Advancing cyber and information security cooperation in ASEAN

Muhammad Faizal Bin Abdul Rahman

2023

Muhammad Faizal Bin Abdul Rahman (2023). Advancing cyber and information security cooperation in ASEAN. RSIS IDSS Papers; 001-23.

https://hdl.handle.net/10356/164280

RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore
Ponder the Improbable since 1996

IDSS Paper
Ponder. Analyse. Prepare. Engage. Refresh.

www.rsis.edu.sg No. 001 – 4 January 2023

No. 001/2023 dated 4 January 2023

Advancing Cyber and Information Security Cooperation in ASEAN

Muhammad Faizal bin Abdul Rahman

SYNOPSIS

The security of the cyber and information space is essential to the digitalisation ambitions of the ASEAN countries. ASEAN must keep abreast of a threat landscape where malicious cyber and information operations are constantly evolving. ***MUHAMMAD FAIZAL*** *notes that, in two specific areas of threat, synergies can arise by coordinating the efforts undertaken by various ASEAN mechanisms such as the ASEAN Digital Ministers' Meeting and the ASEAN Defence Ministers' Meeting.*

COMMENTARY

Given the criticality of the cyber and information space, the ASEAN Digital Ministers' Meeting (ADGMIN) has launched the ASEAN Cybersecurity Cooperation Strategy (2021–2025). To follow through with this strategy, some initiatives were launched in 2022. For example, in January 2022, the ASEAN Senior Officials Meeting on Education (SOM-ED) launched the "Training-of-Trainers Program to Counter Disinformation and Promote Media Literacy" to build up media literacy and critical thinking as defences against disinformation.

In June 2022, the 16th ASEAN Defence Ministers' Meeting (ADMM) adopted the terms of reference of the ADMM Cybersecurity and Information Centre of Excellence (ACICE). The terms outline four primary workstreams, namely, (i) setting up a database on cyber malware and information threats, (ii) increasing awareness and knowledge such as through think tank and academic exchanges, (iii) promoting interactions such as through dialogues and exercises, and (iv) supporting the activities of the ASEAN Cyber Defence Network (ACDN).

In October 2022, the ASEAN Regional Computer Emergency Response Team (CERT) was established to enhance the region's operational readiness and deepen cooperation and information exchanges between national CERTs, academia, and industry. Recognising the criticality of cross-border information infrastructures, the scope of CERT's functions includes the banking, aviation, and maritime sectors.

Many national security and defence agencies around the world are standing up or enhancing existing cyber security infrastructure and capabilities. *Image from Wikimedia.*

To sum up the year's efforts, the Chairman's Statement following the ASEAN Summit in November 2022 acknowledged existing efforts, including the activities of ADMM-Plus Experts' Working Groups (EWGs) and the ASEAN Regional CERT that contributed to building the regional cybersecurity posture. The statement also supports enhanced synergy among ASEAN mechanisms to maintain security and an ASEAN-centric regional architecture.

Importance of Synergy

In two specific areas — the Russia-Ukraine war and maritime security — where malicious cyber and information operations could occur in concert for strategic or tactical advantage, ASEAN countermeasures would benefit from the synergy that arises from cooperation.

Based on current trends, a 2023 forecast by the cybersecurity company Mandiant predicts the continuation of malicious operations in the form of digital credentials theft, "ransomware-as-a-service" attacks, cyber espionage and information operations, including those by hacktivist fronts and outsourced to "hack-for-hire" actors to target state and strategic private sector entities. Moreover, these operations would affect information systems and permeate social media platforms, as predicted by the cybersecurity company Norton.

Such operations may have limited tangible impact during a war. But they could be powerful tools in the continuum between peace and war, also known as the grey zone, where geopolitical contestation among major powers is increasingly intense. For

ASEAN, the grey zone situation due to the action–reaction dynamic spurred by China's influence operations will persist. As articulated by the former foreign minister of Indonesia, Dr Marty Natalegawa, the region is again surrounded by an arc of instability. Hence, ASEAN needs a foresightful approach to maintain security.

A foresightful approach could render the sharing of threat analyses and experiences more meaningful and could be aimed at identifying opportunities for synergy between various ASEAN mechanisms and initiatives. For example, to extract lessons from cyber and information operations in the Russia-Ukraine war, defence agencies should analyse how threat actors could learn from the Russia-Ukraine experience to raise their game. Just as how threat actors may depend on the synergy of cyber and information operations to influence their targeted audiences, defences against such threats require a synergy of preventive and countermeasures. This endeavour of learning from the present to prepare for the future is a role that is best suited for ASEAN-related centres, particularly under the ACICE.

Potential Areas of Synergy

Existing and plausible threat scenarios and their outcomes could be categorised into thematic areas relevant to ASEAN for research. These could serve as a framework to understand how various cyber and information threats overlap and how there should be synergy among ASEAN's various cyber and information security initiatives to address these threats. As a start, ASEAN could focus on two thematic areas based on key security developments in 2022.

First, ASEAN could refer to developments in the Russia-Ukraine war to assess the current assumptions that drive cyber and information operations. On the aggressor side, how may threat actors better integrate cyber and information operations with kinetic operations in the grey zone and in war to achieve greater strategic impact? They could adopt a more intelligence-driven approach to cyber and information operations, notably, engaging in cyber incursions to gather intelligence ahead of launching hostile kinetic operations. But, for plausible deniability, threat actors may conduct such incursions through cyber criminals, who are not bound by norms of responsible state behaviour.

On the defender side, how could ASEAN help to mitigate such malicious operations that destabilise the national cyberspace of ASEAN countries, with a knock-on impact on regional security? In this context, ASEAN would also need to plan for the contingency that private sector tech corporations, for some reason, may calculate that they have less commercial and political stakes in defending the region's digital infrastructures if war breaks out in the Indo-Pacific than they have in defending against threats arising from the Russia-Ukraine war.

To examine these issues, the ADMM-Plus Experts' Working Group (EWG) on Cybersecurity could take the lead in conducting workshops with the support of the ACICE. Given the interconnectedness of the civilian, business and military sectors in the cyber and information space, the workshops should involve representatives from non-military ASEAN mechanisms such as ADGMIN and SOM-ED. Their roles would be essential for plans to engage the private sector and inoculate civilian populations against the psychological impact of cyber and information threats.

Second, ASEAN could assess the tide of cyber threats affecting the maritime sector. This sector, a pillar of global supply chains, is undergoing rapid digitalisation, making it more exposed to cyberattacks. Such attacks could serve military and commercial espionage purposes. But they would be more damaging when interrupting navigation and other onboard systems, resulting in accidents and disrupting business operations. For example, the UK-based NATO Shipping Centre has issued a warning on risks to civilian shipping that may be caused by cyberattacks on vessels' navigation and communications systems.

Likewise, cyberattacks affecting vessels in busy sea lines of communication, such as the Straits of Malacca and Singapore (SOMS), could be disruptive and coercive. Hence, ASEAN cyber and information security initiatives should pay more attention to the maritime sector, primarily as most ASEAN countries depend on maritime connectivity. Given the maritime security angle, there could be synergy between these ASEAN initiatives and other regional/sub-regional efforts such as the ReCAAP Information Sharing Centre (ISC) and the quadrilateral Malacca Straits Patrol (MSP).

Specifically, the ADMM-Plus EWGs on Cybersecurity and Maritime Security could organise joint workshops to better understand the interactions between both security areas and anticipate challenges that may arise from cyberattacks on vessels along the SOMS. These workshops should involve representatives from ReCAAP ISC and MSP. Their roles would be essential for arrangements to share on-the-ground information and spot anomalies that may be indicative of cyber-related maritime incidents, as well as to engage the shipping industry and develop coordinated incident response plans.

Conclusion

The cyber and information threats that ASEAN could face in a landscape shaped by evolving threat actors and intense geopolitical contestation are wide-ranging. ASEAN should ride on existing efforts in this space. But to keep abreast of threats, it must adopt a foresightful approach and seek synergies between various ASEAN mechanisms and initiatives. Amid the rise of new minilaterals and engagements (e.g., the Quad) that are driven by the major powers and are increasingly focused on 5G technologies and cybersecurity, such foresightful thinking and synergistic action could add more structure and substance to the ASEAN-centric regional security architecture.

MUHAMMAD FAIZAL *bin Abdul Rahman is a Research Fellow with the Regional Security Architecture Programme at the Institute of Defence and Strategic Studies (IDSS), S. Rajaratnam School of International Studies (RSIS).*