http://www.internationalaffairs.org.au/australian_outlook/terrorists-hijacking-cyberspace/

Published June 24, 2016

Terrorists Hijacking Cyberspace

By Elina Noor

The use of the Internet by terrorist groups and individuals has been an evolving phenomenon since the 1990s. But the convergence of broadband, social media and mobile devices has compounded the volume and speed of propaganda to a staggering level. It is this current wave of terrorist use of information and communications technology that authorities are grappling with in Malaysia and elsewhere.

On 23 May 2016, "Zainuri" was the top trending word on Twitter in Malaysia. The name belonged to a local, long-time militant and bomb-maker, Zainuri Kamaruddin, who had appeared in a Daesh-released video in the same month. The video, filmed predominantly in Indonesian and interspersed with Arabic and Malay, is a mixture of threats at the *toghut* (transgressing) governments of both countries and propaganda featuring, disturbingly, the indoctrination and combat training of a number of minors. It ends with the group of largely under-aged militants tossing their Indonesian and Malaysian passports into a burning pile.

Reports of the video found their way into mainstream media and then, as is typically the case these days, into social media with the reference to Zainuri peaking a few days later. It is unclear just how much of an impact the video made on sympathisers and supporters but upwards of 30,000 Facebook users were talking about him until earlier this month, not all of them favourably.

The use of the Internet by terrorist groups and individuals has been an evolving phenomenon since the 1990s when right-wing White supremacist and other militant groups began exploiting it as a cost-effective mass means of communication. Authorities could still monitor these sites when radical propaganda was being beamed on desktops through dial-up connections. But the convergence of broadband, social media and mobile devices has compounded the volume and speed of these messages to a staggering level. Groups like al-Qaeda and Daesh, and individual supporters comprising a younger and more technologically apt generation, have demonstrated remarkable agility and sophistication in producing high-definition content in multiple languages and channels. It is this current wave of terrorist use of information and communications technology that authorities are grappling with in Malaysia and elsewhere.

In May 2015, Malaysia's Home Minister Datuk Seri Dr Ahmad Zahid Hamidi informed parliament that of the approximately 100 who had then been arrested on terrorism-related charges, 75 per cent had been recruited through social media. A majority of them were "clean skins" or first-time offenders. Parliament was also told the next month that 500 Facebook accounts in Malaysia had been linked to Daesh. About 100 had been blocked for violating Facebook's regulations. Even if the figure is a conservative one, it is miniscule given the estimated 18 million active Facebook users in the country (hardly 0.003 per cent) so the threat—at least on Facebook—should not be overestimated. It does, however, beg the larger question of how to counter recruitment and radicalisation in cyberspace effectively without undermining intelligence gathering opportunities provided by these very same social media channels.

Blocking or filtering content can prove useful stop-gap measures, especially where a threat or risk is significant and imminent. But given the "whack-a-mole" context where blocking a site creates either

multiple mirror sites or many other similar ones, it is the long-game online and offline that will have more impact.

Southeast Asia is finally catching up to the importance of offering counter-narratives catering to the region. In January this year, the Malaysian government announced that a Regional Digital Counter-Messaging Communications Centre would be launched on 1 May. In Indonesia, the country's largest socio-religious organisation Nadhlatul Ulama reminded the nation and the world of "Islam Nusantara" (Islam of the Archipelago) which is the long-held practice of Islam in Indonesia and the surrounding archipelago modelled on moderation and cultural accommodation, if not syncretism, as history bears testimony.

As Southeast Asia plugs the counter-narrative gap, four considerations need to be met to optimise these initiatives. They have to do with the message, the messenger, the actual messaging and the audience.

First, the message must be credible. Daesh's worldview is a binary, rejectionist and sectarian one. The counter-message must recall and embrace the very character of how Islam was originally practised in Southeast Asia: through pragmatic assimilation, integration and acceptance rather than imposition or compulsion. The hotpot of cultures, traditions and values absorbed over centuries through trade and settlement is now at risk of being renounced for puritanical zeal and a Sunni-Shia sectarian schism alien to the Malay archipelago. In essence, the counter-narrative is really the original narrative of the region. For this narrative to work, however, there must be political courage for consistency in both action and intention. The rhetoric of good governance, moderation and celebration of unity in diversity must be matched by reality. Anything short of this will be fodder for extremism.

Second, while governments must actively counter terrorism, they should not actively be seen to be managing counter-narratives. Daesh and similar groups revel in their anti-establishment appeal. As the establishment, governments despite the best of intentions have minimal credibility to be the overt messenger of counter-narratives. Rather, it is society that should be empowered rather than staged to create, produce and innovate content organic to the local context. Credible messengers include "formers" who have renounced extremist ideology and violence, victims of terrorism and families who have lost their own to the sectarian wastelands of conflict. Governments can quietly support these efforts by affording the space and infrastructure assistance behind the scenes.

Third, given that it is youths who have proven to be the most susceptible to Daesh's appeal, counter-narratives will need to be delivered through multiple channels that appeal mainly to them. As such, delivery will need to be done through social media, both creatively and visually. It will also at times require concise messages (140 characters or less) to cater to increasingly short attention spans. In those instances, questions to sow doubt and prompt reflection may work better rather than long, lecturing sermons.

Finally, in reaching out to the target audience, there must be an acute recognition that there are various drivers of violent extremism that resonate with different individuals. What takes place online is often a reflection of larger troubles offline. Sometimes, there are single triggers like personal trauma; other times, there is a combination of push- and pull-factors that draws a person to the choice of terrorism. Salman Rahim, perhaps Malaysia's most profiled militant who exploited social media for the cause of the al-Nusra Front, was deeply disillusioned with politics and governance in Malaysia. He was also genuinely keen to help alleviate oppression and suffering in distant lands among the Rohingya, Palestinians and Syrian civilians. Rather than humanitarian aid, he chose to take up arms.

Getting counter-narratives in cyberspace right will necessarily involve a hard look at ourselves in the mirror of the real world. It will require more than just an expensive, flashy public relations campaign. It will require honesty, commitment and the political courage to acknowledge and redress what is wrong in the country. If we get strive to get it right in real life, we will have less to counter in virtual reality.

Elina Noor is director of Foreign Policy and Security Studies at the Institute of Strategic and International Studies (ISIS), Malaysia.