For discussion **EC(2016-17)17**
on 14 June 2016

ITEM FOR ESTABLISHMENT SUBCOMMITTEE OF FINANCE COMMITTEE

HEAD 122 – HONG KONG POLICE FORCE
Subhead 000 Operational expenses

Members are invited to recommend to Finance Committee the creation of the following permanent post in the Hong Kong Police Force with effect from the date of approval by the Finance Committee –

1 Chief Superintendent of Police
(PPS 55) ($134,300 - $147,100)

PROBLEM

The Commissioner of Police needs dedicated staffing support at the directorate level to lead the Cyber Security and Technology Crime Bureau (CSTCB), which has been upgraded from the former Technology Crime Division (TCD) since January 2015, to strengthen the Hong Kong Police Force (HKPF)'s capability of preventing and combating technology crimes and responding to cyber security incidents.

PROPOSAL

2. We propose to create a permanent post of Chief Superintendent of Police (CSP) (PPS 55 or D1 equivalent) in the Crime Wing of the HKPF to head the CSTCB, with effect from the date of approval by the Finance Committee, to oversee the formulation of long-term objectives and strategies, and to command the operation and development of the CSTCB.

/JUSTIFICATIONS …..

JUSTIFICATIONS

Upgrading of TCD to CSTCB

3. Today, Hong Kong has one of the highest concentrations of Wi-Fi hotspots in the world, and 97% of households are able to access broadband services. With a high mobile phone penetration rate of 228.7%, which is expected to grow further, individuals, corporations and critical infrastructures are all prone to technology crimes and cyber security threats. The TCD of the Commercial Crime Bureau (CCB) was responsible for preventing, detecting and tackling technology crimes, as well as responding to cyber security incidents.

4. The Chief Executive announced in his Policy Agenda 2014 the upgrading of the HKPF's TCD to form a CSTCB. With the establishment of the CSTCB in January 2015, the HKPF's capability in combating technology crimes and handling cyber security incidents has been greatly enhanced and expanded in the following areas –

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

(b) providing assistance to critical infrastructures in conducting timely cyber threat audits and analyses in preventing and detecting 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.

5. Currently, the bureaux which are involved in the investigation of crimes under the Crime Wing, including the Crime Wing Headquarters, the Crime Support Group, Commercial Crime Bureau, Narcotics Bureau, Criminal Intelligence Bureau, and Organized Crime and Triad Bureau, are all headed by a CSP. CSTCB, with a staff size of 238 officers and work complexity comparable to all other bureaux, is currently headed only by a Senior Superintendent of Police (SSP).

/**Growing** …..

Growing Challenges

6. TCD, the predecessor of CSTCB, was first established in 2002 when there were only 272 reports of technology crimes. 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 April), the number of cases has already hit 1 871. 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 April), the loss is around $1.1 billion. CSTCB needs to cope with the challenges of the increasingly sophisticated technology crimes and cyber security threats by strengthening the overall capability of the HKPF in combating technology crimes and handling cyber security incidents.

7. 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. 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. 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 received 4 928 cyber security incident reports in 2015, representing a 500% increase since 2010.

8. There is a pressing need to strengthen the HKPF's capability in combating technology crimes and handling cyber security incidents. Without a directorate officer with extensive experience in crime prevention and control, 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. CSTCB requires strong and focussed leadership to perform fully and effectively as a separate bureau.

Need for a permanent CSP post as the commander of CSTCB

9. Dedicated attention and strategic planning to tackle the fast growing technology crime trend is a key operational priority of the HKPF. In view of the magnitude, complexity and sensitivity of the work involved, the new CSTCB needs high-level steer at directorate level to devise effective strategies and ensure their

/smooth …..

smooth implementation, and take forward the aforementioned enhanced services. Having considered the transnational nature and the 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.), it is necessary to create a post at CSP rank (to be designated as CSP CSTCB) with an officer possessing the necessary professional police knowledge, exposure and vision to give dedicated attention to commanding the operation of the CSTCB.

10. The CSP CSTCB will be responsible for commanding the operation and development of the CSTCB, engaging other police formations with dedicated functions during major cyber attack incidents against critical infrastructures in Hong Kong and stipulating the objectives, policies and long-term strategies for policing technology crimes. Apart from that, the CSP CSTCB will engage in collaboration and co-ordination with various local and overseas stakeholders in addressing technology crimes and cyber security issues. In view of the increasingly sophisticated technology crimes and cyber attacks as well as the increasing size of the population of users of the Internet in Hong Kong, the role and function of CSP CSTCB to co-ordinate the matters in relation to cyber security and technology crimes will be essential.

11. Without a dedicated CSP, CSTCB has to report to other CSPs within Crime Wing for high-level steer on, for example, allocation of resources. Since those CSPs are already fully engaged in their respective aspect of policing duties, it is practically impossible for them to offer full time, continuous and prolonged supervision for CSTCB without adversely affecting the operational efficiencies of their bureaux. This situation is clearly unsustainable. If left unchecked, this would hamper the management of Crime Wing, in particular the roles and responsibilities of CSPs within Crime Wing, and the effective supervision on the development of CSTCB.

12. A dedicated CSP in CSTCB is urgently required to provide full-time high-level steer for CSTCB. The CSP will need to chart the development of the bureau, and ensure the effectiveness of the HKPF in driving the continuous building of capacities in the two distinct and highly professional streams, i.e. cyber security and technology crime. In the event of large-scale cyber attacks or technology crimes involving extensive cross-jurisdiction elements that take place in Hong Kong, CSP CSTCB will have to play a critical role to assist the HKPF in making high-level, time-sensitive decisions, as well as to effectively coordinate 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. 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 …..

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. The 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 cyber environment of Hong Kong. All the above new initiatives involve significant resources and require strategic planning, monitoring and execution. A senior police officer at directorate level to oversee these initiatives, and to review, improve and sustain their development is necessary.

14. 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 for 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. As a result, there is a genuine need for a directorate officer to act as the HKPF's representative in high-level working groups, conferences and visits to establish the collaboration network with the 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.

15. In general, the rank of officers leading overseas cyber crime units is 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 …..

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.

16. The job description of the proposed CSP CSTCB post is at Enclosure 1. The organisational chart of the HKPF after the proposed creation of the subject CSP post is at Enclosure 2.

Encl. 1
Encl. 2

Non-directorate Support

17. For the establishment of the new CSTCB, TCD has been hived off with the permanent redeployment of 106 posts[1] to the CSTCB. An additional 74 non-directorate posts[2] have been created by January 2015. Upon establishment of CSTCB, two divisions, namely, the Cyber Security Division and Technology Crime Division, were created. The former division is to enhance cyber threat response and capability of conducting intelligence-led investigation, to strengthen research on cyber crime trend and collaborate with local stakeholders and overseas law enforcement agencies. The latter division is to enhance the capability of HKPF in investigating large-scale cyber attacks and cases involving advanced technology.

18. In 2015-16, the CSTCB is reinforced with additional manpower of 58 non-directorate posts to enhance the HKPF's capabilities to mitigate cyber security risks and investigate technology crime cases. In July 2015, the Intelligence and Support Division was set up in CSTCB for collecting, processing, analysing and evaluating intelligence and activities relating to technology crime and cyber security incidents. Moreover, a new Cyber Watch Analysis Support Team was established in Cyber Security Division. Manpower is also enhanced to beef up the function in response to cyber security incidents and to handle technology crime.

19. As at 1 April 2016, the CSTCB has an establishment of 238 (including 226 disciplinary posts), which are all non-directorate posts. The organisational chart of the CSTCB is at Enclosure 3. Having regard to the number of disciplinary posts[3] of other Crime Bureaux headed by CSPs (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, we consider that a commander at CSP level is essential for ensuring sufficient guidance and management within CSTCB.

Encl. 3

/Government's …..

---

1 The 106 posts include 98 posts from the TCD, and four civilian posts and four disciplinary posts from CCB.

2 Comprising 71 disciplined officers ranked from Police Constable to SSP and three civilian staff.

3 As at April 2016.

Government's Responses to Major Concerns

20. Our responses to issues raised by Members during the meetings of the Security Panel on 3 June 2014, the ESC on 11 march 2015 and 29 April 2015 and the briefing for ESC Members on 4 December 2015 have been summarised in Enclosure 4 for Members' reference.

Encl. 4

ALTERNATIVES CONSIDERED

21. 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. The duties and existing work priorities of the 46 CSP posts in the HKPF are at Enclosure 5. 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.

Encl. 5

FINANCIAL IMPLICATIONS

22. 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 $2,557,000.

23. There is sufficient provision in the 2015-16 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.

PUBLIC CONSULTATION

24. We consulted the Legislative Council Panel on Security (Panel) on the staffing proposal on 3 June 2014. Panel Members generally supported the proposal and recognised the importance of combating technology crimes and enhancing cyber security through the setting up of the CSTCB. Some Panel Members requested further information on the manpower of CSTCB and its scope of work. We have provided the information to Members vide our letter on 8 September 2014.

25. This item was discussed at the meetings of this Subcommittee on 11 March 2015 and 29 April 2015, during which members asked for statistical information and raised questions on various issues, including the manpower and work of CSTCB and its Cyber Security Centre, and the trend of cyber security and

/technology …..

technology crimes. In response, we provided further information in our letters to this Subcommittee on 31 March 2015 and 13 July 2015. In April 2015, this Subcommittee did not render its support to the proposal.

26. To enable Members of this Subcommittee to have a more in-depth understanding of the work of the CSTCB, we arranged a briefing session on 4 December 2015.

ESTABLISHMENT CHANGES

27. The establishment changes in the HKPF for the past four years are as follows –

Establishment (Note)	**Number of Posts**			
	As at 1 April 2016	**As at 1 April 2015**	**As at 1 April 2014**	**As at 1 April 2013**
A*	72#	72	72	71
B	3 198	3 138	3 065	2 958
C	30 453	30 096	30 051	30 029
Total	**33 723**	**33 306**	**33 188**	**33 058**

Note:
A - ranks in the directorate pay scale or equivalent
B - non-directorate ranks, the maximum pay point of which is above MPS point 33 or equivalent
C - non-directorate ranks, the maximum pay point of which is at or below MPS point 33 or equivalent
* - excluding supernumerary posts created under delegated authority
\# - as at 1 April 2016, there was no unfilled directorate post in the HKPF

CIVIL SERVICE BUREAU COMMENTS

28. The Civil Service Bureau supports the proposed creation of a permanent CSP post for the CSTCB. The grading and ranking of the proposed post are considered appropriate having regard to the level and scope of the responsibilities required.

/**ADVICE** …..

ADVICE OF THE STANDING COMMITTEE ON DISCIPLINED SERVICES SALARIES AND CONDITIONS OF SERVICE

29. The Standing Committee on Disciplined Services Salaries and Conditions of Service has advised that the grading proposed for the permanent directorate post is appropriate.

Security Bureau
June 2016

Enclosure 1 to EC(2016-17)17

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.

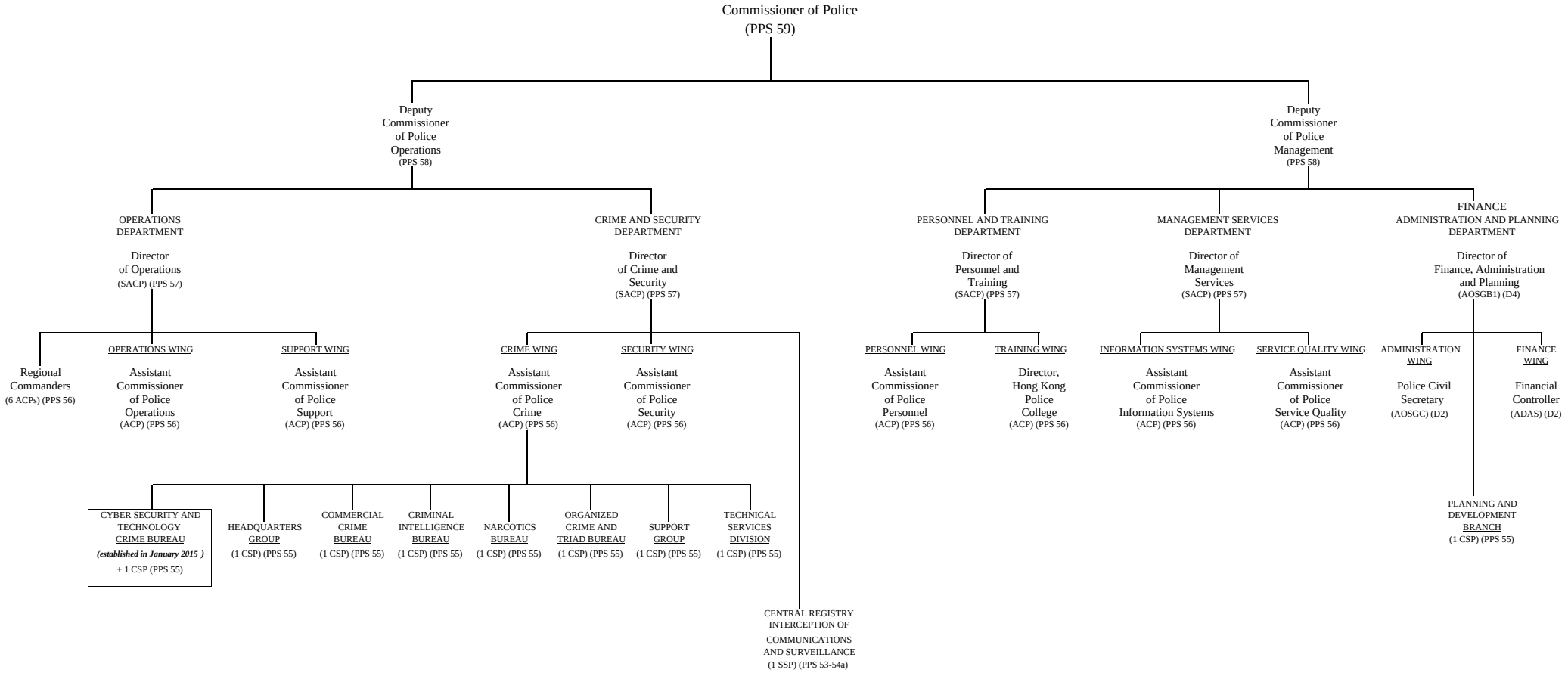
(vii) To engage other police formations with dedicated functions during major cyber attack incidents against critical infrastructure in Hong Kong.

(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 2 to EC(2016-17)17

Organisation Chart of Hong Kong Police Force



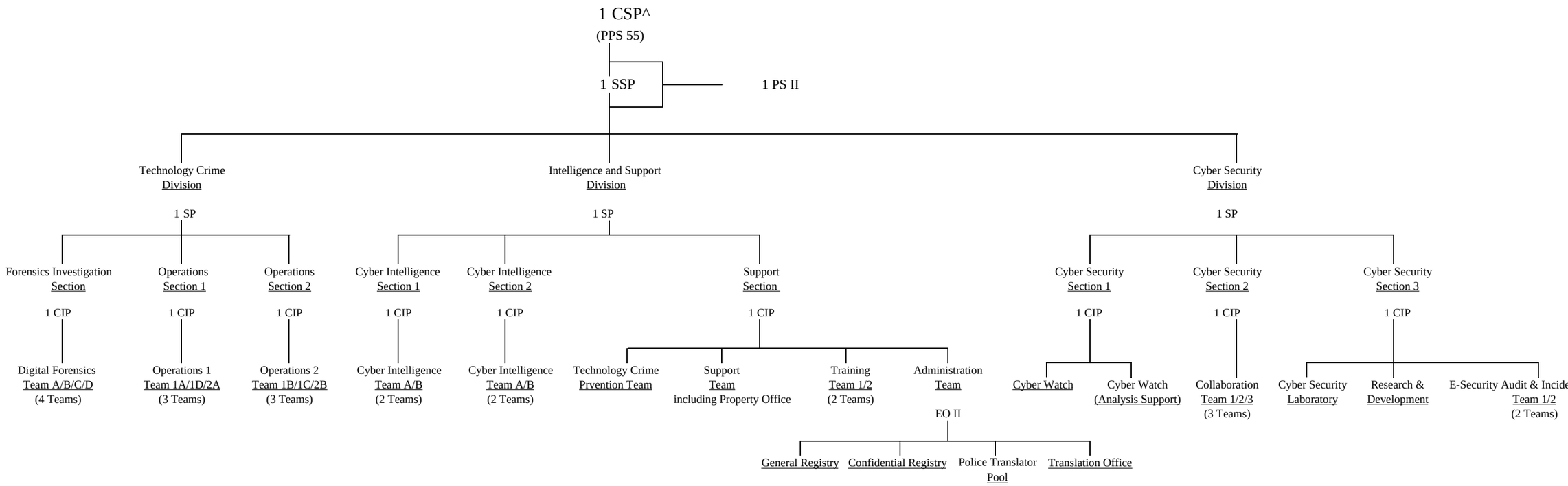
Legend

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

Enclosure 3 to EC(2016-17)17

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



^ Proposed creation of one Chief Superintendent of Police post.

Government's response to major issues raised by Members during the meetings of the Security Panel on 3 June 2014, the Establishment Sub-committee (ESC) on 11 March 2015 and 29 April 2015 and the briefing for ESC Members on 4 December 2015

Technology Crime Trend

In recent years, technology crime cases received by the Police mainly include offences related to online games, online business frauds, unauthorised access to computer systems and other technology crimes.

2. Online game-related offences include those directly or indirectly associated with the loss of computer data solely used for playing online games. Common examples are stealing gaming data from others' online game accounts and obtaining gaming data (e.g. virtual weapons for online games) by deceptive means. Online business frauds include those operated via online shopping or trading platforms, such as e-auction scams, online shopping frauds and misuse of credit cards. Unauthorised access to computers includes unauthorised use of computers, such as computer hacking, abusive use of Internet/email accounts and email frauds. Figures of technology crime cases received by the Police in the past six years are at Table 1.

Table 1: Technology crime figures from 2010 to 2015

Case nature	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**
Online game-related	407	383	380	425	426	416
Online business fraud	623	888	1 105	1 449	2 375	1911
Unauthorised access to computers	337	567	1 042	1 986	1 477	1223
Others[#]	276	368	488	1 273	2 500	3312
Total	**1 643**	**2 206**	**3 015**	**5 133**	**6 778**	**6 862**

[#] Other technology crimes include miscellaneous online frauds, online banking frauds, blackmail, distributed denial-of-service (DDoS) attacks, child pornography, cases involving sexual offences, and criminal intimidation.

/CSTCB's …..

CSTCB's Scope of Work, Manpower and Performance Indicators

3. From 2010 to 2015, the number of reports of technology crimes had increased fourfold and the respective financial loss had increased by almost 29 times, against the background of a decrease in the overall crime rate since 1997. There is a practical need for the Police to strengthen their manpower to cope with the rising and evolving technology crime trend and offer sufficient protection to the public. To enable the Police to better protect the security of the information systems of critical infrastructure, and to enhance the Police's capability in preventing and combating technology crimes, the Police upgraded the Technology Crime Division to the 'Cyber Security and Technology Crime Bureau' (CSTCB) in January 2015. CSTCB is responsible for a wide variety of tasks with a significant number of staff involved in enhancing cyber security, such as handling DDoS attacks, and new tasks, such as undertaking thematic researches, and monitoring the development of malwares, etc. Besides, it is responsible for collaboration and co-ordination with local stakeholders (such as critical infrastructures) and international stakeholders (such as the INTERPOL and law enforcement agencies in the G7 High Tech Crime Sub-group) in addressing technology crimes and cyber security issues. Police officers engaged in such collaborative work are required to abide by the laws of Hong Kong. CSTCB is also responsible for carrying out thematic researches on cyber crime trend and mode of operation, such as new hacking techniques and computer worms.

4. The establishment, including disciplined services and civilian staff, of individual sections under CSTCB is tabulated below –

Table 2: Establishment of CSTCB (as at 1 April 2016)

	Establishment
Headquarters	2
Technology Crime Division	1
Forensic Investigation Section	45
Operations Section 1	29
Operations Section 2	25
Cyber Security Division	1
Cyber Security Section 1	31
Cyber Security Section 2	15
Cyber Security Section 3	27
Intelligence and Support Division	1
Cyber Intelligence Section 1	17
Cyber Intelligence Section 2	17
Administrative support	27
Total	**238**

/5. …..

5. Indicators have been developed for assessing the work and performance of CSTCB, including the number of reports and detection rate of cyber and technology crimes, the number of cyber threat audits conducted for the computer systems of critical infrastructures, the number of contingency plans developed and emergency drills conducted with operators of those critical infrastructures, as well as the number of botnets, malicious programmes and phishing websites detected and responded to by CSTCB.

Qualification requirements for the post of Chief Superintendent of Police (CSP) at CSTCB

6. Given the transnational nature of technology crime and types of offences (such as online shopping frauds, email scams, deception, money laundering, naked chats and publication of child pornography), the head of CSTCB will be taken up by a CSP conversant with policing work, so that he can co-ordinate various tasks and set out the direction of development with an enforcement-led approach. To maintain Hong Kong's overall cyber security and combat technology crimes, the above arrangement will put the Force in a better position to set objectives, devise policies and formulate long-term strategies.

7. The head of CSTCB must possess solid and extensive operational and management skills. He is not required to be an information technology specialist, as he will be supported by officers with relevant computer/information technology qualifications. In fact, the Police have been recruiting officers with relevant computer/information technology qualifications to join CSTCB. At present, 98% of the officers at CSTCB have such qualifications, while the rest of the officers have received internal professional training and possess relevant experience. Some officers also have professional qualifications from SANS Institute which is an internationally renowned provider of cyber security training. In addition, a number of Police officers were certified trainers of the INTERPOL for technology crimes and had assisted in professional training in cyber security and technology crimes for law enforcement agents (LEAs) from Singapore, the Republic of Korea and Thailand. They will be able to provide relevant training to other officers in CSTCB. As for new recruits, they need to have an interest in technology, be creative and possess good acumen in crime investigation.

8. Besides, in collaboration with the Police College, CSTCB organises regular internal professional training programmes which cover topics like technology crime investigation skills and computer forensic examination. Such programmes are offered to maintain CSTCB officers' professional capability in investigation, intelligence gathering and analysis, computer forensic examination

/and …..

and training. Overseas visits are conducted from time to time for officers' participating in training on technology crime investigation skills, digital forensic examination, etc. Apart from gaining international experience, officers may share their experience and insights with other experts of law enforcement agencies in order to acquire the most advanced knowledge.

9. The professional capabilities of the Police in cyber security and combating technology crimes have been recognized internationally. The Senior Superintendent of CSTCB has been the Chairman of the INTERPOL's Eurasian Working Group on Cybercrime since 2015, while the former Senior Superintendent of TCD had served as the Chairman of the INTERPOL's Asia-South Pacific Working Party on IT Crime for about ten consecutive years. In addition, some Police officers were certified trainers of the INTERPOL and have assisted in professional training in cyber security and technology crimes for LEAs in Singapore, Fiji, Australia, the Republic of Korea and Thailand.

The Cyber Security Centre

10. The Cyber Security Centre (CSC) plays an important role in defending against and responding to major cyber attacks in Hong Kong. When drawing up security measures for the CSC, the Police have to take into consideration a basket of factors, including data confidentiality requirement, security technologies involved, effective software and hardware required, safety of the operation site and so forth. To ensure their capability in managing cyber security of Hong Kong, the Police must critically and carefully design the CSC's physical and virtual security initiatives. Among such initiatives, the operating procedure, operation, technology and capability of the CSC must be kept strictly confidential to prevent the CSC from becoming a target of hackers' attack or intrusion, as well as to ensure its capability in defending against major cyber attacks.

11. Moreover, the CSC is required to process and analyse sensitive data in its day-to-day operation, including the flow (not the content) of data traffic as well as data in relation to cyber attacks that stakeholders of critical infrastructures (e.g. computer systems of banking and finance services, traffic and maritime services, communication services, public services and government services) are willing to provide. The collaboration between the CSC and such stakeholders is based on a mutual confidentiality agreement.

12. On account of the aforesaid reasons, matters in relation to the CSC are handled by the Police in strict compliance with the 'need-to-know' principle since the full commissioning of the CSC. This principle is of paramount

/importance …..

importance in safeguarding against leakage of the CSC's classified data, including those about the CSC's capability, method, system operation and technology in support of law enforcement.

13. Owing to the CSC's confidentiality and sensitivity, approval of any person's access to the CSC is determined by the Police strictly on a 'need-to-know' basis.

Prosecutions and Convictions in respect of 'Access to Computer with Criminal or Dishonest Intent' under Section 161 of the Crimes Ordinance (Cap. 200)

14. Section 161 of the Crimes Ordinance (Cap. 200) which targets against access to computer with criminal or dishonest intent is effective in combatting illegal acts such as online frauds, illegal access to computers and the use of computers to commit other offences.

15. Section 161(1) of the Crimes Ordinance reads as follows –

Any person who obtains access to a computer –

(a) with intent to commit an offence;
(b) with a dishonest intent to deceive;
(c) with a view to dishonest gain for himself or another; or
(d) with a dishonest intent to cause loss to another,

whether on the same occasion as he obtains such access or on any future occasion, commits an offence and is liable on conviction upon indictment to imprisonment for 5 years.

16. The Police have invoked section 161 for handling cases such as online frauds, illegal access to a computer system, clandestine photo-taking using smart phones in non-public places such as toilets or changing-rooms, online publication of obscene or threatening information, as well as inciting others on the Internet to engage in illegal activities such as hacker groups threatening to launch cyber attacks on the network systems of Hong Kong and inciting others to carrying out the attacks by using hackers' websites or software. Perpetrators of such cases may also be charged with other related crimes at the same time. Figures of prosecution and conviction under section 161 between 2011 and 2015 are set out below.

/Year …..

Year	Number of prosecutions	Number of convictions
2011	34	32
2012	39	32
2013	55	50
2014	86	80
2015	103	93

Note: the year of arrest, prosecution and conclusion of the same case may be different.

17. It has to be noted that the figures in paragraph 16 are the overall prosecution and conviction figures of the offences under section 161. In order to analyse Hong Kong's overall law and order situation and crime trend, and to understand the profile of our criminal justice system, LEAs and the Judiciary maintain various crime-related statistics, such as the numbers of cases and arrestees, as well as the figures of prosecutions, convictions, penalties imposed, etc. in respect of different offences. The figures recorded are the overall figures of various offences, not separate figures for the offences under the respective subsections. LEAs and the Judiciary only maintain the overall figures concerning section 161, but not the breakdown of the respective figures for the four subsections under it.

18. We consider that the law in place is effective in meeting the demand for combating technology crime and safeguarding cyber security and there is no plan for legislative amendments at this stage. Enhancing cyber security as well as combating technology crimes is one of the Police's operational priorities. The Police shall continue to discharge their enforcement duties in a fair, just and impartial manner in accordance with the law.

19. We understand that Secretary for Justice, in his capacity of the Chairman of the Law Reform Commission (LRC), earlier informed the Legislative Council of the LRC's plan to review the relevant laws in relation to cyber crime. The Government will keep in view the development.

Cyber Patrol

20. Similar to conducting patrols on the streets for prevention of crime, it is necessary for the Police to spot and take action against possible criminal activities in the virtual world of the Internet. Information gathered in patrols will enable the Police to allocate resources more aptly in tackling crimes. The level of

/involvement …..

involvement of CSTCB in an investigation would depend on the complexity of the technology crime involved in the case. Officers at CSTCB usually lead the investigation of crimes involving high-end and more complex technologies. For crimes with a low degree of technological element, CSTCB mainly assists the investigation teams in gathering technological evidence or providing advice on technology-related matters. The purpose of Police's cyber patrol is to watch out for criminal activities or criminal intelligence, not political orientations. It should be stressed that the Internet is open to all and hence users are faced with criminal threats as they would in the physical world.

Existing Duties and Work Priorities of
Chief Superintendent of Police Posts in Hong Kong Police Force

At present, there are 72 permanent directorate posts of which 46 are Chief Superintendent of Police (CSP) posts established under the five departments of Hong Kong Police Force (HKPF), viz. Operations, Crime and Security, Personnel and Training, Management Services, and Finance, Administration and Planning. For day-to-day policing, the HKPF is organised into six Police Regions, viz. Hong Kong Island, Kowloon East, Kowloon West, New Territories North, New Territories South and Marine Regions under the charter of the Operations Department. The distribution and the major responsibilities of the CSP posts are as follows –

(A) Operations Department

(i) *Regional Headquarters (6 CSPs)*

Six CSP posts, one for each Regional Headquarters, are established as Deputy Regional Commanders to assist the Regional Commanders (RCs) at Assistant Commissioner of Police (ACP) rank in overseeing all operational, administrative and financial matters within the Region, giving policy directions and command in the Region in the absence of the RC.

(ii) *District Headquarters (19 CSPs)*

19 CSP posts, one for each of the 19 major Police Districts, viz. Central, Eastern, Wan Chai, Western, Kwun Tong, Sau Mau Ping, Tseung Kwan O, Wong Tai Sin, Kowloon City, Mong Kok, Sham Shui Po, Yau Tsim, Border, Tai Po, Tuen Mun, Yuen Long, Kwai Tsing, Sha Tin and Tsuen Wan Police Districts, under the command of the respective RCs are established as District Commanders. Each District Commander, commanding between 350 to 700 staff, is responsible for the effective enforcement of law and order and the prevention and detection of crimes in his District.

(iii) *Support Wing (3 CSPs)*

Three CSP posts are established in Support Wing under the command of ACP Support, with each responsible for the

/unique …..

unique schedule of duties of the three branches of the Support Wing, viz. Support Branch, Traffic Branch Headquarters and Police Public Relations Branch. The Support Branch is responsible for the efficient administration of operational support, formulating and reviewing Force-wide operational policies, procedures and strategies, and the management of the Hong Kong Auxiliary Police Force. The Traffic Branch Headquarters is responsible for strategic planning, formulating and coordinating all traffic enforcement matters and traffic-related initiatives/programmes. The Police Public Relations Branch acts as a bridge between the HKPF and the public by engaging proactively and building long-term constructive relations with the media, the stakeholders and opinion leaders of the community, thereby enhancing the reputation of the HKPF, maintaining public confidence in the Force and leveraging public support for policing activities.

(iv) *Operations Wing (1 CSP)*

One CSP post is established in the Operations Wing under the command of ACP Operations, responsible for the administration and strategic development of the Police Tactical Unit and the Special Duties Unit including the management and provision of adequate and effective training to ensure the best possible readiness for any threats to public order and internal security, emergencies, anti-crime and counter-terrorism operations.

(B) Crime and Security Department

(i) *Crime Wing (7 CSPs)*

Seven CSP posts, one for each of the seven formations of Crime Wing, viz. the Headquarters Group, the Commercial Crime Bureau, the Criminal Intelligence Bureau, the Narcotics Bureau, the Organized Crime and Triad Bureau, the Support Group and the Technical Services Division, are established under the command of ACP Crime. Each formation deals with specific areas of crime and supports frontline crime units.

(ii) *Security Wing (1 CSP)*

One CSP post is established in the Security Wing to assist ACP Security in handling a range of security-related matters including VIP Protection, counter-terrorism, security

/co-ordination …..

co-ordination, internal security and immediate response to any matters or incidents of security interest in accordance with the Government Intelligence Requirements.

(C) Personnel and Training Department

(i) *Personnel Wing (3 CSPs)*

Three CSP posts, one for each of the three branches of Personnel Wing, viz. Conditions of Service and Discipline Branch, Human Resources Branch and Personnel Services and Staff Relations Branch, are established under the command of ACP Personnel and are responsible for a wide range of human resource management functions relating to recruitment, promotion, manpower and succession planning, career development, posting, performance management, discipline, conditions of service, staff relations and welfare matters involving over 28 000 disciplined staff.

(ii) *Training Wing (2 CSPs)*

Two CSP posts are established in the Training Wing to underpin the Director of the Hong Kong Police College in providing formal structured training aimed at vocational, professional and executive development geared to the needs of officers at different stages of their career. They include basic training for recruits, firearms and tactics training for serving officers, local and mainland as well as overseas training programmes in police leadership and management, professional courses on application of information technology in policing, training on criminal investigation and intelligence management, police driving and traffic training, knowledge management, quality assurance and academic accreditation of police training courses.

(D) Management Services Department

Service Quality Wing (3 CSPs)

Three CSP posts are established in Service Quality (SQ) Wing under the command of ACP SQ, each is responsible for the unique schedule of duties of the three branches of the SQ Wing, viz. the Performance Review Branch, the Research and Inspections Branch and the

/Complaints …..

Complaints and Internal Investigations Branch. The Performance Review Branch is responsible for promoting improvements in value-for-money practices and enhancing awareness and pursuance of issues related to service quality. The Research and Inspections Branch is responsible for developing inspection guidelines, and conducting due diligence inspections on frontline Districts and Policy Wing formations, as well as ad hoc thematic inspections or special audits on specific issues of Force-wide concern. The Complaints and Internal Investigation Branch includes the Complaints Against Police Office and the Internal Investigations Office, and is responsible for investigating complaints against police officers and serious disciplinary matters as well as promoting the Integrated Integrity Management Framework to reinforce the Police Force's values of integrity and honesty.

(E) Finance, Administration and Planning Department

The Planning and Development Branch (1 CSP)

One CSP post is established in the Planning and Development Branch of the Finance, Administration and Planning Department. The post is responsible for initiating strategic planning and development of police facilities and capital works projects in support of the Department's Strategic Action Plan and Commissioner's Operational Priorities, formulating policy on matters relating to the department's properties to meet new policing requirements and operational needs.
