IDSS PAPER

30 June 2026

Securing ASEAN Cyberspace

A Case for Advanced Persistent Defence

Muhammad Faizal Bin Abdul Rahman

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

RSiS 30

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.074– 30 June 2026

Securing ASEAN Cyberspace: A Case for Advanced Persistent Defence

Muhammad Faizal Bin Abdul Rahman

KEY TAKEAWAYS

- *Cyber threats could undermine ASEAN's digital economic integration goals, which are crucial to regional peace and stability in the digital era.*
- *ASEAN needs to adopt an Advanced Persistent Defence (APD) mindset that bridges national and regional cybersecurity initiatives to keep pace with digitalisation and the evolving threat landscape.*
- *Better coordination between civilian and military cyber defenders – through regional initiatives, the implementation of cyber norms, and the optimisation of existing regional initiatives – is important to move this forward.*

COMMENTARY

ASEAN's cyberspace has become increasingly important for regional security, not only because of evolving transnational cyber threats but also because of the enhanced connectivity among ASEAN member states that the ASEAN Digital Economy Framework Agreement (DEFA) would foster. ASEAN officials concluded DEFA negotiations in May 2026, and the agreement is scheduled to be signed at the 49th ASEAN Summit in November 2026.

DEFA aims to strengthen economic development through integration, thereby serving as ASEAN's anchor for regional peace and stability in the digital era. DEFA also represents ASEAN's efforts to uphold multilateralism in a fragmented world, where geopolitical interests may view cyberspace more as a domain of conflict than of cooperation. However, cyber threats, which could become contagious as ASEAN

members become more digitally connected, would not only pose obstacles to DEFA's goals but also undermine trust in the digital economy and in regional cooperation.

Using Singapore as an example, this paper argues that the ASEAN region needs to adopt an Advanced Persistent Defence (APD) mindset that bridges national and regional cybersecurity initiatives to keep pace with digitalisation and the evolving landscape of cyber stakeholders and threats.

Advanced Persistent Defence

Essentially, APD, from an organisational perspective, entails (i) intelligence collection or information sharing to assess threats, (ii) actively monitoring digital systems to hunt for threats, and (iii) responding to threats by mitigating the impact of cyberattacks. It requires continuous vigilance and close coordination between all cyber stakeholders.

From a national perspective, this paper posits that APD requires nation-states to maintain a coherent cybersecurity approach that advances technical capabilities and talent through partnerships with educational institutions and industry stakeholders, and through coordinated information sharing and response that bridge civilian and military efforts.

From a regional perspective, coherent national approaches underpin the regional cybersecurity posture. As the adage goes, a chain is only as strong as its weakest link. Additionally, nation-states could optimise regional initiatives by drawing on their national experience and by endeavouring to enhance coordination between civilian and military initiatives at the regional level.

Underlying national and regional initiatives should be the 11 United Nations Norms on Responsible State Behaviour in Cyberspace. These norms should serve as a common strategic framework to guide any nation-state in leveraging technical capabilities, policies and international cooperation to counter cyber threats. Furthermore, these norms are an important instrument for confidence-building as they represent multilateralism and advocate a rules-based order. Norms promote trust and stability in cyberspace, especially as this domain is increasingly militarised, with nation-states building cyber capabilities to guard against threats and geopolitical uncertainties.

Singapore's National Initiatives

Singapore has demonstrated APD at the national level, especially in recent years. For example, in 2025, the government announced it would share classified threat intelligence with organisations across the critical information infrastructure sector as cyber threats have grown more sophisticated, particularly due to advances in artificial intelligence (AI).

This development coincided with Singapore's largest multi-agency cybersecurity operation, Operation Cyber Guardian, which sought to restrict the movement of the advanced persistent threat (APT) actor UNC3886, which had infiltrated Singapore's telecommunications sector. Given the severity of the threat, various agencies, including the Digital and Intelligence Service (DIS) of the Singapore Armed Forces

and the Centre for Strategic Infocomm Technologies (CSIT) at the Ministry of Defence, supported the operation.

These initiatives align with the seventh UN cyber norm, which calls for nation-states to take technical and organisational measures to "protect critical infrastructure".

In 2024, Singapore law enforcement agencies conducted an operation that resulted in the arrest of foreign nationals linked to a cybercrime syndicate targeting gambling websites, companies and governments worldwide. The syndicate used various hacking tools to penetrate systems and exfiltrate data, including personal information and confidential communications from foreign governments. One of the tools it used was PlugX, a malware frequently associated with state-sponsored APT groups. Over the past decade, various threat actors have used PlugX to target aerospace and military interests.

The initiative to disrupt the syndicate's operations aligns with the third UN cyber norm: the nation-state taking measures to investigate and "prevent misuse of ICTs in its territory".

Singapore's Regional Initiatives at ASEAN/ADMM

Singapore's experience well positions it to support existing ASEAN platforms that aim to strengthen national-level initiatives across ASEAN member states and improve coordination between them, thereby advocating APD at the regional level.

Moreover, supporting these platforms aligns with the first UN cyber norm: the nation-state's participation in international efforts involving operational staff and in international capacity building to support "interstate cooperation on security".

First, Singapore hosts the ASEAN Regional Computer Emergency Response Team (CERT) at the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE). The ASEAN Regional CERT, which began operations in October 2024, aims to facilitate information sharing, ensure continuous knowledge exchange and conduct regional cybersecurity exercises. These exercises could enhance the ASEAN region's collective ability to address cyber threats, including those targeting network edge devices – the hardware or software that act as the entry and exit points between an internal, private network and an external network, such as the internet. Such exercises are relevant as militaries today increasingly use edge computing for autonomous systems, logistics, and battlefield situational awareness.

The ASEAN Regional CERT could serve as a vital platform for responding to any transnational cyber crisis affecting the region. However, it is a strictly civilian entity established under the auspices of the ASEAN Digital Ministers' Meeting (ADGMIN).

Second, Singapore hosts the ASEAN Defence Ministers' Meeting (ADMM) Cybersecurity and Information Centre of Excellence (ACICE), which provides a platform for ASEAN defence officials to cooperate on capacity building and information sharing to address cyber and information threats relevant to the defence sector. An example of a capacity-building effort is ACICE partnering with the United Nations

Institute for Disarmament Research (UNIDIR) this April to conduct the inaugural workshop on cyber norms for ASEAN militaries.

Two key information-sharing mechanisms operated by the ACICE are the ACICE Chat (a Telegram channel) and the Malware Information Sharing Platform (MISP). These mechanisms enable ASEAN militaries to securely share unclassified threat information.

The MISP, when functioning in tandem with the ACICE advisory board, comprising ASEAN senior defence officials who may facilitate communication, could contribute to a coordinated response to transnational cyber threats. This is especially relevant given the growing risk that frontier AI models could create malware and accelerate cyberattacks today. However, these are strictly military mechanisms established under the auspices of the ADMM.

Promoting APD at the Regional Level

As DEFA looms large over the ASEAN region, the regional cybersecurity posture remains shaped by ASEAN member states' varying levels of development in their national cybersecurity approaches. The extent to which ASEAN member states can adopt an APD mindset depends on their national contexts, technology adoption and resource constraints. This situation makes it necessary for ASEAN as a whole to adopt an APD mindset so that regional initiatives can better narrow gaps in national cybersecurity approaches. As Singapore prepares to assume the ASEAN Chair in 2027, member states could work with Singapore to explore several steps to optimise regional initiatives. Three possible steps are outlined here.

First, as the ASEAN Regional CERT evolves in form and function, the ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC) could explore cross-sectoral cooperation between the ASEAN Regional CERT and the military Computer Security Incident Response Teams (Mil-CSIRTs) in ASEAN member states, while preserving sectoral mandates. This step could bridge civilian and military efforts by adapting lessons from the ASEAN Regional CERT's exercises to the military context, thereby supporting national cybersecurity approaches.

Second, while civilian and military cyber defenders often face shared threats, they may operate in parallel rather than in coordination due to a lack of trust and differences in the conceptual language used to define cyberspace. This is a challenge that could be ameliorated by adopting cyber norms as a common strategic framework. ASEAN militaries could use the ASEAN Checklist for the Implementation of the Norms of Responsible State Behaviour in Cyberspace to assess how to incorporate these norms into their national military policies, operations and diplomacy. This is an endeavour in which ASEAN militaries could collaborate more closely with the ACICE.

Third, ASEAN member states could explore how to better leverage existing regional initiatives hosted in Singapore. For example, ASEAN militaries could integrate the MISP and ACICE Chat and contact points into their responses to transnational cyber threats. Additionally, events that ACICE organises for ASEAN militaries and with its invited industry and academic partners could help keep them abreast of issues in the evolving cyber threat landscape.

Singapore, as ASEAN Chair in 2027, could work with member states to better leverage regional cybersecurity initiatives. *Image source: Unsplash.*

Looking at conflict in cyberspace, topical issues for militaries include (i) how cyber operations and psychological information operations amplify each other, (ii) opportunities and threats posed by evolving technologies for cybersecurity, and (iii) international humanitarian law obligations and the roles of civilians and tech companies in cyberspace during conflict. The upcoming 4th Digital Defence Symposium (DDS 2026) in July 2026 is one event that could explore these issues.

Together, these steps could enhance regional cooperation between ASEAN civilian and military cyber defenders while better aligning national and regional cybersecurity initiatives as the region implements DEFA.

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).*

Please share this publication with your friends. They can subscribe to RSIS publications by scanning the QR Code below.