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

RSIS COMMENTARY

www.rsis.edu.sg No. 012 – 16 January 2024

RSIS Commentary is a platform to provide timely and, where appropriate, policy-relevant commentary and analysis of topical and contemporary issues. The authors' views are their own and do not represent the official position of the S. Rajaratnam School of International Studies (RSIS), NTU. These commentaries may be reproduced with prior permission from RSIS and due credit to the author(s) and RSIS. Please email to Editor RSIS Commentary at RSISPublications@ntu.edu.sg.

UN Cybercrime Convention: Relevance to ASEAN

By Helena Huang

SYNOPSIS

The upcoming United Nations Cybercrime Convention is an excellent reference point for ASEAN Member States to leverage and develop bilateral and multilateral regional baselines to combat cybercrime.

COMMENTARY

Since 2001, there has only been one international, non-regional cybercrime agreement: the Budapest Convention on Cybercrime. Despite there being no restrictions on states seeking to be a signatory, the Budapest Convention has been ratified by only 68 countries.

In January 2020, the United Nations General Assembly decided to establish an Ad-Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (AHC).

The AHC has been tasked with drafting the text for a comprehensive UN Cybercrime Convention envisioned to "[counter] the use of information and communications technologies for criminal purposes, taking into full consideration existing international instruments and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes".

The concluding session of the AHC will take place from 29 January - 9 February 2024, during which UN member states will vote for the final version of the convention.

The ASEAN Context

While there is no equivalent cybercrime agreement in Southeast Asia, ASEAN is familiar with the efforts and challenges needed to combat cybercrime. ASEAN established the Senior Officials Meeting on Transnational Crime (SOMTC) in 1999. This was followed in 2014 by the establishment of the ASEAN Working Group on Cybercrime as part of the cybercrime component of the SOMTC's work programme from 2013-2015.

In 2017, ASEAN adopted the Declaration to Prevent and Combat Cybercrime, reaffirming ASEAN Member States' (AMS) commitment to "continue working together in the fight against cybercrime through activities aimed at enhancing each member state's national framework for cooperation and collaboration in addressing the misuse of cyberspace''.

Yet, there is no known document on cybercrime to guide ASEAN's efforts on a regional basis. With eight AMS involved in the text negotiation, there are sound reasons to use the UN Cybercrime Convention as a point of reference for ASEAN to set baselines and coordinate regional efforts at combatting cybercrime.

Defining Working Parameters

Firstly, the UN Cybercrime Convention sets working parameters for what is considered cybercrime. While there was no concurrence on the definition of cybercrime during the negotiation process, the drafted text is clear in the identification of particular cyber-dependent and cyber-enabled offences, including online child sexual exploitation and solicitation, terrorism and arms trafficking, illegal distribution of counterfeit medicines and medical products, and the encouragement of or coercion to suicide.

ASEAN currently does not have a working definition for cybercrime, and neither has it published a list of offences that are considered cybercrimes. Taking reference from what has been set out as cybercrime in the UN Cybercrime Convention could be a way for AMS to harmonise and to ensure that they are all aligned in their understanding of cybercrime. The common understanding will serve as a cornerstone in the designing of an approach to combat cybercrime and a foundation for reliable data collection and metrics, which are essential to measure and monitor cybercrimes in the region.

Establishing Regional Baselines

Secondly, the UN Cybercrime Convention has established a baseline in the norms of international cooperation related to cybercrime which can be duplicated and calibrated by ASEAN for regional, bilateral, and multilateral use. The convention acknowledges the need to protect sovereignty and non-intervention, which are akin to ASEAN's fundamental principle of non-interference.

In the negotiation process, it is likely that the majority of the AMS would be agreeable to much of the draft texts or at least made aware of their respective country's non-negotiables. This could potentially assist in calibrating and aligning current cybercrime conversations in ASEAN and speed up discussions within the region to a common

level of the text, besides helping in establishing the international baseline and requirements put forth in the convention.

As ASEAN consists of ten countries with different cultures and levels of development, it would be unrealistic to copy and implement the clauses in the UN Cybercrime Convention wholesale. Nevertheless, with the common grounds ascertained, the AMS can kick-start conversations for bilateral and multilateral cooperation, such as, for example, mutual legal assistance agreements for cybercrime.

Importance of Capacity Building

Thirdly, the UN Cybercrime Convention emphasises the importance of capacity building and recognises the need for countries to develop the necessary expertise and resources to address cybercrimes. It sets out a clear structure of what would constitute capacity building and technical assistance in this realm, which is not covered by any ASEAN initiatives at the moment.

Currently, there are two ASEAN initiatives on cyber governance and cyber operations but they – the ASEAN-Singapore Cybersecurity Centre of Excellence and the ASEAN-Japan Cybersecurity Capacity Building Centre – are not explicitly about capacity building for skill sets related to cybercrime. These overlooked skill sets range from specialised investigation techniques and the preservation techniques in ensuring the integrity of evidence in electronic form, to policies and practices related to the proper protection of cybercrime victims and witnesses. There is a need to build capacity to address cybercrimes.

It should be noted that a non-ASEAN initiative on cybercrime capacity building exists in the region – the INTERPOL Cyber Capabilities and Capacity Development Project. Funded by the United States Department of State, it is a project intended to "strengthen the ability of countries in [ASEAN] to combat cybercrime and to work together as a region".

Involving Multi-stakeholders

Last, but not least, the UN Cybercrime Convention also highlights the necessity to leverage the expertise of groups such as "non-governmental organisations, civil society organisations, academic institutions and the private sector", most of which have not been currently and routinely involved in cybercrime discussions in ASEAN.

These discussions usually take place at the SOMTC and at the ASEAN Working Group on Cyber Crime, with little or no published information on the discussions that had taken place, nor the action plans on cybercrime matters. The current "eco-system" for cybercrime discussions in ASEAN is top-heavy with minimal leverage on the expertise of non-governmental bodies and academic institutions.

Conclusion

After the conclusion and finalisation of the UN Cybercrime Convention next month, the true test of its importance and relevance would be the number of countries that ratify it. While the draft text is still being negotiated, it should provide enough guidance for

civil society, academics, and legal and enforcement policy makers in AMS to do some preliminary work on cybercrime. Think-tanks in AMS should also consider devoting sufficient resources to Track 1.5 and Track 2 discussions on combatting cybercrime.

Helena Huang is an Associate Research Fellow in the Executive Deputy Chairman's Office, S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. Her research straddles both digital and cyber issues, covering topics such as cybercrime, human rights in the digital space, and how the use of digital technologies impact states and societies.

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
T: +65 6790 6982 | E: rsispublications@ntu.edu.sg | W: www.rsis.edu.sg