1. Singapore recognises that threats to an open, secure, and peaceful cyberspace are increasingly sophisticated, trans-boundary and asymmetric in nature. As a small and highly connected State that has been the subject of several cyber-attacks, Singapore is strongly committed to the establishment of an international rules-based order in cyberspace. This will serve as a basis for trust and confidence between Member States, and enable economic and social progress. To reap the full benefits of digital technologies, the international community must develop a secure, trusted and open cyberspace underpinned by international law applicable to cyberspace, well-defined norms of responsible State behaviour, robust Confidence Building Measures (CBMs) and coordinated capacity building. Collectively, these three streams create a mutually reinforcing triangular loop which will allow for a safe and resilient cyberspace. It is important that the efforts to discuss such laws, rules and norms continue to take place at the UN which is the only universal, inclusive, and multilateral forum, where all States, whether large or small, have a voice. Singapore is committed to this process.

2. Singapore welcomes the establishment of a UN Group of Governmental Experts (GGE) and the decision to convene an Open-Ended Working Group (OEWG). Singapore’s view is that the work of the GGE and the OEWG can and should be complementary. It is important for the major players to work together, in the spirit of consensus, mutual respect and mutual trust. Singapore is optimistic that both platforms can positively supplement each other, and we are committed to contributing constructively to both processes.

3. At the regional level, Singapore has worked with fellow Member States of the Association of Southeast Asian Nations (ASEAN) to issue the first ASEAN Leaders’ Statement on Cybersecurity Cooperation during the 32nd ASEAN Summit in April 2018. In the Statement, ASEAN Leaders reaffirmed the need for a rules-based international order in cyberspace. They also tasked relevant Ministers to identify a suitable mechanism or platform for coordinating cybersecurity policy, diplomacy, cooperation, technical and capacity building efforts across ASEAN, as well as a concrete list of voluntary, practical norms of State behaviour in cyberspace that ASEAN can work towards adopting. Acting on the Leaders’ direction, in
September 2018, participants of the 3rd ASEAN Ministerial Conference on Cybersecurity in Singapore agreed to subscribe in-principle to the 11 norms in the UN GGE’s 2015 Report, as well as to focus on regional capacity building in implementing these norms.

4. Capacity building is essential to ensuring that States develop the ability to successfully implement rules and norms of behaviour. Singapore has a S$10 million ASEAN Cyber Capacity Programme (ACCP), a modular, multi-disciplinary and multi-stakeholder programme that focuses on building capacity in ASEAN on both cyber policy, strategy as well as technical issues. Since its inception in 2016, the ACCP has trained 160 ASEAN officials. Singapore has also partnered the UN Office for Disarmament Affairs (UNODA) to develop a flagship online training course to promote understanding and implement agreements reached by the GGE. We will also work with the UNODA on a UN-Singapore Cyber Programme to build awareness of cyber norms and cyber scenario policy planning in ASEAN Member States. As an extension of the ACCP, Singapore will launch the S$30 million ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) in 2019 to further build cybersecurity policy-making, strategy development as well as technical and operational capacity in ASEAN. The ASCCE will be open and inclusive, and ASEAN Member States can leverage it to engage more closely with international partners.

5. At the national level, Singapore has made significant strides in strengthening the cybersecurity of our systems and networks on three fronts – building a resilient infrastructure, creating a safer cyberspace, and developing a vibrant cybersecurity ecosystem.

a) **Building a resilient infrastructure**: Transboundary cyber threats are increasingly putting countries’ critical infrastructure at risk. This is especially true for supranational information infrastructures like financial, maritime, telecommunications and aviation sectors, where the consequences of a successful cyber-attack could spread beyond national borders to affect inter-connected centres across the globe. A key development in 2018 was the passage and implementation of the Cybersecurity Act, which established a legal framework for the oversight and maintenance of national cybersecurity in Singapore. The Act emphasises the proactive protection of Critical Information Infrastructure (CII) against cyber-attacks, which are computers or computer systems that support the provision of essential services. This is achieved by imposing legal obligations on the owners of CII to, amongst others: (i) establish
mechanisms to detect cybersecurity threats and incidents, and report such incidents, (ii) conduct regular risk assessments and audits on CII, and (3) participate in cybersecurity exercises conducted by the national cybersecurity authority. Besides strengthening the protection of CII, the Act also authorises the national cybersecurity authority to prevent, respond to, and investigate cybersecurity threats and incidents.

b) Creating a safer cyberspace: In January 2019, Singapore attained the status of Certificate Authorising Nation under the Common Criteria Recognition Arrangement (CCRA), which is an international arrangement for the mutual recognition of Common Criteria (CC) certificates across 30 nations. The CC is a technical standard applied to the evaluation and certification of IT security products, and is widely adopted by both governments and the industry. Singapore is now one of 18 out of 30 CCRA nations to be Certificate Authorising. Being a Certificate Authorising Nation allows Singapore to certify IT security products locally, thereby helping to improve the quality of cybersecurity products of SMEs in Singapore by benchmarking them to international security standards.

c) Developing a vibrant cybersecurity ecosystem: Singapore recognises that strengthening cybersecurity involves building up the cyber ecosystem and encouraging innovation within the industry. To this end, Singapore launched its first integrated cybersecurity entrepreneur hub in March 2018, called the Innovation Cybersecurity Ecosystem at Block71 (ICE71). ICE71 aims to strengthen Singapore’s growing cybersecurity ecosystem, by attracting and developing competencies and deep technologies to help mitigate the rapidly increasing cybersecurity risks. It also helps to develop cybersecurity start-ups from around the world, through a range of programmes designed to support entrepreneurs from idea creation, acceleration and scaling of cybersecurity start-ups for the global market.