For discussion
on 6 December 2016

Legislative Council Panel on Security

Measures to combat technology crimes and proposed creation of a permanent Chief Superintendent of Police post of the Cyber Security and Technology Crime Bureau

PURPOSE

This paper –

(a) outlines the strategy and measures of the Hong Kong Police Force (HKPF) to address cyber security threats and combat technology crimes; and

(b) seeks the Panel's endorsement on HKPF's proposal to create a permanent post of Chief Superintendent of Police (CSP) (PPS 55 or D1 equivalent) to head the Cyber Security and Technology Crime Bureau (CSTCB).

MEASURES TO COMBAT TECHNOLOGY CRIMES

Cyber Security Threats

2. With information technology becoming an indispensable part of our lives, the world is also exposed to much higher risks of cyber security threats. In the past year in particular, there were a number of high-profile cyber attacks targeting financial institutions and critical infrastructures. With over one million daily global web attacks in 2015, cyber security and technology crime has become a major challenge facing law enforcement agencies around the world. For example, the hacking of the SWIFT financial platform in April 2016 has caused a loss of US$81 million to the Bangladesh Central Bank. Other banks in Vietnam, Philippines, Ecuador and Hong Kong have also been under similar attacks. In December 2015, cyber criminals struck the power grid of Ukraine resulting in a blackout affecting a quarter of a million people. The industry control systems installed by power plants of other countries, including those in Hong Kong, could be the next target.

3. The Symantec 2016 Internet Security Threat Report indicated that Hong Kong had climbed from 8th to 7th place in the regional threat ranking for Asia Pacific. According to Kaspersky's Security Bulletin 2015, 34.2% of user computers were subject to at least one web attack during the year and more than 750 000 computers worldwide were compromised by ransomware in 2015. The Threat Report of Nexusguard also reported that the number of Distributed Denial of Service (DDoS) attacks increased 43% to more than 34 000 attacks in the Asia-Pacific Region in the first half of 2016, and the largest increase was observed in Hong Kong accounting for a 57% rise in attacks. In addition to these threats, cyber security experts also predicted that malware attack against mobile phones and Internet-of-Things such as webcams, smart TVs, etc. would witness an upsurge and create a huge concern on cyber security. Locally, the Hong Kong Computer Emergency Response Team[1] received 4 928 cyber security incident reports in 2015, representing a 500% increase since 2010.

Technology Crime Trend

4. In Hong Kong, the annual number of local reports of technology crimes has increased significantly by 24 times from 272 cases in 2002 to 6 862 in 2015. In 2016 (as at September), the number of cases has already hit 4 537. Over the past six years, the respective annual financial losses have also increased by 30 times from $60 million in 2010 to $1.8 billion in 2015. In 2016 (as at September), the loss is around $1.87 billion.

5. In recent years, technology crime cases received by the HKPF mainly include offences related to online games, online business frauds, unauthorised access to computer systems and other technology crimes. Figures of technology crime cases received by the HKPF in the past five years are in **Enclosure 1**.

Strategies and Measures to Tackle the Challenges

6. To strengthen the HKPF's capability in combating technology crimes and handling cyber security incidents, the Chief Executive announced in his Policy Agenda 2014 the upgrading of the HKPF's Technology Crime Division (TCD) to form a CSTCB. Following the establishment of CSTCB in January 2015, tremendous efforts have been made to enhance and expand the HKPF's capability in the following areas –

[1] Managed by the Hong Kong Productivity Council, Hong Kong Computer Emergency Response Team Coordination Centre is the centre for coordination of computer security incident response for local enterprises and Internet Users. Its missions are to facilitate information disseminating, provide advices on preventive measures against security threats and to promote information security awareness.

(a) detecting syndicated and highly sophisticated technology crimes and conducting proactive intelligence-led investigations;

(b) providing assistance to critical infrastructures in conducting timely cyber threat audits and analyses to prevent and detect cyber attacks against them;

(c) enhancing incident response capability to major cyber security incidents or massive cyber attacks;

(d) strengthening thematic researches on cyber crime trend and mode of operation, vulnerabilities of computer systems and development of malware;

(e) strengthening partnership with local stakeholders and overseas law enforcement agencies in information exchange and sharing of best practices to counter prevalent technology crimes and cyber threats; and

(f) developing new training programmes on cyber security and technology crimes.

7. To enhance coordination of the Police resources for combating technology crimes and to further increase the awareness of the public on cyber security, the HKPF has continued to set combating technology crime as one of its Operational Priorities, and strived to enhance cyber security and combat technology crime in the following three ways:

(a) Promote public awareness of computer and cyber security as well as the risks associated with social media through a multi-agency approach. CSTCB organizes various publicity items including seminars and multimedia programmes for the general public. It also coordinates annual cyber security events with Government departments and public bodies for stakeholders to exchange cyber security knowledge in the form of recognition, seminar, workshop and conference.

(b) Enhance cooperation with other law enforcement agencies to target technology crime. CSTCB works hand-in-hand with its counterparts in other jurisdictions to prevent, disrupt and investigate cybercrimes. CSTCB will also be hosting the “Cyber Security Summit 2017”, which is an annual event to bring together the professionals from IT industry, Government departments and

law enforcement agencies around the globe to share their experiences in the cyber security field in Hong Kong.

(c) Improve coordination and sharing of expertise in handling and investigating technology crime. To strengthen the competence in cyber crime investigation, CSTCB regularly organises professional trainings for local and overseas law enforcement counterparts. For instance, CSTCB will organise in Hong Kong the "Cybercrime Investigation Training for Eurasian Region" with the INTERPOL in December 2016 to enhance the capabilities of investigators in handling cybercrime.

8. In view of the importance of cyber security, the Hong Kong Monetary Authority (HKMA) has recently launched for the banking system a Cybersecurity Fortification Initiative (CFI), which serves to raise the resilience of the banking system to a level commensurate with Hong Kong's position as the leading international financial centre in Asia. On the policing side, CSTCB has recently launched two new initiatives, namely, the Cyber Range and the Cyber-attack Intelligence Sharing Platform, to address the dynamic cyber threat landscape and the evolution of new and complex cyber attack techniques. The Cyber Range is a facility which can mimic the Internet environment in an enclosed network, allowing the simulation of cyber attacks and technology crime scenes for research and training purposes. The Cyber-attack Intelligence Sharing Platform is a multi-purpose platform which collects and analyses information on cyber attacks from cyber security organisations for dissemination to various local and overseas stakeholders. It will work in collaboration with the Cyber Intelligence Sharing Platform developed by the HKMA as part of the CFI to facilitate the sharing of intelligence on cyber attacks. CSTCB is also preparing a large-scale Cyber Security Drill to strengthen the overall capabilities of local critical infrastructures in responding to cyber security incidents, enhance the existing communications with overseas counterparts as well as intensify the existing protection of the cyber environment of Hong Kong. On top of the above, CSTCB is organising the Cyber Security Professionals Awards to bring together cyber security experience and good practices of various prominent sectors in Hong Kong to jointly promote cyber security awareness and tackle emerging cyber threats.

PROPOSED CREATION OF A PERMANENT CSP POST AS CSTCB'S COMMANDER

9. CSTCB, with all its work as outlined in paragraphs 6 to 8 above and with a staff size of 238 officers, currently lacks a head at directorate level.

Unlike all other bureaux of HKPF involved in the investigation of crimes under the Crime Wing, including the Commercial Crime Bureau, Narcotics Bureau, Criminal Intelligence Bureau, and Organized Crime and Triad Bureau, which are all headed by a CSP, CSTCB is currently headed only by an Senior Superintendent of Police (SSP).

10. As at 1 November 2016, CSTCB has an establishment of 238 (including 226 disciplinary posts), which are all non-directorate posts. The organisational chart of CSTCB is at **Enclosure 2**. Having regard to the number of disciplinary posts of other Crime Bureaux headed by CSPs (as at April 2016, 368 for Narcotics Bureau, 272 for Commercial Crime Bureau, 109 for Organized Crime and Triads Bureau), the comparable size and multiple-layer rank hierarchy of CSTCB, its wide range of duties as well as increasing quantum and complexity of work, a commander at CSP level will be of paramount importance in steering the Bureau, ensuring sufficient guidance and overseeing the management of the Bureau, especially in the areas set out in paragraphs 11 to 16 below. The job description of the proposed CSP CSTCB post is at **Enclosure 3**. The organisational chart of the HKPF after the proposed creation of the subject CSP post is at **Enclosure 4**.

Charting CSTCB's Long-term Development to Fulfil its Mission

11. Dedicated attention and strategic planning to tackle the fast growing technology crime trend is a key operational priority of the HKPF. To take forward such a mission, CSTCB requires high-level steer at the directorate level to devise effective strategies to tackle the challenges referred to in paragraphs 2 to 5 above and ensure their smooth implementation. The strong leadership of a directorate officer with extensive knowledge, exposure and vision in crime prevention and control will be especially vital having regard to the transnational nature and wide variety of crimes committed through the Internet (e.g. online shopping fraud, email scam, deception, money laundering, blackmail associated with naked chat, child pornography, etc.). Otherwise, it would be difficult for CSTCB to formulate strategies and steer management issues such as capacity building, establishment of partnership with local critical infrastructures, cooperation with local and overseas law enforcement agencies and service providers, and allocation and deployment of resources.

Coordinating Responses to Technology Crimes and Cyber Attacks

12. The role and function of CSP CSTCB to co-ordinate matters in relation to cyber security and technology crimes will be essential in view of the increasingly sophisticated technology crimes and cyber attacks as well as the increasing size of the population of Internet users in Hong Kong. Hong Kong

has to be well-prepared for any real and imminent threat of cyber attacks against its critical infrastructures; and any under-preparedness in terms of timing and scope will put Hong Kong to a vulnerable position. To prepare for and in the event of a major cyber attack against local critical infrastructure or technology crimes involving extensive cross-jurisdiction elements that take place in Hong Kong, CSP CSTCB has a critical role to play in assisting the HKPF in making high-level, time-sensitive decisions. Apart from engaging other police formations with dedicated functions during major cyber attacks against critical infrastructures in Hong Kong and stipulating the objectives, policies and long-term strategies for policing technology crimes, CSP CSTCB will be responsible for coordinating joint operations with local and overseas law enforcement agencies, government departments, and other stakeholders for exchanging intelligence and preserving digital evidence that could assist investigation.

13. Without the CSP CSTCB, there is no appropriate officer within the HKPF having the authority, experience and global perspective to lead local and international efforts for providing immediate response to a major attack and handling its aftermath properly. Any further delay in creating the CSP post will seriously impede HKPF's as well as Hong Kong's response to cyber attacks, making Hong Kong extremely vulnerable to cyber criminals to launching cyber attacks against or through our information technology infrastructures.

Strategic Planning, Monitoring and Execution of New Initiatives

14. The new initiatives as mentioned in paragraph 8 above involve significant resources and require strategic planning, monitoring and execution. It is necessary to have in place an officer at directorate level to lead and oversee these initiatives, as well as to implement, review, improve and sustain their development in an effective and efficient manner.

Maintaining Close Liaison with Local and Overseas Stakeholders

15. Globally, cyber security and technology crimes are fast evolving and transcend traditional jurisdictional boundaries. As such, it is one of CSTCB's core businesses to establish close liaison with local and overseas law enforcement agencies for combating cross-border technology crimes and exchanging experience. Whilst an SSP is expected to conduct cross-boundary tactical operations against technology crimes, it is necessary to resort to the steer from a directorate officer at CSP rank to negotiate and undertake collaboration with various stakeholders at senior level. This is especially the case when the interdiction of technology crime involves implementation of

strategic changes, e.g. rationalisation of banking security system, behavioural change of online users, recommendation of redesigning the computer systems of critical infrastructures, etc. There is therefore a genuine need for a directorate officer to act as the HKPF's representative in high-level working groups, conferences and visits to establish collaboration networks with commanding officers of cyber security and technology crime units worldwide. In terms of capability, experience and exposure, CSP CSTCB is of a rank commensurate with the importance of this mission, and will play a crucial role in taking charge of the engagement with overseas organisations, such as the INTERPOL and the G7 High Tech Crime Sub-group.

16. In general, the rank of officers leading overseas cyber crime units is at least equivalent to the rank of CSP of the HKPF. For example, the National Cyber Crime Unit of the National Crime Agency in the United Kingdom is led by an officer in the rank of Deputy Director; the High Tech Crime Operations of the Australian Federal Police and the Cybercrime Command within the Criminal Investigation Department of the Singapore Police Force are led by an officer in the rank of Assistant Commissioner.

ALTERNATIVES CONSIDERED

17. We have critically examined the possibility of redeployment of existing directorate officers in the HKPF to take up the work of the proposed post. At present, there are 46 CSP posts established under the five departments of the HKPF, i.e. Operations, Crime and Security, Personnel and Training, Management Services, and Finance, Administration and Planning. Since all CSP officers are fully committed to duties in their respective subject areas, internal redeployment is operationally infeasible without adversely affecting the discharge of their schedules of duties.

FINANCIAL IMPLICATIONS

18. The proposed creation of the CSP post will bring about an additional notional annual salary cost at mid-point of $1,663,200. The additional full annual average staff cost of the proposal, including salaries and staff on-cost, is $2,634,000. There is sufficient provision in the 2016-17 Estimates to meet the cost of the proposed creation of the CSP post. We will also reflect the resources requirements in the Estimates of subsequent years.

ADVICE SOUGHT

19. The subject on the creation of the CSP CSTCB post was discussed by the Legislative Council Panel on Security on 3 June 2014 and the Establishment Subcommittee (ESC) on 11 March and 29 April 2015. The Government re-submitted the proposal to ESC in June 2016 but discussion could not commence before the expiry of the last Legislative Council term.

20. CSTCB has a pressing need for strong and focussed leadership to perform fully and effectively as a separate bureau, especially in view of the magnitude, complexity and sensitivity of CSTCB's work as described above. Subject to Members' views, we plan to submit the proposal to ESC in the first quarter of 2017**.**

Security Bureau
November 2016

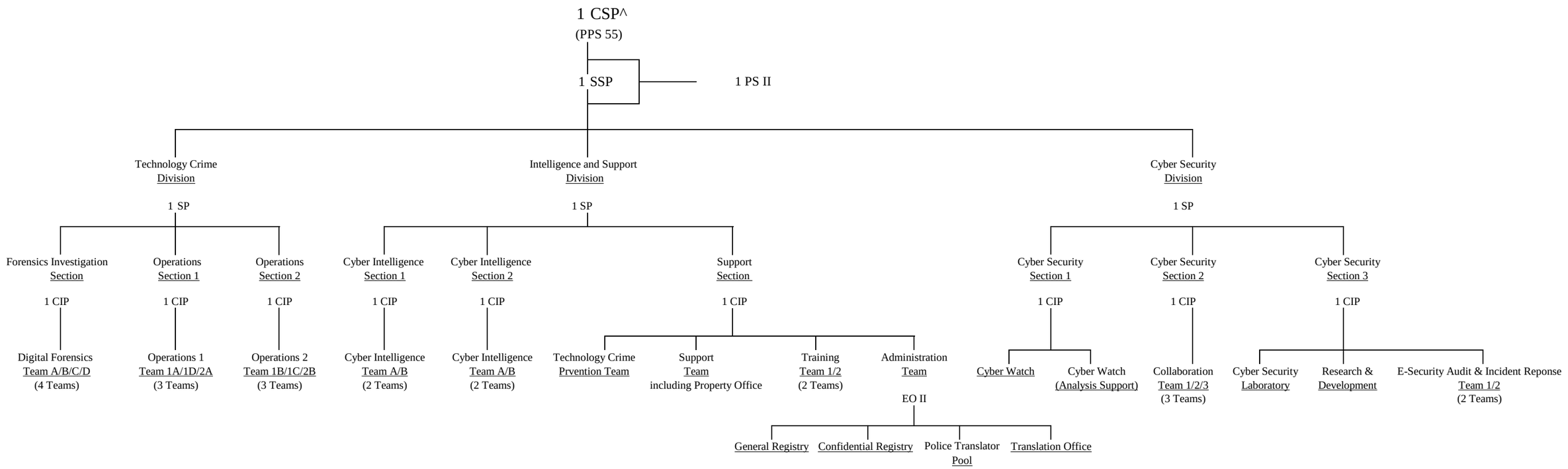
Enclosure 1

Technology crime figures from 2012 to September 2016

Case nature	2012	2013	2014	2015	2016 (As at 30 Sept)
Online game-related	380	425	426	416	304
Online business fraud	1 105	1 449	2 375	1 911	1 217
Unauthorised access to computers	1 042	1 986	1 477	1 223	847
Other Nature	488	1 273	2 500	3 312	2 169
(i) Miscellaneous Fraud	*225*	*435*	*1 436*	*1 733*	*1 133*
(ii) Child Pornography	*28*	*41*	*38*	*53*	*27*
(iii) DDoS Attacks	*25*	*3*	*29*	*35*	*4*
(iv) E-banking	*5*	*40*	*17*	*3*	*2*
(v) Naked Chat	*Not available*	*Not available*	*638*	*1 098*	*588*
(vi) Others	*205*	*754*	*342*	*390*	*415*
Total	**3 015**	**5 133**	**6 778**	**6 862**	**4 537**
Loss (in million $)	**340.4**	**916.9**	**1,200.7**	**1,828.9**	**1,865.2**

Enclosure 2

Organisation Chart of the Cyber Security and Technology Crime Bureau, Hong Kong Police Force



^ Proposed creation of one Chief Superintendent of Police post.

Enclosure 3

Job Description
Chief Superintendent of Police,
Cyber Security and Technology Crime Bureau
Hong Kong Police Force

Rank **:** Chief Superintendent of Police (PPS 55)

Responsible to **:** Assistant Commissioner of Police, Crime Wing

Main duties and responsibilities –

(i) To command the operation and development of the Hong Kong Police Force (HKPF)'s cyber security and technology crimes capabilities.

(ii) To ensure a high standard of duty performance and discipline from personnel under his command.

(iii) To devise strategies in line with the Force's Strategic Directions and Commissioner of Police's Operational Priorities to ensure effective deployment of resources to meet policing requirements for combating technology crimes and cyber security incidents.

(iv) To represent the HKPF in the effective collaboration and co-ordination among various local and international stakeholders in addressing cyber security and technology crimes issues.

(v) To ensure officers are effectively and efficiently trained in order to tackle cyber security and technology crimes related investigations.

(vi) To monitor and tackle cyber security and technology crimes developments both within and outside Hong Kong which may have an impact on policing priorities and activities.

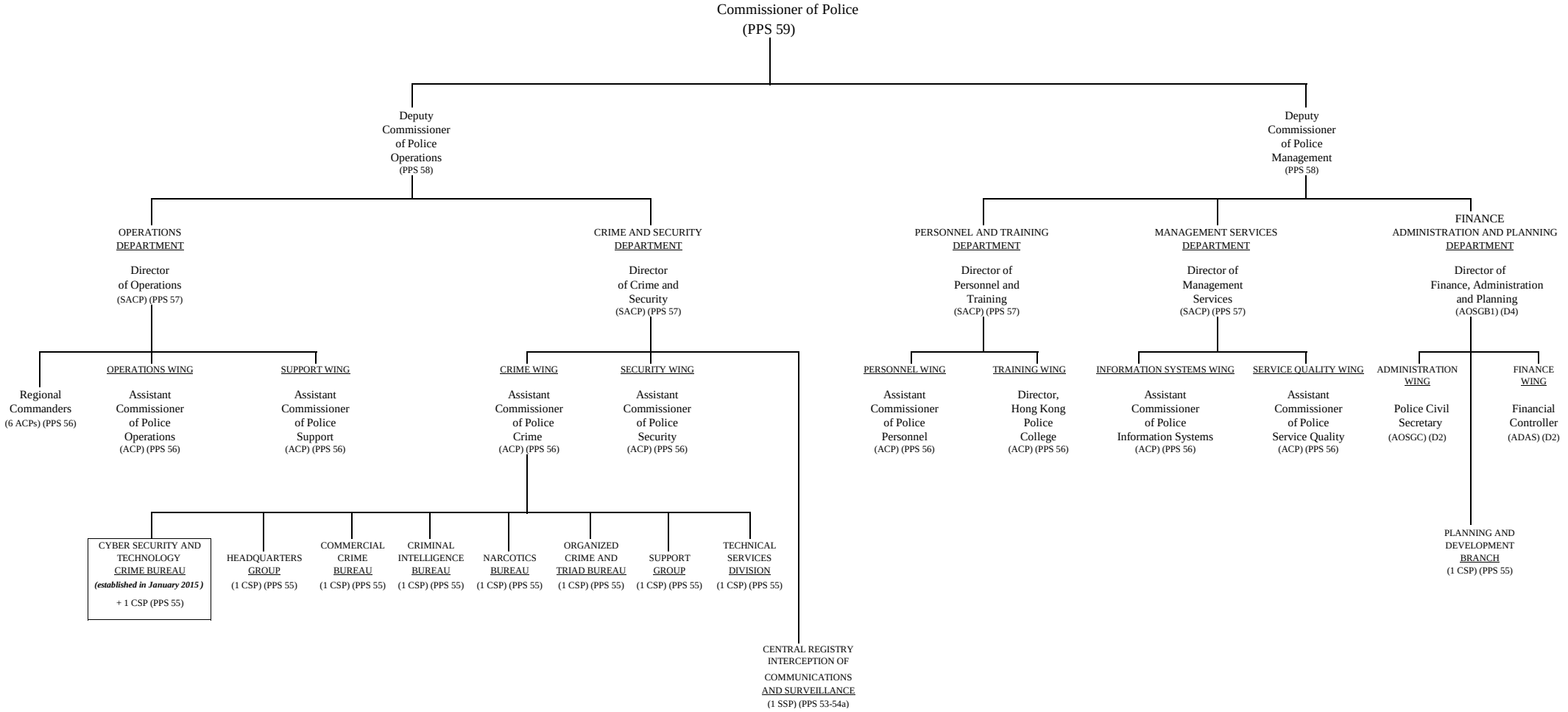
(vii) To engage other police formations with dedicated functions during major cyber attack incidents against critical infrastructure in Hong Kong.

(viii) To exercise personnel management and disciplinary functions as delegated by Police Headquarters.

(ix) To review objectives, policies and implementation plan with other stakeholders for aligning responses in addressing the risks of cyber threat to the computer systems of critical infrastructures in Hong Kong.

Enclosure 4

Organisation Chart of Hong Kong Police Force



Legend

ACP	-	Assistant Commissioner of Police
ADAS	-	Assistant Director of Accounting Services
AOSGB1	-	Administrative Officer Staff Grade B1
AOSGC	-	Administrative Officer Staff Grade C
CSP	-	Chief Superintendent of Police
PPS	-	Police Pay Scale
SACP	-	Senior Assistant Commissioner of Police
SSP	-	Senior Superintendent of Police

☐ - One CSP post proposed to be created as CSP Cyber Security and Technology Crime Bureau