INSTITUTE FOR POLICY ANALYSIS OF CONFLICT

INDONESIA AND THE TECH GIANTS VS ISIS SUPPORTERS: COMBATING VIOLENT EXTREMISM ONLINE

27 July 2018
IPAC Report No. 48

CONTENTS

I. INTRODUCTION

The Indonesian government is cooperating more effectively now with private sector technology giants such as Google and Facebook to remove extremist content from social media platforms. Even as the hiccups in their relationship are being worked out, the extremists seem to be finding low-tech ways around blockages.

The 8-9 May 2018 riot of terrorist suspects detained at the headquarters of the paramilitary police Brimob outside Jakarta showed the government's ability to move speedily to address a spike in online violent extremist exhortations. It also showed how quickly extremists can transfer material to other platforms and mirror sites.

The extremists' wholesale shift to encrypted applications by 2014 made the government's often clumsy efforts to close down websites seem anachronistic. The Information and Communications Ministry (Kominfo) realised it needed the help of the tech companies but found the companies had their own standards and guidelines for removal of material which differed from the ministry's. After the owners of Telegram, the pro-ISIS extremists' encrypted application of choice, failed to respond to Kominfo's requests to remove material, the Indonesian government blocked Telegram's web access, finally getting the company's attention.

New restrictions, coinciding with defeats of ISIS in the Middle East and the weakening of links between ISIS media channels and their supporters in Indonesia, led to a decline in the use of large, semi-public Telegram channels to disseminate propaganda. But the use of highly encrypted private small group and two-person chats over Telegram continues.

As of mid-2018, government and social media companies have stepped up their efforts to detect and remove extremist content by using artificial intelligence and other tools to trawl the web. They also train their respective artificial intelligence (AI) machines to anticipate new tactics such as better encryption or other camouflage technology. While such innovation is commendable, most Indonesian ISIS supporters are not technologically sophisticated. Instead of responding with high-tech countermeasures, they simply create hundreds of back up channels and accounts, move their groups and channels regularly, and store terabytes of propaganda material across various platforms and devices. They are also exploring new encrypted messaging apps to prepare for the day when Telegram is no longer usable.

The problem is that interactive small group discussions among extremists can also be a gold mine of intelligence that allows state agencies to understand how extremists think and make informed analyses about future threats. The challenge is how to manage intelligence-gathering and reduce the public's exposure to extremist material online at the same time, through a combination of domestic regulations, new technologies and a partnership of government, the private sector and civil society.

II. BACKGROUND

Until 2017, the Indonesian government tried to rely on its own agencies and the public to report extremist content and block sites accordingly. It gradually came to realise that social media accounts were more important than websites as a tool for propaganda, recruitment, fundraising, group reinforcement, dissemination of instructional material (including how to make bombs) and occasionally, attack planning.[1] To close these accounts, it needed the help of the companies

1 Planning attacks almost always involves offline contact. See Alexander Babuta, "Online Radicalisation: The Need for an Offline Response", www.rusi.org, 25 September 2017.

behind them: Facebook, Google, Twitter and Telegram. As it reached out to them, it became clear that one of the major problems was trying to distinguish between violent, potentially terrorist content and non-violent hate speech. Even as some of these issues were being worked out, however, ISIS supporters were finding ways around the restrictions.

A. Early Online ISIS Support

Local jihadists had watched the Syria conflict closely since 2011. By 2012, followers of a detained jihadi cleric, Aman Abdurrahman were operating two websites, www.al-mustaqbal.net and www.shoutussalam.com, that provided daily updates from jihadi frontlines in the Middle East (and later became the first in Indonesia to disseminate pro-ISIS propaganda).[2] Other sites were also circulating radical tracts translated from the Arabic, calls for jihad and diatribes against religious minorities. In response to these developments, the National Counter-Terrorism Agency (Badan Nasional Penanggulangan Terorism, BNPT) in March 2013 requested the Ministry of Communication and Information Technology (Kementerian Komunikasi dan Informatika, Kominfo) to block 20 extremist websites including Shoutussalam.[3] At the time, the then minister, Tifatul Sembiring of the Islamist Prosperous Justice Party (PKS), was more preoccupied with blocking pornographic websites.[4]

Tifatul had faced criticism from human rights groups because the legal basis he cited for the March 2013 blockages, Law No. 11 of 2008 on Electronic Information and Transactions (Information Law, for short) did not authorise such closures. To close this legal loophole, Tifatul on 17 July 2014 issued Ministerial Regulation (Peraturan Menteri) No. 19 of 2014 on "the handling of internet sites bearing negative content", vaguely defined as "pornography and other illegal activities".[5] The regulation allowed other government agencies and the general public to report such content via email to Kominfo, with a special emphasis on four categories: violation of privacy, child pornography, violence, and ethno-religious hate speech.[6] If the reports came from the public, Kominfo could investigate, check with relevant government agencies, and if a violation was found, send a warning to the web administrator (if known) or the Internet Service Providers (ISP) to take down the prohibited content or block access to the entire site. Kominfo also set up an online database system called Trust+Positif to regularly announce newly blacklisted sites; ISPs were then required to block those sites and upload their compliance report on the database.[7] But if the reports came from law enforcement agencies or other ministries, Kominfo could bypass the evaluation procedure and simply proceed with the blocking.

On this basis, Kominfo in March 2015 banned 22 radical Islamist websites at the request of BNPT.[8] The banning triggered a massive backlash from Muslim groups because some of the websites were in fact run by non-violent Islamist groups.[9] BNPT and Kominfo pointed fingers at each other, with Kominfo saying that it merely executed BNPT's order and BNPT insisting

2 For more about Aman Abdurrahman, see IPAC, "Online Extremism and Social Media Usage among Indonesian Extremists", Report No. 24, 30 October 2015 and Navhat Nuraniyah, "Aman Abdurrahman: Indonesia's Most Influential Extremist", *Militant Leadership Monitor*, Vol.6, Issue 12, December 2015.

3 "BNPT Blokir 15-20 Situs Internet Milik Teroris", www.antaranews.com, 20 March 2013.

4 "Kontroversi Blokir Laman Bermuatan Negatif", www.viva.co.id, 13 August 2014.

5 Peraturan Menteri Nomor 19 Tahun 2014, Tanggal 17 Juli 2014, tentang Penanganan Situs Internet Bermuatan Negatif.

6 Reports from the public are filtered through Kominfo's internal evaluation process while censorship requests from law enforcement agencies are generally executed by Kominfo without question. IPAC interview with Kominfo official, 22 June 2018.

7 According to Ministerial Regulation No. 19/2014, Kominfo in emergency situations has the authority to take the websites down within 24 hours.

8 "BNPT Minta Kominfo Blokir 22 Situs Radikal", www.kominfo.go.id, 30 March 2015.

9 Three such sites that were banned were www.aqlislamiccenter.com, www.gemaislam.com, and www.eramuslim.com.

that Kominfo should have conducted its own investigation before blocking the sites.[10] In April 2015, Tifatul was replaced and the new Kominfo Minister, Rudiantara, formed an expert panel to evaluate all censorship requests.[11]

The new expert panel, however, could not fix the deeply flawed Information Law. Rights groups had long criticised the defamation article in the law as too broad and prone to abuse; the law also did not have clear provisions on the mechanisms of patrolling the Internet or criteria for content removal.[12] In response to these shortcomings, the national parliament adopted a revised law in 2016, which merely lowered the maximum punishment for defamation without clarifying its definition or scope.[13] It also added Article 40, giving Kominfo the authority to ban prohibited content directly without involving the ISP.

B. Social Media Accounts and the Big Tech Companies

In the meantime, extremist groups were moving toward password-protected social media groups and encrypted accounts. Late 2013 and early 2014 had seen a spike of Indonesian ISIS supporters taking loyalty oaths (*bay'ah*) online to ISIS leader Abu Bakar al-Baghdadi on YouTube, Facebook and Twitter.[14] Pro-ISIS groups used Facebook and Twitter not only for propaganda but also to get contacts in Syria to facilitate the travel of Indonesian fighters there – often with their families. They usually shifted from public social media to the messaging app, WhatsApp, to converse more privately after getting each other's phone numbers. But then they were told by Indonesians and other fighters with ISIS to use more secure messaging services such as Surespot and Telegram.

The first Telegram groups were formed by participants of ISIS rallies and study groups in different parts of Indonesia around 2014. Indonesians with ISIS in Syria at that time had instructed core members of pro-ISIS organisations to move to Telegram mainly because of its end-to-end encryption. Telegram was also a much better propaganda tool than other apps because in addition to offering security and privacy (with secret chat and self-destructive message features), it allowed users to form big groups and quickly send large multimedia files – up to 1.5 gigabytes compared to WhatsApp's 100-megabyte limit. Following Twitter's massive takedown of extremist accounts in 2015, more sympathisers turned to Telegram as well.[15] The simultaneous usage of Telegram, Facebook, and Twitter allowed the online community to grow rapidly, even gaining followers among Indonesian migrant workers in East Asia and Middle East.[16]

The government, however, had no means of taking down social media accounts. It therefore began putting more pressure on social media companies to remove extremist material and ethno-religious provocation, without attempting to define how legitimate (if offensive) political opinion differed from hate speech or criminal incitement. In 2015, Kominfo asked Facebook and Twitter to suspend pro-ISIS accounts, including that of Bahrun Naim, the Indonesian ISIS

10 "BNPT: Tak Perlu Infokan Rencana Blokir ke Pemilik Situs Islam", www.cnnindonesia.com, 5 April 2015.

11 Keputusan Menkominfo Nomor 290 Tahun 2015 tentang Forum Penanganan Situs Internet Bermuatan Negatif. Four types of expert panels were established: 1) pornography, violence against children and internet safety; 2) terrorism and hate speech; 3) illegal investment, fraud, gambling, drugs and illegal substances; and 4) intellectual property rights.

12 "Ketika UU ITE Menjadi Momok Masyarakat", www.tirto.id, 22 January 2016.

13 "4 Poin Perubahan UU ITE hasil revisi yang Mulai Berlaku Hari Ini", www.kompas.com, 28 November 2016. The revised law was Law No.19/2016.

14 "Lagi, Baiat untuk ISIS dari Indonesia," www.liputanislam.com, 14 July 2014.

15 Twitter, widely used by ISIS supporters, claims to have banned 635,000 terrorism accounts worldwide between mid-2015 and late 2016. Natasha Lomas, "Twitter Nixed 635k+ Terrorism Accounts between Mid-2015 and End of 2016", www.techcrunch.com, 22 March 2017.

16 IPAC, "The Radicalisation of Indonesian Women Workers in Hong Kong", Report No. 39, 26 July 2017.

leader and master of social media who used multiple accounts to try and incite attacks and teach bomb-making.[17]

Facebook and Google were more than willing to help as long as government requests met their own global community standards.[18] They did not want to be accused of encouraging hate speech and terrorist propaganda; on the other hand, their business relied on their ability to provide free space for people to express their opinions. Over time they got better at navigating a balance. In 2015, Google removed 78 videos from its subsidiary YouTube at Kominfo's request. Many Twitter accounts were closed as well, though they tended to just pop up again under a slightly different name.

By early 2017, the Indonesian government had established direct communication with Facebook, Google (including YouTube) and Twitter – although it was still unsatisfied with what it saw as their slow response.[19] The government was even more frustrated with Telegram as the company apparently had not responded to a single report filed by Kominfo since 2016, even though it claimed to have become more concerned about extremist content in the wake of the Paris attack in November 2015. [20] In late 2016 it created the "ISIS Watch" channel to release the number of terrorist bots and channels it banned on a daily basis.

On 14 July 2017, Indonesian government blocked Telegram web access and threatened to ban the entire application if the company refused to cooperate. That was enough to get the attention of Telegram chief executive Pavel Durov who came to Indonesia on 1 August to negotiate with Minister Rudiantara. After Durov's visit, Telegram became more responsive to requests to remove pro-ISIS content and close extremist accounts, and the government reopened Telegram web access on 10 August.[21] These developments, coupled with the decline of ISIS propaganda production following the loss of most of its territory in Syria, led to a decline in the size and average lifespan of Telegram groups.

The success of Telegram in removing content depended on the exclusivity of the group. Extremists in Indonesia as elsewhere used four kinds of Telegram functions: one-way broadcasts, semi-public interactive chat groups, exclusive private groups and secret chats for two-person communication. Propaganda broadcasts through public channels or bots were the easiest to identify and shut down. Large semi-public interactive chat groups that advertised their link on public channels (or on Facebook, Twitter or Instagram) as a way of recruiting new members were easily infiltrated, with the infiltrators then reporting to Telegram. Exclusive private groups proved much harder to penetrate, as members often had to be vetted through face-to-face contact. These smaller groups could be formed by senior recruiters to instruct selected cadres or

17 "Kementerian Kominfo Blokir Akun Media Sosial dan Situs 'Radikal' ", www.bbc.com, 16 January 2016.

18 For the guidelines, see https://help.twitter.com/en/rules-and-policies/twitter-rules; https://www.google.com/+/policy/content.html ; and https://www.facebook.com/communitystandards/. Facebook was willing to push back against requests that it considered "unreasonable or overbroad", though all tech companies had to comply with legal orders to block sites or remove material, even when it did not violate their own standards. Content that violate Thailand's draconian lese majeste laws was a case in point. Monka Bickert, "Explaining Our Community Standards and Approach to Government Requests', www.newsroom.fb.com, 15 March 2015.

19 This did not mean relations with the companies always went smoothly. A Kominfo official recalled one incident when a photograph of President Joko Widodo with a pig's head was circulated on Facebook. The Kominfo team maintained that since Muslims consider the pig to be the dirtiest of all animals, the image was a deep insult to the president of a Muslim majority country and could even be seen as incitement to violence. But a member of the US-based Facebook team reportedly replied that the image—at least then—did not violate Facebook's guidelines on hate speech and said: "What's wrong? Pigs are cute". IPAC interview with Kominfo official, 22 June 2018. In an updated version of the guidelines made public on 24 April 2018, Facebook includes "dehumanising speech" in its list of objectionable content, and an official said there is no way such a photograph would be allowed to circulate today. See Facebook community standards: https://www.facebook.com/communitystandards/objectionable_content/hate_speech

20 "Pekan Penuh Lobi Bagi Kominfo ke Facebook, Google, Telegram, Twitter", www.kumparan.com, 4 August 2017.

21 "Kominfo Catat 11 Medsos Punya Konten Negatif, Twitter Terbanyak", www.tirto.id, 8 March 2018.

by peers who wanted to plan something together.[22] The secret chat function has even stronger encryption and a self-destruct timer, making it all but impenetrable.

Before the Jokowi government's partial ban of Telegram in mid-2017, the largest pro-ISIS Indonesian language channel had approximately 8,000 subscribers. By December 2017, the largest channel had only 900. Many channels were suspended within hours or at most days after they were launched (sometimes slightly longer because the intelligence agencies needed them for information gathering). The same decline happened in semi-open and private groups. In 2015-2016, some groups had up to 1,000 members; by early 2018, the largest did not exceed 600. Still, it was remarkable how some well-known channels and groups manage to grow from zero to 100 followers within a day. For example, one well-known group that had been repeatedly banned was closed on 13 July 2018 but by 14 July had 349 participants under a new name. It is worth noting, however, that many groups and channels set up before August 2017 were left untouched, suggesting the limits of Telegram monitoring.

The Telegram ban in July 2017 was a wakeup call for other tech giants wanting to expand their market in Indonesia that they would have to do more to tackle extremist content. They were already committed to doing so internationally – in June, Facebook, Google, Twitter and Microsoft had formed the Global Internet Forum to Counter Terrorism (GIFCT) to fight terrorism online.[23]

The Indonesian government was also putting the companies under pressure to establish local offices that complied with Indonesian tax law. In August, Facebook agreed to open its first permanent office in Indonesia to serve as a bridge between the government and its headquarters in the US; it also agreed to conduct "geoblocking" on contents deemed illegal in Indonesia (though not erasing them entirely).[24] Through Google, Indonesia became the first Asia-Pacific country to be included in YouTube's Trusted Flagger program. Google in partnership with Kominfo conducted "trusted flagger" training for several civil society groups including ICT Watch, Wahid Institute and the Indonesian Anti-Slander Community (Mafindo).[25] The training meant that reports from those organisations would be prioritised for review by YouTube moderators. Twitter for its part also claimed to have provided a special channel for Indonesian government to report prohibited contents.[26]

As of mid-2018, Telegram had not established a branch office in Indonesia but in August 2017 it had announced the appointment of a local moderating team to facilitate direct communication with the government and speed up the review process. At the global level, Telegram allowed users to report illegal and undesirable contents via its email address abuse@telegram.org;

22 This is consistent with a study of international ISIS Telegram groups where the authors classify users into three categories: sympathisers or potential joiners looking for information, supporters trying to get closer to the terrorist group, and full-fledged propagandists that disseminate messages around the clock and recruit more people. See Mia Bloom, Hicham Tiflati and John Horgan, "Navigating ISIS's Preferred Platform: Telegram, Terrorism and Political Violence", *Terrorism and Political Violence*, 11 July 2017.

23 As terrorists tend to move platforms when blocked, GIFCT tries to prevent this by setting up a database of "hashes" – each of which has a "unique digital fingerprint" that is useful to track files and digital activities. Stuart Macdonald, "How Tech Companies Are Successfully Disrupting Terrorist Social Media Activity", theconversation.com, 26 June 2018.

24 Geoblocking is the limitation of access to a website or other Internet contents based on the users' geographic location. For instance, Facebook agreed to create a special algorithm to geoblock pornographic content in accordance with Indonesian standards which were much stricter than its own guidelines. "Facebook Tawarkan Fitur Penangkal Konten Negatif di Indonesia", www.cnnindonesia.com, 2 August 2017.

25 Erwida Maulia, "Google Training 'Trusted Flaggers' for Indonesia," *Nikkei Asian Review*, 5 August 2017. Wahid Institute is a non-government organisation formed in 2004 that focuses on the promotion of moderate Islam and inter-faith harmony. Established in 2002, ICT Watch concerns itself with digital literacy campaign, protecting freedom of expression, and advocating for accountable and transparent internet governance. Mafindo was founded in 2016 as a crowd sourcing-based online platform to find and evaluate fake news and incitement to hatred.

26 "Twitter Beri Jalur Khusus ke Kominfo untuk Lapor Konten Negatif", www.kumparan.com, 4 August 2017.

the in-app "report spam" feature could also be used to report individual accounts responsible for disseminating violent messages.

III. WEAKENING LINKS TO SYRIA

The increased willingness of the big tech companies to remove extremist content coincided with the weakening of communication links between Indonesian ISIS fighters in Syria and their supporters back home. This also diminished the use of Telegram, but as the 8 May 2018 riot by terrorist suspects in the police detention centre outside Jakarta illustrated, it could still be a potent tool for extremist use.

In 2014 when local ISIS supporters were just beginning to use Telegram, the top Indonesian ISIS leader in Syria, Bahrumsyah, initiated a Telegram group whose members consisted of ISIS media workers and activists of jihadi fundraising groups in Indonesia such as Infaq Dakwah Centre (IDC).[27] The group served in part as a control centre for the translation and dissemination of material from ISIS media wings such as Amaq and Al Hayat Media. By 2016, IPAC had identified at least 150 ISIS-related channels and groups that were active in Indonesia, with the actual figure likely much higher. There was also a special group for channel administrators to coordinate their campaigns and make sure that only ISIS-sanctioned images and videos were disseminated in order to avoid security risks (geotag information in image files could reveal the location of ISIS fighters and facilities, for example).

One by one, the top Indonesian ISIS leaders in Syria have been killed. Bahrun Naim, who joined ISIS in Syria around January 2015, was first reported killed in November 2017 and again in early July 2018, but he had disappeared from Telegram by mid-2017.[28] Bahrumsyah was reported killed in April 2018; he or people around him were key links to ISIS media for the coalition that took over Marawi in the southern Philippines in May 2017. One key contact in Syria from late 2015 onwards was Ustadz Ghana Pryadharizal alias Abana Ghaida, a former journalist with *Sabili* magazine and former member of Persatuan Islam (Persis), a conservative but completely non-violent Islamic organisation in Indonesia. He routinely wrote articles which his wife shared on Facebook; the articles were then forwarded onto Telegram by others. He also responded to individual queries and then ISIS supporters would forward his answer to pro-ISIS Telegram groups more widely. An announcement of his death in Syria appeared on Facebook on 23 May 2018.

ISIS losses in Syria seriously affected the quantity and quality of its media output more generally. In a longitudinal study of ISIS propaganda, Charlie Winter noted a 48 per cent decline in ISIS media production between 2015 and January 2017 (from a daily average of 30 products to 15).[29] Production of high quality videos also saw a sharp decline.[30] To make up for the lack of materials, Indonesian propagandists reposted or modified old products (for instance sharing short excerpts from old *Dabiq* articles) or created new ones on their own. One notable example of the latter is Gen 5.54 that emerged around October 2017 and produced a range of materials from sleek infographics to e-magazines and even an Android application. It was unique because until then, most original content in Indonesian had taken the form of text or audio sermons;

27 "Woman Zone" Telegram group, 14 December 2016. Bahrumsyah, also seen as Bahrum Syah, was the leader of Katibah Nusantara, an Indonesian-Malaysian military unit in ISIS set up around September 2014. He was killed in April 2018.

28 In 2016 Bahrum Naim participated in a Telegram group named Warung Kopi using the pseudonym "Bakul Gudeg", helping members develop military capacity and recruiting the most eager into smaller groups where he gave special instructions and sometimes small amounts of funding for terror plots.

29 Charlie Winter, "Apocalypse, Later: A Longitudinal Study of the Islamic State Brand, *Critical Studies in Media Communication*, Vol. 35, Issue 1, January 2018, pp. 103-121.

30 Ibid.

Gen 5.54 was much more creative and technologically skilled. Telegram, however, banned Gen 5.54 groups in May 2018 and its Android app became inaccessible around the same time; there was no sign of their return as of mid-July. Some younger extremists have expanded to Instagram; in early 2018 they created a new media group called Saveme Project that produced original short videos to post on Instagram, YouTube and Telegram.

As ties to Syria weakened and Telegram content shifted to more local content, the subject matter of pro-ISIS discussions in Telegram groups also changed, to the extent that it could be openly monitored. After ISIS lost Mosul and other territories in mid-2017, Indonesian extremists moved away from general chats to more specifically doctrinal material in order to reinforce their ideological beliefs as some members started to doubt the legitimacy of the caliphate.[31] Terror attacks tend to set off a spike of incendiary content. The prison riot described below is an example of how an attack can spark a rash of violent messaging. The government acted quickly to remove the content but the messages, videos and photos still went viral.

IV. THE PRISON RIOT AT BRIMOB HEADQUARTERS, 8-9 MAY 2018

On 8 May 2018, some 50 terrorist suspects detained at the Brimob headquarters in Kelapa Dua, Depok, outside Jakarta, went on the rampage, apparently after grievances over restrictions on visitors and failure to deliver care packages from family members reached the breaking point – but perhaps with some premeditated planning as well. They overpowered guards, seized control of three blocks in the facility, and got access to dozens of guns from a room on the second floor. When it was over, five police investigators had been killed, several by having their throats cut with broken glass. One prisoner was also shot and killed. A sixth police hostage was rescued and police regained control after 36 hours – but not before appeals went out over social media to ISIS supporters across the country to come to the aid of the rioters against the oppressors (*thaghut*). The incident is worth examining to see how social media can come into play even when the government and the tech companies are improving their capacity to take down extremist content.

A. Messaging Before, During and After

On 29 April, a week before the riot, the administrator of an extremist channel on Telegram that called itself "Just Terror Taktik" posted the following exhortation:

> We, the Admin of "Just Terror Taktik" Group, herewith declare that we will no longer be active on the media front. Our advice to *anshar*/soldiers of the caliphate especially those in Indonesia is: Please be true to your good intentions. The enemies have shown their teeth to us and this religion. O men, where are you when our brothers and sisters are being abused in prison and detention centres? Is there not a desire in you to retaliate against their cruelty? Or is your claim to be Anshar Daulah just a claim? If you really are Anshar Daulah, don't just shout on media...O brothers, let's renew our commitment, prepare yourselves from now on to terrorise *thaghut* and their helpers![32]

As the riot was unfolding on the evening of 8 May, this posting was recirculated. The inmates also began live-streaming a video that was then further broadcast over Instagram and many other accounts. In one clip broadcasted by the Instagram account of sem_maliik87, an injured prisoner is saying, "Kill the *thaghut*, wherever you meet them, in the road, anywhere, including in

31 Nava Nuraniyah, "If You Can't Sacrifice Your Life, Sacrifice Your Data: Online Activism of Indonesian ISIS Supporters", in Shashi Jayakumar (ed.), *Terrorism, Radicalisation & Countering Violent Extremism: Political Considerations & Concerns*, London, forthcoming 2018.

32 "Nusantara Kami Datang" Telegram channel, 29 April 2018.

police headquarters! Attack the headquarters! If we die here, we will die as martyrs!" Instagram suspended the account that same night but the video had gone viral as it was forwarded on to Telegram, Facebook and eventually made its way to the mainstream media, which spread it further.

Someone forwarded the video to Amaq, the official ISIS news service, which then released a 26-second news item featuring snapshots from the video. Just after midnight, in the early hours of 9 May, a Telegram channel called Mutiara Nasehat issued a call to the faithful to go to the gates of the Brimob prison and be prepared to enter heaven: "If those detained can kill the kuffar, what about you who are free?"

Then Ustad Ghana, the Indonesian journalist with ISIS, issued a call from Syria to the *mujahidin* in the prison to fight to the death. "It is forbidden to surrender because you will be tortured and sadistically killed," he wrote, and urged the prisoners to "kill the kuffar in cold blood."[33]

An Indonesian fighter in Syria posted a photo of himself holding a sign that reads "Our prayers are with our brothers in the Brimob prison."

From Poso, on 10 May, fugitive Ali Kalora, one of last few fighters still at large from the Mujahidin Indonesia Timur (MIT), called on supporters to go to the aid of the prisoners. Someone on Telegram also circulated a video showing how supporters outside the prison could use Molotov cocktails to create a street riot and divert attention.

In addition to their video, detainees sent around photos of the ammunition they managed to secure and called on supporters in Indonesia to come and help them or conduct attacks elsewhere to weaken the concentration of the police.[34]

Dozens responded to their call. On 10 May, four men were arrested at a train station in Bekasi en route to the prison. On 11 May, another sympathiser – not linked to the first group – stabbed a police officer to death outside the entrance. Similarly, two young women from Central and West Java who received the online exhortation in their Telegram group arranged to go to Depok together, planning to stab the police with scissors, although they were apprehended on 12 May near the detention centre.[35] After the church bombings in Surabaya on 13 and 14 May (which were not connected to the prison riot), there were more exhortations on Telegram to "ignite the flame of war" in other parts of Indonesia.[36] The Surabaya bombings shocked Indonesia and the world because they were carried out by three families, including the wives and children as young as eight.

B. The Government Response to Incitement

Opposition leaders and the broader public demanded answers as the media revealed the ease with which terrorists involved in the Brimob prison riot used smart phones and social media to coordinate their actions and seek reinforcement from outside. The subsequent terror attacks in Surabaya, Riau and elsewhere in May further pressured the government to act faster. Minister Rudiantara told the press on 11 May that Kominfo was helping the police to track the online communications related to the prison riot.

The rash of terror attacks combined with the online exhortations to violence gave new energy to jihadists who had been waiting for instructions and the opportunity to move. At the same

33 "Batalion Iman" Telegram channel, 10 May 2018.
34 "Nusantara Kami Datang" Telegram channel, 9 May 2018.
35 "Jihad Wanita Penyusup Mako Brimob, dari Turn Back Crime ke Suriah", www.tempo.co, 28 May 2018.
36 "Bayyinah" Telegram group, 2 June 2018.

time, the Surabaya church bombing sparked a heated debate among extremists about whether Islam allowed the use of children as suicide bombers and whether Christian women and children were legitimate targets in states like Indonesia that were not at war.

A video statement by Aman Abdurrahman criticising the Surabaya bombing as illegitimate triggered a flurry of online reactions, pro and con.[37] Aman argued that Islam did not allow children to join a war; he also said that it was not permissible to attack Christians in Surabaya because there were no cases of Christians attacking Muslims there. Some ISIS sympathisers wrote lengthy rebuttals that were circulated on Telegram while those who defended him were labelled *amaniyyun* (Aman fanatics). One convicted terrorist who was active in a Telegram group called for Aman's excommunication because of his statement.[38] Ironically, the death sentence given to Aman on 22 June 2018 restored his reputation among jihadists at least temporarily and all the online fury against him immediately ceased.

V. THE CYBER DRONE 9 SYSTEM AND OTHER TECHNOLOGIES

The prison riot provided Kominfo a useful opportunity to show off its new cyberpatrol technology, the Cyber Drone 9 System. The system uses "machine-learning" algorithms to identify negative and illegal contents in a more proactive manner.[39] The main purpose of such technology is to identify and take down undesirable materials so as to cut off their circulation at the earliest stage. The technology, however, is less effective on encrypted messaging applications because it is not yet able to penetrate private groups.

A. New Technologies

Kominfo in January 2018 launched the new "Cyber Drone 9" system to enhance its cyberpatrol capacity. Unlike the old Trust+Positif system, Cyber Drone 9 handles both passive (report-based) and active monitoring by using artificial intelligence tools (which include image matching, syntactic and semantic analyses) to automatically detect violations online. In June, Kominfo proudly claimed that the crawler machine was able to detect over 22,000 cases of radical content in the two weeks after the prison riot and blocked 4,000 of them.[40]

The 58-strong team operates 24 hours a day to review the information collected by the crawler from websites and social media accounts. To blunt criticism about privacy infringement, the head of Kominfo's Investigation and Enforcement Team, Teguh Arifiyadi, notes that Cyber Drone 9 is not equipped with an "account killer weapon" or "Deep Packet Inspection" technology that can mine personal information.[41] Instead it relies on human analysts to verify negative content that is detected automatically by the AI or reported by citizens or other government agencies. Manual monitoring and reporting are particularly important in the case of encrypted messaging apps because extremist content cannot be identified using algorithms; one has to actually be

37 For the video, see https://www.youtube.com/watch?v=ZLhrX-o7mFo.

38 Aman had made these remarks in the context of his final statement at his trial for involvement in the January 2016 Jakarta bombings, for which the prosecutor was seeking the death penalty. Many speculated that he had made the video to try for a lighter sentence, but it would have been totally out of character for Aman to seek concessions from the government or from a legal system that he scorned. It is likely that his statements genuinely represented his views which were not as extreme as some of the other pro-ISIS militants. For an example of his less *takfiri* position in previous ideological debates, see IPAC, "Marawi, 'The East Asia Wilayah' and Indonesia", Report No. 38, 21 July 2017, pp. 21-22.

39 Machine learning is the use of algorithm that is designed to learn from huge datasets to make predictions about something in the future without being pre-programmed with specific instructions. Michael Copeland, "What's the Difference between Artificial Intelligence, Machine Learning, and Deep Learning?" www.blogs.nvidia.com, 29 July 2016.

40 "Sejak Insiden Mako Brimob, 4078 Situs Radikal Diblokir Pemerintah", www.kabar24.bisnis.com, 4 June 2018.

41 "Kenalan dengan Cyber Drone 9, Polisi Internet Indonesia", www.kominfo.go.id, 5 January 2018.

in the group to read it and understand the link to other groups. Then it can be reported to Telegram. Kominfo has hired analysts to do just that.[42] Other agencies like the police and the State Intelligence Agency (Badan Intelijen Negara, BIN) also conduct their own monitoring though they still have to go through Kominfo as the sole implementer of Internet censorship.[43]

A senior staff member of Cyber Drone 9 said that public awareness of radical and hate speech content had increased significantly after the Islamist-led "212" rallies in 2016 that brought down the ethnic Chinese-Christian former governor of Jakarta, Basuki Tjahaja Purnama, better known as Ahok.[44] The May bombings further increased public awareness to report radical content. In February 2018, Kominfo received only 28 reports from the public about radicalism-related materials. In May, it received some16,000. Upon closer scrutiny, Cyber Drone analysts found that only around 11 per cent fulfilled Kominfo's criteria for blockage.[45]

B. Intolerance vs Violent Extremism

While Kominfo classifies ethno-religious hate speech and violent extremism in separate clusters, the public often does not understand the difference or believes that the first leads inexorably to the second. Many of the reports addressed to Kominfo after the May attacks were in fact related to intolerant groups involved in the 212 rallies such as the Islamic Defenders Front (Front Pembela Islam, FPI), rather than to pro-ISIS extremists.[46] FPI has been known to attack Christians attending "illegal" churches or close down the churches themselves, which might have led some citizens horrified by the Surabaya bombing to report FPI sites they came across online. Other reports turned out to be about conspiracy theories accusing the police of fabricating the May attacks to gain more funding.

Kominfo claimed that based on its internal standards, such terrorism-denial materials were categorised as free speech. But at the same time, police arrested at least five individuals who wrote on their Facebook posts that the government staged the May attacks to justify increased counter-terrorism funding and to divert public attention from anti-Jokowi campaigns. The police charged four of them with violation of Article 28 of the Information Law related to the online distribution of hoax and hate speech (in some cases, the police defined hate speech as hurting the feelings of terrorism victims); one individual was accused of defamation of the police as an institution. [47]

Asked about how to draw the line among intolerance, hate speech and violent extremism, one Kominfo official said:

> We don't look at the organisation, but the content. FPI has not been designated a dangerous organisation by the government. When certain FPI-linked accounts are provocative, [inciting] ethno-religious hatred, of course we block them. Hizbut Tahrir Indonesia (HTI) is a different matter. We put it in the cluster of separatism/dangerous organisations. It's been decided by law, the state has declared it an illegal organisation. The Free Papuan Movement (OPM), Darul Islam/NII are also included in that category.[48]

The decision to ban "radical" content comes down to whether it contains explicit incitement

42 Another alternative is to create bot accounts to automatically join new groups.
43 IPAC interview with Kominfo officials, June 2018.
44 IPAC, "After Ahok: The Islamist Agenda in Indonesia", Report No. 44, 6 April 2018, pp. 8-11.
45 IPAC interview with Cyber Drone 9 official, 22 June 2018. IPAC asked for a copy of Kominfo's censorship criteria but was told that it was not for public.
46 FPI is Islamist anti-vice group known for its vigilantism but it does not challenge state sovereignty or advocate the overthrow of the Indonesian government as salafi jihadis do. More on FPI, see IPAC, 2018, op. cit., pp. 8-11.
47 "Jerat Reaktif di Tahun Politik", in *Tempo*, 11-17 June 2018, pp. 74-75.
48 IPAC interview with Cyber Drone 9 official, 22 June 2018.

to violence:

> [We only ban] those that violate the law, the anti-terrorism law. Actually other agencies like BNPT, BIN, and Ministry of Religious Affairs have more authority to determine the criteria. When someone reports radical content to our system, we would assess it using our SOP (standard operation procedure). Sometimes if it's obvious, like bomb making instruction, we can ban it immediately. But if it's about ideology, the views of various *madzhab* (Islamic schools of thought) on jihad, we can't block those. Or even if it contains the words jihad and *thaghut*, it doesn't necessarily violate the law. The point is it has to contain violent incitement. Sometimes if the report [from the public] does not meet our criteria, lacking evidence or there are other issues we need to clarify with the relevant agencies, we would tell the person that we need recommendation from other agencies before banning them. But in the aftermath of the Brimob prison riot, that was an emergency situation, so we processed reports from the public completely on our own, we bypassed BNPT and so on, because it was urgent.[49]

One problem is that each government agency seems to have its own internal standards to determine hate speech and extremism that are not necessarily discussed with each another let alone with the public. The Jokowi government could usefully push for a single inter-agency set of guidelines which could then be shared with the public through civil society leaders.

C. Tech Company Initiatives

The major tech companies have all developed new tools for trying to identify and remove extremist content. Facebook, for example, has been using machine learning algorithms and other technological tools to combat terrorism (including on Instagram, which the company owns) since 2017. It asserts that 99 per cent of ISIS and Al-Qaeda-related materials it erased as of 2017 were discovered by these algorithms and were removed before any user or state actor reported them.[50]

In Indonesia, however, the government tends to evaluate the companies not in terms of their overall effectiveness but only in terms of how they respond to requests to block particular accounts or postings. In March 2018, Minister Rudiantara released a performance report of eleven social media platforms, saying that Telegram had a 100 per cent compliance rate because it blocked 110 accounts out of the 110 recommended by the government. Facebook was labelled "the least cooperative" because it failed to take down 34 per cent of all content flagged by the government.[51] The disagreements relate mostly to different standards for assessing hate speech, especially in the context of political campaigns. Disagreement over violent extremist content is rare. [52]

Despite significant progress in the government's partnership with the tech companies, pro-ISIS online activists still manage to use encrypted private groups with impunity.

---

49 Ibid.

50 Monika Bickert, "Hard Questions: Are We Winning the War on Terrorism Online?" www.newsroom.fb.com, 28 November 2017.

51 "Kominfo Catat 11 Medsos Punya Konten Negatif, Twitter Terbanyak", op. cit.

52 IPAC interview with Cyber Drone 9 official, 22 June 2018.

VI. HOW INDONESIAN ISIS SUPPORTERS ADAPT TO RESTRICTIONS

Extremists are well aware of the various strategies implemented by the government, Telegram and other social media platforms to curb their propaganda. To avoid keyword detection by algorithms, for instance, they use simple numerical codes such as 1515 for "ISIS" or AD#15 for "Anshar Daulah IS". Overall, extremist survival strategies are low-tech and consist of creating backup channels, outlinking or using multiple platforms to store files, hijacking moderate or Islamist groups, identifying spies, and shifting to other apps. While Indonesian extremists are interested in perpetrating cyberattack and cybercrime, few have the skills to do so.

When government and tech companies trained their crawler machines to identify extremist content, they used a database of materials already identified as extremist. They also anticipated new or more sophisticated techniques such as steganography (concealing video, photographic or text files within another file) that was once used by Al Qaeda. There is no evidence, however, that Indonesian extremists have used complex cryptography, encryption or even moved to the dark web, as some pundits predicted.[53] But it is in their interest to remain in popular platforms such as Facebook, Twitter, and Instagram, with 130 million, 22 million and 45 million users respectively in Indonesia as of 2018.[54] As for encrypted chat apps, Telegram thus far remains the most user-friendly, and ISIS supporters have continued to use it despite more frequent removal of accounts and material.

The fact is that extremists quickly find ways around restrictions on Telegram. The most common regeneration tactic is by creating backup groups and channels long before the original group is banned. Certain channels are made especially to advertise backup links. As of June 2018, IPAC had identified two advertisement channels; each had lasted for a month – much longer than the average lifespan of other channels. Sometimes online activists mark the standby channels with numbers (e.g. Dermaga 1, Dermaga 2, etc); some use various terms within the same category (e.g. a play on the names of Indonesian of television channel such as "KomposTV" instead of the real name "Kompas TV"). In Arabic channels, the secondary channels are often marked as *qariban* (coming soon). Administrators usually guard these backups by leaving them in standby mode (not posting anything) and only activate them once the previous channel is gone.

To anticipate account suspension, propagandists use Internet-generated phone numbers and fake emails so they can have multiple Telegram accounts. The savvier users conceal IP addresses using a VPN and TOR browser, but most ordinary supporters would not bother to do so.[55] While identifying every single new group is almost impossible, the government might do better to map the core propagandists – that is, the group administrators. Although they may change their numbers, user ID, or email, their display names tend to follow specific patterns (e.g. use of specific phrase, letters, or writing style), which intelligence analysts can identify and flag to Telegram. Sometimes simpler methods work best: unsophisticated members may share personal pictures or other information that might reveal their location or which network they belong to.

New channels would be useless if they did not offer abundant material. Thus, propagandists in Indonesia like their counterparts elsewhere, developed a multi-layered file storage system. They

53 Gabriel Weimann, "Going Dark: Terrorism on the Dark Web", *Studies in Conflict & Terrorism*, Vol. 39, Issue 3, 2016, pp 195-206.

54 "Indonesia, Fourth Highest Number of Facebook Users in the World", www.thejakartapost.com, 4 March 2018.

55 VPN, a Virtual Private Network, is a service that changes users' IP address and encrypts their Internet traffic, thus permitting users to browse privately and access geoblocked contents. TOR (The Onion Router) software protects users' anonymity by wrapping communication data (including users' locations) in multi-layered encryption and then sending it through a series of randomly selected relays, with each relay decrypting only a layer of the encrypted bundle before passing it along to the next one and so on until it reaches its final destination.

upload videos or other files on free sharing and storage websites such as JustPaste.it, MediaFire, Mega.nz, Tune.pk, and file.fm. Propagandists also teach their followers how to create mirror websites complete with the content. For example to salvage the repeatedly-banned blog of Bahrun Naim that contains hundreds of pages of terrorist tutorials, extremists not only created mirror websites but also compiled the content into PDF and XML files, then forwarded them to their followers to be re-uploaded in separate mirror websites or Telegram groups. Many such repository channels can be found on Telegram, with some storing only terrorist videos, some e-books, and others audio files. For those who have no technical knowledge, administrators tell them to simply forward any material they receive on to their Telegram friends, their own WhatsApp or elsewhere just so everyone has backup.

Some extremists decided to infiltrate moderate Islamist groups (e.g. Himpunan Mahasiswa Indonesia, HMI) and even non-religious ones such as those linked to private companies to reach new audiences. Most of the original group members would leave, however, after the extremists flooded them with ISIS videos. The extremists then realised that they could use the hijacked group to post all kinds of propaganda and not get banned for a long time. Thus hijacking has become a new strategy to store files and avoid blocking as such mainstream groups appear to be beyond the intelligence radar.

Another strategy to evade intelligence monitoring is by spotting spy accounts or bots. ISIS online groups have been doing their own counter-intelligence. Some members say that they have monitored certain accounts that seem to repeatedly join pro-ISIS groups just before they are banned. They take a screenshot of the alleged spy account and alert other groups. After the partial ban of Telegram in 2017, jihadist supporters online tried out other apps such as Threema and Amn Mujahid. The former was abandoned because it limited group size and required users to pay, while the latter never really took off because it was too complicated for most people to use. Since early 2018 some extremists have been using Tam Tam messenger which some media have dubbed a "complete copy of Telegram".[56] As of this writing, Indonesian ISIS extremists have created at least two dozen groups on Tam Tam.

VII. CONCLUSIONS

The Indonesian government and the tech companies, sometimes working together, often separately, have made major strides in trying to define and block extremist content. Even with the most sophisticated technology in the world, and even when the terrorists are effectively operating in a very low-tech world, it is not an easy task. Extremist propaganda and violent incitement are context-specific and often change over time. It may be that governments have to rely on a combination of high-tech algorithms and human infiltration to achieve maximum disruption of violent extremist groups online.

The critical first step for this combination to be effective, however, is to get clear criteria and political consensus on what constitutes unacceptable content. The Indonesian government has to lead and direct the effort to find this consensus; it is not enough to make anodyne pledges of commitment to moderation and Pancasila. Kominfo may have developed clear internal guidelines itself, but if so, then the Jokowi government should ensure that other agencies fall into line so that other policies can follow: rejection of extremist preachers in government-affiliated mosques if their sermons veer into promotion of hatred against minorities, religious "deviants" or even supporters of pluralism. This is not to recommend arrest or more draconian measures – it is merely to say that if the government has a policy that hate speech or support

56 "Mail. Ru's Tam Tam Positions Itself to Replace Telegram in Russia", www.meduza.io, 18 April 2018.

for violent extremism is wrong, then a series of clear-cut policies should logically follow, and banning clerics who violate those guidelines from government-affiliated mosques and schools is an obvious one.

Closer cooperation among government, tech companies, and civil society is more important than ever. One useful form of cooperation would be to compile a database of real examples to distinguish among legitimate political opinion, hate speech, and criminal incitement that can be shared in discussions everywhere from the National Resilience Institute (Lemhamnas), attended by the political elite, to high schools in remote areas. If Indonesian teachers do not have a clear idea of what is acceptable and what is not, it is no wonder that the whole spectrum of negative content lumped under the rubric "radical" continues to go unchallenged. In security agencies in particular, a general inter-agency training should be conducted under the auspices of Kominfo, perhaps with the participation of consultants from the tech companies, to ensure that there is a common understanding of the guidelines and how to deal with violators.

As for encrypted communication, the government's best bet would be to integrate online and offline intelligence in a more coordinated fashion. Ultimately, online blockage means little if extremists can still meet easily in the real world.

INSTITUTE FOR POLICY ANALYSIS OF CONFLICT (IPAC)

The Institute for Policy Analysis of Conflict (IPAC) was founded in 2013 on the principle that accurate analysis is a critical first step toward preventing violent conflict. Our mission is to explain the dynamics of conflict—why it started, how it changed, what drives it, who benefits—and get that information quickly to people who can use it to bring about positive change.

In areas wracked by violence, accurate analysis of conflict is essential not only to peaceful settlement but also to formulating effective policies on everything from good governance to poverty alleviation. We look at six kinds of conflict: communal, land and resource, electoral, vigilante, extremist and insurgent, understanding that one dispute can take several forms or progress from one form to another. We send experienced analysts with long-established contacts in the area to the site to meet with all parties, review primary written documentation where available, check secondary sources and produce in-depth reports, with policy recommendations or examples of best practices where appropriate.

We are registered with the Ministry of Social Affairs in Jakarta as the Foundation for Preventing International Crises (Yayasan Penanggulangan Krisis Internasional); our website is www.understandingconflict.org. The research for this report was conducted with support from the Danish embassy in Jakarta.