ASIA-PACIFIC LEADERSHIP NETWORK

AFTER THE CHECKLIST: SOUTHEAST ASIA'S NEXT STEP ON CYBER NORMS IS ACCOUNTABILITY

Gatra Priyandita, Senior analyst at the Australian Strategic Policy Institute

3 August 2026

Southeast Asian states – through the Association of Southeast Asian Nations (ASEAN) – have done the necessary groundwork on cyber norms, and the grouping's 2024 implementation checklist proves it can turn political commitments into practical tools. But norms mean little without accountability, and the region has yet to develop the capacity and the shared, regional process needed to determine responsibility when those norms are breached (even as they may be voluntary). The logical next step is a collective attribution capability – approached as a technical function before a political one, and sequenced deliberately through pooled forensic capacity, an initial focus on criminal and proxy actors, and a coalition of willing members. Only then will ASEAN's norms of responsible behaviour begin to carry consequences rather than remaining merely declaratory.

ASEAN's progress on cyber norms has outpaced what many expected of a grouping built on consensus and non-interference. In 2018, it became the first regional organisation to subscribe, in principle, to the eleven voluntary and non-binding norms of responsible state behaviour set out by the UN General Assembly. Since then ASEAN has steadily translated a political gesture into practical machinery. The norms implementation checklist finalised in late 2024 is the clearest expression of that trajectory: a working tool that converts abstract commitments into concrete steps against which member states can measure their progress. It is a genuine achievement, and a useful one. But it also marks the end of the easy phase.

The checklist's value lies in making the norms practically legible to officials from a range of policy, operational, and legal backgrounds. It also gives officials a shared reference point and lowers the barriers to participation, which matters in a region where cyber maturity varies enormously. Yet a checklist is a diagnostic instrument, not a guarantor of behaviour. Its adoption tells us that member states know what responsible conduct looks like; it says far less about whether that knowledge has travelled beyond national cyber agencies to the defence ministries, telecommunications regulators and critical-infrastructure operators where the norms actually bite.

Capacity across the eleven members remains starkly uneven, ranging from states with mature national cyber institutions to those only beginning to stand one up. Sustained

political commitment presents an even greater challenge, and there is a real risk that the checklist will calcify into an annual box-ticking ritual, its language recited without its substance being resourced. Guarding against that requires treating implementation as a continuous process rather than a milestone already passed.

Even when implemented effectively, however, norms address only half of what a credible governance framework needs. Norms describe how states ought to behave; on their own, they say nothing about what happens when states fail to comply. The region has agreed on a standard of responsible conduct, and while national frameworks are emerging and the ASEAN Regional CERT provides a channel for information-sharing, it still lacks a shared process for collectively determining when that standard has been breached, let alone how to respond. Norms without a credible prospect of accountability are cheap, and adversaries know it.

The next step, accordingly, should be for Southeast Asian states to begin building towards a collective attribution capability. Attribution – the ability to establish, credibly, who is responsible for a malicious cyber operation – is the hinge on which accountability turns. Without it, the norms remain largely declaratory; with it, they acquire the beginnings of teeth. This is, admittedly, the most demanding thing one could ask of Southeast Asian states. Collective, publicly attributing a cyber operation to a state runs against the grain of the ASEAN Way – consensus, non-interference and a deep reluctance to name and shame – and members' relationships with the actor most often implicated in regional intrusions diverge too widely for consensus condemnation to be realistic any time soon. Furthermore, while a growing number of countries have opted to attribute at a political level, Southeast Asian states have been relatively shy in doing so publicly. However, things are changing as some states, like Singapore, are increasingly willing to attribute, albeit without explicit naming or shaming of state actors.

However, the answer is not to abandon the goal but to sequence it, approaching attribution first as a technical capacity before it becomes a political act. The first and least controversial layer is capability: pooled threat intelligence, shared forensic expertise and a common standard of evidence. These investments are worthwhile regardless of whether a single joint attribution is ever issued, because they raise the analytical floor across the region and build the muscle on which any future accountability mechanism would depend.

The second layer is practice. Coordinated attributions can begin privately and technically, and can focus initially on criminal and proxy actors – where the political stakes are lower – long before they approach the sensitive terrain of state responsibility. Nor do all eleven members need to participate at once; a bilateral arrangement or a coalition of willing states can establish precedent and confidence that others may later join.

Attribution is only the first of a set of countermeasures worth developing. Attribution and accountability are not the same thing: attribution establishes who is responsible, whereas accountability concerns what follows from that finding – what response is warranted, who

delivers it and on what threshold. Coordinated diplomatic démarches, joint statements, aligned indictments and the capacity to impose reputational and material costs all extend the same logic. Crucially, accountability need not fall to ASEAN as a whole. The affected state might respond bilaterally, or a coalition of willing members might act together, with the choice calibrated to the severity of the incident and the appetite of those involved. What matters is that a finding of responsibility becomes not an analytical endpoint but the trigger for a graduated and previously agreed set of responses.

Concretely, this points to a handful of steps. Southeast Asian states should write the eleven norms and the checklist explicitly into their national cyber strategies and mandate cross-agency familiarity with both. The region should resource its capacity-building institutions to develop genuine attribution and incident-analysis expertise, rather than leaving that competence concentrated in one or two members.

Southeast Asian states should also work towards a shared, voluntary evidentiary standard for attribution, beginning at the technical level where agreement is most attainable. And willing members should pilot coordinated responses to lower-stakes incidents, building the precedent and mutual confidence on which anything more ambitious would rest. Each of these steps also reinforces the region's standing in the global process: a region that can attribute and respond coherently carries considerably more weight in the UN Global Mechanism on ICT Security than one that can only subscribe.

The checklist has demonstrated that ASEAN can build practical tools on the foundation of a norms agreement. The real test of those norms, though, is not whether they are documented but whether breaching them carries consequences. Building a collective attribution capacity– patiently, technically and incrementally – is how Southeast Asian states move from defining responsible behaviour to credibly determining when one has not. That is the harder and more consequential next chapter.

*Dr. **Gatra Priyandita** is a Senior Analyst at ASPI's Cyber, Technology and Security Program. His primary research area is in cyber diplomacy and the geopolitics of critical technology. He also provides commentary on foreign and defence policy issues in Southeast Asia.*

The opinions articulated above represent the views of the author and do not necessarily reflect the position of the Asia-Pacific Leadership Network or any of its members.

This commentary is also published on the APLN website.

ABOUT APLN

The **Asia-Pacific Leadership Network (APLN)** is a Seoul-based organisation and network of political, military, diplomatic leaders, and experts from across the Asia-Pacific region, working to address global security challenges, with a particular focus on reducing and eliminating nuclear weapons risks. The mission of APLN is to inform and stimulate debate, influence action, and propose policy recommendations designed to address regional security threats, with an emphasis on nuclear and other weapons of mass destruction threats, and to do everything possible to achieve a world in which nuclear weapons and other WMDs are contained, diminished, and eventually eliminated.