熱點聚焦

恐怖主義與網路安全

持續演變的威脅形式

Terrorism and Cybersecurity: a Critical Assessment of Threats via Cyberspace

姚宏旻

國防大學戰略研究所

壹、前言：全球化下的恐怖主義

2001年9月11日發生了包含對紐約雙子星大樓及五角大廈等多起恐怖攻擊，開啟了以美國為首的反恐戰爭（War on Terror）。然而在伊拉克海珊（Saddam Hussein）政權垮台後，這場仰賴西方國家中心（state-centric）途徑，來打擊恐怖主義能動性的戰爭，其效果似乎有限；全球恐怖主義非但沒有達到如同小布希總統於2003年所稱的「Mission Accomplished」，而遭到有效的削弱與抑制，其後隨著阿富汗塔利班（Taliban）政權的消逝，吾人反而見識到恐怖主義的全球擴散及轉移。也因此，倫敦政經學院Mary Kaldor教授曾直言，反恐戰爭的邏輯與冷戰（Cold War）作戰思維類似，都是屬於仰賴船堅砲利的舊形式戰爭（Old War），它忽略恐怖主義的衝突形式事實是一種新型式的戰爭（New War），並需要考量全球化的現實（the realities of the globalized world）與消失中的國家統合能力（the disintegration

of states）。[1]

雖然「全球化」在不同脈絡下指涉不同概念，惟許多學者紛紛將重點聚焦於瞭解全球傳播科技與恐怖主義的互動，而這其中，網路空間（cyberspace）便扮演著舉足輕重的角色。時序來到 2019 年 3 月，當美國總統川普宣稱伊斯蘭國（Islamic State, IS）於敘利亞建立的「哈里發」已遭到「百分之百」（100 percent of the "caliphate"）摧毀之際，[2]我們似乎忽略了全球各地區仍充斥著不同形式的恐怖主義活動；這當然也包含同月 15 日於基督城清真寺發生的白人至上恐怖攻擊。因此，在「9.11 襲擊事件」已逾 17 年的此時，本文將審慎檢視與回顧恐怖主義與網路空間的相互影響，以降低重蹈過去「Mission Accomplished」的錯誤認知。

貳、恐怖主義、網路空間與安全

首先，恐怖主義（Terrorism）一詞最早源自於十八世紀法國大革命初期，雅各賓黨（Jacobin Club）利用暴力及暗殺等手段形成的恐怖統治，也因此恐怖主義目的在於運用恐嚇及散佈恐懼與破壞。而近年來隨著網路科技受人重視，網路恐怖主義（Cyber terrorism）一詞也大為流行，其中最早以 Dorothy E. Dennig 在 2005 年於美國眾議院軍事委員會的恐怖主義特別監督小組（Special Oversight Panel on Terrorism, Committee on Armed Services）所提出「恐怖主義與網路空間的聚合」（convergence of terrorism and cyberspace）最為周知。惟

[1] Kaldor, Mary. "Old wars, Cold wars, New wars, and the War on Terror." *International Politics*, 42:4(2005), pp.491-498.

[2] Faulders, Katherine, "Trump claims '100 percent' of ISIS caliphate defeated in Syria," *ABC News*, 1 March 2019; https://abcnews.go.com/Politics/trump-claims-100-percent-isis-caliphate-defeated-syria/story?id=61388529

國際間就「網路恐怖主義」定義迄今仍莫衷一是，[3]因此本文將避免就網路恐怖主義一詞定義，而改著重於瞭解恐怖份子如何利用網路空間來製造恐懼氛圍、組織攻擊行動與遂行惡意破壞。

本文所指網路空間並不僅侷限於社群媒體或是網際網路，而是泛指資通科技（Information and communication technology, ICT）所構建的資訊網路，它源起於十九世紀的電報網路（亦被稱為 Victoria Internet），[4]成熟於廿世紀美國高等研究計劃署網路（ARPANET），全球涵蓋範圍更隨著廿一世紀移動通訊技術（Mobile Technology）與時俱進。因此，當前網路空間已成為低成本、跨國境、無限閱眾、全域全時及相對匿名的基礎建設。它的影響力橫跨技術及認知兩種場域，而這樣的傳播管道，也受到恐怖主義的關注，衝擊我們所期望的「安全」（Security）概念。

國際安全研究學者 Barry Buzan 曾說：「安全，是一個爭辯中的概念（an essentially contested concept）」。我們很難就「安全」的概念達成一致共識，每一個國家所處的安全環境不同，也因此所面臨的威脅便不同；而每個人所選用的定義則僅反映出其所重視的利益及價值。Arnold Wolfers 也曾將安全解析為客觀及主觀成分，「客觀的安全」來自缺乏「物質威脅」，「主觀安全」來自於缺乏「恐懼」（本文將之視為「非物質威脅」ideational threat）。也因此，雖然我們很難就安全達成共識，但學界至少可以同意，安全的目的在於避免「威脅」（threat），也因此以下將探討恐怖主義透過「網路空間」的「威脅」，分就兩方面回顧。

[3] T. Chen, Lee Jarvis, and Stuart Macdonald. *Cyberterrorism* (Heidelberg: Springer, 2014), p.198.
[4] T. Standage, *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-line Pioneers* (New York: Walker & Co, 2007).

參、恐怖主義的威脅與社群媒體

首先，恐怖組織利用網路空間中的社交功能（社群媒體），來營造恐怖氛圍，建構「非物質威脅」，或蒐集資源支持恐怖攻擊行徑以強化「物質威脅」；常見手法有宣傳恐怖、資金募集、人員訓練、計劃與執行。在宣傳恐怖部分，恐怖組織常透過多媒體影片或文字記錄的製作，利用各國對網路「言論自由」定義的模糊地帶，來宣揚理念以煽動孤狼式攻擊（lone wolf attack）、激進化（radicalize）更多的認同者、或進一步達到招募支持者的目的；如 2017 年 11 月紐約貨車衝撞致死恐攻事件、過去《紐約時報》大幅報導伊斯蘭國製作的網路視頻往往流露出濃濃的英國腔、以及近期各國討論如何安置敘利亞境內所俘虜來自歐洲各國聖戰士（Jihadist）之去留，都顯示網路宣傳的效果。在資金募集部分，恐怖組織則透過線上系統發起群眾募資，或以線上慈善機構名義販賣商品募集資金，這些資金可以透過傳統第三方支付系統（如 PayPal），或區塊鏈加密貨幣（如比特幣）執行跨國匯兌；例如，過去受聯合國禁止與蓋達組織相關的仁愛國際基金會（Benevolence International Foundation），以及與巴基斯坦境內恐怖組織虔誠軍（Lashkar-e-Taiba）關係密切的達瓦慈善會（Jamaat-ud-Dawa, JuD）等案例。[5]

在人員訓練部分，越來越多的恐怖組織利用網路空間提供周延的多媒體環境執行訓練，利用網路平台易於存取且提供多種語言服務，恐怖組織分享知識說明如何加入攻擊活動、組裝爆裂物並掩飾攻擊意圖；如 2016 年歐洲各國遭到多起孤狼攻擊事件時，網路出現一本名為《孤狼聖戰士安全指南》（*Safety and Security Guidelines for*

[5] 請見 http://www.jamatuddawa.org/ ;另 Dawa 一詞意旨「感召」及「崇拜」，恐怖主義將其視為動員民間力量支持其行動之代名詞。較知名為中東真主黨（Hamas）內部的達瓦部門（Dawa Infrastructure），旨在結合清真寺、學校及醫院等單位。

Lone Wolf Mujahideen）的活動教戰手冊，教導攻擊者如何有效掩飾意圖。在計劃執行方面，網路空間最早建置目的就是通訊，隨著通訊加密技術進步，傳統用於協助在極權政府境內人民隱匿通聯訊息的洋蔥路由器（the onion router）也受到恐怖份子運用於暗網（Dark Web）內活動；[6]此外，政府組織或公眾人物常公開眾多訊息作為與公眾交往的基礎，惟這些網路或社交媒體訊息也成為恐怖組織計劃行動的公開資料情報（Open-Source Intelligence, OSINT），特別是許多針對攻擊目標的後勤訊息也可以透過網路掌握，例如即時路況影片、利用 Google Earth 規劃逃亡路線及掌握設施周邊地形地物等。

綜上所述，社群媒體具有跨國界、隱蔽、互動靈活且成本低廉的特性，也因此恐怖主義可輕易掌握這些優勢，並視網路空間為「工具」傳播與創造恐懼。然而，隨著資通科技透到我們生活的每一個日常，新的威脅形式也隨之產生，特別是二十一世紀受大眾過度仰賴的網路空間，現在也因而成為恐怖主義攻擊的「目標」，這其中又以網路空間中的民生及國家重要資產最受學者關注–關鍵基礎設施之安全。

肆、恐怖主義的威脅與關鍵基礎設施

事實上，早在「9.11 襲擊事件」之前，恐怖份子破壞關鍵基礎設施的可能性，便受到歐美政府部門普遍關注。最著名事件乃是在 1993 年紐約世貿中心停車場爆炸案及 1995 年奧克拉荷馬爆炸案後，柯林頓政府首先以「第 13010 行政命令」於 1996 年建立關鍵基礎設施總統研析小組（President Commission of Critical Infrastructure

[6] Gabriel Weimann, “Terrorist Migration to the Dark Web,” *Perspectives on Terrorism*, 10:3(2016), pp.40-44.

Protection），該小組結果報告後續於 1998 年產生第 62 及 63 號總統決策指導（Presidential Decision Directive, PDD），PDD-62 乃美國首次於官方文件指出「網路恐怖主義」（Cyber terrorism）威脅，而 PDD-63 則同時指出威脅的目標是關鍵基礎設施。美國政府於 1998 年成立國家基礎建設防護中心（National Infrastructure Protection Center），並於 2003 年配合小布希政府於「9.11 襲擊事件」後之政府組織再造作業，併入後續成立之國土安全部（DHS）。

即便政府單位很早便構思關鍵基礎設施遭到恐怖主義網路攻擊問題，但因網路空間之可匿名（Plausible Deniability）特性，造成難以辨識出真正攻擊源頭，也因此對網路安全研究產生「認識論上的侷限」。例如當發生電腦緊急事件時，社會大眾很難瞭解事件本質是肇因於意外、人為錯誤或惡意攻擊，甚至當確認為惡意攻擊時，政府機關也難以辯證攻擊來源是否出自犯罪團體、敵國或者是恐怖組織。特別是自 1998 年起，未曾有明確證據指出關鍵基礎設施遭惡意份子網路襲擊，因此部份學者認為恐怖主義份子攻擊關鍵基礎設施乃部份政府官員、媒體及學者的「語言行動」（Speech Act），[7]並建構出「恐懼」的概念影響「主觀的安全」，而此處的「恐懼」便是「話語建構」的成果，亦或可稱為「網路恐怖主義的社會建構」。

然而，2010 年資安人員於伊朗納坦茲（Natanz）核武設施發現的震網（Stuxnet）蠕蟲，一改學者過去對於網路攻擊是否能影響「客觀的安全」的質疑。震網病毒跳脫傳統電腦病毒於純粹網路空間之拘束，能實際遞送實體破壞威力於電腦裝備上，這樣的特性為恐怖

[7] 例如 Myriam Dunn Cavelty 依據英國分析語言學家 John Austin 的語言行動理論，論證美國恐怖主義網路的威脅根源來自語言。See Myriam Dunn Cavelty, "Cyber-terror: Looming Threat or Phantom Menace? The Framing of the US Cyber-threat Debate," *Journal of Information Technology & Politics*, 4:1(2008), pp.19-36.

份子提供一有效利基點，只要改裝震網病毒內部份程式碼，恐怖份子將能迅速生產威力強大之病毒；曾經為震網執行數位鑑識的德國資安專家 Ralph Langner 便為未來數位武器（digital weapon）之任意擴散提出警告。果不其然，資安人員分別於 2011 及 2012 年發現與震網具類似程式碼之電腦病毒 Flame 及 Gauss，在 2015 年更發生了 BlackEnergy 蠕蟲造成烏克蘭大停電;隨後的 WannaCry 勒索軟體肆虐 150 多個國家，攻擊英國醫院健保系統，其後之變種版更於 2018 年感染台積電生產裝備，廠房停擺並損失數十億元。

可以確信的是，這種網路恐怖攻擊的概念已經受到恐怖組織的注意。2011 年蓋達組織變發佈宣傳影片，鼓勵支持者發動「網路聖戰」，[8]以便對西方國家關鍵基礎建設發起類似「9.11」規模的網路攻擊。2015 年 4 月，FBI 網路犯罪應變中心（Internet Crime Compliant Center, IC3）發佈警告，宣導反制 ISIS 支持者利用網站內容管理軟體 WordPress 系統漏洞破壞網站顯示。[9]同年 3、5 及 8 月，伊斯蘭國駭客部門（Islamic State Hacking Division）成功入侵美國政府網站，並公佈所竊取之政府官員個資，鼓勵支持者向這些人員發起孤狼式攻擊。[10]恐怖份子就網路攻擊投注之關愛眼神是值得讓人憂心的，誠如前 FBI 局長柯米（James Brien Comey）所說：「能產生實體破壞的惡意程式就像炸彈一樣，而恐怖份子總是想辦法獲得炸彈」。

[8] Al-Shabab, Electronic Jihad Video, 2011, www.hsgac.senate.gov/download/?id=483eca14-3c0e-4a30-9038-f4bf4a1fad60.
[9] https://www.ic3.gov/media/2015/150407-1.aspx
[10] S. Stalinsky and R. Sosnow, “Hacking In The Name of The Islamic State (ISIS)”, MEMRI, 21 August, 2015, http://www.memrijttm.org/hacking-in-the-name-of-the-islamic-state-isis.html

伍、大規模殺傷性武器或大規模擾亂性武器

就科技決定論者（Technology Determinism）觀點而言，新科技的誕生必然對傳統遂行作戰之作業方式產生衝擊。隨著可程式控制器（Programmable Logic Controllers, PLCs），以及資料採集與監控系統（Supervisory Control and Data Acquisition, SCADA）於關鍵基礎設施的成熟商業應用，物聯網及人工智慧技術的逐漸興起與普及，未來網路世界與實體世界將越來越密不可分；惟水能載舟、亦能覆舟，當二十一世紀的資訊社會越倚賴資訊科技所帶來之便利，我們就愈易受制於來自網路空間的威脅。

然而，我們無須過度悲觀並消極解讀此一發展趨勢，並誇大或渲染恐怖份子於網路空間的活動，忘卻傳統恐怖攻擊的危害。正如同電視的發明並未取代收音機、飛機的發展並未使汽車消失；對新形態的威脅評估，須包含對恐怖份子動機、能力與網路系統漏洞的整體考量，也因此往往充滿挑戰，但唯一可以確定的是：這樣的科技技術將成為恐怖份子新的機會與攻擊選項。

職是之故，假如世界各國持續研發網路戰爭技術並進行軍備賽，政府不積極打擊網路犯罪致使惡意程式橫行，學界及業界不亟思修補網路空間設計遺留許多安全漏洞，恐怖主義或許受限於當前人力、物力及財力，而無法獨力發展客製化的病毒軟體，但將可輕易複製已知的攻擊手法、改裝隨手可得的惡意軟體，肆意穿透無所不見的系統漏洞；常此發展下，網路空間或許不見得能成為恐怖份子另一種大規模殺傷性武器，但當政府、學界、科技業等各方關係人，未能積極參與重塑對這些科技手段的社會建構過程時，網路空間將是繼傳統炸彈、簡易爆裂物（Improvised Explosive Device, IED）選項外的另一種大規模擾亂性武器。

陸、結論

許多恐怖份子與組織正積極運用網路空間，來達到其戰術、作戰及戰略層級目標。這也顯示透過網路空間所轉化的權力不僅受到國家，也受到非國家武裝組織的重視。然而政府在不斷擔憂來自網路空間的恐怖主義威脅同時，也應反思其在強化網路戰爭的攻擊能量，做法是否合宜?畢竟各國政府對網路空間行為言行不一致的結果，短期除將造成國際社會難以對可允許之網路行為達成國際共識，長期亦將造成恐怖份子毫無阻礙的利用與開發各國所廣泛散布的惡意程式與攻擊手法。或許，正如同 Nicholas Onuf 在所著 *World of Our Making* 中的論點一般，網路世界也是「我們創造的世界」；在我們習於面對當前網路空間充斥的各種威脅形式後，似乎逐漸忘記網路空間曾被稱為一個兼容並蓄的全球公域（Global Commons），而非一個問題叢生且飽受威脅，被視為理所當然的作戰空間。[11]

總而言之，在簡短檢視恐怖主義與網路空間如何影響所謂「安全」並重塑「威脅」後，本文雖認可就網路恐怖主義的恐懼（非物質威脅），部份源自「網路恐怖主義的社會建構」（Social Construction of Cyberterrorism）而影響「主觀的安全」，仍然剴切呼籲降低實體威脅（物質威脅）的對策，可以仰賴「網路空間的社會建構」（Social Construction of Cyberspace），以降低衝擊我們「客觀的安全」

[11] Hon-Min Yau, “Explaining Taiwan’s Cybersecurity Policy Prior to 2016: Effects of Norms and Identities,” *Issues & Studies*, 54:2(2018), 1850004.