ASEAN LEADERS' STATEMENT ON CYBERSECURITY COOPERATION

WE, the Heads of State/Government of the Member States of the Association of Southeast Asian Nations (ASEAN), namely Brunei Darussalam, the Kingdom of Cambodia, the Republic of Indonesia, the Lao People's Democratic Republic, Malaysia, the Republic of the Union of Myanmar, the Republic of the Philippines, the Republic of Singapore, the Kingdom of Thailand and the Socialist Republic of Viet Nam, on the occasion of the 32nd ASEAN Summit;

SHARING the vision of a peaceful, secure and resilient regional cyberspace that serves as an enabler of economic progress, enhanced regional connectivity and betterment of living standards for all;

COGNISANT of the pervasiveness of cyber threats that has long been considered an international problem, and of the urgency and increasing sophistication of the ever-evolving and transboundary cyber threats facing our region amidst widespread economic digitisation and the proliferation of Internet-connected devices across ASEAN;

RECOGNISING that cybersecurity is a cross-cutting issue that requires coordinated expertise from multiple stakeholders from across different domains to address effectively;

FURTHER RECOGNISING that the cyber domain potentially represents an opportunity for significant regional economic and technological development, and can also serve as a significant source of employment;

ACKNOWLEDGING that the promotion of international voluntary cyber norms of responsible State behaviour is important for cultivating trust and confidence and the eventual development of a rules-based cyberspace;

REAFFIRMING that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful Information and Communications Technology (ICT) environment;

ACKNOWLEDGING that State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory;

AFFIRMING the need for ASEAN to speak with a united voice at international discussions aimed at developing international policy and capacity building frameworks with regard to cyber security so as to more effectively advance regional interests at such discussions;

NOTING the outcomes of discussions in various ASEAN sectoral fora that have called for greater regional cooperation in cybersecurity policy development, diplomacy, cooperation and capacity building, such as the Chairman's Statement of the 31st ASEAN Summit on 13 November 2017 in Manila, Philippines; the Joint Communique of the 50th ASEAN Foreign Ministers' Meeting on 5 August 2017 in Manila, Philippines; the Joint Declaration of the ASEAN Defence Ministers on Partnering for Change, Engaging the World of the 11th ASEAN Defence Ministers' Meeting (ADMM) on 23 October 2017 in Manila, Philippines; as well as the outcomes of discussions by ASEAN ICT and Cybersecurity Ministers at the 2nd ASEAN Ministerial Conference on Cybersecurity (AMCC) on 18 September 2017 in Singapore; and EMPHASISING the need to synergise relevant undertakings across ASEAN Sectoral Bodies and Pillars to avoid duplication of efforts, while ensuring that existing and future initiatives on cyber security are coordinated and streamlined;

ACKNOWLEDGING the work that has been done in fostering greater regional cybersecurity cooperation and capacity building, including law enforcement training on cybersecurity and cybercrimes through efforts such as the ASEAN Ministerial Meeting on Transnational Crime (AMMTC), ASEAN Telecommunications and Information Technology Ministers' Meeting (TELMIN), AMCC, ASEAN Cyber Capacity Programme, ASEAN Regional Forum (ARF) Inter-Sessional Meeting on ICT Security and the ADMM-Plus Experts' Working Group Meeting on Cyber Security;

TAKING NOTE of the initiatives to address cyber threats under other multilateral fora, including the United Nations;

DO HEREBY AGREE TO

REAFFIRM the need to build closer cooperation and coordination among ASEAN Member States on cybersecurity policy development and capacity building initiatives, including through the ASEAN Cyber Capacity Programme, the AMCC and the ASEAN-Japan Cybersecurity Capacity Building Centre, towards the promotion of voluntary and non-binding cyber norms, as well as the development of a peaceful, secure and resilient rules-based cyberspace that will contribute to continued economic progress, enhanced regional connectivity within and improved living standards across ASEAN;

RECOGNISE 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 behaviour in cyberspace so as to enhance trust and confidence in the use of cyberspace to its full potential to bring about greater regional economic prosperity and integration;

RECOGNISE ALSO the value of enhanced dialogue and cooperation on cybersecurity issues with Dialogue Partners and other External Parties, and in other ASEAN-led platforms, including the ARF and the ADMM-Plus.

TASK relevant Ministers from all ASEAN Member States to closely consider and submit recommendations on feasible options of coordinating cybersecurity policy, diplomacy, cooperation, technical and capacity building efforts among various platforms of the three pillars of ASEAN, so that ASEAN's efforts are focused, effective, and coordinated holistically on this important cross-cutting issue;

FURTHER TASK relevant Ministers from all ASEAN Member States to make progress on discussions by ASEAN ICT and Cybersecurity Ministers at the AMCC, TELMIN, as well as other relevant sectoral bodies such as the AMMTC, to identify a concrete list of voluntary, practical norms of State behaviour in cyberspace that ASEAN can work towards adopting and implementing, and to facilitate cross-border cooperation in addressing critical infrastructure vulnerabilities, as well as to encourage capacity-building and cooperative measures to address the criminal or terrorist use of cyberspace , taking reference from the voluntary norms recommended in the 2015 Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE).

***