SINGAPORE’S VIEWS ON DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY, PURSUANT TO GENERAL ASSEMBLY RESOLUTION 71/28

As a small and highly connected state, Singapore supports a secure and resilient cyberspace underpinned by international law, well-defined norms of responsible state behaviour and coordinated capacity building efforts to meet these norms. Robust international cooperation is necessary to address the emerging challenges posed by cyber threats, and Singapore will play our part.

Singapore established its Cyber Security Agency in 2015 to provide centralised oversight of national cybersecurity functions. Our Cybersecurity Strategy was launched in October 2016, and outlines Singapore’s holistic approach to protecting essential services from cyber threats and creating a secure cyberspace. Four pillars underpin the strategy – building a resilient infrastructure; creating a safer cyberspace; developing a vibrant cybersecurity ecosystem; and strengthening international partnerships.

Regionally, Singapore is working to build and deepen capacities among our neighbours. Singapore has launched a S$10-million ASEAN Cyber Capacity Programme to complement regional capacity building efforts. Under this programme, Singapore held an ASEAN Cyber Norms Workshop in May 2017, and will hold an ASEAN Cybersecurity Capacity Building Workshop in August 2017. Singapore also hosts the annual Singapore International Cyber Week, which comprises the ASEAN Ministerial Conference on Cybersecurity and the International Cyber Leaders’ Symposium for global leaders across government, industry and academia to engage our region and discuss emerging and cross-cutting issues.

Multilaterally, Singapore supports the work of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, including the 11 norms set out in its 2015 report. It is important to define and implement the norms which enjoy broad agreement, especially operational norms. These include not supporting online activity that intentionally damages critical infrastructure; not supporting activity that prevents computer security incident response teams (CSIRTs) from responding to cyber incidents; and not using CSIRTs to engage in malicious international activity.

***