美國關鍵基礎設施防護的發展與實踐

作者／王政

提要

關鍵基礎設施是現代社會經濟發展與人民生活不可或缺之物，它是由一組實體的資產或虛擬的資訊系統所組成，例如交通運輸、資訊與通信、金融交易、水電供應等。隨著社會的發展越趨向現代化，基礎設施也越來越複雜，彼此相依的程度亦隨之增加，加以關鍵基礎設施往往暴露在公開的環境下，防護難度增加，一旦受創後不僅直接衝擊國家經濟活動，亦將引起民眾恐慌，甚至損害政府形象及領導威信，因此極易成為恐怖份子攻擊的目標。

自911事件以後，各國均已體會基礎設施的脆弱性及其戰略價值，因此，包括美國在內的主要先進國家已針對關鍵基礎設施擬定安全防護計畫，並逐步推動防護政策，然而，綜觀各國之實踐經驗，無論在策略規劃、法令訂頒、組織重整、公私整合方面，仍以美國最為完備，也最具參考價值。

本論文將介紹美國關鍵基礎設施防護的發展歷程、相關政策作為，困難與挑戰、以及學術界的回應與成果，期望美國的實踐經驗，能成為我國推動關鍵基礎設施防護的參考與啟示。

關鍵字：關鍵基礎設施防護、國土安全、非傳統安全、非對稱性衝突、國家基礎設施防護計畫

壹、關鍵基礎設施的戰略價值

冷戰時期，由美蘇兩強所主導的國際政治環境，其安全威脅主要來自於軍事力量和核子武器，冷戰結束後，一些跨國性威脅開始浮現，攻擊手段和目標均非傳統方法所能應付，另一方面，非國家行為者(non-state actors)如恐怖主義組織與份子亦趁機活動，因此，各國所處的是一個更為動態的戰略環境，所遭遇的是更多更廣泛的議題，所面臨的是更小、更機靈的敵人。[1]

此外，由於全球化、資訊化、通訊技術進步、交通便捷、氣候變遷等因素，導致國家安全的概念與範疇產生重大轉變，安全研究的焦點亦從傳統的軍事安全擴及到能源、水資源、糧食安全、公共衛生、跨國組織犯罪、非法移民、資訊網路安全、天然災害威脅等非傳統安全議題。[2]

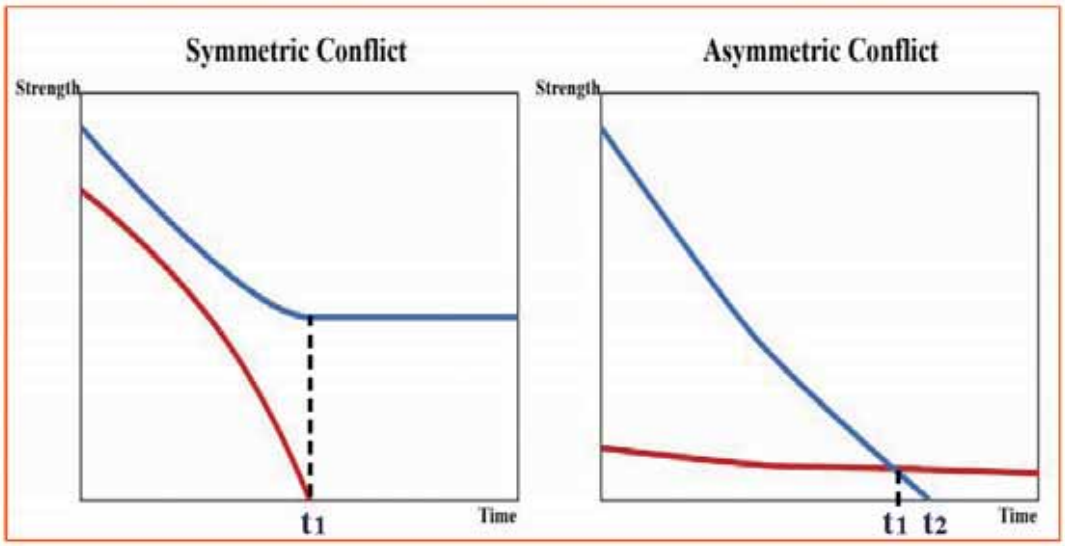
在上述非傳統安全議題中，「關鍵基礎設施」(critical infrastructure)屬於新興的研究主題，但卻已成為美國及其他工業化國家積極推動之政策，因為現代化社會的經濟活動與日常生活不可缺少交通運輸、通信與資訊傳遞、金融交易、水電供應等功能，這些功能是由一組實體資產(physical assets)或虛擬的資訊系統所提供，稱之為關鍵基礎設施。隨著社會的發展越趨向現代化，基礎設施也越來越複雜，彼此的相依性(interdependency)亦隨之增加，一旦某個關鍵基礎設施受到破壞，或運作發生故障，便可能影響到其他部門(sector)的關鍵基礎設施，造成財產或生命的損失，嚴重者甚至危及國家安全。

尤為重要者，關鍵基礎設施對恐怖主義組織或份子而言，具有非對稱性衝突(asymmetric conflict)之戰略價值，以圖一為例，在非對稱性衝突的情況下，如果紅方採取非正規作戰(unconventional warfare)策略，最後反而能夠擊敗實力較強的藍方。在911事件中，全球目睹美國紐約世貿雙子星大樓遭到恐怖份子攻擊，才體會到重要基礎設施的脆弱性及其戰略價值。由於關鍵基礎設施往往暴露在公開的環境之下，很難加以防護，一旦受創後不僅直接影響國家經濟、造成民眾心理恐慌，甚至損害政府形象及領導威信，因此，包括美國在內的主要先進國家已針對關鍵基礎設施擬定安全防護計畫，並逐步推動防護政策。然而，綜觀各國之實踐經驗，無論在策略規劃、法令訂頒、組織重整、公私整合方面，仍以美國最為完備，也最具參考價值。

為瞭解美國關鍵基礎設施防護的發展與實踐，本文首先探討美國基礎設施的發展歷程，再說明關鍵基礎設施的政策演變、定義

1 Jeffrey R. Cooper, *Curing Analytic Pathologies: Pathways to Improved Intelligence* (Washington, DC: Center for the Study of Intelligence, 2005), p.24.

2 Allan Collins (ed.), *Contemporary Security Studies* (New York: Oxford University Press, 2010).



圖一　對稱性衝突與非對稱衝突

資料來源：Ted G. Lewis, Critical Infrastructure Protection in Homeland Security (Hoboken, NJ: John Wiley & Sons, Inc., 2006), p. 63.

與類別，進而闡述相關防護作為，分析政策推動的困難與挑戰，最後並介紹學術界對於此一新安全議題的回應，期望美國的實踐經驗，能成為我國推動關鍵基礎設施防護的參考與啟示。

貳、關鍵基礎設施的定義與類別

從歷史的經驗來看，關鍵基礎設施並非是一個全新的概念，過去人類不僅竭力保護攸關國家存續的基礎設施，也在戰爭時摧毀敵人的基礎設施，以瓦解對方之戰鬥力量。例如，古希臘時期，斯巴達統帥Lysander曾經率領艦隊封鎖了赫勒斯滂(Hellespont)，[3] 導致雅典糧食供應中斷，使得斯巴達在伊哥斯波塔米戰役(Battle of Aegospotami)中擊敗雅典艦隊，結束了伯羅奔尼撒戰爭(Peloponnesian War)。此外，二次世界大戰期間，盟軍聯合參謀本部(Combined Chiefs of Staff)也曾於1943年發佈「卡薩布蘭卡指令」(Casablanca directive)，授權英國皇家空軍和美國空軍對德國的潛艇造船廠、飛機製造廠、運輸、煉油廠等設施進行戰略轟炸(strategic bombing)，不僅摧毀了德國的軍事工業和經濟，也瓦解了德國的民心士氣。[4]

3　赫勒斯滂(Hellespont)即為如今的達達尼爾海峽(Dardanelles Strait)，是土耳其西北方一條狹長的海峽，其長度為61公里，但寬度僅有1至6公里，連接馬爾馬拉海(Sea of Marmara)和愛琴海(Aegean Sea)，屬土耳其內海，是亞洲和歐洲的分界線之一，也是連接黑海及地中海的唯一航道。

4　Kathi Ann Brown, *Critical Path: A Brief History of Critical Infrastructure Protection in the United States* (Fairfax, VA: Spectrum Publishing Group, Inc., 2006), pp. xiv-xv.

然而，相對於其他國家安全的議題而言，「關鍵基礎設施」此一名詞仍屬於較新的概念，其定義與範圍也在建構與演變中。1983年，美國國會預算辦公室(CBO)提出一份報告，將基礎設施定義為「具備資本密集、由各級政府大量投資的特性，對於國家經濟活動具有直接的關鍵性」，當時CBO將基礎設施範圍涵蓋高速公路、大眾運輸、廢水處理、水資源、航空管制、機場、都市自來水供應等七項，但亦指出基礎設施應該廣義地包含學校、醫院、監獄等設施。[5]

1986年的第13010號行政命令(Executive Order 13010)，是美國首度對「關鍵基礎設施」做出定義的官方文件，EO 13010提出極重要(vital)與關鍵(critical)的概念，指出「某些極重要的國家基礎設施，當其失去功能或遭受破壞時，對國防及國家安全會產生將削弱性的衝擊」。EO 13010同時列舉出8項關鍵基礎設施，包括：通信、電力系統、天然氣及石油的貯存及運輸、銀行與金融業、交通運輸、自來水供應、緊急服務(包含醫院、警察、消防、救援)、政府持續運作。

2001年10月26日國會通過的「美國愛國者法案」(The USA PATRIOT Act of 2001)，將關鍵基礎設施定義為「系統或資產，無論是實體的或虛擬的，對美國都極為重要，當這些系統或資產失去功能或遭受破壞時，對安全、國家經濟安全、國家衛生會產生將削弱性的衝擊」。

2003年2月，布希政府發佈了「國家關鍵基礎設施及重要資產防護策略」(National Strategy for the Physical Protection of Critical Infrastructures and Key Assets)，該報告列舉出11個關鍵基礎設施部門(包括農業與食品、水、公共衛生、緊急服務、國防工業、通信、能源、交通、銀行與金融、化學與毒性物質、郵政與貨運)，及5項重要資產(key assets)，包括國家紀念碑及象徵、核能電廠、水壩、政府設施、重要商業資產。[6]

2006年國土安全部首度公布了「國家基礎設施防護計畫」(National Infrastructure Protection Plan, NIPP)，2009年加以修正，其中指定的關鍵基礎設施共有18個部門，分別是：(1)農業與食品、(2)銀行與金融、(3)化學、(4)商業設施、(5)通信、(6)關鍵製造業、(7)水壩、(8)國防工業、(9)緊急服務、(10)能源、(11)政府設施、(12)健康照護與公共衛生、(13)資訊科技、(14)國家紀念碑及象徵物、(15)核子反應爐、原料、廢料、(16)郵政與貨運、(17)交通運輸、(18)水。[7]

5 John Moteff and Paul Parfomak, *Critical Infrastructure and Key Assets: Definition and Identification* (Washington, DC: Congressional Research Service, RL 32631, October 1, 2004), p. 2.

6 White House, *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, February 2003.

7 Department of Homeland Security, *National Infrastructure Protection Plan*, 2009.

參、911事件前關鍵基礎設施防護的政策演進

美國基礎設施的發展，大約可分為幾個階段，第一次世界大戰以前，基礎設施建設基本上是一種毫無計畫、湊合的政策，完全視地方上的需要而修修補補，當時道路修築被列為最優先順序，目的在確保郵件遞送順暢。1803年起，政府開始興建公路，嗣後因工業革命帶來經濟發展的需要，乃開鑿運河、建造水庫、鋪設鐵路，至於電線和電話線則主要是由民間所架設。[8]

一次大戰結束後，羅斯福總統於1933年推出「新政」(New Deal)，大量興建公共基礎設施，至歐洲爆發戰爭及珍珠港事變後，政府更大幅增加軍事基礎設施的預算，進行高速公路、機場、橋樑、鐵路、港口、海軍造船廠等建設，整個中央政府彷彿成為一個基礎設施製造機器(infrastructure-building machine)。[9]

在1962年古巴飛彈危機期間，美國曾經體認到基礎設施的重要性，當時由於通信技術不足，甘迺迪總統和蘇聯共黨總書記赫魯雪夫只能透過信函進行談判，並經由華盛頓和莫斯科的大使館傳遞訊息，致使緊張關係逐漸升高。當危機結束後，甘迺迪下令由國家安全會議組成一個跨部會的委員會，該委員會建議設立一個統一的通信系統，做為總統、國防部、外交及情治單位、甚至民間領袖在緊急狀況時溝通的工具，1963年甘迺迪簽署了總統備忘錄(Presidential Memorandum)，成立了「國家通信系統」(National Communication System, NCS)。[10]然而，美國真正對基礎設施進行檢討，則是從1980年代開始。

1980年代初期，美國政府開始檢討基礎設施問題，1983年國會預算辦公室(Congressional Budget Office)曾經針對7項基礎設施(高速公路、大眾運輸、廢水處理、水資源、航空管制、機場、都市自來水供應)的狀況進行調查，當時檢討的重點在於公共基礎設施的足夠性及老舊問題。該報告指出，美國的公共設施嚴重不足，無法滿足因人口遷移及經濟發展所帶來的需求，許多設施也因為老化和忽略，呈現退化或廢棄的情況。[11]

1990年代期間，國會對於基礎設施的政策焦點主要是集中在解除管制、強化競爭、增進效率為主。當時受到新公共管理(New Public Management)及民營化(privatization)

8 Kathi Ann Brown, pp. 3-6.

9 Kathi Ann Brown, pp. 15-17。例如，1934年公共工程管理局(Public Works Administration)撥給陸軍部(War Department)的經費是100萬美元，1935年為1億美元，1940年增加到4億3200萬美元。

10 Ted G. Lewis, *Critical Infrastructure Protection in Homeland Security* (Hoboken, NJ: John Wiley & Sons, Inc., 2006), pp. 30-31.

11 Congressional Budget Office, *Public Works Infrastructure: Policy Considerations for the 1980s*, April 1983, pp. 6-7.

思潮的影響，政府政策及國會立法主要重點在回應個別產業的需求，解除價格及進入產業的管制，允許基礎設施透過公開競爭機制增加效率並減少服務成本。[12]

相對於國會對於基礎設施的關切重點在於足夠性及市場競爭性，行政部門在1970年代便已開始對於基礎設施的安全問題提出檢討，例如，國防部在1970年的一份報告指出，全國的油管系統(pipeline systems)有126處弱點可能遭受攻擊，導致整個石油供應中斷。此外，根據能源部在1981年的報告發現，全國的電力系統在面對惡意攻擊時暴露出很大的弱點。還有，華府著名的智庫「戰略與國際研究中心」(Center for Strategic and International Studies, CSIS)也在1984年發表「美國隱藏的弱點：網絡社會的危機管理」(America's Hidden Vulnerabilities: Crisis Management in a Society of Networks)報告，呼籲美國重視發電廠、電腦、電話通訊、交通網路的安全性。[13]

1996年7月，柯林頓總統簽署了第13010號行政命令(Executive Order 13010)，設立了「總統關鍵基礎設施防護委員會」(President's Commission on Critical Infrastructure Protection, PCCIP)，並任命Robert T. Marsh將軍擔任主席，該委員會的任務是向總統報告國家關鍵基礎設施的脆弱性和面臨的威脅(以網路威脅為重點)，並提出一套整體的防護政策。1997年10月，委員會向總統提出報告(以下簡稱Marsh Report)，報告指出，由於網路使用人口急遽增加，駭客的技術容易取得，威脅與脆弱性確實存在，故建議政府與民間加強資通安全防護之合作。[14] 為回應Marsh Report，柯林頓總統於1998年5月22日簽署了第63號總統決策令(Presidential Decision Directive 63, PDD-63)，展開一連串關鍵基礎設施的防護措施。

布希總統上任之初，仍然延續柯林頓的關鍵基礎設施防護政策，當時曾有設立一位統籌全國關鍵基礎設施防護的資訊首長(Chief Information Officer)之建議，但未獲布希支持。此外，有關對抗恐怖主義之策略，各界看法亦相當分歧，例如，「21世紀國家安全委員會」(The US Commission on National Security/21st Century，又稱為Hart-Rudman Commission)曾經倡議設立「國家國土安全局」(National Homeland Security

12 Philip Auerswald, Lewis M. Branscomb, Todd M. La Porte, and Erwann O. Michel-Kerjan, "Where private efficiency meets public vulnerability," in in Philip E. Auerswald et al. (eds.), *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability* (New York: Cambridge University Press, 2006), pp.11-12.

13 Kathi Ann Brown, pp.52-53.

14 John D. Moteff, *Critical Infrastructures: Background, Policy, and Implementation* (Washington, DC: Congressional Research Service, RL 30153, July 11, 2011), p.3.

Agency)，以聯邦緊急事務管理總署(FEMA)為主，整合海岸防衛隊(Coast Guard)、邊境巡邏隊(Border Patrol)、海關(Customs Service)及其他單位，並成立關鍵基礎設施防護局，但布希反應並不熱烈。[15] 直到911事件發生以後，美國才針對國土安全防衛體制進行大幅改革，並且強化關鍵基礎設施安全防護工作。

肆、911事件後關鍵基礎設施防護的政策作為

911事件發生後，布希總統在2011年10月8日簽署了第13228號行政命令(Executive Order 13228)，設立了國土安全辦公室(Office of Homeland Security)與國土安全會議(Homeland Security Council)，並於2001年10月16日簽署第13231號行政命令(Executive Order 13231)，設立了「總統關鍵基礎設施防護委員會」(President's Critical Infrastructure Protection Board)，賦予「針對資訊安全及關鍵基礎設施防護進行政策建議及計畫協調」之權。EO 13231也設立了「國家關鍵基礎設施諮詢會議」(National Infrastructure Advisory Council)，其功能包括：提升公私協力(public-private partnerships)、監督「資訊分享與分析中心」(ISACs)的發展狀況、鼓勵民間部門定期針對資訊及通信系統進行脆弱度評估等。[16]

目前美國關鍵基礎設施防護的負責單位為國土安全部(Department of Homeland Security, DHS)，並由該部之「全國保護暨計畫處基礎建設保護局」(Office of Infrastructure Protection, National Protection and Programs Directorate)負責政策推動工作。[17] 此外尚有提供總統建議之國土安全諮詢會議(Homeland Security Advisory Council, HSAC)、國家基礎建設諮詢理事會(National Infrastructure Advisory Council, NIAC)、關鍵基礎設施伙伴諮詢理事會(Critical Infrastructure Partnership Advisory Council, CIPAC)、各級政府協調理事會及跨部會安全委員會等組織，均係協助推動與落實關鍵基礎設施防護之重要機制。

有鑑於資訊安全之重要性，國土安全部成立之初，即將「國家基礎設施防護中心」(National Infrastructure Protection Center, NIPC)、「國家模擬分析中心」(National Simulation and Analysis Center, NISAC)、「國家通信系統」(National Communication System, NCS)等機關整合為「資訊分析暨基礎建設防護處」(Directorate of Information Analysis and Infrastructure Protection, IA/IP)，並賦予下列任務：

(一)經由多元管道取得資訊，並加以分

15 Ibid., p. 8.
16 Ibid., pp. 8-10.
17 國土安全部網頁，http://www.dhs.gov/xabout/structure/gc_1185203138955.shtm

析、整合，以判定及評估恐怖威脅的本質和範圍。

(二)對美國重要資源與關鍵基礎設施實施整體的脆弱度及風險評估。

(三)整合相關資訊及脆弱度評估，以便訂定防護優先順序。

(四)發展出一套全國性、整體的重要資源與關鍵基礎設施防護計畫。

(五)管理「國土安全諮詢系統」(Homeland Security Advisory System)。[18]

(六)與情報圈合作建立情報蒐集優先順序。

(七)建構一套資訊接收與散播的安全的通信系統。[19]

2003年12月17日，布希總統發佈了「第7號國土安全總統指令」(Homeland Security Presidential Directive 7, HSPD-7)，明訂各部會對於關鍵基礎設施的資產辨識、排重要性序、安全防護等責任，並要求國土安全部、聯邦政府、民間部門共同合作致力於資訊分享與關鍵基礎設施防護。HSPD-7也設立了「關鍵基礎設施防護政策協調委員會」(Critical Infrastructure Protection Policy Coordinating Committee)，針對跨部會的關鍵基礎設施政策，向國土安全會議提出建議。此外，HSPD-7也指定國土安全部擔任化學與有毒物質部門的主管部會(原本屬於環境保護署業務)，HSPD-7並要求各主管部會每年向國土安全部部長提出報告。[20]

歐巴馬總統上任後，基本上依循布希總統的關鍵基礎設施防護政策和組織架構，2009年2月，歐巴馬發佈「第1號總統研究指令」(Presidential Study Directive 1)，檢討白宮內的國土安全及反恐組織，主要的爭論核心在於是否將「國土安全會議」與「國家安全會議」合併，2009年5月，歐巴馬下令兩個單位的人員合併，但仍然維持兩個單位的獨立性。2011年5月，歐巴馬政府提出一份關於強化網路安全的法案，主要目的在設立一個管制架構以提升關鍵基礎設施的網路安全，法案尚獲通過，被指定的關鍵基礎設施擁有者或操作者將被要求提出網路安全計畫，經由外部具公信力的機構評估後向「美國證券交易管理委員會」(Securities and Exchange Commission)報告，目前該法案仍在國會審查中。[21]

綜觀美國近十年以來的關鍵基礎設施防護之政策作為，可概略分為四項重點：(1)安全防護戰略之擬定，(2)資訊分享機制之推廣，(3)公私部門協力之建立，(4)公布

18 國土安全部門負責整合情報分析，評估恐怖攻擊對於各州、地方、民間之威脅情勢，並向外界發佈警訊，該系統指標係以紅、橙、黃、藍、綠五種顏色代表威脅重輕程度，且依顏色或威脅程度之不同而發佈相適應之應變措施。

19 John D. Moteff, *Critical Infrastructures: Background, Policy, and Implementation*, p.14。目前IA/IP的業務已經併入到全國保護暨計畫處(National Protection and Programs Directorate)。

20 Ibid., p. 11.

21 Ibid., pp. 12-13.

「國家基礎設施防護計畫」與「個別部門計畫」。

一、安全防護戰略之擬定

美國是提倡或推動關鍵基礎設施防護之首要國家，自1980年代以來，美國政府即透過國會立法、行政部門策略、總統行政命令或指令等作為，對關鍵基礎設施之概念與範圍加以界定、修正與發展。911事件以前，關鍵基礎設施防護的重點在資通訊安全，911事件以後，防護焦點轉為實體設施遭到恐怖份子之蓄意攻擊或破壞。2005年卡翠納颶風(Hurricane Katrina)造成嚴重災害以後，國土安全策略又改為以強調「全災害」(all-hazards)方法的防護政策。

911事件以後，美國曾陸續公布各類有關國土安全或關鍵基礎設施防護的戰略報告，包括2002年及2007年的國土安全國家戰略(National Strategy for Homeland Security)、2003年的國家關鍵基礎設施及重要資產防護策略(National Strategy for the Physical Protection of Critical Infrastructures and Key Assets)、2006及2010年的四年期國防總檢報告(Quadrennial Defense Review Report)。歷年來各種戰略報告或計畫對於關鍵基礎設施防護之宣示如附表一。

二、資訊分享機制之推廣

美國對於關鍵基礎設施的重視是從網路資訊基礎設施開始，1997年公布的第63號總統決策指令(PDD-63)是美國推動關鍵基礎設施防護的轉捩點，PDD-63的重點之一在於推動政府與民間之間資訊分享，並試圖克服若干問題，例如，民間企業與政府分享資訊的意願和能力為何？政府對於私人擁有的基礎設施的監控應該介入到什麼程度？政府與民間在進行資訊分享時會面臨哪些法律問題，如隱私權和義務？[22]

此外，PDD-63也提出由民間企業設置「資訊分享與分析中心」(Information Sharing and Analysis Centers, ISACs)的構想，目的在提供企業足夠資訊和分析能力，以減低風險並有效回應電腦、實體或自然災害。然而，911事件發生以前，只有少數幾個關於金融服務、資訊科技、通信、電力的ISACs獲得建置，911事件以後，陸續又建置了化學、食品、能源、大眾運輸、陸地運輸、水、房地產等ISACs。由於PDD-63並未明確規定ISACs的運作模式，以及其與聯邦政府的關係，因此，上述ISACs的品質、結構、經費來源、管理、運作等都不相同。但911事件以後，與關鍵基礎設施對應的政府部會都開始提供經費給ISACs，以提升其能力，擴大參與的成員，或辦理演習。[23]

22 Daniel B. Prieto, "Information sharing with the private sector," in Philip E. Auerswald et al. (eds.), *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability* (New York: Cambridge University Press, 2006), p. 406.

23 Ibid., pp. 406-407.

除了ISACs的建置以外，國土安全部關於資訊分享的措施還包括：

(一)設置「資訊分析與基礎設施防護處」(Information Analysis and Infrastructure Protection Directorate, IAIP)，負責整合與恐怖主義有關的資訊，以確保關鍵基礎設施的安全。

(二)根據2002年通過的「關鍵基礎設施資訊法」(Critical Infrastructure Information Act of 2002)，擬定「關鍵基礎設施防護資訊計畫」(Protected Critical Infrastructure Information Program, PCII)，並訂定關於私部門資訊傳輸、保密、儲存的統一程序，以鼓勵私人企業自願提供基礎設施的商業敏感資訊給國土安全部。

(三)建立「電腦緊急應變小組」(the US Computer Emergency Readiness Team, US-CERT)，定期發佈最新關於電腦相關威脅、脆弱度資訊，以及特定事件之因應。

(四)建置「國土安全資訊網絡」(Homeland Security Information Network, HSIN)，是一個包含全美50州的網路型態通訊工具，包含電子郵件和地理空間資訊等功能。

(五)成立一個24小時不間斷運作的「國土安全運作中心」(Homeland Security Operations Center, HSOC)，由超過35個政府情報單位及執法機關組成，並且挑選一些私部門關鍵基礎設施，包括貨運、鐵路、化學、石化工業、通信、核能等部門的代表參與。

(六)設立「國土安全部私部門辦公室」(DHS Private Sector Office)，與個別企業、專業協會、非政府組織等機構直接聯繫，以促進資訊分享。[24]

三、公私部門協力之建立

受到古典自由主義之影響，基本上美國政府在經濟活動所扮演的角色較輕，因此，美國超過85%的關鍵基礎設施都是由民間所擁有或操作，例如，幾乎所有的化學工廠、航空公司、大多數的發電廠和電力傳輸設備、許多港口和核能發電廠都是民間擁有，即便各級政府擁有機場、橋樑、水庫、隧道等交通設施，但飛機、貨車、火車、船隻還是由私人擁有及操作，這些交通工具很容易成為恐怖份子利用或攻擊的目標。因此，運用公私協力(public-private partnerships)模式是強化安全防護效能的重要政策工具。

PDD-63曾經建議每一個關鍵基礎設施部門的主管部會(Lead Agency)設置一個部門聯絡官(Sector Liaison Official)代表該部會，另外設置部門協調員(Sector Coordinator)代表各關鍵基礎設施的擁有者或操作者。

布希總統時期，國土安全部曾依據公私協力之概念，分別設置「政府協調委員會」(Government Coordinating Councils, GCCs)、

24 Ibid., pp. 407-409.

「部門協調委員會」(Sector Coordinating Councils, SCCs)、「跨部門委員會」(Cross-Sector Councils)，主要目的在擴大政府與各產業部門關鍵基礎設施擁有者的代表性及參與性。此外，政府也設立「關鍵基礎設施伙伴諮詢委員會」(Critical Infrastructure Partnership Advisory Council, CIPAC)，以便有效協調聯邦、各州、地方政府、民間企業的關鍵基礎設施防護業務，會員則由SCCs及GCCs的會員共同組成。[25]

CIPAC每年召開一次全體會議，以2011年召開的年度會議為例，會議討論的重點包括：

(一)關鍵基礎設施風險管理的倡議，內容包括發展全國風險圖像(National Risk Profile, NRP)，完成全國關鍵基礎設施防護年度報告(National Critical Infrastructure Protection Annual Report, NAR)，提出關鍵基礎設施風險管理計畫(Critical Infrastructure Risk Management Plan, CIRMP)。

(二)由全國防護計畫處(National Protection and Programs Directorate)所屬的基礎設施辦公室(Office of Infrastructure Protection)在2011年春季設立區域性倡議(Regional Initiative)，檢討區域性之防護能力。

(三)全國性可疑活動報告倡議(Nationwide Suspicious Activity Reporting Initiative)，經由資訊分享增進對可疑活動的瞭解，初期以交通運輸及商業設施兩個部門為試辦對象。[26]

目前國土安全部在政策處(Office of Policy) [27] 下設有民間部門辦公室(Private Sector Office)，以功能來分，民間部門辦公室分為兩類：擴大企業服務(Business Outreach Group)及經濟分析(Economics Group)，前者之目的在促進與私人企業、商業工會與非政府組織之間的對話，同時促進公私協力機制，並經由提供最佳範例(best practice)來提升國土安全防護能力。後者主要負責分析國土安全部政策對於民間部門帶來的經濟影響，包括政策分析、程序分析、管制分析、方法論評估等。[28]

四、公布「國家基礎設施防護計畫」與「個別部門計畫」

PDD-63曾呼籲擬定「國家關鍵基礎設施保證計畫」(National Infrastructure Assurance Plan)，國土安全國家戰略

25 有關CIPAC的會員，可參閱國土安全部網頁 http://www.dhs.gov/files/committees/editorial_0848.shtm

26 Department of Homeland Security, *2011 Critical Infrastructure Partnership Advisory Council Annual*, pp. 3-4.

27 國土安全部之政策處(Office of Policy)主要任務在發展、整合及協調全國土安全部的政策與計畫，政策處設有下列單位：政策發展辦公室(Office of Policy Development)、策略規劃辦公室(Office of Strategic Plans)、州與地方政府執法辦公室(Office for State and Local Law Enforcement)、國際事務辦公室(Office of International Affairs)、移民統計辦公室(Office of Immigration Statistics)、民間部門辦公室(Private Sector Office)、國土安全諮詢委員會(Homeland Security Advisory Council)。

28 Charles P. *Nemeth, Homeland Security: An Introduction to Principles and Practice* (New York: CRC Press, 2010), pp. 168-169.

(National Strategy for Homeland Security)及國土安全法(Homeland Security Act)亦有類似建議。2003年布希總統發佈的「第七號國土安全總統指令」(HSPD-7)也宣示在2004年底前完成一份整體性的全國防護計畫，因此，美國在2003年公布了「全國網路空間安全策略」(National Strategy to Secure Cyberspace)及「國家關鍵基礎設施及重要資產防護策略」(National Strategy for the Physical Protection of Critical Infrastructures and Key Assets)，2006年6月30日正式公布「國家關鍵基礎設施計畫」(National Infrastructure Protection Plan, NIPP)，並於2009年修正，作為關鍵基礎設施防護的指導綱領。

NIPP的目標在建立一個更安全、更具韌力的美國，透過預防、嚇阻、抵銷、減輕恐怖份子對於國家關鍵基礎設施及重要資產的蓄意攻擊。當恐怖攻擊、天然災害或其他緊急事件發生後，國家亦可強化整備、及時反應、迅速復原。因此，NIPP是以「風險管理」為架構(包含資產辨識、風險評估、排序、執行防護方案、效能量測等步驟)，以「全災害」方法進行關鍵基礎設施的安全防護。

除了對關鍵基礎設施的威脅進行分析外，NIPP也界定聯邦、州、地方政府、基礎設施擁有者及操作者、諮詢委員會、學術界之角色與權責，並且強調公私協力及資訊分享在安全防護的重要性。最後，NIPP亦針對教育訓練、研究發展、資源分配等問題提出綱要性宣示。[29]

此外，NIPP也宣示將由個別部門主管部會(Sector-Specific Agencies)與SCCs及GCCs共同商議訂定個別部門計畫(Sector-Specific Plans, SSPs)，內容與NIPP架構大致相近。目前美國已經完成18個關鍵基礎設施的SSP，僅有郵政與貨運(Postal and Shipping)部門計畫仍在擬定中。其中政府設施(Government Facilities)部門計畫先提出教育設施(Education Facilities)部門計畫，因為國土安全部將教育設施視為政府設施的「次部門」(subsector)。

伍、政策推動的困難與挑戰

過去幾年來，美國在推動關鍵基礎設施安全防護的政策過程中，曾面臨下列困難與挑戰：

一、關鍵資產認定不易

關鍵基礎設施安全防護之首要工作在於資產認定，因其具備三項目的：第一，透過關鍵資產辨識，以便進行風險評估及排序；第二，欲藉由資產認定提升環境意識(situational awareness)；第三，作為安全防護經費分配的依據。

根據國土安全部所建立的「全國資產資料庫」(National Asset Database)，2006年

29 Department of Homeland Security, *National Infrastructure Protection Plan*, 2009.

時，國土安全部共訂出7萬7千項關鍵基礎設施，由於這份關鍵資產清單是歷年來逐漸演進而來，因此，資料的品質始終是美國國會關切的焦點，例如，若干過去曾被列為關鍵資產的發電廠卻不在2006年的資產清單，有些目前清單上的資產卻已經停止運作，所以資料庫的正確性、一致性、完整性經常受到質疑。[30]

目前建構全國資產資料庫的困難，主要是尚未通過法律強制民間關鍵基礎設施擁有者提供資訊，國土安全部基本上只能仰賴業者自願提供資產資料。其次，在已選定的關鍵資產當中，亦無法確認有多少資產已經受過訪視，該設施是否已經進行的脆弱度與風險分析，是否有防護計畫或預防措施，其時效性為何，優先順序是否更新檢討等問題。

二、資訊分享的挑戰

關鍵基礎設施防護最重要的任務是資訊分享，惟資訊分享需以信任(trust)為基礎，有兩種資訊需要分享：運作資訊(operational information)和風險資訊(risk information)，前者以企業較為熟悉，後者為政府所擅長。然而，民間往往不願分享運作資訊，理由包括：第一，資訊是維持競爭優勢的核心，第二，許多企業與客戶之間都有保密協定，約定不公開客戶的身份、交易情況，和其他資訊，一旦公開上述資訊，不僅會傷害企業信譽，甚至會面臨法律訴訟問題。第三，企業深怕資訊公開太多，有朝一日會受到政府調查。[31] 此外，企業也不願意暴露過去關於安全意外事件的資訊，深怕洩密後影響公司信譽，再則，企業經營的思考邏輯在於如何提升公司營運績效，而非安全政策相關議題，因此對問題的緊急性看法與政府未必相同。[32]

至於風險資訊主要由政府機關掌握，但政府常以國家安全為由拒絕公開，即便不同的政府機關之間，也經常會保留重要情資，如果要與企業分享恐怖主義的機密情報，也必須要求企業相關業務負責人先完成安全查核(security clearance)，由於雙方都認為資訊分享的利益很難看出，但風險和代價卻很直接而且可預見，因此在實務上推動資訊分享仍有相當之困難。[33]

30 John Moteff, *Critical Infrastructure: The National Asset Database* (Washington, DC: Congressional Research Service, RL 33648, July 16, 2007), pp. 6-12.

31 Lewis M. Branscomb and Erwann O. Michel-Kerjan, "Private-public collaboration on a national and international scale," in Philip E. Auerswald et al. (eds.), *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability* (New York: Cambridge University Press, 2006), pp. 429-456.

32 Myriam Dunn-Cavelty and Manuel Suter, "Public-private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection," *International Journal of Critical Infrastructure Protection*, Vol.2, No.4 (2009), pp. 179-187.

33 Lewis M. Branscomb and Erwann O. Michel-Kerjan, "Private-public collaboration on a national and international scale," pp. 398-399. Also Daniel B. Prieto, "Information sharing with the private sector," pp. 404-428.

陸、學術界對於新安全議題的回應

長期以來，美國學術界的研究與發展始終與國家政策密不可分，例如，二次大戰期間國會曾秘密撥款支持「曼哈頓計劃」(Manhattan Project)，大批著名的科學家均加入該計畫，最後成功地研發出原子彈。冷戰期間，各大學紛紛成立有關國家安全事務、東歐或蘇聯研究、國際關係等系所，而工程及基礎科學也蓬勃發展，並將研究成果貢獻給政府，當然，許多研究計畫受到政府直接或間接補助。

911事件發生以後，國土安全的專業人才需求大增，所以政府與學術界也立即做出回應。例如，在美國司法部、國會、海軍共同支持下，2002年海軍研究院(Naval Postgraduate School)成立了「國土防衛與安全中心」(Center for Homeland Defense and Security, CHDS)，自2003年起，該中心接受國土安全部之經費補助，並由國土安全部的「國家整備司」(National Preparedness Directorate)及「聯邦緊急事務管理總署」(FEMA)，及海軍研究院合作開設碩士班，成為全國第一個提供國土安全碩士學位的單位。除了提供碩士班及其他訓練課程以外，海軍研究院的國土防衛與安全中心也出版「國土安全事務」期刊(Homeland Security Affairs)，探討國土安全的策略、政策、組織。

此外，「北方司令部」(United States Northern Command, NORTHCOM)亦於2003年成立了「國土安全與防衛教育財團」(Homeland Security/Defense Education Consortium)，針對國土安全教育建立課程標準。2010年起，國土安全部的「運輸安全局」(Transportation Security Administration)與全美22州25個社區學院合作開設國土安全、執法、消防等相關課程，稱為副學士學程(Associates Program)，2011年此課程將推廣至全美50州。[34]

各大學也陸續在公共行政、危機管理、犯罪防治、公共衛生、工程等領域開設國土安全學程，例如，馬里蘭大學(University of Maryland)設有「衛生與國土安全中心」(Center for Health & Homeland Security)，該校並頒授國土安全、緊急管理、消防科學等理學士文憑。喬治城大學(Georgetown University)的「和平與安全研究中心」(Center for Peace and Security Studies)設有國土安全學程，並授與結業證書。南加州大學(University of Southern California)在工學院授與國土安全證書，賓州州立大學(Pennsylvania State University)公共衛生學院授與碩士學位，密西西比大學(University of Mississippi)及紐澤西市立大學(New jersey City University)於2011年起也開

34 Stanley Supinski, "Security Studies: The Homeland Adapts," *Homeland Security Affairs*, Volume 7 (September 2011).

始設立國土安全博士班。[35]

至於大學設立的國土安全研究中心，最重要的是喬治梅森大學(George Mason University)的「基礎設施防護與國土安全中心」(Center for Infrastructure Protection & Homeland Security, CIP/HS)，該中心雖設於法學院(School of Law)，但卻是一個跨領域的研究中心，提供的課程包括能源、國土安全、資通訊、醫療與公共衛生等。該中心除不定期發表政策白皮書外，每月也發行「關鍵基礎設施防護報告」(CIP Report)，提供政府最新立法、政策、學術研究發展等資訊。

在學術交流方面，George Mason CIP/HS亦積極與其他國內外知名大學、聯邦政府機構、私人企業、國外政府建立密切的伙伴關係，過去幾年來，CIP/HS曾舉辦過各類學術研討會，例如2008年的Supply Chain Security, Resilience & Sustainability Conference、2009年的International Cyber Conflict Legal and Policy Conference、2010年的4th Annual Conference on Security Analysis and Risk Management、2011年的5th Annual Conference on Security Analysis and Risk Management及Workshop on Cybersecurity Incentives，研討會主題涵蓋基礎設施回復力、社區回復力、網路安全與風險、風險分析方法論等。[36]

其他大學如密蘇里科技大學(Missouri University of Science and Technology)設立了「關鍵基礎設施防護中心」(Center for Critical Infrastructure Protection, CCIP)，研究地震、水災、人為災害、網路災害對國家關鍵基礎設施的衝擊。[37] 科羅拉多大學(University of Colorado)設有「國土安全中心」(Center for Homeland Security)，杜克大學(Duke University)、北卡羅萊納大學(University of North Carolina at Chapel Hill)及RTI International則共同設立「恐怖主義與國土安全三角中心」(Triangle Center on Terrorism and Homeland Security)，著名的智庫蘭德公司(RAND)亦設有「國土安全與防衛中心」(Homeland Security and Defense Center)。

值得注意的是，美國西點軍校(United States Military Academy at West Point)自2010年起每年舉辦「關鍵基礎設施研討會」(West Point Critical Infrastructure Symposium)，邀請國內外學者、政府部門及產業界代表參與，顯示美軍亦十分重視關鍵基礎設施防護之研究。

至於學術期刊，目前已有2004年起出版的International Journal of Critical Infrastructures(IJCIS)，2008年起出版的

35 Ibid.
36 喬治梅森大學「基礎設施防護與國土安全中心」網頁，http://cip.gmu.edu/
37 密蘇里科技大學「關鍵基礎設施防護中心」網頁，http://ccip.mst.edu/index.html

International Journal of Critical Infrastructure Protection，加州大學柏克萊分校出版的Journal of Homeland Security and Emergency Management(JHSEM)，以及前述海軍研究院出版的Homeland Security Affairs，足見關鍵基礎設施已經成為學術研究的新領域。

柒、結論

美國自1990年代起開始對關鍵基礎設施的安全性展開分析與檢討，911事件後積極推動相關防護政策，從歷年公布的「國土安全國家戰略」、「四年期國防總檢報告」、及「四年期國土安全檢討報告」的內容來看，美國推動關鍵基礎設施與重要資產的防護主要目的在防範恐怖份子攻擊。雖然目前我國遭受恐怖份子攻擊的機會較低，但仍不能完全排除其他人為的破壞(例如在人潮聚集的機場、地鐵站、火車站放置炸彈或縱火、駭客對網路進行惡意攻擊)，或因人為操縱的疏忽而導致之大規模工安事故。

尤為重要者，由於全球氣候變遷所造成的極端氣候，對台灣的國土安全及關鍵基礎設施形成極大的威脅，加以本身的地理環境特性，使台灣處於高度自然災害風險之脆弱區域，幾乎每年都受到颱風、豪雨及地震等影響，嚴重者往往造成生命及財產損失。

由於我國已經是一個高度現代化的國家，不論在工業生產、商業交易、或日常生活上都高度依賴水、電、能源、通訊、網路、金融、交通等設施，這些設施或系統一旦因為天然災害或人為破壞造成中斷，對整體社會的運作和國家安全將會產生極大的衝擊與傷害。是以，如何有效落實國家關鍵基礎設施防護工作，期能維繫政府持續運作(Continuity of Government Operation)及企業持續經營(Business Continuity Management)，應為政府最重要之施政議題。

因此，我國應參考先進國家之實踐經驗，再評估本身特殊的安全環境(包括地理環境、發展特色、天然災害、意外事件、人為攻擊、敵人威脅等)，進而建構一套具體的法制規範與權責管理體系，作為關鍵基礎設施安全防護的基礎，同時強化公私協力機制，喚醒各主管機關及民間關鍵基礎設施擁有者或營運者對於安全防護工作的重視，才能確保國土安全與國家安全。

附表一　美國歷年來各種戰略報告對於關鍵基礎設施防護之宣示

年度	單位	報告名稱	關鍵基礎設施防護之目標或策略
2002	國土安全辦公室	國土安全國家戰略(National Strategy for Homeland Security)	該報告將「關鍵基礎設施及重要資產防護」(Protecting Critical Infrastructures and Key Assets)列爲重要任務，主要措施包括： 1.由國土安全部統合全美國的基礎設施防護。 2.對關鍵基礎設施及重要資產防護建立及維持一套完整且精確的評估。 3.使州政府、地方政府、民間部門成為有效的伙伴。 4.發展一套國家基礎設施防護計畫 5.強化網路安全。 6.利用最佳的分析或模型工具發展出有效的防護方案。 7.守護美國的基礎設施及重要資產對抗內部的威脅。 8.與國際社會合作防護美國的跨國性基礎設施。[38]
2003	總統辦公室	國家關鍵基礎設施及重要資產防護策略(National Strategy for the Physical Protection of Critical Infrastructures and Key Assets)	該報告將關鍵基礎設施及重要資產防護的戰略目標訂爲： 1.辨識並防護國家最重要的基礎設施 2.針對基礎設施的威脅提供即時的預警措施及防護 3.針對有可能成為恐怖份子攻擊目標的基礎設施，設立一個合作的環境，使聯邦、州、地方政府、民間部門能更有效地防護他們掌管的基礎設施。[39]
2006	國防部	四年期國防總檢報告(Quadrennial Defense Review Report)	該報告將「深化國土防衛」(Defending the Homeland in Depth)列爲戰略目標，報告指出，全球化不僅帶來資本、貨物、人員、資訊的自由移動，也加速了傳染病的擴散、武器的交易、極端意識型態的散播、恐怖份子的流動，非國家敵人也將攻擊目標鎖定在政府設施、商業與金融、文化與歷史標的物、食物、水、電力、資訊、交通、能源等設施，因此國防部已將保護美國人民、國土、關鍵基礎設施列爲防護目標。[40]

38　Office of Homeland Security, *National Strategy for Homeland Security,* July 2002, p. ix.

39　White House, *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, February 2003, p. vii.

40　Department of Defense, *Quadrennial Defense Review Report,* February 2006, p. 24.

2007	國土安全會議	國土安全國家戰略(National Strategy for Homeland Security)	該報告將「保護美國人民、關鍵基礎設施及重要資源」(Protect American People, Critical Infrastructure, and Key Resources)列爲重要任務，主要措施如下： 1.嚇阻恐怖份子威脅。 2.降低脆弱性(包括確保關鍵基礎設施及重要資源的回復力)。 3.將災害後果降至最低。[41]
2010	國防部	四年期國防總檢報告(Quadrennial Defense Review Report)	該報告雖未將關鍵基礎設施防護明確納入戰略目標，但將「在網路空間有效運作」(Operate Effectively in Cyberspace)列爲戰略目標。 報告指出，國防部的網路空間高度依賴商業基礎設施，因此國防部必須與其他部會及國際伙伴共同合作確保在網路空間運作之能力，相互協助措施包括：資訊分享、支持執法、國防支援文人政府、國土防衛。特別應與國土安全部共同防護聯邦的資訊系統。[42]
2010	國土安全部	四年期國土安全檢討報告(Quadrennial Homeland Security Review Report)	該報告將「對關鍵基礎設施、重要領導人及事件的風險管理」(Manage Risks to Critical Infrastructure, Key Leadership, and Events)列爲主要目標，具體作爲包括： 1.瞭解關鍵基礎設施的風險並加以排序：透過辨識、分類、分析，指出哪些關鍵基礎設施最危險。 2.防護關鍵基礎設施：避免資產、系統、網絡、網路等遭到攻擊或中斷。 3.使關鍵基礎設施具回復力：強化關鍵基礎設施系統、網絡的能力與功能，以便承受損害和中斷，並迅速復原。 4.保護政府領導人、設施、及特殊事件：確保政府持續運作，保障全國性重要事件的安全。[43]

資料來源：作者整理

作者簡介

王政

美國北伊義諾大學政治學博士
現任中央警察大學公共安全學系助理教授

41 Homeland Security Council, *National Strategy for Homeland Security,* October 2007, pp. 27-30.
42 Department of Defense, *Quadrennial Defense Review Report,* February 2010, pp. 37-39.
43 Department of Homeland Security, *Quadrennial Homeland Security Review Report,* February 2010, pp. 41-43.