RSIS COMMENTARY

15 July 2025

Safeguarding Singapore: Addressing the Impact of Transnational Scamming Operations in Southeast Asia

Yen Zhi Yi

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

Ponder the Improbable since 1996

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

RSIS COMMENTARY

www.rsis.edu.sg No. 154 – 15 July 2025

Safeguarding Singapore: Addressing the Impact of Transnational Scamming Operations in Southeast Asia

By Yen Zhi Yi

SYNOPSIS

In recent months, heightened media scrutiny has drawn attention to the proliferation of scam centres along Myanmar's border towns and the subsequent crackdowns on them. Concurrently, Singapore has also witnessed a significant increase in scam-related incidents, with the government urging vigilance and taking precautionary measures to safeguard its citizens. Against this backdrop, it is imperative for ASEAN countries to work collaboratively to tackle this growing cross-border scourge. Doing so calls for stepped-up action at home to enhance awareness and enforcement collaboration abroad among regional partners to check this transnational security challenge.

COMMENTARY

Cyber scam centres in Myanmar recently gained considerable attention after the high-profile rescue of a Chinese actor who went missing in Thailand. Thailand then conducted a power cut to Myanmar's border areas to disrupt scam operations, which freed hundreds of trafficked victims from the scam centres. Subsequently, Singapore urged its citizens to be vigilant of various forms of scams and to take precautionary measures against them.

Since 2023, at least 200,000 individuals have been forcibly detained in compounds in Myanmar and Cambodia to execute scams. In 2024 alone, scam operations, the growth of which has been facilitated by technological advancement and political instability, have cost victims a staggering amount exceeding US$1 trillion globally, despite countries already implementing new laws and measures to curb them. There is merit in examining how these massive scam operations can have far-reaching transboundary consequences, affecting Singaporeans and others in the region.

Scams, Technology and Domestic Politics

Transnational scams are not novel to states in the Association of Southeast Asian Nations (ASEAN) and are especially prevalent in the border regions of Myanmar, Thailand, Laos and in the Philippines. Since the 2010s, industrial scam centres began to emerge as China initiated crackdowns on online gambling and money laundering, forcing criminal syndicates to switch to scams for revenue. A 2023 report by the United Nations Office of Drugs and Crime (UNODC) revealed that online casinos proliferated during the COVID-19 pandemic, due to the popularity of digital payments, e-commerce and cryptocurrencies as people are confined to their homes.

Scamming operations have now grown in scale and sophistication, partly due to the increased ease of access to artificial intelligence (AI) tools and the growing number of people spending their time chronically online. AI has enhanced scammers' capabilities, such as enabling the creation of deepfake multimedia and AI-driven phishing.

Another UNODC report in 2024 observed that scammers now utilise deepfake technology to carry out social engineering scams, targeting victims' emotions and trust. For instance, a financial director nearly lost almost S$670,000 (US$523,000) after acting on the instructions of his company's chief executive officer and others who were impersonated using deepfake technology.

Additionally, Southeast Asia's mobile penetration rate is one of the highest in the world at 136 per cent. This means that the risk of exposure to digital scams is significantly higher than before, while scammers get more chances to leverage unsuspecting victims' digital usage patterns.

Another factor contributing to the emergence of scam compounds in the region is the fraught domestic politics of some Southeast Asian states, such as the civil war in Myanmar. For instance, massive scam compounds can be found along the border areas of Myanmar, like Myawaddy.

Most are run by Chinese criminal syndicates, but some are operated by local Ethnic Armed Organisations (EAOs) as well as junta-aligned groups. The revenue generated by scam operations in conflict-torn regions indirectly perpetuates civil conflict, pointing towards the possibility of them keeping scam operations going to fund the conflict.

In Cambodia, some elites have come under fire for being implicated in scam networks. At the same time, a national conglomerate was recently exposed as a lucrative platform for fraudsters dabbling in money and personal data laundering, among others.

Many cases likely remain unchecked due to their murky connections with the domestic political environment. The lack of robust measures and willingness to crack down on scams in these states could prove detrimental to Southeast Asia's economy and human security.c

Implications for Singapore

Scams targeting Singapore have resulted in significant and increasing economic loss for the victims, who are tricked into transferring the money themselves. The Singapore Police Force's (SPF) annual scam brief noted that at least S$1.1 billion (US$860 million) was lost in 2024 through a total of 55,810 scam cases, a sharp increase from 15,756 cases in 2020.

Self-effected transfers also make up more than 80 per cent of cases in 2024, highlighting the importance of understanding the psychological and social factors surrounding susceptibility to scams, the profiling of potential victims by scammers, and the methods used to do so.

The threat of transnational scams could also be detrimental for Southeast Asia's road to technological integration, especially with the ASEAN Digital Economic Framework Agreement (DEFA) coming into play. The proliferation of online scams in the region might compromise the safety of digital monetary mechanisms and impact investors' confidence.

In light of this, the issue of transnational scams is likely to be raised more frequently and urgently at regional summits, as seen in the recent meeting of the ASEAN Working Group on Anti-Online Scam (WG-AS) on the sidelines of the ASEAN Digital Senior Officials' Meeting and ASEAN Telecommunications Regulators' Council (ADGSOM – ATRC) Leaders' Retreat which took place in early 2025.

A Two-pronged Approach

Singapore, as a leading financial and technological centre, has consistently championed robust cybersecurity measures and the raising of digital literacy. This is reflected in the extensive array of public awareness campaigns and official platforms dedicated to equipping public servants and citizens with the necessary knowledge to recognise and counteract scams, as well as shield themselves from becoming victims. For instance, the Global Anti-Scam Organisation (GASO) was founded locally by a former scam victim to extend support to those in the same boat and enhance investigative efforts into the region's scam industry. In January 2025, the country also passed the Protection from Scams Bill to address the large number of cases of self-effected transfers and repeat scam victims.

Singapore has also taken steps to bolster regional efforts in dealing with digital scams. For instance, the Republic hosted the Global Anti-Scam Summit in 2024 to share knowledge and brainstorm protective measures. It chaired the ADGSOM in 2024 and took the initiative to develop an ASEAN anti-scams guide and best practices, which will include a region-wide information-sharing arrangement.

These initiatives are not just symbolic but reflective of a calculated effort to promote regional cooperation and recognition that disrupting scammers' operations would require a multi-layered approach involving both governments and industries. However, the opaque and convoluted nature of scam networks remains an impediment to efforts to hold the principal perpetrators accountable legally.

Individuals must remain vigilant and exercise rigorous due diligence to protect themselves, not least by paying heed to safeguards implemented at the national level. Ultimately, an approach that bridges jurisdictional divides and fosters trust among law enforcement agencies across states is essential to safeguarding the region's digital ecosystem and citizenry against transnational scams.

Conclusion

While media coverage has raised awareness of the scam centres in Southeast Asia, the complex interplay between this flourishing illicit economy, rapid digital transformation and shifting domestic political environments calls for stepping up efforts to counter this cross-border scourge, given the repercussions for Singapore. The country's two-pronged approach in fortifying its domestic defences and enhancing regional coordination reflects an understanding that scams are not merely a local law enforcement problem but also a transnational security challenge.

However, addressing the root of the problem requires a more holistic approach. This includes enhancing data-sharing and fostering robust coordination with ASEAN partners and other key actors, including China, to dismantle scam operations at their source. Addressing the structural drivers and transnational enablers of scams is imperative to safeguarding Singapore's digital ecosystem and mitigating the risks posed by evolving criminal organisations.

Yen Zhi Yi is a Senior Analyst in the National Security Studies Programme at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. Her research interests include Southeast Asian Politics, Civil-Military Relations in Asia, and ASEAN Regionalism and Regional Order.

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798

Please share this publication with your friends. They can subscribe to RSIS publications by scanning the QR Code below.