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

RSIS COMMENTARY

www.rsis.edu.sg No. 101 – 24 July 2023

ASEAN MOVES TO STRENGTHEN DIGITAL DEFENCE COOPERATION

By Muhammad Faizal Bin Abdul Rahman

SYNOPSIS

The member states of the Association of Southeast Asian Nations (ASEAN) are taking substantive steps to strengthen regional security cooperation in the digital domain. A shared conception of the digital domain and strategic conversations among the multiple stakeholders are requisite to address digital security issues as well as promote communications and trust among them.

COMMENTARY

In the joint communique of the 56th ASEAN Foreign Ministers' (AMM) Meeting held in Jakarta from 11 to 12 July 2023, the grouping recognised the importance of the ASEAN Defence Ministers' Meeting (ADMM) as the primary platform for ASEAN defence establishments to promote stability and security in the region including in the area of cybersecurity. The ADMM had earlier approved the establishment of the ADMM Cybersecurity and Information Centre of Excellence (ACICE) at its 15th meeting in June 2021. The AMM joint communique also stated the importance of governments' role in addressing the proliferation and detrimental effects of misinformation and disinformation in the media.

Enhancing ASEAN Digital Defence through ACICE

Moving from statement to implementation, the ACICE officially opened on 18 July 2023 in Singapore. The establishment of the ACICE enhances existing ASEAN digital efforts in several ways.

First, ACICE not only complements the ASEAN Cyber Defence Network (ACDN) and ADMM-Plus Experts' Working Group (EWG) on cybersecurity. It could also promote information sharing and capacity building on broader issues that permeate the vast

and fluid digital domain. This is a crucial point as we are seeing such issues unfolding in real time in the war in Ukraine, where the digital domain is a battlespace featuring a growing nexus between cyber threats (i.e., hacking systems and data to spy or disrupt) and information threats (i.e., hacking the hearts and minds to influence actions).

Second, the digital domain is a multi-stakeholder landscape. This reality makes it necessary to create an institution dedicated to the defence sector and which complements civilian-oriented institutions such as the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) and the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC). Institutions are necessary to pool domain knowledge and forge partnerships with stakeholders and experts across sectors from within ASEAN and beyond the region.

Third, international peace and security is under threat with the return of great power competition, and the war in Ukraine being the first major interstate conflict where digital technologies are re-shaping multi-domain warfare. Never has it been more critical than now to support a rules-based international order for the digital domain.

Recognising the importance of rules in the digital domain, ASEAN became the first regional organisation to subscribe in principle to the United Nations' (UN) norms of responsible state behaviour in cyberspace, which include ensuring supply chain security, refraining from intentionally damaging critical infrastructure and respecting human rights online and offline. The ACICE could be a platform for ASEAN defence establishments to develop the understanding and capacity to implement these norms to support ASEAN's digital ambitions, as stated in the ASEAN Cybersecurity Cooperation Strategy (2021 – 2025).

Knowing the Complex Digital Terrain

To enhance regional digital defence efforts, ASEAN defence establishments should develop some level of shared conception of the digital domain to better appreciate the issues and threats before formulating solutions. In military speak, this step entails understanding the terrain and its complexities.

In chapter 10 of *The Art of War*, the ancient Chinese strategist Sun Tzu emphasised that understanding the terrain is crucial to success. Similarly, in his treatise *On War*, 19th-century Prussian general Carl Von Clausewitz described the importance of understanding the ground and how the adversary acts, feels, and thinks.

However, a fundamental obstacle in promoting multilateral security cooperation in the digital domain is countries having different views on what constitutes this domain with regard to state interests. Adding to the complexity is that the digital domain is a multi-stakeholder landscape. Hence, digital defence efforts should also consider civilian interests, as people and businesses are the primary users and operators of infrastructures and services there.

One way of conceptualising the digital domain is by dividing it into three different but intersecting sub-domains of defence.

i) First, hardware defence refers to protecting physical equipment, including routers, smart devices, data servers, wireless base stations, and submarine cable landing stations that transmit data.

ii) Second, software defence refers to addressing threats concerning codes and data, including smartphone apps, operating systems, data clouds, and algorithms. These two sub-domains relate to cyberspace, where cyber-attacks occur.

iii) Third, cognitive defence relates to the safety of online experiences and information exchange among people and organisations. This sub-domain is where connectivity and algorithmic-driven interactions expose people and organisations to misinformation, disinformation, and harmful activities against their digital identities. In turn, these threats could influence thinking and undermine national cohesion.

Enabling Strategic Conversations

With these three sub-domains in mind, strategic conversations should inform regional digital defence efforts. To enable these conversations, the ACICE and the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), co-organised the inaugural Digital Defence Symposium on 17 July 2023 in the lead-up to the official opening of the ACICE. The symposium brought together defence officials, academia, think tanks, and industry experts from ASEAN and beyond to network and exchange ideas on digital defence and how the civilian and defence sectors could cooperate better.

The symposium was a timely initiative for several reasons. First, the conversations helped to promote a better awareness of the digital domain and the threats that permeate this domain. Second, the conversations also fostered better communications and built trust among digital defenders and other non-defence digital stakeholders in ASEAN. It is hoped that these efforts could engender a more foresightful and holistic approach to digital defence as well as support defence diplomacy, which traditionally is the preserve of the land, sea, and air military forces.

Ultimately, the main strategic value of ASEAN digital defence cooperation lies in its potential to promote a peaceful and stable digital domain with respect to the fundamental principles enshrined in the Treaty of Amity and Cooperation in Southeast Asia and the purpose of ensuring a just and harmonious environment for the people of Southeast Asia as stated in the ASEAN Charter.

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), Nanyang Technological University, Singapore.