中華警政研究學會

警政與警察法相關圓桌論壇(四十三)
【阻斷不法詐欺網站之法制探討】會議紀錄

日期：2021 年 12 月 17 日
地點：內政部警政署刑事警察局科技大樓 13 樓

主持人

中華警政研究學會 林德華理事長

刑事局黃局長，在場各位與會的專家學者及刑事局團隊同仁大家好，今天非常榮幸受刑事警察局邀請一起來探討「阻斷不法詐欺網站之法制探討」的議題。前陣子，打擊詐欺犯罪中心林淵城主任提到在阻斷不法詐欺網站時面臨法律執行面的問題，希望本會予以協助，經由本會章副理事長及許秘書長實地瞭解後，認為此問題並非僅是偵查法制面的問題，同時亦涉及犯罪預防及其他相關層面的問題。

台灣近幾年來詐騙犯罪手法不斷翻新，新興的網路科技犯罪亦產生很多新的問題，因此，防制詐騙犯罪面臨嚴重挑戰，要解決這些問題，非僅單靠法制層面可解決，事實上警察必須依法行事，不可超越法律授權範圍，否則即如「毒樹果理論」，使取得之證據失去其效力。

過去防制電信網路詐騙犯罪包括法制面、管理面、金融面、電信面、網路面、偵查面與預防面等幾個面向，在網路方面，過去一直沒有主管機關，NCC主管電信卻不願多管網路，直至民國106年12月才將TWNIC納入NCC管轄範圍。而在刑事偵查方面，亦必須將偵查技術、偵查方法、偵查能量等與時俱進，有效拓展出來。

在預防層面，自民國93年成立「165反詐騙諮詢專線」，從過去僅受理民眾諮詢服務，到後來整合電信、金融與網路資源，建立「165反詐騙系統平台」，將詐欺類案件資料統合彙整，除了提供給外勤偵查機關外，還提供給NCC或電信業者進行阻斷的工作。遇有是類困難複雜的問題，亦可不斷地透過跨部會平台會議及聯防機制，共謀解決之道。

今天本會特別邀請與談來賓有檢察司林錦村司長、士林地方法院蔡志宏法官、觀晰科技法律事務所王捷拓律師、國安局郭崇信前副局長。郭前副局長是國內打擊電信及網路科技犯罪的頂尖高手，與會各位專家學者在防制犯罪領域亦各有專擅，相信大家一定能提供許多專業意見。藉由本次會議希望從法制面加以深入探討，借重在座各位的寶貴意見，希望能提供阻斷不法詐欺網站有效的策略性建議，謝謝大家。

與會長官致詞

刑事警察局 黃嘉祿局長

非常感謝中華警政研究學會林理事長出錢出力主辦本次論壇，本局林淵城警政監亦盡心安排本次會議，也感謝郭前副局長及各位教授蒞臨指導。自調任至刑事警察局開始，我發現

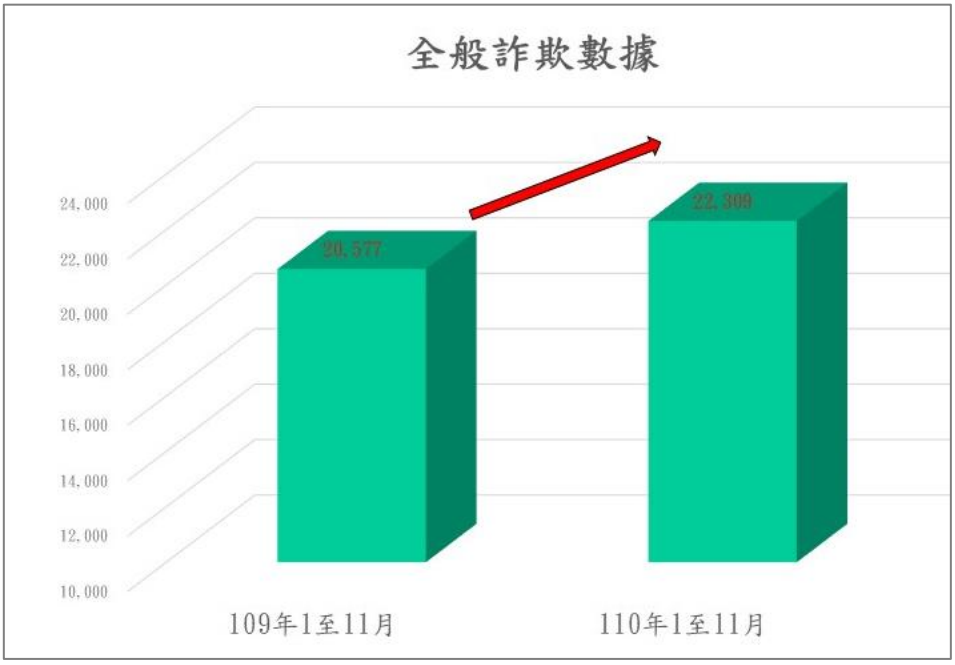
假投資詐騙的情形十分嚴重，因此本人認為應及時阻斷，故以行政先行地方式，依電信管理法要求電信業者先行阻斷。然而查詢所有法律後，發現能夠支持我們阻斷作為之方式鮮少，所以我們先於 165 被害端阻斷後，再於被害端進行資料解析，委託金管會替我們背書，再透過 TWNIC 及電信業者進行阻斷。但是在有些方面卻無法可管，因為僅於牽涉洗錢防制法、資恐防制法時，金管會才會涉入，所以在尾端封阻仍力有未逮，打擊成效不彰。郭前副局長認為可從源頭加以處理，我也要求李副局長找專家組成資通訊的諮詢專責小組協助處理相關問題，因此十分感謝林理事長及本次與會之專家學者的協助，再次代表刑事局感謝大家。

引言人

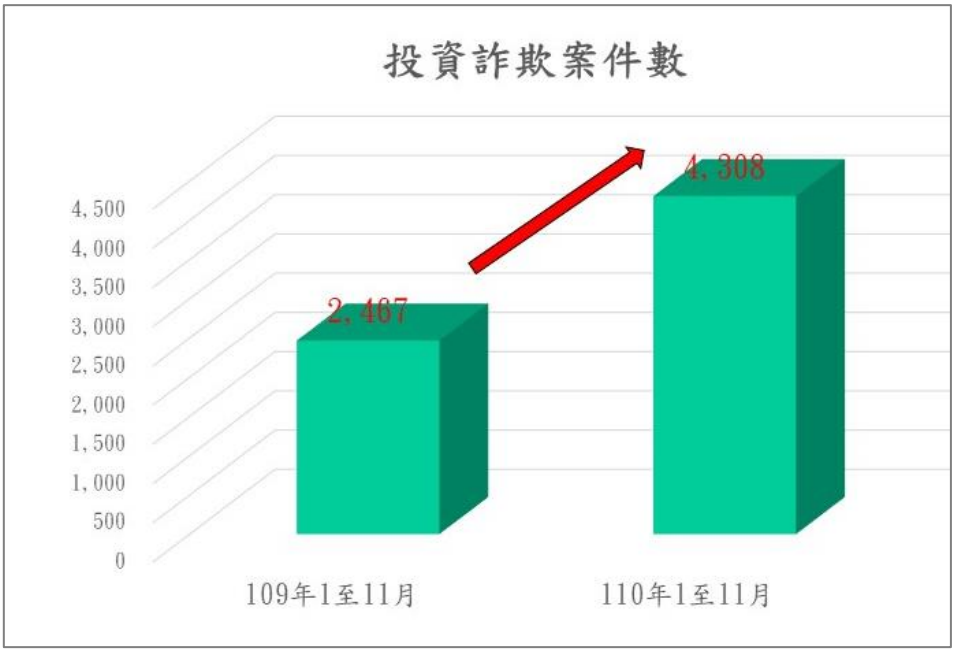
刑事警察局 蔡坤益大隊長

壹、全般詐欺及投資詐欺案件概況

110 年 1 至 11 月全般詐欺計 22,309 件，較去年同期 20,577 件增加 1,732 件。

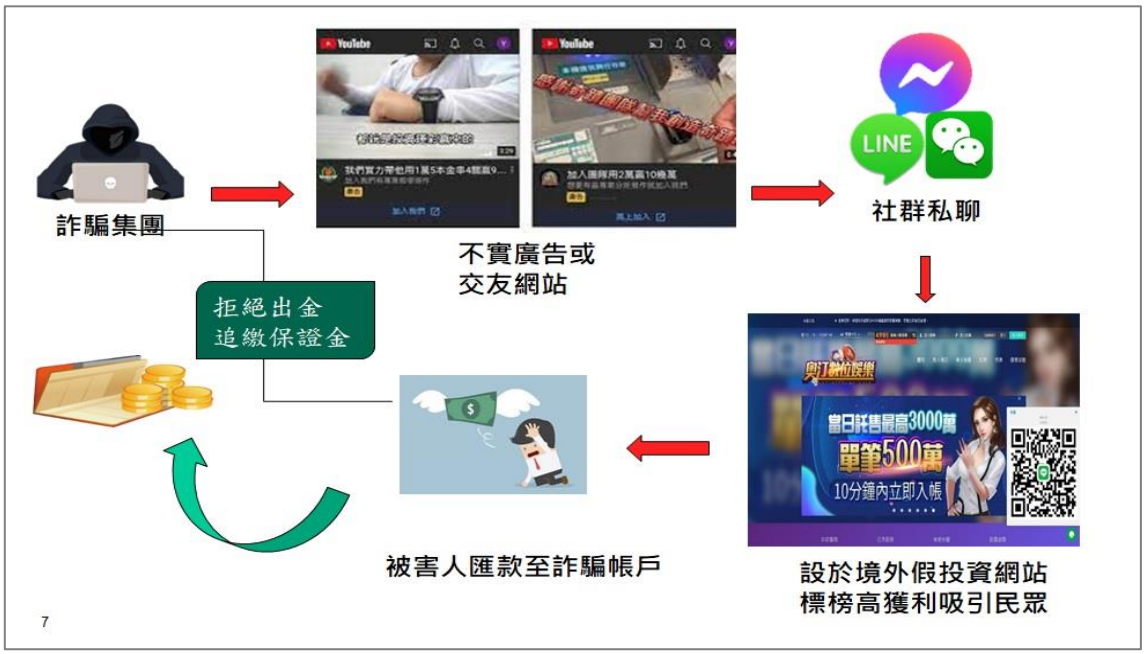


110 年 1 至 11 月投資詐欺計 4,308 件，較去年同期 2,467 件增加 1,841 件，超過全般詐欺增加幅度。



貳、犯罪模式與偵查困境

一、投資詐欺犯罪模式：投資詐欺犯罪模式，詐騙集團會先以廣告或交友軟體找尋被害人，加入社群軟體私聊，表示於某投資網站取得高報酬獲利，並將該網站(平臺)連結提供被害人，被害人信任後，投資大量資金至要出金時，詐騙集團會以各種理由拒絕，被害人此時才發現遭詐騙。



二、投資詐欺偵查困境

(一)假投資網站設於境外：

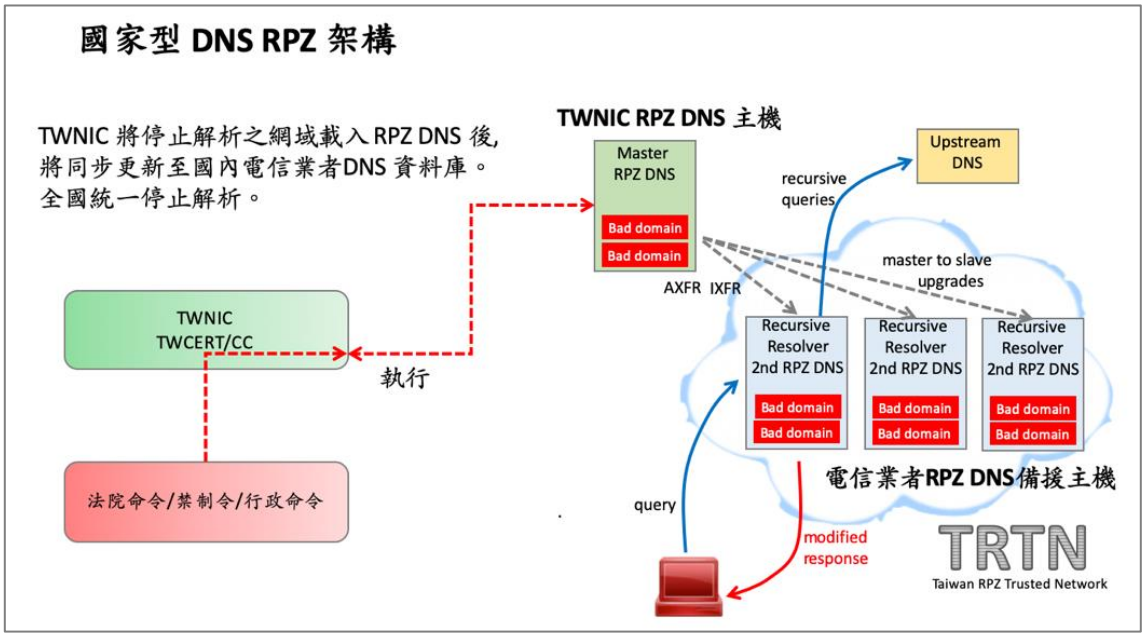
1、 詐欺集團為避免警方查緝，將假投資網站設於境外。

2、架設於境外網站資料調取不易，如發文至美商網域註冊公司 godaddy，因資料調取不易，通常無法獲得回應，無法進行追緝。

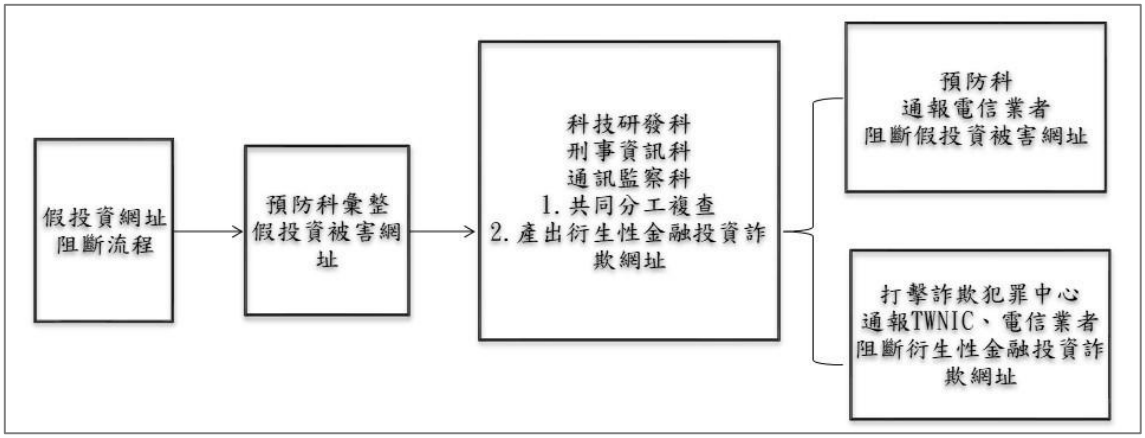
(二)製造詐騙金流斷點: 詐欺集團利用人頭帳戶或第三方支付收取詐騙款項，再利用虛擬貨幣或地下匯兌方式匯至境外，難以溯源集團核心，且如要求其下架亦會遭遇諸多困難，因此應當思考既然難以將該等網站下架，是否應以另一種方式由本局設法使我國民眾難以登入該網站，以預防被害發生，因而須推動境外不法網站停止解析。

參、推動境外不法網站停止解析

一、停止解析簡介: 隨著網際網路的擴展，網路犯罪與網路安全日益惡化。TWNIC 整合國內網路關鍵基礎設施提供者(ISP)建構 DNS RPZ (Response Policy Zone, 以下簡稱 RPZ)，RPZ 可限制境內外惡意網域名稱或 IP 位址接取，可作為資安防護的第一線防衛措施。該中心已與各電信業者更新 DNS 資料庫，可依據法院命令或行政命令，全國統一停止解析網址。



二、刑事局阻斷假投資網址流程:為預防民眾持續受害，本局訂有阻斷假投資網址流程，由預防科 165 彙整假投資被害網址，提供科技研發科、刑事資訊科、通訊監察科共同複查，並經由交叉比對後產出衍生性金融投資詐欺網址進行雙重保護，復由預防科及打詐中心通報電信業者阻斷(依據電信管理法第 8 條第 2 項「電信事業無正當理由，不得拒絕電信服務之請求及通信傳遞」)，此機制相較原有機制更為有效。為何會採



取此一動作，主要是目前實務運作上以電信管理法第 8 條第 2 項之反向解釋、警察職權行使法第 28 條及行政執行法第 36 條加以處理。

三、假投資網站特徵: 假投資網站特徵判斷，有被害人報案，相關詐騙網址會出現一個網站數個網址、數個網站共同版面、網站以假亂真等情形。

肆、停止解析(阻斷)之法律依據探討

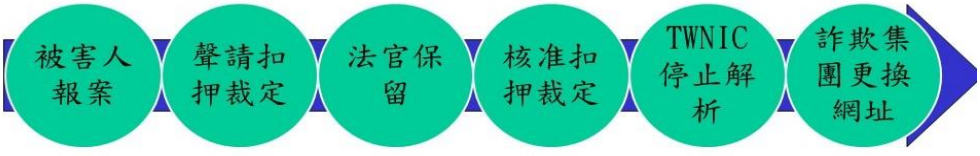
一、社會問題與法律規範:當我們進行網站封阻時，仍然必須考慮適合法之問題，首先要釐清先出現社會問題或法律規範，一般而言會先出現問題，經由社會討論進行立法規範，再由執法機關依法處置。

二、面對問題之態度:身為一名公務人員，我們大可說因為沒有規範所以我們就無所作為，但以警察防止民眾被害的目的，我們必須以更積極的態度來面對此問題，因此在現有法令無法找出絕對相應之法條時，想要解決一個新問題，就必須在現有的法令中，研究一條可以暫行適用的法條，暫時性處理這一新的問題，又不致有違反法令的風險。

三、刑事法令流程

(一)詐欺集團可隨時更換網址，緩不濟急:依據刑事法令流程，自被害人報案至核准扣押裁定，通報 TWNIC 停止解析，須耗費一段時間，且詐欺集團可能已經更換網址，無法及時防止民眾被害，且自被害人報案到停止解析須耗時至少一個星期，但詐欺集團申請一個網址的轉換可能只須一個小時，因此即便刑事法令上以扣押裁定的方式可行，然事實上卻窒礙難行。

(二)詐欺網址數量龐大:詐欺網域數量相當大(假投資案件單月被害+衍生性可達 3000

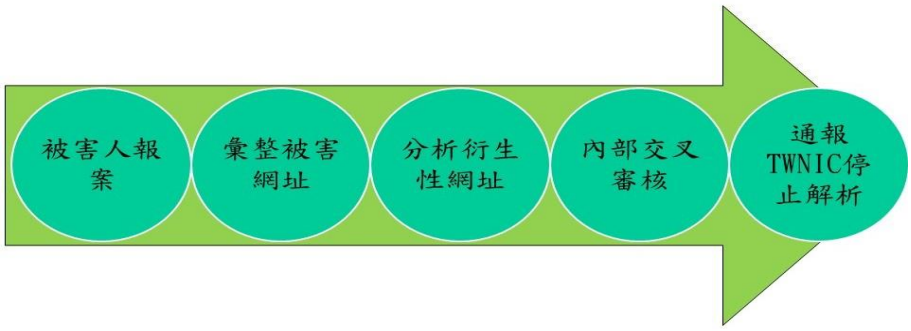


筆網址)，司法單位無法以統案處理，如果要運用司法資源逐案聲請扣押裁定，司法單位恐無法負荷。

四、行政法令流程

(一)由行政機關即時處置，預防民眾持續被害:目前本局從被害人報告到彙整被害網址、分析衍生性網站，並在內控方面做內部交叉審核，最後通報 TWNIC 停止解析或 ISP 業者加以阻斷，整個流程僅耗時半天，甚至更快。

(二)由行政機關全面性規劃處理，避免個案式處理浪費司法資源。



五、臨時性可適用之行政法令

(一)電信管理法第 8 條第 2 項: 電信事業無正當理由，不得拒絕電信服務之請求及通信傳遞。目前本局阻斷網站的依據是以電信管理法第 8 條第 2 項反面解釋(有正當理由如預防犯罪、有犯罪之虞即可拒絕)，協請電信業者協助阻斷詐欺網站。

(二)警察職權行使法第 28 條: 警察為制止或排除現行危害公共安全、公共秩序或個人生命、身體、自由、名譽或財產之行為或事實狀況，得行使本法規定之職權或採取其他必要之措施。警察依前項規定，行使職權或採取措施，以其他機關就該危害無法或不能即時制止或排除者為限。警察職權行使法第 28 條即時強制規定，阻斷詐欺網站可視為避免人民財產損失所採取的必要措施，且其他機關就該危害無法或不能即時制止或排除。

(三)行政執行法第 36 條:行政機關為阻止犯罪、危害之發生或避免急迫危險，而有即時處置之必要時，得為即時強制。阻斷詐欺網站可視為阻止犯罪、危害之發生或避免急迫危險，而有即時處置之必要，並以依法定職權所為之必要處置。

六、長期仍應修法納管

對於阻斷不法詐欺網站上，警察為了達成其法定四大任務，仍應進行積極措施，故而為阻斷詐欺網站，長期仍應修法納管，例如定於數位通訊傳播法(草案由 NCC 處理中)，明確賦予行政機關權限，如有違法事由可據以通報 TWNIC、電信業者停止解析 。

意見交流

◎ 刑事警察局打擊詐欺犯罪中心 林淵城警政監

我們要阻斷不法詐欺網站，必須要有法院之扣押裁定始可有所作為，但如同方才引言人所述，恐緩不濟急且效果有限。今年年初有詐欺集團假冒銀行詐騙客戶，因為當時快接近過年了，如不加緊處理，行政機關及民間單位春節休息，百姓必會求助無門，所以我們馬上請電信業者將這些詐騙網址阻斷。當年從該案件之後，NCC 阻斷了大約 400 萬封的惡意簡訊。

103 年在一份 NCC 會議紀錄中有提到要求各大電信業者配合警政署對於惡意簡訊及惡意網路 IP 進行阻斷，但為何後來 TWNIC 要求必須有法院命令，這部分則是昨是今非的問題，幸好本局黃局長有發現此問題，以行政先行之方式加以阻斷，才能達到阻斷不法詐欺網站之效。

◎ 刑事警察局 李文章副局長

剛才引言人已將問題帶出，我在此提出幾個問題:

一、網路詐騙從目前趨勢來看，未來一定是電信詐騙的主要類型，為何民眾容易遭假投資網站詐騙？雖然現今民眾對於假檢警、猜猜我是誰及解除分期付款等詐騙類型已有一定的辨別能力，但在假投資網站方面，民眾卻無招架之力，乃因這些假投資網站會散發惡意網址，當點擊進入後就會連結到LINE，並由理財專員進行誘導詐騙，因此假投資網站詐騙在未來是我們經常會遇到的問題。

二、目前要求透過法院扣押裁定之方式才能進行阻斷，此法緩不濟急，因此希望透過在座專家、學者找出可授權給我們進行阻斷不法詐欺網站工作的法源，如果沒有，再來考慮以修法的方式解決。

◎ 刑事警察局 黃嘉祿局長

NCC 只管電信卻不管網路，我曾拜訪過 NCC 主委，並將本局目前的做法告訴他們。「數位發展部」明年即將成立，屆時將會制定相關法律。科技發展很快，法令制定很慢，我們也不得不以行政先行之方式來解決問題。

◎ 中華警政研究學會 林德華理事長

剛才引言簡報中有提到，可依據法院命令、禁制令或行政命令去停止解析網址；惟各單位的執法必須精準，以免成為被攻擊的弱點。詐騙犯罪之防治不外乎預防、查緝與偵審等三個層面，而在電信網路方面，目前主要是透過 TWNIC 協助。記得過去跨部會平台會議與各電信事業單位聯防機制成效做得不錯，103 年 6 月 19 日 NCC 召開的會議有完整明確的紀錄，或許可供刑事局參考。當時詐騙犯罪遠端操控小額付費案件突增，除立法院召開專案公聽會外，總統府亦召開專案會議，由我提報標本兼治的防制策略。在治本方面，建構跨部會及各電信單位聯防機制，在治標方面，即時啓動兩岸共打機制，邀請大陸公安部網路局派員共組 0609 專案，標本兼治後使該類詐欺案件從當時高達數千件立即逐漸消失。因此我認為警察在此方面應當要更積極處理，方才引言人蔡大隊長有提到須依賴修法，但修法工作恐緩不濟急，故在此提供過去的經驗讓大家參考。

與談人

臺灣士林地方法院 蔡志宏法官

本議題我已追蹤許久，因為我的博士論文寫的正是網路治理，而 TWNIC 的執行長當時即是我的口試委員，所以我很能理解要阻斷域名解析在資訊技術社群可能遭遇到困難。美國商會已經連續六、七年在白皮書裡指責台灣的盜版侵權完全沒辦法處理，只是網路盜版侵權通常侵犯的是內容業者的權利，而這些業者通常至少還有些財力，而我們今天面對的詐欺網站受害者通常都為市井小民，因此問題就變得更為迫切。在此和大家說明為何 TWNIC 會要求如此嚴格而置警方命令於不顧，因為整個網際網路是從美國開始發展，而一開始是由私部門來領導，此與科技發展有關，因為美國對於自由與財產均採取令狀保護主義，因此若沒有令狀就容易被被冠上網路白色恐怖的汙名，除此之外，對網路治理而言，域名及網路 IP 具有單一識別符的效果，這樣資訊流才能夠在全球互通，而各個國家採取各自停止解析的結果，將導致同個域名在 A 國可以解析接取，但在 B 國卻無法解析接取，此舉將壞破全球單一識別符的基礎，而 TWNIC 成員大多具有網路技術專業背景，因此對此有較強的理念堅持，從而若各行政機關沒有令狀時，他們多半採取較抗拒之態度，因此我一直認為須採取刑事司法解決此問題。在網路治理上，我認為網路治理本應當尊重各國主權的發展，且公共政策是屬於各國主權的範圍，不能因為私部門領導，就置公共利益於不顧，所以於必要時，各國自可以採取相關維護公共利益的措施，只是應當思考如何以公私協力使網際網路的發展更為周延，因此我提出的解決方案仍以刑事強制措施為主，至於在行政手段方面，若 NCC 或 TWNIC 願意支持我們也十分樂見，只是我們可以想見未來人民權利意識高漲，且剛才理事長所提的精準執法，也可能遭到困難，例如：許多詐欺犯可能因其網站遭阻斷而向警察誆報案件以資報復，從而混淆警方視聽以致難以精準執法，因此我認為以刑事扣押、沒收仍為最好的方式。

壹、採取刑事強制處分之適法優越性

一、警察及電信業者：如果警察和電信業者能夠形成共識，確實能夠形成無需法院介入的迅速有效機制，因為電信法第 8 條第 2 項規定：以提供妨害公共秩序及善良風俗之電信內容為營業者，電信事業得停止其使用及電信管理法第 8 條第 2 項規定：電信事業無正當理由，不得拒絕電信服務之請求及通信傳遞。依上述規定，電信業者傾向提供資料，原因是業務使然及擔心如未提供該等資料可能反向使自身被告。不過，電信業法規定傳遞的內容一律由使用人自行負責，電信業者無須負責，似乎應該存在可以合理限縮的空間。例如：如果電信業者明知內容確實會造成他人損害且警方亦已提供相當證據或存證信函，難道法官會認為說所有因通信傳遞所發生的損害，電信業者都不用負責任嗎?固然我們無法苛責電信業者在一開始提供服務時就知道傳遞的內容為何，但如果長期間傳遞有問題的爭議內容，透過檢警函告、甚至法院裁判認定都已經可以知道是違法內容，電信業者難道還要繼續提供服務及傳遞嗎?只不過，因目前實務上，告電信業者的案例好像還沒有一件勝訴的，也無怪乎電信業者仍然傾向提供解析、服務。

二、回想警示帳戶機制之相關問題:早期警示帳戶沒有法律依據因此容易產生爭議，後來在銀行法第 45 條之 2 第 2 項有明確之授權規定，金管會亦訂定相關規定即「銀行對疑似不法或顯屬異常交易之存款帳戶管理辦法」，用來強化凍結警示帳戶之規範密度。目前對於違法網站的扣押及停止解析上仍沒有相關辦法，因此我擔心將來如果誤判所衍生的損害賠償責任，屆時唯一可能免責的，恐怕只剩下法院而已。因此現階段，透過法院依照證據及既有法定程序所為之扣押裁定、沒收判決相較之下，是風險

較低的作法，雖然在程序上比較麻煩，但可免於日後遭致反向訴訟的危險

貳、域名沒收之具體操作流程

刑法第 38 條第 2 項規定：供犯罪所用之物，屬於犯罪行為人者，得沒收之。目前高檢署已成立相關研究小組，期望能推動域名的沒收扣押，但在其相關論述中，對於域名沒收屬於犯罪所得沒收還是供犯罪所用之物沒收；域名扣押是可為證據之物扣押，還是得沒收物之物扣押似乎沒有完整的看法說明。我個人則將其定調為供犯罪所用的沒收，亦即犯罪工具的沒收，同時也就是得沒收物之扣押。故依刑法第 40 條第 3 項：刑法第 38 條第 2 項之物，因事實上或法律上原因未能追訴犯罪行為人之犯罪或判決有罪者，得單獨宣告沒收。刑訴法第 455 條之 34：單獨宣告沒收由檢察官聲請違法行為地之法院裁定之。刑訴法第 455 條之 35：檢察官聲請單獨宣告沒收應以書狀提出於管轄法院，其中應記載之應沒收財產所有人不明時，得不予記載。域名註冊人就沒收其域名事項，準用被告訴訟上權利，故可抗告救濟（刑訴法 455 條之 37 準用同條之 19、同條之 28、第 403 條）。

參、域名扣押之具體操作流程

刑訴法 133 條第 1 項：得沒收之物，得扣押之。即使因為事實上難以執行，我們仍應設法將之沒收、扣押，不能因為難以沒收就不沒收，應先沒收後，再與國外進行商議，而此部分尚須透過網路治理與社群的努力，而在沒收之前，可透過停止解析之方式將之扣押。同條之 1 第 1 項：非附隨於搜索之得沒收物扣押，應經法官裁定（對物強制之令狀主義）。域名屬非附隨於搜索之扣押，因此須遵守令狀主義，而扣押最主要的作用在於剝奪其使用、收益。域名唯一使用收益之權能就在於提供網路上連通指向的功能，如果此功能於我國境內遭扣押，就等同於域名遭到扣押。我認為這部分須進行有意識的司法數位轉型解釋。舉例而言，刑法有處罰供給賭博場所之規定，而在網路空間提供賭博場所，可否構成該罪呢？我國最高法院即認同法條所規定的場所包括在網路空間所虛擬存在的場所。因此當域名成為犯罪工具時，將域名沒收、扣押，也應該存在可以合理解釋的空間，而不至於無法處理。目前無法處理原因，可能只是因為案件未進到法院內，從而法院根本無表示之機會。

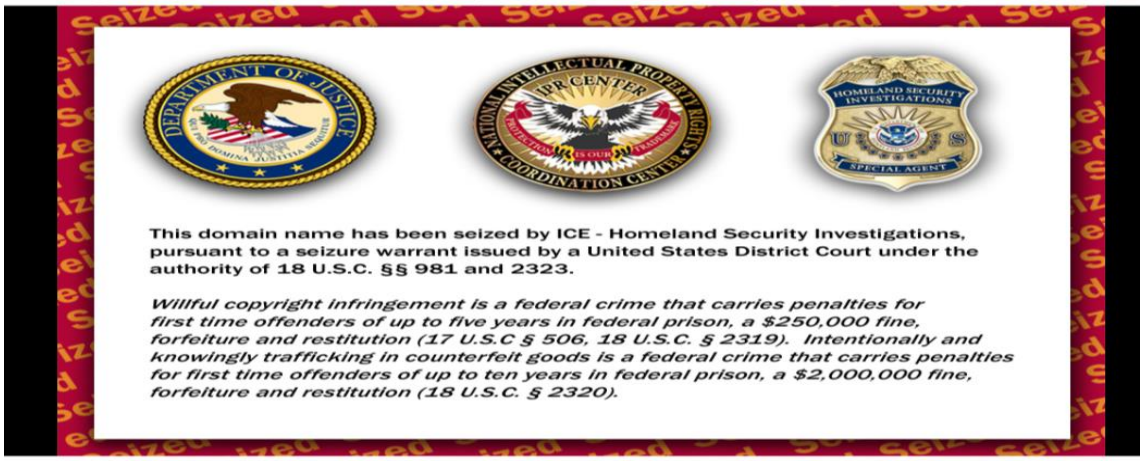
以 DNS RPZ 技術進行域名境內扣押時，不存在提出及收受過程及作動，無需勉強適用同法第 139 條第 1 項制作收據、詳記扣押物名目及付與所有人、持有人、保管人之規定。

同條第 2 項、第 145 條之封緘、蓋印、提示等公示規定，亦均無需勉強適用，但可強制導流至特定執法宣示網頁以符合公示原則。另在救濟方面，域名註冊人可依刑訴法第 404 條第 1 項但書第 2 款救濟。

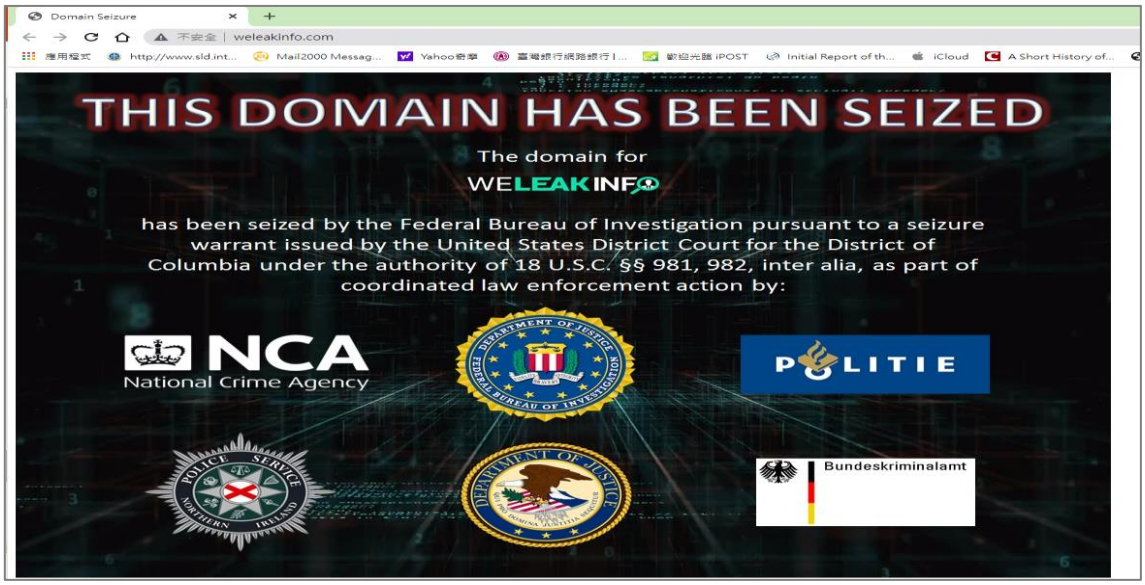
肆、域名沒收及扣押之案例簡介

一、瑞典知名盜版網站之域名沒收

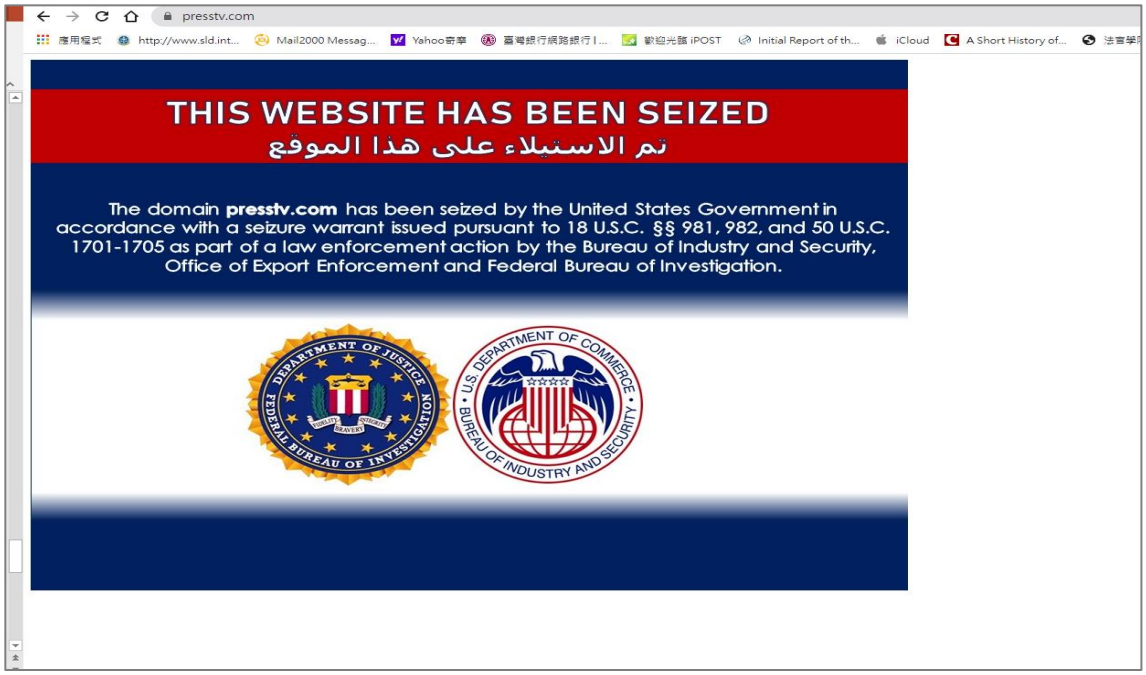
二、美國早期進行的 Operation Seize 行動



三、美國與多國合作進行域名的扣押

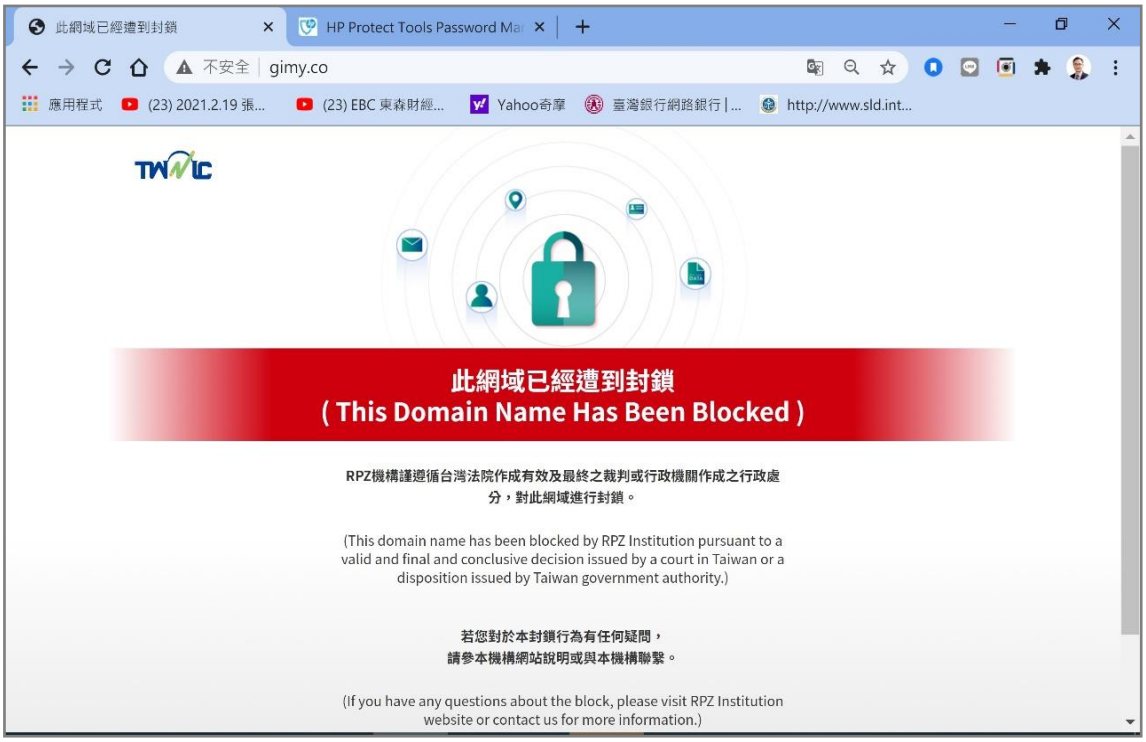


四、針對外國使用者進行詐扣押時以外文書寫(阿拉伯文)



五、開大門、走大路:扣押即應公告周知

六、TWNIC 協助 RPZ 之解析: 透過 TWNIC 協助 RPZ 禁止解析，即便犯嫌不配合提供帳號、密碼，同樣能夠進行扣押，雖然熟悉網路技術的專家還是可以利用境外解析服務來連接違法網站，而無法透過 RPZ 禁止解析，百分之百地禁絕違法網站之接取，但以整個數位轉型的執法而言，能夠有百分之八、九十的效果，即可認為已經達到扣押之目的。



國家安全局 郭崇信前副局長

一、首先，我針對剛才蔡坤益大隊長的簡報做補充說明(如下圖)，假投資網站的特徵有諸多網址對應到相同的 IP 位置，如果以 RPZ 進行解析，其作法是將網址傳送給 DNS，DNS 再回給 IP 後方進行連線。另外對於確定已違法且被禁止的網址，若發現還有人連線，表示有人還想進行投資，應該加以追查主動提醒。而在法律適用面上，應確定所適用的法律應用哪一條。我之前提過 2016、2018 年決戰假訊息，2024 年決戰假視訊，在決戰假訊息方面，發想於當時美國大選假訊息問題嚴重，在假視訊方面，則因擬真技術的發展成熟，因而認為這是我們未來所需面對的問題。

二、詐騙網站犯罪成本過低難以一一阻斷，刑事警察局應以擒賊先擒王將源頭斬斷的思維來辦案，目前我國網路源頭主要有三個:淡水、頭城、枋寮，如果我們能在源頭著手處理，則可將問題解決。

三、以通保法為例，如果不需看到信件裡面的內容則不受通保法限制，更何況虛擬世界裡面的 IP，只要透過先進科技即可解析 3500 多種通訊協定，只要可找出端點而不涉及內容即無法律限制的問題。在應用場景上可找到被駭客入侵的主機，另外在殭屍網路 DDOS 的攻擊，即分散式阻斷式攻擊歸納出的結果為案發前一、兩天可找出 DDOS 攻擊域名情報。且應成立威脅情報資料庫，反向追蹤到駭客主機入侵及未來可能攻擊的目標。

四、應結合檢調專業智慧創造人工智慧。

五、在找到主機 IP 後結合新設備可找出木馬程式，最後再運用結合軟體定義網路即可將所

有犯嫌自動導入刑事警察局的系統，此外，此作法也沒有法律問題，因為此法僅抓取metadata，所謂 metadata 是指網路封包頭的資訊，就像郵差寄信需要知道地址一般，因此不受法律限制。現今不法技術包含惡意軟體、殭屍網站、釣魚網站、DDOS、垃圾郵件，如果要朝此方向努力，未來應該加入人工智慧，例如以 AI 偵測金融信貸詐騙，如同申請信貸時會有原始評分可瞭解申請人的信用度，如同在刷信用卡時即會自動監控是否在一段時間內有多次刷卡紀錄以判定卡片是否遭盜用，另外，應該開闢國際合作，例如 gogaddy 將網址置於美國，我國應可將法院文件傳送該國告知其為違法，請美國提供申請網址等個資以利辦案，另犯罪因為網址在國家間會進行多重轉換，所以應該加強國際合作。

法務部檢察司 林錦村司長

壹、根據 2021 年 11 月 30 日媒體報導，英國線上詐欺廣告已經成為詐欺犯罪主要來源。受害人士和團體提出呼籲，將網路詐欺廣告納入政府規畫的線上安全法案的內容。網路詐欺通常是透過廣告、假冒的網站或電子郵件，來騙取用戶資訊，例如假冒某銀行的通知email，請用戶重新填寫個人資訊。又根據銀行團體UK Finance 的數據顯示，英國在今年首6個月的線上詐欺金額高達7.54億英鎊(約10億美元)，較前一年同期增加了30%，較2017年同期則增加了60%。因此英國金融服務部長John Glen對國會議員表示，政府願意透過立法來阻止網路詐騙廣告的爆炸性增長[1]。

貳、本部阻斷不法詐欺網站之因應作為有三：

一、推動通保法修法及科技偵查法制化，提升偵查能量：近來常見不法網站以違法網站或一頁式廣告進行詐騙、違法吸金或誘騙民眾加入線上博奕，其犯罪手法涉及網路甚至是境外IP，隱密性高且匿蹤迅速，執法機關溯源追查之困難度極大，有無必要在通訊保障及監察法增訂調取「網路流量紀錄」(NetFlow Log)條款，課予業者保存嫌疑人網路連線相關紀錄之義務，並比照調取通信紀錄之程序，使執法機關可以調取網路流量紀錄予以分析，以利溯源追查。另外本部也將持續推動科技偵查法制化，並引入「設備端通訊監察」，賦予偵查機關更多追查網路犯罪之工具。

二、善用扣押裁定及執行DNS RPZ停止解析機制：

（一）財團法人台灣網路資訊中心（TWNIC）提供之DNS RPZ （Response Policy Zone，回應政策區域）機制，亦可稱為「DNS 防火牆」，可藉由將非法網站停止解析之方式，將非法網站封鎖，使網路使用者無法再自國內連線造訪該非法或惡意網站。

（二）扣押裁定：

1. 依照刑事訴訟法第 133 條第 1 項，不法網站之域名，應屬得為證據及得為沒收之物，因此得扣押，現階段已有案例係法院以裁定准予扣押域名，之後即由 TWNIC 來執行「停止解析」機制，避免再有國內民眾造訪非法網站而進一步受害。
2. 「停止解析」較屬損害控制概念，因針對境外域名，停止解析機制僅能達到阻絕自

[1] https://www.chinatimes.com/realtimenews/20211130003513-260410?chdtv(最後瀏覽日期 2021 年 12 月 17 日。

國內民眾連線至該網頁之效果，卻無法將該網域之支配、處分權交予公部門或納於我國公權力下（因域名註冊在國外），若國內民眾或犯罪行為人使用「跳板」等連線方式，仍可能規避 DNS RPZ 機制而再造訪該涉案網站，此與刑事訴訟法上扣押的概念並未完全相合。然在現行法制下，扣押裁定程序仍是較為可行的作法。

3. 檢察機關是否研擬扣押裁定執行 DNS RPZ 機制的計畫，包括實施策略、聲請法院對其域名為扣押裁定之聲請書類、抗告書（駁回時）及研議法律見解等。

三、跨境司法互助：國內使用停止解析的機制將損害先控制住，另一方面同時聲請國際司法互助，取得註冊於國外之違法網站帳號、密碼之支配權，甚至是扣押其伺服器及其內的電磁紀錄，始能完全達到扣押及打擊犯罪溯源之目的。

四、強化新型態洗錢工具之監管及刑事處罰：鑑於新興洗錢犯罪手法係利用虛擬通貨平台、第三方支付作為新型態洗錢工具，亦為網路詐騙犯罪者常見之洗錢手法。就洗錢防制法部分所採之因應措施：(一)107 年 10 月將虛擬通貨平台及交易事業納入洗錢防制範疇，又「虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法」自 110 年 7 月 1 日開始施行。(二)第三方支付服務業經行政院於 110 年 8 月 18 日指定為洗錢防制法第 5 條第 3 項第 5 款之非金融事業或人員。(三)本部除持續與金融監督管理委員會及經濟部通力合作，針對虛擬通貨平台與交易事業及第三方支付業者強化洗錢防制監管外，本部並已著手推動洗錢防制法之修法，研議增訂利用虛擬通貨平台、第三方支付工具為洗錢犯罪之刑事處罰，切斷網路詐欺不法分子之洗錢管道，從切斷金流之方式著手，遏止詐騙亂象。

參、結語：

一、法律及時修法，以適時提供執法人員相應之查緝法律依據。

二、執法人員精進專業及善用科技，俾利提昇能量。

三、執法與業者協力，業者基於社會責任，透過公私協力遏阻犯罪。

四、國際及兩岸司法互助，因網路犯罪有跨境化、組織化、科技化之趨勢，因此透過跨境共同打擊犯罪及司法互助始能竟其功。

五、查緝案件網斷金流，以遏阻犯罪者享受不法經濟利益，阻斷其經濟誘因。

玄奘大學 蔡震榮主任

德國在疫情前為了對抗恐怖活動，授權聯邦刑事警察局採取一些秘密蒐集恐怖組織之電信活動，以及即早發現恐怖活動，對其採取防禦措施，其可區分犯罪預防與刑事偵查，尤其在犯罪預防上授予警察機關更大之裁量權。

壹、德國聯邦刑事局法之規定

一、刑事追訴自我保護

聯邦刑事警察局人員出於刑事訴訟的原因，在聯邦刑事警察局的職權範圍內，於關係人不知情的情況下，為避免對其生命、肢體或自由造成危險的情況下，聯邦刑警局的人員可以利用科技方式，對公寓內外不公開的言論進行收聽、錄音，並進行拍照和錄音。

如果在措施實施過程中有實際跡象表明私人生活的核心領域受到影響，則必須在不危

及受託人的情況下盡快中斷措施。

如果有跡象顯示，僅屬來自私人生活核心領域的某種措施，則該措施錄製是不可為之的，屬於涉及私人生活核心領域的事件，記錄將立即刪除。

二、犯罪預防:由於恐怖活動一發生，即會造成重大傷亡，因此，在預防犯罪上給予警察更寬廣之手段:

(一)要求電信業提供通訊資訊:聯邦刑事警察辦公室可以根據《電信法》相關規定，在下列情形下要求業者提供通訊數據的信息，以避免危險或在個別情況下，某人將在可預見的時間內至少以具體方式實施。根據《電信電信媒體數據保護》第 2 節第 2 款第 2 項的規定，可要求電信業者提供有關嫌疑犯或他人儲存數據的信息。僅可要求提供信息，係在為避免對一個人的生命、肢體、自由或性自決造成特定危險或為了聯邦政府的存在或者一個國家以及公眾的商品，其威脅是人民生存的基礎，可以侵入這些終端設備中使用的存儲設施。

(二)侵入個人資訊系統:如在個人的身體、生命或自由或威脅影響聯邦政府或州的基礎或存在或人類生存基礎下，上述事實證明在可預見的時間段內，至少具體方式發生的可能性，或在可預見的時間內具體發生之可能性。

(三)電訊監控:聯邦刑事警察辦公室可以在當事人不知情的情況下監控和記錄某人的電訊:

1. 根據《聯邦警察法》第 17 條或第 18 條的規定，維護聯邦政府或州的存在或安全或個人或重要事物的生命、肢體或自由造成緊急危險價值公共利益，有必要的情形下。
2. 該事實證明他們將在可預見的時間內以具體方式實施刑事犯罪，
3. 在可預見的時間內犯下刑事犯罪的特定可能性是合理的，
4. 收集電信流量數據和使用數據

(四)聯邦刑事警察局可以在相關人員不知情的情況下收集交通數據（《電信-電信-媒體-數據保護法》第 9 條和第 12 條）:

1. 那些根據《聯邦警察法》第 17 條或第 18 條負責避免對聯邦政府或州的存在或安全，或對個人或具有重要價值的財產的生命、肢體或自由的緊急危險的人之公共利益。
2. 某些事實證明可預見的時間內至少以具體方式實施刑事犯罪的假設是合理的。
3. 證明其在可預見的時間內有可能實施刑事犯罪的具體可能性是合理的，某些事實證明他們將根據第 1 條正在為某人接收或傳遞某些通信，或源自他們的通信的假設。
4. 某些事實證明根據，嫌犯將使用他們的電信連接或終端設備的人。

(五)手機卡和終端的識別和定位:聯邦刑事警察辦公室可以根據第 51 條第 1 款的條件下，透過資訊比對，取得下列資訊：

1. 手機設備號和所用卡的卡號，以及終端的位置。
2. 在無法避免情形下得蒐集他人之資訊，但必須在目的達成後，立即將其刪除。

貳、問題導向

立法政策應由需用機關提出，刑事局在電信監偵察上發現哪些問題，可透過立法方式解決，提供出來，作為解決方案。

開南大學 鄭善印教授

一、問題點：詐欺網站設在境外，但在國內引誘被害人上鉤，當警方查知時，有何法律依據可以阻斷這類詐欺網站？

經由引言人報告得知，所涉案例應分成「偵查犯罪」及「預防犯罪」兩種模式分析。

二、警察偵查犯罪模式

若有被害人報案，該網站即成為嫌疑工具，當然可以成為偵查對象，只是對於網站之搜索或扣押應該都難以如同實體物般容易，同時聲請搜索扣押之通過率僅七成。因此警察人員才會運用電信管理法第 8 條第 2 項：「電信事業無正當理由，不得拒絕電信服務之請求及通信傳遞」規定之反面解釋，亦即因「有正當理由，故得拒絕電信服務之請求及通信傳遞」，而請求電信總局予以阻斷通訊，避免下一個被害人。這種迂迴方法與搜索扣押網站之功能相同，只不過少了一個法院的認證而已。這種方法也不是要積極偵辦網站詐欺犯罪，但鑑於這種網站的 IP 位址都設於境外，在國內無法積極偵辦也是實情。

此外，另有一說認為，可以利用檢察機關搜索扣押不必法官裁定之管道，亦即「檢察機關實施搜索扣押應行注意事項」第 9 條規定：「非附隨於搜索之扣押，其標的屬得為證據之物，且非兼具犯罪物或犯罪所得性質者，得逕行為之，免經法官裁定」。但，我以為該規定有如以往檢察官的無票扣押方式，也就是以一紙公文就將被告不動產為不准移轉登記之扣押，我想檢察機關恐怕很難用該條規定來扣押嫌疑網站。

三、警察預防犯罪模式

若警察發現犯罪嫌疑網站生出許多幾乎相同的畫面與網址，而合理推論可能是詐欺網站主持人所衍生之網站（據說每一網址更換，費時僅 1 小時及 100 元台幣），為預防被害，其所可能適用之法律，首推警察職權行使法第 28 條之規定：「Ⅰ警察為制止或排除現行危害公共安全、公共秩序或個人生命、身體、自由、名譽或財產之行為或事實狀況，得行使本法規定之職權或採取其他必要之措施。Ⅱ警察依前項規定，行使職權或採取措施，以其他機關就該危害無法或不能即時制止或排除者為限。」。蓋以警察為預防犯罪，而該預防工具掌握在他機關手上，他機關又消極不作為或無法作為時，警察應得依上述條文要求他機關予以阻斷通訊，此即為警察補充性原則。但因上述警察的補充性，僅限於臨時性、緊急性事項，故亦只能以個案處理。但若他機關恆常無法排除該危害，則警察機關與其簽訂一抽象性、一般性之職務協助法規，應屬勢所必然，故仍可以處理這類預防事務。

此外，警察職權行使法第 21 條規定「警察對軍器、凶器或其他危險物品，為預防危害之必要，得扣留之。」，此即所謂警察即時強制。這種強制原本對個案性、緊急性事件，為預防危害，警察可以簡便行使此職權，而不生任何疑慮。但網站是否可以當成「危險物品」，亦即是否可以將虛擬之物當成實體之物，恐仍有不同意見，故引用本即時強制條文，仍有尋求堅強解釋之必要。然而，若刑事偵查時搜索扣押該網站沒有問題，亦即刑事偵查時

可以將之視為實體物，則為何在行使即時強制時會有問題？此理顯然不通。相同地，行政執行法第 38 條第 1 項有關「一般行政機關」即時強制之規定：「軍器、凶器及其他危險物，為預防危害之必要，得扣留之。」，亦有與警察職權行使法第 21 條相同之問題。

四、我以為，警察機關執法最喜歡有一個可以適用的法規，再依據既定的 SOP 一一進行，而不必顧慮到其他機關中間的制肘，如此才能專心辦案。因此訂定一個可以適用的法規，而不必事事請示他機關，可能是警察最希望得到的結果了。因此，我以為警察也許可以朝以下兩個方向發展。

(一)在偵查犯罪時，固然以得有法院搜索扣押的認證為上策，但若法院不准或法院假日無法發票時，應可利用警察職權行使法有關即時強制之規定，先予扣留嫌疑網站，暫時不使再生下一個受害人。

倘若認為網站與有體物不同，則應可援引刑事訴訟法第 156-1 條有關數位資料得視為文書之規定，將其視為有體物。當然，嫌疑網站視為即時強制的危險物品，亦應可同意，蓋因法概念必須隨著時代而轉變。倘若認為網站難以扣押，則似可援引「檢察機關實施搜索扣押應行注意事項」第 7、8 條有關扣押方式之規定，予以張貼公告即可。

(二)在預防犯罪時，依警察職權行使法第 28 條的概括條款及補充性原則，應可用來作為訂定職務協助法規的平台。但，我以為警察自行訂定排除危害法規，不如與他機關訂立職務協助法規，蓋因警察機關並無該項工具及技術，不如與他機關合作。

例如，移民署因為無法全面查緝非法外勞，故訂定了一個「內政部入出國及移民署與警察機關協調聯繫要點」。此要點僅為行政法規，同時帶有機關權限委託及職務協助的性質。警政署是否能夠比照辦理，而與電信總局訂定類似的聯繫要點？並在要點中將警察職權行使法第 28 條要旨予以訂列明，且充分規定救濟方式。若受阻斷之人出面要求救濟，則剛好由警察機關接手處理。此方式與 165 專案警察與金融機構合作之方式類似，只不過多了一個法規而已。法規的存在，足以保障合作機關的承辦人員。

雖然如此，但警察在適用警察職權行使法的補充性原則時，仍應限於預防犯罪的領域，而不能用在偵查犯罪的領域，兩者應明確區分。是故，若能在有人報案時，依偵查犯罪程序聲請搜索扣押，一旦扣押該網站，即足讓電信總局人員相信其他衍生之網站亦屬同一主持人所有，而同意於有人受騙前予以阻斷，這樣是否較能合乎法治？

中央警察大學 蔡庭榕館長

壹、扣押問題

扣押標的，依刑事訴訟法第 133 條第 1 項之規定，係指可為證據或得沒收之物。此物之概念，應僅指有體物，但因實務見解對於扣押標的認為可包括權利（學術則多持否定看法），依此看法，對於人頭帳戶之凍結，固可依扣押規定為之。獨立扣押，原則上雖應經法官裁定（刑訴 133-1 第 1 項：「非附隨於搜索之扣押，除以得為證據之物而扣押或經受扣押標的權利人同意者外，應經法官裁定。」），但刑訴第 133-2 第 3 項亦規定「有相當理由認為情況急迫」，司法警察仍得逕行扣押。文內所指扣押裁定若係指人頭帳戶之凍結，認須逐案聲請，恐有誤會。文內所指扣押裁定若係指阻斷網站，其命「阻斷」行為，應非在「扣押」之概念範圍，扣押規定，應非命「阻斷」行為適格之授權基礎，自非適法。

參考法條：

刑事訴訟法第 133 條（扣押之客體）

〔1〕可為證據或得沒收之物，得扣押之。

〔2〕為保全追徵，必要時得酌量扣押犯罪嫌疑人、被告或第三人之財產。

〔3〕對於應扣押物之所有人、持有人或保管人，得命其提出或交付。

〔4〕扣押不動產、船舶、航空器，得以通知主管機關為扣押登記之方法為之。

〔5〕扣押債權得以發扣押命令禁止向債務人收取或為其他處分，並禁止向被告或第三人清償之方法為之。

〔6〕依本法所為之扣押，具有禁止處分之效力，不妨礙民事假扣押、假處分及終局執行之查封、扣押。

第 133 條之 2（扣押裁定之程序）

〔1〕偵查中檢察官認有聲請前條扣押裁定之必要時，應以書面記載前條第三項第一款、第二款之事項，並敘述理由，聲請該管法院裁定。

〔2〕司法警察官認有為扣押之必要時，得依前項規定報請檢察官許可後，向該管法院聲請核發扣押裁定。

檢察官、檢察事務官、司法警察官或司法警察於偵查中有相當理由認為情況急迫，有立即扣押之必要時，得逕行扣押；檢察官亦得指揮檢察事務官、司法警察官或司法警察執行。

〔3〕前項之扣押，由檢察官為之者，應於實施後三日內陳報該管法院；由檢察事務官、司法警察官或司法警察為之者，應於執行後三日內報告該管檢察署檢察官及法院。法院認為不應准許者，應於五日內撤銷之。

〔4〕第一項及第二項之聲請經駁回者，不得聲明不服。

貳、拒絕通信傳遞

電信管理法第 8 條第 2 項規定，電信事業有正當理由，雖得拒絕電信服務或通信傳遞。但正當理由之認定權限在電信事業，非司法警察可得置喙，固然實務運作或可藉由司法警察提出理由協請電信業者配合辦理，惟此一運作模式效能如何，仍待評估。

參考法條：

電信管理法第 8 條（與消費者權益相關之經營義務）【相關罰則】第二項~§76；第四項~§79；第一項~§81

〔1〕電信事業提供電信服務時，應符合下列規定：

一、以明顯公開且易於取得之方式，揭露服務條件、電信網路品質與數據流量管理方式及條件等消費資訊。

二、電信服務及非電信服務費用之帳目應明顯分立，且不得以非電信服務費用未繳交為由，停止提供電信服務。

三、對於逾期未繳交電信服務費用之用戶，應定相當期間催告，逾期仍不繳交者，始得停止提供電信服務。

四、採取適當及必要之措施，保障通信秘密。

五、確保其從業人員嚴守通信秘密。

六、提供用戶消費爭議申訴處理管道。

〔2〕電信事業無正當理由，不得拒絕電信服務之請求及通信傳遞。

〔3〕電信事業因電信網路障礙、阻斷，致電信服務發生錯誤、遲滯、中斷或不能傳遞而造成用戶損害時，其所生損害，除契約另有約定外，電信事業不負賠償責任；其所收之服務費用應予扣減。

〔4〕電信事業對下列通信應予優先處理：

一、於發生天災、事變或其他緊急情況或有發生之虞時，為預防災害、進行救助或維持秩序之通信。

二、對於陸、海、空各種交通工具之遇險求救及飛航氣象等交通安全之緊急通信。

三、為維護國家安全或公共利益，有緊急進行必要之其他通信。

叁、採行必要之警察職權措施

警察職權行使法第 28 條之規定，一般固認為此為「警察職權概括條款」之規定。惟因受制於同條第 2 項「警察補充性原則」之規定，警察任務範疇事項即無適用此一「警察職權概括條款」之餘地。警察若援引以之作為命「阻斷」行為之依據，亦非適法。

參考法條：

警察職權行使法第 28 條（行使職權或採取措施之限制）

〔1〕警察為制止或排除現行危害公共安全、公共秩序或個人生命、身體、自由、名譽或財產之行為或事實狀況，得行使本法規定之職權或採取其他必要之措施。

〔2〕警察依前項規定，行使職權或採取措施，以其他機關就該危害無法或不能即時制止或排除者為限。

肆、採行即時強制措施

行政執行法第 36 條之規定，應僅係即時強制之立法定義，並非即時強制之概括授權基礎。行政機關採行即時強制措施仍須受同條款第 2 項之限制。若僅援引第 36 條之規定作為命「阻斷」行為之依據，自非適法。其次，行政執行法第 39 條固然規定符合法定要件得限制物之使用。惟此一「物」之概念，應係指有體物，若援引以之作為命「阻斷」（無體物）行為之依據，亦非適法。

參考法條：

行政執行法第 36 條（即時強制之時機及方法）

〔1〕行政機關為阻止犯罪、危害之發生或避免急迫危險，而有即時處置之必要時，得為即時強制。

〔2〕即時強制方法如下：

一、對於人之管束。

二、對於物之扣留、使用、處置或限制其使用。

三、對於住宅、建築物或其他處所之進入。

四、其他依法定職權所為之必要處置。 （亦請參考同法第 28 條第 2 項第 5 款：「其他以實力直接實現與履行義務同一內容狀態之方法。

第 38 條（危險物之扣留）

〔1〕軍器、凶器及其他危險物，為預防危害之必要，得扣留之。

〔2〕扣留之物，除依法應沒收、沒入、毀棄或應變價發還者外，其扣留期間不得逾三十日。但扣留之原因未消失時，得延長之，延長期間不得逾兩個月。

〔3〕扣留之物無繼續扣留必要者，應即發還；於一年內無人領取或無法發還者，其所有權歸屬國庫；其應變價發還者，亦同。

第 39 條（得使用、處置或限制使用土地等之情形）

〔1〕遇有天災、事變或交通上、衛生上或公共安全上有危害情形，非使用或處置其土地、住宅、建築物、物品或限制其使用，不能達防護之目的時，得使用、處置或限制其使用。

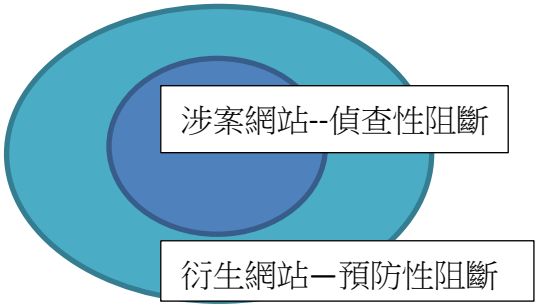
綜上而論，針對新興科技而衍生而有阻斷不法詐欺網站（域名，Domain Name）之必要，除另立新法（例如，科技偵查法）加以規範之外，上開現行法律規定，均難以援引為授權基礎，為資因應而有修正之必要，特別是增加對「無體物（權利或數位資訊）」作為規範客體，抑或是增加授權或刪除限制規定等方式修法，以使因時代進步之科技法律規範而得以合乎法理之適用，並有效保障人權。

中央警察大學 洪文玲教授

本次論壇主題旨在針對近年來利用網站進行詐欺的新興犯罪類型，如何在現行法制與技術下迅速有效防堵，相關法制如何完備？執行困難如何克服？期望提出有效解決問題的具體策略。

本文先分析阻斷之目的與法律性質，再分析現行方法與法據之困難問題，最後提出解決對策與建議。

一、阻斷不法詐欺網站之目的有二：一是找出犯罪行為人，搜索扣押犯罪工具與犯罪所得，進行訴追與課責，這是刑事訴訟法上偵查犯罪保全證據與法院審判的層面；二是如何制止犯罪擴大，避免嫌犯利用偵審期間對被告人權保障的程序機制，其集團繼續經營其他衍生網站，持續讓不知情的人民掉入陷阱蒙受財產損失，這是警察行政法上制止犯罪、防止危害的層面。



二、利用網站不法詐欺犯罪之執法困境：

犯嫌以網站或群組作為平台，設定網址 IP 及帳戶(含人頭)，進而散布不實商業交易或投資資訊，引誘相對人上鉤進行交易，事後以各種理由延遲給付或不給付。或設計斷點，要

求被害人登出群組，換另一人以電話與被害人接洽進行交易，俟被害人驚覺受騙，卻缺少直接證據，無法究責。

被害人報案，舉證上網經過、廣告內容、網頁畫面。警察從網址解析網域名稱、透過註冊商(例如 godaddy)調查架設網站之嫌犯，但國外的業者通常不會提供資料給我國警方。在金流追查方面，民國 94 年透過銀行法訂定相關辦法，警察有權通報銀行警示可疑帳戶，凍結帳戶，並請銀行提供申登人資料，但若是人頭帳戶，或屬於國外帳戶，仍無法溯源查出幕後主嫌。

利用數位犯罪無國界、迅速流通的特性，使犯罪證據難以追查，加上台灣的外交處境，司法互助無法全面，均使偵查強制處分的實施更加困難，實效有限。另衍生人頭帳戶等問題，帳戶所有人常遭警方列為共犯，事實上他可能只是被利用，也是受害者。

三、對策分析：

針對網路犯罪的對策可分為三個部分，即事前預防、事中措施、法律制裁。今天的主題聚焦在第一部分。

事前預防---阻斷衍生網站，停止解析

事前預防方面：除對民眾的防騙宣導教育，仍須因應犯罪新手法持續更新教材並強化宣導外，誠如前面引言人所述，詐欺網域數量相當大，假投資案件已接獲報案的涉案網址，加上相關聯的衍生性網址，每月可達 3000 筆，自被害人報案啟動刑事偵查流程，至法院裁定扣押，通報 TWNIC 停止解析，順利的話，至少耗時一個星期；然而詐欺集團申請一個網址的更換可能只須一個小時，因此即便刑事扣押裁定執行，該集團網路犯罪活動仍未停歇，因此，阻斷範圍必須擴大及於「衍生性網站」，發動阻斷的門檻有必要降低至「合理懷疑」。如同銀行接獲警察通報凍結警示帳戶；食品安全預防機制，發現食材有問題，生產線先停擺、成品先預防性下架；傳染病蔓延期間，群聚性營業先停業，營業自由、遷徙自由、行動自由暫時先管制，相同的道理。這些措施的性質，是暫時性處分，不服者，可以異議，俟警察機關或法院查明後，再解除阻斷。

而民主法治國家，國家所有干預性的公權力，都須依法有據，發動要件明確，權責清楚，讓人民可以預見，可以配合遵循，也避免政府濫用侵權。

阻斷(停止解析)之法律依據分析

現行法關於危害防止、犯罪預防的職權措施規定，大都分散規定在各行政機關的業務法令中。目前刑事局阻斷網站的做法是協請電信業者善盡社會責任，協助阻斷詐欺網站。以電信管理法第 8 條第 2 項: 電信事業無正當理由，不得拒絕電信服務之請求及通信傳遞。反面解釋認電信事業有正當理由如預防犯罪、有犯罪之虞，即可拒絕提供服務。此係電信事業與客戶間之私法契約關係。刑事局只能以行政指導方式通知電信事業。

一般性依據方面，警察法第 2 條、行政執行法第 36 條及警察職權行使法第 28 條可以作為依據嗎？

警察法第 2 條規定警察有依法防止一切危害之任務，然因其太概括，不能作為行使職權之依據，無論學說或司法院第 570 號解釋，均採否定論。行政執行法第 36 條規定行政機關為阻止犯罪、危害之發生或避免急迫危險，而有即時處置之必要時，得為即時強制。其措施包括對人、對物、對處所及其他必要之措施。解釋上似可及於資訊、網站之移除與凍結。惟

衍生性網站，尚未有被害人，是否足以證明危害或犯罪正在發生，在要件合致上存有疑慮；至於警察職權行使法第 28 條規定警察為制止或排除現行危害公共安全、公共秩序或個人生命、身體、自由、名譽或財產之行為或事實狀況，得行使本法規定之職權或採取其他必要之措施。警察依前項規定，行使職權或採取措施，以其他機關就該危害無法或不能即時制止或排除者為限。該條即時強制規定，固然阻斷詐欺網站可視為避免人民財產損失所採取的必要措施，且其他機關就該危害無法或不能即時制止或排除。然而警察機關須證明危害正在發生；且必須其他權責機關不能即時處理時，警察機關才能介入發動職權措施。數位服務網站管理權責機關目前尚不明確，警察是否有法定職權得命令電信業者或網路註冊管理服務人阻斷可能的詐欺網站，均有疑義。故若通知電信業者或網路註冊管理服務人對涉案網站或衍生網站停止解析，其拒絕配合，警察恐也無法強制為之。

阻斷網站，停止解析的可能立法建議

綜上分析，仍宜有專法或行為法性質之職權依據，方符合法律保留與明確性原則。而與防詐騙相關之立法，如前述銀行法，其立法過程與理由，足資主管電信及數位服務業之主管機關(交通部或 NCC 或行政院數位發展部)未來於數位服務管理法令中擬定課予電信業者或網路註冊管理服務人善良管理人責任及時阻斷不法網站之參考。

按銀行法第 45 條之 2 第 2 項、第 3 項規定：「（第 2 項）銀行對存款帳戶應負善良管理人責任。對疑似不法或顯屬異常交易之存款帳戶，得予暫停存入或提領、匯出款項。（第 3 項）前項疑似不法或顯屬異常交易帳戶之認定標準，及暫停帳戶之作業程序及辦法，由主管機關定之。」上開規定係於 94 年 5 月 18 日增訂發布，其立法理由為：「為維護各銀行經管財務之安全，提高金融從業人員之警覺，減低銀行營運上之風險，爰依據行政院強化社會治安第 18 次專案會議結論，增訂銀行安全維護相關行政命令之法律授權依據。」又依上開規定授權訂定之系爭管理辦法第 3 條第 1 款、第 3 款規定：「本辦法用詞定義如下：一、警示帳戶：指法院、檢察署或司法警察機關為偵辦刑事案件需要，通報銀行將存款帳戶列為警示者。……三、通報：指法院、檢察署或司法警察機關以公文書通知銀行將存款帳戶列為警示或解除警示，惟如屬重大緊急案件，得以電話、傳真或其他可行方式先行通知，並應於通知後五個營業日內補辦公文書資料送達銀行，逾期未送達者，銀行應先與原通報機關聯繫後解除警示帳戶。」第 4 條第 1 款第 2 目規定：「本辦法所稱疑似不法或顯屬異常交易存款帳戶之認定標準及分類如下：一、第一類：……（二）屬警示帳戶者。……」第 5 條第 1 款第 2 目規定：「存款帳戶依前條之分類標準認定為疑似不法或顯屬異常交易者，銀行應採取下列處理措施：一、第一類：……（二）存款帳戶經通報為警示帳戶者，應即通知財團法人金融聯合徵信中心，並暫停該帳戶全部交易功能，匯入款項逕以退匯方式退回匯款行。……」第 9 條第 1 項規定：「警示帳戶之警示期限自通報時起算，逾 2 年自動失其效力。但有繼續警示之必要者，原通報機關應於期限屆滿前再行通報之，通報延長以 1 次及 1 年為限。」第 10 條第 1 項規定：「警示帳戶嗣後應依原通報機關之通報，或警示期限屆滿，銀行方得解除該等帳戶之限制。」另依系爭管理辦法 95 年 4 月 27 日訂定發布時之立法總說明略以：「……為維護金融體系運作之完整及消費者權益，銀行法第 48 條第 1 項明訂『銀行非依法院之裁判或其他法律之規定，不得接受第三人有關停止給付存款或匯款、扣留擔保物或保管物或其他類似之請求』，惟對於歹徒利用各式便捷之金融管道進行不法利得移轉以遂行其不法目的之行為，尚無一立即有效之防制規範。鑑於前述之不法犯罪行為，已嚴重斲傷金融秩

序及民眾信心，為遏止不法行為並期身處第一道防線之金融機構，得以貫徹政府打擊犯罪及國際間反洗錢與反恐政策，特於銀行法第 45 條之 2 增訂第 2 項『銀行對存款帳戶應負善良管理人責任。對疑似不法或顯屬異常交易之存款帳戶，得予暫停存入或提領、匯出款項。』及第 3 項『前項疑似不法或顯屬異常交易帳戶之認定標準，及暫停帳戶之作業程序及辦法，由主管機關定之。』

在 NCC 研擬之數位通訊傳播法，明確賦予相關機關權限(包括主管機關、法院、檢察署、警察機關)，如有違法事由可據以通報 TWNIC、電信業者停止解析 。

或在警察職權行使法增訂第 8 條之 1 規定，為防止犯罪，對疑似不法或顯屬異常之網域名稱，警察機關得以公文書通知電信業者或網路註冊管理服務人暫停解析，但如屬重大緊急案件，得以電話、傳真或其他可行方式先行通知，並應於通知後五個營業日內補辦公文書資料送達，逾期未送達者，電信業者或網路註冊管理服務人應先與原通報機關聯繫後解除。

中央警察大學 許福生教授

一、詐團設「賣家幫」網站詐財已成當前防制詐欺犯重要課題

依據聯合報 2021 年 11 月 29 日報導，詐騙集團架設「賣家幫」網站，宣稱與國內外電商合作，匯款加入會員「虛擬下單」可獲紅利，推薦會員還能賺獎金，但收錢不依約出金，向 278 人騙走 2756 萬元。刑事局展開調查，提醒民眾留意。

警方調查，詐團在高雄市成立公司，設網站、APP 等「賣家幫」平台，號稱與內政部合作網路實名認證取信，將被害人拉進 LINE 群組後，指透過「雲計算虛擬下單技術」衝高商品銷售量，不用實際購買商品，訂購商品後可退回本金，待商品賣出後賺取紅利，拉下線還有獎金。

該平台去年 2 月起成立，刑事局統計今年截至昨天，有 278 人被騙 2756 萬元，詐騙手法類似去年「友點讚」、「蝦皮集單」假投資案。「賣家幫」3 個網站最近無預警關閉，數名被害人今天下午赴刑事局報案。

刑事局說，這類假投資號稱零風險、高報酬、穩賺不賠，網站被檢舉下架後會不斷變更網址，民眾提出質疑就被踢出群組。因此，如何以阻斷不法詐欺網站方式，避免民眾上網接觸受騙，已成為當前防制詐欺犯最重要課題。

二、RPZ 簡介

RPZ(Response policy zone)是域名系統服務器上的一種自定義策略的機制，讓遞歸解析器返回可以修改解析的結果。通過修改結果，可以阻止對相應主機的訪問。經由在 recursive resolver 啟用 RPZ 之後，就可以讓使用者在沒有額外的設定下阻止其連到惡意網站。

因此， RPZ 機制係以停止解析之方式，將非法網站封鎖，使民眾無法自國內連線造訪該網站。

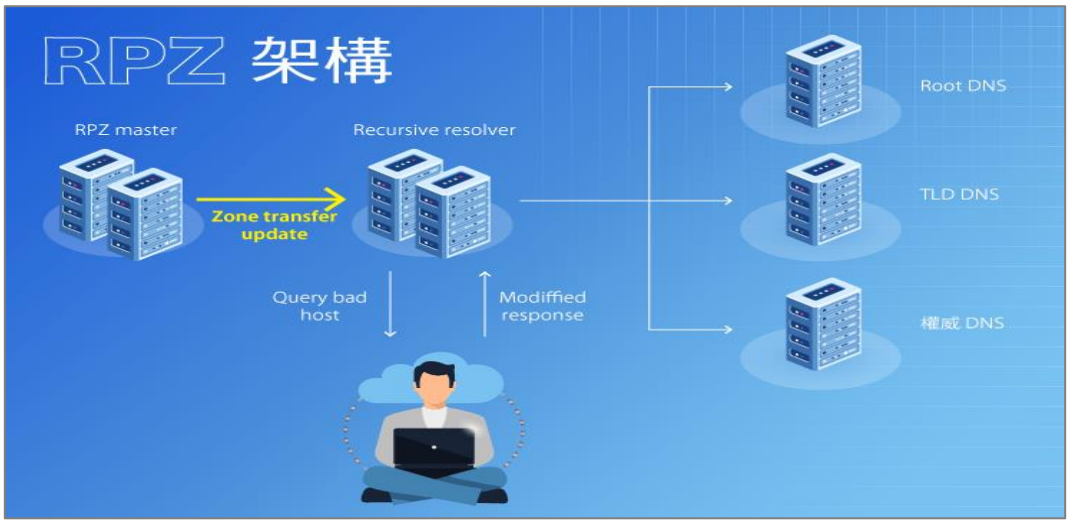


圖 1：RPZ 架構圖（引自 https://rpz.twnic.tw/）

三、現行可以阻斷、下架詐騙網站法令

可以阻斷、下架詐騙網站法令，除了透過長期的修法程序（如引言人所言：訂定如數位通訊傳播法專法、明確賦予行政機關權限、通報 TWNIC、電信業者停止解析等）外，現況可以找出解決方案法令包含：

(一)刑事法令

刑訴法搜索、扣押程序，但需以取得令狀為原則，惟詐騙網站更換網址快速，恐不能達成立即阻斷網站避免民眾持續被害的目的。

(二)行政法令

1. 行政執行法第 36 條：行政機關為阻止犯罪、危害之發生或避免急迫危險，而有即時處置之必要時，得為即時強制。即時強制方法如下：一、對於人之管束。二、對於物之扣留、使用、處置或限制其使用。三、對於住宅、建築物或其他處所之進入。四、其他依法定職權所為之必要處置。
2. 警察職權行使法第 28 條：警察為制止或排除現行危害公共安全、公共秩序或個人生命、身體、自由、名譽或財產之行為或事實狀況，得行使本法規定之職權或採取其他必要之措施。警察依前項規定，行使職權或採取措施，以其他機關就該危害無法或不能即時制止或排除者為限。
3. 電信法第 8 條第 2 項：以提供妨害公共秩序及善良風俗之電信內容為營業者，電信事業得停止其使用。
4. 電信管理法第 8 條第 2 項：電信事業無正當理由，不得拒絕電信服務之請求及通信傳遞。

四、法令之適用

(一)境內域名之適用

刑法第 38 條第 2 項規定，「供犯罪所用、犯罪預備之物或 犯罪所生之物，且屬犯罪行為人者，得沒收之」；再依刑事訴訟法第 133 條第 1 項規定，「可為證據或得沒收之物，得扣押之」。涉案域名如合於上開規定要件，原可為扣押、沒收之客體。若該域名係註冊於我國管理機構之境內域名，可能符合對第三人（即註冊機）之搜索、

扣押，取得法院核發之扣押裁定，令該域名所屬之註冊管理機構或受理註冊之機構，將該域名強制轉向公權力指定之網域，並限制被告對該域名之支配、處分權，達到扣押之目的。

但誠如引言人所言，依照刑事程序，詐欺集團可隨時更換網址，緩不濟急；詐欺網址數量大(假投資案件單月被害+衍生性可達 3000 筆網址)，司法單位無法以統案處理。

(二)境外域名之適用

涉案域名係註冊於境外（此為目前我國網路犯罪絕大部分情形），針對境外域名，TWNIC 之 DNS RPZ 機制僅能達到阻絕自我國內連線至該網頁之效果，屬於犯罪損害擴大之控制，卻無法將該網域之支配、處分權交予公部門或納於我國公權力下，因為國內民眾或犯罪行為人使用跳板（如 VPN）或其他毋需伺服器解析之連線方式，仍可能規避 DNS RPZ 機制而再造訪該涉案網站，犯罪行為人利用共犯，透過不受我國司法管轄之境外域名註冊機構，仍可能繼續支配或處分該網域，此種情形，與我國刑事訴訟法上之扣押，完全剝奪被告對得扣押物之支配權，概念並非完全相符。是停止解析之方式、目的與效果，恐難完全等同於我國法上之扣押。

五、個人之看法

為了即時處理，境內的網站雖可依照一般刑事案件偵辦的方式處理，但因詐欺網址數量大、緩不濟急；另對境外網站之執行，若以刑訴程序之扣押，仍無法完全剝奪被告對得扣押物之支配權，故面對此問題，長期仍需修法明確賦予行政機關權限、通報 TWNIC、電信業者停止解析。然臨時性解決方案，法令依據可更開放些，可依上述警職法第 28 條擴張解釋為之，但需召開跨部會協調及訂明確 SOP 與提供救濟管道，由行政機關即時處置，以預防民眾持續被害。

意見交流

◎ 刑事警察局 林故廷主任秘書

刑事訴訟法有分為三個層次：1.法官保留 2.檢察官保留 3.依照警察職權行使法應如何作為。如依搜索扣押之方式，以一個月高達 3000 餘件之數量，縱然法律上可行，然事實上司法能量卻不足以應付。我在新北市分局長任內查緝毒品或賭場，我利用第三方警政的方式，將不法場所斷水、斷電，因此，此作法或許是較為簡單有效的方式。另在警察職權行使法的修正上，行政院目前已有機制在運作中，欲完成行政程序之要點。另外，檢察機關實施搜索扣押應行注意事項第 9 條規定: 非附隨於搜索之扣押，其標的屬得為證據之物，且非兼具犯罪物或犯罪所得性質者，得逕行為之，免經法官裁定。此條規定很適合網域(非實體物)的範圍，如果以檢察官保留與刑事局合作，則可以達到很好的扣押成效。

◎ 刑事警察局 黃嘉祿局長

高檢署有指導我們如何扣押網域，但這些都是在案件已經起訴或是要判刑才有的作為，是不可行的，所以我和李副局長正在研究扣押這些不法網站、網址的方法。另一方面，羅秉

成政委有在溝通協調，我也向羅政委提到本局現正積極處理這些事情。目前我們在整個運作機制上都十分仔細，再三核對之後，才將資料送請電信業者協助停止解析。

與談總結

銘傳大學 章光明主任

壹、刑事局所提問題界定如下：

一、受騙嚴重：不法詐欺網站之問題日益嚴重。

二、查緝不易：對於境外網站以溯源，且不法網站常設斷點躲避追查。

三、刑事司法流程緩不濟急：刑事流程耗時費工，往往緩不濟急。

四、尋求行政法條的支持：刑事流程不如行政流程有效率，因而須尋求行政法條作為處理手段的支持。

五、如何修法：在行政手段上若目前仍無完全相對應的法條，應當思考如何修訂法律以解決問題。

貳、問題再界定：

一、不法網站層面廣闊：不法網站問題非僅詐欺案件，尚有毒品及其他犯罪問題，非僅止於假投資詐騙問題，還有網路博弈問題，故應將思考層面擴大到網路管理。

二、網路主管機關：我國政府為何沒有網路主管機關？NCC 只管電信，卻不管網路，此情形十分弔詭，乃政府體制的問題，因為政府體制本身的不完善，使得詐欺網站問題無法可管，但這只是表象，須從上位問題源頭的網路管理加以解決。

三、不法詐欺網站本質上為犯罪預防的問題：不法詐欺網站本質上是犯罪預防，問題重點應著重在預防網路被害，而非偵查。

參、可行的方案：

一、刑事法適法優越性：

(一)扣押、沒收：在現行法制下，仍應走向扣押、沒收的途徑。

(二)行政法有反向訴訟風險。

(三)司法數位轉型，此乃司法改革的問題。

(四)發展精準執法模式：刑事局從已發生案件著手，發展精準執法模式。

(五)網絡治理的概念：如剛才許多與談人所提到的聯合處理、網絡治理、司法互助、第三方警政，多方共同協力等解決問題途徑均屬網絡治理概念。

然此一途徑所須配合條件眾多，非警察機關單獨所能處理，雖應努力，也有必要，然難度較高，且為事後亡羊補牢。

二、行政法途徑：

預防方為解決問題的主要途徑，則行政法令的增修便顯得重要，其中，警察職權行使法是為中心:

(一)警察職權行使法：依警察職權行使法第 28 條，並訂作業辦法向下規範，增加其可操作性。

(二)警察職權行使法之即時強制：警察職權行使法之即時強制或可使用，然須以危害存在為前提，恐無法達到預防之效。

三、修法部分：

(一)科技偵查法：或許可透過科技偵查法的修法解決此問題，但因該法遭致許多人權學者的批評，恐難以在短時間內訂定完成。

(二)增訂警察職權行使法第 6 條之 1 或第 8 條之 1，對網路犯罪的預防措施加以規範，此法因侵害程度較低，亦可降低警察人員遭致反項訴訟的可能。

四、技術強化：

(一)網絡科技技術的提升，可使得行政機關及執法部門有能力監管虛擬平台。

(二)透過國際合作強化預防犯罪之成效。