國立政治大學國際事務學院外交學系

碩士論文

指導教授：姜家雄　博士

網路恐怖主義與美國防治政策

研究生：黃書賢

中華民國一百零一年七月

國立政治大學
National Chengchi University

國立政治大學
National Chengchi University

國立政治大學
National Chengchi University

國立政治大學
National Chengchi University

國立政治大學
National Chengchi University

國立政治大學
National Chengchi University

國立政治大學
National Chengchi University

謝辭

對我而言，攻讀碩士學位，除了出於對國際關係領域的興趣，以及培養個人專業能力等目的之外，也是為了挑戰自我，想親身體驗看看「寫論文」到底是什麼樣的滋味。現在回想起來，撰寫論文的過程果真使我有接近極限之感，從天黑到天亮，夜深人靜的研究室一路陪我閱讀、苦思及寫作；在不知不覺中，髮間也冒出了些許白絲。如此辛苦產出的心血結晶，尚不敢自誇在恐怖主義或網路安全學術領域上具有多少重要性，但求盡力而為，問心無愧而已。

身為一個文學院畢業生，在退伍之後毅然選擇轉換領域，報考外交研究所，親愛的父母始終願意支持我任性的決定，不僅給予最大限度的生活自由，同時又讓我在經濟上全無後顧之憂。您們也許對於我的論文內容並不十分理解，但是這麼多年來的養育之恩，孩兒實在無以報答，唯有萬分感謝。

姜家雄老師做為我的論文指導教授，從初期的討論過程之中，已能讓我認識到老師在學術資料閱讀與理解上的深度和廣度，以及嚴謹而不失幽默的學者風範。在我遇到瓶頸和難關，或是在文獻資料的取捨上游移不定時，姜老師每每提點許多不同角度的思考方向，使我撥雲見日，豁然開朗。不僅如此，老師也一直非常細心地批改我的草稿，鉅細靡遺，並且願意從架構到細節，多次與我進行深入討論，讓我在謝過老師，轉身離開研究室之際，總是能夠重拾信心，保持衝勁。學生才疏學淺，但願這本論文沒有辜負老師的辛勞和用心。而盧業中老師的支持與肯定，則是我決定嘗試將全球化課程期末報告發展成學位論文的最重要因素。如果沒有盧老師的鼓勵，我恐怕還得花更多的時間，繼續茫茫然地尋找論文題目，在此也向盧老師致上由衷的感謝。

在三年的研究所生涯中，眾多來自不同領域和背景的同學，使我接觸到更多更廣的知識，擁有更豐富的生活體驗，同時也有幸結交數位好友。感謝胡育瑋、徐裕軒、梁守道、賴昱誠和李季剛，諸位各自的專長、學養和興趣，不但令我佩

服不已，更獲益良多；你們的忠實陪伴、相互打氣與幽默言語，也讓我在論文寫作的漫長道路（以及環島之路）上，不致太過孤單苦悶，能夠認識諸位，我感到非常幸運。

感謝林育正與何明翰，透過小小的聊天視窗，你們經常與我分享生活點滴，排憂解惑，不知帶給我多少歡笑和振奮，甚至靈感。另外，還要感謝大學時期的同窗好友：楊智元、呂美瑩、高偉峻、屈子婷和廖峻宏，無論只是簡單的聚餐或出遊，或是專程驅車來訪，談天說笑之間，你們總是能讓我紓解不少壓力，就如同從水中探出頭來，大口呼吸新鮮空氣一般暢快。

老實說，早在論文尚未完成之前，對於這篇謝辭內容的形塑和想像，便已經被我用以充當暫時擺脫混亂思緒的出口。只是，當真的著手撰寫謝辭之時，卻發現自己實在拙於行文，即使推敲琢磨許久，仍然覺得字裡行間所能表達的感謝之意，尚不及心中的十分之一。再次誠摯感謝親愛的父母、師長、同學，以及所有曾經幫助過我順利完成論文的每一個人，願諸位永遠身體健康、平安順心。

黃書賢　謹識

中華民國一百零一年七月

中文摘要

網路恐怖主義（Cyberterrorism）為「網際網路」（Internet）與「恐怖主義」（terrorism）相互結合之產物，指恐怖份子為求引發嚴重破壞，並造成平民死傷，透過網際網路入侵國家關鍵基礎設施（critical infrastructures），並以之要脅政府或人民完成其政治性、宗教性或社會性目標。至 2012 年 7 月為止，對於網路恐怖主義相關議題之討論雖已持續約 30 年之久，然而各界對於網路恐怖主義之「定義」及「威脅性」兩項基本問題，仍然眾說紛紜，無法取得一致共識，而全球各地缺乏網路恐怖攻擊之實際案例之情況，亦使爭辯益加激烈。

在美國政府方面，經過 2001 年 911 事件的重大衝擊，其對於恐怖主義相關議題之敏感程度已大幅提高，並陸續制定多項反恐政策。美國是當前國際反恐行動的領導者，既為軍事與科技大國，同時也是諸多國際恐怖組織策劃攻擊之主要目標，有鑑於此，美國政府致力於防治網路恐怖主義，保護國內關鍵基礎設施不受侵襲，以維持社會安定及國家安全，其因應方式足以成為世界各國制定類似政策之重要參考對象。

本論文經由探討網路恐怖主義之基本意涵，比較「網路恐怖主義」、「網路犯罪」及「網路戰爭」三個概念之間的差異，嘗試針對網路恐怖主義形成明確之界定；接著綜整各界針對網路恐怖主義威脅性之爭論，以了解網路恐怖主義之真實威脅程度；最後觀察美國自柯林頓（Clinton）政府至今，有關防治網路恐怖主義政策之一系列發展、美國政府如何評估網路恐怖主義之威脅，以及在當前的政策架構之下，為保護國內關鍵基礎設施，其相對應之具體措施為何，試圖對於其整體政策建立客觀評價。

關鍵詞：網路恐怖主義、美國反恐政策、網路犯罪、網路戰爭、保護關鍵基礎設施、國土安全部、網路空間安全國家戰略。

國立政治大學
National Chengchi University

Abstract

Cyberterrorism, the convergence of “Internet” and “terrorism,” refers to the specific terrorist activities that were intended to cause massive destruction and casualties, proceeded by intruding the supervisory control and data acquisition (SCADA) systems of national critical infrastructures via the Internet. Even though the discussion of the related issues of Cyberterrorism has continued for nearly 30 years now, neither the definition nor the evaluation of potential threat concerning Cyberterrorism has been settled. No consensus has been achieved. Furthermore, the lack of actual cases of Cyberterrorism attack around the world makes the debates even more intense.

After the significant impact of September 11, 2001, the U.S. government has substantially raised the degree of sensitivity of the issues related to terrorism and developed a number of counter-terrorism policies. As the leader of the Global War on Terror and the greatest Power in the world, the U.S. is also the main target of many terrorist groups. With its military and scientific capabilities, the practices of the U.S. government on preventing Cyberterrorism, protecting its domestic critical infrastructures from intrusion, and maintaining social stability and national security would be excellent examples to other nations for the development of their own policies.

To clarify the explicit definition of Cyberterrorism, this research refined the basic meaning of Cyberterrorism and distinguished differences among three related concepts: Cyberterrorism, Cybercrime, and Cyberwar. Moreover, this research sought to induct major arguments brought up by scholars in many intense debates on the extent of Cyberterrorism threat. Last but not least, by observing development of the

U.S. related policy frameworks, how the U.S. government evaluates the extent of Cyberterrorism threat, and the corresponding measures for protecting the U.S. domestic critical infrastructures, this research presented an objective assessment on the U.S. overall counter-Cyberterrorism policies.

Keywords: Cyberterrorism, U.S. Counter-Cyberterrorism Policies, Cybercrime, Cyberwar, Critical Infrastructure Protection.

國立政治大學 National Chengchi University

章節目錄

國立政治大學 National Chengchi University

圖表目次

國立政治大學 National Chengchi University

國立政治大學
National Chengchi University

網路恐怖主義與美國防治政策

第一章　緒論

"As we approach the 21st century, our foes have extended the fields of battle from physical space to cyberspace."

President Clinton, 22 May, 1998[1]

網際網路（Internet），如此簡單便利又能接觸到如此巨量資訊之途徑，不僅是人類歷史首見，亦為當今全球化現象的一大重要推手。以網際網路為主要媒介的全球通訊科技系統，使得各國政府能夠更有效率地運作，並對外推動公眾外交（public diplomacy）等各項工作，跨國企業亦透過網際網路進行全球性的佈局和管理。在此同時，世界各地的人們也能自由地傳遞或交換各種意見及想法，甚至推動某些地區的自由化和民主化進程。經由觀察以上種種現象可以發現，網際網路所提供的便利性和迅捷性，對於當前的全球社會而言，可謂至關重要，網際網路已然成為世界經濟、文化和社會等各層面能夠進行交流或整合的關鍵媒介。

不過，隨著網路科技與通訊技術的快速發展，對於公私部門網路安全（cyber security）或資訊安全（information security）相關領域而言，網路犯罪（cybercrime）及網路恐怖主義（cyberterrorism）之潛在威脅亦與日俱增。就在眾多攸關大眾生活品質及社會正常運作之關鍵基礎設施（Critical Infrastructures, CIs）逐漸依賴網際網路進行監控和管理的同時，也正面臨網路恐怖份子隨時可能入侵的風險。

[1] Tim Clark, "Clinton Outlines Cyberthreat Plan," ＜http://news.cnet.com/Clinton-outlines-cyberthreat-plan/2100-1023_3-211497.html＞(Retrieved on February 1, 2012). 本論文提到的諸多外國人名大多尚無通用譯名，因此除了若干已受廣泛使用之譯名，例如：布希、萊斯等等之外，為避免產生混淆或誤解，後文皆採用原文人名，不另行翻譯。

Ron Rhodes 指出，在網際網路的發展過程當中，人們著重的核心理念是「共享」，而非「安全」。[2]換言之，人類開發網路科技的初衷，在於開放、自由，並且讓任何人都能接觸資訊。只要使用者出於良善之目的，網際網路的這些特性固然有益於人類社會，然而，一體總是有兩面，各種出於惡意的濫用及破壞行為，亦使得許多國家的公私部門皆面臨潛在的安全威脅，其中又以高度仰賴網路科技和關鍵基礎設施的先進國家為主，例如美國。

身為科技大國與當今國際體系中的唯一超級強權，美國從何時開始關注網際網路所帶來之潛在威脅？政府如何因應？具體的政策措施演變脈絡為何？本論文經由相關文獻之回顧，綜整學界對於網路恐怖主義之基本意涵與實際威脅的爭論，從而提出問題意識，不僅嘗試界定網路恐怖主義，亦評估其對於國家安全之威脅性，並且檢視在當前美國防治網路恐怖主義的政策架構之下，美國政府如何保護國內的關鍵基礎設施，試圖對於相關政策建立客觀之評價。

第一節　研究緣起

冷戰（Cold War）結束之後，非傳統安全（non-traditional security）議題逐漸成為國際關係研究的討論焦點之一，加上恐怖主義（terrorism）活動的潛在威脅，安全研究之範疇已不僅限於水資源安全、糧食安全、能源安全、通訊安全和運輸安全等等，亦擴及到生態環境、金融秩序、傳染病防治及人口遷移等面向。另一方面，全球化（Globalization）現象亦為當前的熱門議題，相關論述方興未艾，其中也包括許多著重於全球化之負面影響的討論，例如有學者主張，全球化現象不僅帶來正面的影響和獲益，同時也造成負面的衝擊與挑戰，尤其是對於主

[2] Ron Rhodes, *Cyber Meltdown: Bible Prophecy and the Imminent Threat of Cyberterrorism* (Eugene, OR: Harvest House, 2011), p. 73.

權國家構成的五項嚴重威脅：毒品買賣、武器走私、侵犯智慧財產權、人口販運和跨國洗錢犯罪，皆是當今各國所面臨的重大難題。[3]

不過，除了這五大難題之外，針對網際網路的有效管理也是另一個因全球化而起的棘手問題。在科技發展日新月異的時代，網際網路提供了跨區域的人際溝通和交換訊息之管道，與在其之前出現的傳播工具，如郵件、電報、電話和無線電等相比，不僅速度更快，成本也更低。網際網路不僅是全球化的重要媒介，更可說是全球化的一大推手，已為人類日常生活帶來極大的便利和效益，也逐漸成為現代社會不可或缺的一項重要工具。

但是，網際網路同時也帶來了某些危險及威脅，甚至成為犯罪行為與恐怖主義的溫床，危害社會安定與國家安全。目前許多政府部門和私人企業正在進行電子化的轉型，包括將大量的紙本公文轉換為電子文件，並利用電子郵件的方式傳遞公文和訊息，以及在線上（online）服務廣大民眾與客戶等等。不僅如此，許多銀行內部的資料處理作業，以及眾多關鍵基礎設施如水壩、核能發電廠及交通燈號管制中心的「資料擷取與監控系統」（Supervisory Control and Data Acquisition Systems, SCADA）[4]等等，都不免使用網際網路進行資訊連結和交換，對於網路科技的依賴程度也與日俱增。在此情況之下，極大量未經加密保護或保護層級不高的資訊，已暴露在公開的網路空間（cyberspace）之中，在有心人士的眼中，這些資訊正是攔截和濫用的良好目標。就如同全球化現象所帶給世界各國的正面及負面影響一般，網際網路雖然讓人們的生活更加便利，資訊的分享和傳播也更加迅速；然而，當公私部門對網際網路的依賴逐漸加深之同時，潛在的安全危機也不容忽視。

---

[3] Moisés Naím, “The Five Wars of Globalization,” *Foreign Policy*, No. 134 (January/February 2003), pp. 29-34.

[4] SCADA 一般指涉具有監控及資料擷取能力的電腦控制系統，可運用在工業程式、基礎設施等。SCADA 可以是監控及控制所有設備的集中式系統，或是由分散在一個區域中的許多系統之組合。其大部分的監控由「遠程終端控制系統」（Remote Terminal Unit, RTU）或「可程式邏輯控制器」（Programmable Logic Controller, PLC）進行，各項資料及數據則由感測器擷取，並傳送至控制系統。關於 SCADA 系統之說明，可參見：David Maynor & Robert Graham, “SCADA Security and Terrorism: We’re Not Crying Wolf,” pp. 8-15, ＜www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf＞(Retrieved on June 13, 2012).

在此同時，全球各地關鍵基礎設施遭到網路攻擊的案例，亦時有所聞。例如2007 年 1 月，美國當局以重罪指控洛杉磯市（Los Angeles）兩名都會交通系統管制人員，由於他們在 2006 年夏季配合當時的工會示威活動，駭入該市的交通燈號管制系統，導致嚴重的交通堵塞；即使並未造成實際傷亡，這場入侵行動仍然使得相關單位必須耗費四天的時間，始能完全排除損害。[5]

又如今年（2012）6 月，美國官員承認，自小布希（George W. Bush）政府開始，美國國家安全局（National Security Agency, NSA）便與以色列情報部門密切合作，共同研發電腦病毒，用以入侵伊朗的濃縮鈾設施（nuclear enrichment facilities），拖延該國的核子武器研發進程，該行動之機密代號為「Olympic Games」。歐巴馬總統（Barack Obama）上任不久，亦秘密下令擴大網路攻擊的密集程度。2010 年，一隻名為「Stuxnet」的強力電腦病毒，在數週之內癱瘓了伊朗境內約 1000 部提煉濃縮鈾的離心機。[6]

這兩個實例足以說明，有心人士以網際網路入侵國家的關鍵基礎設施，不僅不只是科幻小說情節，尚可能引發實際的破壞及損失。在電影文化方面，2007 年的好萊塢（Hollywood）電影《終極警探 4.0》（Live Free or Die Hard）之中，不法集團網羅多名駭客（hacker）[7]，運用先進的器材和熟練的手法，成功入侵國家的金融系統、電視媒體和運輸交通管理系統，造成交通秩序大亂，民眾的人身安全和國家的財政儲備體系皆遭到嚴重威脅。數名歹徒亦透過電視公開進行恐嚇，以逼迫政府接受其要求。[8]雖然電影是以略為誇張的手法，將國家安全與社

[5] Matt Krasnowski, "Two Men Accused of Hacking into Traffic System," <http://www.utsandiego.com/uniontrib/20070121/news_1n21traffic.html>(Retrieved on July 4, 2012).

[6] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all>(Retrieved on July 4, 2012).

[7] 原意是指對作業系統及程式語言非常熟悉的人，他們不僅熱衷於探討系統與程式之原理，並且具有優異的系統開發與程式撰寫能力。然而，一般大眾及媒體習慣將入侵他人電腦系統、破壞電腦網路安全的「怪客」（cracker）與 hacker 混在一起使用，如今「駭客」這個名詞也常被用來形容攻擊電腦網系統的人。關於駭客更詳細的分類、駭客之動機及入侵手法等，可參見：林義貴，《**資訊社會與網路犯罪**》（臺北：華立，2005），頁 268-273。

[8] 關於電影情節，可參見："Synopsis for 'Live Free or Die Hard'," <http://www.imdb.com/title/tt0337978/synopsis>(Retrieved on June 14, 2012).

會安定的脆弱性（vulnerability）呈現在全球觀眾面前，仍可做為政府反恐工作之借鏡。

由上述之攻擊實例與電影情節可以想見，以電腦和網際網路做為工具及目標的「網路犯罪」行為，其與恐怖主義活動相互結合之「網路恐怖主義」對於國家安全的威脅程度，並不亞於前述伴隨全球化而來的五大難題。事實上，前美國總統小布希早在 2001 年 911 恐怖攻擊事件之前，已於同年 7 月宣布，網路恐怖主義是未來美國國家安全的新威脅。[9]另有專家學者指出，小布希於 2000 年競選總統期間，便提出過「網路恐怖主義即將興起」的主張。[10]

如同前美國國家安全顧問萊斯（Condoleezza Rice）於 2001 年 3 月所言：「很矛盾地，正是完全相同的科技，既使我們在經濟上充滿活力、軍事上擁有壓倒性優勢，也使我們變得更加脆弱。」她同時也提出警告：「破壞了資訊網路，你便瓦解（disrupt）了這個國家。」[11]

綜觀目前的全球化浪潮，國家權力在經濟、文化等議題上，已不免受到一定程度的取代或侵蝕，但是在安全議題方面，國家仍然扮演舉足輕重的角色。尤其是在 911 事件之後，當時的美國總統小布希便提出「向恐怖主義宣戰」（War on Terror），積極要求並推動世界各主要國家進行聯合反恐行動，先後對阿富汗及伊拉克兩國，以反恐為名義發動戰爭。到目前為止，傳統恐怖主義[12]仍未曾銷聲匿

---

[9] Simon Finch, "Cyber-terrorism Poses a Serious Threat to Global Security," in Louise I. Gerdes, ed., *Cyber Crime* (Farmington Hills, MI: Greenhaven Press, 2009), p. 36.

[10] 例如：Joshua Green, "The Myth of Cyberterrorism," *Washington Monthly*, Vol. 34, No. 11 (November 2002), p. 8; Gabriel Weimann, "Cyberterrorism: How Real is the Threat?" p. 3, ＜http://www.usip.org/files/resources/sr119.pdf＞(Retrieved on June 30, 2012).

[11] 引述自：Kevin A. O'Brien, "Information Age Terrorism and Warfare," in David M. Jones, ed., *Globalisation and the New Terror: The Asia Pacific Dimension* (Northampton, MA: Edward Elgar Publishing, 2004), p. 154.

[12] 隨著時代演變與科技發展，恐怖主義的攻擊手段也持續與時俱進。本論文所指涉的「傳統恐怖主義」係相對於「網路恐怖主義」而言，主要著重於攻擊手段的不同，傳統恐怖主義的攻擊手段包括暗殺公眾人物、綁架人質、劫持交通工具、引爆炸彈，或是動用大規模毀滅性武器（weapons of mass destruction, WMD）等等，網路恐怖主義則指涉透過網際網路針對國家關鍵基礎設施之電腦系統、電腦程式、網絡及儲存於其中之資訊及資料，進行非法攻擊或威脅攻擊（請參見本論文第二章第一節）。大規模毀滅性武器的出現，使得暗殺、綁架等行之有年的攻擊手段相對成為傳統恐怖主義，而網路恐怖主義則又取而代之。關於科技與恐怖主義之間的關係，可參見：宋興洲，「科技在恐怖主義與反恐行動中所扮演的角色」，收於姜新立、張錦隆主編，《**政治與資訊的交鋒**》。臺北：揚智，2010，頁 53-89。

跡，各種攻擊手段及行動訴求皆不一而足。反觀網路恐怖主義，眾多專家學者不僅對於它的定義為何，仍然缺乏共識，也由於網路恐怖主義迄今尚未發生重大的實際攻擊案例，使得各界不免懷疑其是否足以形成真實威脅，抑或只是有心人士的炒作，因而引發不少爭論。

在美國政府方面，雖然在 911 事件之後，對於制定國內反恐法案及建立防衛機制等相關措施方面，美國政府皆不遺餘力，盡量將實體形式的各種恐怖攻擊發生之可能性降到最低，然而，網路恐怖主義作為新型態的恐怖主義，結合「虛擬形式、可由境外發動攻擊、難以判別攻擊者確切身分及所在地點」等特色，以及對於關鍵基礎設施及金融秩序具有高度之破壞能力，即使尚未發生網路恐怖主義攻擊的實際案例，但是對於美國及國際社會而言，仍可能構成國家安全的重大威脅，實在不應等閒視之。

目前美國公私部門已高度依賴網際網路，例如軍方向民間大量採購各項高科技產品和服務、通訊系統、電子零組件和電腦軟體等，[13]政府各部門更是依賴網際網路交換資訊，以及提供一般民眾服務；此外，私人企業亦有許多重要的電子資料透過網際網路傳輸，並存放於各種儲存設備，因而暴露在遭到駭客攔截、入侵、竄改及竊取的風險之中。有學者指出，美國依賴電腦系統和網路來維持基礎設施運作的程度，高居世界之冠；[14]另有學者直言，雖然美國高度依賴網際網路控制各種系統，卻又不甚重視國家的網路防禦機制，導致美國在這個面向比俄羅斯或中國更加脆弱。[15]不僅如此，更有學者以「巨大的電子阿基里斯腱」（a massive electronic Achilles' heel）來比喻這個嚴重的潛在危機。[16]

---

[13] Clay Wilson, *Computer Attack and Cyberterrorism* (New York: Nova Science, 2009), p. 1.
[14] Ron Rhodes, *op. cit.*, p. 75.
[15] Richard A. Clarke & Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2010), p. 155.
[16] James A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," report submitted to the Center for Strategic and International Studies, CSIS, Washington, DC, p. 1, < http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf > (Retrieved on February 9, 2012).

美國身為國際反恐行動當中最主要的行為者，同時也是許多國際恐怖組織之攻擊目標。[17]假使以美國如此擁有豐富資源並高度重視反恐工作的先進科技大國，仍無法有效阻止網路恐怖主義攻擊，則其他國家面臨此一威脅，國家安全將更加岌岌可危。有鑑於此，在反恐議題領域（issue area）之中，美國政府對於網路恐怖主義防治政策之制訂、發展及執行成果，可謂極具指標性意義。

第二節　文獻回顧

文獻回顧之目的，在於彙整與研究問題相關的文獻資料，以對於該問題的知識背景建立初步的認識，及了解當前國內外相關研究的最新發展，以此做為研究工作之基礎，確立研究議題之方向，並嘗試提出解釋或批判。本論文在既有文獻之整理與回顧方面，首先針對網路恐怖主義之界定問題，進行背景資料的搜集，以建立相關概念之基礎；進而統整學界之爭辯情況，對照雙方各自的主張和論據，以了解網路恐怖主義威脅的嚴重性；最後則是回溯美國政府近年來相關的重大政策。綜括上述，此部分依據四個面向進行分類：

1. 網路恐怖主義之界定；
2. 網路恐怖主義與網路犯罪及網路戰爭之比較；
3. 網路恐怖主義是否為嚴重威脅；
4. 美國政府防治政策。

經由對於四個面向的各類相關之文獻進行綜整與回顧，歸納重要學者之意見，以及重大政策之演變過程，可初步掌握當前的研究概況及政策發展情形，進而形塑本論文之問題意識。

[17] 原因可能出於宗教衝突、反美情緒、反對經濟全球化等，例如：蔡瑋，「冷戰後的國際恐怖主義：趨勢與挑戰」，收於邱稔壤主編，《**國際反恐與亞太情勢**》（臺北：國立政治大學國際關係研究中心，2004），頁 7-29；邱伯浩，《**恐怖主義與反恐**》（臺北：新文京，2006），頁 15；李偉主編，《**國際恐怖主義與反恐怖鬥爭年鑑**》（北京：時事，2004），頁 23。

壹、網路恐怖主義之界定

網路恐怖主義為傳統恐怖主義與網際網路應用之複合體，可歸類於網路犯罪行為之一類，而網路恐怖主義、網路犯罪及網路戰爭（cyber warfare）三者之間的差異，也容易發生混淆，亦有多位專家學者曾提出各自之見解。本論文參考眾多相關文獻，嘗試比較其彼此之異同，藉此能夠對於網路恐怖主義形成更加清晰之定義。

有鑑於各界對於恐怖主義之定義尚未取得共識，以及美國政府在 911 事件後對於恐怖主義之議題特別關注，本論文因而參考美國政府部門及法律條文中提及之定義，從中了解美國政府如何定義恐怖主義，哪些行為屬於恐怖主義，在定義之中有何不可或缺的要素等等，以建立對於網路恐怖主義之初步理解。

在網路恐怖主義研究領域之中，Dorothy E. Denning 可謂非常重要的一位學者。2000 年 5 月，Denning 面對美國眾議院軍事委員會恐怖主義特別監督小組（Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives）作證時提出，網路恐怖主義之定義為：「網路恐怖主義指涉對於電腦、網絡及儲存於其中之資訊進行非法攻擊或威脅攻擊，以恐嚇或脅迫政府或其人民完成其政治性或社會性目標。此外，若要將一個攻擊行為歸類為網路恐怖主義，應包含對人身或財產之暴行，或至少產生足夠的傷害引發恐懼，例如導致死傷、爆炸或經濟嚴重受創之攻擊等。針對關鍵基礎設施之攻擊可能是網路恐怖主義行為，端視其影響而定。干擾非必要性設施，或只是造成代價不菲的騷擾等，此類攻擊則不包括在內」。[18]包括此定義在內，Denning 對於網路恐怖主義之定義範疇、發展概況與威脅性之評估等方面的深入研究，相關論述文章一直受到廣泛的引用及討論。[19]

---

[18] Dorothy E. Denning, "Cyberterrorism," testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, May 23, 2000, ＜http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html＞(Retrieved on June 19, 2012).

[19] 例如：Süleyman Özeren, "Cyberterrorism and International Cooperation: General Overview of the Available Mechanisms to Facilitate an Overwhelming Task," in Centre of Excellence Defence Against Terrorism, Ankara, Turkey, ed., *Responses to Cyber Terrorism* (Washington, DC: IOS Press, 2008), p.

除了 Denning 之外，Mark M. Pollitt 於 1997 年對網路恐怖主義訂出的操作性定義（working definition），亦時常為其他專家學者引用，[20]其定義為：網路恐怖主義是次國家團體或秘密人員針對資訊（information）、電腦系統、電腦程式和資料（data）有預謀且出於政治動機的攻擊，其目標為非戰鬥人員。[21]Denning 對此加以補充：出於政治動機且造成嚴重損害的攻擊行為，例如經濟困境（economic hardship）或持續的斷電、斷水等，亦應屬於網路恐怖主義之範疇。[22]另外，將美國聯邦法規（U.S. Code）及美國中央情報局（Central Intelligence Agency, CIA）對於恐怖主義之定義，[23]與 Mark M. Pollitt 所做之網路恐怖主義定義相比較可以發現，兩者十分接近，差別僅在於 Pollitt 增加了有關資訊、電腦系統、電腦程式和資料的描述。

一般而言，許多西方國家的政府對於網路恐怖主義之定義，大多採用國際安全與合作中心（Center for International Security and Cooperation, CISAC）在一份名為「網路安全及恐怖主義國際會議提案」（Proposal for an International Convention on Cyber Crime and Terrorism）之文件上所使用的定義：「未經合法權力承認之下，故意使用或威脅使用暴力破壞或擾亂網際網路系統（cyber system），此種行為將可能造成一人或多人死亡或受傷、有形財產的實質毀損、

70; Shilpa Bhatnagar, *Encyclopaedia of Cyber and Computer Hacking*, Vol. 5 (Delhi: Anmol Publications, 2009), p. 1; P. Madhava Soma Sundaram & K. Jaishankar, "Cyber Terrorism: Problems, Perspectives, and Prescription," in Frank Schmalleger & Michael Pittaro, *Crimes of the Internet* (Upper Saddle River, NJ: Pearson Education, 2009), p. 596; Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington: United States Institute of Peace, 2006), p. 153; James F. Pasley, "United States Homeland Security in the Information Age," in Michael Pittaro, ed., *Cybercrime: Current Perspectives from InfoTrac®*, 2nd ed., (Belmont, CA: Wadsworth, 2010), p. 129.

[20] 例如：Maura Conway, "Cyberterrorism and Terrorist 'Use' of the Internet," *First Monday*, Vol. 7, No. 11 (4 November 2002), ＜http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1001/922＞(Retrieved on February 10, 2012); Kevin Curran, Kevin Concannon, & Sean McKeever, "Cyber Terrorism Attacks," in Lech J. Janczewski & Andrew M. Colarik, eds., *Cyber Warfare and Cyber Terrorism* (Hershey, PA: Information Science Reference, 2008), p. 1.

[21] Mark M. Pollitt, "Cyberterrorism: Fact or Fancy?" ＜http://www.cs.georgetown.edu/~denning/infosec/pollitt.html＞(Retrieved on June 19, 2012).

[22] Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in John Arquilla & David Ronfeldt, eds., *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND, 2001), p. 281.

[23] 請參見："U.S. Code Title 22, Ch. 38, Sec. 2656f," p. 920, ＜http://www.gpo.gov/fdsys/pkg/USCODE-2011-title22/pdf/USCODE-2011-title22-chap38-sec2656f.pdf ＞ (Retrieved on July 10, 2012); "Terrorism FAQs," ＜https://www.cia.gov/news-information/cia-the-war-on-terrorism/terrorism-faqs.html＞(Retrieved on June 18, 2012).

社會失序，或是嚴重的經濟損失」。[24]根據這個定義，反面而言，凡是經過國家授權之網路攻擊，便不算是網路恐怖主義，由此可判別網路恐怖主義與網路戰爭之差異。然而，該定義缺乏對於攻擊發動者之政治性或社會性訴求的描述，不容易和一般以個人或所屬團體之利益為動機的網路犯罪行為做出區別。

此外，亦有學者認為，網路恐怖主義即「以網際網路為工具所發動之攻擊行為」，恐怖份子可能入侵電力供應網絡或安全系統，或是散佈極具威力的電腦病毒等，藉以展開恐怖攻擊行動。[25]此可謂十分簡明的定義，網路恐怖主義的基本前提即是以網際網路做為攻擊工具或載體，遂行攻擊者所欲達成之威脅或強迫等目的。然而，各種「以網際網路為工具所發動之攻擊行為」尚可由攻擊動機、攻擊者身分或攻擊行為引發之後果等不同角度，進一步加以細分類別，例如：由網路恐怖份子所發動之網路恐怖攻擊、出於民族情緒等原因而串連攻擊外國網站[26]、因個人利益、商業利益或國家利益而受僱進行之網路間諜（cyber espionage）或網路戰爭（cyber warfare）行為，以及一般駭客或駭客團體出於無聊或惡趣而散佈電腦病毒或惡意程式等等。由此可知，該定義雖十分簡明，然其缺失亦在於過度簡明，若將任何以網際網路為工具所進行之攻擊行為皆涵括在內，便無法精確區別上述幾種不同類型之網路攻擊行為，如此可能導致「一詞多義」的情況。

另一方面，尚有學者提出網路恐怖主義之定義為「非國家行為者為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」。[27]該定義便

---

[24] Andrew Jones, "Cyber Terrorism: Fact or Fiction," *Computer Fraud and Security*, Vol. 2005, Iss. 6, (June 2005), p. 4. 原文引用自：Abraham D. Sofaer, *et al.*, "A Proposal for an International Convention on Cyber Crime and Terrorism," CISAC Report, August 2000, p. 26, ＜http://iis-db.stanford.edu/pubs/11912/sofaergoodman.pdf＞(Retrieved on February 12, 2012).

[25] Eben Kaplan, "Terrorists and the Internet," p. 3, ＜http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005#p6＞(Retrieved on January 31, 2012).

[26] 例如 2001 年 4 月 1 日於南中國海上空發生之「中美撞機事件」，美國海軍一架 EP-3 型偵察機與中國人民解放軍一架殲-8II 型戰鬥機碰撞，中國戰鬥機墜毀，飛行員王偉跳傘，下落不明，後由中國確認死亡，美國軍機則迫降於海南島陵水機場。此事件引發中美兩國外交衝突，並導致雙方國內民族情緒高漲，民間駭客團體相互攻擊或竄改對方政府網頁及各大網站。

[27] 彭慧鸞，「數位時代的國家安全與全球治理」，**問題與研究**，第 43 卷第 6 期（民國 93 年 11、12 月），頁 36。

針對「攻擊者之身分」及「行為動機」提出規範，但是對於攻擊對象是國家軍事部隊及所屬人員，抑或是非戰鬥人員，則沒有進一步細分。

2002 年 3 月，時任美國聯邦調查局反恐／反情報部門副執行助理主任（Deputy Executive Assistant Director, Counterterrorism/Counterintelligence Division, Federal Bureau of Investigation, FBI）的 J. T. Caruso 於國會作證時表示，「網路恐怖主義──基於強迫或威脅政府或人民之目的，使用『網路工具』（cyber tools）導致國家重要基礎設施（能源、運輸或政府機關等）停止運作──已成為一個新興威脅」。[28]而 Gabriel Weimann 所定義的網路恐怖主義亦十分相似：使用「電腦網絡工具」（computer network tools）危害或關閉國家關鍵基礎設施（能源、運輸或政府機關等）。[29]雖然兩者皆未進一步說明何謂「網路工具」或「電腦網絡工具」，卻都明確指出，網路恐怖主義攻擊能使「國家的重要基礎設施停擺」此一嚴重後果。

Clay Wilson 對於網路恐怖主義之定義為：「國際、次國家團體或秘密人員，出於政治性之動機，將電腦做為武器或目標，威脅使用或導致暴力及恐懼，以影響群眾，或迫使政府改變其政策」。並且強調，由於難以完全確定攻擊者的身分、意圖或政治動機，輕易將電腦攻擊視為網路恐怖主義是有問題的做法。其進一步指出，由於任何人皆可透過網際網路，輕易取得有關如何利用電腦程式漏洞的教學文件，加上目前尚缺乏證實國際恐怖組織與大規模網路攻擊有關聯的確切證據，如何確定各種網路攻擊行為的發動者身分，仍然十分困難。但是在此同時，網路安全相關組織卻指出，電腦病毒攻擊日趨頻繁，不僅影響全球許多區域，造成的經濟損失亦越來越嚴重。[30]

---

[28] J. T. Caruso, "Combating Terrorism: Protecting the United States," before the House Subcommittee on National Security, Veterans Affairs, and International Relations, Washington, DC, March 21, 2002, ＜http://www.fbi.gov/news/testimony/combating-terrorism-protecting-the-united-states＞(Retrieved on February 9, 2012).

[29] Gabriel Weimann, "Cyberterrorism: The Sum of All Fears?" *Studies in Conflict & Terrorism*, Vol. 28, Iss. 5 (2005), p. 130.

[30] Clay Wilson, *op. cit.*, pp. 6-8.

Wilson 指出了網路恐怖主義並不等於一般的電腦攻擊，必須以攻擊者的身分、意圖或政治動機等條件來加以認定，即使這可能十分困難。筆者認為，若要對網路恐怖主義進行更清楚的界定，並且與網路犯罪及網路戰爭或資訊戰爭之間做出更明確的區分，或是確定彼此之間的從屬關係，應將著重之焦點增加，包括攻擊者之身份、具政治動機與否，以及攻擊行為之目標等等，盡量將相似概念之間產生混淆的可能性降到最低。

Andrew M. Colarik 則以「次國家團體、秘密人員或個人針對資訊、電腦系統、電腦程式和資料進行有預謀且出於政治動機的犯罪行為，破壞人身安全（physical violence），其目的在於引發非戰鬥人員之恐懼」做為網路恐怖主義之定義。[31]此定義將網路恐怖主義攻擊視為犯罪行為，並強調其對於人身安全之威脅，以及所造成之恐懼。觀察歷年來的恐怖攻擊行動，不論其攻擊手法為何，「引發恐懼」的確是恐怖份子最期盼實現的階段性目的，也是用以逼迫或威脅目標政府或人群服從其意志最有效的工具，然而，倘若網路恐怖份子所攻擊的目標是國家的金融機構，例如干擾金融秩序，或是竊取民眾的帳戶資料、信用卡號碼等等，這類攻擊行為似乎不太可能造成實際的人身安全顧慮，也就是說，人身安全之威脅不一定是必要因素，「引發恐懼」仍是恐怖份子企求的最主要目標。

而在網際網路使用行為之分類方面，Denning 曾將這些行為分為三大類：「Activism」、「Hacktivism」和「Cyberterrorism」，從而將一般以騷擾為目的之駭客攻擊行為與嚴重程度大不相同的網路恐怖主義清楚區分開來。[32]如此的分類方式，不僅廣為學界引用，亦有專家學者特別針對其中某一類型提出專文論述，[33]Denning 所提出的此種分類方式之影響，可謂十分深遠，並且突顯出網路恐怖主義有別於其他網際網路使用行為，應當自成一類的必要。

---

[31] Andrew M. Colarik, *Cyber Terrorism: Political and Economic Implications* (Hershey, PA: Idea Group, 2006), p. 47.

[32] Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," *op. cit.*, p. 241.

[33] 例如：Niranjan Dass, *Globalization of Terror: A Threat to Global Economy* (New Delhi: MD Publications, 2008), Ch. 6 & 7; Andrew M. Colarik, *op. cit.*, Ch. 3; Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington: United States Institute of Peace, 2006), pp.

貳、網路恐怖主義與網路犯罪及網路戰爭之比較

許多專家學者對於網路犯罪皆採較寬鬆之定義，大致上只要是「以電腦及網際網路為工具的犯罪行為」皆屬之。[34]不過，相對於這些較為概括性且模糊之定義，Susan Brenner 則主張，網路犯罪不一定必須以網際網路為工具，僅以一台電腦亦有可能完成網路犯罪，同時尚有某些犯罪行為必須透過網際網路才能完成，應針對網路犯罪和傳統犯罪加以區別。[35]Brenner 亦進一步指出網路犯罪與網路恐怖主義之間的差異，前者係出於個人目的，包括個人私欲、商業利益或是傷害他人之意圖等等，而後者則是出於政治目的，屬於有預謀地引發嚴重破壞，以造成大眾的恐慌，從而傳達其政治訴求之行為。[36]

對於網路戰爭之定義問題，Richard A. Clarke 與 Robert K. Knake 將網路戰爭定義為「一國對於另一國之電腦或網絡的滲透行動，旨在造成損害或破壞」，[37]此定義針對行為者身分及動機提出較為明確的規範，既然戰爭是國家行為者之間的相互行為，網路戰爭自當由國家行為者發動，而不是個人或非國家行為者。相似觀點如 James A. Lewis，其亦主張網路戰爭是為「國家或政治團體出於政治目的使用武力造成損失、破壞或傷亡」。[38]

另一方面，Susan W. Brenner 則認為，網路戰爭是以虛擬方式進行的軍事行動，即國家使用網路空間來達成與使用傳統軍事力量相同的目標。[39]關於網路恐

155-159; Paul A. Taylor & Jan Ll. Harris, "Hacktivism," in Hossein Bidgoli, ed., *Global Perspectives in Information Security: Legal, Social, and International Issues* (Hoboken, NJ: John Wiley & Sons, 2009), pp. 295-317.

[34] 例如：Bernadette H. Schell & Clemens Martin, *Cybercrime: A Reference Handbook* (Santa Barbara, CA: ABC-CLIO, 2004), pp. 2-3; Jeffrey Ian Ross, *Criminal Investigations: Cybercrime* (New York: Chelsea House, 2010), pp. 21-24; Shilpa Bhatnagar, *op. cit.*, Vol. 1, p. 39; Clay Wilson, "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," CRS Report for Congress, p. 4, ＜http://www.fas.org/sgp/crs/terror/RL32114.pdf＞ (Retrieved on February 19, 2012); 馬進保、袁廣林，《**高科技犯罪研究**》（北京：中國人民公安大學出版社，2008），頁 205。

[35] Susan W. Brenner, "'At Light Speed': Attribution and Response to Cybercrime/Terrorism/Warfare," *The Journal of Criminal Law and Criminology*, Vol. 97, No. 2 (Winter, 2007), pp. 382-386.

[36] *Ibid*, pp. 387-389.

[37] Richard A. Clarke & Robert K. Knake, *op. cit.*, p. 6.

[38] James A. Lewis, "Thresholds for Cyberwar," report submitted to the Center for Strategic and International Studies, CSIS, Washington, DC, p. 1, ＜http://csis.org/files/publication/101001_ieee_insert.pdf＞(Retrieved on February 29, 2012).

[39] Susan W. Brenner, "'At Light Speed': Attribution and Response to Cybercrime/Terrorism/Warfare," *op. cit.*, p. 401.

怖主義與網路戰爭之間的區別，Brenner 亦強調，恐怖主義不同於戰爭的最大差異，在於後者所針對的不應該是平民，而是軍事人員及所屬設施等等。[40]由此推論，網路戰爭也不應指涉針對平民及民生設施發動之攻擊，而是屬於網路恐怖主義之範疇。

以上相關文獻皆顯示，若要將網路恐怖主義與其他網際網路使用行為進行區分，以及界定網路恐怖主義、網路犯罪及網路戰爭三個概念相互之差異，必須建立若干判別標準，例如以行為者動機、身分等不同面向判斷等等。透過這些判別標準，始能有效提出網路恐怖主義之明確定義。

參、網路恐怖主義是否為嚴重威脅

除了針對網路恐怖主義如何定義的爭論之外，對於其威脅之程度，專家學者亦有各種看法。例如 Joshua Green 指出，美國軍方指揮系統及關鍵基礎設施之網路防衛機制皆已十分完善，即使恐怖份子能夠入侵系統，由於操作系統需要高度專業知識，難以造成實質破壞。其認為，網路恐怖主義的攻擊效果不若傳統恐怖主義，所需要的資金、知識和籌備時間亦高於後者許多，對於恐怖份子而言，傳統恐怖主義仍是較合理的選擇。Green 進一步主張，網路恐怖主義已受到大眾媒體及有心人士的過度炒作，不論是為了新聞話題性、獲取國家資金挹注，或是個人主導議題的權力等目的，導致美國政府已經投入過多寶貴的資源。[41]

Andrew Jones 亦認為，發動網路恐怖攻擊所需的技術已超出絕大多數的恐怖組織之能力，不必過於強調其威脅性。在 911 事件之後，全世界對於恐怖主義威脅的敏感度已大幅提高，而人類對於網路科技的大量應用和依賴，使得對網際網路的任何干擾都可能引發嚴重影響；這兩個要素結合在一起的結果，便是對於網路恐怖主義潛在威脅的過度反應。

---

[40] *Ibid*, pp. 387-388.
[41] Joshua Green, "The Problem of Cyberterrorism is Exaggerated," in Louise I. Gerdes, ed., *Cyber Crime* (Farmington Hills, MI: Greenhaven Press, 2009), pp. 49-50.

相較於 Joshua Green 針對軍方的網路安全措施給予甚高之評價，Richard A. Clarke 和 Robert K. Knake 則提出質疑，他們以 2008 年國防部機密系統遭電腦病毒入侵之事件為例，指出電腦病毒即使不透過網際網路，仍可利用使用者不經意的疏忽侵襲目標系統，安全機制不僅包含各項軟硬體的適當配置與維護，還應該考慮到使用者的因素。[42]

不僅如此，主張網路恐怖主義確實可能對國家安全帶來威脅的學者們亦指出，目前網路恐怖份子發動攻擊的可能性或許偏低，然而其潛在威脅仍不能不加以重視。例如依據 Simon Finch 之觀察，恐怖份子已開始重視網路恐怖主義之潛力。[43]Dorothy E. Denning 也認為，電腦駭客可能會與恐怖組織合作，如此一來恐將引發嚴重後果，而新世代的恐怖份子自幼即在數位時代中成長，這群人將更加熟悉網際網路的操作知識，並且能夠看出網路恐怖主義所具有的極大潛力，其威脅已非昔日可比擬。[44]

此外，尚有若干專家學者認為，由於近年來網路科技的迅速發展與廣泛應用，各項關鍵基礎設施相互之間的連結性與互賴性已經大幅提高，管理人員的監控和操作亦更加方便，同時卻也使得這些關鍵基礎設施面對網路攻擊威脅的防衛能力隨之下降。[45]

---

[42] Richard A. Clarke & Robert K. Knake, *op. cit.*, pp.171-172.
[43] Simon Finch, *op. cit.*, p. 37.
[44] Dorothy E. Denning, "Is Cyber Terror Next?" ＜http://essays.ssrc.org/sept11/essays/denning.htm＞ (Retrieved on June 30, 2012).
[45] 例如：Yacov Y. Haimes, "Risk of Terrorism to Cyber-Physical and Organizational-Societal Infrastructures," *Public Works Management & Policy*, *Vol. 6, No. 4 (April 2002)*, p. 232; James A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," *op. cit.*, p. 11; Gordon M. Snow, "Cybersecurity: Responding to the Threat of Cyber Crime and Terrorism," statement before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism, Washington, DC, April 12, 2011, ＜http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism＞(Retrieved on June 4, 2012).

肆、美國政府防治政策

觀察諸多美國政府之公開文件可知，自柯林頓（Bill Clinton）時期開始，美國政府逐漸重視境內恐怖主義針對國家安全的威脅。[46]隨著網路科技的快速發展，各項維繫美國經濟、民生、社會與國防等各層面運作之關鍵基礎設施，對於網際網路的依賴程度亦與日俱增，因此，網路空間安全與國家安全之間的關係，也逐漸形成緊密連結。[47]

有鑑於此，柯林頓總統及小布希總統陸續頒布多項重大政策及總統指令，要求相關之聯邦部門密切配合，並且與負責營運眾多關鍵基礎設施的私部門展開對話、協調，並相互分享資訊，以共同保障關鍵基礎設施之安全。[48]

911 事件發生後，小布希政府大幅提高對於反恐相關事務的重視程度，除了成立國土安全部（Department of Homeland Security, DHS）之外，亦頒布「網路空間安全國家戰略」（National Strategy to Secure Cyberspace），將網路安全議題提升至國家戰略層次。以該戰略之架構為基礎，小布希政府頒布多項相關政策，將維護各項關鍵基礎設施安全之職責，詳細分派給有關的聯邦部門，同時也確立國土安全部在整體政策框架之中心角色。[49]

到了歐巴馬政府上台之後，大致維持前任政府之政策路線，強調全國性與全球性的共同合作，協力降低網路恐怖主義對於各國之威脅。[50]在此同時，歐巴馬

---

[46] "President Decision Directives 39: U.S. Policy on Counterterrorism," ＜http://www.fas.org/irp/offdocs/pdd39.htm＞(Retrieved on June 17, 2012).

[47] "Executive Order 13010, EO 13010: Critical Infrastructure Protection, July 15, 1996," ＜http://www.fas.org/irp/offdocs/eo13010.htm＞(Retrieved on June 17, 2012).

[48] 例如："Executive Order 13010, EO 13010: Critical Infrastructure Protection, July 15, 1996," ＜http://www.fas.org/irp/offdocs/eo13010.htm＞(Retrieved on June 17, 2012); "President Decision Directives 63: Critical Infrastructure Protection," ＜http://www.fas.org/irp/offdocs/pdd/pdd-63.htm＞(Retrieved on June 17, 2012); "National Strategy to Secure Cyberspace," ＜http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf＞(Retrieved on June 27, 2012).

[49] "National Strategy to Secure Cyberspace," pp. ix-x, ＜http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf＞(Retrieved on June 27, 2012).

[50] John D. Moteff, "Critical Infrastructures: Background, Policy, and Implementation," CRS report for Congress, p. 12, ＜http://www.fas.org/sgp/crs/homesec/RL30153.pdf＞(Retrieved on June 30, 2012).

政府亦十分重視提升國內民眾對於保護國家關鍵基礎設施的安全意識，並且定期執行相關的演習行動與宣導措施。

經由爬梳上述文獻發現，目前網路恐怖主義之定義仍顯模糊，對於威脅是否真實存在之看法，論述亦相當分歧，認為言過其實者有之，主張重視威脅者亦有之。即使如此，本論文嘗試建立判別網路恐怖主義之界定標準，據以釐清網路恐怖主義之定義，並且評估網路恐怖主義的真實威脅性。此外，在美國政府的防治政策架構方面，經過一系列的政策調整，相關聯邦部門的角色和職責劃分已然明確，根本之政策方向亦十分清晰：美國正力求徹底防止網路恐怖主義的攻擊，以保護關鍵基礎設施的正常運作。

第三節　問題意識

綜觀上述之研究緣起與文獻回顧可知，當前各界對於網路恐怖主義之界定與威脅之嚴重程度，仍未取得共識。面對如此的爭辯情況，美國政府如何擬定相關對策，保護國內各項關鍵基礎設施？由此，本論文之問題意識如下：

1. 恐怖主義與網路科技的結合，產生了網路恐怖主義，但是其定義如同傳統恐怖主義一般，眾說紛紜，莫衷一是，是否可能整理出一個較為完善且全面的定義？
2. 透過檢視相關討論、爭議與著述等文獻資料，比較並分析其中的爭議焦點，嘗試探討若干專家學者為何主張網路恐怖主義之威脅被過分誇大？其主要論據為何？網路恐怖主義對於國家安全是否已構成嚴重威脅？
3. 將美國的反恐政策做為研究主軸，著重在網路恐怖主義此一面向，以美國政府公布的各項文件與資料為背景，試圖分析美國目前對於反制網路恐怖主義方面，如何保護國內各項關鍵基礎設施？其基本策略與政策發展情況為何？是否具有一貫之政策路線？

透過問題意識之釐清，便可在研究過程之中，經由閱讀專家學者的相關著述，逐步了解網路恐怖主義的真實樣貌，並對照美國防治網路恐怖主義之政策，最終能夠對該政策形塑出一個較為客觀之評價。

第四節　研究方法與研究範圍

壹、研究方法

本論文以美國防治網路恐怖主義之政策為個案研究對象，透過文獻分析法，從事相關資料的閱讀與整理，首先探討網路恐怖主義之定義，參照眾多專家學者各自提出之意見，並且經由與電腦犯罪、網路犯罪及網路戰爭三個概念之間的相互比較，找出彼此之異同，從而界定網路恐怖主義之定義。

在形塑出定義之後，針對網路恐怖主義是否為一個真實威脅的爭辯現象，進行分析和比較，經由閱讀文獻之過程，找尋主要的爭議焦點，並且嘗試提出筆者的主觀意見。接著，以美國防治網路恐怖主義之政策為關注焦點，研究其發展趨勢和著重之面向，嘗試提出客觀之評價。

此外，本論文亦運用歷史分析法，針對美國防治網路恐怖主義之政策，由政策路線之歷史進程，觀察其演變脈絡及趨勢，以及 911 事件所造成之影響，嘗試分析美國政府相關政策架構之發展，並探討其是否具有一貫之政策思維。

在文獻資料的選擇方面，以中文及英文資料為主，其中包括專書著述、期刊文章、政府出版品、政府首長之公開發言及聽證會紀錄、新聞媒體報導，以及網頁資訊等等。關於詞彙之定義問題，除了眾多專家學者各自的主張以外，亦參考聯合國、美國政府及軍方等機構所提供之相關定義，包括聯邦法規及各單位之資料等。而在引用及繪製圖表的部分，則以政府公布的資料為主，強調準確性、客觀性與公信力。

貳、研究範圍

在議題範圍的界定上，本論文以「干擾或中斷關鍵基礎設施正常運作，意圖造成大眾生活不便或立即危害之網路恐怖主義活動」為研究議題，包括以駭客手法入侵水壩、核能發電廠或交通管制中心之控制中樞，蓄意造成擾亂未預警之洩洪、核能災害或交通秩序大亂等後果之恐怖主義行為等等。至於一般駭客出於惡作劇、挑戰技術或個人利益等動機，對於各個網站發動之騷擾或攻擊行為、盜用個人身份，以及透過網際網路竊取公私部門之內部資訊及其他商業機密等行為，若非必要，皆不在本論文研究範圍之內。

即使網路恐怖主義可歸類於網路犯罪行為之一類，但是本論文之研究重點仍將聚焦在網路恐怖主義及美國防治政策兩大面向，為了比較網路恐怖主義與網路犯罪的相互異同，必須提及有關電腦犯罪及網路犯罪之討論與研究。除此之外，若無重要關聯性，相關研究即排除在本論文所欲處理的議題領域以外。

在年代切割的選擇方面，雖然早在 2001 年 911 事件發生之前，美國政府已開始察覺網路恐怖主義的潛在威脅，學界亦有相關討論出現，但是直到 911 事件發生之後，美國政府才大幅度地加強其國內反恐政策，其中也包括防治網路恐怖主義的部分，因此本論文研究議題之時間尺度，除了針對 911 事件之前相關政策的分析之外，仍將以 2001 年至目前（2012 年 7 月）為研究重點。

第五節　章節安排

本論文共分為五章，第一章為「緒論」，各小節依序闡述研究緣起、回顧並探討相關文獻資料，以進行要點整理、提出問題意識、說明研究方法並界定研究範圍，以及條列本論文之章節安排。

第二章為「網路恐怖主義之界定」，首先探討網路恐怖主義與傳統恐怖主義之間的異同，根據分析重要學者對於各種網際網路使用行為之分類方式，建立網

路恐怖主義之判別標準，並嘗試提出本論文之定義；進而以各個判別標準為基礎，比較網路恐怖主義與網路犯罪及網路戰爭之間有何異同，相互關係為何。再以 2007 年 4 月愛沙尼亞（Estonia）發生之大規模網路攻擊事件為例，闡述網路恐怖主義對於國家安全之威脅程度，何以值得政府特別重視。

第三章為「網路恐怖主義威脅之爭辯」，著重於觀察當前眾多專家學者對於網路恐怖主義威脅存在與否之爭辯情況，分析他們各自提出之正反論據，找尋主要爭議點所在，從中嘗試建立筆者之意見，以評估網路恐怖主義確切之威脅性。

第四章為「美國防治網路恐怖主義政策」，以 2001 年 911 事件與 2003 年美國政府頒布「網路空間安全國家戰略」做為兩個時間分界點，分析美國政府防治網路恐怖主義一系列政策之發展，探討其如何組織防治體系，相關各部門的權責分配情形，以及歐巴馬政府目前之政策概況。

第五章為「結論與展望」，主要總結各章之研究結果，討論研究發現，並嘗試針對美國防治網路恐怖主義政策進行評價。除此之外，亦說明本論文在寫作過程中曾遭遇之侷限與困難，並展望未來研究之可能發展，期盼能為往後相關研究提供一些論述基礎。

國立政治大學 National Chengchi University

第二章　網路恐怖主義之界定

在研究網路恐怖主義的威脅以及美國防治網路恐怖主義相關政策之前，應先了解「網路恐怖主義」此一概念之意涵。即使目前各界對網路恐怖主義的定義尚無普遍共識，但是經由統整各種觀點，歸納出數個重要的判別標準，並且透過這些標準，試圖提出一個明確的定義，避免與其他概念發生混淆。

因此，本章以既有文獻為基礎，首先對於「恐怖主義」一詞進行初步了解，再以恐怖主義之定義為基礎，界定本論文在提及「網路恐怖主義」此一名詞時所指涉之概念。再者，由於「網路犯罪」及「網路戰爭」相關活動經常被誤解為網路恐怖主義，本章亦將進一步比較分析三者之間的關聯及異同。此外，一旦爆發大規模的網路恐怖主義攻擊，可能導致的災情為何？由於目前尚未出現網路恐怖主義攻擊的真實案例，故選擇性質較為相似之事件，即 2007 年 4 月愛沙尼亞遭受大規模網路攻擊一例，做為個案研究對象，藉以討論該事件對於國家防治網路恐怖主義攻擊，有何值得參考與借鏡之處。

第一節　網路恐怖主義之定義

許多專家學者皆曾提及，「Cyberterrorism」一詞是由 Barry Collin 在 1980 年代所創，用以指涉網路空間與恐怖主義之結合。[1]即使 Collin 所提出的只是一個初始的概念，並未進一步明確界定，不過，搜尋國內外文獻，眾多專家學者縱然因立場或焦點之差異，對於網路恐怖主義做出各有異同的定義，但是目前似乎尚無其他定義超出這樣的範疇。

[1] 例如：Dorothy E. Denning, “Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy,” *op. cit.*, p. 281; Niranjan Dass, *op. cit.*, p. 159; Maura Conway, “Cyberterrorism and Terrorist ‘Use’ of the Internet,” *op. cit*.

然而，如此的描述仍然不夠明確，尚需更加精準的界定。以恐怖主義而言，過於廣泛的定義可能會造成各種普通的犯罪行為、蓄意破壞和駭客活動都被視為恐怖主義，使得「恐怖主義」此一概念變得沒有意義；相對地，過於狹隘的定義，則可能會遺漏許多恐怖主義活動。[2]過猶不及，皆有可能造成政府在反恐政策之制訂面與執行面的失準。

有鑑於此，為了避免過於廣泛或狹隘地界定網路恐怖主義，本章由傳統恐怖主義之定義出發，首先了解何謂恐怖主義，以及某些特定活動被視為恐怖主義之原因，再探討傳統恐怖主義與網路恐怖主義之間的異同，以對於網路恐怖主義形成更精確的界定，做為立論分析之基礎，從而避免在行文當中出現敘述模糊或語意不清的情況。

壹、恐怖主義

「恐怖主義」之概念，多用以指稱個人或團體出於政治性、社會性或宗教性目的，以非武裝的平民百姓或不特定的人員為目標，有計畫地使用暴力或威脅使用暴力，企圖引發大眾的恐慌和關注，以達到其訴求或目的。以下分別統整恐怖主義之定義，以及網路恐怖主義與傳統恐怖主義之間的共同特徵：

一、定義

即使恐怖主義之相關研究並非新興領域，眾多專家學者對於恐怖主義的定義卻仍然莫衷一是，國際社會亦缺乏共識，甚至美國政府各部門對其之定義也多少有所出入。舉例而言，聯合國安全理事會（United Nations Security Council, UNSC）於 2004 年 10 月通過第 1566 號決議，將恐怖主義定義為：「〔一種〕犯罪行為，包括故意造成平民死亡或重傷，或劫持人質，其目的在於在一般民眾、某一群人

[2] Charles Jaeger, “Cyberterrorism,” in Hossein Bidgoli, ed., *The Internet Encyclopedia*, Vol. 1 (New York: John Wiley & Sons, 2003), p. 353.

或特定的人群之中挑起恐怖之狀態，以恐嚇群眾或迫使一國政府或國際組織從事或不從事行為。此類活動包含於國際公約和議定書對於恐怖主義所界定的犯罪行為範圍之內，在任何情況下都不能以政治、哲學、意識形態、種族、民族、宗教或其他類似性質之理由，予以正當化。」[3]

美國聯邦法規針對「恐怖主義」一詞做出明確的法律定義，其為「由次國家團體（sub-national groups）或秘密人員（clandestine agents）所為，有預謀（premeditated）、出於政治動機且針對非戰鬥人員（noncombatant）之暴力行為」。[4]此定義亦為美國中央情報局所採用。[5]

美國聯邦調查局對恐怖主義的定義則為：「對個人或財產非法使用武力和暴力，意圖威脅（intimidate）或強迫（coerce）一國政府、全體人民或其中部分人群，以達成政治性或社會性之目的」。[6]而美國國防部（Department of Defense, DOD）所賦予之定義為：「非法使用暴力或以暴力相威脅，以灌輸恐懼，並且強迫政府或社會。恐怖主義大多出於宗教、政治或其他意識型態之信仰等動機，通常是為了追求政治性目標。」[7]

綜合上述各種定義，恐怖主義是一種計畫性的暴力行為，並以無辜的平民為攻擊對象。此外，恐怖主義的策略是在大眾之中製造恐懼，藉此迫使有關當局做出符合其要求的改變，其目的是希望這種無法預期的暴力行為會在一般大眾的心理上造成陰影，以產生「恐怖」的不安全感。因此，恐怖主義常會藉助媒體來宣傳其活動及主張，以擴大其效果。[8]

---

[3] "United Nations Security Council Resolution 1566, October 2004," p. 2, <http://daccess-ods.un.org/access.nsf/Get?Open&DS=S/RES/1566%20(2004)&Lang=E&Area=UNDOC>(Retrieved on June 18, 2012).

[4] 請參見："U.S. Code Title 22, Ch. 38, Sec. 2656f," p. 920, <http://www.gpo.gov/fdsys/pkg/USCODE-2011-title22/pdf/USCODE-2011-title22-chap38-sec2656f.pdf > (Retrieved on July 10, 2012).

[5] "Terrorism FAQs," <https://www.cia.gov/news-information/cia-the-war-on-terrorism/terrorism-faqs.html>(Retrieved on June 18, 2012).

[6] "Terrorism 2002-2005," p. iv, <http://www.fbi.gov/stats-services/publications/terrorism-2002-2005/terror02_05.pdf>(Retrieved on June 18, 2012).

[7] "Department of Defense Dictionary of Military and Associated Terms," p. 368, <http://ra.defense.gov/documents/rtm/jp1_02.pdf>(Retrieved on June 13, 2012).

[8] 方天賜、孫國祥，「民族主義與恐怖主義」，收於張亞中主編，《**國際關係總論**》，二版（臺北：

二、與網路恐怖主義之間的共同特徵

在網路恐怖主義與傳統恐怖主義之間的關聯性方面，P. Madhava Soma Sundaram 和 K. Jaishankar 指出，即使網路恐怖攻擊是發生於網路空間，但是其與傳統恐怖主義活動依然具有四項共同特徵：

1. 有預謀且並非單純出於憤怒（not simply acts born of rage）：網路恐怖攻擊是有預謀的，網路恐怖份子從撰寫或取得發動攻擊所需要之軟體開始，其行為就是有計劃性的，也不是僅為了宣洩不滿情緒的隨機攻擊。
2. 出於政治動機，且企圖影響政治結構（to impact political structure）：網路恐怖份子是具有政治動機的駭客，透過破壞或摧毀電腦系統，達成其影響政治結構之目的。
3. 以平民及民間設施（civilian installations）為目標：網路恐怖攻擊針對的是平民或財產，旨在造成足以引發恐懼的損失。
4. 由不屬於國家軍隊之特定團體所發動：網路恐怖主義不同於網路戰爭或資訊戰爭，後兩者是由國家所屬人員發動。[9]

綜觀以上幾種定義與共同特徵可知，網路恐怖主義與傳統恐怖主義皆是「有預謀且出於政治動機」之攻擊行動，由「次國家團體或秘密人員」所為，攻擊對象為「非戰鬥人員及民間設施」，行為者具有「政治性或社會性目標」，並以各自的方式「引發恐懼，並恐嚇或脅迫政府或社會」，兩者在這幾個面向，顯然十分接近。

然而，以網際網路為犯罪工具的網路恐怖份子（cyberterrorist），並非透過使用實際武力發動攻擊，而是經由網際網路散佈電腦病毒、在目標電腦或網絡內部植入後門程式或惡意程式（malware）、找出程式安全漏洞以取得管理權限等等方式，以達到破壞、控制、盜取或干擾等目的。因此，即使網路恐怖主義是恐怖主

揚智，2007），頁 207-208。

[9] P. Madhava Soma Sundaram & K. Jaishankar, *op. cit.*, p. 596.

義與電腦及網路科技之間相互結合之後的產物，兩者仍有不同之處，有必要對其進行精確定義。

貳、網路恐怖主義

如同對於恐怖主義之定義多所分歧一般，在諸多研究網路恐怖主義的文獻當中，專家學者們對於「網路恐怖主義」此一概念之定義，也紛紛提出各自的不同看法。除了對於定義無法取得共識之外，某些專家學者將恐怖份子在網路空間的各種活動皆視為網路恐怖主義，如此的觀點有何缺失，亦是本小節所欲探討之問題。此外，即使眾多專家學者對於網路恐怖主義所提出的定義各不相同，但是觀察他們著重的主要焦點，仍集中在「攻擊者之身分」、「行為動機」、「攻擊目標」、「行為目的」以及「影響所及範圍」等五個重要面向。將這五大面向視為判別標準，便能夠針對網路恐怖主義形成更加清楚明確之界定。

以下首先探討網路恐怖主義缺乏明確定義之原因，接著透過分析專家學者對於各種網際網路使用行為之分類方式，說明為何不應將恐怖份子使用網際網路的各種活動皆視為網路恐怖主義，同時以受到廣泛引用之學者定義為基礎，逐步歸納出網路恐怖主義的五大重要判別標準，並建立網路恐怖主義之定義。

一、網路恐怖主義為何缺乏明確定義？

首先，在「恐怖主義」尚且缺乏一個廣為各界接受之界定方式的情況下，網路恐怖主義既為恐怖主義的新型態之一，同時亦與傳統恐怖主義之間具有諸多共同特徵，自然也會在定義部分受到恐怖主義之影響，不易形成一個清晰且精確的界定，Marc D. Goodman 便曾提出過類似觀點。[10]

[10] Marc D. Goodman, "Understanding International 'Cyberterrorism': A Law Enforcement Perspective," in Cecilia S. Gal, Paul B. Kantor, & Bracha Shapira, eds., *Security Informatics and Terrorism: Patrolling the Web* (Washington, DC: IOS Press, 2008), p. 11.

另一方面，Gabriel Weimann 觀察當前社會使用「網路恐怖主義」一詞之情況，提出不同見解，並且將各界眾說紛紜的現象，歸因於兩個因素：

1. 大眾媒體經常從事並主導針對網路恐怖主義的相關討論，然而新聞記者傾向將焦點放在議題的戲劇性和轟動性，而不是為一個新名詞形塑良好的操作性定義（good operational definition）之上，這對於社會大眾建立對網路恐怖主義的正確認知而言，十分不利。
2. 每當處理到有關電腦方面的議題，便直接在字彙前面加上「cyber」、「computer」或「information」以組成新字，如此現象已經越來越普遍，導致如「cybercrime」、「infowar」、「netwar」、「cyberterrorism」、「cyberattack」、「digital terrorism」、「cybertactics」或是「computer warfare」等等眾多新興詞彙的出現，然而它們所指涉的內容，卻常常只是一般軍事和政治戰略家在討論的「新型恐怖主義」（new terrorism）而已。[11]

如同 Weimann 對於大眾媒體之批評，亦有學者亦主張，政府機關和大眾媒體經常濫用「網路恐怖主義」一詞，誤將網際網路上散佈色情資訊、發表激進言論、竄改網頁、盜取或張貼信用卡資料，或是秘密將網際網路流量（Internet traffic）自動重新導向其他網頁等各種行為，皆視為網路恐怖主義。然而事實上，這些行為皆不包括在網路恐怖主義的定義範疇之內。[12]

而在法律規範層面，有學者提到，由於美國法律多採判例法（case law），除非法律條文做出新的修正，否則法院判決通常會遵循先前判例。雖然網路恐怖主義之法律定義會隨著判例法一同演進，但是各種新型態的威脅和其他未曾在判例中出現的網路活動，將會使得網路恐怖主義的法律定義更加複雜。傳統上，法律所處理的是在時間和空間中發生的各種行為，然而，即使網路活動可能在時間和空間中造成實質影響，但是某些造成實質影響的因素卻只存在於網路空間，並獨

[11] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, DC: United States Institute of Peace, 2006), p. 153.
[12] Maura Conway, "What Is Cyberterrorism?" *Current History*, Vol. 101, No. 659 (December 2002), p. 436.

立於時間和空間之外。因此，對於網路恐怖主義，如何發展出一個適切可行的法律定義，可能還需要不少時間。[13]

由此觀察應當如何界定網路恐怖主義之問題，網路恐怖主義不僅承襲傳統恐怖主義長久以來缺乏明確定義的先天因素，加上政府機關和大眾媒體對於網路恐怖主義的不解及誤用，以及專家學者為求方便行事而隨意創造新詞彙等現象，亦造成網路恐怖主義的定義更加模糊不清。在此同時，由於網路科技持續快速變動之特性，法律規範明顯跟不上網路科技發展的速度，因而對於網路恐怖主義尚無法給予精確定義。上述種種情況，除了說明網路恐怖主義在定義上所遭遇之困境，亦突顯出為網路恐怖主義界定出一個清楚明確的定義之必要性。

二、網際網路使用行為之分類

現代資訊科技快速發展，人類對於網際網路的依賴亦與日俱增，當今人們利用網際網路所從事的各種活動類型，早已多不勝數。對於各式各樣的網際網路使用行為，專家學者也提出不同之分類方式，其中主要有以下三種類型：

（一）、「網路策劃」（Cyberplanning）與網路恐怖主義

Timothy L. Thomas 指出，近年來的反恐行動已查扣不少恐怖份子所使用之電腦設備，透過分析這些電腦設備，可發現恐怖份子開始利用網際網路進行搜集資料、宣傳理念、籌措金援、交換情報、遙控指揮、組織動員、招募新血及隱匿行蹤等活動的明確證據，Thomas 將此類活動統稱為「網路策劃」。[14]

另一方面，有部分學者則將恐怖份子在網路空間的所有活動，一概視為網路恐怖主義，例如 Marc D. Goodman 將網路恐怖主義之意涵分為兩大類，一類為「激

[13] Charles Jaeger, "Cyberterrorism and Information Security," in Hossein Bidgoli, ed., *Global Perspectives in Information Security: Legal, Social, and International Issues* (Hoboken, NJ: John Wiley & Sons, 2009), pp. 136-138.
[14] Timothy L. Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning'," *Parameters*, Vol. 33, No. 1 (Spring 2003), p. 122.

進恐怖份子組織在網路空間的各種活動」，包括透過網際網路進行宣傳、鼓動和募款等「支援性活動」（support activities），以及人員培訓、交換資訊、研究及籌劃攻擊，與威脅恐嚇等「操作性活動」（operatinal activities）；另一類為「利用電腦網絡（computer networks）攻擊國家的重要資訊基礎設施」，即透過電腦、電腦網絡及網際網路攻擊與一般民眾日常生活息息相關的各項基礎設施，包括大眾運輸系統、政府訊息溝通系統、銀行及金融機構等等。[15]

然而，Gabriel Weimann 持相反意見，主張：「網路犯罪行為與網路恐怖主義並不完全相同，恐怖份子利用電腦做為恐怖活動之輔助工具，無論是為了宣傳、徵募新血、資料探勘（data mining）[16]、通訊或其他目的，根本不能算是網路恐怖主義。」由此可知，網路犯罪與網路恐怖主義之間，可能存在部分重疊。比較 Timothy L. Thomas 與 Weimman 的分類方式，兩者對於網路恐怖主義皆採取較為精確嚴格之定義，恐怖份子在網路空間所從事的這些活動，不應直接等同於網路恐怖主義。而兩者之差別在於 Weimann 僅將這些活動視為網路犯罪，並未另行歸類。[17]

觀察 Marc D. Goodman 第一類定義之焦點，著重於恐怖攻擊行動的「事前準備」，這部分近似於 Thomas 提出之「網路策劃」。然而，由於「以網際網路為工具」已是目前恐怖主義活動之趨勢，縱使傳統恐怖主義份子不以重要基礎設施為目標，也可能利用網際網路做為宣傳、溝通及籌劃等工作之平台。若將「網路策劃」視為網路恐怖主義，有可能使得傳統恐怖主義與網路恐怖主義之間的區別更加模糊。況且，屬於「網路策劃」的各種行為，其目的並非故意造成嚴重破壞和引發群眾恐懼，理應不能視為恐怖主義活動，遑論網路恐怖主義。

---

[15] Marc D. Goodman, *op. cit.*, pp. 11-13.

[16] 意指針對恐怖攻擊之預定目標，如交通設施、核能發電廠、機場、港口，甚至反恐措施、病疫防治或貨幣流通等體系，預先蒐集大量相關資料，加以分類、排序、運算，以得到特定屬性之資訊。參見：黃秋龍，《**兩岸總體安全下的非傳統威脅**》（臺北：法務部調查局展望與探索雜誌社，2010），頁 140；原文引用自：Gabriel Weimann, "How Modern Terrorism Uses the Internet," *The Journal of International Security Affairs*, No. 8 (Spring 2005), pp. 5-6.

[17] Gabriel Weimann, "Cyberterrorism: The Sum of All Fears?" *op. cit.*, pp. 132-133.

早在電腦及網路科技問世之前，恐怖份子從事的各種宣傳、招募、通訊或搜集情報等活動便存在已久，網際網路只是提供了一個相對廉價、方便、迅速且隱匿性高的良好媒介。恐怖份子若不使用網際網路，仍然擁有電話或信件等其他通訊方式可供選擇，也同樣能夠達成上述活動之目的。在傳統形式的各種恐怖攻擊行為當中，例如炸彈、綁架、暗殺或劫機等，網際網路並未扮演關鍵性的角色，甚至可能完全沒有參與。恐怖份子即使利用網際網路進行諸如宣傳、募款或溝通等活動，仍不應該僅僅由於選擇較先進的方式，就被視為網路恐怖份子，這是因為他們最終選擇的不一定是發動網路攻擊。

由上述討論可知，網路恐怖主義應指涉「以網路攻擊為攻擊關鍵基礎設施之手段」的恐怖主義活動，不應與 Thomas 提出之「網路策劃」相互混淆。因此，要判定恐怖攻擊事件是否為網路恐怖主義，「**網路攻擊手段**」便成為明確的判斷標準。

至於 Goodman 第二類之定義，即「利用電腦網絡攻擊國家的重要資訊基礎設施」，可能較符合網路恐怖主義之意涵，即攻擊手段為「以網際網路為工具」，攻擊目標為「重要基礎設施」之恐怖攻擊行為。不僅如此，所謂「重要基礎設施」亦不應限於「資訊設施」，諸如水壩、核能發電廠、輸油管線等設施，亦可能遭到網路恐怖攻擊。

（二）、「Activism」、「Hacktivism」與「Cyberterrorism」

Dorothy E. Denning 將網際網路使用行為分為三大類：「Activism」、「Hacktivism」和「Cyberterrorism」。其中 Activism 為正常使用網際網路的情況，以討論議題、架設網站、分享資訊、收發電子郵件，或是對決策者進行遊說等活動為主，同時也包括駭客發行電子雜誌以討論程式漏洞與散播軟體工具，以及恐怖份子利用網際網路進行宣傳等活動；Hacktivism 為有意干擾目標網站之正常運

作，但無意引發嚴重破壞的行為，例如封鎖網站、電子郵件炸彈[18]、入侵電腦系統，以及電腦病毒或蠕蟲等；Cyberterrorism 為出於政治動機，有意造成重大的災害，並使他人喪失生命，或導致嚴重的經濟損失之行為，例如入侵空中交通管制系統，誤導兩架班機相撞等等。[19]

許多專家學者皆採用 Denning 的分類方式，以此做進一步發展其論述之基礎，或是發表專文進行深入討論。[20]根據這個分類方式，恐怖份子利用網際網路進行 Marc D. Goodman 所謂的「支援性活動」和「操作性活動」，或是 Timothy L. Thomas 指稱之「網路策劃」行為，例如人員培訓或交換資訊等，皆應視為 Activism，而不是 Cyberterrorism。換言之，Denning 的分類方式提供了「網路策劃」不屬於網路恐怖主義之有力論據。

（三）、「Use」、「Misuse」及「Offensive use」

不同於 Denning 之分類，Kent Anderson 則將網際網路的使用行為分為「Use」、「Misuse」和「Offensive use」三大類：Use 為正常且合法的網路活動，即透過電子郵件、新聞群組（newsgroups）和網頁等等，進行相互通訊，絕大部分的此類活動皆屬於單純的言論自由（free speech）；Misuse 之使用者不只發表想法，更採取擾亂或其他方式損害其他網站，例如發動「拒絕服務攻擊」（denial-of-service or DoS attack）[21]，或是為了表達抗議訴求而故意破壞網頁的

---

[18] 網際網路匿名攻擊的形式之一，由一台或多台電腦向一個或多個電子郵件地址不斷發送大量電子郵件，不僅造成受害者的電子郵件信箱容量爆滿，亦會佔用大量網路頻寬，導致網路塞車，影響許多網路用戶的正常工作。

[19] Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," *op. cit.*, p. 241.

[20] 例如：Niranjan Dass, *op. cit.*, Ch. 6 & 7; Andrew M. *op. cit.*, Ch. 3; Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, DC: United States Institute of Peace, 2006), pp. 155-159; Paul A. Taylor & Jan Ll. Harris, *op. cit.*, pp. 295-317.

[21] 拒絕服務攻擊（DoS attack）的基本方式為針對特定的遠端網頁伺服器，傳送大量或特殊的網路封包，造成伺服器資源耗盡或服務中止的狀況，破壞其正常運行。而「分散式拒絕服務攻擊」（distributed denial-of-service attack, DDoS）則是先控制其他受害電腦，組成「殭屍網絡」（botnet），再對目標伺服器發動 DoS 攻擊。關於 DDoS 之介紹，可參見：Paul Robichaux, "Distributed Denial-of-Service Attacks and You," ＜http://technet.microsoft.com/en-us/library/cc722931.aspx＞ (Retrieved on June 26, 2012); 「botnet」一字係由「robot」和「network」合併而成，可參見：Ron Rhodes, *op. cit.*, p. 34.

駭客行為等等；Offensive use 為導致實際傷害、破壞或竊盜等行為的各種活動，例如竊取個人資料等等。[22]

Charles Jaeger 比較 Kent Anderson 及 Dorothy E. Denning 各自的分類方式之後指出，「Use」近似於「Activism」，「Misuse」則近似於「Hacktivism」，而一部分的「Offensive use」可能屬於「Cyberterrorism」。[23]在 Anderson 所提出的分類基礎上，Jaeger 再做出進一步的劃分，並加入網路犯罪及網路恐怖主義兩個概念。各種網際網路活動之間的鑲嵌關係，如圖 2-1 所示：

國立政治大學 National Chengchi University

[22] 引用自：Maura Conway, "Cyberterrorism and Terrorist 'Use' of the Internet," *op. cit*.
[23] Charles Jaeger, *op. Cit.*, p. 142.

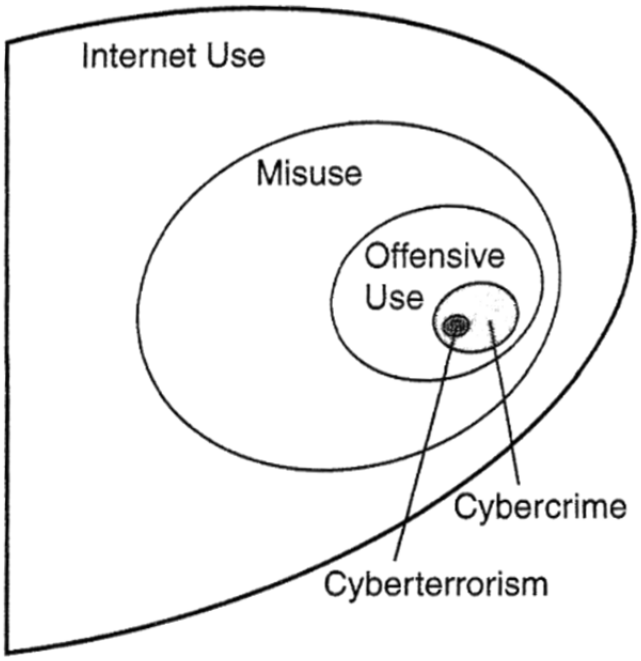

圖 2-1　網際網路活動類型鑲嵌關係圖

資料來源：Charles Jaeger, “Cyberterrorism and Information Security” in Hossein Bidgoli, ed., *Global Perspectives in Information Security: Legal, Social, and International Issues* (Hoboken, NJ: John Wiley & Sons, 2009), p. 142.

Jaeger 將網路恐怖主義包含於網路犯罪之中，兩者皆屬於「Offensive use」。換言之，被歸類為網路恐怖主義之網際網路活動，必須導致實際傷害或破壞效果，如此觀點亦可做為「網路策劃」不屬於網路恐怖主義的另一例證。

綜觀上述，「**網路攻擊手段**」可做為傳統恐怖主義與網路恐怖主義之間的判別標準。而根據以上眾多學者之觀點及分類方式，在恐怖份子使用網際網路的各種行為之中，「網路策劃」亦應排除於網路恐怖主義範疇以外。

三、網路恐怖主義之判別標準

在包羅萬象的網際網路使用行為之中，如何判斷某些行為屬於網路恐怖主義？顯然必須建立若干足以做為判別標準之特徵，始能進行認定。為此，經由參考重要學者之論述，並探討專家學者各自提出之定義，找尋其中共同之處，便可逐步歸納出重要的判別標準。

在定義「網路恐怖主義」概念時，許多專家學者所援引之定義，多為 Dorothy E. Denning 於 2000 年提出之定義，[24]或是以 Mark M. Pollitt 所提出之定義為基礎，再進行延伸或補充。[25]有鑑於此，以下分析兩者的觀點和著重焦點之異同，以歸納出網路恐怖主義最為關鍵的判別標準。

首先，Denning 對於網路恐怖主義的定義為：「網路恐怖主義指涉對於電腦、網絡及儲存於其中之資訊進行非法攻擊或威脅攻擊，以恐嚇或脅迫政府或其人民完成其政治性或社會性目標。此外，若要將一個攻擊行為歸類為網路恐怖主義，應包含對人身或財產之暴行，或至少產生足夠的傷害引發恐懼，例如導致死傷、爆炸或經濟嚴重受創之攻擊等。針對關鍵基礎設施之攻擊，可能屬於網路恐怖主義行為，端視其影響而定。干擾非必要性設施，或只是造成代價不菲的騷擾等，此類攻擊則不包括在內」。[26]此定義著重之焦點，包括：

1. 攻擊目標：電腦、網絡及儲存於其中之資訊；
2. 行為目的：透過攻擊行為造成足夠的傷害引發恐懼，以恐嚇或脅迫政府或人民完成其政治性或社會性目標。

至於 Mark M. Pollitt 所提出之定義則為：「網路恐怖主義是次國家團體或秘密人員針對資訊（information）、電腦系統、電腦程式和資料（data）有預謀且出

---

[24] 例如：Süleyman Özeren, *op. cit.*, p. 70; Shilpa Bhatnagar, *op. cit.*, Vol. 5, p. 1; P. Madhava Soma Sundaram & K. Jaishankar, *op. cit.*, p. 596; Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, DC: United States Institute of Peace, 2006), p. 153; James F. Pasley, *op. cit.*, p. 129.

[25] 例如：Maura Conway, "Cyberterrorism and Terrorist 'Use' of the Internet," *op. cit.*; Kevin Curran, Kevin Concannon, & Sean McKeever, *op. cit.*, p. 1.

[26] Dorothy E. Denning, "Cyberterrorism," *op. cit*.

於政治動機的攻擊，其目標為非戰鬥人員」。[27]與 Denning 之定義相比可以發現，Pollitt 強調之重點在於：

1. 攻擊者之身分：包括次國家團體及秘密人員；
2. 攻擊目標：資訊、電腦系統、電腦程式和資料；
3. 行為動機：有預謀且出於政治動機；
4. 影響所及範圍：非戰鬥人員。

關於「攻擊目標」一項，兩者所指涉之內容頗為接近，可視為相同。不過，倘若網路恐怖份子僅僅針對非必要性設施之電腦系統、電腦程式及資料等展開攻擊，例如民間企業或知名網站的電子資料庫等，其實質影響除了商業機密或個人私密資訊有洩漏之虞以外，通常尚不足以引發廣大民眾的恐懼心理，故攻擊行為針對的必須是關鍵基礎設施之監控系統、電腦程式及儲存資料等，並且造成足夠的實質傷害，始能達到「引發大眾恐懼」此一心理衝擊。

綜合以上兩種受到廣泛引用之定義可知，「**攻擊者之身分**」、「**行為動機**」、「**攻擊目標**」、「**行為目的**」以及「**影響所及範圍**」是網路恐怖主義最為核心之五個重要面向。據此觀察其他專家學者對於網路恐怖主義提出之各種定義，便可發現，無論他們各自強調的重點為何，皆包括在這五大面向之內，同時也能觀察出這些定義的不足之處。

舉例而言，Bill Nelson 等人將「對數位資產（digital property）進行非法破壞、干擾或故意散佈假情報等，以威脅或強迫政府或社會完成其政治、宗教或意識型態之目標」視為網路恐怖主義。[28]此定義聚焦於針對「數位資產」之非法手段，是為「攻擊目標」，並提及攻擊行為具有「政治、宗教或意識型態之目標」，是為「行為動機」，但是對於其他三個面向之相關敘述，便付之闕如。

---

[27] Mark M. Pollitt, *op. cit*.

[28] Bill Nelson, Rodney Choi, Michael Iacobucci, Mark Mitchell, & Greg Gagnon, *Cyberterror: Prospects and Implications* (Monterey, CA: Center for the Study of Terrorism and Irregular Warfare, Naval Post Graduate School, 1999), p. 9.

又如 Charles Jaeger 指出，網路恐怖主義仍是一個發展中（evolving）的概念，其包括「網路空間中的某些活動」和「以網路空間為工具引發群眾恐懼或恐慌之行為」，通常由次國家團體或秘密人員所為，進而威脅或強迫政府或部分非戰鬥人員達成其政治性或社會性目標。[29]觀察此一定義，僅包括「攻擊者之身分」與「行為目的」兩大面向。

再如 John Rollins 和 Clay Wilson 在研究網路恐怖主義之攻擊效果問題時發現，某些專家學者認為，大規模的網路攻擊可能僅僅造成不便（annoyance），而不是如同炸彈、生化武器或核武一般引發恐怖（terror），故「網路恐怖主義」一詞並不適當；另一些專家學者則主張大規模網路攻擊的效果難以預測，亦可能引發恐懼、造成平民死傷或經濟損失，因而可算是恐怖主義。面對如此的分歧現象，Rollins 和 Wilson 認為網路恐怖主義可分為兩個面向：

1. 著重效果（Effect-based）：電腦攻擊引發足以和傳統恐怖攻擊行為相當之恐懼效果時，即為網路恐怖主義。
2. 著重意圖（Intent-based）：非法或出於政治動機的電腦攻擊，其意圖為威脅或強迫政府或人民遂其政治目標，或造成嚴重破壞或經濟損失時，即為網路恐怖主義。[30]

在此定義之中，便包括「行為動機」、「行為目的」及「影響所及範圍」等三大面向，然而同時亦缺乏對於「攻擊者之身分」與「攻擊目標」的精確描述，尚有進一步推敲琢磨的空間。

網路恐怖主義除了侵襲關鍵基礎設施之外，亦可能做為傳統恐怖攻擊之輔助手段，兩者先後或同時進行，例如先以網路攻擊手段干擾或接管交通燈號控制系統，導致交通秩序大亂，藉以聲東擊西，迫使警消單位必須加派人力指揮交通及處理事故，再以傳統恐怖攻擊手段攻擊或威脅攻擊既定目標，如機場、商業中心

[29] Charles Jaeger, *op. cit.*, p. 172.
[30] John Rollins & Clay Wilson, "Terrorist Capabilities for Cyberattack: Overview and Policy Issues," CRS Report for Congress, p. 3, ＜http://www.fas.org/sgp/crs/terror/RL33123.pdf＞(Retrieved on July 1, 2012).

或能源設施等等，使得警消人員分身乏術，難以有效排除交通壅塞，導致救難單位在交通無法正常運作的情況之下，迅速抵達災難現場；或是在發動實體恐怖攻擊入侵銀行等金融機構的同時，透過網際網路攻擊股匯市線上交易系統，造成金融市場更加混亂，以達成恐怖攻擊行動之加乘效果。

結合網路恐怖主義與傳統恐怖主義之間的共同特徵，統整「**攻擊者之身分**」、「**行為動機**」、「**攻擊目標**」、「**行為目的**」及「**影響所及範圍**」等五大判別標準，並參考 Denning 在 Activism、Hacktivism 和 Cyberterrorism 分類中對於網路恐怖主義之闡釋，以及統整眾多專家學者各自之主張，進行重組之後，本論文對於網路恐怖主義之定義為：**次國家團體或秘密人員出於政治、社會或宗教動機，預謀造成重大災害，因而透過網際網路針對國家關鍵基礎設施之電腦系統、電腦程式、網絡及儲存於其中之資訊及資料，進行非法攻擊或威脅攻擊，包括對非戰鬥人員之人身或財產的暴行，使他人喪失生命，或導致嚴重的經濟損失，或至少產生足以引發恐懼的傷害，以恐嚇或脅迫政府或人民完成其政治性、社會性或宗教性目標。**

做為本論文申論之依據，此定義不僅涵蓋前述之五大判別標準，同時以「是否使用**網路攻擊手段**」，強調網路恐怖主義與傳統恐怖主義之間的主要分野，並排除「網路策劃」等與網路恐怖主義無關之網際網路使用行為。以此針對網路恐怖主義、網路犯罪及網路戰爭之間的差異相互比較之後，便能更加清楚地突顯網路恐怖主義之意涵。

第二節　與網路犯罪及網路戰爭之比較

除了皆以「網路攻擊」做為攻擊手段之外，網路恐怖主義與網路犯罪及網路戰爭之間的差異為何？對於國家而言，為何必須建立對於這三個概念的明確界定？本章第一節已整理出網路恐怖主義的「攻擊者之身分」、「行為動機」、「攻擊

目標」、「行為目的」及「影響所及範圍」等五大判別標準，本節便經由這五個判別標準，比較網路恐怖主義、網路犯罪及網路戰爭之間的差異，進一步釐清網路恐怖主義。

壹、網路犯罪

網際網路活動包羅萬象，各種網路犯罪類型也不勝枚舉，如何精確定義「網路犯罪」，實為不易之事。不僅如此，隨著大量電子設備紛紛連結上網際網路，網路犯罪與「電腦犯罪」之間的分野，亦越發模糊。以下首先綜整專家學者對於網路犯罪之定義，以及列舉之各種犯罪類型，接著討論電腦犯罪與網路犯罪之異同，最後則分析網路犯罪與網路恐怖主義之間的關係。

一、定義與類型

國際刑警組織（International Criminal Police Organization, INTERPOL）官方網站對於網路犯罪內容之定義為：「針對電腦資訊及系統之攻擊行為、盜用身分（identity theft）、散佈兒童性虐待圖片及網路拍賣詐欺行為」。[31]不過很顯然地，這樣的描述十分粗略，遠遠不足以涵蓋各種網路犯罪類型，而且就「針對電腦資訊及系統之攻擊行為」而言，若是以設置炸彈或故意縱火等物理攻擊方式破壞電腦資訊及系統，是否仍屬於網路犯罪？

有學者將「以電腦做為支援或輔助工具的犯罪行為（computer assisted and facilitated crimes）」視為網路犯罪，各種犯罪類型包括：竊取智慧財產（intellectual property theft）及財產資訊（proprietary information）、非法複製軟體、音樂及電影、非法入侵電腦系統、散佈惡意程式、盜用身分及散播色情資訊或性交易等；[32]或是認為，網路犯罪係指「不法分子利用現代高科技手段，以網絡隱蔽、快捷

[31] "Cybercrime," p. 1, ＜http://www.interpol.int/content/download/805/6671/version/10/file/FHT02.pdf＞(Retrieved on February 23, 2012).
[32] Jeffrey Ian Ross, *op. cit.*, pp. 21-24.

的通信功能與網絡系統儲存、處理和傳輸的信息為危害對象且具有跨時空特徵的嚴重不法行為」。[33]

此外，亦有學者認為，網路犯罪尚未成為一個具有嚴格定義的概念，只要是「能夠坐在電腦鍵盤前面完成」的犯罪行為，皆算是網路犯罪，包括：非法存取電腦檔案、以電腦病毒干擾其他遠端電腦的正常運作、特洛伊木馬程式（Trojan horses）以及盜用身分等等。網路犯罪的成本低廉，卻難以偵測，同時由於確認犯罪者的地理位置十分不易，也常常在法律管轄權歸屬上發生困難。[34]

以上之定義較為接近，大致只要與電腦或網際網路有關，或以之為犯罪工具的犯罪行為，即屬於網路犯罪。相較之下，Susan W. Brenner 指出，一般認為網路犯罪「與傳統犯罪無異，只是透過電腦網路等非傳統的手法犯罪，即『舊瓶裝新酒』（old wine in new bottles）」之看法，忽略了一個重要問題：即使大多數的網路犯罪，例如網路詐欺、網路騷擾或盜取資料等，其內容與傳統犯罪相同，只是手法不同，但是仍有一些罪行無法在網際網路上完成，例如強暴或重婚，以及某些只能在網際網路上完成的罪行，例如前述之「拒絕服務攻擊」等。[35]

觀察 Brenner 之舉例可知，由於這兩種特殊之犯罪類型，使得網路犯罪有必要在分類上獨立於傳統犯罪之外，而不僅僅是「犯罪手法與電腦及網路系統有關」的犯罪行為。據此，Brenner 對於網路犯罪之定義，是為「利用電腦科技犯罪，其活動足以威脅到社會維持內部秩序之能力」。[36]

綜上所述，大多數學者認為，只要是與電腦及網際網路有關的犯罪行為，通常皆屬於網路犯罪的範疇。然而，考量到若干特殊類型之犯罪行為，Brenner 所提出之見解與定義，可謂較為全面。即使網路犯罪之定義輪廓可能尚不明確，仍有某些特定的犯罪類型多次被專家學者提及，例如非法入侵電腦系統、非法複製

[33] 馬進保、袁廣林，頁 205。
[34] Shilpa Bhatnagar, *op. cit.*, Vol. 1, p. 39.
[35] Susan W. Brenner, "'At Light Speed': Attribution and Response to Cybercrime/Terrorism/Warfare," *op. cit.*, pp. 383-384.
[36] Susan W. Brenner, "'At Light Speed': Attribution and Response to Cybercrime/Terrorism/Warfare," *op. cit.*, p. 386.

軟體、盜用身分或散播色情資訊等等。對照美國聯邦法規，其亦將其中若干行為視為網路犯罪。[37]

二、網路犯罪與電腦犯罪之異同

有學者主張，針對電腦犯罪之定義，主要有廣義說、狹義說和折衷說三種類型：廣義說主張電腦犯罪泛指所有與電腦科技或電腦系統有關之犯罪，或泛指所有與電子資料之處理有關之犯罪；狹義說則認為，電腦犯罪乃指與電子資料處理有關之故意而違法之財產破壞行為；至於折衷說，則為「行為人濫用電腦或破壞電腦而違犯之具有電腦特質之犯罪行為」。[38]另有學者指出，美國聯邦調查局採用廣義說之見解。[39]

在當今眾多電子設備已連接到網際網路的時代，電腦犯罪與網路犯罪之間是否仍有差異？或者已無區分之必要？例如 Susan W. Brenner 便將「電腦犯罪」、「高科技犯罪」（high-tech crime）或「資訊時代犯罪」（information-age crime）皆視為相同概念。[40]

除了 Brenner 之外，亦有學者認為，網路犯罪與電腦犯罪相較，雖有其特殊性，但要與電腦犯罪完全切割，是相當困難的；[41]或是主張電腦犯罪與網路犯罪之間的差異十分細微，兩者可視為相同。[42]

另有學者將網路犯罪視為電腦犯罪之延伸，為電腦系統與通訊網路相結合之犯罪行為，相較於電腦犯罪而言，更偏重於「網際網路」的應用，係指具有網際

---

[37] 依據美國聯邦法規中「電腦相關之詐欺及有關活動」（Fraud and related activity in connection with computers）章節之規定，包括非法入侵電腦、非法取得政府部門或其他受保護之電腦資料，或是非法傳送程式及資訊等等，皆被聯邦政府視為犯罪行為。請參見：U.S. Code Title 18, Ch. 47, Sec. 1030.

[38] 林山田，《**刑事法論叢（一）**》（臺北：臺灣大學法學院圖書部，1997），頁 137-138；許武峰，《**電腦犯罪理論與實務問題研究**》（臺北：司法院，1998），頁 3。

[39] 吳永宗，《**電腦運用所衍生法律問題之研究**》（臺北：司法院，1998），頁 110。

[40] Susan W. Brenner, "Cybercrime: Re-Thinking Crime Control Strategies," in Yvonne Jewkes, ed., *Crime Online* (Portland: Willan Publishing, 2007), p. 13.

[41] 王銘勇，《**網路犯罪相關問題之研究**》（臺北：司法院，2002），頁 21-22。

[42] George E. Higgins, *Cybercrime: An Introduction to an Emerging Phenomenon* (New York: McGraw-Hill, 2010), p. 2.

網路特性的犯罪。即使目前專家學者對網路犯罪並沒有嚴格定義及統一意見，但是電腦犯罪之特性與行為人之特質，仍應適用於網路犯罪。[43]換言之，電腦犯罪與網路犯罪之間即使存在差異，但是程度甚微，不需特別分類。

三、網路犯罪與網路恐怖主義之關係

對於 Bernadette H. Schell 和 Clemens Martin 而言，網路犯罪即是和科技、電腦和網際網路相關的犯罪行為，大致包括：非法入侵電腦系統（Cracking）、非法複製受保護之軟體（Piracy）、利用電腦或其他裝置盜打電話（Phreaking）、騷擾或恐嚇其他電腦使用者（Cyberstalking）、以電腦製作或散播色情資訊（Cyberpornography），以及網路恐怖主義等。[44]據此，網路犯罪與網路恐怖主義之間，可能存在某種程度的重疊。

根據 Clay Wilson 之定義，網路犯罪則是為「以電腦為工具或目標之犯罪」，包括：竊取智慧財產、違反專利或著作權法、阻礙其他電腦正常運作，或是非法複製機密檔案之間諜行為等等。倘若一個恐怖組織發動網路攻擊並造成傷害，如此的行為亦符合網路犯罪的定義範圍。Wilson 也強調，一場網路攻擊是屬於網路犯罪抑或是網路恐怖主義，其主要區別在於攻擊者的「意圖」，即使兩者在行為上可能發生重疊。[45]

不僅如此，Charles Jaeger 也有類似看法，認為網路恐怖主義與駭客行為（hacking）和電腦破壞行為（cybervandalism）之間的主要差異，在於「行為意圖」和攻擊的「嚴重程度」。[46]

另一方面，Susan W. Brenner 也以「行為動機」做為判別網路犯罪與網路恐怖主義之標準。她主張，犯罪是為了個人目的，而恐怖主義則是為了政治目的；

---

[43] 林宜隆，《**網際網路與犯罪問題之研究**》（桃園：中央警察大學出版社，2000），頁 71。
[44] Bernadette H. Schell & Clemens Martin, *op. cit.*, pp. 2-3.
[45] Clay Wilson, "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," CRS Report for Congress, p. 4, ＜http://www.fas.org/sgp/crs/terror/RL32114.pdf＞ (Retrieved on February 19, 2012).
[46] Charles Jaeger, *op. cit.*, p. 172.

犯罪是出於個人及私人的理由，包括個人私欲或是傷害他人之意圖等，而恐怖主義之行為雖然也是犯罪，其目的卻在於直接或間接地使民眾陷入混亂（demoralize a civilian population），例如 2001 年美國 911 事件當中，恐怖份子攻擊紐約世貿中心（World Trade Center）之目的，除了摧毀資本主義的象徵性建築物之外，也是為了造成美國國內人心惶惶、社會恐慌、秩序大亂。[47]

由以上學者之相近主張可知，網路恐怖主義既為網路空間中的不法活動，應當屬於網路犯罪之特定類型。無論是廣義或狹義的定義，皆未特別描述網路犯罪行為者的「特定身分」，或是具有「政治、社會或宗教動機」與否，或企圖「脅迫政府或社會完成其政治性、社會性或宗教性目標」等等。而在犯罪行為「足以引發恐懼」的方面，亦未見到相關的敘述。

除此之外，網路攻擊之行為者曾否企圖引發大眾恐慌，亦可做為判別其行為是否屬於網路恐怖主義之關鍵因素。即使網路犯罪真能引發某人或某些人的恐懼，他們之所以產生恐懼，是由於身為犯罪行為的直接受害者之緣故，例如遭到勒索、騷擾或恐嚇等等，但是對於一般大眾而言，網路犯罪所造成的心理影響或衝擊則是間接性的，難以導致群眾的恐慌及社會的不安。

因此，網路恐怖主義與網路犯罪之間的差異，主要在於「**行為動機**」：網路恐怖主義之行為者具有政治、社會或宗教動機，而網路犯罪尚包括個人利益、商業競爭，甚至只是惡作劇等動機。

貳、網路戰爭

在美國空軍官方網站的歡迎頁面中，對於自身任務內容之描述如下：「在空中、太空及網路空間中翱翔、戰鬥，並且獲勝（to fly, fight and win...in air, space and cyberspace）」。[48]由此可見，美國空軍已認知到，現代戰爭正逐漸與網際網路相結

[47] Susan W. Brenner, "'At Light Speed': Attribution and Response to Cybercrime/Terrorism/Warfare," *op. cit.*, pp. 387-389.
[48] "Air Force Mission," ＜http://www.af.mil/main/welcome.asp＞(Retrieved on February 19, 2012).

合，不若以往侷限於陸、海、空及太空之中，也可能發生在網路空間當中，網路戰爭不再只是科幻小說或電影的情節，更是美國空軍真實面對的重要任務之一。但是，何謂「網路戰爭」？若不了解其內容，美國空軍該如何從中獲勝？以下首先以 2008 年 8 月，俄羅斯向南面鄰國喬治亞（Georgia）發動網路戰爭為例，說明網路戰爭的實際情況，接著統整專家學者對於如何界定網路戰爭之看法。

一、俄喬衝突（2008 年 8 月）

2008 年，俄羅斯與喬治亞針對「阿布卡西亞」（Abkhazia）與「南奧塞梯」（South Ossetia）兩個地區發生領土紛爭，俄國政府支持這兩個地區的獨立運動，而喬治亞則試圖阻止它們從該國分裂出去，雙方爭執不下，衝突持續升高。

同年 7 月 20 日，喬治亞總統的官方網站首次遭到「拒絕服務攻擊」，被迫停止運作長達 24 小時。8 月 7 日，喬治亞陸軍開始進入南奧塞梯地區，俄軍也在一天之內做出回應，迅速組織地面及空中武裝力量進行反擊。在俄軍展開實際的軍事行動之前，便已先對喬治亞發動大規模的網路攻擊，干擾該國所有的網路通訊，除了總統的官方網站再次受到入侵和竄改以外，包括銀行、國會、最高法院、新聞媒體、外交部和國防部等網站，皆遭到網路攻擊。根據專家和獨立機構的追查，雖然有部分網路攻擊的來源位於土耳其，但是主要的攻擊來源仍在俄國境內。俄國以網路攻擊配合實際軍事行動的協同作戰，也是全球首次出現的網路戰爭實例。[49]

由此觀之，做為全新的戰爭型態，網路戰爭以網路攻擊輔助實體的軍事手段，可能產生更良好的攻擊效果。在回顧實際案例之後，經由觀察專家學者如何界定網路戰爭，進而分析網路恐怖主義與網路戰爭之間的差異。

[49] Richard Stiennon, *Surviving Cyberwar* (Lanham, MD: Government Institutes, 2010), pp. 95-99.

二、定義綜整

有學者主張，網路戰爭之定義為「利用網路空間之軟體或硬體漏洞，有意造成他人、資產或經濟上的損害之行為」。[50]不過該定義恐怕過於空泛，和一般的網路犯罪或商業間諜行為等等互相比較，難以做出區別，且未對於行為者身分及動機等方面多加敘述，尚需更進一步的推敲。相較之下，另有學者將網路戰爭定義為「一國對於另一國之電腦或網絡的滲透行動，旨在造成損害或破壞」。[51]此定義便對於行為者身分及動機提出較為明確的規範，並強調「國家行為者」的重要性。

另有學者以歷史上的幾場重大戰爭為案例，說明「資訊」對於贏得戰爭的重要性，並且以撰文當時的時空背景及科技水準為論述架構，針對網路戰爭進行詳盡的分析及定義，預示 21 世紀新型態戰爭的可能樣貌及應對之道，同時主張，網路戰爭指涉「進行及準備進行與資訊相關（information-related）的軍事行動」，其包括：

1. 破壞或摧毀敵方賴以感知各種情報（對手是誰、何時發生、如何反應，以及威脅之優先處理順序等等）的資訊和通訊系統，廣義而言甚至包含軍事文化在內；
2. 盡可能了解敵方的一切，並且不讓敵方了解自己；
3. 使「資訊和知識的平衡」（balance of information and knowledge）倒向對自己有利的一方，特別是當雙方力量不平衡的時候；
4. 利用知識以降低資本和勞力的開銷。[52]

在四項重點當中，第三項可謂國家從事網路戰爭最主要之目的，即盡可能使敵我雙方的資訊平衡不對等，掌握敵方資訊，並隱藏我方資訊，以取得資訊、情

[50] Robert S. Owen, "Infrastructures of Cyber Warfare," in Lech J. Janczewski & Andrew M. Colarik, eds., *Cyber Warfare and Cyber Terrorism* (Hershey, PA: Information Science Reference, 2008), p. 41.
[51] Richard A. Clarke & Robert K. Knake, *op. cit.*, p. 6.
[52] John Arquilla & David Ronfeldt, "Cyberwar is Coming!" in John Arquilla & David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND, 1997), p. 30, < http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/MR880.ch2.pdf > (Retrieved on February 23, 2012).

報和知識上的極大優勢，從而在戰略或戰術層面立於不敗之地，或是做為陸、海、空實體軍事力量之輔助。

此外，有學者在一份為美國國會準備之報告中指出，網路戰爭即是在網路空間中從事的戰爭（warfare waged in cyberspace），包括保衛資訊及電腦網絡、嚇阻資訊攻擊，並且不讓敵方達成上述目標；積極而言，網路戰爭還包括攻擊敵方的資訊及電腦網絡，甚至主宰戰場上的資訊流通等等。[53]雖然 Hildreth 並未提及網路戰爭行為者之身分，不過縱觀該份報告即可發現，論述當中所涉及到的多為國家行為者，包括美國本身，以及俄國、中國、英國及德國等等。

另一方面，有學者反對任意將網際網路上的負面活動稱為「戰爭」或「攻擊」，並主張網路戰爭必須如同實體活動一般，建立判別之高標準。由於「戰爭行為」（act of war）意味國家出於政治目的使用武力對抗另一國家，其中武力包含了暴力（violence）和恫嚇（intimidation），而「攻擊」則是個人有意造成損失、破壞或傷亡之行為，因此，網路戰爭是為「國家或政治團體出於政治目的使用武力造成損失、破壞或傷亡」。[54]觀察其文意，此處之「武力」應當包括網際網路之使用，換言之，由國家出於政治目的所發動之網路攻擊，即為網路戰爭，而政治團體倘若出於政治目的針對國家之資訊或電腦網絡發動網路攻擊，亦可謂網路戰爭。但是，如果政治團體針對非戰鬥人員發動網路攻擊，則不能算是網路戰爭，而是網路恐怖主義或網路犯罪，端視其是否具政治動機，以及是否意圖引發恐懼而定。

除此之外，網路戰爭也是以虛擬方式（by virtual means）進行的軍事行動，國家使用網路空間所欲達成之目標，與使用傳統軍事力量之目標無異，即對與之競爭的國家取得優勢，或是防止競爭國對本國取得優勢。例如 Susan W. Brenner

[53] Steven A. Hildreth, "Cyberwarfare," CRS Report for Congress, p. 16, ＜http://www.fas.org/irp/crs/RL30735.pdf＞(Retrieved on February 20, 2012).
[54] James A. Lewis, "Thresholds for Cyberwar," *op. cit.*, p. 1.

強調，戰爭的特性在於它是「國家之間的對抗」，雖然如同所有人類活動一樣，戰爭也是由個人實現，但是個人實際上是為了特定國家的利益而行動的。[55]

Brenner 進一步分析，恐怖主義不同於戰爭的最大差異，在於戰爭所針對的對象不應該是平民。[56]即使戰爭與恐怖主義通常皆導致大規模的破壞和死傷，然而戰爭僅限於交戰各國軍隊之間的衝突，起碼在理論上是如此；戰爭雖然可能導致平民死傷，不過和財產損失及其他破壞一樣，這些都是軍事衝突的附帶性結果，而非主要目的。縱使犯罪行為與恐怖主義之間的分別可能不甚明確，但是戰爭卻不然，因為唯有國家有能力集結在陸、海、空發動攻擊所需的各種資源，來對抗其他國家。此外，軍事人員所穿戴之制服及階級飾章等，也都是代表其所屬國家之標誌。[57]

綜觀上述，網路戰爭在某種程度上類似於網路犯罪及網路恐怖主義，其攻防的目標同樣都是電腦系統、電子資訊及網絡，和對方的資訊感知能力等等，但是網路戰爭不同於網路犯罪及網路恐怖主義的最大特徵亦十分明顯，其係由「國家所屬人員」或「針對國家資訊或電腦網絡之政治團體」所發動。國家所屬之個體行為者受到國家之命令或委託，故代表其國家進行相關活動，其行為與自身的政治動機並無多少關聯，所做所為皆是為了國家之利益，而非個人利益；針對國家資訊或電腦網絡之政治團體所針對之對象仍是國家，不是非戰鬥人員。除此之外，網路戰爭的攻防行為亦如同傳統戰爭一般，至少在理論上必須侷限於軍事力量的較勁，影響所及不應造成各方非戰鬥人員的傷亡或財產的損失。

參、網路恐怖主義、網路犯罪及網路戰爭差異之比較

網路恐怖主義係為網路犯罪與恐怖主義活動相互結合之產物，而網路戰爭則可謂出於政治目的，由國家所授權，或是政治團體對抗國家之網路犯罪行為，其

[55] Susan W. Brenner, "'At Light Speed': Attribution and Response to Cybercrime/Terrorism/Warfare," *op. cit.*, pp. 401-402.
[56] *Ibid*, pp. 387-388.
[57] *Ibid*, pp. 402-403.

形式上是戰爭，但是手段與網路犯罪之間，並無太大差異。三者之重疊關係，可以下圖表示：

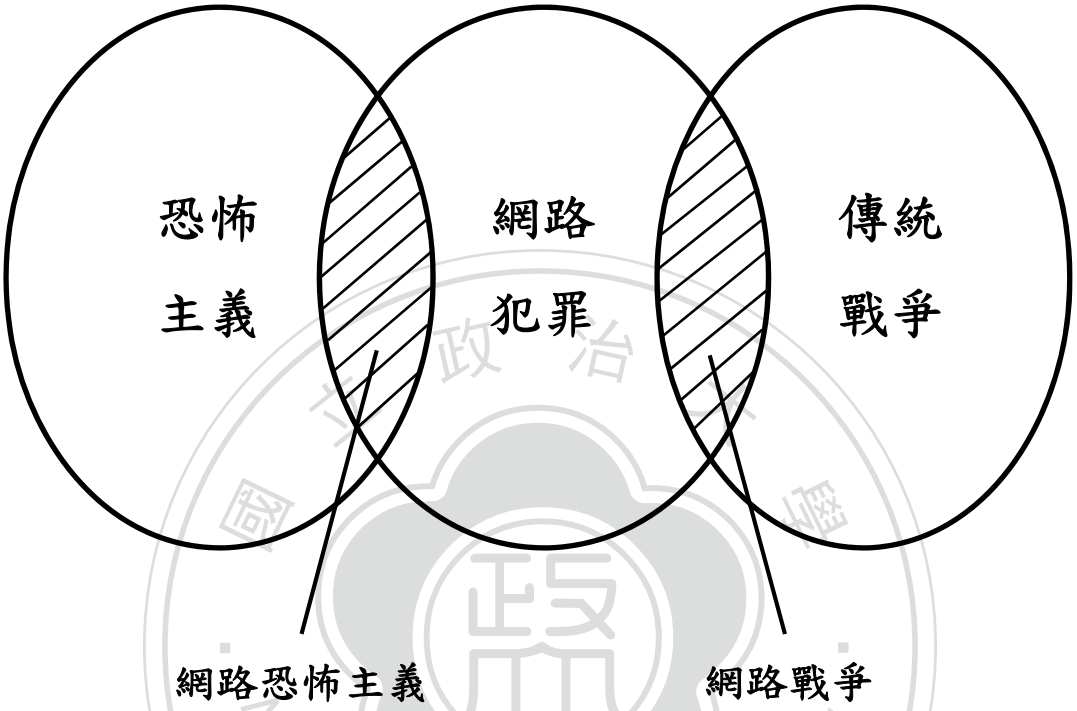

圖 2-2　網路恐怖主義、網路犯罪及網路戰爭三者關係圖

資料來源：筆者自行繪製

即使網路恐怖主義和網路戰爭皆屬於網路犯罪之特定類型，攻擊手段也頗為相似，但是經過仔細比較之後可以發現，三者在「攻擊者之身分」、「行為動機」、「攻擊目標」、「行為目的」及「影響所及範圍」等五大面向，仍然有顯著差異，如表 2-1 所示：

表 2-1　網路恐怖主義、網路犯罪及網路戰爭之比較

	網路恐怖主義	網路犯罪	網路戰爭
攻擊者之身分	次國家團體或秘密人員	具相關技術及知識者，無特定身分	1. 國家之軍事或僱傭人員 2. 針對國家資訊及電腦網絡之政治團體
行為動機	政治、社會或宗教動機	個人利益、商業間諜或惡作劇等	1. 軍事或僱傭人員：國家之命令或委託，與個人利益或政治傾向無關 2. 政治團體：政治動機
攻擊目標	關鍵基礎設施之 SCADA 系統、電腦程式及對外通訊網絡等	個人或公私部門之電腦系統、電腦程式及網絡等	交戰敵方之電腦系統、電腦程式及情報網絡等
行為目的	造成足夠的傷害並引發恐懼，以恐嚇或脅迫政府或人民完成其政治性或社會性目標	個人私欲、商業利益、駭客大戰或民族情緒等	敵我資訊平衡不對等，取得資訊及情報優勢，降低敵方資訊感知能力，並保護己方不受攻擊等
影響所及範圍	非戰鬥人員及民生必需之關鍵基礎設施等	受害之個人及公私部門等	理論上應限於交戰各方軍事力量之衝突，不應影響關鍵基礎設施或平民之生命或財產安全

資料來源：筆者自行整理

根據表 2-1，網路恐怖主義、網路犯罪及網路戰爭除了攻擊手段相近之外，不論在「攻擊者之身分」、「行為動機」、「攻擊目標」、「行為目的」或「影響所及範圍」等五大面向，皆存在明顯差異。因此，網路攻擊行為必須符合五大面向之條件，始能被視為網路恐怖主義。

到目前為止，本章已針對網路恐怖主義之定義進行整理，並且將其與網路犯罪和網路戰爭之間的關係及差異，各自呈現如上。然而，其中也引發另一個問題：一旦發生網路攻擊事件時，如何確認攻擊者之身分？許多文獻及專家皆指出，網路犯罪者與一般犯罪者相同，總是會刻意消除其犯罪活動之足跡以躲避追查，加上網際網路的開放性、匿名性和跨越地理限制等諸多特性，在大多數的網路犯罪或網路攻擊事件中，除非經過費時費力的長時間追蹤，否則確實很難清楚辨認攻擊者之身分及所在位置。例如常見的殭屍網絡（botnet）攻擊，由於發動攻擊的電腦可能遍布全球，以致於追查殭屍網絡之控制者變得十分困難。發動殭屍網絡攻擊的電腦全都遭到入侵者事先植入程式，並設定在某個時間點同時發動攻擊，但是攻擊之程式只在受害電腦的背景下悄悄執行，電腦使用者通常不會知道自己的電腦參與了攻擊事件，只覺得電腦運行速度比平常稍微慢一些，或是連上網站所需的時間變長一點。[58]

對於國家而言，一般的網路犯罪僅需由警方加以追查，網路恐怖主義則需警方、反恐及情報相關部門通力合作，而兩者在法律上皆屬於犯罪行為；相較之下，網路戰爭卻需要動用國家的軍事力量進行反制，或是訴諸外交手段尋求解決。在遭受網路攻擊之後，若不能確定攻擊者之身分及攻擊來源，便無法迅速且適度地反應。例如，近年來美國持續密切關注中國發動網路戰爭之能力的發展情況，有心人士利用此點，事先滲透許多位於中國境內之電腦，以掩護其真實身分和所在位置，再對美國發動大規模網路攻擊。在此情況之下，美國必須確定攻擊行為是由個人或是國家所發動，才能以適當的方式做出回應。

[58] 有關殭屍網絡之運作情形，可參見：Ron Rhodes, *op. cit.*, pp. 34-35.

此外，一旦發生網路恐怖主義攻擊，可能導致的災情為何？由於全球尚未出現網路恐怖主義攻擊之真實案例可供參考，下一節將以 2007 年 4 月愛沙尼亞境內發生之大規模網路攻擊事件，做為類似案例。經由整理該事件的來龍去脈及後續效應，評估網路恐怖主義攻擊對於國家及社會大眾的衝擊層面和影響範圍，以及政府應如何以之為借鏡，徹底防範網路恐怖主義攻擊。

第三節　愛沙尼亞遭受網路攻擊案例（2007 年 4 月）

不論是由於恐怖份子的能力或意願尚且不足，或者是世界各國政府在反制網路恐怖主義工作上的成果相當顯著等因素使然，到目前為止，國際社會尚未傳出過重大的網路恐怖主義攻擊事件。然而，近似於網路恐怖主義攻擊的案例，即使嚴重程度不一，卻始終層出不窮。許多文獻資料皆以 2007 年 4 月愛沙尼亞遭受大規模網路攻擊事件，以及 2008 年 8 月俄羅斯與喬治亞共和國之間的衝突所引發之網路戰爭，作為相關案例研究之背景。由於俄喬衝突屬於網路戰爭之範疇，本論文選擇愛沙尼亞爆發大規模網路攻擊事件做為個案研究對象，討論該事件是否屬於網路恐怖主義，以及對於國家處理網路攻擊之威脅有何啟發。

壹、事件背景

愛沙尼亞為波羅的海（Baltic Sea）三小國之一，由於其地理位置，該地區在歷史上始終受到鄰近強國勢力之影響，歷經丹麥、日耳曼人、波蘭及俄國等列強統治，於 1918 年首次獨立。1939 年《德蘇互不侵犯條約》簽訂，愛沙尼亞被劃入蘇聯勢力範圍，不久之後被迫成為其加盟國。自 1991 年 8 月正式脫離蘇聯獨立之後，成立民主體制之共和國，改採自由市場經濟，以電子科技及資訊工業為國家發展重點。據美國國務院（Department of State）之統計，2010 年愛沙尼亞

服務業之 GDP 所佔比率為 68.8%，工業則佔 28.7%。該國於 1999 年加入世界貿易組織（World Trade Organization, WTO），2004 年 5 月加入歐盟（European Union, EU），2000 年至 2007 年間，該國年平均經濟成長率為 8%。[59]

自 1991 年獨立之後，愛沙尼亞跳過有線傳輸技術，直接朝向無線通訊領域迅速發展，其國內通訊科技發達之程度，使得該國甚至享有「E-stonia」之暱稱。Richard Stiennon 指出，由於國內大多數民眾都不只擁有一支手機，截至 2010 年為止，愛沙尼亞每人擁有手機之比率已超過 100%；超過八成的銀行透過網際網路相互連結；八成的投票是以線上方式完成；首都塔林（Tallinn）市內提供 1200 個 Wi-Fi 熱點；民眾可利用簡訊傳送密碼繳交停車費等等。[60]上述之現象，在在顯示出愛沙尼亞在社會、經濟和民生等各層面對於網際網路的高度依賴。

二次大戰結束後的數十年間，蘇聯當局運送了大量的俄羅斯人進入各個衛星國家，愛沙尼亞亦不例外，目前該國國內俄羅斯民族人口約佔四分之一。[61]蘇聯解體之後，俄羅斯仍然繼續透過這些移民，試圖維持其在各個前衛星國家之內的影響力，包括影響大選結果，以及鼓吹親俄政策等。然而，愛沙尼亞於 2004 年 3 月正式加入北大西洋公約組織（North Atlantic Treaty Organization, NATO），此舉對於俄羅斯拉攏該國之政策而言，不啻為一次重大失利。

貳、事件經過

2007 年 4 月，愛沙尼亞政府決定將塔林市中心一座由前蘇聯當局於 1947 年豎立的士兵紀念銅像移走。愛沙尼亞人普遍認為，移走銅像象徵該國徹底脫離舊政體，迎向自由。然而，如此舉措亦引發國內俄裔人民的強烈不滿，群起示威暴動，該國位於莫斯科的大使館也受到群眾包圍。當月 27 日，銅像剛剛重新安

[59] "Background Note: Estonia," < http://www.state.gov/r/pa/ei/bgn/5377.htm > (Retrieved on February 29, 2012).
[60] Richard Stiennon, *op. cit.*, p. 86.
[61] "Background Note: Estonia," < http://www.state.gov/r/pa/ei/bgn/5377.htm > (Retrieved on February 29, 2012); "The World Factbook," <https://www.cia.gov/library/publications/the-world-factbook/geos/en.html>(Retrieved on February 29, 2012).

置完成，眾多銀行、通訊設施、政府部門網站，以及該國總理所屬政黨的官方網站等等，皆遭到大規模的拒絕服務攻擊。在一般情況下，政府網頁一天的瀏覽次數大約是 1000 次左右，但是在遭受攻擊時，每秒的瀏覽次數卻高達 2000 次。如此大規模的網路攻擊，導致大多數的網站伺服器皆不堪負荷，被迫停機長達數小時之久。[62]

一連串的網路攻擊行為持續數周，甚至擴及到真實世界。5 月 2 日，俄羅斯國有鐵路公司以「必須維修連接兩國之鐵路」為由，宣布暫停向愛沙尼亞輸送原油和煤礦。同日，一群俄國國會議員飛抵塔林，要求愛沙尼亞政府總辭，但是他們立刻遭到拒絕，並隨即被送上飛機，回到莫斯科。[63]據歐洲媒體 Radio Free Europe 報導，愛沙尼亞總統 Toomas Hendrik Ilves 因此向俄國公開呼籲：「試著保持文明！」（try to remain civilized!）[64]並且暗示，該國已掌握可證實某些網路攻擊來自克里姆林宮（Kremlin）的相關證據，即使若要將攻擊行為歸責於俄國政府，還有待更深入的調查。[65]

愛沙尼亞政府在危機之中的反應，可謂十分迅速。首先，在遭到網路攻擊後的 1 小時之內，國防部官員、主要的通訊系統供應商、銀行人員及專家學者之間已開始互相了解情況，並討論如何處理危機。接著，政府決定暫時切斷所有從國外連入的網路連結，將該國隔離在網際網路之外，使得國內銀行的線上作業能夠正常提供服務。最後，在分析各個網站遭受拒絕服務攻擊的情況之後發現，網站被迫關閉的原因，並不是因為伺服器無法處理大量的瀏覽流量，而是由於儲存網頁內容的資料庫存在設計缺陷，導致其無法回應重複且大量的流量所致。因此，強化伺服器資料庫的功能成為必要工作，其做法是將所有網頁的內容備份在各個「內容管理系統」（Content Management System, CMS）之中，這些系統可提供更

[62] Clay Wilson, "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," CRS Report for Congress, p. 7, ＜http://www.fas.org/sgp/crs/terror/RL32114.pdf＞(Retrieved on February 19, 2012).
[63] Richard Stiennon, *op. cit.*, p. 88.
[64] "Newsline - May 3, 2007," ＜http://www.rferl.org/content/article/1143864.html＞(Retrieved on March 1, 2012).
[65] Richard Stiennon, *op. cit.*, p. 88.

完善的網頁內容管理程序，並且應付更多更頻繁的瀏覽要求。在遭受攻擊的 72 小時之內，大多數受到影響的網站已恢復正常運作。[66]

參、後續效應與案例分析

愛沙尼亞「電腦緊急應變小組」（Computer Emergency Response Team, CERT）首席安全官 Hillar Aarelaid 指出，北約在事發後已派出專家協助該國進行調查。[67] 一開始，愛沙尼亞官員指責俄國政府發動網路攻擊，甚至有網路戰爭的指控，但並不是所有專家皆同意這樣的看法。[68]經過深入調查之後發現，在許多俄文討論區（forum）皆可找到用來發動攻擊的程式，有專家因而認為，這場網路攻擊事件並非有計劃性的攻擊行動，而是由若干自發性且關係鬆散的個別攻擊者所為。此外，攻擊目標雖然包括政府網站，但是不包括網際網路系統之外的其他關鍵基礎設施，攻擊亦僅限於阻礙網路傳輸及干擾網站正常運作，並未有人提出勒索等要求。因此，即使攻擊行動是因俄羅斯民族主義而起，專家不認為俄國政府與這場網路攻擊事件之間有直接關聯。[69]

2008 年 1 月，塔林市一名 20 歲男子遭指控涉及 2007 年 4 月的這起事件，當時他與其他身分不明的共犯合作，一同向該國首相的個人網站及政府部門網站發動網路攻擊，因而被判有罪。愛沙尼亞當局隨後對其罰款 17,500 愛沙尼亞克朗（Estonian Krooni），約為 1,641 美元，這個金額等於該國一年的基本工資。[70]

由於愛沙尼亞是北約會員國，該事件使得北約重新思考，一場網路攻擊轉變為網路戰爭的臨界點為何，這關係到其他會員國何時必須依照條約履行支援受侵

---

[66] Richard Stiennon, *op. cit.*, pp. 89-90.
[67] Jeremy Kirk, "Estonia Recovers from Massive DDoS Attack," ＜http://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack＞(Retrieved on March 3, 2012).
[68] Clay Wilson, "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," CRS Report for Congress, p. 8, ＜http://www.fas.org/sgp/crs/terror/RL32114.pdf＞(Retrieved on February 19, 2012).
[69] "Estonian DDoS - A Final Analysis," ＜http://www.h-online.com/security/news/item/Estonian-DDoS-a-final-analysis-732971.html＞(Retrieved on March 1, 2012).
[70] John Leyden, "Estonia Fines Man for DDoS Attacks: Local Pest rather than International Conspiracy," ＜http://www.theregister.co.uk/2008/01/24/estonian_ddos_fine/＞(Retrieved on June 18, 2012).

略國的義務，以及如何適度回應發生在網路空間的戰爭等問題。[71]2008 年 5 月，北約正式成立「卓越合作網路防衛中心」(NATO Cooperative Cyber Defence Centre of Excellence, CCDCOE)，做為該組織有關網路安全及網路衝突領域的研究基地，以加強網路防衛能力為宗旨，其所在位置便設在塔林。愛沙尼亞自此成為歐盟相關議題之領導者，CCDCOE 每年皆舉辦國際會議。[72]

以下首先以網路恐怖主義之五大判別標準，說明這起網路攻擊事件不應被視為網路恐怖主義的原因，接著討論對於國家制訂防治網路恐怖主義及災害應變措施相關政策而言，這起事件有何參考價值。

一、該事件是否屬於網路恐怖主義？

以「攻擊者之身分」、「行為動機」、「攻擊目標」、「行為目的」及「影響所及範圍」等五大面向，觀察這場網路攻擊事件，判斷其是否屬於網路恐怖主義：

1. 攻擊者之身分：在此次事件中，無法確認攻擊者之身分的問題一直存在，從而亦難以追查攻擊者是否得到國家資助或授權、攻擊係由若干個人所為，或是由有組織的政治團體所發起等等。
2. 行為動機：遷移前蘇聯士兵紀念銅像事件，不僅激起愛沙尼亞國內俄羅斯民族主義情緒，亦引發俄國民眾強烈不滿，隨之而來的大規模網路攻擊，依據攻擊開始的時間點推斷，可謂因政治動機而起。
3. 攻擊目標：網路系統以外的關鍵基礎設施沒有遭到網路攻擊，除了網路傳輸受阻和網站系統停機，導致銀行線上作業被迫暫停之外，其他關鍵基礎設施的運作未受到任何影響。

---

[71] Richard Stiennon, *op. cit.*, p. 90.

[72] "Past Events," <http://www.ccdcoe.org/126.html>(Retrieved on March 1, 2012). 關於愛沙尼亞遭受大規模網路攻擊事件之背景、事件經過及後續發展等，亦可參見：Eneken Tikk & Reet Oorn, "Legal and Policy Evaluation: International Coordination of Prosecution and Prevention of Cyber Terrorism," in Centre of Excellence Defence Against Terrorism, Ankara, Turkey, ed., *Responses to Cyber Terrorism* (Washington, DC: IOS Press, 2008), pp. 93-102.

4. 行為目的：攻擊事件沒有導致人員傷亡，或造成大規模財產損失，遑論引發大眾恐懼；除了若干俄國國會議員要求愛沙尼亞政府總辭之外，沒有個人或團體出面向該國政府提出任何恐嚇或脅迫。
5. 影響所及範圍：雖然愛沙尼亞許多公私部門受到網路攻擊之影響，但是絕大部分的民生必需之關鍵基礎設施皆維持正常運作，該國政府也未動用軍事力量回應攻擊。

即使這場網路攻擊事件是出於政治動機，與網路恐怖主義之動機相符，但是除了攻擊者之身分難以確認，因而無法歸類之外，包括「攻擊目標」、「行為目的」及「影響所及範圍」等三個面向皆不合乎網路恐怖主義或網路戰爭之定義，因此，這場網路攻擊事件應當歸類為「具有網路恐怖主義部分特徵之網路犯罪」。

二、該事件對於各國防治網路恐怖主義之啟發

愛沙尼亞國內通訊科技發達，相關產業佔 GDP 比例過半，並且高度依賴網際網路，雖然民眾日常生活十分便利，卻也使得社會對於網路攻擊存在高脆弱性。一旦爆發大規模網路攻擊，極可能迅速對社會各層面造成重大災害。以此對照美國目前的情況，雖然對於網際網路的依賴可能不若愛沙尼亞，但是美國的幅員及人口皆數百倍於愛沙尼亞，其對於世界經濟的重要性而言，亦遠非愛沙尼亞所能相比。隨著科技逐漸普及，公私部門架設之網站數量與日俱增，民眾生活與網際網路息息相關，各種網際網路活動頻繁熱絡，倘若網路恐怖份子發動攻擊，癱瘓重要網站，並入侵關鍵基礎設施之 SCADA 系統，肆意引發重大災害，則愛沙尼亞在 2007 年 4 月網路攻擊事件所受到衝擊和影響的程度，恐怕將遠遠不及美國社會遭遇到的混亂和恐慌。

愛沙尼亞政府在危機之中的快速反應，包括產官學界的通力合作與密切聯繫，迅速且確實地掌握社會各層面受到攻擊影響的情況，並且找出網站癱瘓的原因，在短短幾天之內便恢復正常運作，其危機處理之效率值得各國學習。

此外，在事後追究責任方面，由於攻擊者之身分十分難以確認，時常導致受害國無從報復或要求賠償。網路犯罪屬於國內執法問題，網路恐怖主義是由政治或宗教等動機驅使，而網路戰爭則屬於國家權威之行為，[73]但是三者皆與個人行為者密切相關。在不確定攻擊行為是網路犯罪、網路恐怖主義抑或網路戰爭的情況下，亦無法決定應由司法機制、反恐單位或軍事武力來回應攻擊，或是譴責其他國家等等，這也顯示出，明確區分網路犯罪、網路恐怖主義和網路戰爭之間的差異，對國家而言確實有其必要。除非未來網路追蹤定位相關科技有所突破，否則這將一直會是國家遭受網路攻擊之後，決策者必然面對的一大難題。

小結

本章針對網路恐怖主義之眾多定義進行統整，首先探討網路恐怖主義和傳統恐怖主義之間的主要差異與共同特徵，以及網路恐怖主義缺乏明確定義之原因；接著討論重要學者對於各種網際網路使用行為之分類，其中亦包括「網路策劃」與網路恐怖主義之間的分野，並且主張針對網路恐怖主義採用較嚴格之認定，從而將「網路策劃」排除於網路恐怖主義的定義範疇之外。再者，本章參考重要學者之見解，提出網路恐怖主義之「**攻擊者之身分**」、「**行為動機**」、「**攻擊目標**」、「**行為目的**」及「**影響所及範圍**」等五大重要判別標準，據以檢視網際網路使用行為與網路恐怖主義之關係，並且以之建立本論文對於網路恐怖主義的界定。即使網路恐怖主義、網路犯罪及網路戰爭皆透過網際網路進行攻擊，具有一定程度之重疊，但是透過對照前述之五大判別標準，便可清楚觀察三者之間的顯著差異，不致發生混淆。

2007 年 4 月愛沙尼亞遭受大規模網路攻擊事件一例，雖然依據上述之五大重要判別標準可知，其並不完全符合本論文對於網路恐怖主義之定義，但是藉由檢視該國之危機處理程序與後續政策措施，依然足以做為各國防治網路恐怖主義

[73] Anthony H. Cordesman & Justin G. Cordesman, *Cyber-threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland* (Westport, CT: Praeger, 2002), p. 168.

攻擊之良好借鑒，同時亦突顯出國家應針對網路犯罪、網路恐怖主義和網路戰爭之間的差異，儘速建立明確界定與規範之必要性。

國立政治大學 National Chengchi University

第三章　網路恐怖主義威脅之爭辯

Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb.

National Research Council[1]

There's just one problem: There is no such thing as cyberterrorism—no instance of anyone ever having been killed by a terrorist (or anyone else) using a computer. Nor is there compelling evidence that al Qaeda or any other terrorist organization has resorted to computers for any sort of serious destructive activity.

Joshua Green[2]

截至目前，各界對於網路恐怖主義的定義及威脅程度之看法，仍然是眾說紛紜，莫衷一是。學界、企業界和政府部門所著重之面向各有異同，相關論述散見於學術著作、期刊文章及政府公開文件等等。之所以會形成如此的爭論現象，Andrew M. Colarik 將其歸責於網路恐怖主義仍舊缺乏一個明確的法律定義（legislatively defined meaning）。[3]究其原因，不僅是由於網際網路科技的快速發展，各種日新月異的應用方式，造成此一概念難以精確定義，也根源自恐怖主義本身的定義仍未形成一致的共識，導致網路恐怖主義研究開始步上傳統恐怖主義研究的後塵，兩者皆遭遇到許多困難，相關的學術和政治辯論也非常激烈。[4]

[1] National Research Council, *Computers at Risk: Safe Computing in the Information Age* (Washington, DC: National Academies Press, 1991), p. 7.
[2] Joshua Green, "The Myth of Cyberterrorism," *op. cit.*, pp. 8-9.
[3] Andrew M. Colarik, *op. cit.*, pp. 45-46.
[4] Timothy F. O'Hara, "Cyber Warfare/Cyber Terrorism," p. 13, ＜http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA424310＞(Retrieved on February 1, 2012).

除了針對定義問題未能取得共識之外，由於全球尚未發生過大規模網路恐怖主義攻擊事件，各國的關鍵基礎設施若非因戰爭而遭受破壞，絕大部分仍然是因天災所導致，因而在缺乏實際案例的情況下，更加深了許多專家學者對於網路恐怖主義是否構成嚴重威脅之質疑。例如 Joshua Green 認為，早在 911 事件發生之前，小布希政府便一直不遺餘力地向民眾宣導，除了謹慎提防生物、化學與核子武器攻擊以外，也應重視網路恐怖主義的威脅，然而網路恐怖攻擊卻從未發生過真實案例，即使當前「網路安全」議題的確重要，但是此議題實際上與恐怖份子之間毫無關聯。[5]

不同於 Green 之觀點，Simon Finch 則主張，就在政治家開始重視網路恐怖主義的當下，恐怖份子也同樣注意到了這個未來趨勢，從金融動盪（financial turmoil）、電力中斷、交通大亂、控制通訊衛星到攻擊供應民生物資的公司等等，恐怖份子擁有各式各樣的攻擊選擇。縱使核子武器和敏感度極高的軍用系統已經與網際網路在實體上完全分離，卻仍然有其他非常多的系統正與網際網路保持連接，例如許多民間企業將防火牆程式（firewall）視為安全之保障，但是對於有心人士來說，其實只是聊勝於無。[6]

在各方看法歧異的情況下，如何評估網路恐怖主義潛在的威脅性便顯得十分重要。Dorothy E. Denning 指出，威脅性之評估必須考慮兩個要素：

1. 是否有易受攻擊且可能導致破壞或嚴重傷害的目標存在？
2. 是否有具備如此能力及動機發動攻擊的行為者存在？[7]

要回答這兩個問題，勢必要深入探討學界如何看待網路恐怖主義之威脅程度。許多專家學者認為，美國政府之所以如此重視網路恐怖主義之威脅，其實是該威脅被誤解、過度誇大、刻意炒作，或是由於其他原因所造成的結果，本章首先將整理這些看法，了解他們主張網路恐怖主義不應被視為嚴重威脅的依據為何，以及若過於強調網路恐怖主義之威脅，有何不良後果；接著列舉持贊成重視

[5] Joshua Green, "The Problem of Cyberterrorism is Exaggerated," *op. cit.*, pp. 41-43.
[6] Simon Finch, *op. cit.*, p. 37.
[7] Dorothy E. Denning, "Is Cyber Terror Next?" *op. cit*.

威脅之見解，與第一節相互呼應，做一對照，嘗試理解這些專家學者何以提出不同的觀點；最後則進行主要爭議焦點的整理與評價，並提出筆者之意見，嘗試評估網路恐怖主義之威脅程度，希冀能從各方的爭辯當中，形塑出比較接近實際情況的論述。

第一節　網路恐怖主義並非嚴重威脅之主張

對於網路恐怖主義是否已對國家安全以及關鍵基礎設施構成實質威脅，許多專家學者皆曾提出過懷疑，理由不一而足。以下首先分點列舉專家學者認為網路恐怖主義不應被視為嚴重威脅的主要論據，以及是網路恐怖主義之威脅程度為何會被誇大的原因，最後則是倘若美國社會及政府過於強調網路恐怖主義之威脅程度，可能會有哪些不良影響。

壹、主要論據

目前已發現許多軟體的各種缺陷及漏洞，並且透過網際網路四處流傳，早已廣為眾人所知，即使如此，為何恐怖份子尚未加以利用，發動攻擊並造成任何破壞？主張網路恐怖主義並非嚴重威脅之看法，其所持之主要理由大致可分為下列四項：

1. 網路恐怖攻擊之本益比不及傳統恐怖攻擊；
2. 恐怖份子尚無能力發動網路恐怖攻擊；
3. 關鍵基礎設施足以抵禦網路恐怖攻擊；
4. 「網路策劃」（Cyberplanning）之威脅更加迫切。

由此可知，網路恐怖攻擊之成本—效益比，以及恐怖份子自身的能力皆受到質疑，換言之，發動網路恐怖攻擊所需成本較高，攻擊效果卻不如預期，或是恐

怖份子能力不足，網路恐怖攻擊之發生機率和威脅程度自然不高。在此同時，對於關鍵基礎設施抵禦網路恐怖攻擊的能力，這些專家學者則抱持高度信心，即使網路恐怖份子發動攻擊，亦無法造成太大傷害。相較之下，「網路策劃」所帶來的威脅，可能比網路恐怖主義更加嚴重。

一、網路恐怖攻擊之本益比不及傳統恐怖攻擊

在全球反恐行動的打擊之下，大多數恐怖份子能持有的資源有限，必須妥善運用，以追求最大效果。以此為前提，許多專家學者分別從網路恐怖攻擊之「成本」與「效果」兩方面分析網路恐怖主義，整理如下：

（一）網路恐怖攻擊之成本

以恐怖份子的角度而言，在發動網路恐怖攻擊之前，必須動用大量資金購買電子設備、訓練或招募具備高度專業知識的人員，再耗費長時間嘗試及滲透系統弱點等。相較之下，傳統的恐怖攻擊方式不但較為方便、簡易，所需的資金和時間成本也較低。除非網路恐怖主義能夠達成與傳統恐怖主義相同或是更佳效果，才會成為恐怖份子的理性選擇，否則他們仍然會選擇炸彈或劫機等已知的傳統恐怖攻擊形式。[8]

（二）網路恐怖攻擊之效果

2002 年，美國海軍戰爭學院（U.S. Naval War College）曾舉行一場名為「數位珍珠港」（Digital Pearl Harbor）的電子演習。根據演習結果，該團隊所做出之

[8] 請參見：Joshua Green, “The Problem of Cyberterrorism is Exaggerated,” *op. cit.*, p. 49; Michael Stohl, “Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games?” *Crime, Law and Social Change*, Vol. 46, No. 4-5 (December 2006), pp. 232-233.

結論為：如此規模之攻擊行動，可削弱人口密集區域之通訊能力，但是無法造成人員死亡或其他災難性後果。[9]

除此之外，有不少專家學者也主張，網路恐怖攻擊的效果無法與傳統恐怖攻擊相提並論。例如 Dorothy E. Denning 便認為，除非能夠造成傷亡，否則網路恐怖主義所帶來的戲劇性和情緒感染力，依舊不及傳統恐怖主義。[10]Andrew Jones 則強調，網路恐怖主義何以尚未發生實際案例的主要原因，便是由於其攻擊效果不若傳統恐怖攻擊具有強烈的震撼性。Jones 進一步分析，在發生網路攻擊後的短時間之內，發動攻擊者的真實身分往往非常難以查證，因此恐怖組織若在事後宣布該攻擊行動是由他們發起，可信度不免大打折扣。[11]在尚未確認攻擊來源之前，恐怖組織發言的可信度將嚴重影響他們提出訴求的力度，倘若訴求未獲得有關當局重視，攻擊行動便稱不上成功。

網路恐怖主義亦可能襲擊電力供應網絡，造成大範圍的停電。不過，有幾位專家學者從各自的角度切入，主張攻擊導致停電的效果尚不足以引發大眾的恐懼，這是因為一般人對於偶發的停電狀況早已習慣。例如 Andrew Jones 以 2003 年 8 月曾影響五千萬人口的美國東岸大停電事件為例，即使是在相關單位查明導致大停電的真正原因之前，也沒有明確證據顯示，受到影響的民眾普遍認為這是針對美國基礎設施的恐怖攻擊。倘若大多數民眾已對諸如停電這類偶發狀況習以為常，恐怖份子如何能透過攻擊關鍵基礎設施，達成恐嚇大眾的目標？不僅如此，停電對於極度依賴電力供應的先進國家之影響程度，又遠高於其他較落後的國家，這些國家的民眾更不可能僅因停電便產生恐慌。[12]

另有學者發現，與容易使人聯想到死亡和毀滅景象的墜機事件和炸彈攻擊相比，人們對於一個電力供應系統遭受網路恐怖攻擊，因而被迫關閉並導致停電的情況，將會產生截然不同的反應。部分原因來自於民眾日常生活都曾遇到暫時的

[9] 引用自：Robert Lemos, “What are the Real Risks of Cyberterrorism?” ＜http://www.zdnet.com/news/what-are-the-real-risks-of-cyberterrorism/124765＞(Retrieved on May 28, 2012).
[10] Dorothy E. Denning, “Cyberterrorism,” *op. cit.*
[11] Andrew Jones, *op. cit.*, p. 5.
[12] Andrew Jones, *op. cit.*, pp. 4-5.

電力中斷，已不足為懼。而對於許多恐怖組織而言，他們早已熟知如何操縱視聽大眾的行為反應，必然也會仔細盤算如何有效利用現有資源。[13]

此外，尚有學者根據許多災難後研究的結果指出，當災害發生時，群眾很少出現集體恐慌的情況，多數人仍然保持理性。停電時的情況也十分類似，人們會聚在一起，並且相互協助，雖然感到十分不便及苦惱，卻不致於心生恐懼。即使是嚴重如 911 事件或 2005 年卡崔娜颶風（Hurricane Katrina）等重大災難，民眾的反應仍然與其他災害發生時無異，社會上沒有出現太多的恐慌、癱瘓或失序。況且，911 事件不僅未能瓦解美國社會，迫使美國退出中東，反而使人心益發凝聚，美國的外交政策亦更加著重於中東；2005 年卡崔娜颶風雖然重創美國墨西哥灣沿岸地區的經濟，但仍未導致整體經濟崩潰。經過實證研究顯示，無論是美國的經濟還是人民的集體反應，都具有足夠能力應付天災或人禍所帶來的災害。倘若自然或人為的重大災難都無法導致人心恐慌、社會癱瘓、科技和經濟的崩壞，某些網路安全專家建構出的「網路末日情境」（Cyber-Doom Scenarios）[14]，例如「網路 911」（Cyber-9/11）或「網路卡崔娜」（Cyber-Katrina）等等，也就不太可能引發這些效果。[15]

在成本高昂、效果不佳的情況下，網路恐怖攻擊行動失敗的風險，是否可能對恐怖份子產生嚇阻作用？對此，Dorothy E. Denning抱持肯定的態度。只要傳統攻擊方式仍然有效，恐怖份子不太可能嘗試新手法，尤其是這個新手法需要大量相關知識和技術做為基礎；反之，恐怖份子通常十分保守，如果既有的攻擊手段足以確保攻擊行動能夠順利完成，相較之下，攻擊手法的新奇性和複雜性對他們來說並不重要。[16]

---

[13] Michael Stohl, *op. cit.*, pp. 234-235.
[14] 例如：Richard A. Clarke & Robert K. Knake, *op. cit.*, pp. 64-68.
[15] Sean Lawson, "Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History," pp. 16-21, ＜http://mercatus.org/sites/default/files/publication/beyond-cyber-doom-cyber-attack-scenarios-evidence-history_1.pdf＞(Retrieved on May 29, 2012).
[16] Dorothy E. Denning, "Cyberterrorism," *op. cit*.

二、恐怖份子尚無能力發動網路恐怖攻擊

除了網路恐怖攻擊的效果不彰以外，恐怖份子是否具備足夠能力發動網路恐怖攻擊，也受到許多專家學者質疑。例如 Dorothy E. Denning 指出，許多駭客擁有攻擊電腦系統所需的知識、技術和工具，但是他們通常缺乏引發重大經濟或社會災難的動機；相反地，縱使恐怖份子引發嚴重災難之強烈動機無庸置疑，但是以他們目前的科技能力，尚不足以透過網路恐怖主義遂其所願。[17]

有學者引用 2002 年「數位珍珠港」電子演習團隊的成果報告表示，恐怖份子確實可能針對國家的基礎設施發動大規模網路攻擊，然而也必須具備兩億美元、高度專業知識，以及五年的準備時間等等先決條件。[18]

Andrew Jones 引述一份由美國國會圖書館國會研究中心（Library of Congress congressional research center）向美國國會提交的報告指出，不論是經由大規模、小規模之攻擊方式，甚至以可攜式的電磁脈衝（Electromagnetic Pulse, EMP）武器[19]針對美國電腦系統發動攻擊，其所需的技術皆已超出絕大多數的恐怖組織之能力所及。[20]

對於透過網路攻擊能夠造成實際的人員傷亡或其他持續性的破壞效果，有學者抱持保留態度。例如 Robert Lemos 認為，網路恐怖份子想要從外部入侵 SCADA 系統非常困難，除了必須具備相當程度的相關專業知識，還得克服各種非經電腦控制的保護機制，比方由系統監控人員進行的手動操作及維修等等，再加上各項基礎設施的營運公司大多都有備用系統隨時待命，防範突發狀況等等。因此，與入侵電腦相比，使用炸彈攻擊目標還是相對簡單得多。[21]

---

[17] Dorothy E. Denning, “Is Cyber Terror Next?” *op. cit.*
[18] Robert Lemos, *op. cit.*
[19] 當電磁脈衝武器爆炸時，電磁輻射以光速由爆點向四面八方射出，並和空氣中的氧、氮原子相撞擊，產生帶負電之電子，形成極強的電磁脈衝，進而對衝擊範圍以內的指揮、控制和通信用電子設備、電腦及網路系統造成破壞，並能干擾大部分的無線電通訊。
[20] Andrew Jones, *op. cit.*, p. 5.
[21] Robert Lemos, *op. cit.*

三、關鍵基礎設施足以抵禦網路恐怖攻擊

以上兩小節之反對意見皆針對網路恐怖主義的攻擊方論述，本小節則針對防禦方，亦即關鍵基礎設施抵禦網路恐怖攻擊之能力，統整相關論點。

美國政府對於關鍵基礎設施的維安機制，有不少專家學者給予相當肯定。由於早在 911 事件發生之前，美國政府已非常重視情報安全相關事務，例如軍方早已使用與外界隔離的內部網路，將軍事指揮系統自網際網路徹底分離，國防部某些關鍵系統甚至隔絕於五角大廈（Pentagon）的內部網絡之外，所有新軟體也必須先經過國家安全局的安全檢驗，以阻隔一切可能的外部入侵者。[22]

在私部門方面，重要的民用設施如水壩、發電廠、石油設備和航空指揮管制系統等等，由於通常僅有公司少數員工熟悉操作 SCADA 系統所需的專業知識，即使外人成功入侵系統，想要造成實質的嚴重破壞卻比入侵更加困難，因此入侵者比較可能來自公司內部。雖然恐怖主義團體可能會吸收這些掌握關鍵知識的公司員工，但是這些基礎設施的 SCADA 系統隨時都有人員負責監控，以預防天災或任何意外狀況發生，而員工也對處理突發狀況十分熟練，使得恐怖份子難以引發重大破壞。[23]

另有學者從關鍵基礎設施之防護是否完善的角度，探討網路戰爭及網路恐怖主義對於關鍵基礎設施的攻擊能否構成實質威脅。早在第一次世界大戰時期，便已出現以空軍轟炸敵方關鍵基礎設施，從而削弱敵方戰爭能力的思想，到了第二次世界大戰，英美兩國也大量運用戰略轟炸。然而美國對於戰略轟炸效果評估的報告顯示，戰略轟炸無法有效癱瘓納粹德國的工業力量，實際上，工業社會的抗災能力十分驚人。即使網路攻擊可能使某些關鍵基礎設施失靈，但是關鍵基礎設施偶爾失靈的情況，在現代社會其實平凡無奇，加上維修人員早已習於應付各種突發狀況，因此對國家安全並不構成迫切且嚴重的威脅。網路恐怖份子若企圖引

[22] Joshua Green, *op. cit.*, pp. 43-44.
[23] *Ibid*, pp. 47-48.

發恐懼，必須要同時攻擊多個關鍵基礎設施，並且維持很長一段時間，而他們尚未具備發動如此規模之攻擊的能力。[24]

四、「網路策劃」之威脅更加迫切

第二章曾經提到，Timothy L. Thomas 將恐怖份子利用網際網路進行搜集資料、宣傳理念、籌措金援、交換情報、遙控指揮、組織動員、招募新血及隱匿行蹤等活動，統稱為「網路策劃」，而網路恐怖主義亦可能包括在整個網路策劃當中。Thomas 主張，相較於尚未有實際案例發生之網路恐怖主義攻擊行動，同樣是以網際網路做為輔助工具的恐怖主義活動，「網路策劃」所帶來之威脅，可能與網路恐怖主義之威脅不相上下，甚至更加嚴重，政府應從法律面和政策面限制恐怖份子的網路策劃能力。[25]

貳、網路恐怖主義之威脅程度被誇大的原因

在上述四項反對網路恐怖主義已構成嚴重威脅的主要論據之外，還有一些專家學者提出質疑，認為網路恐怖主義之威脅已被過度誇大，並且舉出三項可能的原因，包括：

1. 人類對於未知事物固有的恐懼心理；
2. 對於網路恐怖主義之誤解；
3. 有心人士的刻意炒作。

以下將依序分析這些原因，從而了解網路恐怖主義的威脅程度倘若確實被誇大，其背景因素和可能動機為何。

---

[24] James A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," *op. cit.*, pp. 2-3.
[25] Timothy L. Thomas, *op. cit.*, p. 122.

一、人類對於未知事物固有的恐懼心理

美國著名小說家 Howard P. Lovecraft 曾寫道：「人類最古老而強烈的情緒，便是恐懼；而最古老最強烈的恐懼，便是對未知的恐懼。」[26]可謂一語道破人類恐懼的根源。Joshua Green 認為，由此觀察政府決策高層和立法機關對於網路恐怖主義的各種災難臆想之所以會層出不窮，可能正是由於網路恐怖主義恰好結合了這些官員並不完全了解的兩個領域：「恐怖主義」與「科技」，而「恐懼」正是源自於「不了解」，這使得他們更傾向於採取任何措施，以求自保。[27]

與此類似之觀點，例如有學者指出，即使網路恐怖主義只是一個潛在威脅而非正在發生的一連串事件，大眾媒體卻已經成功使人們以為「數位珍珠港」事件必然會爆發，只是時間早晚的問題而已，網路安全岌岌可危。而一般人之所以會對網路恐怖主義威脅產生誤解的根本原因有二，一是恐懼，一是無知；恐懼包括對於科技的恐懼，以及對於恐怖主義的恐懼，而無知可能是由於資訊不足，或是過多錯誤資訊所導致。[28]

相較於上述主張人類對於未知事物的原始恐懼之觀點，另有學者則進一步研究人類為何對科技產生不信任感的原因。西方工業社會的人們之所以會對網路戰爭及網路恐怖主義等議題感到如此畏懼，除了出於對恐怖主義、未知事物和新科技的恐懼之外，根本原因乃是源自於上個世紀對於科技失控的恐懼。相對於 19 世紀人們認為科技創新是人類進步的關鍵所在，到了 20 世紀時，即使科技是形塑後現代世界（post-modern world）最重要的力量，人們卻擔心科技發展過快，最終不受人類控制。近年來對於網路安全議題的諸多關切，便是這種擔憂的最新型態。隨著人類生活日漸依賴科技，人們已開始產生一種既驚嘆於現代科技的創

[26] "Supernatural Horror in Literature by H. P. Lovecraft," ＜http://www.hplovecraft.com/writings/texts/essays/shil.asp＞(Retrieved on June 14, 2012).
[27] Joshua Green, "The Problem of Cyberterrorism is Exaggerated," *op. cit.*, p. 49.
[28] Michael Stohl, *op. cit.*, p. 225.

新成果，同時卻又認為人類社會的集體生活終將失去控制之矛盾心理，即「科技悲觀主義」（Technological Pessimism）。[29]

二、對於網路恐怖主義之誤解

既然網路恐怖主義尚缺乏一個明確定義，則一般人會產生誤解，可謂十分自然之事。但是，如果此種誤解導致國家錯估網路恐怖主義之威脅程度，將可能造成國家浪費過多資源，反而忽視真正迫切的威脅。

Robert Lemos 將網路攻擊分為兩種形態，一種是針對電子資料的偷竊、破壞或竄改等等，另一種則是企圖接管或干擾控制系統的能力。許多人對於「網路恐怖主義」一詞倍感困惑，以為其所指涉的是第一種網路攻擊，導致這個詞彙已然成為「一個無所不包的流行語」（a catchall buzzword），更令人聯想到政府加強對人民的監控，以及實施更嚴格的出入境管制等各種政治惡夢。[30]

另一方面，Gabriel Weimann 則強調大眾媒體之影響。出於銷路考量，大眾媒體經常刻意渲染網路恐怖主義的威脅程度，然而它們不僅未能分辨駭客行為和網路恐怖主義之間的區別，更時常進行錯誤的類比，並誇大後者的威脅，例如：「假使一個 16 歲的青少年都能辦到，那麼一個資金充裕的恐怖組織呢？」Weimann 主張，即使學界對於恐怖主義可能有上百種定義，但是「恐懼」（fear）仍然是恐怖主義的關鍵要素，以「恐懼」做為判斷標準，便可將大多數的網路攻擊事件排除在網路恐怖主義之外。據此，恐怖份子以電腦做為宣傳、招募、情蒐或通訊等用途之工具，這些行為都不能算是網路恐怖主義。[31]

[29] Sean Lawson, *op. cit.*, p. 8.
[30] Robert Lemos, *op. cit.*
[31] Gabriel Weimann, "Cyberterrorism: The Sum of All Fears?" *op. cit.*, p. 132.

三、有心人士的刻意炒作

在人類固有的恐懼心理和對於網路恐怖主義的誤解以外，有心人士亦可能操縱議題，使之為其自身利益服務。出於此種疑慮，部分新聞從業者撰文質疑，近年來眾多智庫、網路安全公司、國防工業承包商及企業領袖不斷鼓吹美國政府持續關切網路安全議題，重視網路戰爭及網路恐怖主義之嚴重威脅，其背後動機可能大多都是為個人或公司圖利，並且讓國家因而必須繼續求助於這些專家。例如有人批評，有關網路安全議題的許多細節技術資訊，要不是過於專業，就是屬於機密，一般人無從理解威脅的真實性與否，只能聽信網路安全專家的說法。然而事實上，個人及民間企業皆有足夠動機進行自我保護，政府不應花費鉅額資金，投入早已過度炒作的網路安全議題。[32]還有人直言抨擊美國政府放任某些高層官員在政府部門和民間企業之間頻繁出任重要職位的情況，完全不符合「旋轉門」的利益迴避原則。[33]

在眾多現任及前任政府官員之中，Richard A. Clarke 遭到不少專家學者的非議，包括 Michael Stohl 與 Gabriel Weimann 皆直指他正是炒作網路恐怖主義議題的代表人物。其中 Stohl 指出，在 Clarke 退出小布希執政團隊，並公開批評小布希政府的反恐策略之後，他很快便成為媒體寵兒。每當政府編列預算之際，他也總是提出相關議題引發討論，不遺餘力地讓這個議題的熱度延續下去。[34]而 Weimann 也認為，在 911 事件發生後，包括 Clarke 在內的部分政府官員及顧問，為了各自的目的大力宣揚網路恐怖主義的嚴重威脅，已成功地大幅提高美國政府對於該議題的重視程度。[35]

除了個人倡議者之外，出於銷售商品之考量，許多網路安全公司自然也具備向政府部門提出威脅警告，同時大力宣傳自家產品的充分動機，尤其是在數位科

---

[32] Stephan M. Walt, "Is the Cyber Threat Overblown?" ＜http://walt.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown＞(Retrieved on May 29, 2012).

[33] Glenn Greenwald, "Mike McConnell, the WashPost & the Dangers of Sleazy Corporatism," ＜http://www.salon.com/2010/03/29/mcconnell_3/＞(Retrieved on May 29, 2012).

[34] Michael Stohl, *op. cit.*, pp. 225-226.

[35] Gabriel Weimann, "Cyberterrorism: The Sum of All Fears?" *op. cit.*, pp. 132-133.

技的使用者與日俱增之後，更是如此。[36]在網路產業泡沫化之後，許多民間的網路安全公司必須尋求新的資金來源，這些公司因而不斷向政府強調網路恐怖主義的潛在威脅，企圖營造恐懼氛圍。如此之行為不僅由於有利可圖，也正因為政府的無知已成為最佳的遊說著力點，從而讓這些公司獲得大量的國家資金挹注，維繫自身的生存。[37]

再者，美國的政治生態也扮演了推波助瀾的角色。美國的執政黨和在野黨向來總是會為了大選炒作特定議題，在位者和挑戰者各自向社會大眾展示國家的潛在弱點和威脅何在，並且竭力說明為何必須投資於各種預防措施和改善計畫，1950 年代和 1960 年代的核武議題及軍備競賽都是實例。因此，每逢大選前夕或是編列預算時，美國國內便會出現類似的循環。[38]

參、政府誇大網路恐怖主義威脅之不良後果

人類對於未知事物和科技的固有恐懼，加上個人、大眾媒體、網路安全相關產業及國內政治生態的諸多影響，可能已造成美國國內瀰漫一種不必要的恐懼氛圍。部分專家學者認為，這種氛圍將產生諸多不良後果。例如 Joshua Green 批評，小布希政府大力宣傳網路恐怖主義此一根本不存在的威脅，不僅使得公私部門將大量資金投入於購買各種效果不彰的網路安全相關軟體，還可能導致公眾逐漸忽視其他真正的威脅。在此同時，小布希政府卻拒絕要求軟體業必須提供安全可靠、設計完善的產品，更是本末倒置的政策，無法有效維護國家安全。[39]

Andrew Jones 則認為，911 事件之後，許多國家對於恐怖主義威脅的敏感度已大幅提高，而人類對於網路科技的大量應用和依賴，使得在網際網路上出現的任何干擾或破壞，都有可能引發嚴重影響，而這兩個要素結合在一起的結果，便是許多對於網路恐怖主義潛在威脅不成比例（disproportionate）的過度反應。只

[36] Michael Stohl, *op. cit.*, p. 227.
[37] Joshua Green, "The Problem of Cyberterrorism is Exaggerated," *op. cit.*, pp. 49-50.
[38] Michael Stohl, *op. cit.*, p. 225.
[39] Joshua Green, "The Myth of Cyberterrorism," *op. cit.*, p. 13.

要人們日常生活對網路科技的依賴程度持續與日俱增，固然會存在某些潛在威脅，但是倘若人們習於使用或濫用「網路恐怖主義」這一詞彙，來指稱在網際網路上那些零星且情節輕微的青少年駭客行為，將很可能對於未來真正的網路恐怖主義攻擊毫無反應，或是反應過慢，最終印證「狼來了」的寓言故事。[40]

此外，尚有學者以為，美國政府過於重視威脅程度尚且模糊不清的網路安全議題，其真正的代價可能是縱容國家安全局等政府單位更加全面地掌控網際網路，危害人民自由。[41]由於當前更迫切的恐怖份子威脅仍然是實體的形式，因此，針對網路恐怖主義的熱烈討論，不但會使人們轉移焦點，還可能適得其反，促使恐怖份子更加了解網路恐怖主義的潛力何在。[42]

以上針對網路恐怖主義之威脅抱持保守立場或否定其真實存在的主張，進行敘述及統整。由這些論點來看，網路恐怖主義除了因未曾發生實際案例而引發懷疑，加上人類對於未知事物的恐懼心理，以及對網路恐怖主義之誤解所造成不必要的危機意識之外，目前網路恐怖攻擊的效果仍不及傳統恐怖攻擊，無法成為恐怖份子的優先選擇方案，況且他們也尚未擁有發動網路恐怖攻擊的能力。如果美國國內關鍵基礎設施確實足以抵禦網路恐怖攻擊，則美國政府不僅不應理會部分人士的刻意炒作，還應該調整政策方向，正視其他更迫切的潛在威脅，例如「網路策劃」等等。

第二節　網路恐怖主義確為嚴重威脅之主張

為與上一節之懷疑或否定觀點相互對照，本節整理主張網路恐怖主義已構成嚴重威脅或即將成為嚴重威脅之主張，觀察它們針對同一項議題有何不同之看

[40] Andrew Jones, *op. cit.*, pp. 5-7.
[41] Glenn Greenwald, *op. cit*.
[42] Mark Trevelyan, "Security Experts Split on 'Cyberterrorism' Threat," ＜http://www.reuters.com/article/2008/04/16/us-security-cyberspace-idUSL1692021220080416＞(Retrieved on June 1, 2012).

法，以及所持論據為何。除此之外，一旦發生針對關鍵基礎設施的網路攻擊，專家學者預測可能出現的災情為何，本節也將進行綜整。

壹、主要論據

相對於各種反面意見，主張重視網路恐怖主義威脅之專家學者，也提出各自的論據，以為佐證。主要包括：

1. 網路攻擊造成停電的影響非比尋常；
2. 恐怖份子可能與駭客合作；
3. 關鍵基礎設施無法抵禦網路恐怖攻擊；
4. 恐怖主義不適用於一般風險評估。

由此觀之，這些論點不僅強調網路恐怖攻擊之嚴重後果，恐怖份子亦可能透過駭客獲得發動網路恐怖攻擊的知識，而關鍵基礎設施抵禦網路恐怖攻擊的能力也不足。尤有甚者，由於恐怖份子不一定是理性行為者，恐怖主義可能不應以一般的成本效益比來衡量其發生機率。

一、網路攻擊造成停電的影響非比尋常

有學者指出，即使大多數的美國人都曾經歷過短暫的區域性停電，電力大約在一至兩個小時之內便會恢復供應，然而當針對電力供應網進行破壞的網路攻擊事件發生時，情況卻將大不相同。由於美國發電設施的大部分零件皆需仰賴中國或印度供應，當這些零件因過度負載等原因導致損毀時，美國將缺乏迅速修復的能力。倘若攻擊行為是經中國政府授意發動，中國更沒有在短時間之內將新零件運送至美國的動機。[43]對絕大多數的人們來說，電力長期中斷將是難以忍受的，情況可能會如同 Richard A. Clarke 的描述：「數以百萬計的民眾被迫在黑暗和寒

[43] Ron Rhodes, *op. cit.*, p. 75.

冷中度日，無法取得食物和現金，遑論處理社會上的各種失序現象，如此的情況和城市遭到轟炸後的景象之間，有諸多相似之處。」[44]

對於長期停電之下，美國經濟將遭受如何嚴重的打擊，亦有學者做出預測：在剛開始的幾天之內，停電地區尚能維持運作正常，但是經過八到十天之後，這些地區 72%的經濟活動都會被迫停止。若是大規模的長期停電長達數個月之久，這對於美國經濟將產生近似於遭受核武攻擊的負面影響。[45]

二、恐怖份子可能與駭客合作

Dorothy E. Denning 認為，即使大多數的電腦駭客並不願意訴諸真實的暴力行為，仍不免有少數人會與恐怖份子保持聯繫。此外，新一代的恐怖份子自幼即在數位時代中成長，這群人將更加熟悉網際網路的操作知識，更能掌握威力強大且易於使用的破壞工具，並且可能了解到網路恐怖主義所具有的極大潛力，正當行動電話和其他電子裝置紛紛連上網際網路，實體和虛擬的兩個世界正逐漸結合之同時，除非這些系統皆受到妥善管理，否則未來的網路恐怖份子以虛擬方式造成實質傷害，可能就如同今天的駭客滲透網頁一般輕易。[46]

Susan W. Brenner 及 Marc D. Goodman 在探討「網路恐怖主義為何尚未證實自身的存在？」（why has cyberterrorism not yet manifested itself?）此一問題時提到，有些人對此問題的結論是：國際恐怖份子尚未擁有足夠的技術背景知識和電腦專業能力。不過兩位專家學者指出，如此的結論忽略了兩個問題：

1. 恐怖份子本身可能沒有發動攻擊所需要的技術和能力，但是國家卻不然，恐怖份子可能透過若干恐怖主義活動頻繁的國家，例如巴基斯坦（Pakistan）或斯里蘭卡（Sri Lanka）等，取得相關技術或能力。

---

[44] Richard A. Clarke, "War from Cyberspace," *The National Interest*, Vol. 104 (November/December 2009), p. 32, cited from Ron Rhodes, *op. cit.*, p. 75.

[45] Grant Gross, "U.S. Cyber War Policy Needs New Focus, Experts Say," ＜http://www.pcworld.com/article/174711/us_cyber_war_policy_needs_new_focus_experts_say.html＞ (Retrieved on June 14, 2012).

[46] Dorothy E. Denning, "Is Cyber Terror Next?" *op. cit*.

2. 恐怖份子可能雇用「駭客傭兵」（hacker mercenaries）為其效力，只要他們支付酬勞，這些駭客傭兵便同時擁有發動網路攻擊的專業知識和攻擊誘因。

回到「為何至今尚未出現網路恐怖主義實際攻擊案例」之問題，Brenner 和 Goodman 提出另一個可能原因：目前大多數恐怖組織的領導人都是出生於上個世代的人物，他們可能還沒見識到此種可做為替代方案的攻擊類型。[47]由 Brenner 和 Goodman 的論述可知，恐怖份子可能在其活躍的國家境內獲得電腦及網路知識，或是雇用駭客發動網路恐怖攻擊。在新生代領導人的指揮之下，網路恐怖主義有可能成為恐怖組織的選項之一。

2005 年 2 月，美國聯邦調查局局長 Robert S. Mueller 三世在美國參議院情報委員會的聽證會上強調，美國所面臨的網路威脅來源包括外國政府及獨立行動的個人行為者，兩者的數量皆快速增加中。其中恐怖份子已逐漸了解資訊科技對於美國經濟和國家安全日常活動的重要性，他們正試圖招募擁有數學、資訊工程及其他工程專長的年輕新血，以便攻擊美國的科技系統。此外，以金錢為動機的駭客數量亦不斷增加，形成國家安全的重大疑慮，倘若這個人才庫（pool of talent）為恐怖份子、外國政府或犯罪組織所用，以網路攻擊侵襲美國關鍵基礎設施的成功機率將大幅上升。[48]

另一方面，有學者舉出駭客為雇主提供服務的實際案例：2009 年，一群以色列網路安全人員向駭客購買了「殭屍網絡」服務，並且對黎巴嫩真主黨（Hezbollah）架設的網站發動網路攻擊，最終迫使其離線（off-line）。包含十部電腦的殭屍網絡之租金為一個月 20 美元，包含一千部電腦的殭屍網絡則是一個月 100 美元。該項服務甚至具有便於操作的介面，包括攻擊方式、攻擊速度和目

[47] Susan W. Brenner & Marc D. Goodman, "In Defense of Cyberterrorism: An Argument for Anticipating Cyber-Attacks," *University of Illinois Journal of Law, Technology & Policy*, Vol. 2002, Iss. 1 (Spring 2002), pp. 46-48, cited from Süleyman Özeren, *op. cit.*, p. 71.

[48] Robert S. Mueller, III, "Global Threats to the U.S. and the FBI's Response," testimony before the Senate Committee on Intelligence of the United States Senate, February 16, 2005, ＜http://www.fbi.gov/news/testimony/global-threats-to-the-u.s.-and-the-fbis-response-1＞(Retrieved on June 4, 2012).

標電腦的數量等等選項，提供使用者選擇。[49]明確的交易價格與多樣化的服務方案，顯示出這個市場在供需機制之下運作已久，恐怖份子確實可能以金錢換取駭客的服務。

三、關鍵基礎設施無法抵禦網路恐怖攻擊

針對美國國防體系之網路系統是否安全，Richard A. Clarke 和 Robert K. Knake 以 2008 年 11 月，一個發源於俄國的間諜程式（spyware）襲擊美國國防部的「非加密 IP 路由器網絡」（Non-classified IP Router Network, NIPRNET）[50]為案例說明，當時這個間諜程式在成功滲透進入 NIPRNET 之後，便開始搜尋並自我複製到每一個連接到 NIPRNET 的隨身碟（thumb drives）內。在這些受到感染的隨身碟之中，有一部分隨後又被使用者連接到國防部的「加密 IP 路由器網絡」（Secret Internet Protocol Router Network, SIPRNET）[51]，兩位專家因而認為，所謂「國防部外部網絡和內部網絡之間完全分離」的說法，只是虛有其表。更嚴重的是，由於 SIPRNET 並未連接到網際網路，理應不會遭到電腦病毒攻擊，因此大部分連接到 SIPRNET 的電腦均未安裝防毒軟體或防火牆（firewall）程式。換言之，國防部最重要之內部網絡上的電腦，它們所擁有的保護機制，可能還不如一般人的家用電腦。[52]

除了國防部的機密網絡安全並不可靠之外，美國國家安全最主要的弱點，可能正是關鍵基礎設施的 SCADA 系統，其面臨的安全威脅主要來自兩者，一為網際網路，一為內部人員，分述如下：

[49] Ron Rhodes, *op. cit.*, p. 54.
[50] 美國國防部提供內部人員傳遞敏感但非加密資料的網絡，並且以之連接到網際網路。
[51] 美國國防部提供內部人員傳遞加密資料的網絡，該網絡實體隔離在網際網路之外。
[52] Richard A. Clarke & Robert K. Knake, *op. cit.*, pp. 171-172.

（一）來自網際網路之威脅

就如同網際網路原本的開發理念是「公開」、「共享」一樣，這些依靠網際網路運作的 SCADA 系統在當初設計之時，也並未著重安全機制，因此許多資料時常被直接上傳到公開網路，任何人皆可下載取得。再者，出於經濟考量及自由市場等因素，SCADA 系統越來越仰賴開架式販售（off-the-shelf）的軟體充作安全修補程式（security patch）。然而，根據加州大學柏克萊分校（University of California, Berkeley）及卡內基美隆大學（Carnegie Mellon University）所進行的一項研究顯示，SCADA 系統在更新程式之前，可能需要幾個月的籌備工作，在更新時也必須停止系統運作，因此，頻繁地更新程式和修補安全漏洞的做法，可能並不適用於某些 SCADA 系統，這導致負責營運的公司在經濟因素或市場對其供應之需求孔急的情況下，取消這些程式更新作業。但是對於有心人士而言，這將使得 SCADA 系統成為十分具吸引力的目標。[53]

在網路時代來臨之前，大部分的關鍵基礎設施都是各自獨立的系統，相互之間不論在實體或虛擬連結的程度都不高，互賴程度也低，但是這種情況正在快速轉變當中。由於電腦和通訊科技的迅速進步，關鍵基礎設施管理人員原本以紙本進行的籌劃、設計、建造及營運等等，正逐漸被電子化作業取代，而關鍵基礎設施之間也因連結到網際網路，進而產生緊密關係。資訊科技的革新使得許多關鍵基礎設施之間的相互連結性（interconnectedness）和互賴程度（interdependencies）大幅提升，卻也同時提高對恐怖攻擊的脆弱性。[54]

隨著人類日常活動逐漸依賴自動化及遠端電腦遙控，工業界及關鍵基礎設施也捨棄專用的內部網路，轉而依靠透過網際網路連結的 SCADA 系統運作。然而，一旦國家未能在依賴網際網路和注重網路安全之間取得良好平衡，提高執法

[53] 引用自：Jack Jarmon, “Cyber-terrorism,” *Journal on Terrorism and Security Analysis*, Vol. 6 (April 2011), p. 114.
[54] 請參見：Yacov Y. Haimes, *op. cit.*, p. 232.

效率，並且確保關鍵基礎設施維安機制建全的話，網路恐怖主義可能將不再是言過其實的威脅。[55]

2011 年 4 月，美國聯邦調查局網路部助理部長（Assistant Director, Cyber Division, FBI）Gordon M. Snow 向美國參議院司法委員會犯罪及恐怖主義小組（Senate Judiciary Committee, Subcommittee on Crime and Terrorism）表示，由於惡意程式之取得性與複雜性的提升，加上新科技的應用同時也引發新的安全問題等情形，美國的關鍵基礎設施正面臨日益嚴重的網路威脅。隨著眾多關鍵基礎設施逐漸採用自動化作業，雖然使得營運管理程序更加便利，卻也導致更多可供他人利用的網路存取點（cyber access points）出現。[56]這些網路存取點若未經適當管制，便很可能成為安全漏洞。

（二）來自內部人員之威脅

另一方面，來自內部人員的潛在威脅亦不容忽視。Dorothy E. Denning 指出，由於關鍵基礎設施的系統十分複雜，眾多系統弱點很難完全消除，同時新的弱點也不斷被發現，即使系統所具備的安全機制已十分完善，獨自行動或與恐怖份子勾結的內部人員卻仍然可能濫用職權，引發嚴重災害。[57]

根據 1997 年一份由「總統關鍵基礎設施保護委員會」（President's Commission on Critical Infrastructure Protection）提出的報告顯示，對於心生不滿並試圖引發災難性後果的內部人員而言，SCADA 系統可說是最具吸引力的目標；隨著企業與政府單位之間資訊系統網絡相互連結的數量呈指數性成長，倘若入侵者能夠接觸到 SCADA 系統，並且更動操作指令或修改控制程式，導致關鍵設備向控制中

[55] James A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," *op. cit.*, p. 11.
[56] Gordon M. Snow, "Cybersecurity: Responding to the Threat of Cyber Crime and Terrorism," statement before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism, Washington, DC, April 12, 2011, ＜http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism＞(Retrieved on June 4, 2012).
[57] Dorothy E. Denning, "Is Cyber Terror Next?" *op. cit*.

心回傳的資料有誤，就有可能引發強大的破壞效果。[58]除此之外，內部人員也可能受人指使，或在不知情的情況下參與攻擊行動，例如內部人員所使用的儲存設備遭人植入隱藏的程式碼等等。[59]

而根據 2004 年一份由美國特勤局（U.S. Secret Service）和卡內基美隆大學聯合進行的調查報告也顯示，來自公司內部員工的網路攻擊對於相關產業已造成數百萬美元和機密資料的損失。[60]持有使用權限的內部員工不僅能夠接觸敏感資訊系統，也可以對系統植入惡意程式，並且發動網路攻擊，而這些惡意程式可能來自美國國內，亦可能是透過與國外組織合作取得。[61]

由上述可知，關鍵基礎設施同時面臨來自網際網路和內部人員的雙重威脅，面對網路恐怖攻擊的抵禦能力也因而降低。透過網路駭客或內部人員之手，恐怖份子確實有可能成功入侵關鍵基礎設施，進而引發破壞。

四、恐怖主義不適用於一般風險評估

有學者主張，即使目前恐怖主義的發生機率偏低，但若考量恐怖攻擊總是出其不意的特性，便不應將「高發生機率的低破壞力事件」與「低發生機率的高破壞力事件」以相同的分析模型進行風險評估。在一般的情況下，事件發生的機率（probabilities）對於風險評估的影響很大，然而恐怖份子發動攻擊的行為模式，可能並不合乎普通的趨勢分析或統計模型，個別攻擊事件之間亦無太多關連性，因此，倘若依賴機率來衡量恐怖攻擊發生的可能性，很可能導致分析謬誤。對國家而言，一場災難性的恐怖攻擊事件已是不能承受之重。況且，恐怖主義是雙方力量不對稱（asymmetric）的活動，不應以傳統的「效益－成本」（benefit-cost）

[58] Presidential Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructures," p. 27, ＜http://www.fas.org/sgp/library/pccip.pdf＞(Retrieved on June 7, 2012).
[59] *Ibid*, p. 15.
[60] U.S. Secret Service & Carnegie Mellon Software Engineering Institute, "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector," ＜http://www.secretservice.gov/ntac/its_report_040820.pdf＞(Retrieved on July 1, 2012), cited from John Rollins & Clay Wilson, *op. cit.*, p. 19.
[61] John Rollins & Clay Wilson, *op. cit.*, p. 19.

概念進行分析。[62]易言之，如果存在一個極具破壞力，但發生機率相對較低的潛在威脅，則政府仍然有必要致力使其發生的可能性趨近於零。

以上觀點打破了其他專家學者普遍將恐怖份子視為理性行為者，以及將普通的成本效益比做為行動依據的基本前提，並且認為恐怖份子可能出於宗教狂熱或悲憤情緒等各種原因，選擇一般人認為並非理性選擇的做法，在意想不到的時間和地點，出其不意地發動恐怖攻擊。因此，即使是低發生機率的高破壞力事件，仍不應等閒視之。

亦有學者認為，理論上而言，一個事件尚未發生，並不影響它在未來真正發生的機率。就如同核子戰爭，國際體系中的強權無不針對「核戰爆發情境」（scenario of a nuclear war）持續預做準備，即使這個情境從未發生過。對於網路恐怖份子而言，他們可將電腦病毒發動攻擊的時間設定在未來某個時間點，在那個時刻到來之前，無人得以知曉這些電腦病毒的存在。[63]由此可知，雖然網路恐怖攻擊尚無前例，但是這個現狀與它的發生機率之間並無直接關聯，國家仍然必須防範於未然。

貳、網路恐怖攻擊可能造成之災情

除了上述的四項主要論據之外，亦有專家學者預先設想網路恐怖攻擊可能引發的嚴重後果，以此呼籲政府重視網路恐怖主義之威脅。例如 Richard A. Clarke 與 Robert K. Knake 曾設想美國關鍵基礎設施遭受大規模網路攻擊時的情況：大型路由器（routers）當機，導致網際網路無法運作；各大飛航管制中心與空中數百架飛機失去聯絡，有些飛機在空中相撞；聯邦準備系統（Federal Reserve System, Fed）所儲存的資料及備份資料全遭刪除，金融體系面臨崩潰危機；煉油廠發生大火，通往美國東北部的瓦斯管線爆炸，核能發電廠則因安全考量暫時關閉；大

[62] Yacov Y. Haimes, *op. cit.*, p. 235.
[63] Aviv Cohen, "Cyberterrorism: Are We Legally Ready?" *Journal of International Business & Law*, Vol. IX, No. 1 (Spring 2010), p. 9.

部分地區電力中斷，鐵路運輸停擺；數千人喪命，警察和緊急救難體系都忙得不可開交。在此同時，美國政府高層也礙於通訊系統嚴重受阻，無法迅速了解災情，並制定對策。[64]

此外，亦有學者提到，由於各個關鍵基礎設施相互之間的協同性（synergistic effect），當一部分的關鍵基礎設施失靈，可能將連帶導致其他的關鍵基礎設施一併失靈，引發廣泛的災情。例如針對電力供應網的網路攻擊，迫使電力供應中斷，則供水廠和汙水處理廠依靠電力驅動的機械便無法運轉。2002 年 5 月，新加坡一家天然瓦斯供應商發現，輸送管線上有某個緊急閥門故障，導致其被迫停止向七座發電廠供應瓦斯，後者的發電功率因而下降 30%，即使在啟動備用發電機之後，仍有 8%的供應短缺。在停電期間，幾家化學工廠不得不關閉生產設備，過了幾天才終於恢復產能。網路攻擊伴隨著實體攻擊所造成的這種連鎖反應，可將破壞效果進一步擴大，例如以炸彈炸毀建築物的同時，以「拒絕服務攻擊」迫使電力供應或電話服務中斷，將大幅降低國家的救災能力，使得傷亡人數攀升，並加劇大眾的恐慌程度。[65]

由此觀之，一旦發生大規模網路恐怖攻擊，情況很可能不堪設想，電力中斷所引發的連帶效應，有可能同時讓許多關鍵基礎設施無法正常運作，這將使得社會許多層面皆受到巨大衝擊。不僅如此，若將網路恐怖攻擊做為實體的恐怖攻擊之輔助手段，兩者協同發動，從而增強整體之攻擊效果，更可能讓受害災情和損失益加嚴重。

[64] Richard A. Clarke & Robert K. Knake, *op. cit.*, pp. 64-68.
[65] Dana A. Shea, "Critical Infrastructure: Control Systems and the Terrorist Threat," CRS Report for Congress, pp. 8-9, ＜http://www.fas.org/irp/crs/RL31534.pdf＞(Retrieved on June 7, 2012).

第三節　網路恐怖主義威脅之爭議與評價

本章前兩節已對於網路恐怖主義之威脅程度的各種不同觀點進行綜整，本節則聚焦在主要的爭議點，嘗試尋找比較貼近實情的看法，同時提出筆者之意見，以期能夠正確評估網路恐怖主義的威脅程度。

經過相互對照之後可以發現，關於網路恐怖主義威脅程度之問題，主要爭議有三：

1. 網路恐怖攻擊之效果；
2. 恐怖份子是否有能力發動網路恐怖攻擊？
3. 關鍵基礎設施能否抵禦網路恐怖攻擊？

其中前兩項主要著重在攻擊方的「攻擊效果」與「攻擊能力」，第三項則聚焦於防禦方的「抵抗能力」。本節將依序針對三項主要爭議進行對照與思索，權衡攻擊方與防禦方之間的對抗情況，試圖對於網路恐怖主義之真實威脅性形成更加精確的評估。

壹、網路恐怖攻擊之效果

在分析各種主張網路恐怖攻擊之效果不若傳統恐怖攻擊的觀點之後，可以發現，這些觀點主要圍繞在「成本－效益」概念之上。對於恐怖份子而言，考慮到發動網際網路發動恐怖攻擊之前，必須滿足攻擊行動所需之大量資金、專業知識和長時間滲透及搜尋目標弱點等等先決條件，加上對於視聽大眾面臨突發災變的心理反應和行為模式有所掌握之後，恐怖份子若認定攻擊效果將不如預期，按照邏輯推論，理應不會選擇此一攻擊方式。

觀察目前人類的日常生活模式，電力仍然可說是極為重要的資源，舉凡生活起居、商業行為、交通運輸、通訊科技和緊急救護等等，充沛且穩定的電力供應可說是維持眾多社會機制持續運轉所不可或缺的關鍵能源，同時也是國家安全的

潛在弱點，以及網路恐怖份子的攻擊目標。因此，詳細分析網路恐怖攻擊可能造成的停電現象引發之衝擊，可謂甚具指標性意義。

針對停電對於社會各層面所造成之影響，若干專家學者認為，一般民眾不可能僅因停電便產生恐慌，在災難發生當下，人們仍能以理性面對並處理突發狀況；[66]另一方面， Richard A. Clarke 與其他專家學者，則正是以「停電的影響層面將遠超乎預期」之觀點做為回應，包括通訊、運輸、供水等其他關鍵基礎設施，以及民生經濟和工廠生產能力等，皆會因停電而大受影響。[67]

由於網路恐怖攻擊尚缺乏實際案例，Clarke 等人之觀點較偏向「最壞情況評估」（worst case estimation, WCE）而非案例分析，暫且不論。不過，雖然短時間的停電對於社會許多層面將造成立即的衝擊，但是對於廣大民眾的影響卻可能只是被迫忍受日常生活的諸多不便，距離恐怖份子引發恐懼的意圖，仍然相去甚遠，因此攻擊行動必須造成短期難以恢復的破壞效果。要達到此一目標，可能要在攻擊行動導致關鍵基礎設施某些重要零件嚴重損壞，而美國國內的庫存亦不足，同時又缺乏足夠產能以迅速供應新零件，必須仰賴外國進口等種種嚴苛條件皆能滿足之下，始可能達成。否則，停電持續的時間勢必要拉長，直到社會上的不滿情緒終於爆發，各種失序亂象一一出現，飢寒交迫導致的傷亡人數不斷增加，民眾才有可能產生恐懼。

至於停電持續的時間能否拉長到足以引發民眾恐懼的程度，則關乎恐怖份子的能力，以及意願。其中恐怖份子的能力問題即為第二個主要爭議，容後討論；而恐怖份子的意願問題，便涉及到長時間的心理壓力所造成的恐懼是否符合恐怖份子之需求，以及長時間維持攻擊行動是否有利等兩個層面。首先，突發事件引發的驚訝及恐懼，與長時間受到社會失序所苦，轉而形成的恐懼相比，兩者之間的心理衝擊效果，自然是以突發事件較為顯著。再者，以持續不斷地攻擊關鍵基礎設施而言，網路恐怖份子經由網際網路所獲得的優勢，在這種情況之下反而並

[66] 請參見：Andrew Jones, *op. cit.*, pp. 4-5; Michael Stohl, *op. cit.*, pp. 234-235; Sean Lawson, *op. cit.*, pp. 16-21.
[67] 請參見：Richard A. Clarke & Robert K. Knake, *op. cit.*, pp. 64-68; Dana A. Shea, *op. cit.*, pp. 8-9.

不明顯，甚至變成劣勢。例如網路攻擊所伴隨的高度匿蹤性，在短時間之內固然難以追蹤，但是若對於關鍵基礎設施的攻擊行為長期持續不斷，卻可能使得政府反恐單位擁有充裕時間進行分析，追查攻擊的確切來源，並且實行各種反制措施，造成網路恐怖攻擊難以持續下去。

由此觀之，除非停電能在短時間之內造成災難性或無法迅速恢復的嚴重後果，並且引發民眾的極大恐懼，否則長時間網路攻擊的缺點可能會抵銷原本的優點，以致於恐怖份子因而降低發動網路恐怖攻擊的意願。

此外，Dorothy E. Denning 主張恐怖份子在攻擊手段的選擇上，較傾向保守而非創新，重視成功率多於複雜性之觀點，[68]目前此一說法可能為真。不過，由於恐怖組織屬於秘密團體，外人難以直接得知其成員的心態及想法，研究者多半只能以既有資料加以推論。隨著新生代恐怖份子更加熟悉電腦與網路知識的趨勢，以及近年來世界各國在反恐行動取得的成功，長此以往，難保恐怖份子不會被迫另尋出路，轉而企圖在攻擊手段方面有所突破。

貳、恐怖份子是否有能力發動網路恐怖攻擊？

針對這項主要爭議，首先應避免使用「鑑於未曾發生網路恐怖攻擊之事實，可知恐怖份子的能力仍然不足」此種錯誤推論方式，這是由於如此的推論忽略了一個重要問題：以理性選擇的角度而言，人類採取行動的前提有二，一是能力，一是意願；不論是預期攻擊效果不佳等各種因素所致，只要缺乏意願，即使早已擁有足夠能力，恐怖份子仍然不會發動攻擊。

再回到恐怖份子是否已經掌握足夠的電腦技術及網路知識發動網路恐怖攻擊此一問題之上，對此，抱持保守立場的專家學者不在少數，其中大多數皆主張，目前恐怖份子尚缺乏這種能力，遑論長時間持續性的攻擊。然而，從 Dorothy E. Denning、Susan W. Brenner 及 Marc D. Goodman 等人的研究亦可得知，恐怖份子

[68] Dorothy E. Denning, “Cyberterrorism,” *op. cit*.

也正在學習相關知識，並試圖了解各項關鍵基礎設施對國家安全的重要性。即使恐怖份子仍未擁有網路攻擊能力，透過招募擁有相關專長的新血加入組織，假以時日依然可能順利取得該能力。[69]

另一方面，恐怖份子亦可能與符合其計劃需求的駭客建立僱傭或合作關係，此一假設的潛在威脅也相對嚴重得多。若由了解網路恐怖主義之潛力的新生代領導人所帶領，恐怖組織不論是透過金錢交易或其他方式與駭客合流，必定是恐怖份子得以快速獲取網路攻擊能力的極佳捷徑。

駭客本身具備的高度專業知識固然不易學習，但是在網際網路無遠弗屆之傳播能力的助長之下，駭客的數量仍然必將與日俱增，並且四處流竄。一旦為恐怖組織服務有利可圖，其中難免會出現貪圖個人利益的少數份子。而在「殭屍網絡」服務已經具備明確價目與商品組合的網路空間之中，[70]恐怖組織能否以金錢來換取駭客提供的服務，也可能僅僅取決於雙方是否能在談判價碼方面達成共識而已。因此，即使目前恐怖份子可能確實尚未擁有足夠的網路攻擊能力，此一現況仍然有機會出現重大轉變，各國反恐機構也必須持續監控及追蹤恐怖組織與駭客之間的關係變化，以確實掌握恐怖份子的科技實力。

參、關鍵基礎設施能否抵禦網路恐怖攻擊？

Joshua Green 以美國國防部外部網絡及內部網絡完全分離，徹底隔絕外部入侵之可能的現象為例，說明網路恐怖攻擊無法影響美國政府的軍事指揮能力。[71]然而，Richard Clarke 等人則以 2008 年的真實案例反駁此一論點，並且證實國防

[69] 請參見：Dorothy E. Denning, “Is Cyber Terror Next?” *op. cit.*; Susan W. Brenner & Marc D. Goodman, “In Defense of Cyberterrorism: An Argument for Anticipating Cyber-Attacks,” *University of Illinois Journal of Law, Technology & Policy*, Vol. 2002, Iss. 1 (Spring 2002), pp. 46-48, cited from Süleyman Özeren, *op. cit.*, p. 71.

[70] 請參見：Ron Rhodes, *op. cit.*, p. 54.

[71] Joshua Green, “The Problem of Cyberterrorism is Exaggerated,” *op. cit.*, pp. 43-44.

部在內外部網絡之間仍然存在安全漏洞。[72]不過，會產生此漏洞的原因，並非是隔離措施出現問題，而是在於使用者無意或故意的操作失誤。

以此觀察當前關鍵基礎設施能否抵禦網路恐怖攻擊之問題，便可發現，維安機制包括系統設計和人員操作兩個層面，應當分別討論之。但是，關於 SCADA 系統本身軟體設計的安全機制，是否能夠抵禦網路恐怖攻擊的侵襲，由於涉及不同領域的專業知識，已超出本論文之研究範圍，在此無法討論。即使如此，軟體的複雜程度仍然不等於安全程度，[73]隨著越來越多關鍵基礎設施連上網際網路，相互之間互賴程度的提高，伴隨著脆弱性增加的風險，SCADA 系統在安全設計及軟體維護方面也必然會遭遇到更多挑戰。因此，對於「關鍵基礎設施能夠抵禦網路恐怖攻擊」之觀點，筆者在此持保留態度。

至於人員操作的層面，關於內部人員破壞關鍵基礎設施之問題，應分為獨自行動及協助外人破壞兩個方面進行分析。首先是內部人員獨立破壞行為，除去員工職業操守之外，便是關鍵基礎設施內部人員管理措施是否恰當的問題，這又牽涉到營運公司的組織制度及管理權限分配等問題，本論文在此不多做討論，而是將焦點放在協助外人行動這一方面，其又可分為自願和非自願兩種類型。其中關於內部人員自願協助外人破壞關鍵基礎設施之問題，由於這些員工可能掌握 SCADA 系統的專業知識及操作權限，確實需要詳加管理，防止恐怖組織的滲透或收買。至於非自願協助方面，則需加強內部人員對於網路安全概念的訓練，避免不經意的疏失造成系統安全的嚴重漏洞，引發難以收拾的後果。

---

[72] Richard A. Clarke & Robert K. Knake, *op. cit.*, pp. 171-172.

[73] 以美國微軟公司（Microsoft）之 MS-DOS 系統和在其之後推出的 Windows 系列產品為例，雖然 Windows 系統的複雜程度明顯高於 MS-DOS 系統，然而由於 Windows 系統的使用者數量亦大幅超過 MS-DOS 系統，基於追求造成最大破壞力之設計理念，許多電腦病毒及惡意程式的作者便以 Windows 系統做為基礎，針對其系統安全漏洞進行病毒和程式的撰寫及開發，而這些病毒與程式也僅對 Windows 系統產生作用。

小結

綜觀上述，即使網路恐怖攻擊的效果尚不如傳統恐怖攻擊，恐怖份子亦可能仍未擁有足夠能力發動具規模的網路恐怖攻擊，然而他們正在學習相關知識，也有與駭客進行合作的可能性，而關鍵基礎設施不論在 SCADA 系統的軟體維護或人員操作等方面，仍然具有潛在的安全隱憂。種種跡象說明，雖然目前網路恐怖主義或許尚未構成嚴重威脅，但是這個情況也正在快速變化當中，政府必須密切注意其動態發展趨勢，以事先做好防範措施。

儘管各方針對三大主要爭議的看法相當分歧，但是在「網路末日只是時間問題」和「網路恐怖主義的威脅是被炒作出來的議題」的爭辯當中，真相必然存在於兩個極端之間。由於人類對未知事物經常心生畏懼，網路恐怖主義的定義又已遭到大眾媒體扭曲和模糊，加上某些團體及個人出於各自之目的而誇大威脅程度等因素，導致對於網路恐怖主義威脅嚴重性的熱烈討論，一時蔚為潮流。然而，如同 Gabriel Weimann 所言，雖然網路恐怖主義的威脅可能被誇大或炒作，但仍不應否定或忽視其存在。[74]即使 911 事件屬於低發生機率的高破壞力事件，卻依然千真萬確地發生在世人面前，並且強烈震撼了美國及全世界。基於恐怖攻擊行動強調出其不意、攻其不備的特性，一旦議題熱度消逝殆盡，媒體轉移目光焦點，或是相關討論過於失焦，導致人心懈怠、防備鬆弛，則爆發網路恐怖攻擊的機率，也必定隨之上升，不可不慎。

[74] Gabriel Weimann, “Cyberterrorism: The Sum of All Fears?” *op. cit.*, p. 146.

國立政治大學
National Chengchi University

第四章　美國防治網路恐怖主義政策

Arun Kr. Singh與Ahmad T. Siddiqui主張，預防潛在網路恐怖份子發動攻擊的唯一方法，便是大力資助國家層級的全球監視系統。[1]不過，美國政府除了監控網路恐怖份子的活動，藉以提前預警和防範之外，國內關鍵基礎設施的防護能力是否足以嚇阻網路恐怖份子發動攻擊？在網路恐怖份子和美國關鍵基礎設施之間的攻防較量當中，美國政府是否較強調壓制網路恐怖份子之攻擊能力？抑或較著重於加強關鍵基礎設施之防禦能力？這些都是本章嘗試探討的議題。

本章旨在探討近30年來美國防治網路恐怖主義之政策，主要著重在政策之發展脈絡，並討論其基本架構與指導方針。在時間尺度切割方面，本章選擇以兩個重要事件做為分水嶺，首先是2001年9月的911恐怖攻擊事件，此一重大事件直接導致美國政府大幅提高對於恐怖主義相關議題之重視程度；接著則是2003年2月美國政府所頒布之「網路空間安全國家戰略」，根據該項戰略美國政府確立國土安全部在整體防治政策框架之中心角色，並強調公私部門與個人加強合作，共同參與保護關鍵基礎設施及網路安全相關事務等。

本章首先研究美國政府在911事件發生之前的網路恐怖主義防治政策，探討政策的初期發展；接著分析911事件發生之後，至美國政府頒布「網路空間安全國家戰略」之前這段期間防治政策的發展概況，包括成立國土安全部等等；最後則是美國政府自頒布「網路空間安全國家戰略」至目前（2012年7月）為止，相關政策的發展趨勢及成效評估。藉由觀察一系列之政策，以了解美國政府對抗網路恐怖主義威脅的整體架構與發展脈絡。

[1] Arun Kr. Singh & Ahmad T. Siddiqui, "New Face of Terror: Cyber Threats, Emails Containing Viruses," *Asian Journal of Technology & Management Research*, Vol. 1, Iss. 1 (January - June 2011), p. 5, ＜http://ajtmr.com/papers/vol1issue1/CyberTerror.pdf＞(Retrieved on July 5, 2012).

第一節　911 事件之前的防治政策

第二章曾經提到，諸多專家學者皆認為「Cyberterrorism」一詞是由 Barry Collin 在 1980 年代率先提出，用以指涉網路空間與恐怖主義之結合。[2]而在大眾文化方面，1983 年，一部名為「WarGames」的好萊塢電影，描述一名年輕駭客入侵美國國防體系，幾乎引發第三次世界大戰的過程。[3]這部電影不僅讓美國民眾首次見識到網路恐怖主義的潛在威脅，也使得網路恐怖主義逐漸成為人們熱烈討論和爭辯的話題。[4]

從雷根時期開始，美國海外軍事設施及外交機構或人員頻遭國際恐怖組織發動攻擊，[5]使得美國的反恐政策主要著重在海外的安全議題。因此，美國政府在當時並未十分重視國內關鍵基礎設施的保護工作，也尚未針對網路恐怖主義制訂防治政策。直到 1993 年 2 月，紐約市世界貿易中心（World Trade Center, New York City）發生爆炸案件，成為美國本土遭到國際恐怖組織攻擊之首例；1995 年 4 月，奧克拉荷馬市聯邦大樓（Alfred P. Murrah Federal Building, Oklahoma City）亦發生爆炸案。這兩起重大事件，不但粉碎了美國人民對於本土從未爆發重大恐怖攻擊事件的充分安全感，亦迫使美國政府開始注意國內的恐怖主義問題。[6]

此後，美國政府對於防治網路恐怖主義及保護關鍵基礎設施，共有以下四項重要政策：

1. 第 39 號總統決策指令（President Decision Directives 39, PDD-39, 1995）；
2. 第 13010 號行政命令（Executive Order 13010, EO 13010, 1996）；

---

[2] 例如：Dorothy E. Denning, “Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy,” *op. cit.*, p. 281; Niranjan Dass, *op. cit.*, p. 159; Maura Conway, “Cyberterrorism and Terrorist ‘Use’ of the Internet,” *op. cit*.

[3] 關於電影之介紹，可參考：“WarGames,” ＜http://www.imdb.com/title/tt0086567/＞(Retrieved on June 17, 2012).

[4] Chad Parks, “Cyber Terrorism: Hype or Reality?” *The Journal of Corporate Accounting & Finance*, Vol. 14, No. 5 (July/August 2003), p. 9.

[5] 例如：美國駐黎巴嫩（Lebanon）大使館遭汽車炸彈攻擊（1983 年 4 月 18 日）；美國駐黎巴嫩軍事基地遭卡車炸彈攻擊（1983 年 10 月 23 日）等。

[6] 李明峻，「美國國土安全部的設置與功能」，收於邱稔壤主編，《**國際反恐與亞太情勢**》（臺北：國立政治大學國際關係研究中心，2004），頁 252。

3. 第 62 號總統決策指令(President Decision Directives 62, PDD-62, 1998)；

4. 第 63 號總統決策指令(President Decision Directives 63, PDD-63, 1998)。

以下依序對於這幾項重要政策進行整理及分析，觀察美國政府在防治網路恐怖主義政策初期階段之發展脈絡。

壹、第 39 號總統決策指令（PDD-39）

1995 年 6 月，柯林頓政府簽署並頒布「第 39 號總統決策指令」(以下簡稱 PDD-39)，宣示美國將竭力消除國內外的恐怖主義威脅，阻止恐怖主義活動。PDD-39 不僅正式將美國本土納入反恐政策的範圍，同時亦重視境內恐怖主義之活動。[7]

將 1993 年及 1995 年發生的兩起恐怖攻擊事件，與 PDD-39 之內容相互對照可知，這兩起爆炸案所造成的嚴重傷亡和損失，不僅讓美國政府開始重視本土的恐怖主義威脅，也由於這兩起事件皆以炸彈做為攻擊手段，加上當時美國國內關鍵基礎設施尚未高度依賴網路科技，因此 PDD-39 在針對恐怖主義的相關描述之中，並未提及「電腦系統」或「網路攻擊威脅」等概念，其重點仍偏向於降低傳統恐怖主義之威脅。換言之，美國政府在當時較著重於降低關鍵基礎設施面對實體攻擊的脆弱性，在針對關鍵基礎設施之保護措施方面，僅要求司法部長組成內閣委員會（Cabinet Committee），評估政府機關與關鍵基礎設施面對傳統恐怖主義攻擊的脆弱性，並向總統、內閣成員與相關的聯邦部門首長提供政策建議。[8]

貳、第 13010 號行政命令（EO 13010）

1996 年 7 月，「第 13010 號行政命令」(以下簡稱 EO 13010) 正式頒布。EO 13010 說明，關鍵基礎設施包括通訊、電力系統、石油和天然氣的儲存與運輸、

[7] "President Decision Directives 39: U.S. Policy on Counterterrorism," ＜http://www.fas.org/irp/offdocs/pdd39.htm＞(Retrieved on June 17, 2012).

[8] *Ibid*.

銀行與金融業、交通運輸、供水系統、緊急救護部門，以及政府部門的持續運作等。關鍵基礎設施面對的威脅來自兩個領域：實體威脅（physical threats）與網路威脅（cyber threats）。由於許多關鍵基礎設施是由民間企業負責管理及營運，美國政府有必要與這些私部門合作，發展出保護關鍵基礎設施的戰略，以保證它們的持續運作。因此，柯林頓總統下令組成「總統關鍵基礎設施保護委員會」（President's Commission on Critical Infrastructure Protection, PCCIP），其成員來自財政部、司法部、國防部、商務部、運輸部、能源部、聯邦緊急事務管理部（Federal Emergency Management Agency, FEMA）、中央情報局、聯邦調查局及國家安全局等聯邦機構，專責研擬國內關鍵基礎設施保護計劃，並且評估關鍵基礎設施所面臨之威脅與範圍，提出相關政策建議等等。[9]

相較於 PDD-39 較偏重防範針對關鍵基礎設施之實體攻擊，EO 13010 則進一步對於「關鍵基礎設施」所涵蓋的範圍提出明確的界定，同時提出，關鍵基礎設施所面臨的威脅不僅可能來自實體攻擊，亦可能來自虛擬的網路世界。由此可見，當時的關鍵基礎設施已逐漸運用網路科技進行營運及管理，亦使得美國政府開始注意到網路攻擊對於關鍵基礎設施造成威脅的可能性。不僅如此，由於大部分的關鍵基礎設施皆為民營，美國政府也開始重視公私部門之間的協調與合作，要求政府官員與民間企業共同研究及發展相關策略，以積極提供關鍵基礎設施周全的保護。

參、第 62 號總統決策指令（PDD-62）

1998 年 5 月，柯林頓總統再頒布「第 62 及 63 號總統決策指令」（以下簡稱 PDD-62 及 PDD-63）。其中 PDD-62 顯示出，美國政府已意識到國內關鍵基礎設施對於電腦設備的高度依賴性，並且認為，科技知識的傳播使得恐怖份子所能擁有的破壞力量已非昔日可比擬，他們可能會以先進的電腦科技攻擊關鍵基礎設

[9] "Executive Order 13010, EO 13010: Critical Infrastructure Protection, July 15, 1996," <http://www.fas.org/irp/offdocs/eo13010.htm> (Retrieved on June 17, 2012).

施。因此，白宮（White House）在其「國家安全會議」（National Security Council, NSC）之下，成立「國家安全、基礎設施保護暨反恐協調辦公室」（Office of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism），以負責協調與督導各項反恐政策，並且向總統呈交年度安全防務報告。[10]

另一方面，在「總統關鍵基礎設施保護員會」（PCCIP）的建議之下，柯林頓總統隨後亦簽署並頒布「第 63 號總統決策指令」。

肆、第 63 號總統決策指令（PDD-63）

隨著關鍵基礎設施逐漸依賴網際網路的趨勢，PDD-63 將關鍵基礎設施的定義修正為「維持經濟及政府最低限度運作所必須之各種實體與『基於網路的系統』（cyber-based systems）」，並且將針對關鍵基礎設施的各種非傳統攻擊方式，包括來自網際網路的攻擊等，列為必須消除之重大威脅。同時，PDD-63 擴大聯邦調查局內部「國家關鍵基礎設施保護中心」（National Infrastructure Protection Center, NIPC）之職權，指定該中心負責對於關鍵基礎設施所面對之各種威脅，進行評估、預警、執法及調查等相關工作，並且扮演協調機制的核心角色，維持與公私部門之間相關資訊的流通和共享。[11]

檢視 PDD-62 與 PDD-63 之內容，美國政府此時更加強調關鍵基礎設施逐漸依賴電腦設備及網路科技之趨勢，以及恐怖份子可能會以先進技術發動網路攻擊的潛在威脅，並且將各種「基於網路的系統」納入關鍵基礎設施的範疇之內，以防範各種形式的「非傳統攻擊」。針對各類型關鍵基礎設施保護工作的權責範圍，PDD-63 指派數個聯邦單位做為領導部門，各自統籌相關的保護工作，參閱表 4-1：

[10] "President Decision Directives 62: Combating Terrorism," ＜http://www.fas.org/irp/offdocs/pdd-62.htm＞(Retrieved on June 17, 2012).
[11] "President Decision Directives 63: Critical Infrastructure Protection," ＜http://www.fas.org/irp/offdocs/pdd/pdd-63.htm＞(Retrieved on June 17, 2012).

表 4-1　保護關鍵基礎設施領導部門（PDD-63）

領導部門	**關鍵基礎設施**
商務部	資訊與通訊
財政部	銀行與金融
環境保護局	供水系統
運輸部	航空 高速公路 大眾運輸 輸油管線 鐵路 水上商務
司法部／聯邦調查局	緊急事故執法業務
聯邦緊急事務管理部	消防業務 政府之持續運作
衛生與保健部	公共衛生（包括預防、監測、實驗及個人健康服務）
能源部	電力 石油及天然氣之生產與儲存

資料來源：“President Decision Directives 63: Critical Infrastructure Protection,” ＜http://www.fas.org/irp/offdocs/pdd/pdd-63.htm＞(Retrieved on June 17, 2012).

除了表 4-1 所列之各個領導部門以外，PDD-63 亦指定中央情報局負責國外情報事務，國防部則負責國防安全事務。[12]藉此，各個部門將可在各自熟悉的工作領域發揮所長，共同保護國內關鍵基礎設施，相互之間的權責分配也更加明確。例如在搜集恐怖主義情報方面，聯邦調查局為加強反恐怖及反情報工作，將

[12] “President Decision Directives 63: Critical Infrastructure Protection,” ＜http://www.fas.org/irp/offdocs/pdd/pdd-63.htm＞(Retrieved on June 17, 2012).

專責人力大幅擴增數倍；中央情報局則針對恐怖份子可能利用網際網路或大規模毀滅性武器（weapons of mass destruction, WMD）發動恐怖攻擊之情況，進行相應的組織改造工作，將其「行政管理處」（Directorate of Administration）重新規劃，並且分為：資訊科技（information technology）、財務（finance）、安全（security）、全球支援（global support）及人力資源（human resources）等五個單位，以強化其對於情報分析、情報運用及科技研發等情蒐與支援能力。[13]

此外，為了有效保護國內關鍵基礎設施，PDD-63 延續 EO 13010 強調「必須加強公私部門之間的緊密合作關係」之政策思維，計劃組成一個由各級政府官員與關鍵基礎設施營運公司代表組成的「國家基礎設施保護會議」（National Infrastructure Assurance Council, NIAC），不僅定期召開會議，並要求該會議在 2003 年以前制訂出全面性的「國家基礎設施保障計劃」（National Infrastructure Assurance Plan, NIAP）。[14]不久之後，此計劃之名稱重新修正為「國家基礎設施保護計劃」（National Infrastructure Protection Plan, NIPP）。[15]

除了「國家基礎設施保護計劃」以外，為達成防範網路攻擊的政策目標，PDD-63 也催生了數個相關計劃與報告。例如 2000 年 1 月由白宮提出的「保衛美國網路空間：保護資訊系統之國家計劃」（Defending America's Cyberspace: National Plan for Information Systems Protection），不僅分析國內關鍵基礎設施所面臨之威脅，確立計劃之目標與範圍，也調整或制訂民間及國防部門之關鍵基礎設施保護計劃；[16]又如在邁入新世紀之際，2001 年 1 月，柯林頓總統於卸任之前發表「聯邦關鍵基礎設施保護活動情形之報告」（Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities），概括描述美國政府當時保護關鍵基礎設施的政策執行、人員教育訓練和相關科技研

[13] 李明峻，頁 258。

[14] "President Decision Directives 63: Critical Infrastructure Protection," <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>(Retrieved on June 17, 2012).

[15] Shawn Vandiver, "Critical Infrastructure is Society's Glue," <http://www.abchs.com/ihs/WINTER2010/ihs_articles_column.php>(Retrieved on June 20, 2012).

[16] 請參見："Defending America's Cyberspace: National Plan for Information Systems Protection, Version 1.0," <http://www.fas.org/irp/offdocs/pdd/CIP-plan.pdf>(Retrieved on June 19, 2012).

發等情況，並針對相關計劃的執行成效，進行了初步的評估與了解，以做為後續政策之參考。[17]

PDD-39 未曾提及網路攻擊對於關鍵基礎設施之威脅，但是到了 PDD-63 和相關的國家計劃與報告當中，則開始使用各式各樣的網路時代用語，包括「cyber-terrorism」在內，以「cyber」為字首的詞彙出現頻率已逐漸上升。[18]如此的轉變過程，顯示出網路科技在短短數年之間的快速發展，以及關鍵基礎設施對網路科技的依賴程度，使得美國政府不斷提高對於網路恐怖主義和關鍵基礎設施保護事務的關切程度。

在這段期間，美國本土未再遭到恐怖主義的攻擊，直到 911 事件發生，徹底改變了整個局勢。下一節將討論 911 事件發生之後，至美國政府發表「網路空間安全國家戰略」之前，這段時期的網路恐怖主義防治政策。

第二節　911 事件至頒布「網路空間安全國家戰略」之前的防治政策

2001年9月11日上午所發生的恐怖攻擊事件，是近年來美國本土所遭遇到最嚴重的恐怖攻擊事件，也是「蓋達」恐怖組織（al-Qaeda）在數次失敗的嘗試之後，首次在美國境內成功執行的攻擊行動。[19]就在911事件的後續效應剛開始出

[17] 請參見：“Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities,” ＜http://www.fas.org/irp/offdocs/pdd/CIP_2001_CongRept.pdf＞(Retrieved on June 19, 2012).

[18] 例如在「保衛美國網路空間：保護資訊系統之國家計劃」中，計劃名稱便使用「Cyberspace」一詞，其內容亦多次使用「cyber」與「cyberspace」等詞彙；又如「聯邦關鍵基礎設施保護活動情形之報告」，在這份報告當中，則可看到「hacker」、「cyber-terrorist groups」及「cyber-terrorism」等字眼，請參見：“Defending America's Cyberspace: National Plan for Information Systems Protection, Version 1.0,” ＜http://www.fas.org/irp/offdocs/pdd/CIP-plan.pdf＞(Retrieved on June 19, 2012); “Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities,” ＜http://www.fas.org/irp/offdocs/pdd/CIP_2001_CongRept.pdf＞(Retrieved on June 19, 2012).

[19] Eliot E. Schmidt, “The Evolution of U.S. Policies against Terrorism,” p. 5, ＜http://www.thepresidency.org/storage/documents/Fellows2008/Schmidt.pdf＞(Retrieved on June 20, 2012).

現不久，9月18日，一隻名為「Nimda」[20]的電腦病毒透過電子郵件、感染網頁及利用微軟作業系統（Microsoft operating systems）內部的安全漏洞等方式，在網路空間迅速傳播，並造成嚴重破壞，無數的電子資料遭到刪除，確切損失難以估計。由於病毒出現的時間點與911事件之間相隔僅僅一週，使得美國政府、大眾媒體及一般民眾皆不禁懷疑，這起事件是否為第二波的恐怖攻擊行動。即使事後查明，Nimda電腦病毒與蓋達恐怖組織和911事件之間並無關聯，但是它強大的破壞力與引發的嚴重後果，也讓美國政府正視網路攻擊與恐怖主義可能會相互結合之問題。

911事件之後，面對短時間內接連發生的重大人為災害所造成之死傷及損失，小布希政府除了指揮災後的緊急救難及調查工作以外，在國會的高度支持之下，亦針對聯邦政府的組織架構進行大幅度的調整，並提出數個改革政策，其中與防治網路恐怖主義密切相關之重要政策，包括：

1. 第13231號行政命令（Executive Order 13231, EO 13231, 2001）；
2. 「美國愛國者法案」（USA PATRIOT Act, 2001）[21]；
3. 「網路安全研究與發展法案」（Cyber Security Research and Development Act, 2002）；
4. 國土安全部相關機構與政策（2002年）；
5. 「內部威脅研究」（Insider Threat Study, ITS, 2002）。

以下依序針對 911 事件發生之後，至頒布「網路空間安全國家戰略」之前，此一時期美國政府防治網路恐怖主義之重要政策，統整各項政策之要點，並且進行政策分析，討論 911 事件發生前後，相關政策之間的關聯性及發展趨勢。

[20] 此一電腦病毒名稱係將英文「Admin」（Administrator 之簡寫，意為「系統管理員」）的字母順序顛倒而成。

[21] 其正式名稱為「Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001」，意為「提供適當工具攔截及阻止恐怖主義以團結並鞏固美國之法案」，英文字首縮寫即為（USA PATRIOT Act），取其「美國愛國者」之字義。

壹、第 13231 號行政命令（EO 13231）

2001年10月16日，小布希政府頒布「第13231號行政命令」（以下簡稱EO 13231），特別強調資訊科技革命對於商業交易、政府運作與國防安全之重大影響，這些事務皆十分倚重關鍵基礎設施之間相互連結的網絡。為了確保關鍵基礎設施網絡之安全，小布希總統下令將柯林頓政府時期EO 13010所成立的「總統關鍵基礎設施保護委員會」（PCCIP）改組為「總統關鍵基礎設施保護小組」（President's Critical Infrastructure Protection Board，以下簡稱PCIPB），其成員包括：國務卿、財政部長、國防部長、司法部長、商務部長、運輸部長、能源部長、參謀長聯席會議主席、總統國家安全事務助理，以及總統國土安全助理等高級官員和幕僚，並由總統指定主席與副主席人選。[22]

PCIPB主席將兼任「總統網路空間安全特別顧問」（Special Advisor to the President for Cyberspace Security），所有相關部門和機構應充分且及時地向其告知各自的運作情況。PCIPB主席亦可召集小組成員舉行會議、制定議程，向相關部門提出保護關鍵基礎設施之政策與計劃，並且向總統國家安全事務助理和總統國土安全助理進行報告等等。[23]由EO 13231下令改組之PCIPB，參與的部會首長更多，也更加著重於網路空間安全相關議題。這顯示出，網路安全與關鍵基礎設施之保護任務，已逐漸擴及到多個政府部門，而這項議題在美國政府內部的重要性也持續升高。

貳、美國愛國者法案

2001年10月26日，為了回應恐怖主義對於美國本土的直接攻擊，在參眾兩院的強力支持之下，小布希總統簽署並頒布「美國愛國者法案」，這項重大法案修改並新增多項法律條文，大幅擴張國內執法機關針對可疑人物進行監視、監聽、

[22] "Executive Order 13231 of October 16, 2001: Critical Infrastructure Protection in the Information Age," ＜http://www.fas.org/irp/offdocs/eo/eo-13231.htm＞(Retrieved on June 19, 2012).
[23] *Ibid*.

調查與搜集情報之權限，提高警察與移民管理單位對於移入人口的檢查、居留和驅逐等權力，並且擴大「恐怖主義」之定義，以便將該法案的適用範圍一併擴增，同時亦加重從事或協助恐怖主義活動之犯罪刑罰。[24]其中關於網路恐怖主義與保護關鍵基礎設施之部分，分述如下：

1. 第8章第814條（USA PATRIOT Act, Title VIII, Sec. 814）針對美國聯邦法規第18章第1030條（U.S. Code Title 18, Section 1030）進行修正，不僅擴大法規適用範圍與犯罪行為之認定標準，使之更加適用於起訴包括網路恐怖主義在內之多種犯罪行為，同時亦特別加重刑期和罰則。除此之外，該部分亦將使用「影響美國州際或國際貿易及通訊活動之國外電腦設備」視為網路恐怖主義活動。
2. 第8章第816條（USA PATRIOT Act, Title VIII, Sec. 816）則要求司法部長建立區域性的「電腦鑑識研究室」（computer forensic laboratories），並向既有的其他電腦鑑識研究室提供充分支援，以針對查獲及截獲之有關犯罪活動與網路恐怖主義的電腦證物進行相關鑑識工作，訓練聯邦、各州和地方等各層級執法人員和檢查官對於電腦犯罪及網路恐怖主義之調查、鑑識與起訴之能力，並協助聯邦、各州和地方等各層級執法機關執行法律等。
3. 第10章第1016條（USA PATRIOT Act, Title X, Sec. 1016）除了重申美國公私部門對於關鍵基礎設施高度的依賴性、維持關鍵基礎設施正常運作的重要性，以及公私部門之間相互合作的必要性之外，亦計劃建立「國家基礎設施模擬與分析中心」（National Infrastructure Simulation and Analysis Center, NISAC)，該中心負責統整聯邦與地方公私部門所提供的各項數據，以建立關鍵基礎設施遭受入侵的模擬情境，並且進行分

[24] "Highlights of the USA PATRIOT Act," ＜http://www.justice.gov/archive/ll/highlights.htm＞ (Retrieved on June 20, 2012).

析，從而了解攻擊前預防及攻擊後反應的適當方式與執行效果，提出政策建議。[25]

即使該法案第8章第814條之標題即為「嚇阻及預防網路恐怖主義」（Deterrence and Prevention of Cyberterrorism)，其內文卻未能針對網路恐怖主義提出一個明確的法律定義，從而造成該章節所修正的美國聯邦法規第18章第1030條之對應內容，亦缺乏相關定義。網路恐怖主義缺乏明確法律定義所產生的影響，除了引發各界對於定義問題的爭議之外，也容易使一般民眾對網路恐怖主義產生錯誤認知，更可能導致美國政府在評估網路恐怖主義之威脅時，與其他網路犯罪或「網路策劃」行為發生混淆。由於本論文第二章與第三章已探討過這些問題，在此便不贅述。

相較之下，該法案第10章第1016條則明確提出關鍵基礎設施之定義與種類，美國政府便可據以針對各類型關鍵基礎設施之特性和運作模式，責成相關部門著手研擬保護措施。而透過成立「國家基礎設施模擬與分析中心」之計劃，亦可看出美國政府除了保障關鍵基礎設施之正常運作以外，也試圖充分了解關鍵基礎設施遭受恐怖攻擊後，對於國內社會各層面確切的衝擊和影響程度，從而評估風險。藉由這樣的方式，美國政府可提高相關政策之主動性和積極性。

參、網路安全研究與發展法案

911事件之後，美國政府擔心網際網路可能是恐怖份子發動攻擊的下一個目標，因此除了加強相關防範措施以外，也必須針對網際網路安全進行更廣泛的基礎性研究，始可能解決網路安全的脆弱性問題。[26]2002年2月，美國參眾兩院通過「網路安全研究與發展法案」(Cyber Security Research and Development Act)，預期在五年之內提供8.8億美元的預算，以建立眾多關於網路安全的創新研究及

[25] USA PATRIOT Act, Title VIII, Sec. 814, 816 & Title X, Sec. 1016, cited from "USA PATRIOT Act (H.R. 3162)," ＜http://epic.org/privacy/terrorism/hr3162.html＞(Retrieved on June 20, 2012).
[26] 蔡翠紅，《**美國國家信息安全戰略**》(上海：學林，2009)，頁 161。

教育計劃，針對密碼學、電腦鑑識、入侵偵測、隱私與機密安全，以及脆弱性評估等領域，持續培養並吸引優秀的網路安全專業人才，藉以改善美國面對網路恐怖攻擊的應變能力。[27]

經由「網路安全研究與發展法案」，美國政府大力支持相關人才的專業教育與進階研究，提高美國對於網路科技的理解與應用能力，不僅保障網路安全，亦能維持科技優勢，可謂美國政府防治網路恐怖主義政策的長程計劃，同時也顯示出美國政府重視科研國力的一貫特色。

肆、國土安全部相關機構與政策

美國國土安全部之設立，不僅是針對911恐怖攻擊事件的回應，亦為一系列政策與法案逐步發展之結果。2001年9月12日，即911事件發生翌日，小布希總統緊急設立一個內閣層級的「國土安全辦公室」（Office of Homeland Security），負責協調美國國內的反恐措施。[28]

2002年6月6日，小布希總統宣布，聯邦政府將成立保衛美國本土安全之「國土安全部」，並且在同年7月頒布之「國土安全國家戰略」（National Strategy for Homeland Security）當中，正式對「國土安全」加以明確定義。[29]在國會立法方面，2002年11月19日，美國眾議院通過「國土安全部設置法案」（Homeland Security Act），參議院亦於同年11月22日通過該案，經小布希總統於11月25日正式簽署及頒布之後，美國國土安全部正式成立，並且陸續整併許多政府部門，[30]這也是美

[27] "Public Law 107-305, Cyber Security Research and Development Act," pp. 2-14, ＜http://www.cio.gov/Documents/pl_107_305_nov_27_2002.pdf＞(Retrieved on June 20, 2012).
[28] 李明峻，頁 259。
[29] 美國「國土安全國家戰略」對於「國土安全」之定義為：「統合協調全國作為，以防範美國境內之恐怖攻擊、降低美國對於恐怖主義之脆弱性、減少恐怖攻擊之損害，並儘速於攻擊後進行復原」，請參見：李明峻，頁 271。
[30] "Public Law 107-296, Homeland Security Act of 2002," ＜http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf＞(Retrieved on June 21, 2012).

國自1947年杜魯門總統（Harry S. Truman）設置國防部以來，聯邦政府最重要、規模最龐大的組織改造計劃。[31]

在國土安全部各個附屬機構和組織之中，與防治網路恐怖主義工作密切相關者，主要包括：

1. 「國家網路安全司」（National Cyber Security Division，以下簡稱NCSD）：其負責與公共、私人及國際實體合作，確保網路空間與美國網路資產（cyber assets）的安全。為此，NCSD建立了一個「國家網路空間反應系統」（National Cyberspace Response System），隨時針對各種網路事件進行情報搜集、調查與執法等工作。[32]除此之外，NCSD亦成立「網路風險管理計劃」（Cyber-Risk Management Programs），以對於關鍵基礎設施從事風險評估、資源調配，並執行保護措施等等。自2006年開始，NCSD每兩年舉行一次「網路風暴」（Cyber Storm）演習，以評估各項關鍵基礎設施對於網路攻擊之預防、保護及反應能力，做為相關單位進行政策調整之依據，同時也為下一輪的演習計劃提供設計基礎。「網路風暴」是為美國國內最大規模的網路安全演習行動，不僅全盤檢驗美國國內關鍵基礎設施之安全體系，亦邀請其他國家的相關官員一同參與，並分享經驗，至今已分別在2006、2008及2010年完成演習，而第四次演習則自2011年秋季開始實施，預計於2012年結束。[33]
2. 「國家基礎設施協調中心」（National Infrastructure Coordinating Center，以下簡稱NICC）：做為關於保護關鍵基礎設施之資訊與協調的全國性網絡樞紐，NICC全天24小時保持針對關鍵基礎設施突發狀況或危機的監

[31] 李明峻，頁 253。

[32]「國家網路空間反應系統」包括：網路安全預備與國家網路預警系統（Cybersecurity Preparedness and the National Cyber Alert System）、美國電腦應急準備小組（U.S. Computer Emergency Readiness Team, US-CERT）、國家網路反應協調小組（National Cyber Response Coordination Group），以及網路警察入口網站（Cyber Cop Portal）四個部分，請參見：“National Cyber Security Division,” ＜http://www.dhs.gov/xabout/structure/editorial_0839.shtm＞(Retrieved on June 21, 2012).

[33] “Cyber Storm: Securing Cyber Space,” ＜http://www.dhs.gov/files/training/gc_1204738275985.shtm＞(Retrieved on June 29, 2012).

控和預警。除了分享相關資訊及協調關鍵基礎設施網絡的整合之外，NICC亦負責評估與分析關鍵基礎設施各項數據的準確性、重要性和影響性，以及向關鍵基礎設施營運公司與國土安全部提出建議等等。[34]

3. 「基礎設施保護辦公室」(Office of Infrastructure Protection)：其負責促進公私部門之間對於關鍵基礎設施保護工作的協同參與及互動，以建立一個有效的夥伴關係框架，相互分享情報和資源，共同降低遭受攻擊的風險。由於美國國內約有85%的關鍵基礎設施為私營單位，而政府部門對於威脅資訊、安全控管措施及科技研發等方面則較為了解，可運用的資源亦較豐富，因此，建立公私部門之間良好的夥伴關係，對於保障關鍵基礎設施之安全而言，可謂至關重要。[35]

國土安全部整併若干政府部門，並成立許多新單位或新計劃，以統整及協調各項反恐工作，確保社會各層面皆能受到充分保護。經由「網路風暴」定期的演習和排練，美國政府不僅能了解每段期間的政策執行成效，評估網路攻擊對於關鍵基礎設施之潛在威脅，亦可確保公私部門相關人員的安全意識不致鬆懈。

然而，國土安全部內部龐大的組織架構，以及陸陸續續的改組動作，卻也透露出美國政府在驚魂甫定之際，亟欲亡羊補牢，相關準備工作卻跟不上腳步的困境。以國土安全部防治網路恐怖主義之組織權責分配而言，各個負責單位之業務範圍存在若干重疊，例如NICC與「基礎設施保護辦公室」皆負責有關保護關鍵基礎設施的資訊共享工作，正面而言，當緊急事件爆發時，如此的設計可能成為備用的重要資訊傳遞管道，但是反面而言，則不免形成反恐資源的浪費。因此，各單位之間相互協調與合作的機制，也因而顯得更加重要。

[34] "National Infrastructure Coordinating Center," <http://www.dhs.gov/files/programs/gc_1236629756359.shtm> (Retrieved on June 21, 2012).
[35] "About the Office of Infrastructure Protection," <http://www.dhs.gov/xabout/structure/gc_1185203138955.shtm> (Retrieved on June 22, 2012); "Critical Infrastructure Sector Partnerships," <http://www.dhs.gov/files/partnerships/editorial_0206.shtm> (Retrieved on June 22, 2012).

除了上述的附屬機構與防治政策之外，自2003年2月「網路空間安全國家戰略」正式頒布之後，美國國土安全部亦針對防治網路恐怖主義實施進一步的組織調整，並提出新的政策及措施。關於這些部分，將在本章第三節進行討論。

伍、內部威脅研究（ITS）

美國特勤局於1998年成立「國家威脅評估中心」（以下簡稱NTAC），負責針對國內各類型的潛在威脅提出預警。另一方面，包括關鍵基礎設施在內，公私部門所面臨到之安全威脅，其來源不僅來自外界，亦可能來自內部人員，從而形成安全隱憂。因此，自2002年開始，NTAC與卡內基美隆大學「電腦緊急反應小組」（Computer Emergency Response Team，以下簡稱CERT）合作，對於可能危害關鍵基礎設施或國家安全的網路安全事務進行「內部威脅研究」（以下簡稱ITS），這項研究計劃同時由國土安全部提供資助。ITS監控之對象包括各類型關鍵基礎設施的現任、前任及承包商員工，這些人員不僅擁有接觸及操作關鍵基礎設施的特殊權限，亦可能透過內部電腦系統進行破壞。藉由ITS所提出之研究報告，私人企業、政府機關及執法單位便可有效了解、偵測並預防其內部人員可能引發的損害。[36]

目前，NTAC與CERT已於以下之各年度，共同針對下列公私部門之內部活動情況分別實施檢查：

1. 2004年8月：銀行與金融部門內部之非法網路活動；[37]
2. 2005年5月：關鍵基礎設施部門內部之電腦系統破壞行為；[38]以及
3. 2008年1月：資訊科技及通訊部門與政府部門內部之非法網路活動。[39]

[36] "National Threat Assessment Center," <http://www.secretservice.gov/ntac.shtml>(Retrieved on July 1, 2012).
[37] U.S. Secret Service & Carnegie Mellon Software Engineering Institute, "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector," <http://www.secretservice.gov/ntac/its_report_040820.pdf>(Retrieved on July 1, 2012).
[38] U.S. Secret Service & Carnegie Mellon Software Engineering Institute, "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors," <http://www.secretservice.gov/ntac/its_report_050516.pdf>(Retrieved on July 1, 2012).

ITS報告對於內部人員的個人與組織特徵、攻擊動機、攻擊計劃、攻擊前的可能行為，以及攻擊可能引發之後果等諸多面向，皆進行深入檢視，並提出相應之建議，以使公私部門能夠評估來自組織內部的潛在威脅，更有效地管理及篩選其內部人員與承包商員工，預防他們可能的破壞行為，確保關鍵基礎設施與公私部門之正常運作，同時維護國家安全及社會穩定。

綜觀上列各項重要政策，包括「美國愛國者法案」第10章第1016節之規定，以及國土安全部「基礎設施保護辦公室」之負責業務等，都延續了柯林頓政府EO 13010強調公私部門相互合作，共同維護關鍵基礎設施安全之政策路線，由此可看出EO 13010之政策遠見，以及對於後續政策的重要影響。下一節將討論美國政府頒布「網路空間安全國家戰略」至今的防治政策，同時也將繼續探討EO 13010之政策路線的後續發展概況。

第三節　頒布「網路空間安全國家戰略」至2012年7月的防治政策

為了保障並使所有美國人民有能力維護共同擁有、操作及互動的網路空間，2003年2月，做為「國土安全國家戰略」的一部分，美國政府正式頒布「網路空間安全國家戰略」，並同時頒布「關鍵基礎設施和關鍵資產實體保護之國家戰略」（National Strategy for the Physical Protection of Critical Infrastructure and Key Assets）[40]，以進行細部規範和補充。[41]自從頒布「網路空間安全國家戰略」後，

---

[39] U.S. Secret Service & Carnegie Mellon Software Engineering Institute, "Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector," ＜http://www.secretservice.gov/ntac/final_it_sector_2008_0109.pdf＞(Retrieved on July 1, 2012); U.S. Secret Service & Carnegie Mellon Software Engineering Institute, "Insider Threat Study: Illicit Cyber Activity in the Government Sector," ＜http://www.secretservice.gov/ntac/final_government_sector2008_0109.pdf＞(Retrieved on July 1, 2012).

[40] 根據此戰略，除了關鍵基礎設施之外，美國政府將國家古蹟與塑像（icons）、核能發電廠、水壩、政府設施及重要商業設施（商業中心、辦公大樓、體育場館及主題遊樂園等）列為「關鍵資產」，請參見：“National Strategy for the Physical Protection of Critical Infrastructure and Key Assets,”

美國政府尚未針對網路空間安全事務提出新的國家戰略層級文件。換言之，「網路空間安全國家戰略」目前仍是美國政府處理網路空間安全與關鍵基礎設施保護事務最重要的指導方針。

美國政府在頒布「網路空間安全國家戰略」之前，廣邀政府機構與民間團體提供專業意見，包括各地之高等教育機構、州政府、地方政府、銀行與金融業界等，皆參與研擬公私部門各自專屬之網路空間安全策略。2002年9月，前述之「總統關鍵基礎設施保護小組」（PCIPB）在網際網路上公布「網路空間安全國家戰略」草案，同時徵詢全國各地的個人和團體之想法。數以千計的人們參與並組成多個研討會，透過網際網路發表意見。藉由集思廣益的過程，美國政府得以有效地縮小重點範圍，並檢討優先事項之排序。[42]

「網路空間安全國家戰略」特別強調公私部門之間的合作關係，並提供全國人民皆能為保障網路空間安全做出貢獻之整體框架。有鑑於網路攻擊之速度與匿名性，相關單位十分難以追查並確認攻擊者之身份，因此該戰略之目的即在於降低國家關鍵基礎設施面對網路攻擊之脆弱性，防範於未然。[43]

包括「網路空間安全國家戰略」在內，從頒布該戰略至今，對於防治網路恐怖主義與保護關鍵基礎設施相關事務，美國政府陸續提出的重要政策如下：

1. 網路空間安全國家戰略（2003年）；
2. 第7號國家安全總統指令（Homeland Security Presidential Directive 7, Hspd-7，2003年）；
3. 情報改革與反恐法案（Intelligence Reform and Terrorism Prevention Act, IRTPA，2004年）；
4. 國家基礎設施保護計劃（NIPP，2006年頒布，2009年修訂）。

---

pp. 71-79, ＜http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf＞(Retrieved on June 27, 2012).

[41] "National Strategy to Secure Cyberspace," p. vii, ＜http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf＞(Retrieved on June 27, 2012).

[42] *Ibid*, p. 2.

[43] *Ibid*, p. viii.

以下由「網路空間安全國家戰略」開始，了解該戰略之目標及宗旨；接著依序觀察後續出現的各項政策之發展脈絡，並且提出分析；再者，討論歐巴馬總統就任之後，對於既有相關政策之執行情況，並且延續前兩節所討論之政策趨勢，探討美國政府自1990年代至今，歷經911事件及頒布「網路空間安全國家戰略」之後，一系列網路恐怖主義防治政策的整體面貌。

壹、網路空間安全國家戰略

「網路空間安全國家戰略」提供了保障網路空間與關鍵基礎設施安全之初步架構，其目的不僅在於防治網路恐怖主義，亦是為了增進整體國土安全。隨著關鍵基礎設施及公私部門對於網際網路之依賴持續加深，網路空間安全與關鍵基礎設施和美國國家社會正常運作與否，已然息息相關。因此，「網路空間安全國家戰略」十分重視公私部門之合作關係，與全國人民的共同參與。該戰略主要分為三個部分：(1)綜論與指導方針；(2)五大優先事項；以及(3)結語和附錄，其中附錄部分尚提出47項行動與建議，為整體戰略提供初步的政策指導。以下依序陳述「網路空間安全國家戰略」之主要內容，並且提出分析。

（一）、綜論與指導方針

「網路空間安全國家戰略」重申，關鍵基礎設施對於國家整體運作而言已不可或缺，而關鍵基礎設施的運作與服務，又繫乎網路空間的穩定與安全。換言之，實際上網路空間安全已與國家安全密不可分。對此，「網路空間安全國家戰略」之戰略目標有三：

1. 預防美國關鍵基礎設施遭受網路攻擊；
2. 降低美國遭受網路攻擊之脆弱性；
3. 遭受網路攻擊之後，將損害及復原時間降至最低。[44]

[44] *Ibid*, p. viii.

美國國內維持關鍵基礎設施運作之網際網路，已被用於控制各種網路空間之外的實體，而美國的經濟和國家安全皆完全仰賴這些實體建設。然而，美國政府預估，身份及數量皆不明的有心人士，可能擁有針對關鍵基礎設施發動有組織性的網路攻擊能力，潛在破壞性也會不斷提高，從而形成嚴重的安全威脅。對於這個情況，「網路空間安全國家戰略」制定六項指導方針如下：

1. **鼓勵全國性合作**：美國政府應召集並促進公私部門之間和私部門之間的討論，分享有關網路威脅與弱點之資訊，幫助私部門適當調整其風險管理策略和計劃，鼓勵具專業知識和能力的國民貢獻所學，並增進政府和民間的夥伴關係等等。
2. **保障隱私及公民自由**：聯邦政府有責任阻止網路空間之濫用行為侵害個人隱私及自由權利，網路空間安全計劃必須加強這方面的保護，尊重隱私權利益及其他公民自由權利，務使消費者和作業人員相信，有關單位將會以安全可靠的方式處理他們所分享的隱私資訊。
3. **發揮法律規範與市場力量**：聯邦法規不應成為保障網路空間安全的主要工具，即使目前某些聯邦執法機關已將網路安全考量納入其監督範圍之內，然而，市場本身才是提供改善網路安全最主要的動力。
4. **明確規範各部門之義務與職責**：「網路空間安全國家戰略」著重於建構一個更健全可靠之資訊基礎設施，並指定主要的領導部門發展聯邦網路空間安全計劃，國土安全部則將負責執行「網路空間安全國家戰略」所提出的大多數計劃，而該戰略亦向各級政府、私人企業與美國人民提出各種可行之建議，以共同維護網路空間安全。
5. **確保戰略彈性**（flexibility）：由於網路威脅變動速度極快，「網路空間安全國家戰略」亦強調保持彈性之能力，面對網路攻擊工具發展迅速，潛在的網路攻擊者可能擁有戰略優勢之情況，彈性之規劃可使相關單位得以重新調整安全事務之優先順序與資源分配。

6. **制訂長期規劃**：隨著新科技和及新弱點的出現，保障網路空間安全是為持續性之進程，「網路空間安全國家戰略」提供一個初步架構，以達成維護網路空間安全之目標，然而政府機關不僅必須研擬長期安全計劃，維持各自之角色，亦應鼓勵私部門考慮採行長期計劃。[45]

而在維護網路空間安全方面，「網路空間安全國家戰略」指定國土安全部成為聯邦政府主管網路安全之核心單位，以及整合各州政府、地方政府與私部門之樞紐，其重要責任包括：研擬全面性保障美國重要資源及關鍵基礎設施之安全的國家計劃、關鍵資訊系統遭受攻擊之危機管理、向公私部門提供緊急復原作業之技術支援、預警資訊和安全建議，並且推動和資助各種科技研發工作等。[46]

包括國土安全部在內，「網路空間安全國家戰略」指派多個政府機構做為各類型關鍵基礎設施保護事務之領導部門，詳細的權責分配情況，參閱表4-2：

國立政治大學 National Chengchi University

[45] *Ibid*, pp. 14-15.
[46] *Ibid*, pp. ix-x.

表 4-2　保護關鍵基礎設施領導部門（網路空間安全國家戰略）

領導部門	主管範圍
國土安全部	資訊及電信設施 運輸業（航空、鐵路、大眾運輸、水上商務、輸油管線及高速公路） 郵政及貨運 緊急勤務 政府之持續運作
財政部	銀行與金融
衛生與保健部	公共衛生（包括預防、監測、實驗及個人健康服務） 食品（肉類與家禽類除外）
能源部	能源（電力、石油及天然氣之生產與儲存）
環境保護局	供水系統 化學工業及危險物質
農業部	農業 食品（肉類與家禽類）
國防部	國防工業基地

資料來源：“National Strategy to Secure Cyberspace,” p. 16, ＜http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf＞(Retrieved on June 27, 2012).

對照表4-1與表4-2可以發現，在「網路空間安全國家戰略」的規劃之下，國土安全部整併若干聯邦部門保護關鍵基礎設施之領導職責，同時也突顯出其做為關鍵基礎設施保護事務之核心部門角色。不僅如此，「網路空間安全國家戰略」

亦擴大關鍵基礎設施之範圍，首次納入郵政、化學工業、農業、食品及國防工業等領域。

（二）、五大優先事項

為了確保網路空間與關鍵基礎設施之安全，「網路空間安全國家戰略」舉出五大優先事項，其中第一個優先事項著重於提升國家對網路意外事件的反應能力，並降低此種事件可能引發的危害；第二至第四個優先事項之目標降低網路攻擊之威脅與國家之弱點；第五個優先事項則聚焦在預防可能影響國家關鍵資產之網路攻擊，並增進國際間對於網路攻擊之管理和反應能力。[47]

1. **國家網路空間安全反應系統**：(1)建立公私部門之合作架構，以針對國家層級網路意外事件作出反應；(2)鼓勵民間企業發展並分享增進網路空間安全之能力；(3)擴增國土安全部之預警和資訊網路，加強其危機管理與協調之角色；(4)強化國家層級之意外事故管理能力；以及(5)執行聯邦系統網路安全計劃相關演習等。
2. **降低國家網路空間安全威脅與弱點之計劃**：(1)提升預防及起訴網路攻擊行為之執法能力；(2)建立國家層級之脆弱性評估程序，深入了解網路威脅和潛在後果；(3)減少並修補軟體安全漏洞；(4)認知關鍵基礎設施之間的互賴性，並增進網路系統與通訊設備之實體安全；以及(5)調整聯邦網路安全研發議程之優先順序等。
3. **國家網路空間安全意識與訓練計劃**：(1)推動全國性安全意識計劃，以加強美國民眾確保其自身擁有之網路空間安全；(2)發展合適之訓練與教育計劃，支持美國在網路安全領域之人力需求；(3)改善聯邦現有之網路安全訓練計劃的效率；以及(4)推動公私部門共同支持專業之網路安全認證系統等。

[47] *Ibid*, p. x.

4. **保障政府網路空間之安全**：(1)持續評估聯邦政府網路系統所面臨之各種威脅與弱點；(2)考核並維持合格的聯邦網路系統作業人員數量；(3)確保聯邦無線區域網路之安全；(3)強化政府外包與採購作業之安全；以及(4)鼓勵州政府和地方政府建立資訊科技安全計劃，並參與各級政府之間的資訊共享和分析等。

5. **國家安全與國際網路空間安全合作**：(1)加強網路安全相關之反情報措施；(2)提升追查與反制攻擊來源之能力；(3)加強美國國家安全社群（U.S. national security community）對於網路攻擊之反應能力；(4)與企業合作，並透過國際組織促進國際間公私部門之對話與夥伴關係，著重於資訊基礎設施之保護，並提倡全球之「安全文化」（culture of security）；(5)推動建立全國性與國際性之「監控及預警網絡」（watch-and-warning networks），以偵測並預防網路攻擊；以及(6)鼓勵其他國家接受「歐洲理事會網路犯罪公約」（Council of Europe Convention on Cybercrime）[48]，或確保它們至少在法律及程序方面具備協調性等等。[49]

（三）、結語和附錄

「網路空間安全國家戰略」在結語部分指出，網路空間已經成為美國經濟和國家安全的支柱，必須持續努力確保網路系統與關鍵基礎設施之安全。然而，這是一項複雜且不斷演變的挑戰，即使「網路空間安全國家戰略」已經明訂五大優

[48] 「歐洲理事會網路犯罪公約」是為第一個針對網路犯罪問題尋求協調各國法律、強化調查技術，並且增進國家間相互合作關係的國際公約，請參見："Convention on Cybercrime," <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>(Retrieved on June 29, 2012); Michael Portnoy & Seymour Goodman, eds., *Global Initiatives to Secure Cyberspace: An Emerging Landscape* (New York: Springer, 2009), pp. 8-10. 美國已於 2001 年 11 月簽署公約，2006 年 9 月經國會批准，2007 年 1 月正式生效，請參見："Convention on Cybercrime, CETS No.: 185," <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG>(Retrieved on July 9, 2012).

[49] "National Strategy to Secure Cyberspace," pp. 19-52, <http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf>(Retrieved on June 27, 2012).

先事項，做為預防、嚇阻和保護網路系統對抗攻擊威脅之方法，不過該戰略仍然僅是保障美國資訊基礎設施安全長期計劃的第一步，除了指定國土安全部擔任該戰略執行層面的核心角色，亦分配其他相關部門的職責，同時也為各州政府、地方政府、私部門與個人提供了各自的行動指南，以期共同改善國家整體網路空間安全。在可預見的未來，美國仍將繼續依賴網路空間，聯邦政府亦將尋求建立廣泛的夥伴關係，持續發展、執行與精進「網路空間安全國家戰略」。[50]

而在附錄的部分，針對五大優先事項，「網路空間安全國家戰略」提出47項行動與建議，並且依照優先順序予以編號，這些行動與建議主要說明聯邦政府將採取的具體作為，亦對各個私部門之夥伴提出建議。[51]

「網路空間安全國家戰略」是由政府部門、民間企業、學術單位、個人與團體一同參與討論的成果，這顯示出美國政府針對網路安全議題的慎重態度，不但將網路安全議題提升至國家戰略層級，亦十分重視國內各界的專業意見對於政策制訂過程之影響力。「網路空間安全國家戰略」除了接續之前的政策路線，促進全國公私部門的對話與協調，同時也鼓勵全體國民共同重視網路安全議題，貢獻一己之力。不僅如此，「網路空間安全國家戰略」亦尋求與其他國家建立廣泛的合作關係，嘗試在全球層次處理網路安全議題，這項「提倡全國性及全球性合作」的特點，明顯擴大了以往的政策視野。

此外，在國內政策框架方面，「網路空間安全國家戰略」也正式將國土安全部置於整體政策架構的核心地位，指定各類關鍵基礎設施保護事務之領導部門，並提出五大優先事務及47項行動與建議，為其後的相關政策指出明確的發展方向，可謂充分發揮了承先啟後的關鍵功能。

[50] *Ibid*, pp. 53-54.
[51] *Ibid*, pp. 55-60.

貳、第 7 號國土安全總統指令（Hspd-7）

2003年12月17日，小布希總統頒布「第7號國土安全總統指令」（以下簡稱Hspd-7），正式取代PDD-63，其他先前的相關政策內容也以Hspd-7為準。Hspd-7指示聯邦部門與機構必須確認並優先保障國家關鍵基礎設施與關鍵資源（critical infrastructure and key resources，以下簡稱CIKR）之安全，免於受到恐怖份子攻擊。與PDD-63相比，Hspd-7不僅將農業納入關鍵基礎設施之保護範圍，亦增加「關鍵資源」一項。根據「國土安全部設置法案」,「關鍵資源」意為「維持最低程度的經濟與政府運作不可或缺之公營或私營資源」，[52]而Hspd-7則對其進行細部闡釋，包括水壩、政府及商業設施等，並要求國土安全部與其他相關部門和機構充分配合，保護這些「關鍵資源」。[53]

在Hspd-7的規劃之下，國土安全部部長成為負責領導、整合及協調聯邦部門、各州政府、地方政府與私部門執行保護CIKR相關政策的核心官員，並且將繼續維持網路空間安全事務之溝通樞紐機制，以促進各級政府、私部門、學術機構與國際組織之間的互動與合作。不僅如此，Hspd-7亦依據「網路空間安全國家戰略」之指示，責成其他聯邦部門對於各類關鍵基礎設施進行保護措施，同時要求國土安全部部長與相關聯邦部門、各級政府及私部門之間保持緊密的協調及合作關係，[54]等同於更加確立了國土安全部在整體政策架構之中的重要角色。

包括國土安全部在內，Hspd-7對於各個聯邦專責部門（Sector-Specific Federal Agencies）之角色及責任分配情形，參見表4-3：

---

[52] "Public Law 107-296, Homeland Security Act of 2002," Sec. 2(9), ＜http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf＞(Retrieved on June 21, 2012).

[53] "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003," ＜http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1＞(Retrieved on June 28, 2012).

[54] *Ibid*.

表 4-3　保護關鍵基礎設施專責部門（Hspd-7）

專責部門	關鍵基礎設施
國土安全部	資訊科技 通訊設施 化學工業 運輸系統（包括大眾運輸、航空、海運、地面交通、鐵路及輸油管線系統） 緊急勤務 郵政及貨運
農業部	農業 食品（肉類、家禽類及蛋製品）
衛生與保健部	公共衛生與醫療保健 食品（肉類、家禽類及蛋製品除外）
環境保護局	飲用水及汙水處理系統
能源部	能源（包括石油、天然氣及電力的生產、提煉、儲存和配給，以及商業核電設施以外的電力系統）
財政部	銀行與金融
內政部	國家古蹟及塑像
國防部	國防工業基地

資料來源：“Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003,” ＜ http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1 ＞ (Retrieved on June 28, 2012).

Hspd-7之權責分配大抵遵循「網路空間安全國家戰略」之規劃，因此除了增列「國家古蹟及塑像」等關鍵資源之外，表4-3與表4-2可謂大同小異。即使其中部分項目與網路安全議題已無太大關聯，例如國家古蹟通常無法以網路攻擊手段進行破壞，仍可看出美國政府務求全面保障國家安全與維持社會穩定之決心。在核能設施部分，「網路空間安全國家戰略」未曾提及，而Hspd-7則指示國土安全部應與國家「核能管制委員會」（Nuclear Regulatory Commission）及能源部共同合作，保護全國所有發電、研究、測試和訓練用途之核子反應爐、核原料及核廢料，以及它們的運送、儲存及處置。[55]

參、情報改革與反恐法案（IRTPA）

除了強化關鍵基礎設施面對網路攻擊之防禦能力以外，在增進國家反恐情報能力方面，2004年12月17日，小布希總統簽署並頒布「情報改革與反恐法案」（以下簡稱IRTPA），大幅修改與反恐相關的法律規範。IRTPA重新調整美國國家情報體系，成立「國家情報總監辦公室」（Office of the Director of National Intelligence），直接由總統指揮，負責領導國家情報體系之運作，並且針對國家安全情報事務，向美國總統、國家安全會議與國土安全會議（Homeland Security Council）提供諮詢。[56]

另一方面，根據2004年8月「第13354號行政命令」（Executive Order 13354, EO 13354）所成立之「國家反恐中心」（National Counterterrorism Center，以下簡稱NCTC），[57]則在IRTPA調整情報部門總體架構之後，成為「國家情報總監辦公室」的附屬機構。做為「國家情報總監辦公室」內部最龐大的組織，NCTC的成員大多來自聯邦調查局、中央情報局及五角大廈（Pentagon），由美國總統、美國國

[55] *Ibid*.
[56] "Public Law 108-458, Intelligence Reform and Terrorism Prevention Act of 2004," <http://www.nctc.gov/docs/pl108_458.pdf> (Retrieved on June 28, 2012).
[57] "Executive Order 13354 of August 27, 2004: National Counterterrorism Center," <http://www.fas.org/irp/offdocs/eo/eo-13354.htm> (Retrieved on June 28, 2012).

家安全會議與美國國土安全會議共同指揮，主要負責分析國內外之恐怖主義威脅、分享反恐資訊，以及整合國家一切反恐資源。[58]NCTC與多個聯邦部門建立夥伴關係，包括聯邦調查局、司法部、中央情報局、國務院、國防部及國土安全部等，並且提供恐怖主義活動預警、保存恐怖活動資料、維護國家可疑份子檔案庫，同時發展、整合及評估當前美國反恐活動之戰略行動計劃等。

由此可知，除了國內制度的各種因應措施，美國政府亦未忽略情報工作。以「國家情報總監辦公室」之下的NCTC為核心單位，並由聯邦調查局、中央情報局和國防部等單位提供協助之美國網路安全與反恐情報體系，密切關注潛在的網路恐怖份子之活動情況與實際能力，以確實掌握敵我情勢，提前對於關鍵基礎設施可能之弱點進行補強。換言之，美國政府不僅戮力提高關鍵基礎設施的防護能力，也同時試圖偵測並打擊國內外有心人士的攻擊能力與意願，兩種政策雙管齊下，相輔相成，並發揮更加強勢的嚇阻效果。

肆、國家基礎設施保護計劃（NIPP）

自從PDD-63頒布之後，美國政府便持續醞釀「國家基礎設施保護計劃」（以下簡稱NIPP）的細部規劃。以PDD-63之架構為基礎，NIPP於2006年6月首次頒布，目前（2012年7月）該計劃的最新版本為2009年版。[59]針對保護CIKR之政策目標，NIPP不再僅限於防範恐怖攻擊，亦包括天然災害之預防，強調增進國家對於事前準備、突發事件反應，以及災後復原等各項能力。

對於美國政府而言，NIPP是為呼應Hspd-7所提出之政策需求的產物，包括關鍵基礎設施之界定、優先排序及提供保護等方面，NIPP皆進行詳細的規劃，並提供一個總體方針，以將全國各個保護CIKR的措施統合為單一的全國性合作計劃。針對國土安全部、聯邦政府相關部門、各州政府、地方政府與私部門及其

[58] "About the National Counterterrorism Center," ＜http://www.nctc.gov/about_us/about_nctc.html＞ (Retrieved on June 28, 2012).
[59] "National Infrastructure Protection Plan," ＜http://www.dhs.gov/files/programs/editorial_0827.shtm#0＞(Retrieved on June 28, 2012). 本章所討論之 NIPP 內容，皆根據 2009 年公布之版本。

他合作夥伴所分配之職責與角色，NIPP也做出明確界定。換言之，NIPP提供了一個全面性的風險管理架構，並且由國土安全部負責監督相關政策的執行與管理情況。[60]

依據Hspd-7的政策指示，NIPP針對18種類型之CIKR，分配給各個專責聯邦部門，以領導統籌各自領域內的協調與合作機制。這些專責聯邦部門不僅制訂各自的「專責部門計劃」（Sector-Specific Plans, SSP）[61]，亦提供許多NIPP對於全國性合作架構設計之建議。以NIPP和各項專責部門計劃為基礎，各個專責聯邦部門可針對眾多關鍵資產、系統、網絡及附屬功能進行界定，了解CIKR所面臨之潛在威脅，並且評估它們的脆弱性和受災之影響範圍及程度，以排定各項保護措施的優先順序。[62]

關於NIPP對於18種類型之CIKR專責部門之分配情形，參閱表4-4：

國立政治大學 National Chengchi University

[60] "National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency, 2009," p. 8, ＜http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf＞(Retrieved on June 28, 2012).
[61] 關於各項「專責部門計劃」，請參見："The Sector-Specific Plans," ＜http://www.dhs.gov/files/programs/gc_1179866197607.shtm#2＞(Retrieved on June 28, 2012).
[62] "National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency, 2009," *op. cit.*, p. 8.

表 4-4　保護 CIKR 專責部門（NIPP）

專責部門		**關鍵基礎設施及關鍵資源**
農業部 衛生與保健部		農業及食品
國防部		國防工業基地
能源部		能源（包括石油、天然氣及電力的生產、提煉、儲存和配給，商業核電設施除外）
衛生與保健部		醫療及公共衛生
內政部		國家古蹟及塑像
財政部		銀行與金融
環境保護局		供水系統（包括飲用水及廢水處理系統）
國土安全部	基礎設施保護辦公室	化學工業 商業設施 關鍵生產部門 水壩 緊急勤務 核能反應爐、核原料與核廢料
	網路安全與通訊辦公室	資訊科技 通訊設施
	運輸安全管理署	郵政及航運
	運輸安全管理署 海岸警衛隊	運輸系統
	移民與海關執法局 聯邦保安勤務局	政府設施

資料來源：“National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency, 2009,” p. 3,＜http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf＞(Retrieved on June 28, 2012).

經由對照表4-1、表4-2、表4-3以及表4-4可知，美國亟欲保護國內各項關鍵基礎設施和重要資產，包括核子反應爐在內，相關項目有增無減。NIPP不僅根據Hspd-7之規範，將「關鍵資源」納入權責分配範圍，亦針對國土安全部所負責之項目，詳細分配到相關的附屬機構，進一步明確界定各自之權責與角色。

伍、歐巴馬政府主要措施

美國現任總統歐巴馬於2009年1月上任之後，其相關政策與架構大致延續小布希政府的指導方針，並未做出大幅更動。[63]由此可知，對於防治網路恐怖主義及保護CIKR之相關議題而言，政黨輪替所產生的影響十分有限，國家安全之重要程度仍然超越了政黨政治的分歧。2009年1月，歐巴馬總統甫上任不久，便簽署並頒布「第1號總統國家安全指令」（Presidential Security Directive 1, PSD-1），要求針對當時聯邦政府的網路安全政策及相關活動進行評估，以全盤了解整體的政策成效。[64]

根據評估報告指出，網路科技在當時已幾乎成為美國經濟、關鍵基礎設施和國家安全等各層面的重要基礎，但是美國政府卻面臨艱難的雙重挑戰，其一方面負有確保網路安全、公民權利和隱私權不受侵害的重責大任，另一方面也必須維持一個提倡效率、創新、經濟繁榮與自由貿易的優良環境。不僅如此，各個聯邦專責部門尚缺乏足以全盤解決網路安全問題的視野或權限，應當針對現有的政策架構進行調整。[65]

再者，由於網際網路無遠弗屆，在網路空間中，「國界」的概念幾乎不具意義，單靠美國政府無法全面保障網路安全，從而也無法確保關鍵基礎設施得以不

[63] John D. Moteff, "Critical Infrastructures: Background, Policy, and Implementation," CRS report for Congress, p. 12, ＜http://www.fas.org/sgp/crs/homesec/RL30153.pdf＞(Retrieved on June 30, 2012).
[64] "Presidential Security Directive 1: Organizing for Homeland Security and Counterterrorism," pp. 2-3, ＜http://www.fas.org/irp/offdocs/psd/psd-1.pdf＞(Retrieved on June 30, 2012).
[65] "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," pp. iii-iv, ＜http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf＞(Retrieved on June 30, 2012).

受網路攻擊之侵害。因此，美國政府除了持續加強公私部門之間的對話與合作夥伴關係之外，也必須呼籲國際社會共同關注網路安全議題，建立安全技術標準，並且在法律規範方面取得協調。[66]

2009年6月，除了重新修訂並頒布新版的NIPP之外，自該年開始，每年的12月皆由歐巴馬總統宣布為「國家關鍵基礎設施保護月」（National Critical Infrastructure Protection Month），該行動係由國土安全部領導，不僅藉以提高公私部門對於保護關鍵基礎設施之安全意識，加強安全措施，以對抗網路攻擊與網路恐怖主義之嚴重威脅，同時亦向全國民眾強調保護國家資源的重要性，鼓勵人民參與相關的活動及培訓，以共同提升國家安全與抗災能力。[67]

小結

美國政府自柯林頓時代以來針對網路恐怖主義之防治政策，相關單位涵蓋國土安全部、國防部、聯邦調查局、國家安全局及中央情報局等聯邦政府部門。支持者認為，如此大規模的聯邦層級合作架構，充分顯示出美國政府確實將網路安全議題視為國家優先事務（national priority）。然而，反對者則批評，過多重複且不必要的組織和計劃，肇因於國家缺乏了解網路安全真實威脅程度，或足以清楚界定政府各機構之角色與職責的「連貫性戰略」（coherent strategy）。[68]

即使如此，美國政府在歷經 911 事件之衝擊，並且成立國土安全部之後，依據「網路空間安全國家戰略」及 Hspd-7 之規劃，再經過 NIPP 的調整與補充，

---

[66] *Ibid*, p. iv.

[67] 關於 2009 年至 2011 年美國白宮所發佈之相關文件，請參見：“Presidential Proclamation - Critical Infrastructure Protection Month,” ＜http://www.whitehouse.gov/the-press-office/presidential-proclamation-critical-infrastructure-protection-month＞ (Retrieved on June 30, 2012); “Presidential Proclamation--Critical Infrastructure Protection Month: Critical Infrastructure Protection Month, 2010,” ＜http://www.whitehouse.gov/the-press-office/2010/11/30/presidential-proclamation-critical-infrastructure-protection-month＞ (Retrieved on June 30, 2012); “Presidential Proclamation -- Critical Infrastructure Protection Month, 2011,” ＜http://www.whitehouse.gov/the-press-office/2011/11/30/presidential-proclamation-critical-infrastructure-protection-month-2011 ＞ (Retrieved on June 30, 2012).

[68] John Rollins & Clay Wilson, *op. cit.*, p. 7.

不僅已然確立國土安全部在整體政策架構之中的核心地位，對於各項 CIKR 的保護政策亦越趨完整。縱使某些機構或政策不免出現部分重疊，或是聯邦專責部門各自受限於制度設計與權責分配，無法全面解決網路安全問題，但是以國土安全部做為防治網路恐怖主義及處理網路安全相關議題之主要部門，已是美國政府明確的政策框架。未來各個聯邦專責部門的權責與角色是否會持續轉移至國土安全部，也是日後觀察相關政策之重點。

隨著網路科技逐漸滲透進入美國社會的各個層面，美國政府所欲保護的重要目標也越趨多元，但是整體政策之核心思維卻始終未曾改變。如同第三章之討論所述，即使目前網路恐怖主義的發生機率不高，但是網路空間的瞬息萬變，知識與科技傳播之便利，使得美國政府必須謹慎面對其潛在威脅，並且隨著時代推移，持續修正其防治政策。

由 EO 13010 開始，美國政府便十分重視公私部門之間的對話、協調及資訊分享，以共同維護關鍵基礎設施之安全，並且隨著全球化現象的影響，逐漸將網路安全議題提升至國家戰略層級，同時要求國內民眾與各國政府重視相關議題，提倡全國性與全球性的合作。歐巴馬政府迄今大抵維持前任政府的政策方針，同時亦相當注重全國民眾對於保護關鍵基礎設施之安全意識的提升。回顧 911 事件之所以會爆發的部分原因，來自於安全意識低落，導致反恐戒備鬆散，因此，如何維持政府與人民的安全意識，確實是反恐政策成功與否之關鍵。歐巴馬政府目前的政策方向，應當值得給予肯定。

第五章　結論與展望

做為全篇論文的總結，本章主要目的在於回應第一章之問題意識，同時展望未來相關研究之可能發展。因此，本章首先綜合第二、三、四章之論述重點與分析結果，做一彙整，並且提出筆者之觀察；接著針對本論文選擇之研究範圍進行反思，說明筆者在研究過程中遭遇到的困難與侷限；最後藉由美國防治網路恐怖主義政策強調「全國性及全球性合作」之指導方針，將分析視角由美國擴大到全球，進而思索可供後繼研究者著手的相關議題與方向。

第一節　研究發現

筆者由第一章所提出之問題意識出發，對於網路恐怖主義與美國防治政策進行研究之後，得到初步之研究結果如下：

1. 建立五大判別標準以界定網路恐怖主義；
2. 網路恐怖主義尚非迫切威脅，然情勢仍隨時可能發生轉變；
3. 2007 年 4 月愛沙尼亞遭受大規模網路攻擊事件之啟發；
4. 美國網路恐怖主義防治政策之整體架構與發展脈絡；

以下將依序闡述各項研究發現，藉以具體回應本論文在第一章所提出之各個問題意識。

壹、建立五大判別標準以界定網路恐怖主義

在綜合重要學者之觀點後，筆者提出對於網路恐怖主義之定義，並歸納出「**攻擊者之身分**」、「**行為動機**」、「**攻擊目標**」、「**行為目的**」，以及「**影響所及範圍**」等五大判別標準，據以分析網路恐怖主義之特徵。針對「網路恐怖主義」、「網路

犯罪」和「網路戰爭」三個概念，亦可根據五大判別標準進行比較，避免與後兩個概念之間發生混淆。

此外，雖然網路恐怖主義是為網際網路與恐怖主義相互結合之產物，但是在分析重要學者對於各種網際網路使用行為的分類方式，以及綜整網路恐怖主義與傳統恐怖主義之間的共同特徵之後，可以發現，恐怖份子出於招募新血、籌措資金、交換意見，或是策劃攻擊行動等各種目的之網際網路使用行為，其目的並非造成嚴重破壞或引發大眾恐懼，因此不符合「恐怖主義」之基本要素，本論文皆不視為網路恐怖主義。在此認定之下，本論文參考 Timothy L. Thomas 所提出之見解，將上述這些活動歸類於「網路策劃」行為，而非網路恐怖主義。

透過以上之整理，不僅能夠清楚了解網路恐怖主義與「網路策劃」之間的差異性及關聯性，亦可讓政府的相關防治政策更加聚焦於防範網路恐怖主義對於關鍵基礎設施可能發動之網路攻擊。此外，在閱讀相關文獻時亦能發現，標題雖為「網路恐怖主義」，內容卻著重於「網路策劃」的文獻，依舊十分常見。這也顯示出，各界對於網路恐怖主義之認識及定義，仍然有待進一步的辨證和釐清。

另一方面，由於「網路恐怖主義」所牽涉到的各種層面，包括網路科技本身、各項系統或程式之安全漏洞、惡意程式及電腦蠕蟲、恐怖攻擊之手法，以及可能遭受攻擊之目標設施等等，都正不斷地變動或翻新當中，例如正當某些系統及程式漏洞獲得修補的同時，尚有更多新軟體問世，也隨之出現更多新的漏洞，各種變化皆使得網路恐怖主義比傳統恐怖主義更加難以精確定義。隨著時代推進，筆者所提出之定義仍不免無法顧及各層面的最新演變情形。換言之，該定義僅為初步之界定，尚有必要根據網路科技與現實環境的變化，適時做出修正及調整。

貳、網路恐怖主義尚非迫切威脅，然情勢仍隨時可能發生轉變

針對「網路恐怖攻擊之效果」、「恐怖份子發動網路恐怖攻擊之能力」以及「現有關鍵基礎設施之防衛機制是否完善」等三大議題，筆者亦嘗試進行分析。依照當今許多相關研究之結果顯示，網路恐怖攻擊的效果尚不及傳統恐怖攻擊，而恐怖份子也仍然欠缺發動網路恐怖攻擊的能力，即所謂「具備足夠動機與能力的行為者」尚不存在，這或許能夠解釋世界各地為何至今尚未發生大規模網路恐怖攻擊事件。

不過，由於現有各項關鍵基礎設施對於網際網路的依賴程度不斷升高，包括 SCADA 系統的維護工作，以及內部人員的管理問題，皆形成潛在的安全漏洞，導致「易受攻擊且可能導致破壞或嚴重傷害的目標」存在的機率，不容政府忽視。再加上恐怖份子正逐漸熟悉電腦及網路操作知識，以及他們與駭客利益結合或交換的可能性，恐怖份子確實有可能獲得發動網路恐怖攻擊的能力。考量到上述種種層面，實在不應低估網路恐怖主義的潛在威脅。雖然目前尚未發生網路恐怖攻擊之實際案例，但是看似穩定的局勢，仍然隨時有機會發生徹底的轉變。

911 事件的發生機率雖然極低，然而一旦發生，其破壞力量卻巨大無比；網路恐怖主義也是如此，即使目前爆發網路恐怖攻擊的可能性偏低，尚未構成迫切威脅，各國仍不應掉以輕心，以免重蹈覆轍。以美國身為全球反恐行動的領導者角色而言，倘若如同 911 事件之人為災難再度爆發，不僅顏面無光，人民對政府的信賴也將蕩然無存。在如此草木皆兵、寧枉勿縱的高度警戒氣氛之下，各種安全議題的嚴重性和迫切性皆不免受到各種因素的影響，進而產生程度不一的誇大或扭曲。但是，美國政府對於網路恐怖主義威脅的關切始終未曾稍減，針對保護關鍵基礎設施免於遭受恐怖攻擊侵襲的相關討論及研究，也仍然方興未艾。即使網路恐怖主義的威脅在一定程度上遭到大眾媒體的誤導和有心人士的炒作，美國政府重視潛在威脅並積極保護關鍵基礎設施的基本政策方針，依舊十分明確。

參、2007 年 4 月愛沙尼亞遭受大規模網路攻擊事件之啟發

2007 年 4 月愛沙尼亞遭到大規模網路攻擊之事件，即使並非恐怖份子所為，卻也向全世界清楚揭示，當受到大規模網路攻擊時，一個高度依賴網際網路的國家可能會遇到哪些嚴重災情。在危機之中，愛沙尼亞國內產官學界保持密切聯繫，迅速掌握社會各層面的受災情況，並且相互配合，通力合作，數日之內即恢復大部分網站之運作，其危機處理之效率，足以供各國效法。

愛沙尼亞政府在當時決定暫時切斷所有從國外連入的網路連結，等於將該國隔離在網際網路之外，此種做法有效地阻止大部分的網路攻擊，並且讓部分的線上服務能夠恢復正常運作。然而，愛沙尼亞身為波羅的海三小國之一，而美國不論面積、人口，或是對世界的商業貿易和經濟局勢之影響力等等，卻皆遠非愛沙尼亞所能比擬。試想，美國與世界各國之間所有仰賴網際網路運作的商業往來、遠端通訊、網站服務、線上作業、意見論壇以及股匯市交易等等，全部被迫暫時中斷的景況會是如何？對於世界經濟又將造成何種程度之衝擊？

以此觀之，倘若有朝一日，美國也不幸遭到大規模網路攻擊，美國政府能否不顧與各國之間遍及各種層面的高度互賴，同樣以斷然將自身隔絕於網際網路之外的方式阻絕攻擊，便成為一大疑問。另一方面，如果網路恐怖份子發動大規模網路攻擊的真正目的，正是意圖迫使美國切斷所有對外的網路連結，從而引發全球性的連帶負面效應，美國如此之做法，是否反而促使網路攻擊的影響範圍更加擴大？這些不僅是政府決策者必須謹慎思考的問題，同時也顯示出，網路恐怖份子一旦發動攻擊，其影響可能遍及全球，因而需要世界各國針對法規、制度和技術等層面進行協調，相互分享資訊，培訓專業人才，並擬定適當之防災機制，以共同防範網路恐怖攻擊。

肆、美國網路恐怖主義防治政策之整體架構與發展脈絡

筆者綜整美國政府自柯林頓時代至今的網路恐怖主義防治政策，並且以 911 事件及頒布「網路空間安全國家戰略」為兩大分水嶺，分析並比較美國在兩項重要事件前後，政策發展有何異同。觀察美國政府所公布之相關文件，以及一系列政策所著重之方向可知，在 911 事件的強烈震撼與深刻教訓的影響之下，美國在 911 事件之後便大幅提高對於一切有關恐怖主義之事務的關注，其中自然也包括網路恐怖主義及網路安全等相關議題。

專家學者針對網路恐怖主義應當如何界定爭論已久，對於網路恐怖主義之威脅程度也仍然缺乏共識。儘管如此，諸多防治政策皆反應出，美國政府非常重視網路恐怖主義之威脅，並且選擇避開對於網路恐怖主義缺乏明確法律定義之問題，而從網路恐怖主義之「攻擊方」（網路恐怖份子）與「防禦方」（關鍵基礎設施）兩個面向著手。其採取的基本策略是以加強防禦力量為主，削弱攻擊力量為輔，試圖讓天平倒向於己有利的一方。一方面，藉由將國土安全部做為整體政策架構之核心部門，並針對相關聯邦部門進行權責劃分，美國政府全面加強關鍵基礎設施之保護，確保網路空間安全與穩定，同時提倡全國性與全球性的共同合作，協力對抗網路恐怖攻擊之威脅。透過消除潛在的關鍵基礎設施弱點，強化防護及抗災能力，並以定期之演習與宣導活動，維持全國民眾之安全意識等方式，美國政府致力於將恐怖份子以網路攻擊手段侵襲關鍵基礎設施的意願降到最低。另一方面，針對潛在之網路恐怖份子，美國政府則以全球情報體系為工具，力求確切掌握網路恐怖份子的活動情形，以及目前所擁有之科技實力，並且在他們發動網路攻擊之前先行阻止，或向相關單位提出預警，以加強防範措施。

而在國內相關政策方面，美國亦十分重視網路科技之研究及發展，不但透過援助或成立諸多研究單位，大力推動政府部門與學術機構之間的合作，亦投資多

項研究計劃，廣納全球人才進行培育，積極儲備專業人力資源。如此的政策，不僅能夠維持國家的科技優勢，也是保障網路安全的長久之計。

從法律規範之角度而言，縱使美國政府尚未針對網路恐怖主義提出確切之界定，然而，相關政策的制定和執行不僅並未因而受限，甚至超出了網路恐怖主義的範疇，進而擴及到「網路策劃」之面向。不論美國政府是出於必須提供關鍵基礎設施最周全的防衛機制的心態，或是誤將「網路策劃」一概視為網路恐怖主義之緣故，其政策路線已然證明，美國政府正盡全力防止關鍵基礎設施遭到網路攻擊破壞或干擾，如此的堅定決心，即使經過兩次政黨輪替，依舊未曾改變。

此外，美國境內大多數的關鍵基礎設施皆為民營，如此之特殊條件，促使美國政府積極引導與推動公私部門發展密切的合作夥伴關係，共同維護關鍵基礎設施之安全。然而，國內關鍵基礎設施高度民營之情況，並非舉世皆然，國情之差異，導致其他國家在制定防治網路恐怖主義相關政策時，未必能夠完全仿照美國。即使如此，美國政府加強產官學界緊密合作、提升全國人民之安全意識、定期舉行安全演習，致力降低網路恐怖主義之威脅等種種做法，對於世界各國保障社會及國家安全而言，仍然非常值得參考與借鏡。

除了上述之研究發現，在分析相關文獻的過程中，筆者偶然發覺，針對網路恐怖主義欠缺實際案例與威脅性之各種爭論，在目前網路恐怖主義依然缺乏實際案例的現況之下，若干專家學者對於其威脅程度提出質疑，固然可以理解。然而，以美國政府致力防止網路恐怖份子發動攻擊的各項政策而言，倘若相關政策之嚇阻成效非常顯著，足以使得恐怖份子始終無法將網路恐怖主義視為合理有效的攻擊手段選項，則美國境內發生網路恐怖攻擊真實案例的機率，自然可望降低。而這個情況將導致懷疑論者心中的疑慮仍舊揮散不去，或是隨著時間推進，更進一步加深其懷疑，他們也將持續主張美國政府不應過於重視網路恐怖主義的威脅程度。如此一來，美國政府之防治政策，反而成為眾多意見相左的專家學者繼續爭論不休的原因，此一現象倒也十分有趣。

不過，可以確定的是，除了恐怖份子之外，無人願意見到網路恐怖主義出現實際案例。如果欠缺真實案例的情況能夠長久維持下去，即使各界的爭論可能將永無休止，但是從中激發出的持續思辨與論證，對於維護人類安全而言，無疑具有正面幫助。筆者衷心期盼，眾多對於恐怖主義的相關研究，以及各國為反恐行動所付出的一切努力與犧牲，能夠確保網路恐怖主義始終僅存在於理論層次。

第二節　研究限制與未來展望

在研究過程之中，筆者曾遭遇某些研究困境，同時受限於研究範圍，亦不得不忽略某些無法顧及之議題領域，本節將一併說明之。此外，做為全篇論文之結語，本節也將討論對於未來相關研究之期許及展望，嘗試提供後繼研究者若干論述基礎。

壹、研究限制

首先，世界各國皆未曾出現實際的網路恐怖主義攻擊案例，因此在缺乏真實個案的情況下，筆者僅能針對現有的文獻進行整理與分析；在美國政府相關防治政策方面，由於無從觀察歷年來網路恐怖主義攻擊之次數增減變化，以做為衡量指標，導致如何準確且有效地評估政策執行之具體成效，亦成為研究過程中的一大難題。

目前國內針對網路恐怖主義議題之相關研究著作數量尚不豐富，筆者因而必須盡可能參考眾多英文文獻，以搜集足夠的研究資料。然而，語言的隔閡仍不免造成若干文意解讀方面的誤解或錯譯，力有未殆之處，尚有待諸多先進與後續研究者的批評和指正。除此之外，英文文獻的可取得性，頗大程度上也受限於國內相關資料庫所能搜尋和借閱的範圍，在筆者搜集到的研究資料之中，是否有遺珠之憾，實不無可能。

不僅如此，由於網際網路活動具有高度匿名性和匿蹤性之特色，而恐怖組織與駭客亦多為秘密團體，一般人無從參與或了解，因此在研究過程之中，極不容易取得恐怖份子及駭客之真實身分、行為模式、活動時間、組織結構、線上聊天室之位置，以及相互連結關係等第一手資料，絕大部分只能透過相關文獻取得間接資訊，難免在一定程度上影響本論文對於研究議題之探討和解讀。

另一方面，美國政府防治網路恐怖主義之相關政策，無疑加強了對於網際網路之監控或管制，固然是為了降低網路恐怖攻擊的發生機率，不過，政策執行過程所引發之各種關於侵害人權與違反言論自由的議論和疑慮，以及政府應當如何在反恐政策與人權價值之間取得適當平衡等等，也是目前各界熱烈討論及批評的一項重要議題。舉例而言，對於美國政府是否應該追查並關閉疑似由恐怖份子或駭客所架設的特定網站，便出現相左之意見。[1]然而，本論文礙於研究範圍所限，為求研究議題之集中，並未嘗試觸及上述之議題領域，亦是本論文有所欠缺之處，有待後續研究者進行補充。

最後，美國政府所持有之諸多機密資料，以及關鍵基礎設施內部之技術文件，限於保密機制及專業學識，亦不在筆者能夠接觸與理解的範圍，從而無法更深入地理解目前相關政策與防衛體系的發展情況，這個問題確實是本論文難以克服之障礙。

貳、未來展望

本論文已對於網路恐怖主義之界定、威脅程度，以及美國政府至目前為止相關防治政策的發展概況，進行建構、整理和分析。但是筆者也必須強調，隨著網路科技的快速發展，各種安全防護軟體和惡意程式的持續開發和制衡、駭客技術及知識的交流與傳播、關鍵基礎設施的互賴性和相互連結性持續提高，以及新世代恐怖份子正學習相關知識，或嘗試與駭客合作等等趨勢，皆可能使得本論文所

[1] Carla Mooney, *Online Social Networking* (Farmington Hills, MI: Lucent Books, 2009), pp. 84-85.

提出的網路恐怖主義之界定，以及威脅程度之評估，都必須隨著情勢變化而進行修正。

此外，美國政府相關防治政策在未來的發展走向，例如保護各項關鍵基礎設施之權責，是否將繼續集中於國土安全部，以及與各國之間各層面的互動及協調措施等等，都值得持續觀察，也是後繼研究者可以關注之焦點。

網際網路既然是全球化現象之重要推手，網路恐怖主義自然也是世界各國與國際組織必須重視之潛在威脅，尤其是對於網路科技依賴程度甚高的各個先進國家而言，網路恐怖主義對它們的威脅，也遠大於其他國家。雖然筆者僅針對美國防治政策進行分析，但是就如同全球化所帶來之其他負面效應一般，網路恐怖主義同樣需要各國及國際組織通力合作，降低其攻擊發生的可能性，美國政府也早已意識到這點，大力提倡全球性的對話與協調。關於各國家行為者如何在法律規範、組織架構及防治政策等各個層面進行有效整合，以及國家應如何以全球視角看待網路恐怖主義的潛在威脅及發展趨勢等等，皆是相關研究可以深入發展的空間，筆者也期待未來的研究者能夠多加著墨。

國立政治大學 National Chengchi University

國立政治大學
National Chengchi University

參考文獻

中文部分

一、專書

王銘勇，《網路犯罪相關問題之研究》。臺北：司法院，2002。

方天賜、孫國祥，「民族主義與恐怖主義」，收於張亞中主編，《國際關係總論》，二版，頁 193-218。臺北：揚智，2007。

李明峻，「美國國土安全部的設置與功能」，收於邱稔壤主編，《國際反恐與亞太情勢》。臺北：國立政治大學國際關係研究中心，2004，頁 251-285。

李偉主編，《國際恐怖主義與反恐怖鬥爭年鑑》。北京：時事，2004。

宋興洲，「科技在恐怖主義與反恐行動中所扮演的角色」，收於姜新立、張錦隆主編，《政治與資訊的交鋒》，頁 53-89。臺北：揚智，2010。

林山田，《刑事法論叢（一）》。臺北：臺灣大學法學院圖書部，1997。

林宜隆，《網際網路與犯罪問題之研究》。桃園：中央警察大學出版社，2000。

林義貴，《資訊社會與網路犯罪》。臺北：華立，2005。

邱伯浩，《恐怖主義與反恐》。臺北：新文京，2006。

吳永宗，《電腦運用所衍生法律問題之研究》。臺北：司法院，1998。

馬進保、袁廣林，《高科技犯罪研究》。北京：中國人民公安大學出版社，2008。

許武峰，《電腦犯罪理論與實務問題研究》。臺北：司法院，1998。

黃秋龍，《兩岸總體安全下的非傳統威脅》。臺北：法務部調查局展望與探索雜誌社，2010。

蔡瑋，「冷戰後的國際恐怖主義：趨勢與挑戰」，收於邱稔壤主編，《國際反恐與亞太情勢》。臺北：國立政治大學國際關係研究中心，2004，頁 7-29。

蔡翠紅，《美國國家信息安全戰略》。上海：學林，2009。

二、期刊論文

彭慧鸞，「數位時代的國家安全與全球治理」，《問題與研究》，第 43 卷第 6 期（民國 93 年 11、12 月），頁 29-52。

英文部分

一、專書

Bhatnagar, S., *Encyclopaedia of Cyber and Computer Hacking*, Vol. 1 & 5 (Delhi: Anmol Publications, 2009).

Brenner, S. W., "Cybercrime: Re-thinking Crime Control Strategies," in Yvonne Jewkes, ed., *Crime Online* (Portland: Willan Publishing, 2007), pp. 12-28.

Clarke R. A., & Knake, R. K., *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2010).

Colarik, A. M., *Cyber Terrorism: Political and Economic Implications* (Hershey, PA: Idea Group, 2006).

Cordesman A. H., & Cordesman, J. G., *Cyber-threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland* (Westport, CT: Praeger, 2002).

Curran, K., Concannon, K., & McKeever, S., "Cyber Terrorism Attacks," in Lech J. Janczewski & Andrew M. Colarik, eds., *Cyber Warfare and Cyber Terrorism* (Hershey, PA: Information Science Reference, 2008), pp. 1-6.

Dass, N., *Globalization of Terror: A Threat to Global Economy* (New Delhi: MD Publications, 2008).

Denning, D. E., "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in John Arquilla & David Ronfeldt, eds., *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND, 2001), pp. 239-288.

Finch, S., "Cyber-terrorism Poses a Serious Threat to Global Security," in Louise I. Gerdes, ed., *Cyber Crime* (Farmington Hills, MI: Greenhaven Press, 2009), pp. 35-39.

Goodman, M. D., "Understanding International 'Cyberterrorism': A Law Enforcement

Perspective," in Cecilia S. Gal, Paul B. Kantor, & Bracha Shapira, eds., *Security Informatics and Terrorism: Patrolling the Web* (Washington, DC: IOS Press, 2008), pp. 8-16.

Green, J., "The Problem of Cyberterrorism is Exaggerated," in Louise I. Gerdes, ed., *Cyber Crime* (Farmington Hills, MI: Greenhaven Press, 2009), pp. 40-50.

Higgins, G. E., *Cybercrime: An Introduction to an Emerging Phenomenon* (New York: McGraw-Hill, 2010).

Jaeger, C., "Cyberterrorism," in Hossein Bidgoli, ed., *The Internet Encyclopedia*, Vol. 1 (New York: John Wiley & Sons, 2003), pp. 353-371.

_____, "Cyberterrorism and Information Security," in Hossein Bidgoli, ed., *Global Perspectives in Information Security: Legal, Social, and International Issues* (Hoboken, NJ: John Wiley & Sons, 2009), pp. 127-180.

Mooney, C., *Online Social Networking* (Farmington Hills, MI: Lucent Books, 2009).

National Research Council, *Computers at Risk: Safe Computing in the Information Age* (Washington, DC: National Academies Press, 1991).

Nelson, B., Choi, R., Iacobucci, M., Mitchell, M., & Gagnon, G., *Cyberterror: Prospects and Implications* (Monterey, CA: Center for the Study of Terrorism and Irregular Warfare, Naval Post Graduate School, 1999).

O'Brien, K. A., "Information Age Terrorism and Warfare," in David M. Jones, ed., *Globalisation and the New Terror: The Asia Pacific Dimension* (Northampton, MA: Edward Elgar Publishing, 2004), pp. 127-158.

Owen, R. S., "Infrastructures of Cyber Warfare," in Lech J. Janczewski & Andrew M. Colarik, eds., *Cyber Warfare and Cyber Terrorism* (Hershey, PA: Information Science Reference, 2008), pp. 35-41.

Özeren, S., "Cyberterrorism and International Cooperation: General Overview of the Available Mechanisms to Facilitate an Overwhelming Task," in Centre of Excellence Defence Against Terrorism, Ankara, Turkey, ed., *Responses to Cyber Terrorism* (Washington, DC: IOS Press, 2008), pp. 70-88.

Pasley, J. F., "United States Homeland Security in the Information Age," in Michael Pittaro, ed., *Cybercrime: Current Perspectives from InfoTrac®*, 2nd ed., (Belmont, CA: Wadsworth, 2010), pp. 127-135.

Portnoy M., & Goodman, S., eds., *Global Initiatives to Secure Cyberspace: An*

Emerging Landscape (New York: Springer, 2009).

Rhodes, R., *Cyber Meltdown: Bible Prophecy and the Imminent Threat of Cyberterrorism* (Eugene, OR: Harvest House, 2011).

Ross, J. I., *Criminal Investigations: Cybercrime* (New York: Chelsea House, 2010).

Schell, B. H., & Martin, C., *Cybercrime: A Reference Handbook* (Santa Barbara, CA: ABC-CLIO, 2004).

Stiennon, R., *Surviving Cyberwar* (Lanham, MD: Government Institutes, 2010).

Sundaram, P. M. S., & Jaishankar, K., "Cyber Terrorism: Problems, Perspectives, and Prescription" in Frank Schmalleger & Michael Pittaro, eds., *Crimes of the Internet* (Upper Saddle River, NJ: Pearson Education, 2009), pp. 593-611.

Taylor, P. A., & Harris, J. Ll., "Hacktivism," in Hossein Bidgoli, ed., *Global Perspectives in Information Security: Legal, Social, and International Issues* (Hoboken, NJ: John Wiley & Sons, 2009), pp. 295-317.

Tikk, E., & Oorn, R., "Legal and Policy Evaluation: International Coordination of Prosecution and Prevention of Cyber Terrorism," in Centre of Excellence Defence Against Terrorism, Ankara, Turkey, ed., *Responses to Cyber Terrorism* (Washington, DC: IOS Press, 2008), pp. 89-103.

Weimann, G., *Terror on the Internet: The New Arena, the New Challenges* (Washington, DC: United States Institute of Peace, 2006).

Wilson, C., *Computer Attack and Cyberterrorism* (New York: Nova Science, 2009).

二、期刊論文

Brenner, S. W., "'At Light Speed': Attribution and Response to Cybercrime/Terrorism/Warfare," *The Journal of Criminal Law and Criminology*, Vol. 97, No. 2 (Winter, 2007), pp. 379-475.

Cohen, A., "Cyberterrorism: Are We Legally Ready?" *Journal of International Business & Law*, Vol. IX, No. 1 (Spring 2010), pp. 1-40.

Conway, M., "What Is Cyberterrorism?" *Current History*, Vol. 101, No. 659 (December 2002), pp. 436-442.

Green, J., "The Myth of Cyberterrorism," *Washington Monthly*, Vol. 34, No. 11 (November 2002), pp. 8-13.

Haimes, Y. Y., "Risk of Terrorism to Cyber-Physical and Organizational-Societal Infrastructures," *Public Works Management & Policy*, Vol. 6, No. 4 (April 2002), pp. 231-240.

Jarmon, J., "Cyber-terrorism," *Journal on Terrorism and Security Analysis*, Vol. 6 (April 2011), pp. 102-117.

Jones, A., "Cyber Terrorism: Fact or Fiction," *Computer Fraud and Security*, Vol. 2005, No. 6 (June 2005), pp. 4-7.

Naím, M., "The Five Wars of Globalization,"*Foreign Policy*, No. 134 (January/February 2003), pp. 28-36.

Parks, C., "Cyber Terrorism: Hype or Reality?" *The Journal of Corporate Accounting & Finance*, Vol. 14, No. 5 (July/August 2003), pp. 9-11.

Stohl, M., "Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games?" *Crime, Law and Social Change*, Vol. 46, No. 4-5 (December 2006), pp. 223-238.

Thomas, T. L., "Al Qaeda and the Internet: The Danger of 'Cyberplanning'," *Parameters*, Vol. 33, No. 1 (Spring 2003), pp. 112-123.

Weimann, G., "Cyberterrorism: The Sum of All Fears?" *Studies in Conflict & Terrorism*, Vol. 28, Iss. 5 (2005), pp. 129-149.

三、網路資料

"About the National Counterterrorism Center," ＜http://www.nctc.gov/about_us/about_nctc.html＞(Retrieved on June 28, 2012).

"About the Office of Infrastructure Protection," ＜http://www.dhs.gov/xabout/structure/gc_1185203138955.shtm＞(Retrieved on June 22, 2012).

"Air Force Mission," ＜ http://www.af.mil/main/welcome.asp ＞ (Retrieved on February 19, 2012).

Arquilla, J., & Ronfeldt, D., "Cyberwar is Coming!" in John Arquilla & David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica: RAND, 1997), pp. 23-60, ＜http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/MR880.ch2.pdf ＞ (Retrieved on February 23, 2012).

"Background Note: Estonia," < http://www.state.gov/r/pa/ei/bgn/5377.htm > (Retrieved on February 29, 2012).

Caruso, J. T., "Combating Terrorism: Protecting the United States," before the House Subcommittee on National Security, Veterans Affairs, and International Relations, Washington, DC, March 21, 2002, <http://www.fbi.gov/news/testimony/combating-terrorism-protecting-the-united-states > (Retrieved on February 9, 2012).

Clark, T., "Clinton Outlines Cyberthreat Plan," <http://news.cnet.com/Clinton-outlines-cyberthreat-plan/2100-1023_3-211497.html > (Retrieved on February 1, 2012).

"Convention on Cybercrime," <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>(Retrieved on June 29, 2012).

"Convention on Cybercrime, CETS No.: 185," <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG>(Retrieved on July 9, 2012).

Conway, M., "Cyberterrorism and Terrorist 'Use' of the Internet," *First Monday*, Vol. 7, No. 11 (4 November 2002), <http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1001/922>(Retrieved on February 10, 2012).

"Critical Infrastructure Sector Partnerships," <http://www.dhs.gov/files/partnerships/editorial_0206.shtm>(Retrieved on June 22, 2012).

"Cybercrime," <http://www.interpol.int/content/download/805/6671/version/10/file/FHT02.pdf>(Retrieved on February 23, 2012).

"Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf > (Retrieved on June 30, 2012).

"Cyber Storm: Securing Cyber Space," <http://www.dhs.gov/files/training/gc_1204738275985.shtm>(Retrieved on June 29, 2012).

"Defending America's Cyberspace: National Plan for Information Systems Protection, Version 1.0," <http://www.fas.org/irp/offdocs/pdd/CIP-plan.pdf>(Retrieved on June 19, 2012).

Denning, D. E., "Cyberterrorism," testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, May 23, 2000, <http://www.cs.georgetown.edu/~denning/infosec/

cyberterror.html＞(Retrieved on June 19, 2012).

_____, “Is Cyber Terror Next?” ＜http://essays.ssrc.org/sept11/essays/denning.htm＞(Retrieved on June 30, 2012).

“Department of Defense Dictionary of Military and Associated Terms,” p. 368, ＜http://ra.defense.gov/documents/rtm/jp1_02.pdf ＞ (Retrieved on June 13, 2012).

“Estonian DDoS - A Final Analysis,” ＜http://www.h-online.com/security/news/item/Estonian-DDoS-a-final-analysis-732971.html＞(Retrieved on March 1, 2012).

“Executive Order 13010, EO 13010: Critical Infrastructure Protection, July 15, 1996,” ＜http://www.fas.org/irp/offdocs/eo13010.htm＞(Retrieved on June 17, 2012).

“Executive Order 13231 of October 16, 2001: Critical Infrastructure Protection in the Information Age,” ＜ http://www.fas.org/irp/offdocs/eo/eo-13231.htm ＞ (Retrieved on June 19, 2012).

“Executive Order 13354 of August 27, 2004: National Counterterrorism Center,” ＜http://www.fas.org/irp/offdocs/eo/eo-13354.htm ＞ (Retrieved on June 28, 2012).

Greenwald, G., “Mike McConnell, the WashPost & the Dangers of Sleazy Corporatism,” ＜ http://www.salon.com/2010/03/29/mcconnell_3/ ＞ (Retrieved on May 29, 2012).

Gross, G., “U.S. Cyber War Policy Needs New Focus, Experts Say,” ＜http://www.pcworld.com/article/174711/us_cyber_war_policy_needs_new_focus_experts_say.html＞(Retrieved on June 14, 2012).

“Highlights of the USA PATRIOT Act,” ＜http://www.justice.gov/archive/ll/highlights.htm＞(Retrieved on June 20, 2012).

Hildreth, S. A., “Cyberwarfare,” CRS Report for Congress, ＜http://www.fas.org/irp/crs/RL30735.pdf＞(Retrieved on February 20, 2012).

“Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003,” ＜http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1＞(Retrieved on June 28, 2012).

Kaplan, E., “Terrorists and the Internet,” ＜http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005#p6 ＞ (Retrieved on January 31, 2012).

Kirk, J., “Estonia Recovers from Massive DDoS Attack,” ＜http://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack＞(Retrieved on March 3, 2012).

Krasnowski, M., “Two Men Accused of Hacking into Traffic System,” ＜http://www.utsandiego.com/uniontrib/20070121/news_1n21traffic.html ＞ (Retrieved on July 4, 2012).

Lawson, S., “Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History,” ＜http://mercatus.org/sites/default/files/publication/beyond-cyber-doom-cyber-attack-scenarios-evidence-history_1.pdf ＞ (Retrieved on May 29, 2012).

Lemos, R., “What are the Real Risks of Cyberterrorism?” ＜http://www.zdnet.com/news/what-are-the-real-risks-of-cyberterrorism/124765＞(Retrieved on May 28, 2012).

Lewis, J. A., “Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats,” report submitted to the Center for Strategic and International Studies, CSIS, Washington, DC, ＜http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf＞(Retrieved on February 9, 2012).

_____, “Thresholds for Cyberwar,” report submitted to the Center for Strategic and International Studies, CSIS, Washington, DC, ＜http://csis.org/files/publication/101001_ieee_insert.pdf＞(Retrieved on February 29, 2012).

Leyden, J., “Estonia Fines Man for DDoS Attacks: Local Pest rather than International Conspiracy,” ＜http://www.theregister.co.uk/2008/01/24/estonian_ddos_fine/＞(Retrieved on June 18, 2012).

Maynor D., & Graham, R., “SCADA Security and Terrorism: We’re Not Crying Wolf,” ＜www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf＞(Retrieved on June 13, 2012).

Moteff, J. D., “Critical Infrastructures: Background, Policy, and Implementation,” CRS report for Congress, ＜http://www.fas.org/sgp/crs/homesec/RL30153.pdf＞(Retrieved on June 30, 2012).

Mueller, R. S., III, “Global Threats to the U.S. and the FBI’s Response,” testimony before the Senate Committee on Intelligence of the United States Senate, February 16, 2005, ＜http://www.fbi.gov/news/testimony/global-threats-to-the-u.s.-and-the-fbis-response-1 ＞ (Retrieved on June 4, 2012).

"National Cyber Security Division," ＜http://www.dhs.gov/xabout/structure/editorial_0839.shtm＞(Retrieved on June 21, 2012).

"National Infrastructure Coordinating Center," ＜http://www.dhs.gov/files/programs/gc_1236629756359.shtm＞(Retrieved on June 21, 2012).

"National Infrastructure Protection Plan," ＜http://www.dhs.gov/files/programs/editorial_0827.shtm#0＞(Retrieved on June 28, 2012).

"National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency, 2009," ＜ http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf ＞ (Retrieved on June 28, 2012).

"National Strategy for the Physical Protection of Critical Infrastructure and Key Assets," ＜ http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf ＞ (Retrieved on June 27, 2012).

"National Strategy to Secure Cyberspace," ＜http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf＞(Retrieved on June 27, 2012).

"National Threat Assessment Center," ＜http://www.secretservice.gov/ntac.shtml＞ (Retrieved on July 1, 2012).

"Newsline - May 3, 2007," ＜http://www.rferl.org/content/article/1143864.html＞ (Retrieved on March 1, 2012).

O'Hara, T. F., "Cyber Warfare/Cyber Terrorism," ＜http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA424310＞(Retrieved on February 1, 2012).

"Past Events," ＜http://www.ccdcoe.org/126.html＞(Retrieved on March 1, 2012).

Pollitt, M. M., "Cyberterrorism: Fact or Fancy?" ＜http://www.cs.georgetown.edu/~denning/infosec/pollitt.html＞(Retrieved on June 19, 2012).

"President Decision Directives 39: U.S. Policy on Counterterrorism," ＜http://www.fas.org/irp/offdocs/pdd39.htm＞(Retrieved on June 17, 2012).

"President Decision Directives 62: Combating Terrorism," ＜http://www.fas.org/irp/offdocs/pdd-62.htm＞(Retrieved on June 17, 2012).

"President Decision Directives 63: Critical Infrastructure Protection," ＜http://www.fas.org/irp/offdocs/pdd/pdd-63.htm＞(Retrieved on June 17, 2012).

Presidential Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructures," ＜http://www.fas.org/sgp/library/pccip.

pdf＞(Retrieved on June 7, 2012).

“Presidential Proclamation - Critical Infrastructure Protection Month,” ＜http://www.whitehouse.gov/the-press-office/presidential-proclamation-critical-infrastructure-protection-month＞(Retrieved on June 30, 2012).

“Presidential Proclamation--Critical Infrastructure Protection Month: Critical Infrastructure Protection Month, 2010,” ＜http://www.whitehouse.gov/the-press-office/2010/11/30/presidential-proclamation-critical-infrastructure-protection-month＞(Retrieved on June 30, 2012).

“Presidential Proclamation -- Critical Infrastructure Protection Month, 2011,” ＜http://www.whitehouse.gov/the-press-office/2011/11/30/presidential-proclamation-critical-infrastructure-protection-month-2011 ＞(Retrieved on June 30, 2012).

“Presidential Security Directive 1: Organizing for Homeland Security and Counterterrorism,” ＜ http://www.fas.org/irp/offdocs/psd/psd-1.pdf ＞(Retrieved on June 30, 2012).

“Public Law 107-296, Homeland Security Act of 2002,” ＜http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf＞(Retrieved on June 21, 2012).

“Public Law 107-305, Cyber Security Research and Development Act,” ＜http://www.cio.gov/Documents/pl_107_305_nov_27_2002.pdf ＞ (Retrieved on June 20, 2012).

“Public Law 108-458, Intelligence Reform and Terrorism Prevention Act of 2004,” ＜http://www.nctc.gov/docs/pl108_458.pdf＞(Retrieved on June 28, 2012).

“Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities,” ＜http://www.fas.org/irp/offdocs/pdd/CIP_2001_CongRept.pdf＞(Retrieved on June 19, 2012).

Robichaux, P., “Distributed Denial-of-Service Attacks and You,” ＜http://technet.microsoft.com/en-us/library/cc722931.aspx＞(Retrieved on June 26, 2012).

Rollins, J., & Wilson, C., “Terrorist Capabilities for Cyberattack: Overview and Policy Issues,” CRS Report for Congress, ＜http://www.fas.org/sgp/crs/terror/RL33123.pdf＞(Retrieved on July 1, 2012).

Sanger, D. E., “Obama Order Sped Up Wave of Cyberattacks Against Iran,” ＜

http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all > (Retrieved on July 4, 2012).

Schmidt, E. E., "The Evolution of U.S. Policies against Terrorism," <http://www.thepresidency.org/storage/documents/Fellows2008/Schmidt.pdf > (Retrieved on June 20, 2012).

Shea, D. A., "Critical Infrastructure: Control Systems and the Terrorist Threat," CRS Report for Congress, <http://www.fas.org/irp/crs/RL31534.pdf>(Retrieved on June 7, 2012).

Singh, A. Kr., & Siddiqui, A. T., "New Face of Terror: Cyber Threats, Emails Containing Viruses," *Asian Journal of Technology & Management Research*, Vol. 1, Iss. 1 (January - June 2011), <http://ajtmr.com/papers/vol1issue1/CyberTerror.pdf>(Retrieved on July 5, 2012).

Snow, G. M., "Cybersecurity: Responding to the Threat of Cyber Crime and Terrorism," statement before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism, Washington, DC, April 12, 2011, <http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism>(Retrieved on June 4, 2012).

Sofaer A. D., Goodman, S. E., Cuéllar, M., Drozdova, E. A., Elliott, D. D., Grove, G. D., Lukasik, S. J., Putnam, T. L., & Wilson, G. D., "A Proposal for an International Convention on Cyber Crime and Terrorism," CISAC Report, August 2000, < http://iis-db.stanford.edu/pubs/11912/sofaergoodman.pdf > (Retrieved on February 12, 2012).

"Supernatural Horror in Literature by H. P. Lovecraft," <http://www.hplovecraft.com/writings/texts/essays/shil.asp>(Retrieved on June 14, 2012).

"Synopsis for 'Live Free or Die Hard'," <http://www.imdb.com/title/tt0337978/synopsis>(Retrieved on June 14, 2012).

"Terrorism 2002-2005," p. iv, <http://www.fbi.gov/stats-services/publications/terrorism-2002-2005/terror02_05.pdf>(Retrieved on June 18, 2012).

"Terrorism FAQs," <https://www.cia.gov/news-information/cia-the-war-on-terrorism/terrorism-faqs.html>(Retrieved on June 18, 2012).

"The Sector-Specific Plans," <http://www.dhs.gov/files/programs/gc_1179866197607.shtm#2>(Retrieved on June 28, 2012).

"The World Factbook," ＜https://www.cia.gov/library/publications/the-world-factbook/geos/en.html＞(Retrieved on February 29, 2012).

Trevelyan, M., "Security Experts Split on 'Cyberterrorism' Threat," ＜http://www.reuters.com/article/2008/04/16/us-security-cyberspace-idUSL1692021220080416＞(Retrieved on June 1, 2012).

"United Nations Security Council Resolution 1566, October 2004," ＜http://daccess-ods.un.org/access.nsf/Get?Open&DS=S/RES/1566%20(2004)&Lang=E&Area=UNDOC＞(Retrieved on June 18, 2012).

"USA PATRIOT Act (H.R. 3162)," ＜http://epic.org/privacy/terrorism/hr3162.html＞(Retrieved on June 20, 2012).

"U.S. Code Title 22, Ch. 38, Sec. 2656f," ＜http://www.gpo.gov/fdsys/pkg/USCODE-2011-title22/pdf/USCODE-2011-title22-chap38-sec2656f.pdf ＞(Retrieved on July 10, 2012).

U.S. Secret Service, & Carnegie Mellon Software Engineering Institute, "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors," ＜ http://www.secretservice.gov/ntac/its_report_050516.pdf ＞(Retrieved on July 1, 2012).

U.S. Secret Service, & Carnegie Mellon Software Engineering Institute, "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector," ＜http://www.secretservice.gov/ntac/its_report_040820.pdf＞(Retrieved on July 1, 2012).

U.S. Secret Service, & Carnegie Mellon Software Engineering Institute, "Insider Threat Study: Illicit Cyber Activity in the Government Sector," ＜http://www.secretservice.gov/ntac/final_government_sector2008_0109.pdf ＞ (Retrieved on July 1, 2012).

U.S. Secret Service, & Carnegie Mellon Software Engineering Institute, "Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector," ＜http://www.secretservice.gov/ntac/final_it_sector_2008_0109.pdf＞(Retrieved on July 1, 2012).

Vandiver, S., "Critical Infrastructure is Society's Glue," ＜http://www.abchs.com/ihs/WINTER2010/ihs_articles_column.php＞(Retrieved on June 20, 2012).

Walt, S. M., "Is the Cyber Threat Overblown?" ＜http://walt.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown ＞(Retrieved on May 29,

2012).

"WarGames," ＜http://www.imdb.com/title/tt0086567/＞(Retrieved on June 17, 2012).

Weimann, G., "Cyberterrorism: How Real is the Threat?" ＜http://www.usip.org/files/resources/sr119.pdf＞(Retrieved on June 30, 2012).

_____, "How Modern Terrorism Uses the Internet," *The Journal of International Security Affairs*, No. 8 (Spring 2005), ＜http://www.securityaffairs.org/issues/2005/08/weimann.php＞(Retrieved on February 23, 2012).

Wilson, C., "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," CRS Report for Congress, ＜http://www.fas.org/sgp/crs/terror/RL32114.pdf＞(Retrieved on February 19, 2012).

國立政治大學 National Chengchi University