立法會
Legislative Council

LC Paper No. ESC72/14-15
(These minutes have been seen by the Administration)

Ref : CB1/F/3/2

Establishment Subcommittee of the Finance Committee

Minutes of the 9th meeting
held in Conference Room 1 of Legislative Council Complex
on Wednesday, 11 March 2015, at 10:45 am

Members present:

Hon Kenneth LEUNG (Chairman)
Hon SIN Chung-kai, SBS, JP (Deputy Chairman)
Hon Albert HO Chun-yan
Hon LEE Cheuk-yan
Hon James TO Kun-sun
Hon Emily LAU Wai-hing, JP
Hon Frederick FUNG Kin-kee, SBS, JP
Prof Hon Joseph LEE Kok-long, SBS, JP, PhD, RN
Hon WONG Ting-kwong, SBS, JP
Hon Cyd HO Sau-lan, JP
Hon Starry LEE Wai-king, JP
Hon WONG Kwok-kin, SBS
Hon Mrs Regina IP LAU Suk-yee, GBS, JP
Hon Paul TSE Wai-chun, JP
Hon Alan LEONG Kah-kit, SC
Hon LEUNG Kwok-hung
Hon Albert CHAN Wai-yip
Hon Claudia MO
Hon Steven HO Chun-yin
Hon WU Chi-wai, MH
Hon YIU Si-wing
Hon Gary FAN Kwok-wai
Hon Charles Peter MOK
Hon CHAN Chi-chuen
Dr Hon Kenneth CHAN Ka-lok

Dr Hon KWOK Ka-ki
Dr Hon Fernando CHEUNG Chiu-hung
Hon IP Kin-yuen
Hon POON Siu-ping, BBS, MH
Hon TANG Ka-piu, JP

Members absent:

Hon LEUNG Yiu-chung
Hon Ronny TONG Ka-wah, SC
Hon CHEUNG Kwok-che
Hon NG Leung-sing, SBS, JP
Hon MA Fung-kwok, SBS, JP
Hon KWOK Wai-keung
Hon Dennis KWOK
Hon Christopher CHEUNG Wah-fung, SBS, JP
Dr Hon Helena WONG Pik-wan
Hon Martin LIAO Cheung-kwong, SBS, JP
Hon CHUNG Kwok-pan

Public Officers attending:

Ms Esther LEUNG, JP	Deputy Secretary for Financial Services and the Treasury (Treasury)1
Mr Eddie MAK Tak-wai, JP	Deputy Secretary for the Civil Service (1)
Mr Joseph LAI, JP	Permanent Secretary for Transport and Housing (Transport)
Mr Andy CHAN, JP	Deputy Secretary for Transport and Housing (Transport)2
Ms Macella LEE	Assistant Commissioner for Transport (Management and Paratransit)
Mr John LEE, PDSM, PMSM, JP	Under Secretary for Security
Mrs Millie NG	Principal Assistant Secretary for Security
Ms Irene HO	Chief Superintendent of Police Crime Wing Headquarters
Mr Francis CHAN	Senior Superintendent of Police Cyber Security and Technology Crime Bureau

Clerk in attendance:

Ms Connie SZETO	Chief Council Secretary (1)4

Staff in attendance:

Ms Anita SIT	Assistant Secretary General 1
Mr Jason KONG	Council Secretary (1)4
Ms Alice CHEUNG	Senior Legislative Assistant (1)1
Miss Yannes HO	Legislative Assistant (1)6
Ms Clara LO	Legislative Assistant (1)8

Action

The Chairman drew members' attention to the information paper ECI(2014-15)13 which set out the latest changes in the directorate establishment approved since 2002. He then reminded members that in accordance with Rule 83A of the Rules of Procedure ("RoP"), they should disclose the nature of any direct or indirect pecuniary interest relating to the funding proposals under discussion at the meeting before they spoke on the items. He also drew members' attention to RoP 84 on voting in case of direct pecuniary interest.

EC(2014-15)18 Proposed creation of a supernumerary post of Administrative Officer Staff Grade C (D2) in the Transport Branch of the Transport and Housing Bureau for two years and six months from 1 April 2015 or from the date of approval by the Finance Committee to oversee and steer the Roles and Positioning Review of the Public Transport Strategy Study

2. The Chairman remarked that the Administration's proposal was to create a supernumerary post of Administrative Officer Staff Grade C, designated as Principal Assistant Secretary (Transport) (Public Transport Strategy Study), in the Transport Branch of the Transport and Housing Bureau for two years and six months to oversee and steer the Roles and Positioning Review ("RPR") of the Public Transport Strategy Study ("PTSS").

3. The Chairman advised that, in response to members' requests at the meeting on 16 February 2015, the Administration had provided supplementary information on the proposal which was circulated to members on 5 March 2015 vide LC Paper No. ESC58/14-15.

4. The Chairman informed members that at the previous meeting on 16 February 2015, Mr Albert CHAN submitted a proposed motion in accordance with paragraph 31A of the Establishment Subcommittee ("ESC") Procedure. He had ruled the proposed motion directly related to the agenda

item and the Subcommittee had agreed to deal with it. The wording of the motion was circulated to members on 3 March 2015 vide LC Paper No. ESC55/14-15. The Chairman invited members to speak on the motion. He said that each member would speak only once and for not more than three minutes. The Administration would be given the opportunity to respond, followed by a conclusion from the proposer of not more than one minute.

5. Mr Albert CHAN considered that it was high time for the Administration to carry out a comprehensive transport study ("CTS") through which the roles of various public transport services, their respective impacts on the public and the Government's financial commitments to various aspects of the transport system could be critically and thoroughly examined. He stressed that a CTS would not only cover the public transport system but also other transport-related issues, such as environmental-friendly transport, transport infrastructure, pedestrian facilities, and the interaction between different components of the transport system. Mr CHAN pointed out that there had been considerable changes in the Hong Kong public transport system and services since completion of the third CTS ("CTS-3") in 1999, including the increase in patronage of the railway system vis-à-vis decrease in patronage of franchised buses and commissioning of new mass transit railway ("MTR") lines. Given railway's dominant role in the public transport system, railway-related issues, such as interchange arrangements between MTR and other modes of public transport and discounts in their fares, should be included in PTSS. As the scope of PTSS was limited and most issues concerning the public transport system were already on-going duties of the Administration, he was concerned that PTSS would overlap with these duties.

6. Mr WU Chi-wai remarked that CTS-2 had laid down two important directions, namely restraining private vehicle growth and giving priority to public transport for the use of roads, which were in line with the recommendations made by the Transport Advisory Committee in the Report on Study of Road Traffic Congestion in Hong Kong. Furthermore, CTS-3 had laid down the direction of using railway as the backbone of the public transport system, and the Railway Development Strategy ("RDS") 2014 had already addressed railway-related matters under this direction. He commented that it was important that PTSS would be conducted under the premises of the abovementioned three directions. He said that while he did not object to carrying out PTSS, he supported the Administration embarking on CTS-4 to plan for the long-term development of the Hong Kong transport system.

7. Permanent Secretary for Transport and Housing (Transport) ("PSTH(T)") said that the Administration had reiterated its stance on the proposal for conducting CTS-4 on previous occasions. RDS 2014, announced in September 2014, had reaffirmed the established policy of using

railway as the backbone of the public transport system and set out the blueprint for future development of the railway network up to 2031. Against this background, there was a pressing need to examine how to enhance the complementarity of railway and other public transport services so as to ensure that the public could enjoy multi-modal choices on the one hand and the public transport operators could enjoy sustainable development on the other. PSTH(T) also said that the Administration had reaffirmed in the supplementary information provided to members before the meeting that the public transport-oriented policy and the principle of according priority use of roads to public transport as laid down in CTS-2 remained valid.

8. In his conclusion, Mr Albert CHAN called on members to support his motion.

9. The Chairman put Mr Albert CHAN's motion to vote. At the request of Mr CHAN, the Chairman ordered a division and the division bell was rung for five minutes. The Chairman announced that seven members voted in favour of, nine voted against the motion, and seven members abstained from voting. The motion was not carried. The voting results of individual members were as follows –

For

Mr LEE Cheuk-yan	Mr Frederick FUNG
Mr Albert CHAN	Ms Claudia MO
Mr Gary FAN	Mr CHAN Chi-chuen
Dr Fernando CHEUNG	
(7 members)	

Against

Prof Joseph LEE	Mr WONG Ting-kwong
Ms Starry LEE	Mrs Regina IP
Mr Paul TSE	Mr Steven HO
Mr YIU Si-wing	Mr Charles MOK
Mr POON Siu-ping	
(9 members)	

Abstain

Mr James TO	Ms Emily LAU
Mr Alan LEONG	Mr WU Chi-wai
Dr Kenneth CHAN	Mr SIN Chung-kai
Mr IP Kin-yuen	
(7 members)	

10. The Chairman then put EC(2014-15)18 to vote. At the request of Mr Albert CHAN, the Chairman ordered a division and the division bell was rung for five minutes. Nineteen members voted for and four voted against the item. The Chairman declared that the Subcommittee agreed to recommend the item to the Finance Committee for approval. The voting results of individual members were as follows –

For

Mr LEE Cheuk-yan	Ms Emily LAU
Mr Frederick FUNG	Prof Joseph LEE
Mr WONG Ting-kwong	Ms Starry LEE
Mrs Regina IP	Mr Paul TSE
Mr Alan LEONG	Mr Steven HO
Mr WU Chi-wai	Mr YIU Si-wing
Mr Gary FAN	Mr Charles MOK
Dr Kenneth CHAN	Dr Fernando CHEUNG
Mr SIN Chung-kai	Mr IP Kin-yuen
Mr POON Siu-ping	
(19 members)	

Against

Mr LEUNG Kwok-hung	Mr Albert CHAN
Ms Claudia MO	Mr CHAN Chi-chuen
(4 members)	

EC(2014-15)19 Proposed creation of a permanent post of Chief Superintendent of Police (PPS 55) in the Crime Wing of the Hong Kong Police Force with effect from the date of approval by the Finance Committee to head the Cyber Security and Technology Crime Bureau for preventing and combating technology crime and responding to cyber security incidents

11. The Chairman said that the Administration's proposal was to create a permanent post of Chief Superintendent of Police ("CSP") in the Crime Wing of the Hong Kong Police Force ("Police") to head the Cyber Security and Technology Crime Bureau ("CSTCB") for preventing and combating technology crimes and responding to cyber security incidents.

12. The Chairman advised that the Panel on Security had discussed the proposal at its meeting on 3 June 2014. Some Panel members queried the need to upgrade the original Technology Crime Division ("TCD") to form CSTCB. There were concerns that activities of the public on the Internet

would be kept under surveillance by CSTCB, which would restrict the freedom of speech. The Administration explained that the objective of upgrading TCD to form CSTCB was to strengthen the overall capability of the Police in combating technology crimes and cyber security incidents. The work of CSTCB would remain unchanged despite the upgrading. At the Panel meeting, five members expressed support for and three members was opposed to the Administration submitting the proposal to ESC, while five members did not express any view. In response to members' request, the Administration had provided supplementary information on the duties and manpower of CSTCB.

Manpower and work of the Cyber Security and Technology Crime Bureau

13. Mr LEE Cheuk-yan noted that 74 non-directorate posts had been created in 2014 for establishing the new CSTCB. He said that the Labour Party supported strengthening the manpower of the Police to combat and prevent technology crimes. However, he noted that although the number of reports of technology crimes had increased fourfold, around 70% of the new posts in CSTCB were created in the Cyber Security Division ("CSD") instead of TCD. As such, there was serious concern that the additional manpower would be used to conduct cyber surveillance on the activities of and information disseminated by members of the public on the Internet and social media, in particular information related to social movements, in order to facilitate prosecutions instituted under section 161 of the Crimes Ordinance (Cap. 200) on access to computer with criminal or dishonest intent and to suppress freedom of speech. Mr Charles MOK remarked that the community at large echoed the same concern.

14. Ms Emily LAU noted from paragraph 10 of the Administration's paper that the original TCD had been "hived off with the permanent redeployment of 106 posts to CSTCB". She sought clarification about the current headcount of CSTCB and the purpose of creating the 74 non-directorate posts in 2014. She opined that the Police should give an undertaking that the increased manpower would not be used to conduct surveillance on the Internet activities of the general public, and queried how the Police could ensure the work of CSTCB would not infringe personal data privacy. She also enquired if the Police had received any complaint regarding its monitoring of the public's activities on the Internet and the number of such complaints.

15. Under Secretary for Security ("US for S") responded that from 2009 to 2013, the number of reports of technology crimes had increased fourfold and the respective financial loss had increased by almost 20 times, against the background of a decrease in the overall crime rate since 1997. There was practical need for the Police to strengthen their manpower to cope with the

evolving technology crime trend and offer sufficient protection to members of the public. He added that it was a general trend of law enforcement agencies of various jurisdictions to increase manpower to combat technology crimes and tackle cyber security incidents. He said that the former TCD, when created in 2002, had an initial establishment of 26 posts, and there had been increases in its establishment over the past years to 98 posts in 2014 including creation of 31, 14 and 27 new posts in 2003, 2009 and 2012 respectively. To take forward the plan of upgrading TCD to CSTCB as announced in January 2014, 74 new posts were created in 2014 to undertake the preparatory work which was completed in January 2015. CSTCB currently had 180 non-directorate posts, and there were similar headcounts in its two divisions, TCD and CSD. Among the 74 posts created in 2014, 51 were disciplined officer posts for formation of new teams in CSD, the rest were posts under TCD. There were some civilian posts in CSTCB as indicated in footnote 2 of the Administration's paper. Enclosure 3 to EC(2014-15)19 set out the current organization chart of CSTCB. TCD was mainly tasked for investigation, training and preventing technology crimes, while CSD was mainly responsible for monitoring the overall network traffic, undertaking researches on cyber crime trend, and preventing and handling cyber threats to the computer systems of critical infrastructures. He pointed out that according to the Police Force Ordinance (Cap. 232), all Police officers had the responsibility to prevent and detect crimes, and the Police were required to take appropriate actions when information of crimes came to their knowledge.

16. Mr Charles MOK pointed out that he and a number of Legislative Council ("LegCo") Members had been invited by the Organized Crime and Triad Bureau ("OCTB") to assist in the investigation related to the "Occupy Central" movement. According to some LegCo Members involved, their comments on social media had been gathered by the Police as possible evidence. Mr CHAN Chi-chuen remarked that some protestors of the "Occupy Central" movement had been interrogated by the Commercial Crime Bureau. They enquired about the division of work between CSTCB and other Police bureaux regarding investigation of cases related to the use of computers and the Internet.

17. US for S said that similar to conducting patrols on the streets in the physical world for prevention of crime, it was necessary for the Police to spot and take action against possible criminal activities in the virtual world of the Internet. Information gathered by patrols would also enable the Police to allocate resources more appropriately in tackling the crimes. The level of involvement of CSTCB in an investigation would depend on the complexity of the technology crime involved in the case. Officers in TCD usually led the investigation of crimes involving high-end and more complex technologies. For crimes with a low degree of technological element, TCD would mainly assist investigation teams in gathering the technological evidence or providing

advice on technology-related matters.

18. With reference to "cyber patrols", Ms Cyd HO enquired whether the Police would check both open and private information (e.g. Facebook). US for S responded that, as in the physical world, open information would be checked by the Police. Under normal circumstances, the Police would not access or check private information without the consent of the individuals concerned. For investigation of serious crimes, if considered necessary, the Police could apply to the court for orders to demand parties to disclose the information concerned in the same way as entering and searching a premises in the physical world.

19. Ms Cyd HO expressed concern that in order to find out the identities of Internet users, the Police would conduct undercover operations, use hacking devices, or compel the hosts of online discussion forums or Internet service providers ("ISPs") to hand in personal information of their users. She urged the Police to explain their powers and the procedures in respect of investigation of crimes involving the Internet. Mr CHAN Chi-chuen shared the concern about the Police initiating more prosecutions under section 161 of the Crimes Ordinance.

20. US for S said that he would not discuss the investigation methods of the Police in the public. He stressed that all powers of the Police were conferred by the relevant legislation, and Police officers would only exercise the powers having regard to the actual situations. He clarified that section 161 of the Crimes Ordinance was invoked for only around 10% of all prosecutions related to technology crimes. Other prosecutions were made invoking other relevant legal provisions, such as "bomb hoaxes" under the Public Order Ordinance (Cap. 245), "wasteful employment of the Police" under the Criminal Procedure Ordinance (Cap. 221), as well as other criminal offences under the Crimes Ordinance, etc. Ms Cyd HO and the Chairman commented that the Police should clarify the legal basis for them to check personal data kept by an ISP. US for S reiterated that such information would only be checked when there was a legal basis or with the consent of the parties concerned. There were also provisions in various ordinances for the court to grant a search warrant to the Police if it was satisfied that a criminal offence had been committed or might be contemplated.

21. Ms Cyd HO expressed concern that CSTCB would use techniques used in undercover operations to induce members of the public to engage on online activities which were in breach of section 161 of the Crimes Ordinance. US for S explained that it was unlawful for any person, including a Police officer, to incite other people to commit illegal acts. He stressed that there must be a legal basis for every act of the Police.

Action

22. Mr LEE Cheuk-yan expressed grave concern about the lack of transparency in the work of CSD. While he noted from Enclosure 3 to the Administration's paper that CSD consisted of three sections with 10 teams, there was no information on the duties of each section and team, such as the Cyber Watch Team, the two Cyber Intelligence Teams, the three Collaboration Teams and the Cyber Security Laboratory Team. Mr CHAN Chi-chuen expressed similar concerns and queried whether the Cyber Watch Team was responsible for cyber surveillance. Ms Cyd HO asked the Administration to explain the main tasks performed by the Collaboration Teams and its major partners, and whether the Collaboration Teams would collaborate with the Mainland police in conducting cyber surveillance.

23. US for S responded that CSTCB was responsible for a wide variety of tasks with a significant number of staff involved in enhancing cyber security, such as handling distributed denial-of-service ("DDoS") attacks, and new tasks, such as undertaking thematic researches, and monitoring the development of malwares, etc. The Collaboration Teams were responsible for collaboration and co-ordination with local stakeholders (such as critical infrastructures) and international stakeholders (such as INTERPOL and law enforcement agencies in the G8 technology crime framework) in addressing technology crimes and cyber security issues. Police officers engaged in such collaborative work were required to abide by the laws of Hong Kong. The Research and Development Team carried out thematic researches on cyber crime trend and mode of operation, such as new hacking techniques and computer worms. US for S pointed out that the increase in the manpower in CSTCB actually lagged behind the fast pace of development in Internet activities.

Admin

24. Ms Cyd HO requested the Administration to provide supplementary information on the establishment and manpower strength in respect of each division, section and team of CSTCB.

25. Referring to experience of cyber attacks to his website, Mr LEUNG Kwok-hung asked whether the Police were aware of the matter and whether they would conduct cyber threat analyses for the websites of LegCo Members. He also queried if the Police had the capabilities to handle cyber attacks with possible hacker parties outside the jurisdiction of the laws of Hong Kong. Mr LEE Cheuk-yan expressed similar concerns, and pointed out that the websites of the Hong Kong Alliance in Support of Patriotic Democratic Movements in China and the Public Opinion Programme of The University of Hong Kong had also experienced cyber attacks.

26. US for S responded that any organization or individual who experienced cyber attacks to their systems should report the incidents to the Police, which would provide assistance regardless of the identities of the

parties concerned. Such reports would also provide the Police with valuable information on the cyber crime trend and mode of operation. He explained that cyber threat audits and analyses conducted by the Police were targeted at critical infrastructures only, not individuals or other organizations. Co-operation with CSTCB on cyber threats prevention and contingency measures by critical infrastructures was on a voluntary basis. CSTCB had in place an e-security audit framework to examine various facets of a critical infrastructure and analyze their adequacy in addressing cyber security threats and attacks. CSTCB would monitor the overall network traffic of the computer systems of a critical infrastructure which partnered with the bureau, but it would not check the content of the traffic. As such, identities of the individuals or parties would not be revealed in the monitoring process. To combat cross-boundary cyber attacks and technology crimes, CSTCB would maintain close liaison with INTERPOL and law enforcement agencies in the G8 technology crime framework. Mechanisms were also in place for exchange of intelligence and assistance in enforcement actions among counterparts of various jurisdictions.

27. Ms Emily LAU enquired about the respective numbers of cyber attacks handled by the Cyber Security Centre ("CSC"). US for S responded that in 2014, CSC under CSTCB had discovered 11 927 malicious programmes, 9 674 phishing websites and 10 068 fraudulent websites. The Police had taken responsive actions against 198 botnets, 566 cyber attacks and 81 malicious programmes.

Capabilities of the Cyber Security and Technology Crime Bureau

28. Mr WONG Ting-kwong said that the Democratic Alliance for the Betterment and Progress of Hong Kong supported the Administration's proposal. Mr YIU Si-wing agreed that it was necessary to establish CSTCB having regard to the trend in technology crimes, especially rapid development in cyber techniques that had increased the complexities of technology crimes. The recent alleged "bitcoin" fraud in Hong Kong and the unauthorized extraction of data in the United States National Security Agency system by Mr Edward SNOWDEN were cases in point. Mr WONG and Mr YIU sought details about the Police's plan to cope with the work.

29. US for S said that the Police recognized the need to maintain world-class professional standards in cyber security and enhance its capabilities in the investigation of technology crimes. At present, 94% of the officers in CSTCB had relevant computer/information technology ("IT") qualifications, and some of them possessed masters and doctorate degrees. Police officers also participated in training programmes organized by SANS Institute (an internationally renowned provider of cyber security training). Besides, the Police organized technology crime workshops in Hong Kong in

2013 and 2015 jointly with INTERPOL which were participated by representatives of INTERPOL member countries. Furthermore, the professional capabilities of the Police in cyber security and combat of technology crimes had been recognized internationally. The Senior Superintendent of Police of CSTCB had been the vice chairman of INTERPOL's Eurasian Working Group on Cybercrime since 2013, while the Senior Superintendent of Police of the former TCD had served as the chairman of INTERPOL's Working Group of Experts on IT Crime Asia and South Pacific for about ten consecutive years. In addition, some Police officers were certified trainers of INTERPOL and had assisted in professional training in cyber security and technology crimes for law enforcement agencies in Singapore, the Republic of Korea and Thailand.

30. The Chairman enquired if the Police had recruited or had plans to recruit IT professionals to assist the investigation work of CSTCB. US for S responded that all criminal investigation work must be conducted by Police officers, who were equipped with the relevant knowledge and experience through training. This was because they would have to exercise their legal powers in the investigation work.

31. Mr WONG Kwok-kin expressed support for the Administration's proposal. Pointing out that many technology crimes were committed across boundaries of various jurisdictions, he enquired about the Police's collaboration with overseas law enforcement agencies in this regard. US for S responded that, apart from the G8 technology crime framework, the Police also participated in INTERPOL's "I24/7", which was a global police communications system enabling round-the-clock data exchange and collaboration among law enforcement agencies of various jurisdictions. The Police had also been maintaining close liaison with counterparts in advanced countries in Asia, Europe and North America. In 2014, through INTERPOL, the Police participated in a joint operation with the law enforcement agencies in Singapore, the United States, the United Kingdom and the Philippines against criminal syndicates in the Philippines involving in what were commonly called "naked chat" blackmail cases. Some 100 such cases took place in Hong Kong. The joint operation was based on the intelligence gathered and analyzed by the Hong Kong Police and after collaboration with overseas law enforcement agencies, 58 suspects were arrested. US for S said that the Police would continue to play an active role in international co-operative work for combating technology crimes, and enhance their investigation capabilities in such crimes.

32. The Chairman enquired about the powers of respective law enforcement agencies in instituting prosecutions of cyber and technology crimes committed across borders, and whether the law of extradition applied to technology crimes. Senior Superintendent of Police Cyber Security and

Action

Technology Crime Bureau ("SSP of CSTCB") responded that in the "naked chat" blackmail cases mentioned above, the Hong Kong Police had provided pivotal information to the Philippine National Police through INTERPOL. Pursuant to the bilateral agreement between Hong Kong and the Philippines on mutual legal assistance, the Philippine authorities might request to obtain evidence or statements from persons in Hong Kong, and both the Hong Kong Police and the Philippine National Police had the right to institute prosecutions in the cases. There was no precedent case of extradition in technology crimes.

The trend in cyber and technology crimes

33. Mr CHAN Chi-chuen said that he did not object to the creation of the CSP post to enhance efforts of the Police in combating technology crimes, such as online shopping fraud, email scam, blackmail associated with naked chat, etc. However, with the strengthening of the manpower of CSTCB, he shared some members' concern about the Police conducting cyber surveillance on the public, thus restricting freedom of speech. In this connection, he asked if the Police had changed the definition of technology crime, and whether advocating social movements on the Internet would fall under the definition.

34. US for S said that technology crime was a general crime category. In a nutshell, it covered offences committed using a computer system or through the Internet. In 2014, there were some 6 700 technology crimes reported, around 60% to 70% of which were related to Internet frauds and abuses of online game services. The most common types of technology crime were online business frauds, crimes related to online games and unauthorized access to computer systems. Of note was that reports of DDoS attacks had increased significantly in recent years.

Admin

35. Upon members' request, the Administration was invited to provide supplementary information on the numbers of cyber and technology crimes reported in recent years with a breakdown by various categories and descriptions on the major crimes covered under each category.

Visit to the Cyber Security Centre

36. Ms Emily LAU suggested that the Police should arrange a visit to CSC of CSTCB for ESC members. US for S responded that the operation of CSC involved highly sensitive technical and operational matters which must not be made known to outsiders. As such, CSC must maintain a high degree of confidentiality, and it would not be appropriate to organize such a visit to CSC. He pointed out that overseas law enforcement agencies likewise had tight security controls of their cyber security centres, and requests to visit the

centres by the Hong Kong Police had also been declined before.

37. Mr LEUNG Kwok-hung did not subscribe to the Administration's response. In particular, he queried whether the Administration considered that the location of CSC, where its servers were housed, or both had to be kept unknown to outsiders including LegCo Members. US for S explained that in order to protect the capability and security of CSC, the policy was only to grant access to CSC to parties on a strictly "need-to-know" basis. Even Government officials or police officers who were not involved would be denied access to CSC. As regards how the Police could ensure officers deployed to work in CSC would not cause leakage of their confidential information, US for S responded that the Police conducted integrity checks of the officers concerned, and the officers working in CSC were under obligation to keep all related information which came to their knowledge during work strictly confidential. In addition, the Police adopted the principle of compartmentalization and other risk management systems to reduce the risk and harm of any compromise of confidentiality.

38. Ms Cyd HO remarked that the response of US for S above had aroused more concern over the work of CSTCB. She queried if CSC was located inside or outside Hong Kong. US for S responded that it was located inside Hong Kong.

39. Mr Charles MOK said that he learnt from the information posted on the Facebook of an Executive Council ("ExCo") Member, on 22 April 2013 seven ExCo Members visited CSC located at the Police Headquarters in Wan Chai. He requested the Administration to confirm if the above information was correct; and if so, explain why the Administration had refused to arrange a visit to CSC for LegCo Members.

40. SSP of CSTCB confirmed that some ExCo Members had visited CSC in April 2013 when the centre was not yet fully operational. He reaffirmed the Police's position that the operation of CSC must be kept unknown to outsiders in order to protect its capability. In addition, there were confidentiality clauses in the partnership agreements with critical infrastructure operators. In response to the Chairman's further question, SSP of CSTCB confirmed that no ExCo or LegCo Members had visited CSC after it had become fully operational.

Bureaux under the Crime Wing

41. Noting that CSTCB was upgraded from TCD which was a former division under the Commercial Crime Bureau of the Crime Wing, Mr SIN Chung-kai asked if the establishment size of CSTCB was comparable to other crimes bureaux under the Crime Wing and whether the Police had any plan to

Action

Admin

upgrade other divisions under the bureaux of the Crime Wing. He said that the Police should provide supplementary information on the respective establishment and manpower strength of each bureau involved in the investigation of crimes under the Crime Wing.

42. US for S said that it would be inappropriate to make direct comparison on the establishment of various bureaux under the Crime Wing, as the work nature varied from bureau to bureau and the manpower required in each bureau was dependent on the tasks it handled. For instance, there were some 130 officers in OCTB and some 400 officers in the Narcotics Bureau. Currently the Police did not have any plan to upgrade other divisions under the bureaux of the Crime Wing.

(At 12:38 pm, the Chairman announced that the meeting be extended for not more than 15 minutes. Members agreed.)

43. The Chairman advised that the discussion on this item would continue at the next meeting to be held on 29 April 2015, at 8:30 am.

44. There being no other business, the meeting ended at 12:51 pm.

Council Business Division 1
Legislative Council Secretariat
16 April 2015