ADMM Cybersecurity and Information Centre of Excellence

# UPDATE ON THE CYBER DOMAIN

Issue 03/25 (March)

## Cyber Norms – Forging Towards Implementation

### INTRODUCTION

1. ASEAN's use of the cyberspace has seen rapid growth, with an estimated 564 million Internet users in 2024. Given the expected growth of its digital economy to USD 1 trillion by 2030, ASEAN released an ASEAN Digital Masterplan 2025 (ADM 2025) in Jan 2021 to take stock of the fast developments in cyberspace. This effort also builds on past plans for digitalisation efforts to offer a more comprehensive framework to drive adoption of digital services and support infrastructure in the region. However, ASEAN's rapid digitalisation has left it vulnerable to cybercrime, with cybercrime surging by 82% in the region in 2023. Yet, the region's cyber resilience remains relatively low.

2. Against this backdrop of rising cybercrime, ASEAN has subscribed to and implemented the 11 United Nations (UN) Norms of Responsible State Behaviour in Cyberspace (or 11 cyber norms) to ensure a stable and predictable cyberspace. These 11 cyber norms were first agreed by a UN Group of Government Experts (UN GGE) back in 2015, and the UN GGE's report was subsequently adopted by consensus at the UN General Assembly in 2015 through resolution 70/237. Through voluntary compliance and implementation of these cyber norms, ASEAN can build a safe and secure cyberspace that is an enabler of economic progress and betterment of living standards.

### THE 11 CYBER NORMS

3. Figure 1 shows the Australian Strategic Policy Institute's (ASPI's) summary of the 11 norms of responsible state behaviour in cyberspace. ASPI has grouped the 11 norms into two categories. The first category of norms, which are

those in green, are positive commitments by States that encourage responsible state behaviour in cyberspace. This includes norms such as promoting interstate cooperation on security, protecting critical information infrastructure (CII) and responding to requests for assistance. The second category of norms, which are those in red, constrain States from engaging in irresponsible behaviour in cyberspace. These are preventing misuse of information and communications technologies (ICTs) in a State's territory, a commitment not to damage CII, and a commitment not to harm emergency response teams.

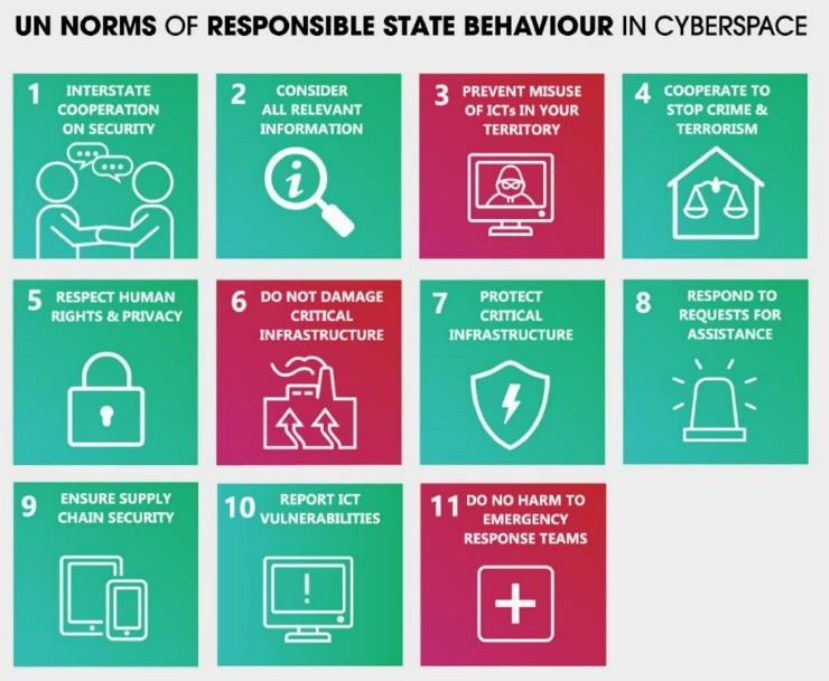


*Figure 1: The 11 UN cyber norms (Source: ASPI)*

## ASEAN'S EFFORTS IN CYBER NORMS

4. Globally, ASEAN stands out as being the first regional bloc to affirm the 11 cyber norms and commit to its implementation. This underscores ASEAN's commitment towards upholding a rules-based world order that extends to cyberspace. ASEAN's efforts to implement the norms can be seen as follows:

a. In 2018, the 3rd ASEAN Ministerial Conference on Cybersecurity (AMCC) adopted a Chairman's Statement where ASEAN Member States "reaffirmed the importance of a rules-based cyberspace as an enabler of economic progress and betterment of living standards, and agreed in-principle that international law, voluntary and non-binding norms of State behaviour, and confidence building measures are essential for stability and predictability in cyberspace". The AMCC agreed to subscribe to the 11

cyber norms in-principle, and focus on regional capacity building in implementing these norms.

b. In 2021, Singapore and Malaysia jointly put forth a matrix Regional Action Plan (RAP) that sought to implement the cyber norms. The RAP seeks to advance cyber readiness, strengthen and harmonise regional cyber policies and enhance trust in cyberspace. As part of the RAP, the ASEAN Cybersecurity Coordinating Committee (Cyber-CC) was established to enhance cross-sectoral cooperation in the development of regional cybersecurity strategies, including in the area of cyber norms.

c. In 2024, Singapore's Minister for Digital Development and Information, Ms Josephine Teo, launched the Norms Implementation Checklist (NIC) during the Singapore International Cyber Week. The checklist was jointly developed by the Cyber Security Agency (CSA) of Singapore and the UN Office for Disarmament Affairs, in consultation with other ASEAN Member States. The NIC provides ASEAN Member States with practical steps that they can adopt in order to implement the 11 cyber norms.


*Figure 2: Minister Josephine Teo delivering her opening remarks at the 2024 Singapore International Cyber Week*

## IMPLEMENTATION OF THE CYBER NORMS

5. Even as the cyber norms have been discussed at the Open-Ended Working Group 2.0 for ICT/Cyber at the UN, many ASEAN Member States have stepped up efforts in support of the implementation of the cyber norms.

6. The Philippines boasts a high Internet penetration rate amongst its minors, with 95% of 12–17-year-olds being Internet users. To safeguard their minors

against online abuse, the Philippines government passed the Philippines' Republic Act No. 11930, also known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) Act, in July 2022. This law defines online sexual abuse and exploitation, establishes measures to prevent, detect and punish online sexual abuse and exploitation, and requires Internet service providers and digital platforms to monitor and report incidents.

7. Malaysia has taken steps to protect its CIIs through the passing of the Cyber Security Act in 2024. The Act also established the National Critical Information Infrastructure (NCII) and set out the duties of NCII entities. The law defines the duties and powers of NCII sectoral leads and mandates specific cybersecurity protocols for NCII entities. To further enhance CII protection, the law also includes provisions for mandatory risk assessments and incident reporting for NCII entities.

8. In 2018, Thailand and Japan jointly set up the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) in Thailand. The AJCCBC provides cybersecurity training to ASEAN Member States so as to improve the skills of their security-related agencies. In 2019, Singapore's CSA opened the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE). ASCCE was launched to conduct research and provide training in areas including international law and cyber norms, provide computer emergency response teams (CERT) technical training, and conduct virtual cyber defence training and exercises for ASEAN Member States. Together, AJCCBC and ASCCE facilitate interstate cooperation amongst ASEAN Member States by building the capacities of ASEAN's cybersecurity agencies.

9. Several ASEAN Member States have set up measures to counter cyber scams, which has become a serious problem throughout ASEAN since the onset of Covid-19. The United Nations Office on Drugs and Crime (UNODC) estimates that US$7.5 billion to US$12.5 billion were lost to such scam industries just in the Mekong region alone in 2024. In recognition of the severity of these threats, Singapore has set up a 24/7 scam hotline, Malaysia a National Scam Response Centre and Vietnam an anti-scam mobile application. Thailand and Cambodia are cooperating bilaterally to stop transnational cybercrime. In 2024, both countries conducted bilateral exercises and operations, which saw law enforcement agencies in both countries share intelligence to improve the success of raids.

## ROLE OF THE DEFENCE ESTABLISHMENTS

10. Discussions on the importance of responsible state behaviour in cyberspace in the ASEAN defence sectoral are nascent, as most discussions have taken place under the AMCC in support of ASEAN's growth of the digital economy. This

notwithstanding, the ASEAN defence sectoral has a role to play in support of the whole-of-government approach to implement the cyber norms. In this regard, the ASEAN defence sectoral is also poised to contribute to the discussions on cyber norms as there are existing initiatives that seek to enhance cybersecurity. The next step for ASEAN Member States is to explore how defence outfits within the ASEAN Cyber-CC can contribute to discussions on implementation of the cyber norms. This can serve as a launchpad for the wider ASEAN defence sectoral to implement the cyber norms in their respective States. The defence outfits within the ASEAN Cyber-CC are:

a. ADMM-Plus Experts' Working Group on Cyber Security (EWG-CS). The EWG-CS was set up in 2017 to promote practical and effective cooperation amongst the ASEAN Member States and Plus Countries to enhance capacity in protecting the region's cyberspace and addressing challenges to cybersecurity. The hosting of biannual meetings enhances the EWG-CS's commitment towards building up cyber resilience in the regional security architecture.

b. ADMM Cybersecurity and Information Centre of Excellence (ACICE). ACICE is Singapore's initiative to the ADMM in 2021. It was established to deepen regional cooperation amongst ASEAN defence establishments against cyberattacks, disinformation and misinformation for the region's collective peace and security. ACICE seeks to promote information sharing and capacity building amongst ASEAN Member States, fostering interstate cooperation in cybersecurity in the region.

c. ASEAN Cyber Defence Network (ACDN). The ACDN was set up by Malaysia in 2021 to link the cyber defence centres across the various ASEAN Member States. It aims to conduct joint exercises and establish operational partnerships, therefore promoting interstate cooperation in cybersecurity issues.

## CONCLUSION

11. We can expect substantial challenges that will hinder progress in implementing the cyber norms. Notably, the 11 cyber norms are political commitments and are voluntary in nature. Furthermore, the increasingly fractious geopolitical landscape can be a distraction that hinders cooperation amongst States from implementing the cyber norms.

12. Nonetheless, ASEAN Member States have made significant progress in putting forth initiatives that have gone towards implementing the cyber norms, serving as a model and thought leader for other States and regional blocs.

However, discussions on cyber norms within the ASEAN defence sectoral remain limited. ASEAN can bring the defence sectoral into these conversations, beginning with the defence outfits in the ASEAN Cyber-CC, so as to explore how defence agencies can meaningfully contribute to ASEAN Member States' whole-of-government efforts to implement the cyber norms.

# 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**

• • • • •

# REFERENCES

1. Now that ASEAN has its cyber norms checklist, the hard work begins – ASPI
https://www.aspistrategist.org.au/now-that-asean-has-its-cyber-norms-checklist-the-hard-work-begins/

2. The Rocky Road to Cyber Norms at the United Nations – Council on Foreign Relations
https://www.cfr.org/blog/rocky-road-cyber-norms-united-nations-0

3. The UN norms of responsible state behaviour in cyberspace – ASPI
https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace

4. The UN norms of responsible state behaviour in cyberspace: Guidance on implementation for Member States of ASEAN – ASPI
https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2022-03/The%20UN%20norms%20of%20responsible%20state%20behaviour%20in%20cyberspace.pdf?VersionId=pwQNsEIHhDSAx_7gJ4XXSGSupVOpvMJi

5. ASEAN-Singapore Cybersecurity Centre of Excellence – CSA
https://www.csa.gov.sg/news-events/press-releases/asean-singapore-cybersecurity-centre-of-excellence

6. How ASEAN is driving global cyber security efforts – Channel Asia
https://www.channelasia.tech/article/1293967/how-asean-is-driving-global-cyber-security-efforts.html

7. ASEAN Cybersecurity Cooperation Strategy – ASEAN
https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

8. Opening Remarks by Minister Josephine Teo at the SICW AMCC – MDDI
https://www.mddi.gov.sg/media-centre/speeches/opening-remarks-by-minister-josephine-teo-at-the-sicw-amcc/

9. Protecting children in the Philippines from online sexual exploitation and abuse: The way forward – Disrupting Harm
https://safeonline.global/wp-content/uploads/2023/12/DH_Philippines_advocacy_note_layout-1.pdf\

10. Internet and Right to Privacy – Situation of Children Philippines
https://situationofchildren.org/internet-and-right-privacy#:~:text=Additionally%2C%20in%20July%202022%2C%20Republic,in%20the%20Republic%20Act%20No

11. Cyber Security Act 2024 (ACT 854) – NACSA
https://www.nacsa.gov.my/act854.php

12. Digital Masterplan: Getting the next five years right for ASEAN – The Business Times
https://lkyspp.nus.edu.sg/docs/default-source/aci/digital-masterplan-getting-the-next-five-years-right-for-asean.pdf?Status=Temp&sfvrsn=a4632b0a_2

13. Strengthening Cyber Resilience in Southeast Asia – Fulcrum: Analysis on Southeast Asia
https://fulcrum.sg/strengthening-cyber-resilience-in-southeast-asia/

14. ASEAN Member States Agree to Strengthen Cyber Coordination and Capacity-Building Efforts – CSA Singapore
https://www.csa.gov.sg/news-events/press-releases/amcc-2018

15. Singapore and ASEAN Member States Deepen Commitment to Enhance Collective Cybersecurity in the Region – CSA Singapore
https://www.csa.gov.sg/news-events/press-releases/singapore-and-asean-member-states-deepen-commitment-to-enhance-collective-cybersecurity-in-the-region

16. ASEAN-Japan Cybersecurity Capacity Building Centre to be launched in Thailand in June 2018 – Open Gov
https://opengovasia.com/2018/03/31/asean-japan-cybersecurity-capacity-building-centre-to-be-launched-in-thailand-in-june-2018/

17. Fraud with Danger: The Rise of Cyber Scams in Southeast Asia – Fulcrum: Analysis on Southeast Asia
https://fulcrum.sg/aseanfocus/fraud-with-danger-the-rise-of-cyber-scams-in-southeast-asia/#:~:text=ASEAN%20member%20states%20have%20implemented,as%20examples%20of%20targeted%20interventions.

18. Digital Payments - ASEAN - Statista
https://www.statista.com/outlook/fmo/digital-payments/asean

19. Number of internet users in Southeast Asia from 2014 to 2029 - Statista
https://www.statista.com/forecasts/1144567/internet-users-in-southeast-asia