andrew. "Authoritarian Communication on Social Media: The Relationship between Democracy and Leaders' Digital Communicative Practices." *International Communication Gazette* 81, no. 1 (April 5, 2018): 20–45. https://doi.org/10.1177/1748048518767798.

Cheong, Nicholas. "Disinformation as a Response to the 'Opposition Playground' in Malaysia." In *From Grassroots Activism to Disinformation: Social Media in Southeast Asia*, edited by Aim Sinpeng and Ross Tapsell, 63–85. ISEAS-Yusof Ishak Institute, 2020.

Dixon, Paul. "'Hearts and Minds'? British Counter-Insurgency from Malaya to Iraq." *Journal of Strategic Studies*, June 1, 2009.

Doyle, Kevin. "Batang Kali: A British Massacre in Colonial Malaya and a Fight for Justice." *Al Jazeera*, December 11, 2023. https://www.aljazeera.com/news/longform/2023/12/11/batang-kali-a-british-massacre-in-colonial-malaya-and-a-fight-for-justice.

Fortifyrights. "'They Gave Them Long Swords.'" Fortify Rights, July 19, 2018. https://www.fortifyrights.org/mly-inv-rep-2018-07-19/

Gabdulhakov, Rashid. "(Con)Trolling the Web: Social Media User Arrests, State-Supported Vigilantism and Citizen Counter-Forces in Russia." *Global Crime* 21, no. 3–4 (February 19, 2020): 283–305. https://doi.org/10.1080/17440572.2020.1719836.

Guess, Andrew M., and Benjamin A. Lyons. “Misinformation, Disinformation, and Online Propaganda.” In *Social Media and Democracy: The State of the Field, Prospects for Reform*, 10–33. Cambridge University Press, 2020.

Guest, Peter. “Malaysia Elections: The inside Story of Malaysia’s Prolific Election Fixer.” *WIRED UK*, May 9, 2018. https://www.wired.co.uk/article/election-malaysia-2018-general-fake-news-day-2008-syarul-ema.

Hem, Mikal. “Evading the Censors: Critical Journalism in Authoritarian States.” Reuters Institute for the Study of Journalism. Reuters Institute Fellowship Paper University of Oxford. https://reutersinstitute.politics.ox.ac.uk/our-research/evading-censors-critical-journalism-authoritarian-states.

Hofmann, Sara, Daniel Beverungen, Michael Räckers, and Jörg Becker. “What Makes Local Governments’ Online Communications Successful? Insights from a Multi-Method Analysis of Facebook.” *Government Information Quarterly* 30, no. 4 (October 2013): 387–96. https://www.sciencedirect.com/science/article/abs/pii/S0740624X13000749

Hopkins, Julian. “Cyber troopers and Tea Parties: Government Use of the Internet in Malaysia.” *Asian Journal of Communication*, January 2, 2014.

Jones, Isabel, Jakob Guhl, and Moustafa Ayad. “Young Guns: Understanding a New Generation of Extremist Radicalization in the US.” *ISD*. Institute for Strategic Dialogue, August 29, 2023. https://www.isdglobal.org/isd-publications/young-guns-understandings-a-new-generation-of-extremist-radicalization-in-the-us/.

Kovic, Marko, Adrian Rauchfleisch, Marc Sele, and Christian Caspar. 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.

Krieg Andreas, Subversion: The Strategic Weaponization of Narratives (Georgetown University Press, 2023).

Leuprecht, Christian, Todd Hataley, Sophia Moskalenko, and Clark McCauley. “Narrative and Counter-Narratives Strategy.” *Perspectives on Terrorism* 3, no. 2 (2009): 25–35. https://www.tandfonline.com/doi/full/10.1080/17440572.2019.1614444

Loh, Benjamin Y. H., and Sarah Ali. “Increased Cybertrooper Activity in Malaysia’s State Elections and Increased Voter Apathy on Social Media.” Fulcrum. ISEAS – Yusof Ishak Institute, August 18, 2023. https://fulcrum.sg/increased-cybertrooper-activity-in-malaysias-state-elections-and-increased-voter-apathy-on-social-media/.

Loveluck, Benjamin. “The Many Shades of Digital Vigilantism. A Typology of Online Self-Justice.” *Global Crime* 21, no. 3–4 (June 4, 2019): 213–41. https://doi.org/10.1080/17440572.2019.1614444.

Mackinnon, Rebecca. “Liberation Technology: China’s ‘Networked Authoritarianism.’” *Journal of Democracy* 22, no. 2 (April 2011): 32–46.

Mahtani, Shibani, and Regine Cabato. “Why Crafty Internet Trolls in the Philippines May Be Coming to a Website near You.” *The Washington Post*, July 26, 2019. https://www.washingtonpost.com/world/asia_pacific/why-crafty-internet-trolls-in-the-philippines-may-be-coming-to-a-website-near-you/2019/07/25/c5d42ee2-5c53-11e9-98d4-844088d135f2_story.html

Maley, William. “Terrorism, Diplomacy, and State Communications.” *Terrorism and Counter-Terrorism Studies*, 2018. https://doi.org/10.19165/2018.1.04.

Moncada, Eduardo. “Varieties of Vigilantism: Conceptual Discord, Meaning and Strategies,” *Global Crime 18,* no. 4 (September 14, 2017): 403–23, https://doi.org/10.1080/17440572.2017.1374183.

Mustaffa, Munira. “Radical Right Activities in Nusantara’s Digital Landscape: A Snapshot.” GNET, April 19, 2022. https://gnet-research.org/2022/04/19/radical-right-activities-in-nusantaras-digital-landscape-a-snapshot/.

Mustaffa, Munira. “Rage Clicks, Hatebomb and the New World Order: How Hard-Right Politics and

Conspiracy Theories Overlapped to Undermine Malaysia's Elections." GNET, December 14, 2022. https://gnet-research.org/2022/12/14/rage-clicks-hatebomb-and-the-new-world-order-how-hard-right-politics-and-conspiracy-theories-overlapped-to-undermine-malaysias-elections/.

Mustaffa, Munira.. "The Deep Dive: Al Malaka Media Center." *Chasseur Group*, March 16, 2023. https://deepdive.chasseur.group/al-malaka-media-center/.

O'Brien, Matt, and Frank Bajak. "Misinformation about the Israel-Hamas War Is Flourishing on X." *AP News*, October 10, 2023. https://apnews.com/article/twitter-x-hamas-israel-war-elon-musk-misinformation-5e344fc9134741d4f5dc17ed04262940.

Office, Special Counsel's. "Report on the Investigation into Russian Interference in the 2016 Presidential Election," n.d. Accessed December 11, 2023.

Ostwald, Kai, and Steven Oliver. "2023/87 'Continuity and Change: The Limits of Malaysia's Green Wave from a Four Arenas Perspective' by Kai Ostwald and Steven Oliver," October 27, 2023. https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2023-87-continuity-and-change-the-limits-of-malaysias-green-wave-from-a-four-arenas-perspective-by-kai-ostwald-and-steven-oliver/.

Pooi, Pauline Yin Leong. "Digital Mediatization and the Sharpening of Malaysian Political Contests." In Digital Mediatization and the Sharpening of Malaysian Political Contests, VII–XXXVIII. *ISEAS–Yusof Ishak Institute Singapore*, 2021. http://dx.doi.org/10.1355/9789814951883-002.

Refworld. "Malaysia: Federal Constitution." Refworld. UNHCR, August 31, 1957.b https://www.refworld.org/legal/legislation/natlegbod/1957/en/40703

Transparency Center. "Inauthentic Behaviour." Meta, n.d. https://transparency.fb.com/en-gb/policies/

Trottier Daniele, "Digital Vigilantism as Weaponisation of Visibility," *Philosophy & Technology 30,* no. 1 (April 2016): 55–72, https://doi.org/10.1007/s13347-016-0216-4.

Ward, Megan. "Walls and Cows: Social Media, Vigilante Vantage, and Political Discourse." *Social Media + Society* 6, no. 2 (April 2020). https://doi.org/10.1177/2056305120928513.

Wendling, Mike. "Wadea Al-Fayoume: Last Words of Knifed US Muslim Boy Were 'Mom, I'm Fine.'" BBC News, October 17, 2023. https://www.bbc.com/news/world-us-canada-67085553.

Winterbotham, Emily, and Eric Rosand. "Do Counter-Narratives Actually Reduce Violent Extremism?" *Brookings*, March 20, 2019. https://www.brookings.edu/articles/do-counter-narratives-actually-reduce-violent-extremism/.

Yin Leong, Pauline Pooi. "Digital Mediatization and the Sharpening of Malaysian Political Contests." In *Digital Mediatization and the Sharpening of Malaysian Political Contests*, VII–XXXVIII. ISEAS–Yusof Ishak Institute Singapore, 2021. http://dx.doi.org/10.1355/9789814951883-002.

Zulkiflee, Wara. "Fahmi: MCMC to Investigate Copycat Social Media Posts." *New Straits Times*, July 11, 2023. https://www.nst.com.my/news/crime-courts/2023/07/929887/fahmi-mcmc-investigate-copycat-social-media-posts.

About the Author

Munira Mustaffa

Munira Mustaffa joined the International Centre for Counter-Terrorism (ICCT) as a Visiting Fellow under the Current and Emerging Threat Programme in October 2023. Her research investigates the impact of pro- and anti-establishment extremism within the Global South, particularly emphasising electoral disinformation and vulnerabilities. As the founder, Executive Director, and principal consultant of Chasseur Group, Munira boasts over a decade of comprehensive experience across private, public, and military security sectors. She has briefed various government, defense, and private-sector stakeholders. She previously served as a counter-terrorism analyst for the Southeast Asia Regional Centre for Counter-terrorism (SEARCCT) and as a civilian analyst for the Counterterrorism Division at the Defense Intelligence Staff Division (now known as the Malaysian Defence Intelligence Organisation, MDIO).

Munira is also a non-resident fellow at the New Lines Institute for Strategy and Policy, a Washington, DC-based policy think tank, and a fellow at Verve Research, an independent research collective focusing on military-society relations in the Indo-Pacific region's political development. Her work primarily identifies and analyses non-traditional security challenges, including terrorism, extremism, paramilitary organisations, clandestine activities, malign influence operations, and media and information warfare.

She has been published by NATO Strategic Communications Centre of Excellence (STRATCOMCOE), Global Network on Extremism and Technology (GNET) Insights, New Lines Institute for Strategy and Policy, Lowy Institute, and Australian Strategic Policy Institute (ASPI). Munira is a graduate of University College London (UCL) in the United Kingdom, where she earned her MSc in Countering Organised Crime and Terrorism at the Jill Dando Institute of Crime Science.

International Centre for Counter-Terrorism

International Centre for Counter-Terrorism (ICCT)
T: +31 (0)70 763 0050
E: info@icct.nl
www.icct.nl