偵查電腦犯罪的主要困難及修改《打擊電腦犯罪法》的主要內容

《打擊電腦犯罪法》為澳門有效打擊電腦犯罪提供重要的法律保障，但該法律自 2009 年 8 月生效至今，社會及科技急速發展，為市民帶來新生活方式、模式的同時，亦衍生出許多現行法律難以應對的新型電腦犯罪手法。故此，為應對電腦犯罪形式和型態的改變，須適時檢視法律未能適用的情況，及時修補相關漏洞，填補法律空白，才能在制度上和能力上有效應對新型電腦犯罪帶來的挑戰。

保安司及司法警察局總結了過去十年執法實務經驗，以及近年來電腦和網絡犯罪的新形勢，針對澳門現實情況和困難，經過充分及深入的分析研究，建議從以下四個方面著手進行修法：

（一）將偽基站獨立成罪；

（二）加強對關鍵基礎設施營運者和其他重要實體電腦系統的刑法保障；

（三）依法提取澳門以外的電腦數據資料副本作為刑事訴訟程序的證據；

（四）將違反職業保密、不正當揭露安全關鍵漏洞的行為獨立成罪。

尤其是上述第（三）點的修法內容備受關注，由於當中涉及較為複雜的法律及技術問題，故在此僅對該點展開詳細論述，作如下說明。

一. 當前就跨境雲端服務環境下電子證據的獲取所面臨的困難

隨著互聯網、跨境通訊及雲計算技術的飛速發展和普及，電腦數據資料跨越地域界限，儲存於不同司法管轄區已成為常態。近年在調查各類犯罪、尤其是網絡犯罪，發現有不少犯罪份子將涉案電子數據資料不再單純儲存於本澳境內，而是儲存在雲端服務平台上，該等做法從技術和法律層面均給偵查、取證等工作帶來巨大的挑戰。

目前涉及獲取儲存於境外雲端服務平台上的電子證據，只能通過傳統刑事司法協助程序在雙邊或多邊框架下開展。但是，司法協助程序複雜且耗時，請求往往得不到及時回應甚至未獲回覆，重要的電子證據可能已經滅失，結果導致刑偵工作不能有效開展甚至被迫中止調查。

在互聯網時代司法協助顯然已不是最佳方案，另一個重要原因是其只適用於能夠明確識別雲端服務提供商及數據儲存地的情況。由於技術上存在一些匿名化或被故意隱蔽的互聯網服務，例如：“深網”、“暗網”、詐騙網站、非法賭博網站等，其網站服務提供商及數據儲存地往往是不明確的，並且無法通過常規方式訪問及追蹤。這類巧妙利用互聯網技術隱藏其真實身份及犯罪事實的手段，對案件偵查及電子證據獲取造成極大困難。

二. 各國應對跨境電子取證的新模式

為應對上述困難，很多國家或地區，比如美國、歐盟（尤其葡萄牙）、中國、新加坡等，已因應互聯網技術發展及雲端服務的特性，立法對互聯網電子數據取證採取新措施。其中最具代表性的措施之一就是已被多國採用、並獲各國普遍認可的“網絡在線獲取”，該措施是指依法在線獲取公開的數據資料，或透過從合法途徑取得之涉案電子設備，在線獲取設備所能直接連接的互聯網服務之數據內容。

三. 依法提取澳門以外的電腦數據資料副本作為刑事訴訟程序的證據

為適應網絡時代之特性，並滿足澳門執法工作之需要，本次修法建議刪除

《打擊電腦犯罪法》第十六條第一款（六）項規定中“位於澳門特別行政區”的地域限制表述，以採納“網絡在線獲取”新模式，但這並沒有改變本澳現行的刑事程序，即警方仍必須先請求司法當局批准，由司法官按案件實際情況依法作出批示許可或命令後，才可循合法程序扣押的電子設備，依法在線獲取該設備所能直接連接的互聯網服務之數據內容資料副本作為刑事訴訟程序的證據，而不論該等電子數據資料是儲存於澳門境內還是境外。同時，對“深網”和“暗網”等雲端服務提供商及存儲位置不明確的電子數據，也可依法適用網絡在線獲取措施進行取證，從而解決目前執法部門在偵查、取證等工作上遇到的困難。

四. 結語

隨著電腦及網絡犯罪手法不斷演進，相關的刑事法律制度亦應隨之及時修訂完善。是次將進行的《打擊電腦犯罪法》修法工作，能令司法當局和執法機關擁有更完善及更具針對性的法律支持，從而保障偵查、取證等執法工作的有效展開，提升預防和打擊電腦犯罪的成效，維護網絡安全，保障廣大市民的合法權益和整個社會的長治久安。