Sydney Recommendations

on Practical Futures for Cyber Confidence Building in the ASEAN region

September 2018

This activity is supported by

Australian Government

AAC
AUSTRALIA-ASEAN COUNCIL
BRINGING TOGETHER THE PEOPLES OF AUSTRALIA & SOUTH-EAST ASIA

Contents

Background to the Sydney Recommendations

In the lead-up to the ASEAN–Australia Special Summit, ASPI's International Cyber Policy Centre launched an initiative with partners across the region to develop the Sydney Recommendations on Practical Futures for Cyber Confidence Building in the ASEAN region. It built on the extensive work undertaken by the think-tank community in the region starting in the early 2010s.

The project received grant funding from the Australia–ASEAN Council of the Australian Department of Foreign Affairs and Trade and the Department of the Prime Minister and Cabinet. The initiative brought together a region-wide group of experts from think tanks and research institutes to discuss practical recommendations to enhance confidence in cyberspace in the ASEAN region.

Between December 2017 and March 2018, the group held a series of online consultations and an in-person roundtable meeting in Sydney on 15 March 2018, as part of ASEAN–Australia Week.

Contributing partners

The partner institutions that contributed to the project were:

- International Cyber Policy Centre, Australian Strategic Policy Institute, Australia
- Sultan Haji Hassanal Bolkiah Institute of Defence and Strategic Studies, Brunei Darussalam
- Institute for Cooperation and Peace, Cambodia
- Centre for Strategic and International Studies, Indonesia
- Institute for Strategic and International Studies, Malaysia
- Cyber Security Lab, University of Computer Sciences, Myanmar
- Stratbase ADR Institute for Strategic and International Studies, Philippines
- Centre of Excellence for National Security, S. Rajaratnam School of International Studies, Singapore
- ICT Faculty, Mahidol University, Thailand
- Diplomatic Academy, Vietnam

This initiative was a collaborative effort. The outcome statement has been collated by ASPI's International Cyber Policy Centre (ICPC) and ICPC takes responsibility for its content.

Practical recommendations to operationalise confidence–building in cyberspace in the ASEAN region

For the Track 2 community in the ASEAN region

- To keep a calendar of planned and ongoing unclassified cyber activities, such as conferences, exercises and workshops and report on their outcomes.
- To conduct comprehensive mappings of laws, regulations, policies, doctrine and incident reporting from the ASEAN region.
- To collate good cybersecurity practices of relevance to the ASEAN region; for example, in coordination with the Global Forum on Cyber Expertise.
- To provide a list of publicly available significant cyber incidents occurring in the ASEAN region.
- To establish a regular forum that is informal, confidential and closed-door in character, where thought-leaders from government, industry, academia, civil society and the tech community consult on cybersecurity issues of strategic interest.

For ASEAN member states

- To equip the ASEAN secretariat with dedicated resources to support the various cyber affairs tracks[1] throughout successive chairmanships.
- To professionalise cyber capacity-building efforts; for example, by establishing a public–private international advisory team that could increase regional capacity to support national processes, enhance the effectiveness and quality of programming, and facilitate coordination and coherence of assistance.

1 ASEAN Telecommunications and Information Technology Ministers' Meeting, ASEAN Foreign Ministers' Meeting, ASEAN Defence Ministers' Meeting, ASEAN Ministerial Conference on Cybersecurity, ASEAN Regional Forum, ASEAN Ministerial Meeting on Transnational Crime.

- To establish a parliamentary track on cyber affairs to enable parliamentarians to strengthen their knowledge, skills and competence in performing legislative and democratic oversight duties.
- To encourage and resource national think-tank capabilities in strategic and regional cybersecurity issues.

For CERTs, cyber security agencies and cyber security centres in the ASEAN region

- To continue, and where possible expand, ASEAN CERT Incident Drills across Southeast Asia.
- To include a policy component in future drills and exercises addressing cross-governmental coordination and policy challenges.
- To explore establishing a scheme for reciprocal observers at national cybersecurity exercises and drills.

For Southeast Asia–based industry partners

- To include cybersecurity in corporate governance reports and initiate a practice of cybersecurity reporting, drawing on existing models of corporate social responsibility reporting such as the GRI Standards (www.globalreporting.org), to facilitate greater regional and sectoral transparency on common vulnerabilities and effective responses.
- To consider inviting observers from the business sector to company and sectoral cybersecurity drills.
- To initiate industry-led sectoral information-sharing and analysis hubs, where needed, in partnership with government regulators, following the example of the FS-ISAC Asia Pacific Regional Analysis Centre (www.fsisac.com).

For the technical community in the ASEAN region

- To support the development of publicly available tools and instruments that enhance trust and confidence in the internet for users and consumers in the region.

For all stakeholders

- To give greater attention to bridging stakeholder cultures.
- To initiate events that increase understanding among ASEAN member states; within individual ASEAN member states among their public, industry and tech sectors; and overall between security agencies and civilian stakeholders.

Explanatory remarks

In April 2018, ASEAN leaders issued their latest statement on cybersecurity. Heads of state and government declared that they 'recognize the need for all ASEAN member states to implement practical confidence-building measures and adopt a set of common, voluntary and non-binding norms of responsible State behavior in cyberspace'.

Practical cyber confidence-building measures (CBMs) include actions that the main stakeholders in cyberspace can take during all stages of a (latent) conflict with the aim of reducing and eliminating causes of mistrust, fear, misunderstanding, and miscalculation that may stem from the use of information and communication technologies.

Examples of CBMs include providing personal contacts, establishing communication channels, sharing information and setting up cooperation formats. Overall, CBMs are helpful in:

- achieving predictability
- seeking clarification
- gaining time
- creating understanding
- enhancing maturity.

While CBMs can be considered universal, perceptions of mistrust and misunderstanding are grounded in the historical experience of a nation or region and other geographical, strategic, political, economic, cultural and social factors.

There is a case to be made for ASEAN stakeholders to operationalise global norms and confidence-building to fit local contexts.

The recommendations presented here are not meant to be exhaustive. Based on our extensive consultations, they reflect what the Track 2 group believes should be prioritised by the ASEAN cybersecurity community.

Next steps

ASPI and its partners will continue to advocate for these recommendations through policy reports, public debate, capacity-building activities and media outreach. Priority will be given to recommendations that Track 2 partners can initiate.


Practical Futures for
Cyber Confidence Building
in the ASEAN region