10.6326/NDJ.2015.30(3).4

美國網路安全防護經驗對我國網路安全情勢之啟示

The US Experience of Cyber Security and Its Implications to Taiwan's National Security

陳育正 (Yu-Cheng Chen)

中興大學國際政治研究所博士生

摘　　要

受惠於網路科技進步，各國之間對話、交流、貿易等活動擴大了全球物品的流動。維持國家內部穩定運作的關鍵基礎設施，也連帶提供非常便利的服務，包括電力、水力、交通以及金融體系，而數位化的關鍵基礎設施，成爲促進經濟繁榮、強大軍事力量、政府施政透明度的重要基石。然而日益依賴網路的同時，可能因爲網路科技產生漏洞，使得國家安全面臨挑戰。美國了解網路安全挑戰，影響層面涵蓋軍事領域、經濟、民生，甚至國際事務等，將網路安全問題視爲重要的威脅來源之一。

本文分析美國應對網路安全威脅實踐過程，探討網路安全對於美國的意義，歸納美國目前面臨的網路安全威脅趨勢；另外也體認出美國應對網路安全威脅的防護經驗，計有「邁向組織創新」、「提升政府部門與私人企業合作」，以及「強化情報與反情報工作」等三項；最後強調借鏡美國網路安全防護經驗，進而建立「完善之前瞻性戰略」與建構「安全工作的新穎情境」等作爲，有助於提升我國網路安全效能。

關鍵詞：網路空間、關鍵基礎設施、國家安全戰略、網路安全、資訊安全

Abstract

Information technology has enhanced international dialogue, exchange and trade and facilitated global flow of goods and services. Key infrastructures which withhold internal stability and operation of country provide convenient services including electricity, water, transportation and financial system. Digitalized infrastructures can promote economic prosperity, strengthen military capability, and enhance the transparency of government. Nevertheless, while the world is increasingly relying on cyberspace, it is likely that loopholes can be generated along with the development of information technology. Thus, key infrastructures can be devastated by cyber attacks and pose great challenges to national security. The US acknowledge the scope of cyberspace challenges which covers the fields of military, economy, livelihood, and even international affairs. The cyber security has also been considered as one of the most serious threats to national security.

Through the practicing process for tackling the challenges of cyber security, this article analyzes the implications of cyber security to the US, and generalizes the trend of cyber threats that the US is currently facing. Secondly, it illustrates the experiences of how America protects its cyber security, including innovation of organization, promotion of public-private partnership, and strengthening the efforts of intelligence gathering and counter-intelligence efforts. Finally, it is worth learning the lessons from American's cyber security protection in order to establish a comprehensive and forward-thinking strategy and to build new circumstances for security works. These efforts are able to enhance the efficacy of Taiwan’ s security works so national security can be ensured.

Keywords: Cyberspace, Key Infrastructure, National Security Strategy, Cyber Security, Information Security

壹、前　　言

因為科技資訊發達與全球化的影響，現代國家所面臨安全的挑戰，除了軍事層面威脅因素外，更包含非軍事層面。其來源是多元化、多面向、綜合性。舉凡可能影響國家主權的行使、政治制度、傳統文化、生活方式，以及國家賴以生存發展的一切有形、無形力量，皆可視為國家安全威脅的範圍。例如，在美國國土安全(homeland security)層面上，有關恐怖主義結合網路空間、跨境犯罪、緊急事態的安全威脅，都改變傳統威脅途徑，不僅超越傳統疆界，亦多指涉其他類領域，與非軍事性的全球治理、政治價值觀、外交政策、經濟等議題相互複合。

然而，美國早在2003年，前總統布希(George W. Bush)執政期間，即公布《確保網路空間的國家戰略》(The National Strategy to Secure Cyberspace)，這是第一次將「網路空間」設定為國家安全戰略報告，內容指出：「透過制定防護措施，保護資訊基礎設施免於遭受破壞、干擾，進而維護美國經濟發展，達成國家安全之目的」。[1]現任美國總統歐巴馬(Barack H. Obama)，對於網路安全威脅的議題也持相同關切態度。2009年5月公布新的國家網路安全戰略(National Cybersecurity Strategy)來協調、整合全國各項網路安全方案，並警示：「網路威脅是美國當前經濟與安全最為嚴峻的考驗」，同時白宮也成立網路空間辦公室(National Office for Cyberspace, NOC)，將全國的數位基礎建設視為國家戰略資產，甚至成立網路司令部(Cyber Command)，專責保護各種聯繫網路裝置，以防止遭到網路攻擊以及快速反應部隊。[2]可以清楚發現美國將網路安全工作納入國家安全戰略的重要發展目標。然而美國在建立應對網路威脅的過程中，筆者歸納出三點作為我國借鏡：提供組織創新、提升政府與民間合作，以及強化情報與反情報工作等。這些經驗對於我國而言，具有知識與政策應用意涵，有助於

1 The White House, “The National Strategy to Secure Cyberspace,” February 2003, p. vii（檢索日期：2015年1月5日）

2 James R. Langevin, Michael T. McCaul, Scott Charney, and Harry Raduege, *Securing Cyberspace for the 44 Presidency,* (Washington, D.C.: CSIS, 2008), pp. 5-6（檢索日期：2015年1月15日）

我國安全工作的發展。

貳、研究問題與概念架構

美國自從二次大戰以來，透過強大軍事科技，以及由美國為首的國際制度，使其能在國際體系當中扮演相當重要角色；在後冷戰時期，許多新興的安全威脅相繼出現，美國不僅持續關注各種威脅來源的發展，也透過戰略報告宣示美國應處的決心。網路安全議題則是美國所面臨重要的威脅來源之一，然而美國在應對網路安全威脅實踐過程中，除整合安全體系外，並強調透過跨部門、跨政府資訊分享、主導政府部門與私人企業進行合作，以及情報與反情報工作等方式，發展出特別的網路安全防護經驗。

本文首先探討網路安全議題對於美國有哪些重要意涵；其次說明近年來美國面臨網路安全威脅的趨勢有哪些；最後分析美國官方重要戰略報告，以及實踐過程中，歸納出美國應對網路安全特有的經驗「邁向組織創新」、「提升政府與民間合作」，以及「強化情報與反情報功能」等三項，而美國應對網路安全威脅特有經驗，有助於我國安全部門理解近來網路威脅趨勢，以及提升知識與政策應用等方面之價值。然而，本文僅以國家安全政策分析之角度出發，尚無法進一步探討有關網路空間帶來國際衝突、競爭等問題，甚至近年來大量學者探討有關美國執行網路安全過程中，可能涉及個人隱私、執法正當性等法律層面問題，本文則留待日後加以探討。

參、網路安全及其挑戰

在網路科技進步發展下，政府、民間企業等業務運作，都是由資訊設施、系統所建構，而網路的快速發展，更成為民眾日常生活不可或缺的重要工具。換言之，對網路設施的依賴性也就越來越高。

一、網路安全之意涵

要了解網路安全，必須先釐清幾項重要名詞、概念。首先「網路空間」(cyberspace)在美國國防部《網路空間行動戰略》(Strategy for Operating in Cyberspace)中定義為：「是組成現代化生活方式，並且提供世界各地的個人、社群進行連結，以及社會化，甚至成為全球經濟的重要關鍵部分」；[3] 其次有關「關鍵基礎設施」(critical infrastructure)方面，美國白宮2003年公布的《確保網路空間安全的國家戰略》(The National Strategy to Secure Cyberspace)報告，指出關鍵基礎設施依賴網路科技進行運作，將國防工業、通訊、資訊技術等18項基礎設施部門列為關鍵基礎設施，並且將核電廠、政府設施等5項列為重要資產，然而報告重點在於政府已開始制定相關防護措施，避免關鍵基礎設施遭受破壞；[4] 另外美國國土安全部報告也描述，截至2014年美國目前至少有12億臺電腦設備，控制國內發電、供水、交通、通訊、經濟，以及政府部門等運作，網路空間是美國與世界接軌重要管道。[5] 由此可

3 U.S. Department of Defense,“Department of Defense Strategy for Operating in Cyberspace,” July, 2011, p. 1, *U.S. Department of Defense*（檢索日期：2015年1月11日）

4 The White House,“The National Strategy to Secure Cyberspace,” February, 2003, p. vii, *The White House*（檢索日期：2015年1月11日）

知，網路空間結合了個人、社會、國家，以及國際經濟的發展，網路空間的安全與否將牽動國家持續和平、繁榮地發展關鍵因素。

美國國防部在2005年公布《國防戰略報告》(The National Defense Strategy of The United States of America)，明確指出網路將和陸、海、空、太空領域發展認為具有同等重要性，美國必須維持這些領域的優勢地位。[6] 對此，美國白宮在2010年版的《國家安全戰略》(National Security Strategy 2010)報告加以呼應。說明某些網路竊密等破壞行為，已造成美國高達數百億的經濟損失，確保網路空間安全穩定是國家發展的重要目標。[7] 顯而易見，人們越依賴網路科技，使網路空間成為建構國家發展的重要基石。同時網路安全問題越來越多，使得國家安全面臨嚴峻挑戰。例如美國主管安全事務的情報首長克萊柏(James R. Clapper)上將，在呈送參議院情報委員會《美國情報社群分析全球威脅評估報告》(Worldwide Threat Assessment of the US Intelligence Community)中提到，美國目前面臨重要的威脅即是網路空間帶來的挑戰。許多國家與非國家行為者大量使用網路攻擊、網路間諜等方式，達到其戰略目的，破壞美國關鍵基礎設施，影響其經濟發展與國家安全；[8] 另外美國國土安全部在2010年也發布《國土安全四年期總檢報告》(Quadrennial Homeland Security Review Report)進一步分析網路安全威脅來源。內容指出，現今的國際環境當中，國家和非國家行為者利用科技來改變社會、經濟和政治力量，便能迅速傳播信息及達成其目標，並利用新的手段來破壞美國。尤其是運用不對稱策略，發展極具殺傷力和高科技武器裝備的恐怖主義與網路攻擊，並針對美國政府網路系統進行入侵與破壞，入侵包括關鍵的能源、財政、衛生、商業與交通等基礎建設。威脅來源涉及到極端主義，可能對人口密集的城市中心進行小規模的爆炸和網絡攻擊與入侵，甚至鎖定其中重要的象徵性指標來進行破壞。[9] 從這些文獻可以發現，美國對於關鍵基礎設施大多依賴網路空間，這些關鍵基礎設施正是能確保國家穩定發展的重要基石。但是，網路空間卻也經常遭受個人、組織、或國家的意志所運用，並入侵、破壞敵人網路設施，達到其特定目的。

二、美國面臨網路安全威脅趨勢

㈠恐怖主義與網路之結合

網路恐怖分子除了應用電腦或通信技術，進行個人或財產等傳統利益之襲擊，也會阻斷網路服務系統，破壞關鍵基礎設施功能。網路恐怖主義一方面引起較傳統犯罪更

5 U.S. Department of Homeland Security,“The 2014 Quadrennial Homeland Security Review,” December 23, 2014, p. 7, *Department of Homeland Security*（檢索日期：2015年1月11日）

6 U.S. Department of Defense,“The National Defense Strategy of The United States of America,” March, 2005, p. 13, *U.S. Department of Defense*（檢索日期：2015年1月11日）

7 The White House,“National Security Strategy 2010,” May 2010, p. 18, *The White House*（檢索日期：2015年1月11日）

8 James R. Clapper,“Worldwide Threat Assessment of the US Intelligence Community,” March 12, 2013, p. 1, *Office of The Director of National Intelligence*（檢索日期：2015年1月11日）

9 U.S. Department of Homeland Security,“A Strategy Framework for a Secure Homeland,” February 2010, p. 7, *Department of Homeland Security*（檢索日期：2015年1月12日）

令人感到恐懼的效應，有時候用來恐嚇、脅迫政府、人民，以達成其政治或社會目的。因此，網路恐怖主義是恐怖主義與網路空間之複合，不僅對個人生命、財產，以及心理層面造成危害，甚至應用至大眾交通工具、關鍵基礎設施等系統，影響範圍將擴大到整個社會，並對國家經濟穩定與進步造成影響。另一方面，恐怖主義若利用網路空間，進行相關宣傳與募款，或者透過網路發布訊息，深深影響廣大人心。這將有利恐怖分子進行人員招募。進一步而言，網路恐怖主義利用網路空間，進行預謀訊息傳遞、募款、建置網絡社群、訓練人員與蒐集資訊等等，都是有利其行動隱匿性提高、效能提升；當然，網路恐怖主義也會運用網路平臺進行宣傳，以影響民眾的心理。[10]

隨著恐怖分子的資金及可襲擊之管道越來越多，其犯罪行動選項也隨之增加，使得他們的破壞能力更加可怕。如恐怖組織運用財力，雇用罪犯發動「殭屍網路」(Botnet)，入侵他人電腦而進行犯罪行為。另如，在網路上傳送數千封甚至數百萬封垃圾郵件、監視與竊取世界各地電腦使用者的個人金融資料，或是阻斷其電腦系統運作的拒絕存取服務的攻擊。[11] 恐怖分子利用網路空間破壞某個特定企業、政府組織或基礎設施的網路系統，造成重大損害，或者入侵與中斷金融商務之重要資料，不僅影響民眾生命、財產安全，也危害國家安定，這些方式，無疑有助於恐怖分子達成其目的，也同時強化他們襲擊手段。恐怖分子越來越了解網路的弱點，使得恐怖分子運用網路空間達成其目的可能性逐漸提高，其危害性跨越傳統國界，是未來無可避免的問題。[12]

㈡網路犯罪出現易變性

美國防毒軟體製造商諾頓(Norton)2010年的報告中說明，每天有蠕蟲電腦病毒影響500萬臺電腦，概略超過一半以上成年的網路使用者。因為遭人入侵電腦或硬碟損壞已經造成資料無法補救的情況。甚至，2009年裡，假冒他人的電子信箱造成用戶損失超過1,400億美元。[13] 網路犯罪除了組織特性與利用新興科技外，其行為態樣與電腦犯罪也具有交互指涉之特性。[14] 常見型態的網路犯罪部分以電腦作為犯罪工具或目標，進一步擴大到通訊、影音、智慧財產權網路空間等非實體層面；另一方面，某些違法行為（如毒品交易、詐欺、勒索、洗錢）也伴隨網路空間方式進行。換言之，犯罪行為經常與網路空間複合，形成網路犯罪。

高科技犯罪調查協會(High Technology Crime Investigation Association)曾在「網路犯罪調查報告」(Report on Cyber Crime Investigation)指出，近年來使用數位科技進行

10 黃秋龍，《非傳統安全論與政策應用》（臺北：結構群文化，2009年），頁14-15。

11 Marian Merritt, Norton, “Cyber Crime Exposed 2010,” 2010, p. 15, *Symantec*, <http://www.symantec.com/content/en/us/home_homeoffice/media/pdf/norton_cybercrime_exposed_booklet.pdf>（檢索日期：2015年1月14日）

12 Colonel Steven P. Bucci, “A Most Dangerous Link,” October 2009, *U.S. Naval Institute*, <http://www.usni.org/magazines/proceedings/2009-10/most-dangerous-link>（檢索日期：2015年1月15日）

13 Marian Merritt, Norton, “Cyber Crime Exposed 2010,” p. 2.

14 Todd G. Shipley, “2010 Report on Cyber Crime Investigation,” 2010, p. 4, *High Technology Crime Investigation Association*, <http://www.htcia.org/pdfs/2010survey_report.pdf>（檢索日期：2015年1月15日）

犯罪之比率已經逐漸提高。許多不同類型的網路犯罪手法結合傳統犯罪正在進行易變。但是，進一步探究這些現象的成因，發現大部分的組織或單位，存在職能重疊(overlap)問題，使得安全工作的預防能力無法有效發揮，進而產生應對能力窒礙問題。[15] 顯而易見的，不論行為者身在何地，只要運用網路與程式，即可對第三方進行資料竊取、干擾與破壞等犯罪行為。這些行為者，可能由個人、團體，或某些組織受到國家資助，所進行網路犯罪行為，犯罪者因為對象抱持不同目標，遂產生不同的網路犯罪事實。

㈢美國與中共在網路空間之競爭

中共近年來利用網路科技，大量招募專業技術人員組成「網軍」，而這批專業人才來自學者與企業界，可執行網路襲擊和防禦手段。[16]政府部門也有單位執行這些工作。中共政府早期大多運用網路空間聚焦有關反政府的對象與行為，後來轉變成對外情報蒐集方式之一，由於情報蒐集有助於了解先進國家重要訊息與技術，進而提升本身經濟與軍事現代化，其中近期利用解放軍的駭客部隊入侵網路系統，以及民間商人貿易經商等過程，進行機敏資料蒐集、竊密，更引發國際以及美國重視。

中共解放軍駭客部隊，自2006年起大約竊取115家美國大企業的機密數據，包括可口可樂收購中國大陸企業、美國無人機科技，以及另有關資訊、電信、航空、能源等行業之重要資料被偷。美國眾議員魯波斯柏格(Dutch Ruppersberger)則指出，2013年期間有關美國遭到駭客竊取商業機密問題，使得美國企業該年度總計損失約3,000億美元，並且以解放軍代號為61398網路駭客部隊所造成的損失最為嚴重。其近年更聚焦美國高科技產品製造技術，例如無人飛機科技。[17] 美國網絡安全公司群擊(CrowdStrike)則說，代號61486的解放軍網路部隊，從2007年起開始對西方國家政府和國防事務承包商資訊系統進行網路攻擊，尤其以太空、通訊領域部分等先進科技技術，更為其關注焦點。甚至進一步發現61486部隊與61398部隊，經常共享電腦資源、相互通訊聯繫。[18] 在中共駭客行為日益猖獗情況下，美國勢必對於這些犯罪行為做出回應。美國司法部在2014年5月大規模起訴5名中共解放軍軍官涉及網路間諜罪，因為美國政府確切掌握渠等入侵網路系統，竊取美國西屋電器公司、美國鋼鐵公司等金屬、太陽能產業機密資訊，進而展開調查，最後正式起訴5名解放軍軍官，並且還進一步發現這5位解放軍軍官也都隸屬61398部隊。[19] 其次，中共利用民間商業往來過程，伺機竊

15 Todd G. Shipley,“2010 Report on Cyber Crime Investigation,” p. 4.

16 United States-China Economic and Security Review Commission,“U.S.-China Economic and Security Review Commission 2009,” November 2009, p. 8, *U.S.-China Economic and Security Review Commission*（檢索日期：2015年1月15日）

17 連雋偉，〈陸駭客竊密　美國年損逾9兆〉，《中時電子報》，2014年5月20日（檢索日期：2015年1月15日）

18〈美報告再指責中國大陸軍方網路間諜活動〉，《BBC中文網》，2014年6月10日（檢索日期：2015年1月17日）

19 Shannon Tiezzi,“U.S. Indicts 5 PLA Officers For Hacking, Economic Espionage,” May 20, 2014, *The Diplomat*（檢索日期：2015年1月16日）

取美國先進科技技術，例如中共商人蘇斌(Su Bin)，涉嫌在2008年至2014年間入侵美國國防承包商之電腦系統，取得F-22、F-35戰機等機敏資料，以轉售中共國營企業，最後遭受美國加州聯邦法院起訴。[20]

值得注意的是，美國前國家安全局雇員史諾登(Edward Snowden)在2013年6月向部分媒體披露美國一直在進行全球監測及收集情報的網絡，包括美國盟友都被監聽，而中共也是美國網路監控下的受害者。[21] 事後引發各國對美國行為進行譴責，特別在中共方面，其反擊力道更為強烈。由於經常被美國指控進行網路竊密行為，如今美國卻也被揭露對其他國家進行大規模網路監控行動。對中共而言，確實是反擊美國的最佳時機，中共人民解放軍軍事科學院教授王長勤在接受新華社採訪時表示，在史諾登事件後，完全打破美國自稱是網路自由捍衛者、網路受害者的形象，是名副其實的駭客帝國。[22]

美國確實已關注中共所展現的國際影響力，同時也擔憂中共在網路科技的發展，不僅運用非法入侵(intrusions)行為，竊取美國重要軍事科技技術、商業機密，甚至在許多人民解放軍所公布的文獻當中，多次強調發展網路戰、網路攻擊、反介入戰略等。顯示美國仍然對於中共網路發展，感受國家安全、利益遭受威脅之嚴峻挑戰，甚至許多國家、團體也可能將網路科技來結合軍事力量，達成其戰略目標。[23] 更重要的是美國在網路空間發展過程中，與中共在網路安全議題上由於意識型態不同，經常發生衝突，然而這些衝突大多涉及到經濟與軍事發展。[24]本文未進一步研究美、中在網路安全不同之意識型態，產生何種影響，而僅就美國立場，聚焦美國如何防範網路入侵行為，或者如何提升處理網路安全問題的效能。

肆、美國應對網路安全威脅之經驗

美國國防、情報安全體系之間向來就存在著制度困境與組織障礙，不同階層、體系，伴隨著各自為政、資源分散、合作協調困境，甚至於在同一機關（構）或部門內，都存在資訊透明度不足、[25] 應對能力窒礙之問題；[26] 另一方面，美國也面臨恐怖分子與網路空間結合、網路犯罪問題，以及中共

20〈美司法部指控中國商人竊取美國防技術〉，《BBC中文網》，2014年7月12日（檢索日期：2015年1月16日）

21 何清漣，〈點評中國大陸：史諾登事件的多重效應〉，《BBC中文網》，2013年6月17日（檢索日期：2015年1月16日）

22 狄雨霏，〈中國軍事專家痛批稜鏡門，指美國為駭客帝國〉，《紐約時報中文網》，2013年6月26日（檢索日期：2015年1月17日）

23 U.S. Office of Secretary of Defense,“Annual Report on Military and Security Developments Involving the People's Republic of China,” August 16, 2010, p. 7, *Department of Defense*（檢索日期：2015年1月17日）

24 James A. Lewis,“Cyber War and Competition in the China-U.S. Relationship,” May 2010, p. 1, *CSIS*, http://csis.org/files/publication/100510_CICIR%20Speech.pdf（檢索日期：2015年1月17日）

25 James R. Langevin, Michael T. McCaul, Scott Charney, and Harry Raduege,“Securing Cyberspace for the 44 Presidency,” pp. 5-7.

26 Todd G. Shipley,“2010 Report on Cyber Crime Investigation,” p. 4.

積極發展網路能力，更是對美國經濟、安全造成嚴重威脅。就美國實踐其網路安全目標過程而言，體認處理網路安全問題並非單一政府部門、組織機構可以獨立處理，而必須站在更高層次的戰略角度，重新整合安全體系，提升跨國、跨部門、公私部門間合作，以及強化情報與反情報工作。

一、邁向組織創新

美國在911事件後，積極提升反恐效能，2002年國會通過《國土安全法案》(Homeland Security of Act)，賦予國土安全部(Department of Homeland Security)五項重要核心任務，包括「預防恐怖主義」、「確保邊境安全」、「強制落實移民法」、「確保網路空間安全」，以及「具有彈性能力應對災害事故」等，[27] 除此之外，在執行網路安全方面，國會同時指定該部必須進行網路安全任務，負有協調國家安全工作、保護所有包含資訊技術與通信技術之領域關鍵基礎設施責任，國土安全部部長更被賦予可運用任何威脅美國的恐怖主義和相關資訊之權力。[28]

歐巴馬總統除承接小布希政府對於網路安全的戰略思維外，也透過許多專家、學術機構所提出各項提升網路空間安全建議，其中特別以《確保網路空間安全---給第44任總統建言》(Securing Cyberspace for the 44th Presidency) 這份報告，深深影響歐巴馬有關網路安全的決策。報告內容有許多關於行政組織變革的具體建議。例如成立網路空間辦公室，負責發展國家網路安全政策，以及督導政府單位執行與考核。[29] 而在2009年5月29日，歐巴馬總統正式宣布成立白宮網路安全辦公室(National Office for Cyberspace)；另外，建立由國家領導人所直接統轄的網路空間之專責單位，與國家安全局共同制定詳盡的國家網路安全策略。隨後前國防部長蓋茲(Robert Gates)在同年6月23日宣布成立網路司令部(Cyber-Command)，說明網路司令部隸屬戰略司令部(Strategic Command)，任務主要負責保護軍事網路免於網路攻擊，以及發展進攻型式網路武器。網路司令部指揮官將增設為四星上將職缺，由當時國家安全局局長亞歷山大(Keith B. Alexander)中將兼任，而網路司令部也在2010年10月正式完全運作。[30] 網路司令部的成立，顯然代表某種程度的意義，就其主要任務面向是負責美國國防部資訊網路安全任務，更被賦予隨時準備進行廣泛軍事網路空間行動，以確保美國與盟友在網路空間的安全。若就戰略規劃角度而言，則顯示向各國展現出積極取得網路空間優勢地位。隨後美國國防部依據歐巴馬總統2010年的《國家安全戰略》(National Security Strategy)報告，制訂《維持美國全球領導地位：21世紀國防優先執行事項》

27 U.S. Department of Homeland Security, "Our Mission," *Department of Homeland Security*, <http://www.dhs.gov/our-mission>（檢索日期：2015年1月17日）

28 The White House, "The National Strategy to Secure Cyberspace," p. i.

29 James R. Langevin, Michael T. McCaul, Scott Charney, and Harry Raduege, "Securing Cyberspace for the 44 Presidency," p. 5.

30 Ellen Nakashima, "Gates Establishes Cyber-Defense Command," *The Washington Post,* June 24, 2009, <http://www.washingtonpost.com/wp-dyn/content/article/2009/06/23/AR2009062303492.html>（檢索日期：2015年1月12日）

(Sustaining U.S. Global Leadership: Priorities for 21st Century Defense)，更明確指出美國正打造一支未來量小質精、即時反應、技術先進，充分利用網路化優勢專業人員。[31] 美國前國防部部長赫格爾(Chuck Hagel)2014年3月29日公開宣布，將擴編網路安全人員至目前3倍以上，以建設更現代化的網路部隊，避免網路空間所造成嚴重危害，進而影響國家安全與經濟發展。[32]

從美國因應新威脅環境下調整其組織，旨在強調職能創新，透過國土安全部賦予確保國內重要基礎設施與網路安全運作外，也建立網路司令部，展現出領先全球優勢的網路科技。然而，在美國網路安全防護的經驗中，本文認為，「邁向組織創新」並非著重建立新的「組織」，而是在政策倡議過程中，同時打破傳統制式觀念。具體而言，組織創新可以在官僚體系下做最小變動，不必全然大肆破壞或變更原有組織，以跨越政府部門、公私部門之間的合作障礙。所以制度創新未必是機構人員精簡或增設之制式反應；相反地，透過人們對於觀念與安全認知的改變，也能成為制度創新的關鍵。

二、提升政府與民間合作

美國前總統小布希(George Bush)在2003年執政期間，即公布《確保安全網路空間的國家戰略》(The National Strategy to Secure Cyberspace)報告，除了針對美國如何在「網路空間」制定相關防護措施，避免關鍵基礎設施遭受破壞外，也指出網路空間行為者來源可能是恐怖分子、犯罪團體或是民族國家。[33] 由此可知，威脅來源對象非常廣泛，同時社會依賴網路的程度日益增加，政府必須主導公私部門之間進行合作，擴大政府與私人企業有效應對網路安全威脅。這項戰略報告為日後處理網路安全問題，奠定良好基礎。

然而，鑑於恐怖分子與網路空間結合等趨勢，除了上述國土安全部被賦予執行網路安全等工作外，也主導結合各民間企業、大學、州政府，來強化對於資訊交換與合作的管道。例如國土安全部下轄的國家網路安全與通訊整合中心(National Cybersecurity and Communications Integration Center, NCCIC)成立美國電腦緊急準備小組(United States Computer Emergency Readiness Team, US-CERT)，主要任務是主動管理網路相關威脅，以及協調網路資訊共享，目的是能夠在複雜環境中，迅速處理網路安全問題。其中重要的合作夥伴即是私人企業、學術界、聯邦機構以及國內外重要組織機構。[34] 甚至後來國土安全部每兩年舉行一次的網路風暴演習(Cyber Storm)，也是強調在政府與私人企業進行合作，提升對於網路安全威脅的因應能力。[35]

31 U.S. Department of Defense, "Sustaining U.S. Global Leadership: Priorities for 21st Century Defense," May 2010, p. 5, *Department of Defense*（檢索日期：2015年1月18日）

32〈赫格爾訪華前宣布擴編美國網路安全人員〉，《BBC中文網》，2014年3月29日（檢索日期：2015年1月18日）

33 The White House, "The National Strategy to Secure Cyberspace," p. i.

34 U.S. Department of Homeland Security, "About us-US-CERT," March 15, 2015, *Department of Homeland Security*,（檢索日期：2015年1月19日）

35 U.S. Department of Homeland Security, "Cyber Storm: Securing Cyber Space," *Department of Homeland Security*（檢索日期：2015年1月19日）

這樣的經驗還可以從2010年出版的《國家安全戰略》報告發現，內容多次強調為了達到目標，必須透過合作手段，特別是必須仰賴「在人力與技術層面的投資」、「強化夥伴關係」等層面。[36] 然而前者強調的「人力與技術層面投資」，已經落實在政府單位與民間企業機構合作模式當中，並且建立有效的網路安全技術，以及保護政府與民間關鍵基礎設施網路系統，使得對於網路安全問題處理、應變作為更具有彈性。例如，美國最大的無線運營商維瑞松(Verizon)與電信營運商AT&T，在政府部門指導下，向用戶提供網路安全工具、提供網頁安全管控服務等等。不僅能擴大政府技術層面運用，也給寬頻用戶帶來更為安全的網路空間。[37] 另一方面，有關「強化夥伴關係」層次，係指強化與擴大和國際夥伴之間交流，降低雙方資訊不對稱，建立網路空間規範、擴大犯罪情報的分享，防範可能造成的危害。[38] 最顯而易見的成功例子，美國於2010年10月28日，破獲一起發生恐怖分子欲從國外透過「優比速」(UPS)與「聯邦快遞」(FedEX)飛往美國的貨機，利用遙控裝置引爆炸彈，卻遭執法單位掌握線索，最後遭到攔截。進一步了解發現，這兩個炸彈包裹具有強烈殺傷力，而目的地均是寄往芝加哥的猶太教堂。所幸一個包裹在杜拜機場查驗過程，被查緝人員發現該包裹裝有火藥之碳粉匣與定時器，另一個包裹則是在英國東密德蘭(East Midlands)機場被查獲該包裹之碳粉匣裝著炸藥。而這類的包裹炸彈攻擊模式，就是運用網路電話(VoIP)或機上無線網路(Wi-Fi)進行遠端遙控，成為許多恐怖分子新型的攻擊模式。[39] 假使郵包沒有被查獲，並進一步通報美國，包裹最後可能在進入美國東岸上空時爆炸，或者在美國境內引發炸彈攻擊事件。因此，有關執法人員與政府部門之間能夠強化資訊分享機制，也有助於提升應變能力與處理之反應時間，減少網路安全威脅或其他威脅情事發生。

三、強化情報與反情報能力

歐巴馬總統自上任以來，接續前任總統小布希基礎上，投入更多資源提升處理網路安全威脅的能力，成為最關切的議題之一。許多重要的戰略報告指出，如前述跨政府、跨部會、以及私人機構之間合作，提升資訊分享能力等重要性之外，值得注意的是，網路安全威脅的來源，是具有高度不確定性與辨別的困難性。在美國官方公布的戰略報告當中，也指出情報單位與反情報單位必須在威脅環境扮演重要的角色。如同2010年出版的《國家安全戰略》報告中，有關情報工作部分，即強調國家之所以能夠安全與繁榮的發展，在憑藉蒐集情報的質量與分析的準確度，政府必須加強投資情報工作。[40]

該年度所公布的另一份報告《綜合性

36 The White House,“National Security Strategy 2010,”p. 18.

37〈網路安全吸引全球目光〉，《人民日報》，2009年10月30日（檢索日期：2015年1月19日）

38 The White House,“National Security Strategy 2010,”pp. 27-28.

39 蔡裕明，〈蓋達組織空中郵包炸彈恐怖攻擊事件評析〉，《地緣政治》，2011年1月，<http://www.geopolitician.org/index.php?option=com_content&view=article&id=21:2011-01-28-07-37-11&catid=28:2011-01-28-03-29-40&Itemid=27>（檢索日期：2015年1月19日）

40 The White House,“National Security Strategy 2010,”pp. 15-16.

國家網路安全倡議》(The Comprehensive National Cybersecurity Initiative, CNCI)，也強調美國必須強化情報與反情報能力，以增加與重要資訊科技之間的應用，同時制定聯邦法律作為執行依據，來確保國家網路空間安全。[41] 然而，這種積極作法，其實早在2007年已被落實。美國情報首長辦公室在2007年公布《國家反情報戰略》(National Counterintelligence Strategy of the United States of America)，已經將網路安全議題納入重要威脅來源，情報體系將透過所有可能運用的情報技術來進行蒐集、調查與分析，有效打擊網路空間的入侵者。[42] 顯見，美國非常重視如何防範於未然，特別是各種威脅來源越來越廣泛，應對有關網路安全威脅時，處理問題之前即具備專業性與獨特性。情報體系更必須在龐大的組織體系中，發揮其專業能力，同時提升傳遞訊息的效率，才能將危害降到最低，進一步確保國家安全。

伍、對我國網路安全的啓示

透過美國官方戰略報告及實踐過程，可以清楚發現網路安全威脅可能涉及個人、社會、經濟、軍事等層面，影響程度將嚴重危害國家安全。然而，美國在政府、民間與私人部門共同關切網路安全問題，不僅有助於了解網路安全潛藏何種危機，更有助於政策與實際行動能夠結合知識概念，整合最完善治理模式。因此，建立完善之前瞻性戰略與建構安全工作的新穎情境可提供為我國安全工作的啟示。

一、建立完善之戰略規劃

美國目前除了面臨傳統的安全威脅問題，必須關切跨境犯罪、緊急事態處理、環境生態，以及網路安全等非傳統安全威脅。同時美國更了解其所面臨威脅是可能超越傳統地域疆界，或者指涉外交政策、軍事發展、經濟、社會穩定等議題。因此，發展適切的戰略規劃是必須的。基本上，戰略是一種決策的整體過程作為，也是一種國家體制與環境之間的關係，戰略制定的標準基於國家利益。進一步而言，戰略即是清楚了解國家要完成何種目的？運用何種工具追求此目標？運用何種方式達成此目的？[43] 就過往經驗來說，政府行政運作經常受限於官僚體系之龐大，產生職能重疊與資訊透明度不足之情況，使得決策者無法快速做出最完善的判斷。但是美國透過私人機構不斷提供政策倡議，作為政府部門形成政策規劃之參考方向，這過程是經過許多單位研究與評估之後，最終得以形成戰略。美國政府持續透過戰略報告，隨時修正應對網路安全威脅的作為，更在過程當中展現「邁向組織創新」、「提升政府與民間合作」，以及「強化情報與反情報工作能力」等行動能力，進而形成知識性的制度框架，提供決策者即時性的洞察

41 The White House,“The Comprehensive National Cybersecurity Initiative,” March 2010, p. 6, *The White House*（檢索日期：2015年1月20日）

42 U.S. Office of The Director of National Intelligence,“National Counterintelligence Strategy of the United States of America,” 2007, p. 1, *Office of The Director of National Intelligence*（檢索日期：2015年1月10日）

43 翁明賢，〈國家安全戰略研究典範之轉移—建構淡江戰略學派之芻議〉，《臺灣國際研究季刊》，第6卷第3期，2010年秋季號，頁9-10，《臺灣國際研究學會》，<http://www.tisanet.org/quarterly/6-3-3.pdf>（檢索日期：2015年2月10日）

能力，確保達成國家安全的目的。

對於我國來說，103年12月29日已成立「行政院資通安全辦公室」，統籌規劃國家資通安全政策、通報應變、重大計畫推動與管考及辦理相關會議。[44] 行政院安排簡任第十二職等至第十三職等或相當層級具行政經歷人員兼任指揮之責，兩位副主任則由科技部與法務部派員兼任，而辦公室所需人員也由行政院指派；另一方面，也成立「國家資通安全會報」，該項會報主要負責國家資通訊安全政策、通報應變機制、重大計畫之諮詢審議及跨部會資通訊安全事務之協調及督導。上述「行政院資通安全辦公室」、「國家資通安全會報」均是特別設置單位，由行政院派員指揮，並統籌各部會（機關）執行。值得注意的是，美國認識到網路安全將影響國家的政治、軍事、經濟、社會與個人等面向，早在2003年將網路安全工作列為國家戰略目標之一。相較我國是否能有更為主動、明確的戰略規劃，顯然在未來仍有發揮空間；另一方面，我國在網路安全的執行成效，大多是在「資通安全會報」召開期間，才透由媒體公開，在平時似乎很少獲得關切，不免讓社會大眾質疑政府執行網路安全工作是否過於被動；最後，美國國防體系在網路安全威脅當中，扮演著非常重要角色。如網路司令部之成立，不僅負責防護軍事網路免於遭受有心人士滲透、竊密，以及破壞，更是被賦予發展進攻型式之網路武器，作為其進行嚇阻戰略的強而有力之後盾。對照我國國防而言，我國軍事戰略構想是「防衛固守、有效嚇阻」，網路攻擊也應視為國家重大挑戰之一。實質上軍隊運作必須謹守「網路資安防護」之思維。此項戰略思維仍過於保守，面對中共每年持續增加的軍事投資，何以有效嚇阻，自然使吾人無法樂觀看待。是否能夠運用網路空間之隱匿、快速之特性，發展網路進攻能力，可以真正提升「有效嚇阻」。我國若能夠逐步前瞻未來網路安全或其他重大威脅問題時，重新釐清我國的安全戰略思考與途徑，將有助於了解危機本質，進而轉化成實際行動，才能整合出最完善的治理模式。

二、建構安全工作的新環境

美國在911事件後進行之反恐戰爭，係一種反伊斯蘭教的作法，使得美國與廣泛的伊斯蘭社群更加疏離，造成美國經常面臨極端分子對其進行恐怖攻擊事件。因此，歐巴馬總統上任後，逐步調整政策方向，進而將其立國價值、利益，推廣至伊斯蘭世界，例如：宣布結束伊拉克軍事戰鬥任務，進行撤軍行動，並轉向對伊拉克提供後勤與訓練工作等綜合治理任務，其目的即在透過改變認知，重新建構兩種不同文明之間信任感。同時，在美國官方報告中，也經常發現「跨越政府部門與私人機構侷限」、「建構職能空間」(building capacity)，然而落實在跨部門合作當中，即所謂提高雙方的資訊透明度(transparency)，以及進行訊息分享(information sharing)，使得相關安全單位能夠快速了解威脅全貌，並且迅速發展出應對作為。換言之，安全單位若能夠在公部門或私部門之間，加強資訊分享與提高資訊透明度，進而建立跨界菁英與研究社群之間的

44 行政院國家資通安全會報，〈行政院資通安全辦公室設置要點〉，2014年12月29日（檢索日期：2015年4月13日）

良好關係，將有助於打破彼此認知行為差異與制度上之複雜性，這種新穎環境提供僵化的安全單位組織運作模式一種新的思維，一方面也更實質地擴大安全單位整合與協調能力。

陸、結　　論

網路空間與現代社會發展息息相關，美國的經濟、民生、公共安全及國家安全的基礎。然而，網路安全威脅也造成國家安全與發展的重大挑戰。美國在911事件後，不僅內部組織面對外在環境迅速且大幅的變化，傳統的政府治理必須在行政組織、立法原則與社會生活型態面向上尋求創新，甚至在外部威脅上，面臨中共等國家，每年投入在網路空間資源都逐年攀升，甚至是非國家行為者，也利用網路對美國進行入侵、竊密等行為。因此，美國為確保網路空間的安全，不論從小布希政府時期提出的《確保安全網路空間的國家戰略》，或是現在歐巴馬政府陸續發表《國家安全戰略》、《綜合性國家網路安全倡議》等，這些政策倡議以及執行過程中不難發現，美國處理有關網路安全威脅等議題時，不僅僅是外部敵人所發起的網路襲擊，也透露包括內部機制不完善、運作模式僵化等原因。然而，綜觀美國近年來重新整合安全體系、重視跨政府、跨部門、公私部門合作關係，強化溝通之方式，以及重視情報與反情報工作，確實建立起有效防護措施；另一方面，美國應對網路安全威脅過程中，係由政府部門政策規劃、進行資源整合等工作，才能有效推展網路安全防護工作，更能符合國家安全以及經濟繁榮的原則。

的確我國當然可能遭受不同型態的敵人，運用網路持續的刺探、蒐集，破壞關鍵的基礎設施，甚至複合成跨境犯罪。這些潛在威脅都顯示出我國無法對於網路安全議題置身事外。值得注意的是，美國在面對網路空間策略的弱點，雖然存在職能重疊、制度僵化等組織窒礙問題，卻又能藉各項政策倡議，持續朝向正確的方向前進。顯然政府部門必須擔負起領頭羊的角色，首先將網路安全議題正式制定為國家層級戰略目標，其次，加強各個相關部門、機構、私人企業之間的合作，跨越不同單位之間本位主義，建立共同認知與信念。

總體來說，美國在面臨網路安全威脅過程，展現出富有彈性與應對能力，並就美國目前在國際社會的影響力而言，仍然是超級強權。但是歐巴馬總統卻積極運用「強化溝通」、「增進合作」等概念，來處理安全等議題。相較與我國目前應對網路安全議題等安全威脅，以及我國在現實條件下，面臨資源不足等問題，或許無法完全複製美國執行網路安全的經驗，然而如探究美國在應對網路安全威脅過程，仍然是具有知識意涵與政策應用的價值。

（收件：104年1月23日，接受：104年4月14日）

參考文獻

中文部分

專書

黃秋龍，2009。《非傳統安全論與政策應用》。臺北：結構群文化。

Langevin, James R., McCaul, Michael T., Charney, Scott and Raduege, Harry, 2008. *Securing Cyberspace for the 44th Presidency.* Washington, D.C.: CSIS.

官方文件

United States, 2013/3/12. "Worldwide Threat Assessment of the U.S. Intelligence Community," *Office of The Director of National Intelligence*, p. 1.

United States, 2010/5. "National Security Strategy 2010," *The White House*, p. 18.

United States, 2003/2. "The National Strategy to Secure Cyberspace," *The White House*, p. vii.

United States, 2010/3. "The Comprehensive National Cybersecurity Initiative," *The White House*, p. 6.

United States, 2011/6. "Department of Defense Strategy for Operating in Cyberspace," Department of Defense, p. 1.

United States, 2005/3. "The National Defense Strategy of The United States of America," *Department of Defense*, p. 13.

United States, 2010/5. "Sustaining U.S. Global Leadership: Priorities for 21st Century Defense," *Department of Defense*, p. 5.

United States, 2010/8/16. "Annual Report on Military and Security Developments Involving the People's Republic of China," *Department of Defense*, p. 7.

United States, "Our Mission," *Department of Defense*.

United States, 2010/2. "A Strategy Framework for a Secure Homeland," *Department of Homeland Security*, p. 7.

United States, "About us-US-CERT," *Department of Homeland Security*.

United States, "Cyber Storm: Securing Cyber Space," *Department of Homeland Security*.

United States, 2014/11/23. "The 2014 Quadrennial Homeland Security Review," *Department of Homeland Security*, p. 7.

United States, 2007. "National Counterintelligence Strategy of the United States of America," *Office of The Director of National Intelligence*, p. 1.

United States, 2009/11. "U.S.-China Economic and Security Review Commission 2009," U.S.-*China Economic and Security Review Commission*, p. 8.

報紙

2009/10/30。〈網路安全吸引全球目光〉，《人民日報》，<http://big5.lanecat.cn/news/20091030.asp>。

2014/3/29。〈哈格爾訪華前宣布擴編美國網路安全人員〉，《BBC中文網》，<http://www.bbc.co.uk/zhongwen/trad/world/2014/03/140329_us_cyber_defence.

shtml?>

2014/6/10。〈美報告再指責中國大陸軍方網路間諜活動〉，《BBC中文網》，<http://www.bbc.co.uk/zhongwen/trad/world/2014/06/140610_usa_china_cybersecurity>。

2014/7/12。〈美司法部指控中國商人竊取美國防技術〉，《BBC中文網》，<http://www.bbc.co.uk/zhongwen/trad/world/2014/07/140712_us_chinese_hacking_defense>。

何清漣，2013/6/17。〈點評中國大陸：史諾登事件的多重效應〉，《BBC中文網》，<http://www.bbc.co.uk/zhongwen/trad/focus_on_china/2013/06/130617_cr_snowden>。

狄雨霏，2013/6/26。〈中國軍事專家痛批稜鏡門，指美國為駭客帝國〉，《紐約時報中文網》，<http://cn.nytimes.com/world/20130626/c27hack/zh-hant/>。

連雋偉，2014/5/20。〈陸駭客竊密　美國年損逾9兆〉，《中時電子報》，<http://www.mingpaocanada.com/Tor/htm/News/20140520/taa4.htm?m=0>。

網際網路

Lewis, James A., 2010/5.“Cyber War and Competition in the China-U.S. Relationship,”*CSIS*, p. 1, <http://csis.org/files/publication/100510_CICIR%20Speech.pdf>.

Merritt, Marian, 2010.“Cyber Crime Exposed 2010,”*Symantec*, p. 15, <http://www.symantec.com/content/en/us/home_homeoffice/media/pdf/norton_cybercrime_exposed_booklet.pdf>.

Bucci, Steven P., 2009/10.“A Most Dangerous Link,”*U.S. Naval Institute*, <http://www.usni.org/magazines/proceedings/2009-10/most-dangerous-link>.

Shipley, Todd G., 2010.“2010 Report on Cyber Crime Investigation,”*High Technology Crime Investigation Association*, p. 4, <http://www.htcia.org/pdfs/2010survey_report.pdf>.

Tiezzi, Shannon, 2014/5/20.“U.S. Indicts 5 PLA Officers For Hacking, Economic Espionage,”*The Diplomat*, <http://thediplomat.com/2014/05/us-indicts-5-pla-officers-for-hacking-economic-espionage/>.

Nakashima, Ellen, 2009/6/24.“Gates Establishes Cyber-Defense Command,”*The Washington Post*, <http://www.washingtonpost.com/wp-dyn/content/article/2009/06/23/AR2009062303492.html>.

翁明賢，2010／秋季號。〈國家安全戰略研究典範之轉移—建構淡江戰略學派之芻議〉，《臺灣國際研究季刊》，第6卷第3期，頁9-10，《臺灣國際研究學會》，<http://www.tisanet.org/quarterly/6-3-3.pdf>。

蔡裕明，2011/1。〈蓋達組織空中郵包炸彈恐怖攻擊事件評析〉，《地緣政治》，<http://www.geopolitician.org/index.php?option=com_content&view=article&id=21:2011-01-28-07-37-11&catid=28:2011-01-28-03-29-40&Itemid=27>。