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

香港中區立法會道 1 號
立法會綜合大樓
人事編制小組委員會秘書
（經辦人：司徒少華女士）

司徒女士：

EC(2016-17)23
建議在香港警務處開設 1 個總警司常額職位
以領導網絡安全及科技罪案調查科

就羅冠聰委員 2017 年 2 月 3 日致人事編制小組委員會主席信件中要求政府提供的資料，我們回應如下：

（一） 警隊編制以及「網絡安全及科技罪案調查科」的工作成效

1. 香港警隊一直的目標，是讓香港繼續成為世界上其中一個最安全及穩定的城市。為達到這目標，警方必須配備足夠的人手資源。若與其他大都會城市正規警務人員人手與人口比例作比較，香港的警力屬中等規模。事實上，各地警察的職責範圍均有所不同，而各地警隊編制亦視乎當地的情況而定，因此難以直接比較。香港警隊的職能範疇多元化，除負責維持社會治安外，也要執行一些外地警察一般無須執行的職務，例如邊境、海岸和鐵路的巡邏、爆炸品處理、反恐工作等。香港警隊一直因應本地社會的情況，適時評估人手需要，以維持一支高效的警隊，防止及偵破罪案，確保公共安全和保障市民生命財產。

2. 2012 至 16 年警方就科技罪案每年的拘捕人數如下:

年份	拘捕人數
2012	465
2013	679
2014	691
2015	825
2016	907

警方沒有備存有關科技罪案的檢控及定罪數字。

3. 網絡安全及科技罪案調查科成立兩年間曾經進行多項專題研究，主要分為網絡攻擊趨勢(例如：勒索軟件及疆屍網絡)、犯案手法(例如：裸聊勒索及電郵騙案)以及科技趨勢(例如：物聯網及雲端科技)。

4. 全球網絡攻擊的手法層出不窮，日新月異，涉及的專業技術更是越趨複雜。網絡攻擊可以源自世界各地，對全球大眾帶來實質而直接的影響。加上精密的惡意程式在各種電腦平台均越趨普遍，令香港的市民大眾面對極為嚴峻的風險。為達至防止及偵破罪案的目的，網絡安全及科技罪案調查科會因應國際網絡罪行趨勢、攻擊手法以及惡意程式的發展等因素來針對不同黑客集團來進行專題研究。

5. 網絡安全及科技罪案調查科轄下「網絡安全中心」24小時運作，加強警隊和不同持份者的溝通和協調，以預防及更有效應付可能發生的攻擊事故，包括在發生針對關鍵基礎設施的網絡安全事故時提供即時協助。由於現今科技發展迅速，各地執法部門與網絡犯罪分子在科技和技術層面的角力和比拼愈來愈激烈，警方認為不適宜公開針對關鍵基建設施所作的網絡攻擊的數字。

6. 2012 年至 2016 年本港遭多宗大型網絡襲擊，當中顯著的的例子包括：

(a) 以「分散式阻斷服務攻擊」作勒索；

(b) 勒索軟件；

(c) 涉及『SWIFT』系統的入侵個案；及

(d) 未經授權股票交易的案件。

7. 2012 至 16 年各科技罪案每年涉及的損失金額，詳列如下：

分類	損失金額(百萬元)				
	2012	2013	2014	2015	2016
網上遊戲	0.8	1.6	2.1	2.4	2.8
網上商業騙案	26	43.1	48.4	40.4	32.1
非法進入電腦	189.6	766.2	1,004.1	1,462.4	1,813.2
其他	124	106	146.1	323.7	452.7
總數	340.4	916.9	1,200.7	1,828.9	2,300.8

8. 網絡安全及科技罪案調查科有三個組別：

(a) 科技罪案組 - 負責科技罪案調查以及數碼法理鑑證；

(b) 網絡安全組 - 負責網絡安全測試、進行專題研究、網絡安全審定、事故應變、海外及本地聯絡事務及網絡偵測及網絡攻擊情報分析；及

(c) 情報及支援組 - 負責收集、整理及分析與科技罪案及網絡安全有關的資料，就趨勢及犯案手法作出以情報主導的方式調查，並就打擊科技罪案的策略作出建議。

（二） 網上巡邏

在網上巡邏方面，警方現時採用三層情報架構，透過總部、總區及警區情報組別搜集情報。互聯網是公開的，因此其用戶面對的刑事威脅與在現實世界的威脅相同。正如在現實世界中，警方會在街上巡邏，防止罪案發生；在互聯網的虛擬世界，警方亦有必要留意可能發生的犯罪活動並採取行動。因此，為達

及偵破罪案的目的，除網絡安全及科技罪案調查科外，警方其他有關部門亦會進行網上巡邏，按需要在互聯網的公眾平台搜尋相關資料。警方會根據行動優先次序，針對性及專業地在互聯網的公眾平台搜尋可能與罪案有關的資料。藉着巡邏收集得來的資料，會使警方能夠更恰當地分配資源及分析當前的犯罪趨勢，以打擊不同類型的罪案。

不論在虛擬或現實世界，收集刑事情報是有效執行警務工作的其中一項主要元素。警方各有關部門在有需要時，為達至防止及偵破罪案的目的，會在不同渠道按針對性策略及罪案趨勢來選取網上巡邏的目標，以收集網上有關資料作刑事情報，協助打擊相關的罪案，例如行騙、非法賭波活動、兒童色情物品的發佈、毒品販賣、刑事恐嚇等。如有行動需要，警方會作出如現實世界一樣的部署，進行所需行動。

我們強調，警方在有需要時會按照相關的法例、既定的程序和守則，要求相關人士或機構，包括互聯網服務供應商及網絡平台，提供資料或作出配合。警方並沒有恆常向互聯網服務供應商及網絡平台索取網民資料。

警方沒有備存信件要求的統計數字。

（三） 黑客軟件

網絡黑客會利用不同渠道入侵網絡及進行攻擊，包括透過軟件入侵系統犯案。面對科技日新月異，執法機關必須與時並進，了解黑客的犯罪方法、科技罪行的趨勢以及有關科技的發展，從而有效制定應對及打擊策略，並提升市民大眾的資訊保安意識，防範網絡世界潛在的保安風險及網絡攻擊。

執法機關為有效防止和打擊罪案，會因應案件性質從不同渠道蒐集情報。任何蒐集情報的方式都必須合法，並按既定的程序或守則進行。不論執法機關獲取情報的行動使用何等技術，若有關行動可構成《截取通訊及監察條例》所定義的截取通訊或秘密監察行動，有關行動必須取得小組法官或指定授權人員的授權，行動的各個階段均受條例嚴格監控，而截取通訊及監察事務專員亦會監督有關執法機關遵守條例下各項規定的情況。

至於蒐集證據，警方在調查罪案時會按每宗個案的情況採用不同方法，當中涉及不同的工作程序，例如接觸不同人士以取得與個案有關的資料、面見證人及錄取口供等。如有需要，執法機關可根據相關條例向法庭申請法庭手令，以向任何機構／人士（包括網絡服務供應商）檢取文件或資料。不過，不論調查時採用何等方式蒐證，警方都必定遵守相關法例的要求。

保安局局長

（曾裕彤 代行）

2017 年 2 月 6 日

副本送
警務處(網絡安全及科技罪案調查科)