

Muhammad bin Ibrahim: Readying the financial sector amid the evolving war on terrorism financing

Welcoming remarks by Mr Muhammad bin Ibrahim, Governor of the Central Bank of Malaysia (Bank Negara Malaysia), at the Third Counter-Terrorism Financing Summit 2017 "Powering Regional Solutions Through Strengthened Alliances and Innovations", Kuala Lumpur, 22 November 2017.

* * *

“Readying the financial sector amid the evolving war on terrorism financing”

Welcome to Sasana Kijang, Bank Negara Malaysia. We are pleased to host the 3rd Joint Regional Counter-Terrorism Financing Summit 2017 with our partners, the Australian Transaction Reports and Analysis Centre (AUSTRAC) and Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) Indonesia.

The Summit, which was first held in 2015 in Sydney, has now become a hallmark event for many across the region; policy makers, law enforcement personnel, the financial intelligence community and financial industry players. The Summit is a cumulation of the year’s work in producing impactful outcomes for counter terrorism financing. With over 400 participants from over 30 countries and international organisations, this Summit is a testament to our commitment and determination to strengthen our cooperation in combating undesirable financial activities across the globe.

The nature of terror and terrorism financing is much more complex, say, compared to ten years ago. Numerous new methods to raise, move and store funds, were conducted through small-scaled transfers via banks or money services businesses. And in some cases, via physical transportation of cash. Recent advancements in financial technology provide new opportunities for anonymity. We should envisage that terrorist financiers will attempt to benefit from anonymous transactions made possible by innovations of new payment products and services such as internet-based payment systems, prepaid cards and virtual currencies.

Likewise, fundraising through social media and other online platforms such as “*crowdfunding*” have increased in prominence, in addition to other more traditional sources of funds such as proceeds of criminal activities, conventional donations, and funding from legitimate purposes.

As change is a constant, collation of data points that this environment will continue to persist. Global internet users have increased from 397 million in the year 2000 to nearly 3.9 billion as of June 2017, an impressive growth of almost 1000%.

Similarly, global investment activities in the FinTech industry have increased from USD9 billion in 2010 to USD25 billion in 2016. If this trend is anything to go by, the financial industry will be hard pressed to mitigate, identify and prevent cases of abuse in the system.

There is no doubt that rapid technological developments have offered immense potential for economic growth. Unfortunately, they have also spawned new ways for terrorist organisations to acquire, move and manage their funds. There are other risks not anticipated before, such as remote radicalisation via the internet that has resulted in an increase in the number of small terrorist cells and “lone wolf actors” that makes detecting and halting terrorism financing even more challenging.

In light of this development, the role of financial sector as a bulwark against terrorists financing becomes even more critical. The financial system must always be in a state of readiness to identify and effectively prevent any emerging risk of terrorism financing.

Let me suggest a three-pronged strategy to erect stronger defences within the financial system. This will include capitalising on technology, promoting clever partnership between the authorities and industry, and closer international cooperation.

Capitalising on technology

While technological misuse poses a danger to society's wellbeing, technology is also an effective tool to counter terrorism financing. Akin to using a diamond to cut a diamond, we must harness the vast potential in technological innovations to reinvent and reinforce our lines of defence.

A rule-based system, which is at the core of many of such preventive programmes today is becoming increasingly ineffective. The reliance on automated systems to monitor and detect suspicious transactions have served us well, but as we move forward, we need to do more. We need new tools. The adoption of artificial intelligence, machine learning, and big data technology are tools that would likely be imperative, as suspicious transactions become more complex and harder to detect.

As we learned from the Innovation Forum at this Summit, the use of artificial intelligence and big data will have the potential to increase efficiency and accuracy of assessments that is essential in a dynamic environment. The banking sector needs to adopt the latest and most advanced technologies to improve its risk management framework.

We need to prepare ourselves, as according to many pundits, digital currencies will become the new norm. The advent of digital currencies as some have forecasted, will mark the beginning of a new era in the financial sector. As authorities, we cannot be oblivious to these developments.

As such, Bank Negara Malaysia has initiated the foundational work for the development of a regulatory structure for digital currencies. Beginning 2018, Bank Negara Malaysia will designate persons converting crypto currencies into fiat money currencies as reporting institutions under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001. This is to prevent the abuse of the system for criminal and unlawful activities and ensuring the stability and integrity of the financial system.

Strategic partnership

Dynamic collaboration between the public and private sector is imperative to create an environment conducive for the creation of innovative solutions. One of the main findings from the Global FinTech Report published by PWC recently is that legislation is not keeping pace with innovation, creating significant uncertainty. This tells us that a more adaptable structure in policy-making, that minimises bureaucratic hurdles or "red tape", could be advantageous under the current dynamic environment to encourage potentially important innovations.

For that reason, Bank Negara Malaysia launched its very own FinTech Regulatory Sandbox in 2016 to allow experimentation of FinTech solutions in a 'live' environment. A number of innovative financial solutions have been allowed to operate under this Sandbox initiative, including an e-KYC solution that could revolutionise the AML/CFT framework in the financial sector in Malaysia. This initiative allows for the viability of new technologies to be tested in a controlled environment while simultaneously exploring potential risks and the mitigating measures.

In addition, Bank Negara Malaysia will continue to foster cooperative platforms between the authorities and financial institutions to enable "rapid responses" to terrorism financing threats. Early this year, we facilitated an information sharing platform between law enforcement agencies and selected financial institutions to swiftly and effectively mitigate risks and respond to threats.

Greater access of intelligence information for financial institutions and the increased threats from ISIL had resulted in the upward trend of reporting of Suspicious Transaction Reports (STRs). To

put it in perspective, in 2015, the financial intelligent unit (FIU) received 93 terrorism financing related STRs which led to 14 disclosures to law enforcement agencies. In comparison, between January and June 2017, we received 346 terrorism financing related STRs which have led to 34 disclosures to law enforcement agencies. Importantly, the quality of STRs submitted has also improved.

Bank Negara Malaysia is also in the midst of finalising the details of a new requirement for the Banking and Money Services Business sector to report remittances in high risk areas. The high risk areas will be determined based on the law enforcement agency's intelligence on areas that they view may pose higher risks for funding of terrorism activities.

This is consistent with the Terrorism Financing Regional Risk Assessment findings at the 2nd CTF Summit in 2016 in Bali, where one of the priority actions identified was for FIUs to improve the visibility and insights into the nature of terrorism financing in the region. The idea is intended to help FIUs gain better insights into the role of financial and transit hubs in regional and international terrorism financing networks.

Closer international cooperation

Another area to ensure an effective mitigating strategy requires closer regional and global cooperation, particularly in the sharing of intelligence and technical know-how. Terrorism and terrorism financing are global issues that demand global solutions. Sharing of intelligence and expertise across borders will go a long way towards enhancing the effectiveness of our risk management framework.

In this regard, the various working groups under the CTF Summits, the Financial Intelligence Consultative Group and International Community of Experts have done commendable efforts and initiatives in building capacity and sharing operational experiences in the region. This must continue to be strengthened given the challenges that we will face.

Conclusion

The fight against terrorism financing is an on-going battle that will continue to evolve in line with the ever-changing landscape of the financial industry. In the era of rapid technological advancements, it is essential that the financial sector's risk management strategy remains agile in order to mitigate emerging risks. This requires not only the development of innovative technology-based deterrents and pro-active detection systems, but also effective cooperation between the public and private sector, law enforcement domestically and across borders.

We stand ready to work alongside all key stakeholders, in both the public and private sectors, local and abroad, to ensure our financial sector is resilient to face the threat of terrorism financing within the country and in the region.