ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON
THE
INFORMATION DOMAIN

Issue 02/26 (Jun) – Special Edition Op-Ed

Cooperation in the Digital Domain: Building Capacity and Situational Awareness in ASEAN

by Yeo Seow Peng, Executive Director, ACICE

INTRODUCTION

1. The digital revolution has transformed Southeast Asia over the past two decades and delivered unprecedented economic opportunities. The region's digital economy, projected to reach $1 trillion by 2030, demonstrates how advancement in technology and connectivity boosts its economies. With more than 560 million internet users and digital penetration rates averaging 78.2% across the region (excluding Laos, Myanmar and Timor-Leste), the 11-member Association of Southeast Asian Nations (ASEAN) is riding this wave. Indonesia, for example, has 212 million internet users, ranking fifth worldwide, and Singapore has 96% internet adoption.

2. Running in tandem with rapid digital expansion, however, is an increase in threats in the cyber and information domains. The cost of cybercrime was estimated at $9 trillion globally in 2024, with ASEAN members experiencing a huge increase in cyberattacks compared to counterparts worldwide. East and Southeast Asian countries have lost up to $37 billion to cyber-enabled fraud in recent years.

3. Traditional and social media, meanwhile, remain the region's primary sources of information, with social media platforms gaining prominence as hubs for communication, entertainment and commerce.

As elsewhere, a preference for information that conforms to existing beliefs at the personal and community levels leaves Southeast Asian societies vulnerable to misinformation and disinformation, especially around sensitive and emotive topics, including national security. With high rates of social media penetration in the region, misinformation and disinformation can be created and exchanged at unprecedented scale and speed, often outpacing verification or fact-checking efforts.

4. Compounding this challenge are significant disparities in digital literacy across age groups, geographical locations and socioeconomic strata. This creates fertile ground for exploitation by malicious actors seeking to manipulate public opinion or destabilize societies. The World Economic Forum's Global Risks Report 2025 identified misinformation and disinformation as the top global risk in the short term (defined as a two-year outlook) and ranked it fifth among long-term risks (a 10-year outlook). The report noted that technological advancement has dramatically amplified these threats. Fake accounts, divisive narratives and coordinated bot networks operate alongside sophisticated synthetic media, creating information pollution that can undermine institutional trust. The advent of generative artificial intelligence has further reduced the cost and complexity of creating disinformation, enabling even relatively unsophisticated actors to launch campaigns to manipulate public opinion and fracture societal cohesion.

Confronting Digital Threats

5. For the region's armed forces, developments in the digital space represent a fundamental shift in operational reality. The battlefield no longer is confined to, or defined by, physical terrain. Information warfare can complement or precede kinetic operations. Occurring in the grey zone, such slow-drip operations can appear innocuous at first and be difficult to detect.

6. Information campaigns also have emerged as strategic tools to create confusion during military operations. This has been evident in recent conflicts stretching from Europe to the Middle East and South

Asia, with such tactics deployed across online platforms to influence domestic and foreign opinion.

7. Protecting against digital threats requires a whole-of-government approach incorporating the military, homeland security and other public entities, as well as the private sector and industry. Multilateral and regional cooperation is crucial to effectively defend against evolving threats.

8. Defence establishments across Southeast Asia, however, are not yet fully structured to address information domain challenges. Some militaries view such issues primarily through a cybersecurity lens, focusing on the cyber domain as the main vector for misinformation and disinformation due to rampant online crimes and scams. Additionally, responsibility for tackling information threats typically falls under national communications or information ministries rather than defence establishments, creating coordination challenges when military operations intersect with information warfare. This highlights the complex nexus between information and cybersecurity, as well as the comprehensive approach required to address digital challenges.

Establishment of ACICE

9. Digital domain threats were amplified during the COVID-19 pandemic when many services were digitalised and moved online. Since then, the scale and sophistication of threats have grown considerably, threatening critical infrastructures and networks, as well as potentially fracturing social cohesion within and across states. As such, during the ASEAN Defence Ministers' Meeting (ADMM) in 2021, the Defence Ministers approved Singapore's proposal to establish the ADMM Cybersecurity and Information Centre of Excellence (ACICE). The decision reflected the defence sectoral's appreciation of the evolving landscape and the importance of leadership, initiative and foresight in addressing such threats.

10. ACICE embraces a dual approach. It promotes information sharing among militaries and other defence establishments regarding fake news, misinformation and disinformation, and cybersecurity

threats. The centre also builds regional capacity in dealing with cyber and information threats through exchanges and other cooperation, boosting trust and confidence.

11. The ACICE Malware Information Sharing Platform enables real-time dissemination of cyber threat intelligence, malware indicators of compromise, and common vulnerabilities and exposures among ASEAN militaries. The platform leverages ASEAN's collective knowledge to provide defence establishments with early warning, thereby facilitating timely mitigation of cyberattacks.

12. ACICE maintains a messaging app with daily and weekly updates on the cyber and information domains. The centre has produced more than 130 analytical reports covering developments and trends, providing tactical insights into evolving techniques used by malicious actors. The reports provide situational awareness of emerging threats and analysis of case studies. By promoting information sharing, ACICE supports ASEAN members in developing fit-for-purpose defences and mitigation measures.

Building Regional Capacity

13. ACICE focuses on practical cooperation by strengthening ASEAN's capabilities to address cyber and information threats through three main aspects:

a. **A panel of Experts** provides insights into trends and developments, bringing together academics, specialists and industry representatives to analyse challenges and share best practices.

Figure 1: Convening of 5th Experts Panel Meeting in July 2025

Source: MINDEF

b. **Seminars and dialogues** facilitate the exchange of perspectives and expertise. ACICE's flagship event, the annual Digital Defence Symposium, includes senior defence and military officials, academics, and industry experts. The platform is the first of its kind in the region. The 2025 iteration attracted more than 300 participants from 30 countries, including China, Germany, Japan, the United Kingdom and the United States.

Figure 2: Lt. Gen. Susan Coyle, the Australian Defence Force's joint capabilities chief, gives the keynote address at the 3rd Digital Defence Symposium in Singapore in July 2025

Source: MINDEF

c. **Training courses and simulated exercises** address how technology is transforming the information landscape. They prepare participants to recognize and assess disinformation threats and their potential impact on military operations, and to develop communication strategies for countering disinformation campaigns.

Figure 3: Participants in discussions at the ACICE-UNIDIR Cyber Norms workshop in April 2026

Source: ACICE

14. ACICE represents a milestone in ASEAN's approach to address the complex challenges of the digital age. As cyber and information threats evolve and transcend national boundaries, the centre serves as an inclusive platform for cooperation. While ACICE is anchored within ASEAN, its outlook extends beyond regional boundaries, leveraging a network of partners to further enhance the capacity of ASEAN militaries to deal with digital threats. The approach reflects the understanding that regional security in the digital domain requires internal cohesion and external partnerships. The region will only be stronger and more resilient if we can draw on the collective expertise and experience of our partners.

**This month's digest is adapted from Ms Yeo Seow Peng, Executive Director of ACICE's presentation to INFOPAC that was held in Honolulu in Oct 2025.*

CONTACT DETAILS

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE at ACICE@defence.gov.sg

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

….