RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 167 – 29 October 2024

RSIS Commentary is a platform to provide timely and, where appropriate, policy-relevant commentary and analysis of topical and contemporary issues. The authors' views are their own and do not represent the official position of the S. Rajaratnam School of International Studies (RSIS), NTU. These commentaries may be reproduced with prior permission from RSIS and due credit to the author(s) and RSIS. Please email to Editor RSIS Commentary at RSISPublications@ntu.edu.sg.

Social Media's Dark Side in Online Radicalisation

By Noor Huda Ismail

SYNOPSIS

Online radicalisation is a complex issue characterised by the different roles of digital propagandists and potential perpetrators, as highlighted by the recent security threats surrounding the Pope's visit to Indonesia. To combat this threat effectively, we need to prioritise real-time monitoring and interdisciplinary collaboration, utilising AI tools to analyse and mitigate extremist content while advocating targeted interventions instead of punitive measures. Addressing radicalisation necessitates collective societal action and significant investment of relevant resources.

COMMENTARY

As we navigate the complexities of online radicalisation, it becomes clear that different roles exist within the extremist landscape, especially among those active on platforms like Facebook, WhatsApp and TikTok. A striking dichotomy has emerged between individuals who use social media for propaganda and those who execute acts of violence.

This distinction became particularly evident from the security threats surrounding Pope Francis' visit to Jakarta, Indonesia, from 3 to 6 September 2024. We need to confront the reality that the platforms designed to connect us could also be breeding grounds for division and violence.

During the Pope's visit, Indonesian authorities coordinating efforts across multiple locations arrested seven persons. While two of them faced charges under terrorism laws for planning an attack, the others were linked to online radical discourse without direct violent involvement. These arrests underscore a critical reality: not all who spread extremist rhetoric online necessarily pose an immediate threat of violence, yet their influence can still be dangerous.

Those most active on social media often function as digital propagandists, inciting others with their rhetoric and amplifying extremist ideologies. Their reach extends beyond physical boundaries, requiring only a keyboard to inspire others to act. They use social media's anonymity to create a facade, spreading inflammatory messages and recruiting followers into radical networks. In this way, they wield significant influence without taking direct action themselves.

In contrast, those less visible online may represent a more immediate and tangible danger. These individuals, inspired by extremist messages, might take steps toward actual violence, executing plans developed from the incitement they encounter online. This difference between online propagandists and real-world actors highlights the complexity of online radicalisation, showing how a network of influence operates in both virtual and physical realms.

The Role of Social Media in Threat Detection and Intervention

During the Pope's visit, alerts from social media platforms like Facebook, WhatsApp, and TikTok proved vital for early intervention. These platforms flagged suspicious activities and provided the authorities with the necessary leads to prevent attacks. However, such vigilance also requires a robust response mechanism from law enforcement, emphasising the need for enhanced digital monitoring capabilities. Each piece of extremist content represents more than just words; it can translate into potential actions with real-world consequences.

The response to these incidents also sheds light on a nuanced approach to handling such threats. Authorities referred five of the arrested individuals to regional police rather than charging them under terrorism laws, recognising that not all cases of extremist rhetoric indicate an imminent threat. Some individuals may be seeking validation of their beliefs or connection with people of the same religious bent rather than actively planning violent acts. This distinction allows for more targeted interventions, prioritising psychological support over punitive measures when appropriate.

A recent case illustrates these complexities well. A food vendor from West Java who earned a meagre daily income became known for his inflammatory social media activity. He was remarkably active online, using aliases and anonymity to voice provocative messages about the Pope's visit. While his posts might have seemed trivial at first glance, they gained traction in the chaotic echo chambers of social media, where incendiary statements can quickly escalate into serious threats. Recognising his lack of real-world capabilities, authorities opted for his brief detention rather than imposing formal terrorism charges, offering psychological intervention as a more appropriate response.

This case highlights how social media platforms can become outlets for individuals seeking power and identity, especially when they feel marginalised or disregarded in their "offline" lives. It also illustrates how the lines between online bravado and genuine threats can blur, complicating the role of law enforcement in assessing risk.

Combatting Radicalisation: The Need for a Collaborative Approach

Under newly elected President Prabowo Subianto, who aims to tackle the sources of polarisation and radicalisation in online spaces, there is a pressing need for a comprehensive understanding of the issue. The Indonesian government holds a wealth of data on Indonesians radicalised online, providing a unique opportunity for deeper analysis.

From 2013 to 2022, Indonesian courts dealt with 721 terrorism-related cases, with 360 involving individuals radicalised through digital platforms. This mirrors global trends, including in Singapore, and the rise of internet subcultures like Incels in Western countries and far-right online extremism in the United States.

A comprehensive research initiative is needed, leveraging Indonesia's leadership through its National Counter Terrorism Agency (BNPT), international donor support, and collaboration with experts in social psychology, computer science, digital anthropology, and religious studies.

The methodology will include several key approaches.

- Social psychologists will conduct surveys and interviews with individuals exposed to radical content to understand their psychological profiles and cognitive vulnerabilities.

- Computer scientists will analyse algorithms and content recommendation systems on social media platforms to study how extremist content is promoted or suppressed. They will focus on data analysis of interactions, user engagement, and content patterns.

- Digital anthropologists will use ethnographic methods to explore digital communities and their dynamics, focusing on the narrative analysis of radical content and how online communities foster a sense of belonging.

- Religious studies scholars will examine the religious discourses used by radical groups online, identifying key themes and narratives that resonate with potential recruits.

- Field practitioners will collaborate with counter-terrorism experts, civil society organisations, and rehabilitation programmes to contextualise findings and design effective intervention strategies.

- Collaboration with online platforms such as Facebook, Instagram, TikTok, and Telegram will provide insights into content moderation practices, challenges in detecting radical content, and effective counter-narrative strategies.

The expected outcomes include actionable recommendations for digital platforms, policy suggestions for the Indonesian government, tools for NGOs and communities, and a framework for ongoing collaboration to counter online extremism while balancing freedom of expression and national security.

Conclusion

Thus, to counter the spread of radical ideologies online, we must understand the algorithms that amplify them, the psychological process that makes individuals vulnerable, and the communities that give them a home. Only through a united effort – bridging technology, social science, and frontline experience – can we reclaim the digital space and build resilience against extremism.

Noor Huda Ismail is a Visiting Fellow at RSIS and a strategic communication consultant for Southeast Asia with the United Nations Office on Drugs and Crime (UNODC). He also runs the award-winning interactive community website, www.ruangobrol.id.