Hedayah
Countering Extremism & Violent Extremism

BADAN NASIONAL PENANGGULANGAN TERORISME
BNPT

UNDERSTANDING AND PREVENTING ONLINE EXTREMISM AND VIOLENT EXTREMISM IN SOUTHEAST ASIA

INDONESIA COUNTRY REPORT

Understanding and Preventing Extremism & Violent Extremism Online in Southeast Asia

INDONESIA COUNTRY REPORT

Farangiz Atamuradova, Galen Lamphere-Englund & Emma Allen

Hedayah
Countering Extremism & Violent Extremism

BADAN NASIONAL PENANGGULANGAN TERORISME
BNPT

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 vast 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 Indonesia's National Counter Terrorism Agency / Badan Nasional Penanggulangan Terorisme (BNPT) for their collaboration and support through this project.

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 Online in Southeast Asia.

Finally, we extend our thanks to the reviewers and other contributors to this Report, including Anna Sherburn (Hedayah), Orissa Sofyan and Charlotte Gerdes..

BADAN NASIONAL PENANGGULANGAN TERORISME
BNPT

Suggested Reference:

Farangiz Atamuradova, Galen Lamphere-Englund & Emma Allen. (2025) *Understanding and Preventing Extremism & Violent Extremism Online in Southeast Asia – Indonesia Country Report*. Hedayah, the International Center 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, this accessibility, engagement and reach is also exploited by malicious actors. As one of the world's largest and most active online communities, Indonesia both benefits socially and economically, and faces challenges such as increased exposure to harmful online content.

To support future online counter extremism activities in Indonesia, 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 Indonesia, 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 Indonesia, ranging from the use of different platforms to major emerging technologies and niche (yet relevant) issue areas that warrant continued attention. Finally, this Report outlines **existing responses in countering extremism and violent extremism online**, ranging from strategic communications efforts to education, research and coordination, and discussion key challenges, needs and lessons learned.

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

- Continuing to develop local capacity to create positive and alternative narratives responding to multi-channel and platform-specific efforts used by terrorists
- Strengthening technical capacities for research and narrative monitoring
- Engaging with private sector and tech companies to harness the potential of AI for counter extremism efforts
- Building on existing coordination and collaboration mechanisms to create and/or strengthen formal and informal information sharing networks
- Focusing on tailored and sustainable approaches to media and information literacy interventions
- Leveraging successes in Women, Peace and Security (WPS) agenda efforts and applying a gender lens that incorporates other factors of identity to strengthen understandings of gendered radicalization dynamics

These recommendations are not exhaustive, but seek to build on existing positive efforts and strengths in the Indonesian context to continue to enhance the ability of online counter extremism practitioners to respond to terrorist and extremist exploitation of online spaces.

1. INTRODUCTION

1. Introduction

Today's digital age has seen rapid developments in technology, connecting people locally, regionally, and globally. While this provides ample positive opportunities for communication and access to information, its accessibility is also exploited by malicious actors to support their operations in online spaces. Extremist, violent extremist and terrorist groups have been leveraging new online trends and tools for recruitment and radicalization, planning and communication, fundraising, and propaganda dissemination. These actors tailor their tactics and methods to exploit platform dynamics and algorithmic amplification while increasingly relying on encrypted or semi-closed spaces to evade detection.

With around 212 million internet users as of early 2025 (Kemp, 2025), Indonesia ranks among the world's most active and expansive online communities. While this digital growth offers significant social and economic opportunities, it also presents challenges — notably, increased exposure to harmful online content such as extremist propaganda and other online activities. Youth remain particularly vulnerable to radical narratives and approaches that adapt swiftly to new technologies and platforms. As extremist actors continue to evolve their digital strategies, understanding Indonesia's information environment is critical for developing targeted and sustainable responses.

This Country Report presents findings from field research on Indonesia's media and information landscape, focusing on the strategies of online extremist actors, the challenges faced by frontline practitioners, and lessons learned from current responses. The report also offers practical, context-specific recommendations for practitioners and policymakers who are working to identify and disrupt extremist activity online. Rather than proposing one-size-fits-all solutions, it emphasizes locally informed approaches based on insights from those engaged in counter-extremism across sectors. Further, it assesses how extremist networks in Indonesia use online digital spaces, and develop multi-platform strategies to maximize both visibility and operational security – providing an in-depth understanding of how public platforms like Facebook, TikTok, Instagram, and X (formerly Twitter) are leveraged to disseminate narratives and influence mainstream discourse, while messaging apps with encryption functionalities such as Telegram and WhatsApp serve as hubs for recruitment, coordination, planning. The report also examines emerging trends in the use of digital spaces by extremists, such as financing their activities through digital currencies.

Finally, the report explores existing responses to these threats through legislative measures, platform regulations, inter-agency cooperation, and prevention programming -ranging from Indonesia's counter terrorism legislation which criminalizes online terrorist propaganda and recruitment, the National Action Plan for Preventing and Countering Violent Extremism (RAN P/CVE) which facilitates government, civil society and private sector responses, and regional efforts such as Indonesia's leading role in ASEAN's Plan of Action to Prevent and Counter the Rise of Radicalization and Violent Extremism (2018-2025). Civil society plays a vital role in raising awareness, promoting digital literacy, and amplifying positive narratives—particularly when efforts involve youth, women, and minority communities. This report seeks to provide practical examples of promising existing practices, while identifying areas that require further support and innovation to build a more resilient and informed digital society and prevent extremists from exploiting the online sphere.

2. METHODOLOGY

2. Methodology

To support future online counter extremism activities in Indonesia, 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 the 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. The main research questions for the project are outlined below. Additionally, more detailed questions were developed and broken down thematically to help researchers cover all the necessary themes to thoroughly assess the situation in the country.

- 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 conducted two specific research activities in Indonesia to assess the media and information landscape, with a focus on media and information literacy (MIL) skills as well as the extremist engagement on digital platforms in these selected countries. Both activities sought to elucidate 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 and civil society actors engaged with youth and with countering extremism and violent extremism or MIL efforts, and secondary research assessing existing literature on the topic. An inclusive approach was employed throughout the research, seeking a diverse representation of perspectives and experiences across gender, age, religious, and minority groups within the limitations of the planned sample size and timelines. In summary, the research included the following activities:

- A comprehensive review of existing literature covering the topic of online extremism in Indonesia in the past five years to help identify available data, existing gaps in literature, and validate findings from primary findings
- Two focus group discussions (FGDs) with key stakeholders such as ministry representatives and civil society organizations in Jakarta and Bandung, Indonesia, to gain insights on the perception and attitudes related to the research questions and validate findings from the literature review
- 23 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.


Average Sales Per Day
37% Planning
97% Design
28% Research
17% Implementation
Active Tasks
Mode A
Mode B
Mode C
Mode D

These research tools were developed to consider not only these primary research questions, but to apply gender and human rights lenses, and to consider the perspective of various types of stakeholders and issue areas that were relevant to online extremism.

Data Analysis

Data analysis for this research consisted of qualitative coding of primary research outputs. Utilizing a thematic coding approach, the primary data collected through KIIs and FGDs was coded using qualitative analysis software, Dedoose, by a team of coders from the research team (Hedayah and consultants). Coding was conducted using a deductive approach, working from a codebook developed by the research team based on the research questions, but which included identifying:

- Considerations for different stakeholder groups and/or sectors
- Different issue areas in line with the research questions articulated earlier in this report (such as existing landscape, emerging trends, etc.)
- Cross-cutting issues such as gender and inclusion concerns or impacts

Further, external expert opinions were also sought to validate findings, including government and civil society stakeholder review and validation.

3. KEY FINDINGS

3. Key Findings

The findings of the research are presented to follow, based on the previously outlined research methodology, breaking down the research into three components. The first considers the existing media and information landscape in Indonesia and how it is leveraged by extremists. The second focuses on emerging threats in the online space, exploring the most prominent trends and developments. The final section examines existing responses from government and non-government actors, as well as the challenges and needs identified for future work in the sphere.

3.1. The Online Information Landscape

The first section of the report addresses the following question:

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

This section of the report investigates the current online landscape in Indonesia based on the insights of local experts as well as existing literature to better understand how extremist organizations are exploiting digital spaces for their own means of communication and coordination.

3.1.1. The Online Information Landscape and Extremist Exploitation

While new platforms and applications can increase connectedness and access to information, they are also tools for malicious actors to reach and engage Indonesia's 212 million internet users. In practice, extremists in Indonesia continue to radicalize individuals offline through more traditional methods such as sermons and private study groups and use online or digital radicalization to spread propaganda and direct individuals to closed online and offline groups (Rahman et al., 2021). International terrorist groups such as Daesh increasingly adapt their tactics to target individuals in Indonesia by translating material into local languages in a practice known as "e-jihad" or online jihad (ibid). Recent reporting by UNICRI "found instances of Indonesian-speaking Telegram users expressing neo-Nazi views, including in discussions of Mein Kampf and the manifesto produced by the Christchurch attacker" (Bradley, 2025, p.77). While there is more limited evidence of far-right or radical right activity in offline spaces, it is important to take into consideration and closely monitor this trend. Interviewed Indonesian experts underlined that, based on the studies conducted with prisoners in jail for extremist charges, online ecosystems were one of the main sources of radicalization (IND25). In fact, the latest terrorism-related arrests in Indonesia were radicalized online (Newton, 2025). This includes the arrest of a 19-year-old male in East Java in July 2024 who was reportedly radicalized through social media and planned to bomb two churches in his region (Anuar, 2024). This further highlights an important 'offline' challenge in the intersection between online radicalization and offline recruitment and radicalization in prisons.

While there is visible progress on how online platforms are improving their regulations on content moderation and other relevant approaches to tackle this issue, the situation is still one that requires continuous attention as malicious actors, such as extremists, are quick to identify loopholes in the approaches and adapt their content to evade detection and removal through use of "borderline content" (Saltman & Hunt, 2023). Additionally, with increasing amounts of content posted online on a daily basis, moderation needs are increasing. While not unique to Indonesia, interviewees pointed out the rise of intolerance, hate speech, and hoaxes in the online space as persistent challenges (IND18). These are present within and beyond extremist narratives and online tactics; however, all can be leveraged by extremists to radicalize, recruit, and mobilize specific groups or fuel further division among communities (ibid).

This issue was further underlined when it came to the exposure of online audiences to harmful content, and the lack of ability to identify false or harmful information (IND19). With the Internet becoming the primary source of information for many individuals, and with an increasing prevalence of younger violent perpetrators, there is a growing concern that youth are most susceptible to falling prey to extremist narratives and disinformation when seeking out answers to their questions (IND9). With many of their interactions taking place online and with content moderators playing catch-up, extremist groups can leverage this as an opportunity to recruit new followers among youth (Ware, 2023). Another trend worth noting, and exploring further, is the relationship between family dynamics and radicalization of youth on online platforms, as experts highlighted the search for a sense of belonging is often found to be a critical driver for youth radicalization (IND19). Finally, in comparison to earlier uses of internet by extremist groups, women are no longer viewed as passive actors playing supportive roles and are actively targeted in the online spaces by extremists (IND17). A RUSI report on Indonesia underlined that "through social media, women are now able to play more active roles as propagandists, recruiters, financiers, and even suicide bombers" (Nuraniyah, 2019, p.2).

Online ecosystems have also played a role in shifting social individual identities and interactions, providing individuals with an opportunity to shape and build a different identity online and to act differently to their offline selves – living a "double life". As elsewhere in the world, an interviewee underlined that the offline civility index of Indonesians is currently higher than that of online (IND22). While many are welcoming and accepting in offline settings, latest evidence has shown that different trends emerge online (Dawitri & Amara, 2023). While online spaces can amplify incivility, a recent survey suggests that offline intolerance is also a growing concern (LSI, 2023). In the report, a significant number of respondents expressed discomfort with or rejection of certain minority groups, highlighting that intolerance is not limited to the digital sphere alone (ibid). Differences between an individual's online and offline behavior can make it harder to detect changes, or identify early signs of radicalization offline. This can be leveraged by online recruiters and extremists to radicalize individuals and groom them until they are ready to carry out offline attacks (IND19; Ware, 2023).

3.1.2. Prevalent Extremist, Violent Extremist & Terrorist Narratives Online

Extremist narratives and propaganda play a critical role as a tactic used by actors to spread their messages online and incite violence, hatred, and division among communities. Leveraging digital platforms, extremists develop and amplify their messages to provide alternatives to their followers to their existing grievances. Interviewees see extremists as highly sophisticated in manipulating information online, developing and spreading online narratives in the most strategic manner to reach their target audience (IND23). While extremist narratives are seen to be decreasing due to the work carried out by local authorities and tech companies, their presence online persists (IND24). Hence, it is essential to understand and explore existing narratives in Indonesia to effectively address them and build a more resilient community. Extremists often use local, regional or international issues, adding elements of their ideology, and leveraging mis- or dis-information to amplify their message for their target audience.

Local Narratives

While global extremist narratives are more prominent and present in online discourse, local narratives often play a bigger role, uniquely tailored to the country's context. Extremists leverage local grievances, religious interpretations, and national events to develop their local messages, making them powerful and attractive for the Indonesian population. Local practitioners reported an increase in region-specific extremist narratives, often focused on local and identify issues (IND21, IND13, IND10, IND1).

One of the most common type of narratives found in Indonesia is anti-statism, revolving around the political climate and elections. Through such narratives, extremist groups portray elected governments as "inherently illegitimate and unjust," calling them "Muslim apostates (murtad)" (Harmoni Program 2023, p.9). As such, political narratives often leverage an "us vs them mentality," seeking to cause a divide in the population and call for the rule of more extremist leaders (IND21). Extremist groups also exploit political tensions around the time of local elections to divide the population and produce "narratives of identity politics and sectarian

politics to not vote for political figures or local government candidates who are of different religion, different groups from them" (IND1). They increase narrative output on "sensitive topics like religion and ideology, such as anti-Christian or pro-Islamic rhetoric" to increase political mobilization during elections (IND10). Additionally, local extremist organizations leverage existing Daesh propaganda and narratives, reframing and translating it to the local languages and context, "targeting issues including the 2019" and the 2024 elections in Indonesia (Mok & Satria, 2024). For example, a faction of Jemaah Ansharut Daulah's (JAD) in the province of Riau urged its followers through social media to cause disruption during the 2024 elections (ibid).

Extremists in Indonesia are also seen to be adjusting their narratives and messaging to avoid detection and labelling as extremist, violent extremist or terrorist organizations, as well as broadening appeal and gaining more popularity among people, often done through hijacking popular and mainstream local narratives while maintaining an extreme ideology and promoting intolerance toward members of the out-group, such as minority groups and individuals of different religious backgrounds (IND24). As one interviewee underlined, "extremist narratives have softened in tone but are still pushing extreme religious views. They normalize this uniformity, which opposes diversity" (IND16). This was supported by other interviewees and highlighted as a threat to existing diversity, inclusion, and tolerance within the Indonesian community. As religious content is widespread within the online ecosystem, extremist groups often leverage and distort it to promote their narratives and recruit new members under the banner of religious education (IND15).

Extremists are also seen to often embed their messaging subtly in engaging content. Practitioners report an increase in glorification of convicted terrorists and militant leaders via TikTok. According to one interviewee, "some of TikTok's AI-based narratives significantly glorify groups of former and convicted Bali terrorists" (IND1). For instance, both deepfake and original content celebrating figures like Ali Imron (a Bali bomber who has since publicly apologized for his actions) is widespread. Some TikTok-based narratives have even reportedly influenced perceptions of certain viewers toward figures such as Ali Imron, creating more positive perceptions by highlighting his perceived repentance (IND1, IND25). At the same time, other deceased extremist leaders from the Bali bombings (e.g. Dr. Azhari bin Husin and Noordin M. Top) are mythologized for a new, younger generation of viewers through viral soundbites and pop-culture references on the platform (IND11). An interviewee noted a TikTok video invoking a catchphrase and iconography from a Japanese anime, "seni adalah ledakan" ("art is explosion"), to glorify a terrorist's "significant accomplishment," indicating how extremist creators weave militant themes into youth cultural idioms (IND1). This repackaging of extremist heroes in elements of existing popular content is a worrying trend that could make extremist ideology more palatable to young Indonesians.

Lastly, extremist groups are shifting their narratives toward topics unrelated to religion, like personal wellbeing, the environment, and other topics that may resonate with urban audiences, continuing to "plant seeds of extremism, but without using violent narratives" (IND24). It is worth noting that while the main branch of Jamaah Islamiyah (JI), the largest extremist group in Indonesia, announced its plans to disband in summer of 2024, there are substantial concerns that its members will continue to operate under different names but spreading the same ideology (Hwang & Frank, 2024), while others may defect to similar groups that support their ideological views (IND25). Such changes within the internal structure of organizations call for a continued investigation of how groups shift their online tactics and narratives to ensure presence and spread of their ideology in the local context.

It is worth noting that while these narratives may resonate with a portion of the online audience, they do not reflect broader public sentiment in Indonesia. In general, Indonesian society rejects all forms of terrorism and violence, and supports peace, unity, and pluralism within the country. The above trends are important to take into consideration in developing appropriate responses to the existing narratives.

Disinformation and Misinformation

As extremist groups continue to adapt their tactics and narratives based on the shifting political and social landscape in Indonesia, they are often found to be producing messaging that aligns with their ideology through the spread of deliberately false narratives, or disinformation and misinformation. Social media platforms and

messaging applications have made it easier for extremists to share and spread their narratives swiftly and globally, "using mis and disinformation tactics to amplify their impact" (Monaghan & Rodriguez, 2023). They often exploit online echo chambers to spread their narratives and target those who already share similar views to the group (ibid).

In Indonesia, disinformation and misinformation are particularly deployed around politically sensitive periods such as elections and times of political change (IND25, IND5). This was observed by experts during both the 2019 and the 2024 local elections (Harmoni Program, 2023; Mok & Satria, 2024). In 2019, JI launched an "information war" through several of their platforms to disrupt the local election proceedings (Mok & Satria, 2024). Experts believe that the intent of using disinformation and misinformation around election time is not to influence the results, "but to provoke conflict in society and undermine the electoral process ahead of the nationwide polls" (Ayuningtiyas, 2024). Extremists often use unverified user-generated content to "create and disseminate false narratives," which has become easier with the increasing availability of generative AI platforms for everyday use (IND15). Extremists are seen to leverage algorithms to "feed users" content that already aligns with their beliefs, seeking to exploit low levels of digital literacy and inability to detect and critically assess false content shared online, "making them more susceptible to believing and sharing" the information further with their peers (ibid).

Extremist groups are also seen to be using more organized ways of sharing narratives by setting up illegitimate media outlets, which are often referred to as "media farms" by Indonesian journalists (IND24). They use these platforms to share false narratives and disinformation about current affairs, sowing racism and violence within communities (ibid). The closed nature of certain platforms means misinformation and hate speech can circulate unchecked The concept of "idea hijacking" to push their own interpretation and narrative is not new, and was found to be used by other groups such as Daesh and their sympathizers (Yilmaz & Atamuradova, 2022). However, this method of embedding within existing ideologies or concepts makes identifying disinformation and misinformation even more difficult. As extremist groups blend nationalist or political and religious themes with disinformation tactics, it becomes more complicated to distinguish legitimate information from extremist narratives, which are intended to disrupt peace and democratic processes.

The impact of these narratives can be very real, and they can feed directly into support for extremist and violent extremist organizations. For the past seven years, Indonesia has been considered to be one of the most generous countries in the world (Charities Aid Foundation, 2025), and extremists in Indonesia have leveraged traditional mechanisms of open charity appeals into their narrative strategies, which has now gone digital. Extremist-linked groups often pose as charitable or humanitarian organizations to solicit donations by crafting emotionally charged narratives targeted at the general public. In Indonesia, "open fundraising is often framed as appeals to support the families of martyred and imprisoned mujahideen" (Nuraniyah, 2019, p.12). Such campaigns may be advertised on social media and messaging apps, pulling at communal heartstrings to gather money ostensibly for needy families, which in reality bankrolls extremist activities. An interviewee confirmed seeing social media narratives asking for donations to build Islamic boarding schools affiliated with extremist groups such as JI-linked pesantren (religious schools) (IND25). At the same time, oversight is limited: "In many Islamic organizations, there's no audited reporting… everyone gives money and they don't know [where it goes]. And some of it is to finance terrorism activity in Indonesia" (IND23). Essentially, extremist actors can hide in plain sight among Indonesia's numerous legitimate charities and crowdfunding drives, especially if those organizations lack transparency. This blurs the line for donors, many of whom may genuinely believe they are giving to provide religious education or humanitarian relief. To counter this poses as challenge, as "maybe counter-narratives can still be used [to dissuade people from extremism], but what about funding narratives like this?" (IND25). Countering extremist fundraising appeals requires different tactics than countering ideological propaganda, since the former often piggyback on positive social values like the forms of charity deeply embedded in Indonesian identity and national values.


01101110
00100000
0001
01110
00100000
00001
01101111
0101

Global Conflicts as Narratives

The recent events in the Middle East have been leveraged by extremist and violent extremist organizations globally to recruit new followers (Fahmy, 2024). This trend is also observed in Indonesia, where extremist groups are leveraging regional conflict to build solidarity, justify violence and radical responses, recruit new followers and sympathizers, and raise funds (IND23, IND21). As highlighted by one of the interviewees, such global, identity-rooted conflicts "trigger strong reactions among Indonesian users, who see them as injustices toward the Muslim community, thus amplifying religious glorification and solidarity" (IND15) – one expert further highlighted that these global conflicts "are being interpreted through local lenses to resonate with domestic audiences", a process referred to as "glocalization". (IND19). Extremist groups share information online on how local supporters can get involved (IND21, IND23). While the general Indonesian population express genuine concern and solidarity (Arshad, 2024), extremist actors exploit this sentiment for their own benefit and agendas, blurring the line between humanitarian support and ideological mobilization. Beyond solidarity, including calls to violence, local extremist groups also exploit global situations to undermine and "demonize" government and "'fortify the perceived legitimacy of IS' ideology" (Hasbi et al., 2023). By weaponizing emotional narratives around existing global conflicts and events, extremist actors are able to build strong bridges between distant conflicts and local radicalization processes.

3.2. Emerging Trends in Online Threats

Internet connectivity in Indonesia is expanding rapidly. With over 212 million users online, the average Indonesian scrolls, streams or plays for over 7 hours a day, four and half of which they spend on their phone (Kepios & We Are Social, 2025). Within that hyper-connected milieu, extremist actors are re-engineering their playbooks, blending platform opportunism (for example, TikTok for virality and Telegram for secrecy) with algorithmic sleights-of-hand, agile fundraising efforts, and an early embrace of technologies such as generative AI propaganda and online gaming. Frontline actors interviewed for this study, ranging from civil society prevention practitioners to counter terrorism financing investigators in Jakarta, describe adversaries who are improvisational rather than monolithic, "always one step ahead" of conventional countermeasures (IND25). Their testimonies, triangulated with academic and grey sector research, seeks to answer the core question for this chapter:

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

This section holds that the online extremist ecosystem in Indonesia is no longer anchored to any single ideology or platform but is instead a fluid environment of tactics and procedures that are co-evolving along with the wider digital economy (Nuraniyah, 2019; Harmoni Program, 2023). The following chapter maps that ecosystem across three sections: dominant platform uses and shifts, emerging technologies already deployed, and other frontier technologies that are yet to be used at scale.

3.2.1. Dominant Platform Usage and Adversarial Shifts

Current Tactics and Platform Use

Frontline practitioners interviewed consistently highlighted a shift toward visual, algorithm-driven social media – especially TikTok and Instagram – as core channels for extremist content dissemination in Indonesia. TikTok, in particular, has surged as a platform, reaching a broad demographic across social classes (Kepios & We Are Social, 2025). One interviewee noted that "TikTok in Indonesia is currently the platform most accessed by [young] people…the issues raised on TikTok will be the first source which then becomes a trending topic" (IND1). Its popularity with younger audiences makes it a ripe venue for spreading extremist narratives and recruitment material. Researchers echo this observation, viewing the platform as "a new tool

for spreading potentially violent ideological extremism and recruiting new members" (Suseno Sarwono, 2024). The app's "For You Page" algorithm can rapidly funnel content to target audiences, despite platform trust and safety efforts to mitigate exploitation by extremists and violent extremists. Daesh propaganda, for example, has effectively leveraged TikTok's algorithm to gain quick visibility "designed to align with user behaviour, [facilitating] the effective targeting of IS content to its intended audience," with videos that "rapidly gain broad recognition" among users who might not otherwise encounter them, mirroring the group's efforts to leverage the platform globally (MEMRI, 2025; Suseno Sarwono, 2024).

TikTok's governance and design create unique challenges. Frontline practitioners observed that TikTok content is "less controlled and spreads very quickly," often outpacing moderation efforts (IND24). They cite cases of online harassment and intolerance on TikTok that illustrate a broader problem: minority groups and even mainstream public figures can become targets of extremist trolling and incitement. For example, a prominent journalist, Najwa Shihab, faced violently misogynistic and racist attacks on TikTok amplified by swarms of coordinated accounts after criticizing political leaders (IND24). Such incidents underscore how the virality of TikTok can be weaponized not only to push militant extremist ideas but also to spread hate and intimidation, contributing to an ecosystem of intolerance that extremists thrive in. Such misogynistic violence has also been shown to reduce resilience against violent extremism in the Indonesian context (Lamphere-Englund et al. , 2022). In short, platform trends indicate that TikTok is critical for extremist and violent extremist communication in the Indonesia context. Its predominantly young user base (often from lower-income groups), as well as their grievances toward authorities, are precisely what extremist actors seek to exploit (IND24). As one interviewee put it, "extremist groups may see platforms like TikTok as an opportunity to expand their influence and reach, targeting users who might be more susceptible to their messaging" (IND17).

Instagram, likewise, plays a role, though experts assess it is used in a more curated way. A recent study from the multi-year Harmoni P/CVE project in Indonesia found that "Facebook and, increasingly, Instagram were… used to push messages to a broader audience, often in a more subtle format designed to evade platform moderation policies" (Harmoni Program, 2023, p.6). Extremist actors treat Instagram as a channel for broad outreach with mild content attenuated to avoid takedowns while relying on other platforms for direct calls to action. Interviewees note that Instagram (along with other Meta properties including Facebook) have become responsive in removing blatant extremist content, so perpetrators adapt by toning down explicit violence or sectarianism on those platforms. Still, Instagram's wide reach among Indonesian youth (84.6% of internet users older than 16 use the platform each month) and influencers means it cannot be ignored (Kepios & We Are Social, 2025). Extremist groups maintain accounts and circulate memes or coded messages there to shape perceptions but only reveal their full ideological aims on less regulated channels.

While TikTok and Instagram serve as the most discussed dissemination tools, frontline actors stress that encrypted messaging apps and private forums remain critical infrastructure for extremist networks, and further, can be key spaces for ideological reinforcement, networking and recruitment. Telegram, in particular, is a platform of choice for Indonesian extremist actors due to its security (optional encryption) features and community building functions. Research finds that extremists select online platforms based on four main criteria: "user-friendliness, free of charge, security and privacy, and leadership initiative" (Nuraniyah, 2019, p.137). By these measures, Telegram is a clear choice. It was adopted early by pro-Daesh elements around 2014 for its then-novel end-to-end encryption and ability to host large group chats. Unlike WhatsApp at the time of its launch, Telegram "is seen as more trustworthy and independent from governments" (Nuraniyah, 2017, p.170). This long-term reputation, combined with being free and easy to use, made Telegram a relatively reliable home base for Indonesian Daesh supporters through the mid-2010s (Harmoni Program, 2023). Even after Telegram came under pressure – the Indonesian government temporarily blocked Telegram's web version in 2017 to force stricter moderation and coordinated INTERPOL action globally during the pandemic shifted Daesh groups off the platform – extremist communities proved resilient and chose to remain on the platform. One interviewee mentioned that a bomb-making tutorial on Telegram – part of the wider Terrorgram network – had remained online for four years, illustrating how instructional videos or files can circulate beyond the reach of authorities. Today, many use "extra security measures such as anonymous virtual

phone numbers…VPNs or other devices to conceal location and IP address" in conjunction with Telegram rather than migrate to less familiar apps and risk losing their followers (Nuraniyah, 2019, p.142). In the words of one interviewee, "at the moment, [extremists] mostly use Telegram. [It has] more private security… makes it a bit difficult for us to follow or monitor them" (IND1).

WhatsApp is another crucial platform, given its ubiquity in Indonesia: over 92% of internet users are on the platform (Kepios & We Are Social, 2025). It is often used to maintain smaller cells or intimate networks. Field practitioners describe a typical pathway in which public content on open platforms serves as a hook, after which sympathizers are funneled into closed WhatsApp or Telegram groups for deeper indoctrination. As one interviewee explained, after initial online contact, "somebody will…get them closer to the small groups through WhatsApp groups, Telegram groups, where you can intensify those things" (IND22). Within these private group chats, extremist narratives can be pushed more directly—ranging from ideological training to operational planning—without outside interference. New features on WhatsApp are also on the radar as an emerging risk: for example, the introduction of WhatsApp Channels (one-to-many broadcast feeds), which could enable clandestine propaganda broadcasts to larger subscribed audiences (IND2).

Facebook remains part of the extremist ecosystem, though its role has evolved. Interviews suggest Facebook is used less for direct extremist messaging and more for networking and regrouping. Facebook's friend recommendation algorithms can inadvertently help extremists find one another. Notably, when an Indonesian female-only pro-Daesh Telegram group was disrupted (after its administrator's arrest in Hong Kong), "its members sought each other out on Facebook and immediately had an online reunion. Facebook's 'friend suggestion' and 'related pages' features could come in handy in this regard" (Nuraniyah, 2019, p.10). Extremist actors leverage these recommendation algorithms to reconnect and rebuild communities after bans. They exercise caution on Facebook due to stricter and more effective moderation: "messaging is more circumspect on Facebook than it is on Telegram, presumably to avoid stricter content moderation policies" (Harmoni Program, 2023, p.8). They may maintain Facebook profiles and pages to signal their presence, recruit sympathizers, or share sanitized ideological content, then redirect followers to less-regulated or more encrypted spaces to move towards explicit recruitment and radicalization. From a counter-extremism perspective, Meta properties like Facebook and Instagram are comparatively responsive in removing terrorist content (IND19). However, this creates adversarial shifts, as extremists simply work to exploit those platforms' networking features while hosting overtly terrorist or extremist material elsewhere.

X (known formerly as Twitter) is another platform mentioned by frontline actors, particularly as it is used by certain factions such as caliphate advocacy groups. Indonesia's so-called "caliphate" activists use X to amplify their messaging through coordinated campaigns elaborated on below. Such tactics illustrate how extremist actors manipulate mainstream platforms' algorithms to boost their visibility. It is worth noting that X's moderation approach has become extremely relaxed, and Indonesian interviewees lamented that content removal requests for terrorism often go unfulfilled on X, similar to Telegram (IND2). As a result, X continues to host a subset of extremist and violent extremist discourse, including violent jihadist cheerleading or extremist rhetoric, albeit usually phrased in ways that skirt direct incitement to violence.

Finally, YouTube and other media-sharing sites play a supporting role. While not highlighted as much as social networks by interviewees, YouTube is commonly used to share longer-form extremist content (lectures, documentaries, tutorials) either openly or via unlisted videos. Some extremist preachers maintain YouTube channels with coded language to avoid bans, and militants have been known to search YouTube for training material. YouTube's live-streaming – along with Twitch, DLive, and other sites – have also been exploited globally (e.g. live "gaming" streams used to propagate extremist views or showcase terrorist attacks) and Indonesian actors may be following suit (Wiegold et al. , 2024). However, increased moderation on major platforms has generally pushed the most egregious content off mainstream sites and into harder-to-reach forums.

The Role of End-to-End Encryption and Closed Groups

A notable trend identified by frontline actors is the migration of extremist activities from open forums to closed, end-to-end encrypted (E2EE) channels, which mirrors a global trend. As pressure increased on public platforms, Indonesian extremist groups "used to use open platforms, but now… use closed platforms and one-on-one communication platforms such as Telegram and WhatsApp" (IND1). These encrypted platforms provide privacy and secrecy that dramatically complicate efforts to monitor extremist content. From a practitioner's perspective, "once they [extremists] used open platforms like Facebook, Instagram, YouTube, X…but now they use…Telegram and WhatsApp…to internalize extremist ideologies and narratives in their circles" (ibid). Encrypted messaging platforms are used as "safe spaces for ideological reinforcement, networking, and recruitment" (IND19). This shift into encrypted spaces means more radicalization processes are happening out of sight, in invitation-only group chats or secret channels.

The implications of E2EE are two-fold. First, successfully implemented encryption shields communications from law enforcement or third-party observation, enabling extremists and violent extremists to share violent content, manuals, or plans with less fear of interception. As noted, Telegram's strong encryption, when activated, along with user-controlled groups have made it a prime venue for everything from propaganda dissemination to plotting. One interviewee recounted how the 19-year old Malang attacker (2024) as a teenager "joined a Telegram group and got radicalized…He became a lone wolf…[with] no formal ties to any terrorist group" (IND6). In this case, the perpetrator was reportedly influenced entirely through online interactions in encrypted channels. The interviewee highlighted that "terror groups don't have a framework. All they have to do is provide narratives and see who buys into them…they provide a lot of angry narratives…Meanwhile, our civil society organizations don't have [the] mature capacity…to tackle issues like that" (ibid). This vignette highlights how E2EE platforms empower amorphous extremist networks to recruit and indoctrinate individuals remotely, while civil society and government struggle to even detect these interactions, let alone counter them in real time.

Second, encrypted closed groups foster communities and can facilitate building new roles within extremist movements. Interestingly, research and interviews indicate an increased involvement of women in Indonesian extremist circles attributable in part to these private online spaces. "More private platforms such as Telegram or WhatsApp really allow women to be further involved in violent extremism," one expert noted, adding that women's participation in extremist activities and plots "has increased since 2020" (IND1). Encrypted group chats afford a degree of anonymity and freedom from social scrutiny, which can enable women – who might face greater societal barriers in participating in more militant circles publicly – to engage in extremist networks behind the scenes:

> *"These more private platforms are comfortable platforms for women, because they are free to express themselves in a more private space and it cannot be monitored by people who consider them dangerous or have a tendency to intolerance"(IND1).*

In other words, E2EE fora can help facilitate radicalization of women and facilitate their coordination in ways that were less common when networking is carried out in public.

For authorities, the "walled garden" effect of encrypted apps is a major concern. Unless an infiltrator or a group member shares information, security services have limited visibility. Government requests for content takedown or user data often fall short on privacy-focused platforms. Informal reports from interviewees note that that Telegram's compliance with takedown requests is below 50% – "only content that contains pornography and gambling is taken down; for terrorism it is rather difficult on Telegram" (IND2). This means extremist propaganda and coordination channels can persist for years, as demonstrated by the persistence of at least three phases of Terrorgram and associated networks on the platform (Barbarossa, 2024). Such gaps underscore how E2EE, while protecting civil liberties for the public, is exploited by extremists to dodge surveillance and content removal.

Furthermore, encrypted or private group chats tend to intensify echo chambers. Within closed extremist circles on WhatsApp and Telegram, messages go unchallenged and can become more extreme over time:

"Once you are there [in a private chat group], it's very difficult to really scrutinize, …moderate or police that kind of situation…[making it] really difficult to monitor and somehow control" (IND22). Discussions in these insulated groups can reinforce grievances and escalate commitment to a cause, especially during triggering events like political elections, sectarian clashes, or geographically distant events (see Section 1). Indeed, backup channels and accounts are typically created across Telegram and similar platforms to ensure that even if one channel is exposed or shut, the network survives in another form. This resiliency is a direct product of the encrypted, anonymous environment to encourage redundancy and regeneration out of sight.

Amplification Mechanisms and Moderation Loopholes

Despite increased content moderation and surveillance on major platforms, extremist and violent extremist actors continually adapt creative amplification tactics to spread their message. Frontline respondents and studies describe a cat-and-mouse dynamic in which extremists exploit loopholes in platform policies and algorithmic systems to ensure their content is seen by target audiences.

One major mechanism is the manipulation of algorithms and up-ranking systems to amplify extremist narratives. In Indonesia, as noted, extremists harnessed X's trending topic feature as early as the mid-2010s. An interviewee recounted how the conservative "hijrah" religious movement expertly "utilized trending topics to gain massive traction, combined with tailored language for different target groups," well before diversity advocates caught on (IND24). According to one source, these actors deliberately post en masse during off-peak hours and employ "random hashtags…that are not meaningful" to trick X's algorithm while creating trending content (IND8). By inserting irrelevant or unique hashtags in each post, they ensure each post appears distinct, avoiding X's duplicate content filters and making automated detection harder. This mass hash tagging strategy allows them to flood the platform with content and even push extremist talking points into trending topics during low-traffic hours. This practice of hashtag hijacking or manipulation is a "very common practice among such groups… especially when it comes to [X]," confirming that Indonesian extremists are part of a global pattern of algorithmic exploitation (IND8). The outcome is that extremist slogans or themes intermittently appear in mainstream discourse (e.g., as trending topics or recommended content), lending extremist narratives a veneer of popularity or legitimacy.

Another amplification strategy involves exploiting content moderation blind spots through coded language and ephemeral content. To evade detection by automated filters or human moderators, Indonesian extremists often resort to obfuscation. One study noted that many use "Internet 'leet speak' (replacing letters with numbers and symbols) to disguise controversial terms," as well as new platform features like disappearing Stories to slip past content censors (Newton et al. 2021, p.9). For example, supporters of Daesh in Indonesia have been known to use numeric codes such as "1515" to signify "ISIS" or abbreviations like "AD#15" for Anshar Daulah (a pro-Daesh group) (IPAC, 2018, p.12). By avoiding obvious trigger words, they bypass simple keyword-based detection. They also take advantage of ephemeral, time-bound, posts (e.g. Instagram and TikTok Stories, WhatsApp Statuses, etc.) which vanish after 24 hours, making it harder for moderators or authorities to catch the content in time. In theory, these could be reviewed by platforms after the fact, but, in practice, are often not unless the account is flagged. Practitioners note seeing incendiary images or videos in time-limited story feeds, which often dodge both automated and human content monitors.

Beyond stealth, extremist actors plan for resilience in the face of content removal. Indonesian extremist channels exhibit high adaptability: when one account or channel is shut down, backup channels spring up almost instantly. Analysts documented over 100 Indonesian Daesh Telegram channels that were taken down, "though most of them bounced back almost instantaneously" (Nuraniyah, 2019, p.142). Channel administrators employ various survival tactics: changing channel names to innocuous titles to avoid attention, creating multiple mirror channels as fallbacks, and pre-emptively compressing and storing important content in PDF files or e-books that can be re-uploaded or shared elsewhere. One common strategy is to maintain dedicated "feeder" channels whose sole purpose is to advertise the latest backup links to followers, ensuring the community can regroup with minimal downtime, in a similar fashion to drug dealers or pornographic actors elsewhere online.

Moderation loopholes on specific platforms also play a crucial role. Frontline practitioners point out that some platforms notably choose not to cooperate or are under-resourced to remove terrorist and extremist content, so malign actors concentrate their efforts there. Telegram's stance is a clear example, while X has been identified as "very difficult" in granting takedown requests outside of clear-cut illegal content like pornography or gambling (IND2). This effectively creates a loophole where extremist propaganda (which may not explicitly violate laws or can be framed as political/religious speech) remains online under the banner of free expression. The result is that Indonesian extremist networks can openly maintain a presence on such platforms to push ideological narratives or disinformation, knowing that enforcement is limited compared to stricter platforms. Indeed, one interviewee discussed the contrasts between platforms, noting challenges alongside a positive example where one platform proactively alerted authorities to a credible threat (a planned attack on a visiting religious figure) meaning that, within hours, police had arrested the suspects, showing how effective platform cooperation can be (IND19). Unfortunately, such cooperation is often the exception; extremists bank on platforms where moderation is minimal or enforcement uneven.

In essence, extremists treat content and channels as temporary and likely to be noticed or shut down, and thus cultivate multiple different streams to ensure that some are always active despite moderation. An IPAC report summarized this cat-and-mouse game: "Instead of responding with high-tech countermeasures, they simply create hundreds of backup channels and accounts, move their groups and channels regularly, and store terabytes of propaganda material across various platforms and devices" (IPAC, 2018, p.1). This low-tech persistence can often move faster than the more bureaucratic process of content removal.

Extremists also exploit the inherent echo chambers and recommendation systems of social media to amplify their reach. As noted, algorithms that tailor content to user preferences can inadvertently create reinforcing loops for those dipping into extremist content. Social media alters perceptions of reality: if someone interacts with extremist or intolerant posts, the algorithms will show more of the same, making it appear that such views are more widespread than they truly are (IND15). This "echo chamber effect" means a user who shows interest in radical content will be fed even more extreme material, possibly from multiple platforms cross-posting and out-linking (e.g., a YouTube recommendation leading to a Telegram link). In Indonesia, where digital literacy is uneven, many youths may be vulnerable to mistaking algorithmic curation for genuine popular sentiment. Thus, even without deliberately manipulating algorithms, extremists benefit from recommender systems that prioritize engagement over quality, often pushing sensational or polarizing content.

Financing Mechanisms: A Slow Shift to Digital

Experts in Indonesia are also closely watching how extremist, violent extremist and terrorist groups finance their operations and how these methods are evolving. Traditional funding channels remain dominant, but there is a clear trend toward diversifying into digital and online fundraising mechanisms.

Many Indonesian extremist groups continue to rely on traditional methods such as cash donations, bank transfers, and informal value transfer systems (hawala). Studies show that financial flows from overseas sympathizers – the Indonesian diaspora or foreign supporters – still often move via traditional channels into Indonesia. For example, recent research noted that "terrorism financial flows involving the diaspora from overseas into Indonesia are prevalent in the United States, Malaysia, Philippines, Australia and Afghanistan," while funds from Indonesia have also flowed out to Malaysia, the Philippines, and beyond (Ismail, 2023, p.15). These transfers typically occur through regular banking systems or money services and are small enough to avoid red flags. One study of terrorist financing in Indonesia concluded that while online platforms are available for fund-raising, "traditional banking transfers and hawala methods are still prioritized due to the small amount of funds required…and the need to maintain cash availability for operational purposes" (Wibisono et al., 2024, p.141). Essentially, it is often simpler and safer for extremists to move funds in cash or through local bank deposits, especially for domestic operations that don't need large sums of funds. This also highlights overall the potentially significant role of diaspora communities in online radicalization, recruitment and financing efforts, which should an important factor for consideration in developing responses.

Extremist groups like Jemaah Islamiyah (JI) historically built extensive community-based funding networks. An interviewee familiar with the group noted that "for JI, online is not a primary channel. They have schools, communities, [and] foundations. So, the primary channel is not online… But for [Daesh]… they use online [fundraising]" (IND23). JI has reportedly amassed significant assets through member contributions, charitable fronts, and business ventures. By one rough estimate discussed in an interview, JI may have controlled funds on the order of a trillion rupiah (IDR), or some $59.5 million USD in 2025 dollars, thanks to a norm among members to donate (zakat/infaq) regularly to the cause (IND23). These traditional fundraising norms have made JI financially resilient without needing modern fundraising. An interviewee quipped that JI's fundraising success could be likened to "a unicorn startup no one knows about" in Indonesia (IND23). This underscores that traditional fundraising is still very effective for groups with established offline networks and that these groups may see less need to expose themselves through online fundraising. However, this online ecosystem still enables and enhances traditional methods. Extremists routinely use encrypted apps to coordinate money movement while ultimately using conventional banks or remittances to finalize the transaction. For instance, Telegram has been used to orchestrate physical cash transfers:

> *"The online chat platform Telegram has been utilized to coordinate bank transfers for the purchase of firearms and travel of members of the MIT [East Indonesia Mujahideen] group in preparation for an attack on the 2019 presidential election… Transfer of funds is made by cash in bank branch offices and confirmation is communicated through Telegram" (Wibisono et al., 2024, p.146).*

Similarly, relatives of Indonesian foreign fighters overseas "have used online platforms to communicate, coordinate activities and fund their relatives abroad" (ibid). Thus, apps provide real-time coordination and secrecy to facilitate old-school funding tactics (hand-delivering cash, bank-in transfers made under false names, or with female relatives, etc.). Even when extremist actors move money internationally, they often prefer layering traditional methods with minor tech support: an arrested extremist in 2017 used Telegram's secret chat functionality to arrange a money transfer from Syria to Indonesia via Western Union, using multiple couriers to relay the funds in a convoluted way to avoid detection (Nuraniyah, 2019, p.13). This shows a merging of new tech with old tactics: encrypted messaging to coordinate, but conventional remittance methods to move funds. Extremist actors have also been known to exploit women's bank accounts – wives or female relatives often have clean criminal records and attract less scrutiny, making them ideal conduits for funding terrorism (ibid).

Investigators are increasingly concerned about the emergence of cryptocurrency and other fintech tools in terrorist financing. While still not the primary conduit of financing, there have been notable instances and a clear uptick in interest in these methods. Indeed, Indonesia already experienced a significant terrorism finance incident involving cybercrime and Bitcoin. The January 2016 Jakarta attack (Daesh-linked) was partly funded via an elaborate online scheme. Indonesian authorities revealed that militants "were using Bitcoin as a means of funding the operations of affiliated terror cells in Indonesia," with one cell collecting "donations in Bitcoin arranged via darknet forum sites, before subsequently hacking into a forex trading site," yielding nearly US $600,000 (Wibisono et al., 2024, p.142). This combination of crowdfunding on the dark web and outright cyber theft provided substantial capital for the attack. Another group, MIT, similarly "managed to embezzle funds from a… Malaysian finance company and collect US $33,000 from this hacking operation" (ibid, p.146). These cases, though a few years old, illustrate the potential windfall from cyber-enabled financing.

However, they also appear to be exceptions. Today, according to one financial investigator, Indonesian terrorism financing cases are more likely to show complex laundering sequences where the money might only eventually, "in the fifth layering… end[s] up using cryptocurrency" (IND5). Interviewees highlighted that Bitcoin and other cryptocurrencies are attractive because they are "universal and… difficult to track" (IND8). One expert explained that extremists are shifting to using not just well-known cryptocurrencies but privacy-focused ones such as Monero and similar coins that have enhanced privacy features that can hide the sender, receiver, and amount, making them even harder to trace than Bitcoin (ibid). This insight aligns with global observations: "The growing market of cryptocurrencies such as Bitcoin [has] provided a level of anonymity and decentralization that can be exploited by criminals and terrorists", and indeed Daesh, along with far-right groups, have been reported to solicit crypto donations on platforms like Telegram (Ismaizam, 2023, p.162). Current evidence suggests these instances are limited – one study notes that "systematic usage of cryptocurrencies by terrorist groups… has not been seen," highlighting instead isolated cases (Dion-Schwartz et al., 2020, cited in Ismaizam, 2023, p.162). This aligns with global trends, as recent analysis of global terrorist financing estimates that less than 7% of terrorism funds are channeled via cryptocurrency (Jofre et al., 2024). Still, when used, tracking crypto remains challenging, as many exchanges are based overseas outside Indonesian jurisdiction (IND5). New firms like Chainanalysis can track crypto transactions, but actioning specific wallets can remain a jurisdictional challenge. Terror operatives can exploit this by converting funds into crypto after a series of hops through e-wallets or bank accounts, thereby obscuring the audit trail. Indonesia's Financial Transaction Reports and Analysis Center (PPATK) can track banking transactions, but once funds enter decentralized crypto networks, tracing becomes far more challenging without international cooperation.

There is evidence that Indonesian extremist and terrorist networks have begun to experiment with other digital payments. Officials noted a "growing movement in Indonesia to use barcodes for payment" and a general "encouragement to go cashless," raising concerns that "terrorist/VE groups can use [digital payments] for funding" (IND20). Apps like OVO, Dana, GoPay (from Gojek), which use QR codes and digital wallets, are extremely popular in Indonesia's online economy and could be misused to collect funds under false fronts. Thus far, no major terrorism cases using e-wallets have been confirmed, but the infrastructure exists and is reportedly insufficiently unregulated against terrorism financing.

Other emergent methods also include exploiting online marketplaces and crowdfunding platforms. Globally, there is concern that terrorists could sell fake goods online (through e-commerce sites or social media marketplace features) to launder money – essentially receiving "payments" for non-existent products that are donations, or by selling actual merchandise for the group. Interviewees suggested that there have so far not been any reports of such e-commerce abuse in Indonesia (IND5). Nonetheless, the possibility has practitioners uneasy.

Looking forward, online gaming and Web3 technologies present new frontiers for illicit financing. While not yet recorded in Indonesian cases, experts warn that these technologies could offer even more anonymity and creative methods to raise funds. Micro-transactions in online gaming or in metaverse settings could enable extremists to launder funds or run in-gaming fundraisers under the radar. As one foresight study

notes, "the metaverse may prove an ideal environment for the laundering and transfer of funds controlled by terrorist actors," for example through ambiguous NFT art sales "whereby substantial money can be exchanged without regulation and with limited risk" (Hunter et al., 2024, p.106). An extremist could, in theory, sell a unique digital artwork (NFT) or virtual real estate to a donor for a large sum, and this would appear as a legitimate transaction in a largely unregulated space. Such methods could "go unnoticed" much more easily than conventional bank transfers. Though this is speculative, Indonesian policymakers are taking note of such trends to plan for potential threats.

3.2.2. Emerging Technologies Already in Use: Gaming & AI

Beyond social media platforms and messaging apps, frontline practitioners in Indonesia are examining how emerging technologies might enable the next wave of extremist activity. Three areas stand out in their analysis: online gaming ecosystems, artificial intelligence, and other technologies (such as the dark web and the metaverse) that extremists could leverage. While some of these trends are nascent, the consensus is that staying ahead of them is crucial for effective prevention of extremism.

Online Gaming Ecosystems as Recruitment and Propaganda Spaces

Online gaming is identified as a growing frontier for extremist influence in the country. Indonesia has a massive and youthful gamer population, with some 150 million people playing games regularly. The rise of e-sports and mobile gaming means millions of young Indonesians spend hours each day in immersive, social virtual environments (Newzoo, 2025). Frontline experts observe that extremist groups are aware of this and have begun to infiltrate gaming platforms and communities, which has been observed and recorded globally (Lamphere-Englund & White, 2023; White et al., 2024). One interviewee warned that "electronic games are now a propaganda ground…[From Call of Duty, Roblox, Fortnite] it turns out that there are those who use it [for malign purposes]" (IND25). The concern is two-fold: extremists may use games to insert propaganda content or narratives, and they may use gaming communities to directly radicalize and recruit inside of. As illustrated by the Extremism and Gaming Research Network (2021), these align with the six primary typologies of harm posed by extremist actors on gaming surfaces: creating new video games and modifications, exploiting gaming social environments, recruiting and communicating in games, gamifying terrorist content, using games for propaganda, and financing or laundering funds through games (Lamphere-Englund, 2024). For example, across a seven-country study of extremism on gaming platforms, gamers surveyed in Indonesia were the most likely to report seeing images, videos, or symbols promoting extremism on gaming surfaces (44%), while 26% reported seeing recruitment attempts, 18% were exposed to donation requests to extremist groups, and 36% saw people endorsing violence against particular social groups on gaming platforms (White et al., 2024).

Several characteristics make gaming platforms attractive for extremist actors. First, many online games (and gaming-centered platforms like Discord) often have limited moderation of content, especially compared to mainstream social media. Unlike Facebook, gaming networks historically have not received scrutiny for extremist content, though that is changing in 2025, leading to a lax attitude on monitoring hate or terrorism related chatter. Research confirms that "many gaming and gaming-adjacent platforms make little to no effort to moderate extremist content", as they haven't been pressured to do so (Lamphere-Englund & White, 2023, p.20). In-game chat functions or voice communications can be rife with toxic language, which can include misogynistic or racist sentiments, yet often only blatant cheating triggers bans. Extremist actors take advantage of this moderation gap. For instance, voice chats on consoles or in-game are essentially ephemeral and unmonitored; they are less easily picked up by detection measures than text posts, and once a voice conversation ends, there's usually no record for authorities to action (Modulate, 2024). Indonesian extremists could similarly use gaming voice chats or private game lobbies for covert communications.

Second, gaming provides a cover of entertainment that can mask extremist recruitment and radicalization. Parents or authorities might see a teenager playing a popular game and have no suspicion that anything is amiss, as opposed to noticing involvement in a known forum. This dynamic worries Indonesian activists:

"when Gen Z plays games…we have no control. Because we think they are just doing entertainment," but in reality, there is a possibility they are being targeted by recruiters in-game (IND25). Recruiters, or simply extremist-minded gamers present in such a large community, can gradually build trust with young players over chat, then invite them to closed channels (Telegram groups, or Discord servers). In particular, "in-game chat functionalities allow rapid and easy access to a wide range of users, including younger demographics, which can help recruitment, propaganda and potentially intragroup communication" (Lamphere-Englund & White, 2023, p.19). Southeast Asia-focused research similarly notes that "in-game communication features… serve not only as a covert platform for disseminating extremist ideologies but also as a venue to reach young people in Southeast Asia for recruitment" (Sulaimarl & De Lang, 2024, p.26). This is particularly relevant for Indonesia's youthful population. There have been anecdotal regional cases (for example, two Singaporean youth radicalized through Roblox), highlighting that this threat is not merely theoretical.

Specific instances of extremist content in games have already been observed by Indonesian monitors. One interviewee shared a striking example of gamification of propaganda: a modified scenario in the popular shooter game Call of Duty or a similar first-person shooter title was circulated with a twist – players were given identities aligned to real-world conflict, in this case referencing conflict in the Middle East. This mod or custom game emphasized a narrative of Muslims vs. enemies, effectively turning a recreational game into a tool to reinforce extremist worldviews (IND25). Potentially this referred to Knights of al-Aqsa, an FPS shooter title with antisemitic undertones, which Indonesian gaming live streamers have reviewed (Lamphere-Englund & Thompson, 2024). Footage of this was found on YouTube, and it had been promoted via Telegram channels, showing a clear link between encrypted extremist networks and gaming content. By "including certain religious attributes in the game… they emphasize that we are friends and they are enemies… [the idea] that those enemies must be killed", the propagandists delivered an interactive extremist message to players (IND25). This kind of immersive propaganda can be powerful – it engages users emotionally and actively, rather than just passively watching a video. It also illustrates how extremists repurpose existing popular games (instead of building their own from scratch) to subtly indoctrinate players.

That said, the extent of extremist penetration into Indonesian gaming communities (beyond just exposure) is still an open question. Some practitioners remain cautious about overstating the phenomenon. A gamer among the interviewees noted, "as an avid gamer myself… I haven't personally observed extremist narratives in the games I play, especially not violent extremism" (IND13). Occasional racist and nationalist slurs were observed, often arising from conflicts between players of different nationalities, however, overt recruitment or propaganda was not evident (ibid). This is a reminder that extremist exploitation of gaming is not universal, with only 44% being exposed to such content in Indonesia in 2024 polling (White et al., 2024). Recent research into gamer identities in the country found that despite a reluctance to play with gamers from different cultural or national backgrounds (only 36% of males and 22% of females were comfortable), most Indonesia gamers demonstrated strongly resilient traits against extremism (Lamphere-Englund et al., 2025).

Financing through gaming is another angle of this trend. Extremists can potentially use gaming platforms and monetization features to raise funds or launder money and, as illustrated earlier, some 18% of gamers in Indonesia have seen such requests on gaming surfaces (White et al., 2024). Literature highlights several methods: trading of in-game currencies or rare items for real money (which can be moved in obscure ways), using gaming gift economies (like donations during livestreams) to funnel money, or even selling custom game modifications with proceeds going to extremist coffers (Saiz, 2025). For example, "there is evidence of loopholes to sell games, in-game items and other gaming products in exchange for cryptocurrency or fiat currency…many games use virtual currency exchanges that often do not align with anti-money laundering standards" (Lamphere-Englund & White, 2023, p.20). A concrete instance involves the popular game Fortnite: it features loot boxes and gift cards which have been "implicated in money laundering schemes" by organized criminal groups – an extremist group could buy gift cards with illicit funds and resell them, or use loot boxes to obscure transactions (ibid). Additionally, streaming platforms like Twitch have been misused: right-wing extremists have made money by streaming video games while disseminating their political messages, effectively getting viewer donations for propaganda (Schlegel, 2021). Indonesian extremist groups could mirror these techniques, especially as Indonesian gaming influencers and streamers attract large youth audiences.

In sum, online gaming represents an emerging ecosystem that extremist actors are probing. Indonesian experts see the potential for gaming platforms to become to the 2020s what social media was to the 2010s – a new vector for radicalization and coordination that can fly below the radar. The challenge is amplified by the interactive and transnational nature of gaming. The trend is still developing, and while not yet at crisis levels, it is "the opportunity and challenge for the younger generation in Indonesia" (IND25) that policymakers and civil society aim to get ahead of. Proactive measures – such as awareness for parents and gamers, and engagement with the gaming industry to help improve moderation – should be considered to prevent extremist infiltration from gaining a foothold in Indonesian gaming communities.

The Use of Artificial Intelligence in Propaganda and Operational Planning

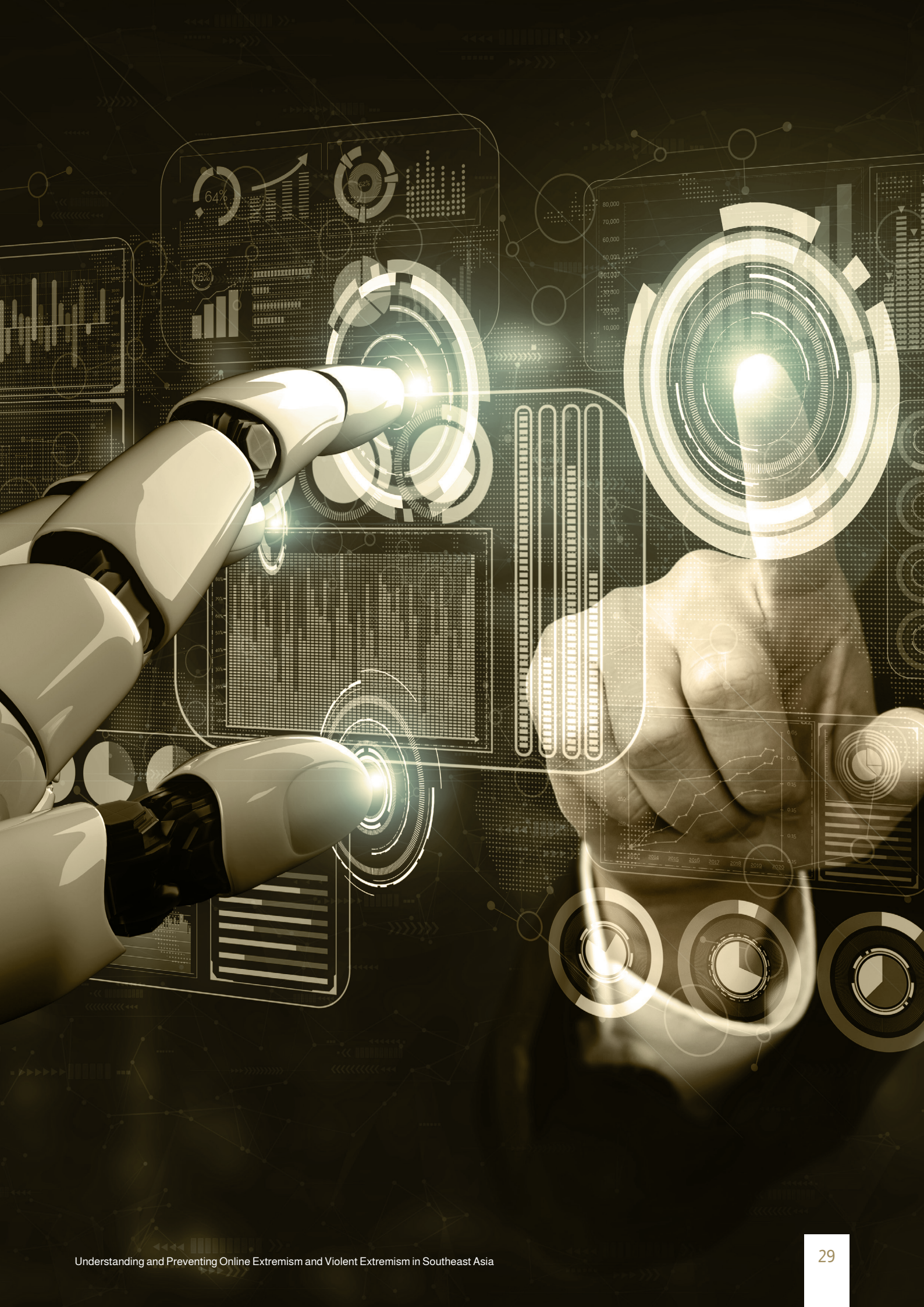
Artificial Intelligence (AI) is rapidly transforming the online ecosystem, and frontline actors in Indonesia are noting both current signs and future possibilities of its exploitation by extremist groups. From generative AI propaganda creation to algorithmic targeting and chatbots, extremists stand to benefit from AI, and practitioners warn that if pro-social actors do not keep up, extremists could gain a technological advantage despite the strong potential benefits from AI for preventative work.

One immediate concern is the use of generative AI to produce extremist propaganda that is more persuasive and harder to discern as inauthentic. Generative AI tools (for text, images, video, and audio) allow users to easily create content. Researchers note that terrorists are already adopting such tools:

> *"Terrorist groups are increasingly adopting generative AI to enhance and spread their propaganda, making it more efficient and tailored to specific audiences. This includes creating synthetic images, videos, or audio to intensify their messages and influence emotions" (Sulaimarl & De Lang, 2024, p.23).*

Indonesian experts are already noticing content online that seems suspiciously polished or erudite coming from extremist circles. One interviewee shared an example of TikTok/Instagram posts that discussed philosophy and religious concepts with a surprising depth – these posts subtly conclude that "philosophy is wrong and there is only one true belief," aligning with hardline views (IND24). The interviewee stated, "I'm convinced these were created using AI because…these groups are anti-philosophy. The linguistic and religious studies presented…appear very deep, giving the impression that the creators are experts, [yet] that's often not the case. The content is made to look impressive, creating the illusion that the creator is a scholar or expert" (IND24). In other words, AI text generation can help extremists produce well-written, authoritative-sounding narratives that their actual propagandists might struggle to create. Simultaneously, practitioners showed examples of anime-styled, AI-generated content on extremist Telegram and Instagram channels in Indonesia with VEOs actively "trying to make it interesting for young people" (IND21). These pieces, while being visually stimulating, can also feature overlay text with a call to action (ibid). In short, AI tools are already being used in Indonesia to help extremist messaging resonate more with educated or skeptical audiences and flood social feeds with high-quality, well-targeted content.

AI is also entwined with the development of misinformation and deepfakes, which can fuel extremist narratives or cause social chaos that extremists exploit. With image diffusion models embedded in AI tools, it is easier than ever to fabricate realistic images or videos and inject them into social media. Indonesian experts are warily eyeing the global uptick in deepfakes. One interviewee mentioned the possibility of extremists using AI to create bogus statements or videos of respected Indonesian figures to erode trust. "Important people who are moderate…their faces are used [in deepfakes]…They convey [fake extremist] utterances…even though we know this person as a good person" (IND25). The recreation of the Bali Bombers via deepfakes on TikTok in Indonesia, as noted previously, provide a clear illustration of how this can be leveraged (IND1). The psychological impact of a convincingly faked video could be significant. Extremists are often a step ahead in adopting new tech: prevention and enforcement actors need to keep up.



AI could also assist in micro-targeting and personalization of recruitment messaging. Using analytical AI, extremist actors can in theory analyze large datasets (social media profiles, engagement metrics) to identify individuals who might be susceptible to radicalization and then tailor propaganda to them. As one researcher has noted, "analytical AI can be used to analyze individuals' data to personalize recruitment tactics" (Sulaimarl & De Lang, 2024, p.23). Publicly available information – for example, a person's likes, shares, and group memberships – could be processed by AI tools to infer their grievances or interests (much as social media algorithms do) and automatically generate content that speaks to those specific sentiments: "AI-driven natural language generation (NLG) algorithms possess the capability to craft persuasive text-based content… that resonate deeply with specific individuals," effectively "tailoring their messaging to align seamlessly with the pre-existing beliefs and grievances of the individual" (Ismaizam, 2023, p.163). While there are no confirmed cases of Indonesian extremists executing such highly personalized campaigns, apart from these anime-based campaigns, the technology is available and needs to be closely observed, and in practice, some interviewees believe extremist outfits are already using simpler forms of AI-driven targeting. One noted that these groups "use AI to map content and audiences on social media" – essentially analyzing what narratives work with which demographics – and then "identify market segments that extremist groups can target…crafting narratives tailored to attract those audiences" (IND24). This indicates a level of strategic media operation, where AI or at least some level of data analytics guide propaganda focus (e.g., pushing anti-government content to users who show distrust of the state, or sectarian narratives to those with conservative views). Such segmentation improves propagandistic efficacy. Finally, one expert highlighted the use of AI to translate text from English and Arabic into Bahasa, creating a "new layer of accessibility and autonomy" for followers and recruiters (IND19). Leveraging AI as a way to produce personalized messages as well as recycling existing messages in other languages increases opportunities for extremist actors to produce and share propaganda online.

Another threat are AI-powered interactive agents or chatbots. Extremist and violent extremist groups could deploy chatbots on platforms (Telegram, Terrorist Operated Websites (TOWs), or even mainstream social media via direct messages) to engage with curious individuals or potential recruits. These bots, powered by large language models, can simulate human conversation and answer questions about extremist ideology, effectively acting as 24/7 radicalization agents. Security experts caution that "terrorists could utilise chatbots powered by large language models (LLMs), such as ChatGPT, to engage with potential new recruits" (Sulaimarl & De Lang, 2024, p.23). Ismaizam (2023, p.163) similarly notes that "AI chatbots and virtual assistants operate adeptly on social media platforms, actively engaging with users…skillfully mimic[ing] human interactions, progressively indoctrinating users with extremist ideologies." Jailbroken models are available and can provide such interactions. This one-to-one engagement can be powerful, especially if human recruiters are scarce, with worrying precedent in other domains (e.g., scam networks using bots for fraud) and current trends showing that the top use case of AI is for therapy and companionship (Zao-Sanders, 2025), while radicalizing companion bots have pushed individuals to attempt violence in the UK.

Interestingly, interviewees noted that moderate and counter-extremist groups in Indonesia have perhaps not yet leveraged AI extensively out of ethical or philosophical hesitation. One interviewee observed that "moderate religious groups… haven't yet utilized AI to counter extremist content because they still believe that their work should come from original thought" (IND24). This principled stance, while admirable, may put prevention actors at a disadvantage if extremists fully weaponize AI. The interviewee implied that without adopting new tools, prevention and counter extremism practitioners "will always lag in terms of leveraging technology," as extremist and terrorist actors often lack these ethical concerns (IND24).

Another forward-looking worry is AI being used in attack planning or cyber-attacks. Analytical AI tools could help extremists conduct reconnaissance (e.g., analyzing satellite imagery or Google Maps data to pick targets or plan routes). On the cyber front, AI can automate the crafting of phishing emails or identify software vulnerabilities, potentially lowering the bar for extremist groups to engage in hacking. As one source noted, "cyberattacks can be used by terrorists to inflict significant damage; AI can help create even more convincing phishing emails and other misuse" (Ismaizam, 2023, p.162). While not yet observed in Indonesia, the risk remains as these tools proliferate.

There is also an inadvertent way that AI is influencing the extremism landscape: through how the public uses AI for information. One interviewee pointed out that young people are increasingly turning to AI chatbots to ask complex questions, including religious or ideological ones. "AI tools like ChatGPT are also being used to ask religious questions… and they provide quick and convincing answers. This makes the information appear real and authoritative" (IND24). The danger here is twofold: AI might provide answers that, while neutral, lack necessary context or nuance for sensitive questions. Worse, if the AI's training data is insufficient or poorly aligned to these questions, it could echo extremist-leaning viewpoints (Shah et al., 2025). In general, it is less about extremists creating AI tools and more about the public unwittingly trusting AI outputs that could reinforce extremist narratives.

AI represents a double-edged sword in the context of extremism. Frontline actors in Indonesia see that extremists are beginning to exploit AI for content creation and targeting, giving them potentially far-reaching capabilities to influence and avoid detection. Meanwhile, those working against extremism are working to catch up – to use AI to amplify positive narratives and to detect AI-generated malign content. The key message for a policy audience is that AI is accelerating the challenge - from deepfake propaganda to personalized radicalization, these emerging AI-driven trends could significantly shape the future of extremism if proactive measures are not taken.

3.2.3. Less Used Technologies: Dark Web, VR/XR, Drones, 3D Firearms and Beyond

Frontline experts also identify a mix of other technological trends that, while somewhat peripheral today, could soon become major enablers of extremism . These include evolving financial technologies (cryptocurrencies and NFTs, often facilitated via the dark web) as well as immersive platforms (the metaverse) and even hardware like drones and 3D printed firearms. These tools and domains are generally transnational and anonymized, which is why terrorist actors find them attractive.

The dark web – the hidden part of the internet accessible via specialized browsers and tools– often goes hand in hand with crypto in terrorist financing. On dark web forums or marketplaces, extremists can solicit donations or trade illicit goods with a degree of anonymity. A recent study pointed out that "fundraising and financial transactions are increasingly conducted on the dark web through digital cryptocurrencies like Bitcoin and Monero. These platforms allow terrorist organizations to raise funds via Bitcoin donations, online extortion, and even human and organ trafficking" (Sulaimarl & De Lang, 2024, p.25). While Indonesia's P/CVE practitioners have not reported homegrown dark web terror marketplaces, they are aware of this global phenomenon. In fact, Indonesian security officials have identified terrorism financing transactions using the dark web and crypto (IND3, IND8, IND23). The dark web's relative obscurity in Southeast Asia might be temporary; the United Nations Office on Drugs and Crime (UNODC) warned nearly five years ago that although data on dark web activity in the region is limited, "it is likely to expand in scope and scale in the near future" (UNODC, 2020). Therefore, building capacity to monitor and counter dark web dealings is on the agenda for Indonesian authorities, lest extremists exploit this blind spot.

The concept of the metaverse – shared virtual worlds and games often accessed through VR/AR/XR(virtual/augmented/extended reality) – is still emerging, but analysts are preemptively considering its implications for extremism. Many of these potential harms blur into those already covered under the gaming section. Still, because VR experiences can blur the line between simulation and reality, they could intensify the impact of extremist content and also be useful for attack planning and training. This kind of immersive hate training is speculative but not far-fetched as the tech becomes mainstream – and is already in place across other online gaming platforms (Lamphere-Englund & Thompson, 2024).

Drones and 3D printed firearms also warrant mention. Cheap FPV drones have been used by terrorist groups in other contexts and Indonesian security forces have noted interest in them (McDonald, 2024). Thus far, Southeast Asian terrorists have not significantly used drones in attacks. A review noted that terrorists "have started to use drones for surveillance or propaganda purposes, but they have not yet become a central tool," and use in actual attacks has been limited (West, 2021, p.31). Drone usage would likely be coordinated

via online (or fly-by-wire) means, and any increase in drone activity might coincide with online tutorials and procurement. One interviewee indicated that there is a growing concern over members of local groups such as JI and Jamaah Ansharut Syariah (JAS) have been trained overseas on use of drones and called for closer monitoring of this trend as well as its future implication in the country (IND19). Meanwhile, 3D printed firearms are becoming easier to create and far more durable, readily circumventing firearms restrictions (Veilleux-Lepage and Füredi, 2025). At least one interviewee in Indonesia noted their concern that groups may soon use 3D printing (IND19).

Another trend is the possible convergence of organized cybercrime and extremism. Indonesian officials observed that some non-local actors in conflict-affected regions engage in "underground fundraising… disguising themselves within Islamic schools" (IND10). This might point to overlaps between criminal networks and terrorist networks, with rampant online scams, a potential fundraising approach. Already, a historic Indonesian terrorism financing case, an 2011 online bank-skimming operation that netted militants $700k, shows this convergence (Nuraniyah, 2019, p.6). If extremist groups tap into the Indonesian or regional Southeast Asian cybercrime underworlds, we could see more hybrid financing plots.

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. Further perspectives from research are incorporated to triangulate results and broaden the discussion.

3.3.1. Existing Responses

Indonesia's community-based approaches, such as the government-led National Action Plan (NAP, or in Bahasa Indonesia, "RAN PE") and CSO initiatives like Komuji, PeaceGen, and Indika Foundation, appear to have fostered a greater degree of collaboration and innovation. For example, Komuji's ArtVocation initiative integrates storytelling, art, and music workshops to build counter-narratives, especially among youth. Another example is PeaceGen's collaboration with KHub, mentoring CSOs to develop alternative narratives, emphasizing critical thinking and empathy. Common challenges include resource and training gaps, including around online strategic communications, though Indonesia's counter-narrative campaigns are perceived to be targeted and exciting (including those categorized in the national RAN PE Strategic Communications Strategy).

While Indonesian youth are often seen as the most vulnerable to radicalization, their role is as pivotal to CEVE strategies. Programs aiming to empower young people to create and disseminate counter-narratives have shown promise but often remain small-scale. While there are a range of MIL programs active in Indonesia, they serve a variety of actors (i.e. not only youth) and they are not necessarily integrated into schooling systems, nor large enough to reach this significant segment of the population.

Content moderation faces various challenges - linguistic and cultural diversity creates significant hurdles for tech platforms in moderating extremist content via machine learning approaches, and extremists can exploit linguistic nuances, encrypted language, and cultural references that are often misunderstood or missed by global moderation tools. Efforts to address these challenges have limited resources and lack a systematic approach to incorporating local expertise into content moderation frameworks, though many actors also highlighted positive cooperation and engagement for these purposes between government and

tech sector. Similarly, many stakeholders interviewed emphasized constructive progress in coordination and collaboration between governments, civil society, and tech platforms, while noting that challenges in this regard remain. As in many contexts, resource constraints and inconsistent funding also limit the scale and impact of initiatives.

Legislation, Policy & Legal Approaches or Frameworks

A key focus of discussion when it comes to legal and policy frameworks for response in countering extremism and violent extremism online is Indonesia's RAN PE. As a recent article notes, "the government issued a presidential regulation in 2021 to enact a National Action Plan to Prevent Violent Extremism (RAN PE), following advocacy and planning from the National Counterterrorism Agency (BNPT) and partners. Among a raft of processes and intentions, the plan sought to improve coordination among stakeholders and encourage regional ownership of prevention strategies. […] Despite persistent challenges, the Indonesian government is constructing highly promising P/CVE infrastructure that can produce long-term benefits, if enthusiasm and resources are mobilized and sustained over the coming years" (Sumpter, 2024, p.10).

RAN-PE is consistently emphasized as a major enabler of coordination and engagement with local level actors (IND24), with one interviewee noting it has "opened doors for meaningful collaboration" (IND17). Thematic working groups were seen to have improved the focus of programs and given key local actors and CSOs a framework with which they could align, and thus focus, their efforts (IND24). It has also facilitated collaboration with various parties, and decreased reluctance to collaborate amongst some actors (IND24). One CSO interviewee noted that it had facilitated better engagement with ministries which had in turn enabled them to better integrate a gender perspective in their programming through engagement with relevant ministries. It was also highlighted that the RAN PE has built greater recognition of the work of CSOs and elevated among them and other relevant local actors the issue of counter extremism and violent extremism efforts (IND17). One interviewee noted:

> *"RAN PE significantly enhances our approach to moderating online extremism by promoting collaboration among diverse stakeholders who can address both online and offline extremism in a coordinated way. Traditional actors [..] focus on enforcement and online monitoring, but RAN PE brings in ministries, local governments, and civil society organizations to work together. This collaboration allows us to tackle online extremism with more preventative and community-based strategies" (IND12).*

RAN-PE is perceived to have strengthened approaches across the issue areas discussed in this Report, including countering extremist narratives online, enhancing content moderation, and promoting MIL (IND12).

Legal frameworks also have major importance for content moderation efforts (see 3.1.2. Content Moderation below). Indonesia has legislation to provide government with abilities to remove or block access to platforms or Internet Service Providers (ISPs) that facilitate the circulation of extremism propaganda, along with enabling prosecution of online speech and other cyber offences, mandating content removal and user bans, and requiring online platforms to follow outlined regulations and "register with the Ministry of Communication and Informatics . Together, Law No.5/2018 on Eradication of Terrorism and Law No.19/2016 on Digital Information and Transactions constitute the legal foundations of the prosecution of violent extremist content on the internet" (Wibisono et al., 2024, p. 149 & 150f). Other relevant legislation includes Government Regulation No. 77/2019 on the Prevention of Terrorism and Protection of Investigators, Public Prosecutors, Judges and Correctional Officers and the Decree of the Minister of Communication and Information Technology Number 172 Year 2024, which provides guidance on fines related to user-generated content.[1]

1 Please note that this research did not undertake a comprehensive mapping of relevant legislation, and the legal frameworks listed herein are not intended to constitute a full listing of all applicable legislation but rather key frameworks highlighted by literature and research participants.

Content Moderation, Policing & Law Enforcement

A common point of reference, for government stakeholders in particular, was the Information and Electronic Transaction (ITE) Law. This ITE Law enables the Ministry of Communication and Information Technology to block violating information online directly (Paterson, 2019, p.225). Interviewees note that the Ministry of Communication and Information Technology does active takedowns of accounts based on information shared by various departments who identify violating material. The State Intelligence Agency (BIN) also conduct surveillance / intelligence online and offline (IND23). Reporting identified that from 2017 to 2022, 27,443 websites were blocked in Indonesia for 'preaching radicalism' or related violations (Wibisono et al., 2024, p.152), demonstrating a relatively robust content identification and moderation mechanism. Increased powers under the 2018 anti-terrorism legislation have also been noted as having increased the volume of associated arrests (alongside increase in staffing and budget) (Jones, 2022, p.163). Effective legal mechanisms to allow for moderation and takedown of harmful content are key, though some research has raised concerns regarding the wide application of this legislation – government actors also acknowledged in interviews that freedom of speech and expression were a vital lens for their takedown efforts, and emphasized the necessity of preserving 'uncomfortable' speech that some actors may not embrace or approve of but which does not violate the ITE Law (IND8). Interviewees illustrate a relatively clear framework for engagement from the actors involved in these content moderation efforts, which involves actors such as the National Cyber & Crypto Agency (BSSN) and the BNPT at national level, and cooperation with regional and local partners like the Ministry of Communication and Information Technology (IND8). Some interviewees also noted that the technical capabilities of actors like the Ministry of Communication and Information Technology to identify and take down harmful content have improved (IND10).

Practitioners and stakeholders interviewed also emphasize the need to consider, and address, the 'pipeline' of content that can make its way online. In particular, engagement by Ministry of Religious Affairs with religious instructors who can convey positive, legitimate religious messaging both offline and online (IND9) and reduce the need for content moderation (IND9).

Strategic Communications - Countering Extremist and Violent Extremist Narratives

Government Strategic Communications

Under the most recent RAN PE, BNPT is tasked to "increase the role of various public figures, mass media and influencers on social media in conveying messages to prevent violent extremism [...] coordinate counter-narrative strategies through both online and offline media" (Wibisono et al. 2024, p.148). This is further enforced by the RAN PE Strategic Communication Roadmap document (KOMSTRA PE), which is aligned with existing regional and global communication strategies, such as the one of the UNOCT's Preventing Violent Extremism (PVE) through Strategic Communications program and the ASEAN Plan of Action to Prevent and Counter the Rise of Radicalization and Violent Extremism (2018). In this vein, BNPT has ongoing strategic communication efforts and works to deliver counter narratives and monitor emerging and prevalent narratives both offline and online to respond effectively, which includes tactics such as 'flooding' media with positive, moderate content through moderation Islamic media outlets (IND8, IND25). In addition to its own online counter narrative efforts, BNPT has set up initiatives such as Duta Damai Dunia Maya, a community of volunteers creating "positive and peaceful content so that the development of negative content and radicalism can be reduced" (Abdullah & Alfatra, 2019, p.159). Multiple frontline practitioners flagged the important role of BNPT's 'Peace Ambassadors' as key messengers both online and offline for counter-propaganda efforts (IND25), which brings together youth online content creators who receive training and support to create their own online and offline counter narrative or positive narrative content and to teach other creators to do so (Tio & Kruber, 2022).

Interviews also highlight various related government efforts to increase online safety and address misinformation, through efforts such as short video series about online gambling, predatory loans, hoaxes, and scams (IND5). The Ministry of Communication and Information Technology (previously known as Kominfo, now Komdigi) has in the last decade had active efforts intended to increase digital literacy, such as briefings on recent hoaxes that are posted online (Paterson, 2019).

Non-Government and Civil Society-Led Strategic Communications Efforts

It is widely acknowledged that civil society organizations (CSOs), often deeply connected to the communities they serve, are extremely well positioned for effective strategic communication due to their knowledge of their target audience and their trust within that audience. Indonesian CSOs are actively conducting various types of strategic communications efforts, some specifically targeted at preventing and countering extremism and violent extremism, and others with potential positive impacts in this area around peacebuilding, tolerance, and diversity, or critical thinking, for example. The CSOs interviewed for this Report highlighted several efforts they advocate for and have found to be effective. These include developing a range of targeted 'brands' or channels for different kinds of content (for example, a channel reaching out to millennial Islamic audiences; others more general on tolerance and diversity; one specific channel for students) and highlighted that this had increased engagement and effectiveness (IND6). The CSO Mubadalah highlighted key strategies such as using alternative narratives (rather than 'countering'), emphasizing mutual respect by using approaches that resonate with their audience, and providing inclusive and positive interpretations of religious teachings (IND14).

Other actors manage websites with counter narratives to promote moderate Islam (Wibisono et al., 2024; Suryana, 2018); for example, Nahdlatul Ulama (NU), Indonesia's largest independent Islamic organization, launched a global anti-extremism campaign 'to spread messages about a tolerant Islam (Islam toleran) to curb radicalism, extremism and terrorism' (Varagur, 2015), and to do so, NU has embraced media and strategic communications, leading initiatives like the documentary Im Rahmat Islam Nusantara (2015) and the 'cyber warrior' initiative (Schmidt, 2021, p.237), as well as training volunteers to create and disseminate counter and alternative narratives on social media (Schmidt, 2018). There are other similar websites which aim to counter extremism and promote moderate Islam, often by 'debunking' extremist ideologies or interpretations with religious knowledge, producing content by former extremists, or creating alternative narratives (Rahman et al., 2023, p.275). Others seek to create a platform for positive content, such as Mikrofon.id, a platform comprised of journalists, artists, and cultural practitioners that worked to build capacity and support other community media outlets to address sensitive issues through art and creative works (IND24).

Other civil society and non-government actors seek to empower content creators to develop counter or alternative narratives, such as the social enterprise Peace Generation Indonesia (PeaceGen) who led a Google Project Inspire-supported Creator Academy, or the Love Frankie-designed YouTube and UNDP joint initiative 'Creators for Change' which provided small grants in Indonesia and other Southeast Asian countries (Tio & Kruber, 2022). A throughline in these efforts is the engagement and amplification of affected, marginalized and/or local communities, and various CSOs emphasized this – for example, INFID highlighted its positive experience engaging youth to inform content creation (IND21).

Education, Building Tolerance, and Developing Media & Information Literacy (MIL)

Positively, in terms of tolerance and gender equality efforts, research from 2023 suggests decreases in intolerance in Indonesia (Halida et al., 2023). CSOs have highlighted successes in introducing gender perspectives in religious spaces through social media, by supporting positive role models like women religious scholars (IND17) and the Women's Ulama (such as KUPI, Indonesian Women Ulama Congress). They note an increase in the number of platforms offering more diverse, inclusive, and gender-sensitive Islamic content (IND11, IND14). Building on this, various Media and Information Literacy (MIL) efforts, as well as work to increase tolerance exist across Indonesia, targeting a wide range of audiences. For example, the Ministry of Education and Culture maintains 'Merdeka Mengajar,' an online learning platform for teachers where content about diversity and tolerance can be propagated and reach hundreds of thousands of users, providing online dissemination that supports offline efforts (IND3).

National movements such as Siberkreasi, Mafindo, and AIS Nusantara in Indonesia aim to teach MIL to the broader public in order to combat disinformation, predominantly through offline activities (Ummah & Al Fajri, 2020). Programs like CekFakta, a "fact-checking and verification project launched by twenty-two media companies with the aim of training journalists to combat misinformation and disinformation" (Liu, 2018) have also addressed this challenge, in this case resulting from collaboration between Google News, the Indonesian Cyber Media Association (AMCI), the Indonesian Anti-Slander Society (Mafindo), the Alliance of Independent Journalists (AJI) and Internews (Paterson, 2019, p.224); Facebook (now Meta) has also previously supported similar efforts through local CSOs (Tio & Kruber, 2022). Ruangobrol develops alternative narratives and is reported to be trialing a 'redirect' approach, wherein those searching for extremism-related terms may be redirected to Ruangobrol or to trusted sources guiding users to balanced information (IND12). While interviews with practitioners and key stakeholders conducted for this research highlighted a range of innovative approaches, they also emphasized the continued need for technical support and capacity building for CSOs, media practitioners, and government actors, which organizations like AJI and BNPT have previously supported or conducted but remain relatively limited in scale and reach and could ideally include broader audiences, such as community leaders, educators, and policymakers (IND10).

A wide range of CSOs note having, or being part of, various MIL interventions, incorporating elements from digital security to freedom of religion and gender justice (IND24). MIL was commonly a component of broader programming or initiatives – for example, Komuji's work with youth and artists in Bandung, while not focusing specifical on MIL, encourages young people to "think critically about the information they receive, process it with an inclusive perspective, and respond to it creatively" (IND24). Other organizations are collaborating with digital media and alternative media to promote media literacy (IND14); or to promote inclusion or religious freedoms (IND24). Responding to the new digital landscape, organizations in Indonesia – like Bersinergi - are working to offer training on 'AI literacy' which has a strong MIL component, and others have 'debunking' efforts that identify misinformation and seek to strengthen digital literacy, such as Mafindo or SafeNet (IND15, IND10), and Koalisi Cek Fakta (Fact-Checking Coalition), supported by Google Initiative (IND11). Recent evidence has also suggested the potential of gamification – a tactic already used by various actors, including extremist groups – as a tool for communication and learning (Mohd Nor, 2023). Moonshot and IREX created the media literacy game Gali Fakta, which was tailored to the Indonesian context, and found that participants "exhibited significantly greater skepticism toward false news headlines and expressed a reduced likelihood of sharing them" after engaging with the game (Facciani et al., 2024, p.1).

In short, efforts to increase MIL frequently go hand-in-hand with broader inclusion efforts and exist to target a wide variety of audiences in Indonesia from media actors to youth and local communities.

Understanding Impact

Understanding impact in online countering and prevention efforts can be challenging in a variety of ways. However, interviewees highlighted strong models for understanding their impact. These included:

- **Social Return on Investment** – "a systematic way of incorporating social, environmental, economic and other values into decision-making processes" (BetterEvaluation, n.d.)
- **Prioritizing outcomes-focused monitoring and evaluation** – focusing on the 'outcomes' level in monitoring and evaluation, i.e. the concrete changes in knowledge, skills, attitudes or behavior we can observe resulting from programming
- **Utilizing Social Media metrics** – considering key metrics like reach, likes, engagement, but also verifying these with additional research to probe understanding and impact among audiences and Net Promoter Scores (NPS) – "a quick, effective survey tool to evaluate an organization's training, workshops, services, communications or any other event" (CIVICUS, n.d.)

While this list is not exhaustive, it is a strong indication of positive and concerted efforts to understand the impacts of countering and preventing extremism and violent extremism online.

Coordination Mechanisms & Information Sharing Across Sectors

Interviews consistently emphasized the immense value of cooperation, coordination, collaboration, and information sharing mechanisms, both across sectors and within government. As the number of CSOs who engage in counter extremism and violent extremism efforts continues to grow (IND1), this need will only increase.

A range of initiatives were highlighted for their positive contributions to coordination, collaboration, and cooperation despite the ongoing need. The AIPJ-supported and PeaceGen-led 'community knowledge hub' as well as platforms like I-KHub and the WGWC were mentioned frequently by interviewees. Positive engagement with social media and tech companies, facilitating content moderation, were also highlighted by interviewees who spoke about Meta and Google engagement positively (IND2) and noted the law enforcement portals that enabled easier data requests (IND5). Similarly, research highlights Meta's permanent office in Indonesia, Google's inclusion of Indonesia as its first 'trusted flagger,' and established communication channels between X (formerly Twitter) and Telegram and the Indonesian government (IPAC, 2018, p.5). Research by the Royal United Services Institute (RUSI) noted that

> *"Indonesia is more advanced […] in terms of fostering relationships with tech platforms, which has led to some success in stemming the flow of extremist propaganda online [while p]ressure on platforms helped the Indonesian government achieve security objectives. […] Indonesia's intervention in Telegram also helped shake the tech sector out of inaction. It was a wake-up call to other major platforms such as Facebook, which has been criticized by the Indonesian government for its insistence on abiding by its own community standards rather than national laws" (Nuraniyah, 2019, p.14).*

While there are few locally-owned or based social media platforms, though the massive Gojek e-commerce platform stands as a local success story, these few were characterized as being very cooperative (IND2). Civil society interviewees also flagged the usefulness of approaches like TikTok's verified 'expert partners' (including local research organizations like the Wahid Foundation) who can be asked to provide recommendations, input, and context related to extremism content (IND1) to strengthen and contextualize content moderation approaches.

3.3.2. Key Challenges, Needs, and Lessons Learned

Thus far, this Section has outlined existing responses and focused on efforts, interventions, and approaches highlighted by literature and primary research as being effective or useful in the Indonesian context. However, this Report also sought to identify challenges, needs, and lessons learned, in order to consider where support, resourcing, and solutions are required in the view of relevant experts and frontline practitioners. Many interviewees, regardless of their role and organization, highlighted the need for capacity building to respond to evolving challenges and ensure responses could match the scale of the challenge, across the issue areas to follow.

Identifying and Addressing Cooperation, Coordination & Collaboration Challenges

As previously noted, interviewees consistently emphasize the immense value of cooperation, coordination, collaboration, and information sharing mechanisms, both across sectors and within government. Many see a range of positive developments and existing efforts in this regard (see 3.1.5. above) but the need for further efforts and continued emphasis is also frequently noted . For example, building better collaboration between NGOs, CSOs and government, engagement at local level, bottom-up approaches, and balanced, collaborative approaches with strong leadership were well received.

However, a range of challenges were also identified by interviewees and in literature. For instance, while many lauded the RAN PE for making positive progress, some actors felt they had not yet seen a major impact on online moderation (IND13) or that it was still too early to see the broader impact of the RAN PE (IND24). Challenges noted included not effectively implementing RAN PE objectives effectively at local level –

many grassroots actors, interviewees feel, still perceive terrorism and extremism as 'central government' issues. As a result, local actors may feel unprepared to intervene when this issue arises locally. RAN-PE's effectiveness could be enhanced by continued local level sensitization, engagement, and capacity building (IND12). Others agreed that while RAN PE has been a positive force, there is a need to translate its effects to a local level, and that challenges in coordination, funding, and stakeholder engagement remain (IND10).

Key Strategic Communications Challenges & Opportunities: Reaching Key Audiences, Engaging Offline

While there were a range of successful and sophisticated strategic communications approaches highlighted by the interviewees who took part in this research (and by literature on this topic), a range of challenges persist. The context continues to evolve, and strategic communications efforts must also grapple with the changing landscape of extremism and violent extremism – such as trends of harmful or violent narratives shifting to less public spaces, reported in the Indonesian context and a common trend in other contexts also, with many extremist messengers moving away from public forums like Facebook to private WhatsApp groups or other closed and encrypted spaces (IND24).

Strategic communication efforts also present risks – for example, one online campaign in 2019 found very high reach and attention capture, but evaluations could not confirm any significant effect on attitudes and indeed noted there may have been backfiring effects (Bodine-Baron et al., 2020). This is not an uncommon challenge and an area for caution – while strategic communications efforts like counter or alternative narratives can be a useful tool in broader preventing and countering extremism and violent extremism efforts, over-investing in this approach can be risky as evidence on its impacts remains mixed (see for example de Carvalho, 2023; Tio & Kruber, 2022; Alava et al,. 2017). Similarly, research has indicated that the relationship between extremist and violent extremist narratives and radicalization and recruitment is increasingly complex (see for example: Newton et al., 2021; Nuraniyah, 2019). Further, research has raised questions about the effectiveness of moderate Muslim online media institutions in tackling digital extremist content, for reasons including limited funding and cultural challenges among others (Suryana, 2023), and noted that CSOs have in some cases been very effective counter narrative creators, they have also often missed younger audiences that are vulnerable to radicalization and have not always been adept at selecting their platform or evaluating their impact (Ismail, 2024). Many of these risks and challenges can be addressed by careful tailoring and contextualization and utilizing various complementary approaches, but are important to consider.

Barriers to Media & Information Literacy

Interviewees also note that despite several good initiatives, efforts on MIL were largely not comprehensive enough to match the scale of content spreading on social media (IND15). This is particularly relevant with research noting a lack of digital literacy and high levels of susceptibility to misinformation in the Indonesian context (Yani, 2021; Paterson, 2019.; Facciani et al., 2024). With various forms of misinformation increasing online, ranging from political to health and finance-related forms (McRae et al., 2022; Mujani & Kuipers, 2020; Nasir & Nurmansyah, 2020), this is a key concern. Recent research also highlights the limited capacity of many students in Indonesia in distinguishing between false and factual news (Syam & Nurrahmi, 2020) and the widespread practice of sharing content without reading it (McDonnell & MacKinnon, 2020). Research has also flagged the tension between creating direct in-person engagement, but generally decreasing reach, by engaging offline (Ummah & Al Fajri, 2020), highlighting the importance of complementary offline and online approaches to building MIL capacity.

Gender, Inclusion, & Tolerance

While issues of gender, inclusion and tolerance are cross-cutting concerns for preventing and countering extremism online and as such, are dealt with throughout various sections of this report, it is also useful to specifically highlight their role in existing and potential responses. Many interviewees, particularly those affiliated with CSOs working on the issue, emphasize a need for ongoing efforts towards not only making preventing and countering extremism and violent extremism efforts more inclusive, but ensuring that gender dimensions of extremism and violent extremism are effectively engaged with. As literature has long confirmed

(Johnston et al., 2020), and interviewees echoed, extremism and violent extremism are gendered phenomena. Extremist and violent extremist groups use gender roles and norms in their radicalization, recruitment, and operations. They are adept at crafting targeted narratives for both men and women that engage with their gendered experiences. Preventing and countering extremism and violent extremism efforts must do the same, not only to be inclusive, but to be effective. As noted earlier, research from 2023 has suggested slight decreases in intolerance in Indonesia but also noted ongoing marginalization and stigma against some social groups, and women's rights remaining 'broadly unpopular' among the population surveyed (Halida et al., 2023). Research considering the linkages between gender and violent extremism in the region, including Indonesia, demonstrates the relevance of these concerns, finding "a positive and significant correlation" between support for violent extremism and support for violence against women (Johnston et al, 2020). CSOs interviewed in this research emphasized a number of key needs, including the need for safe reporting on these vulnerable minorities (IND24); to mainstream gender in prevention programming and policy (IND14); and to create contextualized and non-confrontational messaging to introduce gender-related issues (for example, using kesalingan (variously translated as 'reciprocity', or 'mutuality') rather than 'gender equality') (IND14).

Literature highlights that the need for these efforts is pressing. Extremists use propaganda and online messaging to espouse misogynistic and hostile views towards women (Phelan et al., 2022) and to explicitly reach women based on their different motivations (Johnston et al., 2020). Gender norms remain rigid and unequal, in the Indonesian context (ibid). Extremist and violent extremist groups continue to actively engage and use women recruits to circumvent surveillance (Nuraniyah, 2019) and provide various forms of support. Social media has enabled women to access spaces that would likely be male-only if offline, due to either anonymity (Curtis, 2020) or lack of physical restrictions on movement or spaces, which groups like Daesh have leveraged to bring women into supporter roles (Johnston et al., 2020) and as active combatants (Nuraniyah, 2017).

Given this, the need for a gender lens is extremely clear. However, recent research has suggested further efforts are needed – a survey of local, regional, and national experts in Southeast Asia (primarily Indonesia, Thailand and the Philippines) suggested that:

> *"Only 26% of participants agreed that existing P/CVE policies adequately address misogynistic and hostile beliefs espoused towards women by violent extremist groups. In fact, 50% of the respondents disagreed that existing policies adequately address misogynistic and hostile beliefs towards women, and 48% who disagreed were from Indonesia" (Phelan et al., 2022, p.42f.).*

It argues further that "[m]ore gender-responsive policies could address the gender-specific dimensions of increasing online radicalization and its impact on both men and women's offline recruitment to violent extremism" (ibid, p.9). This highlights that despite positive progress, continued efforts are needed. Additionally, literature notes that continued efforts to address imbalances in security forces can be part of the solution (Curtis, 2020). Indonesian police have made a positive and concerted effort to increase recruitment of women, but the overall number of women in the force remains low (Jones, 2022).

Content Moderation Gaps & Coordination Challenges

Interviewees drew attention to the importance of coordination between traditional law enforcement actors like Densus 88 and BNPT with agencies who have technical capabilities in communications like Ministry of Communication and Information, or BSSN (National Cyber and Encryption Agency) (IND12). They also flagged some coordination issues in the process of sharing information about potential VE actors or messengers online: for example, classified information often poses a hurdle to information sharing (IND23). It was also flagged that takedowns can still face identification challenges (for example, when academic content discussing extremism is classified as extremist content) (IND12). Research has echoed that interagency coordination efforts on responding to extremist, violent extremist and terrorist content can still be strengthened, noting examples of limits to coordination such as a lack of coordination between terrorist designation processes (produced the criminal justice system) and the governance of online content and digital platforms resulting in digital platforms being less encouraged to moderate or report this content

(Wibisono et al., 2024). Research has also encouraged Indonesia to consider the overall effectiveness of platform-level moderation efforts, rather than a narrower focus on compliance rate metrics (IPAC, 2018). Similar, interviewees noted the broader challenge of harmful content online, noting that – as in many other contexts – those working to moderate content online often consider extremism and violent extremism only as one lens among many, and are also managing broader efforts to moderate other forms of harmful content (IND20) which can split focus and make efforts to specifically moderate extremist, violent extremist or terrorist content online even more challenging.

The challenge of balancing human rights with counter extremism efforts was also raised – literature has cautioned that legal frameworks which have been useful for moderating extremist, violent extremist or terrorist content online can be over-used and result in reductions in freedom of speech or expression (Paterson, 2019). Similarly, strengthened intelligence and cyber-monitoring can have positive effects but clear lines on what is permissible for preventive purposes and what is not are vital (Jones, 2022). Interviewees also emphasized the now well-known challenges of moderating linguistically diverse content, particularly when led by international companies who are predominantly English-speaking and likely have limited (if any) capacity for reviewing content in local languages with nuance (IND5), and are further handicapped by the many ways in which context can inform what extremist content looks like.

Other ongoing challenges included that, while social media platforms have in many ways been cooperative partners in the Indonesian context, interviewees find that content moderation or account removal has worked well for 'bigger' or high-level figures but less so for those with less recognition or rank in these organization (IND1). Further, "the blocking of websites and social media accounts relies heavily on the compliance of internet service providers (ISPs) and platform providers" (Wibosono et al., 2025, p.153). Indonesia, by virtue of its large population and high internet penetration is also highly exposed to global challenges in this space – such as, for example, that many gaming and gaming-adjacent platforms "make little to no effort to moderate extremist content as they are not under the same scrutiny as social media platforms (Lamphere-Englund & White, 2023, p.20) and "in-game chats are often less moderated than other social media platforms and unencrypted messaging apps" (ibid, p.19).

New and Emerging Technologies – AI for Counter Extremism?

While new technologies like generative artificial intelligence (AI) have promising benefits for law enforcement, it comes with many legal and political challenges (human rights concerns, admissibility of AI-generated evidence in court), technical challenges (false positives/negatives, bias, explainability, complexity of human-generated content), and is "not a quick and easy solution" (UNICRI & UNCCT, 2021). Research has noted that:

> *"[C]hallenges related to operations and capacity within law enforcement and counterterrorism agencies mean the use of AI has been seen as a holy grail in combatting violent extremism. AI's capacity to process vast amounts of data faster and with greater ease, and to correlate such data and discover patterns and themes, means intelligence agencies see it as an appealing commodity to confront the problem of managing information overload" (Wan Rosli, 2024, p.48).*

However, it is important to note that AI also has limitations (such as content moderation models struggling with terrorist 'jargon', irony and humor, and minority languages (UNICRI & UNCCT, 2021) and poses risks as well as opportunities. An informed, 'right-sized' response will not only harness the potential of AI to improve content moderation, develop counter narratives, and scale up interventions, but will also need to grapple with its impacts on the media and information environment through updated MIL approaches, strengthened anti-misinformation and disinformation efforts, and continued education for not only practitioners and students but across all segments of society, among other efforts (Craanen et al., 2025).

4. RECOMMENDATIONS

4. Recommendations

This Country Report seeks to provide actionable recommendations that could be used to build on the lessons identified in literature and by practitioners, to focus future efforts, address key needs and to harness existing capacities. Please note that for each recommendation, specific recommendations are further elaborated, along with potential actions that could contribute concretely to such efforts, which are not intended to be exhaustive but rather to provide more concrete guidance to support implementation.

These recommendations include:

Continue to develop and support strategic communication capacity for civil society, local influencers and other community actors

Strategic communications efforts represent a key pillar in efforts to respond to extremist and violent extremist content, narratives and propaganda in online spaces. Continuing to develop capacity and support – through providing technical assistance, resourcing, or funding – local organizations and government stakeholders to create effective counter narratives, and importantly, alternative and positive narratives, will be an important component of supporting healthy online information ecosystems and growing digital resilience. Similarly, these efforts must respond to the multichannel and platform-specific approaches used by terrorist and extremists by meeting audiences where they are online.

Specific Recommendations	Potential Actions / Examples
Gather and review evidence on what works locally (through investing in research, monitoring and evaluation), and for different groups, in counter narratives and further, emphasize positive or alternative narratives, and train local actors where needed on effective strategies.	• Support or fund organizations conducting strategic communications interventions to conduct detailed target audience analyses and evaluations of the impact of their campaigns. • Train local, community-level actors on effective strategic communications to increase community resilience to extremist narratives. • Prioritize alternative or positive narrative campaigns rather than seeking to counter existing narratives - for example, focus on campaigns for creating resilience rather than seeking to discredit or debunk extremist narratives.
Consider creative strategic communications approaches with greater emphasis on storytelling, including diverse narratives. Similarly, prioritize engaging through different channels to meet audiences where they are – this might be through gaming influencers, or on TikTok, as relevant. Focus on increasing awareness among those online on existing tactics of extremists, to help prevent people falling prey to disinformation as well as recruitment tactics	• Conduct research and analysis to understand audiences and the best ways to reach them before developing campaigns. • Consider how new formats can be leveraged in an authentic manner to tell stories that can encourage critical thinking, tolerance, and open-mindedness. • Work with trust and safety actors in tech, government practitioners, and strategic communications practitioners to develop new ways to raise awareness of recruitment tactics, disinformation in the places where it is happening.

Engage youth as key actors in the development and delivery of messaging; similarly, ensure marginalized or minority groups are engaged to ensure strategic communications efforts are inclusive and effective.	• Develop campaigns or interventions through co-design processes including actors from marginalized or vulnerable groups. • Conduct risk assessments considering the specific vulnerabilities of marginalized groups to ensure that strategic communications approaches do not further marginalize or stigmatize.

Strengthen capacity for identifying trends, generating evidence and monitoring narratives and activities online amongst practitioners

Specific Recommendations	Potential Actions / Examples
Technical capacities for use of digital platforms for research and narrative monitoring, particularly in local dialects (such Bahasa Indonesian) should be a focus for capacity enhancement efforts.	• Fund training of local practitioners and provide necessary tools to conduct digital monitoring in local dialects. This can include capacity-building workshops on social media analytics and use of emerging technologies and tools tailored for local context and languages. • Collaborate with local universities and tech partners to develop language-specific keyword libraries that will help with content detection in line with local specificities.
Updated and timely research on terrorist, violent extremist and extremist narratives, activities online, and current trends are needed to inform tailored responses.	• Establish mechanisms for timely development of research and analysis on new trends to maintain up-to-date awareness and response to trends and developments. • Support and leverage existing platforms that conduct this type of research, such as the Indonesia Knowledge Hub on Countering Terrorism and Violent Extremism (I-KHub on CTVE). • Ensure research is locally informed and aligned with recent trends, and are shared across with relevant stakeholders to ensure a collaborative and unified response to extremism, violent extremism, and terrorism.
Continued learning to be aware of, and to effectively utilize or counter, latest technologies is needed to help practitioners keep up with the ever-evolving digital landscape. Frontline practitioners noted the need to learn to harness new technologies and trends for their work. Early warning systems for online threats are still needed to facilitate proactive or preventative actions, requiring both monitoring efforts and information sharing mechanisms.	• Develop and apply capacity-building trainings on emerging technologies (such as AI, algorithmic amplification), digital trend analysis. • Establish an information-sharing network to support timely efforts and prevent duplication of efforts. • Engage with tech as well as other relevant sectors to ensure practitioners are aware and informed on the rapidly developing digital environment.

Close monitoring of trends around the use of E2EE, generative AI, and concerns regarding potential extremist exploitation of digital financial services and technologies, to ensure policy and programming can keep pace with new technologies and online trends.	• Regularly review and adapt strategies based on emerging and developing trends in the digital sphere to help ensure effective and relevant response to extremist and violent extremist exploitation of the online spaces, while maintaining digital privacy, security, and human rights.

Engage with private sector and tech companies to harness the positive potential of AI, including efforts such as supporting the development of AI training models that can monitor extremist, violent extremist and terrorist activity and discourse across platforms ethically and effectively and in local languages

As noted in this Country Report, while AI and other emerging technologies present threats, they also offer opportunities for counter extremism practitioners to not only keep pace with terrorist and extremist exploitation but to leverage them in new and innovative ways. The potential of AI for content moderation and reducing harms to human moderators has already been flagged; similarly, its potential to support analysis of needs and trends, as well as large scale development of targeted counter or alternative narratives, are a few amongst many possibilities.

Specific Recommendations	Potential Actions / Examples
Engage with private sector and tech companies to leverage different forms of relevant expertise and create collaboration for counter extremism and prevention efforts.	• Develop structured working partnerships with private and tech sector through establishing working groups or similar regular meetings, to leverage relevant expertise, build relationships, and co-develop tools to monitor and moderate online content.
Ensure that use of new technologies for prevention and countering is informed by a do-no-harm approach, contextualized, and based on lessons learned and good practices from the counter extremism and violent extremism space in past decades.	• Adopt a context-specific and sensitive approach in employing technological tools in prevention and countering extremism efforts – for example, working with tech sector to train models on local languages and culturally-specific dynamics of extremism. • Apply ethical considerations based on local realities and lessons learned to avoid unintended consequences such as stigmatization, securitization, profiling, and community alienation, based on specific marginalized groups in this context. • Develop a formal review mechanism or expert advisory group to ensure oversight, safe and ethical development, and appropriate contextualization in any program design or implementation leveraging AI tools.
Consider how AI can be used ethically and safely for large scale and/or targeted strategic communications efforts such as narrative disruption, including approaches such as leveraging natural language processing (NLP) to detect veiled extremist language and coded messaging patterns.	• Continue to research how AI tools can be applied to detect extremist online narratives while ensuring strong safeguards on privacy, accuracy, and prevention of biases in the context of Indonesia's regulatory environment and online extremism landscape. • Advocate for human oversight in AI systems used in counter extremism efforts to ensure responsible and ethical use of AI.

Build on existing coordination and collaboration mechanisms to create and/or strengthen formal and informal information sharing networks.

While RAN PE has made great strides in creating more holistic engagement with a wider range of actors for prevention outcomes, community level engagement requires ongoing efforts to ensure effective policy and programming can have broad reach. Prioritizing dialogue and information sharing is key to facilitating such engagement. Government stakeholders emphasized opportunities to increase or strengthen formal information sharing across government to communicate regarding emerging threats more effectively.

Specific Recommendations	Potential Actions / Examples
Strengthening information sharing and engagement with the tech sector and in particular, trust and safety actors, should be an ongoing goal in order to support content moderation but also to help identify trends and diagnose needs for response.	• Enhance multi-stakeholder information-sharing mechanisms to facilitate engagement and knowledge sharing between government, tech, academia and civil society, in order to ensure early warning and coordinate responses to emerging threats in the digital sphere. • Establish a rapid-response framework that can help provide timely responses to emerging threats through sharing anonymized data and co-developing mitigation tools and strategies.
Broadly, and where possible, efforts to continue, strengthen or enhance collaboration and coordination across sectors, levels of government, and between different actors from government to civil society, media and tech, should remain priorities in order to support effective prevention and countering of online extremism.	• Promote multi-sectoral collaboration by strengthening and committing to coordination frameworks and mechanisms that link national, local, and sectoral actors. • Encourage regular joint planning sessions, cross-sectoral dialogues, and information sharing for prevention efforts.

Tailor media and information literacy interventions to the needs of the target audience (in terms of language, platform engagement, etc.) and focus on long-term, sustainable efforts that provide training, mentoring and support.

Multi-stakeholder media and information literacy (MIL) efforts have the potential to incorporate, and positively impact, a range of spheres. This may include:

Specific Recommendations	Potential Actions / Examples
Considering AI literacy and safeguards as part of prevention and awareness raising. Applying MIL in different online environments, such as online gaming spaces or in closed forums (like E2EE platforms).	• Integrate AI literacy and digital safety as part of MIL initiatives, with tailored content for emerging digital environment. • Ensure awareness raising efforts include development of skills to critically assess AI-generated content and recognize manipulation.
Develop behaviorally-informed MIL programs (for example, leveraging real-world online scenarios) to increase the practical capacities of those trained.	• Incorporate simulations, interactive exercises, and platform-specific case studies – for example, adapted to gaming environments - in training programs to build practical, context-relevant competencies for recognizing and responding to harmful content in the online sphere.

Engaging with broader, related harms such as scams, gambling, hoaxes, and disinformation.	• Broaden the scope of digital resilience efforts to include interconnected online harms such as scams, gambling, hoaxes, and disinformation. • Apply a holistic approach and recognize that other existing threats and harms can serve as a gateway or amplifiers for extremist content and information manipulation.
Developing skills for media actors to report responsibly on terrorism and violent extremism.	• Develop targeted training for journalists and media professionals on responsible reporting of terrorism, extremism, and violent extremism. Such trainings can include considerations such as ethical framing, avoiding sensationalism, protecting individual and communities, harmful and extremism content without amplifying it. • Collaborate with relevant stakeholders such as press councils and universities to support the long-term impact of this type of effort.

Continued efforts to apply a gender lens in preventing and countering extremism and violent extremism both offline and online is needed to ensure that gendered radicalization and recruitment dynamics and drivers are understood, and to ensure efforts to engage different genders through programming, alternative narratives, or other forms of intervention are effective and gender sensitive; further, ensure consideration of other factors of identity such as ethnicity, class, religion, etc. alongside gender.

Ongoing research across terrorism, gender, and prevention has highlighted linkages between gender and violent extremism, and continues to demonstrate that different genders are vulnerable to extremism and violent extremism in different ways, may perform different roles based on gender, and be targeted different by extremist or terrorist organizations, among other gendered dimensions of extremism as a phenomenon. This applies no less in online spaces, where additional factors such as gendered access to, or literacies, online spaces or new technologies may be at play. Given this, there is an urgent ongoing need to ensure that prevention and countering efforts consider extremism, violent extremism and terrorism through a gender lens, and that responses are designed to effectively reach and affect audiences of different genvders.

Specific Recommendations	Potential Actions / Examples
A gender lens that not only considers gender but other factors of identity such as age, religion, culture, etc. is needed to understand needs and to respond effectively.	• Adopt an intersectional gender lens in both research and programming to better understand the diverse needs, vulnerabilities, and roles of different groups in relation to online extremism. • Research and analyze how certain specificities such as age, gender, religious identity, and cultural background can impact individual online experiences to help develop a more targeted responses and protective mechanisms.
Build on successes in Indonesia's policy environment from the Women, Peace, and Security (WPS) agenda, aligning online prevention efforts with a WPS framework.	• Promote women's leadership in digital safety and their active role in preventing online extremism. • Design online interventions reinforcing gender equality and peacebuilding based on the national WPS framework.

REFERENCES

References

Abdullah, S. D. A., & Alfatra, S. (2019). Narration of Islamic moderation: Counter over negative content on social media. Millati: Journal Of Islamic Studies And Humanities, 4 (2), 153–165. https://doi.org/10.18326/mlt.v4i2.153-165

Alava, S., Frau-Meigs, D., & Hassan, G. (2017). Youth and violent extremism on social media: Mapping the research. UNESCO. https://doi.org/10.54675/STTN2091

Anuar, M. I. K. (2024, August 6). Indonesia police investigate social media terrorism recruitment after arrest of teen suspect. Bernama. https://www.bernama.com/en/news.php?id=2326037

Arshad, A. (2024, November 11). Indonesians join peaceful rally in Jakarta in solidarity with Palestine. The Straits Times. https://www.straitstimes.com/asia/se-asia/indonesians-join-peaceful-rally-in-solidarity-with-palestine

ASEAN. (2018). ASEAN plan of action to prevent and counter the rise of radicalization and violent extremism. https://asean.org/wp-content/uploads/2025/03/ASEAN-Plan-of-Action-to-Prevent-and-Counter-the-Rise-of-Radicalisation-and-Violent-Extremism-2018-2025.pdf

Ayuningtiyas, K. (2024, January 4). Experts: Extremist groups spread disinformation online to provoke conflict during Indonesian election. BenarNews. https://www.benarnews.org/english/news/indonesian/extremist-groups-spread-disinformation-to-provoke-conflict-during-poll-01032024150241.html

Barbarossa, E. (2024, May 6). The three phases of Terrorgram (ACC Reports). Accelerationism Research Consortium. https://www.accresearch.org/accreports/the-three-phases-of-terrorgram

BetterEvaluation. (n.d). Social return on investment. https://www.betterevaluation.org/methods-approaches/approaches/social-return-investment

Bodine-Baron, E., Marrone, J., V., Helmus, T. C., & Schlang, D. (2020). Countering Violent Extremism in Indonesia: Using an online panel survey to assess a Social Media Counter-Messaging campaign. RAND. https://www.rand.org/pubs/research_reports/RRA233-1.html

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

Charities Aid Foundation. (2025). World Giving Index 2025: A global view of giving trends. https://www.cafonline.org/insights/research/world-giving-index

CIVICUS. (n.d.). Net Promoter Score. https://monitoring-toolkits.civicus.org/toolkit/net-promoter-score/

Craanen, A., Allen, E., & Atamuradova, F. (2025, forthcoming). Artificial Intelligence for Counter Extremism: exploring threats, challenges, opportunities and needs for leveraging generative AI in counter extremism. Hedayah.

Curtis, G. (2020). What Indonesia is getting wrong about women and violent extremism. The Habibie Center, No. 18. https://www.habibiecenter.or.id/img/publication/04eff47fc8417409c08ec9432c2b894f.pdf

Dawitri, N., & Amara, M. (2023). Indonesia's low digital civility index -Two sides of Indonesia. https://doi.org/10.13140/RG.2.2.17889.58721

de Carvalho, C. M. (2023). Digital counter and alternative messages to extremist content: Effectiveness and way forward. In Special Issue: Building Digital Resilience In Preventing and Countering Violent Extremism. SEARCCT'S Selection of Articles 2023. 72-78. https://www.searcct.gov.my/wp-content/uploads/2024/08/SOA-2023d.pdf

Facciani, M. J., Apriliawati, D., & Weninger, T. (2024). Playing Gali Fakta inoculates Indonesian participants against false information. Harvard Kennedy School (HKS) Misinformation Review, 5 (4). https://doi.org/10.37016/mr-2020-152

Fahmy, S. (2024, January 25). The Gaza War and the danger of extremism. Carnegie Endowment for International Peace. https://carnegieendowment.org/sada/2024/01/the-gaza-war-and-the-danger-of-extremism?lang=en

Halida, R., Hanan, D., Prasetyo, H., Lamphere-Englund, G., & Hamonangan, A. (2023). 2022 National Survey Report: Violent extremism, democracy, and religious attitudes in Indonesia. Lembaga Survei Indonesia (LSI). Jakarta, Indonesia. https://www.lsi.or.id/post/copy-of-violent-extremism-report

Harmoni Program. (2023). Violent Extremism and Social Media. Trends in Indonesia: 2018-2023. USAID Harmoni. Jakarta, Indonesia

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

Hwang, J. C., & Frank, H. (2024). Jemaah Islamiyah disbands itself: How, why, and what comes next? The Soufan Center. https://thesoufancenter.org/intelbrief-2024-september-26/

IPAC. (2018). Indonesia and the tech giants vs ISIS supporters: Combating violent extremism online. In IPAC: Vol. No. 48. http://file.understandingconflict.org/file/2018/07/IPAC_Report_48.pdf

Ismail, N. H. (2022). Countering online radicalisation in Southeast Asia through the 5M framework. RSIS. https://rsis.edu.sg/rsis-publication/rsis/countering-online-radicalisation-in-southeast-asia-through-the-5m-framework/

Ismail, N. H. (2023). Online radicalisation of the Indonesian diaspora. Counter Terrorist Trends and Analyses, 15(3), 15–20. https://www.jstor.org/stable/48732712

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

Jamhari, J. & Testriono, T. (2021). The roots of Indonesia's resilience against violent extremism. Studia Islamika, 28(3). http://dx.doi.org/10.36712/sdi.v28i3.23956

Jofre, M., Aziani, A., & Villa, E. (2024). Terrorist financing: Traditional vs. Emerging financial technologies. Terrorism and Political Violence, 1–14. https://doi.org/10.1080/09546553.2024.2433635

Johnston, M. F., Iqbal, M., & True, J. (2020). The Lure of (violent) extremism: gender constructs in online recruitment and messaging in Indonesia. Studies in Conflict and Terrorism, 46(4), 470–488. https://doi.org/10.1080/1057610x.2020.1759267

Jones, S. (2022). Terrorism and extremism in Indonesia and the Southeast Asian region. Southeast Asian Affairs, 162–174. https://www.jstor.org/stable/27206

Kemp, S. (2025, February 25). Digital 2025: Indonesia - DataReportal – global digital insights. DataReportal. https://datareportal.com/reports/digital-2025-indonesia

Kepios and We Are Social. (2025, February). Digital 2025: Indonesia (v. 02) [Report]. We Are Social & Kepios. https://wearesocial.com/wp-content/uploads/2025/02/Digital_2025_Indonesia_v02.pdf

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. (2025) 2024 Resource List: Violent extremism, radicalization, and gaming. GIFCT. https://gifct.org/wp-content/uploads/2025/02/GIFCT-25WG-0225-EG-Resources-1.1.pdf.

Lamphere-Englund, G., White, J., Wallner, C., Newhouse, A., (2025, pending), Building Resilience Against Violent Extremism Digitally: Trialing a new gender-based approach among gamers, Frontiers in Psychology.

Lamphere-Englund, G., Hamonangan, A., and Putri, F. (2022). Pathways of resilience to violent extremism in indonesian higher education: A mixed method study using the building resilience against violent extremism (BRAVE) Approach. USAID Harmoni. Jakarta, Indonesia. https://www.crisconsortium.org/research-reports-pathways-to-resilience

McDonald, B. (2024). The drones of Hayat Tahrir al-Sham: The development and use of UAS in Syria. GNET. https://gnet-research.org/2024/12/20/the-drones-of-hayat-tahrir-al-sham-the-development-and-use-of-uas-in-syria/

McDonnell, I., & MacKinnon, T. (2020). Case study: Misinformation in Indonesia. GeoPoll. https://www.geopoll.com/misinformation-indonesia/

McRae, D., del Mar Quiroga, M., Russo-Batterham, D., Doyle, K., & Platform, A. (2022). A progovernment disinformation campaign on Indonesian Papua. Harvard Kennedy School (HKS) Misinformation Review, 3(5). https://doi.org/10.37016/mr-2020-108

Middle East Media Research Institute. (2024, February 2). Dari-language review: TikTok accounts show widespread use of the platform by Afghan Taliban and Islamic State. MEMRI Jihad and Terrorism Threat Monitor. https://www.memri.org/jttm/dari-language-review-tiktok-accounts-shows-widespread-use-platform-afghan-taliban-and-islamic

Modulate. (2024). Modulate and Activision case study. https://www.modulate.ai/case-studies/modulate-activision-case-study

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

Mok, B., & Satria, A. (2024). Indonesian terrorists' attempts to interfere with the 2024 indonesian election. GNET. https://gnet-research.org/2024/02/12/indonesian-terrorists-attempts-to-interfere-with-the-2024-indonesian-election/

Monaghan, K., & Rodriguez, C. (2023). Mis-and Disinformation: Extremism in the Digital age. CTPN. https://www.london.gov.uk/sites/default/files/2023-12/CTPN%20Report%202023%20-%20Mis-and%20Disinformation%2C%20Extremism%20in%20the%20Digital%20Age%20%28Single%20Pages%29.pdf

Mujani, S., & Kuipers, N. (2020). Who believed misinformation during the 2019 Indonesian election? Asian Survey, 60(6), 1029–1043, https://doi.org/10.1525/as.2020.60.6.1029

Nasir, N. M., & Nurmansyah, M. I. (2020). Misinformation related to COVID-19 in Indonesia. Institutional Repository UIN Syarif Hidayatullah. https://repository.uinjkt.ac.id/dspace/handle/123456789/63519

Newton, J. (2024). Staying Alive: The Indonesian pro-IS community's online resilience and the 'Lone Actor' threat in 2025. RSIS. https://rsis.edu.sg/ctta-newsarticle/staying-alive-the-indonesian-pro-is-communitys-online-resilience-and-the-lone-actor-threat-in-2025/

Newton, J., Prasad, H., Moner, Y., & Kyaw, N. N. (2021). Polarising narratives and deepening fault lines: Social media, intolerance and extremism in four Asian nations. GNET. https://gnet-research.org/2021/03/02/polarising-narratives-and-deepening-fault-lines-social-media-intolerance-and-extremism-in-four-asian-nations/

Newzoo. (2025). Global games market report 2024. Newzoo. https://newzoo.com/insights/trend-reports/newzoo-global-games-market-report-2024-free-version

Nuraniyah, N. (2017). 10. Online extremism: the advent of encrypted private chat groups. In E. Jurriens (Ed.), Digital Indonesia: Connectivity and Divergence (pp. 163-186). Singapore: ISEAS Publishing. https://doi.org/10.1355/9789814786003-016

Nuraniyah, N. (2019). The evolution of online violent extremism in Indonesia and the Philippines. GNET. https://gnet-research.org/wp-content/uploads/2019/12/5.pdf

Paterson, T. (2019). Indonesian cyberspace expansion: a double-edged sword. Journal of Cyber Policy, 4(2), 216–234. https://doi.org/10.1080/23738871.2019.1627476

Phelan, A., Gayatri, I. H. O., True, J., Marddent, A., Riveros-Morales, Y., & Gama, S. J. (2021). Gender analysis of violent extremism and the impact of COVID-19 on peace and Security in ASEAN: Evidence-based Research for Policy. UN Women – Asia-Pacific. https://asiapacific.unwomen.org/en/digital-library/publications/2022/03/gender-analysis-violent-extremism-covid19-peace-and-security-asean

Rahman, M. F., Irsyadi, M. M., Ferdiansyah, H., Suma, M. A., & Trinanda, D. (2023). Strategic efforts of Bincangsyariah.com and Islami.co editorials in spreading counter-narrative extremism on the Internet. Al-Balagh: Jurnal Dakwah Dan Komunikasi, 8(2), 249 – 282, https://doi.org/10.22515/albalagh.v8i2.7582

Rahman, M. F., Suma, M. A., Ferdiansyah, H., & Irsyadi, M. M. (2021). Kontra narasi ekstremisme online melalui media islam moderat di Indonesia. Lembaga Penelitian dan Pengembangan Masyarakat (LP2M), UIN Syarif Hidayatullah Jakarta.

Sadeghi, M., & Blachez, I. (2025, March 6). A well-funded Moscow-based global "news" network has infected Western artificial-intelligence tools worldwide with Russian propaganda. NewsGuard's Reality Check. https://www.newsguardrealitycheck.com/p/a-well-funded-moscow-based-global

Saiz, G. (2025). Virtual Threats: Terrorist Financing via Online Gaming. RUSI. https://www.projectcraaft.eu/research-briefings/https/static1squarespacecom/static/5e399e8c6e9872149fc4a041/t/681ccf124419647df74eb0ac/1746718484160/594-craaft-ii-bp1-terrorist-financingpdf

Saltman, E., & Hunt, M. (2023). Insight: Borderline Content: Understanding the gray zone. GIFCT. https://gifct.org/2023/06/29/borderline-content-understanding-the-gray-zone/

Sarwono, J. S. (2024). CaliphateTok: How Islamic State (IS) leverages social media in Indonesia and the Power of Counter-Narratives. GNET. https://gnet-research.org/2024/11/28/caliphatetok-how-islamic-state-is-leverages-social-media-in-indonesia-and-the-power-of-counter-narratives/

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

Schmidt, L. (2018). Cyberwarriors and Counterstars: Contesting Religious Radicalism and Violence on Indonesian Social Media. Asiascape: Digital Asia, 5(1-2), 32-67. https://doi.org/10.1163/22142312-12340088

Schmidt, L. (2021). Aesthetics of authority: 'Islam Nusantara' and Islamic 'radicalism' in Indonesian film and social media. Religion, 51(2), 237–258. https://doi.org/10.1080/0048721X.2020.1868387

Shah, R., Irpan, A., Turner, A. M., Wang, A., Conmy, A., Lindner, D., ... & Dragan, A. (2025). An approach to technical AGI safety and security. arXiv preprint arXiv:2504.01849. https://arxiv.org/abs/2504.01849

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

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/

Sumpter, C. (2024). Decentralising and coordinating P/CVE through the Indonesia Knowledge Hub (I-KHub). Counter Terrorist Trends and Analyses, 16(4), 10–16. https://www.jstor.org/stable/48794705

Suryana, A. (2023). Indonesia's moderate Muslim websites and their fight against online Islamic extremism. ISEAS – Yusof Ishak Institute. https://www.iseas.edu.sg/wp-content/uploads/2023/09/TRS15_23.pdf

Syam, H. M., & Nurrahmi, F. (2020). "I don't know if it is fake or real news": How little Indonesian University students understand social media literacy. Jurnal Komunikasi: Malaysian Journal of Communication, 36(2), 92–105. https://doi.org/10.17576/JKMJC-2020-3602-06

Tio, R. & Kruber, S. (2022). Online P/CVE Social Media Efforts. In G. Barton, M. Vergani, & Y. Wahid (Eds.), Countering Violent and Hateful Extremism in Indonesia. Islam, Gender and Civil Society (pp. 233-254). Palgrave Macmillan. https://doi.org/10.1007/978-981-16-2032-4_11

Ummah, N. H., & Fajri, M. S. A. (2020). Communication strategies used in teaching Media information Literacy for combating hoaxes in Indonesia: A case study of Indonesian National Movements. Informacijos Mokslai, 90, 26–41. https://doi.org/10.15388/im.2020.90.48

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

United Nations Office on Drugs and Crime. (2020). Darknet cybercrime: Threats to Southeast Asia. UNODC Regional Office for Southeast Asia and the Pacific. https://www.unodc.org/roseap/uploads/archive/documents/darknet/index.html

Varagur, K. (2015, December 2). World's Largest Islamic Organization Tells Isis to Get Lost. The Huffington Post. https://www.huffingtonpost.com/entry/indonesian-muslims-counter-isis_us_565c737ae4b072e9d1c26bda?guccounter=1

Veilleux-Lepage, Y., & Füredi, Z. (2025). Beyond the FGC-9: How the Urutau redefines the global 3D-printed firearm movement. GNET. https://gnet-research.org/2025/01/08/beyond-the-fgc-9-how-the-urutau-redefines-the-global-3d-printed-firearm-movement/

Wan Rosli, W. R. (n.d.). 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

Ware, J. (2023). The third generation of online radicalization. Program on Extremism at George Washington University. https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/2023-06/third-generation-final.pdf

West, L. J. (2021). The impact of technology on extremism. In L. Close & D. Impiombato (Eds.), COUNTERTERRORISM YEARBOOK 2021 (pp. 29–32). Australian Strategic Policy Institute. http://www.jstor.org/stable/resrep31258.9

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

Wibisono, A. A., Kumendong, R., & Maulana, I. (2024). Indonesia's Handling of Terrorists' Cyber Activities: How Repressive Measures Still Fall Short. Journal of Asian Security and International Affairs, 12(1), 134-160. https://doi.org/10.1177/23477970241298764 (original work published 2025)

Wiegold, L., Winkler, C., & Jaskowski, J. (2024). Camera, action, play: An exploration of extremist activity on video- and livestreaming platforms. GNET. https://gnet-research.org/2024/07/18/camera-action-play-an-exploration-of-extremist-activity-on-video-and-livestreaming-platforms/

Yani, A. A. (2021). An examination of Indonesia's Anti-Terrorism policy during the COVID 19: The rise of Digital-Based Terrorism Propaganda among Youths. Hasanuddin Journal of Social & Political Sciences, 1(2), 77–85. https://journal.unhas.ac.id/index.php/hjsps/article/view/19920

Yilmaz, K., & Atamuradova, F. (2022). A comparative analysis of ISIS Channels On Telegram. Sicurezza, Terrorismo E Società, 16, 67-68. https://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2022/12/SicTerSoc16-Kamil-Yilmaz-%E2%80%93-Farangiz-Atamuradova-A-comparative-analysis-of-ISIS-Channels-On-Telegram.pdf

Zao-Sanders, M. (2025, April 9). How people are really using gen AI in 2025. Harvard Business Review. https://hbr.org/2025/04/how-people-are-really-using-gen-ai-in-2025

Annex A: Summary of Country Presentation Session

At the close of the research, Hedayah, in collaboration with Indonesia's BNPT, hosted a hybrid session in Jakarta, Indonesia on June 19th 2025 to present the findings of the research, to allow for questions and discussion with stakeholders who had participated in research, and to highlight complementary research and activities led by the Indonesian government.

Opening Remarks

Opening remarks were kindly given by:

- Mr. Andhika Chrisnayudhanto - Deputy for International Cooperation, National Counter Terrorism Agency of the Republic of Indonesia (BNPT)
- Ms. Esther Perry - Councillor, Australian Embassy in Jakarta
- Ms. Anna Sherburn - Deputy Executive Director, Hedayah

The distinguished speakers highlighted the range of efforts ongoing to address extremism and violent extremism online, the importance of continuing to understand and respond to this challenge, and reaffirmed commitments to such efforts.

Discussion Panel

Framed by these remarks, the session proceeded with a research discussion panel.

This included the presentation of results on the Indonesia Country Report on Understanding & Preventing Extremism and Violent Extremism Online in Southeast Asia authored by Hedayah. More information on Hedayah's findings and recommendations can be found in the earlier sections of this Country Report.

A presentation from the Ministry of Communication and Digital Affairs (Digikom) outlined their mechanisms for content moderation, and how these processes work in practice, providing vital context on the methods used and the challenges associated with such efforts. A key recommendation highlighted was encouraging increased media literacy and awareness of extremism challenges and content, not just for government but among other key actors, and expanding cooperation with other agencies to better respond to these threats and needs.

A presentation from BNPT's Indonesia Knowledge Hub on Countering Terrorism and Violent Extremism (I-KHub on CT/VE) shared results from their recent Outlook. Noting the decrease in attacks linked to ongoing government responses, this presentation also noted increasing trends of extremist content seen across multiple platforms. Therefore, it highlighted the need to consider the intersection between the technical threat and social vulnerability, which together shape the context of radicalization. Key recommendations included strengthening non-formal approaches to resilience building and investing in regional efforts to utilize artificial intelligence to detect extremist content with the engagement of civil society partners.

This Outlook and other products are available on the I-KHub at www.ikhub.id.

Feedback & Discussion

Following these presentations, time was taken for questions and discussion with attendees. This discussion highlighted the following:

- Ongoing challenges around gender and inclusivity: Highlighting positively that this Country Report mentions these challenges, and emphasizing that narratives around extremism, violent extremism and terrorism online are never gender neutral, and usually targeted based on gender, even noting trends of extremist or violent extremist groups co-opting language from women's rights to advocate for engaging in violent extremism to support women's bodily autonomy. The use of regressive gender narratives by extremist and violent extremist offline also poses a risk of spilling over to offline spaces and discourse, echoing the Country Report's findings on incivility, and further emphasizing the need to ensure that marginalized groups which are not seen as vulnerable to extremist and violent extremist narratives are not ignored by counter extremism efforts, and can be partners in potential responses.
- The role of effective counter narratives in reducing radicalization: Emphasizing the need for collaborative efforts to create and disseminate counter narratives (or positive and alternative narratives), noting that takedowns (i.e., content moderation) efforts may be strong but new content is constantly generated and we cannot rely on moderation efforts alone to build online resilience and prevent extremism online.
- The changing landscape online, media and information literacy, and artificial intelligence: Emphasized the challenge posed by low digital and media and information (MIL) literacies, particularly in the face of generative AI, noting the need to continue to monitor the emergence of new technologies.

Questions raised by participants regarding the findings of the research also included:

- What trends were noted in the report around how online tools were used to recruit, radicalize and mobilize, in order to support prioritization of efforts and strategic interventions.
- Which groups are most prolific in sharing extremist or violent extremist content online?
- What is the intent in terms of targeting young children in gaming platforms, and what are the goals of such efforts?
- What types of extremist or violent extremist content, and what types of narratives, are evolving currently online? How may global political events be shaping and amplifying the messaging of local Indonesian content?

Participating Stakeholders

The session was attended (in-person and online) by representatives from the following organizations:

- National Counter Terrorism Agency (BNPT)
- Ministry of Communications and Digital Affairs
- Counterterrorism Special Detachment 88 (INP)
- Ministry of Foreign Affairs
- National Cyber and Crypto Agency
- Ministry of Religious Affairs
- Ministry of Primary and Secondary Education
- Australian Embassy Jakarta
- British Embassy Jakarta
- Activism Beyond Borders
- Center for the Study of Radicalism and Deradicalization (PAKAR)
- International NGO Forum on Indonesian Development (INFID)
- PeaceGeneration Indonesia
- AMAN Indonesia
- Wahid Foundation
- Nanyang Technological University
- Hedayah

Hedayah thanks all those who took part in the research and shared their expertise and feedback through the research process, and those who attended this event.

Hedayah

Countering Extremism
& Violent Extremism

WWW.HEDAYAH.COM

HEDAYAH_CVE

HEDAYAH