MEDIA FACTSHEET **Annex B**

National Cybercrime Action Plan

Mr K Shanmugam, Minister for Home Affairs and Minister for Law, announced the National Cybercrime Action Plan (NCAP) on 20 July 2016 at the RSA Conference Asia-Pacific & Japan.

2 The NCAP sets out the Government's strategies in combating cybercrime. The Plan also details the Government's ongoing efforts, as well as future plans, to effectively deal with cybercrime.

3 Four key principles underpin the Government's strategies in the NCAP to combat cybercrime:

a) Prevention is key;
b) Agile responses are needed to combat the evolving threat of cybercrime;
c) Our criminal justice system must be robust and supported by effective laws; and
d) Combating cybercrime is a shared responsibility.

4 These strategies are grouped into four key priorities:

a) Educating and empowering the public to stay safe in cyberspace;
b) Enhancing the Government's capacity and capability to combat cybercrime;
c) Strengthening legislation and the criminal justice framework; and
d) Stepping up partnerships and international engagement.

Ensuring a safe and secure online environment for Singapore

Key priorities	The Government will:
a. Educating and empowering the public to stay safe in cyberspace	i. Conduct outreach to the general public regarding cybercrimes and cybercrime prevention measures; ii. Engage vulnerable groups to increase their level of awareness and vigilance; and iii. Work with the National Crime Prevention Council (NCPC) to transform the Scam Alert website (www.scamalert.sg) into a one-stop self-help portal against scams. ***New initiative: One-stop self-help portal*** The Singapore Police Force (SPF) has worked with NCPC to transform the Scam Alert website (www.scamalert.sg) into a one-stop self-help portal against scams. Members of the public will be able to access the portal from 20 July 2016. The portal will provide the following resources for the public: b. Up-to-date information on the latest scams and methods of carrying out the scams, for the public to learn and safeguard themselves from falling prey to such scams; c. Links to major online e-commerce platforms, so that the public can approach the platform administrators for assistance regarding transactions on these platforms; d. A platform for members of the public to share their personal experiences of scam encounters, so that others can be forewarned if they encounter similar experiences. The information shared on this platform will also aid SPF in identifying emerging crime trends and in dealing with them expeditiously; and e. A channel for victims of scams to lodge reports for police investigations via SPF's Electronic Police Centre.
b. Enhancing the Government's capacity and capability to combat cybercrime	i. Continue to integrate SPF's cyber-related investigations, forensics, intelligence and crime prevention capabilities within the SPF Cybercrime Command, thereby improving the coordination and coherence of SPF's response to cybercrime; ii. Enhance cybercrime investigation and forensics capabilities by making use of the latest technology; ***New initiative: DIGital Evidence Search Tool (DIGEST)*** SPF has embarked on several new technology initiatives to improve its cybercrime investigation capabilities.

Key priorities	The Government will:
	One such initiative is DIGEST, which will automate the forensic processing of voluminous data. This will in turn lighten the workload of investigation officers, and enable investigation officers to focus their efforts on more specialised investigation functions. The tool will also reduce the processing time for digital evidence, ensuring that investigation officers can follow up on leads expeditiously, and solve cases in a shorter time. iii. Equip public officers handling sensitive data with the relevant skills to combat cybercrime; ***New initiative: Equipping public officers handling sensitive data with the relevant skills to combat cybercrime*** The Centre for Cyber Security Studies (CCSS)[1] facilitates the capability and capacity development of Home Team Departments and key stakeholders responsible for the protection and operations of sensitive infocomm systems across the public sector. CCSS will expand its curriculum to offer a variety of skills-based courses to public officers handling sensitive data. These skills range from cyber security fundamentals and cyber defence, to incident response, digital forensics and malware analysis. iv. Strengthen coordination between SPF and government agencies.
c. Strengthening legislation and the criminal justice framework	i. Amend the Computer Misuse and Cybersecurity Act, to ensure that the Act remains effective in dealing with the transnational nature of cybercrimes and the evolving tactics of cybercriminals; ii. Review other laws (e.g. the Criminal Procedure Code) to ensure that our laws are relevant in dealing with traditional crimes that are committed in cyberspace; and iii. Strengthen regulatory frameworks to prevent cybercriminals from exploiting potential loopholes in digital platforms and processes.

[1] The Centre for Cyber Security Studies (CCSS) was established in 2014, within the Home Team Academy.

Key priorities	The Government will:
d. Stepping up partnerships and international engagement	**Industry and academic partnerships** i. Increase cybercrime awareness in the private sector; ii. Collaborate with the private sector to develop capabilities to respond to the latest cyber threats; ***New initiative: Malware analysis tools*** MHA is working with industry to develop customised malware analysis tools. This will enable more effective incident triage and case assessment by cybercrime investigators. ***New initiative: Temasek Advanced LEarning, Nurturing and Testing (TALENT) Lab*** The Temasek Advanced Learning, Nurturing and Testing Laboratory (TALENT Lab) is a joint collaboration between the Ministry of Home Affairs and Temasek Polytechnic (TP). The TALENT Lab will foster deeper cooperation between MHA and the Institutes of Higher Learning (IHLs) in the areas of cyber-forensics and cyber-investigations. The TALENT Lab will be located in TP, and will support students specialising in cybercrime and cyber security courses from other local IHLs. This aims to facilitate the sharing of knowledge and ideas among staff and students from the different IHLs. The TALENT Lab will provide a conducive and realistic environment for students to design and validate their innovations, in order to assess if the innovations are effective in dealing with the latest cyber-threats. This practical approach will prepare students well for future careers in cyber security. The TALENT Lab is expected to be operational next year. **International engagement** iii. Foster regional (i.e. ASEAN) and global connectivity and cooperation; iv. Partner INTERPOL and other countries in areas of operational collaboration and capability building at the regional and global levels. These leverage Singapore's capacity as host for the INTERPOL Global Complex for Innovation (IGCI) and as ASEAN's Lead Shepherd on Cybercrime;

Key priorities	The Government will:
	New initiative: ASEAN Cyber Capacity Development Project (2016 – 2018) Singapore is the project proponent of the 2-Year ASEAN Cyber Capacity Development Project. This Project is funded by the Government of Japan through the Japan-ASEAN Integration Fund (JAIF) 2.0, implemented by the IGCI and targeted at ASEAN Member States. The Project aims to: a. Strengthen ASEAN Member States' capacity and capability to fight cybercrime; and b. Promote cooperation between ASEAN, Japan and INTERPOL. The Project will be implemented in the second half of 2016. It will leverage IGCI's expertise and facilities to: a. Boost a common understanding of cybercrime and cyber-enabled crime; b. Consolidate ASEAN Member States' challenges with regard to cybercrime; and c. Provide training workshops for ASEAN's law enforcement officers to address these challenges.
	Key initiative: Airline Action Day 2016 (15 – 16 June 2016) SPF participated in the 2-day Airline Action Day operation jointly coordinated by INTERPOL, Europol and Ameripol. This operation targeted criminals using fraudulent credit cards to purchase airline tickets. A total of 74 airlines and 43 countries were involved in this operation, which took place at more than 130 airports across the world. INTERPOL coordinated the information exchange and investigation in the Asia Pacific and Middle East regions through IGCI. INTERPOL also conducted checks against its criminal databases such as the Stolen and Lost Travel Document (SLTD) database. 252 suspicious transactions were reported worldwide during the operation. This led to 140 individuals being detained, denied boarding and questioned by the police.

Key priorities	The Government will:
	New Initiative: ASEAN Plus Three Cybercrime Workshop (18-19 Jul 2016) SPF and IGCI jointly organised the ASEAN Plus Three Cybercrime Workshop in Singapore, from 18-19 July 2016. The theme for the workshop was: 'Combating Cybercrime Today! ASEAN and Beyond, for a Safer Global Community'. Heads of Cybercrime Units from the ASEAN Member States and ASEAN Plus Three dialogue partners (People's Republic of China, Japan and Republic of Korea) were invited to attend the workshop. The workshop provided a platform for ASEAN cybercrime agencies to tackle cybercrime by (i) taking stock of their common gaps; (ii) exchanging information on prevention measures, law and regulatory policies; (iii) sharing of best practices on cybercrime forensics and investigations to strengthen their overall cybercrime response, giving rise to a concerted effort among the ASEAN member states to tackle cybercrimes. ***New Initiative: Institute of Safety and Security Studies*** MHA has established a new Institute of Safety and Security Studies (ISSS) as an autonomous entity under the Home Team Academy. The ISSS offers professional training such as in cybercrime forensics and investigation to Home Team officers, the industry and ASEAN Member States. ISSS will start the Cyber Investigation Essential Course for ASEAN Member States in 2016. Participants in the Essential Course will be equipped with skills needed to carry out cyber investigations. Such courses aim to help participants, including those from the ASEAN Member States, to build strong capabilities to deal with the threat of cybercrime. v. Bring global experts and thought leaders together to discuss the latest threats, trends and solutions in the cyber domain, and share best practices and solutions.

***

MINISTRY OF HOME AFFAIRS
20 JULY 2016