前瞻科技與管理　2卷2期，1－14頁（2012年11月）
Journal of Advanced Technology and Management Vol.2, No.2, 1-14 (November, 2012)

國家主權延伸至網路空間之討論

梁德昭[1,*]　朱志平[2]　林凱薰[2]
[1]淡江大學資訊管理學系
[2]淡江大學管理科學研究所

摘要

網際網路加速了全球化的發展，將人類帶入了e化時代，形成跨越國界平行式互動的模式，動搖了以國家主權為基礎所建構的法律制度。各國致力推行網路化後所帶來的國家安全及利益上的威脅，使網路空間成為各國政府極力維護的目標，甚至在國際上引發許多不同層面的爭議。雖然在網路空間中並無國家主權立基的條件，但國家主權似乎已經延伸至網路空間之中。無論是基於攻擊上的防護，或是限制資訊的傳遞，都必需藉由彰顯國家主權的存在來執行。挹注國家主權新的意涵，在網路空間提供國籍識別，以及界定網路邊疆，是未來解決國際間網路衝突的有效解決方案。

關鍵詞：網路空間、國家主權、網路戰、網路自由、虛擬領土

壹、前言

20世紀90年代，源自美國國防部ARPANET（Advanced Research Project Agency Net），以光纜為骨幹聯繫全球的網際網路，加速了全球化（Globalization）的發展（Hauben and Hauben, 1997）。網際網路的TCP/IP通訊協定，承載了雙向互動的線上行為及大量的數位資料傳輸，將人類帶入了e化時代，對人類社會生活、經濟發展等各領域產生極其深遠的改變。

在網網相連所形成的網路空間中，人類的互動不再受到地理、氣候等客觀自然條件的限制，甚至打破了非技術型態的人為封鎖，形成跨越國界平行式互動的模式。例如：電子商務跨國網路交易的模式，衝擊著全球各國長期基於實體交易發展的傳統規範，撼動以國家主權為基礎所建構的法律制度。

網際網路的遠距及去中心化特性，使各國在資訊化發展的過程中，將國防及民生等各項關鍵基礎建設，逐步掛載在網路空間中控制及運行。國家推行資訊化的結果雖增進了管理上的效率，但也因此造就了僅需運用數位手段，即可形成在國家安全及利益上嚴重威脅的機會，給予國與國之間在軍事上運用超限戰的重要力量，因此，網路空間成為各國政府極力維護的目標。例如：美國於2011年7月發佈《網路空間行動戰略》，不只將網路空間與陸、海、空、太空並列為軍事行動領域，更視網路攻擊為侵犯國家主權的戰爭行為（Bame, 2011）。

除了極力保護網路化的各項設施及系統，國家在網路空間也面臨了各種涉及主權的問題，如：跨國的網路犯罪、駭客入侵（中國與美國互相駭客入侵）、網路反恐等。而

* 通訊作者：梁德昭
電子郵件：tcliang@mail.tku.edu.tw

網路空間非實體、去集中化及隱匿的特性，使得國家主權在網路空間難以伸張，如何才算是網路空間的武裝攻擊？如何辨別攻擊來源以釐清責任歸屬？在管制不當資訊的散播及偵查網路犯罪上，如何避免侵犯資訊隱私之保護與造成網路自由的箝制，也在國際間造成極大的爭議。是以，國家主權在網際網路空間之當否延伸及如何延伸？勢必將成為全球基於主權所建構的政治實體所必須面對的重要課題。

然而，國家主權在網際網路空間的課題涉及跨領域的研究，如：政治學、國際關係、管理學、資訊科技等，在學術界的討論並不多見。本文嘗試一探索性研究，進行各領域在討論時一個概念性的整合，期望能對未來相關的學術研究上貢獻價值。

貳、網路空間國家主權爭議之緣起

一、國家主權內涵的變化

國家主權（State Sovereignty），是指一個國家對內、對外的完整權力。國家主權理論起源於16、17世紀的歐洲，資本主義生產方式的興起及歐洲民族國家的出現，國家主權在以國家為中心主義的觀念推動下，逐步藉由國際關係與國際法具體實踐。一般來說，以1648年的西發利亞條約（The Treaty of Westphalia）結束了30年的宗教戰爭，不再堅持「神權」，而形成現代主權國家體系。

根據1933年《蒙特維多國家權利義務公約》，主權國家的要件有：（一）永久的人口；（二）固定的領土；（三）有效的政府；（四）與他國交往的能力。國家在國際法上所具有的權利，相對的是國家所應承擔的義務，主要得以獨立（Independence）、平等（Equity）與和平共存（Peaceful co-existence）等三個方面來加以展現。在國際上，主權國家是國際法的主體，也是國際法權利和義務的承擔者。1946年聯合國大會通過的《國家權利義務宣言草案》第一條規定：「各國有獨立權，因而有權自由行使一切合法權力，包括其政體之選擇，不接受其他任何國家之命令。」1970年聯合國大會通過的《各國依聯合國憲章建立友好關係及合作之國際法原則宣言》指出：各國一律享有主權平等，包括各國法律地位平等、充分主權之應有權利、國家之領土完整及政治獨立不得侵犯、有權自由選擇並發展其政治、社會、經濟及文化制度等。

國家主權對國內有完全而至高的管轄權，對國外有完整的獨立代表權與自衛權。雖然各國因歷史、環境與人為因素而有不同的主權表現，但大體而言，國家主權最明確而主要的權力展現為：對內貫徹其管轄權、對外具有代表權（含自衛權），且可以表現在下面三個方面：（一）對內表現為最高權即國家對其領土內的一切人和物以及領土外的本國人享有屬地優越權和屬人優越權；（二）對外表現為獨立權，即國家在國際關係上是自主和平等；以及（三）自衛權（吳嘉生，1999）。

隨著國際社會的不斷發展和演變，國家主權的內涵和範疇的延伸也跟著不斷的改變和調整。20世紀90年代以來，隨著資訊技術革命的迅速興起所形成的網路空間和全球化浪潮的交互作用，導致國際政治格局發生了重大變化，對傳統的國家主權帶來前所未有的衝擊，使得國家主權理論與實務上逐漸出現分離的現象，致使當今國家主權理論陷入困境。國際法學界因此出現了主權弱化、受限、讓渡、過時等不同國家主權遭到削弱的看法。現今網路空間有逐漸侵蝕國家主權的跡象，以致各國為致力防範網路時代所帶來的國家安全及利益上的威脅，從而引發國際上許多不同層面有關國家主權在網路空間存有之爭議（黃惠康，2012）。

二、網路空間對國家主權實踐的影響

網路空間（cyberspace）一辭字根源自Cybernetics，而Cybernetics源自希臘語kubernetes（控制方向的舵手）。Wiener（1965）在《模控學》中使用Cybernetics

一辭，意即動力控制、傳播學、電子技術、無線電通訊、神經生理學、心理學、醫學、數學邏輯、電腦技術及統計力學等多種學科相互滲透的學科。1984 年，William Gibson 出版了小說 *Neuromancer*，創造了「cyberspace」一辭（Gibson, 1984），現在 cyber 則作為字根，代表與網際網路相關或電腦相關的事物。美國國防部軍事辭典 JP-02 對網路空間的定義為，[1] 資訊環境內的一個全球領域，由相互依存的資訊技術基礎設施網所構成，包括網際網路之電信網路與電腦系統及其內建之處理（控制）器。

資訊網路技術的快速發展把人類帶入了網路社會，同時以前所未有的速度影響改變著人類的政治形態。藉由網際網路所構成的自由化、無邊界性的網路空間，與國家獨立性、固有領土的特質有著顯著的不同。工業化社會集中、統一的特徵所造就的現代國家主權理論中對疆域、資源、權威的歸屬意識，也在網路空間開放的、分散的特性中失去了支撐。世界經濟趨勢大師梭羅（Lester C. Thurow）認為資訊革命增加了個人的權力，打破了階級性的組織結構，使得誕生於工業時代維持世界秩序的三大支柱：國家主權、國家經濟和軍事力量面臨著嚴峻的挑戰（齊思賢譯，2000）。

網路時代的到來，也開始削弱在國際政治中以國家為中心的觀念，網路空間在全球相互依存的多中心國際體系的地位日漸凸出，國家之間的相互依賴性日漸增強，僅憑一國之力無法有效解決國際上的政治及法律問題。由於國際組織地位的提升和權力的強化，使得國家也不得不讓渡或自我限制部分主權，以達成有效的合作來解決衝突或問題。然而國家主權是國際政治的基礎，也是維持目前世界秩序的重要支柱，探討網路空間對國家主權實踐的影響，是思考資訊網路技術的廣泛應用對國際政治的影響時不能迴避的重要課題，也是繼生態、能源及反恐後最貼近政治但又最容易被忽略的議題。

三、網路空間中國家主權爭議的緣起

網路空間扮演全球化的關鍵角色，除了成為推動全球化的主要動力外，本身亦是最重要的全球化平台。國家與國家間在貿易、交通、文化等範疇藉著網路空間互動交流，形成安全與利益錯綜複雜的國際關係，國際形勢只要稍有變動，許多國家都將因之而受牽連。

網際網路的發明源自美國，以美國為首的西方先進國家，向來都是資訊科技領先的政治群體。這些國家資訊化的程度讓開發中國家難以追趕，在全球的發展上，國家間的數位落差也日益擴大。這也衍生出無論是在網路戰力的提升、相關規範的制定上等種種的優越因素，都使先進國家領先一步，形成主導網路空間發展局勢的態勢。

近年來西方國家紛紛宣告，其政府與企業受到來自於網路的攻擊在規模和範圍上的不斷擴大，而積極進行網路戰力的提升。如曾在 911 事件發生時擔任布希總統國土安全特別助理 Frank Cillufo 所說：「在網路上，我們已經不可能通過建立防火牆來解決問題，這是我得出的結論。我們必須討論建立攻擊能力，這樣才能嚇阻敵人。」（Hopkins, 2012）。

此外，隨著歐美國家強調個體技術優勢的先來者先占原則，與諸多相對弱勢國家看重的人類共同財產原則之間的競爭日趨激烈。在網路空間安全規範上，美歐聯手向其他國家推銷《網路犯罪公約》（Convention on Cybercrime），計劃逐步將其打造成覆蓋全球的國際性公約，從而確立網路犯罪國際立法領域的主導地位（方鈞、趙青海，2012）。

網路空間雖然提高了國家彼此之相互依賴程度，但也造成了國際現實主義下在網路空間的衝突日漸增多的現象。國家為了想降低他國造成本國利益損失的任何可能，開始尋找干涉他國內部問題的理由，而以國家為

[1] 美國國防部軍事辭典 JP-02 目前最新版本為 2010 年版，參見 US Department of Defense（2010）。

主要行為體的國家主權，便成為他國捍衛的首要目標。以 2010 年至 2011 年源自北非突尼西亞的茉莉花革命為例，該項運動後來襲捲了大中東地區（北非和西亞）眾多阿拉伯國家，並延燒至部分歐洲、美洲、亞洲國家，形成一系列的反政府社會運動。在一連串的發展中，網路空間扮演著重要的串聯平台。事件發展過程中曾傳出美國利用社交網站的運作以支持革命勢力，以及西方國家呼籲網路開放的聲援，在開發中國家眼中則視之為干涉內政。

資訊網路技術處於相對弱勢地位的開發中國家遭受先進國家的全方位衝擊，由於難以控制和阻止來自網路空間的強大力量，開發中國家不得不尋求支持者的認同而加劇了民族主義的抬頭，被壓迫的一方必須找出被壓迫的理由以加快團結的速度。而處於先進國家的政治群體，必須塑造遭受威脅的氛圍，據以建立基於保護網路設施及各項重要系統而發展網路戰力的理由。在這種國與國之間的網路衝突或競爭中，不管是保衛受到網路攻擊的目標，或者是阻止他國干涉本國內政，國家主權的捍衛又成為不論是先進國家或開發中國家爭論的立基，網路空間中的國家主權爭議於焉興起。

參、國家主權應否存在於網路空間之正反面意見

一、網路管制爭論浮現的網路空間國家主權

西方民主制度的演進，使得以美國為首的先進國家認為，開放的網際網路將為所有國家的人民帶來更安全更繁榮的生活，透過建立有關普世價值觀和共同規則的全球共識，致力使網際網路成為全球的開放空間。美國副總統 Biden 曾表示，並沒有單獨的經濟網際網路、政治網際網路和社會網際網路，網路空間是整體的，並且已經成為 21 世紀的公共空間，是一個對各種背景、各種信仰的全體人民開放，展開各種活動的空間。

長期以來，西方先進國家主張網路空間自由開放的政策，在開發中國家有不同的觀點與立場，俄羅斯多年來即致力提倡全球網路限武協定，但將網路「意識型態侵略」（ideological aggression）列入其中（Komov et al., 2007）。而中國及俄國盟邦政府，尤其是中東及非洲亦持相同看法，網路限武協議似乎成為政府擴張管轄權至網路空間的合法依據。

俄羅斯於 1998 年在聯合國發起網路限武的倡議，認為透過網際網路傳遞的資訊可能危及國家穩定，之後引起許多國家支持，如中國、白俄羅斯、古巴、緬甸、土庫曼、越南、辛巴威等國家。在 2005 年突尼西亞突尼斯所召開的世界資訊安全高峰會（World Summit on the Information Security, WSIS）中，與會國重申各國均具有制訂其網際網路政策的「主權」（World Summit on the Information Society, 2005）。

2009 年 8 月，上海合作組織（SCO）6 個會員國俄羅斯、中國、哈薩克、吉爾吉斯、塔吉克、烏茲別克，通過一份有關「資訊戰」定義的協定，將「有害他國精神、道德、文化」列為安全威脅的範疇，似乎是將政府審查網際網路上異議言論的做法合理化，並禁止任何國家支持他國從事上述網際網路活動。西方國家則認為，俄國於聯合國所提的資訊安全決議案是出於非民主的思維（Gjelten, 2010）。

聯合國經濟社會理事會（United Nations Economic and Social Council）亦於 2010 年 2 月指出，涉及網際網路的公共政策問題的決策權是國家主權，各國有權利和責任處理與國際網際網路相關的公共政策問題。國際電信聯盟策略長 Alexander Ntoko 也認為，在符合國家需求的網際網路管轄政策上，與主權關係很大（Intellectual Property Watch, 2010）。

面對開發中國家在網路空間伸張國家主權日益高漲的情勢，以及 2010 年 Google 在中國遭受封鎖的事件，美國國務卿克林頓 Hilary（Clinton, 2011）於 2011 年 2 月在

華盛頓大學就「網際網路自由」（Internet Freedom）問題發表演講表示，如果網際網路受到封鎖和審查，便只會斷送和平與進步的機會，扼殺創新和創業的精神。並強調網路自由與言論、集會、結社自由一樣具有普世價值，唯有自由的網路才能有永續的國家發展，不可能只管制政治言論，但卻允許經濟活動的進行。同時，特別點名中國、突尼西亞、埃及、越南和古巴等國家，在控制網路、遏止政治言論的同時，也妨礙了經濟、教育和文化等許多面向的發展機會，國家發展將因此受害。

Hilary 更指出，美國政府除了將在世界各地幫助更多國家能享有網際網路所能帶來的方便性外，更將斥資研發網路技術，以支持人權與民主活動人士，使他們擁有上網的技術能力，即使在政府試圖壓制人民的聲音或阻隔他們上網的情況下，仍然可以有效又安全地向外界互通資訊。Hilary 的演說隱含著美國已經公開將利用網路空間干涉他國在內政上的管理。

2011 年 9 月，俄羅斯、中國、塔吉克、烏茲別克四國向聯合國大會提交《資訊安全國際行為準則》（中華人民共和國外交部，2011）。重申與網際網路有關的公共政策問題的決策權屬於各國的主權。至於與網際網路有關的國際公共政策問題，各國都擁有基本權利並承擔責任。

美國副總統 Biden 隨後於 2011 年 11 月倫敦網路空間會議（London Cyber Conference 2011）（“VP’s Remarks to London Cyberspace Conference,” 2011）指出，任何國家的公民，都不應受制於一種具有壓制性的全球性規定，不能僅僅因為有國界相隔就阻止他們與全球的消費者分享他們的創新成果。英國外長 William Hague 在會議結論時針對俄羅斯和中國在聯合國所提出來的《資訊安全國際行為準則》表示，政府不得將網路空間視為己有，認為所有試圖阻止網路空間透明化或限制言論自由表達的行動終將失敗（Hague, 2011）。

總體來說，開發中國家對於網路空間治理採取不同於西方的自由開放立場，西方國家認為網路空間有助於個人能力的提升進而達成集體福祉，反對政府介入。而東方國家將網路空間的管制視為凝聚共識，是確保國家整體安全的必要手段，因此傾向於國家介入的治理模式（彭慧鸞，2011）。是以，西方國家普遍認為國家主權不應及於網路空間，全世界的人在網路空間中均應有相同的網路人權。而一些開發中國家陣營則認為，國家應該在其境內的網路空間有其主張的立場，也有限制網路空間功能的權力。

二、網路管轄權隸屬國家主權的立場

（一）防範網路攻擊所呈現的主權問題

由於資訊化的推行，國家關鍵基礎設施如電力網、金融體系，均掛載在網際網路中提供重要服務的伺服器上運行，而網路空間的跨越國界、移動速度快與隱匿性的特徵，導致網路攻擊事件層出不窮。無論是惡意舉動，或是犯罪者的工具，或成為諜報戰的管道，由於網路空間主權尚無定論，司法管轄權之隸屬無法明確界定，無明確責任追訴之客體與應承擔責任之主體，國際仲裁力量也無發揮之著力點，網路攻擊之防範成為國際社會重視的議題。

運用網路技術發展資訊化越成熟的國家，遭受的網路威脅機會就越大。在近年的網路威脅事件中，美國及西方民主國家漸漸意識到不對稱作戰是開發中國家極度重視且有效的軍事發展方向。網路空間提供了不對稱作戰的最佳戰場，網路技術發展同時也為開發中國家帶來了足以向先進國家示威的機會，保衛關鍵基礎設施及重要系統，成了西方先進國家越來越重視的項目，甚至將網路空間的挑釁行為，視同侵犯國家主權而拉回現實世界中究責。這無形中認同網路空間上的惡意活動有挑釁其國家主權之實，從而為以國家力量進行網路攻擊防禦的必要性得到合理的支撐。簡而言之，以美國為首的西方國家陣營雖然主張國家主權不應及於網路空

間，然而卻視來自網路空間對其國家主權所保護之客體的侵犯為挑釁國家主權之行為，得以國家力量來進行反制。

2002 年，美國總統布希簽署了《國家安全第 16 號總統令》，要求美國國防部組織中央情報局、聯邦調查局、國家安全局等政府部門制定網路戰戰略。2005 年 3 月，美國防部公佈的《國防戰略報告》明確將網路空間和陸、海、空、太空定義為同等重要、需要美國維持優勢的 5 大空間。2011 年，美國國防部首次發表「網路攻擊形同戰爭」的言論，表示如果網路攻擊威脅到美國國家安全，美國將保留一切回應重大網路攻擊的所有必要方式，包括外交、資訊技術、軍事和經濟手段（US Department of Defense, 2010）。

弔詭的是，美國欲以國家主權來保護之客體也是網路空間的一部分，既然國家主權不應及於網路空間，則對網路空間中之被攻擊的客體又如何能以國家主權被挑釁之名而以國家力量進行防衛與反制？更甚者，一旦以國家力量所遂行之防衛與反制作為在網路空間上發動，則其進行防衛或反制行動之機器設備與通訊連線必然無法自外於網路空間，如若這類在網路空間上的活動代表國家主權力量的伸張則必然與其主張國家主權不應及於網路空間之論點相悖。是以，國家主權之概念已無形地存在於網路空間中，吾人以為，網路空間中國家主權爭議的重點應在於國家主權的意涵應如何被重新詮釋，以符合網路空間特殊之情境，而非就國家主權應否存有於網路空間進行爭辯。

開發中的弱勢國家在面對先進國家有關網路空間訴諸主權侵犯問題的做法，傾向以訴諸國際組織仲裁的方式來解決。美國國務卿 Hilary 於 2011 年 2 月的演說（Clinton, 2011）對開發中國家反映了一個重要訊息：西方國家在網路空間中技術優越的威脅。在 2011 年 9 月俄羅斯、中國、塔吉克、烏茲別克四國向聯合國大會提交《資訊安全國際行為準則》（中華人民共和國外交部，2011）中，倡議避免將資通訊技術用於與維護國際穩定和安全的宗旨相悖的目的，以避免帶給各國國內基礎設施的不利影響，並強調必須透過聯合國和其他國際及區域組織建立行為準則，以加強各國的協調和合作打擊非法資訊技術的濫用。

（二）全球網路位址管理權歸屬之爭

除了網路自由限制及網路主權的爭議外，網路位址及網域功能變數名稱解析的管理權歸屬，也是各國爭論的議題。目前網際網路位址分配由美國政府所創立、具實質網路管轄權的非營利組織——網際網路指定名稱及位址管理機構（Internet Corporation for Assigned Names and Numbers, ICANN） 進行分配，[2] 而現今全球網域功能變數名稱解析級別最高的根伺服器計 13 部，主根伺服器在美國維吉尼亞州，輔助根伺服器位於美國計 9 部，瑞典、荷蘭、日本各 1 部（＜國際瞭望——網際網路，美國的獨門武器＞，2010）。依照名稱伺服器的架構，其他的輔助根伺服器只在於轉映主根伺服器的內容，本身並不獨立定義任何名稱與位址的對應，因此，網路空間中的位址管轄權目前仍在美國的控制之下。

美國國防部早於 2005 年將網路與海、陸、空和太空並列為五大空間，美軍在 2009 年曾提出，21 世紀掌握制網路權與 19 世紀掌握制海權、20 世紀掌握制空權一樣具有關鍵性意義，公開將網路安全與國防安全連結。全球不少國家對源於美國國防部設計的網際網路早有疑慮，認為美國正利用網路進一步遂行其霸權利益。2003 年在瑞士日內瓦及 2005 年突尼西亞突尼斯所召開的世界資訊安全高峰會（WSIS）中，各國基於對美國具有控制全球網路意圖的認知，要求美國停止 ICANN 的網際網路管理權。世界資訊安全高峰會與會國決議：在國際上，所有國家對網際網路的管轄都具備平等的地位與責

[2] 參閱：台灣網路資訊中心網站：http://www.icann.org.tw/。

任，同時賦予聯合國所屬組織——國際電信聯盟（International Telecommunication Union, ITU）進行網路管轄事務的變革（World Summit on the Information Security, 2003）。

2010 年 10 月在墨西哥瓜達拉哈拉舉行的 ITU 全權代表會議中，則浮現了一個議題，網際網路是否該由國際管轄組織管制？雖然美國已經同意其政府將逐漸脫離 ICANN，但 ITU 的會員國仍持續敦促將 ICANN 的管理權轉由國際組織管理，甚至提案討論在 ITU 下成立一個具有否決 ICANN 決策的特別單位。未來在全球網路位址管理權上，似乎已經形成由全球各國委託一國際組織進行管理的趨勢，事態發展則取決於美國的態度和做法。在不釋放出其在網路空間中網路位址及網域功能變數名稱解析的管轄權之前，美國似乎在無形中掌握了整個網路空間的支配權，此狀況在沒改變之前，網路空間主權的爭論似乎並無實質意義。

肆、國家主權觀念用於網路空間對網際網路生態的影響

一、集團化對立與網路衝突的法則制定

回顧國家主權於網路空間的緣起，似乎像與冷戰時期世界集團國家對立的延續。美國於 2011 年 5 月宣佈《網路空間國際戰略》（International Strategy For Cyber Space）（The White House, 2011）後，在法國所召開的第 37 屆八大工業國領袖高峯會中，英、美西方民主國家在會中重申開放的的網路空間及網路自由的主張；2011 年 6 月，大西洋公約組織國家達成網路防衛的共識（盧映孜譯，2011）；隨後美國與澳洲宣告共同防衛條約將擴及網路空間，意即一國受到網路攻擊，兩國將共同採取行動（陳成良，2011）；2011 年 11 月，歐盟 20 個國家與美國首度聯合舉辦一場網路資訊安全演習（Cyber Atlantic 2011），成員為歐盟網路與資訊安全局（EU's Network and Information Security Agency, ENISA）及美國國土安全局（US Department of Homeland Security, DHS）（沈經，2011）。在美國於 2011 年積極布局網路空間的舉動後，以美國為首的西方國家網路空間防衛集團正在集結（彭慧鸞，2011）。然則從防衛的觀點而言，必有其所宣稱受攻擊之客體存在，此一存在於網路空間之客體若無國家主權之宣告，又如何能憑藉所遭受之攻擊動員聯盟成員國進行聯合防衛與反制？

而中國和俄羅斯在 2011 年 6 月所簽署的《上海合作組織 10 周年阿斯坦納宣言》（Astana Declaration of the 10th Anniversary of the Shanghai Cooperation Organization）中宣示，上海合作組織成員國將加強國際資訊安全領域協同合作；[3]2011 年 9 月，中國、俄羅斯等國便向聯合國提交《資訊安全國際行為準則》草案，並呼籲各國在聯合國框架內展開進一步討論，儘早就資訊和網路空間行為的國際準則和規則達成共識（雷東瑞，2011）。

不難看出，網路空間集團化對立的態勢正逐漸形成，基本上仍像是西方先進國家與開發中國家的集團集結，集團是主權國家的集合，推動這種發展現象的背後，仍不脫離國家主權的驅動。隨之而來要處理的課題，則是網路衝突的解決。

網際網路被強調的是一個開放的虛擬場所，受到的規範很少，因此僅受到非常低限度的約束（Deeks et al., 2005）。換句話說，網路空間正處於一個法律規範極度缺乏的狀態。美國國家安全局局長 Keith B. Alexander（2010）認為，網路管轄權應開放國際討論，在多數國家的共識下界定網路衝突（Center for Strategic and International Studies, 2010）。聯合國裁軍系列第 33 號報告（Disarmament Study Series No.33）提及，

[3] 參閱：上海合作組織官網：http://www.sectsco.org/EN/show.asp?id=294。

建立各國使用資通訊技術的通用規範有其價值，而且隨著時間演進仍可發展其他通用規範（United Nations, 2011）。然而，國際間所形成的集團雖是以網路作戰防禦為動機而集結的西方先進國家，對網路空間的國家主權尚無明確定義及論述；另一集團則為以保護內政不受干涉形成的開發中國家，對網路空間的國家主權宣示的範疇僅侷限在其境內網路行為之管制。在未來網路空間的國際法則上，不論是國際法規範以及效力的實踐，仍待長時間的觀察。無論如何，強調網路空間的國家主權，仍扮演著國際規則制定的催化角色。

二、網路自由的限制

資訊力量與政府可以控制的傳統力量工具（軍事、外交和經濟）不同，絕非政府所能完全掌控，亦即政府不再能夠控制資訊，這項力量要素已經普及到大眾的手上（中華民國國防部史政編譯室譯，2012）。但是，網際網路的現狀已非最初所定義的無國界空間，爭取國家主權的呼聲提出了各種可能的網際網路版本，都是以各國政府重要利益為優先考量（Gjelten, 2010）。

網際網路被設計成分散化的系統，每個節點都應該連接許多節點，這種設計有助於系統抵禦審查或外來攻擊。然而事實上，大部分個人使用者都在網路末端，只能透過網路供應商（Internet Service Provider, ISP）連到其他節點，只要這條連線遭阻斷，就連不上網際網路。在極權國家，政府靠著切斷或阻擋網路來阻隔資訊的流通。在西方民主國家，網路業者的整併，使網路流量集中到少數企業手中，誘使美國 Comcast、AT&T 這類公司運用這種力量，提高自己媒體合作夥伴的網速來打壓競爭者（Dibbell, 2012）。

網路傳播不當資訊是世界各國政府面臨的共同問題，在世界大多數國家，憲法賦予公民言論自由的權利，但這並不意味著人們的言論毫無拘束，一旦影響社會秩序就會受到法律嚴懲。雖然各國或多或少皆有立法對網路傳播不當資訊的行為加以懲處，但網路監管、網路自由的問題爭議一直未曾稍歇。

美國國會及政府各部門先後通過了《聯邦禁止利用電腦犯罪法》、《電腦犯罪法》、《通訊正當行為法》、《兒童網際網路保護法》等約 130 項相關法律、法規，限制網路傳播內容，國防部、國土安全部、聯邦調查局等部門均設有網路安全監管機構。歐巴馬擔任總統後，成立了白宮網路安全辦公室。美國聯邦政府多個部門則通過設立社交網路監控中心等措施，對網路論壇、部落格、留言板等進行監控。

其他國家亦有類似的政府監控網路的立法，舉例來說，新加坡於 2003 年所成立的媒體發展管理局係負責網路資訊管理的職能，並鼓勵網路行業建立自己的評判標準（＜新加坡媒體發展局＞，2010）；印度《資訊技術法》（Information Technology Act 2000 [No. 21 of 2000]）的重點在政府有關部門有權查封可疑網站和刪除內容，同時網站運營商還需要在聲明中清楚告知用戶，不得發佈有關煽動民族仇恨、威脅國家團結與公共秩序的內容（湯先營，2011）。2010 年 9 月起，印度政府為維護國家安全，要求對社交網站進行監控，並多次要求網路營運商協助政府刪除涉嫌違法網路內容；法國法律對網路謠言也有明確規定，危害國家安全、煽動社會動亂、煽動種族歧視、損害他人名譽、侵害他人隱私、鼓動和推薦反社會道德等網路行為均將受到懲處（趙海建，2012）。

2011 年 10 月 26 日美國眾議院所提出的《禁止網路盜版法案》（Stop Online Piracy Act, SOPA），引發網路隱私和自由的爭議。該法案一旦通過，網站上只要有少數用戶涉及盜版行為，美國政府就有權力全面封鎖網站。支持法案的有好萊塢娛樂產業，以及 Microsoft、Adobe 等科技公司，反對者大多為網路公司，如社群網站 Facebook、Google、Twitter 等（＜美國研議「禁止網路盜版法案」引發美國遊戲界不同看法＞，2012）。紐約時報（*New York Times*）和洛杉

磯時報（*LA Times*）提出質疑，SOPA 為了防止盜版活動，就要求全面被監控用戶行為，將嚴重侵犯個人隱私權，這樣跟中國大陸的網路管制政策並無分別（董菁，2012）。

Google 於 2010 年 4 月 20 日推出「政府請求工具」（Government Requests tool）網頁（“Google Transparency Report,” n.d.），首度呈現各國政府查詢某一使用者資料的次數，以及要求 Google 從旗下搜尋網頁、YouTube 等網站移除某篇內容的次數。根據 Google 引述的資料，由於網路使用者人數大增，進行網路審查的政府，已從 2002 年的 4 國，增加到 40 國以上。據 2011 年上半年的統計，各國政府要求刪除訊息的國家排名依次為德國、挪威、美國、巴西、韓國（中國數據無法得知），在要求提供網路用戶數據的國家排名依次為美國、印度、法國、英國、德國（陳曉莉，2010）。Google 的數據不但顯示了即使是強調網路自由的西方國家，其對網路監控的著力高居排名，另一個值得觀察的現象則是，對網路監控的國家有著越來越多的趨勢。

Rebecca Mackinnon 於 2012 年 4 月美國《外交政策》雙月刊發表文章表示，全世界用來鎮壓網上言論自由和不同政見的最尖端工具事實上恰恰出自美國，而美國政府是美國監視技術的最龐大和最強大的客戶。美國才是全球網路自由的最大威脅（Mackinnon, 2012）。

美國知名法學教授 Daniel J. Solove 認為，應該在捍衛言論自由和保障個人隱私權的兩難困境中找到新的平衡，網路監管既不能全盤扣殺也不能放任自流。他還特別建議，應推動相關法律的進一步完善，最終實現增強網路內容發布個體的責任感、阻止謠言在網路空間肆意傳播的目標（Solove, 2007）。

無論是在管制網路謠言、反恐偵測行動及智慧財產保護，美歐西方民主國家與中國、俄羅斯的網路言論過濾，似乎異曲同工，都脫離不了封鎖網路、過濾網路內容的手法，此種狀態無異是在宣告網路空間是國家主權的管轄範圍。而如果網路業者共識這些網路上的治理行為，則必須配合國家的法令執行網路管制政策並透過技術實現，在各入口及節點等網際網路賴以建構的實體基礎上實施相關管制措施，網際網路成為不屬於國家主權的人類的公共領域將更形艱難。

伍、網路空間國家主權聲明與劃分原則之芻議

一、挹注國家主權新的意涵

國家主權的範疇並非固定不變，而是隨著歷史的發展，依照現實的需求而進化。其內涵隨著的歷史、主體的可變更性及行使的範疇而演變。世界各國都一直堅守和發展國家主權原則，而這一原則也一直貫穿國際法始終，用發展的眼光看待國家主權就顯得尤為必要（韓洵，2008）。

國家主權的演化到了現代，經歷了一個發展劇變的過程，隨著全球化的來臨，不僅包括了政治主權，還擴大到經濟和文化主權，主權行為體也由神權、君權而到了以民為主的國家，甚至由國際組織代表各國行使主權。國家主權的涵蓋範疇，也由領土、領海，到了涵蓋領空。

國家主權的發展，在網際網路時代似乎遇到了瓶頸，因為網路空間似乎並不符合國家主權要件中所具備的條件。然而，基於主權演進的經驗，文化、經濟也非有具備固定的實體要件，欲定義網路空間的國家主權，吾人不妨可以從構成網路空間之資訊平台的角度出發，發展出新的國家主權意涵，亦即，回歸網路空間構建的基礎：主機與線路構成的實體平台管理，取其實而避其虛，以國土延伸之概念在網路空間中發展出國家主權宣告與辨識的機制。

二、提供網路空間國籍識別界定虛擬領土

網際網路是將各自獨立的終端設備通過線路（電話線或光纖）連接而成，以無數相

互協作的電腦資訊網路組成的系統。[4] 網路中的各個節點可以連接分散於各處的資訊系統，而在網上形成共用的資源。由實體的主機及線路構成的網路空間，雖然沒有人類的行為，但仍然是一個可以界定如何區域分隔的實體。

網路空間雖然是藉由許多科學技術標準建構而成，而行為在網路與實體世界中卻無法截然二分，具體而言，網際網路上所從事的行為仍受現實世界的規範所規制（鄭嘉逸，2009）。從這個觀點視之，似乎提供了國家主權延伸在網路空間的支點。

提供一個網路空間國籍識別的方法，在網路空間展現國家主權，是一個可以考慮的方向，如此網路功能變數名稱解析就不再是界定所屬國家的標準。在網路空間若能識別所屬國家，就可如同航空器或船舶，建構一個虛擬上的領土宣告與識別，換句話說，可視同國家主權的延伸。至於如何提供網路空間國籍識別的方法與架構，則必須是在確定網路空間國家主權之意涵後，才能從網路管理的技術面所找出的解決方案。基本上，在技術與可行性上應無太大的困難，由於涉及網路通訊協定與技術細節，將另文詳細討論。

陸、結論

網際網路的發展與應用造成國家主權有逐漸被侵蝕的跡象，各國無不致力於對付網路時代國家安全及利益上的威脅，引發了國際上不同陣營的國家不同立場，對於國家主權是否當存有於網路空間的爭論。以美國為首的西方先進國家認為，網路空間應為一中立的空間，全人類在網路空間中應有相等的網路人權，因此反對以國家主權之名干預網路空間的活動。開發中的國家陣營則視來自網路空間對其政體與制度的挑戰為干預內政的威脅，而以國家主權之名進行必要的管控。吾人以為，無論是基於攻擊上的防護，或是限制資訊的傳遞，都必需藉由彰顯國家主權的存在來運作。此外，跨國的網路犯罪，亦須由實體的國家力量來進行整治，凡此種種，在在都彰顯了網路空間無法脫離國家主權的概念的事實。然而，就國家主權原本的意涵而言，網路空間中並無符合國家主權立基的條件，且現今國際法對國家主權之要件尚無法用以宣稱或識別網路空間中的國家主權，以致於對網路空間中虛擬世界國家主權的挑戰與侵蝕，終究將回歸到現實世界來具體解決。唯有挹注國家主權新的意涵以符合網路空間的現狀，以國土延伸的概念來解決網路空間中主權宣告與識別。運用網路資訊管理技術來奠立解決國家主權政治問題的基石，在網路空間提供國籍識別，以及界定虛擬的網路疆域，是未來提供有關網路空間國際法的制定，以及得以運用國際仲裁來解決國際間網路衝突的有效解決方案。

參考文獻

＜美國研議「禁止網路盜版法案」引發美國遊戲界不同看法＞，2012 年 1 月 13 日，《中時電子報》，<http://news.chinatimes.com/tech/171710/172012011300590.html>（瀏覽日期：2012 年 3 月 28 日）。

＜國際瞭望——網際網路，美國的獨門武器＞，2010 年 1 月 26 日，《中國時報》，<http://www.crtv.tv/doc/1012/0/9/9/101209997.html?coluid=0&kindid=0&docid=101209997>（瀏覽日期：2012 年 3 月 28 日）。

＜新加坡媒體發展局＞，2010 年 11 月 11 日，《文化部・文化創意產業推動服務網》，<http://cci.culture.tw/cci/cci/market_detail.php?sn=4305>（瀏覽日期：2012 年 3 月 28 日）。

[4] 網際網路最早起於 1969 年由美國國防部的尖端研究計畫局（Advance Research Projects Agency, ARPA）所提出一項網路整合計畫，該計畫的計畫名稱為「ARPANET」，最初設計的目的是作為軍事單位通訊之用（Hauben and Hauben, 1997）。

方鈞、趙青海，2012 年 3 月 29 日，＜我國戰略機遇期所面臨的國際格局演變＞，《中國改革論壇》，<http://www.chinareform.org.cn/open/view/201203/t20120329_138081.htm>（瀏覽日期：2012 年 4 月 15 日）。

中華人民共和國外交部，2011 年 9 月 12 日，＜資訊安全國際行為準則＞，《中華人民共和國外交部》，<http://www.fmprc.gov.cn/chn/pds/wjb/zzjg/jks/fywj/t858317.htm>（瀏覽日期：2012 年 4 月 15 日）。

中華民國國防部史政編譯室譯，Armistead L 著，2012，《資訊作戰》，台北：作者。

沈經，2011 年 11 月 7 日，＜歐盟與美國首次舉辦網路資安聯合演習＞，《iThome Oline》，<http://www.ithome.com.tw/itadm/article.php?c=70678>（瀏覽日期：2011 年 12 月 3 日）。

吳嘉生，1999，《國家之權力與國際責任》，台北：五南。

陳成良，2011 年 9 月 16 日，＜美澳協防，首度納入網路戰＞，《自由時報》，<http://www.libertytimes.com.tw/2011/new/sep/16/today-int3.htm>（瀏覽日期：2012 年 1 月 28 日）。

陳曉莉，2010 年 4 月 21 日，＜各國政府對網路內容／資料要求：Google 透明化＞，《iThome Online》，<http://www.ithome.com.tw/itadm/article.php?c=60769>（瀏覽日期：2012 年 4 月 28 日）。

黃惠康，2012 年 1 月 13 日，＜外交部官員：網路主權隸屬國家主權之下＞，《中國新聞網》，<http://big5.chinanews.com:89/gn/2012/01-13/3604104.shtml>（瀏覽日期：2012 年 2 月 10 日）。

湯先營，2011 年 10 月 20 日，＜印度完善《資訊技術法》加強網路監控＞，《光明日報》，<http://big5.chinanews.com:89/gj/2011/10-20/3403260.shtml>（瀏覽日期：2012 年 1 月 28 日）。

彭慧鸞，2011，＜網路安全治理的新紀元——從美國網際網路國際戰略談起＞，《2011 年度國際及中國大陸情勢發展評估報告：國際情勢發展與評估》，台北：國立政治大學國際關係研究中心。

雷東瑞，2011 年 9 月 13 日，＜中俄等國向聯合國提交「資訊安全國際行為準則」檔＞，《新華網》，<http://news.xinhuanet.com/world/2011-09/13/c_122022390.htm>（瀏覽日期：2012 年 1 月 28 日）。

趙海建，2012 年 4 月 18 日，＜盤點各國治理網路謠言方法，奧巴馬曾受謠言困擾＞，《廣州日報》，<http://big5.ce.cn/gate/big5/intl.ce.cn/qqss/201204/18/t20120418_23251005.shtml>（瀏覽日期：2012 年 4 月 20 日）。

董菁，2012 年 1 月 19 日，＜美國媒體：反盜版不可損害互聯網自由＞，《人民網——國際頻道》，<http://world.people.com.cn/BIG5/16922129.html>（瀏覽日期：2012 月 2 月 13 日）。

齊思賢譯，Lester CT 著，2000，《知識經濟時代》，台北：時報。

鄭嘉逸，2009，＜網際網路管轄權之擴張與緊縮＞，《經社法制論叢》，43 期：頁 127 － 159。

盧映孜譯，2011 年 6 月 9 日，＜駭客猖獗，北約擬設專組因應＞，《大紀元》，<http://www.epochtimes.com/b5/11/6/9/n3281146p.htm>（瀏覽日期：2012 年 1 月 28 日）。

韓洵，2008，《全球化背景下的國家主權理論思考》，青島大學國際關係學院碩士論文。

“Google Transparency Report,” n.d., *Google*, <http://www.google.com/transparencyreport/> (accessed April 28, 2012).

“VP’s Remarks to London Cyberspace Conference,” November 1, 2011, *The White House*, <http://www.whitehouse.gov/the-press-office/2011/11/01/vps-

remarks-london-cyberspace-conference> (accessed January 15, 2012).

Alexander KB, June 3, 2010, "U.S. Cybersecurity Policy and the Role of U.S. CYBERCOM," *Cyberwar Resources Guide, Item #155*, <http://www.projectcyw-d.org/resources/items/show/155> (accessed March 19, 2012).

Bame M, July 22, 2011, "Strategy for Operating in Cyberspace (DSOC)," *About.com*, <http://defense.about.com/b/2011/07/22/dod-strategy-for-operating-in-cyberspace-dsoc.htm> (accessed March 19, 2012).

Center for Strategic and International Studies, June 3, 2010, "CSIS Cybersecurity Policy Debate Series: U.S. Cybersecurity Policy and the Role of U.S. Cybercom," *National Security Agency/Central Security Service*, <http://www.nsa.gov/public_info/_files/speeches_testimonies/100603_alexander_transcript.pdf> (accessed January 15, 2012).

Clinton HR, February 15, 2011, "On Internet Rights and Wrongs: Choices & Challenges in a Networked World," *America.gov*, <http://www.america.gov/st/texttrans-english/2011/February/20110215155718su0.3556896.html?CP.rss=true#> (accessed April 15, 2012).

Deeks AS et al., 2005, "Combating Terrorist Uses of the Internet," in *Proceedings of the Annual Meeting: American Society of International Law*, Washington, DC, US: American Society of International Law, 103-115.

Dibbell J, February 16, 2012, "Internet Freedom Fighters Build a Shadow Web," *Scientific American*, <http://www.scientificamerican.com/article.cfm?id=the-shadow-web> (accessed March 19, 2012).

Gibson W, 1984, *Neuromancer*, London, UK: HarperCollins.

Gjelten T, 2010, "Shadow Wars: Debating Cyber 'Disarmament'," *World Affairs*, <http://www.worldaffairsjournal.org/article/shadow-wars-debating-cyber-disarmament> (accessed April 15, 2012).

Hague W, November 1, 2011, "Cultural Differences No Excuse to Dilute Online Rights," *Tech Europe*, <http://blogs.wsj.com/tech-europe/2011/11/01/cultural-differences-no-excuse-to-dilute-on-line-rights/> (accessed April 15, 2012).

Hauben M and Hauben R, 1997, *Netizens: On the History and Impact of Usenet and the Internet*, Los Alamitos, CA, US: Wiley-IEEE Computer Society Press.

Hopkins N, April 16, 2012, "Militarisation of Cyberspace: How the Global Power Struggle Moved Online," *The Guardian*, <http://www.guardian.co.uk/technology/2012/apr/16/militarisation-of-cyberspace-power-struggle> (accessed April 28, 2012).

Intellectual Property Watch, April 6, 2010, "ITU in a Converging World: Interview with ITU Strategist Alexander Ntoko," *Intellectual Property Watch*, <http://www.ip-watch.org/2010/04/06/itu-in-a-converging-world-interview-with-itu-strategist-alexander-ntoko/> (accessed April 15, 2012).

Komov S et al., 2007, "Military Aspects of Ensuring International Information Security in the Context of Elaborating Universally Acknowledged Principles of International Law," *Disarmament Forum*, 3, 35-43.

Mackinnon R, April 3, 2012, "Internet Freedom Starts at Home, Foreign Policy: The United States Needs to Practice What It Preaches Online," *Foreign Policy*, < http://www.foreignpolicy.com/articles/2012/04/03/The_Worlds_No_1_Threat_to_Internet_Freedom?page=0,2> (accessed April 10,

2012).

Solove DJ, 2007, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*, New Haven, CT, US: Yale University Press.

The White House, May 17, 2011, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," *The White House*, <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf> (accessed January 15, 2012).

United Nations, 2011, *Disarmament Study Series, No.33: Developments in the Field of Information and Telecommunications in the Context of International Security*, New York, US: United Nations.

US Department of Defense, November 8, 2010, "Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms (As Amended Through 15 April 2012)," *DOD Dictionary of Military Terms*, <http://www.dtic.mil/doctrine/dod_dictionary/index.html> (accessed January 15, 2012).

Wiener N, 1965, *Cybernetics: Or Control and Communication in the Animal and the Machine* (2nd ed.), Cambridge, MA, US: MIT Press.

World Summit on the Information Society, 2003, *Plan of Action -- Document WSIS-03/GENEVA/DOC/5-E*, Document of the World Summit on the Information Society Geneva2003-Tunis 2005.

World Summit on the Information Society, 2005, *Compilation of Comments Received on the Report of the Working Group on Internet Governance, WSIS-II/PC-3/DT/7(Rev.1) E 26*, Document of the World Summit on the Information Society Geneva2003-Tunis 2005, 39-47.

前瞻科技與管理　2卷2期，1－14頁（2012年11月）
Journal of Advanced Technology and Management Vol.2, No.2, 1-14 (November, 2012)

On Extending State Sovereignty over Cyber Space

Te-Chao Liang[1, *], Chih-Ping Chu[2], and Kai-Hsun Lin[2]
[1]Department of Information Management, Tamkang University
[2]Graduate Institute of Management Sciences, Tamkang University

Abstract

The Internet has accelerated the development of globalization. It not only forms a parallel communication mode across states, but also changes the legal system constructed on the basis of national sovereignty. Governments are doing their best efforts to maintain the cyber space owing to the threat for national securities and interests are created from the cyber space worldwide. That leads to controversies of state sovereignty from different aspects. Although it is difficult to explore the state sovereignty in cyber space, but ineluctable, the controversies of state sovereignty have already existed among nations in the cyberspace. Whether to defense from a network attack or to limit the network information transmission, these must be through the state sovereignty to justify the actions. To resolve the international conflicts in cyberspace, international arbitration has to be involved thus a new implication of state sovereignty has to be explored, so that we can have a nationality identification mechanism as well as the boundaries of nations for the bases of arbitration in cyberspace.

Keywords: cyberspace, state sovereignty, cyberwarfare, Internet freedom, virtual territory

* Corresponding Author: Te-Chao Liang
E-mail: tcliang@mail.tku.edu.tw