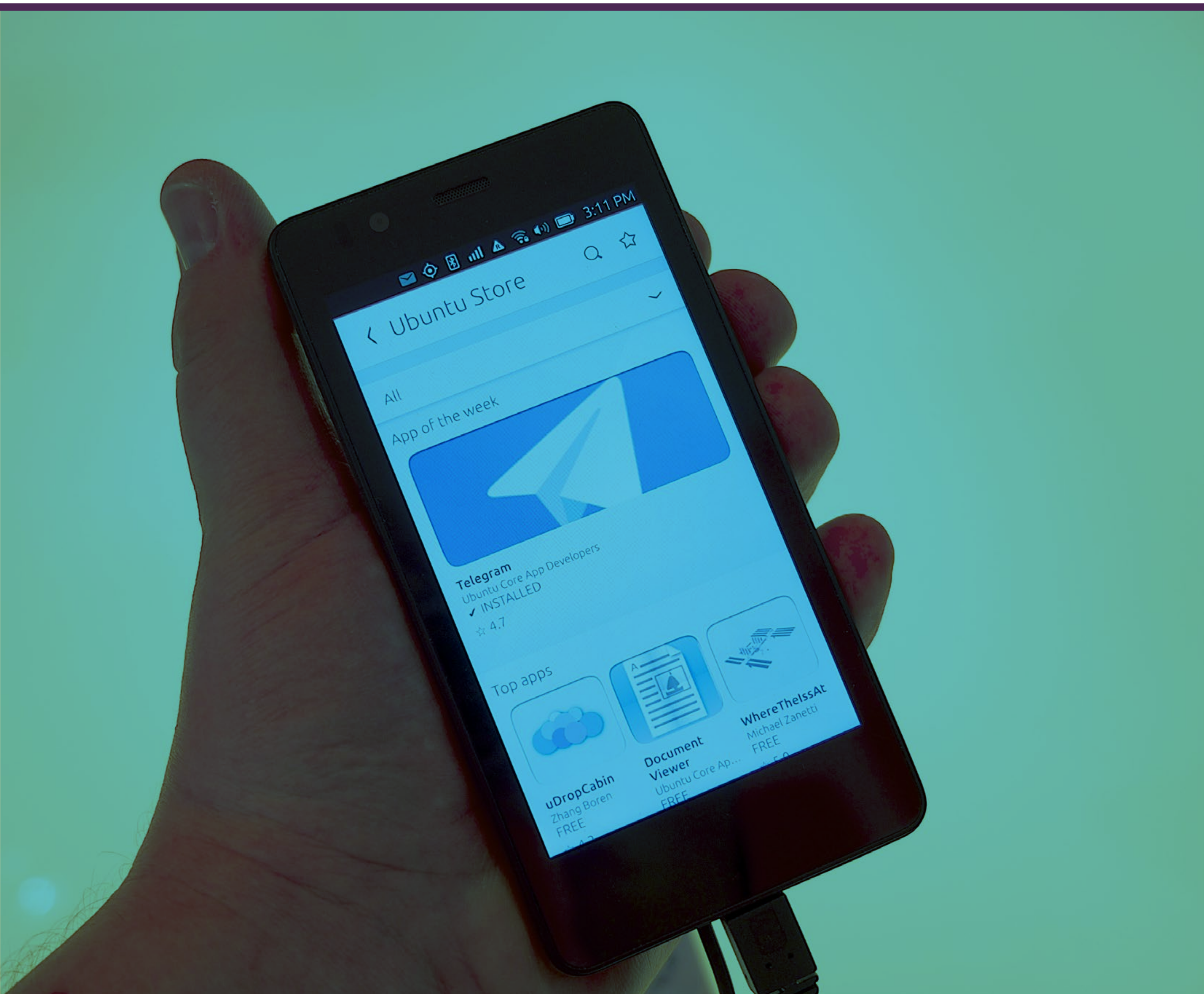
Royal United Services Institute
for Defence and Security Studies

INSTITUTE FOR POLICY ANALYSIS OF CONFLICT

Global Research Network on Terrorism and Technology: Paper No. 5

The Evolution of Online Violent Extremism in Indonesia and the Philippines

Nava Nuraniyah



Pro-Daesh (also known as the Islamic State of Iraq and Syria, ISIS) groups in Indonesia and the Philippines have come to rely on social media for propaganda, fundraising and disseminating instructional material, but in different ways. While Indonesian online extremism has deep roots, with local networks exploiting various online platforms over the past decade, extremist social media in the Philippines only really took off as a consequence of the May 2017 siege in the southern Philippine city of Marawi by pro-Daesh militants.

This paper outlines the evolving use of online platforms by pro-Daesh groups in both countries and how this has enabled extremists to develop and strengthen their networks. Social media and encrypted chat apps have shaped the development of extremism in Indonesia and the Philippines in four main areas: branding, recruitment, fundraising, and the increasing role of women. For groups in the Philippines, direct communication with Daesh headquarters via Telegram facilitated their rebranding as the face of Daesh in Southeast Asia, more than just a local insurgency group. In both countries, social media facilitates vertical and horizontal recruitment, but not lone-actor terrorism. Extremist use of the internet for fundraising is still rudimentary – sophisticated financial cybercrime is still virtually non-existent. In all these aspects, women's roles have become much more visible. For a long time, women had been barred from accessing extremist public spaces, let alone taking an active role as combatants.[1] But through social media, women are now able to play more active roles as propagandists, recruiters, financiers, and even suicide bombers.

This paper briefly discusses government responses to online extremism, noting that there have been mixed results between Indonesia and the Philippines. Indonesian authorities have undoubtedly been the more successful of the two regimes – both in terms of law enforcement and engagement with the tech sector – but its counterterrorism police now face the problem of how to judiciously use their powers in a democratic manner. The Philippines, meanwhile, is still at the starting line in terms of dealing with online extremism, with the military more accustomed to removing threats than trying to understand them.

Policy Recommendations

- Analysts and policymakers should go beyond identifying new platforms or technology that terrorists might exploit. They should also understand the contextual dynamics that inform how terrorists exploit social media.
- Digital surveillance is useful to an extent; it should be conducted alongside conventional law enforcement and intelligence collection.

[1] Institute for Policy Analysis of Conflict (IPAC), 'Mothers to Bombers: The Evolution of Indonesian Women Extremists', IPAC Report No. 35, 31 January 2017, <http://file.understandingconflict.org/file/2017/01/IPAC_Report_35.pdf>, accessed 2 July 2019.

- To avoid the misuse of internet content regulations, governments, in partnership with civil society groups, should draw up criteria for how to distinguish legitimate political criticism from hate speech and incitement to violence.

Background

Violent Islamist extremism has very different roots in Indonesia and the Philippines, which has had an impact on how extremists in both countries have used the internet. In Muslim-majority Indonesia, violent Islamist extremism emerged in the 1950s from a movement to establish an Islamic state.[2] In Muslim-minority Philippines, it emerged from a variety of armed insurgencies fighting for autonomy or independence for the Muslim-majority Mindanao island group. The two movements first encountered each other on the Afghanistan–Pakistan border in the mid-1980s, where both sought training to fight their governments at home.[3] They forged a relationship with the then-preeminent global jihadist organisation Al-Qa'ida (AQ) and with each other – leading to the establishment of training camps for members of Indonesia's Jemaah Islamiyah (JI) in the Philippines under the protection of the Philippines Moro Islamic Liberation Front (MILF). Although neither operated under AQ's direction, both received money from the group and launched attacks in its name in the 2000s – including the 2002 Bali bombings and the 2004 SuperFerry bombing in Manila.[4]

In the mid to late 2000s, the ground for jihadism in both countries began to shift. Facing extreme counterterrorism pressure, JI withdrew from violence in 2007 and newer groups emerged in its place, each with an online presence. One was the ideological, globally-oriented movement led by former Salafist cleric Aman Abdurrahman and a group of technologically aware supporters.[5] Another was the Poso-based Eastern Indonesia Mujahidin, led by former JI member Santoso, which created a jihadi forum called Forum Al-Busyro and sought to develop ties with AQ's Global Islamic Media Front. Meanwhile, in the Philippines, MILF's rapprochement with the government led to the closure of JI's camps and militants, such as the Abu Sayyaf Group (ASG), dispersed

[2] See Solahudin, *The Roots of Terrorism in Indonesia: From Darul Islam to Jemaah Islamiyah*, translated by Dave McRae (Singapore: National University of Singapore Press, 2013).

[3] Malcolm Cook and Kit Collier, 'Mindanao: A Gamble Worth Taking', Lowy Institute Papers, 20 November 2006, p. 15.

[4] For the SuperFerry and Bali bombing incidents, see Andrew Tan (ed.), *A Handbook of Terrorism and Insurgency in Southeast Asia*, (Northampton, MA: Edward Elgar Publishing, 2007), pp. 74, 110, 212.

[5] Beginning in 2007, followers of Aman Abdurrahman created many websites, most prominently <www.millahibrahim.wordpress.com>, which was taken down in 2015.

following the death of its leader.[6] This led to a period of low-intensity activity in both Indonesia and the Philippines, as networks regrouped online and offline, attempting to adapt to the new environment.

Daesh's declaration of a caliphate on 29 June 2014 injected renewed energy into Indonesian and Philippine extremist networks. Ceremonies pledging loyalty to Daesh leader Abu Bakr Al-Baghdadi took place across both countries, ultimately leading to the formation of the Indonesian Daesh coalition Jama'ah Anshorul Daulah (JAD) in 2015 and Daesh's East Asia Province in the Philippines in 2017.[7] JAD has largely faltered in the face of a robust police counterterrorism response, although Daesh supporters in Indonesia conducted global attention-grabbing attacks in Jakarta (2016) and Surabaya (2018).[8] Meanwhile, Daesh's Philippines affiliate – which also included some Malaysian and Indonesian fighters among its ranks – scored a stunning success with the five-month capture of the prominent southern Philippines city of Marawi in 2017, as well as a devastating bombing targeting a church on Jolo in February 2019. Both groups are now largely on the back foot in the face of counterterrorism pressure.

The Evolution of Online Extremism in Indonesia and the Philippines

These different roots of extremism – urban terrorism in Indonesia and rural insurgency in the Philippines – have shaped how extremists in both countries have engaged with the internet. In Indonesia, the evolution of extremist use of the internet mirrors the rapid development of communication technology and the Islamic media industry. Islamic literature did not cause terrorism, but the flourishing Islamic publishing industry – both in print and online – did inspire some individual members of JI to establish their own publishing companies and carve a small niche in the business.[9] The scarcity of Islamic publishing in the Philippines may have been one of the reasons why jihadist media developed more slowly. More importantly, local factors such as

[6] International Crisis Group (ICG), 'The Philippines: Counter-Insurgency vs. Counter-Terrorism in Mindanao', Asia Report No. 152, 14 May 2008, <https://www.refworld.org/docid/482be4cd2.html>, accessed 2 July 2019.

[7] Joseph Franco, 'Assessing the Feasibility of a "Wilayah Mindanao"', *Perspectives on Terrorism* (Vol. 11, No. 4, 2017). For a background on Jama'ah Anshorul Daulah, see IPAC, 'Disunity Among Indonesian ISIS Supporters and the Risk of More Violence', IPAC Report No. 25, 1 February 2016, <http://file.understandingconflict.org/file/2016/04/IPAC_25_-_5.pdf>, accessed 2 July 2019.

[8] Kirsten Schulze, 'The Surabaya Bombings and the Evolution of the Jihadi Threat in Indonesia', *CTC Sentinel* (Vol. 11, No. 6, 2018), pp. 1–5.

[9] ICG, 'Indonesia: Jemaah Islamiyah's Publishing Industry', Asia Report No. 147, 8 February 2008, <https://www.refworld.org/pdfid/47c6c9912.pdf>, accessed 2 July 2019.

conflict dynamics and levels of internet penetration influenced the different development of online extremism in the two countries.

Indonesia

Extremists in Indonesia have been quick to adapt to changes in the global tech environment. The pioneer of online violent extremism in Indonesia was Bali bomber Imam Samudra. As internet cafés became popular in 2000, he joined JI's Yahoo listserve which contained news from local jihad battlefronts (mostly in Ambon and Poso).[10] This inspired him to create a series of websites to claim credit for JI's operations, aided by a friend who had learned from the AQ media unit in Pakistan. In 2004, after being imprisoned for the Bali bombing, Samudra pioneered an online religious study group via relay chat (mIRC) and experimented with credit card fraud. Before his execution in 2008, Samudra had groomed a group of computer specialists and wrote a best-selling memoir promoting 'cyber-jihad', complete with hacking tips.[11]

One man who joined Samudra's mIRC chatroom was Tuah Febriwansyah, better known as Fachry, a former Hizbut Tahrir member who became deeply influenced by Al-Muhajiroun UK through online (Paltalk) lectures by its leader, Omar Bakri Muhammad.[12] In 2007, Fachry was employed by Muhammad Jibril, the son of a senior Afghan jihad veteran, to develop Arrahmah, the first professionally run jihadist news site in Indonesia with salaried staff and daily updates.

Most jihadist websites and blogs in the 2000s focused on ideological propagation and raising awareness of global jihad rather than serving as terrorist manuals. This is because many of those running the sites were intellectuals, not combat veterans, and there were security concerns about discussing any dangerous topic too freely.[13] One exception to this rule was a website created in 2005 for the JI splinter group Noordin Top, which combined religious content with detailed, illustrated instructions for mounting attacks.[14]

[10] IPAC, 'Online Activism and Social Media Usage Among Indonesian Extremists', IPAC Report No. 24, 30 October 2015, <http://file.understandingconflict.org/file/2015/10/IPAC_24_Online_Activism_Social_Media.pdf>, accessed 2 July 2019.

[11] Imam Samudra, *Aku Melawan Teroris [Me Against the Terrorist]* (Solo: Jazera, 2004).

[12] IPAC, 'The Evolution of ISIS in Indonesia', IPAC Report No. 13, 24 September 2014, p. 3, <http://file.understandingconflict.org/file/2014/09/IPAC_13_Evolution_of_ISIS.pdf>, accessed 2 July 2019.

[13] IPAC, 'Online Activism and Social Media Usage Among Indonesian Extremists'.

[14] Jennifer Yang Hui, 'The Internet in Indonesia: Development and Impact of Radical Websites', *Studies in Conflict and Terrorism* (Vol. 33, No. 2, 2010), pp. 171–91.

In the late 2000s, as extremists created more exclusive password-protected online forums, such as Forum Arrahmah and Al-Busyro, carefully vetted members began to feel more comfortable with discussing more dangerous topics including their bomb-making experiments based on 'How to Make a Bomb in the Kitchen of Your Mom', an article that first appeared in *Inspire*, the online English-language magazine of AQ in the Arabian Peninsula.[15]

Very few of these sites hosted original content. However, the blogs created by Abdurrahman's followers contained his prison writings from 2004 to 2008, which became the basic texts of Indonesia's jihadist movement, especially one called the 'Tawhid Handbook'. A skilled linguist, Abdurrahman also translated Arabic texts, especially those by Abu Muhammad Al-Maqdisi, the former mentor of the Islamic State in Iraq (ISI) founder, Abu Mus'ab Al-Zarqawi.[16] ISI thus became the role model for post-JI militants. The fundraising video produced by organisers of a terrorist training camp in Aceh, Indonesia in early 2010 marked the first known use of YouTube for the dissemination of locally produced extremist propaganda.[17]

As smartphone ownership has risen spectacularly since 2011, online forums have given way to BlackBerry Messenger, Twitter and Facebook.[18] The first major financial cybercrime – conducted by one of Samudra's recruits – also occurred in 2011, resulting in one terrorist cell netting almost $700,000 from an online skimming operation.[19] No extremist has engaged in such sophisticated hacking since, although conventional online fundraising methods continued with appeals for funds for disaster and conflict victims and for the families of martyrs and prisoners.

The Philippines

Extremist use of the internet and social media developed more slowly in Muslim-majority Mindanao, where the rate of internet penetration has

[15] *Ibid.*

[16] For a profile of Abdurrahman, see Navhat Nuraniyah, 'Aman Abdurrahman: Indonesia's Most Influential Extremist', *Jamestown Foundation Militant Leadership Monitor* (Vol. 6, No. 12, December 2015).

[17] ICG, 'Indonesia: Jihadi Surprise in Aceh', Asia Report No. 189, 20 April 2010, <https://www.crisisgroup.org/file/1951/download?token=Rc9xR_f5>, accessed 3 July 2019.

[18] See Statista, 'Number of Smartphone Users in Indonesia from 2011 to 2022 (in Millions)', last edited 19 February 2019, <https://www.statista.com/statistics/266729/smartphone-users-in-indonesia/>, accessed 2 July 2019.

[19] *Berita Satu*, 'Soal Teroris Peretas, Aset Yang Disita 5 Milliar Lebih' ['For the Terrorist Hacker, the Confiscated Asset was Over 5 Billion'], 22 June 2012.

always been among the lowest in the country.[20] As late as 2003, few MILF fighters had email addresses.

Early media jihad enthusiasts in the Philippines were either Muslim converts from metropolitan Manila or foreign fighters who took inspiration from global jihadists. One early advocate of 'jihad by the pen', as online propaganda was anachronistically termed, was Ahmed Santos, the founding leader of the Rajah Solaiman Movement (RSM), a militant offshoot of Balik Islam (Christians who convert to Islam).[21] Santos was imprisoned in 2005 over his involvement in the 2004 SuperFerry bombing but has been active as a preacher-scholar behind bars, apparently without the knowledge of Manila prison authorities.[22]

Under the pseudonym Kuya Ghareeb aka Aboo Abdillaah Al-Ghareeb, Santos translated numerous religious books written by Wahhabi scholars, including Ibn Abd Al-Wahhab and Ibn Al-Uthaymin, into Tagalog, as well as more overtly jihadist texts by AQ-affiliated scholars such as Yusuf Al-Uyayri and Anwar Al-Awlaki, and also the speeches of Al-Baghdadi and former Daesh spokesperson Mohammed Al-Adnani.[23] The translations were circulated online and in print. By 2015, Santos was operating at least three websites and a few Telegram channels. He also made contact with Suraya, a Hong Kong-based Indonesian nanny and master networker who had helped several Indonesians travel to Syria via Hong Kong.[24] But Santos was not the only one to communicate with fellow Daesh supporters in the region via the group's most preferred apps to date: Telegram and Facebook.

[20] By 2006, only 2% of households in Muslim-majority Mindanao had internet access. Islamic media and book publication were also scarce. Even as late as 2005, the translation of the Qur'an into Tagalog was not yet completed. See Iremae D Labucay, 'Patterns of Internet Usage in the Philippines', in Jonathan D James (ed.), *The Internet and the Google Age: Prospects and Perils* (Dublin: Research-publishing.net, 2014).

[21] For more on the Rajah Solaiman Movement, see ICG, 'Philippines Terrorism: The Role of Militant Islamic Converts', Asia Report No. 110, 19 December 2005, <https://www.crisisgroup.org/asia/south-east-asia/philippines/philippines-terrorism-role-militant-islamic-converts>, accessed 2 July 2019.

[22] Author email communication with a Philippine law enforcement official, 3 May 2019.

[23] It appears that Santos translated from the English version of these books rather than the original Arabic ones. His translations and other writings are published on https://aklatannikuyaghareeb.wordpress.com/kuya-al-gharib/, accessed 3 July 2019.

[24] For the radicalisation of overseas workers, see IPAC, 'The Radicalisation of Indonesian Women Workers in Hong Kong', IPAC Report No. 39, 26 July 2017, <http://file.understandingconflict.org/file/2017/07/IPAC_Report_39.pdf>, accessed 2 July 2019.

How Violent Extremists Use Telegram and Facebook

As in other regions, the rise of social media has been a game changer for violent extremists in Indonesia and the Philippines, providing them with more avenues for communication, radicalisation and recruitment than ever before. Daesh's emergence coincided with a massive increase in internet access in Mindanao – with the percentage of residents in the region reporting to have used the internet increasing from 8% in 2006 to 24% in 2014.[25] Daesh supporters around the world began to shift from Facebook and Twitter to encrypted chat platforms in 2014.[26] Syria-based Southeast Asian fighters reportedly instructed their followers to use Telegram – instead of the more popular WhatsApp and Viber – to take advantage of its end-to-end message encryption and its perceived independence from government interference. That said, many supporters continued to use Facebook – which remains the largest social media platform in both countries – along with various platforms exploited simultaneously. In fact, as Telegram grew more vigilant, many extremists have turned to Facebook as a fall-back option for regrouping.

Telegram in particular has provided multiple opportunities for extremists seeking new recruits. Outreach typically consists of four layers: public or semi-public channels used for broadcasting propaganda; private groups where sympathetic new supporters are courted by the more committed members; exclusive groups where carefully vetted members discuss planning and virtual training; and secret chat or personal messaging. Some private groups have become like a virtual family and support group where members discuss their personal matters as much as they reinforce each other's faith in Daesh.[27]

But it has been hard work for extremists at times, particularly as social media companies have begun to clamp down on their activities. In early 2019, the size of Indonesian pro-Daesh channels and groups on Telegram stagnated at 200–300 members, whereas in 2016–2017 most channels had

[25] Labucay, 'Patterns of Internet Usage in the Philippines'.

[26] The shift happened following a major Twitter crackdown on extremist contents and because Daesh supporters believed that Telegram, with its end-to-end encryption, was safer than other messaging apps at the time. See J M Berger and Heather Perez, 'The Islamic State's Diminishing Returns on Twitter: How Suspensions are Limiting the Social Networks of English-speaking ISIS Supporters', George Washington University Program on Extremism Occasional Paper, February 2016, <https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/downloads/JMB%20Diminishing%20Returns.pdf>, accessed 3 July 2019.

[27] Nava Nuraniyah, 'Online Extremism: The Advent of Encrypted Private Chat Groups', in E Jurriens and R Tapsell (eds), *Digital Indonesia: Connectivity and Divergence* (Singapore: ISEAS Publishing, 2017).

thousands of subscribers.[28] This was caused by Telegram's restriction and the decreasing supply of materials from Daesh official media.[29] However, Daesh online activists have proven to be extremely resilient: some popular groups generally bounce back within a day of being banned and could amass over 100 joiners in less than an hour.[30] They create multiple back-up accounts in anticipation of bans and back up contents on multiple platforms (for example, as Telegram saved messages or e-books or on file-sharing websites). Indonesian extremists have also branched out to Instagram, which is now more popular among young people than Facebook, creating their own sleek infographics and short videos – sometimes by repackaging old materials from Daesh's *Rumiyah* bulletins.[31]

Filipino Telegram groups reached a peak in 2016–2017, with at least 50 groups and channels posting a variety of original videos and news from various battlefronts. One channel, Al-Bayyinat, notably had its own professional video production team, although it was not the official media channel of Daesh's Philippines branch. To the extent that it could be openly monitored, there were at least 10 Filipino groups/channels as of April 2019; half of them had not been updated since mid-2018 and the other half were merely Amaq posts translated into Tagalog and other local languages.

Even with increased pressure on Telegram, extremists were still able to find outlets on other platforms – even returning to old venues. On Facebook,

[28] Nava Nuraniyah, 'If You Can't Sacrifice Your Life, Sacrifice Your Data: Online Activism of Indonesian ISIS Supporters' in Shashi Jayakumar (ed.), *Terrorism, Radicalisation, and Countering Violent Extremism: Political Considerations and Concerns* (London: Palgrave Pivot, 2018), pp. 135–48. For Telegram's global crackdown on Daesh-related contents, see Bennett Clifford and Helen Powell, 'Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram', George Washington University Program on Extremism, June 2019, <https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/EncryptedExtremism.pdf>, accessed 3 July 2019.

[29] Charlie Winter, 'The ISIS Propaganda Decline', International Centre for the Study of Radicalisation Insights, 23 March 2017, <https://icsr.info/2017/03/23/isis-propaganda-decline/>, accessed 2 July 2019.

[30] IPAC, 'Indonesia and the Tech Giants vs ISIS Supporters: Combating Violent Extremism Online', IPAC Report No. 48, 27 July 2018, <http://file.understandingconflict.org/file/2018/07/IPAC_Report_48.pdf>, accessed 2 July 2019.

[31] As of 2019, 120 million Indonesians were on Facebook (45% of the population) while Instagram had 56 million users. The average age of Indonesia's Instagram users was 18–24 years old while Facebook had more mature users, averaging 18–34 years old. Agung Pratnyawan, 'Pengguna Facebook dan Instagram di Indonesia Terbesar ke-4 di Dunia' ['Indonesia's Facebook and Instagram Users the Fourth-Largest in the World'], *Hitekno*, 19 June 2019.

most pro-Daesh accounts were personal. Some Facebook groups existed that were linked to Telegram. For instance, in July 2017, some Filipinos joined a new Indonesian–Filipino group on Telegram after their own Facebook group was shut down. The reverse is also true: in August 2017, when an Indonesian female-only Telegram group disappeared following the deportation of its administrator (a radicalised Indonesian maid 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.[32]

Three types of social media activity are particularly worthy of further discussion: branding, recruitment and fundraising. Women have displayed increased activity in all three.

Branding

Social media has enabled Southeast Asian extremists to establish a clear brand – with associated symbols and messages – to attract new followers. The Daesh brand appeals to second-generation rebels in Muslim-majority Mindanao because it can set them apart from their predecessors. For the pro-Daesh coalition in the Philippines, Telegram was strategically used for one main purpose: to send propaganda out of Marawi that would gain formal recognition from Daesh central – rather than to fight in Syria.[33]

The patterns of Telegram messaging further indicate a command structure between Syria and Southeast Asia which adds credibility to the local expression of the Daesh brand. Updates from the front line were sent out of Marawi by one Semion Al-Mujahid, who claimed that all his posts had been pre-approved by their leader, Isnilon Hapilon. Semion directly fed information to Daesh official media, especially Amaq. At the same time, an Indonesian using the name Abu Sulayman Al-Globali exclusively delivered

[32] This is also true in the Philippines. Someone opening the Filipino Facebook group Pamantasan Ng Tawheed At Jihad would be directed to another pro-Daesh group, Alharakatul-Islamiyya Jolo-Sulu.

[33] Issue 7 of Daesh's online magazine, *Dabiq*, outlined the conditions that must be met for a territory to be acknowledged as a 'province' of the caliphate: documenting pledges to Daesh; unifying all local groups; holding consultations to nominate a leader; and controlling territory that fully implements Sharia. Philippine Daesh social media messages followed that sequence: publicising pledge videos in 2014; circulating video footage of the anointment of Isnilon Hapilon as leader in 2016; and finally seizing Marawi in 2017. They had hoped to set up a government structure which would presumably have met the fourth condition, but the war with the Philippine army made that impossible. See IPAC, 'Marawi, the "East Asia Wilayah" and Indonesia', IPAC Report No. 38, 21 July 2017, <http://file.understandingconflict.org/file/2017/07/IPAC_Report_38.pdf>, accessed 2 July 2019.

official messages from Bachrumsyah, the Indonesian Daesh leader in Syria, regarding the East Asia province.

That said, unofficial media personnel and translators still played an important role in maintaining the relevance of the brand. One of these translators was a woman named Green Bird who spoke Maguindanaon (the local language of Maguindanao Province, Mindanao) Indonesian, English and some Arabic. She worked with Indonesians and Malaysians on the Telegram groups to promote the East Asia province brand regionally and internationally, ensuring that readers continued to view the regional affiliate as part of the main Daesh machine.

Recruitment

While Islamic study groups and kinship remain the dominant recruitment vectors in both countries, social media increasingly facilitates both vertical and horizontal recruitment, but it rarely produced lone-actor terrorists in either Indonesia or the Philippines. In both places, violent extremism is very much a social activity. Vertical recruitment can be top-down (leaders seeking recruits) or bottom-up (fans reaching out to a known terrorist leader). The former is best exemplified by the late Mahmud Ahmad, a Malaysian Daesh recruiter who moved to Mindanao in April 2014. By 2016, he was using Telegram to organise Malaysian and Indonesian militants to join him in the Philippines.[34]

Likewise, supporters could seek direct connection with the top leadership via social media – something unthinkable for earlier generations of jihadists. One example is Karen Aisha Hamidoon, the Filipina social media influencer who created dozens of international Telegram groups. Karen managed to approach the leader of Ansarul Khilafah Philippines, Tokboy, and persuaded him to marry her – although he soon divorced her after suspecting she might be a spy. By that time, the global Daesh media community was already hunting her down due to rumours that she had exposed an Indian Telegram activist arrested in January 2016.[35] Karen's case reveals that while social media is useful for extremist networking, it is also vulnerable because online groups can be broken up by sowing suspicions.

Facebook and Telegram also make peer-to-peer recruitment more accessible and faster than ever before.[36] This is especially useful for female supporters

[34] Katerina Francisco, 'Fast Fact: Who is Mahmud Ahmad', *Rappler*, 17 October 2017.

[35] Vijaita Singh, 'Arrested IS Recruit Wanted to Train His Son for Jihad', *The Hindu*, 1 May 2016.

[36] On the different types of online recruitment in the Philippines, see The Asia Foundation and Rappler, 'Understanding Violent Extremism: Messaging and Recruitment Strategies on Social Media in the Philippines', 2018, <https://asiafoundation.org/wp-content/uploads/2019/02/Understanding-Violent-

whose dream of direct involvement in violence has historically been denied by male leaders. Ika Puspitasari, a radicalised Indonesian maid in Hong Kong, is one woman who has taken advantage of this technology. Having been radicalised online and chosen a husband from her pro-Daesh Telegram group in 2015, she wanted to finance a terrorist operation back home.[37] To make her investment worthwhile, she identified talented bomb-makers through Facebook and Telegram. She then created a special Telegram group to discuss money transfer and attack planning with her recruits, but her plans faltered when her husband was arrested.

Fundraising

Social media has provided a platform for extremists to raise funds more easily than they could in previous generations. Open fundraising is often framed as appeals to support the families of martyred and imprisoned mujahideen. This includes the Gashibu Project (a closed Facebook group and Telegram channel) and the Aseer Crue Centre (a Telegram channel) that collect donations for the wives and children of approved extremist inmates. Public appeals that explicitly mention *amaliyah* (terror plots) are rare but a few examples exist. One was the attempt of Rio Priatna, a Daesh supporter in West Java, who in 2016 raised money from his Facebook and Telegram friends to build an explosives laboratory. His online girlfriend, who was working in Hong Kong, gave him a substantial amount via bank transfer.[38] However, such open fundraising efforts that are apparently heedless of security precautions are often (and sometimes correctly) suspected by Daesh sympathisers as attempts at fraud or entrapment.[39]

Extremism-Messaging-and-Recruitment-on-Social-Media-in-the-Philippines.pdf>, accessed 2 July 2019.

[37] The account is based on Ika Puspitasari's trial testimony. See Supreme Court of the Republic of Indonesia, 'Verdict No. 479/PID. Sus/2017/PN. Jkt. Tim.', <https://putusan.mahkamahagung.go.id/putusan/downloadpdf/f814fb193908f38473314580aaff2fd3/pdf>, accessed 2 July 2019. This pattern of radicalisation – in which women progressed from low-risk activities such as online propaganda and fundraising to high-risk ones such as terrorism plotting or travelling to Syria – was found among other pro-Daesh Indonesian migrant workers. This includes Anggi Indah Kusuma, a former migrant worker who was arrested in West Java in August 2017 while preparing a bomb with her husband and colleagues. For her trial testimony, see Supreme Court of the Republic of Indonesia, 'Verdict No. 259/PID. Sus/2018/PT.DKI', <https://putusan.mahkamahagung.go.id/putusan/downloadpdf/ccec2b29531096845ee07babb334869e/pdf>, accessed 3 July 2019.

[38] *Tempo.com*, 'Rio Priatna, Tersangka Pembuat Bom Diduga Didanai TKI' ['Rio Priatna, Bomb-Maker Suspect Allegedly Funded by Indonesian Overseas Workers'], 25 November 2016.

[39] There have been several corruption cases in the Indonesian Daesh community – one woman who pretended to be a travel agent who could arrange safe

More serious operatives use Telegram's secret chat function to arrange money transfers, representing a merging of new technology with old tactics for moving funds between countries. Between 2014 and 2016, the Malaysian operative Mahmud Ahmad successfully arranged a series of transfers from Syria to Indonesia and then on to the Philippines. Rather than using bitcoin or other advanced methods, he used the traditional Western Union service, employing a convoluted route with the assistance of multiple couriers whom he instructed via Telegram.[40] Mahmud and other extremists in both countries often use women's bank accounts to avoid suspicion.[41]

State Response

Regional governments have had mixed success in combating the spread of extremism online. Both Indonesia and the Philippines have legislation enabling them to monitor and disrupt terrorists' cyber activities (Indonesia's Law No. 11 of 2008 on Electronic Information and Transaction and the Philippines' Cybercrime Prevention Act 2012). The Indonesian government has gradually become more sophisticated in detecting and prosecuting extremist activity online, although its first attempts were very clumsy. In 2015, the government banned 22 allegedly radical websites in an effort to curb Daesh propaganda. Some of the banned sites were pro-Daesh but a few were clearly anti-Daesh and others belonged to legal Islamist organisations, which prompted a backlash from conservative Muslim groups.[42] Most of the sites were reinstated. In the Philippines, similar issues have emerged regarding misuse of internet content regulations. For example, on 13 February 2019 the National Bureau of Investigation's cybercrime division,

journeys to Syria and Iraq managed to steal $10,000 from naïve clients wanting to join Daesh. See IPAC, 'Mothers to Bombers', p. 16.

[40] IPAC, 'Marawi', p. 15.

[41] The use of women's bank accounts for terrorism-related money transfers dates back to the early 2000s and the same tactic remains prevalent among Filipino and Indonesian violent extremist groups. See ICG, 'Southern Philippines Backgrounder: Terrorism and the Peace Process', Asia Report No. 80, 13 July 2004, p. 19, <https://d2071andvip0wj.cloudfront.net/80-southern-philippines-backgrounder-terrorism-and-the-peace-process.pdf>, accessed 3 July 2019. See also IPAC, 'Pro-ISIS Groups in Mindanao and Their Links to Indonesia and Malaysia', IPAC Report No. 33, 25 October 2016, p. 13, <http://file.understandingconflict.org/file/2018/04/IPAC_Report_33_Edit.pdf>, accessed 3 July 2019. For a detailed account on how members of the Eastern Indonesia Mujahidin used their wives' bank accounts to move funds, see Supreme Court of the Republic of Indonesia, 'Verdict No. 775/PID. Sus/2015/PN. Jak Tim', <https://putusan.mahkamahagung.go.id/putusan/downloadpdf/446f808b6ab7925914f15e127073bdad/pdf.>, accessed 3 July 2019.

[42] *CNN Indonesia*, 'Situs Islam Radikal yang Diblokir Kominfo Bertambah' ['More Radical Sites Blocked by the Ministry of Communication and Information Technology'], 31 March 2015.

instead of pursuing online extremist propagandists, arrested Maria Ressa, CEO of the online news portal Rappler, for ‘cyber-defamation’.

The Cyber Patrol of Indonesia’s counterterrorism police, Detachment 88, has proven to be by far the most capable unit in identifying extremists. In one case in March 2019, police combined online surveillance and offline tips to gather sufficient evidence to make an arrest. The Cyber Patrol was tracking Rinto Sugianto, who often posted Daesh materials to attract fellow sympathisers and then direct-messaged individuals with the most interesting comments.[43] Rinto was untouched until months later when his worried parents told the police that he had explosive materials. His interrogation led to the uncovering of autonomous cells from three different islands communicating via Facebook.

Indonesia is more advanced than the Philippines in terms of fostering relationships with tech platforms, which has led to some success in stemming the flow of extremist propaganda online. Pressure on platforms helped the Indonesian government achieve security objectives. In July 2017, the government specifically targeted Daesh content on Telegram by shutting down Telegram web access, and threatened to ban the entire platform if the company refused to take action against violent extremist contents. Telegram’s CEO Pavel Durov immediately flew to Jakarta to meet the Ministry of Communication. Since then, bans on Telegram groups and channels have become common.

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 criticised by the Indonesian government for its insistence on abiding by its own community standards rather than national laws.[44] In August 2017, Facebook agreed to open its first permanent office in Indonesia to bridge the gap between the government and its headquarters in the US; it also agreed to geo-block certain content deemed illegal in Indonesia.

But Indonesia’s advances against online extremism have brought with them a new host of challenges. There is a growing realisation by police that in the broad wording of the Electronic Information and Transaction Law, as amended in 2016, it has a tool not just for curbing online extremists but for pursuing alleged defamers, blasphemers and others whose comments

[43] IPAC, ‘The Ongoing Problems of Pro-ISIS Cells in Indonesia’, IPAC Report No. 56, 29 April 2019, p. 10, <http://file.understandingconflict.org/file/2019/04/Report_56_Final.pdf>, accessed 2 July 2019.

[44] Author interview with an official of the Indonesian Ministry of Communication and Information Technology, Jakarta, 22 June 2018. See also *Kumparan.com*, ‘Facebook Bentuk Tim Khusus Pemblokir Konten Negatif di Indonesia’ [‘Facebook Formed a Special Team to Block Negative Contents in Indonesia’], 2 August 2017.

on the internet caused offence. There will be a temptation – particularly in the current heated political environment – to use these laws more for political ends than public security, which could affect public trust in counter terrorism efforts.

By comparison, the Philippines has far less capability in dealing with online extremism. As the military is the lead counter terrorism agency there has been less of a focus on understanding how online radicalisation takes place in preference to merely seeking to eliminate threats through kinetic force. Because social media played a major role in the lead-up to and conduct of the Marawi siege, it would be useful to undertake an in-depth study, based on interviews with some of those now under arrest, into how online propaganda was incorporated into the pro-Daesh strategy.

The Philippines is beginning to sound out cooperation with the tech sector, but for now there is little to show for these efforts. The Philippine law enforcement authority is in the initial phases of working with Facebook and Google to combat online extremism.[45] But elsewhere extremist material is still freely available. As of mid-2019, some of the most popular violent extremist websites – including those created by Ahmed Santos from as far back as 2014 – have not been taken down. Some pro-Daesh Facebook groups that have been active since 2015, such as Pamantasan Ng Tawheed at Jihad, are still accessible. Because reports from Mindanao still regularly appear in the Daesh newsletter *Al-Naba*, police believe there may be a social media operative who receives information from the field and then transmits it to a Daesh media contact.[46]

Conclusion

In conclusion, there are at least three policy lessons that can be drawn from the Indonesia and Philippine cases.

- In anticipating the next evolution of violent extremism online, analysts should not only focus on identifying new platforms or technology that terrorists might exploit. They should also understand the contextual dynamics that inform how terrorists exploit social media. This includes: how imprisonment of key leaders is likely to increase terrorist online activity or change it in ways not seen before; how security concerns and the lack of hacking skills limited internet exploitation for terrorist financing; and how local Daesh sympathisers use Telegram, the app recommended by their Syria-based colleagues, and other locally popular apps simultaneously rather than choosing one over the other.

[45] Author interview with a Philippine law enforcement official, Manila, 8 February 2019.

[46] *Ibid.*

- As shown in the case of Indonesian Rinto Sugianto, digital surveillance is useful but does not always provide key information to effect arrests. Thus, online monitoring should complement conventional law enforcement and intelligence collection.
- To minimise the negative impact of internet content regulations on freedom of speech, governments, in partnership with civil society groups, should draw up criteria for how to distinguish legitimate political criticism from hate speech and incitement to violence.

Nava Nuraniyah is an analyst at the Institute for Policy Analysis of Conflict (IPAC) in Jakarta, Indonesia.

About RUSI

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 188 years.

About The Global Research Network on Terrorism and Technology

The Global Research Network on Terrorism and Technology is a consortium of academic institutions and think tanks that conducts research and shares views on online terrorist content; recruiting tactics terrorists use online; the ethics and laws surrounding terrorist content moderation; public–private partnerships to address the issue; and the resources tech companies need to adequately and responsibly remove terrorist content from their platforms.

Each publication is part of a series of papers released by the network on terrorism and technology. The research conducted by this network will seek to better understand radicalisation, recruitment and the myriad of ways terrorist entities use the digital space.

The network is led by the Royal United Services Institute (RUSI) in the UK and brings together partners from around the world, including the Brookings Institution (US), the International Centre for Counter-Terrorism (Netherlands), Swansea University (UK), the Observer Research Foundation (India), the International Institute for Counter-Terrorism (Israel), and the Institute for Policy Analysis of Conflict (Indonesia).

The research network is supported by the Global Internet Forum to Counter Terrorism (GIFCT). For more information about GIFCT, please visit https://gifct.org/.

The views expressed in this publication are those of the author, and do not reflect the views of RUSI or any other institution.

Published in 2019 by the Royal United Services Institute for Defence and Security Studies.

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)