IDSS PAPER

17 November 2025

Southeast Asia's Cybersecurity Trajectory Beyond the UN OEWG

Bich Tran

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

Ponder the Improbable since 1996

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.108– 17 November 2025

Southeast Asia's Cybersecurity Trajectory Beyond the UN OEWG

Bich Tran

KEY TAKEAWAYS

- Southeast Asia has made considerable progress across the four pillars of the UN framework on responsible state behaviour in cyberspace: norms, international law, capacity building, and confidence-building measures.

- Key priorities moving forward include further operationalising the ASEAN Norms Implementation Checklist, articulating clearer positions on the application of international law in cyberspace, establishing systematic digital literacy programmes, and strengthening transparency and communication mechanisms.

COMMENTARY

In July 2025, the conclusion of the five-year mandate of the United Nations (UN) Open-Ended Working Group (OEWG) on the security of, and in, the use of information and communications technologies (ICT) marked a significant juncture for international cybersecurity governance. In the OEWG's final report, states agreed to establish the Global Mechanism (GM) – a permanent structure to continue multilateral dialogue on cybersecurity governance.

As states prepare for the inaugural meeting of the GM scheduled for March 2026, it is timely to evaluate where Southeast Asia stands across the four pillars of the UN framework on responsible state behaviour in cyberspace: norms, international law, capacity building, and confidence-building measures (CBM). While the region has achieved notable progress, considerable work remains ahead.

Progress and Implementation Gaps on Norms

Southeast Asia has made important strides in the first pillar of norms. Since 2018, the Association of Southeast Asian Nations (ASEAN) has endorsed the 11 norms of responsible state behaviour in cyberspace developed by the UN General Assembly in 2015. ASEAN has further signalled its willingness to align with global standards by publishing a Norms Implementation Checklist in February 2025.

Nevertheless, the implementation of the 11 norms remains challenging. For example, the proliferation of scam centres in several Southeast Asian countries persists despite the third norm, which calls for states to prevent misuse of ICTs within their territories. This has been attributed to corruption, where local authorities have allegedly overlooked scam centre operations in exchange for personal gain.

Towards Greater Clarity on Applying International Law

The application of international law to cyberspace is the second pillar of the UN framework. While all UN member states have agreed that existing international law, particularly the UN Charter, applies to cyber activities, the articulation of detailed national positions remains limited. According to one estimate, only 37 UN member states, including two ASEAN member states – Singapore and Thailand – have publicly issued such positions as of November 2025. The lack of national positions by other ASEAN members represents a missed opportunity for legal clarity and regional leadership.

Capacity Building: Institutional Progress and Educational Imperatives

The third pillar of the UN framework focuses on building national capacities to address cyber threats through technical, legal, and policy measures. ASEAN has benefitted from several cooperation initiatives in this area with its dialogue partners and between member states.

The ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC), created in 2017, exemplifies cooperation between ASEAN and its dialogue partners. The centre was initially funded by the Japan–ASEAN Integration Fund between 2018 and 2023 and implemented by Thailand's Electronic Transactions Development Agency. It has been managed by Thailand's National Cyber Security Agency, in partnership with the Japan International Cooperation Agency since 2023.

Complementing this initiative, the ASEAN–Singapore Cybersecurity Centre of Excellence (ASCCE), established in 2018, represents intra-organisational cooperation between member states. Whilst AJCCBC emphasises technical skills development, ASCCE addresses higher-level policy concerns such as international law, cyber strategy, legislation, and norms implementation. Together, these initiatives form a capacity-building architecture that spans the technical and policy dimensions.

However, a critical gap persists in these initiatives, as their primary focus remains on government officials. Sustainable cybersecurity also requires a digitally-literate population. While various public awareness campaigns exist in some ASEAN member states, the region lacks a comprehensive digital literacy framework equivalent to the

AJCCBC or ASCCE. At the national level, initiatives tend to be sporadic and lack systematic implementation.

Confidence-Building Measures: Enhancing Transparency and Communication

Thirdly, the ASEAN Regional Computer Emergency Response Team, launched in 2024, was an example of CBMs which aim to foster trust and predictability among states through transparency and communication. One of its key roles is to build and sustain an ASEAN Point of Contact (POC) network comprising experts and organisations in cybersecurity.

However, this differs from government-to-government POCs, like the intergovernmental Points of Contact Directory launched in May 2024 by the OEWG, which are essential for crisis communication and conflict prevention. As the global directory is not publicly available, it remains unclear whether ASEAN member states have designated their representatives.

Another step towards transparency is the publication of national cybersecurity strategies or policies, which most Southeast Asian nations have done in recent years. This includes Singapore in 2016 (updated in 2021), Thailand and the Philippines in 2017 (with the latter issuing an update in 2023), Malaysia in 2020, Vietnam in 2022, as well as Indonesia and Myanmar 2023. The next priority is for the remaining member states to publish their national cybersecurity strategies as standalone documents, while those with existing strategies should ensure regular updates to remain relevant.

Conclusion: From Commitment to Implementation

Southeast Asia's engagement with the UN framework for responsible state behaviour in cyberspace reveals a region in transition – from norm adoption to implementation. However, significant gaps remain. Moving forward demands sustained political commitment, institutional development, and regional cooperation.

As Southeast Asia transitions from adopting UN cyber norms to implementing them, progress will hinge on sustained political commitment, institutional development, and international cooperation.
Image source: Pixabay

On the norms pillar, ASEAN member states should further operationalise the Norms Implementation Checklist. For example, to address the challenge posed by scam centres – which violate the norm prohibiting the misuse of ICTs within their territories – states should use tools such as the UN Convention against Cybercrime to freeze assets, a key step in dismantling these criminal enterprises. The Convention provides

a legal foundation for such efforts, particularly through Article 41, which establishes a 24/7 assistance network for cybercrime cases.

Regarding international law, ASEAN states should clarify their positions through two potential pathways. Individual member states could issue national positions, contributing to a diverse regional perspective on international law's application to cyberspace. Alternatively, ASEAN could adopt a common position, following the precedent set by the African Union and the European Union. Either approach would enhance legal clarity and contribute to the development of customary international law in this domain.

In terms of capacity building, integrating digital literacy into mandatory school curricula – while accounting for pedagogical and sociocultural considerations – is a logical and necessary next step. Curriculum development will inevitably involve choices about priorities and values. There is no right answer when it comes to who should develop these curricula and learning materials. Notwithstanding these considerations, a structured, nationwide approach to digital literacy education is preferable to current ad hoc efforts.

As for confidence-building measures, the ASEAN POC network of experts and organisations could support governmental participation in the global POC directory. Additionally, all ASEAN member states should appoint a unit or multiple individuals as national POCs to ensure coverage and continuity.

As the international community continues the work of the OEWG through the GM, Southeast Asia must ensure its diplomatic engagement translates into operational reality. Only through comprehensive implementation of the UN framework can the region effectively address the complex challenges of cybersecurity governance.

Bich Tran *(pronounced "Bik Trahn") is a Research Fellow with the Military Transformations Programme at the 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.