National Cybercrime Action Plan

EXECUTIVE SUMMARY

1. The Internet has afforded criminal elements the opportunity to commit cybercrimes quickly, easily and on a large scale. Criminals have also exploited the anonymity provided by the Internet and the transnational nature of cybercrime to escape detection. These characteristics of cybercrime pose significant challenges for law enforcement agencies around the world.

2. As the use of the Internet becomes more prevalent in Singapore, the number of cybercrime cases has risen sharply in Singapore. A coordinated national effort is required to effectively deal with the threat of cybercrime.

3. The National Cybercrime Action Plan (NCAP) sets out the Government's key principles and priorities in combating cybercrime. The Plan also details the Government's ongoing efforts, as well as future plans, to effectively deal with cybercrime.

VISION

4. The vision of the NCAP is to ensure a safe and secure online environment for Singapore. We will achieve this by effectively deterring, detecting and disrupting cybercriminal activities.

KEY PRINCIPLES

5. Four key principles underpin the Government's strategies to ensure a safe and secure online environment for Singapore:

a. Prevention is key

More often than not, the adoption of simple and inexpensive measures by businesses and individuals will prevent the vast majority of cybercrimes. Stepping up efforts to educate the public and boost awareness of cyber hygiene[1] practices is critical in preventing individuals and organisations from becoming victims of cybercrimes.

b. Agile responses are needed to combat the evolving threat of cybercrime

As technology progresses rapidly, cybercriminals will frequently make use of new and complex tools and methods to commit cybercrimes. The Government needs to constantly

[1] Cyber hygiene refers to steps that users can take to protect themselves online. Examples of cyber hygiene practices include using a firewall, maintaining strong passwords and updating anti-virus software.

conduct horizon scans to detect emerging trends, patterns and technologies which will shape the nature of threats, capabilities and opportunities in cyberspace. The Government also needs to regularly review and develop new capabilities, and adopt the best practices from industry and overseas jurisdictions.

c. Our criminal justice system must be robust and supported by effective laws

A robust criminal justice system, supported by tough and effective laws, will enable the Singapore Police Force (SPF) to effectively investigate cybercrimes, and obtain the evidence needed for successful prosecution of those responsible. Criminal justice procedures and processes must be nimble and efficient to deal with new types of cybercriminal activities, as well as the speed and scale with which cybercrimes are perpetrated.

d. Combating cybercrime is a shared responsibility

Fighting cybercrime is a shared responsibility between the public, industry and the Government. The Government needs to work closely with industry partners and Institutes of Higher Learning (IHLs) to share the latest information and expertise. The transnational nature of cybercrime also means that digital evidence and information pertaining to cybercriminals may not be located within Singapore's jurisdiction. SPF will need to continue its close cooperation with overseas law enforcement agencies and other key international partners, in order to successfully bring cybercriminals to justice.

KEY PRIORITIES

6. The Government's strategies to combat cybercrime are grouped into four priority areas:

a. Educating and empowering the public to stay safe in cyberspace

In order to achieve this, the Government will:

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.

b. Enhancing the Government's capacity and capability to combat cybercrime

In order to achieve this, the Government will:

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;

iii. Equip public officers handling sensitive data with the relevant skills to combat cybercrime; and

iv. Strengthen coordination between SPF and government agencies.

c. Strengthening legislation and the criminal justice framework

In order to achieve this, the Government will:

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.

d. Stepping up partnerships and international engagement

Through the forging of close partnerships with industry and IHLs, the Government will:

i. Increase cybercrime awareness in the private sector; and

ii. Collaborate with the private sector to develop capabilities to respond to the latest cyber threats.

To ensure effective international cooperation, Singapore will:

i. Foster regional (i.e. ASEAN) and global connectivity and cooperation;

ii. Partner INTERPOL and other countries in areas of operational collaboration and capability building at the regional and global levels; and

iii. 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.

CONCLUSION

7. The activities of cybercriminals will continue to grow in scale, complexity and severity worldwide, and the transnational nature of cybercrime will continue to pose legal and operational difficulties for law enforcement agencies. Prevention is therefore still the key strategy in countering the threat of cybercrime. The NCAP will prioritise educating and empowering the public to be safe in cyberspace.

8. The Government will foster strong partnerships between industry, institutes of higher learning, the public and law enforcement agencies, and forge a sense of shared responsibility in the fight against cybercrime, so that collectively we create a safe and secure online environment.

INTRODUCTION

1. The growth of the Internet has created numerous opportunities for Singapore. Today, vast amounts of information are exchanged via the Internet; the Internet has become an indispensable communication and business tool for many of us.

2. Where there are opportunities, there are also risks. The Internet has been exploited by criminal elements to commit cybercrimes like scams, hacks and thefts, causing financial loss and harm to many. We therefore need a concerted and coordinated response to effectively deal with the cybercrime threat. The National Cybercrime Action Plan (NCAP) sets out the Singapore Government's plans to deter, detect and disrupt cybercrimes.

What is cybercrime?

3. In Singapore, the term 'cybercrime' refers to two categories of offences[2]:

a. Offences where a computer system is the target of a criminal act; and

b. Offences where traditional crimes are committed via the means of a computer system.

4. The first category of offences is covered by the Computer Misuse and Cybersecurity Act (CMCA), and includes criminal acts like the unauthorised access and the unauthorised modification of a computer system.

5. The second category of offences describes traditional crimes that are committed via the Internet. In the digital world, crimes like fraud and extortion are committed online in the form of e-commerce scams and cyber-extortions respectively. The Internet has afforded criminals anonymity, as well as the opportunity to commit crimes quickly, easily and on a large scale. These characteristics of cybercrime pose significant challenges to law enforcement.

The current situation

Prevalence of the Internet

6. The Internet is becoming more prevalent and indispensable to everyday life in Singapore. The proportion of resident households in Singapore with household Internet access has climbed steadily in recent years, from 65% in 2004 to 88% in 2014[3]. More Singaporeans are transacting

[2] The two categories are not mutually exclusive; there may be cybercrimes that fall into both categories (e.g. causing physical injury by sabotaging an Internet-of-Things enabled appliance, or the theft of data stored on a computer, which is then sold to criminal syndicates).

[3] "Annual survey on infocomm usage in households and by individuals for 2014." iDA. <https://www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/Facts%20and%20Figures/SurveyReport/2014/2014%20HH%20public%20report%20final.pdf>

online as well; the number of Singapore residents shopping online in 2014 was about 1.44 million, increasing by a compound annual growth rate of about 14% from 2012[4]. As the use of the Internet becomes ubiquitous in Singapore, there will be an increasing number of opportunities for cybercriminals to strike.

Rapid increase in cybercrimes

7. With the increase in online activity among Singaporeans, Singaporeans are increasingly becoming victims of cybercrimes. Cases investigated under the CMCA increased by 81 (+41.1%) cases in 2015 to 278 cases, compared to 197 cases in 2014. Traditional crime is also migrating online. While almost all physical crime classes registered a decrease in 2015 as compared to 2014[5], commercial crimes increased by 2,642 (+46.5%) cases in 2015 to 8,329 cases, compared to 5,687 cases in 2014. Within this class of crimes, cheating involving e-commerce, credit-for-sex scams and Internet love scams saw the largest increase in the number of cases (see Table 1).

Table 1: Cheating involving e-commerce, credit-for-sex scam and Internet love scam cases (2014-2015)

	Number of cases in 2014	Number of cases in 2015	Increase (% change)	Total sum cheated in 2015
Cheating involving e-commerce	1,665	2,173	508 (+30.5%)	S$1.76 million
Credit-for-sex scams	66	1,203	1,137 (+1,723%)	S$2.9 million
Internet love scams	198	383	185 (+93.4%)	S$12 million

8. The impact of cybercrimes in Singapore has been high. The 2016 Norton Cybersecurity Insights Report found that cybercrime victims in Singapore had lost an average of S$545 to cybercrime in the past year, higher than the global average of US$358 (S$510)[6].

Need for better cyber hygiene

9. The growing number and impact of cybercrimes pose a credible threat to Singapore and Singaporeans. There is a need for greater public awareness of cyber hygiene practices, so that individuals and enterprises are able to take care of themselves in cyberspace. A survey by the Infocomm Development Authority of Singapore (iDA) in 2013 found that only about 14% of local

[4] "Annual survey on infocomm usage in households and by individuals for 2014." iDA. <https://www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/Facts%20and%20Figures/SurveyReport/2014/2014%20HH%20public%20report%20final.pdf>

[5] Crimes Against Persons, Violent/Serious Property Crimes, Housebreaking and Related Crimes, and Theft and related crimes registered a decrease in 2015, compared to 2014.

[6] "Norton Cybersecurity Insights Report." Norton. <http://us.norton.com/cyber-security-insights>, as reported in Lim, Jessica. "Cybercrime victims here 'lost $545 on average'." The Straits Times. 25 Nov, 2015. <http://www.straitstimes.com/singapore/cybercrime-victims-here-lost-545-on-average>

enterprises had invested in educating their employees on infocomm security[7]. Another iDA survey in 2014 found that while about 80% of Internet users had previously installed anti-virus software and security updates on their computer at home, only about 30% of smartphone users surveyed had installed anti-virus software on their smartphones[8]. Individuals and enterprises in Singapore need to adopt better cyber hygiene practices, so as to reduce opportunities for criminals to commit cybercrimes.

10. The threat of cybercrime poses several key challenges for law enforcement:

a. Anonymity afforded by the Internet

The Internet allows cybercriminals to hide behind a veil of anonymity, through the use of Virtual Private Network (VPN) services or other anonymous proxy services like The Onion Router (TOR). This impedes detection efforts, and cybercrimes are not easily traced back to perpetrators.

b. Transnational nature of cybercrime

The Internet is borderless, and cybercrimes are easily perpetrated across geographical borders. This problem is compounded by the fact that some foreign countries do not have cybercrime laws. Where there are cybercrime laws in operation, cybercrime offences in other countries may also not be defined in the same manner as in Singapore. An act which constitutes a cybercrime offence in Singapore may therefore not be an offence in another country. The lack of dual criminality makes it a challenge to prosecute cybercriminals who operate from a different country, as well as to secure the necessary digital evidence required for a successful prosecution.

c. Speed and scale of perpetration

The Internet also allows for simultaneous and instantaneous communication en masse; criminals can easily make use of the Internet to target large numbers of victims at the same time, and carry out criminal activities rapidly.

d. Easy access to sophisticated cybercrime tools and services

The rise of the 'cybercrime-as-a-service' model in the cybercrime underground market has lowered the entry barriers into the world of cybercrime. Tools such as malicious software, supporting digital infrastructure, stolen personal data, as well as the means to monetise criminal gains, are now available for purchase or hire as a service. This model allows criminals without much technical expertise to carry out cyber-attacks and other cybercrimes, by acquiring the necessary tools and services, which may be easily available in the cybercrime underground market[9]. The number and sophistication of cyber-attacks and cybercrimes are likely to grow over time.

[7] "Annual survey on infocomm usage by enterprises for 2013." iDA. <https://www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/Facts%20and%20Figures/SurveyReport/2013/InfocommUsage_Survey%202013%20public%20report.pdf>

[8] "Annual survey on infocomm usage in households and by individuals for 2014." iDA. <https://www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/Facts%20and%20Figures/SurveyReport/2014/2014%20HH%20public%20report%20final.pdf>

[9] "Cybercrime Exposed: Cybercrime-as-a-Service". McAfee. <http://www.mcafee.com/sg/resources/white-papers/wp-cybercrime-exposed.pdf>

THE NATIONAL CYBERCRIME ACTION PLAN

11. The NCAP sets out the Government's key principles and priorities in combating cybercrime. The Plan also details the Government's ongoing efforts, as well as future plans, to effectively deal with cybercrime. The threat of cybercrime affects all of us; in implementing the NCAP, the Government, academia, businesses and the public need to work closely together.

Vision

> Our vision is to ensure
> a safe and secure online environment for Singapore.
>
> We will achieve this by
> effectively deterring, detecting and disrupting cybercriminal activities.

Key principles

12. Four key principles underpin our efforts to create a safe and secure online environment for Singapore:

a. Prevention is key

More often than not, the adoption of simple and inexpensive measures by businesses and individuals will prevent the vast majority of cybercrimes. It is much easier to prevent cybercrimes from happening, than to respond after the cybercrime has occurred. Stepping up efforts to educate the public and boost cyber hygiene awareness is critical in preventing individuals and organisations from becoming victims of cybercrimes.

b. Agile responses are needed to combat the evolving threat of cybercrime

As technology progresses rapidly, cybercriminals will frequently make use of new and complex tools and methods to perpetrate cybercrimes. User behaviours are also constantly evolving, exposing new vulnerabilities for cybercriminals to exploit. In order to effectively understand and deal with the evolving threat of cybercrime, the Government needs to constantly conduct horizon scans to detect emerging trends (e.g. FinTech), patterns and technologies (e.g. Bitcoin) which will shape the nature of threats, capabilities and opportunities in cyberspace. The Government also needs to regularly enhance current capabilities, develop new ones and adopt the best practices of industry and overseas jurisdictions.

c. Our criminal justice system must be robust and supported by effective laws

Where prevention efforts fail to thwart the efforts of cybercriminals, a robust criminal justice system, supported by tough and effective laws, will be essential in deterring and dealing with the perpetrators. A strong criminal justice system will enable the Singapore Police Force (SPF) to effectively investigate cybercrimes, and obtain the evidence needed for successful prosecution of those responsible. Criminal justice procedures and processes must be nimble and efficient to deal with new types of cybercriminal activities, as well as the speed and scale with which cybercrimes are perpetrated.

d. Combating cybercrime is a shared responsibility

Fighting cybercrime is a shared responsibility between the public, industry and the Government. The leading expertise to deal with cybercrimes will likely reside within industry and Institutes of Higher Learning (IHLs). The Government therefore needs to work closely with industry partners and IHLs to share the latest information and expertise. The transnational nature of cybercrime also means that digital evidence and information pertaining to cybercriminals may not be located within Singapore's jurisdiction. SPF will need to continue its close cooperation with overseas law enforcement agencies and other key international partners, in order to successfully bring cybercriminals to justice.

Key priorities

13. The Government's strategies to combat cybercrime are grouped into four priority areas. Strengthening our response to cybercrime in these four areas will prepare us as a nation to comprehensively and capably deal with the threat of cybercrime:

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.

KEY PRIORITY #1: EDUCATING AND EMPOWERING THE PUBLIC TO STAY SAFE IN CYBERSPACE

14. Educating and empowering the public and businesses to better protect themselves in cyberspace is a key priority. Prevention is the best way to combat cybercrime; the majority of cybercrimes can be prevented if businesses and individuals are educated on the risks of cybercrime, as well as the simple cybercrime prevention measures that can be adopted in order to protect themselves online.

15. In order to educate and empower the public to stay safe in cyberspace, SPF regularly shares cybercrime prevention messages with the public via different media platforms. In addition, SPF has tailored its cybercrime prevention outreach programmes to match the profile of different vulnerable groups in society, thereby ensuring that the message of cybercrime prevention is effectively communicated to all segments of society. SPF has worked 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. The portal will provide further information to the public on the different typesof scams, and empower the public to take steps to guard against scams.

(i) Conducting outreach to the general public

16. The majority of SPF's outreach programmes focus on the general public. Through its Public Cyber-Outreach & Resilience Programme (PCORP), SPF will explore the use of behavioural insights to influence the general public to adopt good cyber hygiene practices (e.g. using stronger passwords).

17. SPF has also stepped up its mass media advertising efforts. SPF's cybercrime prevention messages are regularly publicised via various media platforms, such as television (in particular, during the SPF's monthly televised Crimewatch episodes), newspapers, social media, text messages sent to vulnerable target groups, as well as posters at public transport nodes and lifts in public housing blocks.

18. At the local community level, SPF's Neighbourhood Police Centres frequently engage the community through Community Safety and Security Programmes and educational roadshows. In 2015, more than 80 roadshows were conducted island-wide, with 180 Crime Prevention Ambassadors sharing anti-scam messages with the public.

19. Through its Police Cyber-Awareness Programme (PCAP), SPF will equip its officers with the relevant skills and knowledge to effectively reach out and educate the public on cybercrimes and cybercrime prevention measures. The PCAP will provide SPF officers with insights on cybercrime trends and common types of cybercrimes; officers will be able to recognise cybercrimes reported by the public and advise the public how to reduce their vulnerability to cybercrimes, during their interactions with the public.

(ii) Engaging vulnerable groups in society

20. Certain groups in society (e.g. senior citizens and children) may be particularly vulnerable to cybercrime. Through its COllaborative Social Programme (COSP), SPF will work with schools and Non-Governmental Organisations (NGOs) to raise cybercrime prevention awareness among vulnerable groups. SPF regularly analyses cybercrime trends to identify the victim demographic for each type of scam, before customising its outreach efforts and content to suit the profile of the different target victim groups.

21. SPF has recognised that there is a need to raise the level of cybercrime awareness among senior citizens. This will ensure that senior citizens do not fall prey to cybercriminals, as they pick up the use of technology and the Internet. SPF plans to tap on existing senior citizen engagement platforms (e.g. iDA's Silver IT Fest 2016) to reach out to senior citizens and raise the cybercrime awareness of this vulnerable group.

22. Other than senior citizens, SPF will also focus its outreach efforts on children. Mindful that children start to use the Internet from an early age, SPF has enhanced its cybercrime prevention outreach and education efforts for children. In 2011, SPF launched 'Cyberonia' in collaboration with NCPC, a virtual game with the objective of educating children on being safe in cyberspace. Riding on the success of this initiative, NCPC will be launching the 'Cyro' apps for children, a series of first person

shooter games that contain cybercrime prevention messages. The apps will educate children on the risks of cybercrime, as well as cybercrime prevention measures.

23. In 2016, SPF incorporated cybercrime and cyber-wellness education materials in the regular outreach talks conducted by SPF at secondary schools. The cybercrime education materials included content on good cyber hygiene practices (e.g. safe conduct on social media), as well as cybercrime prevention tips. SPF will continue to work with partners like the Ministry of Education (MOE) to build on these efforts.

(iii) Providing a one-stop self-help portal against scams

24. SPF and NCPC launched a dedicated Scam Alert website (www.scamalert.sg) in November 2014, to keep the public informed of the latest scams and the modus operandi of various scams. The website has attracted more than 315,000 visitors since its launch.

25. SPF has worked with NCPC to transform the Scam Alert website into a one-stop self-help portal against scams. Members of the public will be able to make use of the different resources that are offered on the portal, depending on the circumstances of their scam case. The portal will provide the following resources for the public:

a. 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;

b. Links to major online e-commerce platforms, so that the public can approach the platform administrators for assistance regarding transactions on these platforms;

c. A platform for members of the public to share their personal experiences of scam encounters, so that others can be forewarned if they should 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

d. A channel for victims of scams to lodge reports for police investigations via SPF's Electronic Police Centre.

KEY PRIORITY #2: ENHANCING THE GOVERNMENT'S CAPACITY AND CAPABILITY TO COMBAT CYBERCRIME

26. The transnational nature of cybercrimes, coupled with the speed and scale at which such crimes are perpetrated, present formidable challenges for traditional law enforcement approaches. In order to effectively combat cybercrime, the Government has taken steps to (i) establish the SPF Cybercrime Command, (ii) boost cybercrime investigation capabilities, (iii) equip public officers with the relevant skills to combat cybercrime, and (iv) enhance coordination between SPF and government agencies.

(i) Establishing the SPF Cybercrime Command

27. The SPF Cybercrime Command was established in December 2015, with the aim of increasing the agility and effectiveness of the SPF to respond to cybercrimes. The Cybercrime Command integrates SPF's cyber-related investigation, forensics, intelligence and crime prevention capabilities within a single command, thereby improving the coordination and coherence of SPF's response to cybercrime. This also enables SPF to work together more effectively with other government agencies, industry and the public, in responding nimbly to the constantly evolving nature of cybercrime. For example, analysis of a new cybercrime modus operandi that is shared within the Command can quickly trigger changes in the content of cybercrime prevention messages; this will allow the public to be informed early of the new cybercrime trend.

28. The SPF Cybercrime Command also oversees the Cybercrime Response Teams that are based in every Police Land Division. These teams assist investigation officers in responding to reports of cybercrime, by collecting and processing digital evidence, and conducting forensic analysis of computers and mobile phones. The Cybercrime Response Teams support the Police Land Divisions in responding more quickly and effectively to cybercrime cases. In addition, these teams are trained to recognise when more complex cases require the additional support of the Cybercrime Command's specialist investigators.

29. The SPF Cybercrime Command also develops the curriculum for SPF's specialised cybercrime investigation training modules. The Cybercrime Command has incorporated cybercrime modules in the basic training for new Police officers, as well as in the different training courses for investigation officers. Through the modules, SPF investigation officers are equipped with specialised cybercrime investigation skills like email header analysis and the process of recognising, collecting and preserving digital evidence.

(ii) Boosting cybercrime investigation capabilities

30. SPF has embarked on several new technology initiatives to improve its cybercrime investigation capabilities. These initiatives will enable SPF to effectively investigate the rising number of cybercrime cases, as well as to process increasingly large volumes of digital information, in order to sieve out necessary evidence for a successful prosecution.

31. One such initiative is the DIGital Evidence Search Tool (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.

32. SPF will develop a Video Trawling and Analytics System (VTAS), which will speed up analysis of video footages. With VTAS, investigation officers will be able to quickly search videos for images of interest, based on certain defined parameters. VTAS will also allow for the detection, tracking and recognition of faces, as well as optical character recognition.

(iii) Equipping public officers handling sensitive data with the relevant skills to combat cybercrime

33. In recognition of growing cyber security and cybercrime threats, the Centre for Cyber Security Studies (CCSS) was established in 2014 within the Home Team Academy (HTA). CCSS 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. One of CCSS' functions is to equip these officers with the necessary skills to deal with cybercrime effectively. To achieve this, a Cyber Security Lab (CSL) has been set up in the CCSS, as a modern hands-on facility for training and familiarising trainees on approaches to mitigate cyber threats and investigate cyber incidents. CCSS will expand its curriculum to offer a variety of skills-based courses, ranging from cyber security fundamentals and cyber defence, to incident response, digital forensics and malware analysis. These courses are tailored to the needs of officers, depending on their professional roles.

(iv) Strengthening coordination between SPF and government agencies

34. SPF works closely with its partner agencies to ensure an effective and coordinated response to cybercrimes:

a. Cooperation with the Attorney-General's Chambers (AGC) on complex cybercrime cases

Traditionally, prosecutors only have access to a case at the conclusion of police investigations. In recent years, due to the complexity of cybercrime cases, AGC and SPF have worked closely together on sensitive and high-profile cybercrime cases, from an early stage in investigations. AGC's expertise has helped SPF to ensure that crucial evidence is secured at an early stage and that police investigations are watertight; this is especially important where digital evidence stored on cloud servers is concerned. Time is of the essence in such cases, because cloud evidence can be deleted from the server remotely at any time.

b. Strengthening coordination arrangements with the Cyber Security Agency of Singapore

Given the closely-related nature of cyber security and cybercrime, SPF and the Cyber Security Agency of Singapore (CSA) work together to ensure an effective response to cyber-related incidents. Aside from the active sharing of information pertaining to cyber threats, SPF and CSA have established a joint workflow that clearly delineates the responsibilities for both agencies, and strengthens coordination between both agencies. In 2016, SPF and CSA conducted Exercise CyberStar, a joint exercise that stress-tested existing workflows, coordination arrangements and procedures for both agencies. SPF and CSA will continue to conduct regular joint exercises.

KEY PRIORITY #3: STRENGTHENING LEGISLATION AND THE CRIMINAL JUSTICE FRAMEWORK

35. The investigation of cybercrimes and prosecution of cybercriminals must be supported by a robust criminal justice framework. Laws need to be updated to ensure that they are relevant and effective in dealing with new cyber-offences and traditional crimes committed online. Regulatory frameworks have to be strengthened, to prevent criminals from taking advantage of loopholes in new technologies.

(i) Amending the Computer Misuse and Cybersecurity Act

36. The primary legislation that deals with cybercrime is the Computer Misuse and Cybersecurity Act (CMCA). The Act was last amended in 2013 to better protect Singapore's Critical Infocomm Infrastructure (CII) against cyber threats. The Ministry of Home Affairs (MHA) intends to amend the CMCA, to ensure that the Act continues to be effective in dealing with the transnational nature of cybercrimes, as well as the evolving tactics of cybercriminals.

(ii) Reviewing other laws

37. In addition to amending the CMCA, MHA will also review other laws (e.g. the Criminal Procedure Code) to ensure that these laws are relevant in dealing with traditional crimes that are committed in cyberspace.

(iii) Strengthening regulatory frameworks

38. Aside from public education and outreach, a key method of cybercrime prevention is to increase the difficulty of committing such offences by plugging potential loopholes in digital platforms and processes. The Government will regularly review regulatory frameworks, to ensure that cybercriminals are not able to exploit vulnerabilities in technology.

KEY PRIORITY #4: STEPPING UP PARTNERSHIPS AND INTERNATIONAL ENGAGEMENT

Industry and Academic Partnerships

39. The private sector plays a critical role in Singapore's fight against cybercrime, as the leading expertise to deal with cybercrimes likely resides within industry and IHLs. Given the rapidly evolving nature of cybercrime, it is important for the Government to work closely with industry and IHLs, so that the necessary information and expertise to deal with the latest threat posed by cybercrime can be shared seamlessly.

40. Key private sector stakeholders (e.g. the banking and IT industries) are attractive targets for cybercriminals. The Government needs to work with stakeholders in these industries to ensure that they are aware of the threat posed by cybercrime and that they adopt cybercrime prevention measures.

41. The Government will partner industry and IHLs to (i) increase awareness of cybercrimes in the private sector, and (ii) jointly develop capabilities to combat cybercrime.

(i) Increasing cybercrime awareness in the private sector

42. SPF regularly engages key private sector stakeholders (e.g. stakeholders in the IT and banking industries) to enhance cybercrime prevention efforts. CSA and the Singapore Infocomm Technology Federation (SITF) lead the Cyber Security Awareness Alliance (CSAA), which includes SPF, the Media Development Authority of Singapore (MDA), iDA, the Media Literacy Council, as well as other IT companies. Through CSAA, SPF works closely with IT companies in Singapore, to raise awareness of cybercrimes in the private sector and in Government, and to encourage the adoption of good cyber hygiene practices.

(ii) Developing capabilities to combat cybercrime

43. SPF has partnered local research institutes to develop new cybercrime investigations and forensics capabilities:

a. Cyber-Forensics Project
Under the National Cyber Security Research & Development Programme (NCRP), SPF is working with the Institute for Infocomm Research (I^2R) to enhance capabilities in digital forensics.

b. Video trawling and analytics
SPF has partnered the Nanyang Technological University (NTU) to develop deep learning capabilities to enhance object detection and recognition, including the detection and recognition of everyday objects, such as caps, backpacks and car models.

c. Online and social media analytics
SPF and Temasek Polytechnic have jointly developed a tool to assist investigators in advanced social media analysis, so as to identify useful leads for cybercrime investigations.

d. 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.

44. MHA has also worked with IHLs to create conducive environments for the development of cyber-related innovations. One example is MHA and Temasek Polytechnic's joint establishment of the Temasek Advanced LEarning, Nurturing and Testing (TALENT) Lab, which serves as a platform for students from IHLs to design and validate innovations, to see if they are effective in dealing with cyber-threats. The TALENT Lab will foster deeper cooperation between MHA and IHLs in the areas of cyber-forensics and cyber-investigations, and facilitate knowledge sharing among students from the different IHLs.

International Engagement

45. No country is immune from the threat posed by cybercriminals and syndicates. Even as countries fortify defences against cyber-attacks and educate their citizens to be vigilant against cybercrimes, cybercriminals continue to exploit vulnerabilities with little regard for national borders. What we do within our own borders is not enough by itself to keep Singapore and Singaporeans safe.

46. Strong international partnerships enable countries to deal with cybercrime more effectively. For example, SPF works closely with foreign law enforcement agencies to foil the actions of foreign cybercrime syndicates. In 2015, after SPF received reports of credit-for-sex scams committed by syndicates operating in the People's Republic of China, SPF worked with Chinese law enforcement counterparts to conduct simultaneous raids, resulting in the arrest of 43 members of a syndicate. Countries need to cooperate bilaterally, regionally and internationally, to develop capacities and capabilities, and to tackle cybercrime in a concerted manner.

47. Through its international engagement efforts, Singapore will (i) foster regional and global connectivity and cooperation, (ii) build capacities and capabilities through a collaborative environment, and (iii) bring global experts and thought leaders together.

(i) Fostering regional and global connectivity and cooperation

48. Singapore is at the forefront of working with foreign countries to enhance our operational cooperation against cybercrime. At the regional level, Singapore is the Association of Southeast Asian Nations (ASEAN) Voluntary Lead Shepherd on Cybercrime, responsible for charting ASEAN's initiatives against cybercrime. With the unanimous support of ASEAN Member States, Singapore established the ASEAN Senior Officials Meeting on Transnational Crime (SOMTC) Working Group on Cybercrime in 2013. The Working Group, chaired by Singapore, provides a platform for the ASEAN Member States to coordinate the regional approach to cybercrime, and work together on capacity building, training and the sharing of information to combat cybercrime. This is also the platform through which the ASEAN Member States engage ASEAN Dialogue Partners such as the People's Republic of China, Japan and the Republic of Korea on cybercrime collaboration.

49. At the international level, Singapore hosts the INTERPOL Global Complex for Innovation (IGCI). The IGCI is INTERPOL's global hub on cybercrime. Singapore has led the IGCI Working Group and INTERPOL Operational Expert Group on Cybercrime, working with other INTERPOL member countries to define INTERPOL's cybercrime programme. Singapore's goal is to leverage INTERPOL's resources to build global operational networks, capacities and capabilities to tackle cybercrime, especially within Asia.

50. Today, the IGCI comprises the INTERPOL Digital Crime Centre (IDCC), which houses a Digital Forensics Lab (DFL) and a Cyber Fusion Centre (CFC). The DFL supports global law enforcement agencies by utilising the latest techniques and solutions in the forensic examination of digital devices. The CFC conducts real-time gathering and analysis of information, providing INTERPOL's 190 member countries with actionable intelligence on cyber threats. The IDCC has coordinated several successful global operations out of Singapore, such as Operation Strikeback 1 and Strikeback 2 in the Philippines, which resulted in the arrest of a total of 66 suspects believed to be involved in

sextortion activities[11], as well as the global operations to take down the Dorkbot botnet[12] and the Simda botnet[13] in 2015. Singapore will continue working closely with the IGCI and INTERPOL, as INTERPOL's cybercrime programme expands to cover the full spectrum of Internet and cyber-enabled security threats.

(ii) Building capacities and capabilities through collaboration at the regional and global levels

51. Singapore believes that the virtual world will be a safer place when every country has strong cybercrime enforcement and investigation capabilities. Capacity and capability building is therefore key. Singapore spearheads international capacity building initiatives, and works with government counterparts, ASEAN and INTERPOL to introduce programmes that would aid countries in enhancing their defences against cybercriminals.

52. Singapore has rolled out several programmes with partner countries and INTERPOL. This includes the two-year (2016 – 2018) ASEAN Cyber Capacity Development Project funded by Japan and implemented by INTERPOL, the Singapore-United States Third Country Training Programme, and the ASEAN Plus Three Cybercrime Workshop, involving the People's Republic of China, Japan and the Republic of Korea. The involvement of key Asian partners, ASEAN Member States and INTERPOL facilitates an effective environment for collaboration on cybercrime issues, which is anchored in Singapore. This environment enables the sharing of best practices between countries and across regions, and the forging of effective operational links.

(iii) Bringing global experts and thought leaders together

53. Aside from fostering cooperation between governments, countries need to also tap on the knowledge and capabilities of stakeholders in the private sector. Singapore continues to contribute actively in the global effort to bring the public and private sectors together.

54. Since 2013, Singapore has been driving thought leadership platforms for multi-stakeholder, regional and international dialogues on cybercrime. The RSA Conference Asia Pacific and Japan (RSAC APJ) held annually in Singapore is Asia Pacific's leading conference on information security. Alongside the RSAC APJ, Singapore also organises the annual ASEAN Senior Officials Roundtable on Cybercrime (SORC), which is a unique platform for high-level discussions between industry leaders and senior governmental officials from ASEAN and Dialogue Partner countries, as well as INTERPOL and Europol. This year, Singapore organised a "Forum on the Future of Cybercrime" in conjunction with the RSAC APJ 2016. The Forum brought RSAC APJ speakers, ASEAN Plus Three ministers, SOMTC leaders and leaders of private corporations together to discuss the current and future global cybercrime threat situation. The bi-annual INTERPOL World organised by the IGCI in Singapore also brings together law enforcement officials, academia and industry leaders to share best practices and solutions.

[11] Sextortion is a crime where cybercriminals meet victims through social media platforms and invite them to perform sexual acts on web cameras. The cybercriminals will then record the footage of these sexual acts and extort the victims.

[12] The Dorkbot botnet is believed to have infected more than one million computers worldwide in 2015. The Dorkbot botnet was used for a variety of illegal activities, most commonly (i) stealing account information for online payment, (ii) Distributed Denial of Service (DDoS) attacks and (iii) providing a mechanism for the download and installation of dangerous malware on the victim's computer.

[13] The Simda botnet is believed to have infected more than 770,000 computers worldwide. The Simda botnet was used by cybercriminals to gain remote access to computers, enabling (i) the theft of personal information (including banking information), and (ii) the download and installation of dangerous malware on the victim's computer.

55. These platforms provide opportunities for experts and thought leaders in cybercrime to discuss the latest threats, trends and solutions in the cyber domain. The discussions seed new ideas for R&D, as well as opportunities for deeper collaboration across the public and private sectors.

CONCLUSION

56. The activities of cybercriminals will continue to grow in scale, complexity and severity worldwide, and the transnational nature of cybercrime will continue to pose legal and operational difficulties for law enforcement agenceis. Prevention is therefore still the key strategy in countering the threat of cybercrime. The NCAP will prioritise educating and empowering the public to be safe in cyberspace.

57. The Government will foster strong partnerships between industry, IHLs, the public and law enforcement agencies, and forge a sense of shared responsibility in the fight against cybercrime, so that collectively we create a safe and secure online environment.

We are the Home Team, keeping Singapore safe and secure