網路恐怖主義發展與因應對策之研究

陸軍上校　王鵬程

提　要

全球化趨勢的快速變遷，國家所面臨的安全議題已不同於冷戰時期的安全威脅型態。在非傳統安全威脅層面上，已超越國家安全的界線，成為跨國性安全議題。恐怖組織在既有的生存空間受到嚴重壓縮與限制的多重壓力條件下，將實體化的運作方式，逐漸轉向虛擬空間發展模式，規避該國政府高壓打擊。本文從探究「網路恐怖主義」的發展導因，逐步對網路恐怖主義的定義與攻擊模式進行分析與歸納，續就網路恐怖主義的挑戰與影響，提出因應網路恐怖攻擊發生之思考策略與防制措施，以維護國家安全。

關鍵字：網路恐怖主義、無領袖反抗運動、網路駭客、不對稱作戰、網路安全觀

前　　言

冷戰結束後，軍事威脅明顯降低，國際環境從原先的「意識型態」與「軍事力量」的兩極對抗，趨向於強調以「合作」的安全機制所取代。隨著全球化趨勢的快速變遷，國家所面臨的安全議題已不同於冷戰時期的安全威脅型態，國家安全的定義與範疇，除了傳統的政治、軍事或外交威脅層面之外，在非傳統安全威脅層面上，如恐怖攻擊、經濟安全、天然災害、傳染疾病等，已超越國家安全的界線，成為跨國性安全議題。尤其，全球恐怖活動情勢方興未艾，致其對物質與心理的破壞，為非傳統安全議題之首，已對各國國家安全及國際秩序造成嚴重衝擊。[1]事實上，恐怖主義隨著時代的演變，恐怖分子藉由網際網路的便利性，在網路平台上密集散播殘酷、血腥及暴力事件的文章、照片與影片，成功製造劇場效果，吸引國際社會的目光，營造全球恐懼氛圍；[2]同時運用網路資訊的易取性，招募有心人士及志同道合夥伴成為恐怖組織成員，並「啟發與激化」潛在的、具特殊背景的孤狼式恐怖分子，不待命令對全球各地發動恐怖行動。[3]

對我國而言，臺灣並不是國際恐怖組織攻擊的主要目標，且至目前為止沒有形成恐

1 楊永明，〈聯合國反恐策略與人權保障問題〉，《月旦法學雜誌》(臺北)，第131期，2006年4月，頁21。
2 林泰和，〈國際恐怖主義研究-結構、策略、工具、資金〉，《問題與研究》(臺北)，第47卷第2期，2008年6月，頁134-135。
3 張福昌，〈孤狼恐怖主義與內部安全〉，發表於「第九屆恐怖主義與國家安全」學術研討會(桃園：中央警察大學，2013年11月19日)，第18頁。

怖組織的條件，但隨著全球化趨勢的快速變遷，恐怖組織早已視我國為不友善的國家，[4]國內亦不能排除成為恐怖分子匿藏地點或犯罪活動的中繼站，然考量恐怖主義已朝國際化與網路化發展，恐怖組織可能與國內不法分子勾結，伺機發動恐怖攻擊事件，對我國家安全帶來嚴峻挑戰。因此，為適應全球化時代的來臨，消弭恐怖主義潛藏於國內的威脅與影響，本文透過探究「網路恐怖主義」(Cyber Terrorism)的發展導因，逐步對網路恐怖主義的定義與攻擊模式進行分析與歸納，續就網路恐怖主義的挑戰與影響，提出因應網路恐怖攻擊發生之思考策略與防制措施，以維護國家安全。

網路恐怖主義發展導因

一、西方國家長期進行的反恐戰爭

911事件使美國深刻體認，無法運用自身優勢單獨對抗國際恐怖主義。因此，美國為避免再次受到恐怖組織的威脅與襲擊，必需調整國家安全戰略方針，在節約國家整體資源的考量下，加強區域安全合作層面，[5]建構全球性的「反恐怖聯盟」(Global Coalition Against Terrorism)。[6]美國運用暨有的軍事、政治與經濟優勢力量與國際社會合作，交換恐怖主義活動的各種情資，希望透過國際合作共同改善邊界安全。由美國政府所主導的「反恐怖聯盟」架構不同於以往歷史上的聯盟形式，因「反恐怖聯盟」成員所共同打擊的目標不是某個特定的敵對國家，而聯盟成員也不會一成不變。誠如美國前國防部長倫斯斐(Donald Rumsfeld)的說法，「反恐怖聯盟」的成員所扮演的角色不同，貢獻的方式也不一樣。有些國家在外交上表態支持美國，有些國家給予財政援助，有些國家派兵實際參與反恐活動，有些國家基於政治、外交等各方面考量，只能秘密的透過其它管道支持美國反恐戰爭。[7]因此，國際社會在美國的主導下，聯合國安全理事會迅速且無異議的通過1373號決議案，設立「反恐怖主義委員會」(Counter-Terrorism Committee, CTC)，[8]由安全理事會十五名成員組成，其目的為加強各會員國打擊國內、外恐怖主義活動的能力。[9]基此，國際政治自911事件發生後，

4 賴昭穎，〈亞太反恐同盟歐巴馬提到台灣〉，《聯合新聞網》，2015年11月24日，<http://udn.com/news/story/8988/1333731>(檢索日期：2018年8月5日)

5 2002年美國國家安全戰略(National Security Strategy, NSS)第一章即明白指出，將「打擊恐怖主義」列為國際戰略執行首要任務之一。2006年國家安全戰略報告書中再次強調消滅恐怖主義及大規模毀滅性武器(Weapons of Mass Destruction, WMD)決心。2008年，歐巴馬政府上任後，因美國政府深陷反恐戰爭與金融危機之中，在節約國家整體資源的考量下，被迫調整國際戰略，加強區域安全合作層面。

6 林正義，〈美國因應911 事件的危機處理〉，《戰略與國際研究季刊》，第4 卷第1 期，2002年1月，頁109。

7 吳東野，〈全球反恐聯盟及其相關問題之探討〉，《遠景季刊》，第4卷第1期，2003年1月，頁11。

8 聯合國反恐怖主義委員會網址：http://www.un.org/en/counterterrorism/overview.shtml。(檢索日期：2018年10月9日)

從聯合國最高國際性組織，到區域安全合作或國家間的雙邊會談等相關議程與議題，均圍繞於如何防範及有效打擊恐怖主義為主。由於反恐議題已成為國際議程的優先執行項目，即使各國遭受恐怖主義威脅程度無法與美國相比，但國際間深受全球化的影響及「反恐怖聯盟」的主導下，各國勢必投入更多的時間、經費、軍力及資源，共同支助或參與由美國政府所發動的反恐戰爭，[10]大幅壓縮恐怖組織活動空間。

有鑑於團體或組織型恐怖活動容易成為反恐單位打擊目標之缺點，恐怖組織所執行的恐怖活動容易引起國際社會關注，間接暴露恐怖攻擊計畫與行動，且易成為該國政府及情報單位搜尋與反恐部隊打擊的對象。恐怖組織在既有的生存空間受到嚴重壓縮與限制的多重壓力條件下，反而迫使恐怖分子藉由網際網路的隱密性與匿名性，將實體化的運作方式，逐漸轉向以電子訊息、網路交流平台等虛擬空間發展模式，強力散播恐怖主義思想、募集恐怖活動資金、吸收恐怖組織新成員及指揮、調度、下達攻擊指令等，[11]藉以規避該國政府高壓打擊。

二、移民社群長期飽受歧視

1970年代後，西方國家為鼓勵移民團體保留自身的文化，並與其他的文化實施交流，多元文化政策廣為歐美等西方民主國家推崇與接受，希望藉由此項政策，使西方社會形成多民族、多信仰及多文化的和平相處與彼此融合，達到共同繁榮與進步的目標。[12]然根據英國皇家智庫國際事務研究所(Chatham House)公布的最新調查顯示及近期西方國家接續發生重大恐怖攻擊事件分析得知，西方國家之所以成為恐怖組織發動恐怖攻擊的主要目標，究其原因，乃西方國家複雜的政治、外交、經濟與移民政策，使得許多移民團體無法與當地社會群眾相互融合，增加文化間的衝突，且大多數的西方國家民眾反對接收穆斯林新移民；分析認為，由於伊斯蘭信仰的獨立與排他性，大部分的穆斯林社群，無法融入當地社會，形成了獨立的群體及社會的邊緣人。[13]

9 劉承宗，〈聯合國反恐委員會十年的回顧與展望〉，《嶺東通識教育研究學刊》，第4卷第2期，2012年2月，頁158-161。

10 王高成，〈恐怖主義對當前國際關係的影響〉，發表於「第一屆恐怖主義與國家安全」學術研討會(桃園：中央警察大學，2005年12月29日)，頁17-19。

11 王朝煌，〈網際網路恐怖活動資訊搜尋技術之探討〉，發表於「第二屆恐怖主義與國家安全」論文集(桃園：中央警察大學，2006年12月28日)，第113頁。

12 美國學者杭廷頓(Samuel P. Huntington)在「文明衝突與世界秩序的重建(The Clash of Civilization and The Remarking of World Order)」書中指出，後冷戰時期，全球政治趨勢已從過往強調意識形態、政治或經濟的不同，逐步沿著文化及文明的界限進行重組，並圍繞在文化與文明的「斷層線」兩側。國際社會強調以文明為基礎的世界秩序正在成形，西方世界觀和其他文明間的衝突逐漸升高，且多半發生於穆斯林和非穆斯林之間。

13 常青、東海，〈歐洲大多數人拒絕穆斯林新移民〉，《希望之聲》，2018年10月10日。< http://www.soundofhope.org/gb/2017/02/16/n740465.html>(檢索日期：2017年8月28日)

而西歐國家自2010年歐債危機爆發後，區域內經濟就陷入了疲軟，歐洲的社會福利在削減，社會矛盾在激化，本來已經存在多年的歐洲極端主義思潮開始不斷蔓延，另穆斯林移民及其後代長期受到歧視及就業機會貧缺的惡劣條件下，加上2015年後，西方各國為彰顯人道主義，持續對敘利亞難民展開了懷抱，造成二戰以來最大的難民潮向北非及歐洲地區擴散。由於歐盟國家是不設關卡的，所以難民及潛伏於其中的恐怖分子可從敘利亞到土耳其，再從土耳其到東歐，並直接跨越與進入西歐和北歐國家，[14]助長恐怖勢力如癌細胞般向歐洲地區快速擴散外，[15]恐怖組織更利用網路平台擴大「宣傳」、「激化」與「感召」各國穆斯林裔青年及各地潛在支持者投奔恐怖組織行列，並運用網際網路的高度隱密性，將「傳統恐怖攻擊手段」結合「網路駭客技術」，針對各國政府資訊、金融、軍事、能源等國家重大基礎建設進行「網路恐怖攻擊」，並鼓動每一位孤狼式恐怖分子運用隨手可得的殺戮工具、毒物、爆裂物等，[16]鎖定重大公開活動、人潮聚集處所等進行恐怖襲擊，製造恐怖攻擊悲劇。[17]

網路恐怖主義定義、攻擊模式(型態)分析

一、定義

「網路恐怖主義」是恐怖主義的一種，因此在定義「網路恐怖主義」前必須對恐怖主義定義具備基本認知。鑑於時下的恐怖主義定義約有200多種，且恐怖主義所牽涉的層面往往觸及上層的政治問題，而非簡單的學術議題或法理研究所能清楚界定。而各國在界定「恐怖主義」定義時，所謂「恐怖分子」與「自由鬥士」的分別，乃基於確保該國「國家利益(National Interest)」為優先考量，導致國際社會對恐怖主義定義給予不同的解釋與定義，[18]嚴重影響「反恐怖聯盟」的效能。根據我們對於恐怖主義的理解，發現構成恐怖主義內涵的有「仇恨」、「不滿」、「挫折」、「反抗」等多種因素。[19]

14 〈歐洲近年為何被IS盯上？六大原因：根本是自惹的〉，《中時電子報》，2016年3月23日。< http://hottopic.chinatimes.com/20160323003457-260803>(檢索日期：2018年10月13日)

15 李昱德，〈恐攻＋難民潮後 歐洲現在怎麼了？〉，《台灣英文新聞》，2016年2月13日。< https://www.taiwannews.com.tw/ch/news/2880832>(檢索日期：2018年10月15日)

16 鼓吹孤狼式恐怖主義的重要文件。第一份文件出現於2003年初，在一個極端網路論壇Sada al Jihad(Echoes of Jihad)上，鼓吹追隨賓拉登思想者不待命令對全球各地發動恐怖行動(encouraged Al-Qaida sympathizers to take action without waiting for instructions)；第二份文件出現於2004年，阿布·穆薩布·蘇瑞(Abu Musab al-Suri)在網路上發表名為「號召全球伊斯蘭反抗運動(Call for Worldwide Islamic Resistance)」的文章，內文強調由個人或小型獨立團體所帶領的「無領袖反抗運動」(Leaderless Resistance)，將擊敗敵人；第三份文件出現於2006年，由蓋達組織的精神領袖阿布·吉哈德·馬斯里(Abu Jihad al-Masri)發表一篇「如何獨立戰鬥」(How to Fight Alone：Proposed Ideas and Methods)。

17 林泰和，〈近期歐洲恐怖主義發展之研析〉，《問題與研究》，第55卷，2016年12月，頁118。

18 林泰和，〈國際恐怖主義研究-結構、策略、工具、資金〉，《問題與研究》，第47卷第2期，2008年6月，頁123。

探究「恐怖主義」概念，可追朔至1795年的法國大革命時期，當時「恐怖主義」被視為是基於本身的信念與要求外界對其訴求的重視，必需採取極其高壓的手段與措施，亦是建立18世紀民主秩序不可缺少的工具。

當前「恐怖主義」主角是由非國家或次國家行為者(no state actor)所構成，其執行恐怖攻擊主要目的是反對該國政府的革命行動，所從事的暴力行為已發展成為非傳統安全威脅之首，對各國國家安全帶來前所未有的巨大挑戰。[20]

既然「恐怖主義」有這麼多不同的定義，而「網路恐怖主義」又以新興恐怖主義新姿態呈現；因此，各國政府、專家及學者在缺乏研究個案的情況下，如何定義「網路恐怖主義」所遇到的困難將大於定義團體或組織型恐怖主義。本文僅就各界對「網路恐怖主義」的定義臚列於后：

(一)詞典定義：

1.牛津辭典(Oxford Living Dictionary)將其定義為：「出於政治動機使用電腦和資訊技術造成社會嚴重破壞或普遍恐懼。」[21]

2.劍橋辭典(Cambridge Dictionary)將網路恐怖主義定義為：「出於政治或其他原因使用網路對破壞或摧毀它國電腦系統。」[22]

(二)政府定義：

1.美國國防部(Department of Defense)將網路恐怖主義定義為：「次國家行為體利用計算機及電信能力針對資訊系統、程式實施的犯罪行為，以造成暴力與破壞公共設施，製造社會恐慌，旨在影響政府或社會，實現特定政治、宗教或意識形態目標。」[23]

2.美國聯邦調查局(Federal Bureau of Investigation, FBI)將其定義為：「有預謀的，出於政治動機的攻擊資訊系統、電腦系統、電腦運算及數據資料，導致非戰鬥目標等地方團體或組織的嚴重受損。」[24]

3.北大西洋公約組織(North Atlantic Treaty Organization, NATO)將其定義為：「利用電腦或通信網路製成各種破壞行動，使人們產生恐懼或迫使社會進入恐怖意識形態。」[25]

(三)學者定義：

1.美國國家關鍵基礎設施保護中心主任羅納德・迪克(Ronald L. Dick)認為網路恐怖

19 邱伯浩，《恐怖主義與反恐》(臺北：新文京開發，2006年11月)，頁3。
20 同註18，頁124。
21 Oxford English Dictionary, <https://en.oxforddictionaries.com/definition/cyberterrorism>(檢索日期：2018年10月17日)
22 Cambridge Dictionary, <https://dictionary.cambridge.org/zht/%E8%A9%9E%E5%85%B8/%E8%8B%B1%E8%AA%9E/cyberterrorism>(檢索日期：2018年10月17日)
23 鄒文豐，〈新興恐怖主義的挑戰與因應對策：社會建構論的觀點〉，《復興崗學報》，第111期，2017年12月，頁7。
24 U.S. Federal Bureau of Investigation, <https://searchsecurity.techtarget.com/definition/cyberterrorism>(檢索日期：2018年10月17日)
25 NATO Review Magazine, <https://www.nato.int/docu/review/2011/11-september/cyber-threads/en/index.htm>(檢索日期：2018年10月17日)

主義係指：「透過網路從事暴力行為，導致死亡、財產損害或威脅政府改變其既定政策。」[26]

2.美國資訊安全研究學者多蘿西・丹寧(Dorothy Denning)將網路恐怖主義定義為：「針對電腦、網路及資訊儲存系統執行非法攻擊手段，對其產生嚴重威脅或破壞，並強迫或恐嚇政府及人民，達到恐嚇、脅迫政府或社會，進而達成其政治目的。」[27]

3.美國加州大學洛杉磯分校教育與資訊學院學者斯圖爾特・比格爾(Stuart Biegel)對網路恐怖主義的定義為：「計劃及持續性的透過電腦及網路系統製造極端暴力手段，迫使政府及社會秩序造成嚴重混亂。」[28]

4.澳洲國際事務學院學者凱蘭・哈迪(Keiran Hardy)將網路恐怖主義的定義為：「運用資訊設備(如電腦蠕蟲，病毒或惡意軟件)，執行滲透並嚴重干擾關鍵基礎設施。關鍵基礎設施是指設施、服務和網路，如果長時間離線，將對國家公共衛生、經濟、環境或安全造成嚴重危害。」[29]

二、行為模式

(一)網路支援恐怖活動

網路成為新興恐怖主義「號召」、「鼓吹」及「發動」恐怖攻擊的最佳工具。恐怖分子在伊斯蘭極端組織的號召下，運用網路、媒體兩項工具進行資料蒐集、通訊聯繫、招募新員、募集資金、製造文宣及散發病毒外，更利用上述工具執行恐怖攻擊指導與命令傳達，且在大眾媒體的宣傳、傳播等全力配合之下，製造劇場效果，吸引國際社會的目光，成功營造全球恐懼氛圍，成為當前恐怖攻擊浪潮。[30]以全球最大的伊斯蘭慈善組織，曾經資助全球各地恐怖活動的「國際伊斯蘭紓困組織」(International Islamic Relief Organization, IIRO)為例，恐怖主義支持者可透過網路得知其捐款帳號與最新消息，進行跨國網路捐款，再由恐怖組織將匯入資金

26 時任美國國家關鍵基礎設施保護中心主任羅納德·迪克(Ronald L. Dick)於2002年6月24日主持「網絡恐怖主義和關鍵基礎設施保護」時指出2001年9月11日的紐約恐怖襲擊直接和嚴重影響了美國銀行、金融、電信、航空和鐵路交通、能源和供水。Ronald L. Dick,"Testimony", June 24, 2002< https://archives.fbi.gov/archives/news/testimony/cyber-terrorism-and-critical-infrastructure-protection>(檢索日期：2018年10月19日)

27 喬治城大學電腦科學部資訊安全研究學者多蘿西.丹寧(Dorothy Denning)於2000年指出網絡恐怖主義行為如爆炸，飛機失事，水污染或嚴重經濟損失等對該國重要基礎設施的攻擊將產生重大影響。Dorothy Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy" 2001< http://www.mtholyoke.edu/~lwpoole/politics116/cyberterrorism.html>(檢索日期：2018年10月19日)

28 Stuart Biegel, "BEYOND OUR CONTROL? CONFRONTING THE LIMITS OF OUR LEGAL SYSTEM IN THE AGE OF CYBERSPACE," Harvard Journal of Law & Technology, Volume 15, Number 2 spring 2002, p544.

29 Keiran Hardy,"Is Cyberterrorism a Threat?", 20 FEB 2017 < https://www.internationalaffairs.org.au/australianoutlook/is-cyberterrorism-a-threat/>(檢索日期：2018年10月19日)

30 林泰和，〈國際恐怖主義研究-結構、策略、工具、資金〉，《問題與研究》，第47卷第2期，2008年6月，頁134-136。

進行分配與運用，提供恐怖組織基地設施的維護及執行恐怖攻擊所需的費用。尤其，國際恐怖組織為避免被執法單位查獲通常以「哈瓦拉」(hawala)，貨幣轉換網路(money transfer networks)體系做為恐怖活動資金流動的方式；相較於合法金融機構，「哈瓦拉」擁有較好的匯率與較低的手續費，且由於「哈瓦拉」，保證資金交易後不會留下任何書面紀錄，因此成為恐怖組織金融交易的主要方式，且深得恐怖分子信賴。[31]

此外，在新員招攬與訓練方面，從「伊斯蘭國」藉由網際網路傳播綁架人質、處決異議人士、屠殺無辜民眾及歐美國家遭受「孤狼式恐怖攻擊」等各種殘忍手段內容，[32]造成歐美、中東地區人心惶惶與周邊國家動盪不安等影響國際社會秩序行為得知，當前恐怖組織乃透過網際網路進行人員募集、人員訓練及特殊專長養成等，促使偏見人士及社會邊緣族群，藉由網路媒體輕易獲得恐怖攻擊相關資訊，陸續加入恐怖主義行列，製造恐怖攻擊悲劇。[33]

(二)實體網路攻擊

恐怖主義是全世界共同的敵人，就發展與演變速度而言，已成為非傳統安全威脅之首。「網路恐怖主義」亦是恐怖主義的另一種呈現方式，恐怖分子將網際網路視為工具，利用專業技術針對網路系統運作進行干擾或破壞其系統運作，也就是將「傳統恐怖主義」與「網路駭客」相互結合，大幅提升恐怖攻擊成效。就威脅程度而言，遠超越傳統恐怖主義所產生的殺傷力與破壞力。當恐怖分子利用網際網路工具，對政府部門資訊設備進行竊取資訊、破壞系統、植入病毒等嚴重干擾該國水力、電力、通訊、能源、交通、金融、軍事等國家關鍵基礎設施與公共服務及民生系統正常運作時，將導致系統被迫中斷，造成無法彌補的重大損失。此等恐怖攻擊行為以網路為工具，所執行的恐怖攻擊力度更強、攻擊範圍更廣、防範難度更大，對於攻擊目標已不再是單純的針對平民百姓或政治對立者，所涉及的安全議題已明顯超越國家安全層面。[34]以2017年3月，歷史上最大的勒索軟體「想哭(WannaCry)」襲擊了全球近100個國家為例，恐怖分子利用「勒

31 同註30，頁140。

32 歐美國家有利於孤狼式恐怖主義的快速興起與迅速蔓延，主要原因如下：1.歐美經濟不景氣，加上意識形態和價值觀上對於移民政策的排斥；2.西方國家極右翼思潮快速上升，導致社會分裂，排外民族主義再度崛起；3.武器管制不嚴，槍支及爆裂物容易獲得，使得孤狼式恐怖攻擊得以實現；4.恐怖分子可經由網際網路獲得製作爆裂物之相關資訊；5.孤狼式恐怖攻擊「成本低、效益高」，具隱蔽性與機動性，且執行恐攻行動前，不易遭情報單位鎖定。

33 從「全球恐怖主義資料庫(Global Terrorism Database, GTD)」數據顯示，恐怖分子仍活耀於全球各地，尤其以中東、北非及歐洲地區恐怖攻擊事件最為頻繁與嚴重。對國際社會而言，恐怖主義並未因美國及全球反恐聯盟的掃蕩而消失，且恐怖組織為規避該國政府高壓打擊，已從過往「團體型」的嚴密組織，調整成「單獨型」的恐怖活動，全面將「組織」、「結構」與「行動」方面進行轉型與調整。

34 同註23，頁6。

索軟體(ransomware)」針對全球各大醫院、公司、政府部門系統進行網路勒索攻擊，造成數以萬計的資料流失及遭到封鎖。英國、西班牙、葡萄牙及俄羅斯等國家部分醫療體系遭到「想哭(WannaCry)」軟體攻擊後，造成醫療系統中斷而無法正常運作，部分病患甚至被迫停止一切醫療行為，為接續治療必須移轉至其它醫院。

根據研究得知，惡意郵件藉由欺騙方式誘使受害者打開「勒索軟體」的同時，勒索病毒隨即將受害者的電腦系統或重要文件進行數據加密，並勒索受害者支付300到600美元贖金，而大部分的受害者乃經由網路購買比特幣(bitcoin)支付勒索金額，才能恢復原系統或文件使用權。美國國土安全部針對此次勒索軟體事件，進行跨部會技術支援與分享，並於日後七大工業國(G7)組織會議時，共同與他國財政部長及央行總裁就「勒索軟體」對於各國金融交易與財政措施影響，進行討論並承諾聯手打擊日益嚴重的網絡攻擊威脅等發表了一份聲明草案。[35]

挑戰與影響

一、利用資訊平台吸收特定族群

911事件後，恐怖組織因全球反恐聯盟的共同合作與有效打擊，使得恐怖分子的避難所及訓練營地遭到摧毀與破壞，致使恐怖勢力為從實體化的團體，走向虛擬化、沒有架構、無領導階層的小規模獨立組織，並利用網路空間的虛擬化、隱蔽性等優異條件，執行一系列無攻擊重心的恐怖攻擊行動。恐怖分子藉由網際網路的線上平臺運用，大量吸收長期飽受西方社會歧視背景條件下的穆斯林青年與移民社群，伺機激化、招募及吸引各國弱勢及邊緣化穆斯林裔青年，投奔「蓋達組織」及「伊斯蘭國」懷抱的絕佳機會，並對其進行心理戰、宣傳戰、線上教學、虛擬訓練及募集資金等一系列網路策劃與整合。[36]

事實上，恐怖分子透過網路散播近期恐怖攻擊行動影像、圖片與資訊，製造全球恐慌與威脅，造成人們心理上對恐怖主義產生巨大恐懼，並乘機宣傳恐怖分子所執行暴力活動，主要目的為深陷西方世界不平等對待的同袍們發聲，試圖引起同情者共鳴及強調恐怖行動的正當性。此外，恐怖分子亦運用電子郵件、影音資料、線上社群等互動與教學等方式對於具有保護色功能的本國籍激進人士及極端分子，[37]進行線上教學與虛擬

35 "Biggest ransomware outbreak in history' hits nearly 100 countries with data held for ransom", 13 May 2017 < https://www.abc.net.au/news/2017-05-13/biggest-ransomware-outbreak-in-history-hits-nearly-100-nations/8523102>(檢索日期：2018年10月29日)

36 Gabriel Weimann著，馬浩翔譯，《新一代恐怖大軍：網路戰場》(台北：中華民國國防部，2018年10月)，頁40-65。

37 張福昌在「歐美本土恐怖主義的發展與因應策略」提出本土恐怖主義是一種新型恐怖主義，其特色在於「利用具有保護色功能的本國籍人民作為遂行恐怖活動的工具，以避人耳目，躲避情資單位的監視、調查與破壞，使當事國防不勝防，進而達到製造恐怖攻擊、擾亂公共秩序的目的。」

訓練，使他們不需集中訓練，便能藉由網路資訊實施自我激化並執行恐怖攻擊任務。以2009年11月5日，美軍精神科醫生哈桑(Nidal Malik Hasan)少校在美國德克薩斯州胡德堡基地開槍造成14人死亡，30人輕重傷的重大案件為例，哈桑少校深受葉門「基地」組織精神領袖安瓦爾·奧拉基的影響，長久以來與其有電郵往來，而哈桑的同事也於事發前即察覺哈桑少校近年來在思想及行為舉止上有越發激進的現象。因未適時反應上級長官知悉，終究造成無法彌補的重大悲劇。美國國防部和聯邦調查局對於未能防止這起槍擊案亦展開全面調查，也對此舉行聽證會。[38]

二、鼓動孤狼式恐怖分子發動攻擊

有鑑於團體或組織型恐怖活動容易成為反恐單位打擊目標之缺點，自2000年代初期，出現三份鼓吹孤狼式恐怖主義的重要文件。第一份文件出現於2003年初，在一個極端網路論壇Sada al Jihad(Echoes of Jihad)上，鼓吹追隨賓拉登思想者不待命令對全球各地發動恐怖行動(encouraged Al-Qaida sympathizers to take action without waiting for instructions)；第二份文件出現於2004年，阿布·穆薩布·蘇瑞(Abu Musab al-Suri)在網路上發表名為「號召全球伊斯蘭反抗運動(Call for Worldwide Islamic Resistance)」的文章，內文強調由個人或小型獨立團體所帶領的「無領袖反抗運動」(Leaderless Resistance)，將擊敗敵人；第三份文件出現於2006年，由蓋達組織的精神領袖阿布．吉哈德．馬斯里(Abu Jihad al-Masri)發表一篇「如何獨立戰鬥」(How to Fight Alone：Proposed Ideas and Methods)，鼓動每一位孤狼恐怖分子運用隨手可得的殺戮工具、毒物、爆裂物等採取攻擊行動。[39]恐怖組織將網路視為平台工具，藉以宣傳恐怖思想及下達攻擊指令等，為當前新興模式的無領袖反抗運動，亦是全面將「組織」、「結構」與「行動」方面進行轉型與調整。根據IEP資料，[40]2017年《全球恐怖主義指數》(Global Terrorism Index 2017, GTI)研究報告指出，自2008至2017年間，經濟合作暨發展組織(Organization for Economic Co-operation and Development，OECD)所遭受的恐怖攻擊事件中，[41]計有250件是由深受伊斯蘭國極端組織影響的孤狼恐怖分子所執行(如圖一)，[42]其中又以美國、英國、法國、德

38 Robert D McFadden,"Army Doctor Held in Ft. Hood Rampage," New York Times, November 5 2009,<http://www.nytimes.com/2009/11/06/us/06forthood.html>(檢索日期：2018年12月6日)

39 張福昌，〈孤狼恐怖主義與內部安全〉，發表於「第九屆恐怖主義與國家安全」學術研討會(桃園：中央警察大學，2013年11月19日)，第18頁。

40 澳洲知名智庫「經濟與和平研究所(Institute for Economics and Peace, IEP)」在「恐怖主義與因應策略全國聯盟研究中心, START」的協助下，於2012年公布第一版《全球恐怖主義指數》(Global Terrorism Index 2012, GTI)年度研究報告。

41 是全球35個市場經濟國家組成的政府間國際組織，總部設在巴黎米埃特堡(Chateau de la Muette)。

42 Institute for Economics and Peace, "Global Terrorism Index 2017：Measuring and Understanding the Impact of Terrorism," p71.

圖一　2008-2017年經濟合作暨發展組織遭受孤狼式恐怖攻擊死亡人數統計圖

資料來源：Institute for Economics and Peace, "Global Terrorism Index 2017：Measuring and Understanding the Impact of Terrorism," p.71.

國及比利時所受到的恐怖攻擊最為嚴重。以美國為例，孤狼恐怖分子共發動81次攻擊，造成177人死亡；其次為英國，遭受47次孤狼恐怖攻擊，造成69人死亡。

三、高度隱密造成查緝困境

2011年美國蘭德公司詹金斯(Brian Michael Jenkins)研究員發表一篇名為《蓋達組織網路戰略是否有效？》(Is Al Qaeda's Internet Strategy Working？)的研究報告。文中指出，全球各地恐怖組織無不將網際網路視為當前計劃、執行恐怖行動的主要工具，以往恐怖行動必須透過面對面交流才能完成人員訓練、情報交換等，現在藉由網際網路、臉書、部落格及聊天室等多元化管道，使得恐怖主義思想與恐怖攻擊行動的執行更加容易。根據詹金斯博士的研究，蓋達組織將網站區別為三個層級：第一層為蓋達組織的官方網站，主要用來發布官方訊息；第二層為提供聖戰英雄於網站上討論戰略議題；第三層為藉由許多聊天室及個別網站，使恐怖主義追隨者能於該網站中大談闊論，並發表他們的作戰企圖、威脅恐嚇並彼此鼓勵行動方案討論與執行。[43]在全球眾多恐怖組織中，蓋達組織將傳統恐怖戰術與網路科技結合發揮得淋漓盡致，而新型網路恐怖主義亦實現了「無領袖反抗運動(Leaderless Resistance)」及「不對稱作戰(Asymmetric Warfare)」的攻擊模式，也就是不屬於任何恐怖組織與團體的孤狼式恐怖主義。近年在探究孤狼恐怖分子執行恐怖攻擊的動機方面，更以政治的對立、伊斯蘭基本教義、種族及宗教極端狂熱分子及個人訴求等四個方面為主要因素，其中以政治對立所佔比例最高，為孤狼恐怖分子發動恐怖攻擊因素之首；其次為伊斯蘭基本教義。此外，就近年國內、外學者從事孤狼式恐怖主義研究所提之類型、行為模式，將孤狼式恐怖主義分為世俗型(secular)、宗教型(religion-based)、單一議題型(singe-issue)、犯罪型(crime)和古怪型(quirky)等五種類型。[44](如下表所示)：

由於孤狼式恐怖分子行事低調，行蹤隱密，且藉由網路獲得訊息、激化訓練等，使得執法及情治單位在孤狼式恐怖分子執行恐怖活動前，無法有效且精準掌握其攻擊動向、地點與時間。

43 Brian Michael Jenkins, "Is Al Qaeda's Internet Strategy Working? ", December , 2011, pp1-2.

44 周勇進，〈「一個人的軍隊」：「獨狼」緣何兇猛〉，《北京新浪網》2013年5月6日。<http://news.sina.com.tw/article/20130506/9530260.html>(檢索日期：2018年12月13日)

類型	世俗型	宗教型	單一議題型	犯罪型	古怪型
時間	2011年7月22日	2009年11月5日	2002年5月6日	2001年9月18日	2016年7月22日
案例	挪威爆炸和槍擊事件	胡德堡基地槍擊事件	暗殺荷蘭政治家	炭疽攻擊事件	慕尼黑槍擊事件
地點	首都奧斯陸市、烏托亞島	美國德克薩斯州胡德堡基地	阿姆斯特丹	美國	慕尼黑奧林匹亞購物中心
恐怖分子	布雷維克(Anders Behring Breivik)	哈桑(Nidal Malik Hasan)少校	葛拉夫(Volkert van der Graaf)	布魯斯·愛德華茲·艾文斯(Bruce Edwards Ivins)	戴維·桑波里(David Sonboly)
犯案事由	移民政策	深受「基地」組織影響、歧視	保護回教少數族群以及社會弱勢團體	促進疫苗生產	精神抑鬱
攻擊方式	汽車炸彈、槍枝	槍枝	槍枝	炭疽桿菌	槍枝
造成傷害	77人死亡，百人受傷，政府大樓損毀	14人死亡，30人輕重傷	1人死亡	5死亡，17人被感染	9人死亡，27人受傷

資料來源：

1. 胡蕙寧，〈挪威大屠殺逾90人喪生〉，《自由時報》2011年7月24日。<http://news.ltn.com.tw/news/focus/paper/510994>(檢索日期：2018年12月11日)
2. Robert D McFadden,"Army Doctor Held in Ft. Hood Rampage," New York Times, November 5 2009,<http://www.nytimes.com/2009/11/06/us/06forthood.html>(檢索日期：2018年12月11日)
3. 暗殺荷蘭政治家佛圖恩兇嫌判刑18年〉，《臺灣性別人權協會》，2003年4月18日，< http://gsrat.net/news/newsclipDetail.php?ncdata_id=187 >(檢索日期：2018年12月11日)
4. United States Department of Justice, "AMERITHRAX INVESTIGATIVE SUMMARY Released Pursuant to the Freedom of Information Act", February 19, 2010, pp38-40.
5. 易聞，〈慕尼黑商場槍擊9死 槍手獨立犯案〉，《新唐人新聞》，2016年7月24日，<http://www.ntdtv.com/xtr/b5/2016/07/24/a1277670.html >(檢索日期：2018年12月11日)
6. 本研究整理

因應對策

一、加強國際合作、分享情報資訊

精準的情報才是打擊恐怖活動最佳的利器，沒有正確的恐怖活動訊息，各國或國際間情報單位在執行反恐怖活動時將事倍功半。然而情報蒐集與分析亦是國內、外情治單位有效監控、預防與打擊網路恐怖主義的重要部分。以美國及中國大陸雙邊反恐合作為例，911事件後，美國為爭取國際社會的支持，中國大陸乃是美國全球反恐戰略中不可缺席且極力拉攏的主要國家之一。尤其，自911事件後，中國大陸是第一個作出正式反應的亞洲國家，[45]中國大陸明確表示將運用一切方法徹底打擊國際恐怖主義，在兩國加強反恐情報交流和溝通的基礎上，建立反恐情資與技術交流平台。[46]

2002年10月，美、中兩國經過磋商，中國大陸同意美國聯邦調查局(Federal Bureau Investigation, FBI)在美駐中國大陸使館內設立臨時辦公室；中國大陸同意的目的是基於

45 2001年9月12日，中共國家主席江澤民於攻擊事件後，立即致電美國總統小布希表達慰問及強烈譴責暴力行為，江澤民強調「此次攻擊事件不僅給美國人帶來了災難，也是對世界人民向往和平的真誠願望的挑戰。中共政府，強力譴責這起駭人聽聞的恐怖活動。中共願意與美方及國際社會加強對話，發展合作，共同打擊一切恐怖主義暴力活動」。 中、美兩國除元首對話外，雙方也利用上海合作組織及亞太經合會等國際性組織，實際推動各層面反恐合作。

46 朱鋒，〈911和中美關係〉，《BBC中文網》，2002年9月18日，〈http://news.bbc.co.uk/hi/chinese/china_news/newsid_2266000/22662262.stm〉(檢索日期：2018年12月25日)

美、中雙方情資共享與交流，中國大陸也保留在美國設立相應機構的權利。[47]然就美、中雙方加強執法領域合作方面，雙方同意採取促進執法人員交流、完善磋商機制、建立有關部門之間熱線聯絡渠道、即時交換情報資訊等措施，加強雙方在緝捕和遣返在逃犯罪嫌疑人、反恐、打擊跨國犯罪、毒品走私、偽造貨幣、洗錢、侵犯智慧財產權和網路犯罪、遣返非法移民等方面的合作。中國大陸公安部與美國司法部簽署一系列合作文件，其中包括「中國大陸公安部與美國聯邦調查局關於反恐情報資訊交流與合作的諒解備忘錄」，[48]雙方持續加強在反恐情報交流合作。

二、立法構建秩序、保護網路安全

2001年9月28日聯合國安全理事會第4385次會議通過第1373號決議，呼籲各國應在國內法中明確規定恐怖行動為嚴重犯罪，並在行政和司法事項上合作，以防制恐怖行動外，更鼓勵透過雙邊或多邊協議，共同合作制止恐怖行動。聯合國各會員國依照該項決議，迅速採取反恐怖作為或制定相關法律，美國於同年(2001年)10月26日通過「2001年提供阻絕恐怖主義所需適當手段以鞏固美國法案(Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001)」(簡稱「愛國者法案(USA PATRIOT)」)、日本通過制定「恐怖對策支援法」、德國通過制定「反國際恐怖主義法」、加拿大通過「C-36」法案(簡稱「反恐怖行動法」)，其他國家亦配合聯合國措施，制定反恐專法或修改相關法律。[49]

上述各國所制定之反恐法案乃針對團體或組織型恐怖主義，對於網路恐怖主義所產生安全威脅，已引起各國高度重視。以中國大陸為例，習近平上任後在2016年4月19日，網路安全和資訊化工作座談會上提出「網路安全觀」的核心概念，強調為建構全天候、全方位的「感知網路安全」必須將網路安全法治化，才能維護國家主權、安全和發展利益，並堅持「依法治網、依法辦網、依法上網」的原則，制定立法條文。[50]《中華人民共和國網路安全法》為基於上述條件下，2016年11月7日經第十二屆全國人大常委會第24次會議表決通過，並於2017年6月1日正式施行。[51]

47 張雅君，〈中共反恐外交的實踐與成效之分析〉，《中國大陸研究》，第48卷第1期，2005年3月，頁67。
48 徐海濱，〈中美簽署加強執法合作聲明 將交流反恐情報資訊〉，《國際線上》，2006年7月31日，<http://big5.chinabroadcast.cn/gate/big5/gb.cri.cn/8606/2006/07/31/1062@1153680.htm> (檢索日期：2018年12月25日)
49 法務部，「法務部研擬完成反恐怖行動法草案」，2005年11月27日發表於中華民國法務部：<https://www.moj.gov.tw/cp-21-49487-f3feb-001.html>(檢索日期：2019年1月2日)
50 中華人民共和國國家信息網辦公室，「習近平的網路安全觀」，2018年02月02日<http://www.cac.gov.cn/2018-02/02/c_1122358894.htm>(檢索日期：2019年1月2日)
51 中華民國大陸委員會，「有關中國大陸實施「網絡安全法」相關新聞參考資料」，2017年06月04日<https://www.mac.gov.tw/News_Content.aspx?n=A0A73CF7630B1B26&s=C69752E507927000 >(檢索日期：2019年1月2日)

三、 建立偵測系統、完善通報機制

我國情治單位除參考先進國家打擊新興恐怖主義作法外，亦應透過網路監控、情報交流與傳遞，事先掌握可能犯案的本國人士、外籍人員與犯案地點，並針對民眾經常聚集、出入頻繁及重大集會的地點，加強情蒐偵防及現場的巡邏，都將有助於預防及降低恐怖事件的發生。[52]此外，美國第一份「美國國土安全國家戰略報告(National Strategy for Homeland Security, 2002)」，將「情報及預警系統建立(Intelligence and Warning)」列為首要任務。內文強調，為避免恐怖分子以猝不及防的方式發動恐怖攻擊，在提升「情報及預警系統建立」主要有下列五項目標：(1)提高聯邦調查局的分析能力；(2)建立資訊分析及重要基礎設施安全維護部門；(3)落實國土安全顧問體系；(4)運用交叉分析、比對，預防恐怖攻擊；(5)建制「假想敵」(Red Team)單位。[53]然2007年所出版的「美國國土安全國家戰略報告」亦是在前述資料的基礎上，將當前美國內、外部環境威脅及容易遭恐怖分子入侵、利用與攻擊部分提出更為深入的研究，並以「網路安全」為其中探討重點方向，強調恐怖分子利用「網路」成為犯案工具已是不爭的事實，一旦恐怖分子利用網路攻擊我關鍵基礎設施、政府財政或科技部門等，都將造成國家安全重大危機。[54]因此，我國在整合反恐資訊及完善通報機制時，行政院「國土安全辦公室」須在既有的反恐行動基礎上，採取不同的思維與作法，除整合跨部會合作機制外，在組建反恐打擊力量方面必須參考國外一流反恐部隊的訓練與訓場的建置，並針對恐怖活動可能發生的處所，如機場、火車、捷運、高鐵、巴士、船舶等人群聚集環境，加強巡邏密度及建立通報與危機處理機制。

結　　論

對國際社會而言，今日的恐怖攻擊模式，已非昔日傳統式恐怖攻擊。恐怖組織在有限的資源下，為成功躲避國際反恐聯盟的追緝，勢必化整為零，從實體化的運作，逐漸轉換成以網路交流平台為主要傳遞媒介的作戰方式。因此，當各國對於恐怖攻擊提高警戒的狀態下，「網路」乃成為恐怖組織最有利、最廉價且最有效的作戰工具。對於當前國際社會而言，要有效防範、掌握與打擊恐怖主義，在網路安全的維護、管理與治理層面，必須從研擬自動化、快速化、精準化的網頁資訊搜尋引擎與比對處理技術等，才能在資訊化的時代中，成功偵獲恐怖活動動向，確保國家安全不受威脅。

參考文獻

中文部分

書籍

52 邱吉鶴，〈獨狼式恐怖主義興起與因應策略之探討〉，《健行學報》，第35卷第2期，2015年4月，頁93。
53 U.S. Department of Homeland Security, "National Strategy for Homeland Security", July, 2002, pp27-31.
54 U.S. Department of Homeland Security, "National Strategy for Homeland Security", October, 2007, pp28.

一、邱伯浩，2006/11。《恐怖主義與反恐》(臺北：新文京開發)，頁3。
二、Gabriel Weimann著，馬浩翔譯，2018/10。《新一代恐怖大軍：網路戰場》(台北：中華民國國防部)，頁40-65。

期刊論文

一、楊永明，2006/4。〈聯合國反恐策略與人權保障問題〉，《月旦法學雜誌》(臺北)，第131期，頁21。
二、林泰和，2008/6。〈國際恐怖主義研究-結構、策略、工具、資金〉，《問題與研究》(臺北)，第47卷第2期，頁134-135。
三、林正義，2002 /1。〈美國因應911 事件的危機處理〉，《戰略與國際研究季刊》，第4 卷第1 期，頁109。
四、吳東野，2003/1。〈全球反恐聯盟及其相關問題之探討〉，《遠景季刊》，第4卷第1期，頁11。
五、劉承宗，2012/2。〈聯合國反恐委員會十年的回顧與展望〉，《嶺東通識教育研究學刊》，第4卷第2期，頁158-161。
六、林泰和，2016/12。〈近期歐洲恐怖主義發展之研析〉，《問題與研究》，第55卷，頁118。
七、林泰和，2008/6。〈國際恐怖主義研究-結構、策略、工具、資金〉，《問題與研究》，第47卷第2期，頁123-136。
八、鄒文豐，2017/12。〈新興恐怖主義的挑戰與因應對策：社會建構論的觀點〉，《復興崗學報》，第111期，頁7。
九、張雅君，2005/3。〈中共反恐外交的實踐與成效之分析〉，《中國大陸研究》，第48卷第1期，頁67。
十、邱吉鶴，2015/4。〈獨狼式恐怖主義興起與因應策略之探討〉，《健行學報》，第35卷第2期，頁93。

研討會論文

一、張福昌，2013/11/19。〈孤狼恐怖主義與內部安全〉，發表於「第九屆恐怖主義與國家安全」學術研討會。桃園：中央警察大學，頁18。
二、王高成，2005/12/29。〈恐怖主義對當前國際關係的影響〉，發表於「第一屆恐怖主義與國家安全」學術研討會。桃園：中央警察大學，頁17-19。
三、王朝煌，2006/12/28。〈網際網路恐怖活動資訊搜尋技術之探討〉，發表於「第二屆恐怖主義與國家安全」論文集。桃園：中央警察大學，第113頁。

網際網路

一、賴昭穎，2015/11/24。〈亞太反恐同盟歐巴馬提到台灣〉，《聯合新聞網》，<http://udn.com/news/story/8988/1333731>。
二、常青、東海，2017/2/16。〈歐洲大多數人拒絕穆斯林新移民〉，《希望之聲》，<http://www.soundofhope.org/gb/2017/02/16/n740465.html>。
三、2016/3/23。〈歐洲近年為何被IS盯上？六大原因：根本是自惹的〉，《中時電子報》，<http://hottopic.chinatimes.com/20160323003457-260803>。

四、李昱德，2016/2/13。〈恐攻＋難民潮後 歐洲現在怎麼了？〉，《台灣英文新聞》，< https://www.taiwannews.com.tw/ch/news/2880832>。

五、周勇進，2013/5/6。〈「一個人的軍隊」：「獨狼」緣何兇猛〉，《北京新浪網》http://news.sina.com.tw/article/20130506/9530260.html。

六、朱鋒，2002/9/18。〈911和中美關係〉，《BBC中文網》，<http://news.bbc.co.uk/hi/chinese/china_news/newsid_2266000/22662262.stm>。

七、徐海濱，2006/7/31。〈中美簽署加強執法合作聲明 將交流反恐情報資訊〉，《國際線上》，http://big5.chinabroadcast.cn/gate/big5/gb.cri.cn/8606/2006/07/31/1062@1153680.htm。

八、法務部，2005/11/27。「法務部研擬完成反恐怖行動法草案」，發表於中華民國法務部：https://www.moj.gov.tw/cp-21-49487-f3feb-001.html。

九、中華人民共和國國家信息網辦公室，2018/2/2。「習近平的網路安全觀」，http://www.cac.gov.cn/2018-02/02/c_1122358894.htm。

十、中華民國大陸委員會，2017/6/4。「有關中國大陸實施「網絡安全法」相關新聞參考資料」， https://www.mac.gov.tw/News_Content.aspx?n=A0A73CF7630B1B26&s=C69752E507927000 。

外文部分

書籍

一、Stuart Biegel, 2002 /spring "BEYOND OUR CONTROL? CONFRONTING THE LIMITS OF OUR LEGAL SYSTEM IN THE AGE OF CYBERSPACE," Harvard Journal of Law & Technology, Volume 15, Number 2, p544.

政府文件

一、Institute for Economics and Peace,"Global Terrorism Index 2017：Measuring and Understanding the Impact of Terrorism," p71.

二、Brian Michael Jenkins, 2011/12. "Is Al Qaeda's Internet Strategy Working? ", pp1-2.

三、U.S. Department of Homeland Security, 2002/7,"National Strategy for Homeland Security", pp27-31.

四、U.S. Department of Homeland Security, 2007/10,"National Strategy for Homeland Security", pp28.

網際網路

一、Oxford English Dictionary, https://en.oxforddictionaries.com/definition/cyberterrorism.

二、Cambridge Dictionary, https://dictionary.cambridge.org/zht/%E8%A9%9E%E5%85%B8/%E8%8B%B1%E8%AA%9E/cyberterrorism.

三、U.S. Federal Bureau of Investigation, https://searchsecurity.techtarget.com/definition/cyberterrorism.

四、NATO Review Magazine, https://www.nato.int/docu/review/2011/11-september/cyber-threads/en/index.htm

五、Ronald L. Dick,"Testimony", 2002/6.< https://archives.fbi.gov/archives/news/testimony/cyber-terrorism-and-critical-infrastructure-protection>.

六、Dorothy Denning, 2017/2. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy" 2001< http://www.mtholyoke.edu/~lwpoole/politics116/cyberterrorism.html>.

七、Keiran Hardy,"Is Cyberterrorism a Threat?", < https://www.internationalaffairs.org.au/australianoutlook/is-cyberterrorism-a-threat/>.

八、2017/5."Biggest ransomware outbreak in history' hits nearly 100 countries with data held for ransom", < https://www.abc.net.au/news/2017-05-13/biggest-ransomware-outbreak-in-history-hits-nearly-100-nations/8523102>.

九、Robert D McFadden,"Army Doctor Held in Ft. Hood Rampage," New York Times, November 5 2009,http://www.nytimes.com/2009/11/06/us/06forthood.html.

作者簡介

王鵬程上校，陸軍官校85年班，美國陸軍指參學院2010年班，國立中正大學戰略研究所碩士，國防大學戰爭學院103班。曾任連長、營長、陸院教官，現任戰爭學院學員隊長。

E-2K預警機(照片提供：張洲豪)