For discussion **EC(2016-17)23**
on 4 January 2017

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) ($139,950 - $153,250)

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 in preventing and combating technology crimes and handling 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 CSTCB, with effect from the date of approval by the Finance Committee, to command CSTCB's operation and development, to oversee the formulation and execution of long-term objectives and strategies in tackling the growing challenges in cyber security, as well as to coordinate the Government's responses to technology crimes and cyber attacks.

/**JUSTIFICATIONS** …..

JUSTIFICATION

Upgrading of TCD to CSTCB

3. With information technology becoming an indispensable part of our lives, the world is exposed to much higher risks of cyber security threats. 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 227.8%, which is expected to grow even further, individuals, corporations and critical infrastructures are all prone to technology crimes and cyber security threats.

4. The TCD of the Commercial Crime Bureau (CCB) used to be responsible for preventing, detecting and tackling technology crimes, as well as responding to cyber security incidents. 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 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 –

(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 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 (LEAs) 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.

/**Growing** …..

Growing Challenges

5. 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.

6. 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 have become major challenges faced by LEAs 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 regions, including those in Hong Kong, could be the next target.

7. The Symantec 2016 Internet Security Threat Report indicated that Hong Kong had climbed from the 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 attacks increased by 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 registering 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] (HKCERT) received 5 146 cyber security incident reports in the first ten months of 2016 representing more than 500% increase since 2010. Among those reports, the cases of ransomware record a significant increase, which are fivefold the total reports of the same nature in 2015. Thus, there is a pressing need to strengthen the HKPF's capability in combating technology crimes and handling cyber security incidents.

/**Need** …..

[1] Managed by the Hong Kong Productivity Council, the HKCERT 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 promote information security awareness.

Need for a permanent CSP post as the commander of CSTCB

8. CSTCB has been tasked with the mission to cope with the above-mentioned challenges as posed by the increasingly sophisticated technology crimes and cyber security threats. However, unlike all other bureaux of the HKPF involved in the investigation of crimes under the Crime Wing, including the CCB, Narcotics Bureau (NB), Criminal Intelligence Bureau, and Organized Crime and Triad Bureau (OCTB), which are all headed by a CSP, CSTCB (with 226 disciplinary posts) is currently headed only by a Senior Superintendent of Police (SSP). Having regard to the number of disciplinary posts of other Crime Bureaux headed by CSPs (as at April 2016, 368 for NB, 272 for CCB, 109 for OCTB), 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 9 to 14 below.

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

9. 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 5 to 7 above and ensure their smooth implementation. The strong leadership of a directorate officer with extensive knowledge, exposure and vision in crime prevention and control would 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 LEAs and service providers, and allocation and deployment of resources.

Coordinating Responses to Technology Crimes and Cyber Attacks

10. 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 …..

will expose 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 and 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 LEAs, government departments, and other stakeholders for exchanging intelligence and preserving digital evidence that could assist investigation.

11. 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 the HKPF's as well as Hong Kong's response to cyber attacks, making Hong Kong extremely vulnerable to cyber criminals to launch cyber attack against or through Hong Kong's information technology infrastructures.

Strategic Planning, Monitoring and Execution of New Initiatives

12. 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 …..

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. All the above new initiatives 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

13. 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 LEAs for combating cross-border technology crimes and exchanging experience. Whilst a 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.

14. In general, the rank of officers leading overseas cyber crime units, for example, the National Cyber Crime Unit of the National Crime Agency in the United Kingdom; the High Tech Crime Operations of the Australian Federal Police and the Cybercrime Command within the Criminal Investigation Department of the Singapore Police Force, is higher or equivalent to the rank of CSP of the HKPF.

Current Unsatisfactory Situation

15. As mentioned in paragraph 8 above, the other bureaux involved in the investigation of crimes under the Crime Wing are headed by a CSP. CSTCB requires 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. Without a dedicated CSP, CSTCB, since its inception, has to report to other CSPs within the Crime Wing for high-level steer. 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 the Crime Wing, in particular the roles and responsibilities of CSPs within the Crime Wing, and the effective supervision on the development of CSTCB.

16. CSTCB has a pressing need for strong and focussed leadership to perform fully and effectively as a separate bureau. 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. 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. With the establishment of the new CSTCB, TCD has been hived off with the permanent redeployment of 106 posts[2] to CSTCB. An additional 74 non-directorate posts[3] have been created by January 2015. Upon the 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 LEAs. The latter division is to enhance the capability of the HKPF in investigating large-scale cyber attacks and cases involving advanced technology.

18. In 2015-16, CSTCB was 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 …..

[2] The 106 posts include 98 posts from the TCD, and four civilian posts and four disciplinary posts from CCB.

[3] Comprising 71 disciplined officers ranked from Police Constable to SSP and three civilian staff.

security incidents. Moreover, a new Cyber Watch Analysis Support Team was established in the 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 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 3. Having regard to the number of disciplinary posts of other Crime Bureaux headed by CSPs as mentioned in paragraph 8 above, 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

ALTERNATIVES CONSIDERED

20. 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 4. 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. 4

FINANCIAL IMPLICATIONS

21. The proposed creation of the CSP post will bring about an additional notional annual salary cost at mid-point of $1,732,800. The additional full annual average staff cost of the proposal, including salaries and staff on-cost, is $2,634,000.

22. 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.

PUBLIC CONSULTATION

23. During the last term of the Legislative Council (LegCo), this staffing proposal was discussed by the Panel on Security on 3 June 2014 and this Subcommittee on 11 March and 29 April 2015. The Government re-submitted the proposal to this Sub-committee in June 2016 but discussion could not commence

/before …..

before the expiry of the last LegCo term. We consulted the Panel on Security again on the proposal on 6 December 2016. The Panel Members generally agreed to the submission of the proposal to this Subcommittee. The information sought by Members at the Panel meeting is set out in Enclosure 5.

Encl. 5

ESTABLISHMENT CHANGES

24. The establishment changes in the HKPF since April 2014 are as follows –

Establishment (Note)	Number of Posts			
	As at 1 December 2016	As at 1 April 2016	As at 1 April 2015	As at 1 April 2014
A*	72#	72#	72	72
B	3 212	3 198	3 138	3 065
C	30 639	30 453	30 096	30 051
Total	**33 923**	**33 723**	**33 306**	**33 188**

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 December 2016, there was no unfilled directorate post in the HKPF

CIVIL SERVICE BUREAU COMMENTS

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

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

26. 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
December 2016

Enclosure 1 to EC(2016-17)23

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.

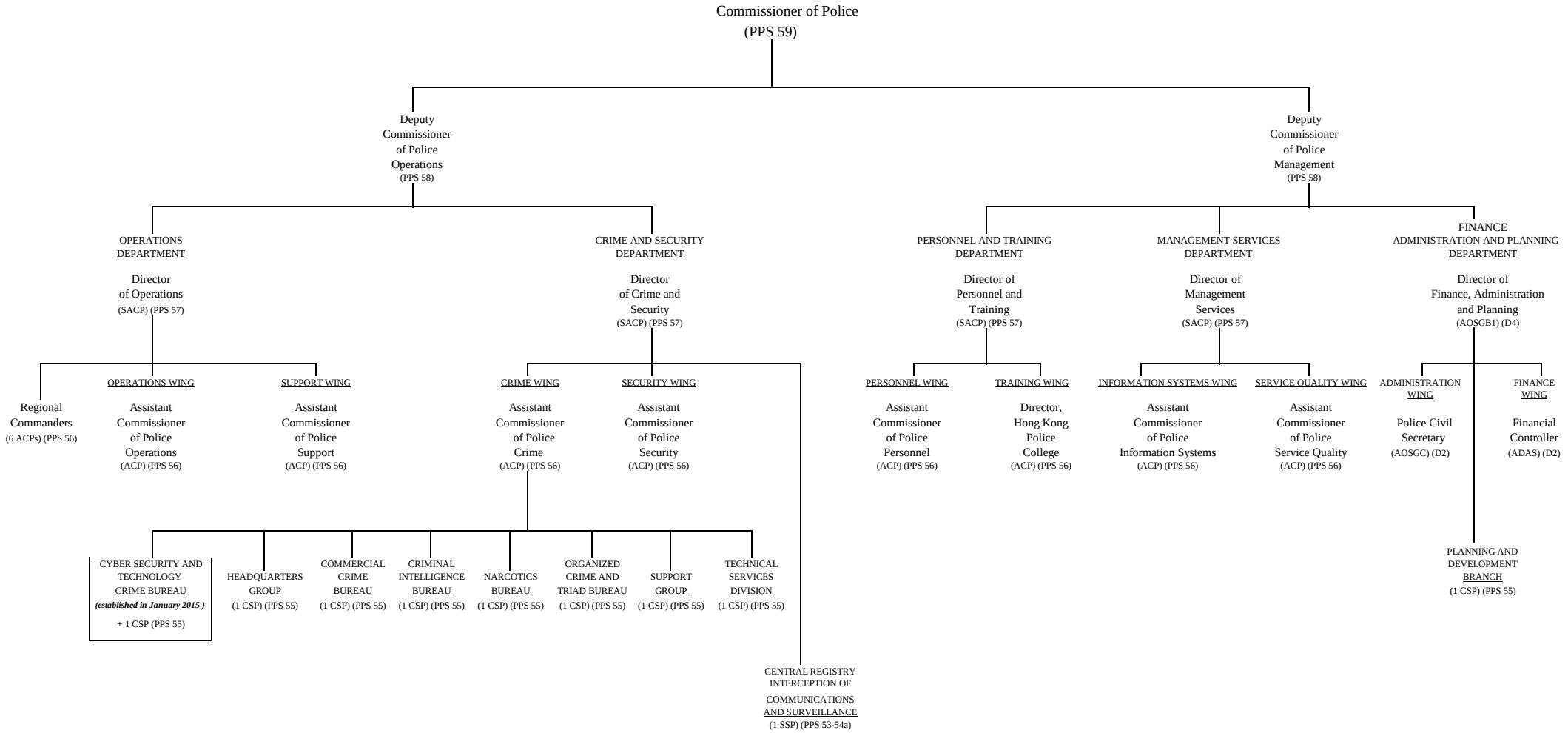
(vii) To engage other police formations with dedicated functions during major cyber attack incidents against critical infrastructure in Hong Kong.

(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)23

Organisation Chart of Hong Kong Police Force



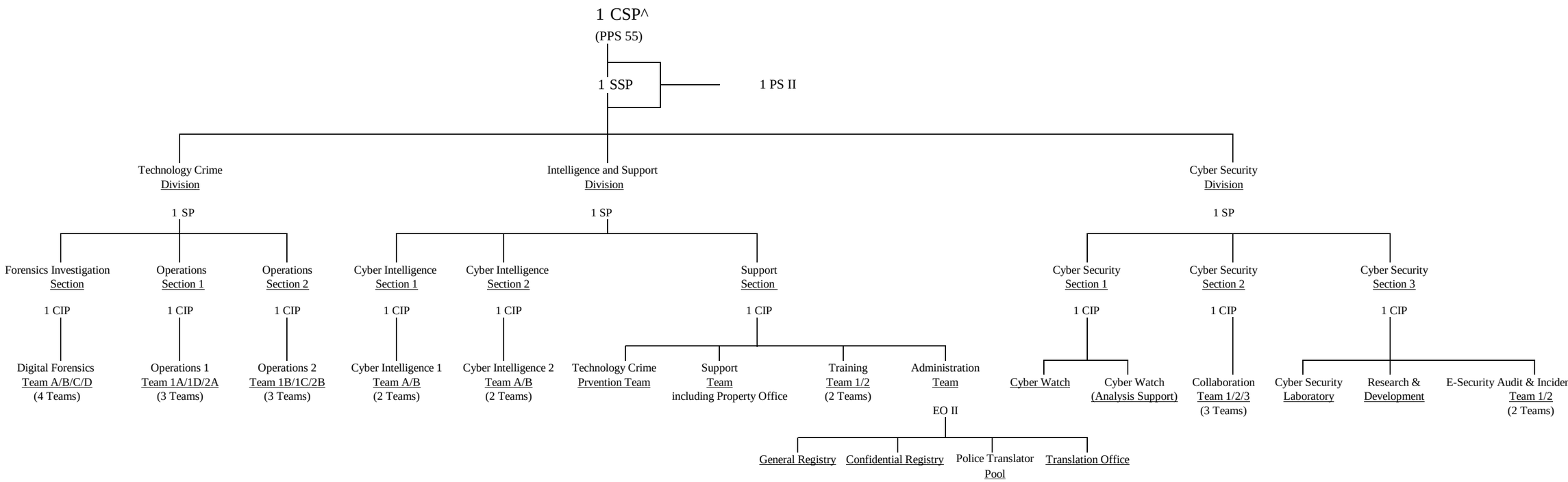
Legend

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)23

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



^ Proposed creation of one Chief Superintendent of Police post.

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) …..

(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, 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)** …..

(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 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.

Enclosure 5 to EC(2016-17)23

Information Sought by Members at the Meeting of the Legislative Council Panel on Security on 6 December 2016

Technology Crime Trend

In recent years, technology crime cases received by the Police involve different types of offences, such as those related to online games, online business frauds and unauthorised access to computer systems. Relevant figures in the past five years are at Table 1.

Table 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) Distributed Denial of Service 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) Other Blackmail	*66*	*509*	*46*	*71*	*93*
(vii) Criminal Intimidation	*23*	*61*	*81*	*87*	*60*
(viii) Sexual Exploitation	*42*	*92*	*79*	*96*	*114*
(ix) Miscellaneous	*74*	*92*	*136*	*136*	*148**
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**

* As an example of the case types under 'miscellaneous', further breakdown of the 148 cases in 2016 is set out as follows –

Online gambling-related	37	Aiding, abetting, suborning, etc. others to commit criminal act	9	Tampering computer	4
Access for data without hacking activities	22	Forged document	8	Miscellaneous theft	3
Identity theft	19	Data leakage from mobile phone/ social media account	6	Bomb hoax	2
Publishing indecent and obscene article	18	Theft of customers' credit point by cashier	5	Claiming to be member of triad society	1
Phishing URL	10	Bogus/ unauthorized website or social media account	4	Total	148

/Qualification …..

Qualification requirements for the Cyber Security and Technology Crime Bureau (CSTCB)'s officers and its proposed Chief Superintendent of Police (CSP)

2. 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), CSTCB should be headed 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.

3. 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; some of them even possess relevant Doctorate or Master Degrees, while the rest of the officers have received internal professional training and possess relevant experience. Some officers have professional qualifications from SANS Institute which is an internationally renowned provider of cyber security training. The professional capabilities of the Police in cyber security and combating technology crimes have also been recognized internationally. Some Police officers were certified trainers of the INTERPOL and have assisted in professional training in cyber security and technology crimes for law enforcement agencies (LEAs) in Singapore, Fiji, Australia, the Republic of Korea and Thailand. These officers 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.

4. 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 training. Overseas visits are conducted from time to time for officers' participation 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 LEAs in order to acquire the most advanced knowledge.

/Arrests, …..

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

5. Section 161[Note] of the Crimes Ordinance (Cap. 200) targets access to computer with criminal or dishonest intent and is effective in combatting illegal acts such as online frauds, illegal access to computers and the use of computers to commit other offences. Over the years, among technology crime cases detected by the Police, only around 10% were charged under section 161; the remaining 90% were charged with other offences.

6. 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 arrests, prosecutions and convictions under section 161 in 2014, 2015 and 2016 (up to June) are set out below.

Table 2: Figures of arrests, prosecutions and convictions under section 161 in 2014, 2015 and 2016

Year	Number of arrests	Number of prosecutions	Number of convictions
2014	113	86	80
2015	143	103	93
2016 (Jan – Jun)	69	57	48

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

/7. …..

Note 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.

7. The above figures are the overall arrest, 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.

8. The figures recorded are the overall figures of various *offences*, not separate figures for the offences under the respective *subsections*. For example, there are two subsections under the offence of 'burglary' (Section 11 of the Theft Ordinance). LEAs only maintain an overall figure of such an offence, without a breakdown of the respective figures for subsections (a) and (b). As in the case of 'burglary', 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.

9. We consider that the law in place is effective in guarding against the rising and serious threats to cyber security and there is no plan for legislative amendments at this stage. Enhancing cyber security as well as combating technology crimes is and will continue to be a Police's priority. The Police shall continue to discharge their enforcement duties in a fair, just and impartial manner in accordance with the law.

10. We understand that the Secretary for Justice, in his capacity as 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 this development.

<u>Cyber Patrol</u>

11. The Police currently adopt a three-tier intelligence framework, including intelligence units at the levels of the headquarters, regions and police districts, for gathering intelligence. The Internet is open to all and hence users are faced with criminal threats as they would in the physical world. Similar to conducting patrol 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. Hence, for the purpose of crime prevention and detection, various departments in the Police conduct 'cyber patrol', meaning to search for relevant information via public platforms on the Internet on a need basis. The Police will, according to their operational priorities, conduct specific and

/professional …..

professional search via such platforms for possible crime-related information (e.g. fraudulent bank websites, illegal football betting activities, dissemination of child pornography, trafficking of dangerous drugs and Internet criminal intimidation etc.). Information gathered on patrol will enable the Police to allocate resources more aptly and analyse the prevailing crime trend, in a bid to combat various types of crimes such as illegal gambling, publishing of child pornography, drug trafficking and other organised crimes.

12. The level of involvement of CSTCB in any 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. In any event, the Police's information search via public platforms on the Internet is only one of the many means of research for the combat of crimes. The purpose of Police's cyber patrol is to watch out for criminal activities or criminal intelligence regardless of their backgrounds or orientations. The Police do not maintain the statistics of cyber patrols.
