Hedayah
Countering Extremism & Violent Extremism

UNDERSTANDING AND PREVENTING ONLINE EXTREMISM AND VIOLENT EXTREMISM IN SOUTHEAST ASIA

MALAYSIA COUNTRY REPORT

Understanding and Preventing Online Extremism and Violent Extremism in Southeast Asia

MALAYSIA COUNTRY REPORT

Farangiz Atamuradova, Galen Lamphere-Englund, Emma Allen, Nurul Hidayah Mohd Noar, Kennimrod Sariburaja & Siti Hikmah Musthar

Hedayah
Countering Extremism & Violent Extremism

SEARCCT

Table of Contents

The views expressed in this report are the opinions and work of the authors, and do not necessarily reflect the opinions or views of Hedayah or any of the participating organizations or individuals.

ABOUT HEDAYAH

Hedayah was created in response to a growing desire from the international community and members of the Global Counter-Terrorism Forum (GCTF) - which now represents 31 countries and the European Union - to establish an independent, multilateral 'think and do' tank devoted to countering extremism and violent extremism. Since its inception, Hedayah has evolved into a passionate, driven, and international organization that brings together a network of unparalleled experts and practitioners to counter and prevent extremism and violent extremism. Twelve members of the GCTF are representatives of our diverse Steering Board, which provides strategic oversight. As the International Center of Excellence for Countering Extremism and Violent Extremism, we are committed to innovation, neutrality, integrity, diversity, and technical excellence by delivering groundbreaking research, innovative methodologies, and programs. Our approach is to deliver real and sustainable impact to governments, civil society and people impacted by extremism and violent extremism through local ownership and collaboration.

Hedayah
Countering Extremism & Violent Extremism

ACKNOWLEDGMENTS

Hedayah expresses its deepest appreciation and gratitude to all the experts, practitioners and partners who took part in the research, and to Hedayah's Malaysian research partners, the Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT), Ministry of Foreign Affairs of Malaysia for their immensely valuable contributions to shaping this report. Hedayah also thanks the Australian Department of Foreign Affairs and Trade (DFAT) for funding this research as part of the broader Hedayah program on Understanding and Preventing Extremism and Violent Extremism in Southeast Asia. Finally, we extend our thanks to the reviewers and other contributors to this Report, including Anna Sherburn (Hedayah) and Charlotte Gerdes.

Suggested Reference:

Farangiz Atamuradova, Galen Lamphere-Englund, Emma Allen, Nurul Hidayah Mohd Noar, Kennimrod Sariburaja & Siti Hikmah Musthar. (2025) *Understanding and Preventing Online Extremism and Violent Extremism in Southeast Asia - Malaysia Country Report*. Hedayah, the International Centre of Excellence for Countering Extremism and Violent Extremism. United Arab Emirates (UAE).

Executive Summary

Today's world has seen rapid developments in technology and an increased connectedness and engagement online. While this has grown the global economy and enabled new connections, learning, and innovation for Malaysia's 34.9 million internet users, this accessibility, engagement and reach can also be exploited by malicious actors.

To support future online counter extremism activities in Malaysia, this qualitative research study sought to identify existing good practices and models for responses as well as present and emerging trends and challenges. Research conducted included secondary review of recent literature on the online media and information landscape, its exploitation by terrorist or extremism organizations, and documented response efforts, as well as primary research conducted with frontline practitioners of online countering extremism and violent extremism efforts and other relevant key stakeholders.

The Report outlines a range of key findings across three main areas. First, it considers the **online information landscape** in Malaysia, discussing trends in online spaces, narratives utilized by extremist, violent extremist and terrorist groups and the impacts of mis- and disinformation. Second, it considers **emerging threats online** and their local dimensions in Malaysia, ranging from the use of different platforms to major emerging technologies and issue areas that require continued attention. Finally, this Report outlines **existing responses in countering extremism and violent extremism online**, ranging from strategic communications efforts to relevant legal frameworks and Media and Information Literacy (MIL) interventions, and discussion of key challenges, needs and lessons learned around content moderation, MIL, coordination efforts and inclusive approaches.

This Report concludes with **contextualized and actionable recommendations** for future efforts in online counter extremism in Malaysia, to support ongoing efforts in this space and help to tailor and target new approaches. **These include:**

- Emphasizing contextualized approaches to countering extremism while leveraging global lessons and trends to inform local prevention
- Balancing online and offline efforts to effectively combat extremism, and employing different 'toolkits' to strengthen counter online extremism efforts
- Engaging with platforms and enhancing digital literacy to respond effectively on emerging fronts like gaming
- Considering opportunities for counter extremism efforts presented by Artificial Intelligence (AI) as well as responding to potential threats from terrorist or extremist exploitation of new technologies
- Continuing to proactively build coordination between a wide range of actors can improve outcomes, increase inclusivity, and strengthen resilience

These recommendations seek to build on Malaysia's existing efforts and strengths and provide evidence to enable policymakers and practitioners to continue to innovate and enhance prevention, moderation and other related intervention areas in order to address the constantly evolving challenge of terrorist and extremist exploitation of online spaces.

1. INTRODUCTION

1. Introduction

Malaysia's rapid digital transformation has significantly increased connectivity across the country, linking individuals locally, regionally, and globally. While this connectivity brings numerous benefits—enhancing communication, expanding access to information, and supporting economic growth, it has also created new vulnerabilities. Malicious actors, particularly extremist groups, have adapted to this evolving landscape by exploiting digital tools and platforms to spread propaganda, radicalize individuals, recruit supporters, and fundraise for the group. These groups adapt their approaches to align with platform-specific dynamics, leveraging algorithms and trending content for amplification and exploiting encrypted or semi-closed channels to evade detection and increase reach.

As of early 2025, Malaysia has approximately 34.9 million internet users, reflecting widespread digital access and increasing reliance on the online ecosystem across the country (Kemp, 2025). This digital expansion, however, also exposes users to harmful content, including extremist narratives that appeal to personal, religious, and socio-political grievances. These narratives often draw on local and global events, mis- and disinformation, and emotionally charged appeals to manipulate perceptions, draw social divides, and legitimize violence. In Malaysia, where identity politics and ethno-religious dimensions are deeply embedded in public discourse, extremist actors have leveraged these themes to fuel social division and establish their ideologies.

This country report presents key findings from research on Malaysia's online media and information environment, with a focus on how online extremist networks operate, the challenges faced by practitioners and policymakers in responding, and emerging opportunities to counter online extremism. The report examines the strategies extremists use to exploit public platforms such as TikTok, Instagram, and X (formerly Twitter) for narrative dissemination, while using encrypted applications like Telegram and WhatsApp for recruitment, planning, and coordination purposes. It also highlights emerging trends in the use of ecosystems by extremists globally to preempt the issue from arising in Malaysia.

Finally, the report considers current responses — including legislative frameworks, platform regulation, and multi-stakeholder cooperation—and the critical roles of both government and civil society in promoting media literacy, countering harmful narratives, and building digital resilience. Special attention is given to initiatives that empower youth, women, and marginalized communities, recognizing their unique potential in creating sustainable and contextualized counter extremism strategies. Findings and lessons learned from this research are aimed at supporting the existing response mechanisms to online extremism in the country, as well as informing any future work in the field.

2. METHODOLOGY

2. Methodology

To support future online counter extremism activities in Malaysia, this research sought to identify existing good practices as well as present and emerging trends and challenges. This section details the methodology used for this qualitative study of the needs, challenges and lessons learned identified by frontline practitioners of countering extremism and violent extremism online and other relevant key stakeholders.

Research Objectives & Questions

The overarching objective of this Country Report is to produce evidence-based research on the information and media landscape in the contexts studied, how extremist groups are acting within that landscape, and what the needs identified to respond to the challenge of online extremism are based on both literature and frontline practitioner expertise. The overarching research questions for the project were as follows:

- What lessons, challenges, responses, and needs are identified by frontline actors working to prevent and counter extremism and extremism online?
- How does the existing media and information landscape contribute to the dissemination of dangerous content through online platforms?
- What emerging trends related to the online ecosystem do frontline actors identify, and see as being most important to address?

Research Approach & Methodology

Hedayah, in collaboration with SEARCCT, conducted a research study in Malaysia to assess the media and information landscape, with a special focus on media and information literacy (MIL) skills as well as the extremist engagement on digital platforms in this country, and vitally, to consider frontline practitioner-identified needs and challenges.

The research methodology included primary qualitative research including semi-structured interviews and focus group discussions with key stakeholders, which included ministries, academics, and civil society actors engaged with youth and with countering extremism and violent extremism (CEVE) or MIL efforts, and secondary research assessing existing literature on the topic.

In summary, the research included the following activities:

- A comprehensive review of existing literature covering the topic of online extremism in Malaysia in the past five years to help identify available data, existing gaps in literature, and validate findings from primary findings
- One focus group discussion (FGD) with key stakeholders such as ministry representatives and civil society organizations in Kuala Lumpur, Malaysia, to gain insights on the perception and attitudes related to the research questions and validate findings from the literature review
- 12 key informant interviews (KIIs) with selected experts to gain additional in-depth perspective and insights related to the research questions and validate findings from both the literature review as well as the focus group discussions

Data Analysis

Utilizing a thematic coding approach, the primary data collected through KIIs and FGD was coded using qualitative analysis software, Dedoose, by a team of coders from the research team (Hedayah and consultant). Coding was conducted based on a deductive approach, working from a codebook developed by the research team. External expert opinion was also sought to validate the findings and themes, which were used to draft this Report.

3. KEY FINDINGS

3. Key Findings

The findings of the research are presented below, breaking down the main research question into three parts. The first section will look at the existing media and information landscape in Malaysia and how it is leveraged by extremists in dissemination of content. The second section will focus on emerging threats in the online space, exploring the most prominent trends and developments. The final section will look at the existing responses from government and non-government actors, as well as the main challenges and key needs identified for future work in the sphere.

3.1. Extremist Exploitation of the Information Landscape

The first section of the report addresses the following research question:

How does the existing media and information landscape contribute to the dissemination of dangerous content through online platforms?

This section investigates the current online landscape in Malaysia based on the insights of local experts as well as existing literature to better understand how extremist organizations are exploiting digital spaces for communication, coordination, recruitment and radicalization.

3.1.1. Online Information Landscape and Extremist Exploitation

Malaysia's highly-connected digital environment - characterized by widespread internet access and social media use - provides fertile ground for extremist exploitation. With estimates as high as 96% of Malaysian youth having online connectivity (MLY11), the country's digital spaces have become increasingly saturated with a range of content, including religious, political, and identity-based narratives. It is also important to recognize that online presence spans across all age groups with "more and more of all the demographics on the internet", indicating a broadening digital landscape (MLY9). Extremist actors have seized this opportunity, adapting their recruitment and propaganda strategies to fit popular platform dynamics in the most effective way and "sow the seeds of radicalism and extremism" among the local population (Satria et al., 2024, p.22). Interviewed experts highlight that location of Malaysia citizens no longer plays a role, with even those residing in rural or remote areas falling prey to radicalization processes through exposure to harmful and extremist content, while also noting that despite online spaces being seen to be growing in popularity as a means for extremists to disseminate information and recruit individuals, some local groups still prefer to apply more traditional and offline methods of recruitment (MLY3).

Extremists, as well as other types of malicious actors, have been exploiting the growing and ever-evolving digital ecosystem to support their activities - spread their narratives, gain more supporters, raise funds, and communicate among members. Their tactics often involve strategically amplifying existing local grievances, such as economic inequality, corruption, and socio-political marginalization and seeking to create or exacerbate social divides through disinformation campaigns, targeted trolling, and "DDoS and web defacement attacks" (Bradley, 2025, p.78). Some experts suggest that mass media outlets are contributing to the problem - clickbait headlines, divisive imagery, and lack of diverse perspectives in coverage of sensitive issues can reinforce existing biases and deepen social divides (Mohd Nor, 2024).

3.1.2. Narratives

Extremist narratives and propaganda remain a persistent challenge globally, including in Malaysia where they serve as powerful tools to radicalize individuals and deepen societal divisions. These narratives are strategically developed and widely disseminated across digital platforms, exploiting local grievances, ethno-religious tensions, and broader global events to justify violence and mobilize support. Interviewees note

that while authorities may dismantle the physical structures of extremist organizations—such as arresting leaders or cutting off financial flows – their ideological presence continues to persist in the online ecosystem (MLY3). Extremists in Malaysia are skillfully using mis- and disinformation, often embedded with local cultural cues and identity politics, to reinforce these narratives and manipulate public opinion. Understanding these evolving local narratives and disinformation tactics is essential for developing effective countermeasures and increasing social resilience.

Local Narratives

In Malaysia, local narratives around identity, religion, and nationalism continue to be the most prominent themes used by extremists. While open calls to violence are not always central to these movements, the narratives they disseminate serve to embed exclusivist ideologies and exacerbate societal tensions and divides. Currently, Malaysia is seeing an increasing in ethno-nationalism intertwined with religious supremacy – these movements, in the Malaysian context, are often referred to as the far-right, and literature highlights that such far-right groups have learned to exploit Malaysia's ethno-religious divides to further their agenda and prominence in the country (Yunus, 2022). Core beliefs of these movements center around both Islamic religion and Malay supremacy, which are sustained through a historical-religious narrative that ties Malay identity to the Middle East (Mustaffa, 2022). Through such narratives, extremist groups undermine anyone who is outside this group, targeting them on digital platforms, as well as those who challenge conservative norms. Their messaging is often found to be amplified through digital "cross-pollination" tactics, where content is shared across multiple accounts and platforms, further embedding and spreading their ideology across the digital landscape. Extremist discourse in Malaysia often revolves around sensitive topics such as race and religion. These themes are frequently manipulated by extremists to build division within communities. As one expert observed, what may seem like a benign expression of identity can quickly grow into supremacist calls for domination (MLY11).

Local narratives in Malaysia have been found to combine identity politics and economic campaigns to propagate their ideology and embed their presence. Malaysian experts highlighted examples of movements like "Buy Muslim First" and businesses such as "Malakat Mall", which emerged under the guise of solidarity with Muslims but masked a deeper goal of economic dominance and exclusion of other groups and religions (MLY1). These campaigns, though often short-lived, have lasting cultural impacts. As one interviewee noted, such movements initially present as harmless identity affirmations but can blur into exclusionary and supremacist politics (ibid). These far-right extremist groups' efforts increasingly seek to adopt institutional and professional fronts to legitimize their ideology. They are leveraging platforms like WhatsApp, Telegram, Facebook, and TikTok to cast wide nets, drawing in moderate followers before identifying and grooming the more ideologically aligned for deeper engagement—mirroring recruitment tactics once used by groups like Jemaah Islamiyah (JI) and Daesh (ibid). The dominance of far-right voices in Malaysia's online space is enforced by digital operatives known as 'cytros' (cyber troopers) and troll armies. These actors deploy swarming tactics to flood discourse, intimidate dissenters, and shift narratives in favor of their extremist agenda. Micro-celebrities and influencers are also enlisted to guide and amplify these efforts, blurring lines between organic opinion and planned propaganda (Mustaffa, 2022).

Experts highlight that in addition to these general ideological narratives, Malaysia's extremist groups are also often seen to be holding deeply patriarchal views, and leverage online spaces to promote traditionalist values. Finally, these groups are also observed to be "othering or marginalizing migrant workers or refugees" — especially Rohingya, Bangladeshi, and Nepalese workers — portraying them as a threat to the Malaysian community and labelling them as "Pendatang Asing Tanpa Izin (PATI)" (illegal immigrants) (ibid, p.17).

Extremist narratives in the Malaysian context are shaped by a variety of ideological elements such as religiously-inspired extremism, ethno-religious nationalism, and gendered authoritarianism. These narratives are frequently propagated through digital platforms. While traditional militant threats persist, another now lies in the normalization of supremacist narratives falsely portrayed as elements of local identity, culture, and faith. In this evolving landscape, the digital sphere has become both a battleground and a breeding ground for ideologies that threaten Malaysia's social cohesion.

Disinformation and Misinformation

Similar to other extremist organizations, extremist groups in Malaysia have increasingly turned to disinformation campaigns to amplify their narratives and manipulate public sentiment in their favor. Extremists' narratives and campaigns in Malaysia are often highly localized, using cultural cues, religious symbolism, and local dialects to resonate deeply with target audiences while evading detection by platform moderators. As mentioned earlier, Malaysia's far-right discourse leverages historical revisionism — glorifying the Malay kingdom and distorting national history — to reinforce nationalist and supremacist ideologies (Mustaffa, 2022). For example, one of the interviewees highlighted a case of misinformation narratives about market takeovers by Rohingya and Bangladeshi migrants in Pasar Borong Selayang, which spread rapidly on social media and ignited public outrage, demonstrating the rapid impact of such digital disinformation (MLY12).

A key driver of online disinformation campaigns are cyber troopers, or cytros – digital activists who enforce and employ tactics such as hate speech, red-tagging, and conspiracy propagation to disrupt local social cohesion and justify discriminatory policies (Mustaffa, 2024). Examples of their activities include targeting of the 2013 general election, where they spread false information about tens of thousands of Bangladeshi nationals who were flown in to vote for the ruling coalition. These narratives led to harassment of individuals perceived as foreigners (Yatid, 2019). While cyber troopers may not necessarily be tied to a particular extremist movement, the outcome of their activities may lead to a more polarized community, leading to extremist and radical ideas. As Malaysia's political landscape evolves, these tactics are likely to persist, posing a continued threat to the local online ecosystem.

Global Affairs Narratives

Exploitation of global affairs as narratives to mobilize support is a long-used tactic by extremist groups worldwide. Currently, extremists in Malaysia are particularly seen to be leveraging conflicts in the Middle East to construct radicalizing narratives that blend emotion, ideology, and perceived logic. According to one interviewed expert, these narratives typically unfold through what can be described as a "four-quadrant radicalization model" (MLY13). The first quadrant, cognitive radicalization, involves the use of global political grievances to logically justify violence ("other people have done this to us" and hence "we" must respond). This is followed by emotive radicalization, where emotional appeals rooted in shared suffering are intensified through religious framing. They leverage references to scriptures and scholarly opinions to compound these sentiments, feeding both cognitive and emotional levels until they combine, potentially leading to action-based radicalization. Exposure to such narratives may be facilitating this process (ibid).

This process is part of what has been termed "Glorecal": a pattern of radicalization that is "locally created, regionally connected, and globally inspired" (ibid). Extremist actors draw inspiration from transnational extremist narratives while forming regional alliances, thereby embedding global issues in local contexts. For instance, Malaysian foreign fighter Mohd Lotfi Ariffin did not explicitly call for violence within Malaysia but urged followers to migrate (hijrah) to Syria, presenting the conflict as a righteous struggle against oppression (Yasin, 2017). Similarly, lone actors influenced by Daesh material and global grievances have launched attacks domestically, demonstrating how international political situations can serve as potent catalysts in Malaysia's extremist landscape (MLY13). Such events can also be leveraged by local groups to strengthen their presence and narratives. For example, the Hizb ut-Tahrir Malaysia (HTM) network rejects secular democracy and Western influences, advocating instead for the establishment of a global Islamic caliphate governed by shariah law (Satria et al., 2024). While the activities and presence of HTM has been partially restricted by the government, the group has shifted its presence online, leveraging global issues, such as the conflict in the Middle East, to mobilize support and reinforce its ideological message in Malaysia (Fakirra, 2024).

3.2. Emerging Threats Online

As elsewhere in the world, frontline practitioners in Malaysia are observing a rapidly evolving online ecosystem in which violent extremist actors are constantly adapting their tactics to new platforms, technologies, and loopholes. These emerging trends range from shifts in platform usage (e.g., the rise of TikTok, Instagram, and encrypted messengers) to novel amplification techniques, fundraising methods, and the exploitation of cutting-edge technologies like online gaming and artificial intelligence. The Malaysian context, with nascent capacity across civil society CEVE groups and a state-driven content regulation approach, shapes how these trends manifest and are addressed. Authorities maintain strict regulatory oversight of overtly terrorist content, yet malign actors have often learned to circumvent controls and outpace the responses of government and civil society. This chapter seeks to answer the following question:

What emerging trends related to the online ecosystem do frontline actors identify and see as being most important to address?

This section considers dominant platform usage and adversarial shifts, amplification mechanisms, financing methods, emerging technologies already in use, and other emerging technologies.

3.2.1. Dominant Platform Usage and Adversarial Shifts

Current Tactics and Platform Use

As elsewhere in the region, Malaysian frontline experts highlight the prominence of social media platforms such as TikTok and Instagram as channels for extremist content dissemination. These visually focused, algorithmic recommender-based platforms have massive youth user bases, making them attractive for propagating narratives. TikTok videos of incendiary religious sermons are popular: "There are some concerns concerning TikTok videos. Sometimes, it's just sermons and speech…For some people, they are just talking, but…[others] see this person spewing hate" (MLY4). Such short-video content can blur the line between passionate dialogue and extremist hate speech, and it easily goes viral on the platform. Another practitioner emphasized TikTok's ubiquity in Malaysia: "TikTok is everywhere. Content creators are almost, like, everyone who has TikTok. How can you fight this?" (MLY3). The ease of content creation on platforms like TikTok (and similarly on Instagram Reels) presents a challenge for authorities: extremist messaging can proliferate rapidly before it is even noticed. These platforms' emphasis on short, catchy content is actively being weaponized to deliver polarizing messages.

Still, practitioners caution against fixating on any one platform as "the source" of disinformation or extremism. As one expert argued, bad actors are platform-agnostic and will "leverage any spaces that they can…they're instrumental actors - they use whatever is available to them. You can't say that one platform has more disinformation, misinformation than others. I think the question we should be asking is what is it about [this] information that makes people so receptive to it?" (MLY12). In other words, TikTok and Instagram may be in the spotlight due to their popularity, but extremists also exploit other platforms in parallel.

In addition to the new(er) platforms, traditional social media and messaging platforms remain in use by extremist actors in Malaysia. Facebook continues to be utilized for extremist discourse, particularly in the form of groups or pages disseminating ultra-conservative or hate-filled narratives under the guise of religious discussion. One interview respondent noted that fake accounts are also commonplace (MLY2). Similarly, short videos (Reels) with rigid religious injunctions are common, and orchestrated networks of fake accounts amplify those messages and shut down dissenting voices. The presence of such fake supporters creates an illusion of consensus and can intimidate or silence moderate viewpoints, thus entrenching extremist ideas in these online communities. Despite Facebook's community standards, religiously framed extremist content in local language and dialects can often slip through, reflecting a moderation gap.

Meanwhile, Telegram has emerged as a platform of choice for closed one-to-many or small group communications. Interviewees pointed out that extremist organizers often push followers from open platforms into closed forums: for example, radical pages on Facebook might post "follow these Telegram channels" to funnel interested individuals into a more secure space (MLY4). One Malaysian practitioner even confessed surprise upon realizing the extent of extremist material on Telegram: "I think [the most popular channel] is Telegram. I just discovered one today [that was] new to me" (MLY11). Research confirms that Telegram is perceived by regional extremist groups as a secure, private hub. For instance, Daesh supporters in Southeast Asia have used Telegram for tightly vetted groups, considering it safer from surveillance than open social media (Mustaffa, 2022; Mohd Nor & El-Muhammady, 2021), and as early as 2021, analysts identified a spectrum of far-right online communities in Southeast Asia operating not only on mainstream platforms like Facebook, X (formerly known as Twitter), and Instagram, but also on more private platforms such as Telegram and Discord (Basha, 2024). As one expert noted, Muhammad Wanndy's approach on Telegram illustrated how "strategic use of language, imagery and the camaraderie which he established" (MLY7), cultivated a sense of belonging and shared purpose. These findings underscore the fact that extremist actors use a multi-platform ecosystem: using public platforms for broad reach and recruitment and then migrating committed or vetted individuals to closed platforms for coordination.

Beyond Telegram and Facebook, other platforms also play roles, especially usage of end-to-end encrypted (E2EE) communication channels. WhatsApp (along with WeChat and other chat apps) is popular in Malaysia and is used for disseminating extremist content in private group chats or broadcast lists. One interviewee confirmed that "Mainly WhatsApp, and encrypted messaging platforms" are popular among extremist groups for engaging their members (MLY1). Malaysian interviewees stressed that savvy extremist groups intentionally avoid mainstream public forums when it comes to sensitive coordination or recruitment, opting instead for encrypted apps to evade surveillance (MLY4). This creates an audience funnel - extremists use public social media to attract initial interest, then move the conversation to encrypted groups (Telegram, WhatsApp, Signal, where radicalization intensifies, along with active recruitment, loyalty tests, and operational planning (or links to offline meetings). In short, frontline practitioners observe that no platform is off-limits: extremist networks use platform-specific strategies, leveraging each channel's unique features and user demographics. TikTok and Instagram offer mass outreach through viral videos; Facebook provides wide reach among general audiences and the ability to form groups; Twitter/X allows rapid coordinated campaigns; and Telegram/WhatsApp/Signal grant privacy for deeper indoctrination.

Amplification Mechanisms

Extremist actors also manipulate amplification mechanisms to maximize their reach and engagement online. In a country like Malaysia with relatively stringent controls on overt extremist content, such tactics are especially important for these actors to avoid rapid removals. As one expert put it, "bad actors will leverage any spaces that they can" (MLY12) and use every trick to ensure their content remains accessible and amplified. Extremists avoid content moderation systems through a variety of techniques. According to recent research, "extremist groups have found ways to avoid detection in spreading radicalized content online by subverting moderation, using AI tools to design multiple variants of propaganda specifically engineered to bypass… techniques put in place by law enforcement" (Wan Rosli, 2024, p. 53f). This might involve automatically generating many slightly altered copies of a video or image so that even if one is flagged, others slip through content filters. Observers in Malaysia concur that such evasion tactics are on the rise, including in local languages and cultural contexts that automated moderation (often tuned for English) may not catch. For example, they may disseminate vernacular or culturally specific propaganda (such as memes in local language or videos with local religious references) which may not trigger global moderation systems as readily, thus flying under the radar until they have gained traction.

Another method is camouflaging extremist content as seemingly benign or mainstream material. Malaysian practitioners pointed to instances of ideological messaging embedded in popular culture formats – what one called the "hijacking [of] popular culture" like gaming (MLY4). A regional example is the use of nasheeds (a genre of religious music) to propagate Daesh ideology on platforms like Facebook, YouTube, and


News
Top Stories
Latest
Politics

Instagram: one network, Upherogy Media, "champions IS ideology through songs" posted publicly, thus evading censorship by using art rather than overt slogans (Hasbi & Mok, 2023, p. 5). Similarly, extremists exploit trends and innocuous hashtags or label their groups with innocuous names to avoid detection by both algorithms and casual observers (Dass, 2025). A Malaysian interviewee described this as remaining "relatable" to the current online culture: extremist content creators will latch onto whatever is trending or familiar to users, so that their content blends in and is more likely to be shared (MLY4). This could mean using trending music, references to Roblox, or memes in their propaganda. Thus, the content carries a subtext of extremist messaging, but the delivery mechanism appears entertaining, thereby bypassing superficial moderation and appealing to a wider audience.

In addition to content camouflage, extremists amplify their reach through coordinated inauthentic behavior, such as deploying networks of fake accounts and bots. As noted earlier, one frontline actor observed that extremists often have "fake accounts that tend to support their argument" (MLY2). By swarming comment sections or boosting posts with likes and shares from multiple fake accounts, they create the impression of widespread agreement or a grassroots movement. This can trick platform algorithms into further promoting the content (since high engagement can be interpreted as popularity rather than manipulation), a loophole in moderation enforcement that focuses primarily on content substance rather than behavioral patterns. The result is a snowball effect: messages get algorithmically amplified, reaching many users before platforms realize that the engagement was artificially generated.

Moreover, extremists take advantage of any gaps in content moderation. Even in Malaysia's tightly regulated space, enforcement is rarely instantaneous. One interviewee suggested that new tactics can often outpace detection efforts, and that subsequently, by the time action is taken, "it is often too late" (MLY2). Extremist actors exploit this window by using ephemeral content (like live videos or stories that disappear) and by rapidly re-posting removed content from new accounts. Live-streaming is a particularly troublesome surface in this regard: "livestreaming is notoriously difficult to police, not only because it is happening live but because spoken word is less easily picked up by detection measures… streams may simply disappear after they end, making it almost impossible to analyze them unless watched in real-time" (Schlegel, 2021, p.6). Additionally, if one account is banned, they often have backup accounts or channels to continue broadcasting, effectively leapfrogging over enforcement and evading deplatforming.

Financing Methods

Frontline actors in Malaysia note that as financial technologies (fintech) evolve, so do the methods by which extremist groups raise, move, and utilize funds. Traditional methods, such as physical cash collection or hawala networks (informal money transfer network), are increasingly supplemented, and in some cases supplanted, by online fundraising, digital transactions, and even gaming-related monetization. In Malaysia's case, the government maintains regulatory oversight of formal financial channels and has outlawed the use of cryptocurrencies through platforms not authorized by the Securities Commission Malaysia. However, extremists find ways around these constraints by exploiting newer platforms and loopholes in the regulatory framework (Zahari et al., 2023).

For example, extremist and terrorist-linked groups have used humanitarian appeals on social media and streaming platforms to solicit donations from the public, posting images and videos of suffering families to evoke sympathy and persuade people to donate, claiming the funds will go to relief efforts. As one researcher put it, "these methods of crowdfunding are now common," with pictures of malnourished children or disaster victims used to gain sympathy and funnel donations to extremist-linked organizations (Zahari et al., 2023, p. 9). In Malaysia and the region, such campaigns might be framed as aid for conflict zones, but some proceeds may be diverted to extremist organizations. The online nature of these appeals allows them to reach large audiences quickly and directly receive funds via platform-integrated payment systems. Enforcement officials often find it challenging to distinguish genuine charity from extremist fundraising without extensive investigation.

With the rise of mobile finance apps, online currency exchanges, and cryptocurrencies, extremist actors also have new channels to move money. Malaysian authorities have observed a surge in interest in foreign-currency exchange apps, cryptocurrency exchanges, and even digital loan applications (Zahari et al., 2023). While Malaysia's regulations limit legal crypto platforms and officially ban cryptocurrency as legal tender in the country, many international apps remain accessible via app stores, a regulatory gap that can create challenges for enforcement capacity. When too many users utilize these platforms, it "challenges the resources of enforcement agencies" (ibid, p.11). Extremist networks can exploit this by sending or receiving funds through semi-regulated apps that operate outside the purview of local financial authorities.

More technologically sophisticated actors turn to the dark web forum to raise and hide funds. On darknet forums hosted on Tor, organizations solicit Bitcoin or Monero donations, run online extortion schemes, or even engage in illicit trade (human trafficking, weapons trade, etc.) to fund their activities (Sulaimarl & De Lang, 2024, p.25). These methods are attractive because crypto transactions can provide a degree of anonymity, and the dark web provides a clandestine marketplace away from law enforcement surveillance. While there is limited data on Southeast Asian extremism via the dark web, the available evidence indicates it exists and is likely to expand in scope in the near future (UNODC, 2020; Sulaimarl & De Lang, 2024). Malaysian extremists so far have not prominently figured in associated terror financing cases on record, but regional watchdogs are wary of this frontier as internet penetration and technical know-how increase. Tor's decentralized and encrypted nature makes jurisdictional enforcement difficult, emphasizing the need for international cooperation and advanced cyber-investigative capabilities.

Recent research has pointed out that online gaming can be used for money laundering and terrorist financing by trading in-game items, selling actual games, or by abusing live-streaming monetization (Lamphere-Englund & Thompson, 2024; White et al, 2024; Lamphere-Englund & White, 2023). For instance, extremists can convert dirty funds into in-game currency or valuable in-game using mules, then trade or sell those to unsuspecting players for real money, thereby "cleaning" the funds. Many games use virtual currency exchanges or player-to-player trading markets that often do not align with anti-money laundering (AML) standards (Kelly, 2021). This lack of scrutiny is a loophole being noticed: there is evidence of extremists exploiting virtual item sales for cryptocurrency or fiat currency (ibid). Additionally, live-streaming platforms linked to gaming (such as Twitch or YouTube Gaming) allow viewers to give donations or "gifts" to streamers. An extremist propagandist might pose as a gaming streamer and receive donations that fund their cause – indeed, there have been instances of far-right actors raising money through streaming while spreading extremist messages (Jost and Sick, 2024; Fielitz, Marcks and Bitzmann, 2023). Even the sales of extremist and terrorist produced standalone games can be used to fundraise, as cases from Hezbollah and proscribed neo-Nazi groups alike show (Lamphere-Englund & Thompson, 2024). For Malaysian extremist actors, tapping into global game marketplaces or the local online gaming scene and livestreaming milieus could become an emerging way to generate funds and reach new audiences discreetly.

3.2.2. Emerging Technologies Already in Use

Frontline actors in Malaysia are also looking ahead to emerging technologies that are creating new frontiers for extremist exploitation. Key areas of concern include online gaming, artificial intelligence (AI), and a grab-bag of other developing technologies such as the metaverse, dark web-hosted sites, and NFTs. These tools and environments did not even figure in violent extremism discourse a decade ago, but today they represent the cutting edge of how extremist influence and operations may expand. Malaysia, as a technologically-connected society with high social media usage and a youthful population, is seen as vulnerable to these trends. Malaysian authorities and civil society acknowledge and are studying these emerging threats (MLY3).

Gaming

The gaming ecosystem – encompassing video games, online multiplayer platforms, and gaming-centric social media – has become a significant new arena for extremist activity. In Malaysia, gaming is extremely popular among youth, with an estimated 15-20 million gamers engaging in everything from mobile games to console titles and e-sports (Newzoo, 2020; ZCOM Engagement Lab, 2023). Frontline observers note that extremists see an opportunity here to embed their narratives into a space where young people's guard might be down. One interviewee suggested a possible emerging trend of attempts to gamify extremism and attract young Malaysians through interactive media. This reflects the reality of a critical emerging threat: extremists are diversifying beyond text and video into the immersive, engaging world of games to radicalize individuals in more subtle (and entertaining) ways. This mirrors global trends over the last 30 years, during which over 150 extremist and terrorist games have been produced, with the majority made in the last five years (Lamphere-Englund & Thompson, 2024).

Beyond dedicated extremist games, there is evidence of extremist exploitation of mainstream gaming platforms and cultures. According to recent research, many gaming and gaming-adjacent platforms (like Steam) have limited moderation of extremist content, and have not historically been under the same scrutiny as social media platforms (Lamphere-Englund & White, 2023). Extremist actors can exploit in-game communication features and gaming community hubs as channels for recruitment and propaganda. Attention is shifting to those exploits, especially amid regulatory scrutiny in Singapore following the arrests of two young people in the country who created Daesh training scenarios in Roblox during 2023 (Singapore Ministry of Home Affairs, 2023). Notably, "in-game chats are often less moderated than other social media platforms and unencrypted messaging apps" (Lamphere-Englund & White, 2023, p.19), providing a covert way to disseminate ideology during gameplay. A multiplayer session in a popular game can become an avenue for a terrorist recruiter, or simply an ideologically inspired individual, to befriend a younger player under the guise of gaming camaraderie. After first contact is established, they may move the conversation to encrypted or more private channels such as Discord, helping to radicalize and isolate the individual (Kilmer & Kowert, 2024). Similarly, voice chats on games or services like PlayStation Network can be even harder to monitor than text, and security agencies have noted this challenge – audio communication "leaves less evidence that can be traced… [it] is believed by some to be even more difficult to monitor than private chats on WhatsApp" (Schlegel, 2021, p.7). A chilling real-world parallel was the suspicion that the perpetrators of the November 2015 Paris terrorist attack may have used the PlayStation network's voice chat to coordinate, thus evading detection (ibid, 2021). For Malaysia, with an ever-expanding gaming community, such possibilities cannot be ignored.

Extremist use of gaming manifests in multiple ways: from producing their own video games or modifications with extremist storylines, infiltrating in-game chat and forums, using gaming-adjacent platforms (like Discord servers dedicated to specific titles) to spread propaganda, referencing gaming culture in their memes and recruitment pitches, and even employing gamification to incentivize extremist engagement (Schlegel, 2021; Lamphere-Englund & White, 2023). Interviewees in Malaysia highlighted how the boundaries between gaming communities and general social media are blurring. One noted that TikTok has become popular for gamers to livestream and share content in Malaysia (MLY4). This means extremist content seeded in gaming circles can quickly jump to mainstream platforms and vice versa. As the interviewee explained, different youth subcultures (gamers and non-gamers) interact heavily online, so if extremists target a message to gamers, it can nonetheless spill over to a wider audience because "that group is also interacting with other groups" (MLY4). For instance, a meme originating in a gaming forum with subtle extremist undertones might end up trending on X or Facebook. Critically, with an estimated 85% of youth in Malaysia playing some form of video games, targeting gamers is an apt tactic for extremist groups seeking to reach a core recruitment demographic (ZCOM Engagement Lab, 2023).

One particular trend mentioned by practitioners is the prominence of sandbox game platforms, especially Roblox, in the region. Roblox, an online game platform popular with children and teens, allows users to create and share their own mini-games and interviewees noted its potential impacts on this young audience (MLY4). Elsewhere, white supremacist actors have recreated internment camps and terrorist attacks, while the aforementioned Daesh cases from Singapore demonstrate the ideological spread on the platform (Mahmoud,

2023; ADL, 2024). Roblox and similar platforms, such as Minecraft, can host games that, for example, simulate a conflict with religious or racial overtones or that glorify a militant hero, thereby planting seeds of extremist ideology in impressionable minds under the guise of play. The gamification of extremist propaganda can make it more palatable and engaging: it hijacks popular culture and entertainment for nefarious ends. As one interviewee observed, "Gaming used to be a niche area, but it has become mainstream. So, it's like hijacking popular culture" (MLY4). Extremist and terrorist propagandists latch onto whatever is popular and inject their ideas, knowing it is a way to reach a mass audience.

Artificial Intelligence

Malaysian frontline actors are, along with their global counterparts, very aware of the hype around generative AI. New AI models offer powerful tools that can be exploited by extremists, but can also contribute to prevention efforts. Currently, generative AI tools (which create text, images, video, or audio) are becoming more easily accessible, and extremist actors have begun experimenting with them to enhance their propaganda, while analytical AI (data analytics, algorithms) can help them micro-target and automate aspects of recruitment. One interviewee, reflecting on national security implications, noted ongoing national discussions about the potential role of AI in radicalization, recruitment and financing (MLY3), which is further reflected in the Malaysian government's AI development roadmap. This proactive stance is vital, with research indicating that terrorist groups are utilizing generative AI to enhance and spread their propaganda, making it more efficient and tailored to specific audiences, for example, by creating synthetic images, videos, or audio that intensify their messages and manipulate emotions (Sulaimarl & De Lang, 2024). A vivid example raised by a Malaysian respondent involved deepfakes of religious figures: "They use faces of mullahs, you see deepfakes – Mullahs' mouth opening and talking… but it's basically a deepfake, [with] fake accounts" (MLY2). In this case, extremists created a video where a respected mullah appears to say something he never actually said – likely endorsing an extreme viewpoint – in order to deceive viewers. This underscores the urgency of public awareness about the origins and intent behind online materials, as one expert pointed out – "people need to be aware of how some contents have been created" (MLY9).

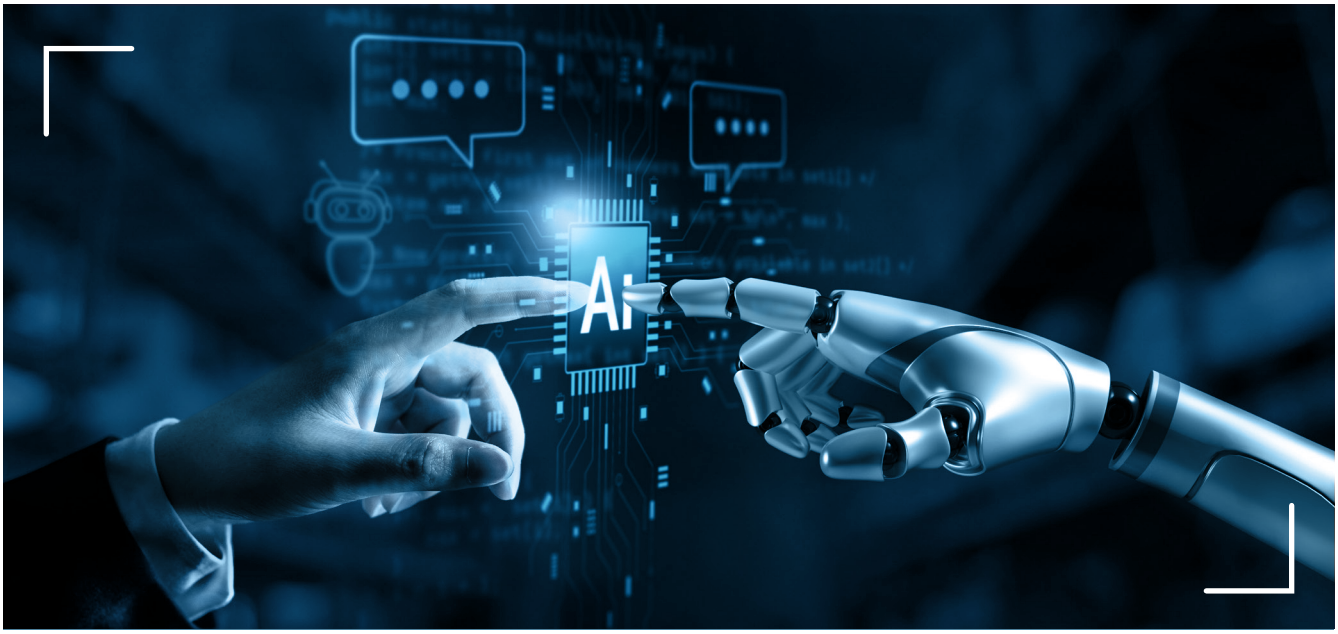
Similar tactics elsewhere in Southeast Asia are also accelerating. AI may also enable hyper-personalization of propaganda and recruitment. As one study describes, AI-driven natural language generation and companion AI bots can craft persuasive text or messages "that resonate deeply with specific individuals… enabling terrorists to customize their textual narratives, strategically catering to the unique interests and convictions of their target audience. Moreover, AI can scrutinize publicly accessible data on individuals to formulate highly personalized recruitment tactics, tailoring messaging to align with the pre-existing beliefs and grievances of the individual (Ismaizam, 2023, p.163). In practical terms, an extremist propagandist could use AI to analyze a Malaysian youth's social media profiles and generate a message or pre-trained chatbot interaction that speaks directly to that youth's profile (whether that may be referencing their favorite football team or using a tone that matches theirs). Similarly, there is speculation that sophisticated chatbots (using large language models similar to ChatGPT) could converse with users, mimicking human recruiters and indoctrinating users (Sulaimarl & De Lang, 2024; Ismaizam, 2023). This level of personalization, at scale, would have been prohibitively labor-intensive in the past, but AI may make it possible. Such scenarios are not mainstream yet but are flagged by experts as a potential threat.

However, some frontline experts urge a measured view on AI, warning against overstating its current capabilities or overlooking simpler, ongoing problems. One expert contended that "trying to say that it [the current threat] is singularly AI is a misrepresentation" (MLY12). In short, AI on its own is not a magic bullet for extremist actors: the content still must tap into existing prejudices or misinformation. The same expert observed that we might be "putting too much stock on AI being that effective" because, in practice, many AI outputs are often of low quality – e.g., absurd images with "six fingers" that savvy viewers will "laugh off" (ibid). They noted that many extremists in Malaysia are still just using basic Photoshop, clip art, or memes to spread messages; these "cheap fakes" and low-tech manipulations remain effective. This perspective is important. We should not neglect effective conventional propaganda methods while fixating on the trending AI hype, nor should we overemphasize the potential for abuse of AI over its positive potential for counter extremism efforts.

Nevertheless, AI's role in online extremism is likely to grow in the short term and must be proactively addressed (MLY3, MLY12). ASEAN security experts have explicitly highlighted that online recruitment and funding are being aided by AI, which makes detection more challenging (Wan Rosli, 2024). We can expect to see more "fully synthetic propaganda" – content entirely generated by AI, including text, voice, imagery, and even video games – as well as "personalized propaganda" finely tuned to audience demographics (Wan Rosli, 2024, p.53).

Other Emerging Technologies (including metaverse, dark web, NFTs)

Beyond gaming and AI, several other emerging technologies are on the radar of both practitioners and researchers as potential game-changers in the extremist online ecosystem. These include immersive virtual environments (often dubbed the metaverse), the dark web, and new digital assets like non-fungible tokens (NFTs). Each of these presents unique opportunities – and challenges – for extremist exploitation, and while they may not yet be front and center in Malaysia's violent extremism landscape, frontline actors believe it is important to stay ahead of the curve. A recent study suggests that extended or virtual reality (XR/VR) could enable realistic training and even virtual planning or rehearsals of attacks (Hunter et al., 2024, p.106). Additionally, many metaverse platforms plan to have integrated digital economies, often built on cryptocurrencies and NFTs for ownership of virtual goods. This creates new channels for moving money. As one analysis highlights, the emergence of crypto and NFTs may "serve as the foundation" for how organizations can use the metaverse to move money and generate revenue (ibid, p.106). Similarly to financing via games, an extremist group could potentially purchase virtual real estate or NFTs and then resell them to launder money, or set up fake "events" in the metaverse where entry requires a donation in cryptocurrency. At present, Malaysia's terrorist, violent extremist, and extremist realm has not notably embraced metaverse platforms (which are still nascent globally), but the forward-looking concern is evident.



3.2.3. Key Priorities for Response

Overall, the online ecosystem for extremist and violent extremist activity in Malaysia is rapidly changing, shaped by global technological shifts and local socio-political dynamics. Frontline actors interviewed for this research identified several emerging trends as most critical to address: the migration to and exploitation of new platforms (especially TikTok, Instagram, and encrypted messengers), the use of clever amplification mechanisms to evade moderation, innovative financing methods leveraging digital tools and gaming, and the widespread adoption of new technologies like gaming and AI as vehicles for extremist influence. These trends do not occur in isolation – they intertwine to create multifaceted challenges. By addressing the emerging online ecosystem(s) holistically and proactively, Malaysia can work to ensure that the digital space becomes harder for extremist actors to abuse and safer for open, inclusive discourse.

3.3. Responses: Past and Future

The final findings section presented in this report will consider the following research question:

What lessons, challenges, responses, and needs are identified by frontline actors working to prevent and counter extremism online?

As such, this section in particular highlights the perspectives of the frontline practitioners and stakeholders who work towards preventing and countering extremism and violent extremism online, and the lessons they have learned, challenges they are experiencing, and subsequent needs they have pinpointed, broken down thematically. Further perspectives from research are incorporated to triangulate results and broaden the discussion.

3.3.1 Existing Responses

This section will outline existing responses positively highlighted by interviewed stakeholders and identified by literature. These include relevant legal frameworks that facilitate counter extremism, violent extremism and terrorism efforts such as content moderation; strategic communication efforts from government and civil society organizations (CSOs); media and information literacy (MIL) efforts.

The frontline practitioners, academic experts and government and CSO stakeholders interviewed for this research varied in their reports on the level of coordination (MLY2, MLY3), including both national and regional cooperation (MLY2), suggesting positive but uneven coordination that may be strong between some related actors in the counter extremism and violent extremism space, but less so amongst others.

Legal Frameworks, Law Enforcement and Content Moderation

Counterterrorism legislation in Malaysia includes various mechanisms ranging from the Prevention of Terrorism Act (POTA) to anti-financing legislation, and elements of the penal code (UNDP, 2022). In late 2024, the Malaysian government announced its Malaysian Action Plan on Preventing and Countering Violent Extremism (MyPCVE) to "boost combating activities and ideologies of terrorists in the country" (Prime Minister's Office of Malaysia, 2024). Content moderation or removal is enabled by various frameworks – research notes "approximately 14 different legislations which can be used to limit freedom of expression" (Mohd Nor, 2023, p.102) including "legislations like the Communications and Multimedia Act 1998 [which] seek to prevent offensive or false material from circulating online, including extremist content" (Yunus, 2022, p.12). Recent frameworks have also incorporated a digital resilience approach, which is "embedded as an aspiration under Strategies 26 to 28 of the recent National Security Policy, as well as the impending NAP on P/CVE" (ibid, 2022, p.15) and has been further advanced by a proposed "Digital Resilience Initiative (DRI) framework that aims to prevent and counter violent extremism in the digital realm" (The Star, 2023) which emphasizes "awareness and knowledge, support and empowerment, regulation and accountability, and cooperation and collaboration" (Wei, 2023, p.136).

Interviewees outlined that moderating power rests with both police and with the Malaysian Communications and Multimedia Commission (MCMC) [1], and many applauded the countering online extremism and counter mis- and disinformation efforts of the MCMC (ML3, MLY4). The Royal Malaysian Police also engages in online monitoring and detection of extremist, violent extremist, and terrorist content on social media and online, led by its counterterrorism division (MLY3). Research notes investigations into Daesh and al Qaeda linked accounts in particular (Satria et al., 2024). Interviewees noted that Malaysia's government and law enforcement takes an active approach to monitoring, investigation and, when needed, arrests and prosecution regarding extremist, violent extremist, and terrorist content on social media and online, and are perceived to be 'clamping down' on this content on platforms like TikTok (MLY11, MLY1, MLY2).

Countering Extremist and Violent Extremist (CEVE) Narratives

Malaysia's counter extremism and violent extremism efforts include a strong strategic communications focus that is well documented in literature and evidenced by various initiatives.

> "Malaysia's National Unity Blueprint 2021-2030 [...] aims to strengthen national unity through inclusive policies and programmes. The blueprint emphasizes the importance of dialogue and engagement with various ethnic and religious communities, reflecting a diplomatic approach to fostering understanding and tolerance. By promoting dialogue and collaboration, Malaysia seeks to address the root causes of hate speech and create a more cohesive society. This diplomatic approach is further bolstered through the Malaysia MADANI national framework introduced by Anwar Ibrahim" (Mohd Nor, 2024, p.54).

Various actors have been noted as undertaking counter or alternative narrative campaigns and public awareness campaigns with counter extremism goals, including the Royal Malaysian Police, the Department of Islamic Development of Malaysia (JAKIM), and various civil society organizations (Jani, 2017). These include the Counter-Messaging Centre (CMC) under the Ministry of Home Affairs [and] the Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT)" (ibid, p.9).

SEARCCT, in particular, has led various youth-focused campaigns, lectures, and digital media initiatives to counter extremism and violent extremism and hate speech online, using strategic communications and creative content to promote tolerance and prevent radicalization (Yunus, 2022; Mohd Nor, 2024; Yusof et al., 2021; UNDP, 2022). SEARCCT has conducted programs aimed at preventing radicalization in society and among the youth, such as the University Lecture Series (ULS), which has engaged approximately 9,000 students from across Malaysia (Mohd Nor, 2024, p.67). Initiatives at SEARCCT also include the development of strategic communications campaigns designed to dispel online VE narratives, as well as promoting public awareness among youths (Yunus, 2022, p.12).

SEARCCT has further advanced creative content campaigns to inspire grassroots youth participation. Notable examples include the Targeting and Preventing Extremism for Youths (TAPESTRY) initiative, which trained students to produce and disseminate mobile-generated counter-narrative content (UNDP, 2022, p.52), and the Hebat Youth Positive Expressions (HYPE) campaign, a content creation campaign that aimed to encourage Malaysian youth to formulate creative community-based solutions in order to address potential drivers of radicalization such as intolerance and racial prejudice (ibid, p.56). Another standout initiative is the #SenjataSaya (Translation: #MyWeaponIs) campaign under the Malaysian Voices Opposing Violent Extremism (MOVE) banner, where SEARCCT collaborated with local influencers which sought to redefine the word "weapon" into something more positive (ibid, p.57).

1 "The Malaysian Communications and Multimedia Commission (MCMC) is a statutory body established under the Malaysian Communications and Multimedia Commission Act (1998). MCMC regulates and promotes the communications and multimedia industry development, including telecommunications, broadcasting, postal services, and digital signature." (Wan Ahmad Dahlan 2021, 12).

Other efforts have also included a number of resources or knowledge sharing platforms – for example, the International Institute of Islamic Thought and Civilization (ISTAC-IIUM) together with the Malaysian Press Institute (MPI) and SEARCCT have launched MyCVEGuide, an online repository of P/CVE resources for journalists and researchers [and] UNDP Malaysia and SEARCCT [...] a handbook for media practitioners to guide reporting on preventing VE through the promotion of social cohesion (Yunus, 2022, p.14).

Research notes that Malaysia has "sought to promote a more moderate and inclusive version of Islam through the concept of Rahmatan Lil 'Alamin (Mercy to all Creations)" (Yunus, 2022, p.12) in countering the narratives of groups like Daesh or al Qaeda. Further, as noted earlier, Malaysia has taken a proactive 'digital resilience' approach. Research demonstrates that the reach and impact of counternarratives are complex, and while they can be powerful they can also be counterproductive if poorly received; therefore, any effective strategic communications efforts must not only seek to 'counter' narratives but also to build resilience to those narratives – fortunately, as one articles notes, "stakeholders are looking into a more long-term and sustainable solution, which is to empower communities to be digitally resilient" (ibid, p.14), such as the proposed Digital Resilience Initiative (DRI) framework (see Section 3.1.1. above).

Civil society efforts in prevention and countering extremism and violent extremism have historically been relatively rare and limited, but recent increased funding opportunities and a growing focus on prevention and resilience building have increased this space and the possibilities for CSO-led efforts to complement government initiatives (Yunus, 2022). Research has found that "Local CSOs have fared particularly strongly in terms of education, dialogue and awareness raising initiatives to counter extremism, as well as championing issues like governance, development and human rights, which altogether help mitigate the structural drivers or grievances leading to VE" (ibid, p.13). Examples of notable efforts have included:

- "The Malaysian Islamic Youth Movement (ABIM) has enjoyed success on this front, leveraging its vast network of followers nationwide to detect and prevent radicalization online and offline, mainly by reinforcing moderate Islamic ideals. In 2021, ABIM collaborated with the Ministry of Youth and Sports to develop a guidebook and webinar series on preventing extremism among youths. IKRAM is another popular Muslim NGO that promotes healthy religious discourse and seeks to correct the distorted perceptions of jihad in IS' online messaging. Amidst the pandemic, community actors played another crucial role as fact-checkers against virus disinformation and ensuring information accessibility among vulnerable populations like migrants and refugees" (Yunus, 2022, p.13);
- The "Young Leaders for Online Preventing and Countering Violent Extremism (PCVE) in Southeast Asia" project by United Nations Office of Counter-Terrorism (UNOCT)/United Nations Counter Terrorism Centre's (UNCCT) Global Programme on PCVE ran from June 2023 to June 2024 in Indonesia, Malaysia, the Philippines and Thailand "to develop locally-tailored PCVE strategic communication campaigns, and to equip these same young people to sustainably build the capacity of their peers" (Roberts & Matsushima, 2024, p.7);
- "The Malaysian Youth Council [which] hosts online forums, workshops and campaigns to address radicalization and foster social cohesion among young people" (Cabanes Ragandang, 2024, p.31);
- "The Islamic Youth Movement (ABIM) and the Global Movement of Moderates (GMM) [who] combined to form a task force to counter IS ideology from as early as September 2014. Since the establishment of the task force, ABIM and GMM have produced posters and short videos that aim to create public awareness on extremist narratives and prevent youths from joining terrorist groups" (Jani, 2017, p.8).

These civil society efforts - while positive - remain overall relatively small in scale, emphasizing potential for further collaboration and complementary work.

Developing Media & Information Literacy (MIL)

Malaysia has a strategy for media literacy in high school and university contexts, with the involvement of ministries such as the Ministry of Education, Ministry of Youth and Sports, and Ministry of Higher Education. However, the approach is designed not to have a specific curriculum for media literacy – there is no MIL education in the formal education curriculum (Yee & Shyh, 2024, p.345) - but to integrate these ideas across existing activities and subjects (MLY2). However, Malaysia has integrated digital skills in the national curriculum, with a focus on digital competencies which includes media and information literacy (Subramaniam, 2023, p.24). I

Interviewees also noted critical thinking modules at university level (MLY3), and research highlights a number of broader initiatives, such as the JomCheck alliance (an academic, media and civil society alliance in Malaysia to mitigate harms of misinformation) whose partners – "such as independent educational groups like Arus Academy, the Media Education For All (ME4A) movement, and the Society of Media and Information Literacy Educators (SMILE)" (Kwan Yee Kow, 2024) have conducted youth training and workshops; along with media literacy initiatives such as "the "Countering misinformation" initiative by FaqCheck Lab, the #KitaBukanKami campaign by IDEAS and Imagined Malaysia and "counter-narrative campaigns, aimed at combating harmful or intolerant narratives, by the Initiative to Promote Tolerance and Prevent Violence" (Shamsuddin, 2022, p.4).

3.3.2. Key Challenges, Needs and Lessons Learned

This section draws on both primary research conducted for this Report and related literature on the Malaysian context to highlight expert and practitioner perspectives on key challenges, needs, and lessons learned in preventing extremism and violent extremism online in Malaysia today. Key challenges and concerns highlighted varied, but included how to ensure balanced and effective content moderation, how to strengthen media and information literacy (MIL) and digital literacy, how to strengthen and increase coordination and ensure inclusive approaches to prevention, and how to leverage research and evidence to understand needs and tailor responses. Interviewees highlighted various areas where gaps in resourcing or knowledge could be addressed. These included funding to not only conduct research but translate its results into actionable programming and policy efforts (MLY12), calls for validated tools or metrics to measure radicalization (MLY3), and to broadly continue to develop the base of local expertise for counter extremism and prevention efforts (MLY12).

Addressing Content Moderation Challenges

"People need to be realistic about the fact that you can't take down everything that's online." (MLY1)

Broader challenges in content moderation – such as its inability to identify and understand "linguistic and cultural nuances, such as humor or codes (dog whistles)" (UNICRI & UNCCT, 2021, p.30; Mustaffa, 2022, p.4), often resulting in removal delays (Leong & Loh, 2025,) – were identified in literature on the Malaysian context, however more specifically, balanced moderation approaches as well as coordination for moderation efforts were key challenges identified by this research.

Interviews and literature both highlight the need to strike a balance between security and other impetuses, emphasizing the need for moderating extremist or violent extremist content but also for allowing youth, and society more broadly, freedom to engage online and have positive debate (MLY1, MLY2, MLY11).

Research has noted that, in Malaysia, the "laws limiting freedom of expression to combat hate speech are vague" and that "these problems of definition (or lack thereof) can cause arbitrary restrictions of speech" (Mohd Nor, 2023, p.102). Multiple interviewees flagged the challenges posed by the Sedition Act, which some felt was designed to be very punitive and could be applied very broadly (MLY1, MLY12). Research has also noted that the use of this legislation to address hate speech may be inadequate for "cultivating digital resilience" and highlight a need for attention to the delicate balance of preserving security and national values

and upholding human rights (Wei, 2023); further, that its application can be uneven (Muhaimi, 2022). Similarly, the Communications and Multimedia Act 1988 has been described as being "used in an expansive manner" (Gilder, 2022, p.295). Social media platforms have also been criticized in literature regarding the nature of their response on these issues in the Malaysian context, and for limited engagement on removing or moderating hate speech content in the region (Mustaffa, 2022), efforts towards which have been called "inconsistent" (Liu, 2023, p.549f.).

Literature has also identified coordination challenges in moderation efforts between government, broader media and civil society, and individual tech companies or platforms (Mohd Nor, 2023; Mustaffa, 2024; Gilder, 2022; Liu, 2023). It is important to note that engagement with all such platforms cannot be uniformly characterized, as many have flagged that engagement, approach and coordination varies from one platform to another. Interviewees emphasized challenges such as limited understanding of content moderation and its complexities – a challenge across many contexts – as well as a common strong outcome focus (i.e. how much content is taken down how quickly) over process (considering how content is identified, who may be affected by its moderation) by some Malaysian actors in considering the effectiveness of moderation (MLY12). A need for more linguistic capacity, as well as training to address biases among moderators (MLY3), was also highlighted, with multiple examples of how coded language in local dialects or contextual narratives were able to evade detection by moderation noted (MLY12, MLY1). Continuing to develop and increase local expertise to identify, understand and address these narratives was also recommended (MLY3), as was the need for further support mechanisms for policymakers and law enforcement in preventing extremism online (MLY12). Others highlighted that engagement with CSOs and experts in moderation processes would strengthen content moderation and inclusivity, as these are key actors in keeping digital spaces safe (ibid).

Building Media & Information Literacy

There is contrasting information in the literature, and in the perspectives of interviewees, on the general levels of media and information literacy (MIL) and digital literacy in Malaysia, and its implications are mixed. Literature highlights challenges among Malaysian users in differentiating real news from mis- or disinformation (Yatid, 2019, p.215), but conversely notes high levels of digital literacy (Dass, 2025), both potential contributors in different ways to online radicalization.

Literature noted fact checking and anti-misinformation efforts with relatively wide reach, but emphasized the need for concurrent trust-building and whole of society engagement to increase their effectiveness (Yatid 2019, p.217). Research also notes that forms of MIL education that actively involves students in media production can help to develop their "critical analytical, creative, and argumentation skills while promoting tolerance in society" (Yee & Shyh, 2024, p.345) and thus is recommended for future MIL efforts, and that "public awareness on topics such as violent extremism and hate speech needs to be improved [and] incorporating these topics into the educational syllabus may be a viable option" (Dass, 2025). In this environment, developing "a critical mind" (MLY9) becomes essential, not just for youth but for all internet users. Looking at AI, interviewed experts cautioned that many people are using AI without understanding its limitations or how it may perpetuate negative stereotypes or biased worldviews (MLY7). Additionally, educational responses remain limited, as while current modules tend to focus primarily on fake news (MLY7), there is a need for a more holistic media and information literacy framework – one that addresses hate speech, its impact, and how to critically engage with such content.

Interviewees noted the need to start this kind of education from school age (MLY11) through to universities, but for university-level efforts did not advocate adding it to core curricula, but rather finding ways to build these skills through extracurricular efforts or existing platforms or non-core topics (MLY11, MLY4). Further, they highlighted the need for these efforts to take into account new developments in technology, such as artificial intelligence and gaming (MLY4), and for engaging with civil society and grassroots organizations, including religious actors (MLY2), both to design and implement such initiatives in order to increase their impact (MLY4, MLY12).

Strengthening Coordination

Both literature and interviewees highlight the importance of coordination within government, but also with a broader range of actors in society and regionally (Habulan et al., 2018; Fernandez, 2022) to support efforts to prevent and counter extremism and violent extremism, but also note a range of challenges. As one interviewed expert observed, while there are many good campaigns, "it is not centralized" (MLY8). Literature highlights space for improvement in cooperation between government institutions to decrease overlapping roles and clarify demarcation of responsibilities (Fernandez, 2022; Jani, 2017; Dass, 2025). These gaps points to the urgent need for a more coordinated approach.

CSOs are frequently flagged as key actors, but ones with whom trust building and active coordination are needed (MLY11), and for whom "organizational barriers, such as funding and human resources, are a hurdle [...] in championing PCVE issues" (Shamsuddin, 2022, p.2); they may also be excluded from traditionally state-centered counter extremism and violent extremism efforts (Kamaruzzaman et al., 2023; Mohd Nor, 2024; Shamsuddin, 2022). Literature strongly advocates for increased engagement between CSOs and government to strengthen efforts to prevent and counter extremism, and various interviewees echoed this (MLY2). Further, engaging not only cross-sectorally – with private sector and business, including tech platforms (MLY1) – but also prioritizing interdisciplinary approaches to address the complexity of this challenge (MLY11) was highlighted by interviewees. A whole-of-society approach must also recognize the critical role of families. As one expert pointed out, there is a "lack of understanding for the need for parents and guardians to play a role" (MLY8) in safeguarding youth in the digital space.

Multiple interviewees noted the presence of regional coordination frameworks as well as personal or professional networks to tap into regional knowledge on preventing and countering extremism and violent extremism, but also emphasized the importance and need for continuing to grow and strengthen such mechanisms (MLY12, MLY2). As one author notes, "considering the borderless efforts by IS couched within narratives of a 'global caliphate', the Southeast Asian nations need to work in tandem to counter such narratives through collective countering violent extremism (CVE) and policy-based initiatives geared towards promoting tolerance, moderation and coexistence" (Habulan et al., 2018, p.29). Regional cooperation, including information sharing, was broadly recommended in literature (Habulan et al., 2018, p.29; Fernandez, 2022, p.94). Engagement and coordination at all of these levels strengthens the preventive approaches that are needed to effectively counter extremism and violent extremism but building resilience and preventing radicalization (Shamsuddin, 2022, p.3).

Enhancing Strategic Communications

Interviews highlighted various potential avenues for strengthening strategic communications efforts. These included the need for identifying and engaging relevant stakeholders – i.e. the target audience – in the development of counter or alternative narratives to ensure they are effective, not only by tailoring narratives but by leveraging trusted and credible messengers (MLY4). Many interviewees particularly emphasized the need for understanding audiences and developing customized content (MLY3, MLY4), as well as highlighting a need for more and better counter narratives (MLY1, MLY2), suggesting a need for more innovative and engaging content (MLY2). Even when initiatives are well-intentioned, they may "lack the right packaging" (MLY7), limiting their ability to effectively reach and resonate with target audiences. Increased training and resources to support this was suggested, including training community actors on how to develop narratives and use innovative tools but also for strategic communications practitioners to enable use of new technologies like artificial intelligence (MLY1).

The need for resourcing to create content in a wider range of languages in order to reach a broader audience was also highlighted as particularly relevant in the linguistically diverse Malaysian context (MLY11), suggesting a further need to engage community actors to create effective counter or alternative narratives in their own language to broaden reach and impact.

Understanding Needs, Ensuring Inclusive Approaches

Literature emphasizes the importance of understanding how youth are engaging online to inform effective responses (Ismail et al., 2022), and interviewees echoed that a focus on youth agency and empowerment in prevention processes (MLY11) and understanding their motivations and providing positive avenues for engaging and finding meaning was critical to support these efforts (MLY4), including not only developing strategic communications content but moderating it (MLY2). However, other interviewees noted that while this was an effective approach, it could be a very resource intensive one (MLY1) and needed to be led by a do-no-harm approach (MLY4), and that youth needed training and expert guidance to do this effectively and safely (MLY1, MLY4). One interviewee highlighted that most young people who witness harmful content online do not report it unless personally affected (MLY7), but it is worth noting that even exposure to such content may influence attitudes. This underscores the importance of adopting inclusive and participatory approaches – ones that not only empower but equip youth with the skills to recognize, resist, and respond to harmful content.

Gender is also a key lens when considering how to ensure prevention efforts are effective. Extremism and violent extremism are gendered phenomena, and research has indicated that women in Malaysia had more grievances than men in this context, making them potentially more vulnerable to violent extremist content or radicalization (Wei, 2023). Literature on the intersection of gender and extremism in the Malaysian context recommends specific collaboration between CSOs and relevant Ministries (in particular the Ministry of Women, Family and Community Development) to build digital resilience among women (ibid, 2023). Interviewees emphasized the need for inclusion and for greater engagement of a wide range of diverse stakeholders – including women, youth, cultural groups, and indigenous actors, for example (MLY3, MLY2, MLY4, MLY12). Interviewees also emphasized the important role of female experts and practitioners in counter extremism disciplines and advocated strengthening efforts to support them (MLY12), highlighting that more diverse perspectives strengthen policy and programming (MLY4). Overall, a strong argument for holistic, whole-of-society approaches as a foundation for resilience and prevention emerged from interviews and literature.

Interviewees further cautioned over-emphasis on the online components of radicalization and extremism, noting that offline elements also play a key role and highlighting the complexity of this issue (MLY12). Finally, interviewees highlighted that monitoring and evaluation was a critical tool in efforts to understand needs of diverse stakeholders and to avoid siloed responses (MLY11), and further, to assess the effectiveness of policy and programming (MLY4). Interviewees highlighted that monitoring and evaluation can be a powerful tool to identify lessons learned, citing examples of cases where this helped to identify approaches that had not worked as intended (MLY1).

4. RECOMMENDATIONS

4. Recommendations

Building on the wide range of challenges, threats, lessons, needs and opportunities identified by Malaysian practitioners, government, civil society and academics in this research, this section provides recommendations which highlight areas for potential focus or action to continue to strengthen counter extremism efforts in today's media and information landscape.

Contextualized approaches to countering extremism are needed, and global lessons and trends can inform local prevention

Understanding extremist narratives in Malaysia requires a nuanced, context-specific approach. Analysts and policymakers must therefore assess narratives and dynamics within the socio-political and historical framework in which they emerge (MLY3). However, while each context is unique, emerging trends playing out in other parts of the world or in neighboring countries can point to the kinds of challenges or issues that prevention efforts may need to grapple with in future. Policy makers and practitioners should keep a close eye on developments in the digital sphere around the world to preempt new tactics from being employed in the Malaysian context. Regional coordination, and private sector engagement, are particularly vital in a proactive approach to countering emerging threats.

Balancing online and offline efforts is vital to effectively combat extremism, and employing different 'toolkits' to counter online extremism will strengthen efforts

As radicalization processes rarely happen solely online, and experts note the presence of radicalization dynamics offline, approaches that consider resilience to online extremism holistically are most likely to be effective. This may mean supplementing media and information literacy with 'AI' or digital literacy; it may look like traditional media messaging combined with social media; it could embed efforts to build resilience to extremist narratives not only in online forums but in offline spaces like formal and informal education. Similarly, ensuring that there is a focus on resilience building and prevention efforts, equipping society with the tools to encounter extremist content or narratives and not be drawn in, in combination with content moderation efforts to reduce their likelihood of encountering malicious content, will strengthen efforts overall. Content moderation can be informed by both a security and a resilience lens, and experts and practitioners emphasized the need to balance security concerns with creating online spaces that promote dialogue, engagement and social cohesion.

Gaming is an emerging front in counter extremism, and engagement with platforms and enhancing digital literacy are key

Malaysian counter extremism practitioners can build on recent efforts by engaging gaming communities and companies to promote digital literacy, self-regulation, and inclusive youth-led initiatives that increase resilience and counter extremism in online spaces. Gaming has not been a major focus of existing efforts, though there are positive new efforts led by SEARCCT. Given the trends highlighted in this Report, stakeholders need to engage with gaming companies and communities to raise awareness and encourage self-regulation, resilience building, and community moderation. This challenge also calls for enhancing digital literacy among youth, and teaching young gamers to recognize when someone is trying to manipulate or radicalize. Community organizations could create programs that involve gamers in positive, inclusive campaigns. Youth-driven counter-narratives and media literacy initiatives were noted by interviewees as showing promise - empowering young gamers in the same way could be a powerful tool against extremism online.

Artificial Intelligence (AI) presents threats but also opportunities

Malaysia, as a country that is quickly adopting AI in various sectors, is likely to need to find ways to incorporate counter extremism and violent extremism safeguards into its digital strategy, such as investing in AI tools to detect deepfakes and bot-driven influence campaigns; monitoring using LLM-based tools; training law enforcement and analysts in AI literacy; and promoting public education campaigns about verifying information (for example, teaching people how to use reverse image searches or AI image detection tools). Interviewees also call for more research on the impact of AI on information flows in the country. Policymakers might support collaborations between tech firms, researchers, and security agencies to study AI-generated extremist content and develop early warning systems. Importantly, this must be balanced with the understanding that older forms of propaganda are still effective – a dual approach is needed that tackles emerging AI threats without losing sight of the baseline propaganda techniques that continue to radicalize individuals daily.

Emphasizing coordination with a wide range of actors can improve outcomes, increase inclusivity, and strengthen resilience

Holistic approaches that can respond to new and emerging threats in both online and offline spaces require coordination and engagement with a wide range of actors. Ongoing efforts to engage and coordinate at national and regional level are critical, leveraging Malaysia's existing expertise in institutions like SEARCCT, MCMC, Ministry of Home Affairs, the Royal Malaysia Police, and other counter extremism actors as well as engaging regionally and globally with tech platforms and regional forums to respond proactively in the face of emerging extremist threats online. Finally, engagement with civil society to support building resilience both online and offline is an important pillar in effective prevention. Such efforts can enhance potential to regulatory and monitoring frameworks when new threats emerge or new technologies mature.

REFERENCES

References

Anti-Defamation League. (2024). Addressing Extremism in Online Games Through Platform Policies [Report]. ADL Center for Technology & Society. https://www.adl.org/resources/report/addressing-extremism-online-games-through-platform-policies

Basha, S. (2024). The creeping influence of the extreme right's meme subculture in Southeast Asia's TikTok community. GNET. https://gnet-research.org/2024/04/08/the-creeping-influence-of-the-extreme-rights-meme-subculture-in-southeast-asias-tiktok-community/

Bernama. (2024). Govt launches MyPCVE Action Plan to Counter Terrorism Intelligence, Extreme Activities. https://www.pmo.gov.my/2024/09/govt-launches-mypcve-action-plan-to-counter-terrorism-intelligence-extreme-activities/

Bradley, A. (2025). Right- and left-wing violent extremist abuse of digital technologies in South America, Africa and Asia. UNICRI. https://unicri.org/Publication-Right-Left-Wing-Violent-Extremist-Digital-Technologies-SouthAmerica-Africa-Asia

Cabanes Ragandang, P. I. (2024). Young people challenging violent extremism online: insights from Asia. GNET. https://gnet-research.org/wp-content/uploads/2024/08/GNET-45-Young-People-Challenging-Extremism_web.pdf

Dass, R. (2025, February 11). The continued threat of online radicalization in Malaysia. The Diplomat. https://thediplomat.com/2025/02/the-continued-threat-of-online-radicalization-in-malaysia/

Fakirra, N. I. (2024). Reassessing the threat of Hizbut Tahrir. In RSIS. https://rsis.edu.sg/wp-content/uploads/2024/06/CO24071.pdf

Fernandez, K. (2022). Reasoning the Need for a National Action Plan to Counter-Violent Extremism in Malaysia in the Post-IS Period: Internet Soul Searching among Muslim Youth. SEARCCT's Selection of Articles 2022, 75-99. https://www.searcct.gov.my/wp-content/uploads/2023/01/SEARCCT-Selection-Of-Articles-2022.pdf

Fielitz, M., Marcks, H. & Bitzmann, H. (2023). "Jeder wirbt für sich allein? Wie auf Telegram der Aufruhr zum Geschäft wird" [Everyone advertises for themselves? How rebellion becomes business on Telegram], Machine Against the Rage, no. 3.

Gilder, A. (2022). "Chapter 14 Contracting Space for Opposing Speech in South East Asia and Restrictions on the Online Freedom of Expression". In The Asian Yearbook of Human Rights and Humanitarian Law, (pp.293–308). Brill. https://doi.org/10.1163/9789004520806_015

Habulan, A., Taufiqurrohman, M., Jani, M. H. B., Bashar, I., Zhi'An, F., & Yasin, N. A. M. (2018). Southeast Asia: Philippines, Indonesia, Malaysia, Myanmar, Thailand, Singapore, Online Extremism. Counter Terrorist Trends and Analyses, 10(1), 7–30. http://www.jstor.org/stable/26349853

Hasbi, A. H. bin M., & Mok, B. (2023). Digital Vacuum: The evolution of IS Central's media outreach in Southeast Asia. Counter Terrorist Trends and Analyses, 15(4), 1–8. https://www.jstor.org/stable/48743372

Hunter, S., d'Amato, A. L., Elson, J. S., Doctor, A. C., & Linnell, A. (2024). The Metaverse as a future threat landscape: An interdisciplinary perspective. Perspectives on Terrorism, 18(2), 100–118. https://www.jstor.org/stable/27315310

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

Ismaizam, M. A. (2023). Malicious use of artificial intelligence by terrorists: Assessing future risks. In Special Issue: Building Digital Resilience In Preventing and Countering Violent Extremism. SEARCCT'S Selection of Articles 2023. 161-165. https://www.searcct.gov.my/wp-content/uploads/2024/08/SOA-2023d.pdf

Jani, M. H. B. (2017). Countering violent extremism in Malaysia: past experience and future prospects. Counter Terrorist Trends and Analyses, 9(6), 6–10. http://www.jstor.org/stable/26351526

Jost, J. and Sick. H. (2024). Cash for Incitement: The Monetisation of Digital Hate in Germany. Global Network on Extremism and Technology (GNET). https://gnet-research.org/2024/05/01/cash-for-incitement-the-monetisation-of-digital-hate-in-germany/

Kamaruzzaman, K. B., Mokhtar, R. a. M., Aziz, A. R. A., Al-Tahitah, A. N. A., & Melhem, I. I. a. B. (2023). Meneroka perspektif menangani ektremisme di Malaysia melalui pendekatan naratif alternatif digital. Malaysian Journal of Social Sciences and Humanities (MJSSH), 8(9), e002525. https://doi.org/10.47405/mjssh.v8i9.2525

Kelly, S. (2021). Money Laundering Through Virtual Worlds of Video Games: Recommendations for a New Approach to AML Regulation. Syracuse Law Review, 71(1487). https://lawreview.syr.edu/wp-content/uploads/2022/01/1487-1512-Kelly.pdf

Kemp, S. (2025). Digital 2025: Malaysia — DataReportal – Global Digital Insights. DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2025-malaysia

Kilmer, E. D. & Rachel K. (2024). Grooming for Violence: Similarities Between Radicalisation and Grooming Processes in Gaming Spaces. GNET. https://gnet-research.org/2024/02/08/grooming-for-violence-similarities-between-radicalisation-and-grooming-processes-in-gaming-spaces/

Kow, K. Y. (2024, May 3). Learning to see through the lies with media literacy. 360info. https://360info.org/learning-to-see-through-the-lies-with-media-literacy/

Lamphere-Englund & White, J. (2023). The Online Gaming ecosystem: Assessing digital socialisation, extremism risks and harms mitigation efforts. GNET. https://gnet-research.org/2023/05/26/the-online-gaming-ecosystem/

Lamphere-Englund, G., & Thompson, E. (2024). 30 years of trends in terrorist and extremist games. GNET. https://gnet-research.org/2024/11/01/30-years-of-trends-in-terrorist-and-extremist-games/

Leong, P. P. Y., & Loh, B. Y. H. (2024). State-sponsored Disinformation through digital media in Malaysia. In Routledge eBooks (pp. 287–301). https://doi.org/10.4324/9781032632940-21

Liu, D. (2024). Borderline content and platformised speech governance: Mapping TikTok's moderation controversies in South and Southeast Asia. Policy & Internet, 16, 543–566. https://doi.org/10.1002/poi3.388

Mahmoud, F. (2023). From Atari to Allahu Akbar: Comparing White Supremacist and Jihadist Uses of Gamified Extremism. GNET. https://gnet-research.org/2023/02/08/from-atari-to-allahu-akbar-comparing-white-supremacist-and-jihadist-uses-of-gamified-extremism/ GNET

Ministry of Home Affairs. (2023, February 21). Issuance of Orders Under the Internal Security Act Against Two Self-Radicalised Singaporean Youths [Press release]. Government of Singapore.

Mohd Nor, M. W., & El-Muhammady, A. (2021). Radicalisation and paramilitary culture: the case of Wanndy's Telegram groups in Malaysia. In Springer eBooks (pp. 95–122). https://doi.org/10.1007/978-981-16-5588-3_6

Mohd Nor, M. W. (2023) All-of-society approach to address hate speech. In Special Issue: Building Digital Resilience In Preventing and Countering Violent Extremism. SEARCCT'S Selection of Articles 2023, 97-107. https://www.searcct.gov.my/wp-content/uploads/2024/08/SOA-2023d.pdf

Mohd Nor, M. W. (2024). From Hate to Hope: A Holistic Approach to address Hate speech. Institute of Diplomacy & Foreign Relations (IDFR). https://www.idfr.gov.my/images/pdf_folder/IDFR_Book-From_Hate_to_HOPE.pdf

Muhaimi, H. (2022). Holistic Recommendations to Tackle Hate Speech, a Driver of Intolerance in Malaysia. INITIATE. MY Policy Brief, No. 3. https://initiate.my/holistic-recommendations-to-tackle-hate-speech-a-growing-intolerance-in-malaysia-2/

Mustaffa, M. (2022). Radical right activities in Nusantara's digital landscape: A snapshot. GNET. https://gnet-research.org/2022/04/19/radical-right-activities-in-nusantaras-digital-landscape-a-snapshot/

Mustaffa, M. (2024). When Opposition is Extremism: The dangers of oversecuritisation and online vigilantism. In ICCT Policy Brief. ICCT. https://icct.nl/sites/default/files/2024-02/Munira_When%20Opposition%20is%20Extremism%20The%20Dangers%20of%20Oversecuritisation%20and%20Online%20Vigilantism_1.pdf

Mustaffa, M. (n.d.). Radical right activities in Nusantara's digital landscape: A snapshot. GNET. https://gnet-research.org/2022/04/19/radical-right-activities-in-nusantaras-digital-landscape-a-snapshot/

Newzoo. (2020, January 30). Insights into Malaysia's games market and its gamers. https://newzoo.com/resources/blog/insights-into-malaysias-games-market-and-its-gamers

Roberts, S., & Matsushima, N. (2024). Young leaders for Online Preventing and Countering Violent Extremism (PCVE) in Southeast Asia. UNOCT. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/yl4pcve_evaluation_report_30_september_2024.pdf

Satria, A., Yeo, K., Dass, R., Bashar, I., Chalermsripinyorat, R., Singam, K. V., & Leong, A. (2024). SOUTHEAST ASIA: Indonesia, Philippines, Malaysia, Myanmar, Thailand, Singapore. Counter Terrorist Trends and Analyses, 16(1), 11–46. https://www.jstor.org/stable/48756305

Schlegel, L. (2021). Extremists' use of gaming (adjacent) platforms: Insights regarding primary and secondary prevention measures. In EUROPEAN COMMISSION Radicalisation Awareness Network. https://home-affairs.ec.europa.eu/system/files/2021-08/ran_extremists_use_gaming_platforms_082021_en.pdf

Shamsuddin, A. (2022). National Action Plan on Preventing and Countering Violent Extremism: Civil Society Deserves a Seat at the Table. INITIATE.MY Policy Brief, No. 1. https://initiate.my/policy-brief-issue-1-2022/

Subramaniam, N. K. (2023). Technology in Education: A case study on Malaysia. UNESCO. https://doi.org/10.54676/qxeg1330

Sulaimarl, N., & De Lang, N. E. (2024). Emerging threats and trends of terrorism and violent extremism online. SEARCCT'S Selection of Articles 2024, 21–29. https://www.searcct.gov.my/wp-content/uploads/2024/12/v4_Draft-SOA-2024-Publisher.pdf

The Star (2023, June 13). Zambry suggests digital resilience initiative to prevent, counter violent extremism. https://www.thestar.com.my/news/nation/2023/06/13/zambry-suggests-digital-resilience-initiative-to-prevent-counter-violent-extremism

UNDP. (2022). Preventing and Countering Violent Extremism (PCVE) in Malaysia: Handbook for Civil Society Organisations (CSOs). https://www.undp.org/malaysia/publications/preventing-and-countering-violent-extremism-pcve-malaysia-handbook-civil-society-organisations-csos

UNICRI & UNCCT. (2021) Countering terrorism online with Artificial Intelligence - An overview for law enforcement and counter-terrorism agencies in South Asia and South-East Asia. https://unicri.org/Publications/Countering-Terrorism-Online-with-Artificial-Intelligence-%20SouthAsia-South-EastAsia

UNODC. (2020). Darknet Cybercrime Threats to Southeast Asia. https://www.unodc.org/roseap/uploads/documents/Publications/2021 Darknet_Cybercrime_Threats_to_Southeast_Asia_report.pdf

Wan Rosli, W. R. (2024). Violent extremism and Artificial intelligence: A Double-Edged Sword in the context of ASEAN. Commonwealth Cyber Journal, 46–48. https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/s3fs-public/2024-06/ccj-2-1-violent-extremism-ai-wan-rosli.pdf

Wei, H. K. (2023). Building digital resilience in Preventing and Countering Violent Extremism. In Special Issue: Building Digital Resilience In Preventing and Countering Violent Extremism. SEARCCT'S Selection of Articles 2023, 136-142. https://www.searcct.gov.my/wp-content/uploads/2024/08/SOA-2023d.pdf

White, J., Wallner, C., Lamphere-Englund, G., Love Frankie, Kowert, R., Schlegel, L., Kingdon, A., Phelan, A., Newhouse, A., Saiz Erausquin, G., & Regeni, P. (2024). Radicalisation through gaming: The role of gendered social identity (Whitehall Report). RUSI. https://www.rusi.org/explore-our-research/publications/whitehall-reports/radicalisation-through-gaming-role-gendered-social-identity

Yasin, N. A. M. (2017). The evolution of online extremism in Malaysia. Counter Terrorist Trends and Analyses, 9(4). https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/RSIS-CTTA%20Volume%209,%20Issue%207.pdf

Yatid, M. M. (2019). Truth Tampering through social media: Malaysia's approach in fighting disinformation & Misinformation. IKAT the Indonesian Journal of Southeast Asian Studies, 2(2), 203. https://doi.org/10.22146/ikat.v2i2.40482

Yee, K. K., & Shyh, T. H. (2024). Problem-Based Learning: Media and Information Literacy Project to combat misinformation for future communicators. Journalism & Mass Communication Educator, 79 (3), 340-364. https://doi.org/10.1177/10776958241256404

Yunus, A. (2022). Countering online radicalisation during the COVID-19 pandemic: the case of Malaysia. Counter Terrorist Trends and Analyses, 14(2), 9–15. https://www.jstor.org/stable/48663621

Yusof, D. M., Kamal, S. M., & Ismail, A. I. (2021). Wisma Putra and PCVE (Preventing and Countering Violent Extremism): Sustaining Malaysia's Narrative of Peace and Security. Journal of Diplomacy and Foreign Relations, 20(1), 75–90. https://www.idfr.gov.my/images/JDFR/Vol20_No1_Nov_2021.pdf

Zahari, A. I., Said, J., Abdullah, K., & Noor, N. M. (2023). Financial innovations in terrorism financing: a case study of Malaysian terror financing. Journal of Criminological Research Policy and Practice, 10(1), 1–18. https://doi.org/10.1108/jcrpp-11-2022-0056

ZCOM Engagement Lab. (2023, September 7). Survey Report: Navigating the Malaysian Gaming Industry 2023. https://engagement.z.com/resource/survey-report/malaysian-gaming-2023

Hedayah

Countering Extremism
& Violent Extremism

Hedayah

Countering Extremism
& Violent Extremism

WWW.HEDAYAH.COM

HEDAYAH_CVE

HEDAYAH