



OPENING REMARKS BY
H.E. DR KAO KIM HOURN, SECRETARY-GENERAL OF ASEAN
9th ASEAN MINISTERIAL CONFERENCE ON CYBERSECURITY (AMCC)
Singapore, 16 October 2024

Excellency Josephine Teo, Minister for Digital Development and Information and Minister-in-charge of Smart Nation and Cybersecurity of the Republic of Singapore,

Excellencies, Ministers from the ASEAN Member States and Dialogue Partners,

Distinguished participants, ladies and gentlemen,

A very Good Morning to all.

1. I would like to start by expressing my sincere gratitude to the Government of Singapore for the invitation to deliver the Opening Remarks at the 9th ASEAN Ministerial Conference on Cybersecurity (AMCC). Over the past decade, this high-level platform has become a vital forum for ASEAN Member States to exchange perspectives, share experiences, and coordinate efforts to address cybersecurity challenges in the region. It offers a unique opportunity to enhance dialogue and deepen collaboration with external partners, advancing global cyber-security cooperation.
2. In this digital era, continued sustained economic growth hinges on our ability to anticipate, mitigate, and manage cybersecurity threats because the digital economy has become a new driver of growth for ASEAN. In 2023 alone, it expanded by 11%, adding a substantial USD218 billion in Gross Merchandise Value to the region's economy.¹ This trajectory is likely to accelerate further with the launch of negotiations for the ASEAN Digital Economy Framework Agreement (DEFA). The agreement is poised to play a transformative role in the region's economic landscape, with its

¹ [e-Economy SEA 2023](#) covering 6 ASEAN countries

contribution to ASEAN's economy expected to potentially double, from USD1 trillion to as much as USD2 trillion by 2030.²

3. This rapid growth underscores the urgency of addressing cybersecurity on a regional scale. It is crucial not only for safeguarding critical infrastructure but also for maintaining the trust of citizens and businesses within our digital ecosystem. Therefore, this year's theme for Singapore International Cyber Week, "Trust and Security in the Digital Era," is particularly timely, as it resonates with our collective aspiration to build a resilient and trustworthy digital future for ASEAN.

Excellencies, Ladies and Gentlemen,

4. The cybersecurity landscape faces increasingly sophisticated and ever-evolving threats due to rapid digitalization, the rise of disruptive technologies, and the growing interconnectivity of critical infrastructure. Cyberattacks are becoming more advanced, with threats such as ransomware, phishing, data breaches, identity thefts, online scams and supply chain attacks targeting governments, businesses, and individuals. One of the biggest challenges is staying ahead of cybercriminals who exploit vulnerabilities faster than defenses can be developed.
5. The consequences are far-reaching, resulting in substantial financial losses across multiple sectors while endangering the security and well-being of citizens. An IBM research indicates that by 2024, the average cost of a single data breach for companies in ASEAN will reach USD3.23 million, reflecting a 23% increase since 2019.³ Meanwhile, the rise in online scams has been alarming. Malaysia for example recorded USD277 million in losses from over 32,000 cases in 2023, while Thailand reported USD1.25 billion in losses from more than 300,000 cases. Singapore also faced losses exceeding USD480 million during the same period.⁴ A cyberattack in Indonesia in July this year affected 282 government agencies and caused large-scale outages and disruptions.⁵ These figures underscore the urgent need for coordinated and collective action to mitigate these risks and protect our economies and societies from further cyber harm.
6. Strengthening our national and regional cybersecurity capabilities is essential in addressing these evolving challenges. In the 2024 Global Cybersecurity Index (GCI) published by the International Telecommunication Union, we are proud that five

² <https://asean.org/asean-defa-study-projects-digital-economy-leap-to-us2tn-by-2030/>

³ <https://www.ibm.com/reports/data-breach>

⁴ Southeast Asia Public Policy Institute (2024), "Policy State of Play – Online Fraud in Southeast Asia",

⁵ <https://www.thejakartapost.com/opinion/2024/07/09/ransomwares-hard-lesson.html>

ASEAN Member States have attained Tier 1 status, placing them among the 46 leading nations globally recognised for their robust cybersecurity maturity and advanced capabilities.⁶ This accomplishment showcases our region's progress and our shared commitment to enhancing cybersecurity. However, there is still room for improvement to further build regional capacity and foster a truly resilient and secure digital ecosystem.

Excellencies, ladies and gentlemen,

7. Addressing these disparities will require a multi-faceted approach. I would like to take this opportunity to highlight three priority areas where enhanced cooperation among ASEAN countries and dialogue partners can make a significant impact.
8. **First**, we must continue working towards an inclusive regional cybersecurity strategy, grounded in the principles of the 2018 ASEAN Leaders' Statement on Cybersecurity Cooperation. This strategy aims to promote policy coherence across the three pillars of the ASEAN Community while reinforcing the region's central role in its cybersecurity architecture. A key aspect of this involves strengthening the ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber CC) to ensure strategic alignment, with a clear governance structure assigning specific roles and initiatives to relevant stakeholders. This will help prevent duplication and foster the development of new initiatives where needed.
9. The full operationalisation of the ASEAN Regional Computer Emergency Response Team (CERT) in 2024 will be a pivotal milestone in building a robust regional mechanism for coordinated cybersecurity responses. It will address cross-border threats and incidents by closely collaborating with national CERTs from ASEAN Member States. This team will standardize cybersecurity protocols, assess vulnerabilities in network infrastructures, conduct cybersecurity exercises, and enhance knowledge-sharing across the region.
10. **Second**, we must intensify our capacity-building efforts and launch a region-wide cyber awareness campaign to strengthen resilience. ASEAN can leverage existing resources, such as the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC), the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE), and the ASEAN Cyber Shield Project. By integrating initiatives across various sectors, including the ASEAN Cyber Defense Network (ACDN) and the ADMM Cybersecurity and Information Exchange of Excellence (ACICE), we can reduce program

⁶ <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>

fragmentation, avoid duplicating efforts, and enhance the effectiveness of our initiatives.

11. In addition, we must ramp up efforts to raise cybersecurity awareness, especially in addressing the growing threats of online scams and disinformation. Adopting a whole-of-ASEAN approach will ensure that we build a secure digital ecosystem, particularly for vulnerable groups. In support of this, we back initiatives developed by the ASEAN Task Force on Fake News and the ASEAN Working Group on Anti-Online Scams. Our commitment to sustaining and integrating these efforts is vital to achieving ASEAN's goal of a safe and trustworthy online environment for all citizens.
12. **Third**, we need to enhance dialogues and cooperation with external partners to strengthen coordination in finding global solutions to cybersecurity threats. While ASEAN must ensure that cybersecurity norms are relevant to our unique regional context, it is equally important to expand our partnerships and engage actively in global cybersecurity discussions. In this regard, I welcome the Inaugural ASEAN-India Cyber Policy Dialogue, which complements ASEAN's growing list of cyber dialogues with key partners such as the US, China, and Russia. These collaborations allow ASEAN to meaningfully contribute to shaping global cybersecurity governance while protecting regional interests.
13. As disruptive technologies like artificial intelligence (AI), synthetic biology, and quantum technologies rapidly emerge, their impact on security and cyber diplomacy is profound. Given their potential for intelligence gathering and cyber operations, ASEAN must work closely with international partners to establish norms and principles for their responsible use. We should leverage ASEAN mechanisms to share best practices on oversight and regulatory frameworks and promote transparency and confidence-building measures in using these technologies. Crucially, this should involve multiple stakeholders, including academia, the private sector, and civil society, to ensure a diversity of perspectives. Moving forward, ASEAN must adopt a balanced approach that manages risk, protects individual rights, and fosters trust while encouraging innovation.
14. Finally, I also would like to highlight that as ASEAN economies increasingly digitalize, the region faces a significant shortage of skilled cybersecurity professionals, with a predicted gap of around 1.5 million workers in the Asia-Pacific by 2025. The cybersecurity talent shortage requires immediate attention and action from governments, educational institutions, and the private sector to ensure a secure digital future. I am glad to note that Singapore is also proactively addressing this challenge through initiatives like the Cybersecurity Skills Framework, specialized

degree programs at local universities, and funding for lifelong learning. All these are aimed at enhancing the nation's cybersecurity capabilities and resilience.

Excellencies, Ladies and Gentlemen,

15. Ultimately, our primary objective must be to build a secure, trusted, and resilient digital ecosystem that will underpin ASEAN's continued economic growth and regional stability in the digital era. Achieving this will require sustained commitment to establishing strong and effective regional mechanisms that foster unified policies and enhance our cybersecurity preparedness for the future. At the same time, collaboration with our strategic partners will allow us to leverage collective strengths.
16. I am confident that our discussions today will greatly contribute to realizing this goal for the ASEAN Community and its dialogue partners.

Thank you.

