大灣區電子政務信息安全威脅及其防範策略

司法警察局一等刑事偵查員　劉宇

【摘要】互聯網及相關技術的急速發展，對世界各國在政治、經濟、文化等方面的影響深遠，由於網絡無遠弗屆，一般信息在不同地域之間的傳遞速度極高，成本接近於零，這既為人類社會帶來了巨大的利益，同時亦衍生了新的安全威脅。在新的安全治理形勢下，澳門與內地及香港等地警務部門的合作交流日趨緊密，利用網絡進行數據化的信息互通成為趨勢；然而，高效、準確的信息交流除了建基於互信互助的理念及法律制度的保障外，亦必須排除信息在傳遞過程中的各種安全隱患及威脅，以達至彼此緊密合作、互通情資、聯動執法的跨境警務合作目標。

【關鍵詞】跨境警務合作　信息安全威脅　電子政務雲　信息保護

一、前言

近年，本澳與內地及香港等地的合作日趨緊密，透過各地政府之間簽署的一系列協議、相關法律法規的日漸完善，以及粵港澳大灣區上升為國家戰略，建立灣區一體化的社會經濟體制必然是未來的發展趨勢。伴隨着時代的變革發展，澳門與內地及香港等地警務部門的合作交流必將更為密切，警務雲、大數據等新技術的應用，各地警務部門間的信息及情報交流將變得更為便捷及頻密。然而，在電腦網絡發展帶來便利的同時，不法份子利用相關漏洞進行網站入侵、竊取用戶信息及散播電腦病毒等活動，均對信息安全及系統穩定帶來嚴重威脅，並對用戶的工作生活造成重大的危害。為使各警務部門之間能進行有效安全的信息交流，避免信息傳遞過程中可能出現的風險，電腦網絡信息安全的技術專家必須做好防護工作，同時，警員作為警務情報及信息的使用者，亦應重視信息安全的理念，審慎評估具體情況下可能出現的問題，進而做到從多角度、多層次、整體地將信息安全風險發生概率減到最低。

二、信息安全及其相關概念

信息的概念，其出現的時間遠遠早於電腦技術，它能以任何可以被人類認知的形式存在，並在人們互相交流的過程中發揮重大的作用。本文着重於探討透過電腦及互聯網進行的且已被數碼化的信息之流動，以及其在傳遞過程中可能存在的各種被獲取、截取、更改、破壞或刪除等安全隱憂，由於信息安全問題可以出現在每個細節之中，因此，我們要對使用電腦上網的過程及機理有一個相對完整的理解，才能更好地應對信息安全問題的威脅。

從電腦運作的原理出發，無論是各種物理設備或數據的傳輸，均須遵循一定的標準，當人們按同一標準進行數據的發送、接收和處理時，互聯網中各種不同的系統、設備，以及各種產品之間才能順暢地鏈接起來，而這些標準則稱之為協議（protocol）。常見的互聯網協議，由物理設備的基礎通訊到最頂層的應用，可分為七層，如較為基礎的TCP/IP、UDP協議，以及建於其上的訪問互聯網協議（如HTTP、HTTPS）、郵件收發協議（如POP、SMTP、IMAP）及遠程登錄協議（如Telnet、SSH）等應用協議，在具有相同功能及目的的

協議之間，最重要的分別是數據的傳輸是以明文還是加密的方式進行，這直接影響到黑客截取數據後是否須要作進一步破解，亦是實際損害會否發生的關鍵。

從設備的角度考慮並以此作分類，一個典型的上網過程，通常涉及客戶端、網絡傳輸層和服務端。客戶端是指使用者的個人電腦、智能手機等設備，傳輸層包括交換機、路由器及移動網絡設備（如電訊公司的基站）等，而服務端則包括各個大型互聯網公司之機房，以及雲計算服務商的設備等；此外，作為例外情況，有近年十分流行的去中心化系統（如比特幣）以及早已出現的P2P網絡，兩者均不按上述原理運作，故不能按上述分類進行理解，與去中心化系統相對，一般互聯網的服務和流量往往集中於特定的實體，具中心化的特點。

鑑於在客戶端、傳輸層或服務端均有可能出現安全隱患，如警員使用的個人移動設備可以被植入病毒，透過移動設備與警務雲的信息往來可以被截取，以及運行警務雲系統的機房設備也可能被入侵，因此，信息安全問題不單純是維護系統的技術人員的責任，作為系統使用者的警員及相關工作人員更應特別注意相關風險。

三、常見的黑客入侵方式及其防範思路

警務信息通常涉及敏感性及機密性資料，防止信息洩漏及維護警務系統穩定便顯得極為重要，加上互聯網的跨地域性和信息轉移的高效率低成本等特徵，從技術的角度來預防信息安全風險，比問題發生後透過行政或司法途徑進行處罰或追究更為重要。故此，作為警務人員，應對不法份子可能使用的技術原理有一定程度的瞭解，儘量做到預防優先。

以下介紹一些常見的不法技術手段及其入侵思路。

（一）彩虹表及密碼碰撞

彩虹表（Rainbow Table）可以理解為一個為了破解帳號密碼，而預先對常見的明文密碼進行哈希函數（Hash Function）[1]及相關運算後得出密文，再將該等密文與明文建立對應關係的大型數據庫。現時，互聯網服務方為了與使用者進行互動，通常是使用帳號及密碼的方式識別客戶的身份，服務方通常會將相關密碼進行非對稱加密後保存，使服務方的工作人員或黑客不能直接獲取明文密碼。而彩虹表則是一個基於密文反向查找明文的數據庫，因而在密文被不法份子以各種方法知悉後，便能使用彩虹庫進行碰撞，從而得到明文密碼，並進行相關帳號的入侵；常見的大型彩虹庫的數據量以萬億計算，故此，當密碼的強度不足時，明文極易被碰撞出來。

針對這種入侵手段的防護方法，作為客戶端，應使用防護性強的密碼，減少使用常見字組成的密碼，從而降低被碰撞破譯出明文的機率；而作為服務端，使用隨機加鹽[2]是最有效的防護方法。

（二）DNS劫持及網絡釣魚

DNS（Domain Name Service，網域名稱系統）的主要功能之一是為了方便人們訪問互聯網，當人們在瀏覽器上輸入便於記憶的域名，如zh.wikipedia.org，透過DNS服務便能找到與其對應的IP地址208.80.154.225，從而準確訪問相關網站。而DNS劫持（DNS hijacking）的危害在於即使用戶輸入了正確的域名，也會被劫持者引導至另一網站，該網站通常與劫持者利益相關，甚至是木馬網站或釣魚網站；劫持者通常是透過惡意軟件修改用戶的TCP/IP設定，使其指向由劫持者操控的流氓DNS伺服器，從而達至上述效果。

作為DNS劫持的上位概念（superordinate concept）[3]，劫持可以發生在上網過程所需經歷的各個階段，從客戶端的瀏覽器、操作系統的配置文件（如HOSTS）、內網的交換機、上述的DNS服務器、路由器，到服務端等均可發生。劫持的表現形式可以是域名的劫持，也可以是內容的替換或刪除，甚至是作為實施高級持續性威脅（Advanced Persistent Threat，APT）手段的重要環節，在這種手法中，劫持者像中間人般，長期截取用戶的輸入，將其中

的請求轉交給真實的服務商，並將真實的反饋傳送給用戶，使用戶難以發現自己已被劫持，這樣就能從中收集大量重要的資料。

網絡釣魚（Phishing），是指利用仿真的網頁騙取他人輸入帳號及密碼，從而控制其帳號的手段。入侵者通常是利用相似域名，使經驗不足的人士上當，只要上網者留意相關的域名，單純的釣魚網站很容易識別；然而，當劫持與釣魚聯手出擊時，即便是用戶輸入了正確的域名，也可以被引導進入釣魚網站的頁面，使入侵得逞的機率大增。

針對這些手段，防護劫持發生的難度雖大，但卻最為關鍵。作為用戶，應安裝可靠的安全防護工具，手動設置安全可靠的DNS，並儘可能使用加密協議傳輸數據，另外，使用某些平台功能時，應留意其安全證書是否已經過審核；作為服務端，應禁止沒有安裝安全防護工具的電腦接入內網，做到一人一密碼登入系統，並注意交換機、路由器的模式及安全設置，以及加強機房管理等措施，儘量使劫持發生的機會降低。

（三）嗅探偵聽

嗅探偵聽（sniffer），一般是指針對在網絡中傳輸的信息進行截獲的行為。在使用廣播模式的內聯網環境中，一般情況下，使用者只能獲取與其有關的數據信息，並丟棄與其無關的信息，但如電腦安裝有數據包的分析工具，可以在不作丟棄的情況下收集所有信息，如該等信息是用明文傳輸的（如Telnet、POP協議）方式進行交互，則其中包含的帳號、密碼以及郵件內容均能被截取者知悉；特別是在互聯網的環境下，由於網絡是一個存在大量節點的拓撲結構（topological structure），要保證各個節點的絕對安全存在巨大的困難，因此，警務信息交流平台必須做好相應的防護。作為維護的技術人員，應注意分析網絡鏈接狀態，熟悉訪問目標網址所經過的網絡節點，瞭解系統是否開啟了伺服程序，是否存在遠程鏈接，以及做遠程掃描，如須對市民提供公開服務，應將敏感資料放在加密的環境中傳輸，此外，還須注意加密證書是否安全；作為平台的使用者，應儘可能使用安全加密的傳輸協議，在安全性成疑的網絡環境下，不要登入重要的系統，以及根據自身的安全需求，不應在不安全的網絡環境下傳輸敏感資料。

（四）木馬植入及電腦蠕蟲

木馬（Trojan Horse），是指隱藏在正常的文件或應用程式中的惡意代碼，其功能通常是作為一種後門（back door），使入侵者能繞過系統正常的驗證手續，進入系統並獲取操作權限；而電腦蠕蟲（computer worm）強調的是惡意程式或代碼的傳播方式，主要是借助宿主或主動搜索易感系統，以達到不斷自我複製及不斷傳播電腦病毒的目的。

木馬亦可以透過自動執行程序傳播，如透過感染病毒的移動硬盤及在其中儲存的文件檔案，電腦一旦接入該硬盤或轉錄該等文件，便有可能被感染，這種方式可以理解為借助宿主的傳播。另外，現時更為常見的是主動搜索傳播，其施行的手段是利用被害人的網絡，掃描附近的裝置，如該裝置開啟了特定的服務，且由於未安裝最新的補丁而存有漏洞的話，木馬便能利用該漏洞複製自己並植入該裝置，與舊有的透過文件、附件傳播的方式相比，這種傳播方式在用戶無需進行任何操作的情況下便能自動完成。

為了防範木馬蠕蟲，個人使用者應做到：不訪問不明來歷的網頁、不開啟可疑的文件或附件、注意外來的移動硬盤、安裝必要的安全工具、及時更新系統補丁，以及應從官方網站下載軟件（如軟件不是由源地址下載，則應從源地址取得軟件的MD5來核對，以確定軟件是否已被改動）；作為系統或平台的管理者，如系統由外包開發完成，必須取得源代碼，並對源代碼作深入全面的審核，如使用編譯器開發程序或系統，則應注意編譯器的安全。

（五）SQL注入及跨站腳本

SQL注入（SQL injection）是一種惡意篡改，由於數據庫通常會作為應用的支援後台，其通用的編程語法是SQL，當一段需要調用數

據庫內容的查詢語言，通過使用者交互資訊進行查詢的時候，例如，查詢使用者輸入的帳號密碼是否和資料庫裏的帳號密碼一致，如果黑客在交互的資訊中，不是輸入密碼，而是刻意編寫為一段代碼，當服務端的程式沒有對交互的資訊做格式校驗和二次編碼時，就直接進行查詢操作，進而被這段代碼改寫查詢邏輯，從而跳過原本應該確認的邏輯。例如，最常見的手段是入侵者在不知道被害人的密碼的情況下，透過編寫的代碼使邏輯判斷必然為真，從而在不需要輸入密碼的場景下直接控制了用戶帳戶。此外，SQL注入不一定發生在用戶輸入層面，還可以通過修改query參數或在cookie裏植入特殊字串，以實現入侵和破壞的目的。

跨站腳本（Cross-site scripting，XSS），其入侵的邏輯與SQL注入相似，都是利用了系統對用戶交互的資訊沒有做足夠的確認和校驗而達成，但跨站腳本通常發生於客戶端的腳本執行，而SQL注入則常見於服務端應用腳本數據庫的處理之中。

為了防範這些入侵，系統管理者的工作至關重要，他們必須對用戶的輸入作分析，校驗客戶端傳遞的所有參數；而作為系統的使用者，儘量不要在不知名的網站保存重要的資訊，以免網站被入侵時相關資料被黑客知悉，又或帳號被盜時蒙受重大的損失。

（六）緩衝區溢位攻擊

緩衝區溢位攻擊（buffer overflow）是一種針對系統級重大安全漏洞的攻擊手段，屬於零日漏洞（0day）的一種，目前是安全專家或黑客研究入侵手段最為重要的方向之一。

一般運作正常的情況下，應用程式伺服器針對遠程交互傳遞而來的數據（可以是用戶輸入的、參數攜帶的，或cookie信息中存在的）而作出執行時，在內存中，由代碼段提取數據段的內容作處理，並給予用戶反饋，用戶因而得到執行的結果。由於數據段在前、代碼段在後，如果系統沒有對交互的數據做充足的校驗和處理，複製到內存的數據又超出了數據段的長度限制時，超出的部份就會覆蓋到代碼段，這時用戶的系統會提示出現溢位錯誤，一般表現為系統崩潰，如core dump。

由於緩衝區溢位屬於系統漏洞，要防範這種入侵，主要依靠系統更新補丁以阻塞漏洞，然而，在溢位漏洞被不法份子利用實施攻擊前，不易發現系統相關隱患的存在，故往往難以有效防止黑客利用這種漏洞進行入侵。現時，大量系統安全公司會設計一種虛擬的系統環境，稱之為蜜罐系統（Honeypot system），專門用來引誘黑客的入侵，從而發現新的攻擊方法和入侵途徑，並針對性地填補相關漏洞，由於0day漏洞價值不菲，且在這種攻防背景下，黑客往往會利用其實現極為重要的戰略目的，不會輕易濫用。對於警務系統而言，作為系統的管理者，最為重要的工作是對交互信息作嚴格的校驗和控制，作為系統的使用者，應儘可能減少使用中的電腦所開啟的服務和端口，以減低風險。

（七）軟件架構耦合

電腦的各個應用場景，通常涉及多個不同的應用、服務或產品，它們互相組合以提供特定的功能，但在某些情況下，為了實現更為複雜的工作目標或訴求，各個應用或產品組合在一起後，卻出現了設計者始料不及的問題。

架構耦合漏洞的特點在於單獨考慮各個應用時並沒有問題，但組合在一起時便出現了嚴重的後果，例如2003年的Windows 2000操作系統中文版本的登錄入口可以調用輸入法，輸入法調用系統幫助，系統幫助可以加載遠程資訊從而調用瀏覽器，瀏覽器可以調用本地文件，最終實現不用輸入密碼而直接操作系統盤的目的，這些步驟單獨考慮時並沒有不合理之處。現今，隨着智能裝置及海量應用程式的不斷出現，這些硬件與硬件之間，軟件與軟件間的交互也日趨複雜多變，可以預見，這種漏洞亦將不斷花樣翻新，而作為警務系統的管理者及使用者，必須對架構耦合問題保持高度警覺性，一旦發現問題應即時通報，並交由相關的技術人員修補漏洞，防止被別有用心的人士利用以實施入侵。

（八）高級持續性威脅

高級持續性威脅（Advanced Persistent

Threat，APT）是一種針對特定目標的全方位、多角度、持續性及系統性的滲透攻擊，黑客通過技術手段（如上述各種手段的混合使用）、間諜[4]、社交媒體、公開信息等各種方式全面捕獲並分析資訊，而且不以一次性破壞為目的，反而以長期滲透、持續跟蹤作為實現不法目的之主要手段。其特點在於，被滲透者往往察覺不到自己已被入侵，故常常難以發現問題；對於滲透者而言，較為容易得逞的方法是選擇缺乏相關安全知識及意識的工作人員作為滲透目標（例如秘書、一般行政人員等），並在其不知情的情況下成為入侵重要系統的跳板，從而掌握機密資料，實現其不法目的。

從防禦的角度考慮，所有曾經接觸警務系統或相關系統的工作人員，尤其是警員，必須提高安全意識及敏感性，對於一些異常的操作結果或跡象，應能意識到滲透風險的存在，並儘可能立即上報處理。當收到上級或同事的奇怪或不合理要求時，例如要求自己作出某些高危行為，應立即向該上級或同事作二次核實，以防範黑客冒充相關人員的身份以騙取重要資訊。

（九）雲洩露及雲穿透

隨着技術的進步，人們使用雲服務已變得極為普遍，透過將資料上傳至雲端，其後便能在各個裝置下載或使用相關內容，因而十分便捷，然而，由雲服務平台引起的各種安全問題越來越受到重視，如某些雲平台洩露各種不雅照片或視頻的新聞，已引起了社會的廣泛關注。

雲洩露出現的原因多種多樣，如資料被搜索引擎捉取、在不知情的情況下被廣播、各種智能攝像頭因存在後門或未更改預設密碼而被他人控制，又或是保存在雲端的資料由於雲平台被攻破而洩漏，即使是大如美國蘋果公司，其雲平台亦曾出現洩漏事故。因此，在使用雲服務享受生活便捷的同時，應特別注意其安全隱患，而相關的防範手法涉及多個層面，總括而言，第一，不應將重要的文件或資料上傳至雲端；第二，上傳文件前應充分核查，以防止其中夾雜了重要資訊；第三，儘可能使用技術成熟的大型公司提供的雲服務，將風險減至最低。

雲穿透是入侵者利用雲平台的安全漏洞，進入上層操控平台以控制雲平台使用者的雲空間，並實現其不法目的之攻擊手段。鑑於入侵手法可以涉及多個層面，為了防範相關風險，信息安全技術專家的工作至關重要。

四、國內外雲計算安全標準的發展狀況

現今，為了消除“信息孤島”和政府部門各自為政而導致的效率低下和資源浪費等困境，以雲計算為支撐的電子政務雲必定是大勢所趨。警務雲是其中的一個分支，雲計算技術有利於實現政務資源、信息及情報的互聯互通，極大地降低政府行政成本，並提高行政效率，因此亦十分有利於落實大灣區警務合作的理念。然而，電子政務雲的技術核心是統一，這意味着信息安全的風險及其施行後的危害必將成倍地放大，由於電子政務雲系統及其中的信息具有極高的法律保護價值，相比起入侵發生後進行刑事追究，構建事前及事中的法律保障則更為關鍵，可以中國內地及一些先進國家的做法作為參考：

（一）中國內地

近年，我國積極推進電子政務雲相關技術標準的編制，特別是雲計算安全方面的標準。2013年，工信部開展國家標準的編制工作，目前已確立29項技術標準編制方向。目前，全國信息安全標準化技術委員會已經出台《雲計算服務安全指南》[5]和《雲計算服務安全能力要求》[6]兩項重要標準。《雲計算服務指南》從政府角度描述適用風險，規範政府適用雲計算的基本流程和步驟，也對雲計算服務的生命周期各階段提出安全管理和技術要求。建議政府部門在風險評估的基礎上根據具體業務系統和信息類型，部署和適用雲計算。《雲計算安全能力要求》規範了雲服務商在為政府部門提供服務時應當具備的信息安全能力，其標準分為一般性要求和特殊要求兩部份，並根據不同服務對象

提出不同的技術要求。目前，雲計算安全的國家標準《雲計算安全參考框架》和《雲計算服務安全能力評估方法》正在抓緊研擬中。

在警務雲方面，2014年10月，中國公安部科技信息化局和雲存儲專業委員會（Cloud Storage Professional Committee，CSPC）聯手組織部份地方公安廳、局，以及雲存儲專業委員會的六家成員企業，開始着手打造警務雲存儲系統的行業標準，正式起草和制定《警務雲平台存儲總體技術要求》。2015年8月21日，中國公安部科技信息化局在北京召開警務雲平台存儲相關標準與國家標準對接工作會，並在會上鄭重向外界宣佈中國雲存儲標準與應用工作正式啟動，進一步深化國家標準和警務雲行業的制定與應用工作[7]。

（二）美國

美國政府以美國國家標準與技術研究院（National Institute of Standards and Technology，NIST）為主體，制定並出台了SP800和SP500系列標準，並以美國聯邦安全角度為核心，提出雲計算定義、雲計算體系架構、服務模式和配置模式[8]。針對採購問題，美國通過《SP800-144公有雲中的安全和隱私指南》[9]及《SP800-146雲計算概覽和建議》[10]，對政府選取雲服務、選擇雲服務商提供了指導性標準，其中規定了美國聯邦政府採購雲服務主要分為兩種：集中採購與自行採購。集中採購就是由聯邦總務署作為所有聯邦機構的採購代表，匯總採購需求，與雲服務商簽訂長期的雲服務一攬子採購協定，一攬子採購協定有兩種訂立方式：可以採用預競價機制，即美國聯邦總務署在與服務商協商確定各個種類雲服務的最高限價後，各部門以此為限，採購時不得高於此價格；也可以採用定點採購的方式，對常用典型業務的雲服務商進行認證、評估後，確立雲服務商名錄，聯邦各部門從中選擇合適的雲服務。而在自行採購模式方面，是由聯邦總務署授權後，聯邦各部門自行採購所需的雲服務。另外，NIST公佈《建立有效的政府採購雲服務合同》[11]，制定了政府採購雲服務合同模板，其中包括在使用者協定、服務等級協定、資料保護和資料所有權、安全審查、電子記錄、資訊自由法以及各自的權利義務等最需要關注的方面進行詳細的指導和規範，以便聯邦各部門可以安全地採購政府雲服務。

美國在2010年設立聯邦政府風險和授權管理項目（Federal Risk and Authorization Management Program，FedRAMP）專案認證，要求所有參與政府採購的雲服務商必須經過FedRAMP安全認證，並以“一次認證，多次使用”[12]的認證模式，規定了高、中、低三個雲服務等級以及相對應的四種交付服務模式；美國聯邦政府亦要求雲服務商在每年度進行自認證、事件事故通知以及提供持續性監控資料回饋，以落實政府的持續監管職能。

（三）歐盟

歐盟網絡與資訊安全局（前稱European Union Agency for Network and Information Security，ENISA；現時名稱為European Union Agency For Cybersecurity，下同）於2009年提出《雲計算資訊安全保護框架》[13]、2012年出台《雲計算合同安全服務水準檢測指南》[14]及《釋放歐洲雲計算潛力》[15]、2013年出台《審計安全措施的方案》[16]、2014年提出《政府雲安全框架》[17]等。總括而言，從政府採購雲服務的角度確立一系列科學標準，規範了政府採購、管理、應用的整個環節，如提出了12套針對雲服務商安全能力的審計標準，建立雲服務安全認證體系；在持續監測方面，設計出一套適合不同“生命周期”的政府持續監測雲服務商運行情況的操作體系，並提出了PDCA（計劃－執行－檢查－行動）邏輯模型，為持續監控統一部署。

（四）澳大利亞

澳大利亞政府資訊管理辦公室（Australian Government Information Management Office，AGIMO）於2012年出台《實現雲服務指南》[18]、2012年出台《澳大利亞政府機構的隱私及雲計算》[19]及2014年出台《資源管理指南406：澳大利亞政府雲計算政策》[20]，針對雲採購環節提出評估標準，例如

AS / NZS ISO 31000: 2009、HB 167: 2006等評估標準，構建電子政務雲的安全評估體系，並為政府評估雲服務採購風險構建評估體系。

（五）英國

2012年，英國政府啟動G-Cloud安全認證工作，並表示政府部門可以在G-Cloud名錄中選擇各類雲計算服務。G-Cloud認證結果由低至高分為IL0、IL1、IL2、IL3四個認證等級，IL0等級的雲服務不硬性要求通過安全認證，IL1和IL2等級的雲服務須通過ISO 27001的安全認證標準，IL3則在ISO 27001的基礎上，進一步滿足英國政府資訊標準（HMG Information Standards No.1 & 2）的要求[21]。通過G-Cloud認證的雲服務商可以進入雲市場（Cloud Store），政府部門可以自行依據業務安全需求選擇相應的雲計算服務；在採購方面，英國的採購則以類似在網上商城購物的方式，要求進入雲市場的雲服務商必須經過G-Cloud安全認證，並獲得G-Cloud不同等級認證，雲市場會對雲服務商所提供的雲服務進行詳細描述、表明價格和安全認證等級，而需要採購雲服務的政府部門，需要預先設定好採購標準和所需求的雲服務類型，之後就可以在雲市場上進行搜索，並對搜索結果中的雲服務進行詳細比較，最終選出最適合的雲服務，在確定採購的雲服務後，雲市場提供指導性的政府採購服務合同，以規範雙方權利和義務，防範未來可能發生的安全風險。此外，英國政府為採購雲服務提供了指導性的合同規範，並同時令合同能符合G-Cloud雲服務合同框架。

五、本澳信息安全保障制度之概況

隨着科技的發展，電腦系統、數據資料、網絡信息安全等領域在社會生活中已變得極為重要，更為刑法須要保護的法益，現時澳門刑法體系中專門針對信息保護的相關規定包括：

（一）第11/2009號法律《打擊電腦犯罪法》

該法律是經參考歐洲委員會《打擊網絡犯罪公約》後編制，澳門雖然沒有加入該公約而不受其約束，但仍自願追隨公約所倡議的其中一個基本目標[22]。

該法律第四條至第十一條的規定，主要是針對具體的犯罪技術手段，並結合實害的發生從而制定相應的法律條文，包括不當進入電腦系統；不當獲取、使用或提供電腦數據資料；不當截取電腦數據資料；損害電腦數據資料；干擾電腦系統；用作實施犯罪的電腦裝置或電腦數據資料；電腦偽造；電腦詐騙等八項犯罪行為。同時，法律亦訂定了有關搜查和扣押的程序和法律規定，通過建立一個搜集和保存任何犯罪的電子證據的特別制度，以應對電腦犯罪的偵查工作所面對的巨大困難。

為應對資訊科技犯罪的快速變化，尤其是應對越趨猖獗的“偽基站”犯罪對本澳帶來的嚴重影響，澳門保安司統籌司法警察局完成了《打擊電腦犯罪法》的修法研究工作，並爭取儘早完成修法工作，將針對“偽基站”犯罪設立專門罪名，有關罪行一般可判處三年徒刑，屬加重情節者判罰更可提高至最多五年徒刑，以提高犯罪成本及加強阻嚇力。此外，司警局亦會與內地警方及電訊企業緊密交流，加強對“偽基站”犯罪的調查工作，強化情報主導，採取主動警務的多種策略，制訂“快速察點、機動打擊”的行動模式。

（二）第8/2005號法律《個人資料保護法》

該法律的核心是保護作為個人基本權利的隱私權，個人資料的保護與資訊技術密不可分，法律對個人資料的保護不限於針對電腦儲存、處理及網絡傳輸的規管。當個人資料被人侵犯時，違法的後果可以是行政處罰（如該法律第30條至第36條的規定），當達至犯罪時則採取刑事處罰（如該法律第37條至第42條的規定）。

（三）第13/2019號法律《網絡安全法》

這是一部以“守護”、“防範”及“管理”為主的法律，透過監察關鍵基礎設施營運者是否履行網絡安全義務，以及檢視關鍵基礎設施營運者資訊系統與互聯網之間的網絡流量

及特徵等，瞭解網絡安全狀況，達至防範、偵察及打擊網絡入侵及攻擊，確保關鍵基礎設施網絡安全，保障本澳公共安全、公共利益或公共秩序；應對網絡安全事故，推行網絡安全義務及措施，進一步完善網絡安全防範管理制度；發出預警信息，防止或減少關鍵基礎設施的網絡安全事故；以及開展針對性的宣傳教育活動，提升關鍵基礎設施營運者的網絡安全意識等目的[23]。

（四）其他

為了降低因資訊科技發展而衍生的資訊安全風險，除了上述法律外，特區政府還制定了《電信綱要法》、《電子文件及電子簽名法》、《電子認證郵戳公共服務規章》、《電子文件收發及管理指引》、《流動應用程式開發的指引》、《資訊保安政策指引》和《資訊安全管理框架》等規範性文件，作為保護資訊安全、電子文件效力、個人資料保護、網站構建及數據交換等領域的指引及規範，以貫徹特區政府依法施政的原則。

可見，與事後處罰的保障相比，事前及事中的保障同樣重要，將於2019年底生效的《網絡安全法》便正正是為了填補這方面制度上的空白而擬定的法律。然而，基於網絡安全的具體防護機制及措施，因應不同情勢，須隨時進行更新和調整，並強調專業性和技術性，因此特區政府遵照適度立法的原則，《網絡安全法》不會直接規範維護網絡安全的具體措施，例如防火牆、加密系統、電子認證和病毒入侵檢測系統的採用標準等技術標準，此類措施將按照政府所訂定的總體方向，透過監察實體的指示及傳閱文件作出規範。

六、改善建議

根據澳門特區審計署於2018年8月發表的衡工量值式審計報告，本澳電子政務的發展仍有很大的改善空間[24]，如何建立符合規範的電子警務系統的相關法律法規更是幾乎完全空白，相信在2019年12月22日《網絡安全法》正式生效後，仍然會有大量技術性規範需要根據情勢的變化而持續制訂，並極可能以補充性行政法規或內部規範性文件等形式出台，其中亦應包括電子警務系統方面的相關制度。總括而言，為了對電子政務雲作全方位的保障，筆者在參考上述各國的標準做法後，認為創設制度的關鍵節點在於下述四點：

第一、構建電子政務雲的相關安全標準

安全技術標準具有指引各應用部門的作用，有助於各部門按指引發現自身的問題並作出修正，缺乏標準則會導致各個部門之間難以協調，在安全管理上良莠不齊，更不利於建立粵港澳大灣區警務部門之間互聯互通的合作基礎。

第二、設立全國統一的電子政務雲安全認證制度

認證制度之目的在於排除不達標的政務雲系統提前被應用的可能性，並減少不合格的電子政務雲洩漏信息的風險，如缺乏統一的安全認證制度，亦會導致各地的有關部門在採購時缺乏衡量的依據，因而亦將阻礙區域合作的成效，統一的電子政務雲安全認證體系可以從源頭控制雲服務商的安全風險，並且將這種控制能力上升到中央層面。

第三、設立統一有效的電子政務雲監管制度

電子政務雲的運營及管理通常依賴於雲計算服務商，如政府無權對其進行監督管理，在出現雲服務商的工作人員濫用權力、疏忽或為了不法目的而故意侵犯系統及信息時，政府便不能及時介入。因此，制定相關制度有利於政府在出現事故時及時處理問題，並防止事態進一步惡化，而建構統一的監督管理制度則有利於區域合作的展開，以及防止出現安全隱患的“低窪效應”。

第四、建設政府採購雲服務的完善制度

從信息安全的角度考慮，採購是保障安全最為關鍵的防線之一，對建構電子政務雲的服務供應商具有篩選的作用，如果無法將不合資格的電子政務雲排除在外，便會為日後可能建成的系統埋下重大的安全隱患，因此，各國對採購及其相關方面的制度均極為重視，為了進一步規範政

府的採購工作，可以參考上述各國的做法，以提供合同範本的方式指導採購的進行。

對於警務雲的構建問題，應在基本完成政務雲的制度建設及基礎建設後，再針對警務雲的特殊需要，制定特別規範，並以政務雲的制度作為補充適用的一般性規範，全面保障警務信息安全。

七、結語

2018年4月21日，國家主席習近平出席“全國網絡安全和信息化工作會議”並發表重要講話，強調“沒有網絡安全，就沒有國家安全”[25]，信息安全作為網絡安全的基礎，既牽涉國家、國防、公共秩序等層面的利益，亦與個人隱私等信息法益密切相關。澳門特別行政區作為國家的一部份，在國家作為網絡大國的背景下，必須配合並貫徹將信息安全上升為國家安全戰略的大政方針。

警務信息安全作為國家信息安全的一個分支，不單止是預防、調查及打擊犯罪活動的關鍵，更是大灣區警務部門互聯互通、情報交流、互利共贏的基礎。因此，警員應對信息安全技術及其漏洞有足夠的瞭解，在日常工作中特別注意風險出現的可能性，儘可能避免實害的發生。然而，由於現行的法律制度難以適應信息安全隱患的威脅，特別是在面對警務雲系統建成後將帶來的機遇與挑戰時，為了填補該等漏洞，應從信息安全技術及刑事、行政等法律技術的角度，對信息安全作事前、事中及事後的全方位保護，以完善相關法律體系，促進各地警務部門的跨境警務合作。

註：

1. 又名雜湊函數，是指把輸入的數據轉換成固定長度的不規則的值的函數，得出的不規則的值也可視為數據的摘要，適用於各種情況。
2. 在密碼學中，是指通過在密碼任意固定位置插入特定的字串，讓散列後的結果和使用原始密碼的散列結果不相符，這種過程稱之為“加鹽”。
3. “概念”被哲學家、語言學家、心理學家甚至不同領域的學科專家各賦予多元的意義，Braund（1991）將“概念”解釋的範圍，分為基本概念（basic concept）、上位概念（superordinate concept）及下位概念（subordinate concept）。
4. 指潛入敵對勢力或競爭對手從事秘密刺探情報或是進行破壞活動的人，以此來使其所效力的一方有利。（引述自維基百科）
5. 全國信息安全標準化技術委員會：《信息安全技術　雲計算服務安全指南》（GB/T 31167-2014），北京：中國標準出版社，2014年。
6. 全國信息安全標準化技術委員會：《信息安全技術　雲計算服務安全能力要求》（GB/T 31168-2014），北京：中國標準出版社，2014年。
7. 劉敏玲：〈構建警務雲區際信息共享平台的設想〉，載《第五屆“澳門．珠海警務論壇”交流論文集》，2018年6月，第28頁。
8. 陳興蜀、楊露、羅永剛、葛龍：〈國內外雲計算安全標準研究〉，《信息安全研究》，2016年第五期，第424至428頁。
9. Wayne Jansen & Timothy Grance, Guidelines on Security and Privacy in Public Cloud Computing (US: National Institute of Standards and Technology, 2011), ＜https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf＞.
10. Lee Badger & Tim Grance ET AL, Cloud Computing Synopsis and Recommendations (US: National Institute of Standards and Technology, 2012), ＜https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf＞.

註：

11. National Institute of Standards and Technology, Creating Effective Cloud Computing Contracts for the Federal Government, 2012, ＜https://www.fedramp.gov/assets/resources/documents/Agency_Cloud_Procurement_Best_Practices.pdf＞.
12. 張曉娟、郭娟：〈國外政府雲計算安全標準建設及啟示〉，《電子政務》，2016 年第四期，第83至89頁。
13. European Union Agency for Network and Information Security (ENISA), Cloud Computing Information Assurance Framework, 2009, ＜https://www.enisa.europa.eu/publications/cloud-computing-information-assurance-framework＞.
14. European Union Agency for Network and Information Security (ENISA), Procure Secure: A guide to monitoring of security service levels in cloud contracts, 2012, ＜https://www.enisa.europa.eu/publications/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts＞.
15. European Commission, Unleashing the Potential of Cloud Computing in Europe, 27.09.2012, ＜https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF＞.
16. European Union Agency for Network and Information Security (ENISA), Schemes for auditing security measures, 2013, ＜https://www.enisa.europa.eu/publications/schemes-for-auditing-security-measures＞.
17. European Union Agency for Network and Information Security (ENISA), Security Framework for Governmental Clouds, 2014, ＜https://www.enisa.europa.eu/publications/security-framework-for-governmental-clouds＞.
18. Australian Government Information Management Office, A Guide to Implementing Cloud Services, 2012, ＜https://www.finance.gov.au/files/2012/09/a-guide-to-implementing-cloud-services.pdf＞.
19. Australian Government Information Management Office, Privacy and Cloud Computing for Australian Government Agencies, 2012, ＜https://www.finance.gov.au/files/2012/02/Cloud-Privacy-Better-Practice-Guide-FINAL.pdf＞.
20. Australian Government Information Management Office, Resource Management Guide No. 406 Australian Government Cloud Computing Policy, 2014, ＜https://www.finance.gov.au/sites/default/files/Resource%20Management%20Guide%20406%20Australian%20Government%20Cloud%20Computing%20Policy_0.pdf＞.
21. 同12。
22. 參見第三常設委員會：《第3/III/2009號意見書》，＜http://www.al.gov.mo/uploads/lei/leis/2009/11-2009/parecer_cn.pdf＞。
23. 參見《網絡安全法》諮詢文本，＜https://www.gss.gov.mo/media/Documento_C.pdf＞。
24. 參見澳門特別行政區審計署：《衡工量值式審計報告──電子政務的規劃及執行》，2018年8月。＜http://www.ca.gov.mo/files/PA4018cn.pdf＞。
25. 〈習近平這些金句照亮新時代網路強國之路〉，《新華網》，2018年4月21日。＜http://www.xinhuanet.com/politics/2018-04/21/c_1122720100.htm＞。

參考資料：

1. 趙春暉：《我國電子政務雲的法律保護研究》，北京交通大學2017年碩士論文， 第23至26頁。
2. 于志剛、李源粒：〈大數據時代數據犯罪的制裁思路〉，《中國社會科學》，2014年第10期，第100至120頁。
3. 周棟樑：〈比較內地與澳門網絡犯罪的規定〉，馬耀權、張強主編：《區域警務合作的實踐與探索（2010-2016）》，中國人民公安大學出版社，2016年5月1日，第243至253頁。