International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cross-Border Digital Narratives: India's Evolving Response to Online Extremism from Arab Conflict Zones

Simpal Tripathi[1], Akhilendra Kumar Singh[2], Prof. Mamta Mani Tripathi[3]

[1,2]Research Scholar, Department of Political Science, Deen Dayal Upadhyay Gorakhpur University (DDUGU), Gorakhpur, Uttar Pradesh
[3]Principal, Udit Narayan Post Graduate College, Padrauna, Kushinagar, Uttar Pradesh

Abstract:
The proliferation of extremist content across national borders represents a critical challenge in the digital era. This paper examines how propaganda originating from Arab conflict zones is localised and disseminated within India's complex online ecosystem. Through qualitative digital trace analysis, semi-structured interviews with fact-checkers, cybercrime officials, and community organisers, as well as limited observation of encrypted online groups, the study investigates how foreign extremist material is adapted to exploit domestic socio-political and communal divisions.
Findings indicate that while India has strengthened its legal and technological responses—such as expanded surveillance and stricter intermediary liability rules—these measures are often outpaced by the agility of extremist networks. Messaging is reframed in regional languages, circulated via encrypted platforms, and promoted by a network of domestic actors, including fringe religious leaders and opportunistic social media influencers. Such tactics significantly limit the efficacy of conventional censorship and takedown approaches.
The research argues that sustainable counter-extremism efforts must move beyond reactive regulation. Building grassroots resilience—through community entered digital literacy initiatives and strategic partnerships with independent fact-checking organisations—emerges as a more promising approach. Comparative insights from Germany, the United States, and Indonesia suggest that combining legal enforcement with civic engagement and platform accountability produces stronger results in combating transnational digital extremism.
Situated within the broader context of global information flows, this study addresses a notable gap in scholarship on the re contextualisation of conflict-zone narratives in regional settings. It concludes with targeted recommendations for a multi-layered policy framework that upholds fundamental rights while addressing both the social drivers and technological vectors of extremist content.

Keywords: cross-border extremism, digital propaganda, Arab conflict, radicalisation, counter-narratives, digital literacy, policy response.

INTRODUCTION

Over the past two decades, armed conflicts in parts of the Arab world have not only reshaped regional politics but have also transformed the global dissemination of extremist ideologies. Groups such as Al-Qaeda and the so-called Islamic State (ISIS) have weaponised the internet, deploying emotionally charged narratives, sophisticated videos, and calls for transnational solidarity that reach audiences far beyond conflict zones (Badawy & Ferrara, 2017). Where once extremist propaganda moved through covert networks and word-of-mouth, it now spreads rapidly via Twitter hashtags, private Telegram channels, and encrypted messaging apps, complicating efforts to trace and disrupt these flows (Ceron, Curini & Iacus, 2018).

Cyber trolls are increasingly active in India's massive and complex online space, which now includes over 881.3 million users across diverse languages and regions. This diversity also makes it more vulnerable to challenges like misinformation, hate speech and the spread of extremist ideas. Religious leaders and politically motivated influencers have been known to reuse videos or images from conflict zones such as Syria or Yemen to circulate, to arouse strong emotions and deepen political or community-based tensions within the country.

In response to such concerns, the Indian government has implemented stricter digital regulations. The revised Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules of 2021 place increased accountability on digital platforms to identify and remove unlawful or extremist content. Under these rules, platforms with more than 5 million users must appoint compliance officers, provide verifiability to originators of messages and respond to grievances within 24 hours. Failure to comply can result in legal liability or even platform bans. Law enforcement agencies have also expanded their cyber surveillance capabilities, employing artificial intelligence and big data analytics to monitor digital communication. Indian Cyber Crime Coordination Centre (I4C) and state-level cyber cells are working in collaboration with major tech companies like Meta and Google to track and disrupt the spread of radical networks, particularly on encrypted apps like Telegram and WhatsApp, which is used to recruit and radicalise youth. However, these measures' effectiveness and ethical implications remain subjects of ongoing debate. Digital rights activists hold that, although such policies may limit the privacy and freedom of expression, they fail to address the underlying socio-economic and psychological factors, such as unemployment, marginalisation and identity-based grievances, that make individuals vulnerable to radical ideologies, hence there is need for more holistic approach which covers both root cause and also makes balance between security and human rights, offering more sustainable path to counter radicalisation in global age.

Censorship or takedowns can push extremist conversations into more private and less visible parts of the internet. Thus, this can alienate communities whose support is essential for long-term counter-extremism efforts. 2023 report by the Observer Research Foundation (ORF) noted that without parallel efforts in community engagement, digital literacy, and mental health support, policy enforcement alone may only offer a short-term solution. Hence, solutions must go beyond regulation and include proactive steps that build digital literacy, strengthen community trust and help people resist manipulation.

The main aim of this paper is to examine how radical narratives originating from Arab conflict zones are adapted and expanded within Indian cyberspace. It identifies key actors involved in religious extremism, political opportunists, and online troll networks. Further, the paper addresses notable gaps in the current literature, particularly concerning how local socio-political dynamics shape the reception and reinterpretation of transnational extremist content.. Finally, the paper advocates for a more holistic,

Community-entered approach to countering online extremism. It includes policy reform that balances security with civil liberties, civic education to build digital literacy and resilience, greater accountability from digital platforms, and localised engagement strategies that empower community leaders, educators, and civil society organisations. Such an integrated response is essential to effectively confront the transnational and evolving nature of digital radicalisation

Problem Definition

India is facing a complex and evolving security challenge rooted in the online spread of radical ideologies influenced by conflicts in regions like Syria, Iraq and Yemen. In the age of digital globalisation, the diffusion of extremist ideology within India's digital sphere is the main concerning issue. As the ease flow of unregulated and uncontrolled messages are often edited and emotionally reframed to provoke reactions, especially during periods of tension—such as videos from Aleppo or Gaza reappearing in Indian WhatsApp groups to agitate division in Uttar Pradesh. Current counter-extremism efforts primarily target surface-level symptoms like content removal and account suspensions. Still, they fail to address why people are drawn to such content or how local actors weaponise foreign imagery. The real challenge is not a one-time wave of foreign influence, but a steady, emotionally charged, and locally adapted flow of content that deepens divisions, erodes public trust and threatens the integrity of India's digital and social fabric, thus effecting societal harmony.

Knowledge Gap

While high-profile terrorist attacks often dominate media coverage, there remains a surprising lack of in-depth academic research on how global jihadist narratives are repurposed and circulated within India's densely populated digital spaces. Existing literature has explored the spread of fake news and hate speech in Indian languages (Mathew et al., 2019), as well as the mechanisms of extremist recruitment in Europe and the Middle East. However, detailed empirical work examining how Arabic or Urdu-language extremist content is adapted, translated, and shared within India, particularly across regional languages—remains notably scarce.

There is limited understanding of the actors responsible for this translation and adaptation. Questions remain unanswered: Who modifies these messages for Indian audiences? How are foreign narratives tailored to exploit local fears, historical grievances, or communal rivalries? Which networks—whether fringe religious leaders, social media influencers, or anonymous administrators—facilitate their distribution across platforms?

Equally under-explored is the behaviour of everyday users. Do individuals share such content because they sympathise with its message, out of fear, or simply due to its shock value? Furthermore, while India's updated internet regulations (Ministry of Electronics and Information Technology, 2021) have placed greater responsibility on platforms to remove extremist content swiftly, there is little empirical evidence assessing the real-world impact of these interventions. Specifically, it remains unclear whether top-down content removals effectively curb radicalisation or merely displace harmful material into harder-to-monitor spaces, such as encrypted apps and closed groups.

This paper seeks to address this significant blind spot by mapping the adaptation, dissemination, and reception of cross-border extremist narratives within India's digital ecosystem, and by evaluating the effectiveness of current regulatory responses in countering such content.

Issues This Paper Tackles

This study seeks to develop a deeper and more context-specific understanding of how transnational extremist narratives take shape and spread within India's digital ecosystem. It focuses particularly on the ways in which propaganda linked to conflicts in Arab regions is reshaped for Indian audiences. The research explores how such content whether visual, audio, or video is translated, reframed and emotionally charged to align with local political and communal dynamics.

How Narratives Cross Borders and Take Root

Building on these concerns, this section explores how extremist narratives, originally crafted in the context of Arab conflict zones, are re contextualised and embedded within India's digital landscape. While much has been written about the mechanics of propaganda production in the Middle East, less attention has been paid to how these messages are transformed as they traverse linguistic, cultural, and political boundaries. Extremist groups operating in the Arab world have demonstrated considerable expertise in producing emotionally charged content that emphasises fear, outrage, and perceived victimhood (Badawy & Ferrara, 2017). These materials—typically short videos, sermons, or audio clips—are optimised for digital vitality and often stripped of geographic specificity to enhance their universal appeal. However, when such content enters Indian digital spaces, it rarely appears in its original form. Somewhere along the chain, it is localised: subtitles are added or altered, clips are shortened or re-edited, and captions are rewritten in Urdu, Hindi, Malayalam, or other regional languages to resonate with targeted audiences.

Private messaging platforms like WhatsApp and Telegram serve as the primary vectors for this adapted content. Due to having an end-to-end encrypted system, the message can only be seen by the sender and receiver, making it difficult for a third party to monitor communication. Hence, these private or semi-private spaces allow for the rapid, unchecked circulation of extremist material. Content shared in these spaces is often framed as exclusive, "leaked," or censored elsewhere, lending it an air of authenticity and top priority that fuels its spread, especially during communal tension and protest.

The spread of extreme content is often supported and shared by local figures who help adapt and promote the material for different audiences. These may include lesser-known religious leaders, self-appointed speakers, social media influencers and anonymous group moderators. Their reasons for sharing such content vary. Some strongly believe in the messages they promote, while others use them to gain attention, build followers or influence public opinion. For example, research by the Institute for Strategic Dialogue (2023) showed that fewer than 10% of users were responsible for more than 70% of harmful online content during times of social tension. Personal belief, political goals and the desire for online popularity are often closely connected.

This process highlights the need to move beyond the binary "foreign versus domestic" radicalisation framework. For instance, videos depicting the conflict in Aleppo, Syria, have been widely circulated in regions like Uttar Pradesh—not by organised extremist groups, but by ordinary users. Such widespread circulation reflects how international events, intertwined with local grievances and adapted by online actors such as cyber trolls, can rapidly invade digital spaces. Encrypted platforms further complicate efforts to trace, verify or regulate such content. In this context, digital globalisation facilitates a fusion of global and local narratives, rendering the foreign–domestic distinction increasingly obsolete in understanding radicalisation dynamics. This further calls for more cooperative, multi scaler and community connected policies like network awareness to tackle extremism strategies.

Why the Infrastructure Matters

The spread of cross-border extremist narratives is made even more powerful by India's vast and uneven digital landscape, which allows such content to circulate widely and stay active over time. A key factor that makes India especially vulnerable is the massive growth of its online population. In the past decade, hundreds of millions of people have gained internet access, often through low-cost smartphones and without formal training in how to identify reliable information. As a result, dramatic or emotional messages are often shared without being verified. Some people share because they believe the message, while others do so simply because it is shocking or attention-grabbing. In many smaller towns and rural areas, access to fact-checking tools or trusted information sources is limited, making it easier for rumours to mix with extremist narratives. This challenge is made worse by the diversity of languages and scripts across the country, which makes it difficult for major platforms like Meta or Google to moderate harmful content effectively.

Even the most advanced algorithms struggle to detect misleading videos hidden behind false hashtags or accounts with fake identities (Chakraborty et al., 2021). Once such content enters private messaging groups, it can remain there for years and be reused whenever it supports a particular agenda. Hence, it is need of the time, to establish institutional frameworks capable of tackling emerging non-traditional security challenges

Gaps in the Current Playbook

The structural weaknesses are made worse by gaps, which focus more on visible enforcement than on long-term prevention of countering extremism. Indian government primary focus over legal provision and surveillance to counter cyber sphere threats . Laws like Unlawful Activities Prevention Act and Information Technology Rules, which works upon the top down centre approach, such laws mainly allows authorities to remove content and take legal action against the anti state activities and the person who commits such activities. Such visible enforcement lacks long term prevention as they lack to tackle soft radicalisation issues of the people under which they get influenced by ideologies through continuous messagings. When people worry that any interaction with radical content, whether out of curiosity, concern or criticism, could lead to being labelled a supporter, they may avoid reporting suspicious behaviour or participating in open discussions. In addition, because extremist groups and accounts can easily reappear under new names, each ban or takedown is often followed by another similar presence, which creates a vicious cycle where enforcement struggles to keep up with the constantly changing digital tactics such actors uses.

What the World Shows us

Early preventive intervention and community involvement have been seen as a prominent tool in combating radicalisation. Countries like the UK and Germany follow early preventive and community involvement tools to prevent radicalisation. In the UK, radicalisation is controlled through monitoring and training teachers, social workers and even parents to recognise the early signs of radicalisation (Neumann, 2013). Under the Hayat program in Germany, vulnerable youth are focused on building trust through policies with the help of families. In Asia, repeated challenges from radical groups have emerged in recent years with international links. Under such circumstances, Indonesia follows a training programme for religious leaders and runs a local awareness programme to tackle online radicalisation.

Methodology

This study adopts a qualitative design combining digital trace analysis with interviews and limited online observation. It is guided by two core questions:

1. What kinds of conflict-zone narratives are being reframed for Indian audiences?
2. How effective are India's existing digital monitoring and counter-extremism frameworks in responding to such content?

Data Collection

A case-based approach was used to track specific pieces of content—videos, images, and short texts—that originated in regions like Syria, Iraq, or Palestine and later reappeared in India during periods of communal or political tension. These cases were selected from verified fact-checking sources such as Alt News, BOOM Live, and India Today Fact Check. Supplementary material came from news reports, legal filings, and official press releases. Wherever possible, the digital path of such content was traced to understand how it was reframed and timed with domestic events.

Semi-Structured Interviews

Between January and April 2025, sixteen semi-structured interviews were conducted with individuals directly involved in monitoring or responding to digital extremism: six fact-checkers, four former cyber cell officials, three community organisers, and three journalists. Interviews were conducted in person or via secure channels (e.g., Signal), and focused on how extremist content is encountered, adapted, and interpreted in local contexts.

Limited Digital Observation

To supplement the above, limited non-participatory observation was carried out in a small number of closed Telegram groups where such content is often shared. The aim was not to map entire networks, but to observe how original media is translated or reframed for Indian audiences. A research-only account was used, and no interaction with participants occurred.

Analytical Strategy

An inductive, theme-based coding approach was applied to both digital content and interview transcripts. Common patterns—such as visual tropes, religious framings, or reuse of old footage—were identified, especially in response to specific Indian events. Where available, government takedown orders (Ministry of Electronics and Information Technology, 2025) were compared against actual online activity to highlight gaps between policy and practice.

Ethical Considerations

Strict ethical protocols were followed. All interview participants provided informed consent, and no identifiable information is included. Observational data was anonymised, and no extremist content was shared, downloaded beyond what was essential, or redistributed in any form.

Discussion

Information circulation doesn't depends on national boundaries in the digital globalisation age. Conflicts occurring in one part of the world can now be instantly absorbed into the socio political fabric of distance

societies. Under such the conflict related digital content from regions like Syria and Gaza, shapes and reframe domestic political narratives in India. A recent case from March 2025 involved a video of Syrian fighter that was misrepresented as footage from Kashmir in the aftermath of the Pahalgam terror attack. Although this claim was quickly debunked by independent fact-checkers, the video still gained resistance across encrypted platforms, demonstrating how easily foreign content can be co-opted and localised to serve regional agendas. The interviews in this study show a clear pattern: misleading or harmful content often reappears during times of communal tension or political protest.

This trend can be seen in cases from Kerala; Kasaragod (2016) and Palakkad (2020). These cases show that online radicalisation in India is being increasingly influenced by ideas coming from conflicts in Arab countries. In both areas young people used encrypted apps and watched extremist content related to the wars in Syria, Iraq and Palestine. Apps like Telegram and WhatsApp were used to secretly recruit and indoctrinate individuals, while platforms like YouTube and Facebook shared videos that praised violence and martyrdom.

To contextualise this phenomenon, Table 1 categorises the online tools involved and their specific roles in propagating extremism:

Table 1: Online Tools and Their Role in Extremism Propagation

Tool Category	Examples	Role in Extremism Propagation
Mainstream Social Media	Facebook, Twitter, YouTube	Dissemination of propaganda; creation of echo chambers; viral spread of misinformation and recruitment content
Messaging Apps	WhatsApp, Telegram	Encrypted private channels used for recruitment, radicalisation, planning, and sharing extremist manuals
Video Platforms	YouTube, Facebook Videos	Dissemination of ideological propaganda; glorification of violence; tutorials for radical action
Blogs and Forums	Niche ideological blogs, forums	Sharing of manifestos, radical literature; ideological networking for deeply engaged users
Memetic and Visual Media	Memes, infographics, viral images	Emotional propaganda targeting youth; simplification of complex ideas through viral formats

This table demonstrates how a wide spectrum of digital platforms contributes to the radicalisation ecosystem. From mainstream apps to niche online communities, each plays a distinct role in fostering extremist discourse.

Expanding upon this, Table 2 links specific conflict triggers—such as communal riots or insurgencies—to the radicalisation processes and tools involved. It underscores how online platforms amplify grievances and convert them into pathways for mobilisation.

Table 2: Influence of Conflicts on Extremist Groups via Online Tools

Conflict Trigger	Radicalisation Process	Online Tools Utilised	Propagation Methods / Functions
Communal Tensions(e.g., Muzaffarnagar riots)	Grievances → Emotional arousal → Group identity framing	WhatsApp, Facebook, YouTube	Viral videos, hate speech, misinformation, community polarisation

Conflict Trigger	Radicalisation Process	Online Tools Utilised	Propagation Methods / Functions
Kashmir Insurgency Conflict	Personal/political grievances → Ideological adoption → Mobilisation	Telegram, YouTube, encrypted messaging apps	Video propaganda, recruitment, encrypted communications
Right-Wing Extremism (Cultural Nationalism)	Collection of grievances → Online community building → Action	Facebook groups, Twitter, Instagram	Memes, conspiracy narratives, mobilisation via online calls to action
Left-Wing Extremists(Naxal Movement)	Socioeconomic grievances → Radical discourse → Offline violence	Blogs, YouTube, encrypted social media	Ideological literature, recruitment via grievances

After a deep analysis of the two tables presented above, we find clear support for the trends discussed. The first table shows how various digital tools—from mainstream social media to niche blogs—aid extremist propagation by circulating propaganda, forming echo chambers, and distributing radical content. The second table connects specific conflict triggers to online radicalisation pathways, emphasising how socio-political grievances are amplified digitally, leading to real-world consequences. In the Kerala context, grievances over global Muslim victimhood were reframed locally through digital networks—particularly via memes, encrypted chats, and ideological videos—mirroring the structural logic in these tables. Thus, both visuals and the Kerala case highlight how Arab-world conflicts are repurposed online to radicalise and mobilise individuals in Indian regions.

Closed platforms like Telegram have observed that these actors are not merely spreading misinformation but are critically curating it, showing the elaborate and strategic adaptation of global narratives into their domestic contexts. This indicates that cross-border influences contribute to deepening societal divisions, increasing public distrust and exposing significant weaknesses in regulatory enforcement mechanisms in India. Taneja (2021) explains that VoH (Voice of Hind) magazine presents global issues such as the persecution of Muslims in Syria and Palestine as local problems by linking them to communal violence, political marginalisation and perceived discrimination by the Indian state. They appeal emotionally by using stories of martyrdom, violent imagery and messages calling for religious unity. This orientation is consistent with what Badawy and Ferrara (2017) describe as the "blending of extremist messages". These messages often build mistrust within Muslim communities, particularly in sensitive regions such as Lucknow, Hyderabad and Kashmir.

Addressing the spread of extremist content requires more than just top-down censorship, as it demands more grassroots engagement and genuine community involvement. Countries like Indonesia, Britain and Germany have shown that community involvement can bring significant changes. These country policies show that through preventive community-based programs, people feel heard and supported, and as a result, they're far less likely to be drawn into destructive ideologies. In India, empowering educators, clerics and civil society leaders to speak directly to their communities with culturally relevant counter-narratives could have similar impact.

It is also noticeable that people who share harmful content online do so without full awareness. 64% of users spreading extremist messages in India were unaware of the content's true nature (Mathew et al., 2019). This highlights a serious need for digital education at the ground level. With over a billion mobile

users, India has a unique opportunity. By investing in school-based programs, community workshops and mobile-friendly fact-checking tools, we can equip people with the skills to question and verify what they see online.

Holding platforms accountable is another crucial dimension. Despite the 2021 intermediary guidelines, only a fraction of harmful content is being effectively removed, especially on encrypted apps like WhatsApp and Telegram, which serve over 881 million users. Germany's NetzDG law, which has achieved rapid takedown of illegal content (Heldt, 2019), offers a blueprint. India can adapt preventive models, ensuring more vigorous enforcement while safeguarding freedom of expression and respecting cultural diversity. This will boost societal harmony, resulting in trust amongst different sections of society. But regulation must be handled with care. Heavy-handed or unclear laws—such as the now-defunct Section 66A—can backfire, creating fear, fuelling mistrust, and deepening societal divides. That's why ensuring transparency, judicial oversight, and clear legal standards is critical to curing the problem of online radicalisation. Partnerships at community grassroots levels could also enhance the early identification of dangerous content, making prevention a shared responsibility of the citizens. As extremist narratives is depends local grievances of the citizens, hence human centred approach that builds trust, emotional awareness and long term resilience is the need of time; to close the gaps on which these narratives exploits.

Conclusion

The study reveals that extremist digital narratives originating in Arab conflict zones do not merely enter India's online space—they are deliberately reshaped to align with local frustrations and social dynamics, seen through the mentioned cases. Through digital trace analysis, interviews and observations across encrypted platforms, it becomes clear that the actual danger lies not in the content's origin but in how it's emotionally re-contextualised in the specific context. These narratives gain traction because they are made to feel deeply personal; memes, local-language videos and private messaging apps like WhatsApp and Telegram carry these ideas in a form that blends seamlessly with everyday digital life. In states like Kerala, global themes of Muslim victimhood are adapted to reflect regional concerns, blurring the line between personal grievance and global ideology. Although state-led monitoring and takedowns policies remain essential, they often fall short when facing the slow, subtle spread of radical influence in decentralised, emotionally charged digital ecosystems which makes situation more complicated.

Addressing this challenge requires shifting from top down approach to more bottom up approach, where connection also plays important role along with control. Communities need more than regulations; they need people they trust under such government should focus over education civil society. Policies must also focus over educators, social workers and local fact-checkers. So that they can uniquely placed to offer grounded, culturally relevant alternatives before extremist ideas take hold. International examples like Indonesia's cleric-led initiatives or the United Kingdom's community-based preventive model show the potential of early, community-based intervention. At the same time, platforms must not treat encryption as an excuse for inaction. Transparent standards and local enforcement are crucial and legal responses must balance urgency with fairness to preserve free expression. Ultimately, the research underscores that radicalisation succeeds through content and emotional resonance amplified by social fault lines. Combating it will take long-term investment in digital literacy, inclusive storytelling and resilient communities—because only a people-first approach can truly protect democracy in India's rapidly expanding digital world, as technology shapes options and democratic empowerment begins with ensuring

that all individuals have equal access to credible and reliable information.

References

1. Awan, I. (2017). Cyber-extremism: ISIS and the power of social media. Society, 54(2), 138–149. https://doi.org/10.1007/s12115-017-0114-0
2. Badawy, A., & Ferrara, E. (2017). The rise of jihadist propaganda on social networks. Journal of Computational Social Science, 1(2), 453–470. https://doi.org/10.1007/s42001-018-0015-z
3. Bertelsen, P. (2015). Danish preventive measures and de-radicalization strategies: The Aarhus model. In C. Bjørgo (Ed.), Preventing crime: A Holistic Approach (pp. 241–256). Palgrave Macmillan.
4. Bradshaw, S., & Howard, P. N. (2019). The global disinformation order: 2019 global inventory of organised social media manipulation. Oxford Internet Institute. https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf
5. Ceron, A., Curini, L., & Iacus, S. M. (2018). ISIS at its apogee: The Arabic discourse on Twitter and what we can learn from that about ISIS support and foreign fighters. https://air.unimi.it/retrieve/dfa8b99e-624d-748b-e053-3a05fe0a3a96/air-isis.pdf
6. Freedom House. (2022). Freedom on the Net 2022: Countering an authoritarian overhaul of the internet. Freedom House. https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet
7. Heath-Kelly, C. (2017). The geography of pre-criminal space: epidemiological imaginations of radicalisation risk in the UK Prevent Strategy, 2007–2017. Critical Studies on Terrorism, 10(2), 297-319. https://doi.org/10.1080/17539153.2017.1327141
8. Heldt, A. P. (2019, June 12). Reading between the lines and the numbers: An analysis of the first NetzDG reports. Internet Policy Review, 8(2). https://doi.org/10.14763/2019.2.1398
9. Ingram, H. J. (2016). An analysis of Islamic State's Dabiq magazine. Australian Journal of Political Science, 51(3), 458–477. https://doi.org/10.1080/10361146.2016.1174188
10. Institute for Strategic Dialogue. (2025). Think tank operations and insight into disinformation ecosystems. Retrieved from ISD publications Wikipedia
11. Institute for Strategic Dialogue. (2023). Uisce Faoi Thalamh: Landscape study of mis- and disinformation in Ireland (2020–2023) Wikipedia+7ISD+7ofcom.org.uk+7
12. Institute for Policy Analysis of Conflict. (2019, April 29). The ongoing problem of pro-ISIS cells in Indonesia (IPAC Report No. 56). https://understandingconflict.org/en/publications/The-Ongoing-Problem-of-Pro-ISIS-Cells-in-Indonesia
13. Mathew, B., Illendula, A., Saha, P., Sarkar, S., Goyal, P., & Mukherjee, A. (2019, September 24). Hate begets hate: A temporal study of hate speech (arXiv preprint arXiv:1909.10966). arXiv. https://doi.org/10.48550/arXiv.1909.10966
14. Ministry of Electronics and Information Technology. (2021). Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Government of India. https://www.meity.gov.in
15. Neumann, P. R. (2013). The trouble with radicalization. International Affairs, 89(4), 873–893. https://www.jstor.org/stable/23479398
16. Nisa, E. F. (2018). Social media and the birth of an Islamic social movement: ODOJ (One Day One Juz) in contemporary Indonesia. Indonesia and the Malay World, 46(134), 24–43. https://doi.org/10.1080/13639811.2017.1416758

17. Shahbaz, A., & Funk, A. (2022). Freedom on the Net 2022: Countering an authoritarian overhaul of the internet.Freedom House. https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet
18. Tufekci, Z. (2017). Twitter and Tear Gas: The Power and Fragility of Networked Protest. Yale University Press. Also summarized via Wikipedia and scholarly reviews WIRED+12Wikipedia+12Wikipedia+12