RSIS COMMENTARY

15 April 2026

Staying Ahead of Cyber Threats for a Secure Regional Cyberspace

Muhammad Faizal Abdul Rahman and Audrey Chairunnisa

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

RSiS 30

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

RSIS COMMENTARY

www.rsis.edu.sg No. 080 – 15 April 2026

Staying Ahead of Cyber Threats for a Secure Regional Cyberspace

By Muhammad Faizal Abdul Rahman and Audrey Chairunnisa

SYNOPSIS

Singapore announced enhanced cybersecurity initiatives during the annual Committee of Supply debates in March 2026. By staying ahead of evolving cyber threats, Singapore could demonstrate its defensive cyber capabilities, maintain its position as Southeast Asia's cybersecurity thought leader and convenor, and continue to contribute to the regional cybersecurity architecture.

COMMENTARY

Singapore invests heavily in cybersecurity as cyberspace is crucial to its national interests. Lacking natural resources, the city-state has been utilising cyberspace as an essential virtual resource to promote economic growth, good governance, and efficient public services.

The cyber capabilities and international partnerships developed over the years have also put Singapore in an advantageous position to promote a secure regional cyberspace. Maintaining this position requires Singapore to keep pace with the evolving threat landscape, demonstrate credibility by decisively defending itself against cyber threats, upholding its commitment to responsible state behaviour in cyberspace, and integrating cybersecurity into ASEAN's digital economic frameworks.

Three key considerations underpin these necessary efforts. Firstly, cybercrime, especially online scams, remains a regional security concern, as it continues to operate on a large scale with increasing sophistication, victimising people across Southeast Asia and beyond. The presence of global scam centres in the region has also brought diplomatic pressure from major powers, namely, China and the US.

Secondly, the fractured international order and decline of multilateralism are also influenced by cyberspace, which has become increasingly insecure due to the return of the law-of-the-jungle and power play by belligerent states and their proxies. Digitalisation has been exploited in cyber operations between geopolitical rivals to advance their respective strategic interests.

Thirdly, Singapore will assume the chairmanship of the Association of Southeast Asian Nations (ASEAN) in 2027. This will give Singapore the opportunity to enhance regional digital resilience through collaborative cybersecurity initiatives under ASEAN's economic and political-security pillars.

Keeping Pace with Evolving Threats

The enhanced cybersecurity initiatives that Singapore announced during the annual Committee of Supply (COS) debates in March 2026 showed that the country is keeping pace with evolving cyber threats.

One of the announced initiatives was the mandatory Cyber Trust Mark certification for Critical Information Infrastructure (CII) owners, requiring them to attain the highest level (Level 5) by the end of 2027. CII auditors and licensed cybersecurity service providers will be subject to corresponding requirements. This initiative addresses a supply chain vulnerability exposed by the Singapore government's Operation Cyber Guardian. It was found that Advanced Persistent Threat (APT) groups are increasingly targeting systems adjacent to CII to exploit weaker links as entry points into critical networks.

Complementing this initiative is the Singapore government's plan to provide CII owners with proprietary threat-detection systems and to share classified threat intelligence selectively.

Another initiative is the plan to increase the mandatory cybersecurity requirements for residential routers from Level 1 to Level 2 under the Cybersecurity Labelling Scheme (CLS) by the end of 2027. This was in response to evidence that consumer network devices are being exploited as botnet nodes in global botnet operations. This is an important initiative following the discovery in 2025 that some 2,700 devices, including internet routers and baby monitors, were used in a malicious global botnet for cyber espionage and disruptive activities.

These initiatives are timely, as recent global developments have shown that CII and internet-linked devices could be targeted or exploited in cyber operations to support the strategic goals of hostile operations. The conflict between the US, Israel, and Iran, and the US military operation against Venezuela, are replete with examples: Hackers linked to Iran had reportedly compromised home security cameras in Israel for surveillance and missile targeting, while Israel had reportedly hacked traffic cameras in Iran to create a surveillance network that supports military strikes. In Venezuela, US forces had reportedly used cyber operations to cause internet disruption and power outages to support their military operation.

By ensuring that policies and capabilities keep pace with evolving cyber threats, Singapore is better positioned to defend its national interests and support regional countries.

Demonstrating Defensive Capabilities

Credibility in cybersecurity is earned through action, not only declaration. Four recent examples demonstrate Singapore's willingness to act decisively.

Firstly, in July 2025, Singapore publicly attributed malicious cyber activities targeting its CII to the APT group UNC3886, which cybersecurity firms in the West believe is linked to a state. Singapore's attribution language was notably measured: It used the threat designation by Google's cyber intelligence company Mandiant and did not explicitly name a state, signalling resolve while maintaining diplomatic flexibility. In February 2026, Singapore announced that it had carried out a multi-agency cybersecurity operation – Operation Cyber Guardian – spanning 11 months to counter the threat posed by UNC3886, which targeted all four major telecommunications companies: Singtel, StarHub, M1, and SIMBA Telecom. The operation demonstrated Singapore's resolve and capability to defend itself against cyber threats.

Secondly, in November 2025, Singapore convicted three Chinese nationals who were members of an organised criminal group and had entered Singapore using fraudulent documents to carry out a malicious cyber operation targeting foreign governments. They used sophisticated malware tools, such as PlugX, which APT groups believed to be state-sponsored have utilised. This case sent a clear message: Singapore will not tolerate the misuse of its territory for malicious cyber operations, demonstrating its commitment to the United Nations (UN) Norms of Responsible State Behaviour in Cyberspace, particularly the norm on "preventing misuse of information and communications technology (ICT) in your territory".

Thirdly, Singapore collaborates with international partners to counter online scams. For example, in September 2025, Singapore announced that it had conducted a joint law enforcement operation with Cambodia to disrupt scams operating out of Phnom Penh and targeting victims in Singapore. In January 2026, Singapore proposed an ASEAN-wide traceback mechanism and capacity-building efforts to enable authorities and telcos in the region to trace scam messages and calls across jurisdictions.

Together, the above constituted cyber anti-access/area denial (A2/AD) systems, demonstrating that Singapore has the means to detect, deter, and deny cyber threats from operating freely in its digital networks.

Additionally, they also show that Singapore adheres, in both principle and practice, to the 11 UN norms of responsible state behaviour in cyberspace, particularly the norms pertaining to the prevention and misuse of ICT, interstate cooperation on security, and cooperation to prevent crime and terrorism.

These actions also buttress Singapore's position as an advocate for the implementation of the UN cyber norms in the ASEAN region and the host of regional cybersecurity cooperation centres, which are the ASEAN Regional Computer Emergency Response Team (CERT), ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE), and the ASEAN Defence Ministers' Meeting (ADMM) Cybersecurity and Information Centre of Excellence (ACICE).

The focus on cyber norms and regional cooperation underscores Singapore's policy emphasis on good order and multilateralism in cyberspace, while avoiding taking sides in the digital rivalry between major powers and other conflicting parties.

Supporting Regional Cyberspace Security

When Singapore assumes the ASEAN chairmanship in 2027, it will be a strategic opportunity to leverage its expertise and credibility in cyberspace to advance the regional cybersecurity agenda. Can Singapore, through ASEAN, assist member countries in accelerating their defences against evolving cyber threats in an increasingly contested geopolitical cyberspace?

Why is this important? Essentially, ASEAN plans to sign its Digital Economy Framework Agreement (DEFA) in 2026. The implementation of DEFA would follow. Cybersecurity is a key priority in DEFA, as it is essential for building a resilient digital economy in ASEAN by protecting digital systems and networks, anticipating threats, and recovering from cyber incidents.

Furthermore, as Southeast Asian countries become more digitalised, cybersecurity is inherently linked to the ongoing stability and growth of the regional economy. Malicious cyber activities impacting Southeast Asia could hinder DEFA's objectives by causing economic damage, slowing digital adoption, and potentially damaging trust among regional countries, especially if the effects are "contagious".

Before 2027, regional countries could also begin discussions and collaborate with Singapore through regional cybersecurity platforms such as the ASEAN Regional CERT, ASCCE, and ACICE to develop ideas to shape the regional cybersecurity agenda for next year. This effort is necessary, as Southeast Asian countries seek to integrate their economies amid a more chaotic world, where cyberspace and the digital economy are part of the geopolitical battlespace.

Muhammad Faizal Bin Abdul Rahman is a Research Fellow with the Regional Security Architecture Programme at the Institute of Defence and Strategic Studies (IDSS), RSIS. Audrey Chairunnisa is a Student Research Assistant with the Military Studies Programmes and an MSc student in Strategic Studies at RSIS.

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