RDEC-TPG-098-004（委託研究報告）

網路犯罪防治體系之政府職能與角色分析

行政院研究發展考核委員會編印
中華民國九十八年十二月

RDEC-TPG-098-004（委託研究報告）

網路犯罪防治體系之政府職能與角色分析

受委託單位：國立臺灣大學
執行單位　：行政院研考會委辦臺灣公共治理研究中心
研究主持人：楊永年
協同主持人：楊士隆
研究助理　：邱柏嘉、李宗憲

行政院研究發展考核委員會編印
中華民國九十八年十二月

目　次

表 次

圖 次

提 要

在 2009 年 11 月行政院研考會的調查發現，電話與網路詐騙爲民怨之首（網路票選爲第二大民怨），其原因和整個市場技術和科技快速地分工及快速地整合有關。例如目前已出現數位匯流（或合流）。但面對數位匯流衍生的網路犯罪問題，政府部門的分工緩慢、整合更慢。背後的原因包括政府跨層級與跨部門間無整合誘因，政府爲符合依法行政的原則作行動設計時，又發現缺乏彈性與法律依據。例如個資法的複雜政治因素，包括管制者（政府）無誘因推動，被管制者（財團）希望政府不要管制、個資法不要通過。換言之，詐騙案的存在是真實的，但因犯罪者充份應用網路與電話科技進行詐騙，加上「網路犯罪」管制不易或政府職能與分工難以發揮應有的功能。

不管是網路犯罪或一般犯罪都是犯罪，問題在於網路是一種工具，透過網路工具犯罪，但工具本身是中性的，重點是在於實體而不是工具，以及如何去對工具本身的內容作管制。網路交易通常會留下痕跡，或者網路社會多存在盲點，然而網路社會的主管機關又很多，如 ISP（網路服務供應業）、ICP（網路內容供應業）、網路平台，背後除了有商業利益，也有許多政府主管機關。嚴格來說，若有交易行爲、商業行爲（網購）就與經濟部有關係，但因與網路科技管理有關，因此也和國家通訊傳播委員會的業務有關。而交易過程就存在交易成本，或者交易過程本身就存在風險。可以說，網路社會的主管機關很多，目前整合存在盲點，使得政府在網路犯罪預防與偵查的職能難以發揮，因此這是本研究的重點內容。

政府的角色職能要做得好，須有政策形成、管制規劃、如何執行、回饋後再規劃，而這些政策內涵都要具預防和偵查的理念，不過政策的連結經常存在落差。舉例而言，網路犯罪案例與國家通訊傳播委員會(NCC)管制政策有關係，而刑事局是執行單位，管制者與執行者就存在落差，理論上 NCC 係主管或管制機關。實際上，NCC 又認爲他們無此權限，或權限在其它部門（部會）。換言之，管制單位與執行單位需要有很強的關連性與連結性，從偵查再將偵查所得的問題回饋到預防（或政策管機機關）的部分進行連結。因

此，政府如何預防網路犯罪，以及誰來設計預防政策，這是政府必須努力的地方。而政策規劃也是如此，規劃要有整合性，應作跨部門之結合。至於政策執行也有很多主管機關，難免出現整合的困境或問題。

爲因應網路犯罪的專業化與複雜化，國家資通安全會報成立，從國家資通安全基礎建設的角色區分圖，清楚完整的將各相關部會（部門）納入整體規劃。但似乎沒有發揮應有功能，甚至體系內成員存在負面評價，原因在於目前係以科技思維而非行政整合的方式進行運作。因爲網路犯罪涉及跨部會人文社會與官僚體制議題，導致整合上出現盲點。使得目前資通會報機制難以說服不同部會達成共識。目前網路犯罪相當嚴重，最大宗的犯罪案是電話與網路詐騙。由於目前科技上電話與網路已有密切連結，透過網路打電話可更改發話號碼，因此冒用政府部門電話號碼，因而出現很多的詐騙犯罪。重點在於，發話地點（電腦）不在台灣（國內），也就是說電腦網址（IP address）經常在大陸或國外，使得偵查人員無法或難以追緝。換言之，牽涉跨國、兩岸的網路犯罪問題，也是政府要克服的環節。再者，警察屬末端之政策執行單位，但屬前端的政策形成、規劃的部分，則經常被忽略。

本研究發現，地方政府的對抗網路犯罪的資源與角色從中央到地方政府都非常有限，這是訪談和焦點座談的結果。建議中央政府、NCC 與網路犯罪相關部門可以扮演更積極的角色，發揮政府職權分工之整合的有效功能，以及如何使用權力，怎樣用法令，如何讓被規範的行政部門能發揮整體的效果，本文也從這個角度去作思考，並做出具體可行之研究發現與建議。

一、政策面建議：（一）修法，特別是個資法部分，導致個資洩漏，應有求償機制；同時訂定管制條文，要求業者投資設計防止個資洩漏軟體。（二）建立中央政府跨部會、地方政府跨局處、中央與地方政府跨政府層級的合作誘因；甚至鼓勵網民一起加入個資洩漏查處的工作。（三）網路犯罪偵查機關法制化，與網路管制部門（含政府與民間）有更多的連結。

二、服務傳送之分析建議：（一）行政院資通會報功能強化，發揮應有整合功能，勿使其淪爲開會的型式，並應結合治安會報情資，發揮功能；更重要的是資通會報應從科技設計取向，轉化爲政府官僚執

行取向。（二）設立單一窗口受理民眾通報及申訴，強化 165 反詐騙專線之功能。（三）策進政府憑證管理中心，以管制個資洩漏紀錄不良之網路業者；不同的網路犯罪類型，要求由不同的主管機關出面整合。（四）加強兩岸與國際合作，共同打擊網路犯罪。

三、民間參與之分析建議：（一）加強民間參與網路安全技術的研究。（二）協調整合產官學研有關網路安全方面機制的整合，以提供國人更完善之服務與安全資訊。

網路犯罪防治體系之政府職能與角色分析

第一章　緒論

隨著網路的快速發展，如網路上的虛擬文化特性、新形成的網路生活型態、電腦科技所帶來的學習新技能與新工作程序，在網際空間之下，網際網路可說是現今資訊社會最重要的應用，它固爲人類在資訊的流通與掌握上，帶來莫大的便利，使得網路犯罪越來越氾濫。但也因爲如此，原本在實體世界裡，被嚴格遵守的規範，開始出現小小的鬆動，以虛擬空間爲犯罪地點的不法事件越來越多，色情訊息、盜版、詐欺等犯罪事件時有耳聞，隨之而起的，網際空間也成爲各種犯罪滋生的溫床，並衍生出許多法律問題，則限制網路環境裡傳輸資訊的使用，又將對網路環境的發展及資訊的流通形成阻礙。由於網路科技存在市場誘因，具快速分化、分工、匯流與整合的特性，使得網路犯罪呈現多元化、多樣化的形態。但政府職能角色卻因法令規定與組織文化，無法隨著網路變遷的腳步調整。

因此，在網路犯罪防制體系中，有關政府職能與角色之扮演，成爲現代網路社會的重要課題，所以政府部門與角色如何整合及分工，在網際網路此一領域中，現爲當務之急。

第一節　研究背景與範圍

今年「性侵的遊戲軟體三不管」內政部、經濟部、通傳會（NCC）遭監察院糾正。但糾正之後，似乎也沒有進一步處理的機制形成，這可能是未來政府職能與角色應改善之處。「電車之狼」是一種模擬性侵的遊戲軟體，曾在國內的拍賣網站上公開販售。監察院調查後指出，內政部、經濟部及NCC等相關主管機關，對於色情遊戲軟體沒有善盡把把關、查處的責任，怠忽職守，決定予以糾正。

「電車之狼」（Rapely）是日本的色情遊戲軟體，內容是玩家從地鐵站跟蹤並性侵少婦及幼童。「電車之狼」曾在國內的兩大拍賣網站以149元就可購得，勵馨基金會向內政部、經濟部及NCC等相關主管機關提出檢舉，但是

當時卻被這些機關互推皮球。監委程仁宏、趙榮耀調查後指出，內政部爲兒少福利、性侵防治主管機關，沒有積極主動查察性侵遊戲軟體，怠忽職守在先，之後又沒有積極查處；而經濟部是拍賣網站的中央主管機關，只一味要求業者負起社會責任，建立自律機制，自己卻未負起主管機關執法及監督之責；NCC沒有主動整合相關部會查處網路不當內容，杜絕教導犯罪商品於網路販售，也沒有極協調業者訂定自律規範。監察院認爲，內政部、經濟部及NCC等主管機關都有違失，因此提出糾正。監察委員程仁宏：『我們認爲內政部、經濟部及NCC這三個單位，對於網路管理，尤其是教導性侵的遊戲軟體管理怠惰，因此提出糾正。』

網路科技日新月異，網路犯罪已成爲新興的犯罪模式，甚至結合許多傳統犯罪，成爲現代重要的犯罪工具（手法）。目前各種網路犯罪類型，似以網路詐騙與網路駭客（入侵）兩種犯罪之影響層面最廣。本研究定義網路詐騙，係指與所有以電腦或新興科技相關之詐騙犯罪。由於這樣的定義使得網路犯罪內容包含很廣，下文將做分類論述。由於個資外洩可能造成數萬筆個資遭歹徒利用，造成更多的相關的網路犯罪案例。例如，就有網路駭客指出，民眾的個人資料外洩後，經常被犯罪集團利用於詐欺犯罪。關於網路駭客犯罪，立法、司法與行政部門聯手祭出「天文數字的重罰」加以遏止，近日朝野更達成重大共識，一舉將立法院審議中的「個人資料保護法」草案內容，個資外洩賠償上限，從現行法二千萬元提高到十億元。這改革的方向是正確的，換言之，除了賠償之外，其他管制方法也不能忽略。

關於網路犯罪的定義，林山田、林宜隆、廖有祿等都有，評語眾多，本研究「網路犯罪防治體系之政府職能與角色分析」的操作型定義是：政府之職能應如何加強防範經由網路被竊取的個人資料或是消費行爲習性所伸出各種犯罪。如前文所述，這定義範圍很廣，因此下文將進行網路犯罪之分類，但重點在於，本研究希望從政府職能與角色之方向，配合與找尋具代表性之網路犯罪實際案例進行研究。

一、網路犯罪現況

表 1 我國電腦網路犯罪概況（2007 年 1-10 月）

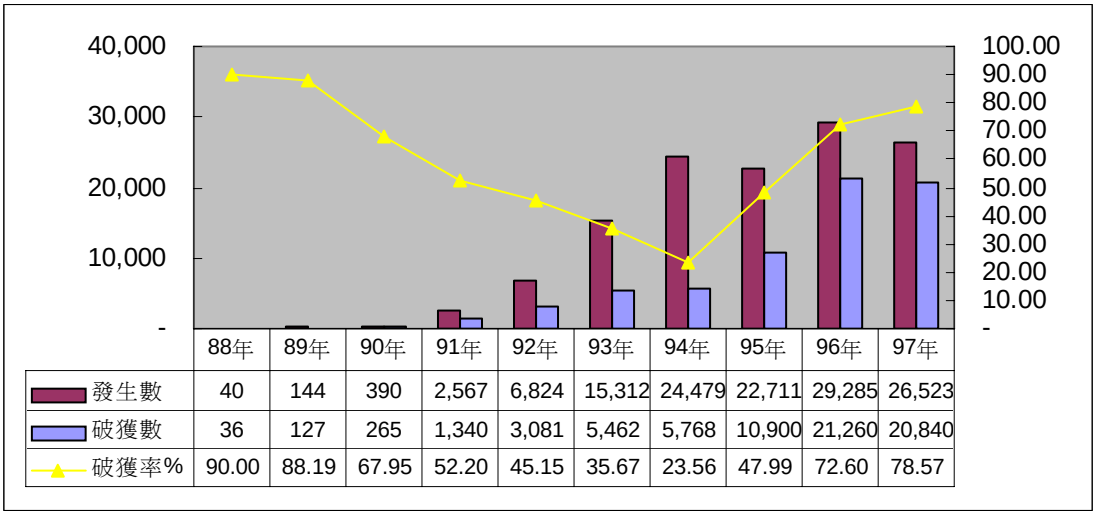
發生數	本期（件）	上期（件）	增減率（%）
總計	22,111	25,092	- 11.88
詐欺	9,437	8,458	11.57
妨害電腦使用	3,519	5,878	- 40.13
一般妨害風化	2,864	1,036	176.45
違反兒童及少年性交易防制條例	2,646	5,353	- 50.57
智慧財產權	2,415	2,795	- 13.60
妨害名譽（信用）	566	531	6.59
賭博	118	159	- 25.79
偽造文書	100	86	16.28
強制性交	69	109	- 36.70
妨害自由	66	49	34.69
毒品	63	57	10.53
竊盜	36	207	- 82.61
槍彈刀械	33	27	22.22
妨害秘密	30	24	25.00
野生動物保育法	21	14	50.00
侵占	18	10	80.00
電腦處理個人資料保護法	18	108	- 83.33
一般恐嚇取財	14	42	- 66.67
其他	78	149	- 47.65

資料來源：內政部警政署

以我國警政署統計[1]，我國97年1-10月電腦網路犯罪發生數共22,111件

[1] 內政部警政署全球資訊網-統計資料-警政統計通報-97 年第 48 號(97 年 1-10 月電腦網路犯罪概況)。http://www.npa.gov.tw/NPAGip/wSite/public/Attachment/f1227506587476.doc

，較前一年同期減少2,981件（-11.88%），主要案件爲詐欺案9,437件（占42.68%）爲最多，其次爲妨害電腦使用案3,519件（占15.92%）次之，第3爲妨害風化案件2,864件（占12.95%）；詐欺案件較前一年同期增加979件（+11.57%）。可見網路詐騙仍爲目前網路犯罪類型的最大宗，且有逐漸增高趨勢。廣義而言，表1的網路犯罪概況，均可視爲（網路）詐欺犯罪，因爲這些都是網路使用者和犯罪者互動，因認知差距產生的犯罪行爲。



	88年	89年	90年	91年	92年	93年	94年	95年	96年	97年
發生數	40	144	390	2,567	6,824	15,312	24,479	22,711	29,285	26,523
破獲數	36	127	265	1,340	3,081	5,462	5,768	10,900	21,260	20,840
破獲率%	90.00	88.19	67.95	52.20	45.15	35.67	23.56	47.99	72.60	78.57

圖 1　近 10 年網路犯罪案件發生數、破獲數(率)

資料來源：內政部警政署刑事局

依據美國全國消費者聯盟（The National Consumer League）的網路詐欺觀察小組（Internet Fraud Watch[2]）在2007年統計資料[3]，美國最常見的網路詐欺行爲是假支票詐騙、網路購物與網路拍賣。顯然，網路詐欺也是美國政府與網路頭痛的犯罪問題。至於我國的網路詐騙行爲，根據王秋惠（

[2] http://www.fraud.org/internet/intinfo.htm
[3] 2007 Top 10 Internet Scams, NCL's Fraud Center http://www.fraud.org/internet/2007internet.pdf

2006）所進行的調查研究[4]顯示，網路詐欺犯罪類型以「僞稱買賣」（21.5%）、「詐騙款項」（21.4%）、詐騙帳號密碼等電磁記錄（15.9%）、假冒名義（15.9%）佔最大宗。而如果將假支票詐騙、一般商品販售、網絡拍賣等三者之網路詐欺行爲進行加總，共有65%和網路金融交易有關，也顯見網路交易存在許多衍生的犯罪問題。

表 2 美國 2007 年常見網路詐欺行爲

排名	詐騙方式	比例	平均損失
1	假支票詐騙Fake Check Scams[5]	29%	$3,310.87
2	一般商品販售General Merchandise[6]	23%	$1,136.84
3	網路拍賣Auctions[7]	13%	$1,371.08
4	奈及利亞貨幣服務Nigerian Money Offers[8]	11%	$4,043.14
5	彩券 Lotteries/Lottery Clubs	7%	$998.43
6	免費貸款 Advance Fee Loans	3%	$1,310.77
7	中獎 Prizes/Sweepstakes	3%	$1,181.58
8	網路釣魚Phishing[9]	3%	$220.47
9	線上情人 Friendship and Sweetheart Swindles[10]	1%	$3,038.31
10	網路服務Internet Access Services[11]	1%	$896.99

資料來源：2007 Top 10 Internet Scams, NCL’s Fraud Center

[4] 王秋惠撰，網路詐欺被害特性與被害歷程之研究。中央警察大學犯罪防治研究所碩士論文，95 學年度。
[5] 因爲交易或抽獎活動，被害人收到假支票，在發現其爲假支票之前，已將手續費匯出。
[6] 在購物網站上購物，付款後未收到商品，或收到的商品不符。
[7] 在拍賣網站上交易，付款後未收到商品，或收到的商品不符。
[8] 被害人接受到來自奈及利亞政府官員的訊息，要求提供銀行帳戶以協助其轉移數百萬美金的資金至海外，被害人被許諾或得一定百分比的金額作爲籌賞。
[9] 假冒知名網站要求用戶確認個人資料，例如以gmai1（數字 1）假冒gmail（小寫L）。
[10] 網路交友或網路情人，對方要求給予金錢協助。
[11] 收到網路服務的假帳單要求付費。

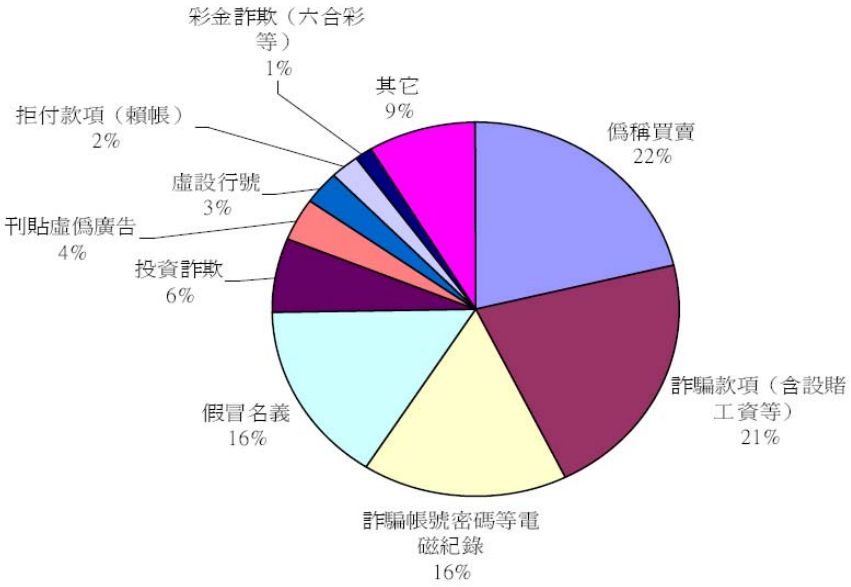


圖 2　網路詐欺犯罪類型分佈

資料來源：王秋惠，2006

曾百川[12]以近年來國內外司法警察所偵破的各類型網路詐欺犯罪案件及相關文獻資料進行分析，依網路使用目的區分爲網路拍賣、網路購物、商業金融、網路遊戲、色情網站及其他類型六類網路詐欺型態。顯見國內相關的詐欺犯罪和國外有相似性，也有差異性。和金融交易相關的網路詐欺，國內與國外是類似的；至於國內網路購物與網路遊戲詐欺則似乎較爲嚴重。因此，有關國外政府在職能角色的經驗上，有些可提供我國參考。

[12] 曾百川撰，網路詐欺犯罪歷程之質化研究。中央警察大學犯罪防治研究所碩士論文，95學年度。

表 3 網路詐欺犯罪型態

網路詐騙類型	詐騙方式	
網路拍賣詐欺	賣方	假冒向買方發送得標信件詐欺 假冒其他消費者競標哄抬價格 買方得標後假借其他理由加價
網路購物詐欺	賣方	架設外國購物網站詐欺 收到買方轉帳後之詐欺
	買方	藉故不付款 收到商品卻要求退費 假冒買方向賣方匯款而騙貨
商業金融詐欺		網路銀行轉帳詐欺 至信用卡公司竊取個人資料後詐欺 冒牌銀行網路詐欺 網路老鼠會詐欺
網路遊戲詐欺		買方以交易金額騙賣方 假裝網路遊戲公司進行詐欺 僞稱好友並詐欺
色情網站詐欺		國際數據機撥號 提供免費網頁詐欺
其他		網路交友詐欺 網路虛設行號詐欺

資料來源：曾百川，2006

二、網路犯罪類型

網路犯罪類型可分爲兩種，茲分述如下：

第一、以電腦作爲犯罪之場所：所謂以電腦作爲犯罪場所，是指犯罪行爲是在電腦（網路）上進行的，亦即，犯罪行爲是在電腦上發生的。例如，在電子佈告欄（BBS）上，誹謗或公然侮辱他人；又如藉著網路，散布或販

賣猥褻圖畫，該散布行爲是在電腦上發生的。雖然，網路只是一個虛擬的場所，並非物理意義或實體意義的場所，但是，隨著網路時代來臨，有些在虛擬場所所作的行爲，也可以達到如同在實體場所所作行爲的效果，甚至，因爲網路快速大量傳播的特性，在虛擬場所，所作的犯罪行爲，其殺傷力，往往比在實體場所來得大。不過，因爲這部分犯罪因爲證據清楚，而且不難從IP(Internet Protocol Address)地址追查出涉案人。所以這部分讓警察機關負責是合理的，唯若更多警察有這方面的電腦常識，較容易發揮功能。

第二、以電腦作爲犯罪之客體：網路興起後，電腦系統容易成爲犯罪客體，換句話說，電腦系統容易成爲攻擊的目標，此種情形，例如：電腦駭客入侵他人網路系統並施放病毒，即屬之，此爲新興的犯罪，因爲網路就傳統的犯罪行爲客體而言，可以說是一種新的犯罪客體。但是，以電腦作爲犯罪客體之情形，也同時有可能是一種傳統犯罪。例如，電腦駭客在甲的網路系統中放入後門程式，並且威脅甲需交出一百萬元，否則該程式會在一小時內，將甲電腦系統的重要檔案毀掉。這可構成傳統的恐嚇取財罪（刑法第346條）。

有關網路駭客犯罪涉嫌者，有些是有金錢動機，有些則非金錢動機，如果受攻擊的對象是政府部門，目前係由法務部調查局負責偵辦。如果受駭客攻擊的客體係非政府部門，類係警察機關的管轄範圍。不過，就駭客涉案人而言，不一定會限定只攻擊政府或私人部門，因此警察機關與調查局其實也有合作的必要性與重要性。例如，面對駭客攻擊，美國政府與民間可能也感覺束手無策，因此美國電信公司決定聘用「天才駭客」爲資安顧問[13]。這種用人的創新作法，在台灣政府部門不見得可行（主要因爲在公部門任職需通過國家考試），但私部門已有前例。例如在1999年時，陳盈豪以尚在大同大學四年級就讀的身分，製造病毒程式，導致全球六千萬元電腦當機。其能力受到資訊業者肯定，目前任職於民間公司[14]。

重點在於，電腦（網路）犯罪具有以下六種特性（內政部警政署刑事警察局，2009）：第一，散布迅速；第二，身分易藏；第三，證據有限；第四

[13] http://www.libertytimes.com.tw/2009/new/mar/26/today-int6.htm，瀏覽日期 2009/10/24。
[14] http://forum.slime.com.tw/thread176155.html, 瀏覽日期 2009/10/24。

，適法困難；第五，跨國管轄；第六，偵查不易。由於前述六種特性，形成對政府職能與角色之挑戰，因爲政府公務人員有其既定的工作規範，不易對抗網路犯罪；不過，由於網路犯罪仍有偵查的必要性，爲發揮政府對抗網路犯罪，政府的職能與角色應進行彈性調整。雖然我國電信、傳播及資訊三者之技術與服務匯流發展快速，爲因應全球性之數位匯流發展及監理革新趨勢，以及整合現行通訊及傳播分散之事權，政府乃依通訊傳播基本法與國家通訊傳播委員會組織法，規劃成立電信資訊傳播整合監理機關，並於95年2月22日，正式成立國家通訊傳播委員會（NCC），以收事權統一，政策整合之綜效，開啓了我國通訊傳播監理的歷史新頁，並成爲我國通訊傳播監理的最高機關。

我國網路管理分散於各機關網管人員，關於網路犯罪之管轄偵查機關，目前中央以刑事局科技中心（結合資訊室、偵九隊、研發室、通訊監察中心之任務編組）和調查局資訊室爲主，地方則是各縣市警察局（刑警大隊科技偵查小組任務編組）和各調查處站爲主，機關雖有中央地方之分，但是網路犯罪技術日新月異，因應局勢的任務編組形態，實已不足應付。網路犯罪已經成爲政府必須重視的問題，97年1-6月（內政部警政署，2008），臺灣電腦網路犯罪案第一名爲網路詐欺（97年1-6月電腦網路犯罪發生數12,007件），而電腦網路犯罪發生數，主要爲網路詐欺案4,981件（占41.48%）爲最多。因該問題牽涉中央與地方政府之分工合作，網路已經無所不在，中央與地方政府，在實務運作上，因爲各部會（局處、單位）各有所司，可能存在許多整合的盲點。

因此，透過網路犯罪防治之政府職能與角色分析（實證）研究，可以找出理想的政府職能與角色分工，或提供政策建議。爲避免研究問題過大，本研究將以網路詐欺爲主體，並輔以其它類型網路犯罪進行研究。鑒於個人資料於網路遭人竊取販賣及外洩個資，被犯罪集團利用於詐欺的犯行相當嚴重，導致各種電話詐騙行爲橫行，影響社會治安甚鉅，成爲本研究的重點之一，但爲求週延亦會加入其它案例進行比較。

我國雖針對網路犯罪防治長期投入公共資源，也健全相關法令的規定，例如現行「電腦處理個人資料保護法」的制訂、修改等。但網路犯罪的狀況卻是每況愈下，駭客侵入、個資洩漏、網路詐欺等逐年升高，引發許多社會

治安問題與社會成本損失。面對前述迫切的網路犯罪問題，亟需要各階層政府及跨機關、跨部門的合作，結合中央與地方各方的資源，共同釐清政府在此類議題中應有的職能與角色，期能爲如何消彌並有效解決前述迫切的公共治理議題，提出立即可行及中長期的政策建議。

「網路犯罪」是犯罪學上的新犯罪型態，學者間對於「網路犯罪」亦無明確的定義，網路犯罪亦常與電腦犯罪混爲一談。網路犯罪固屬電腦犯罪的延伸，卻獨具有一種利用網路獨有的特性，而爲犯罪手段或犯罪工具之網路濫用行爲，「網路犯罪」應爲電腦系統與通訊網路相結合之犯罪行爲，其較偏重於網路科技的應用，而具有網路性質的犯罪，其與「電腦犯罪」只偏重於電腦或相關設備之使用及破壞之犯罪行爲是有區別的，是利用網路特性，以網路或連結在網路上的電腦和通信傳輸系統作爲犯罪客體、手段、工具和場所的一種犯罪行爲，屬於「透過網路所提供的服務型態來從事非法之電腦犯罪行爲」[15]。

以美國白宮「網路非法行爲工作小組」（President’s working group on unlawful conduct on the Internet）對網路犯罪的分類方式，網路犯罪可以區分爲三類[16]：

1、犯罪目標：如駭客入侵、恐怖主義者攻擊電腦、飛客盜打電話、阻斷服務及郵件炸彈等。

2、儲存裝置：如盜取通行碼、信用卡號碼、專利資訊、商業軟體等。

3、通訊工具：利用電子郵件進行威脅、騷擾、追蹤、誘騙或散佈色情圖片等行爲。

[15]林宜隆撰，「網路犯罪問題及其偵防機制之探討」，警學叢刊，第三十一卷第一期，民 89 年 7 月。
吳國清、廖有祿、高大宇等人撰，「電腦犯罪與執法認知之探討」，中央警察大學，警學叢刊，第三十一卷第三期，民 89 年 11 月，頁 127-187。
沈榮華著，網路犯罪相關問題之研究，國防管理學院法律研究所碩士論文，九十一學年度。

[16] The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of Internet. http://www.usdoj.gov/criminal/cybercrime/unlawful.htm

許慈健[17]以「行爲人以網路爲標的、場所或工具，在網路空間裡進行任何致生嚴重危害社會之刑事不法行爲」之定義，將網路犯罪區分：爲以網路爲犯罪客體、以網路爲犯罪場域、以網路爲犯罪工具的三種類型，此分類方式基本上與美國白宮網路非法行爲工作小組對網路犯罪之分類相近：

1、以網路爲犯罪客體之犯罪類型

行爲人利用網路的特性，將「網路」本身或連結在網路上的電腦系統，做爲實施犯罪的對象，是網路犯罪中最典型的一種。其犯罪行爲形態主要可分爲入侵型犯罪、攻擊性犯罪、攔截型犯罪及病毒之散佈等四種類型，其特徵是「行爲的目的在於破壞網路本身及電腦系統」，而此類型犯罪之行爲人通常稱之爲「電腦駭客」(hacker)。

（1）入侵型犯罪：行爲人透過網路連結的特性，入侵他人的電腦系統後，再從事各種不法活動，例如竊取、更改電腦檔案資料。

（2）攻擊性犯罪：行爲人透過網路作爲跳板直接攻擊網路系統，以破壞網路系統或使之陷於癱瘓。

（3）攔截型犯罪：行爲人以截取在網路線上傳輸之網路資料方式，進而實施竊聽、攔阻、僞變造或干擾等行爲。

（4）散佈病毒型犯罪：行爲人設計電腦病毒，透過網路傳輸至不特定人或特定人之電腦系統，藉由不斷的複製或感染，進行破壞、干擾網路及電腦系統之行爲。

2、以網路爲犯罪場所之犯罪類型

利用網路之空間特性，在網路虛擬空間內實施現實社會的犯罪行爲。例如網路色情、網路賭博、網路誹謗、網路恐嚇、網路販售違禁物品及網路煽惑犯罪等。

（1）網路色情：包括在網路上張貼、傳送色情或猥褻性質的圖片或文字等資訊，在網路上媒介色情交易或進行網路援交等形態。

[17] 許慈健撰，網路犯罪偵查與我國關於網路服務提供者協助偵查法制之研究。國立交通大學管理學院在職專班科技法律組碩士論文，94 學年度。

（2）網路賭博：透過網路所提供的虛擬賭場，在網路線上進行賭博的犯罪行爲。

（3）網路誹謗：透過網路或電子郵件散佈不實的內容給不特定人，致他人的名譽遭受損害之行爲。

（4）網路恐嚇：透過網路散佈或以電子郵件傳遞威嚇的言語或文字，使不特定人或特定人心生畏怖之行爲。

（5）網路販售違禁物品：透過網路討論區張貼訊息或利用電子郵件傳遞訊息，在網路上兜售違禁物品，例如槍枝與毒品之行爲。

（6）網路煽惑犯罪：利用網路通訊的功能，於網站上張貼或以電子郵件傳遞違法犯罪的訊息，煽惑他人犯罪。

（7）侵害智慧財產：包括盜拷、散佈軟體、侵害商標及重製他人著作…等。

3、以網路爲犯罪工具之犯罪類型

利用網路之通訊功能所進行之犯罪行爲，其與以網路犯罪場所之犯罪類型不同處，在於後者係利用網路虛擬空間之特性，直接將犯罪行爲施行於網路上，而前者則是藉由網路爲犯罪工具針對特定目標所進行之犯罪行爲。其犯罪型態包括網路詐欺、網路竊盜、網路洗錢、網路洩密及網路釣魚等。

（1）網路詐欺：透過網路或電子郵件，刊登或傳遞不實的訊息，致不特定人受騙，而從中牟利的犯罪行爲。例如虛設行號、詐騙帳號、網路情人等類型。

（2）網路竊盜：透過網路通訊的功能從事「虛擬物品」竊盜之犯罪行爲。

（3）網路洗錢：利用網路銀行或各種新支付系統進行交易之機會，從事洗錢犯罪活動。

（4）網路洩密：透過網路將機密的資料傳遞給特定人或不特定人，藉以牟利之犯罪行爲。

（5）網路釣魚：「網路釣魚」（phishing），乃飛客[18]（phreak）及釣魚（fishing）的結合，是目前全世界網路犯罪中最常出現的手法，主要攻擊電子商務。常見的手法包括偷帳號、偷線上寶物及盜領網路銀行存款，及藉下載修補程式，植入木馬進行遠端遙控，竊取電腦中的資料，窺探隱私。

第二節 研究目的與問題

在網路世界中凡走過必留痕跡，就純技術而言要找到犯罪證據並非難事，問題在於業者電磁記錄的留存與資料提供，以及藉由所在網路上留下的痕跡追查出現實世界中的身份，這部分是電腦稽核紀錄的問題，與業者的管理有關，包括包含網路服務業者（Internet Service Provider, ISP）、網路內容提供（Internet Content Provider, ICP）、網路應用服務平台（Application Service Provider, APS）的主管機關與管理問題，可能是比較複雜，可能的原因在於這些網路管理機關並非犯罪偵查機關，沒有責任與權力進行網路犯罪偵查；甚至有些網路管理的跨國經營業者，可能沒有誘因配合國內偵查機關進行犯罪查緝，因此存在網路犯罪偵查的漏洞。

所以，本研究「網路犯罪防治體系之政府職能與角色分析」的定義是：政府之職能與角色如何定位，可以達到網路犯罪預防與偵查的目的，至於網路犯罪的意義如前所述，包括透過網路竊取個人資料，以及與網路相關消費行爲習性所衍生出各種犯罪。如此定義的原因在於，網路犯罪係新興的犯罪模式，政府因法令規定跟不上科技進步的腳步，使得政府整體職能角色與分工存在盲點，因此有必要進行這方面的研究。在此定義下，本研究並將找尋具代表性之網路犯罪實際案例，進行政府職能與角色之研究。

本研究的目的（網路犯罪），在針對我國網路犯罪洩漏個資的資訊安全事件，以及所衍生出的各種網路犯罪，透過重要個案，從政府（含中央與地方）相關部門進行研究，探討相關政府部門職能與角色，是否發揮應有功能

[18] 飛客（Phreak）最初是指一群探索電話網路技巧的玩家，利用欺騙電話公司的電子裝置，免費打長途電話、行動電話。

。而所謂相關部門，包括：國家通訊委員會、教育部、內政部（警政署，特別是警政署資訊室、刑事局偵九隊）、國安局、地檢署、調查局；地方政府主要指縣市政府（含教育局、警察局、建設局）等；民間組織主要指相關之營利與非營利公司（主要係擁有龐大個人資料之網路購物公司、信用卡公司、銀行或其它公司等）。

因此，本研究之目的爲：

（一）網路犯罪在我國當前之嚴重性探討。

（二）在網路犯罪防治方面，政府職能角色該如何地扮演。

（三）在網路犯罪防治之法制上，應如何從事。

（四）在網路犯罪之防治上，中央政府與地方政府應從事之角色扮演爲何。

以下分別探討之。

第三節 政府防治網路犯罪現況

一、目前我國政府所架構之職能系統

我國政府針對網路，目前所架構之政府職能系統，分別如下：

1、網路化政府中程計畫：配合1996年網際網路世界博覽會（EXPO96），我國開始推動以網際網路爲基礎的電子化政府，啓動政府資訊建設的新里程，並研擬相關計畫及配合措施，全面推動政府機關運用網際網路提供政府資訊及服務。行政院研考會於1997年11月策訂「電子化／網路化政府中程計畫（1998至2000年度）」，透過各機關的通力合作，推動政府網際網路骨幹網路、骨幹網路基礎服務、「村村有電腦、里里上網路」、「課股有信箱、訊息瞬間通」等重要計畫（ 電子化政府，2004） 。

2、知識經濟發展計畫：2000年8月行政院核布實施「知識經濟發展方案」，政府在推動知識經濟發展計畫中，將網路建設列入其中的重點項

目，包括建構網際網路應用之基礎環境、擴展資訊科技及網際網路在生產及生活上之運用；在建構網際網路應用之基礎環境上，主要推動內容包括加速寬頻網路建設及電信市場開放，建立競爭機制創造優良的電子商務發展環境；加速網際網路相關法規及制度之建構，以確保網路交易安全及公平競爭環境；規劃整合型計畫以使實體配送與虛擬交易環境相互配合，以健全全球運籌的運作體系；促進跨電信及媒體事業整合，並規劃跨業競爭環境之規範；至2001年底，以具競爭性的價格，提供國人單向1.5Mbps之頻寬，滿足寬頻上網之頻寬需求，並使寬頻上網比例達百分之十五以上；至2005年底，以具競爭性的價格提供國人單向6Mbps之頻寬，滿足多媒體通信之頻寬需求，使寬頻上網比例達百分之五十以上（知識經濟發展方案，2003）[19]。

3、國家資訊通信基本建設計畫：國家資訊通信基本建設計畫，其內容係參酌NICI民間諮詢委員會2001年度策略規劃會議之結論：「勾勒資訊化優質社會的藍圖」之精神，並邀請相關學者、專家詳細討論及審慎規劃而成，以ｅ- 臺灣爲發展願景，運用資訊科技，以電子化政府、產業電子化、網路化社會及基本建設爲推動架構，構建資訊化優質的社會（電子化政府，2004）。

4、電子化政府推動方案：2001年4月行政院研考會會同各機關延續「網路化政府中程計畫」策訂「電子化政府推動方案」，透過健全的網路基礎環境，致力推動政府與政府間（G2G）、政府與企業間（G2B）及政府與民眾間（G2C）的網路服務。

5、挑戰2008年國家發展重點計畫：行政院於2002年5月通過「挑戰2008：國家發展重點計畫」，進一步以ｅ化政府計畫作爲核心，結合600萬寬頻到家、ｅ化生活、ｅ化商務、ｅ化交通等計畫共同打造「數位臺灣」，並與「ｅ世代人才培育」、「文化創意產業發展」、「國際創新研發基地」、「產業高值化」、「營運總部」等重點投資計畫緊密結

[19]知識經濟發展方案，取自 http://www.cedi.cepd.gov.tw/document_info.php?fPath=1_180&documents_id=370，visit on 2009/08/16。

合，推動政府資訊建設，凸顯政府推動電子化政府的決心。另爲提振經濟景氣，增加就業機會，促進經濟成長，總統府於2003年5月公布「擴大公共建設振興經濟暫行條例」，並將行政「ｅ化計畫」納入其中，透過11項行政ｅ化計畫之推動，期能加速達成電子化政府推動方案及國家發展重點計畫之目標（電子化政府，2004）。

二、綜合實施成果

至2004年底共有138項重點計畫完成，重點如下：全國行政機關已全部連接網際網路；政府網站設置普及率85％、公務人員使用電子郵遞普及率94％、使用瀏覽器普及率98％；建立我國政府憑證總管理中心，除了政府憑證管理中心之外，自然人及工商憑證管理中心均已正式營運；建立各機關網路安全通報及防護機制，防止駭客入侵之各項作業應全力配合，確保我國資訊通訊的安全；推動公務人員網路學習，由行政院人事行政局、行政院研考會及行政院主計處分別建立線上學習（e-learning）網站；健全電子認證服務機制；落實推動戶籍、地籍謄本減量；強化網站經營管理與安全隱私保護等（電子化政府，2004）。

1、國家通訊傳播委員會NCC之成立與權責範疇

爲因應全球性之數位匯流發展及監理革新趨勢，以及整合現行通訊及傳播分散之事權，政府乃依1998年行政院第8次電子、資訊與電信策略會議（SRB會議）建議，規劃成立電信資訊傳播整合監理機關—國家通訊傳播委員會NCC，以收事權統一，政策整合之綜效。

ＮＣＣ成立時間短，運作方式難免不是非常成熟。所以，ＮＣＣ所作的管制處罰（分），可能因政策配套不足或管制機制仍不完善，因而存在爭議。從過去案例顯示，ＮＣＣ的確存在許多管制盲點，以目前本研究之「網路犯罪治理」研究爲例，初步發現虛擬社會的網路犯罪並無主管機關，僅有末端的警察出面「管轄」或作犯罪之處理，因此不存在整體網路犯罪治理的機制。

就網路犯罪屬性而言，係屬於資訊安全管理的一部分，ＮＣＣ應爲主管機關，而且也擁有許多資源與管制權力。然而，ＮＣＣ卻未被賦予相對的管制責任，未能針對網路相關業者進行必要的規範，使得犯罪源頭的網路管理

出現真空。目前雖「行政院資通會報」應付「重大」的網路安全事件，但僅聊備形式，難以從管制的源頭遏止網路犯罪。換言之，ＮＣＣ對於許多政策議題上，在管與不管之間，存在許多模糊地帶。

再詳細說明，臺灣屬於大陸法系，背後的精神是「罪刑法定主義」，也就是法無規定者不罰或不予管制；而英美法是海洋法系，係以判案作爲管制依據。顯然，ＮＣＣ對於第一次的管制決策，可能因爲缺乏案例，或缺乏法律規範，導致行政處分之不夠周延。在此情形下，可能就得尋求配套措施，降低處分結果的負面效應。或者，即便存在（或通過）法律規定，仍可能因爲認知或解讀落差，導致對結果有不同的認定，許多爭議或衝突就這麼發生。因此，雖有國外的管制案例，但因爲制度或文化的差異，同樣存在執行的難處，這也是ＮＣＣ的管制困境。

再就ＮＣＣ的組織體質分析，ＮＣＣ係由原交通部電信總局、郵政總局（郵電司），以及新聞局廣電部門所組成。有些人可能認爲，把業務相近的部門進行結構調整，就可以發揮功能，卻忽略了組織結構的背後，有更重要的組織文化存在。或可以說，ＮＣＣ組織轉化的過程缺乏願景與整體規畫，ＮＣＣ可以說是一部拼裝車，在沒有詳細監督檢查機制設計的情形下，就上路運作，難免因爲許多處分案難以符合業者、社會大眾或其它利益團體的期待。

因此，ＮＣＣ的組織定位還有長路要走，到底什麼該管、什麼不該管，或者管制的程度如何，都有待進一步作制度的設計或磨合。雖然，ＮＣＣ組織法第四條明訂，委員具電信、資訊、傳播、法律或財經專業知識或實務經驗，但實際運作其實比這四個領域要複雜的多。具體而言，ＮＣＣ因爲具有龐大的行政權，益發凸顯監督、救濟、民主審議機制配套設計的重要；也就是說，ＮＣＣ的決策除前述領域外，還涉及政治、社會（文化）、政策與行政管理內涵。

綜言之，ＮＣＣ設立的精神或前提是希望讓該獨立機關獨立於政治之外，主要希望不受政黨掌握。但卻不能因此失去監督與救濟制度的配套設計，畢竟ＮＣＣ仍是在現行系統之下運作，不能自外於政治與行政制度。

2、我國網路犯罪之偵查

我國網路犯罪偵防工作，目前分別由四個單位，法務部高等法院檢察署、內政部警政署、法務部調查局、交通部電信總局與教育部，按職權分工即政策擬訂、犯罪偵防、技術研發及教育宣導，分別隸屬不同單位體系，彼此溝通及聯繫不易，各自爲政，易形成多頭馬車，事權不易統一，缺乏嚴密分層負責指揮系統，難以發揮抗制網路犯罪的最大效益。

三、資安國家標準之制定

資通安全相關國家標準的制定（資通安全產品驗證、管理系統驗證、管理系統認證及資安技術相關標準），如果只是累積過去經驗而無深入研究並與理論結果，成果將受到限制。此外，民間企業在資訊科技水準已有提升，若能進一步結合，同時推動研發高階資通安全產品，及設立資安產品檢驗或測評認證單位，將能提升我國資通安全技術能力與品質。或者，若能針對資安國家通準制定進行研究，將有助資通安全機制的建立，唯這不是本研究的重點。

四、政府現行網路犯罪防治架構

就目前我政府網路犯罪防治架構而言，如圖6國家資通安全基礎建設的角色區分所示，我國在行政院院長召集下（擔任召集人），設有國家資通安全會報，副召集人爲行政院副院長兼。委員包括相關部會首長及北高市長，執行長爲行政院NICI（國家通訊電信發展推動小組），以下再分標準規範工作組（經濟部、研考會、國防部、交通部、財政部）、稽核服務工作組（主計處、國防部、交通部、經濟部、財政部）、資訊蒐集工作組（國科會、中科院、工研院、資策會、相關公協會、民間業者）、網路工作組（法務部、內政部、國防部、交通部）、危機通報工作組（主計處、內政／國防部、交通／財政部、經濟／教育部、衛生署／研考會）、技術服務中心（經濟部、資策會、中科院／工研院、電信所／國防部、交通部／業者）等。國家資通安全會報同時在國家安全會議顧問指導下，進行組織的運作。因此，表面上看來這樣的運作架構是完整的。不過，因爲這樣的組織架構涉及的部會（單位）過多，難免產生協調聯繫上的困難；而且該會報只是臨時任務編組問題，各參與人員的工作承諾難免受到影響。

在實務運作上，刑事警察局負責網路犯罪末端的部分，也就是具有犯罪

事實，而且需要偵查的，多由刑事局偵九隊負責。而目前刑事局亦成立科技犯罪防制中心任務編組，整合刑事局偵九隊、通訊監察中心、資訊室、刑事研究發展室等單位，電信警察大隊亦隸屬於該防制中心。在縣市警察局部分，刑事警察大隊亦多成立網路犯罪小組（任務編組）以應付網路犯罪之偵查。法務部調查局，則亦負責部分網路犯罪業務，主要的業務在駭客攻擊政府部門網頁的部分。警政署另設有165專線電話，以應付層出不窮的電話詐騙事件。至於網路犯罪所衍生的網頁管理、網路購物、金融管理、藥品管理等問題，則又和國家通訊傳播委員會、經濟部、財政部、衛生署等有關係。這部分相關的網路犯罪問題，主要由前段之資通會報處理。

第二章　文獻探討

關於網路犯罪政府職能之角色研究相關文獻至少包括網路犯罪與政府職能與角色兩大領域。重點在於，政府做些什麼？怎麼做？可以發揮網路犯罪預防與偵查的效果。在行政學領域上，針對政府職能與角色，有很多的討論（Wilson, 1989; Shafritz & Russell, 2007; Rosenbloom & Kravchuk, 2005），這些論述，這些文獻也提供很多的政府職能與角色的工具與作法，唯並未就「網路犯罪」進行討論。重點在於，政府職能與角色在於「政府」或「市場」的概念。換言之，針對網路犯罪到底應由政府來管理，或以市場的思維進行規範，所謂市場思維的原義在於政府不主動進行干預或介入，市場背後有一隻看不見的手，會自動進行平衡的調整。

然而，網路犯罪其實是市場失靈的一種（含公共財與資訊不對稱的問題，因爲網路犯罪是公共議題，而資訊不對稱存在於業者與網路者使用之間，而網路使用者又可分爲犯罪嫌疑者與被害者），需要政府介入，或需要政府扮演積極的角色，以彌補政府失靈帶來的問題。只是，政府也可能失靈，或前美國總統雷根經常說的，政府本身即是問題（Government is the problem），政府的問題包括繁文縟節（Red Tape）、利益團體（Interest Group）、民主機制或政治等問題。因此持一主張的學者或實務者，多認爲政府對市場的管制應愈少愈好，政府的規模也是愈小愈好。在此前提下，我們針對網路犯罪，如何進行政府職能與角色調整，而且在不妨礙市場發展的情形下，發揮網路犯罪預防與偵查的效果，的確值得深入研究。

但另一方面，爲能深入探討政府在網路犯罪的職能與角色，必須先瞭解網路犯罪的意義。事實上，「網路犯罪」是犯罪學上的新犯罪型態，學者間對於「網路犯罪」亦無明確的定義，網路犯罪亦常與電腦犯罪視爲同義。網路犯罪固屬電腦犯罪的延伸，卻獨具有一種利用網路獨有的特性，而爲犯罪手段或犯罪工具之網路濫用行爲。從這看法而言，網路犯罪的重點在於網路成爲犯罪工具。或者，「網路犯罪」應爲電腦系統與通訊網路相結合之犯罪行爲，其較偏重於網路科技的應用，而具有網路性質的犯罪。另一方面，「電腦犯罪」只偏重於電腦或相關設備之使用及破壞之犯罪行爲是有區別的，

是利用網路特性，以網路或連結在網路上的電腦和通信傳輸系統作爲犯罪客體、手段、工具和場所的一種犯罪行爲，屬於「透過網路所提供的服務型態來從事非法之電腦犯罪行爲」[20]。

本研究主要以網路犯罪進行問題的建構，而政府職能與角色主要也是從網路犯罪模式或態樣而來，因此下文先從實際網路犯罪案例進行論述，再從這些案例探討政府職能與角色。

第一節　網路犯罪之基本理論

網路犯罪根據古典學派犯罪學之理性選擇犯罪理論(Rational Choice Theory)及日常活動犯罪理論(Routine Activity Theory)即可說明其發生原由，亦是本文所要探討的重要依據。前者強調犯罪事件特殊化及犯罪人專門化，而後者強調犯罪的動機和犯罪人可說是一常數，亦即社會上有固定比例的人總會因特殊的理由(需要、貪婪及好奇等)而犯罪。再者，美國犯罪學者L. Cohen 與 M. Felson在1979年所提日常活動犯罪理論，其認爲犯罪是人們日常生活型態的一種結果，且犯罪事件要發生必須有三種要素(M-O-P)在時空的聚合：(1)有動機及能力的犯罪者(Motivation)、(2)合適的犯罪標的物(Object) 及(3)抑制犯罪發生者的不在場(Protect)，如圖一所示。(E1，E2及E3分別表示家庭環境，學校環境及社會環境)。由於網際網路使用普及，已成爲家庭、學校、社會等不同環境日常生活的一部分。因此，可以預期的是，有網路犯罪動機與能力的犯罪者與合適的犯罪標的物將愈來愈多；而因網路使用有其隱密性，使得抑制犯罪發生的因素變弱。這些因素，都導致網路犯罪愈來愈嚴重。

[20]林宜隆撰，「網路犯罪問題及其偵防機制之探討」，警學叢刊，第三十一卷第一期，民 89 年 7 月。
吳國清、廖有祿、高大宇等人撰，「電腦犯罪與執法認知之探討」，中央警察大學，警學叢刊，第三十一卷第三期，民 89 年 11 月，頁 127-187。
沈榮華著，網路犯罪相關問題之研究，國防管理學院法律研究所碩士論文，九十一學年度。

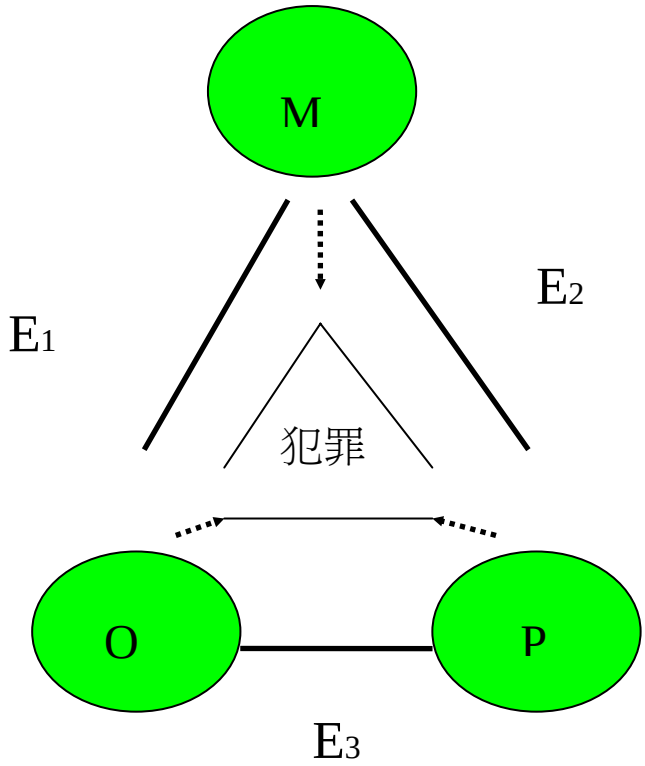


圖 3　日常活動犯罪理論之 M-O-P 犯罪三要素動態模式

資料來源: 林宜隆，2006

綜言之，從上述日常活動M-O-P理論，得知下列一個推論：「當網際網路使用愈普及，則網路犯罪愈是必然發生」，爲防止網路犯罪發生，必須相對提高網路安全科技(如防火牆 (Firewall)設置)(即代表P)、儘速制定網路使用管理辦法(即代表M)或資訊使用相關法令(即代表O)，以及降低生活環境存在的網路犯罪風險等，以確保資訊網路系統之安全。而資訊網路系統安全的潛在威脅，主要包括環境(即代表P&O)及人員(即代表M)兩方面。

第二節 政府職能角色與政策形成、規劃與執行理論

一、政府防治網路犯罪職能與角色之定義

網路的發明不僅促進了現代人類生活上許許多多的便利，更使得人們可以藉著其所獨有的功能及特性，從事一些在以往社會中不所能做到的事，如知曉瞬息萬變的世界新知、從臺灣到美國下單購物、提供視訊會議等等；然而在探討網路之前，我們必須先了解網路的意義、起源及演進過程，並了解其所具有的獨特特性，方可在研討網路犯罪時，能有更深一層之認識與了解。至於本研究「網路犯罪防治之政府職能與角色分析」的操作型定義是：政府之職能應如何加強防範經由網路被竊取的個人資料或是消費行爲習性所衍生出各種犯罪。本研究並將找尋具代表性之網路犯罪實際案例，進行政府職能與角色之研究。

理論上，公共政策目標的確定是政策規劃的首要工作。現實上，真正要做到政策目標的明朗化，還不是想像中的容易；政策制訂者常常在政策目標的抉擇上面臨進退維谷的困境，主要是因爲內外在條件、主客觀因素的影響和限制，另外，政策目標本身往往也是多元、相互衝突的價值（competing values）選擇。儘管如此，政策目標的釐清和確認毫無疑問地仍是政策規劃最必要的工作。政策目標的定義是政策主體爲了解決政策問題所要達成的目的、指標和效果；從這個定義來看，它應可歸納爲二項特性，即問題的針對性和未來的預期性（政策推動所追求的情境變化或價值觀的轉化）。

公共政策目標的分類，從社會需求的優先地位來看，公共政策目標可分爲基本目標和具體目標；具體目標一般又是從基本目標衍生出來，這種關係就如憲法與法律的地位關係。基本目標是關係到一個國家或社會生存與發展的基本價值，可以說幾乎是普世追求的目標；它包括安全（人身安全、財產安全、社會安全、國家安全、資訊安全）、自由（具體反映在市場準則，也涵蓋效率）、平等（即公平的意義，涵蓋機會公平、分配公平及考量自然差異性的實質公平）等。然而，這些價值的追求有時會產生排斥或衝突，如公平與效率、自由與安全；因此，在確立政策目標的時候必須要非常謹慎，應以宏觀的思維做整體的考量。

其次是關於具體目標的內容，如果從不同的層面來看，也會有不同的分

類。我們可以分別從時間、空間、議題及服務的焦點群體（target group）的角度來探討。從時間的角度，政策目標可分爲長期目標、短期目標、中長期目標、中短期目標等；從空間來看，政策目標可分爲全國性目標、地方（區域）性目標、國際性目標；從議題而言，政策目標有政治性目標、管理性目標、經濟政策目標、文化政策目標、社會政策目標；從服務的焦點團體來看，政策目標可分爲普遍性公益的政策目標及特殊性（弱勢團體）的政策目標。

如果依此做綜合考量，我們將可以歸納出確定政策目標的原則爲：（1）運用科學思維及方法分析客觀情勢，從實際的公共政策問題去思考，確立政策目標的可行性及可成性；（2）因爲政策目標具有未來的預期性，所以應該以前瞻性的眼光和思維來確立政策目標，簡單的說就是要有尋求「願景」的思維；（3）由於政策目標追求的價值常形成衝突或排擠的現象，政策目標的確立就必須要有整體觀，要從整體的價值系絡去協調和規劃；（4）既然政策目標是政策制訂一切行動所依循的基礎，那麼它的確立就必須具體、明確；包括相關的概念、時間要求、目標內容、焦點對象等都要清楚、明白的界定或說明，務必做到「表達準確、含義清楚單一、各項要求具體詳細」。

公共網絡政策方案的規畫即爲一般所稱的「狹義政策規畫」，具體而言是指在公共問題進入相關的政策議程之後，爲了達成政策目標，政策主體針對該目標進行研擬、評估及執行相關網路政策方案的行動進程。首先，我們應該瞭解這個政策階段所說的「政策主體」是誰。根據Larry N. Gerston的說法，這個「政策主體」包括政府（包括總統或總理、官僚體系）、立法機關、司法機關、利益團體、社會團體等。另外，隨著民主社會的推進，也有學者提出屬於次政府團體（包括　　政府的執行機構、國會的委員會和社會的利益團體）結合而成的「鐵三角」組合。還有從議題網絡（issue network）及政策網絡（policy network）的現代民主化運作所勾勒出來的「倡議聯盟」。從以上種種，我們概可以把政策主體定性爲「政府主導下的多元組合」。

至於網路政策方案的規劃也應該從它的特性及功能找出可依循的設計原則：（1）既然網路政策方案是爲了達成目標，那麼規劃上就必須扣緊目標；（2）由於現代民主化的社會具有快速變遷的特性，再加上人性的善變特性

，而政策的進程有時繁複、緩慢，所以網路政策方案的規劃應採取多重方案的原則。所謂「條條大路通羅馬」，各路景緻各宜，提供決策者評估與選擇；（3）在多重方案的原則下，必須要各方案彼此獨立，否則決策者如何選擇；（4）時代在變，社會也在快速進化，方案的設計當然要有創新的思維，才能更有效地解決快速變化的公共政策問題；（5）方案的設計更重要的是要可操作，也就是依照既有的條件要有可行性。

網路政策方案的評估工作包括二項內容，即評估與方案建議，也就是對各項網路政策方案的成本與效果做分析、預測和比較，然後提出建議。然而，既然談到比較，那麼就必須確立標準；而毫無疑義地，網路政策方案的評估標準應該是從政策目標延伸而來的。當前對於這項評估的工作已有一些普遍性的標準：目標可成性（效能）、技術可行性、財務可行性、政治可行性（包括正當性、合法性、回應性、公正性）、行政操作性（組織、人力、通訊、權威）等；然而一般來說，很少有網路政策方案能夠同時滿足上述所有標準，政策規劃者必須根據實際的情況列出其優先次序，然後選用。

一般稱網路政策方案的選擇爲決策，是決策者根據政策規劃者所擬定的方案和建議，考量各層面的相關事項，按照一定的決策制度和程序規範，做出決定性選擇的過程。由於決策對國家和社會的重要，我們就不能不瞭解「決策主體」到底有那些人。現實運作上，隨著政策制定過程的推進，相關的參與者也趨於減少，到了決策階段，大部份非國家機構的參與者將被排除，只有部分政治人物、法官和依法授權執行決策的政府官員。

顯然，決策者是公共政策的最終決定者，相對來說，他的職位也較高，不僅擁有資訊的優勢，也占有眼光的高度，總的來說，在決策的工作上，決策者應該可以比別人做得更好，但同時也會有一步錯則全盤皆輸的危機。所以，決策者最好能依循科學化、民主化、制度化及合法化的要求：要尊重科學分析、平衡各方利益、發揮理性及果斷的能力、嚴守政策內容及決策程序的合法化。

二、政策形成規劃與執行理論

公共政策一般分爲政策形成、規劃、執行與評估等四個階段，四個階段

都存在政治的影響或介入。而在政策形成之前，必須先形成議題，才可能形成政策(Weimer & Vining, 2005)。雖然網路犯罪相當嚴重，不只是民眾關心的議題，也是政府非常重視政策議題。但什麼樣的因應政策，以及如何操作化，成爲重要的政策規劃與執行重點，而且也有許多研究空間。而其重要內涵主要以政府職能與角色的方式呈現，問題在於，政府職能與角色之扮演或執行是否存在應有之成效。

政策方案的具體規劃，當政策議題被啓動，順利由「系統議程」邁入「制度議程」，政策主體就必須開始推動政策方案的具體規劃，以利政策的進程能夠順利完成；這項工作或進程階段，也就是一般所謂「狹義的政策規劃」。簡單的意義就是，用適當及可接受的行動計劃來處理政策議題，並進一步將其立法。而這整個工作的核心就是要先確立政策議題的「期望價值」，也就是「公共政策目標」。政策執行過程所涉及之問題至爲複雜，如執行機關人力運用與資源分配不當、持本位主義、法規不合時宜、或未能充分反應民意等，均對政策執行產生不利影響，應如何強化政策執行，應深入探討。

政策方案的評估工作包括二項內容，即評估與方案建議，也就是對各項政策方案的成本與效果做分析、預測和比較，然後提出建議。然而，既然談到比較，那麼就必須確立標準；而毫無疑義地，政策方案的評估標準應該是從政策目標延伸而來的。當前對於這項評估的工作已有一些普遍性的標準：目標可成性（效能）、技術可行性、財務可行性、政治可行性（包括正當性、合法性、回應性、公正性）、行政操作性（組織、人力、通訊、權威）等；然而一般來說，很少有政策方案能夠同時滿足上述所有標準，政策規畫者必須根據實際的情況列出其優先次序，然後選用。

一般稱政策方案的選擇爲決策，是決策者根據政策規畫者所擬定的方案和建議，考量各層面的相關事項，按照一定的決策制度和程序規範，做出決定性選擇的過程。由於決策對國家和社會的重要，我們就不能不瞭解「決策主體」到底有那些人。現實運作上，隨著政策制定過程的推進，相關的參與者也趨於減少，到了決策階段，大部份非國家機構的參與者將被排除，只有部分政治人物、法官和依法授權執行決策的政府官員。

顯然，決策者是公共政策的最終決定者，相對來說，他的職位也較高，

不僅擁有資訊的優勢，也占有眼光的高度，總的來說，在決策的工作上，決策者應該可以比別人做得更好，但同時也會有一步錯則全盤皆輸的危機。所以，決策者最好能依循科學化、民主化、制度化及合法化的要求：要尊重科學分析、平衡各方利益、發揮理性及果斷的能力、嚴守政策內容及決策程序的合法化。

第三節　網路犯罪案例分析

網路犯罪係新興犯罪，而且又具有各種不同的模式，因此政府職能與角色難以在短時間內調整。爲就網路犯罪有深入瞭解，下文首先針對網路犯罪進行定義。

一、網路犯罪之意義

「網路犯罪」，主要係利用電腦系統之操作進而連結至網路，才能進行犯罪之行爲，所以有學者認爲其係「電腦犯罪」中的一部分；也有將網路犯罪與電腦犯罪混爲一談，因網路犯罪係電腦犯罪中藉由網路之管道，而達犯罪目的，所以認爲網路犯罪是電腦犯罪中逐漸衍生出來的一種犯罪型態。[21] 主要因爲科技的發展與電腦及網路使用的普及，帶給我們極大的便利，卻出現了一些利用網路來從事犯罪行爲之人，這些犯罪帶給人們的損害，較以往傳統犯罪更是爲甚，所以便稱此類犯罪爲「網路犯罪」。故「網路犯罪」應爲電腦系統與通訊網路相結合之犯罪行爲，但其較偏重於網路科技之應用，而具有網路性質的犯罪；也就是說行爲人故意或過失所違犯的犯罪行爲，應具有網路之特性者，始可謂爲網路犯罪；此爲與電腦犯罪只偏重於電腦或相關設備之使用，及破壞之犯罪行爲有所區別。

要如何爲網路犯罪做一個最爲適當的定義，可說是見人見智；有學者認爲以網路爲犯罪工具時，應排除於網路犯罪之外[22]，實務上之見解亦有此一

[21]馮震宇研究主持「網路使用犯罪問題及預防措施之研究」行政院研究考核委員會編，民國八十九年四月，第九頁。
[22]蔡美智著「談網路犯罪」資訊法務透析，民國八十九年一月，第三十六頁。

說[23]；本研究以爲所謂的「網路犯罪」，並不是專指某一種特定的犯罪行爲的類型，而是對於網路活動所涉及個人資訊流失，即爲一種犯罪方式或現象之類型；若將以網路爲犯罪工具之類型排除於網路犯罪類型之外者，吾見以爲這樣對於網路犯罪之定義則不夠周延完備，亦難以包含所有網路犯罪之類型，故吾人認爲對此應採廣義之見解，即不限於利用網路之特性所爲之犯罪行爲，尚應包括單純利用網路作爲犯罪工具或媒介者；換言之，於犯罪行爲人利用網路從事犯罪行爲時，即犯罪行爲人以網路或連結在網路上的電腦系統作爲犯罪工具或犯罪場所或作爲犯罪客體的犯罪行爲時，亦將之歸納爲網路犯罪範圍內較爲妥適[24] 。

二、網路犯罪之特質與分類

在政府用心經營下，我國網路建設一日千里，每年上網人數都扶搖直上，使用者也朝向年輕族群發展之趨勢。據統計，目前國內上網人口已超過1200萬人，其中12~30歲占90%以上，家庭使用寬頻上網比例接近83%，每天都要上網的人幾達64%。顯示我國已朝向高度資訊化、網路化發展。

電腦網路犯罪乃係因資訊發展後始新興的犯罪型態，其特質與傳統犯罪類型有所差異，一般而言，網路犯罪應具有以下之特質與分類（李柏宏、廖有祿，1996）：

（一）網路犯罪之特質

以下就網路犯罪之特質與分類，網路犯罪乃係因資訊發展後始新興的犯罪型態，其特質與傳統犯罪類型有所差異；一般而言，網路犯罪應具有以下之特質：

1、係利用電腦之特性遂行其犯罪目的：網路犯罪並非專指刑法中之某

[23]張紹斌著「電腦犯罪及網路犯罪概述」資訊安全通訊，九十年十二月，第三十二頁。

[24]如堅持網路犯罪必須具有網路之特性者，則以網路爲犯罪工具者，雖類似持刀搶奪之刀爲工具一般，惟網路並非像刀僅得爲威嚇他人使之心生畏懼之工具，因網路所獨具特性，包括高效率性、隱匿性、開放性及犯罪黑數高等特性，讓利用網路爲犯罪工具從事傳統犯罪之行爲人與日劇增，也因其特性對其他人民權利的侵害更較一般傳統犯罪更爲重大、影響更爲廣泛，所以網路犯罪之行爲人雖然係以網路爲工具，但此工具應不得與傳統之犯罪工具相提並論，就其特性而言，亦應認爲其有網路之特性，故應係屬網路犯罪之一環。

些犯罪類型，絕大多數犯罪均可能透過電腦的特性予以實施，所謂電腦之特性，包括：分散性、開放性、互通性、隱密性、立即性等

2、行爲與結果間之時間與空間的區隔：網路犯罪的行爲實施與結果發生，在時間與地點上通常均有所間隔，換言之，行爲可能須經過一段時間後，才既遂其犯罪目的，或行爲地與結果發生地有相當大之區隔。

3、難以發現：網路犯罪因係行爲人利用電腦進行犯罪，無聲無息，秘密進行，在本質上即難以發現。

4、白領犯罪：通常電腦犯罪者多半爲程式設計師、系統分析師或職務上常操作電腦者。

5、專業性與業務性：實施電腦犯罪須運用電腦專業知識，此外根據國外統計，大多數電腦犯罪都爲內部員工所爲，故與業務有關。

6、損害性高：近來人們對電腦依賴程度高，如數量龐大、複雜的金額款項全交由電腦管理，一旦遭到侵害，後果不堪設想

7、高犯罪黑數：犯罪黑數（Dark figure of crime）是指已發生但沒有被政府機構登錄的犯罪行爲。據美國聯邦調查局估計，只有百分之一的電腦犯罪爲人所知，而在發現的電腦犯罪案件中，只有百分之四到達偵查機關之手。

8、持續性：行爲人會重複再犯，或犯行本身爲繼續的狀態，整個案件會延續到被發覺爲止。

9、行爲與結果時間和地點分離：此類犯罪後，結果不馬上突顯，且犯罪地點與結果地亦分屬不同管轄，甚至跨國界。

10、偵查與起訴有技術上之困難：除了前述高犯罪黑數外，證據取得亦非常不易，或檢察官等對電腦認識不夠等，均是造成起訴困難之主因。

11、處罰太輕：國內目前立法機關尚未制定出專法來針對電腦犯罪加以處罰，僅能依一般刑案中目的相似的詐欺罪、毀損罪、誹謗罪、竊

盜罪等懲處，刑度與行爲成功能所獲得利益不成比例。

（二）網路犯罪之分類

表 4 網路犯罪之分類及其常見類型

分類標準	特點	常見型態	知悉程度	偵查難度	負責單位
以網路罪空間爲犯罪場所（被動）	被動性質，引誘吸引一般人進入	1、 網路色情 2、 網路援交 3、 販賣盜拷 4、 網路賭博 5、 網路遊戲 6、 販賣槍械 7、 教授製仿炸彈	高	低	警察
以網路爲犯罪工具（特定目標）	針對特定目標予以侵害性質，藉由網路作爲犯罪工具	1、 網路恐嚇 2、 網路誹謗 3、 網路詐財	中	中	警察
以網路爲犯罪客體（爲攻擊目標）	對網路或電腦系統的攻擊性或破壞性	1、 網路入侵（駭客） 2、 散播電腦病毒 3、 網路竄改 4、 SQL Injection	低	高	警察、調查局

資料來源：研究團隊彙整

網路犯罪之分類，就技術層面而言，援引學者對電腦犯罪分類，可區分爲：阻害電腦網路機能系列的之犯罪，非法使用電腦網路系列之犯罪等兩大領域，惟如前所述，輔以對於「網路犯罪」之定義，則其在概念應僅限於利用網際網路，而具有網際網路特性者，包括：分散性、開放性、互通性、隱密性、立即性等。

故依網際網路在犯罪中所扮演的角色，可將網路犯罪分爲以下三類：

1、以網路空間作爲犯罪場所。

2、以（網際）網路爲犯罪工具。

3、以（網際）網路爲犯罪客體。

如表4所示，有不同的網路犯罪類型，不過這些網路犯罪，特別是前兩類，都是警察機關職責的範圍。第一項由於犯罪證據多較具體，而且易於採證，所以警察機關較能掌控；不過前提是網路空間係透過國內業者提供網域，才比較能控制。關於第二項網路犯罪，警察若能掌握證據，在偵查上亦非難事；但因爲該項網路犯罪多和網路電話匯流，使得偵查難度提高，因爲發話地點經常不在國內，必須進行國際或兩岸合作。第三項駭客入侵，通常偵查難度較高，而且若受攻擊對象爲政府部分，則可能演變成國安事件，所以該類案件由法務部調查局負責。但前述分類仍有不足之處，例如個人資料外洩案件就不在分類之中，但其嚴重性不下於這些犯罪類型。

（三）另亦有學者就網路犯罪之犯罪型態分類爲：

1、網路服務提供型：如網路色情、利用網路發表不當言論、網路詐欺、利用網路煽惑他人犯罪、網路賭博等。

2、入侵篡改、破壞資料類型：如利用網路無權侵入、利用網路入侵而篡改他人資料、利用網路散布病毒。

3、其他侵害類型：如非法重製電腦程式或檔案、網址名稱與商標權之侵害等三類。

同樣的，這樣的分類方式將會留下犯罪證據，但若網址設於國外，同樣面臨犯罪證據蒐集不易的困境。重點在於，不同的網路犯罪類型，需要不同政府職能與角色因應。就國內網際網路管理而言，如果政府能有效管理網路供應業者或網路內容供應業者，或可減少國內網路犯罪的案例。或如果台灣能和國外政府簽訂合作協助，也有助跨國網路犯罪的偵辦。

（四）規範網路犯罪之立法例

依據沈榮華（2002）網路犯罪相關問題研究，關於網路犯罪之立法例，有制定專法的立法例，如德國的「聯邦資訊與電信服務架構性條件建構規制法」（Gesetz des Bundes zur Regelung der Rahmenbedingungen fuer Informations-und Kommunikationsdienste-InKDG），簡稱「多元媒體法」（das Multimedia-Gesetz），德國對於網路各種事項之規範，包括網路犯罪在內，均以之爲據。有散見於各相關法規者，如我國，美國、日本均是。我國刑法於92年6月25日修正公布，增定第36章「妨害電腦使用罪」（358-363條）。此外，其他與電腦犯罪有關之規定，有201之1、204、205、220、315之1-315之3、318之1、318之2、323、339之1-339之3等條。其規範範圍涵括僞造有價證券、僞造文書、妨害秘密、竊盜及詐欺等罪。

無論「妨害電腦使用罪」章或其他各章之規定，仍未脫傳統刑法所規範的犯罪態樣，只不過將電磁紀錄或藉由電腦處理所顯現之聲音、影像或符號，以文書論，對於利用電腦犯罪或破壞、入侵他人電腦之行爲，加以規範處罰。嚴格而言，較屬於電腦犯罪之範疇，並非規範網路犯罪行爲。

三、網路犯罪之類型

由於我國網路的廣泛使用，網路人口幾達國內人口的二分之一，網友素質參差不齊，網路近年成爲另一個新型的犯罪工具與犯罪場所及犯罪的目標，致近年網路色情與網路犯罪成爲各級民意代表質詢政府相關單位的重點議題，並常見一些民間團體召開記者會抨擊政府相關單位，坐視網路色情氾濫戕害青少年身心。有關電腦網路犯罪之類型，本文不是要網羅各個類型之案例做詳盡的介紹，而是想先就國際上一般電腦網路犯罪型態作分類，然後再進一步說明國內之犯罪型態

近五年來，詐欺案件占全部刑事案件之比率有增無減，其中利用網路犯罪更是歷歷可數，根據資策會FIND／經濟部技術處「創新資訊應用研究計畫」統計，2007年第1季臺灣經常上網人口爲990萬人，網際網路連網應用普及率爲43％，藉由網路使用逐漸普及，藉由網路產生的犯罪行爲亦不斷成長。而國內一般犯案約可分成以下兩大類：

（一）以網際網路作爲犯罪之客體或場所：此類型以網際網路爲犯罪場所，亦以網際網路爲犯罪工具，甚至以其作爲攻擊之客體。刑法

第36章妨害電腦使用罪所規範之妨害電腦使用行爲，即爲最典型之類型。另外，若在BBS或是部落格上散佈不實謠言，因而涉嫌誹謗或對他人之公然侮辱；或是藉由網際網路散布、販賣猥褻資訊等，在刑法第310條誹謗罪、第235條散布販賣猥褻物品及製造持有罪亦有明確規範。

（二）以網際網路爲犯罪工具：此犯罪類型，不一定是以網際網路及連結在其上之電腦系統爲攻擊目標，也不一定是以網際網路爲犯罪場所，僅以網際網路爲犯罪之工具。例如藉由僞造第三人網頁在網際網路竊取或誘騙他人帳號密碼（網路釣魚），以達到竊取他人財物或詐欺取財之目的等行爲，即屬此類犯罪行爲，有可能同時觸犯刑法第210條僞造文書罪、第339條之3不正使用電腦詐欺罪及第358條入侵電腦或其相關設備罪等。

至於國內網際網路爲犯罪現況，根據警政署刑事警察局的統計資料顯示，近年來的網路犯罪手法一再翻新，主要的案例型態如下所示：

（一）網路詐欺案：爲以網路爲工具騙取財物之案件。96年1-6月電腦網路犯罪發生數以網路詐欺案4,603件爲最多，較上年同期增加1,267件（+37.98%），破獲率增加27.58個百分點。

（二）妨害電腦使用：妨害電腦使用罪主要針對無故入侵電腦、無故取得刪除、變更電磁紀錄、無故干擾他人電腦及製作專供電腦犯罪之程式等行爲予以處罰。96年1-6月妨害電腦使用3,675件，較上年同期減少820件（-18.24%），破獲率增加2.94個百分點。妨害電腦使用案多數爲網路遊戲，偵辦時發現上網來源端爲中國大陸、香港等地，追查不易。

（三）違反兒童及少年性交易防制條例：主要爲在網路上所散布、販賣之猥褻圖畫、影片、光碟，其係以未滿18歲之人爲內容者或使未滿18歲之人爲性交易者，96年1-6月經由網路違反兒童及少年性交易防制條例共2,374件，較上年同期增加1,117件（+88.86%）。

（四）侵害智慧財產權：包含違反著作權法、商標法及專利法，例如在

網路上販售大補帖、違法張貼、下載散布他人著作及販賣仿冒品等。96年1-6月經由網路侵害智慧財產權共1,515件，較上年同期增加742件（+95.99%）。

美國加州大學聖塔巴巴拉分校心理學教授布拉斯柯維奇（Dr. James Blascovich），曾在一項網路犯罪的研究報告中指，「貪婪」與「恐懼」是騙徒最常利用的兩個人性弱點。國內詐騙集團彷彿修過這門「詐騙心理學」課程，從早期的金光黨、刮刮樂、六合彩明牌，到冒充國稅局、健保局的假退稅、假退費，基本上都是利用被害人貪婪或貪小便宜的心態，遂行詐財之目的。等到類似手法逐漸被識破，再改從民眾的恐懼心理下手。

近五年來，根據警政署統計，至於民國96年1-6月電腦網路犯罪發生數13,608件，較上年同期增加2,835件（+26.32%），破獲數8,749件，較上年同期增加4,251件（+94.51%），破獲率64.29%，較上年同期增加22.54個百分點，呈現發生數增加、破獲率增加的情形，主要係警察機關加強偵查網路犯罪所致。

四、網路詐欺案例研析

以某網路詐欺案例說明，刑事局曾偵破署名「王經理」等人涉嫌在網路販賣個人資料，查扣1百多萬筆個資資料庫案。查獲時間爲民國97年12月02日上午00時00分。查獲地點係在高雄地區；查獲嫌犯爲王○雄（71年次，有強盜、竊盜前科）。查獲贓證物包括作案用手機、郵局提款卡、資料庫主機（內含1百多萬筆個資）等不法贓證物。查獲單位爲刑事警察局偵九隊、中正第二分局。再詳細說明，由刑事局破獲案件內容如下：

（一）刑事局偵九隊近來發現署名「王經理」等人，大肆於網路上廣發廣告販賣公司行號負責人名單（工商名錄）、百貨公司VIP卡持有人信用卡持有人、公務人員名單、銀行合作社定存名單、老人健檢名單（65歲以上）、幼兒0-6歲名單等等個人資料，爲避免大量個人資料遭詐騙及不法集團利用，導致廣大無辜百姓受害受騙，刑事局偵九隊獲線後，即向局長黃茂穗報告，黃局長獲報後極爲重視，指示偵九隊全力偵辦，偵九隊1組即與台北市政府警察局中正第二分局共同組成專案小組積極偵辦。

（二）經專案小組追查相關資料，發現該販賣個人資料犯罪集團，已將個人資料入電腦資料庫化，可依據購買者需求（地區、性別、年齡層、職業……等等條件），設定資料產出範圍，影響民眾權益重大，本案被害人多人指稱接過僞稱台新銀行台中分行的金融帳戶被盜領等詐騙電話及販賣不知名肝藥銷售員電話推銷藥品等云云，經專案小組向臺灣高雄地方法院檢察署及臺灣高雄地方法院聲請搜索票搜索王嫌等人住處，查扣作案用手機、郵局提款卡、資料庫主機（內含1百多萬筆個資）等不法贓證物等不法贓證物，全案將王○雄等人依違反電腦處理個人資料保護法等罪嫌，解送臺灣高雄地方法院檢察署偵辦。

（三）刑事警察局偵九隊傾全力偵辦此一重大販賣個資案件，終能宣告破案，對於不法集團企圖藉由網路資訊的便捷性及隱匿性，以非法的手段，俟機竊取被害人所有上網私密個人資料，販賣給不法集團，影響社會安定之犯罪行爲，予以迎頭痛擊，對遏阻犯罪集團繼續利用此一手法犯案，有積極正面意義，警方將持續全力維護網路秩序，防杜不法情事的發生，以確保民眾資通安全，警方也特別呼籲全民提昇危機意識，加強資通安全防護措施。

前述案件雖已偵破案件而且係個案，但從這個案例發現，政府職能與角色出現問題，這個案的背後，可能有許多案例存在類似問題，才會發生這麼嚴重的問題。例如，究竟這些個人資料係以竊取或販賣方式獲得（其實均有可能），仍值得深入追查；背後的問題包括政府與（或）公司（個人）之個人資料管制機制可能存在漏洞（包括預防、預警與查緝等三大功能）。由於個人資料對犯罪者而言，存在龐大的誘因，才導致這些問題的發生。從被害者的角度思考，前述三大功能都涉及政府的角色與職能，最接近受害者的是地方政府，但中央負責政策方向，特別政策具全面性的影響，所以中央政府也不能袖手。因此，從負責網絡詐欺犯罪案例切入，檢測政府的職能與角色，對於未來對防治網路詐欺犯罪很有幫助。

第三章　研究設計

本章就本研究所運用之方法與研究架構，論述如下。

一、研究架構

本研究從我國目前的網路犯罪防治政策切入（研究架構圖如下文所示），從網路犯罪政策之形成、規劃、執行，檢視政府（含中央與地方）職能與角色之內涵。

資訊科技蓬勃發展，網際網路隨之興起，基於開放、自由、易於使用等特性，網路已成爲個人、組織、政府間訊息之交換、傳遞的重要管道。隨著各行各業加深資訊化應用的同時，電腦及網路資訊設備應用的安全風險也隨之提高。國際上，早於2001年11月由歐洲理事會的26個歐盟成員國，以及美國、加拿大、日本和南非等30個國家的政府官員，在布達佩斯所共同簽署的國際公約，自此「網路犯罪公約」成爲全世界第一部，針對網路犯罪行爲所制訂的國際公約。而該公約制定的目的之一，是期望使國際間對於網路犯罪的立法，有一致共同的參考準據，也希望國際間在進行網路犯罪偵查時，有一個國際公約予以支持，而得以有效進行國際合作。

本研究藉由政府職能角色之研析，來達成整合及分工之結果，因此，本研究之架構詳如圖4所示。依變項爲政府職能，自變項爲中央政府、地方政府與民間組織，至於網路（犯罪）政策形成、規劃、執行則爲中介變項。目前我國網路犯罪防治成效不甚良好的可能原因在於缺乏整合機制，使得網路犯罪（網路詐欺）防治成效不如預期。而這整合機制的原因在於網路犯罪（網路詐欺）防治政策形成、規劃、執行過程，仍有改善空間。因爲既言政策，就需要有更多的政策配套，也就是政府相關部門在政策形成、規劃、執行過程，應有更多的溝通與合作。

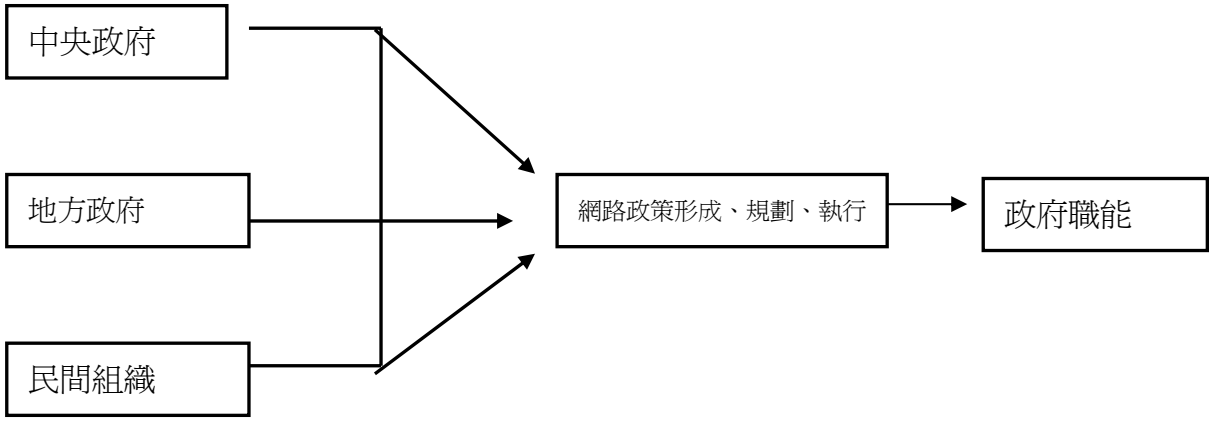


圖 4　研究架構圖

二、研究方法

本研究所探討之主題，爲「網路犯罪防治體系政府職能角色分析」，因其網路犯罪屬新興犯罪型態，在實務上報導的案件發生數及破獲數均屬少數，不如傳統性犯罪隨手可得，且網路犯罪型態呈現多樣趨勢之下，就目前國內而言，網路犯罪案件經披露者屬數量有限，且資料散布各機關蒐集與整理不易，未經披露者（即所謂犯罪黑數），有因當事人或機關不願公開，或本身受害而不自知等眾多因素，而無法知悉，因此，案例來源不多。

因此，所採取之研究方法如下：

（一）內容分析法

即參考有關之文獻（如剪報及網站網路內容），加以整理、分析，並探討各種影響網路犯罪因素間之關係，藉由概念的釐清，確實掌握研究問題的重點，對網路犯罪問題能提出合理的解釋。本研究兼採質化的文件分析法，理由在於，網路犯罪者經常在被逮捕後，才能瞭解犯罪模式；加以，政府職能角色議題研究，有其獨特性，不易由問卷獲知，因此本研究以透過質性的資料收集與分析的原則。重視研究者的反省及其文件兩者的交互作用，對文件內容進行深入分析，以發現、證明該文件內容的環境背景及其意義。

因此，爲深入瞭解「網路犯罪」所處脈絡，中央政府與地方政府對於網路管理之間交互作用所產生之深層意義，本研究主要以「質」化剖析進行分析，以網路及媒體之相關報導爲主。因案件數不多，所蒐集與網路犯罪有關之案件有限，以現有之案例爲分析的對象，本文從案例的解析，透過框架結構（Frame）犯罪分析對資料進行研究，藉以瞭解網路犯罪案例所存之內涵與訊息。

（二）焦點團體訪談

團體深度訪談，或稱焦點團體，是社會科學中最廣爲使用的研究工具之一。焦點團體成爲從事方案評估、行銷、公共政策、廣告及傳播等應用社會科學家重要研究工具之一。雖然多數的團體技巧有顯著之共通性，但焦點團體訪談只是團體研究的其中一種。由於團體是由一群有共同興趣或目的個體所組成，訪談可能造成訪問者與受訪者的互動。就本研究的設計而言，主要的方法是邀請相關專家，透過對特定網路犯罪議題進行討論，包括政策面、規劃面、執行面、評估面等，都有邀請專家學者討論。

（三）深度訪談

深度訪談，又稱質性訪談，是一種帶有目的的對話。此類訪談法往往沒有預設問題的答案，問題是採用開放式的。又可區分爲半結構式和非結構式的訪談。半結構式訪談的研究者會訂出訪談大綱；談話的內容沒有嚴格限制，大多根據談話的進度，適時的追問和修正問題。非結構式訪談則是完全去除訪談問題的順序，沒有標準化程序，大多以一種日常生活對話進行訪談，本研究主要以非結構性的訪談爲主，資訊係透過訪談者與受訪者間的互動而獲得。

三、本研究之焦點團體座談與深度訪談

本研究所欲探之政策形成，係整個政策之源頭，政策執行則爲政策執行之末端，從政策末端檢測整個政策流程，即爲本研究最重要之研究方法思維。本研究以焦點座談法和深度訪談法來進行深入研究。將從地方治理的觀點，也就是以問題導向方式，瞭解不同部門針對網路犯罪問題，其所扮演之職能與角色，以及對目前其所認知之政策成效進行評析。初期將從台南地區（地方）之警察局、調查站、地檢署..等，以及資策會、中央的國家通訊傳播

委員會（NCC）、刑事局、調查局等，進行焦點座談與個別深度訪談等，以發現問題的根源。然後，再設計和中央與地方政府相關之政策議題，舉辦焦點座談或個人深度訪談，以深入瞭解網路犯罪（網路詐欺）存在之政策問題，而從政策問題，藉以發掘不同政府部門之職能與角色問題與盲點。

本研究透過訪談網路犯罪涉及之相關人員，希能發現一些因素，這些因素無法用表面的觀察和普通的訪問可以獲得，涉及某些基本的資訊和訊息，期能蒐集更多資料以爲佐證，而使研究結果能更爲可靠、周延。

（一）深度訪談對象

表 5 訪談名單

專家名單	服務單位	訪談時程	編號
○○○　警務正	刑事局 科技中心（偵九隊）	98 年 3 月 20 日	A
○○○　主任	警政署 資訊室	98 年 7 月 9 日	B
○○○　主任	資策會	98 年 7 月 9 日	C
○○○　主任	警察大學 刑事系	98 年 7 月 13 日	D
○○○　隊長	南區電信警察隊	98 年 7 月 13 日	E
○○○　組長	台南市警察局科技犯罪偵查組	98 年 8 月 17 日	F
○○○　主任	行政院科技顧問組 (資安辦公室主任兼企畫組長)	98 年 8 月 31 日	G
○○○　簡任技正	國家通訊傳播委員會 （NCC）營運管理處	98 年 10 月 17 日	H
○○○　科長	調查局 資通安全處	98 年 10 月 19 日	I

本研究設計和中央與地方政府相關之政策議題，舉辦焦點座談或個人深度訪談，以深入瞭解網路犯罪（網路詐欺）存在之政策問題，而從政策問題，藉以發掘不同政府部門之職能與角色問題與盲點，選擇之邀請中央與地方人員詳列如下。受邀訪談對象力求多元化，如表5所示，包括中央與地方政府官員，資策會人員，以及第一線查緝人員等，都在受邀訪談之列，主要的訪談內容聚焦在網路犯罪政府職能與角色。

（二）深度訪談題綱設計

本研究設計和中央與地方政府相關之政策議題，舉辦焦點座談或個人深度訪談，以深入瞭解網路犯罪存在之政策問題，而從政策問題，藉以發掘不同政府部門之職能與角色問題與盲點，問題如下：

1、「資訊安全」與「網路犯罪」相關之議題。

2、「網路犯罪」牽涉到的相關政府部門及中央與地區(職能)區分，服務傳送機制。

3、由破獲的具體案例分析牽涉到的相關政府部門。

4、就犯罪的各項手法如何加強相關政府部門的各項職能。

第四章　研究分析與發現

由於網路犯罪既無中央與地方之別，亦經常無國界之別，所以網路犯罪主要爲中央政府的責任是合理的推論。但是很多網路犯罪執法係地方政府警察機關負責，所以嚴格說來，若將網路犯罪議題以政策形成、規劃與執行三大部分思考，中央政府主要負責網路犯罪的政策形成與規劃，地方政府主要負責執行或執法。但實際運作上，屬中央政府的刑事警察局（偵九隊與科技犯罪中心）亦負責很大部分的網路犯罪執行。而且從訪談中可發現，這些偵查人員其實亦存在網路犯罪規劃的能力，甚至亦可對政策形成提供建議。但從研究發現似乎顯示，這些（中央）的警察人員，在政策規劃與形成所能扮演的角色非常有限。既然如此，那麼中央政府就應該負擔更大的網路犯罪（預防與偵查）的責任。

網際網路的發展，正將完全改變現代人的生活型態，如何建構網路新世界的法律秩序，已成爲刻不容緩的問題，而其中最令人擔憂的，莫過於網路的普及讓犯罪隱形化，嚴重挑戰現實社會之法律秩序。傳統社會重視一般性犯罪，而忽略了網路犯罪的重要性，隨科技的發展與進步，犯罪也隨之變遷，這種犯罪現象，已經跳脫重「電腦犯罪」而輕「網路犯罪」的舊有巢臼，慢慢轉向重「網路犯罪」的境界。這種轉變雖然會讓大家對網路犯罪者產生極爲負面的印象，但是隨著電腦網路科技的普遍，這種「網路犯罪」的受害者也越來越多，讓電腦網路科技蒙上一層陰影。由於國內資訊教育的普及與網際網路的發達，此類案件有逐漸蔓延的趨勢。從接二連三的網路色情、強暴、網路遊戲、網路恐嚇、破壞、網路入侵、隱私權受侵害、毀謗、侵害著作權等等網路犯罪的事件增加，顯示我國網路犯罪率明顯的提高，大眾對網路安全問題的重視，更甚以往。

本研究就政策議題分析之面向，分別從：「中央與地方政府職權劃分」、「服務傳送機制、民間參與」、「法令架構之分析」等三個面向，分別論述之。本章針對網路犯罪政府職能與角色之研究發現與分析進行論述，共分政策形成、規劃與執行等三節，探討有關網路犯罪治理部分。

第一節 網路犯罪防治政策形成，政府職能與角色

網路犯罪防治（包括預防與偵查）政策，係中央政府應有之職能與角色，而所謂中央政府，依資通會報的架構，行政院要負最大的責任。從該架構分析，這部分職能與角色專業能力最強的是資策會與通傳會，而根據受訪者行政院科技組的官員表示，國科會也扮演一些角色。唯資策會是財團法人，所以最能扮演政策形成功能的應該是通訊傳播委員會（簡稱NCC）。再從實務運作上瞭解，在網路犯罪未端問題處理上，主要是由警察機關（刑事局偵九隊與縣市警察局刑事警察大隊的網路犯罪偵查小組）負責。但從受訪的意見上，似乎顯示，警察在政策執行末端的困境，幾乎無法或難以反應在政策形成（或形成整體的中央政策）上。

從資通會報的組織架構圖看來，這是一個完整的資訊安全（或網路犯罪）維護很完整的分工與整合架構圖。但從幾位受訪者的資料中，發現資通會報所能發揮的功能非常有限。只讓一位（或至多五位）科技背景的官員，進行跨部會協調，因此才會出現警政署受訪者官員認爲資通會報幾乎沒有任何功能的意見。可能的原因在於，資通安全會報主要希望解決網路犯罪的問題，這部分其實警察負責最大宗的業務，但整個資通會報組織架構中，警察所佔的角色非常渺小。對資通會報所能造成的影響，相對也就非常微小。而從東森網購個資洩漏與老婦人向165報案仍被騙兩件案例，其實就可以窺知政府在網路犯罪議題政策形成、規劃、執行存在許多困境。

網際網路的誕生爲人類帶來便利，但在同時網際網路強大的功能若不幸爲有心人所惡用，則其所造成的危害實在難以想像。「水能載舟，亦能覆舟。」雖然網際網路可能帶來危害，但其所具有的功能卻也是不容忽視的。運用電腦網路科技的資訊時代是時勢的潮流，在利用網際網路興利的同時，對其弊端事先予以防範，「善用」網際網路的功能，達其正面的功效。使其爲人類的發展提供助力，此是吾人所樂見的。在政府組織的環節中，面對網路犯罪的問題，政策如何形成，政府實際上如何因應？

網路犯罪政策會受到許多社會因素的影響，同時，在網路無國界，全球化科技發展的情況下，網路犯罪政策當無法自外於這股科技發展的潮流，故而網路犯罪政策的制定亦必須隨時代與科技進步的需求來改變。是以，在網

路犯罪政策的制定上，除了要考量組織制度之外，政府這種職能是否需要加強也是我們所應加以研究的課題。事實上，網路犯罪政策在形成過程中所可能受到的影響因素，也不亞於其他政府部門在制定公共政策過程中所需考量的範圍及程度。因此，我們要在了解網路犯罪政策的形成過程或甚至要推動網路犯罪政策的執行，就必須觀察及瞭解在網路犯罪政策的形成過程中政府組織制度和參與者，也就是所謂的組織制度和決策者所可能對政策形成產生之影響。其次，網路犯罪政策的形成過程中，組織制度之間的互動情形是否會影響網路犯罪政策的形成與執行成效。是以，本研究以各訪談人之間所提的個案做探討與分析，來瞭解網路犯罪政策的形成過程中，組織制度之間的互動情形是否會影響政府職能政府職能該如何加強，並提高對網路犯罪防治政策的形成與執行成效。

在政策形成方面，有關政府面對網路犯罪之職能與角色，又可分預防與偵查進行討論。

一、「中央與地方政府職權劃分」

1、預防

從公共政策的形成理論中，從影響網路犯罪政策形成的因素，自此切入，瞭解政府各機關對網路犯罪政策影響之情形，及組織制度之間的互動關係，最後在藉由對政策分析與政策價值之追求與取捨之探討，來勾勒出網路犯罪政策形成所欲追求的目標。

案例一：三重老婦人被詐欺700萬而引起劉兆玄院長的個案。

最近，三重一個老婦人被電話詐騙了700萬，引起劉院長的關注，就在治安會報中要政府去瞭解，就請科技政務委員處理。

所以在網路犯罪防制政策預防議題形成上：

（1）就是要有「由上而下」的重視，然後政府職能體系資安會報再發揮角色與功能。

就G主任所言「最近，一個老婦人雖向警政署165反詐騙中心報案，但仍被電話詐騙了700萬，引起劉院長的關注，就在治安會報中要政府去瞭解，就請科技政務委員處理。當我們介入去看，在執行面的確有些

問題，我們就找出這些漏洞來規劃，也對警政署不足的部分來加強規劃，並對警政署資源不夠的地方爭取資源。」

由於G主任係科技背景，擔任資通安全會報協調角色，有其專業性。這段談話間接與直間認同警政署職能角色不足，需要更多資源。但G主任並未提出解決或建議方案。針對這點，研究團隊認爲，可能的原因在於警政署165反詐騙專線目前係由警政署保一總隊員警負責，其犯罪偵查的機動性與功能性自然不足，如何進一步整合警政署（特別是犯罪偵查部門）資源，投入反詐騙行動，應係未來重要的發展方向。

（2）網路犯罪政府職能與角色之政策形成－跨部會協調不夠。

就G主任所言「我們就做策略規劃和跨部會協調。像剛才700萬的案子，還有跟通傳會NCC有關，像各機關有何管理或是技術可以突破的，就請NCC協調中華電信過濾來話國碼。所以我們協調各單位我們都在想辦法。…像東森個資外洩，最大的業管機關是誰呢，其實我們不能單純化，網路本身就有好多單位，應就其所業管的來發揮其規劃，網路犯罪主管機關是內政部，但是這是末端。但是，說網路無主管機關是把問題過度簡單化。…例如，網路平台大都是第2類電信事業，是通傳會管，網路是無店面購物，是經濟部主管，若賣的東西是衛生署業管，當然是衛生署管…等等，但是主管機關中要有一個主窗口。」

就前述G主任的說法有幾個問題存在，首先，過濾來話國碼比較算是被動的預防方式，應該有其一定之網路犯罪預防功能。比較大的問題，是跨部會協調的機制沒有建立，因爲從其談話中，似乎隱含跨部會協調機制並不存在。所謂的「主窗口」似乎未見提及，可能並未建立「主窗口」。問題在於，一般主管機關多缺乏執法能力，除非上級要求，或與警察機關合作，否則多不願出面執法。換言之，要求主管機關出面整合，是未來迫切需要進行的工作。

（3）網路犯罪政府職能與角色之政策形成－制定法源要快。

G主任所言「在這個架構圖裡，有一個網路偵防工作組，包括法務部和內政部等，我們做政策的規劃，刑法2003年刑法妨害電腦使用專章就是網路偵防工作組重要法源。…我們會在政策的層次去建議要有法源

，比如內政部成立警政署偵九隊，2005年要法務部建置資安鑑識實驗室。…比如我們又追蹤法務部修個資法的進度，像這法案一躺躺了3年，我們也在管制，像東森個資外洩，個資法是基本法，其他還有一些目的主管機關依個資法去訂定管理辦法。有的則原有管理辦法的，有的會修正。」

就G主任的說法，資通安全會報的確很積極地在進行資通安全的政策制訂。這說法背的理由卻隱含，如果這些法源不通過，似乎問題就無法解決。而另一個問題是，就算法案通過，仍可能存在執法困境。因此，問題也在於行政機關是否願意積極承擔責任，在未修法前即願意想辦法思考網路犯罪之預防與查緝。

「個資洩漏資部分就像東森，就是協調各相關主管部會，就會要求各主管機關，就其業管開罰，讓東森該負起責任，有些資安外洩是內部人員所為，有些機關例如銀行安全機制較高，像是金管會和金檢局就會要求各銀行，像東森也在想辦法，其實，個資法保護是夠的，民眾可以去告，只是還沒發生，當然修正新的個資法也還沒三讀通過。」

如前述與後面刑事局官員所述，東森個資洩漏的問題存在已久，政府跨部門機關卻遲遲未建立整合的工作小組，積極介入個資洩漏問題。這也難怪詐騙案件不斷發生，因爲主管機關並未確實負起責任，因爲媒體不見得知道去要求主管機關負責，在此情形下，網路犯罪的偵查與預防當然成效不彰。

2、偵查

在「中央與地方政府職權劃分」上，政府職能角色部分與業者配合偵查，對此有幾個核心問題需要說明一下：

（1）網路犯罪的相關規範與制度是中央建立的，地方政府並沒有權限規範。

這是針對地方政府所能因應的進行整理，主要從形成層面切入，地方政府也是有規劃，只是能力非常薄弱。受訪者F的描述是「地方政府主要由警察局刑事警察大隊組成網路犯罪小組…」，F又說「中央刑事局

和地方警局其實沒分工，網路無國界，但是重大的刑事局都會主動偵辦，中央刑事局人員比較完整，人才比較多，但是中央刑事局雖是科技中心，跟我們地方警局一樣，也不是法制化的單位，是任務編組。…網路的案子一般移到地檢署，大都會尊重我們的專業，地檢署對網路不知是否有分專組，網路是一種專業，但是網路犯罪比較隱性，不像辦槍毒等大案，所以偵辦網路犯罪可能也就沒誘因，這情況在警界中也是一樣。…網路犯罪向派出所報案，派出所送分局偵查隊，分局有偵辦能力存疑，地方警察局科技小組連我組長才4個人，人才人力都不夠，其實網路這個東西，真的其實很專業，刑事局人員人才人力比較多，地方警局科技小組有時也要分擔其他專案，所以在地方警局其實專業度也不夠。」

從F組長所述，地方政府警察局有能力偵辦網路犯罪的僅有「網路犯罪小組」少數員警，派出所、分局偵查隊，以及警察局刑事警察大隊等大部分員警，幾乎均無能力偵辦網路犯罪。加上偵辦網路犯罪的獎勵（績效配分）或誘因太低，使得這些員警對於網路犯罪的偵辦興趣不高。或許，建構網路警察可以是未來警察組織的工作重點（楊永年，1999）。

（2）屬於地方的偵查部分

績效評定標準與警察的職能培訓都由中央政府制訂與執行，並不屬於地方權限。因此，地方警察如何因應「績效評定標準」和中央政府高度相關。另一方面，從F組長所述，似乎也顯現警察人員網路犯罪之「職能的培訓」專業能力不足。這也是未來警察機關應該努力的，或至少可以如作者在網路警察一文所建議，應多鼓勵民眾進行「網路巡邏」同時和警察連結，應可提升警察投入網路犯罪的意願。

（3）網路無國界涉及司法管轄權

由於網路無國界的特性，涉及到我國與該國的邦交、協定…等，亦涉及國外業者是否能配合，亦是制度面的問題，而不是業者層次的問題。F所說「網路犯罪有時查出的IP都是在外國，但是外國或是國外我們也都沒有司法管轄權，駭客也常在國外，境外犯罪有待努力，有些國家查資料還要當地國家法院的許可，所以國外的資料不好拿，若是SKYPE

網路電話根本調不到資料，即時通是在伺服器都有資料，若是網路監聽叫做封包側錄，公共場所像網咖就很難側錄，個人的家用電腦比較可行。」

持平而論，固然網路犯罪的IP設在國外，但不表示犯罪嫌疑人也在國外。因此，除了建立國際合作機制共同偵辦網路犯罪，如何強化警察偵辦網路犯罪的意願也是重點。

「網路業者要加強把關，要有被害人報案，若是境外來的，偵查就困難，網路若真的存心要犯罪，偵查真的困難，只能偵辦一些比較無知無意的犯罪，真的是集團專業的、境外的，很難查得到，中央刑事局為地方警局半年辦一次講習，其實辦的不錯，地方警局比較沒能力辦講習，人才和時間都不夠，若查到管轄權在境外，真的沒輒，所以，希望有心人不要犯罪去，網路人才會越來越多，到時候犯罪可能越多，地方警局教育訓練太多元太雜了，根本沒辦法深入，警察每項業務都重要，每項都重要，急迫性最急的才處理，三角詐騙產生的無辜受害者，縱使釐清了關係，都還是要移送給檢察官認定，所以都還是很麻煩的。」

顯然，以目前偵辦網路犯罪的警察人力，可能不足以應付龐大的網路犯罪案件。如作者在網路警察之研究一文所述（楊永年，1999），網路警察可以是網際網路上的警察靜態或資訊化的產物，或在網路上個人對警察的認知或虛擬之結果，不過因爲網路科技的更新與使用人口激增，使得網路警察具互動性或動態性效果。也就是說，網路警察係網路的產物，警察的存在是因爲網路而生，所以網路是網路警察的先驅，或謂網路警察與傳統警察的不同點在於網路之使用與否。又因網路警察係根源於網路而生，是因爲有網路才有網路警察的存在，所以影響網路警察的最重要因素是網路，不是政治(雖然可能也會有所影響)。因此，網路警察可以很容易超越政治障礙，或謂藉由網路科技可以讓警察運作突破政治禁忌。也可以說，網際網路的發明顛覆了傳統警察的思維模式，讓警察可以虛擬化的方式，在網路上存在。

再詳細論述，所謂網路警察可以有四類，第一類每位使用網際網路者，都可以是網路警察，又可稱爲私立非營利網路警察。只是，因爲網

路治安屬公共財，若非具警察身份，可能無法依賴從事網路治安工作維生，就可能難以全心投入網路治安工作；或者，若具警察身份人員，但因員警個人興趣在勤餘之暇投入網路治安工作，當然也算網路警察，這是第二種網路警察，性質則係介於公立與私立的警察。這種網路警察可能因爲時間與勤務限制，或因警察組織或上級不鼓勵的前題下，投入網路治安的工作的時間與心力(工作承諾)就可能有所不足；第三種是私立營利警察，如保全公司或其它電腦科技公司，透過網路進行治安收取費用服務的警察。

第四種網路警察是，具備警察身份並有網際網路專業知識，而且網路治安的工作係爲其工作的一環，例如各警察單位在網路上設置網站之員警，他們必須經常上網更新資訊，或直接回答與解決網友的問題和接受報案，這些員警當然可以稱爲網路警察。另一方面，就是專責網路犯罪的員警，或知道如何利用網路偵查犯罪的員(刑)警，也可以是網路警察，例如我國刑事警察局，就設有專責偵辦網路犯罪(以網路爲犯罪工具，或以電腦科技專業知識進行犯罪)的外勤單位，而且因網路知識的普及，目前已漸有更多警察單位知道透過網路偵查犯罪。爲治安良莠著想，前述四種網路警察應該都可以是未來的努力方向，不應只侷限在第四種具警察身份的網路警察。

（4）資通安全會報應有更多積極作爲

目前資通安全會報係非正式的任務編組，以開會的模型存在，有時是等資安事件發生了，才進行討論。如受訪者D所說「資通會報有把機關分等級，但是，民間的有否分等級沒規範到，例如東森儲放民眾的個資，也沒分等級，若有主管機關應可迎刃而解。…NCC一直認為網路不是其全管（全部管轄），當然是否包括人力或是人員仍還不足，國內企業東森資料外洩是一個例子，其本身應該負責任才是的，企業資料外洩規定通報，私人機構用罰則比較恰當，比如說資料外洩企業本身要負責，當然，政府若是對企業負責把關的資料庫測試攻擊，企業做不好定期公佈讓民眾選擇，並不是企業資料外洩就要用刑法來規範，反而用民事賠償的處罰更好，以高額的賠償，外國企業有因為這樣破產的。」

雖然國外的處理模式，是以處罰（罰金）方式規範違反個資洩漏的企業，但國內的情形，似乎仍停留在三不管的模糊地帶。或許，我們可以學習國外的模式，以高額罰款方式處罰企業。但在法律未通過前，可能還是要透過跨部門合作，或結合媒體，針對個資洩漏的累犯，進行道德勸說或譴責。但這必須要有「主管機關」出面協調才行，唯受訪者D又說：

「政府機構若已經負責一個工作，要再接另一個工作，除非有誘因，不然不會自我找砸的，像NCC不接網路主管，可能是其人才或是物力技術不夠，所以公務機關要律定一個主管真是不簡單的，又網站的規範若是有主管機關給個證照，民眾也會比較有保障。」

可能的情形是，媒體或上級的壓力不足，使得NCC不願意承認或出面進行協調聯繫，使得類似個資洩漏的問題，仍層出不窮。在此情形下，個資洩漏後的網路犯罪，當然層出不窮。

（5）主管機關不願負責

從訪談資料顯示，政府主管機關其實不太願意負責，如B所言「政府應該跳出來，網路應該有主管機關，要明定出來，要成立一個常設機構，要成立一個網路安全機構，其實NCC應該成立一個主管機關，NCC有一個網路內容處，可是它也認為不是主管機關，所以網路安全一定要有人管，例如，雅虎不是2類電信所以沒人管、PC Home也都沒主管機關管，若有主管機關的話，妳網站上面為何詐欺那麼多，不實的東西那麼多，我們可以行政作為啊，可以減少頻寬，可以逼得業者注意資安啊。」

換言之，面對新興的網路犯罪類型，主管機關其實不願負責，即便是行政作爲，好像也不願意有所動作。

（6）網路有無主管機關之爭議？

另一個問題是，到底網路有無主管機關？受訪者B提出「首先我要說明的是NICI不存在，國家的資訊安全目前是委外的，資安會報全部都是資策會的人，從主任到底下的都是資策會的人，沒有一個公務員，資安怎會好，NICI不存在，從綜合業務組以下從主任到底下的都是資策會

的人，沒有一個公務員，我們國家從不會承認資安不好。」

從這段文字，似乎可以發現，關於網路犯罪已非政府職能與角色所能扮演。在此情形下，由委外單位負責相關資安工作，當然和政府機關的連結就會較弱，難免受訪者B會有這樣的批評。針對這點，或許未來可以思考的是，應讓NICI的員工和政府官員（特別是和網路犯罪相關的公務員）有更多的接觸或合作。

受訪者B又強調[NICI（行政院國家資訊通信發展推動小組，英文名稱為National Information and Communications Initiative Committee）不存在，從綜合業務組以下從主任到底下的都是資策會的人，技服以下也都是資策會的人，技服負責國家整個資安，全部是資策會的人沒有一個公務員，NICI是一個開會型式，從綜合業務組到NICI都是資策會的人，就是國家的資安委外等於說國家目前的資訊安全都委外。第二點，網路主管機關是誰，剛剛所講的NICI不是，行政院科顧組也擔任資安會報的召集人，其實都是資策會的人NICI是一個任務編組一種開會的型式裡面的網路犯罪工作組。…資安會報，其實只是一種開會型式的任務編組，不是常設機構，這個架構圖從綜合業務組技服中心的主任…都是資策會的人，都是資策會在主導，資策會裡面沒一個公務員，其實，網路主管機管要明定出來，其實目前資安是民間的資策會在主導，其實資安會報是開會才有，不開會就沒有。」

由於受訪者B是現任政府官員，而且擁有豐富的網路犯罪辦案經驗，有這樣的聲音應該受到重視，或該受訪者可能是愛之深責之切。或許可以立即思考的是，我們已有很多NICI的員工到政府部門工作，我們也應思考，是否讓具公務員身份的警察人員或其它人員，進駐NICI並搭起政府部門間合作的橋樑。

誠如B所說的「政府應該跳出來，網路應該有主管機關，要明定出來，要成立一個常設機構，要成立一個網路安全機構，其實NCC應該成立一個主管機關，NCC有一個網路內容處，可是它也認為不是主管機關，所以網路安全一定要有人管，例如，雅虎不是2類電信所以沒人管、PC Home也都沒主管機管，若有主管機關的話，妳網站上面為何詐欺那

麼多，不實的東西那麼多，我們可以行政作為啊，可以減少頻寬，可以逼得業者注意資安啊。…台灣因有鄰居大陸，所以，木馬程式台灣是世界最多的，因為大陸把這邊當練兵場，有些人專門賣偷到的資料庫，我認為NCC應該是它來主管沒錯。但是，目前是分散的，因為資安分成網路安全和資訊安全，現在二者是分散，現在網路內容是新聞局管分級、電子商務是經濟部管、電子的ISP是NCC管、網路犯罪歸警政署管....權責都分散了，其實應該有一個主管機關。」因此，讓NCC擔負更多的責任或發揮更多的職能與角色，應該未來的工作重點。

但如受訪者H所言「進一步說明如下，網路與現實世界一樣，要由一個主管機關管到全部，實際上不可能的，現實世界有多少事情有多複雜，虛擬世界就有這般現象，那當然就會牽涉到各單位或是各目的事業主管機關，至於網路犯罪，是內政部警政署主管的，相關資料或許那邊會較齊全，像刑事局科技中心研發室黃組長就常代表與會。…若現行法律對網際網路上之行為規範仍有所不足，可研修相關法律以為規範。」因此，我們得要回到前文所述，跨部會合作與協調聯繫要加強。問題在於，跨部會合作等於還是回到沒有機關負責的老問題。

二、「服務傳送機制、民間參與」

1、預防

（1）政府預防成效不彰

G所言「我跟○○○主任看法若有些許的不同，那是角度的問題。在這個架構圖裡，有一個網路偵防工作組，包括法務部和內政部等，我們做政策的規劃，刑法2003年刑法妨害電腦使用專章就是網路偵防工作組重要法源。」受訪者G顯然不同意資通會報功能不彰，並認爲他們很積極進行網路犯罪相關政策擬訂。但合理的說法是，畢竟受訪者G係科技背景人員，對於官僚體系，特別是對執行網路犯罪的警察人員，瞭解相當有限，所以認知上當然有落差。

再如受訪者C所言「資策會不是政府部門，NICI只是一個會報方式開會用的，資策會責任應是有限的，像這圖示會報方式都不是一個常設機構，資策會是經濟部委託的單位，應該是比較技術性的，若這個資安

會報架構圖之中的綜合業務組NICI，應該是要由NCC來派人員才合宜，因為NCC才是政府機關啊，NICI其實本身是幕僚，它不是行政院的科技顧問組（目前科技顧問組是由前暨南大學校長張進福主持）例如我們的資策會另外一位專家，是從事honey net，honey net是一種誘捕網路的工作，他的上班地點在北指部那一邊，他們是負責網路是否被破壞，也不管民間的，像購物網站他們也不管，至於，網路犯罪範圍廣泛，你們研究的範圍應該是類似網路資料被外洩。」

關於受訪者C所提之建議，由NCC派員進駐NICI或許是可行的方式，只是NCC可能意願不高，主要的原因可能還是在於法源的不足。或者，另種方式是讓懂網路犯罪且具警察身份的警察人員進駐NICI，也是選項之一。

受訪者C又說「現在沒有一個法定機關管理網路，像資安會報中的NICI不是正式機關，人員都是資策會的，若是NCC派員進駐資安會報綜合業務組NICI才對，那情況又不一樣囉，但是目前的NCC〈由新聞局廣電處和電信總局等等單位拼組〉也不認為網路是由其主管，目前網路普及，政府和民間業者都應該很重視才對，由網路洩漏出的個資而衍生出各類型犯罪已經太多，詐欺猖獗就是這樣來的，至於網路犯罪都是已經發生了才由警察來主管，這些都是已經是末端的事情了，所以在前端的網路管理真的很重要，但是網路管理牽涉到資安的部分我們這一邊是不負責民間的，例如他們的網站被入侵。至於，網路犯罪的前端管理以及還沒犯罪前之網路管理目前是沒人管。…資策會不負責民間的，例如他們的網站被入侵個資外洩，也是新聞紕漏民眾才知道的，我們資策會也不管這個。…其實，網路在管理方面牽涉到政策面的，若是網路定一個最低標準，達到最低標準有給一種標章，其餘由民眾和輿論去判斷取捨，也是一個可行方式，但是，基本上網路要有一個主管機關的。」顯然，受訪者C對NCC有高度期待。

（2）業者若洩漏個資，出事後未能被追討大筆金錢

事實上，業者若洩漏個資，出事後能被追討大筆金錢，這是加強政府職能對網路犯罪防制政策執行上最有效的，因此新修正的個人資料保

護法應導入這種精神。因此，受訪者D認爲「並不是企業資料外洩就要用刑法來規範，反而用民事賠償的處罰更好，以高額的賠償，外國企業有因為這樣破產的。…國外，也有說有電腦前科不得從事電腦相關工作，對有電腦專業想作姦犯科的有赫阻的作用。」

2、偵查

事實上，如前文所述，中央的資安會報很完整，但是這卻是開會的型式，沒開會即不存在，很多時候都需要綜合規劃組（科顧組）聯繫協調的，綜合規劃組（科顧組）聯繫協調了好多事情，包括造成政策的形成，雖然效果亦不錯，但是，包括網路犯罪偵查面向上和社會大眾媒體都不滿意。何以如此？可能的原因即在於網路犯罪案件的量實在太大。

受訪者B認爲「資安會報，其實只是一種開會型式的任務編組，不是常設機構，這個架構圖從綜合業務組技服中心的主任…都是資策會的人，都是資策會在主導，資策會裡面沒一個公務員，其實，網路主管機關要明定出來，其實目前資安是民間的資策會在主導，其實資安會報是開會才有，不開會就沒有，其實網路主管機關要明定出來，技服中心掌握國家的資安，竟然都是民間資策會的人，現在都是民間在主導，若明天他辭職了，或是到大陸去了怎麼辦，公務員才有權利義務啊，召集人和副召集人其實都是掛名，例如，承認我們資安有什麼問題，向民眾說明和公佈我們資安有什麼問題，例如，說哪個網站或資料外洩了會造成許多詐騙電話，詐騙為什麼會成立，就是資料外洩的問題，東森只是被蘋果報導出來，沒報出來的更多。」顯然，網路犯罪問題應受更多的重視。

或許警察大學刑事系主任D的說明更爲合理，「NCC一直認為網路不是其全管（全部管轄），當然是否包括人力或是人員仍還不足，…政府機構若已經負責一個工作，要再接另一個工作，除非有誘因，不然不會自我找砸的，像NCC不接網路主管，可能是其人才或是物力技術不夠，所以公務機關要律定一個主管真是不簡單的，…又網站的規範若是有主管機關給個證照，民眾也會比較有保障。」換言之，政府（或NCC）仍可扮演更積極的管制角色，唯就研究團隊訪談NCC官員得到的回應是，

這不是他們可以完全掌握的，很多業務在其它主管機關，例如購物網站在經濟部。因此，很清楚的是，我們還是需要組成跨部會的協調小組進行討論。

三、「法令架構之分析」面向

1、預防

（1）法令修改訂定跟不上時代

有關網路犯罪的法令修訂太慢，也直接或間接影響到執行的成效。例如受訪者G主任所言「比如我們又追蹤法務部修個資法的進度，像這法案一躺躺了3年…」除此之外，如果能針對不同的法令內容，包括設證照進行規範，或許也是方法之一。只是，這樣的作法可能又會回到立法過程可能出現的弊病。因此，透過行政機關進行行政管制，也是可行的方法。

2、偵查

（1）各目的主管機關訂定之管理辦法，未能即時因應配合

事實上，各目的主管機關，不應只立即跟上網路犯罪變遷，法令修正也應作快速因應。就如G主任所言個資法硬是在立院躺了三年不動。再如受訪者D所言透過民事補償的方式可是可行。綜言之，這有時牽涉到政府部門公務人員的工作態度，是否願意主動積極負責。當然也可能和媒體是否形成一定的壓力有關。

第二節　網路犯罪防治政策規劃，政府職能與角色

我們研究的目的，在提供解決目前政府最棘手的網路犯罪政策建議。我們的方法，是從目前政府最頭痛的網路犯罪案例著手，往回探討政府職能與角色的問題。以我們討論很多的詐騙案，不一定和「網路犯罪」的定義完全相符，理由在於，這可能只是單純的詐騙案，所使用的也可能是傳統的電話

，但也不能說完全無關，因爲詐騙者可能以網路電話爲工具進行犯罪，再者，這問題又可能與個資洩漏有關，這部分就必須由政府進行職能與角色的調整。

研究建議：政府多宣導，請業者提供國碼顯示服務(根據目前的問題，因爲不知道該「詐騙」電話由那個國家而來。

從地方政府職能角色來看，對網路犯罪的防治僅落在末端的偵查，但網路犯罪類型繁雜，所需要的技術層次高，對網路犯罪的防治，地方政府能處理的層面有限。

在政策規劃方面，有關政府面對網路犯罪之職能與角色，又可分預防與偵查進行討論。

一、「中央與地方政府職權劃分」

1、預防

從公共政策的形成理論中，探討影響網路犯罪政策形成的因素，並自此切入，瞭解政府各機關對網路犯罪政策影響之情形，及組織制度之間的互動關係，最後在藉由對政策分析與政策價值之追求與取捨之探討，來勾勒出網路犯罪政策規劃所欲追求的目標。

（1)「中央規劃、地方執行」之成效不彰。

E所言「我們辦過高雄縣市國中基測外洩的檔案，那是一個16歲的年輕人駭的，主管機關知道入侵，但是，沒有通報，像資安會報這個組織架構是在中央的，地方的根本沒這個架構，所以當事人工程師知道外洩，但是也沒通報，所以中央光有這個會議組織，地方在執行面根本都沒做到。」

顯然，資訊安全通報系統是中央與地方職能角色另個盲點，所以地方發生的事，中央並不知道。或許，未來可以仿照災害應變中心，不論中央或地方，均有災害應變中心的設置。只是，不論資通會報或災害應變中心也是任務編組，所能發揮的功能仍然有限。因此，受訪者E也談到，由各機關副主管（首長）確實負起相關責任，進行相關網絡之連結，或許也是解套的方法之一。

（2）網路犯罪資訊安全人力不足，地方專業性不夠。

如前文所述，「網路警察」嚴重不足也是問題所在。其實，很大的原因是目前警察人員擁有資安能力的仍在少數。F所言「網路犯罪向派出所報案，派出所送分局偵查隊，分局有偵辦能力存疑，地方警察局科技小組連我組長才4個人，人才人力都不夠」不過，如前文所述，我們仍不應忽略現職非在網路犯罪部門任職的員警，仍可施以一定的訓練，或鼓勵更多非警察人員參與，也是可行的方法。

2、偵查

在「中央與地方政府職權劃分」上，網路犯罪政府職能角色部分在政策執行上之偵查，對此有幾個核心問題需要說明一下：

（1）網路無國界

網路無國界的偵查問題已在前文討論，如F所說「網路犯罪有時查出的IP都是在外國，但是外國或是國外我們也都沒有司法管轄權，駭客也常在國外，境外犯罪有待努力…網路業者要加強把關，要有被害人報案，若要是境外來的偵查就困難。」重點是，除了進行跨國合作，鼓勵警職與非警職人員投入這領域，協助警察偵查，也是可行的方法。

（2）網路犯罪的相關規範與制度是中央建立的，地方政府沒有權限規範並負責執行。

如F所說「地方政府主要由警察局刑事警察大隊組成網路犯罪小組…中央刑事局人員比較完整，人才比較多，但是中央刑事局雖是科技中心，跟我們地方警局一樣，也不是法制化的單位，是任務編組。…刑事局人員人才人力比較多，地方警局科技小組有時也要分擔其他專案，所以在地方警局其實專業度也不夠。」

應該說，中央政府的人力比地方政府充裕，再者，屬於地方的偵查部分，績效評定標準與警察的職能培訓都是中央制訂的，亦不屬於地方權限。地方警察如何因應「績效評定標準」是遵循中央，「職能的培訓」專業能力不足。研究團隊原本提出，取消警察績效配分制度可以是未來的改革方向，不過於警大服務的受訪者卻認爲不可行。無論如何，未

來仍得提升網路犯罪工作小組之誘因。或者，有些基本的分工項目，可能也沒有做的很好，如受訪者E所言，有關資安資報的問題，有待進一步研究、解決。

二、「服務傳送機制、民間參與」

1、預防

有關民間參與進行網路犯罪預防方面，事實上，因爲資策會的成立，已在進行這方面的工作，這也算是民間參與。再如前述，鼓勵其它非警察人員和政府資安人員進行連結，也是重要的思考方向。只是，資訊安全有太多外來的參與，也可能出現資訊安全漏洞的問題。因此，這中間如何連結，還得要進一步研究。

2、偵查

由此可知，中央的資安會報很完整，但是這卻是開會的型式，沒開會即不存在，很多時候都需要綜合規劃組（科顧組）聯繫協調的，綜合規劃組（科顧組）聯繫協調了好多事情包括造成政策的執行，雖然效果亦不錯，但是，包括網路犯罪偵查面向上和社會大眾媒體都不滿意。資安會報是開會的型式，綜合規劃組（科顧組）負責聯繫協調，民間參與、服務傳送機制不良如G所說「在這個架構圖裡，有一個網路偵防工作組，包括法務部和內政部等，我們做政策的規劃，刑法2003年刑法妨害電腦使用專章就是網路偵防工作組重要法源。我們會在政策的層次去建議要有法源，比如內政部成立警政署偵九隊，2005年要法務部建置資安鑑識實驗室。」

三、「法令架構之分析」面向

1、預防

（1）法令修改訂定跟不上時代

G所言「比如我們又追蹤法務部修個資法的進度，像這法案一躺躺

了3年，我們也在管制，像東森個資外洩，個資法是基本法，其他還有一些目的主管機關依個資法去訂定管理辦法。有的則原有管理辦法的，有的會修正。」

D所言「又網站的規範若是有主管機關給個證照，民眾也會比較有保障。」

H所言「進一步說明如下，網路與現實世界一樣，要由一個主管機關管到全部，實際上不可能的，現實世界有多少事情有多複雜，虛擬世界就有這般現象，那當然就會牽涉到各單位或是各目的事業主管機關，至於網路犯罪，是內政部警政署主管的，相關資料或許那邊會較齊全，像刑事局科技中心研發室黃組長就常代表與會。

在實體世界所發生之行為會受到相關法律之規範，而在虛擬網路世界發生相同之行為，並不會因其行為發生在虛擬網路世界即不受規範，現行法律對實體世界或虛擬網路世界之行為，大致已有相同之規範。各政府機關可依主管法律對於在網路上違法行為依權責處理。若現行法律對網際網路上之行為規範仍有所不足，可研修相關法律以為規範。」

2、偵查

從中央到地方皆不是法定常設機關，各目的主管機關法令未能即時因應配合，這部分前文已有論述，因此不再重複。

第三節　網路犯罪防治政策執行，政府職能與角色

以東森網購爆發的個資洩漏案，該案爲社會大眾所周知，是在2009年8月時，蘋果日報記者假扮客戶希望購買個資，竟能以很少的花費，一次購買萬筆的個人信用卡交易資料。事實上，本研究團隊在同年4月時，就已經訪問到偵查人員發現這個嚴重的問題。顯然，這四個月的時間，中央政府從偵查人員查獲的重大個資洩漏個案，並未啓動（或可能無法啓動）預防機制。或者，面對東森個案，政策執行者好像只有具警察身分的「偵查員」在扮演角色，其它部門好像都沒有扮演任何角色。可能的原因是，該偵查員並未將

相關問題反應給相關部門（如通傳會與掌管交易的商業部分）。但作者猜測，即便該偵查員向這兩個單位通報，可能的潛在問題是，找不到對口承辦人員，或找到承辦人員，因爲從屬關係，該承辦人不見得願意「幫忙」（因爲可能得不到上級重視，或已有承辦人認爲重要的工作在進行中），所以不便「幫忙」。

那麼爲什麼老婦人向165報案，何以還會被騙鉅款？在這個案上，行政院科技組的官員說，他們已努力向通傳會與業者溝通，增加預防（付費）的功能，讓消費者（或潛在的受害者）在電話響時，若是國際電話，立即有警示的提示語，以強化預防的功能。研究團隊肯定這樣的作法，但進一步認爲165無法在第一時間立即採取行動，或165無立即行動的功能，應該也是重要的原因。

政策執行是實現政策目標和解決政策問題的實際行動，C.O.Jones進一步指出：政策執行是將一項政策方案付諸實施的所有活動的總和，而這當中以解釋、組織與運行三項工作最爲重要。首先，解釋是指將政策方案的內容轉化爲一般人可以接受的和可行的計畫和指令；其次，所謂組織，就是設立政策執行機構，擬定使政策內容產生效果的措施，以落實政策目標；最後，運行則是指提供支援和設備，運用預算經費，以達成政策目標。簡言之，就是把參與者、組織、資源、程序及技術予以有效組合，推動已立法通過的政策方案，完成政策目標。

政策執行的具體工作內容有：

（1）立法機關通過法案後，相關部門開始進行聽證程序（包括說明會、座談會及媒體宣導），做政策行銷；

（2）政府相關部門負責制定管理規則及執行政策的行政程序；

（3）政府提供政策執行所需的資源，包括財力及人力；

（4）透過立法監督，建立權威機制，要求政府執行部門貫徹政策方案；

（5）評估政策執行的狀況，針對原方案的缺失，政策制定者重新規畫政策方案予以修正。

政策執行的主體－從上述的說明，我們可能需要先釐清政策執行的主體以及它們所採用的職權和方式。一般而言，有權推動政策執行的主體爲行政機關（透過行政裁量權制定施行細則）、立法機關（擴大立法權，將政策執行的具體細節一並規範於法律條文之中，擠壓行政裁量權）、司法機關（透過對法令、行政命令和規則的解釋權，以及對個別行政決定的事前審查，發揮實質的政策執行效果）、利益團體（透過對政府的施壓，影響政府的行政裁量空間）、社會團體（扮演第三部門的角色，有時也參與攸關公共計畫的政策執行工作）。

一、「中央與地方政府職權劃分」

地方係與中央相對稱，乃將國家之統治權力，分屬於地方或中央行使之，換言之，地方政府在其管轄區域內之事務，不論其性質如何，概以地域爲劃分之標準，以歸屬於地方。

我國之地方自治則不然，凡屬中央職權範圍內之事務，雖在地方，仍由中央行使之，地方所得行使者，僅以地方之自治事項爲限，因在五權憲法下之地方自治，乃以均權主義爲其職權行使之基本原則，關於事權之劃分，不以地域爲標準，而以性質爲標準，凡事務有全國一致之性質者，劃歸中央；有因地制宜之性質者，劃歸地方，不偏於中央集權或地方權，因而地方自治，自與地方分權之觀念有別。

然網路犯罪無國界，無分地方和中央，故事務牽涉多元。

1、預防

（1）網路犯罪地方預防人力專業性都不夠。

I所言「資訊安全與網路犯罪其實五花八門，目前本局資通安全處負責機關保防的資訊安全，偏向公務部門，刑事局是社會保防，所謂社會保防 ，一般所謂社會案件皆有包括，但是有一些案件無法去分割，或是在法律上亦無法切割牽連，由那個單位先承辦或是線索哪邊先掌握，即由該單位承辦。」

2、偵查

（1）網路犯罪的相關規範與制度是中央建立的，地方政府並沒有權限規範，地方只負責執行。

（2）屬於地方的偵查部分，績效評定標準與警察的職能培訓都是中央制訂的，亦不屬於地方權限，地方警察如何因應「績效評定標準」是遵循中央，「職能的培訓」專業能力不足。

（3）國內業者是否能配合偵查，需要有相關法令規定，否則會觸及個人資料保護與隱私權問題，國外業者是否能配合偵查，除了該國對個人資料與隱私的規範不同外，亦涉及到我國與該國的邦交、協定…等議題。

根據受訪者I所言「資訊安全與網路犯罪其實五花八門，目前本局資通安全處負責機關保防的資訊安全，偏向公務部門，刑事局是社會保防，所謂社會保防，一般所謂社會案件皆有包括，但是一些有案件無法去分割，或是在法律上亦無法切割牽連，由那個單位先承辦或是線索哪邊先掌握，即由該單位承辦。」因此，從受訪者I的說法，可以發現政府在分工整合上，的確存在問題。

（4）無正式的組織架構。

資安會報是會議型式，是開會之模型，很多事件事發生了才在討論要如何執行。

（5）國家沒司法管轄權。

這部分已在前文論述。

二、「服務傳送機制、民間參與」

在「服務傳送機制、民間參與」上，政府職能角色部分與業者配合偵查，對此有幾個核心問題需要說明一下：

1、預防

（1）資訊安全委外存在問題

就B主任所言「首先我要說明的是NICI不存在，國家的資訊安全目前是委外的，資安會報全部都是資策會的人，從主任到底下的都是資策

會的人，沒有一個公務員，資安怎會好，…我們國家從不會承認資安不好或是資料外洩，把國家資安委外，裡面沒有一個公務員，…我們國家從不會承認資安不好或是資料外洩的，資策會的人不是公務員…。」

（2）資安會報，其實只是一種開會型式的任務編組。

就B主任所言「資安會報，其實只是一種開會型式的任務編組，不是常設機構，這個架構圖從綜合業務組技服中心的主任…都是資策會的人，都是資策會在主導，資策會裡面沒一個公務員，其實，網路主管機關要明定出來，其實目前資安是民間的資策會在主導，其實資安會報是開會才有，不開會就沒有，其實網路主管機關要明定出來，技服中心掌握國家的資安，竟然都是民間資策會的人，現在都是民間在主導…。」

（3）資安委外，綜合顧問組（科顧組）無正式考試通過之公務員。

G所言「我們就做策略規劃和跨部會協調，裡面雖沒參加國家考試，但是借調到科顧組，等同公務員的身分在做工作。」

（4）制定法源政策執行慢。

就G主任所言「比如我們又追蹤法務部修個資法的進度，像這法案一躺躺了3年，我們也在管制，像東森個資外洩，個資法是基本法，其他還有一些目的主管機關依個資法去訂定管理辦法，個資法是基本法，一些目的主管機關依個資法去訂定管理辦法。有的則原有管理辦法的有的會修正。」

「個資洩漏資部分就像東森，就是協調各相關主管部會，就會要求各主管機關，就其業管開罰，讓東森該負起責任，有些資安外洩是內部人員所為，有些機關例如銀行安全機制較高，像是金管會和金檢局就會要求各銀行，像東森也在想辦法，其實，個資法保護是夠的，民眾可以去告，只是還沒發生，當然修正新的個資法也還沒三讀通過。」

（5）業者若洩露個資，出事後未能被追討大筆金錢。

這是加強政府職能對網路犯罪防制政策執行上最有效的，新修正的

個人資料保護法有導入這種精神。

D說「資通會報有把機關分等級，但是，民間的有否分等級沒規範到，例如東森儲放民眾的個資，也沒分等級，若有主管機關應可迎刃而解。NCC一直認為網路不是其全管，當然是否包括人力或是人員仍還不足，國內企業東森資料外洩是一個例子，其本身應該負責任才是的，企業資料外洩規定通報，私人機構用罰則比較恰當，比如說資料外洩企業本身要負責，當然，政府若是對企業負責把關的資料庫測試攻擊，企業做不好定期公佈讓民眾選擇，並不是企業資料外洩就要用刑法來規範，反而用民事賠償的處罰更好，以高額的賠償，外國企業有因為這樣破產的。

國外，也有說有電腦前科不得從事電腦相關工作，對有電腦專業想作姦犯科的有赫阻的作用。」

2、偵查

網路犯罪本身具有隱匿性、無國界性等特性，雖然「凡走過必留痕跡」，但網路上的一切活動紀錄皆儲存在網路服務提供者之主機伺服器中，網路犯罪偵查若無網路服務提供者配合協助，絕難偵破。

網路犯罪防治的效果是「預防重於偵辦」，偵辦是最後手段，從預防網路犯罪之角度而言，網路服務提供者若能採取主動過濾方式或預防，對傳輸之資料進行檢核，發現可能有犯罪問題時立即加以攔阻，便可有效降低網路犯罪發生率。但我國並無任何法律規範可以要求業者進行網路資料的主動過濾。但依據電信法第8條及第22條，若網路服務提供者主動發現或經第三人通知使用者張貼或傳遞之意見、資訊涉有違法情事時，電信業者得以停止提供以妨害公共秩序及善良風俗內容爲營業之用戶（例如提供色情資訊營利的用戶）之虛擬主機租用、連線等網路服務之權利，或停止並拒有危害國家安全或從事販售槍毒違禁品等妨礙治安之違法內容之用戶繼續提供網路連線、e-mail 等服務之權利。但法令僅賦予業者權力（得刪除或停止使用權力），並未規範其義務（應刪除或停止使用權力），且此法令僅能規範國內網路服務業者，對境外網路業者並無適用餘地。

網路服務提供者主動過濾、刪除或阻斷網路上之犯罪資訊，目的乃在預

防網路犯罪之發生與損害，若網路犯罪已經發生，則網路業者是否能保存相關資料並提供作爲偵察與證據使用，更顯得重要。針對國內網路服務業者，有個人資料保護法上的限制，需由司法機關申請調閱特定範圍內之資料，較不易引發爭議，例如用戶連線IP，但如調閱使用者的資料傳輸內容，則恐有侵害個人秘密問題，例如調閱電子郵件信箱內容。針對國外網路服務業者，在無國際邦交、合作關係、法令限制下，要求配合偵查困難度將更高。

（1）資安會報只是一種開會的型式，預防偵查二面向協調皆不足。

中央的資安會報很完整，但是這卻是開會的型式，沒開會即不存在，很多時候都需要綜合規劃組（科顧組）聯繫協調的，綜合規劃組（科顧組）聯繫協調了好多事情，包括造成政策的形成規劃和執行，雖然效果亦不錯，但是，包括網路犯罪偵查面向上的形成規劃和執行，社會大眾媒體都不滿意。

中央警署B所講「首先我要說明的是NICI不存在，國家的資訊安全目前是委外的，資安會報全部都是資策會的人，從主任到底下的都是資策會的人，沒有一個公務員，資安怎會好，NICI不存在，從綜合業務組以下從主任到底下的都是資策會的人，沒有一個公務員，我們國家從不會承認資安不好…，等於全部委外裡面沒有一個公務員，我們國家從不會承認資安不好或是資料外洩，把國家資安委外，裡面沒有一個公務員…，我們國家從不會承認資安不好或是資料外洩的，資策會的人不是公務員，若是到大陸掛了，怎麼辦呢。NICI不存在，從綜合業務組以下從主任到底下的都是資策會的人，技服以下也都是資策會的人，技服負責國家整個資安，全部是資策會的人沒有一個公務員，NICI是一個開會型式，從綜合業務組到NICI都是資策會的人，就是國家的資安委外，等於說國家目前的資訊安全都委外…。」

第五章　結論與建議

第一節　政策面 （兼建議）

一、修法

在實體世界所發生之行爲會受到相關法律之規範，而在虛擬網路世界發生相同之行爲，並不會因其行爲發生在虛擬網路世界即不受規範，現行法律對實體世界或虛擬網路世界之行爲，大致已有相同之規範。但是，往往跟不上實際的腳步，各政府機關可依主管法律對於在網路上違法行爲依權責處理。由於修法可能曠日廢時，因此修法建議屬中長期，至於立即可行部分，則必須請主管機關出面進行協調。

若現行法律對網際網路上之行爲規範仍有所不足，可研修相關法律以爲規範，常見網路違法行爲及規範之法律如下，建請隨時針對網路犯罪現象，儘速修法：

表 6 修法類型建議表

犯罪類型	適用法律	列舉有關管轄機關
網路詐騙	中華民國刑法	警政署、電信局、通傳會 NCC
網路駭客（入侵）	中華民國刑法	警政署、調查局、通傳會 NCC
網路援交	兒童及少年性交易防制條例	兒童局、警政署
網路販賣色情商品	中華民國刑法、兒童及少年福利法	商業司、警政署
網路販賣盜版音樂、	著作權法	智財局、工業局、警政署

電影或軟體		
網路販賣違法食品	食品衛生管理法、健康食品管理法	衛生局
網路販賣管制藥品	管制藥品管理條例、毒品條例	衛生局、警政署
網路販賣性侵軟體	性交易防制條例、刑法	商業司、警政署、通傳會NCC
洩漏個人資料	電腦處理個人資料保護法	警政署、調查局、通傳會NCC

資料來源：本研究整理

又「電腦處理個人資料保護法」修正案已經在立法院躺了 3 年，此修正案對洩漏個資保護較週延，並牽涉到司法機關執法的法源，應儘速通過，是爲當務之急。

二、國家主政機制之建立

關於國家主政機制之建立屬中長期建議，立即可行的建議則請各主管機關出面整合。但因可能發生互相推諉的問題，若能央請檢察官或監委，可能發揮立即的整合功能。網路犯罪是一門新興的犯罪類別，係利用網路透過一個以往未見的虛擬空間，爲相關不法行爲致影響現實空間的犯罪行爲，而傳統的犯罪防治方法，對於網路犯罪雖亦有部分可資適用之對策，惟畢竟網路空間實迥異於現實空間，故傳統犯罪防治措施，實不足以完全預防網路犯罪的衍生，使網路空間的產生，雖造就了新的人類文明與生活，卻也形成傳統犯罪預防策略所不能防治的黑暗角落，以致網路犯罪預防工作漏洞層出不窮，終致網路犯罪不斷增加及不斷擴大，因此，我們應將重點置於政府管理體系之建立，尤其是以國家主管機關機制之建立，是當務之急。

目前「網路」並沒有主管機關，沒有管理的單位。網路的組成相當複雜，包含網路服務業者（Internet Service Provider ISP）、網路內容提供（Internet Content Provider ICP）、網路應用服務平台（Application Service

Provider APS），主管機關分歧。NCC目前不負責「網路內容」的規範，例如違反著作權法的部分屬於智慧財產局，線上遊戲的管理就屬於工業局。因此，應強化該機制，並建立一國家主管機關，爲目前所應從事之事宜。

國家資通安全基礎建設的角色區分，可參考下，目前國家資通安全會報的組織架構圖中，其實是作爲開會用的，俟開會時才臨時聚合，未能發揮功能，又其中的綜合業務組（科顧組）是關鍵，竟然都是不具公務員的經濟部委外的資策會人員擔任，這些人竟然召集管理網路犯罪工作組…等等（內政部警政署、法務部調查局、國防部、交通部）。

目前行政院資通會報，請行政院通傳會NCC邀集內政部、法務部、經濟部、交通部及金管會等相關機關組成「防治網路犯罪技術工作平臺」，共同研議網路犯罪防制措施。此爲通傳會NCC召集，「防治網路犯罪技術工作平臺」，此爲開會之性質，共同研議網路犯罪防治措施，然皆爲事後討論網路事件發生後需由哪些機關負責主政。

又通傳會雖然有與網際網路業務相關之單位（通傳會與網際網路業務相關之單位如下：(1)網際網路接取服務：營運管理處；(2)網際網路內容分級：傳播內容處；(3)濫發商業電子郵件管理條例：法律事務處；(4)資通技術安全：技術管理處），然網路範圍和牽涉機關眾多，未成立「網路安全處」，功能似乎不足。

行政院97年10月22日召開「防止電信及網路犯罪相關權責協調會（第2次）」，會議主席張政務委員進福裁示：有關網路犯罪防治議題，請通傳會邀集內政部、法務部、經濟部、交通部及金管會等相關機關組成「防治網路犯罪技術工作平臺」，共同研議網路犯罪防治措施。此工作平臺雖由通傳會NCC召集，但犯罪偵防仍是內政部警政署之職責。另有關網際網路平臺及內容之管理[25]，原則依下列分工辦理：

[25]又網際網路服務提供者（ISP）可分爲網際網路接取服務提供者（IASP）、網際網路平台提供者（IPP）、網際網路內容提供者（ICP）及網際網路應用服務提供者（ASP）等四大類。
1、IASP：係指以 xDSL、FTTx、Cable Modem、專線、3G 無線、撥接等方式提供網際網路連線服務之業者。
2、IPP：係指提供連線上網後各項網路平臺服務，包含在網際網路上提供儲存空間，或利用網際網路建置網站提供資訊發布及網頁連結服務等功能者。
3、ICP：係指實際提供網際網路網頁資訊內容者。
4、ASP：係指透過網際網路以租賃方式提供使用者應用軟體與系統軟體使用、管理與維護相關之服務。

1、網路平臺管理（IPP）：

（1）屬第二類電信事業之網際網路接取服務（IASP）爲通傳會NCC主政。

（2）非屬第二類電信事業之網路平臺爲相關權責機關主政。

2、網路內容管理（ICP）：

（1）電子商務由經濟部（商業司）主政。

（2）網路不當內容(色情暴力)由內政部主政。

（3）網路銀行由金管會主政。

（4）線上遊戲由工業局主政。

（5）網路盜版音樂由智慧財產局主政。

（6）網路僞藥由衛生局主政。

是以，遠程的話，建議國家成立網路安全局之類的機關。

目前當務之急，建議國家通訊傳播委員會（NCC）增訂法源和增加人才，似可成立網路安全處，國家通訊傳播委員會（NCC）並要正式派員進駐所謂行政院資通安全會報的組織架構圖中的綜合業務組（科顧組），以利督導傳遞彙整各公務機關之力量，對於機關組織、職掌功能及人力配置等建議，指定刑事局偵查員、NCC網路技術人員、經濟部商業局、資策會網路技術人員等，作爲對口合作人員，並定期提出解決方案，以維資通安全和網路犯罪

表 7 網路主政機制建立表

遠程	中程	近程
成立網路安全局	國家通訊傳播委員會（NCC）增訂法源和增加人才，成立網路安全處	國家通訊傳播委員會（NCC）正式派員進駐行政院資通安全會報的科顧組

資料來源:本研究整理

三、網路犯罪偵查機關法制化

科技警察跨部會整合力弱，刑事局科技（網路）犯罪偵查人員科技能力很強，問題是他們偵查過程發現的源頭管制問題，無法獲得其它部會的重視。例如，明明大家都知道網購問題重重，個資側錄與洩漏問題嚴重（個人交易紀錄洩漏或遭賤賣屢見不鮮），但因這至少牽涉國家傳播通訊委員會（NCC）、財政部（金融管理與通匯業務）、經濟部（商業登記）、法務部（詐騙與個資洩漏的處罰規定）等部門。這背後跨部會的協調聯繫與問題解決，就不是科技警察能力所及。

具體而言，例如針對電話與網路詐騙，行政院下設有「國家資通安全會報」(院長爲召集人，相關單位包括內政部、資策會、國科會、經濟部、財政部、衛生署、交通部、研考會)，警政署設有一六五專線，警政署刑事警察局設有科技中心（含偵九隊與電信警察隊，主要針對大型網路犯罪進行偵辦，包括大筆個資洩漏案件），各縣市警察局刑事警察大隊設有網路犯罪小組。從前述結構看來，主要面對電話與網路詐騙犯罪進行處理的是警察，資通會報的形式功能大於實質功能。但實際上警察只能作末端犯罪處理（所以才有在全國反詐騙日動員全國警察在ATM前站崗的反詐騙策略），對網路犯罪源頭（如個資洩漏）著力有限。因此，以目前政府的結構與分工，所能發揮的功能就受到限制。

通傳會邀集內政部、法務部、經濟部、交通部及金管會等相關機關組成「防治網路犯罪技術工作平臺」，共同研議網路犯罪防制措施。此工作平臺雖由通傳會NCC召集，但犯罪偵防仍是內政部警政署之職責。政府職能與角色，整體性、結構性與系統性看法：整體而言，僅網路犯罪之末端（警察）發揮一些功能，但警察（網路犯罪小組）偵辦網路犯罪的誘因不高，因爲績效配分低（必須和其它偵查員比績效配分）。

現在很多犯罪都跟網路、通信結合，但警察單位的整合是比較緩慢的，例如偵九隊不會和偵一隊共同偵辦犯罪，負責暴力犯罪的偵查隊沒辦法偵辦網路部分問題，這是專業分工下的缺點，資通合流，電信與資訊合併，刑事局偵九隊職能應擴充。目前成立針對網路犯罪，不管是中央的刑事局的科技中心的整合和地方的各縣市警察局刑警大隊科技犯罪偵查組，這雖然是一個

很重大的進步，但是，皆是任務編組，並不是法制化的單位，建請儘速法制化。

因此，立即可行建議：提高網路犯罪偵查小組之績效配分。短中期建議：指定相關單位對口合作人員，要求定期提出解決方案。長期建議：網路犯罪偵查小組績效不與其它小組作績分比較，行政院內部增設網路犯罪辦公室。

表8 網路犯罪偵查機關法制化政策建議表

立即可行建議	提高網路犯罪偵查小組之績效配分
短中期建議	指定相關單位對口合作人員，要求定期提出解決方案
長期建議	網路犯罪偵查小組績效不與其它小組作績分比較，行政院內部增設網路犯罪辦公室

資料來源：本研究整理

表 9 網路偵查機關法制化中央與地方執行單位建議表

中央	地方
刑事局科技中心 （結合資訊室、偵九隊、研發室、通訊監察中心之編組）	各縣市警察局刑警大隊 科技犯罪偵查組

資料來源：本研究整理

第二節　服務傳送之分析

一、行政院資通會報功能強化，發揮應有整合功能，勿使其淪爲開會的型式，並應結合治安會報情資，發揮功能。

短期而言，資通會報應與治安會報結合；長期而言，應由行政院網路犯罪辦公室作爲整合之專責部門。源頭管制部分，跨部會結合亦明顯不足，國家資通安全會報是依據總統於2000年8月30日核定之「建立我國資通資訊基礎建設安全機制」，而成立的組織（資通安全報告書，2001）。國家資通安全會報續開並發揮功能，勿使其淪爲開會的型式，並應結合治安會報情資，發揮功能，行政院資通會報功能強化。

具體的建議是，資安會報應與治安會報結合，但因治安會報所發揮的跨部會整合或結合功能亦非常有限，建議增設熟悉治安工作之政務委員。資通會報功能有限，例如電話與網路詐騙涉及電信、網路通訊（科技）、商業行爲、跨國網址與伺服器等跨領域與跨部門業務。當詐騙集團已形成跨領域與跨地域（含跨國）的緊密團隊，我們政府仍以「鬆散」的分工架構因應。並不是我們政府官員不認真，而是整合機制沒有出來。

例如就筆者瞭解，資通會報因係任務編組，且屬科技取向，所能發揮功能相當有限。可行辦法是與目前「治安會報」結合，只是目前的治安會報也是任務編組，因此，除非在行政院本辦指定整合單位，否則難以發揮整合功能。

二、設立單一窗口受理民眾通報及申訴。

短期而言，應加強165反詐騙專線報案與處理詐騙刑案功能；長期而言，宜就警察組織角度支持165專線功能。目前國內對網路採低度管理，政府應就網路管理，積極辦理規劃並落實權責分工，也應整合各單位設立單一窗口受理民眾通報及申訴，不要讓網路成爲販售非法物品的溫床，也避免各單位互相卸責的狀況繼續發生。

三、加強國際合作。

短期而言，應強化刑事局國際科之國際合作進行反詐騙功能；長期而言，則應由行政部門（含警政署與外交部）建構國際合作管道。因爲網路無國

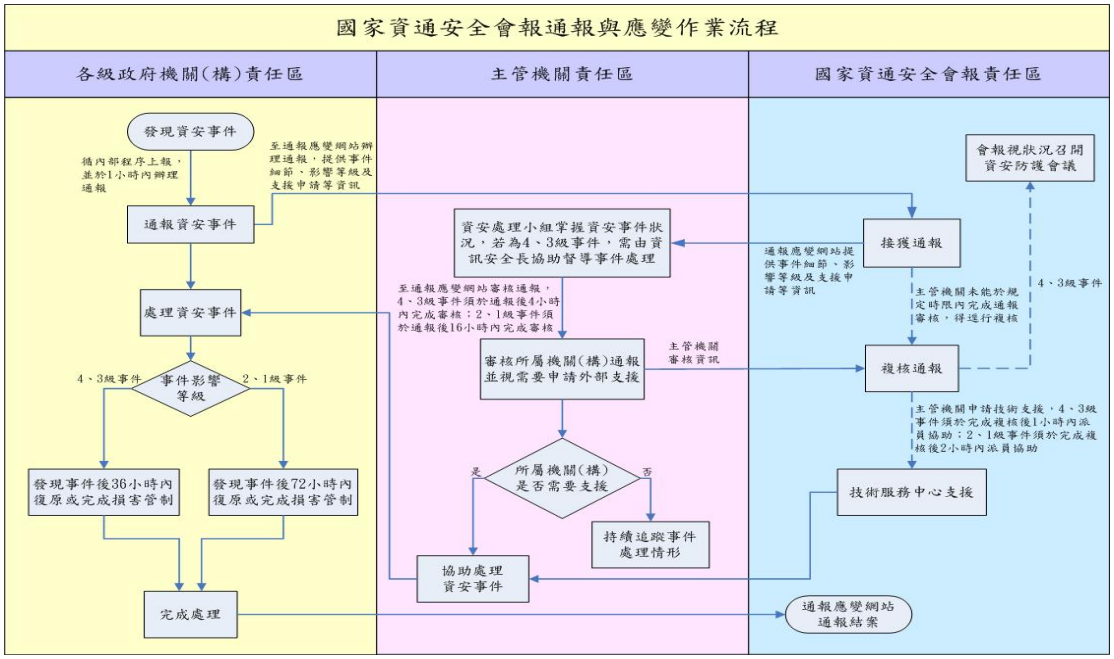
界，各國雖有司法管轄權問題，但是仍應加強國際合作與其他國家共同爲網路安全盡一份心力，跨國合作機制應強化，兩岸合作機制應強化。

四、策進政府憑證管理中心。

短期而言，應強化憑證管理中心功能，長期而言，則應建立憑證管理機制，讓憑證管理中心機制獲得更多之認同。政府憑證管理中心（Government Certification Authority, GCA），成立於西元1998年2月，目的是爲了將來在電子化政府中，確保民眾個人資料在網路傳輸的安全性，提供各項相關的安全憑證認證管理服務，故在電子化政府中，策進憑證管理，以確保民眾個人資料在網路傳輸的安全。

圖5便是我國國家資通安全會報通報與應變作業流程，可供參考。

圖 5　我國國家資通安全會報通報與應變作業流程



資料來源：行政院國家資通安全會報 98年2月5日

第三節、民間參與之分析

一、加強民間參與網路安全技術的研究

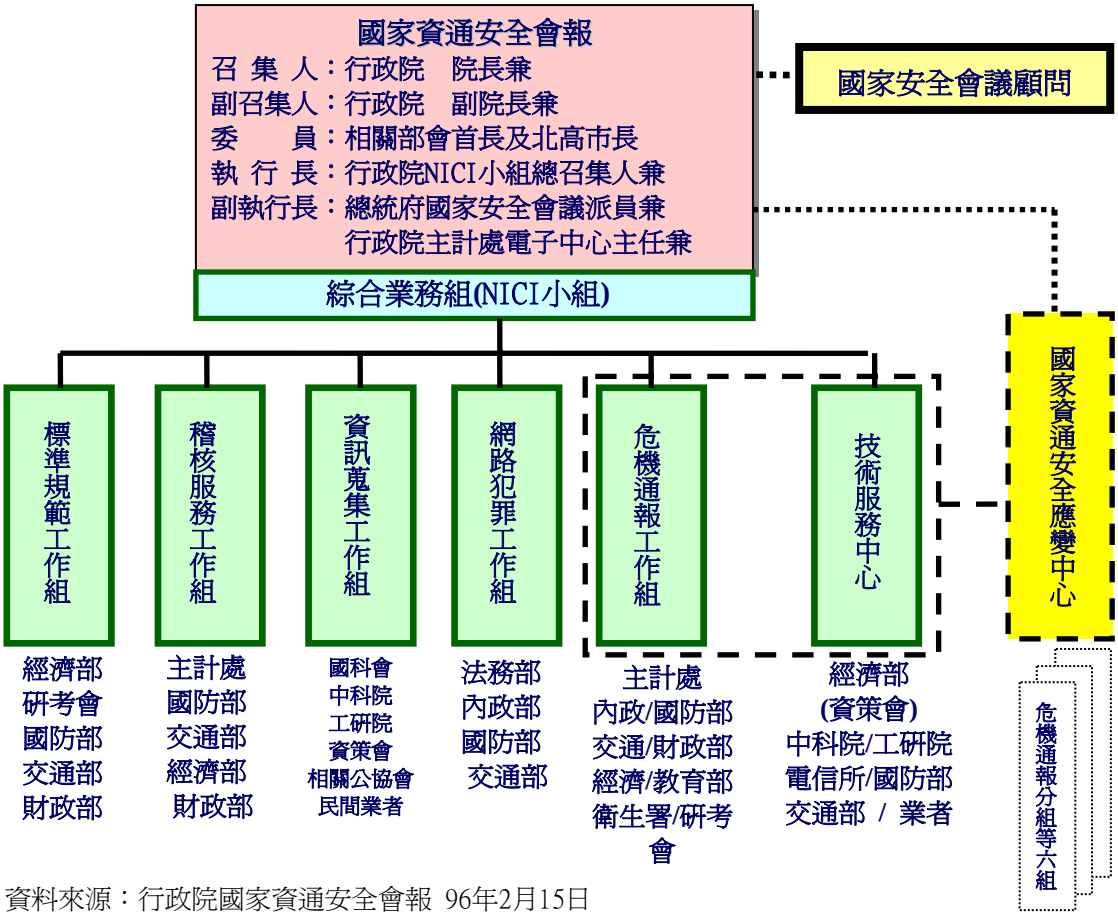
短期而言，應透過行政法規，要求業者重視網路安全技術之使用；長期而言，宜建立機制或誘因，鼓勵業者與網民重視網路資訊安全問題。重點包括：安全認證（Certification）技術、網路管理技術提昇、安全基礎技術，進行研究及實驗，以因應未來需要。

二、協調整合產官學研有關網路安全方面機制的整合，以提供國人更完善之服務與安全資訊

政府與民間皆對網路安全研究有所預防貢獻，但是要協調和整合產、官、學、研有關網路安全機制的整合，這部分仍有待政府努力。短期而言，可委託學術單位進一步研究結合之機制；長期而言，宜透過法規修正，鼓勵產、官、學不同領域人員進行合作。

在網路犯罪預防工作的實踐上，經常需要有多方面的配合才得以奏效，在所採取的各種防預措施或策略中，亦如傳統犯罪預防方式一般，並沒有單一的方法可以解決，各機關勢必對於不同的個案、環境，給予不同的處遇方式，或是數種方法策略併用，才能達到預防網路犯罪行爲發生的效果，是以，政府職能待加強且勢在必行。

圖 6　國家資通安全基礎建設的角色區分



資料來源：行政院國家資通安全會報 96年2月15日

參考書目

內政部警政署（2008），警政統計通報（97年第30號）。臺北：內政部警政署。Web site: http://www.npa.gov.tw/NPAGip/wSite/ct?xItem=41587&ctNode=11393&mp=1，visited 2009/4/6。

內政部警政署刑事警察局（2009），第三章　電腦與網路犯罪預防，web site: http://www.cib.gov.tw/crime/Crime_Book_Content.aspx?chapter_id=0000007&rule_id=0000003，visited 2009/4/6。

王秋惠（2006），網路詐欺被害特性與被害歷程之研究。中央警察大學犯罪防治研究所碩士論文。

李柏宏、廖有祿（1996），電腦犯罪之問題與對策。*警學叢刊*，第26卷，第6期，桃園：中央警察大學。

沈榮華（2002），網路犯罪相關問題研究。臺北：國防管理學院法律學研究所碩士論文。

林山田（2008），*刑法通論*。臺北：臺灣大學法學院。

林宜隆（1998），網路使用犯罪問題與防範對策之探討。第三屆資訊管理學術暨警政資訊實務研討會論文集，桃園：中央警察大學。

林宜隆（2000），網路犯罪之案例分析。*中央警察大學學報*，第37期，桃園：中央警察大學出版社。

林宜隆（2001），*網際網路與犯罪問題之研究*。桃園：中央警察大學出版社。

黃光雄、簡茂發（1993），*教育研究法*。臺北：師大書苑。

楊永年（2005），*組織行為*，桃園：中央警察大學。

楊永年（1999），網路警察之研究， 12月20日，中央研究院社會學研究所

三主辦(研討會地點)，第三屆資訊科技與社會轉型研討會。

楊國樞、文崇一、吳聰賢、李亦園編（1996），*社會及行爲科學研究法*（下冊）。臺北：東華書局。

Rosenbloom, D. H. & Kravchuk, R. S. (2005). *Public Administration: understanding management, politics, and law in the public sector.* New York: McGraw Hill.

Shafritz, J. M. & Russell, E.W. (2007). *Public Administration*. 5th ed. NY: South-Western College.

Weimer, D. L. & Vining, A. R.(2005). *Policy Analysis: Concepts and Practice, 4th Edition*. Upper Saddle River, New Jersey: Prentice Hall.

Wilson, J. Q. (1989), *Bureaucracy: what government agencies do and why they do it*, New York: Basic book.

附錄一：專家訪談紀錄

論文訪談對象代號對照表

專家名單	服務單位	訪談時程	編號
○○○　警務正	刑事局科技中心（偵九隊）	98 年 3 月 20 日	A
○○○　主任	警政署資訊室	98 年 7 月 9 日	B
○○○　主任	資策會	98 年 7 月 9 日	C
○○○　主任	警察大學刑事系	98 年 7 月 13 日	D
○○○　隊長	南區電信警察隊	98 年 7 月 13 日	E
○○○　組長	台南市警察局科技犯罪偵查組	98 年 8 月 17 日	F
○○○　主任	行政院科技顧問組 (資安辦公室主任兼企畫組長)	98 年 8 月 31 日	G
○○○簡任技正	國家通訊傳播委員會（NCC）營運管理處	98 年 10 月 17 日	H
○○○　科長	調查局資通安全處	98 年 10 月 19 日	I

一、**受訪談人：A**

訪談內容：

問：對「資訊安全」與「網路犯罪」職掌相關之議題和「網路犯罪」牽涉到的相關政府部門及中央職能區分，就犯罪的各項手法如何加強相關政府部門的各項職能。

答：整個詐騙的流程，大致上可以分爲個人資料取得轉帳、資料分析、詐騙、轉帳匯款，通常是利用 ATM 轉帳或電話語音轉帳，詐騙得手後再透過車手集團取款，之後進行兩岸匯兌之後，整個詐騙案件就結束了。

關於詐騙犯罪技術：

詐騙案件都是利用讓個案會覺得恐慌的方式，例如檢察官傳喚、銀行帳戶凍結等，讓個案覺得很恐慌之後，讓個案到 ATM 前詐騙。

早期詐騙集團是在網路上設置病毒或假網站，取得被害人的基本資料後再進行詐騙，但現在集團分工越來越細，在大陸就有一些集團專門在販售個人資料給一些詐騙集團，其資料來源大多是由購物網站進行資料的攔截與竊取，例如客戶登錄的姓名、電話、個人基本資料、住址、帳戶、信用卡號碼等。我們跟大陸在字碼的使用上是很相近的，大陸集團看到繁體資料就轉賣給大陸沿海地區的台灣詐騙集團。

取得個人資料有一些方式，例如設置假網站竊取使用者的帳號密碼後，再進入真正的網站竊取個人資料，或設置木馬程式竊取使用者的資料，但這樣的速度太慢，近幾年來已經轉換成入侵電子商務網站，竊取資料庫的資料。取得個人資料後就可以進行第二階段的詐騙。

整個詐騙犯罪流程中，詐騙是屬於比較低階技術水準的犯罪，比較高階技術的犯罪是駭客入侵資料庫竊取整個資料庫，很多駭客並不是爲了竊取資料而入侵資料庫，而是爲了成就感，但有機會可以販售獲利的時候他們也會販售。

目前詐騙集團取得個人資料後，會針對資料內容進行分析，分析個案是屬於哪一種身份，例如公務人員、老師、學生、現役軍人…等，再使用不同的詐騙手法去詐騙被害人。例如軍人用援交的方式，對學生用購物匯款錯誤，或涉嫌詐欺案件等，對老師、公務人員則使用退稅等方式。

詐騙手法需要取得被害人的信任，現在多會利用僞造來電顯示的方式，藉由市內電話漏洞，以第二類電信快於市內電話速度的方式，用第二類電信連結市內電話，然後僞造來電顯示號碼，或接聽電話。

現今防治詐騙工作：

目前台灣有 165 反詐騙專線的幫忙，已經對詐騙手法進行了詳細的分析，在詐騙預防上其實已經有相當大的成效了。詐騙偵查能破獲的案件數有限，在詐騙案件上，預防宣導所發揮的作用還是大於犯罪偵查

目前「資通合流」已經是全球趨勢。科技犯罪防治中心是一個任務編組，結合了刑事研究發展室、資訊室、通訊監察中心和偵查九隊、電信警察中隊。電信警察中隊屬於 NCC 屬於行政警察，偵九隊是爲了網路犯罪而成立，通訊監察中心則是關於通訊、電信方面的電信偵查、還有地下電台的案件，資訊室有刑案資料系統，屬於靜態的資料整合提供，研發室則是幕僚單位。這些單位是需要整合的，例如 SKYPE 可以由網路打到電信，電信警察中隊對 SKYPE 不瞭解，但對偵九隊來講 SKYPE 很簡單，但偵九隊不懂第二類電信的問題，所以必須互取有無彼此合作。

詐騙防治實務問題：

網路監聽在技術面上問題不大，透過伺服器可以鎖定特定人員調閱監聽資料，但由於伺服器通常設置在國外，外國並不同意調閱，這就變成行政上的問題了，在國內就沒問題了。

網路犯罪偵查的目的就是在鎖定當事人的 IP 位置，知道 IP 位置後就可以找到行爲人，在無限網路的部分，由於無線網路本來就比較屬於公眾使用範圍，因此比較難鎖定 IP 位置。

網路犯罪的偵查最重要的是犯罪資料的取得，很多技術層面上很簡單的事，但在行政上就變的很複雜，例如 SKYPE，直接伺服器將特定封包下載後經過解碼便可解讀，但在行政上卻沒辦法這樣做。因爲網路會跨許多國界，我們國家在國際上並未被視爲一政治實體，在國際上欠缺地位，沒辦法去要求業者提供支援。例如世界僵屍病毒台灣都沒辦法列席，因爲他們認爲我們不是一個政治實體，如果我們需要協助，就必須要透過中國大陸提出。GMAIL 也是，GOOGLE 亞洲地區總公司設在中國大陸，我們如果需要協助，也必須要經過中國大陸，所以在實務上我們有很大的行政限制，而不是在技術面上的問題。

現在詐騙集團幾乎都是兩岸合作，實務上比較麻煩的是對詐騙集團的掌握，我們目前跟大陸方面並沒有相關的合作協議，因此在整個集團的破獲上很頭痛。以往兩案刑事交流大多限定在重大刑犯的遣返，可是現在慢慢提升到互相合作。

現在很多犯罪都跟網路、通信結合，但警察單位的整合是比較緩慢的，

例如偵九隊不會和偵一隊共同偵辦犯罪，負責暴力犯罪的偵查隊沒辦法偵辦網路部分問題，這是專業分工下的缺點。目前科技中心的整合就是一個很重大的進步。

目前「網路」並沒有主管機關，沒有管理的單位。網路的組成相當複雜，包含網路服務業者（Internet Service Provider，ISP）、網路內容提供（Internet Content Provider，ICP）、網路應用服務平台（Application Service Provider，APS），主管機關分歧。NCC 目前負責的是「網路內容」的規範，例如違反著作權法的部分，但線上遊戲的管理就屬於工業局。

如果我們能夠爭取電腦網路公司在台灣設置分公司或辦事處，就可以協助解決很多網路犯罪問題，例如僵屍電腦與魁儡網路（Botnet）的問題，台灣其實有不少電腦被植入 BOT 程式（木馬、間諜、遠端遙控），我們也協助國際偵查不少案件。網路犯罪（Cybercrime）是一個全球性的問題，在偵防上也會走到全球化的趨勢。

目前我們和大陸的合作都需要透過香港來結合三地，沒有真正警察對警察的合作，我們要調大陸的資料，必須要透過偵查科兩岸組，藉以聯繫海基會-海協會-大陸警察，如果大陸警察不提供資料也沒辦法。針對重大刑案，兩岸警察合作比較順暢，但網路犯罪在大陸方面並非是重大案件，在處理上就比較緩慢。

透過警察-警察的方式取得的資料是有證據能力的，但在處理時程上十分緩慢，甚至無回應，透過業者之間的協調可以比較快速取得偵辦網路犯罪所需要的訊息，但在證據能力上就比較受限，這是我們法律上定位的問題。

目前我們對數位證據的證明能力比較沒有明確的規範，但電磁紀錄並不容易判讀，法官或律師也不懂這些東西，證據能力都是倚靠法官的自由心證，整個法庭上懂數位證據的可能只有嫌犯和偵辦的電信警察。

二、受訪談人：B

訪談內容：

問：對「資訊安全」與「網路犯罪」職掌相關之議題和「網路犯罪」牽涉到

的相關政府部門及中央職能區分，就犯罪的各項手法如何加強相關政府部門的各項職能。

答：首先我要說明的是 NICI 不存在，國家的資訊安全目前是委外的，資安會報全部都是資策會的人，從主任到底下的都是資策會的人，沒有一個公務員，資安怎會好，NICI 不存在，從綜合業務組以下從主任到底下的都是資策會的人，沒有一個公務員，我們國家從不會承認資安不好…，等於全部委外裡面沒有一個公務員，我們國家從不會承認資安不好或是資料外洩，把國家資安委外，裡面沒有一個公務員…，我們國家從不會承認資安不好或是資料外洩的，資策會的人不是公務員，若是到大陸掛了，怎麼辦呢。

NICI 不存在，從綜合業務組以下從主任到底下的都是資策會的人，技服以下也都是資策會的人，技服負責國家整個資安，全部是資策會的人沒有一個公務員，NICI 是一個開會型式，從綜合業務組到 NICI 都是資策會的人，就是國家的資安委外等於說國家目前的資訊安全都委外，是行政院研考會委託給資策會成立資安會報。

第二點，網路主管機關是誰，剛剛所講的 NICI 不是，行政院科顧組也擔任資安會報的召集人，其實都是資策會的人。NICI 是一個任務編組，一種開會的型式，裡面的網路犯罪工作組，裡面法務部就派一個檢察事務官，內政部警政署就是我們每次去開會開半天，沒有一個主管機關，例如，剛剛東森購物憑什麼存這些資料，洩漏有什麼責任，有何相關法令，現在個資法是損害才賠償，現在要修訂成洩漏就要賠償了，現在警政署和刑事局提出要請行政院網路是誰管，結果是電子商務什麼什麼歸哪邊管，什麼什麼歸哪邊管，當然這也不是推啦，但是散在各地方，先天上就有問題了，例如，雅虎關鍵字廣告誰管，它不是第 2 類電信業者，那誰管，不歸電信法管。

資安會報，其實只是一種開會型式的任務編組，不是常設機構，這個架構圖從綜合業務組技服中心的主任…都是資策會的人，都是資策會在主導，資策會裡面沒一個公務員，其實，網路主管機關要明定出來，其實目前資安是民間的資策會在主導，其實資安會報是開會才有，不開會就沒有，其實網路主管機關要明定出來，技服中心掌握國家的資安，竟然都是民間資策會的人，現在都是民間在主導，若明天他辭職了或是到大陸去了怎麼辦，公務員

才有權利義務啊，召集人和副召集人其實都是掛名，NICI 是鍾教授台大電機系的教授，例如，承認我們資安有什問題，向民眾說明和公佈我們資安有什問題，例如，說哪個網站或資料外洩了會造成許多詐騙電話，詐騙爲什麼會成立，就是資料外洩的問題，東森只是被蘋果報導出來，沒報出來的更多。

資安是攻與防，防是很費心的，攻的武器絕對比防的多很多，資料在網上就要考慮安全資安，顯現出來的就是治安詐騙電話，爲何還得逞，就是講的資料太準了，就是資料外洩。

電話詐騙和網路詐騙來的資料庫一樣的，犯罪使用的手法不一樣，但是，共同點就是資安，爲何會受騙，因爲不法分子講的太正確了，就是資料庫外洩，就是資訊安全啊，資訊的外洩歹徒掌握民眾資訊就會造成詐欺等等犯罪。

政府應該跳出來，網路應該有主管機關，要明定出來，要成立一個常設機構，要成立一個網路安全機構，其實 NCC 應該成立一個主管機關，NCC 有一個網路內容處，可是它也認爲不是主管機關，所以網路安全一定要有人管，例如，雅虎不是 2 類電信所以沒人管、PC Home 也都沒主管機關管，若有主管機關的話，妳網站上面爲何詐欺那麼多，不實的東西那麼多，我們可以行政作爲啊，可以減少頻寬，可以逼得業者注意資安啊。

所以，像美國 FCC 不知是否是網路主管機關，外國網路不知有沒有主管機關，日本、英國…等，台灣因有鄰居大陸，所以，木馬程式台灣是世界最多的，因爲大陸把這邊當練兵場，有些人專門賣偷到的資料庫，我認爲 NCC 應該是它來主管沒錯，但是，目前是分散的，因爲資安分成網路安全和資訊安全，現在二者是分散，現在網路內容是新聞局管分級、電子商務是經濟部管、電子的 ISP 是 NCC 管、網路犯罪歸警政署管....權責都分散了，其實應該有一個主管機關。

像技服中心的主任是劉陪文，是資策會的副處長，成大博士班剛畢業就指揮辦案 20 年的我們，技服中心副主任是吳家祺。綜合業務組的主任陳如芬，是資策會的經理，大家都是資策會的人，其實裡面要有政府的人，現在我們是倒過來，由他們主導政府部門，上下好像有倒置，綜合業務組由政府

派人就對了，不管是 NCC 或是研考會，國安局透過總統上大簽成立資安會報，國安局若主導綜合業務組也可啊，現在變成民間的資策會主導，很多公部門的 sense 民間的人士沒那個 sense，所以架構圖當中綜合業務組應有政府人員，又技服中心現在歸研考會管，研考會負責技服中心，吳啓文也是中科院的人不是公務員是薦派的，所以。至少綜合業務組應有政府人員進駐，甚至資安會報中分配的各組變成常設機構都可以，因爲資安實在太重要了，希望國家真的能看到這重要性。

三、**受訪談人：C**

訪談內容：

問：對「資訊安全」與「網路犯罪」職掌相關之議題和「網路犯罪」牽涉到的相關政府部門及中央職能區分，就犯罪的各項手法如何加強相關政府部門的各項職能。

答：資策會不是政府部門，NICI 只是一個會報方式開會用的，資策會責任應是有限的，像這圖示會報方式都不是一個常設機構，資策會是經濟部委託的單位，應該是比較技術性的，若這個資安會報架構圖之中的綜合業務組 NICI，應該是要由 NCC 來派人員才合宜，因爲 NCC 才是政府機關啊，NICI 其實本身是幕僚，它不是行政院的科技顧問組（目前科技顧問組是由前暨南大學校長張進福主持）例如我們的資策會另外一位專家，是從事 honey net，honey net 是一種誘捕網路的工作，他的上班地點在北指部那一邊，他們是負責網路是否被破壞，也不管民間的，像購物網站他們也不管，至於，網路犯罪範圍廣泛，你們研究的範圍應該是類似網路資料被外洩。

現在沒有一個法定機關管理網路，像資安會報中的 NICI 不是正式機關，人員都是資策會的，若是 NCC 派員進駐資安會報綜合業務組 NICI 才對，那情況又不一樣囉，但是目前的 NCC〈由新聞局廣電處和電信總局等等單位拼組〉也不認爲網路是由其主管，目前網路普及，政府和民間業者都應該很重視才對，由網路洩漏出的個資而衍生出各類型犯罪已經太多，詐欺猖獗就是這樣來的，至於網路犯罪都是已經發生了才由警察來主管，這些都是已經是末端的事情了，所以在前端的網路管理真的很重要，但是網路管理牽涉到資安的部分，我們這一邊是不負責民間的，例如他們的網站被入侵。至於，

網路犯罪的前端管理以及還沒犯罪前之網路管理目前是沒人管。

資策會不負責民間的，例如他們的網站被入侵個資外洩，也是新聞紕漏民眾才知道的，我們資策會也不管這個。

其實，網路在管理方面牽涉到政策面的，若是網路定一個最低標準，達到最低標準有給一種標章，其餘由民眾和與論去判斷取捨，也是一個可行方式，但是，基本上網路要有一個主管機關的。

四、**受訪談人：D**

訪談內容：

問：對「資訊安全」與「網路犯罪」職掌相關之議題和「網路犯罪」牽涉到的相關政府部門及中央職能區分，就犯罪的各項手法如何加強相關政府部門的各項職能。

答：因爲資料被拿出去，資通安全會報雖有規定要通報，但是在執行面上，一般被入侵根本就不知道，縱使察覺也不知道哪些資料被複製，第三個因素，各機關縱使被入侵，因爲面子問題，也不會通報，又各機關負責資訊安全的很多都是行政兼職的，做做網管而已，若有罰責，則更不敢通報，若是通報有鼓勵，倒還是有正面意義，其實每年各機關都有演習都有入侵和資訊演習，看看各機關的通報速度，在政府的測試攻擊中，各機關有不同層次的攻擊，所以這資訊安全的通報很弱，各機關能夠自己處理就處理，很少通報，各單位被入侵很少治本來解決，都是治標的，這不包括很多未發現的，大的單位人才較多，比如警政署的防衛系統就是比較好，另一種入侵被植入木馬這也是一種方式。

資通會報有把機關分等級，但是，民間的有否分等級沒規範到，例如東森儲放民眾的個資，也沒分等級，若有主管機關應可迎刃而解

NCC 一直認爲網路不是其全管（全部管轄），當然是否包括人力或是人員仍還不足，國內企業東森資料外洩是一個例子，其本身應該負責任才是的，企業資料外洩規定通報，私人機構用罰則比較恰當，比如說資料外洩企業本身要負責，當然，政府若是對企業負責把關的資料庫測試攻擊，企業做不好定期公佈讓民眾選擇，並不是企業資料外洩就要用刑法來規範，反而用民

事賠償的處罰更好，以高額的賠償，外國企業有因爲這樣破產的。

國外，也有說有電腦前科不得從事電腦相關工作，對有電腦專業想作姦犯科的有赫阻的作用。

一般偵查員也不喜歡辦網路犯罪，具我所知，第一配分低，第二業者不配合，第三辦案時間長，第四在網咖等場所犯罪，網路犯罪警察都辦比較有功獎的、好辦的、技術層次低的，技術層極高、難辦的配分又低，所以大家也不辦，縱使有專責單位，也沒有專責在專責的工作上，反而找些有功獎的技術層次低、不困難的網路犯罪在辦。

政府機構若已經負責一個工作，要再接另一個工作，除非有誘因，不然不會自我找砸的，像 NCC 不接網路主管，可能是其人才或是物力技術不夠，所以公務機關要律定一個主管真是不簡單的，

又網站的規範若是有主管機關給個證照，民眾也會比較有保障。

五、**受訪談人：F**

訪談內容：

問：「資訊安全」與「網路犯罪」相關之議題和「網路犯罪」牽涉到的相關政府部門，中央與地區(職能)區分，地方服務傳送機制。如何加強相關政府部門的各項職能。

答：網路詐欺 2 大宗，一在露天一在雅虎，雅虎在把關方面的審核機制愈來越嚴格，除了電話認證外，加上雙證件且一個身份證只能申請 2 個或是 3 個帳號，要申請垃圾帳號比較少，露天只要用手機認證就可以了，身分證就可以申請，所以用身分證產生器，申請一堆垃圾帳號上去開始貼了把別的賣場網複製過來，把電話改一改，價錢改一改，帳號帳戶填的資料都是假的和人頭手機等都是假的，詐騙的成本因爲警察查緝金融帳戶，所以詐欺集團金融帳戶現在成本較高。

從人頭電話人頭帳戶的詐騙到現在的三角詐騙，到 8591 等等詐騙，用到虛擬帳號、三角詐騙….等等.案例中也有 13 歲的少年就開始詐騙，若一般的網路詐騙，雅虎.蕃薯藤..等等查一查 IP 單純的就這麼查了，若複雜的用無線網路寬頻的上去的，學校的無線上網寬頻，有時根本不知道誰上網的

，網咖也常不知是誰上去的，所以這些都是治安的死角，現在網路普及，上網速度其實都一樣了，會到網咖去的，有時都是有問題的，比以前複雜很多，網咖也是一個管理的漏洞，像駭客入侵…等等犯罪，所以網咖、一些公部門或是公共場所，反而是管理的漏洞，在追來源的時候，反而是困擾，因爲使用者沒留下任何資料，查到最後只查到最後的 IP 而已，所以只要你不留下真實的身分。

其實，任何一台電腦連接到雅虎會產生一組 B-COKY，B-COKY 比較少人知道，有時可以以假的搜出真的，國外的根本調不到資料，連台灣的公司，也故意給你英文的，很多搜尋引擎要不到資料，中央刑事局調資料應該比較好調。

中央刑事局和地方警局其實沒分工，網路無國界，但是重大的刑事局都會主動偵辦，中央刑事局人員比較完整，人才比較多，但是中央刑事局雖是科技中心，跟我們地方警局一樣，也不是法制化的單位，是任務編組。

網路的案子一般移到地檢署，大都會尊重我們的專業，地檢署對網路不知是否有分專組，網路是一種專業，但是網路犯罪比較隱性，不像辦槍毒等大案，所以偵辦網路犯罪可能也就沒誘因，這情況在警界中也是一樣。

網路犯罪向派出所報案，派出所送分局偵查隊，分局有偵辦能力存疑，地方警察局科技小組連我組長才 4 個人，人才人力都不夠，其實網路這個東西，真的其實很專業，刑事局人員人才人力比較多，地方警局科技小組有時也要分擔其他專案，所以在地方警局其實專業度也不夠。

網路犯罪有時查出的 IP 都是在外國，但是外國或是國外我們也都沒有司法管轄權，駭客也常在國外，境外犯罪有待努力，有些國家查資料還要當地國家法院的許可，所以國外的資料不好拿，若是 SKYPE 網路電話根本調不到資料，即時通是在伺服器都有資料，若是網路監聽叫做封包側錄，公共場所像網咖就很難測錄，個人的家用電腦比較可行。

網路業者要加強把關，要有被害人報案，若要是境外來的偵查就困難了，網路若真的存心要犯罪，偵查真的困難，只能偵辦一些比較無知無意的犯罪，真的是集團專業的、境外的很難查得到，中央刑事局爲地方警局半年辦一次講習，其實辦的不錯，地方警局比較沒能力辦講習，人才和時間都不夠

，若查到管轄權在境外，真的沒輒，所以，希望有心人不要去犯罪，網路人才會越來越多，到時候犯罪可能越多，地方警局教育訓練太多元太雜了，根本沒辦法深入，警察每項業務都重要，每項都重要，急迫性最急的才處理，三角詐騙產生的無辜受害者，縱使釐清了關係，都還是要移送給檢察官認定，所以都還是很麻煩的。

六、**受訪談人：G**

訪談內容：

問：貴單位承辦的網路相關業務，那些和資訊安全(網路犯罪有關)，做些什麼？「網路犯罪」牽涉到的相關政府部門及中央職能區分，就犯罪的各項手法如何加強相關政府部門的各項職能。

答：電話和網路詐騙，是目前犯罪的大宗，像這個資安會報組織架構圖是否有發揮功能，要到某個政策的層次才會上這個會報，若是工作的層次則不會上這個會報。

所以我跟警署○主任看法若有些許的不同，那是角度的問題。

在這個架構圖裡，有一個網路偵防工作組，包括法務部和內政部等，我們做政策的規劃，刑法 2003 年刑法妨害電腦使用專章就是網路偵防工作組重要法源。

我們會在政策的層次去建議要有法源，比如內政部成立警政署偵九隊，2005 年要法務部建置資安鑑識實驗室。

比如我們又追蹤法務部修個資法的進度，像這法案一躺躺了 3 年，我們也在管制，像東森個資外洩，個資法是基本法，其他還有一些目的主管機關依個資法去訂定管理辦法。有的則原有管理辦法的，有的會修正。

最近，一個老婦人被電話詐騙了 700 萬，引起劉院長的關注，就在治安會報中要政府去瞭解，就請科技政務委員處理。

當我們介入去看，在執行面的確有些問題，我們就找出這些漏洞來規劃，也對警政署不足的部分來加強規劃，並對警政署資源不夠的地方爭取資源。

我們就做策略規劃和跨部會協調，裡面雖沒參加國家考試，但是借調到科顧組，等同公務員的身分。

像剛才 700 萬的案子，還有跟通傳會 NCC 有關，像各機關有何管理或是技術可以突破的，就請 NCC 協調中華電信過濾來話國碼。

所以我們協調各單位我們都在想辦法。

個資洩漏資部分就像東森，就是協調各相關主管部會，就會要求各主管機關，就其業管開罰，讓東森該負起責任，有些資安外洩是內部人員所為，有些機關例如銀行安全機制較高，像是金管會和金檢局就會要求各銀行，像東森也在想辦法，其實，個資法保護是夠的，民眾可以去告，只是還沒發生，當然修正新的個資法也還沒三讀通過。

像東森個資外洩，最大的業管機關是誰呢，其實我們不能單純化，網路本身就有好多單位，應就其所業管的來發揮其規劃，網路犯罪主管機關是內政部，但是這是末端。

但是，說網路無主管機關是把問題過度簡單化，例如，網路平台大都是第 2 類電信事業，是通傳會管，網路是無店面購物，是經濟部主管，若賣的東西是衛生署業管，當然是衛生署管…等等，但是主管機關中要有一個主窗口。

七、**受訪談人：H**

訪談內容：

問：請就 NCC 對「資訊安全」與「網路犯罪」職掌相關之議題，以及所牽涉到的相關政府部門提出說明。

答：行政院 97 年 10 月 22 日召開「防止電信及網路犯罪相關權責協調會」會議，主席張政務委員進福所裁示之網際網路平臺及內容管理分工之原則，本會與網際網路業務相關之單位如下：(1)網際網路接取服務：營運管理處；(2)網際網路內容分級：傳播內容處；(3)濫發商業電子郵件管理條例：法律事務處；(4)資通技術安全：技術管理處。

進一步說明如下，網路與現實世界一樣，要由一個主管機關管到全部，

實際上不可能的，現實世界有多少事情有多複雜，虛擬世界就有這般現象，那當然就會牽涉到各單位或是各目的事業主管機關，至於網路犯罪，是內政部警政署主管的，相關資料或許那邊會較齊全，像刑事局科技中心研發室黃組長就常代表與會。

在實體世界所發生之行爲會受到相關法律之規範，而在虛擬網路世界發生相同之行爲，並不會因其行爲發生在虛擬網路世界即不受規範，現行法律對實體世界或虛擬網路世界之行爲，大致已有相同之規範。各政府機關可依主管法律對於在網路上違法行爲依權責處理。若現行法律對網際網路上之行爲規範仍有所不足，可研修相關法律以爲規範。

八、**受訪談人：I**

訪談內容：

問：請就「資訊安全」與「網路犯罪」相關之議題，偵查職掌，提出說明。

答：資訊安全與網路犯罪其實五花八門，目前本局資通安全處負責機關保防的資訊安全，偏向公務部門，刑事局是社會保防，所謂社會保防，一般所謂社會案件皆有包括，但是有一些案件無法去分割，或是在法律上亦無法切割牽連，由那個單位先承辦或是線索哪邊先掌握，即由該單位承辦。

附錄二：審查意見處理對照表

審查意見	修正
在網路犯罪、法規研究、政府角色及公共政策四大面向間之結構聯結性似仍有所不足。	在各篇章已針對政府職能與政策角色未扮演之處再著墨，以加強結構聯結性。
研究發現均整理自訪談結果，而焦點座談與深度訪談的對象多爲政府機關(構)相關專業人員，所提出的論點，多係基於其所屬機關(構)之立場與角度，而無法對議題本身提出整體性、結構性或系統性的看法，不免有見樹不見林之憾。這些問題致使本報告對於「政府職能與角色」所作之推論及建議，欠缺具說服力的邏輯論證與較爲深入且具體可行的實質性建議。	本文已經加入計劃主持人楊永年所著之「反詐騙有那麼難嗎」一文，於第五章結論與建議回應。
受限於既定之分析架構，於「政策形成」、「政策規劃」與「政策執行」等三層面所提出之研究發現與結論，內容有相當比例之重複，如缺乏主管機關、專業不足、急待修法及跨機關協調不夠等諸多問題，多同時出現於政策形成、規劃及執行等不同層面。	重複之部分，業已刪除，至於專家說話跨議題之部分則保留。
在建議事項方面，所提出之建議確可切中問題，具相當之參考價值，惟其中部分似流於浮面，較欠缺具體可行的實質方案，如建議資通安全會報應發揮其整合功能，勿使其淪爲開會的形式。惟究	已經就所述增補內容，做出建議。

應如何在組織或功能上進行檢討重組，方可使該會報不致淪爲一個僅是被動解決問題的會議組織，則未有任何較爲具體可行的建議或方案。另如建議成立國家網路安全局或 NCC 下的網路安全處，對於機關組織、職掌功能及人力配置等亦未有相關積極建議，建請酌作補充。	
本研究報告內容有極高比例係引述深度訪談及焦點座談對象之談話內容(報告內容中斜體字部分)，並將談話內容直接作爲報告內容文字，未以研究團隊之角度另作彙整論述，且引述之談話內容係直接以逐字紀錄稿方式呈現，未作任何修飾整理，其中不乏語意有欠通順、口語化甚至較爲情緒性之字語，建請酌作修飾調整。	已作修飾整理。
在文字部分，第四章「研究分析與發現」之內容，對不同議題之討論，引用相同受訪者之看法，且內容雷同之處極多，這種文字重覆出現的情形前後共有十餘處，影響報告品質至鉅，建請重作調整修正。另第 19 頁第 10 行稱我國政府網路犯罪防治架構如圖 4，惟圖 4 是研究架構圖而非防治架構如圖。又第 45 頁最後 1 行「有關網路犯罪政治理度分，如圖 4-1 所示」，惟查報告內文並無圖 4-1 及第 51 頁「NICI」建請加註中英文全銜。併請修正。	已經修正。
本研究報告第五章結論與建議，建請針	已經修正。

對所研提之建議區分短、中長期之政策建議，以及明列主協辦機關。	