立法會
Legislative Council

LC Paper No. CB(2)602/16-17
(These minutes have been seen by the Administration)

Ref : CB2/PL/SE

Panel on Security

Minutes of meeting
held on Tuesday, 6 December 2016, at 2:30 pm
in Conference Room 1 of the Legislative Council Complex

Members present	:	Hon CHAN Hak-kan, BBS, JP (Chairman) Hon James TO Kun-sun (Deputy Chairman) Hon Jeffrey LAM Kin-fung, GBS, JP Hon WONG Ting-kwong, SBS, JP Hon Starry LEE Wai-king, SBS, JP Hon CHAN Kin-por, BBS, JP Dr Hon Priscilla LEUNG Mei-fun, SBS, JP Hon Paul TSE Wai-chun, JP Hon LEUNG Kwok-hung Hon Claudia MO Hon Steven HO Chun-yin, BBS Hon Frankie YICK Chi-ming, JP Hon WU Chi-wai, MH Hon YIU Si-wing, BBS Hon MA Fung-kwok, SBS, JP Hon Charles Peter MOK, JP Hon CHAN Chi-chuen Hon CHAN Han-pan, JP Hon LEUNG Che-cheung, BBS, MH, JP Hon Kenneth LEUNG Hon Alice MAK Mei-kuen, BBS, JP Hon KWOK Wai-keung Dr Hon Fernando CHEUNG Chiu-hung Dr Hon Helena WONG Pik-wan Dr Hon Elizabeth QUAT, JP Hon POON Siu-ping, BBS, MH Hon CHUNG Kwok-pan Hon Alvin YEUNG

Hon Jimmy NG Wing-ka, JP
Dr Hon Junius HO Kwan-yiu, JP
Hon LAM Cheuk-ting
Hon Holden CHOW Ho-ding
Hon SHIU Ka-chun
Hon Wilson OR Chong-shing, MH
Hon YUNG Hoi-yan
Hon CHAN Chun-ying
Hon Tanya CHAN
Hon CHEUNG Kwok-kwan, JP
Hon HUI Chi-fung
Hon LAU Kwok-fan, MH
Dr Hon CHENG Chung-tai
Hon Jeremy TAM Man-ho
Hon Nathan LAW Kwun-chung

Members attending : Dr Hon KWOK Ka-ki
Hon Martin LIAO Cheung-kong, SBS, JP

Members absent : Hon Abraham SHEK Lai-him, GBS, JP
Hon WONG Kwok-kin, SBS, JP
Hon Michael TIEN Puk-sun, BBS, JP
Hon Dennis KWOK Wing-hang
Hon Christopher CHEUNG Wah-fung, SBS, JP
Hon CHU Hoi-dick
Dr Hon YIU Chung-yim

Public Officers attending : Item IV

The Administration

Mr LAI Tung-kwok, GBS, IDSM, JP
Secretary for Security

Mr Joshua LAW Chi-kong, JP
Permanent Secretary for Security

Ms Mimi LEE Mei-mei, JP
Deputy Secretary for Security 1

Mr Andrew TSANG Yue-tung
Principal Assistant Secretary for Security E

Mr CHIU Man-hin
Assistant Secretary for Security E2

Independent Commission Against Corruption

Mr Steven LAM Kin-ming
Assistant Director / Operations 3

Ms Winky HSU Man-wai
Senior Principal Investigator / R Group

Item V

The Administration

Mr John LEE Ka-chiu, PDSM, PMSM, JP
Under Secretary for Security

Mr Andrew TSANG Yue-tung
Principal Assistant Secretary for Security E

Mr Stanley CHUNG Siu-yeung
Assistant Commissioner of Police (Crime)

Mr Anthony TSANG Ching-fo
Senior Superintendent (CSTCB)
Hong Kong Police Force

Dr Frank LAW Yuet-wing
Superintendent (CSD CSTCB)
Hong Kong Police Force

Clerk in attendance : Miss Betty MA
Chief Council Secretary (2) 1

Staff in attendance : Mr Timothy TSO
Senior Assistant Legal Adviser 1

Mr Raymond LAM
Senior Council Secretary (2) 7

Ms Mina CHAN
Council Secretary (2) 1

Miss Lulu YEUNG
Clerical Assistant (2) 1

Action

I. Confirmation of minutes of previous meeting
(LC Paper No. CB(2)280/16-17)

The minutes of the meeting held on 11 November 2016 were confirmed.

II. Information paper issued since the last meeting

2. Members noted that no information paper had been issued since the last meeting.

III. Date of next meeting and items for discussion
(LC Paper Nos. CB(2)282/16-17(01) and (02))

Regular meeting in January 2017

3. Members agreed that the following items would be discussed at the next regular meeting on 3 January 2017 at 2:30 pm:

(a) Amending the United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575);

(b) Redevelopment of Junior Police Officers Married Quarters at Fan Garden, Fanling; and

(c) Replacement and enhancement of the closed-circuit television systems for Tai Lam Correctional Institution, Tong Fuk Correctional Institution and Tung Tau Correctional Institution.

Action

Special meeting on 24 January 2017

4. The Chairman reminded members that a special meeting would be held on 24 January 2017 from 2:00 pm to 4:00 pm to receive a briefing by the Commissioner of Police on the crime situation in 2016.

Visit to the Fire and Ambulance Services Academy

5. The Chairman informed members that a visit would be made to the Fire and Ambulance Services Academy on 4 January 2017 and the Director of Fire Services would host a luncheon for members immediately before the visit. Members would be informed of the details of the visit once available.

IV. Results of study of matters raised in the Annual Report 2015 to the Chief Executive by the Commissioner on Interception of Communications and Surveillance

(LC Paper Nos. CB(2)282/16-17(03), (04) and Annual Report 2015 to the Chief Executive by the Commissioner on Interception of Communications and Surveillance)

6. Members noted a Summary of the Annual Report 2015 ("the Annual Report") to the Chief Executive by the Commissioner on Interception of Communications and Surveillance ("the Commissioner") prepared by the Secretariat of the Commissioner, which was tabled at the meeting.

(*Post-meeting note*: The Summary tabled at the meeting was circulated to members vide LC Paper No. CB(2)333/16-17 on 7 December 2016.)

7. Secretary for Security ("S for S") briefed Members on the results of the Government's study of matters raised in the Annual Report, the details of which were set out in the paper to the Panel.

8. Members noted an updated background brief entitled "Results of Study of Matters Raised in the Annual Report to the Chief Executive by the Commissioner on Interception of Communications and Surveillance" prepared by the Legislative Council ("LegCo") Secretariat.

Action

Cases of non-compliance and irregularity in 2015

9. Ms Claudia MO said that according to paragraph 6.6 of the Annual Report, there was interception of a wrong facility for about four days and an incorrect statement contained in the affirmation supporting the application for interception on another facility used by the subject. She expressed concern that the disciplinary actions taken on the officers concerned were mainly written warnings or advices.

10. Referring to paragraph 6.6 of the Annual Report, Mr YIU Si-wing asked whether improvement measures had been introduced by the law enforcement agency ("LEA") concerned to prevent the recurrence of similar incidents. He asked whether disciplinary actions had been taken against the officers concerned.

11. Referring to paragraph 6.11 of the Annual Report, Mr CHAN Chun-ying asked whether disciplinary actions had been taken against LEA officers who were so forgetful and not being able to recall or recollect the details of various important events in relation to the case concerned.

12. S for S advised that under the existing regime, LEAs would be required to notify the Commissioner on identifying any instance of non-compliance and irregularities, followed by a case investigation report. After examination of such a report, the Commissioner would, as the case might require, make recommendations on areas requiring improvement and, if necessary, comment on the appropriateness of the disciplinary actions to be taken on the officers concerned. He stressed that heads of LEAs were very concerned about cases of non-compliance and irregularities. In the case concerned, the LEA had introduced improvement measures to address the inadequacies identified in the interception verification and application procedures. The Annual Report set out the actions taken against the LEA officers concerned and the Commissioner's conclusion of not finding sufficient evidence of any ill will or ulterior motive relating to any of the LEA officers concerned.

13. Referring to paragraph 6.8 of the Annual Report, Mr CHAN Chun-ying asked whether measures had been introduced to address the unsatisfactory verification process regarding the interception of the correct facility. S for S responded that the LEA concerned had reminded its officers that in any event, the internal verification form should be fully completed with its details verified before applying to the panel judge for a relevant prescribed authorization.

Action

14. Noting that the number of authorizations for Type 2 surveillance had increased over the previous year, Dr CHENG Chung-tai expressed concern about whether LEAs were shifting from carrying out Type 1 surveillance to Type 2 surveillance.

15. S for S responded that the carrying out of Type 1 or Type 2 surveillance was subject to the needs in the circumstances of each case and the elaborate requirements under the Interception of Communications and Surveillance Ordinance (Cap. 589) ("ICSO"). He said that the Commissioner's comments in paragraph 6.12 of the Annual Report were made in relation to a specific case involving interception. The LEA concerned had proposed improvement measures, which, as stated in paragraph 6.14 of the Annual Report, were considered appropriate by the Commissioner. The Commissioner also stated in paragraph 9.11 of the Annual Report that he was generally satisfied with the performance of LEAs and their officers in their compliance with the requirements of ICSO in 2015.

16. Mr LAM Cheuk-ting said that he had been involved in interception and covert surveillance operations in his previous employment with the Independent Commission Against Corruption ("ICAC"). He pointed out that there was stringent legislation and a well established regime for monitoring the interception and covert surveillance work of LEAs. The consequences of deliberate non-compliance could result not only in dismissal but also criminal sanction. There was thus no reason for deliberate non-compliance on the part of law enforcement officers. He expressed concern that in order to avoid making mistakes, LEAs were reluctant to submit surveillance applications, thus resulting in a substantial drop in the number of applications for Type 1 and Type 2 surveillance from 136 and 120 in 2007 to 37 and 13 in 2015 respectively. He considered that the Administration should bring this trend to the attention of the Commissioner and panel judges.

17. S for S said that while the interception and covert surveillance work of LEAs was subject to stringent monitoring by the Commissioner in accordance with ICSO, the stringent regulatory regime would not result in reluctance on the part of LEAs to conduct relevant operations as might be required in the circumstances of each case.

Action

18. Mr CHEUNG Kwok-kwan sought information on whether the nine cases of non-compliance or irregularity referred to in Chapter 6 of the Annual Report were mainly related to any particular LEA. While noting the Commissioner's comment that there was no finding of any deliberate disregard of the requirements in ICSO, he expressed concern about why there were still cases of non-compliance arising from the carelessness or non-vigilance of LEA officers.

19. S for S responded that such information was not available to the Government, as the monitoring of compliance of LEAs with ICSO was carried out independently by the Commissioner. He stressed that the heads of LEAs were very concerned about cases of non-compliance or irregularities and had introduced improvement measures in response to the comments of the Commissioner on such cases. He said that frontline LEA officers were subject to heavy pressure in carrying out duties relating to interception and covert surveillance. There was usually a need for an application to be submitted within a very short time.

20. Referring to paragraph 6.12 of the Annual Report, Dr CHENG Chung-tai expressed concern about the Commissioner's comments regarding the lax attitude of officers in the case concerned.

21. Referring to the Commissioner's comments in paragraph 6.11 of the Annual Report, the Deputy Chairman said that unless the penalty for non-compliance with ICSO had a sufficient deterrent effect, it would be difficult for law enforcement officers to be vigilant enough when carrying out interception or covert surveillance work.

22. S for S responded that the compliance of LEAs with ICSO was strictly monitored by the Commissioner. The disciplinary actions to be taken on LEA officers for non-compliance were reported to the Commissioner, who might comment on the appropriateness of the disciplinary actions.

Examination of protected products by the Commissioner and his designated staff

23. Noting that the Commissioner and his designated staff were empowered to examine protected products following the passage of the Interception of Communications and Surveillance (Amendment) Bill 2015 in June 2016, Mr MA Fung-kwok expressed concern about how such examination would be conducted and whether there were measures

Action

to prevent the leakage of information in the process. He asked whether relevant training were provided to the Commissioner's staff designated for carrying out examination of protected products.

24. S for S responded that the examination of protected products was carried out at the premises of LEAs. The Commissioner had drawn up confidentiality requirements, internal guidelines and procedures as well as provided training to relevant staff on the examination of protected products.

Cases involving legal professional privilege

25. Referring to paragraph 9.11 of the Annual Report, Dr Priscilla LEUNG expressed concern about the Commissioner's comment that there were still occasions when officers were careless or not vigilant enough in conducting covert operations. She asked whether LEAs had adopted measures to address the problem and whether training were provided on the handling of cases involving legal professional privilege ("LPP") and journalistic materials ("JM").

26. S for S responded that LEAs were particularly concerned about the proper handling of cases involving LPP or JM. He said that besides the provision of induction training and refresher training, workshops and experience-sharing sessions were organized for LEA officers involved in interception or covert surveillance. It was the objective of LEAs to strike a proper balance between law enforcement and protection of the rights of individuals.

27. Referring to paragraphs 4.14 and 4.15 of the Annual Report, Ms YUNG Hoi-yan asked how LEAs would deal with cases of heightened LPP likelihood and cases of assessed LPP likelihood after having reported such cases to panel judges.

28. S for S responded that an LEA applicant was required to state his assessment of LPP likelihood in his affidavit or statement in support of his application. Whenever there were any subsequent changes which might affect the assessment, such as heightened LPP likelihood or obtaining of LPP information, the LEA applicant had to notify the panel judge, who would immediately reassess if the criteria of the operations concerned were still met as regard to section 3 of ICSO, and if the prescribed authorization should be allowed to continue with additional conditions. He referred to the Commissioner's statement in

Action

paragraph 9.8 of the Annual Report that "The LEAs were observed to have recognised the importance of protecting information which might be subject to LPP/JM. They continued to adopt a very cautious approach in handling these cases."

29. Regarding cases assessed to involve LPP, Mr Holden CHOW sought information on when a prescribed authorization would be continued with additional conditions imposed and when it would be discontinued.

30. S for S explained that where LPP information had been obtained in an interception operation or there was a heightened likelihood of obtaining such information, the LEA concerned must report the matter to the panel judge as soon as practicable. The panel judge might impose additional conditions if the prescribed authorization was allowed to continue. In case of an operation being discontinued by the LEA concerned , a discontinuance report must be submitted to the panel judge.

Application for examination

31. Noting from paragraph 5.8 of the Annual Report that there were 11 applications for examination, among which one could not be entertained by the Commissioner because matters raised in the application were not within the ambit of the function of the Commissioner, Mr LEUNG Kwok-hung asked whether there was any further development regarding the latter application.

32. S for S responded that the Government had no information regarding the application concerned, which had been dealt with independently by the Commissioner in accordance with ICSO.

Definition of "communication" in existing legislation

33. Mr Nathan LAW said that a decrease in the number of prescribed authorizations might not reflect to a decrease in interception and covert surveillance by LEAs. He considered that the definition of "communication" in ICSO should be amended having regard to the proliferation of use of social media and instant message applications among members of the public. Deputy Secretary for Security 1 responded that the issue had been thoroughly deliberated by the Bills Committee on Interception of Communications and Surveillance (Amendment) Bill 2015. The existing definitions in ICSO were adequate and there was no need to amend the definitions.

Action

Surveillance device management

34. Mr Jimmy NG sought information on the existing system for recording the issue and return of surveillance devices. He asked whether improvement measures had been introduced in response to the Commissioner's comments on Report 3 in Chapter 6 of the Annual Report. He also asked whether consideration would be given to the use of Quick Response ("QR") Code in surveillance device management to avoid human errors.

35. S for S responded that LEAs had, in response to the recommendations of the first Commissioner, computerized its system for the issue and return of surveillance devices. In response to the Commissioner's comments on Report 3 in Chapter 6 of the Annual Report, the LEA concerned had enhanced its computer system for surveillance device management and strengthened training in the area for LEA officers. LEAs had already adopted the use of QR Code to facilitate accurate records of the issue and return of surveillance devices.

Other issues

36. Mr YIU Si-wing asked whether there were measures to avoid two or more LEAs carrying out interception on a subject at the same time. S for S responded that such a situation had not occurred in the past. He explained that under ICSO, all interception required the prescribed authorization of a panel judge. When making an application for a prescribed authorization, an LEA applicant had to submit information on whether any previous application regarding the subject person had been approved or refused.

37. Mr LAU Kwok-fan asked whether a person whose communication had been wrongly intercepted would be notified and whether the proposed apology legislation would be applicable to such a situation. S for S responded that under section 48 of ICSO, the Commissioner had to give notice to the relevant person when he discovered a case in which interception or covert surveillance had been carried out without prescribed authorization by an officer of the four LEAs covered by ICSO, subject to the requirement that such giving of notice would not be prejudicial to the prevention or detection of crime or the protection of public security. He said that at this stage when details of the proposed apology legislation had yet to be drawn up, it was too early to comment on its precise scope of application .

Action

38. Mr Nathan LAW expressed concern about pervious media reports that according to Wikileaks, ICAC had sought information about an encryption-cracking surveillance software from an overseas cyber intelligence firm. He also expressed concern about whether this was in contravention of the provisions in ICSO. The Chairman requested ICAC to provide a written response.

ICAC

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

(LC Paper Nos. CB(2)282/16-17(05) and (06))

39. Under Secretary for Security ("US for S") briefed Members on the Administration's measures to combat technology crimes and proposed creation of a permanent post of Chief Superintendent of Police ("CSP") in the Cyber Security and Technology Crime Bureau ("CSTCB"). With the aid of powerpoint presentation, Superintendent of Police, Cyber Security Division, Cyber Security and Technology Crime Bureau outlined the Police's measures to combat technology crimes and Assistant Commissioner of Police (Crime) ("ACP(C)") briefed Members on the proposal to create a permanent CSP post in CSTCB.

40. Members noted a background brief entitled "Proposed creation of a permanent Chief Superintendent of Police post for the Cyber Security and Technology Crime Bureau" prepared by the LegCo Secretariat.

41. The Chairman drew Members' attention to Rule 83A of the Rules of Procedure concerning the requirement of disclosing personal pecuniary interest.

Statistics relating to technology crimes

42. Mr POON Siu-ping sought information on the major types of technology crimes and their detection rate. Mr YIU Si-wing also sought information on the percentage of transnational technology crime cases and their crime detection rate.

43. US for S responded that LEAs of different countries faced similar challenges in investigating technology crime cases, which were mostly transnational in nature, and shared the same difficulties in gathering

Action

evidence. ACP(C) added that a majority of technology crime cases fell under the categories of online fraud and unauthorized access to computers, and email scam cases contributed to a large portion of the financial losses.

44. Referring to Enclosure 1 to the Administration's paper, Mr CHAN Chi-chuen and Mr LEUNG Kwok-hung requested the Administration to provide a breakdown of the 415 technology crime cases (as at 30 September 2016) under the category of "Others" under "Other Nature". The Chairman requested the Administration to provide such information in its paper for the Establishment Subcommittee.

Admin

Arrests and prosecutions under section 161 of the Crimes Ordinance

45. Ms Claudia MO said that the scope of section 161 of the Crimes Ordinance (Cap. 200) in relation to access to computer with criminal or dishonest intent was very broad. She pointed out that the proposal to create a CSP post had been voted down by the Establishment Subcommittee in the last session.

46. US for S responded that technology crimes were not confined to offences under section 161 of Cap. 200. There were more than 6 000 reports of technology crimes in a year, including Internet frauds, money laundering, bomb threat and wasteful employment of the Police. Among the prosecuted cases, about 90% were unrelated to offences under section 161 of Cap. 200. He added that for those prosecuted under section 161, the conviction rate was more than 90% with no negative comments by the Court.

47. Mr CHAN Chi-chuen expressed concern that the Police had not, despite Members' requests, provided a breakdown of prosecutions under section 161 of Cap. 200. US for S responded that the Police could not provide statistics they did not maintain. The Police had the overall figures of section 161 but did not maintain its breakdown into subsections. They had always provided LegCo with the overall figures of section 161. It was only the offence's breakdown which LegCo did not receive, for the simple reason that the Police did not maintain it. Crime statistics had been compiled and classified having regard to the need for the Police's law enforcement. It was inappropriate to alter the statistics system merely in response to isolated requests for a breakdown of any particular item.

Action

48. Mr Alvin YEUNG said that many social movement campaigners had been arrested for breach of section 161 of Cap. 200 but eventually prosecuted for breach of other offences. He requested the Admin Administration to provide information on the number of arrests under section 161 of Cap. 200. US for S agreed to examine the request to see if the statistics was available. He said that the charge preferred against an arrested person was based on the advice of the Department of Justice where it was needed. He pointed out that there were only 86 and 103 prosecutions under section 161 of Cap. 200 in 2014 and 2015, resulting in 80 and 93 convictions respectively. The Chairman requested the Administration to include the requested information in its paper for the Establishment Subcommittee.

Issues relating to the proposed creation of post

49. Mr POON Siu-ping asked whether the proposed CSP post would be an additional one or upgraded from the existing post of Senior Superintendent of Police. He also asked how the proposed post would be filled. Mr YIU Si-wing sought information on the qualification requirements for the proposed CSP post.

50. US for S responded that the proposed CSP post would be an additional one to be filled by internal promotion. It would be taken up by an officer conversant with policing work , with good skills and quality in decision-making on complex issues, coordinating relevant tasks and developing contingency plans as well as formulating the strategic direction for enforcement. The proposed post would be supported by officers with relevant computer and information technology qualifications and skills.

51. Dr Elizabeth QUAT expressed concern that financial losses relating to technology crime cases had increased to $1.87 billion for the first nine months of 2016. She said that the Democratic Alliance for the Betterment and Progress of Hong Kong supported the Administration's staffing proposal.

52. Mr Holden CHOW expressed concern that although the Police's Commercial Crime Bureau and the Narcotics Bureau, the staff establishment of which were similar to that of CSTCB, were each led by a CSP and the rank of officers leading overseas cyber crime units were at least equivalent to the rank of CSP, CSTCB was currently led by a Senior Superintendent of Police. US for S said that many overseas cyber crime

Action

units were led by an officer at a rank equivalent to Assistant Commissioner of Police. Without the leadership of a directorate officer with extensive relevant experience, it would be difficult in the long term for CSTCB to establish partnership and engagement with overseas LEAs.

53. Mr LEUNG Kwok-hung sought information on the qualifications of the staff of CSTCB. US for S responded that 98% of the officers appointed to CSTCB possessed relevant computer or information technology qualifications, among whom some possessed doctor or master degrees. A number of these officers were certified trainers of the INTERPOL for technology crimes and had assisted in professional training in cyber security and technology crimes for LEAs from other countries.

Cyber attacks

54. Mr CHAN Chun-ying expressed support for the proposed creation of CSP post. He asked how the creation of the proposed CSP post would contribute to the tackling of cyber attacks such as those referred to in paragraphs 2 and 3 of the Administration's paper. US for S responded that the proposed CSP post would be responsible for formulating strategies, steering management issues, capacity building, establishing partnership with local critical infrastructures and overseeing the launch of large-scale cyber security drills.

55. Mr Nathan LAW said that although he supported in principle the combating of technology crimes and cyber attacks, his personal computer had been subject to cyber attacks at national level on many occasions. He expressed concern about cyber attacks on the personal computers of political figures in Hong Kong and asked whether the Police had investigated into such cases or carried out thematic studies on cases of such a nature.

56. US for S responded that any person who believed his or her computer had been hacked should report the matter to the Police for investigation. He stressed that the Police had always carried out investigation into cases impartially in accordance with the law, regardless of the background or political orientation of the person making the report. With the consent of the person making the report, the Police could examine the computer for investigation and evidence gathering. He said that in regard to the trend and modus operandi of cyber crime, thematic researches were conducted on the trend and mode of operation of cyber crime.

Action

57. Dr CHENG Chung-tai said that he was not supportive of the proposed creation of the CSP post. He said that there were reports about 25% of distributed denial-of-service ("DDoS") attacks having been launched from the Mainland. According to a media report, DDoS attacks on certain websites of the Government were launched by a Mainland-based hacker group on 1 September 2016. He queried whether the Police had taken actions against such hacker groups.

58. Dr Elizabeth QUAT said that it was unfair to make groundless allegations on the Police's law enforcement work against hacker groups.

59. US for S responded that the sources of DDoS attacks had been found to be at different locations of the world, including locations in Asia and the Americas. The Police had paid every possible effort in combating all cyber attacks, irrespective of the identity of the person or group launching the attack.

[To allow sufficient time for discussion, the Chairman advised that the meeting would be extended by 15 minutes.]

60. Ms YUNG Hoi-yan expressed concern that a student had been convicted of launching more than 6 000 DDoS attacks at a local bank by a click of a link provided by a hacker group on a social media website. She asked whether measures were taken by the Police to combat such hacking links on social media websites. US for S responded that the Police would monitor crime trends and modus operandi in the cyber space. As for the flow of data traffic, the Police would only monitor that of the major critical infrastructures with which the Police had established partnership.

61. Mr MA Fung-kwok expressed support for the Police's effort in combating technology crimes and the proposed creation of CSP post. He sought information on the measures against cyber attacks at local critical infrastructures. Referring to paragraph 8 of the Administration's paper, he sought information on how the Police would launch the large-scale Cyber Security Drill.

62. US for S responded that there were five major sectors in the local critical infrastructures, i.e. banks and financial institutions, communication service, transport and maritime service, public utilities and government service. Assistance was provided to the operators of

Action

those critical infrastructures regarding the requirements on security, system design as well as simulation on cyber attacks. He said that CSTCB would launch a large-scale Cyber Security Drill in 2017 to test preparedness and response so as to strengthen the overall capabilities of local critical infrastructures in responding to cyber security incidents.

Admin

63. Mr Nathan LAW requested the Administration to provide supplementary information on the object and scope of cyber patrol, the manpower deployed for carrying out cyber patrol, as well as whether operators of online discussion boards were required to submit information on their members to the Police.

(*Post-meeting note*: The Administration subsequently advised that the requested information would be included in its paper for the Establishment Subcommittee.)

64. In concluding the discussion, the Chairman said that members generally agreed to the Administration's submission of the proposal to the Establishment Subcommittee.

65. There being no other business, the meeting ended at 4:40 pm.

Council Business Division 2
Legislative Council Secretariat
13 January 2017