二零一六年十二月六日
討論文件

立法會保安事務委員會

打擊科技罪行的措施及為網絡安全及科技罪案調查科開設一個總警司常額職位的建議

目的

本文件 –

(a) 介紹香港警務處（警務處）對應網絡安全威脅及打擊科技罪行的策略及措施；及

(b) 徵求委員會同意，警務處開設一個總警司常額職位（警務人員薪級第55點或相等於首長級薪級第1點），以領導網絡安全及科技罪案調查科。

打擊科技罪行的措施

網絡安全的威脅

2. 當資訊科技成為我們生活不可或缺一部分的同時，全球在網絡安全威脅方面亦面對更高的風險。尤其去年，世界各地發生了多宗針對金融體系和關鍵基建設施的高調網絡攻擊。在 2015 年，全球每日有超過 100 萬宗網絡攻擊，網絡安全和科技罪行已成為世界各地執法機關面對的主要挑戰。舉例來說，黑客於 2016 年 4 月入侵環球銀行財務電訊協會的金融平台，令孟加拉中央銀行損失 8,100 萬美元。越南、菲律賓、厄瓜多爾和香港等地的其他銀行亦遭到相類攻擊。2015 年 12 月，網絡罪犯攻擊烏克蘭的電網，令 25 萬名當地市民受到停電影響。其他國家發電廠所設置的工業控制系統，包括位處香港的工業控制系統，可能會是下一個攻擊目標。

3. 賽門鐵克公司發表的2016年《互聯網安全威脅報告》指出，在亞太區的互聯網安全威脅評級中，香港的排名由第八位升至第七位。根據卡巴斯基實驗室於2015年公布的《保安通訊》，年內有34.2%用戶的電腦受到至少1次網上攻擊，而在2015年全球有超過75萬部電腦遭勒索軟件入侵。Nexusguard發表的《威脅報告》亦指出，2016年上半年在亞太區錄得的分散式阻斷服務攻擊次數超過34 000宗，增幅達43%，而據觀察所得，升幅最高的地方是香港，攻擊次數上升57%。除這些威脅外，網絡保安專家亦預測，針對流動電話和物聯網（例如網絡攝影機、智能電視等）的惡意軟件攻擊將會飆升，成為網絡安全的重大隱憂。在本港，香港電腦保安事故協調中心[1]在2015年接獲4 928宗網絡安全事故報告，自2010年以來增幅達500%。。

科技罪案的趨勢

4. 在香港，警方每年接獲的本地科技罪案數字，由 2002 年的 272 宗增至 2015 年的 6 862 宗，激增 24 倍。在 2016 年（截至 9 月），案件宗數高達 4537 宗。過去 6 年間，每年相關的損失亦由 2010 年的 6,000 萬元增至 2015 年的 18 億元，增幅達 30 倍；而在 2016 年（截至 9 月），損失約為 18 億 7 千萬元。

5. 近年，警方接獲的科技罪案主要包括與網上遊戲有關的罪行、網上商業騙案、非法進入電腦系統及其他科技罪案。過去 5 年，警方接獲的科技罪案數字，載於**附件 1**。

應對挑戰的策略及措施

6. 為加強打擊科技罪行及應付網絡安全事故的能力，行政長官在 2014 年施政綱領中公布，將警務處的科技罪案組升格，設立新的網絡安全及科技罪案調查科。隨着網絡安全及科技罪案調查科在 2015 年 1 月成立，警務處致力提升及擴展在下述範疇的能力：

(a) 偵查集團式及高度複雜的科技罪行，以及積極進行情報主導的調查工作；

[1] 香港電腦保安事故協調中心由香港生產力促進局管理，是本港的資訊保安事故協調中心，為本地企業及互聯網用戶提供資訊保安事故的消息和防禦指引、事故回應及支援服務，及提高保安意識。

(b) 適時進行網絡威脅的審計及分析，以防止及偵查針對關鍵基建設施所作的網絡攻擊，從而為該等設施提供支援；

(c) 提升重大網絡安全事故或大規模網絡攻擊的事故應變能力；

(d) 加強對網絡罪行趨勢、犯案手法、電腦系統弱點及惡意軟件的發展進行專題研究；

(e) 在情報交換和最佳做法分享方面，加強與本地持份者和海外執法機關的合作夥伴關係，以應付常見的科技罪行和網絡威脅；以及

(f) 制訂有關網絡安全和科技罪行的新培訓課程。

7. 為了更有效地統籌警隊資源打擊科技罪行並進一步提高市民的保安意識，警隊繼續把打擊科技罪案列為首要行動項目，以加強網絡安全和打擊科技罪行，並從以下三方面着手：

(a) 採用多機構合作模式，加強市民對電腦及網絡保安和使用社交媒體所帶來風險的意識。網絡安全及科技罪案調查科舉辦不同宣傳項目，包括為公眾舉辦講座及多媒體活動。網絡安全及科技罪案調查科亦與政府部門及公營機構統籌年度網絡安全活動，讓持份者以認證、講座、工作坊及會議形成交流網絡安全的知識；

(b) 加強與其他執法機構合作，打擊科技罪行。網絡安全及科技罪案調查科與其他司法區的夥伴攜手合作，預防、打擊及調查科技罪行。網絡安全及科技罪案調查科亦會籌辦網絡安全高峰會 2017，該年度活動匯聚世界各地的科技界專業人士、政府部門及執法機關，齊集香港分享網絡安全方面的經驗；以及

(c) 在處理和調查科技罪行方面，加強專業知識的統籌及分享。為加強科技罪行的調查能力，網絡安全及科技罪案調查科定期為本地及海外執法機關舉辦專業培訓。例如在 2016 年 12 月，網絡安全及科技罪案調查科會與國際刑警在香港合辦「歐亞地區科技罪案調查培訓」，以加強處理科技罪案調查人員的能力。

8. 鑑於網絡安全的重要性，香港金融管理局（下稱「金管局」）最近為銀行體系推出網絡防衛計劃，旨在提升銀行體系的防衛能力，使其水平與香港作為亞洲首屈一指國際金融中心的地位相稱。在警務工作方面，網絡安全及科技罪案調查科最近推出兩項新措施，即網絡靶場和網絡攻擊情報交流平台，以應付瞬息萬變的網絡威脅形勢和日趨複雜的新網絡攻擊技術。網絡靶場是一項能在封閉網絡中模仿互聯網環境的設施，可模擬網絡攻擊和科技罪案情況，作研究和培訓用途。網絡攻擊情報交流平台是個多用途平台，可從網絡安全組織蒐集網絡攻擊的資料並加以分析，然後廣發給香港和海外各個持份者。該平台會與金管局開發的網絡風險資訊共享平台相輔相成，成為網絡防衛計劃的一部分，以方便分享有關網絡攻擊的情報。此外，網絡安全及科技罪案調查科正籌備進行大規模的網絡安全演習，以加強本地關鍵基建設施應對網絡安全事故的整體能力、改善現時與海外同類機構的溝通，以及提升現時對香港網絡環境的保護。除此之外，網絡安全及科技罪案調查科正在籌辦網絡安全精英嘉許計劃，藉此匯集香港各個主要界別的網絡安全經驗和良好作業方式，共同推廣網絡安全意識及應付層出不窮的網絡威脅。

擬議開設一個總警司常額職位出任網絡安全及科技罪案調查科的指揮官

9. 負責上文第 6 至 8 段概述的所有工作並擁有 238 名人員的網絡安全及科技罪案調查科，現時缺少一名首長級的領導。警務處刑事部轄下負責參與罪案調查工作的科別（包括商業罪案調查科、毒品調查科、刑事情報科和有組織及三合會調查科）目前均由一名總警司領導，但網絡安全及科技罪案調查科目前只由一名高級警司領導。

10. 截至 2016 年 11 月 1 日，網絡安全及科技罪案調查科的編制有 238 人（當中紀律人員職位有 226 個），均屬非首長級職位。網絡安全及科技罪案調查科的組織圖載於**附件 2**。有見及多個因素，包括：由總警司率領的其他刑事調查科別中紀律人員職位的數目（在 2016 年 4 月，毒品調查科有 368 個、商業罪案調查科有 272 個、有組織罪案及三合會調查科有 109 個）、網絡安全及科技罪案調查科與這些科別相若的規模及其多層職級架構、廣泛的職

務、不斷增加的工作量及日益繁複的工作，屬總警司職級的指揮官對帶領調查科至關重要，從而確保調查科充分得到所需的領導和管理，尤其推行下文第 11 至 16 段所述的工作。擬設的網絡安全及科技罪案調查科總警司職位的職責說明載於**附件 3**。警務處在擬議的總警司職位開設後的組織圖載於**附件 4**。

規劃網絡安全及科技罪案調查科的長遠發展以達成使命

11. 科技罪行現時有迅速增加的趨勢，安排專責人手及進行策略規劃以對付這類罪行，是警務處須優先執行的主要行動。為落實該項使命，網絡安全及科技罪案調查科需要由首長級人員作高層領導，以制訂有效的策略，從而應付上文第2至5段所述的挑戰，並確保該等策略得以順利推行。鑑於通過互聯網干犯的罪行屬跨國性質，而且種類繁多（例如網上購物騙案、電郵騙案、詐騙、洗黑錢、與裸聊有關的勒索案、兒童色情物品等），特別需要由1 名對預防及控制罪行具廣博知識、閱歷和視野的首長級人員發揮強而有力的領導，才能應付。否則，網絡安全及科技罪案調查科將難以制定策略和督導管理事宜，例如提升能力、與本地關鍵基建設施的管理當局建立合作夥伴關係、與本地及海外執法機關及服務供應商合作，以及分配和調撥資源。

統籌應對科技罪行及網絡攻擊的措施

12. 鑑於科技罪行和網絡攻擊日趨複雜，加上香港的互聯網用戶不斷增加，在協調與網絡安全及科技罪行有關的事宜方面，網絡安全及科技罪案調查科總警司將擔當十分重要的角色和職能。香港必須準備就緒，以應付針對關鍵基建設施的任何確實及迫切的網絡攻擊威脅；若然不把握時機或防備範圍方面有所不足，將會令香港處於非常不利的境況。為準備應付或萬一香港出現針對本地關鍵基建設施的大規模網絡攻擊或發生涉及多個跨司法管轄區的科技罪案，網絡安全及科技罪案調查科總警司須肩負重任，協助警務處作出高層次和刻不容緩的決定。除了在香港的關鍵基建設施受到大規模網絡攻擊時動員警隊其他專責單位參與行動，以及就偵查科技罪行訂立目標、政策和長遠策略外，該總警司將負責統籌與本地及海外執法機關、政府部門及其他持份者所採取的聯合行動，以便交換情報及保存有助調查工作的數碼證據。

13. 如不設立網絡安全及科技罪案調查科總警司職位，警務處內部便沒有合適的人員，具備所需職權、經驗及環球視野，率領本地和國際機構，即時應對大規模攻擊並妥為處理善後工作。總警司職位如進一步延遲開設，將會嚴重影響警務處及香港對網絡攻擊的應變能力，繼而令香港極容易為主網絡罪犯的目標，針對或通過我們的資訊科技基建設施發動網絡攻擊。

新措施的策略規劃、監察和執行

14. 上文第 8 段所述的新措施涉及大量資源，需要進行策略規劃、監察和執行工作，因此有必要指定由一名首長級的高級警務人員，負責督導並監察這些措施，以及有效和高效地落實、檢討、改善並維持該等措施的發展。

與本地及海外持份者維持緊密聯繫

15. 環顧全球，網絡安全問題及科技罪行迅速演變，並超出傳統司法管轄區的界限。因此，網絡安全及科技罪案調查科的核心職務之一，是與本地及海外執法機關建立緊密聯繫，以打擊跨境科技罪行和交流經驗。儘管高級警司應可採取打擊科技罪行的跨境策略性行動，但始終仍需總警司級別的首長級人員參與談判及予以督導，以便與各個高層次的持分者攜手合作，尤其是在遏止科技罪行時要將策略上的轉變赴諸實行，例如重整銀行保安系統、改變網絡用戶習慣、建議重新設計關鍵基建設施的電腦系統等。為此，網絡安全及科技罪案調查科確實需要有首長級人員代表警務處參與高層次的工作小組、會議及訪問，與世界各地網絡安全及科技罪案執法單位的指揮官建立合作關係。從能力、經驗及見識而言，網絡安全及科技罪案調查科總警司的職級與這項使命的重要程度相稱。該名人員將擔當關鍵角色，負責與海外機構（例如國際刑警及G7高科技犯罪工作小組）聯絡。

16. 在海外國家，打擊網絡罪行的執法單位主管的職級一般等同警務處總警司的職級。舉例來說，英國國家打擊犯罪總署轄下的國家打擊網絡犯罪組由副處長職級的人員率領。至於澳洲聯邦警察轄下的高科技犯罪偵查小組及新加坡警務處刑事調查部轄下的打擊網上罪行指揮中心，則由助理署長職級的人員率領。

曾考慮的其他方案

17. 我們已審慎考慮可否重行調配警務處現有的首長級人員，以承擔擬設職位的工作。目前，警務處轄下 5 個部門，即行動處、刑事及保安處、人事及訓練處、監管處和財務、政務及策劃處，共設有 46 個總警司職位。由於所有總警司職級的人員處理各自範疇的職務已分身不暇，要在不影響他們執行本身職務的情況下重行調配內部人手，在運作上並不可行。

對財政的影響

18. 按薪級中點估計，開設擬議的總警司職位所需增加的年薪開支為 1,663,200 元。實施這項建議所需增加的每年平均員工開支總額（包括薪金和員工附帶福利開支）則為 2,634,000 元。我們已在 2016-17 年度的預算內預留足夠撥款，以支付開設擬議的總警司職位所需的開支，並會在其後年度的預算內反映所需資源。

徵求意見

19. 立法會保安事務委員會（2014 年 6 月 3 日）及人事編制小組委員會（2015 年 3 月 11 日及 4 月 29 日）曾討論為網絡安全及科技罪案調查科開設一個總警司職位的建議。政府於 2016 年 6 月向人事編制小組委員會再次提交建議，但在上屆立法會任期結束前，討論一直無法展開。

20. 網絡安全及科技罪案調查科急切需要強而有力的專職領導，才能全面有效地獨立運作，特別是如上文所述，該科須處理大量繁複、敏感的工作。就開設一個總警司常額職位領導網絡安全及科技罪案調查科的建議，待徵詢委員的意見後，我們計劃在 2017 年首季將建議提交人事編制小組委員會。

保安局
二零一六年十一月

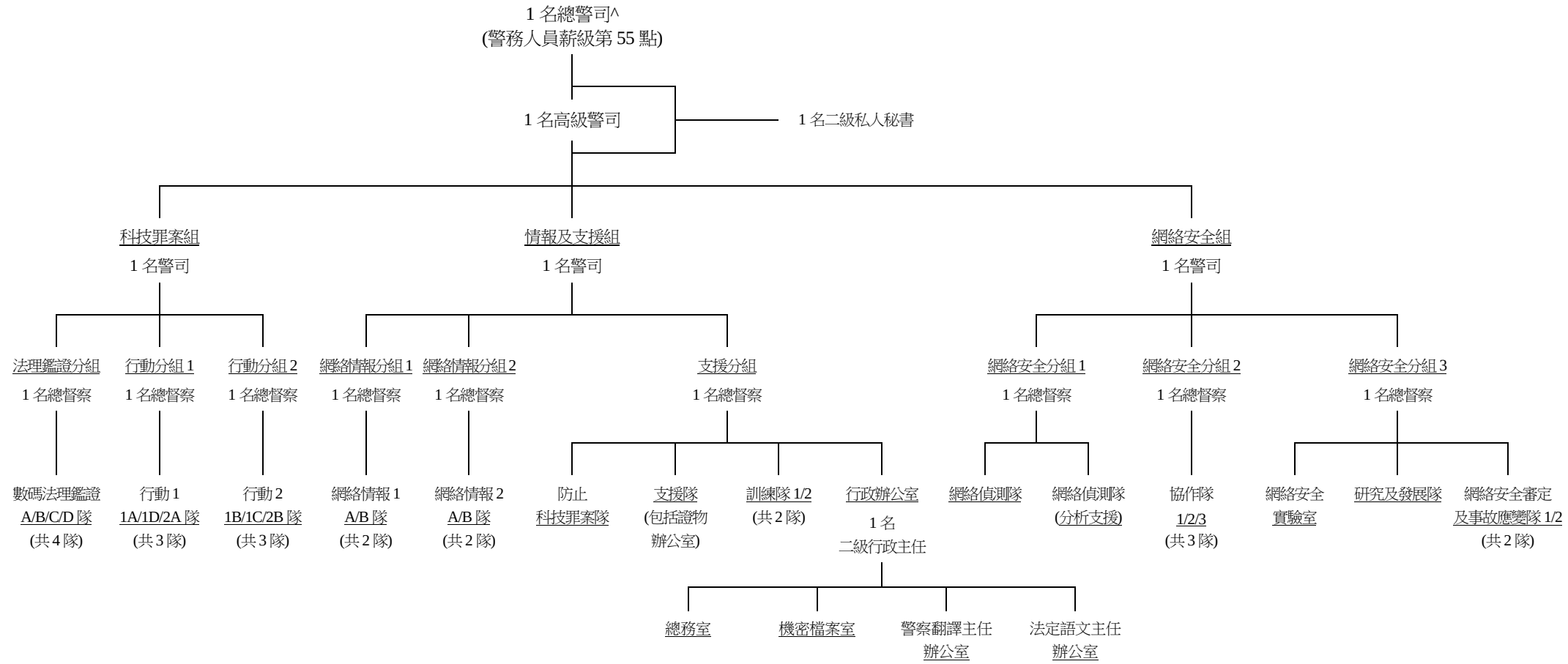
附件1

2012 年至 2016 年九月的科技罪案數字

案件性質	2012 年	2013 年	2014 年	2015 年	2016年 (截至 9月30日)
與網上遊戲有關	380	425	426	416	304
網上商業騙案	1 105	1 449	2 375	1 911	1 217
非法進入電腦系統	1 042	1 986	1 477	1 223	847
其他性質	488	1 273	2 500	3 312	2 169
(i) 網上雜項騙案	*225*	*435*	*1 436*	*1 733*	*1 133*
(ii) 兒童色情物品	*28*	*41*	*38*	*53*	*27*
(iii) 分散式阻斷服務(DDoS)攻擊	*25*	*3*	*29*	*35*	*4*
(iv) 網上銀行	*5*	*40*	*17*	*3*	*2*
(v) 裸聊	*沒有備存*	*沒有備存*	*638*	*1 098*	*588*
(vi) 其他	*205*	*754*	*342*	*390*	*415*
總計	**3 015**	**5 133**	**6 778**	**6 862**	**4 537**
損失(百萬元)	**340.4**	**916.9**	**1,200.7**	**1,828.9**	**1,865.2**

附件 2

香港警務處網絡安全及科技罪案調查科組織圖



^ 擬開設的 1 個總警司職位。

附件3

香港警務處
網絡安全及科技罪案調查科
總警司
職責說明

職級　　：總警司（警務人員薪級表第 55 點）

直屬上司：警務處助理處長（刑事）

主要職務和職責－

(i)　指揮香港警務處（下稱「警務處」）與網絡安全及科技罪案功能有關的行動及發展。

(ii)　確保屬下人員的工作表現及紀律均保持高水平。

(iii)　根據警隊策略方針及警務處處長首要行動項目制定策略，以確保有效調配資源，配合打擊科技罪案和應付網絡安全事故的警務工作需求。

(iv)　代表警務處與本地及國際相關各方有效合作和協調，以處理網絡安全及科技罪案事宜。

(v)　確保人員已接受實用而有效的訓練，以處理有關網絡安全及科技罪案的調查。

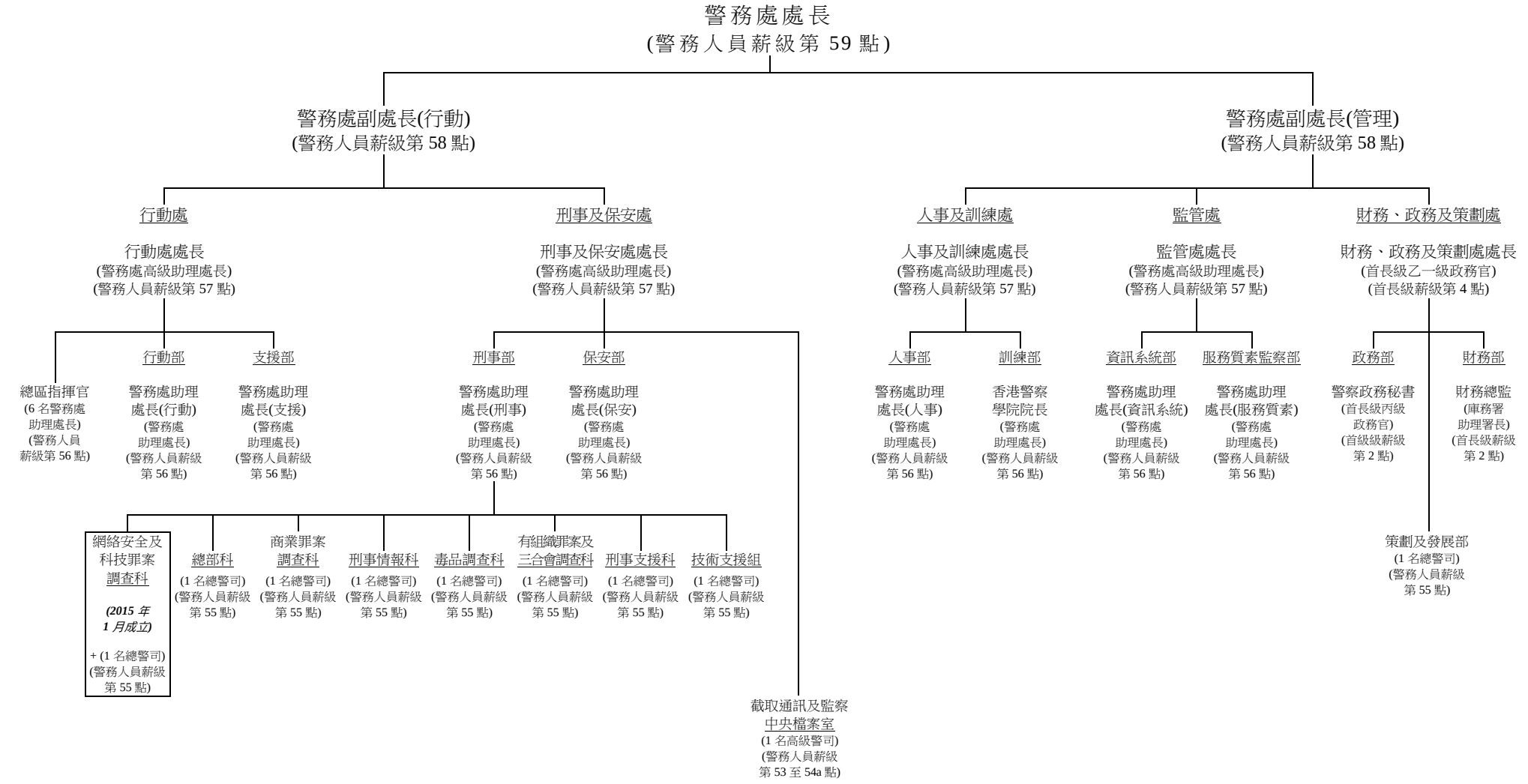
(vi)　監察並處理本港和外地可能影響警務行動優先項目及活動的網絡安全事故及科技罪案。

(vii)　當香港的關鍵基建設施受到重大網絡襲擊時，動員其他具備專責職能的警察單位參與行動。

(viii)　執行警察總部委任的人事管理及紀律職務。

(ix)　與其他相關各方檢討目標、政策及實施計劃，以統整應對策略，處理本港關鍵基建設施電腦系統面對的網絡威脅。

香港警務處組織圖



說明： ☐ 擬開設的 1 個總警司職位，職銜為網絡安全及科技罪案調查科總警司