全球政治評論　*Review of Global Politics*

第七十九期（2022）No.79 頁 69-89

學術論文

網路恐怖主義在中國：威脅、應對與影響

Cyber Terrorism in China: Threats, Responses and Impacts

張凱銘 *Kai-Ming Chang*
國立臺中科技大學通識教育中心助理教授
Assistant Professor of Center for General Education
National Taichung University of Science and Technology

劉泰廷 *Tai-Ting Liu*
國立中興大學通識教育中心助理教授
Assistant Professor of General Education Center
National Chung Hsing University

摘要 / Abstract

本文試圖對中國當前面臨的網路恐怖主義威脅進行概要評估，探討中國面臨的網路恐怖主義威脅、政府近年的反恐努力，以及相關反恐工作可能造成的複雜影響。研究結果顯示中國面臨的網路恐怖威脅與其邊境地區的分離主義運動相關，且中國政府已採取行動積極因應，例如加強網路審查、擴大立法規範與推進和鄰近國家及國際組織間的反恐合作等。然而中國政府的相關努力除為回應恐怖主義威脅，似乎也有利用反恐名義擴大管制國民網路自由，並主導網際網路國際治理進程的考量。

This article aims to explore China's Anti-cyberterrorism policy by analyzing the types of threats it faces today, the government's response, and the

possible impact of related actions. The research shows that the cyber-terrorism problem in China is mainly caused by the separatist activities in its border areas, and the Chinese government has taken actions to respond, such as strengthening cyber censorship, formulating relevant laws, and cooperating with neighboring countries and international organizations. However, China's relevant actions seem not only to respond to the threat of cyberterrorism but also to take the opportunity to expand monitoring of people's online activities and to dominate the international Internet governance process.

關鍵詞：網路恐怖主義、網路反恐、國際網路政治、中國網路政策、網路主權

Keywords: Cyberterrorism, Anti-cyberterrorism, International Cyber Politics, China's Cyber Policy, Cyber Sovereignty

壹、前言

網路科技自 1990 年代起迅速發展，逐漸成為當代人類文明中不可或缺的重要成分。綜觀當前世界，各國政經體系、社會運作與民眾日常生活，都和網路服務密切相關。隨著人類對網路科技依賴程度持續提高，資安防護不再僅是傳統意義上的技術事項，而是具高度戰略價值的核心議題。對各國政府而言，如何在善用網路科技促進國家發展的同時，有效防護網路系統安全無虞，已成為國安層級的重要工作。

現代國家在網路空間中面臨的安全威脅，較為外界熟悉者應屬駭客與敵對國家發起的惡意網路攻擊，諸如滲透網路系統竊取情資、癱瘓網路系統引發實體混亂等。過往十數年間，包含愛沙尼亞、喬治亞、韓國、英國、美國在內的許多國家都曾遭遇大規模網路攻擊，各國政府在這一背景下也紛紛強化資安體系並發展網路軍事部隊。

然而，除了來自駭客及其他國家的威脅外，網路科技與恐怖主義的結合，也是漸獲外界重視的新興安全挑戰。恐怖主義在人類文明中歷史悠久，進入二十一世紀後更因天主教文明與伊斯蘭文明間矛盾升級、地緣政治情勢複雜化等因素而更趨多發危險，世界上多數國家都曾遭遇恐怖威脅，其中部分恐怖攻擊如九一一事件等更對國際關係造成深遠影響。考慮到現代國家及民眾生活對網路科技的依賴，恐怖組織若成功對網路系統發起攻擊，不但將造成巨大經濟損失與社會動盪，也可能導致嚴重生命傷亡。另一方面，即便沒有發起網路恐攻行動，網路科技的便利性也可為恐怖組織的集團運作、技術學習、資源募集及理念傳播創造顯著效益。部分學者注意到，許多新興恐怖組織已嫻熟於應用推特(Twitter)等網路社交媒體，藉其出色的人際連結和傳播效果助長組織發展。[1]

近年來，許多國家對於恐怖主義陰影滲入網路空間的趨勢深有警覺，

[1] J. M. Berger and Jonathon Morgan, *The ISIS Twitter Census* (Washington, D.C.: The Brookings Institution, 2015), pp. 9-14.

自部門編制、法規制定與技術開發等面向採取因應作為。其中，擁有當前世界上最大網路用戶群體的中國，對於網路反恐的態度尤為積極。中國的反恐工作重心長期聚焦於邊境地區分離運動，其中部分為其界定為恐怖團體的組織，近年透過網路途徑募集人物力資源，同時傳播激進民族及宗教思想、分享發動恐怖攻擊所需的武器知識等，相關現象使中國政府深為警覺，進而採取行動加以因應。本文以中國的網路反恐政策為研究主題，下文首先將釐清網路恐怖主義的定義、構成要素及危害形式，其次探討中國面臨的網路恐怖威脅態樣、相關威脅的成因及可能危害。再次則分由國內與國際層次彙整中國政府近年採取的具體網路反恐措施。最後，本文將就中國網路反恐成效及相關政策可能衍生的影響進行綜合評估，並在此基礎上前瞻其施政前景。

貳、網路恐怖主義的概念界定與構成要素

網路恐怖主義這一概念的初始界定，可回溯至美國智庫「安全與情報研究所」(Institute for Security and Intelligence)資深研究員柯林(Barry C. Collin)於 1996 年犯罪與司法議題國際座談會(Proceedings of the 11th Annual International Symposium on Criminal Justice Issues)中發表的專文〈網路恐怖主義的未來：位在物理世界與虛擬世界的交會處〉(The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge)。柯林在文中指出，恐怖主義未來很可能不再透過炸藥、毒氣等傳統手段發動攻擊，而改以科技手段集中打擊網路系統，鑑於現代人類文明對網路技術倚賴廣泛深厚，不論是交通設施、醫療儀器、軍事裝備、通訊系統，以及藥品、能源、糧食的製造生產流程皆大量採用網路服務，恐怖份子將積極探索發動網路攻擊的可能，期望藉此創造嚴重的生命財產損害，導致大眾陷入恐

慌情緒之中。[2]

柯林對於網路恐怖主義的表現形態與可能危害的具體描繪，促使美國政府及戰略安全學界對此一議題賦予更多重視，許多研究者陸續提出有關網路恐怖主義的概念界定。例如曾為聯邦調查局(Federal Bureau of Investigation, FBI)資深官員的中佛羅里達大學(University of Central Florida)教授波利特(Mark M. Pollitt)將其界定為「次國家組織或隱蔽行動者，針對資訊系統、電腦設備、程式及數據資料發起的具預謀及政治動機的攻擊行動，其目標多為非戰鬥人員。」[3] 喬治城大學(Georgetown University)教授丹寧(Dorothy E. Denning)認為網路恐怖主義意指「出於宗教或意識形態目的而向電腦系統發起的攻擊和攻擊威脅。這類行動因具備相當破壞性，諸如導致人命傷亡、交通癱瘓、電力中斷、水源污染或重大經濟損失等，進而引發與傳統恐怖攻擊相類的恐懼效應。」[4] 馬里蘭大學全球分校(University of Maryland Global Campus)教授威爾遜(Clay Wilson)則主張網路恐怖主義是「具政治動機的國際組織、次國家組織或隱蔽行動者以電腦系統作為武器或目標，藉由發動或威脅發動暴力攻擊以製造恐懼，期望藉此影響民眾或改變國家政策。」[5]

除西方學界的討論外，中國政府與學者也十分關注網路恐怖主義的危害並嘗試對其做出定義。例如學者范明強在《社會學視野中的恐怖主義》一書中指出，網路恐怖主義的定義應涵蓋兩個層面，第一是指恐怖份子將

---

[2] Barry Collin, “The Future of Cyber Terrorism,” *Proceedings of the 11th Annual International Symposium on Criminal Justice Issues*, The University of Illinois at Chicago, 1996, https://www.crime-research.org/library/Cyberter.htm.

[3] Mark M. Pollitt, “Cyberterrorism — Fact or Fancy?” *Computer Fraud & Security*, No. 2 (February 1998), pp. 8-10.

[4] Dorothy E. Denning, “Is Cyber Terror Next?” *Social Science Research Council*, November 1, 2001, http://essays.ssrc.org/sept11/essays/denning_text_only.htm.

[5] Clay Wilson, “Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress,” *Congressional Research Service Report*, October 17, 2003, https://nsarchive.gwu.edu/document/22181-document-04.

網路科技作為發動攻擊的技術工具，第二是指恐怖份子將網路空間做為攻擊行動的目標，譬如打擊網路系統、散播線上謠言製造恐慌，或推廣激進理念等。[6] 中國公安部反恐怖局於 2008 年編製發表的《公民防範恐怖襲擊手冊》提到，網路恐怖襲擊活動是指「利用網絡散布恐怖信息、組織恐怖活動、攻擊電腦程序和信息系統等。」[7]朱永彪與任彥兩位學者則在《國際網絡恐怖主義研究》一書中，提出較細緻的定義，指出網路恐怖主義在基本意義上，是網路科技和恐怖主義的結合，但根據運作形式不同，又可概要劃分為「工具型網路恐怖主義」和「目標型網路恐怖主義」兩類，前者意指運用網路科技支持恐怖主義事業發展，後者則指將網路作為攻擊目標或攻擊工具的恐怖活動。[8]

觀察各方研究者對網路恐怖主義的界定，可發現其中雖不乏差異處，但不同觀點間仍有明顯交會。透過概要歸納，吾人可將網路恐怖主義的基礎定義總結為：「網路恐怖主義意指各種型態的恐怖主義勢力，受到政治、宗教或其他動機驅使，運用網路科技發起數位或實體攻擊行動，以及利用網路技術服務恐怖主義事業發展，進以對國家政策和公共事務發揮影響的情況。」以此為基礎，又可進一步劃分網路恐怖主義的四項核心構成要素：

- 行為主體：網路恐怖主義作為傳統恐怖主義在資訊時代的變體，其行為主體與學界過往對恐怖主義活動的認知相仿，同樣涵蓋了國家、非國家組織以及個人等多元型態。
- 行為動機：網路恐怖主義既為恐怖主義的分支，發起者應持有政治、宗教等方面的動機，希望透過對網路技術的操作產生破壞效應，或是拓展其恐怖事業經營，從而在社會中創造恐怖氛圍，對政府治理或公共事

[6] 范明強，《社會學視野中的恐怖主義》（北京：解放軍出版社，2005 年），頁 67。
[7] 〈公民防範恐怖襲擊手冊〉，《中國政府網》，2008 年 7 月，http://www.gov.cn.qingcdn.com/fwxx/content_1051949_4.htm。
[8] 朱永彪、任彥，《國際網絡恐怖主義研究》（北京：中國社會科學出版社，2014 年），頁 19。

務造成影響。

- 行為手段：不同於傳統恐怖主義側重應用軍火武器或交通工具作為攻擊工具，網路恐怖主義的主要特徵在於高度依賴網路科技，例如由網路途徑入侵特定電腦系統發動攻擊，或是應用特定網路服務對外散播資訊等。
- 行為表現：網路恐怖主義的表現十分多元，常見者包括三種類型：第一是「具體破壞行動」，例如癱瘓電腦系統、損毀數位資料或透過網路連結攻擊實體設施等；第二是「虛擬破壞行動」，例如透過網路空間散播謠言引發社會混亂，此類行動可與傳統的實體恐怖攻擊相結合以創造更嚴重的恐慌效應；第三是「應用數位服務」，例如透過影音串流平台傳播激進的政治和宗教理念、講授恐攻武器使用方式、唆使民眾參與恐怖主義活動，或是透過社群媒體整合組織運作、聯繫招募成員，以及對外募集金錢及物質資源等。

參、中國面臨的網路恐怖主義威脅

作為當前國際社會的主要行為體之一，中國雖不若美國一般因深度介入中東地緣政治而面臨嚴峻的恐怖威脅問題，但恐怖主義帶來的安全危害同樣是中國政府長期關注的國安挑戰之一。回顧近年發生於中國的多起恐怖攻擊事件，主要和境內的少數民族及分離主義(Separatism)運動有關，相關人士參與恐怖活動的動機多與政治層面的民族獨立訴求，或信仰層面的激進宗教理念有關。

在網路科技—尤其是行動通訊網路—大為普及，以及影音串流、社群媒體等多元服務蓬勃發展的背景下，許多中國學者也注意到部分恐怖活動逐漸與網路科技合流，雖然尚未出現造成重大損害的網路攻擊，但恐怖主義勢力似乎越來越積極地應用網路輔助其發展，並為實體恐攻行動提供助

力。若以前節提到的行為表現分類來看，相關活動以「應用數位服務」為主，間或出現部分影響有限的「虛擬破壞行動」。

例如 2014 年 3 月 1 日發生於雲南省昆明火車站，造成 29 人死亡與約 130 人受傷的恐怖攻擊事件，該事件雖在行為表現上屬於持械攻擊的傳統恐攻型態，但慘案發生後即有名為「突厥斯坦伊斯蘭黨」(Turkistan Islamic Party, TIP)的新疆分離主義組織在網路上發表影片，表達對此一攻擊行動的肯定與支持，雖然此事件是否確由該組織策動仍存爭議，但網路影片分享對於後繼相類恐攻行動的產生很可能發揮了激勵效果，[9] 烏魯木齊市火車站於一個月後發生形態相同的恐怖攻擊，導致 3 人死亡與 79 人受傷。[10]

烏魯木齊恐攻事件發生後，中國政府除針對涉案人士展開刑事偵緝外，也擴大追查在網路空間傳播和恐怖主義、激進宗教與民族主義訴求相關影音資料的用戶，時任中國共產黨新疆維吾爾自治區委員會書記張春賢對外表示，這些涉入恐怖主義活動的數位影音資訊和攻擊事件間毫無疑問存在聯繫；部分媒體也在追蹤調查此事件的過程中，注意到「東突厥斯坦伊斯蘭運動」(East Turkestan Islamic Movement, ETIM)等組織，確實會利用網路服務散播包含聖戰(Jihad)思維與槍械使用教學等內容的煽動影片 。[11]

此外，北京清華大學於 2016 年 1 月 17 日遭遇駭客攻擊，除造成學校官方網站短時間癱瘓外，網頁上更被置入「伊斯蘭國」(Islamic State of Iraq and al-Sham, ISIS)旗幟及疑似該組織的宣傳影片（請見圖 1）；由於「伊斯蘭國」於 2015 年時曾宣布中國為敵對國家，對外聲稱處決一位中國籍公民，外界咸認該組織為此次網路攻擊事件的主導者。[12]

---

[9] 夏榕，〈傳一維吾爾伊斯蘭組織視頻表示支持昆明砍人事件〉，《法國國際廣播電台》，2014 年 3 月 18 日，https://reurl.cc/ZAlQx6。

[10] 亓樂義，〈烏魯木齊恐怖爆炸攻擊 3 死 79 傷〉，《風傳媒》，2014 年 5 月 1 日，https://www.storm.mg/article/30617。

[11] 楊眉，〈232 名維族人涉嫌傳播恐怖音視頻被捕〉，《法國國際廣播電台》，2014 年 5 月 12 日，https://reurl.cc/YvkdWL。

[12] Anthony Cuthbertson, “ISIS Hackers Carry Out First Attack on Chinese Target,” January 20, 2016, https://www.newsweek.com/isis-hackers-carry-out-first-attack-chinese-target-417765.

圖 1 2016 年 1 月北京清華大學網路攻擊事件畫面截圖

資料來源：Cathy Wu, “Tsinghua University Website Attacked by 'ISIS Hackers',” *That's*, January 18, 2016, http://www.thatsmags.com/china/post/12116/tsinghua-university-website-attacked-by-isis-hackers.

藉由歸納相關事例的同異特質，部分中國學者對於網路在中國當前面臨的恐怖主義威脅中扮演的角色進行了探討。概要而言，中國當前面臨的網路恐怖問題，在型態上接近於前節提到的「應用數位服務」，即著重使用各種網路服務支持恐怖事業發展，常見態樣包含以下五類：[13]

第一是「宣傳極端思想」，指相關組織團體透過網路科技利於迅速及大量傳播資訊的技術特質，向普羅大眾或特定受眾播送激進宗教與民族主

[13] 舒洪水、黨家玉，〈網絡恐怖主義犯罪現狀及防控對策研究〉，《刑法論叢》，2017 年第 3 期（2017 年 7 月），頁 396-399。

義理念，或是分離主義等政治主張，有助於恐怖勢力擴大群眾基礎、爭取民間支持。

第二是「招募組織成員」，指相關組織團體透過架設網站等途徑對外招募所需人才，或是經由社交媒體網站，篩選出身背景、學識經歷與技術能力等條件符合組織期望的人士，進而主動探詢招募。

第三是「聯繫指揮組織」，指相關組織團體以網路技術為輔助，得以更有效地管理內部系統運作，配合組織發展和任務需求配置人物力資源，以及指揮派遣組織成員發起有計畫的恐怖攻擊。

第四是「煽動攻擊行動」，指相關組織團體利用網路傳媒與應用程式挑唆、號召各地認同其理念的群眾採取自發行動，向政府機關或平民大眾發起孤狼式恐怖攻擊(Lone Wolf Terrorist Attack)。

第五是「募集財務資源」，指相關組織團體經由網路平台對外募集營運所需之財務資源，除各類網路影音與社交平台的發展有利於散播募款資訊外，各類虛擬貨幣的發展普及，也為恐怖主義募款工作提供許多便利與隱密性。

中國學者也注意到，恐怖份子對於網路工具的前述利用，不僅使其事業拓展、活動推行更為順利，亦使中國當前面臨的恐怖威脅，相對於過往而言，展露出幾項明顯特徵：第一是碎片化，便利迅速的網路連結使恐怖活動更為靈活分散，即便缺乏大型組織作為依托，小型團體乃至個人都可發起攻擊行動。第二是年輕化，意指與網路技術應用有關的恐怖組織成員在年齡分布上有日益下降的趨向，原因在於年輕世代既多有接觸網路傳媒的習慣而易於遭受線上恐怖資訊煽動，同時也更具操作網路工具發起前述各項行動的能力。第三是低廉化，指經由網路途徑募集人物力資源、利用網路影音傳遞製作炸彈等專業知識等作法，使恐怖組織培育人力與執行攻擊行動的成本較過往更低廉。第四是激進化，部分學者指出，由於網路資訊通常需具備醒目、新奇與簡單易懂等條件方能快速散播，因此近年透過網路途徑傳遞的涉恐資訊和激進理念，內容上較為空洞虛無，與傳統恐怖

主義宣傳相比，較少具深度的宗教教義或政治論述。[14]

肆、中國政府的網路反恐努力

面對網路恐怖威脅逐漸上升的態勢，中國政府近年已採取多重手段加以因應，以下分就國內社會與國際社會層次說明其具體作為。

一、國內社會層次的網路反恐努力

從國內社會觀察，中國政府近年針對網路恐怖主義威脅採取的因應措施可概括為「加強監管網路資訊」、「制訂法令規章」及「加強公民教育宣導」等三個面向。

在加強監管網路資訊方面，中國透過國家互聯網信息辦公室作為統一指揮的軸心機構，和各地方政府的網路治理部門保持密切交流，要求地方部門務必將網路反恐列為優先工作事項，並於 2014 年後大力推動「網絡暴恐音視頻專項清理行動」，積極掃蕩網路空間中涉及恐怖主義、激進宗教和政治理念，以及製作使用非法武器等內容的影音資訊，力求阻斷恐怖勢力利用網路煽動民眾、傳遞危險思想的路徑。[15] 中國國家互聯網信息辦公室同時制訂了檢舉獎勵措施，鼓勵民眾主動向其舉報網路中涉及「宣揚宗教極端思想」、「教唆實施暴力恐怖襲擊」、「傳授暴恐犯罪技能」、「煽動民族仇恨」、「鼓吹分裂主義」等特徵的影音資訊，若經該機構核查舉報屬實，將根據資訊內容威脅程度，向舉報人發放人民幣一千元至一萬元不等的金錢獎勵。若舉報資訊被認定為具有特殊重大威脅，甚至可能獲得高達十萬元人民幣的檢舉獎金。[16]

---

[14] 杜娟，〈當前我國網絡恐怖主義的特點、原因及對策〉，《雲南警官學院學報》，2016 年第 1 期（2016 年 1 月），頁 39。

[15]〈國家網信辦召開視頻會議部署打擊網絡暴恐音視頻〉，《中國國家互聯網信息辦公室》，2014 年 5 月 28 日，http://www.cac.gov.cn/2014-05/28/c_126557992.htm。

[16]〈關於鼓勵網民舉報暴恐音視頻等違法信息的公告〉，《中國國家互聯網信息辦公室》，

在制訂法令規章方面，中國雖尚未就網路恐怖主義問題制訂專門法典，但近年與恐怖主義、網路安全及國安事務相關的多部法律中，已逐漸增加涉及網路恐怖主義問題的規範。例如 2014 年 9 月時，由中國最高人民法院、最高人民檢察院與公安部聯合發表的《關於辦理暴力恐怖和宗教極端刑事案件適用法律若干問題的意見》中，提到除傳統攻擊行為外，「建立、開辦、經營、管理網站、網頁、論壇、電子郵件、博客、微博、即時通訊工具…或者利用手機、移動存儲介質、電子閱讀器等登載、張貼、複製、發送、播放、演示載有宗教極端、暴力恐怖思想內容的圖書、文稿、圖片、音訊、視頻、音像製品及相關網址，宣揚、散佈、傳播宗教極端、暴力恐怖思想」等行為，都應納入查緝懲處範圍之中。[17] 2015 年 7 月公布的《中華人民共和國國家安全法》，第 25 條關於強化國家網路資訊系統安全保障的規定中，提到政府應「加強...防範、制止和依法懲治網絡攻擊、網絡入侵、網絡竊密、散布違法有害信息等網絡違法犯罪行為…。」[18] 為政府部門處理網路恐怖威脅的各項舉措提供原則性法律授權。

2015 年末通過的《中華人民共和國反恐怖主義法》第 18 條與第 19 條處，規定網路電信業者應配合政府部門查辦網路空間中的恐怖主義訊息，及時「採取技術措施，阻斷傳播」。[19] 2016 年 11 月通過的《中華人民共和國網絡安全法》第 12 條處，明令人民「不得利用網絡從事危害國家安全...宣揚恐怖主義、極端主義、宣揚民族仇恨…等活動。」[20] 此外，中國刑法第 285 條與第 286 條關於入侵網路及電腦系統的犯罪規定，也為警政

2014 年 7 月 10 日，http://www.cac.gov.cn/2014-07/10/c_1111550120.htm。

[17]〈關於辦理暴力恐怖和宗教極端刑事案件適用法律若干問題的意見〉，《中國國家互聯網信息辦公室》，2014 年 9 月 21 日，http://www.cac.gov.cn/2014-09/21/c_1112712390.htm。

[18]〈中華人民共和國國家安全法〉，《人大新聞網》，2015 年 7 月 10 日，http://npc.people.com.cn/BIG5/n/2015/0710/c14576-27285049.html。

[19]〈中華人民共和國反恐怖主義法〉，《中國人大網》，2015 年 12 月 27 日，http://www.npc.gov.cn/zgrdw/npc/xinwen/2018-06/12/content_2055871.htm。

[20]〈中華人民共和國網絡安全法〉，《中國國家互聯網信息辦公室》，2016 年 11 月 7 日，http://www.cac.gov.cn/2016-11/07/c_1119867116.htm。

單位處理相關問題時提供了可資遵循的辦案方向。[21]

在加強公民教育宣導方面，中國政府體認到對於網路恐怖主義的處理，以行政手段強化監管並制訂嚴密法令規章固然重要，但提高民眾警惕心理與協作意願，使其在網路活動中不易受到相關涉恐資訊影響，並願意向政府部門主動舉報，才是提升反恐行動效率的長治久安之道。[22] 因此，中國政府近年致力強化教育宣導，除發送前文提到的《公民防範恐怖襲擊手冊》外，中國國家互聯網信息辦公室等單位也以製作專題紀錄片的方式，完整闡述網路恐怖主義的表現形態與重大危害。例如該辦公室與公安部、國務院新聞辦公室等部門共同製作的紀錄片「恐怖主義的網上推手－『東伊運』恐怖音視頻」，經由整理近年發生於北京、昆明、烏魯木齊等地恐怖攻擊事件與網路科技間的關聯，佐以訪談反恐事務專家學者，較完整地呈現了網路科技對於當前中國恐怖主義問題的巨大影響，呼籲民眾協助配合政府的反恐工作。[23]

二、國際社會層次的網路反恐努力

在國際社會中，中國近年對於國際網路反恐合作的重視程度持續提升。中國政府在 2017 年 3 月發表的《網絡空間國際合作戰略》中強調網路恐怖主義是世界各國面臨的共同安全挑戰，呼籲各國加強合作以資應對；該文件並以專節闡述中國在打擊網路恐怖主義和網路犯罪方面的對外合作思路，指出中國將依循「全球合作」、「地區合作」與「國家間合作」三類路徑開展相關努力。[24]

---

[21]〈中華人民共和國刑法〉，《中國人大網》，1997 年 3 月 14 日，http://www.npc.gov.cn/zgrdw/npc/lfzt/rlys/2008-08/21/content_1882895.htm。

[22]〈舉報中心呼籲廣大網民積極舉報網上暴恐有害信息〉，《中國國家互聯網信息辦公室》，2016 年 2 月 4 日，http://www.cac.gov.cn/2016-02/04/c_1117990744.htm。

[23]〈國家網信辦發佈「恐怖主義的網上推首」電視專題片〉，《中國國家互聯網信息辦公室》，2014 年 6 月 24 日，http://www.cac.gov.cn/2014-06/24/c_1111294786.htm。

[24]〈網絡空間國際合作戰略〉，《新華網》，2017 年 3 月 1 日，http://www.xinhuanet.com/politics/2017-03/01/c_1120552767.htm。

在全球合作方面，中國承諾將全力支持聯合國(United Nations, UN)作為促進全球網路反恐合作的協調平台，不僅承諾持續提供對聯合國反恐辦公室(UN Office of Counter-Terrorism, UNOCT)的政治及財務支持，也經由「中國—聯合國和平發展基金」(China-UN Peace and Development Fund)框架贊助該機構於非洲的反恐工作，以及國際大型賽事安全保障等事務。中國也將在〈聯合國全球反恐戰略〉(UN Global Counter-Terrorism Strategy)，與〈防止暴力與極端主義行動計畫〉(Plans of Action to Prevent Violent Extremism)等聯合國法制框架的實踐及後續修訂中，[25] 持續扮演積極參與者的角色。[26] 除聯合國外，中國也透過其他管道持續推動全球網路反恐合作，例如在「全球反恐論壇」(Global Counter-Terrorism Forum)架構下籌辦探討網路恐怖主義問題的研究會議，促進國家間意見交流與建立協作共識；[27] 在金磚國家(BRICs)合作中導入網路反恐議題；[28] 以及在中國自身籌辦的「世界互聯網大會」(World Internet Conference, WIC)中向與會各國強調網路恐怖主義的危害及國際合作的必要性。[29]

在地區合作方面，「上海合作組織」(Shanghai Cooperation Organization, SCO)是中國於鄰近區域中推動網路反恐合作的最重要途徑，該組織成員對

---

[25] 相關文件內容請見：UN Office of Counter-Terrorism, "UN Global Counter-Terrorism Strategy," September 8, 2006, https://www.un.org/counterterrorism/un-global-counter-terrorism-strategy；UN Office of Counter-Terrorism, "Plans of Action to Prevent Violent Extremism," December 24, 2015, https://www.un.org/counterterrorism/cct/plans-of-action-to-prevent-violent-extremism.

[26]《中國常駐聯合國代表：弘揚多邊主義對反恐努力至關重要》，《中國國防部》，2020 年 7 月 12 日，http://www.mod.gov.cn/big5/action/2020-07/12/content_4868031.htm。

[27]〈全球反恐論壇框架下第二次打擊網路恐怖主義研討會在京舉行〉，《中國國家互聯網》信息辦公室，2016 年 10 月 21 日，http://www.cac.gov.cn/2016-10/21/c_1119764953.htm。

[28]〈金磚國家反恐工作組去極端化分工作組舉行視頻會議〉，《中國外交部》，2022 年 4 月 22 日，https://www.fmprc.gov.cn/web/wjb_673085/zzjg_673183/swaqsws_674705/xgxw_674707/202204/t20220422_10672083.shtml。

[29]〈烏鎮世界互聯網大會「獻計」網絡「反恐戰爭」〉，《人民網》，2016 年 11 月 17 日，http://it.people.com.cn/BIG5/n1/2016/1117/c1009-28876883.html。

反恐事務向具合作共識，自 2015 年起以兩年一度的頻率持續辦理網路反恐聯合演習，邀集各國專業團隊共同以模擬作戰和兵棋推演等形式，應對網路恐攻造成的各類危機情境。[30] 此外，中國近年逐步強化與「東南亞國協」(Association of Southeast Asian Nations, ASEAN)交往的同時，亦試圖增進和該組織間的網路反恐合作，公開邀請東協與其共建網路反恐技術互助框架，建議雙方成立「常態合作機制」，[31] 部分學者也呼籲東協國家可和中國在「瀾滄江—湄公河」次區域架構下籌組網路反恐合作平台。[32] 而中國近年積極推動的「一帶一路倡議」 (One Belt One Road Initiative, OBOR)也成為北京當局推進區域網路反恐合作的重要管道，例如中國於推進「絲綢之路經濟帶」(Silk Road Economic Belt)建設的過程中，成功與阿富汗及巴基斯坦簽訂「三方合作打擊恐怖主義諒解備忘錄」，將網路恐怖主義納入其中；[33] 中國另於衍生自「一帶一路」倡議的「數字絲綢之路」(Digital Silk Road, DSR)計畫中，藉由推動與沿線各國網路事務合作的過程，將反恐工作一併納入其中。[34]

在國家間合作方面，中國近年逐次將網路反恐事務納為與各國雙邊交流的重要項目。舉例而言，中國與印尼兩國於 2015 年 3 月時共同發表了〈中華人民共和國和印度尼西亞共和國關於加強兩國全面戰略夥伴關係的聯合聲明〉，其中提到雙方將在網路反恐領域相互支持，協助彼此提升

[30]〈第三屆上合組織網絡反恐聯合演習在中國舉行〉，《新華網》，2019 年 12 月 12 日，http://big5.xinhuanet.com/gate/big5/www.xinhuanet.com/mil/2019-12/12/c_1125340396.htm。

[31]〈外交部傅聰：願與東盟建立多雙邊網絡對話機制〉，《中國網》， 2014 年 9 月 18 日，http://tech.china.com.cn/news/special/dmwllt/20140918/142026.shtml。

[32] 孟璐，〈論瀾湄國家網路反恐機制構建〉，《湖北警官學院學報》，2021 年第 1 期（2021 年 1 月），頁 29-37。

[33]〈第二次中國—阿富汗—巴基斯坦三方外長對話聯合聲明〉，《全球法規網》，2018 年 12 月 15 日，http://policy.mofcom.gov.cn/pact/pactContent.shtml?id=3019。

[34]〈將「數字絲路」建設成為「平安絲路」〉，《人民網》，2015 年 12 月 17 日，http://it.people.com.cn/n1/2015/1217/c1009-27942750.html。

反恐能力。[35] 以此為基礎，中國與印尼政府隨即共同推動網路作戰演習、網路戰略規劃、管理網路危機及強化網路監控和數據復原能力等多項具體合作計畫。[36] 中國與白俄羅斯在 2015 年 5 月發表聯合聲明，宣布兩國將加強因應網路恐怖主義挑戰，在人員、技術、情資等方面加強合作互助。[37] 此外，中國與德國在 2018 年 7 月舉辦的第五輪政府間磋商中，也首度將網路恐怖主義問題導入副部長級會談，宣示兩國將在此領域擴大合作。[38]

伍、中國網路反恐工作的影響評估

透過上文的概要梳理，當可察見中國政府在面對網路恐怖威脅時，確已採取諸多因應措施。然若細究相關反恐工作的深層意圖，則可從中發現三項值得注意的特點：第一，北京當局似有意利用網路反恐名義強化對分離主義和民族矛盾的壓制；第二，網路反恐工作將使政府部門更有能力箝制國民網路自由；第三，網路反恐似乎成為中國在國際網路政治中抗衡美國的策略手段之一。於下分別進行說明：

一、利用網路反恐加強壓制分離主義、民族矛盾與激進宗教問題

以新疆維吾爾自治區為主的分離主義運動及相關民族與宗教摩擦，是

---

[35]〈中華人民共和國和印度尼西亞共和國關於加強兩國全面戰略夥伴關係的聯合聲明〉，《中國政府網》，2015 年 3 月 26 日，http://big5.www.gov.cn/gate/big5/www.gov.cn/xinwen/2015-03/27/content_2838995.htm。

[36] Greg Austin, “China and Indonesia: Joint Cyber War Simulations,” *The Diplomat*, January 26, 2016, https://thediplomat.com/2016/01/china-and-indonesia-joint-cyber-war-simulations/.

[37]〈中華人民共和國和白俄羅斯共和國關於進一步發展和深化全面戰略夥伴關係的聯合聲明（全文）〉，《新華網》，2015 年 5 月 11 日，http://www.xinhuanet.com/world/2015-05/11/c_1115235825.htm。

[38]〈第五輪中德政府磋商聯合聲明〉，《中國日報網》，2018 年 7 月 10 日，http://china.chinadaily.com.cn/2018-07/10/content_36549747.htm。

困擾中國政府許久的內部問題。當地許多民眾由於在民族認同、文化傳統及宗教信仰上與多數中國國民不同，長期以來皆有脫離中國統治尋求獨立的呼聲。為避免過於嚴酷的壓制行動招來國際社會批評而損及國家形象，中國自改革開放以來對於新疆獨立運動的處理一向謹慎，在動用警政力量查緝激進抗爭和暴力事件外，同步採取移民實邊、促進在地經濟發展，以及和土耳其與中亞各國合作查緝分離主義勢力等策略。

然而九一一恐怖攻擊事件的發生為中國的新疆治理帶來機遇，藉由積極參與其時國際社會高度關注的反恐議題，並表達對小布希(George W. Bush)政府發起反恐戰事的大力支持，北京當局成功地使「東突厥斯坦伊斯蘭運動」於 2002 年時被列入聯合國安全理事會(United Nations Security Council)的恐怖組織名單之中，這使中國對當地的嚴格監控、大規模查緝與拘禁行動在形式上獲得更多正當性，降低歐美各國以人權保障名義介入其中的空間。[39]

隨著網路恐怖主義威脅逐漸受到世界各國重視，以及部分新疆獨立運動成員透過網路影音服務對外宣傳獨立訴求，中國政府似乎有意再次以反恐為由，順勢對新疆當地民眾的線上活動進行更嚴格的監管。美國國務院於《2019 年度反恐怖主義報告》(*Country Reports on Terrorism 2019*)的中國國別報告部分指出，中國政府意圖利用對網路恐怖主義的模糊界定，將其作為擴大壓制宗教及少數民族群體網路言論和通訊活動的藉口。[40]

二、配合網路反恐強化管制國民網路自由

自 1990 年代以來，中國政府對網路科技的認知便抱持極為複雜的雙重觀點：一方面注意到此新興技術的深厚應用潛力及經濟效益，另一方面

[39]〈911 事件 20 週年：美國全球反恐為中國打開了「機遇之門」？〉，《BBC 中文網》，2021 年 9 月 9 日，https://www.bbc.com/zhongwen/trad/world-58382524。

[40] U.S. Department of State, “Country Reports on Terrorism 2019: China (Hong Kong and Macau),” June 24, 2020, https://www.state.gov/reports/country-reports-on-terrorism-2019/china/.

則關注網路科技在牽動公眾輿論、挑戰統治權威方面的可能影響。因此，中國過去數十年間的網路施政具有相當明顯的雙面性，既利用各種政策工具支持資訊產業成長茁壯，推動國內網路環境的軟硬體建設工作，同時也經由技術監管與法規制訂等途徑，確保政府部門對國民線上活動和資訊傳播的控制力不受削弱。[41]

中國民眾對本國政府的網路監管政策並非全無意見，許多國民也會使用 VPN 等技術試圖突破管制。為避免過於嚴格的管理政策引發民怨，中國政府對於監管強度的拿捏頗為審慎，譬如對政治敏感資訊的過濾工作，往往不是由政府出面處理，而是由網路服務業者或社群媒體平台業者先行篩選，盡可能避免使民眾感受自身網路活動遭受限制。[42] 不過網路恐怖主義威脅似乎為中國政府堂皇正大地擴大網路管制提供了一個堂之合理，且對民眾有一定說服力的理據。例如自 2016 年 1 月起施行的《中華人民共和國反恐怖主義法》要求網路服務與電信業者需配合政府反恐工作，提供「技術介面和解密」等支持，主管機關也有權刪除特定資訊、提供通訊記錄或關閉有關網站。[43] 換言之，中國網路反恐工作的推行，很可能將導致國民網路自由進一步下降。

三、擴大國際網路政治合作以抵制美國影響

對於中國網路反恐政策的第三項評估，可回歸至國際政治中的強權競逐加以觀察。早於歐巴馬(Barack H. Obama)政府任內，美中兩國學者便注意到雙方看待網路事務的視角歧異，似乎正逐漸成為根深蒂固的戰略互疑

---

41 陳建功、李曉東，〈中國互聯網發展的歷史階段劃分〉，《互聯網天地》，2014 年第 3 期（2014 年 7 月），頁 6-13。

42 James Griffiths, *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet* (London: Zed Books, 2019), pp. 71-72.

43 請參考該法規第 18 條與第 19 條，詳見：中國人大網，《中華人民共和國反恐怖主義法》，2015 年 12 月 27 日，http://www.npc.gov.cn/zgrdw/npc/xinwen/2018-06/12/content_2055871.htm。

中(Strategic Distrust)最尖銳難解的一環。[44] 華府與北京不僅相互關注對方的網路間諜活動及網路戰力發展如何影響本國安全，兩國對網際網路空間的治理思維也有明顯歧異。

作為全球最具影響力的資訊強權，美國長年來積極倡導「網路自由」(Freedom Online)與「網路人權」(Human Rights Online)價值，呼籲各國政府尊重網際網路的無國界特性，確保資訊能在其中自由開放流動，不對國民線上活動進行過度干預。[45] 透過將政治層面的民主與人權價值導入網際網路治理，美國持續邀集持有相同信念的國家加強合作，漸進構築一個以美國為核心，以民主國家為主要成員的同盟陣線。[46]

面對這一情勢，中國政府本於自身的政治價值，提出迥異於美國的網際網路治理論述，主張所有國家對本國網域皆有「網路主權」(Cyber Sovereignty)，網路空間應處於「有國界」狀態，各國理當對本國網域運作及國民線上活動持有完整管轄權限。[47] 與美國相同，中國近年也透過推廣「網路主權」觀念，積極號召俄羅斯、伊朗、阿爾及利亞與「上海合作組織」成員等信念相仿的國家擴大合作，隱然建立起一個與美國相對立的外交陣線。[48] 雖然中國的「網路主權」論述常引起外界有關網路自由可能在此名目下遭受侵害等質疑，但恐怖主義的危害、網路恐怖主義持續增生的

---

44 Kenneth G. Lieberthal and Wang Jisi, *Addressing U.S.-China Strategic Distrust* (Washington, D.C.: The Brookings Institution, 2012), p. 6.

45 The White House, *International Strategy for Cyberspace* (Washington, D.C.: The White House, 2011), p. 5.

46 Jessica Brandt, "How Biden can make His Internet Freedom Agenda a Success," *The Brookings Institution*, December 8, 2021, https://www.brookings.edu/techstream/how-biden-can-make-his-internet-freedom-agenda-a-success/.

47 Li Zhang, "A Chinese Perspective on Cyber War," *International Review of the Red Cross*, Vol. 94, No. 886 (Summer 2012), p. 806.

48 請參考：中國外交部，〈信息安全國際行為準則〉，2015 年 3 月 5 日，https://www.fmprc.gov.cn/web/ziliao_674904/tytj_674911/zcwj_674915/201109/t20110913_9869162.shtml；陳健、龔曉鶯，〈「一帶一路」沿線國家共同應對網絡恐怖主義研究〉，《新疆社會科學》，2017 年第 5 期（2017 年 10 月），頁 85。

態勢，以及日益迫切的網路反恐需求，似乎成為北京當局正當化其論述的極佳依據。中國官員在推動與周邊國家的網路反恐合作時，也利用各種國際場合呼籲各國應接受其「網路主權」論述，承認各國有權監管本國網域與國民網路活動，藉以有效防治網路恐怖主義危害。[49]

陸、結論

作為資訊化時代新興的國際安全議題，網路恐怖主義近年漸受各界重視。放眼全球，幾乎每個仰賴網路科技支撐起政治、經濟與社會體系運作的國家，皆難免受其影響，擁有全球最大網路用戶群體的中國自不例外。

相較於部分國家，中國目前面臨的網路恐怖威脅程度尚屬有限，並未遭遇大規模網路攻擊，且相關恐怖活動多源自於邊境分離主義運動及民族宗教摩擦等傳統問題，其源流大致上明確可溯。雖然如此，有鑒於部分恐怖勢力近年積極應用網路平台與影音串流服務從事募集人物力資源、宣傳激進理念和傳遞武器製作知識等活動，政府部門若不及時採取因應措施，其國家安全必然遭受衝擊。

在此脈絡下，中國近年於國內社會與國際社會中同步推行了一系列網路反恐政策作為。在國內社會中，中國政府漸進強化對本國網域的資訊審查，嚴格查緝涉嫌恐怖活動的影音資訊和國民線上活動，同時推動多項立法與修法措施，完善司法體系對違法網路活動的監管。為增進國民反恐意識並配合國家網路反恐政策，中國政府也積極推動宣導教育工作，利用製作公民反恐手冊和反恐紀錄片等途徑，向民眾闡釋網路恐怖主義的危害及防範之道。在國際社會中，中國一方面肯定聯合國作為全球網路反恐合作平台的價值，提供其各類資源支持，也在「全球反恐論壇」、「世界互聯網大會」等框架中和世界各國就網路反恐事務進行交流。此外，中國與周

[49] 中國國家互聯網信息辦公室，〈網絡反恐論壇舉行，加強國際交流合作打擊網絡恐怖主義〉，2016 年 11 月 18 日，http://www.cac.gov.cn/2016-11/18/c_1119943188.htm。

邊各國及「上海合作組織」等多邊機制亦於此領域實施了多項具體合作措施。

整體來看，中國的網路反恐行動堪稱積極，若細究其政策作為背後的意圖考量，可察見中國政府在應對恐怖主義危害之外，也希望利用網路反恐名義，擴大壓制少數民族與邊境地區、強化監控國民網路活動，並在國際網路政治中合理化其提出的「網路主權」等治理觀點，藉以抵制美國及其友邦的影響力。

長遠而言，中國的網路反恐前景仍存在諸多變數，其中有三個事項尤其值得觀察：第一，隨著中國的國內網路監控在反恐名義下日益加嚴，網路用戶群體的態度和迴響變化有待評估，北京當局或有必要在加強管制的過程中拿捏適度地妥協空間，以避免進一步提高政府與網路用戶間的矛盾。第二，中國與其鄰近國家在反恐名義下的網路合作，似乎存在著使中國發展多年且頗有所成的網路監管技術順勢輸出至周邊威權國家，使相關國家網路自由水準進一步降低的風險。第三，中國似乎有意以網路反恐名義為其強調的「網路主權」治理觀點增添論述上的正當性，美國及其友邦將如何回應，及美中兩國在網路事務上的對立會否進一步加劇，同樣值得觀察者持續關注。

責任編輯：傅家鈺