萬維網專業人員（香港）協會
對《電腦相關罪行跨部門工作小組報告書》
的回應

萬維網專業人員（香港）協會
政策關注小組
於二零零一年一月三十一日
呈交予立法會保安事務委員會

摘要

1 本會基於以下原則對報告書作出回應：

1.1 相關法律必須符合《人權法》和《基本法》第三十九條。

1.2 能夠填補現行法例未能涵蓋的司法漏洞。

1.3 營造良好的網上環境，而不是只是消極地在事後緝拿元凶補救。

2 本會根據上述原則作出的建議包括：

2.1 司法管轄權問題：

2.1.1 本會建議政府暫時不對司法管轄權問題作出任何改動，應交由法律改革委員會研究相關問題，再由法律改革委員會提出建議，交付公眾諮詢。

2.1.2 本會建議特區政府向公眾進一步披露更多與中港兩地電腦罪案司法管轄權的資料。與中國方面作出商討前，必先取得香港業界、法律界人士和市民的共識，並不是在公眾毫不知情下便與中國方面商討有關事項。

2.2 調查時與加密技術相關的問題：

2.2.1 由於強迫交出加密鍵事茲體大，權力不宜被廣泛行使。因此，建議只限調查與《有組織及嚴重罪行條例》相關之罪行、謀殺、大金額商業詐騙（涉及金額超過一千萬）、強姦、販毒和走私戰略物資等數項嚴重罪行時，才可向法庭申請命令，要求當事人交出加密鍵。

2.2.2 由於只有涉及相當嚴重的罪行才可向法庭申請有關搜令，故此應直接由高等法院原訟法庭處理有關申請。

2.2.3 爲了保證每項申請都是極有必要的情況下提出，因此所有申請均應由律政司司長代調查人員提出。律政司司長必須親自細閱案情後，與律政司內之專業法律人員會商後才向法院提出有關申請。

2.2.4 因現時「國家安全」之定義極爲含糊，爲顧及言論自由和公民權利，調查與「國家安全」有關的罪行時，不應可申請強迫當事人交出加密鍵的命令。

2.2.5 根據有關命令而解密的文本，應可獲法庭接納爲證據。

2.3 迎合未來需要的新機制：

2.3.1 在資訊科技廣播局下另立新組織，地位專責有關電腦罪行的立法工作、協調業界和用戶應付電腦保安問題以及維持 CERT 的有效運作。

2.3.2 該新組織地位有如現時電訊管理局。

2.3.3 電訊管理局現時與電腦保安有關的職能，移交該新組織。

2.3.4 CERT 由該組織負責其營運。

2.3.5 由於新組織專門負責應付與電腦和互聯網有關的犯罪問題，更能有效率集中處理相關問題。

2.4 新的法律

2.4.1 本會建議在《電腦罪行條例》中另立罪行針對新興的非法行爲。

2.4.2 任何人如曾蓄意在未經授權情況下，取用載有洩露予第三者可致重大損失之資料，可判處與盜竊罪相同之刑罰。

2.4.3 任何人蓄意利用機器程式漏洞，使他人蒙受損失，即屬違法。

2.4.4 任何人編寫程式，引導機器作出令他人蒙受損失之決策，亦屬違法。

2.4.5 我們同意電腦行騙的刑罰不應輕於《盜竊罪條例》上同類罪行的刑罰。

2.4.6 任何人蓄意製造大量垃圾封包予對方亦屬違法。

2.4.7 法律改革委員會亦應就新罪行的訂立作出研究，並諮詢公眾。

2.4.8 警方應考慮另設電腦罪行調查科，專門調查相關罪行。

2.5 針對互聯網供應商保留用戶登出登入紀錄問題

2.5.1 本會建議業界諮詢執法人員、私隱專員和用戶組織的意見後，自行訂立實務守則。

2.5.2 由該自願守則統一規定資料紀錄格式和保留期限。業界組織可多向用戶介紹有關做法，給予用戶信心。

本會所堅持的基本原則

1.1 本會基於以下原則對報告書作出回應：

1.1.1 相關法律必須符合《人權法》和《基本法》第三十九條。

1.1.2 能夠填補現行法例未能涵蓋的司法漏洞。

1.1.3 營造良好的網上環境，而不是只是消極地在事後緝拿元凶補救。

司法管轄權

2.1 背景及立場

2.1.1 在互聯網普及下，電腦罪案往往涉及大量跨境罪案，司法管轄權問題確實相當棘手。而報告書中的第四章，亦有提及有關問題。

2.1.2 司法管轄權此問題極爲敏感，特別是涉及中港兩地罪行。報告書中沒有提及中港兩地跨境罪行，但張子強案後，公眾對中港兩地司法管轄權有關的事極爲關注。

2.1.3 由於互聯網的發展，電腦罪案的司法管轄權問題亦會涉及對現有法律的改革，牽一髮動全身。

2.2 對有關問題的建議

2.2.1 本會建議政府暫時不對司法管轄權問題作出任何改動，應交由法律改革委員會研究相關問題，再由法律改革委員會提出建議，交付公眾諮詢。

2.2.2 本會建議特區政府向公眾進一步披露更多與中港兩地電腦罪案司法管轄權的資料。與中國方面作出商討前，必先取得香港業界、法律界人士和市民的共識，並不是在公眾毫不知情下便與中國方面商討有關事項。

加密

3.1 問題背景

3.1.1 在報告書的第五章中，有提及在罪案調查上與加密相關的問題。

3.1.2 在現時的加密技術發展下，有些犯罪資料可能隱藏於一些可見和可讀的電子文件中，例如圖像檔或一些經過處理的文字檔。在這技術發展下，就算電子文件以可見和可讀形式展示，亦不會提取相關之犯罪證據，因而錯失檢控良機。

3.1.3 從執法者的角度，可能認爲強迫當事人交出加密鍵有助調查工作的進行，並使解密後的資料不容易受到挑戰。但倘若可以強迫當事人交出加密鍵解碼，可以會有要求當事人交出可能令其入罪證據之嫌。

3.1.4 需要加密的檔案資料往往涉及個人私隱，強迫當事人交出加密鍵亦是不尊重私隱。

3.1.5 對大企業來說，有時候可能數名員工共用一套加密鍵，交出解密鍵可能會導致公司需要更改所有員工的解密鍵，造成極大的不便，成本亦相當高。

3.2 基本立場

3.2.1 加密技術對電子商貿的發展相當重要，因此本會反對政府規管加密技術。

3.2.2 交出已解密文本，有迫令當事人交出導致其入罪證據之嫌。基於保護公民權利的原則，本會反對任何機構有權迫令當事人交出已解密文本。

3.2.3 在平衡調查時的技術需要、大企業所面對的技術困難和當事人的權益後，本會認爲強迫披露資料的權力應授與予法院，由法官根據法例決定強迫當事人交出加密鍵與否。

3.3 具體建議

3.3.1 由於強迫交出加密鍵事茲體大，權力不宜被廣泛行使。因此，建議只限調查與《有組織及嚴重罪行條例》相關之罪行、謀殺、大金額商業詐騙（涉及金額超過一千萬）、強姦、販毒和走私戰略物資等數項嚴重罪行時，才可向法庭申請命令，要求當事人交出加密鍵。

3.3.2 由於只有涉及相當嚴重的罪行才可向法庭申請有關搜令，故此應直接由高等法院原訟法庭處理有關申請。

3.3.3 爲了保證每項申請都是極有必要的情況下提出，因此所有申請均應由律政司司長代調查人員提出。律政司司長必須親自細閱案情後，與律政司內之專業法律人員會商後才向法院提出有關申請。

3.3.4 因現時「國家安全」之定義極爲含糊，爲顧及言論自由和公民權利，

調查與「國家安全」有關的罪行時，不應可申請強迫當事人交出加密鍵的命令。

3.3.5 根據有關命令而解密的文本，應可獲法庭接納爲證據。

新經濟新法例

4.1 背景

4.1.1 報告書由第五章起到第十三章，都是針對非法取用電腦等連串保安問題作出建議。

4.1.2 由於在可見的將來，全港大部分企業，包括中小企業都會在網上進行 B2C 和 B2B 的電子商貿，政府亦積極推廣公共服務電子化。防範日新月異的電腦罪行已是與公眾利關攸關的課題。

4.1.3 根據思科電腦的資料，黑客有四種方法破壞或盜取電腦系統內的資料：

4.1.3.1 破壞系統保安系統取得系統控制權。

4.1.3.2 使用虛假資料或利用系統漏洞進入系統或瞞騙系統。

4.1.3.3 奪取路由器的控制權，在公眾或 ISP 路由器上截取網絡通訊封包（packet）。

4.1.3.4 製造大量垃圾封包，導致網絡通訊癱瘓。

4.2 現時法例的漏洞

4.2.1 對數據的保護

4.2.1.1 若黑客入侵時沒有刪改電腦內的任何數據，當只要黑客曾瀏覽電腦中的一些重要數據，或在通訊封包中解讀出一些重要數據，如源程式碼，已可使對方蒙受損失，行爲與盜竊無異。

4.2.1.2 現時的《盜竊罪條例》的定義，只是定義「盜竊」爲非法轉移資產，而以上入侵行動並沒有轉移資料，根本不足以涵蓋上述「盜竊」行爲。

4.2.2 欺騙電腦

4.2.2.1 現時法例已足以對付使用虛假資料人士。

4.2.2.2 但在可受預設程式控制的機器越來越多的情況下，機器不可能受騙的普通法原則已經不合時宜。因爲在後 PC 時代，會越來越多可供程式控制的機器出現。現時已有可接受八達通的自動販賣機出現，此類機器日後只會有增無減。

4.2.3 對拒絕服務襲擊沒有防範

4.2.3.1 在 2000 年的夏天雅虎及多個美國網站曾受此類方法襲擊，對電子商貿來說是極大的威脅。

4.2.3.2 現時的法例亦不足以涵蓋使用 DoS（拒絕服務）方法進行破壞的黑客。

4.3 現時機制的問題

4.3.1 現時沒有中央統籌機制專責與電腦相關法律的制訂。

4.3.2 基於人類可以藉電腦程式應用電腦於極廣泛用途上，彈性極大，未來發展難以預計，現在法例窮於應付。

4.3.3 電腦連接而成的互聯網，更是有本身內在規則的新社會。

4.3.4 在沒有統籌機制針對電腦進行相關立法，導致很多網上衍生的新罪行，包括上述黑客行爲以及網絡侵權、賭博和色情資訊問題，政府無計可施。

4.3.5 亦由於沒有中央統籌，使針對有關問題的教育工作缺乏效率。亦難以有效協調各方，迅速杜絕未來出現的新問題。

4.3.6 電腦保安問題可以造成廣泛的災難，而沒有中央統籌機制，報告書中 CERT 在沒有經常性經費下運作，難以符合國際上 24/7 要求。

4.4 對新架構的建議

4.4.1 在資訊科技廣播局下另立新組織，地位專責有關電腦罪行的立法工作、協調業界和用戶應付電腦保安問題以及維持 CERT 的有效運作。

4.4.2 該新組織地位有如現時電訊管理局。

4.4.3 電訊管理局現時與電腦保安有關的職能，移交該新組織。

4.4.4 CERT 由該組織負責其營運。

4.4.5 由於新組織專門負責應付與電腦和互聯網有關的犯罪問題，更能有效率集中處理相關問題。

4.5 新的法律

4.5.1 本會建議在《電腦罪行條例》中另立罪行針對上述非法行爲。

4.5.2 非法盜取電腦上資料

4.5.2.1 任何人如曾蓄意在未經授權情況下，取用載有洩露予第三者可致重大損失之資料，可判處與盜竊罪相同之刑罰。

4.5.2.2 該資料是否可導致重大損失的機密資料，舉證責任在控方，以保障被控一方的權益。

4.5.3 欺騙電腦

4.5.3.1 任何人蓄意利用機器程式漏洞，使他人蒙受損失，即屬違法。

4.5.3.2 任何人編寫程式，引導機器作出令他人蒙受損失之決策，亦屬違法。

4.5.3.3 我們同意電腦行騙的刑罰不應輕於《盜竊罪條例》上同類罪行的刑罰。

4.5.4 任何人蓄意製造大量垃圾封包予對方亦屬違法。

4.5.5 法律改革委員會亦應就新罪行的訂立作出研究，並諮詢公眾。

4.5.6 警方應考慮另設電腦罪行調查科，專門調查相關罪行。

保存用戶資料紀錄

5.1 基本立場

5.1.1 報告書的第八章有提及保存用戶登出登入資料的問題。

5.1.2 用戶登出登入紀錄對執法人員調查一些甚高明的罪犯作案並無太大幫忙，因爲水平較高的犯案者已經能夠迴避多個技術關卡，不讓執法人員根據在互聯網供應商紀錄中追查其行蹤，但有關資料仍有助執法人員調查某些電腦罪案。

5.1.3 若然法例規定互聯網供應商保留一定格式和時期的紀錄，將使公眾對其私隱是否受到保障存有疑慮。因爲用戶的登出登入紀錄本身已是私隱，一般人都不願其上網行爲模式讓第三者知悉。

5.1.4 對用戶資料此類並非極爲重要的問題上，由業界自行決定遠比政府介入爲佳。

5.2 具體建議

5.2.1 本會建議業界諮詢執法人員、私隱專員和用戶組織的意見後，自行訂立實務守則。

5.2.2 由該自願守則統一規定資料紀錄格式和保留期限。業界組織可多向用戶介紹有關做法，給予用戶信心。

5.2.3 現時硬碟的成本不高，基本上保存六個月用戶登入登出紀錄並不會令成本劇增，相信業界會接受自行訂立守則的做法。