

**立法會**  
**Legislative Council**

LC Paper No. CB(1)480/19-20  
(These minutes have been seen  
by the Administration)

Ref : CB1/PL/ITB

**Panel on Information Technology and Broadcasting**

**Minutes of meeting**  
**held on Monday, 13 January 2020, at 2:30 pm**  
**in Conference Room 3 of the Legislative Council Complex**

- Members present** : Hon Charles Peter MOK, JP (Chairman)  
Hon Elizabeth QUAT, BBS, JP (Deputy Chairman)  
Hon James TO Kun-sun  
Hon WONG Ting-kwong, GBS, JP  
Hon Mrs Regina IP LAU Suk-ye, GBS, JP  
Hon Claudia MO  
Hon YIU Si-wing, BBS  
Hon MA Fung-kwok, SBS, JP  
Hon CHAN Chi-chuen  
Ir Dr Hon LO Wai-kwok, SBS, MH, JP  
Hon Alvin YEUNG  
Hon SHIU Ka-fai, JP  
Hon YUNG Hoi-yan, JP  
Hon CHAN Chun-ying, JP
- Members absent** : Hon CHAN Han-pan, BBS, JP  
Hon CHUNG Kwok-pan  
Hon CHU Hoi-dick  
Hon HUI Chi-fung
- Members attending** : Hon Holden CHOW Ho-ding  
Hon KWONG Chun-yu

**Public officers  
attending**

: Agenda item IV

Commerce and Economic Development Bureau

Mr Clement LEUNG, JP  
Permanent Secretary for Commerce and Economic  
Development (Communications and Creative  
Industries)

Mr Keith GIANG  
Principal Assistant Secretary for Commerce and  
Economic Development (Communications and  
Creative Industries)A

Office of the Communications Authority

Mr Chaucer LEUNG  
Director-General of Communications

Mr Sanda CHEUK  
Deputy Director-General  
(Telecommunications)

Agenda item V

Innovation and Technology Bureau

Dr David CHUNG Wai-keung, JP  
Under Secretary for Innovation and Technology

Ms Eva YAM Ya-ling  
Principal Assistant Secretary for Innovation and  
Technology (3)

Office of the Government Chief Information Officer

Mr Victor LAM Wai-kiu, JP  
Government Chief Information Officer

Mr Jason PUN Si-keung  
Assistant Government Chief Information Officer  
(Cyber Security and Digital Identity)

**Clerk in attendance** : Mr Daniel SIN  
Chief Council Secretary (1)6

**Staff in attendance** : Ms Mandy LI  
Senior Council Secretary (1)6

Mr Patrick CHOI  
Council Secretary (1)6

Miss Yolanda CHEUK  
Legislative Assistant (1)6

---

Action

**I. Confirmation of minutes of meetings**

(LC Paper No. CB(1)242/19-20 -- Minutes of policy briefing held on 29 October 2019)

LC Paper No. CB(1)258/19-20 -- Minutes of meeting held on 11 November 2019)

The minutes of the meetings held on 29 October and 11 November 2019 were confirmed.

**II. Information paper issued since the last meeting**

(LC Paper No. CB(1)305/19-20(01) -- Letter dated 6 January 2020 from Hon Elizabeth QUAT regarding the overall strategy and the allocation of resources for promoting Hong Kong's innovation and technology development)

2. Members noted that the above paper had been issued for the Panel's information.

Promoting innovation and technology development in Hong Kong

3. The Chairman referred to a letter dated 6 January 2020 from the Deputy Chairman suggesting that an item be put on the agenda of a Panel meeting to discuss the overall strategy and the allocation of resources for promoting Hong Kong's innovation and technology development. The Chairman informed members that he had instructed the Secretariat to seek a

written response from the Administration on the Deputy Chairman's letter, and would, having considered other members' views, determine how the matter should be pursued, such as whether a joint meeting of this Panel and the Panel on Commerce and Industry ("CI Panel") should be held to discuss the subject matter or whether members of CI Panel should be invited to join the discussion of the item at a Panel meeting. Members had no objection to the proposed arrangement.

*(Post-meeting note: The Administration's written response was circulated to members vide LC Paper No. CB(1)458/19-20(01) on 13 March 2020.)*

#### Data centre development in Hong Kong

4. The Chairman said that, at the meeting on 9 December 2019, Mrs Regina IP suggested that the Administration should brief the Panel on the development of data centres in Hong Kong. The Secretariat had requested the Administration to provide a response on the issue raised. According to the Administration, the Office of the Government Chief Information Officer ("OGCIO") was conducting a review of the current facilitation measures for data centre development. Meanwhile, there was a judicial review case filed by a company against Hong Kong Science and Technology Parks Corporation. In view of these developments, the Administration suggested that an information paper setting out the latest position regarding the policy and facilitation measures on data centre development would be submitted to the Panel in April 2020. The Chairman further said that members' views would then be sought on the need for a meeting to be held to discuss the issue in the light of the Administration's response. Members had no objection to the proposed arrangement.

### **III. Date of next meeting and items for discussion**

(LC Paper No. CB(1)306/19-20(01) -- List of outstanding items for discussion

LC Paper No. CB(1)306/19-20(02) -- List of follow-up actions)

#### Regular meeting on 10 February 2020

5. Members noted that the next regular Panel meeting would be held on Monday, 10 February 2020 at 2:30 pm to discuss the following items:

(a) Strengthening regulation of person-to-person telemarketing calls

("P2P Calls"); and

- (b) Capital Works Reserve Fund Head 710 Computerization Major Project – Electronic Recordkeeping System.

6. The Chairman said that as members of CI Panel had expressed concerns over the proposed regulation of P2P Calls, they would be invited to join the discussion of the item at the regular meeting scheduled for 10 February 2020. Members had no objection to the proposed arrangement.

*(Post-meeting note: Members were informed under LC Paper No. CB(1)395/19-20 dated 6 February 2020 that on consideration of the latest situation of the novel coronavirus infection, the Chairman directed that the meeting on 10 February 2020 be rescheduled to a later date.)*

Visit to Smart Government Innovation Lab and Hong Kong Applied Science and Technology Research Institute in February 2020

7. The Chairman informed members that the Panel would conduct a visit to the Smart Government Innovation Lab and the Hong Kong Applied Science and Technology Research Institute on Tuesday, 11 February 2020. By the deadline for reply, 10 Panel members and four non-Panel Members had signed up for the visit.

*(Post-meeting note: Members were informed under LC Paper No. CB(1)388/19-20 dated 3 February 2020 that on consideration of the latest situation of the novel coronavirus infection, the Chairman directed that the visit to Smart Government Innovation Lab and Hong Kong Applied Science and Technology Research Institute originally scheduled for 11 February 2020 be rescheduled to a later date.)*

**IV. Hong Kong's external telecommunications connectivity**

(LC Paper No. CB(1)306/19-20(03) -- Administration's paper on Hong Kong's external telecommunications connectivity

LC Paper No. CB(1)306/19-20(04) -- Paper on Hong Kong's external telecommunications connectivity prepared by the Legislative Council Secretariat (Background brief)

Briefing by the Administration

8. At the invitation of the Chairman, Permanent Secretary for Commerce and Economic Development (Communications and Creative Industries) ("PS(CCI)") and Deputy Director-General (Telecommunications), Office of the Communications Authority ("DDG(T)/OFCA") briefed members on the current situation of Hong Kong's external telecommunications ("ET") connectivity and reported on its future development. PS(CCI) highlighted that Hong Kong had been holding a leading position internationally in its capacity of ET facilities. With the aid of a powerpoint presentation, DDG(T)/OFCA informed members that while ET capacity in Hong Kong was sufficient to meet its medium to long-term demand, in anticipation of the continual increase in the demand for ET services expected to be brought about by, among others, the fifth generation mobile telecommunications ("5G") technology, the Administration proposed to make available suitable sites in Chung Hom Kok Teleport for the construction of satellite earth stations and additional submarine optical fibre cable landing facilities. In addition, the Administration was proactively exploring with satellite operators the feasibility of relocating the existing satellite earth stations for telemetry, tracking and control of satellites in orbit from Tai Po to Chung Hom Kok Teleport, with a view to removing completely the 5G restriction zone in Tai Po in the long run. Details of the briefing were given in the Administration's paper (LC Paper No. CB(1)306/19-20(03)).

*(Post-meeting note: A soft copy of the powerpoint presentation materials (Chinese version only) was issued to members vide LC Paper No. CB(1)313/19-20(01) by email on 13 January 2020.)*

Discussion

*Competitiveness of Hong Kong's external telecommunications sector*

9. Mr CHAN Chi-chuen and the Chairman asked how Hong Kong was performing in its ET connectivity as compared to its counterparts in the Asia-Pacific region. PS(CCI) responded that it was unclear whether our neighbouring economies made public similar information that would enable such comparison. The Administration would try to obtain relevant data from various sources for members' reference after the meeting. As evidenced by the fact that telecommunications operators had been taking steps to further increase the capacity of Hong Kong's ET networks when only 11% of the overall designed capacity was used, PS(CCI) was of the view that international investors considered Hong Kong a very attractive centre for ET facilities. Hong Kong also had an excellent geographic location for the development of earth stations

for satellites covering the Asia-Pacific region.

10. Mr CHAN Chi-chuen asked whether Hong Kong was competitive in terms of the costs for maintaining ET infrastructure. PS(CCI) responded that the Administration did not have information on the costs of maintaining ET infrastructure in different cities, which was commercially sensitive information. The Chairman commented that operators would often determine where to install the landing facilities based on the geographic location and the associated costs of all potential sites. Hong Kong, being at the heart of Asia, had a definite geographical advantage over its competitors.

11. Ms Claudia MO asked whether the construction of an external submarine optical fibre cable system between Los Angeles and Hong Kong was aborted due to national security reasons as suggested in news reports. Mr CHAN Chi-chuen asked whether incidents like this would affect Hong Kong's competitiveness in ET connectivity and if so, whether the Administration would provide other incentives to restore Hong Kong's competitiveness.

12. PS(CCI) said that the relevant construction works in Hong Kong waters had been completed and the said cable system was scheduled for service commissioning within this year. The submarine cable system would straddle multiple jurisdictions and the operator of the system would liaise with relevant national authorities on compliance issues. The Administration had not received any request for assistance from the operator in this regard, but would be prepared to provide assistance if necessary.

13. The Chairman asked where the above external submarine optical fibre cable system between Los Angeles and Hong Kong would land in Hong Kong and whether the necessary administrative arrangements had been completed. PS(CCI) said that OFCA had been providing one-stop service which helped coordinate operators' applications for approval by various departments within Hong Kong, with the objective of helping them save processing time and compliance costs. The cable system would land in Deep Water Bay and the required administrative arrangements, including consultation with the relevant District Council, had been completed.

14. The Chairman reflected concerns from the trade that the Administration had not formulated policies to enable the satellite television industry to flourish in Hong Kong, and many regional operators had moved their investment to Singapore. PS(CCI) said that the television broadcasting policy in Singapore might not be directly comparable to that of Hong Kong, as the two governments have different regulatory frameworks and supportive measures. Besides, the wide use of the 3.4 – 4.2 GHz band for satellite services by the relevant

authorities in the Asia-Pacific region might pose difficulty for their re-allocation of the 3.5 GHz band for 5G development. PS(CCI) considered that the overall development of the satellite television industry in Hong Kong was satisfactory.

15. The Chairman commented that the policies on Hong Kong's ET capacity and the development of data centres were closely correlated, and suggested that relevant bureaux should coordinate with each other on formulating such policies. PS(CCI) responded that the Commerce and Economic Development Bureau had been working hand in hand with the Innovation and Technology Bureau on implementing the relevant policies. For instance, facilitated by the two bureaux, a submarine optical fibre cable had recently been built between Tseung Kwan O and Chai Wan for use by data centres.

16. The Chairman asked the Administration to provide more details about the overland optical fibre cables connecting to the Mainland. Director-General of Communications, OFCA ("DGC/OFCA") said that all the 20 overland cables were installed at crossing points such as Lo Wu, Lok Ma Chau, Man Kam To and Shenzhen Bay. These cables were extended to continental Europe or the Middle East via the Mainland. Looking ahead, completion of the Hong Kong-Zhuhai-Macao Bridge would enable new overland cables for better connectivity with the Greater Bay Area.

*Relocation of satellite earth stations from Tai Po*

17. Ms Claudia MO enquired about the justifications and urgency for exploring the feasibility of relocating the existing satellite earth stations for telemetry, tracking and control of satellites in orbit from Tai Po to Chung Hom Kok Teleport. Mr CHAN Chun-ying asked when the relocation project and the preparation for Chung Hom Kok Teleport were expected to complete, how many operators the Teleport could host, and whether 5G services would be available in the restriction zones in the interim.

18. PS(CCI) explained that from 1 April 2020, the Communications Authority ("CA") would re-allocate the 3.5 GHz band currently used for the operation of satellite earth stations for mobile service developments, although the satellite earth stations would still need to make use of the 3.4 – 3.7 GHz band to operate the satellites already launched. To ensure that satellite services operated by these satellite earth stations could coexist with future 5G services, CA had set up restriction zones in Tai Po and Stanley to constrain the deployment of mobile base stations operating in the 3.5 GHz band in these areas. Operators might make use of other 5G frequency bands (e.g. the 3.3 GHz, 4.9 GHz and 26/28 GHz bands) or re-farm spectrum in other bands currently used for providing the second to the fourth generation mobile services under their existing licences to



provide 5G services within the restriction zones. PS(CCI) noted that the operators were aware of the arrangement and there was no delay in their plan to launch 5G commercial services in the second quarter of this year, despite the 5G restriction zone in Tai Po.

19. PS(CCI) added that the Administration had been exploring with satellite operators the feasibility of relocating the satellite earth stations in Tai Po. It would involve identifying suitable land lots at Chung Hom Kok Teleport, seeking approval for using the sites, preparing land documents, carrying out civil engineering works to construct the new satellite earth stations and ancillary buildings/facilities before shutting down the existing facilities in Tai Po. Even if all the parties were able to fully cooperate with each other, the whole process would take several years to complete. The Administration would do its best to facilitate the relocation.

*Abundance of Hong Kong's external telecommunications capacity*

20. Mr MA Fung-kwok noted that the equipped capacity of the existing ET infrastructure accounted for only about 11% of the overall designed capacity, and the capacity of Hong Kong's ET networks would more than double the current capacity after the eight new external submarine optical fibre cable systems were put into service by 2023. Mr MA asked how much the launch of 5G service was expected to lift the demand for ET services; and how abundant the capacity of the telecommunications infrastructure in 2023 would compare to the demand.

21. PS(CCI) replied that during the initial implementation stage of the development of 5G service, there would be difficulty in predicting the extent of increase in data transmission demand it might cause. While 5G technology was in theory suitable for various purposes, there was not yet wide adoption among overseas markets with 5G technology in service. As there seemed to lack a killer application necessitating the use of 5G technology and the initial user feedback overseas had not been overwhelmingly positive, it was difficult to determine at the moment how popular 5G would become in the near term. However, given the large margin between the equipped capacity and the overall designed capacity of the existing ET infrastructure, the Administration was confident that Hong Kong's medium to long-term ET demand would be met, while the currently unused land lots could be deployed for future expansion of ET infrastructure should there be additional demand.

22. DGC/OFCA added that the total equipped capacity of ET facilities increased by more than 400% over the past five years, and at present the usage represented only 11% of the overall designed capacity. By installing relevant

termination equipment, the remaining 89% of capacity could be released for use. By 2023, the capacity of Hong Kong's ET networks would more than double the current capacity after the eight new external submarine optical fibre cable systems were put into service. The capacity would be further enhanced with additional ET infrastructure to be constructed on the land lots to be released in Chung Hom Kok Teleport. DGC/OFCA was confident that the capacity of ET infrastructure would be adequate in the 5G era.

23. The Chairman commented that while the popularization of 5G services might affect the demand for ET services, purely local 5G data transmission would not consume ET capacity. In comparison, Hong Kong's status as a regional telecommunications hub would be a more relevant factor affecting the demand for ET capacity.

## **V. Update on information security**

(LC Paper No. CB(1)306/19-20(05) -- Administration's paper on update on information security

LC Paper No. CB(1)306/19-20(06) -- Paper on information security prepared by the Legislative Council Secretariat (Updated background brief))

### Briefing by the Administration

24. At the invitation of the Chairman, Under Secretary for Innovation and Technology ("US for IT") briefed members on the latest situation of information security in Hong Kong and Government's work in information security in the past year. Details were set out in the Administration's paper (LC Paper No. CB(1)306/19-20(05)).

### Discussion

#### *Overall situation of information and cyber security*

25. Referring to the statistics on technology crimes handled by the Hong Kong Police Force ("HKPF"), as set out in Annex II to the Administration's paper (LC Paper No. CB(1)306/19-20(05)), Mr CHAN Chi-chuen asked the Administration to provide a breakdown by nature of the cases of technology-related crimes, including the number of cases reported, number of arrests, number of prosecutions and number of convictions made. Mr Holden CHOW

expressed a similar view. The Chairman shared the views of Mr CHAN and Mr CHOW, and commented that the Administration should obtain the relevant information from the Security Bureau ("SB") and provide relevant breakdown of information to facilitate consideration and discussion by the Panel in future. US for IT said that the statistics on technology crimes referred to the number of cases reported. He undertook to ask HKPF to provide information requested by Mr CHAN after the meeting.

26. Mr KWONG Chun-yu noted that HKPF recorded a total of 4 573 technology crime cases in the first three quarters of 2019, showing a decline when compared with 2018, whereas the average monetary loss per case had increased from about \$350,000 in 2018 to about \$490,000 in 2019. Expressing concern about the total financial losses caused by technology crimes which stood at \$2,248 million in the first three quarters of 2019, Mr KWONG asked what measures the Administration would take to prevent recurrence of similar incidents, and the reasons for the increase of monetary losses. Mr Holden CHOW made a similar query.

27. Government Chief Information Officer ("GCIO") responded that as the global cyber security landscape had been changing, OGCI worked closely with the Hong Kong Computer Emergency Response Team Coordination Centre ("HKCERT") and HKPF to promote public awareness of information security, such as disseminating information on security-related issues and providing advice on preventive measures against security threats. Besides, the Hong Kong Internet Registration Corporation Limited ("HKIRC") had launched a new and free website scanning service to assist small and medium enterprises ("SMEs") in identifying potential security vulnerabilities. About 300 local SMEs had benefited from the service since its launch in June 2019. GCIO further said that in the 2018/2019 school year, OGCI collaborated with professional bodies to organize school visits, during which OGCI had conveyed information security messages to more than 10 000 teachers and students.

28. Mr KWONG Chun-yu commented that the damages of technology crimes caused to the victims were heavy. He sought the Administration's views regarding the financial losses of \$2,248 million due to technology crimes. GCIO replied that, to raise public awareness and knowledge about information security, OGCI would step up efforts to disseminate information security messages to the public through various promotional channels such as broadcasting radio announcements in the public interest.

29. Mr Holden CHOW pointed out that many technology crimes were cross-boundary in nature and committed outside Hong Kong, thus posing investigation difficulties for the Police. He asked how the Administration would combat

cross-boundary technology crime, such as whether and how the Administration would strengthen cooperation with overseas stakeholders and law enforcement agencies to counter prevalent technology crimes and cyber threats, and stop the payment to fraudsters being remitted through Hong Kong.

30. GCIO explained that as the subject matter of technology crimes investigations fell within the remit of SB and HKPF, he did not have relevant information. GCIO said that, to his understanding, the Police would exchange intelligence with various law enforcement agencies to keep track of the crime trend and study the ways to combat cross-boundary criminal activities.

*Measures to tackle cyber security threats in Government*

31. Mr CHAN Chi-chuen queried whether HKPF had brought some Russian-made hacking software which allowed them to unlock smartphones and access user data inside. He was particularly concerned about whether the acquisition of such software was ethical or legal. He also asked whether bureaux and departments ("B/Ds") including HKPF had consulted OGCI's views prior to their procurement of information technology ("IT") security software.

32. GCIO responded that B/Ds would, according to their needs, implement security technology measures and procure IT security software. While there was no need for B/Ds, including HKPF, to consult OGCI's views prior to their procurement of relevant equipment and software, B/Ds should ensure that the procurement would comply with relevant laws and regulations. In response to another enquiry from Mr CHAN Chi-chuen as to whether HKPF had sought advice from OGCI on the procurement of relevant security software, GCIO replied in the negative.

33. Noting that OGCI had an established mechanism to assist B/Ds in conducting webpage scanning and penetration testing, Mr YIU Si-wing sought information on the government departments that were more vulnerable to cyber attacks and the major types of government services being attacked. He took the view that the Administration should actively share relevant cyber threat intelligence with large enterprises as well as SMEs as it would provide useful pointers for local companies to strengthen their precautionary measures.

34. GCIO indicated that in 2019, OGCI had received a total of 12 information security incident reports from government departments, about half of which involved ransomware while some incidents were related to distributed denial-of-service ("DDoS") attacks. When an information security incident occurred, B/Ds had to report the incident to OGCI and take appropriate responsive measures. GCIO further informed Panel members that

ransomware attacks were typically delivered by phishing emails. If users clicked the links or opened the attachments in phishing emails, their devices might get infected by the malware. Some files would then be encrypted and a ransom demanded. Given the worsening threats of phishing emails, OGCI launched a "Government-wide Phishing Drill Campaign" in May 2019 to alert civil servants of the proper way to handle emails and watch out for phishing emails. Meanwhile, OGCI also stepped up publicity efforts to promote public awareness of the phishing attacks.

35. The Chairman asked if the Administration had anticipated any different emerging cyber threats arising from the increasing adoption of cloud computing services by government departments, and how the Administration would help B/Ds manage those risks. To cope with the rapid technological development such as the fifth generation mobile services and Internet of Things, the Chairman was concerned about how the Administration would prepare departments and help the industry to be prepared to tackle any new risks involved.

36. GCI replied that OGCI had commenced a new round of review on the "Government IT Security Policy and Guidelines". The review would examine, inter alia, the existing government regulations, policies and guidelines related to IT security including that of Internet of Things, and recommend appropriate updates with reference to latest international standards ISO/IEC 27701 on the protection of privacy in IT systems. OGCI expected to complete the review within 2020 and publish the updated guidelines for reference by the public. GCI added that OGCI had conducted a comprehensive review in 2016 on the "Government IT Security Policy and Guidelines" to strengthen the security requirements in individual areas, including the protection and encryption requirements for information systems and data assets.

*Measures to strengthen information security management of enterprises*

37. Mr YIU Si-wing noted that HKIRC had assisted about 300 SMEs with ".hk" domain names in scanning malware in the system, and provided information security improvement solutions to them. He asked how many websites of enterprises were registered under the ".hk" domain, and the proportion of local SMEs which had received the service. Apart from scanning malware in the system, Mr YIU enquired if concrete plans were in place to render continuous support to SMEs, such as recommending preventive measures and encouraging SMEs to enhance their cyber security measures through the Technology Voucher Programme ("TVP").

38. GCIO advised that there were about 130 000 enterprises registered with ".hk" domain names. OGCIO was exploring with HKIRC on how best to raise enterprises awareness of information security management and the related technologies. In addition to providing free website scanning services for SMEs, HKIRC would encourage local enterprises, including SMEs, to adopt solutions for enhancing their cyber security through TVP, so as to further mitigate information security risks.

39. Mr YIU Si-wing and the Chairman commented that SMEs' subscription of the website scanning service was far from satisfactory. Mr YIU considered that there was much room for the Administration to foster the use of website scanning services by SMEs. He suggested that the Administration should actively work with industry associations to organize seminars so as to enhance the promotion of TVP and promote the awareness of large enterprises and SMEs on system security risks. The Chairman said that the Administration should promote cyber security awareness and best practices in different sectors such as travel industry, import and export industry given the importance of cyber security to individual sectors.

40. GCIO informed members that HKCERT would continue to collaborate with the industry associations and HKIRC to organize thematic seminars with a view to further promoting cyber security awareness. In the past year, more than 20 seminars were held and attended by about 2 000 practitioners from various sectors, including financial services, healthcare, retail and trade, property management, hotels and tourism, manufacturing, education, IT, etc.

41. The Chairman requested the Administration to consider enhancing support measures for other SMEs and organizations without ".hk" websites, so as to help them cope with potential information security risks and enhance overall cyber security in Hong Kong. GCIO responded that the website security scan services were mainly provided for all .hk domain owners to identify and alert them to potential security issues. That said, HKIRC would review the need to extend the services as appropriate.

42. Ms Claudia MO noted that the number of reported DDoS cases in 2019 was more than double the number in 2018. She enquired about the origins and the motives of those cyber attacks. Ms MO also expressed concern on the offence of access to computer with criminal or dishonest intent. She said that some news websites had been subject to cyber attacks from state-level hackers, and asked whether and how the Administration would take the initiative to assist the organizations, particularly those news websites, in taking measures to guard against cyber threats.

43. GCIO advised that most of the DDoS attacks were launched from other regions outside Hong Kong. As observed from local and overseas technology crimes, the motivation behind cyber attacks was mainly to gain commercial advantage. For example, cyber attacks had rendered a number of websites paralyzed and the attackers demanded ransom to be paid. While the Police was responsible for a wide range of duties in tackling cybercrime, individual organizations could seek assistance from HKCERT in case of cyber attack.

44. Ms Claudia MO further sought the Administration's advice on whether a victim of ransomware should pay the ransom, and she further queried whether the affected users could reserve the rights to claim compensation from the Administration if they had suffered from a further loss after refusing to pay a ransom. GCIO stressed that, as advised by the Police, government departments and other users should not pay any ransom when demanded. The Chairman echoed the GCIO's view. GCIO further said that OGCI had reminded B/Ds to perform data backup, which would provide a way to restore original data.

45. The Chairman was of the view that financial gain was the most common objective of attacks. The Chairman pointed out that many enterprises and news websites had already strengthened their cyber security measures such as using the cloud platform to protect their information systems and data assets. Given that cyber threats, cyber attacks and risks continued to grow, the Chairman asked the Administration to step up promotional efforts focusing on the follow-up actions that should be taken in the aftermath of the attack.

*Law reform proposals under consideration or in the process of being implemented*

46. Noting that a sub-committee under the Law Reform Commission of Hong Kong ("LRC") had commenced a study on cybercrime, Mr CHAN Chi-chuen enquired whether the Administration would introduce relevant legislative proposal(s) to combat cybercrime before the completion of the sub-committee's study. US for IT responded that as LRC had established a sub-committee to study the topic of cybercrime, the Administration currently had no plan to introduce any legislative amendment before the completion of the study but would closely monitor its progress.

47. The Chairman remarked that in light of the impact brought about by the Court of Final Appeal's judgment on an appeal case handed down on 4 April 2019 with regard to section 161 of the Crimes Ordinance (Cap. 200)<sup>1</sup>,

---

<sup>1</sup> On 4 April 2019, the Court of Final Appeal held in *Secretary for Justice v Cheng Ka Yee & 3 Others* [2019] HKCFA 9 that the text, context and purpose of section 161 (1)(c) of the Crimes Ordinance (Cap. 200) pointed towards construing the provision so that it does not

SB had indicated that it would consider introducing relevant legislation, such as provisions against voyeurism, reviewing "access to computer with criminal or dishonest intent" under section 161 of Cap. 200, reviewing existing legislation on cybercrime, etc. The Chairman urged the Administration to commence the relevant legislative process as early as practicable.

*Protection of privacy*

48. Mr Alvin YEUNG commented that the relevant stipulations and penalties under the Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO") were ineffective in regulating leakage of personal data. With reference to the General Data Protection Regulation adopted by the European Union, Mr YEUNG urged the Administration to consider amending PDPO so as to impose more stringent sanctions against data leakage and to ensure protection of privacy.

49. GCIO replied that in view of the recent incidents relating to leakage of personal privacy and data, the Constitutional and Mainland Affairs Bureau ("CMAB") was reviewing and studying possible amendments to PDPO jointly with the Office of the Privacy Commissioner for Personal Data ("PCPD") with a view to strengthening the protection of personal data, in particular with respect to mandatory personal data breach notification mechanism and data retention period. OGCIO would provide technical advice as necessary. US for IT added that government departments and private sector were subject to the regulations of PDPO.

50. In response to Mr Alvin YEUNG's enquiry on the demarcation of duties between CMAB and Innovation and Technology Bureau in the review of PDPO, GCIO advised that with reference to the latest development in other places, OGCIO had planned to commence a study in 2020 to work out a set of technical guidelines on the application of artificial intelligence ("AI") and big data analytics for internal adoption within the Government, including the handling of ethical and privacy issues arising from such application, in order to assist government departments in planning and applying emerging technologies like AI and big data analytics. OGCIO would liaise closely with PCPD in the course of the study.

51. Mr Alvin YEUNG further asked whether the Administration would identify technology solutions to enhance and improve the privacy management programmes of government departments, so as to avoid the recurrence of similar

---

extend to the use of the offender's own computer. In other words, on its proper construction, section 161(l)(c) of Cap. 200 does not apply to the use by a person of the person's own computer, not involving access to another's computer.



incidents relating to leakage of personal privacy and data, such as the loss of Registration and Electoral Office notebook computers containing voters' information. GCIO advised that OGCIIO endeavoured to promote the awareness and knowledge of cyber security threats, preventive measures and best practices among the industries and enterprises. Meanwhile, OGCIIO would continue with the on-going efforts of disseminating cyber security information to the public through various channels, including education programmes, publicity programmes on radio, etc.

52. The Chairman enquired how OGCIIO could ensure that all B/Ds would comply with the security requirements of the Government. GCIO responded that all B/Ds were required to conduct information security risk assessments and audits once every two years to ensure that they had adopted effective security measures. In addition, OGCIIO conducted independent information security compliance audits for all B/Ds every two years to assist them in continuously improving their security management systems to tackle emerging security threats. OGCIIO had completed the previous round of audits for all government B/Ds in mid-2019.

**VI. Any other business**

53. There being no other business, the meeting ended at 4:14 pm.