【解牛集】— 刊於〈信報〉，2017 年 4 月 25 日

香港須加強網絡犯罪攻擊防線

許佳龍

科大資訊、商業統計及營運學系教授

電話騙徒踏入今年頻密出擊。警方上周公布，今年第一季便接獲 171 宗電話騙案，當中 127 宗有損失，涉及金額高達 4058 萬元，一半案情都是假冒官員行騙； 3、4 月的電話騙案尤其活躍，較 1 月及 2 月明顯上升，在剛過去的復活節假期，便有 11 宗假冒官員的騙案，涉及款項 1245 萬元，可見電話騙案「撲之不滅」，市民須加倍留神。

迄今，不少香港人每一天仍收到這種不知來處的電話。為何電話騙案源源不斷，難以撲滅？對於這個很多人心中的「疑團」，筆者將於下文加以解答。

香港成為網絡犯罪攻擊目標

另一方面，於 4 月初， 澳大利亞電訊（Telstra）委託諮詢公司 Frost & Sullivan 進行調查，並發表了一份《網絡安全調查報告 2017》。這次調查對象是澳洲和亞洲區內三百六十名資訊科技（IT）領導及企業管理高層。報告指出，亞洲國家受到網絡攻擊數目不斷增加，超過半數（59%）受訪的亞洲企業，每月至少遭受到一次引致業務中斷的網絡攻擊。其中，印度企業面臨網絡攻擊的風險最高，有 14.8%印度企業平均每周受到攻擊；緊隨其後者為香港，有 14.7% 的企業每周都會遭遇網絡攻擊（參見《Security Asia》, *Cyber security attacks on the rise in Asia; India, HK most at risk* 一文的報導 • http://www.networksasia.net/article/cyber-security-attacks-rise-asia-india-hk-most-risk.1491178674），可見香港已成為全球網絡犯罪份子攻擊的主要目標之一。

事實上，近年網絡技術的發展一日千里，與此同時，也在全球範圍內衍生了令人防不勝防的網絡罪犯（cyber criminals）。今天，網絡犯罪分子可以輕易地向其他國家的受害者發起攻擊；他們利用國與國之間的政治制度分歧或刑事犯罪的定義分歧來逃避起訴，從中作弊並逍遙法外。

「肯雅案」帶出的問題

記得 2014 年 11 月底，肯雅（Kenya）警方調查一宗華人男子火災致死案時，連帶破獲了一宗涉及 77 名華人（包括 28 名台灣人）的電信詐騙案。案件輾轉到去年 4 月 5 日審結，宣判當中 37 名華人（包括 23 名台灣人）無罪，因為電話詐騙受害人不是肯雅人，所以沒有起訴，即使犯這類網絡罪行遭當地執法機構起訴，判刑也很輕。這些人被判無罪後，就被肯雅遣送出境。

由於中國和肯雅有邦交，所以中國透過外交途徑，要求把該案的涉嫌人全數遣送回中國，但其中 15 名台灣人因拒絕被遣送往中國大陸，而遭到肯雅警方強行帶離看守所進行遣送，同時引發兩岸一次外交風波。為什麼拒絕被遣送到中國大陸，冀回台灣受制裁呢？原因很簡單，因為台灣對於這類網絡犯罪的判刑遠比中國大陸為輕。

再看另一宗個案。去年 12 月，香港、尼日利亞及馬來西亞三地執法人員展開聯合行動，搗破一個跨國網上情緣騙案集團，包括肯雅案所顯露的案情，撇開政治因素不談，案件其實帶出了一個很重要的問題，也是很多人心中的疑竇——為什麼嫌疑犯不惜長途拔涉，遠赴肯雅和馬來西亞等地進行電話行騙？原因也很清楚了，因為犯案地對網絡犯罪的判刑不重。

法律灰色地帶成犯罪溫床

解開了這個「謎團」，不僅可以幫助我們了解為何香港成為「電話騙案」歹徒攻擊的目標，也可以看到香港在防範網絡犯罪行為上處於很被動的位置。事到如今，防患於未然，讓社會洞悉箇中的不足，並找出應對方法，是本文所要表達的主旨。

可以這樣說，網絡犯罪份子選擇肯雅和馬來西亞等第三方國家，作為「經營基地」，因為這種網絡犯罪勾當遭揭發後，究竟是由那個主權國進行起訴和作出量刑懲罰？答案並不清晰，存在強烈的灰色地帶；往往多國之間缺乏協調遣返的法律安排。

若然不法份子在作案地的國家還沒有為最新的網絡犯罪立法、或者國與國之間缺乏明確的引渡與驅逐出境協議，那麼，犯罪分子可能遠赴海外，以最小的「犯罪成本」，在這些國家向受害目標進行數碼攻擊。換言之。國與國之間的地域及立法差異，為網絡罪犯提供了一個犯案溫床。

據本港傳媒引述警方的統計數字，本港整體罪案數字由 2011 年近 80,000 宗，跌至 2015 年約 65,000 宗，整體呈持續下降趨勢；相反，科技罪案數字則持續攀升，由 2011 年約 2,000 宗， 至 2015 年已近 7,000 宗，涉及的損失金額更由 2011 年的 1.4 億多港元，激增 12 倍至 2015 年的 18 億。

另據香港警務處於去年 11 月 11 日交給立法會保安事務委員會的資料顯示，電話騙案，由 2006 年的 1 738 宗，增至 2015 年的 2 880 宗，升幅達 65.7%。2016 年 1 至 9 月，警方共接獲 732 宗電話騙案，雖然 2015 年同期有所減少，但損失金額依然超過 1.5 億港元（見立法會 CB(2)110/16-17(04)號文件）。

香港法律防禦力量薄弱

對付網絡犯罪，香港在現行律法當中，的確有針對性的執法條例，如透過「刑事法」中，以「不誠實取用電腦罪名」進行檢控。「電訊條例」亦禁止未經授權使用他人電腦等。細看針對電話騙案的檢控法律，據「立法會 CB(2)110/16-17(04)號文件」顯示，警方會援引《盜竊罪條例》（ 第 210 章） 第 16A 條「欺詐罪」，以及同一條例第 17 條「以欺騙手段取得財產」，作出檢控。

至於從犯罪得益者，則援引《有組織及嚴重罪行條例》（ 第 455 章） 第 25 條，以「處理已知道或相信為代表從可公訴罪行的得益的財產」作出檢控。然而，這些條例只有當罪犯實際在香港犯案，或與香港有引渡或驅逐出境協議的國家犯案時，才有威懾作用。但對於從海外地方發動的網絡攻擊，這些法律是否仍然有效？明顯存在糢糊不清之處。

基於網絡犯罪的跨國/跨境性，正如前文指出，電話騙案的涉案源頭在肯雅和馬來西亞等地方。因此，對網絡犯罪定義和執法等達成集體性協議，以及處理涉嫌網絡犯罪分子提供互助，是很重要的法律救濟手段，同時也藉此堵塞目前犯法份子逍遙法外的法律漏洞。

網路犯罪公約可堵塞漏洞

事實上，香港可借鏡其他國家的執法經驗。於 2001 年，歐洲委員會啟動了「網絡犯罪公約」（Convention on Cybercrime）。這是全球首部針對網絡犯罪行為所制訂的國際公約，目標之一，是冀望國際間對於網絡犯罪立法有一致共同的參考圭臬；同時，國際間進行網絡犯罪偵查時，有一個國際公約予以支持，以達致有效的國際合作。

截至 2015 年底，參與「公約」的國家包括了加拿大、日本、美國以及歐洲許多國家在內的 47 國，公約並已得到各國議會的批准和執行。根據「公約」，參與國對於涉嫌網絡犯罪的電腦流量和存儲數據，允許進行互助性的調查。若有需要並認為適當，成員國可將存儲的電腦資料，提供跨境評估，並把涉嫌犯罪分子安排進行引渡。

筆者透過犯罪資料作出一項實証研究，結果發現，加入「網絡犯罪公約」後的國家，於 2004 至 2008 年期間，受到「分散式阻斷服務攻擊」（distributed denial-of-service attack， DDoS）降低至少 10%。「黑客」採用 DDoS 手段，一般是針對重要服務進行攻擊，如銀行，信用卡支付閘道器，甚至根域名伺服器，對這些機構進行金錢勒索。之所以取得威懾成效，主要因為參與國進行互助，彼此呼應，令犯罪者鑽法律灰色地帶的機會和空間變小，被起訴和懲罰的機會也愈大，犯罪的成本愈來愈高，因此，愈多的國家參加「公約」時，威懾效應愈加趨強。

黑客攻擊香港恐變本加厲

然而，「公約」也是一把雙刃劍。我們發現，當更多的國家參加「公約」時，對非參與國家受到的襲擊也告增加，意味犯罪者將攻擊目標轉移到「受保護較少」的國家。畢竟，網絡罪犯是聰明的，懂得如何選擇更佳目標。這也說明為什麼電訊詐騙案多發生在如中國、肯雅、馬來西亞和台灣等國家或地區，因為這些國家或地區都沒有加入「網絡犯罪公約」。

可以說，當前我們是進行一場「協調博弈」，若然全球所有國家和地區都達成了一個共同的標準，來處理網絡犯罪，那麼，我們將取得最優的威懾效果。但如果並非全體一起共同協調工作，則沒有參與的國家或地區便會吃盡苦頭。香港究竟應該如何選擇？

在可見未來，香港受到海外「黑客」攻擊而受害的網絡犯罪行為，可能會愈來愈多。正如 Telstra《網絡安全調查報告 2017》的資料顯示，香港是繼印度之後最大的攻擊目標；直至目前，不少香港人每天仍收到不明來歷的行騙電話，面對如此形勢，基於香港也非「網絡犯罪公約」成員，因此，當務之急，是我們實有必要強化本身的法律系統和加強對外的關係，避免受到這些網絡攻擊，也避免更多人受害。

〔本文由科大商學院傳訊部筆錄，許佳龍教授口述及整理定稿〕