2018 ASEAN-UNITED STATES LEADERS' STATEMENT ON CYBERSECURITY COOPERATION

Adopted in Singapore on 15 November 2018

WE, the Heads of State / Government of the Member States of the Association of Southeast Asian Nations (ASEAN) and the United States of America, gathered in Singapore on 15 November 2018 on the occasion of the 6th ASEAN-U.S. 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 digitalisation and the proliferation of Internet-connected devices across ASEAN;

Reaffirming our shared commitments to promote security and stability in cyberspace consistent with norms of responsible State behaviour;

Recalling the ASEAN Leaders' Statement on Cybersecurity Cooperation, which underscored the importance of closer cybersecurity cooperation among ASEAN Member States, stronger coordination of regional cybersecurity policy development and capacity building initiatives, including through the ASEAN Cyber Capacity Programme and the ASEAN Ministerial Conference on Cybersecurity (AMCC) and strengthening ASEAN discussions on cybersecurity at the Ministerial and Senior Officials levels;

Welcoming the adoption of the ASEAN Cybersecurity Cooperation Strategy in enhancing collaboration to address cybersecurity challenges, as well as the work by the ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN), ASEAN Ministerial Meeting on Transnational Crime (AMMTC), the ASEAN Regional Forum (ARF), and the ASEAN Defence Ministers' Meeting-Plus (ADMM-Plus), as well as the ASEAN Ministerial Conference on Cybersecurity (AMCC);

Recognising the importance of the ASEAN Information and Communications Technology (ICT) Master Plan (AIM) 2020 as part of the effort to propel ASEAN toward a digitally-enabled economy that enables an innovative, inclusive and integrated ASEAN Community;

Welcoming the establishment of the ARF Inter-Sessional Meeting on the Security of and in the Use of ICTs (ARF ISM on ICTs Security) to facilitate cooperation among ARF members in addressing cybersecurity issues, including strengthened practical cooperation on risk reduction and confidence-building measures, in accordance with the ARF Work Plan on Security of and in the Use of ICTs, and assessments of basic and common regional needs, especially in capacity building;

Welcoming the establishment of the ADMM-Plus Experts' Working Group on Cyber Security, which aims to promote practical and effective cooperation among the ASEAN Member States and Plus Countries to enhance capacity in protecting the region's cyberspace and addressing challenges to cybersecurity, related to the defence and military sectors;

Welcoming 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) and its recommendations;

Acknowledging that voluntary, non-binding norms of responsible State behaviour in the ICT environment and implementation of confidence building measures can reduce risks to and strengthen international peace, security and stability and are important for cultivating trust and confidence and strengthening of a rules-based cyberspace;

Noting that no State should conduct or knowingly support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors; and

Considering the importance of Governments' engagement with relevant stakeholders in countering the misuse of the Internet, including for terrorist purposes;

Hereby:

1. Commit to broadening and deepening our cooperation to promote an open, interoperable, reliable and secure ICT environment that fosters efficiency, innovation, communication and economic prosperity;

2. Reaffirm United Nations General Assembly (UNGA) resolution 71/28 and its call for all States to be guided in their use of ICTs by the 2015 Report of the UNGGE, including its recommendations to enhance trust, confidence and cooperation, as well as to promote an open, secure, stable, accessible and peaceful ICT environment;

3. Reaffirm that international law, and in particular the Charter of the United Nations (UN), is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment and recognise the need for further study of how international law applies to the use of ICTs by States;

4. Commit to increase efforts in implementing practical confidence-building measures to reduce the risk of misperception and escalation, including through the ARF ISM on ICTs Security;

5. Commit to promote certain voluntary, non-binding norms of responsible State behaviour in cyber space in peacetime, taking reference from the voluntary norms recommended in the 2015 Report of the UNGGE;

6. Pledge to expand cooperation on the strengthening of cybersecurity that includes promoting regional capacity building programmes such as the ASEAN Cyber Capacity Programme, the protection of critical infrastructure and combating cybercrime, among others;

7. Encourage active participation and cooperation through ASEAN-led mechanisms and efforts such as the ARF ISM on ICTs Security, ADMM-Plus Experts' Working Group on Cyber Security, ASEAN Ministerial Conference on Cybersecurity, and the Singapore International Cyber Week;

8. Encourage economic growth through policies that build trust and confidence in the digital economy, such as but not limited to frameworks that strengthen consumer protection, intellectual property rights and cybersecurity, and promote effective personal data protection across jurisdictions, as well as policies in areas such as education and technology competency;

9. Encourage support for the multi-stakeholder approach to Internet governance, which involves active participation by governments and relevant stakeholders from across industry, academic, civil society and other domains;

10. Resolve to bridge the digital divide and ICT development gaps within ASEAN, including for Least Developed Countries (LDCs) through developing digital competencies, market-driven approaches and policy cooperation along with the relevant regulatory framework; and promote efficient investment in digital infrastructure to drive robust, inclusive economic growth and prosperity;

11. Reaffirm that, as stated in UNGA resolution 71/199, the same rights that people have offline must also be protected online;

12. Work with the UN with due regard to confidentiality, respecting human rights and in compliance with other obligations under international law, to explore ways and means to:

    - Coordinate efforts at the international and regional level to counter terrorism in all its forms and manifestations on the Internet;

    - Use the Internet as a tool for countering the spread of terrorism, while recognising that States may require assistance in this regard;

13. Support ASEAN in building its capacity to counter the use of ICTs, in particular the Internet, including social media platforms, for terrorist purposes.