RSIS COMMENTARY

29 May 2026

Beyond Counter Narratives: Why Indonesia Needs a Prosecutorial Turn on Online Extremism

Prakoso Permono and Nauval El Ghifari

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

RSIS 30

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

RSIS COMMENTARY

www.rsis.edu.sg No. 117 – 29 May 2026

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 with due credit to the author(s) and RSIS. Please email to Editor RSIS Commentary at RSISPublications@ntu.edu.sg.

Beyond Counter Narratives: Why Indonesia Needs a Prosecutorial Turn on Online Extremism

By Prakoso Permono and Nauval El Ghifari

SYNOPSIS

Counter-narratives, content blocking and removal, and digital literacy are insufficient to address the root causes of online radicalisation and violent extremist content. Law enforcement in Indonesia against those who produce and disseminate harmful content has proven to be inadequate. The authorities should recalibrate their approach to addressing violent extremism online.

COMMENTARY

Online radicalisation among youth, driven by an increasingly complex and ideologically diverse landscape, has become a major global concern. The 2026 Global Terrorism Index documents recruitment timelines compressed to days, sometimes even hours. Gaming communities are one such route, with 23 per cent of users encountering right-wing extremist propaganda. Indonesia is not exempt, and authorities are already investigating the recruitment of children into terrorism via platforms such as Roblox.

Many people have suggested that online radicalisation and the use of the Internet for violent extremism can be addressed through three main approaches: strengthening critical thinking and digital literacy; continuing to flag, report, block, and take down content; and actively engaging credible voices to deliver counter-narratives and strategic communication.

These measures have their limitations. Digital literacy shows promise but requires a long-term investment. Counter-narratives are less likely to work against those already consumed by violent extremism online, while flagging, taking down and blocking content are major undertakings that require vigilance and consistency, and involve substantial resources.

Underutilised Law Enforcement

While the above measures focus on the audience, on disrupting the distribution network, and on working against the echo chamber of algorithms, none of them addresses the recruiters, producers, and distributors. These measures overlook an existing tool: law enforcement, which is underused and has neither been adaptive nor extended into the digital world.

The inaugural report on terrorism trends, compiled by the National Counter-Terrorism Agency (BNPT), shows that 169 of 362 terrorist cases involve online activity, with only seven cases prosecuted for inciting violence online between 2023 to 2025. Furthermore, the Ministry of Communication and Digital Affairs and BNPT exposed 35,957 items of violent extremism and terrorism content across various digital platforms during the same period.

Less than 0.02 per cent of the total number of cases were charged with online violent extremist incitement. These were charged under Article 13A of the Counter-Terrorism Law Number 5 (2018), which applies to individuals associated with terrorism who incite others to commit violence and carry a maximum prison sentence of five years, depending on the court's assessment of the impact. Their activities include translating, sharing, and producing propaganda materials.

During the same period, most terrorists in Indonesia have been convicted under Article 15, which criminalises individuals who have committed terrorism or conspired to commit terrorism. This offence is considered legally easier to prove, as it primarily requires demonstrating a connection between the defendant and a terrorist network, often fulfilled by acknowledgement of *bay'at* with the Islamic State of Iraq and the Levant (ISIL) and involvement in pro-terrorist activities and meetings.

Law enforcement, including prosecution, against incitement to violence are, in fact, part of global calls. The UN Security Council Resolution 1624 (2005) underlines the importance of member states addressing and criminalising the incitement to and glorification of terrorist acts. In Indonesia, the law and regulations, often seen as a threat to civil liberty by unchecked authorities, are, in reality, a legal instrument that gives the state the right to protect the greater public good and a tool aimed at the producers, distributors, and digital platforms that harbour online violent extremist content.

Another issue is the lack of cross-agency coordination with the law enforcement process, despite BNPT serving as the coordinating agency. A BNPT report revealed that a Telegram channel, cited in at least 10 terrorism cases documented in police reports, prosecutors' indictments, and court rulings, remained online for at least three years before it was taken down. The channel, which was followed by 80 accounts, provided hundreds of pages of terrorist training materials, organised into 107 modules in Bahasa Indonesia.

Counter-Terrorism Paradigm Digital Shift

Online radicalisation should not be seen as a mere concern; it must transform the paradigm in counter-terrorism policy in digital space. This suggestion might prompt criticism of over-criminalisation and exacerbating the problem of overcrowded detention facilities. However, the philosophy underlying law and order is that every individual is accountable for their actions. The due process of law and cross-examination during trial should ensure justice for both the public and the accused.

At the policy level, Indonesia is slowly adapting to address the misuse of the digital world. The government launched a regulation on digital governance and the protection of children in 2025 – becoming the first in Southeast Asia to do so – to enforce a minimum age requirement for accessing social media, following in the footsteps of countries like Australia. This offers a promising short-term solution, although it has loopholes.

In addition, the new 2026 Presidential Regulation on the National Preventing and Countering Violent Extremism Action Plan also incorporates a specific theme: strategic communication, media, and electronic systems. It sets out mandates related to research, promoting alternative narratives, empowering credible voices and victims of terrorism, training and capacity building, and engaging with multistakeholders, including digital platforms, to address the growing misuse of the digital space.

In light of the recent influence of the far-right True Crime Community on youth across the region, law enforcement has become a more pressing issue. Earlier this year, the Indonesian National Police revealed 70 children across 18 provinces, mostly under 19, identified with far-right networks and at risk of committing violence arising from their online activities.

This development raises an important distinction between perpetrators and those exploited by extremist ecosystems online. These children are treated as victims rather than offenders, recruited and exploited online by violent extremist networks. This framing draws on a principle Indonesia co-sponsored and originally drafted at the United Nations, the resolution on the Treatment of Children Associated with Terrorist Groups, adopted by consensus at the session of the Commission on Crime Prevention and Criminal Justice (CCPCJ) in 2024, which holds that children recruited and exploited by such groups should be regarded as victims whose best interests are the primary consideration.

The people who bear true responsibility are the ones who, in the first place, incite, produce, and share content. The prevailing counter-terrorism law in Indonesia has designated offences to carry an additional one-third of the maximum penalty if they involve children under the age of 18. Although a good approach, engagement with digital platforms to take down malicious content frequently involves a lengthy bureaucratic process.

Regional law enforcement agencies should also be more adaptable. This is essential to the paradigm shift needed, especially given the requirement to preserve evidence

and the burden of proof in establishing, beyond a reasonable doubt, the connection between the content, its criminal intent (*mens rea*), and its links to terrorist networks. This is particularly challenging given the potential misuse of AI and creative content in producing less obvious violent extremist content, and requires robust human resources, with investigators equipped with an understanding of how violent extremists shape their narratives online.

Meanwhile, regional law enforcement's ability to detect early is credibly demonstrated by a series of arrests related to online terrorist activities. Last February, Malaysian authorities apprehended six youths aged 16 to 21 under the Security Offences [Special Measures] Act 2012 (SOSMA) for involvement in messaging groups discussing plots to attack the police and places of worship. Similarly, in Singapore, the authorities issued a restriction order under the Internal Security Act on a 14-year-old who had been self-radicalised online with ISIL ideology.

The successful apprehension of these individuals by regional authorities demonstrates the feasibility of enforcing the laws against content producers and distributors. Far from merely ensuring deterrence, retribution, and justice, it is the sole measure aimed directly at the source.

Conclusion

Takedown, prevention, and counter-narrative remain necessary components of Indonesia's response, yet they engage the audience and the channel, whereas the producer operates beyond their reach.

Law enforcement should therefore serve as the backbone that complements these approaches. Anchored in prosecutorial accountability for those who incite and disseminate, it is the one instrument that addresses the source rather than the symptom.

Prakoso Permono is a terrorism researcher with a PhD in Political Science from the Faculty of Social Sciences at Universitas Islam Internasional Indonesia. Nauval El Ghifari is a master's student in Strategic Studies at the S. Rajaratnam School of International Studies (RSIS), at Nanyang Technological University (NTU), Singapore.

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798

Please share this publication with your friends. They can subscribe to RSIS publications by scanning the QR Code below.