S. RAJARATNAM SCHOOL
OF INTERNATIONAL STUDIES
A Graduate School of Nanyang Technological University

RSIS COMMENTARIES

No. 003/2014 dated 3 January 2014

Indonesia's Cyber Counterterrorism: Innovation Opportunities for CT Policing

By Sulastri Osman and Navhat Nuraniyah

Synopsis

Indonesia has seen more terrorism-related activities online and in the social media in recent years. While they pose new challenges for counterterrorism policing, they also offer opportunities for innovation.

Commentary

BALI BOMBER Imam Samudra's final message to his supporters was that they should be "hackers, bombers and fighters". Now, more than five years after Samudra was executed for his role in the 2002 terrorist attacks in Bali, a new generation of like-minded extremists have realised his last will as they acquire the technological skills necessary to exploit online tools to facilitate their offline terrorist operations.

Indonesian police's heavy clampdown on terrorist cells across the country, particularly in the aftermath of the 2009 Jakarta hotel bombings, have been paralleled by increasing Internet penetration and the mushrooming of smartphones. These developments have contributed to the rise of terrorism-related activities online.

New generation of tech-savvy terrorists

The rise is not simply about terrorist activities shifting into the cyber realm following the tough police measures. It is also a reflection of how the new actors are of a technologically savvy generation comfortable with their high-tech devices that are fast, mobile and perennially connected. According to a 2013 survey, Indonesia now has 75 million Internet users, a 22% jump from the year preceding, about a third of whom get access to the Internet through their smartphones.

Newfound connectivity and mobility have increasingly facilitated terrorists to reach out to and recruit new members online. The individuals involved in the Myanmar embassy bomb plot in May 2013, for example, had networked over Facebook. Plot mastermind Sigit Indrajid and accomplice Sefa Riano had reached out to others based on their postings on the Rohingya situation, communicated the need to avenge Rohingya persecution and then conspired, even declared their intentions, to attack the embassy over Facebook.

Police have confirmed that the amateur cell had learned to make the pipe bombs intended for use in the attack from an explosives manual they sourced online, highlighting the ease with which terrorists can find tradecraft materials to help them prepare for operations. They were not the first. Pepi Fernando, the mastermind behind the 2011 book bombs, had similarly learned to put together explosives from the Internet.

Indonesia has also seen more cyber hacking activities. To fund ongoing terrorist activities in Poso, Central Sulawesi, Rizki Gunawan, a known militant linked to the cell, and Mawan Kurniawan, an IT specialist and supporter of imprisoned extremist figures, recently made away with over US$625,000 through credit card fraud and hacking activities. Additionally, there have also been more cases of attacks on government websites. The state military website was hacked in late 2012 and early 2013 by Poso-based terrorists who wanted to send a threat to the counterterrorism authorities. The police website had also become a target in 2011.

Wider context impacting counterterrorism policing

There have also been creeping uses of online and social media to tactically facilitate real-time terrorist operations. Investigations into the 2009 bombing of the J.W. Marriott had revealed that the teenage suicide bomber was monitored via an online video call by his handler throughout the operation to circumvent the possibility that he could change his mind. Police had also reported that terrorists use video calls to purchase weapons, on the assumption that the risks of tracing such calls were lower.

The fact that terrorists increasingly use the Internet to support their offline operations is only one part of the problem. There are other factors that in general complicate counterterrorism policing efforts and investigations in cyberspace. Among other things, a key challenge remains the constant tension between maintaining a free cyberspace and ensuring security.

Moreover, with the increasing blurring between online and offline activities, it is difficult to determine whether a particular terrorism-related activity is indeed cyber-specific. This has implications on policies to prevent the exploitation of largely commonplace online technology as well as on measures such as content filtering and restrictions. As cyberspace continues to lack international norms guiding users' online behaviours and actions, counterterrorism policing becomes even more challenging.

What is perhaps more difficult than teasing apart online activities from offline ones is determining their causal links. This particularly affects attempts to understand the actual radicalisation processes of an individual.

Opportunities for counterterrorism innovation

Nevertheless, despite the challenges facing counterterrorism policing, there are equally opportunities for counterterrorism innovation on online and social media platforms.

Among other things, law enforcement agencies could leverage such platforms to gather intelligence. Advanced analytics tools such as sentiment analysis and implicit profiling can help trawl through vast amounts of data online. Much like in the real world, good intelligence lies at the crux of effective counterterrorism policing online. However, in using such tools, restraint and accountability need to be prioritised to avoid the moral hazards of over-surveillance. Also, trained human analysts need to be present to help interpret the data collected and distil meaningful intelligence.

Ultimately, what is needed is a repertoire of responses to the key concern of extremist content in cyberspace, especially the incitement to violence. While a special law to punish individuals who incite violence online can certainly benefit law enforcement, online communities can also be encouraged to conduct self-policing.

Particularly if the Internet is to remain open, there is no need for strict laws to govern every concern since not every dubious activity online translates into a security threat. Self-policing also means that wider education regarding the dangers of extremist content and extremist individuals has to take place alongside the development of norms online.

A way forward is for counterterrorism agencies to not merely see the risks and dangers associated with online and social media but also the opportunities that the same tools can lend them. That said, Samudra's call for his supporters to be hackers, bombers and fighters should act as a reminder that terrorist operations straddle the online and offline worlds simultaneously. Accordingly, any counterterrorism policing efforts online have to account for offline dynamics as well.

Sulastri Osman is Research Fellow and Navhat Nuraniyah is Associate Research Fellow at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University.