數位時代的國家安全與全球治理

Digital Security and Global Governance

doi:10.30390/ISC.200412_43(6).0002

問題與研究, 43(6), 2004

Issues & Studies, 43(6), 2004

作者/Author： 彭慧鸞(Hwei-Luan Poong)

頁數/Page： 29-52

出版日期/Publication Date：2004/12

數位時代的國家安全與全球治理

彭 慧 鸞

（國立政治大學國際關係研究中心
第二研究所副研究員）

摘 要

由於新的戰爭與衝突形式是建立在人類科技不斷創新的基礎上，因此，科技與國際安全議題的聯結將成為國際間建立新秩序，或是進行全球治理的過程中不可忽略的重要課題。如何架構一個以數位科技所衍生的安全問題（以下簡稱為數位安全）為核心的全球治理模式已是當務之急。「九一一事件」的發生，再次提醒了我們，當前人類或國家所面臨的迫切安全威脅，不只來自於門檻較高的核子大戰，也來自於隨時可能出現的不對稱恐怖戰爭。也因為數位科技的無所不在，產生了資訊社會高度依賴數位科技之後的易脆性（vulnerability），而這個易脆性正是國家安全（state security）與人民安全（civilian security）彼此鑲嵌（embedded）的結果。

本研究試圖說明數位科技的不當使用將成為二十一世紀國家安全的新威脅，雖然為了因應數位科技世代所面臨的安全威脅，全球與區域網路安全治理建制已經逐步在形成之中，然而跨國性的數位安全治理仍將因為制度行為者本身安全易脆性的差異性、國家主權的衝擊以及數位科技犯罪的監督不易等因素，無法發揮應有的功能。本研究嘗試提出「鑲嵌安全」的概念，主要目的在於破除「國家安全」與「人民安全」傳統分界，並主張唯有國家行為者與非國家行為者確實認知數位時代「鑲嵌安全」的本質，並將此認知具體落實在政策層面，才可能擺脫前述治理困境，並架構一個全球數位安全網。

關鍵詞：數位安全、國家安全、人民安全、網路安全、網路恐怖主義、不對稱戰爭、全球治理、反恐外交、安全的鑲嵌性

* * *

前 言

自從二〇〇一年九月十一日在美國紐約和華盛頓發生了自殺飛機恐怖攻擊事件之後，反恐成爲各國政府與人民最關切的安全議題。從聯合國決議文到區域組織與論壇的共同宣言，乃至於各國政府的反恐政策與措施，不難看出，二十一世紀的國際政治所要面對和處理的，除了傳統的國家安全議題之外，還包括了非國家行爲者（non-state actor）對國家行爲者（state actor）所產生的非對稱性的威脅，或者稱之爲不對稱戰爭（asymmetric warfare）所帶來的安全問題。

而數位科技的發展，也衍生出不對稱戰爭的新行爲模式。歷史經驗顯示，從火藥、核子彈的發明，到運輸通訊等技術的演進，導致戰爭與衝突形式有了不斷創新的基礎。本研究的目的乃是試圖檢視網路恐怖主義（cyber terrorism）對國家安全的威脅，以及目前形成中的全球治理機制及其治理困境。「九一一事件」的發生，再次提醒了我們，當今人類或國家眼前迫切的安全威脅，不只是一場發動門檻較高的核子大戰，更是隨時可能出現的不對稱恐怖戰爭。而網路恐怖行動則又凸顯數位化之後所產生的安全易脆性。從數位科技無國界無時差的特性來看，此種數位化所衍生的易脆性將國家安全與人民安全緊密鑲嵌在一起。

從安全治理的角度來看，此種安全的易脆性直接衝擊到國家安全與人民安全治理上彼此區隔的制度結構。因此，如何在制度上協調國家機關與非國家行爲者，放下傳統制度角色的堅持，彼此分工合作是突破困境的關鍵。然而，制度結構的調整往往必須從概念的釐清開始，本研究的目的即在嘗試提出國際關係研究的一個新議題方向，就是從國家安全與人民安全彼此釀嵌的角度，探討數位安全的治理模式。

壹、數位安全之定義與分析架構

數位科技的發展對人類社會乃至於國際社會互動行爲模式的影響到底有多深？這是所有社會學者必須正視的問題。在社會科學的學術市場中，研究者從不同的面向詮釋數位科技的衝擊，例如，經濟學者可以直接從市場的角度觀察科技對人類交易行爲的影響，社會學者可以從數位落差的角度研究數位化發展所帶來的社會衝擊，政治學者可以嘗試從政治參與的觀點探討數位化民主的問題，而政治經濟學者可以剖析數位化發展的制度結構問題，傳播學者可以從溝通學的角度切入數位傳播的議題，對於國際政治和國際關係研究學者而言，如何從傳統國際政治研究方法中，找到切入點作爲連結數位科技與國際政治與國際關係研究的分析界面（interface），則仍處於探索階段。但是從數位科技的安全治理的角度切入，或許可以提供國際政治與國際關係學者一個新的議題領域，本文擬從數位安全與安全治理兩個層次的問題作進一步分析。

一、數位安全的意涵

無論是希臘城邦時期，或是西發利亞和約時期，到如今數位科技時代，戰爭與和平一直是人類與國際社會不能迴避的國際政治核心問題。沃爾夫（Arnold Wolfers）在 1962 年的著作**衝突與合作**（*Discord and Collaboration*）一書中提到「安全、權力和財富是每個國家所追求的三大核心價值。…財富的價值在於是否實際的擁有，權力的價值在於對其它行爲者的控制時，安全的價值則在於國家追求這些核心價值時能免於受到威脅。」①易言之，國家安全是指國家對已經獲得的價值的保障。如果將沃爾夫在二十世紀中對安全的界定，放在二十一世紀數位時代的人類追求多元價值的普遍趨勢中，一樣能完全適用。對應於沃爾夫對國家安全的定義，本文所稱之「數位安全」所探討的是國家在追求數位科技所帶來的價值的同時，如何免除其不當使用所產生之後果的相關問題。②因此，數位安全在概念上應該是資訊安全（information security）、網路安全（cyber security）和網絡安全（network security）的綜合概念。例如，在針對重大基礎設施的網路恐怖行動之中，安全威脅的層面從內部管理網絡的掌控開始，進而入侵內部網路系統、破壞資訊處理的能力，最後癱瘓基礎設施的網絡系統。換言之，與基礎設施相關的軟、硬體安全都應該包涵在「數位安全」的概念之中。

更明確而言，數位科技的不當使用所衍生的個人安全問題或許不是國際政治學者關注的議題。然而，當非國家行爲者透過數位科技，跨越國界威脅到他國人民大規模生命財產的安全時，個人層次的安全問題立即提昇爲國際層次的安全問題。隨著科技的精進，此類跨越國界的安全威脅將有增無減。然而數位安全問題的探討至今似乎仍僅止於一些會議論文或是政策研究，有系統的學術研究則付之闕如。基於數位科技，尤其是網際網路本身具有跨越疆界、跨越層級、跨越時空等特性，它對國家和人民生命財產安全的有形與無形威脅程度，未必低於核武軍備競賽。③因此，數位安全的研究是國際關係研究責無旁貸的重要議題。

就研究範疇而言，數位安全應該涵蓋國家安全與人民安全兩個不同層次又彼此鑲嵌的的安全議題。但是就安全概念的關鏈性來看，本研究所稱「數位安全」的概念，

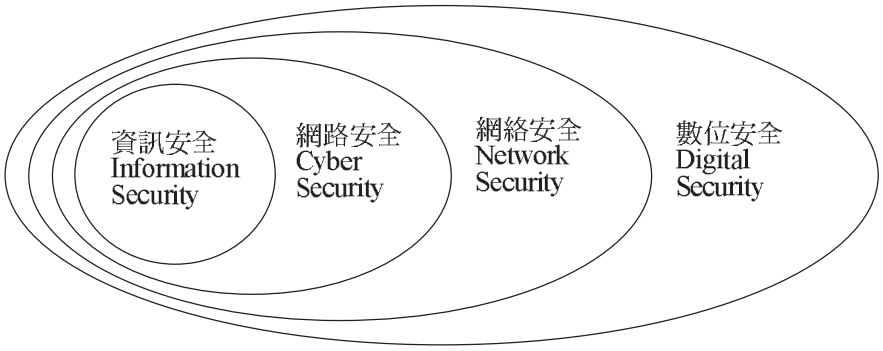
註① Arnold Wolfers, *Discord and Collaboration: Essays on International Politics* (Baltimore, Maryland: The Johns Hopkins Press, 1962), p. 150.

註② 而此處之「數位科技」除了網際網路之外，也涵蓋了衛星通訊、傳眞、手機、錄影機、錄音機等設備。

註③ 網路攻擊的主要目的是「阻斷服務」(denial-of-service, DOS)。通常非法入侵網路者（俗稱「駭客」）可以透過置入病毒碼，垃圾郵件或電子郵包炸彈、竄改網頁等方式達到阻斷服務的目的。一般網路病毒攻擊通常是敵我不分，但是垃圾郵件則可以設定目標展開攻擊。例如 1997 年美國一家網路服務公司因爲接受支持西班牙巴斯克分離主義的網頁登記而受到西班牙民族主義者抗議，發動電子郵包炸彈攻擊，癱瘓該公司的網路設備，造成其客戶的嚴重損失。至於正規軍的資訊戰則是將網際網路應用在部隊間、與政府部門、其他民間部的通訊，以及情報收集上。對於軍方而言，這些網路系統也可能成爲被攻擊的目標。

基本上含蓋了國家安全層次的「網絡安全」（Network security）以及以網際網路爲核心的「網路安全」。至於「網路安全」的意涵，可以引用二〇〇三年聯合國世界資訊高峰會總結報告曾對網路安全作出範圍的界定，「凡在一國之內受到來自境外電腦病毒、木馬程式等病毒碼破壞網路系統，造成網路或資料上的破壞，則稱之爲網路安全（Cyber security）」。④因此，網路安全，只是網絡安全中的一環。換言之，網路的不當使用造成個人網路安全的干擾或威脅，在程度上不同於網路恐怖行動間接導致人民生命財產的損失所帶來的傷害。但是網路恐怖行動有時必須透過網路安全漏洞進行恐怖行動。因此在安全治理的實務運作上，「數位安全」與「網路安全」仍有密不可分的鑲嵌關係。（請參考圖一）

圖一　資訊安全、網路安全、網絡安全與數位安全的安全鑲嵌概念圖



資料來源：作者自製。

儘管資訊戰與網路恐怖主義都是利用網路攻擊敵人的戰爭或準戰爭行爲。但是資訊戰在本質上，是屬於國家與國家之間戰爭手段的資訊化，有別於網路恐怖主義是發生在非國家行爲者與國家行爲者之間的非傳統的超限戰。前者並未改變戰爭衝突的兩造是國家行爲者的基本結構。因此，本文所稱的「數位安全」是針對後者而言。就網路恐怖行動者而言，網際網路既是其發動恐怖活動的重要工具，因此有別於一般的網路駭客，網路恐怖份子有其特定的攻擊標的，且通常是爲了特定政治目的而行動，譬如「遠端操控」入侵所謂「關鍵基礎建設」（critical infrustructure），包括資訊通信、金融電子交易系統、食品衛生醫藥製造流程、航空地面交通指揮系統、各種能源管線輸送控管系統、維生服務系統，造成全國性的破壞。因爲網路恐怖主義的特色是「境外決戰」，無需現身就能從「虛擬實境」中取得戰果。以一九九五年阿根廷網路

註④　WSIS Executive Secretariat, "Report of the Geneva Phase of The World Summit on the Information Society," Geneva-Palexpo, 10-12 December 2003. Document WSIS-03/GENEVA/9(Rev.1)-E 18 February 2004, p. 49. <http://www.itu.int/wsis/documents/doc_single-en-1179.asp>, 在報告中並未將垃圾郵件（SPAM）問題列入網路安全範圍。

駭客入侵美國海軍作戰指揮系統的案例來看，⑤隨著駭客行動能力的不斷提昇，恐怖份子利用駭客行動入侵上述「關鍵基礎建設」的內部網路系統並非不可能。

以美國爲例，85％的關鍵基礎建設由民間部門負責設計、建造、維修。事實上，有關「關鍵基礎建設」的戰時安全防護緊急應變方案早已存在多年，只不過這些措施基本上是針對硬體保護所設計。然而近年來，由於資訊科技的普遍應用，使得大部份的基礎建設開始大量仰賴電腦系統提昇運作效能，進而促使各國政府開始重視基礎建設相關的數位安全問題，也就是政府部門必須確實掌握民間部門對其電腦網路系統提供服務時，不致受制於後者。基於以上考量，美國柯林頓政府在一九九六年曾以行政命令總統辦公室成立了「關鍵基礎建設保護委員會（Presidential Commission for Critical Infrustructure Protection, PCCIP）」。然而九一一事件發生之後，國土安全部隨之成立，將關鍵基礎建設的防護責任納入該部所屬的「國家基礎建設顧問委員會」（National Infrustructure Advisory Committee），其主要的功能之一就是在保護民生相關的關鍵基礎建設資訊系統的安全。

總之，對主管國家安全戰略的政府部門而言，傳統的戰略思維與安全治理模式已不足以因應不對稱戰爭所衍生出來的安全問題。因此，數位安全概念的建立，是安全治理不可或缺的一環。

二、分析架構

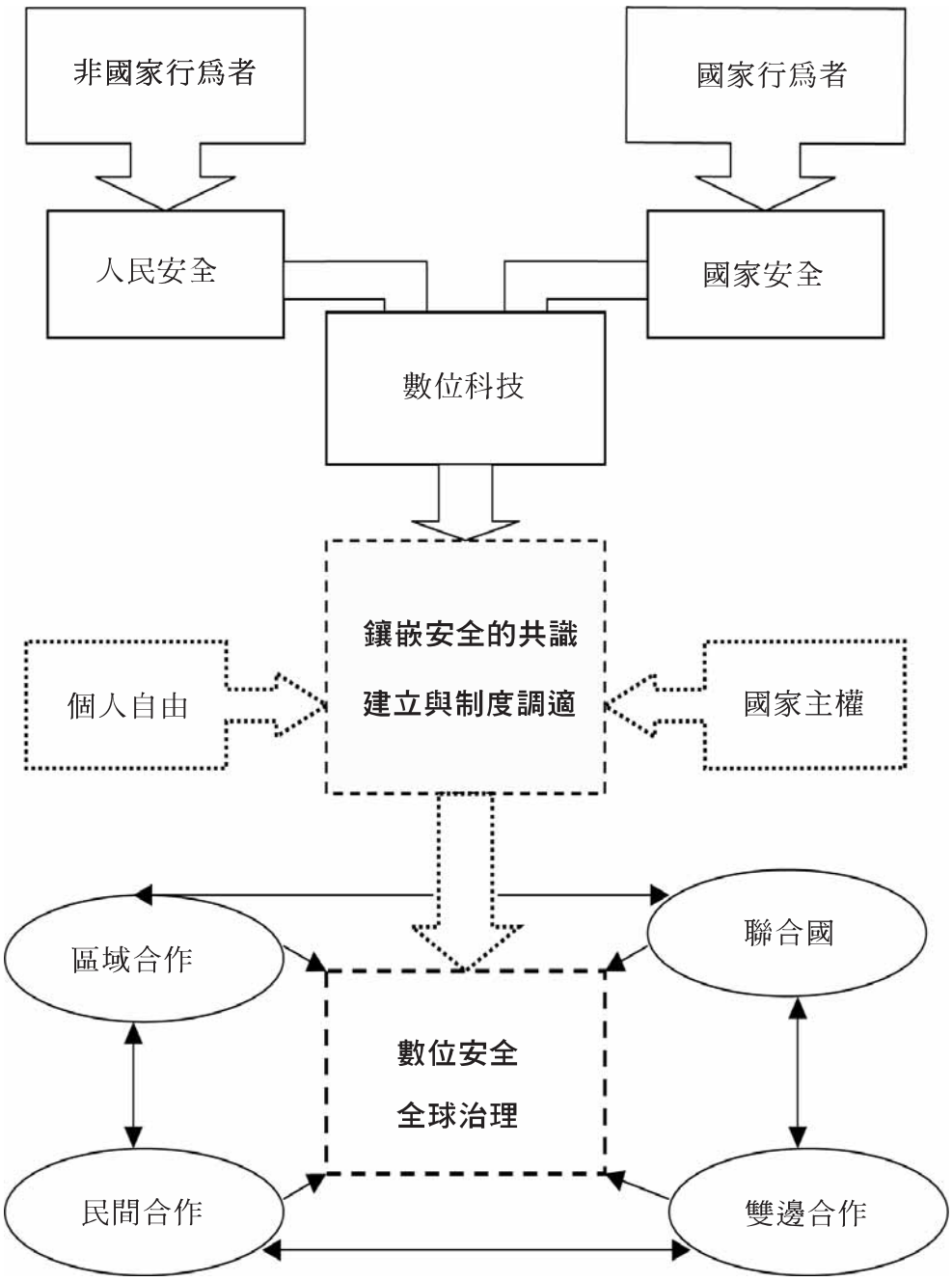
圖一的分析架構圖旨在說明，「鑲嵌的安全」是一個國家安全與人民安全的界線模糊，而且無法完全分割的安全概念。例如，在數位安全議題上，國防與民防之間處於必須彼此合作與共享資源的新制度關係。同時，受到數位科技普及化的影響，個人的影響力大幅提昇，經由「人民安全」的威脅啓動「國家安全」危機的機率正逐漸提昇。因此，在數位安全治理的建制過程中，非國家行爲者的參與是建制運作成功與否的重要關鍵。以二〇〇〇年「電腦千禧蟲」危機事件爲例，「資訊分享與分析中心」（Information Sharing and Analysis Center, ISAC）、「電腦緊急應變小組」（Compater Emergency Readiness Team, CERT）等民間組成的電腦監督組織，成功地在世紀交替之際成功地完成防堵的 Y2K 電腦「千禧蟲」災難的治理工作。⑥

然而數位安全治理的基礎在於國家行爲者與非國家行爲者間，鑲嵌安全的共識建立與制度調適。以現有的數位安全治理的工作包括聯合國、歐盟和亞太經合會（Association of Asia-Pacific Cooperation, APEC）區域合作組織、美國爲核心的雙邊合作機制以及以資訊分享與緊急應變爲主的民間機構等，雖然已經在安全治理的不同層面展開協調與合作，但是仍免不了出現一些治理困境。因此圖二中虛線部份說明了傳統國家主權與人民自由的基本價值，面對鑲嵌安全的衝擊時，能否建立安全共識並進行制度調適，是數位安全治理必須克服的首要工作。

註⑤ 詳細資料，請參考 <http://www.hanford.gov/oci/ci_spy.cfm>.

註⑥ Olivia Bosch, "Cyber Terrorism and Private Sector Efforts for Information Infrastructure Protection," paper presented at Workshop of the ITU Strategy and Policy Unit on Creating Trust in Critical Networks, on 20-22 May 2002, Seoul, <http://www.itu.int/osg/spu/ni/security/workshop/presentations/cniBosch%20paper.pdf>.

圖二　鑲嵌安全與數位安全治理分析架構



資料來源：作者自製

依據此一分析架構圖，本文將首先說明數位科技普及化對國家安全與人民安全認知上的衝擊，其次將比較當前不同層級數位安全治理的形式，及其治理的困境。本研究的目的在於解釋，「數位安全治理」的建制工作，必須在國家行爲者與非國家行爲者，對「鑲嵌安全」有共識的基礎之上進行制度的調適，才有可能突破傳統安全治理的障礙。⑦國家行爲者必須認知「數位安全」沒有國界之分，因此局部讓渡國家主權是有效安全治理的重要基礎。非國家行爲者也必須了解在網際網路時代的「個人自由」是建立在「集體安全」的前提下才能獲得眞正的保障。

叁、數位時代的國家安全

一、高度數位化的安全易脆性

依據二〇〇三聯合國電子商務發展報告書的分析，從一九九七年開始，網際網路通信正以每年二倍的速度成長。依據加州大學資訊管理學院的研究統計，到二〇〇七年爲止，人類每天在網路上流通的資訊量，換算成書本文字，將需要 5,400 萬公里的書架來陳列，而這個長度則相當於地球到火星的距離。⑧在這高度數位化的資訊社會中，人類是否會因爲擁有更多的資訊與選擇而更爲安全？還是會面臨如奈伊（Joseph Nye）與柯漢（Robert Keohane）所定義的相互依賴的易脆性? 這種相互依賴的易脆性的大小，和相互依賴者具備替代選項的能力有關。⑨因此，數位化發展的國家而言，如果民生供應運輸相關的基礎建設數位化發展的同時，忽略了替代方案的建構，則其相對脆弱性也將提高。

例如，二〇〇三年八月十四日北美洲發生長達 29 小時有史以來最大規模的無預警大停電，在紐約和西徹斯特郡所有 310 萬名家庭和企業用戶，以及美國 8 州和加拿大 2 個省份計 4900 萬名家庭用戶飽受斷電之苦。雖然由美國和加拿大共同組成的調查小組未能証實此一事件的發生與恐怖主義或是駭客攻擊有關，但是報告中特別提到軟體程式錯誤是造成該次大停電的重大原因之一。此一無預警大停電造成將近 70 至 100 億美元的經濟損失。民生網絡系統的易脆性在此顯露無遺。⑩理論上，數位化程度愈高

註⑦ Ernst B. Haas, *When Knowledge is Power: Three Models of Change in International Organizations* (Berkeley, Calif.: University of California Press, 1990).

註⑧ United Nations Conference on Trade and Development, *E-commerce and Development 2003 Report,* <http://www.unctad.org/ch/docs//ecdr2003overview_ch.pdf>.

註⑨ Joseph S. Nye and Robert Keohane, *Power and Interdependence: World Politics in Transition* (Boston, Mass.: Little, Brown and Company, 1977); Joseph S. Nye and Robert Keohane, "Power and Interdependence in Information Age," a policy research group of Kennedy School of Government, Harvard University. <http://www.ksg.harvard.edu/prg/nye/power.pdf>.

註⑩ "Final Report on the August 14, 2003 Black Out in the United States and Canada: Cause and Recommendations," <https://reports.energy.gov/BlackoutFinal-Web.pdf>.

的國家，其承受網路攻擊的機會比低度數位化的國家爲大，因此對於「數位安全」的重視程度也愈高。職是之故，由於「數位落差」（digital divide）問題的存在，也影響到「數位安全」共識的建立。

二、數位科技助長衝突的不對稱性

所謂的網路恐怖主義，是指非國家行爲者爲了政治目的使用電腦及電子網路散播恐嚇言語，或是發動大規模破壞行動。由於非國家行爲者與國家行爲者之間先天性的實力不對等關係，因此恐怖行動者只能透過不對稱性攻擊方式才能達到政治要脅的目的。一九九〇年代以來，隨著科技的進步，恐怖行動者獲得網際網路的挹注，一方面可以更有效的執行跨國性大規模破壞行動，引起全球媒體和政府的注意，而達到向國家行爲者進行政治要脅的目的。另一方面，透過網際網路無所不在且又能匿名行動的特性，恐怖組織可以更有效的進行集結發動攻擊。其行動所帶來的破壞性與人員傷亡效果，甚至不亞於一場以武力對峙的戰爭。

以賓拉登（Osama Bin-laden）爲首的「國際恐怖網際網路」（international terrorist internet），是一個相對自主的網路系統，其創始者賓拉登以自己的財富支持多個回教極端份子聯盟，而聯盟的基地就是所謂的「蓋達」（Al-Qaeda），由賓拉登本人親自指揮，其主要的任務是與聯盟內其他團體或單位聯合行動。他利用網際網路進行調度，具備快速轉換見機行事的能力，因此不易被反恐行動者偵測到發動者的行蹤。⑪因此，全球連網化提高了恐怖分子的戰力。依據訪問過賓拉登的記者報導，賓拉登擁有電腦、通訊裝備與資料儲存用的磁碟。並在埃及裔的阿富汗電腦專家協助下設置了一個全球資訊網、電子信箱與電子佈告欄，提供極端份子自由交換資訊而不會被反恐行動發現的管道。⑫蓋達組織的連網形式（chain-net）說明了網際網路對恐怖行動的加乘效果，已經對現今國家安全造成了重大威脅。

三、人民安全與國家安全的鑲嵌性

就數位安全而言，由於資訊化社會對網際網路的高度依賴性，舉凡重大基礎建設與民生供應系統也都已經朝向數位化發展。在網際網路時代，這些非軍事地區正好成爲網路恐怖份子發動恐怖攻擊的最佳目標。因此，傳統國家安全決策者在面對數位安全問題時，需要具備「鑲嵌的安全」，亦即安全不可分割的概念，突破部門本位主義進行資源的整合。

註⑪　John Arguilla, David Ronfeldt, and Michele Zanini, "Networks, Netwar, and Information-Age Terrorism," in Zalmay Khalilzad, John P. White, Andrew W. Marshall, eds., *Strategic Appraisl: Changing Role of Information-Age Warfare* (Santa Monica, Calif.: Rand Corporation, 1999), p. 95, <http://www.rand.org/publications/MR/MR1016/MR1016.chap4.pdf>.

註⑫　同註⑪。

具體而言，網路恐怖份子的行爲包括遠端遙控衛生食品工廠的生產流程，製造對人體有害的產品；或者透過遠端電腦操控的炸彈，進行大規模恐怖攻擊造成民衆的重大傷亡；或者破壞金融電子交易系統，擾亂經濟秩序；或是攻擊航空或鐵導交通控制系統，癱瘓甚至釀成大規模的交通事故或災難；或是改變油管內的壓力指數，造成管線輸送系統癱瘓。也就是說，透過網際網路遠端遙控的技術，網路恐怖份子不需要冒著生命危險，可以很方便進入基礎建設或是民生供應系統進行破壞，遂行政治恐嚇。

四、 數位安全政策的國際化

數位時代的國家安全就如網際網路所呈現的的無國界特性，也面臨國家安全治理無國界的考驗。由於網路恐怖主義的攻擊行動經常是境外遙控跨國界進行，而且是利用安全政策不完備的地區發動攻擊，例如二〇〇〇年造成全球電腦嚴重災情的「I LOVE YOU」電腦病毒，就是利用菲律賓政府並未立法禁止未經授權進入他人電腦的行爲。易言之，反制網路恐怖行動的國家安全政策，若無法獲得國際合作則將功虧一簣。

因此，無論是聯合國反恐決議案、二〇〇一年十一月十七日完成的「歐盟網路犯罪協約」（Council of Europe Convention on Cybercrime）或是美國政府公布的「網路空間國家安全戰略」（National Strategy to Secure Cyberspace）都強調網路空間安全，必須仰賴國際合作。[13]依據聯合國的定義，全球治理的目的是通過制定和實施全球的或跨國的規範、原則、計畫和國際公共政策來實現共同的目標和解決共同的問題。[14]因此，在網路安全治理相關政策的立法與執行都將涉及各國國內制度的調整。

以歐盟網路犯罪協約爲例，互惠立法（reciprocal legislation）目的是相互協助提供網路攻擊的電子舉証或跨國蒐證是數位安全政策國際化的基礎。其他如即時網上蒐證（real-time collection of tragic data）、網路資料跨國攔截（interception of content data）、罪犯引渡、最輕刑度（minimum penalty）等的共同約定都將使得數位安全政策加速朝向國際化發展。

註[13] 其他各項分別是：(一) 全國網路空間安全反應系統；(二) 全國網路空間安全威脅與弱點排除計畫；(三) 全國網路空間安全認知與訓練計畫；(四) 政府網路空間的防護。參考 Executive Summary of The National Strategy to Secure Cyberspace. <http://www.whitehouse.gov/pcipb/executive_summary.pdf>.

註[14] 1995 Report of UN Commission on Global Governance, *Our Global Neighborhood*. <http://www.sovereignty.net/p/gov/gganalysis.htm>.

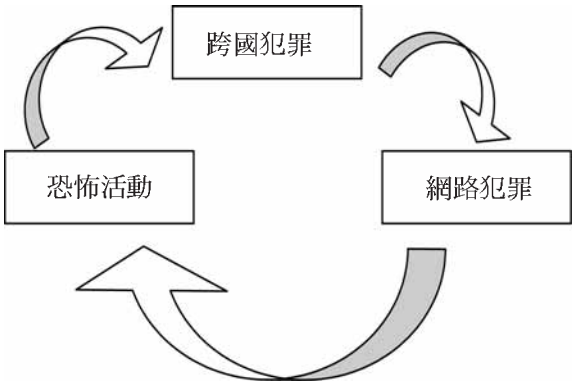
肆、數位時代的安全治理

依據聯合國「全球治理委員會」之定義，⑮全球治理是從地方到全球的多層面公共權威與私人機構之間的種正式與非正式的政治合作體系，其目的是通過制定和實施全球的或跨國的規範、原則、計畫和國際公共政策來實現共同的目標和解決共同的問題。⑯因此，數位安全的全球治理基本上也是針對數位科技不當使用之行爲所設計出來的規範、原則、行動綱領與政策安排。

一、數位安全網絡的共犯結構

隨著全球化的發展，跨國犯罪、恐怖活動的日益嚴重，使得「人民安全」與「國家安全」的釀嵌性成爲二十一世紀人類必須嚴肅面對的新課題。尤其是當科技的發展與網際網路的普及化，更加添了跨國犯罪與恐怖活動的組織動員能力。因此跨國犯罪、恐怖活動與網路犯罪（cyber-crime）已經形成跨國安全的結構性潛在威脅。（圖三）事實上，單純的網路犯罪未必一定就有恐怖行動的意圖，而恐怖份子也未必都具備網路攻擊的能力。

圖三　數位安全威脅的共犯結構關係



資料來源：作者自製。

註⑮　聯合國在一九九三年設立了「全球治理委員會」(Commission on Global Governance)，委員會的運作經費主要是來自「聯合國開發計畫」(United Nation Development Program, UNDP)，一九九五年正式以「我們的全球鄰舍」(Our Global Neighborhood) 爲題發表了一篇重要報告，在410頁的報告中建議聯合國大會在一九九八年召開世界治理會議(World Conference on Governance)，從此聯合國召開了一系列有關全球治理的會議。1995 Report of UN Commission on Global Governance, "Our Global Neighborhood," <http://www.sovereignty.net/p/gov/gganalysis.htm>.

註⑯　同註⑭。

但是具備網路攻擊能力的業餘玩家一旦受到金錢利誘時，則可能被吸收成爲網路恐怖行動的代理人或幫兇。⑰同時，所有網路恐怖行動，爲了自身安全的保障，通常是利用國內司法管轄權互不侵犯的制度偏差，透過境外伺服器迂迴展開攻擊，因此，數位安全治理所要處理的是由跨國犯罪集團、恐怖份子與網路攻擊業餘玩家（cracker）所形成的共犯結構問題。因此，無論是在多邊層次的聯合國或區域組織，與數位安全相關之共同宣言或協約，其內容皆涵蓋上述三個層面的問題。易言之，數位安全治理必須與跨國犯罪和反恐議題連結才有實質意義。

二、聯合國的數位安全治理原則

早在二〇〇〇年九月聯合國大會總務委員會在第 9 次全體會議中作成決議，依據一九九八年十二月四日通過的 53/70 號決議文和一九九九年十二月一日通過的 54/49 號決議文，正式將國際安全相關的資通發展議題交付「第一委員會」討論，⑱同年九月十四日在第一委員會的第二次會議討論裁武與國際安全議題的同時，特別就前述議題進行辯論並完成決議草案。第一委員會會議總結報告是以「資訊通信發展對國際安全的影響」（Developments in the field of information and telecommunications in the context of international security）爲題獲得委員會無異議通過。報告獲得以下初步結論，包括：(1) 多層次推動網路安全對策之研究；(2) 強化全球資訊與通信系統安全概念的正確認知；以及(3) 對資訊安全的界定。⑲該報告爲數位安全的全球治理提供了重要的架構方向。

除了聯合國第一委員會之外，「國際電信聯盟」（International Telecommunication Union, ITU）也是推動數位安全全球治理的重要機構。二〇〇三年在瑞士日內瓦召開的「世界資訊社會高峰會議」（World Summit of Information Society, WSIS）中，⑳ITU在會議總結報告中首次提出了建設資訊社會的基本原則。㉑其中與數位安全

註⑰ "The Future of Cyber Terrorism: Where the Physical and Virtual Worlds Converge," remarks by Barry C. Collin, presented at 11th Annual International Symposium on Criminal Justice Issues, August 7, 1996, <http://afgen.com/terrorism1.html>.

註⑱ 聯合國大會共設有六個委員會，第一委員會主要是負責安全相關議題。

註⑲ Report of the First Committee, UN General Assembly Fifty-fifth session, Developments in the field of information and telecommunications in the context of international security.

註⑳ 二〇〇一年十二月二十一日聯合國大會通過決議案，由聯合國秘書長負責籌辦「世界資訊社會高峰會議」，「國際電信聯盟」負責相關行政事務。並決定分別於 2003 及 2005 分別在日內瓦和突尼斯舉行兩次高峰會議。所有會議議程及籌備工作由跨政府籌備委員會(Intergovernmental Preparatory Committee, PrepCom)負責。

註㉑ 十一個重要原則爲：(一)政府與民間以及國際組織在資訊化社會建構過程中扮演不可或缺的角色；(二)資訊與通信基礎建設是資訊化社會發展的最重要根基；(三)資訊與知識的取得必須機會均等；(四)提昇個人或國家參與資訊化社會的基本能力；(五)建立對資訊通信安全的信心；(六)以資訊通信技術強化全球治理；(七)創造資訊通信技術的應用環境；(八)尊重文化差異；(九)確認言論自由以及獨立多元的媒體對資訊化社會的重要性；(十)資訊社會道德問題的強化；(十一)國際與區域合作加速資訊化社會發展。"Report of the Geneva Phaseof the World Summit on the Information Society."

全球治理相關的內容重點包括，資通安全的信心建立（表一）與資通技術全球治理（表二）。從行動綱領中的項目內容來看，網路安全治理的重點在於建立政府與民間合作關係，透過法規、制度的建立，資訊與經驗的分享以及網路技術的更新，重建使用者對網路安全的信心。並邀集政府、民間及國際組織和相關團體，共同研擬包括加速推動相關概念的釐清與加強教育宣導工作的「網路治理」工作。

表一　ITU有關資通安全信心建立的行動綱領

（一）加強聯合國會員國政府間合作，同時透過論壇強化使用者對網路的信心；
（二）政府與民間合作建立指導綱領、推動相關立法、建立相互支援機制、強化國際間建制性的支援查察犯罪事實，乃至於教育宣導等事項，共同防範與打擊網路犯罪；
（三）政府及利益相關團體應積極推動網路使用者有關網路穩私權及保護的常識及警覺性；
（四）在國內和國際層面應正視垃圾郵件問題並採取必要的措施；
（五）各國加速電子認証的立法；
（六）透過隱私權與消費者的保護的強化建立信心安全架構；
（七）彼此分享資訊安全與網路安全的實務經驗；
（八）邀請有興趣的國家設立提供立即事件處理反應實際運作據點，並在據點之間建立合作網絡，彼此分享相關資訊與處理的技術；
（九）開發更安全可靠的網路應用技術；
（十）歡迎有意願的國家主動參與進行中的聯合國網路安全信心架構計畫。

資料來源：同註④。

表二　ITU「網路安全治理」相關的行動綱領㉒

（一）各國政府必須採取透明化、鼓勵競爭、可預期的政策與法規架構吸引投資發展資訊化社會；
（二）呼籲聯合國設置「網路治理工作小組」（working group on internet governance），邀請包括已開發和開發中國家的政府與民間團體，以及相關的跨政府組織和國際組織或論壇，共同研議網路治理相關的行動建言：其內容應包括：(1) 網路治理的定義；(2) 釐清與網路治理相關的公共政策議題；(3) 就各參與的政府、組織和論壇的相關角色和責任形成共識；(4)將研議的結果會整成報告提交二〇〇五年突尼斯回合WSIA會議時討論。
（三）建議各國政府設置各自國內以及區域的網路交換中心；負責各所屬國家域名（domain name）的監督和管理；加強各自國內對網路的宣導。
（四）與相關機構合作推行跨越區域的伺服器及國際域名以便克服上網障礙問題。
（五）政府應持續修定消費者保護法以因應資訊化社會的需求。
（六）鼓勵開發中國家和經濟轉型中的國家參與（International Counter-Terrism, ICT）的國際論壇，進而獲取其他國家的發展經驗。

（續下頁）

註㉒　同註④。

（接上頁）

（七）各國需要積極推動電子化政府，以利行政透明化、效率化與民主化。
（八）政府與相關機構應積極主動對民眾進行網路隱私權保護的宣導教育。
（九）提供電子商務運作環境，同時讓使用者可以有所選擇。並建立健全而有效的爭端解決機制。
（十）通過有助於 ICT 發展的創新投資政策，特別協助中小企業獲得資金與企業再造，進而有能力參與在 ICT 相關的計畫中。
（十一）政府應率先在電子商務上示範作用。建立全球電子商務的國際標準。採用公開、可互通、不歧視，而且是需求導向的標準。

資料來源：同表一。

三、區域性數位安全治理規範

歐盟的「歐盟網路犯罪協約」是目前唯一的多邊數位安全協議。早在一九九七年歐盟便成立「網路犯罪專家小組」並開始研擬網路犯罪防制對策。並在二〇〇一年公佈協約內容正式提交由各簽約國政府立法追認生效程序。雖然名稱爲「歐盟網路犯罪協約」，但是歐盟主要成員至今仍未參與簽署。截至二〇〇三年爲止，包括日本、美國、加拿大、南非等非歐盟成員簽約國已達 36 個。簽約國中以美國布希政府最爲積極，並於二〇〇三年十一月正式提交參議院外交委員會討論。

此一協約內容大致包括對網路犯罪的界定，以及推動各國政府相關立法與國際合作。依據協約規定，駭客（包括製造、銷售、散播工具者）、兒童色情網站、侵犯智慧財產權等屬於犯罪行爲，㉓該協約詳細內容包括四章 48 條，除了第一條的名詞定義，以及第三十六至四十八主要說明條約之執行與效力問題之外，第二至第十二條的內容主要是詳列電腦犯罪的行爲認定，第十三至二十二條則是要求簽約國配合相關立法與政策執行的項目，第二十三至三十五則詳列國際合作項目。依據第二十三條的說明，簽約國必需本於互惠精神，完成國內相關立法，以便於各國進行網路攻擊事件的調查以及相關電子事証的收集。

亞太地區國家的數位安全治理，基本上是架構在 APEC 的兩次重要會議之結論上。其一是二〇〇一年十月「APEC 非正式領袖會議」發表的「反恐共同宣言」，以及二〇〇二年五月「APEC 電信部長會議」在上海發表的有關「資訊通信基礎建設安全行動計畫」。在安全治理的實務運作方面，首先由二〇〇三年成立的 APEC「反恐工作小組」（Counter Terrorism Task Force, CTTF）協調各國政府的反恐行動，同時委由「電信資訊工作小組」（APEC Telecommunications and Information Working Group, TEL）協助會員體強化網路安全。由 APEC 電信資訊工作小組所主導的 APEC 數位安全策略（APEC Cybersecurity Strategy），基本上是遵循聯合國 55/63 及 1390

註㉓ “Convention on Cybercrime, Explanatory Report,” <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

號決議案，以及歐盟網路犯罪協約的內容所架構而成。㉔

就實際內涵來看，「APEC數位安全策略」大致涵蓋六個層面的合作，包括（一）法制基礎：如網路犯罪法、網路犯罪調查權與國際合作共同查緝網路犯罪的法源基礎；（二）資訊的分享：如網路犯罪預警機制的設立，透過事前評估與即時支援，將威脅擴散危機降至最低，如網路犯罪防專責單位與「電腦緊急應變小組」（CERT）的設置，作爲各會員體間相互協助的對口；（三）安全與技術指導：發展更精進的資訊安全加密技術與認証標準，協助政府與企業打擊網路犯罪，進而保護「關鍵基礎建設」；（四）觀念宣導：透過引介經濟合作發展組織（Organization for Economic Co-operation and Development, OECD）資訊網路指導方針，以及設立相關網站等方式向會員體政府、企業、消費者加強網路安全與網路倫理（cyberethics）的公民教育；（五）訓練與教育：透過政府與民間部門雙軌進行，加強各會員體政府與企業部門有關網路安全技術與法律人才訓練。一方面提昇安全技術專業教育、專業認証規畫，同時注意相關教育資源的重分配，並透過網站公佈立各會員體訓練與教育機會；（六）無線安全：由於無線上網（wireless connectivity）的技術與服務價格逐漸普及化，而現今區域無線網路安全（Local area networks, LANs）認証技術仍未成熟，導致LANs可能成爲數位安全防制網的一大漏洞。

比較歐盟與APEC的數位安全治理建制發現，歐盟的數位安全建制主要是依附在緊密的歐盟組織內推動網路犯罪司法調查的國際合作，而APEC的建制則是依附在較鬆散的機制下，同時加強與其他既有的制度性安排連結，強化區域治理的監督執行機制。從全球治理的角度來看，APEC的數位安全策略涵蓋了治理的規範、原則、計畫，但是在解決問題的國際公共政策部份則顯然不如「歐盟網路犯罪協約」。不過APEC也鼓勵會員體加入其他相關的安全治理機制如八大工業國家高峰會（G8）主導的24/7高科技連網系統（points of contact），㉕就是提供參與國即時電子証據作爲辦案的依據。

四、以美國爲核心的數位安全治理計畫

美國政府自九一一事件之後，有鑑於網路犯罪、跨國犯罪與恐怖組織的共犯結構，已經對美國國家安全造成新的威脅，爲了防止恐怖組織以「不對稱戰爭」型式對抗美國，從二〇〇一年開始，布希政府採取了以「反恐外援計畫」爲核心的「反恐外交」。所謂雙邊合作的網路安全治理架構，基本上是包裝在以美國爲軸心的外援計畫中。類似於二十世紀，二次大戰之後的美國反共產主義外交政策，此計畫的基本前提是要建構一個全球反恐怖主義（Global War on Terrorism）的安全網。爲了達到此一目的，需要從各國網路反恐認知以及制度與能力建構開始。恐怖主義與共產主義最大的差異

註㉔　APEC Telecommunications and Information Working Group (TEL), "APEC Cybersecurity Strategy," <http://www.apectelwg.org/apecdata/telwg/28tel/h/telwg28-HRDSG-15.pdf>.

註㉕　24/7代表每天24小時每週七天不間斷的連網通報系統。

在於，沒有一個國家願意承認自己是恐怖主義國家。因此，反恐行動較反共行動更容易取得合作共識。

九一一事件以後，從二〇〇一到二〇〇三年間美國和加拿大、印度以及澳大利亞等十六個國家合作，完成「反恐援助計畫」（Antiterrorism Assistance Program, ATA），包括「預防措施」、「網路攻擊的因應與調查技巧」、「強化高階官員處理網路事件的能力」等三種不同的網路恐怖主義訓練課程。同時，ATA也提供各國執法和安全單位人員安全課程。美國國務院特別透過各地大使館和當地安全官員共同設計，因應當地需要除了傳統的反恐訓練課程之外，也增加了網路犯罪的調查與查緝，甚至透過研討會形式協助這些國家強化相關立法，尤其是針對一些發展落後國家的反恐訓練是安全治理的重要環節。㉖

美國的反恐外援計畫結合了反恐議題與網路安全議題，同時透過聯合國與其他區域組織積極推動數位安全，逐漸形成以美國爲首的全球數位安全反恐聯盟。但是數位安全治理所涉及的制度面調適問題如何形成共識是治理建制順利運作的關鍵。因此，美國將反恐與網路安全結合的用意，是可以將網路安全的位階提升爲國家安全層級的數位安全議題。此舉，可以更方便凝聚數位安全治理的共識，同時也爲制度調適提供合理化的基礎。

五、民間部門數位安全治理建制

就網路犯罪而言，無論其是否已經危害到國家安全，其犯罪途徑通常是從個人用戶端進入全球連網系統，因此，犯罪事証的取得或防制與民間業者的配合程度有關。在歐盟的網路犯罪協約內容中要求簽約國必須立法要求民間業者提供網路使用紀錄，作爲查緝防制犯罪的情報資料。因此，民間業者部門有關恐怖攻擊的情報是評估國家安全危機程度的重要依據。但是從民間業者的商業利益考量，提供政府這類情報將有損於其公司信譽。許多民間業者傾向於隱瞞內部安全管理疏失，如金融服務業寧可自行吸收網路安全管理疏失的損失，而不願意投入資金改善內部網路安全系統，成爲數位安全防制的死角。

因此，民間部門數位安全治理工作的重點在於加強電腦網路事件情報的掌握與技術資訊的分享。現有的相關民間組織包括「電腦緊急應變小組」；電腦主要硬體與軟體廠商聯盟與產業協會（Information Technology Association of America, ITAA）；世界資訊科技服務聯盟（World Information Technology and Services Alliance, WITSA）；以及商業軟體聯盟（Business Software Alliance, BSA）等民間團體都是重要的參與者。另外於九一一世貿大樓攻擊事件之後，美國關鍵基礎建設民間業者成

註㉖ Testimony by Ambassador Cofer Black Coordinator for Counterterrorism, Department of State to the Senate Appropriations Subcommittee on Foreign Operations Foreign Assistance and International Terrorism, Washington, D. C., <http://foreign.senate.gov/testimony/2003/BlackTestimony030318.pdf>.

立有關能源、金融「資訊分享與研判中心」，這些民間團體或協會皆爲重要的民間治理機制。㉗

民間業者參與數位安全治理機制的主要目的，一方面是取得重要安全情報；其次是分攤因爲高度依賴所產生的安全風險，其最終目的是形成制度化的機制，結合政府代表、跨產業的企業負責人、跨政府部門與情報單位的參與，甚至於相關國際組織代表共同解決數位安全所衍生的問題。㉘

整體而言，聯合國與區域合作的多邊組織提供了數位安全治理的原則和規範，美國政府則將安全治理放在雙邊架構下執行，而民間機制則提供了技術與實務上數位安全合作的機制與經驗。

伍、數位安全的治理困境

儘管數位安全治理的原則、規範、計畫甚至協約在二〇〇〇年之後陸續在國際間形成共識，但是其迫切性卻是在「九一一事件」發生之後才逐漸受到國際間，尤其是美國的重視。嚴格說來，美國本身作爲全球網路交通最頻繁的地區，數位安全的全球治理符合美國的國家利益，因此，數位安全的全球治理是在美國政府的主導下展開，即便是「歐盟網路犯罪協約」也可以見到美國政府積極參與的意圖。美國政府一方面透過國土安全部的成立，積極展開一系列國內數位安全的制度結構性的改革。同時透過雙邊及多邊機制建立全球反恐聯盟。㉙然而，不可諱言，即使美國試圖透過科技優勢，以柔性權力主導全球治理，但是由於網際網路的虛擬特性，犯罪事証不易取得，導致其安全治理上容易出現「搭便車」的問題，㉚因此數位安全治理必須先克服以下困境。

一、數位落差的結構性因素

根據聯合國「貿易暨發展委員會（United Nations Conference on Trade and Development, UNCTAD）」之報告（E-commerce and Development Report 2003）全世界十大遭受網路攻擊國家中，美國爲首要對象，佔35.4％，其次是巴西，英國居第三，德國及義大利分別爲第四、五。（表三）同時報告也顯示，全世界發動網路攻擊的前十名國家中，美國佔35.4％，其次是韓國的12.8％，中國以6.9％居第三，台灣則以3.9％排名第六位，德國及法國分別爲第四、五。（表四）

註㉗ 同註⑥。

註㉘ 同上註。

註㉙ 吳東野、鄭端耀著，**九一一與國際反恐**（台北市，遠景基金會，民國92年）。

註㉚ Perri 6, "Global Digital Communications and the Prospects for Transnational Regulation," in David Held & Anthony McGrew, *Governing Globalization: Power, Authority and Global Governance* (Cambridge, U. K.: Polity Press, 2003) p. 146.

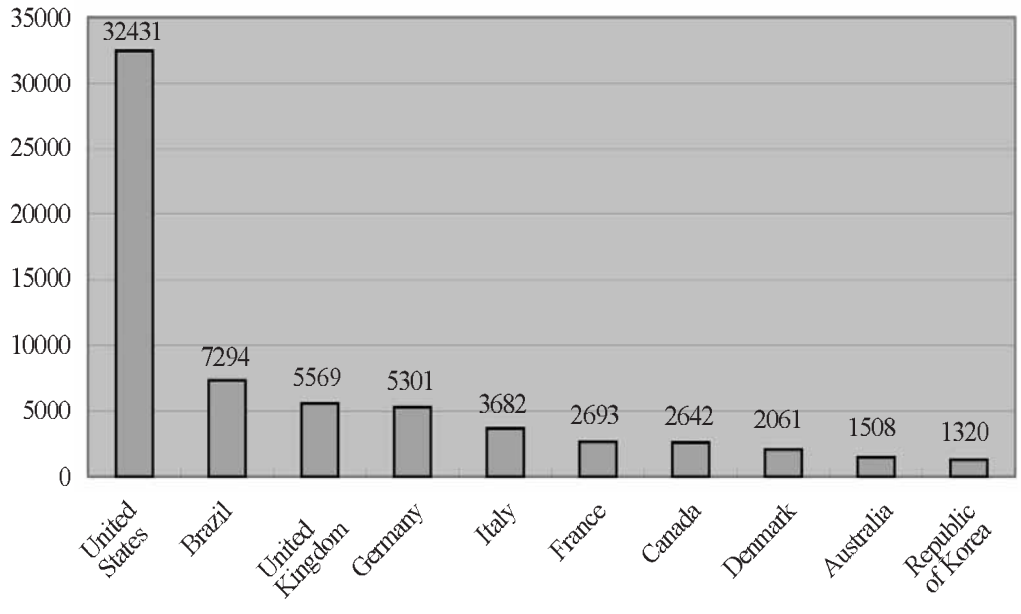
有趣的是，依據表五的二〇〇三年政府網路系統受攻擊的統計數據，中國的政府線上系統受到 187 次攻擊，居榜首；其次爲美國政府的 177 次，巴西及土耳其分別爲第三、四名。台灣的政府線上（Government-on-line）系統遭遇 77 次攻擊，居全球第五。從政府網路受攻擊的前二十個國家來看，有一半以上是開發中國家。由於開發中國家在數位發展上的結構性落差，造成這些國家數位安全的概念也相對薄弱，在安全治理能力的建構上也會相對落後。

如何縮小數位落差是建立數位安全共識進而完成全球治理建制的先決條件。 換言之，縱使資訊強權有較強的資訊科技能力設計安全防護網，但是駭客或網路恐怖攻擊可以經由防護較弱的數位落後地區的伺服器展開。因此，眞正有效的安全治理不單靠科技能力，而更重要的是對於數位安全共識的建立。

然而數位落差問題的改善曠日費時，而數位安全的防護已經迫在眉睫。九一一之後美國試圖主導與反恐行動結合的全球數位安全治理，其目的即在透過議題連結（linkage policy），突破數位落差的結構性障礙，創造各國在「國家安全政策」議題上的合作空間。換言之，無論是基於反恐或是數位安全合作，結構性數位落差問題的解決應該是數位安全治理首先要嚴肅面對的課題。

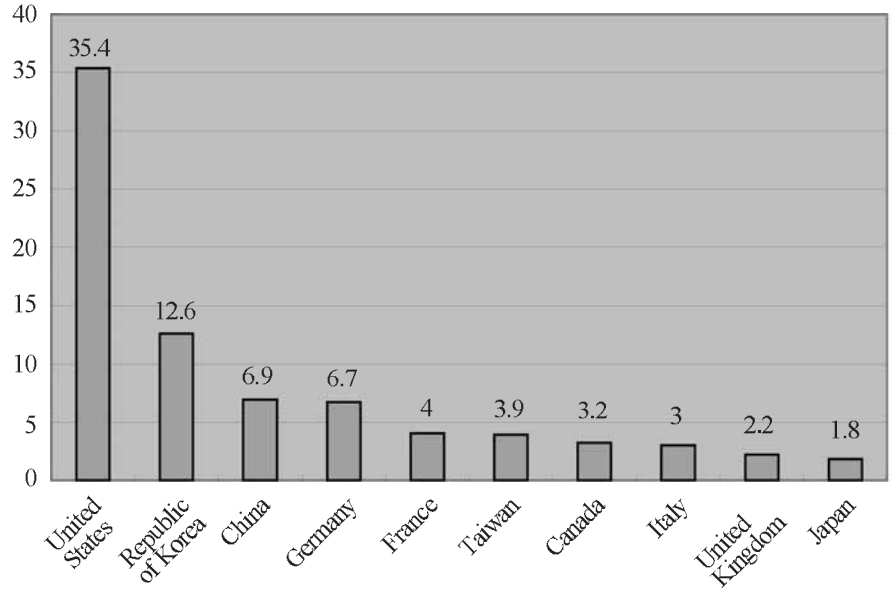
表三　二〇〇二年前十名遭受網路攻擊的國家

單位：次



資料來源：United Nations Conference on Trade and Development, "E-commerce and Development 2003 Report," p. 29, <http://www.unctad.org/en/docs//ecdr2003_en.pdf>.

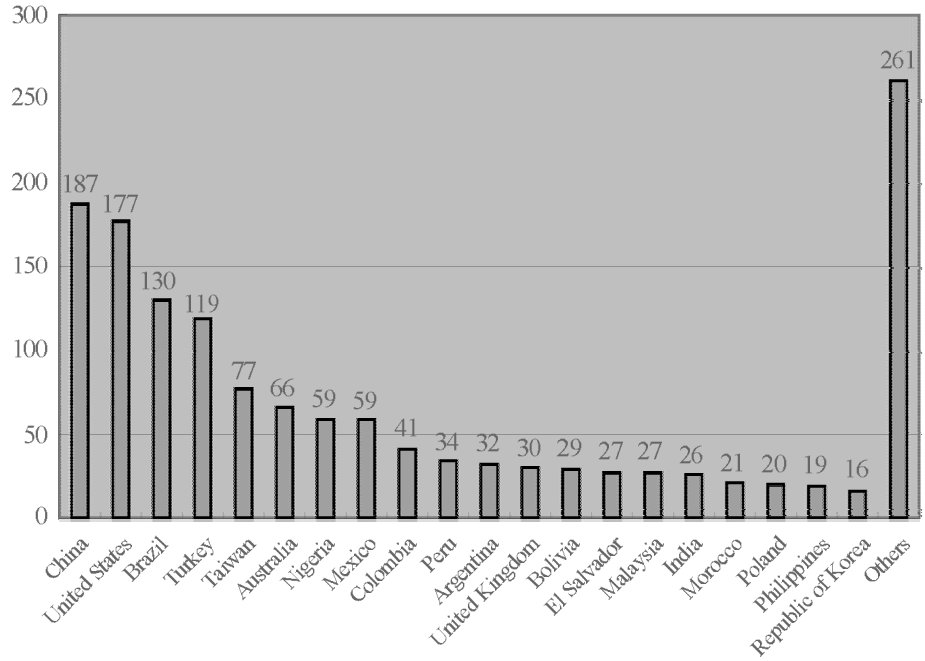
表四　二〇〇二年發動網路攻擊前十名國家所佔百分比



資料來源：同表三。

表五　二〇〇二年政府網站受攻擊最多的20個國家

單位：次



資料來源：同表三。

二、言論自由與國家安全的抉擇困境

人類社會朝向民主化發展最重要的前提之一就是言論自由。網際網路技術的應用，也使得人類在網路的虛擬世界中，可以暢所欲言達到前所未有的境界。然而，在網路無政府狀態之下，網路的不當使用造成他人的傷害時，適度的規範成爲保護個人「必要的惡」。

網際網路上的言論自由是否應當或是如何規範的爭議，自然也影響到數位安全治理的推動。也是拜恐怖主義威脅，二〇〇四年三月十日，美國聯邦司法部（Department of Justice）正式向聯邦通訊委員會（Federal Communications Commission, FCC）提交建議，要求 FCC 立法規範所有寬頻網路提供者，包括利用纜線數據機與 DSL（Digital Subscriber Line）提供服務的公司，都應重新組裝其設備，建置讓執法人員能有效實施通訊監察的環境。㉛在這份由司法部、聯邦調查局與毒品管制局聯合向 FCC 提出的文件中所提出的具體建議包括：強迫業者在提供服務（從即時簡訊服務、網路語音電話（VoIP）服務、到使用微軟 Xbox 線上遊戲服務等）時，應在客戶端裝設後門程式；要求業者在推出新服務時，該服務在技術上應能支援警方後門程式的運作，若未能支援者，該服務可能被宣告違法；而對於業者現有的服務項目，則給予業者 15 個月的緩衝期間調整之。

由於數位安全治理涉及電子犯罪事証的取得，對人民在網路上的言論自由造成一定程度的侵犯，因此歐盟網路犯罪協約中最受爭議的部份，主要是關於簽約國的司法調查單位將被授權調查電腦相關犯罪所需之電子資料証據。而且，基於跨國合作的必要性，協約的簽約國必需排除可能的法律障礙，提供任何簽約國進行網路恐怖行動相關的跨國調查工作。㉜以目前歐盟主要成員國仍對網路犯罪協約持觀望態度來看，國際合作打擊網路犯罪的多邊機制的實際運作仍有相當大的障礙。除了國家司法主權的衝擊之外，㉝其主要原因，是由於協約中涉及言論自由的敏感議題。爲此，美國資訊、法律學界爲主的民間團體「電子隱私權資訊中心」（Electronic Privacy Information Center, EPIC）結合各國關心網路自由的非政府組織在一九九七年十二月一日成立「國際網路言論自由聯盟」（International Internet Free Expression Alliance, IIFEA），㉞其主要訴求與跨國合作進行網路電子蒐証的理念背道而馳。換言之，如果美國政府部門無法在此一問題上先獲得內部共識，則數位安全的全球治理將是一段漫長的道路。

註㉛ Declan McCullagh and Ben Charny, "FBI Adds to Wiretap Wish List," *C Net Tech News,* <http://news.com.com/2100-1028-5172948.html>.

註㉜ "President Bush's Message to the Senate of the United States," <http://www.whitehouse.gov/news/release/2003/11/print/20031117-11.html>.

註㉝ 高少凡，倪炎元，「國家主權在網路時代所面臨的處境與衝突」，**美歐季刊**，第 14 卷第 4 期（民國 89 年冬季號），頁 471～501。

註㉞ 請參考國際網路言論自由聯盟網站，<http://www.ifea.net/members.html>.

三、數位科技的無國界特性成爲監督的障礙

任何全球治理的制度安排能否有效運作的重要關鍵之一在於監督機制能否有效運行。㉟否則該制度將因爲「搭便車」問題而喪失公信力。雖然聯合國以及區域性有關數位安全治理的制度安排，一再強調司法調查跨國合作的必要性，但是數位安全治理涉及網路非法行爲者認定標準等司法問題。然而網路非法行爲的認定往往會受到政治、社會、文化等因素的影響而形成治理上的局限性，如在二〇〇三年因爲美國雅虎入口網站設立反猶太人的納粹網站，因而引起法國反種族歧視與猶太學生聯盟的不滿，向法國政府提出控訴。但是雅虎公司提出四個理由反駁：（一）法國政府對美國公司沒有司法管轄權；（二）雅虎公司爲網路服務公司不負網路內容之責任；（三）美國憲法第一修正案保障言論自由；（四）任何透過 IP 網路位址（Internet Position, IP）篩檢網站無法有效查証眞實個人資料，也不符經濟效益。以該公司爲例，30％的 IP 網路位址（Internet Position, IP）地址的國籍資料填寫不實，更加深查証的困難。㊱換言之，即便是美國本身面臨數位安全治理的跨國合作時，也難免受到不同歷史文化與國家利益考量的挑戰。

陸、結　論

當科技不斷創新，將人類現實世界的極限推向另一個無限可能的虛擬空間時，個人和國家所面對的考驗，就是如何爲自己在虛擬世界中重新建構新的秩序。因此，當我們在討論如何透過「數位機會」改善「數位落差」的同時，若未能建立「數位安全」的認知共識，其結果將會是將人類社會帶向一個數位科技的無政府世界，而未蒙其利之前，反而先受其害。本研究的目的在於一方面強調「數位科技」將「人民安全」與「國家安全」彼此鑲嵌的現實，同時指出鑲嵌安全共識建立與制度調適是建立數位安全全球治理的基本前提。因爲，網路恐怖行動對資訊化社會的威脅，基本上是跨越「人民安全」與「國家安全」的全方位安全威脅，甚至，在網路時代的戰爭，已經不存在前線與後方，因此，戰爭的引爆點可能就在未設防的家用電腦中。也因此，電腦網路系統或無知的電腦玩家很可能成爲恐怖行動最佳的助攻者。

總之，數位安全秩序的建立，除了網路安全系統的維護之外，數位安全規範、原則與計畫的制定，以及跨國政策協調與合作，已經是國家選擇數位化發展的必經之路。然而不可諱言地，所有的集體行動總免不了會有「搭便車」的行爲者。就數位安全治理而言，「搭便車」的行爲可能留給網路攻擊者可趁之機，進而造成防護漏洞，這也

註㉟　同註㉚。

註㊱　依據美、日、法三人專家小組在雅虎公司的訪視報告。資料引自“Benoît Frydman and Isabelle Rorive,” a keynote speech presented on February 11, 2002 at the Cardozo School of Law during the Conference: “Hate and Terrorist Speech on the Internet: The Global Implications of the Yahoo! Ruling in France,” <http://pcmlp.socleg.ox.ac.uk/YahooConference/>.

是所有制度運作過程中必然存在的現象。因此，在數位安全的全球治理架構下，國家必須釋出或分享部份的司法檢查主權，而人民則須放棄部份的隱私權（如電腦上網紀錄），惟有從相對且互惠的「人民自由」與「國家主權」之中，才能享有更大的數位安全。

然而，在數位安全治理的模式與權力結構上，仍可能出現霸權主導的現象。如美國在九一一之後，主導全球反網路恐怖主義行動，可以說是數位安全的幕後推手。部份國家在面對美國以反恐包裹數位安全的政策訴求時，由於本身在反恐方面危機意識或是經驗不足，因此也多半樂意接受美國的「反恐外援計畫」。再者，在恐怖組織行動不可捉摸的共同威脅下，數位安全治理將順勢成爲一股不可抵擋的發展趨勢。

再就國際關係學門而言，有鑑於科技快速變遷的數位時代，國際關係研究學者也必需提早加入此類課題之研究，否則將因研究議題上的缺席，而陷入學術研究上的「數位落差」。本論文屬於前瞻性研究，其目的是對於未來可能面臨之問題提出概念之釐清。由於目前主要相關之論文大多出自美國和澳洲軍方之研究分析，對於數位安全之探討，尚未進入社會學科學術研究領域。本文嘗試從國際關係安全研究與全球治理的角度，提供不同於軍事的觀點，期望能爲國際關係與制度研究提供一新的議題方向。

*　　*　　*

（收件：93年7月5日，修正：93年10月1日，接受：93年10月15日）

Digital Security and Global Governance

Hwei-luan Poong

Associate Research Fellow, Second Division
Institute of International Relations
National Chengchi University

Abstract

According to conventional wisdom, state security and civilian security are two separate concepts. Those who study state or national security will basically be categorized as scholars of international politics, while those who study civilian security criminologists. However, in the era of informationalization and globalization, one can hardly differentiate the boundary of these two levels of analysis. In view of the emerging unconventional warfare and the high degree of dependency of human beings on informationization, this paper tries to explore a new dimension of security studies that combines these two concepts. The author argues that the interdependence and the nature of embeddedness of the two levels of security under the threat of misuse of information technology necessitate the recognition of the vulnerability of separate security management. Learning about embedded security in the digital era might be the key to global governance of any transnational security issue.

Keywords: Digital Security; Network Security; Cyber Security; State Security; Civilian Security; Cyber-Terrorism; Asymmetric Warfare; Global Governance; Anti-Terrorism Diplomacy; Embedded Security

參考文獻

吳東野、鄭端耀著（2003），《九一一與國際反恐》，台北，遠景基金會。

高少凡、倪炎元（2000），「國家主權在網路時代所面臨的處境與衝突」，《美歐季刊》，14:4，471-501。

郭承天（1994），《國際建制與國際組織》，台北，時英出版社。

Arguilla, John, David Ronfeldt, and Michele Zanini (1999), "Networks, Netwar, and Information-Age Terrorism," in Zalmay Khalilzad, John P. White, Andrew W. Marshall (eds.), *Strategic Appraisal: Changing Role of Information-Age Warfare*, Santa Monica, Calif.: Rand Corporation.

Ball, Desmond (2000), *The Council for Security Cooperation in the Asia Pacific: Its Record and Its Prospects,* Canberra, Australia: Strategic and Defence Studies Centre, Research School of Pacific and Asian Studies, The Australian National University.

Bosch, Olivia (2002), "Cyber Terrorism and Private Sector Efforts for Information Infrastructure Protection," paper presented at *Workshop of the ITU Strategy and Policy Unit on Creating Trust in Critical Networks*, on 20-22 May 2002, Seoul.

Clausewitz, Carl Von (1968), *On War* (first published in 1832), London: Pelican Books.

Cossa, Ralph A. (1995), *Asia Pacific Confidence and Security Building Measures*, Washington, D. C.: The Center for Strategic and International Studies.

Denning Dorothy E. (1999), *Information Warfare and Security*, New York: ACM Press.

Dickens, David (ed.) (2002), *The Human Face of Security: Asia-Pacific Perspectives, Strategic and Defence Studies Centre*, Canberra: Australia National University.

Haas, Ernst B. (1990), *When Knowledge is Power: Three Models of Change in International Organizations,* Berkeley, Calif.: University of California Press.

Held, David & Anthony McGrew (2003), *Governing Globalization: Power, Authority and Global Governance*, Cambridge, U. K.: Polity Press.

Khalilzad, Zalmay M. & Andrew W. Marshall (eds.) (1999), *The Changing Role of Information in Warfare*, Santa Monica, Calif.: Rand.

Noor, Elina, Mohamed Jawhar Hassan (eds.) (2003), *Asia Pacific Security Uncertainty in A Changing World Order*, Kuala Lumpur, Malaysia: ISIS Malaysia.

Nye, Joseph S. and Robert Keohane (1977), *Power and Interdependence: World Politics in Transition*, Boston, Mass.: Little, Brown and Company.

Pease, Security and Conflict Prevention (1998), *Sipri-UNESCO Handbook*, New York: Oxford University Press, Inc.

Rosenau, James N. (1992), *Governance Without Government: Order and Change in World Politics*, Cambridge, U. K. : Cambridge University Press.

Report of the First Committee, UN General Assembly Fifty-fifth session (2001), *Developments in the field of information and telecommunications in the context of international security*.

United Nations Conference on Trade and Development (2003), E-commerce and Development 2003 Report, <http://www.unctad.org/ch/docs//ecdr2003overview_ch.pdf>.

WSIS Executive Secretariat (2004), *Report of the Geneva Phase of The World Summit on the Information Society*, Geneva-Palexpo, 10-12 December 2003. Document WSIS-03/GENEVA/9(Rev.1)-E 18 February 2004, p. 49. <http://www.itu.int/wsis/documents/doc_single-en-1179.asp>.

Wolfers, Arnold (1962), *Discord and Collaboration: Essays on International Politics*, Baltimore, Maryland: The Johns Hopkins Press.

1995 Report of UN Commission on Global Governance, *Our Global Neighborhood,* <http://www.sovereignty.net/p/gov/gganalysis.htm>.