線上遊戲盜寶案件偵辦標準程序

涂　仕　瑋

大　綱

壹、代前言—線上遊戲盜寶案件之實體法問題簡介

隨著電腦與網際網路的普及，在地域及身分逐漸模糊的互動下，網際網路的使用者逐漸形成多元而虛實難辨的社交空間。對於法律學者及實務運作者而言，傳統法律及法學思維，能否一成不變地適用於此等新興的生活範疇，抑或須修正舊有的遊戲規則，甚至大破大立，建立網路世界專有的法秩序，尚無定論。

就我國而言，最普遍而特有的網路相關非行，當屬所謂「線上遊戲盜寶案件」。2005 年臺灣地區線上遊戲市場會員營收(Subscription Revenue)約有 2.1 億美元，在亞太地區高居第四位。[註 1] 而就線上遊戲盜寶案件之規範而言，我國先於實務認定適用竊盜罪，繼而於民國 92 年間立法通過刑法第三十六章「妨害電腦使用罪章」，並在立法理由之中，首開各國之先例，默示線上遊戲之電磁紀錄具有財產價值：「...有可能發生強盜無形電磁紀錄之情形(例如：以脅迫方式使人不能抗拒而交付線上遊戲之虛擬寶物)」。[註 2] 自此我國所謂「網路犯罪」案件暴增，線上遊戲案件估計占全體妨害電腦使用案件接近八成。[註 3]

惟有爭議者，線上遊戲盜寶案件是否應以刑法相繩？首先分析盜寶行為與可能相對應之刑法條文如下：

一、行為人在自己所使用之電腦上，未經被害人授權，輸入被害人之帳號、密碼，以被害人身分進入遊戲公司之遊戲伺服器，進行遊戲。此為盜寶之前階段行為，該當於刑法第 358 條之「無故輸入他人帳號密碼，而入侵他人之電腦者」。

二、行為人以被害人帳號進入遊戲中，即得以

註 1：http://www.idc.com.tw/report/Column/column_061030_1.htm (2008 年 6 月 30 日)

註 2：中華民國刑法部分條文修正草案(電腦網路犯罪部分)第三百二十三條說明二，立法院第五屆第三會期第十二次會議議案關係文書，院總第二四六號，政府提案第八八六二號之一

註 3：經以法務部檢察書類查詢系統進行查詢，截至 2008 年 6 月 29 日止，全國地檢署以妨害電腦使用為案由之結案案件書類共 2447 件(包括起訴、聲請簡易判決、緩起訴、不起訴之案件)，經以「網路」、「遊戲」為關鍵字進行過濾，共得 1905 件，占全體 77.85%。

支配被害人在遊戲中所持有之虛擬寶物電磁紀錄。行爲人即將該等虛擬寶物，在遊戲中移轉與其他遊戲進行者。此等移轉虛擬寶物之行爲，就電腦之運作而言，實係變更遊戲伺服器或遊戲公司資料伺服器中之資料電磁紀錄，該當於刑法第 359 條之「無故變更他人電腦之電磁紀錄」；若從被害人之觀點言，遊戲公司伺服器中資料庫內關於被害人項下之相關電磁紀錄可謂被刪除，不復存在，該當於刑法第 359 條之「無故刪除他人電腦之電磁紀錄」；若從行爲人之觀點言，其因此取得對於該等電磁紀錄之支配，又該當於刑法第 359 條之「無故取得他人電腦之電磁紀錄」。

由形式觀之，線上遊戲盜寶行爲似以二行爲該當於刑法第 358 條、第 359 條，二行爲間具前後階段關係，前行爲宜論以與罰（不罰）前行爲；或以入侵及取得、變更或刪除電磁紀錄爲社會上一行爲，論以想像競合。惟於適用時並非毫無疑義，至少有以下二爭點：

一、就刑法第 358 條所規範之單純入侵電腦行爲而言，歐洲理事會網路犯罪公約(我國亦爲簽約國)就單純入侵電腦(Illegal Access)之行爲，亦僅課予簽約國以立法或其他措施規範之義務，並未強制須將該行爲入罪化。[註 4] 就比較法而言，先進之英國濫用電腦法(Computer Misuse Act 1990 (c.18))及美國聯邦法典第 18 章第 1030 條(18 USC Sec. 1030)並無類似規定。[註 5] 僅日本不正侵入禁止法第三條有類似規定。再就其立法目的而言，在於保護電腦系統之安全性。[註 6] 盜寶者原則上均係以遊戲者身分進入遊戲伺服器，由資訊管理之觀點，顯然僅具一般使用者之權限，除非另闢蹊徑，否則無從影響系統安全。

二、就刑法第 359 條之取得電磁紀錄等行爲而言，尚設有「致生損害於公衆或他人」之實害結果要件。易言之，必因行爲人之取得、變更或刪除電磁紀錄行爲而造成損害，且行爲與損害之間具有相當因果關係，始足當之。問題在於，盜寶行爲是否「致生損害」？易言之，虛擬寶物是否具有客觀、普世之財產價值？若有，是交換價值，抑或使用價值？是否因入罪化而形同減免遊戲公司之民事責任？凡此均非本文討論重點，茲不贅。我國立法時雖相當程度參考日本法，然日本之司法實務似尚未承認所謂虛擬寶物具有財產價值。[註 7] 惟我國現行實務既多採肯定見解，是以本文乃以此爲前提，討論相關之程序問題，期能提升相關案件之偵辦效率。

註 4：Council of Europe - ETS No. 185 - Convention on Cybercrime
Article 2 - Illegal access
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right.

註 5：上揭註 3 之第三百五十八條說明二稱上開英、美二法律設有處罰，諒係誤解，筆者當另文討論之。

註 6：該條立法說明二：「電腦系統遭惡意入侵後，系統管理者須耗費大量之時間人力檢查，始能確保電腦系統之安全性，此種行爲之危害性已達應已達科以刑事責任之程度，爲保護電腦系統之安全性，爰增訂本條。」同註 3

註 7：http://www.digitalcontent.org.tw/e/files/94/0928/940928-2.htm (2008 年 6 月 30 日)

貳、本文

一、線上遊戲盜寶案件之管轄權

(一) 實務見解

就管轄地之決定而言，依刑事訴訟法第 5 條第 1 項規定，應由犯罪地或被告之住所、居所或所在地之法院管轄。因此，欲確認管轄權之有無，應以被告之住、居所、所在地或犯罪之行爲地、結果地爲依歸。不過隨新興科技漸次深入生活，犯罪行爲人之能力亦因之擴張，如何將適用數十年的管轄權規定，與現代社會事實契合，實務亦著實煞費苦心，茲列舉三則實務見解：

1. 臺灣高等法院 89 年度上訴字第 1175 號判決

「有關網路犯罪管轄權之問題，有別於傳統犯罪地之認定，蓋網際網路不同於人類過去發展之各種網路系統（包括道路、語言、有線、無線傳播），藉由電腦超越國界快速聯繫之網路系統，一面壓縮相隔各處之人或機關之聯絡距離，一面擴大人類生存領域，產生新穎之虛擬空間。是故網路犯罪之管轄權問題，即生爭議。在學說上有採廣義說、狹義說、折衷說及專設網路管轄法院等四說，若採廣義說，則單純在網路上設置網頁，提供資訊或廣告，只要某地藉由電腦連繫該網頁，該法院即取得管轄權，如此幾乎在世界各地均有可能成爲犯罪地，此已涉及各國司法審判權之問題，且對當事人及法院均有不便。若採狹義之管轄說，強調行爲人之住居所、或網頁主機設置之位置等傳統管轄，又似過於僵化。又我國尚未有採專設網路管轄法院，即便採之，實益不大，亦緩不濟急，故今各國網路犯罪管轄權之通例，似宜採折衷之見解，亦即在尊重刑事訴訟法管轄權之傳統相關認定，避免當事人及法院之困擾外，尚應斟酌其他具體事件，如設置網頁、電子郵件主機所在地、傳輸資料主機放置地及其他有無實際交易地等相關情狀認定之。」本件判決之氣度恢宏，胸襟廣博，惜忽略所謂「網路犯罪」爲一不確定概念，本不能也不必專採一說，宜分別案件類型，具體認定管轄權之有無。

2. 臺灣高等法院 92 年度上易字第 1987 號判決

「經查：本件被告乙之住居所及被告丙之住所，分別係在臺北縣蘆洲市...及臺北縣永和市…；被告丙居所係在臺北縣板橋市…。而被告乙、丙二人係在被告丙...住處，分別以…等暱稱登入遊戲橘子公司所管理維護之「天堂」網路連線遊戲之戰神雅典娜伺服器，由被告乙以…，誘騙被害人至臺北縣蘆洲市…之「Ｅ世代網路贏家」、臺北縣板橋市…之「哈啦客棧」及臺北縣板橋市…之「生活資訊館」等處之網路咖啡廳，於獲得被害人之帳號及密碼後，共同意圖爲自己不法之利益，以被害人丁、戊、甲等二十餘人之帳號及密碼，連續多次在前揭網路咖啡廳，以該處電腦主機連接至台北縣中和市...遊戲橘子公司所維護之「天堂」線上遊戲伺服主機，竊取被害人等人在「天堂」線上遊戲所扮演角色所擁有之…等虛擬財物。是被告乙、丙二人之犯罪地，係在臺北縣板橋市…、臺北縣蘆洲市…之「Ｅ世代網路贏家」、臺北縣板橋市…之「哈啦客棧」及臺北縣板橋市…之「生活資訊館」、台北縣中和市…遊戲橘子公司等處，俱不在台灣台北地方法院之轄區。原審據此認並無管轄權，論知管轄錯誤之判決，並將全案移送於被告乙、丙住居所及犯罪地所在之臺灣板橋地方法院，認事用法，均無不合。」本件判決係就線上遊戲案件，認被告使用電腦連上網路之處所(被告自宅或網咖)爲妨害電腦使用之行爲地，遊戲伺服器之所在地或妨害電腦使用之結果地。

3. 臺灣高等法院高雄分院 95 年度上訴字第 1306 號判決

「本件被告之住所地、居所地固分別在台南縣、市，公司之電腦主機固設於桃園縣，固非原審法院管轄區域。惟本件被告係透過電腦網路設備，連線至傳奇網路公司之遊戲網，利用網上對話方式，向另一電腦使用端之澎湖縣民甲，騙取其夫藍哲星之帳戶密碼，再以該密碼進入藍哲星之網路倉庫盜取裝備，致藍哲星之財產利益受損，而該甲、藍哲星之電腦均係設於其等澎湖縣之住處，揆諸上開說明，原審法院對本件犯罪自應有管轄權。」本件判決亦係針對線上遊戲案件，首認存在告訴人(被害人)之「網路倉庫」，次認該等「網路倉庫」位於告訴人之電腦，因此認告訴人之住所地為犯罪地而有管轄權。

(二) 本文看法

1. 線上遊戲係主從式架構之應用

新興科技現象萬千，司法人員往往如入五里霧中，惟若能正確辨明事實部分，或能發現法律之適用不盡困難。就線上遊戲案件而言，首應對於二種基本網路傳輸架構—點對點(peer to peer)及主從式(client-server)—知其梗概。所謂主從式架構，係指依功能將電腦系統區分為客戶端(client)及伺服端(server)，通常由客戶端軟體〔註8〕啓動通訊，與伺服端建立連線，然後客戶端提出要求，伺服端受命提供服務。〔註9〕因此雙方具有主從之關係。至點對點式架構，係指雙方之地位平等，互相可以提出要求及提供服務，並不區分客戶端或伺服端，亦可說是同時得為客戶端或伺服端。〔註10〕

至線上遊戲，係由遊戲公司提供遊戲伺服器，執行伺服端軟體，參與遊戲者則使用安裝有客戶端軟體之電腦，透過網際網路，對伺服器提出要求，由遊戲伺服器提供服務，而服務之內容至少有三：

⑴於參與遊戲者登入時，驗證其帳號及密碼。

⑵應客戶端之要求，提供「進行遊戲」之服務，亦即透過伺服器之運算，將結果顯現於參與遊戲者之電腦螢幕。

⑶提供「資料儲存」之服務，亦即將參與遊戲者之各種遊戲歷程及結果(包括虛擬財物之種類、數量等)，以電磁紀錄方式儲存於遊戲伺服器之資料庫。

由上述可知，遊戲之相關紀錄係存於遊戲公司之遊戲伺服器，並未存於玩家或參與遊戲者之電腦（客戶端）。因此，參與遊戲者的電腦縱然毀損，亦不必擔心遊戲紀錄遺失，還可以在家中、同學家，乃至各地網咖，以不同電腦，連上遊戲伺服器，以同一身分進行遊戲。

2. 線上遊戲案件之管轄地與告訴人住所地無關

綜上，所謂線上遊戲盜寶行為，實係被告利用任一安裝遊戲(客戶端)軟體之電腦，連上網際網路，輸入被害人帳號密碼，進入遊戲伺服器，並取得、變更或刪除遊戲伺服器內之電磁紀錄。是以被告操作上開客戶端電腦之所在地，即犯罪之行為地；被入侵或取得電磁紀錄等之遊戲伺服器所在地，即犯罪之結果地，均有管轄權。上開臺灣高等法院 92 年度上易字第 1987 號判決，誠屬妥適。

至告訴人於遊戲中所獲得之虛擬寶物等，實不過為儲存於遊戲公司伺服器之電磁紀錄，而該等電磁紀錄，自始至終，從未進入玩家所

註 8：嚴格而言，所謂「伺服端」或「客戶端」係就特定應用程式而言，而非指電腦硬體，惟為避免因本文說明過簡致生誤會，在此暫不作區分。以下敘述混用於軟、硬體，以使讀者能簡易明瞭為原則。

註 9：http://en.wikipedia.org/wiki/Client-server (2008 年 6 月 30 日)

註 10：http://en.wikipedia.org/wiki/Peer_to_peer (2008 年 6 月 30 日)

使用之客戶端電腦，僅係告訴人自客戶端透過網際網路與遊戲公司伺服器連線後，得以知悉其「虛擬擁有」該等電磁紀錄而已。上開臺灣高等法院高雄分院 95 年度上訴字第 1306 號判決意旨所稱「告訴人網路倉庫」云者，實亦不過爲遊戲公司伺服器資料庫之一筆或數筆電磁紀錄而已，判決意旨竟據此認爲該等電磁紀錄係自告訴人電腦處取得，不無將「伺服端」、「客戶端」及實體世界與虛擬世界二概念混淆之處。因此，告訴人之住所地或所在地，並非妨害電腦使用罪之行爲地或結果地，原則上與管轄權無涉。

二、目前一般偵辦線上遊戲盜寶案件之程序及問題

(一) 一般程序

線上遊戲盜寶案件發生時，一般處理程序如下：

1. 報案：被害人通常在其住所或所在地就近報案。
2. 處理：轄區員警受理報案後，通常著手以下偵查作爲：
   ⑴自線上遊戲公司取得線上遊戲歷程紀錄及盜寶者帳號之申登資料。
   ⑵以上開盜寶者帳號之登記人爲犯罪嫌疑人，並通知其到案說明。
   ⑶根據上開歷程紀錄所載取得虛擬寶物之 IP 位址，查詢使用該 IP 位址者之實體位置。
3. 移送：移送地檢署偵辦。

(二) 易滋生之問題

上開程序在實務運作時，易滋生如下問題：

1. 報案地之管轄權問題：

被害人就近報案，轄區員警爲便民而受理報案，均無可厚非。然基於網路犯罪之跨地域特性，以及線上遊戲盜寶案件被害人所在地與犯罪之行爲地或結果地往往無關如上所述，受理報案地之法院就此等案件通常並無管轄權。

2. 犯罪嫌疑人之認定：

線上遊戲案件經過數年來之「進化」，已趨向集團化、精緻化，同時由多人控制多數帳戶，一旦取得特定虛擬財物後，恆於極短時間內連轉數手，而自被害人帳號直接取得虛擬財物者，往往亦爲被盜用帳號密碼之人。兼以網路之匿名性，加上遊戲公司把關不嚴，申登帳號資料之可靠性甚低，以此認定犯罪嫌疑人，若無 IP 位址等資料佐證，誤判率甚高。若員警鍥而不捨，持續追蹤虛擬財物去向，[註 11] 可能會找出一連串之前後手，然而前後手之實際關係如何，係同一集團，甚至同一人所爲，抑或毫無關係，均不易求證。

3. 犯罪嫌疑人之通知與證據保全：

基於該等案件之跨地域性，犯罪嫌疑人住所地與報案地以不在同一處爲常態，員警基於職責，固應通知其到案說明。惟犯罪嫌疑人因路途迢迢，常不到案；因此通知兩次不到後，往往移送當地地檢署，此時通常距案發時間已逾六月，無法根據 IP 位址續行追查；縱或到案，全盤否認者占絕大多數，而員警基於比例原則之考量，極少出現長途跋涉以聲請搜索犯罪嫌疑人電腦之例，致證據保全有所窒礙。日後若被告被起訴，縱使 IP 位址相符，亦往往主張木馬抗辯，即「可能有駭客植入木馬，進行遠端遙控」等語，使承審法院陷入困擾。若通

註 11：此種「追蹤」較實體之追贓爲易，因所追蹤者，實係遊戲伺服器內之電磁紀錄，且該等電磁紀錄，只有存在於遊戲伺服器內方有意義，故可由遊戲公司提供。困難之處在於：該等虛擬財物持有者之眞實身分及實體位置何在。

知被告到案說明後，方才對其電腦進行搜索，以確認有無木馬程式，此時該電腦十有八九已重灌(重新安裝作業系統)，以致無從積極破解其抗辯。(註12)

4. IP位址紀錄之蒐證及卷證整理：

按全球之IP位址分配，可概分爲四階層：第一層係非營利機構ICANN(Internet Corporation for Assigned Names and Numbers)，由ICANN負責分配予第二層之全球各區域組織、國家級組織，再由該等組織分配予第三層大型公司或網路服務提供業者(ISP, Internet Service Provider)，最後由上開公司或ISP提供IP位址予一般使用者。欲知特定時間之特定IP位址係何人使用，可先利用網際網路之whois服務，查得第三層業者，若該業者在國內，再向其發函查詢使用該IP位址之申請人及實體位址。

然目前一般員警或受限於經驗或時間，間有未查詢IP位址之情形，或僅查詢數十IP位址之一二，且僅將業者回覆之申請人資料或上線紀錄附卷，並未將whois查詢結果之網頁影本及函詢業者之函稿一併附上，待移送地檢署時，承辦檢察官往往因已逾業者保存紀錄期限而無從續爲偵查，且面對不全之卷證，在理解上亦生困難。

5. 移送與管轄權問題：

受理被害人就地報案之警局，若於偵查作爲告一段落後，逕移送當地檢察署，基於上述原因，通常必須移轉管轄，此舉又再度造成偵查延宕，對於證據之保全，亦是一大戕害。

三、本文之建議—建立合理之標準程序

綜合考量報案之便民性，網路活動之跨地域性、保存證據之時效性，以及管轄權之合法性等因素，本文嘗試建立線上遊戲案件之合理標準程序如下：

(一) 受理報案警局之處理：

1. 受理報案：取得告訴人之指述，以及線上遊戲歷程紀錄。
2. 立刻以whois服務查詢IP位址。查詢結果，若該IP位址屬我國所配發，則函詢受配發之業者或機構。
3. 若犯罪嫌疑人之住所地在受理警局轄區，則斟酌個案情形，決定是否聲請搜索(例如與IP位址之實體所在相符)，或僅通知其到案說明(例如與IP位址之實體所在不符，復別無其他證據以增強心證)。
4. 若犯罪嫌疑人之住所地不在受理警局轄區，則連同whois查詢網頁影本及其他卷證，迅速移送犯罪嫌疑人住所地之轄區警局續行偵辦。若已對於國內ISP等受配發IP位址之業者函詢，並應附上所發函文影本。俟業者回覆後，即轉送其回覆於受移送警局。若行政程序許可，於函詢時即可副知受移送分局，並請業者同時回覆二警局，如此可省去轉送回覆之不便。

(二) 犯罪嫌疑人所在地警局之處理：

1. 收受上述IP位址之函詢副本、移轉案件之卷證，及業者就IP位址之回函。
2. 斟酌個案情形，決定是否聲請搜索(例如與IP位址之實體所在相符)，或僅通知其到案說明(例如與IP位址之實體所在不符，復別無其他證據以增強心證)。

註12：此爲我國實務習見所謂「幽靈抗辯」之數位版本。依證據法則，被告爲有利於己之主張時，應負提出證據責任，證明至「有合理懷疑」程度。請參照：吳巡龍，刑事舉證責任與幽靈抗辯，刑事訴訟與證據法實務，2006年，第57頁以下。

3. 偵查作爲告一段落後，移送當地檢察署。

(三) 受移送地檢署之處理：

1. 收送移送之案件卷證，並確認管轄權之有無。
2. 若被告之住所地或所在地與 IP 位址之實體所在明顯不合(例如 IP 位址係境外機構所配發，表示與遊戲伺服器直接連線之電腦位於境外)[註 13]，本文以爲，若別無支持被告涉案之證據，似尚未達到起訴所須之「表面證據」(prima facie case)程度。[註 14]
3. 若被告之住所地或所在地與 IP 位址之實體所在明顯契合，本文以爲，應認已達起訴所須之表面證據程度。惟目前被告主張木馬抗辯之情形極其普遍，肇因於法院就類似案件往往頗有疑慮，若欲免除木馬抗辯之疑慮，不妨考慮對於被告之電腦進行搜索，送請刑事警察局或調查局進行鑑定，內容至少包括：(1)該電腦作業系統之安裝日期，以確認在案發後有無重灌；(2) 若扣案電腦在案發後並未重灌，其次鑑識該電腦有無被植入木馬或類似之遠端遙控程式。方式包括：在依標準鑑識作業程序下，掃描硬碟複本，檢查有無已知木馬之程式碼；在虛擬機器(Virtual Machine)或類此環境下啓動複本作業系統，確認有無不明之對外連線，以檢查有無存在未知之木馬程式。
4. 尚有一點待補充者，即有無傳喚告訴人，於偵查中具結作證之必要？本文以爲，就證據容許性而言，偵查中具結證言證據能力之有無，尚在未定之天；就證明力而言，類此案件告訴人之指述，通常僅在陳述其虛擬財物不脛而走之事實，甚少能提供其他有助於偵查之陳述。因此於偵訊之中，若告訴人住所地不在地檢署管轄內，原則上似無非傳喚並具結不可之必要。

參、代結論—網路犯罪與偵查之挑戰

網際網路發展迄今，已儼然形成一空前的資訊巨獸，不論儲存、運算乃至傳輸資訊之質量、速度，均已遠遠超出吾人所能駕馭。網際網路本身雖屬中性，提供吾人生活、工作之相當便利，然一如光與影之二元對映，負面資訊亦不免隨之與時俱增，此一力量，看似無形，實則沛然莫之能禦，造成司法者不能承受之輕。執法人員不僅在技術上，要能在資訊洪流中，迅速篩選出必要之一瓢飲；在人力、時間有限之情形下，要如何分配資源，以求有效率地實踐正義，維持法秩序於不墜，誠屬不易。本文作者希冀就此略盡棉力，期能拋磚引玉，並致力於新興科技知識之普及，使司法人員終能視此爲普通常識，俾便正確認定事實、適用法律，是爲文。

（本文作者現職為臺灣臺南地方法院檢察署檢察官，具 MCP、CWNA、CCNA、Security+、TCSE、TCCF、TCSM 等資訊管理、安全及鑑識等相關認證）

註 13：IP位址在境外之原因：⑴行爲人確實在境外。⑵行爲人在境外，但被告與行爲人有犯意聯絡。⑶行爲人在境內，但透過境外之代理伺服器(proxy)或類此機制，自境外連回境內之遊戲伺服器，以致遊戲伺服器連線紀錄之IP位址位於境外。後二者之情形，在現今之國情及技術下，甚難查證。

註 14：同註 13，63-64 頁。