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

RSIS COMMENTARY

www.rsis.edu.sg No. 189 – 6 December 2024

How ASEAN's Cybersecurity Push Could Protect People and Economies

By Muhammad Faizal

SYNOPSIS

As ransomware attacks and cyber scams surge across Southeast Asia, ASEAN is stepping up to create a more secure regional cyberspace.

COMMENTARY

With cyber criminals targeting the region's critical infrastructure, including data centres, and young and old users at risk of falling victim to digital scams, ASEAN's efforts are not only about digital security — they're also aimed at protecting economic and social stability.

In October 2024, ASEAN members launched two major initiatives. First, the ASEAN Regional Computer Emergency Response Team (CERT) opened its Singapore headquarters to boost collaboration on cybersecurity incident response, with Malaysia leading as the first overall coordinator. This response team focuses on critical areas including information-sharing and strengthening public-private partnerships to bolster defences across the region.

In the same month, the Cyber Security Agency of Singapore and Malaysia's National Cyber Security Agency introduced the Norms Implementation Checklist. This list of action points aims to guide ASEAN nations in promoting responsible behaviour in cyberspace, based on United Nations cybersecurity norms.

Responding to a Surge in Cyberattacks

This year, the region has experienced a spate of major ransomware attacks. For example, a major incident occurred in June, when the Brain Cipher ransomware group

disrupted the data centre operations of more than 200 government agencies in Indonesia.

Critical information infrastructure supports government and other essential services, so any disruption can cause severe socio-economic impacts that undermine public trust in government.

The threat of disruption from cybersecurity incidents extends to the private sector where, for example, in Singapore, three out of five companies polled had paid ransom during cyberattacks in 2023.

In addition, cyber scams are a major crime concern: they often impact vulnerable groups and are now so common they have become a regional security threat. The rapid pace of digitalisation in Southeast Asia, coupled with low digital literacy and the ease of conducting online financial transactions, has facilitated a sharp increase in cyber scams such as phishing and social media scams.

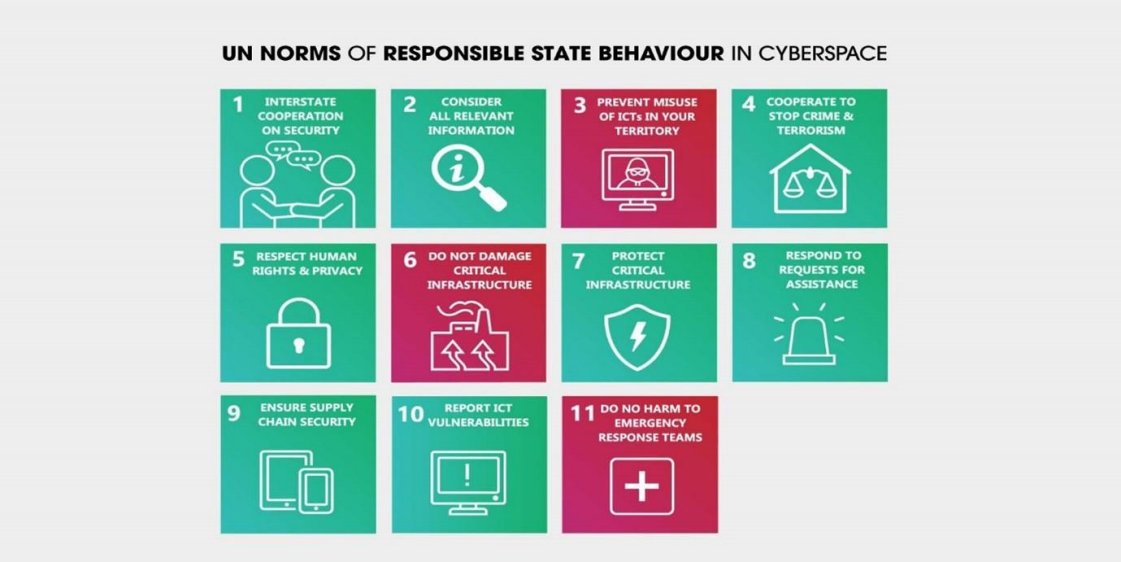
Tackling cyber scams at the source is challenging. Transnational organised crime groups thrive in Southeast Asian countries with limited cybersecurity and insufficient law enforcement capabilities. They often collude with local power structures: for example, they operate in conflict areas near the border of Myanmar, where they collude with militia groups.

Given these increasing threats, the launch of the ASEAN Regional CERT is a promising effort to enhance cooperation among Southeast Asian countries. The eight functions of the response team — which include information-sharing, training and exercises, as well as developing partnerships with academic institutions and industry — aim to strengthen regional coordination on cyber incident response.

Incident response is a critical part of the region's attempts to mitigate the impact of malicious cyber activities such as ransomware and the epidemic of cyber scams.

Strengthening ASEAN's Strategic Position in Cyberspace

In 2018, ASEAN agreed to subscribe in principle to the 11 UN norms of responsible state behaviour in cyberspace. While their full potential has not yet been realised, these 11 norms, set out in the UN's Norms Implementation Checklist, could play a crucial role in helping ASEAN member states progress from "in principle" to "in practice" in the cybersecurity space. These norms aim to guide countries' national cyber policies to align with the rules-based international order set out by the UN.



Source: Australian Strategic Policy Institute

Adherence to these cyber norms (such as fostering inter-state cooperation on security, preventing misuse of information and communications technologies, and cooperating to stop crime and terrorism) could, ideally, complement the work of the ASEAN Regional CERT in responding to malicious cyber activities and fighting cyber scams.

Regional implementation of these norms could contribute to an environment of trust and confidence among ASEAN countries, to create stability in Southeast Asia's cyberspace.

There are strategic reasons for creating regional cyberspace stability. As the UN Secretary-General Antonio Guterres has warned, cyberspace is increasingly being exploited as a weapon in conflicts — by criminals, non-state actors, and even governments. This trend is inimical to ASEAN's regional ambitions, strengthening the argument for nations in the region to proactively adopt a cyber rules-based order.

What's more, ASEAN aims to be a zone of peace, freedom and neutrality. This goal emphasises keeping the region free from interference by external powers that could create insecurity. As ASEAN established this goal in 1971 during the analogue era and Cold War, it is only appropriate that the organisation develop new initiatives to adapt to the digital era and Cold War 2.0.

ASEAN should also promote the Norms Implementation Checklist as a guide for other countries that are its dialogue partners but are embroiled in geopolitical and cyber rivalry (such as China and the United States).

Observers warn that the inability of the regional group to address the Myanmar civil war and rising tensions in the South China Sea, both of which involve cyber activities, is eroding its relevance. This crisis consequently shapes how some ASEAN members and external powers view ASEAN centrality. It is also among the reasons why non-ASEAN security arrangements — such as the Quad, Indo-Pacific Four and Japan-Philippines-US Trilateral Summit — are establishing cooperative efforts, including on cybersecurity, in the Indo-Pacific.

Taking the lead on cybersecurity, both through the Norms Implementation Checklist and the ASEAN Regional CERT, is therefore crucial to the security of people and economies in Southeast Asia.

It could also prevent ASEAN's centrality in regional security matters from eroding further. But this is contingent on ASEAN nations providing sufficient resources, policy thinking and political will to make these two initiatives deliver results.

Muhammad Faizal Abdul Rahman is a Research Fellow (Regional Security Architecture Programme) with the Institute of Defence and Strategic Studies (IDSS) at S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.

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