(Translation) LC Paper No. ESC52/16-17(01)

香港特別行政區政府
保安局

香港添馬添美道 2 號

The Government of the
Hong Kong Special Administrative Region
Security Bureau

2 Tim Mei Avenue, Tamar, Hong Kong

本函檔號 Our Ref.: SBCR 1/1805/13

來函檔號 Your Ref.:

電話號碼 TEL. NO.: 2810 2632
傳真號碼 FAX. NO.: 2877 0636

6 February 2017

Clerk to the Establishment Committee
Legislative Council Complex
1 Legislative Council Road
Central, Hong Kong
(Attn: Ms Connie Szeto)

Dear Ms Szeto,

EC(2016-17)23
Proposed creation of one permanent post of Chief Superintendent of Police in the Hong Kong Police Force ("HKPF") to lead the Cyber Security and Technology Crime Bureau ("CSTCB")

Regarding Hon Nathan LAW Kwun-chung's request for information from the Government in his letter to the Chairman of the Establishment Subcommittee dated 3 February 2017, our response is as follows:

(I) Police establishment and effectiveness of the work of CSTCB

1. It has always been the objective of HKPF to maintain Hong Kong as one of the safest and most stable cities in the world. To achieve this, HKPF must be equipped with sufficient manpower resources. Compared with the ratio of regular police strength to population of other metropolitan cities, our police force is of a moderate scale. In fact, it is difficult to draw a direct comparison because the scope of police responsibilities varies with places and police establishment is subject to local circumstances. With diversified functional responsibilities, HKPF have to, apart from maintaining law and order in our society, perform certain duties normally not required to be carried out by police forces elsewhere, such as patrolling the boundary

areas, coastlines and railways; handling explosives; and implementing counter-terrorism initiatives. All along, HKPF have conducted timely assessment on manpower needs in the light of circumstances of the local community, with a view to maintaining an effective police force, preventing and detecting crimes, ensuring public safety and safeguarding the lives and property of the public.

2. The annual numbers of technology crime offenders arrested by the Police from 2012 to 2016 are tabulated below:

Year	Number of arrestees
2012	465
2013	679
2014	691
2015	825
2016	907

The Police do not maintain prosecution and conviction figures on technology crimes.

3. During the two years since its establishment, CSTCB carried out a number of thematic researches, mainly covering the trend of cyber attacks (e.g. ransomware and botnet), mode of operation (e.g. naked chat blackmail and email scam) and technology trend (e.g. Internet-of-Things and cloud technology).

4. With emerging and evolving modes of operation, global web attacks involve increasingly complex professional techniques. Such attacks, which may originate from anywhere in the world, pose genuine and direct impact on the global community. Coupled with growing prevalence of sophisticated malware on various computer platforms, members of the public in Hong Kong are exposed to grave risks. For the purpose of crime prevention and detection, CSTCB will, having regard to factors such as the trend of international cyber crimes, mode of attacks and malware development, carry out thematic researches on various hacker syndicates.

5. The Cyber Security Centre under CSTCB operates around the clock to strengthen communication and co-ordination between the Police and various stakeholders, with a view to preventing possible attacks and responding to them more effectively, including the rendering of immediate assistance in case of cyber security incidents involving

critical infrastructures. Given the rapid advancement of modern technology, the wrestle and competition between law enforcement agencies ("LEAs") and cyber criminals on technological and technical fronts are intensifying. The Police consider it inappropriate to make public the figures on cyber attacks against critical infrastructures.

6. From 2012 to 2016, a number of large-scale cyber attacks were launched against Hong Kong. Some notable examples include:

(a) blackmail by Distributed Denial of Service attacks;

(b) ransomware incidents;

(c) intrusions into the SWIFT system; and

(d) cases involving unauthorised share trading transactions.

7. The annual loss resulting from technology crimes from 2012 to 2016 are tabulated below:

Classification	Loss ($ million)				
	2012	2013	2014	2015	2016
Online game-related	0.8	1.6	2.1	2.4	2.8
Online business fraud	26	43.1	48.4	40.4	32.1
Unauthorised access to computers	189.6	766.2	1,004.1	1,462.4	1,813.2
Others	124	106	146.1	323.7	452.7
Total	340.4	916.9	1,200.7	1,828.9	2,300.8

8. The three divisions under CSTCB are:

(a) Technology Crime Division – responsible for crime investigation and digital forensic examination;

(b) Cyber Security Division – responsible for cyber security tests, thematic researches, E-security audits, incident response, overseas and local liaison, cyber watch, and analysis of intelligence on cyber attacks; and

(c) Intelligence and Support Division – responsible for gathering, collating and analysing information relating to technology crimes and cyber security, conducting intelligence-led investigation on crime trend and mode of operation, and advising on tactics to combat technology crimes.

(II) Cyber Patrol

On cyber patrol, the Police currently adopt a three-tier intelligence framework to gather intelligence through intelligence units at the levels of headquarters, regions and police districts. The Internet is open to all and hence its users are faced with the same criminal threats as in the physical world. Similar to the Police patrolling the streets for crime prevention in the physical world, it is also necessary for them to spot and take action against possible criminal activities in the virtual Internet world. Therefore, for the purpose of crime prevention and detection, not only CSTCB but also relevant departments of HKPF conduct cyber patrol to search for relevant information via public platforms on the Internet on a need basis. According to operational priorities, specific and professional search will be performed via such platforms for possible crime-related information. Information gathered on patrol will enable the Police to allocate resources more aptly and analyse the prevailing crime trend, in a bid to combat various types of crimes.

Be it in the virtual or physical world, gathering criminal intelligence remains one of the key elements for effective policing. Where necessary for the purpose of crime prevention and detection, relevant departments of HKPF will select targets for cyber patrol through different channels based on specific strategies and the crime trend, with a view to gathering relevant online information as criminal intelligence to help combat related crimes, such as fraud, illegal soccer gambling activities, publication of child pornography, trafficking of dangerous drugs and criminal intimidation. Should operational needs arise, the Police will make deployment and take necessary actions as in the physical world.

We stress that the Police may, as and when necessary, request information or co-operation from relevant persons or organisations, including Internet service providers and Internet platforms, in accordance with relevant laws, established procedures or codes. The Police do not request information of netizens from such providers or platforms on a regular basis.

The Police do not maintain the statistics as requested in Hon LAW's letter.

(III) Hacking Software

Hackers launch cyber intrusions and attacks via different channels, including the use of software to hack into systems and commit crimes. LEAs must keep abreast of the ever-changing technology to discern their mode of operation, the trend of cyber crimes and relevant technological development, thereby effectively formulating strategies to address and combat such crimes. They must also enhance public awareness towards information security so as to safeguard against potential security risks and cyber attacks in the virtual world.

To prevent and combat crimes effectively, LEAs will gather intelligence through various channels, having regard to the case nature. All intelligence must be gathered by legitimate means and in accordance with established procedures or codes. Irrespective of the technology adopted by LEAs in gathering intelligence, such an operation must be authorised by a panel judge or a designated authorising officer if it may constitute interception of communications or covert surveillance as defined by the Interception of Communications and Surveillance Ordinance. Every stage of the operation is subject to strict control under the Ordinance. The Commissioner on Interception of Communications and Surveillance also monitors the compliance with various requirements under the Ordinance by LEAs concerned.

As for evidence collection, the Police will, depending on the circumstances of each case, employ different methods for crime investigation which involves various procedures, such as contacting different people to obtain information related to the case, interviewing witnesses and taking statements. When necessary, LEAs may apply to courts according to relevant ordinances for court orders to seize documents or information from any organisations/persons (including Internet service providers). However, the Police must comply with the requirements under relevant legislations, regardless of the means of evidence collection adopted in investigation.

(Andrew Tsang)
for Secretary for Security

c.c.
HKPF (CSTCB)