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

RSIS COMMENTARY

www.rsis.edu.sg No. 159 – 15 August 2019

Cybercrime: Financing Terrorism in Indonesia

By V. Arianti

SYNOPSIS

Indonesian terrorist groups could resort to cybercrime, specifically hacking, to finance terrorism in the future. The encouragement and guidance by each generation of terrorists is coupled with possible money-laundering paths using virtual payments. This poses a challenge for the authorities to disrupt terrorism financing in the country.

COMMENTARY

TERRORISM FINANCING typically comprises three stages: fund-raising, fund-moving, and fund-using. In the fund-raising stage, terrorist groups have resorted to criminal activities online such as hacking – defined by US cyber security expert Dorothy E. Denning as "activities conducted online and covertly that seek to reveal, manipulate, or otherwise exploit vulnerabilities in computer operating systems and other software" – to finance terrorism.

Is there a propensity for Indonesian terrorist groups to resort to hacking? How do the terrorists move and use the proceeds from their hacking activities? Events in the past point to signs of a potential capability.

History of Hacking

The first successful hacking incident to fund terrorism in Indonesia was reported in 2012, when terrorist group Mujahidin Indonesia Timur (MIT) trainees Rizky Gunawan and Cahya Fitriyanta worked with an extremist hacker, Mawan Kurniawan, to hack a Multi-Level Marketing (MLM) currency trading website by penetrating members' accounts and selling the members' "currency" in 2011.

Of the approximately Rp 6 billion (around US$428,500) proceeds, around Rp 667 million (about US$47,600) was allocated to MIT's military training, including weapons procurement; a tiny amount of Rp 250,000 (around US$17) was used for the September 2011 suicide bombing of a church in Solo, Central Java.

Since then, there has been no reported incident of Indonesian terrorist groups committing fund-raising through hacking to finance terrorist operations, although that they may have attempted to do so – successful or otherwise – undetected.

The Terrorist Hacking Manual

Each generation of Indonesian extremists has produced a hacking manual – with extremist ideological justification – to fund their operations that cater to their era. A Washington Post article mentioned that Imam Samudra, one of the perpetrators of the 2002 Jemaah Islamiyah (JI) Bali Bombings, devoted a chapter in his infamous 280-page book published in 2004, *Aku Melawan Teroris* (I Fight the Terrorists), which encouraged readers to commit cybercrime.

The chapter, titled "Hacking, Why Not", urged his fellow extremists to conduct "carding" (credit card fraud). The chapter outlined a rudimentary carding manual, by first learning computer programming systems and scanning websites vulnerable to hacking. He advised his followers to find mentors and build networks with potential extremist hackers, listing six chat rooms as sources.

Manuals on hacking and carding, including those from non-extremist sources, continue to circulate among the extremist community online. The subsequent generation, namely Bahrun Naim, one of the most tech-savvy Indonesian fighters with the Islamic State (IS) who was killed in 2018 in Syria, had written manuals on his websites on the basics of hacking and carding.

He incorporated those topics in a chapter titled "technology" in his 335-page "manifesto" written in 2016. Some sections in the 96-page chapter on technology provided technical details on hacking and carding, including methods to launder the proceeds using various virtual payments such as PayPal, Western Union, and virtual currency Bitcoin, or cashing them out by purchasing other items online. He specifically provided an example, complete with a picture, on how to hack a PayPal account, one of which was using a scam webpage.

Bahrun's manual on hacking suggested that he himself had attempted to conduct carding and was consulted on the matter. Bahrun Naim's protégé group in Batam, namely Katibah Gonggong Rebus (KGR) led by Gigih Rahmat Dewa, was instructed in 2016 to learn how to hack a PayPal account. KGR was the group which, in 2015, plotted to launch a rocket targeting Singapore.

Money Laundering

Due to the technical expertise required for hacking, a majority of the younger generation of Indonesian extremists may not be savvy enough to do so. Nevertheless, they may aid terrorist groups with fund-moving – laundering the money obtained from the hacking activities, or at least assisting them in transferring funds.

While Bahrun Naim used to have difficulties finding operatives who had PayPal accounts that enabled him to transfer money, this may not be the case for current and future operations, as increasing numbers of individuals become more familiar with virtual payments such as e-money.

The last stage of terrorism financing, fund-using from the cybercrime's proceeds for terrorist operational expenses – i.e. accommodation, transportation, and other logistic items including bomb-making ingredients – can also be performed entirely through virtual payment, without the need to transit the money via a bank account. More e-marketplaces provide options for buyers to make payment via virtual payment providers, rather than the usual bank transfers.

This poses a great challenge as police, in cooperation with the Indonesian Financial Transaction Reports and Analysis Centre (PPATK), are thus far only able to track transactions when the intended recipient cashes out the virtual money into their own, friends' or relatives' bank accounts. This becomes more complicated if the recipients use the funds for their living expenses, rather than for plotting an attack.

Mitigation Efforts

To address terrorist fund-raising, authorities should beef up their surveillance of sympathisers and members of terrorist groups who have the technical expertise to conduct hacking, typically those who are trained or work in the field of information technology.

Most of the cybercrime perpetrators in Indonesia were graduates in computer science or information and technology. A Preventing Violent Extremism (PVE) initiative in universities that is specifically catered to students of those field may be considered, as groups such as JI have specifically targeted students from these fields for recruitment.

On the fund-moving and fund-using end, the Indonesian central bank's policies on licensing virtual payment companies operating in the country and forbidding conventional banks and other non-bank payment companies from processing payments in virtual currencies such as Bitcoin, can further be strengthened.

This can be done by extending cooperation between law enforcement agencies and virtual payment companies that do not have offices in Indonesia. This could assist the former in detecting, investigating and charging terrorist suspects who have committed cybercrime to finance terrorism.

V. Arianti is an Associate Research Fellow at the International Centre for Political Violence and Terrorism Research (ICPVTR), a constituent unit in the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.