第九章　關鍵資訊基礎設施

吳宗翰*

壹、前言

2020年世界科技發展受到加劇的美中競爭關係以及突然爆發的新冠肺炎雙重背景影響頗深。後者席捲全球，至今未見緩解，許多國家紛紛採取封城封區（lockdown）措施，政府也提倡互動之間應保持社交距離（social distance），減少接觸。在這樣情況下，人們對數位工具的使用與需求較過去不僅猛然暴增，生活型態的改變也大為促進整體社會數位化發展。緊接著，相關基礎設施的建構、資安問題也隨之增加並浮現，成為各國政府正在積極應付的課題。

從軍事國防的角度來看，關鍵資訊基礎設施（critical information infrastructure, CII），以及關鍵基礎設施（critical infrastructure, CI）可謂是發動「混合威脅」與「不對稱戰」的極佳場域，這是由於相關設施高度互相依存（或稱為互賴，interdependency），牽一髮可能動全身，特別是基於網路與資通訊系統已無不貫穿多數關鍵基礎設施的事實。尤其，關鍵基礎設施廣泛分布於社會各民用領域，一旦敵人透過這種連結性對己方發動攻擊，造成的損害難以估算，更是混淆了軍／民間的二分概念界線。從這樣的角度言，網路安全（cybersecurity）的重要性相較過去有增無減。美國前國防部長潘內達（Leon Panetta）就曾提出慎防「網路珍珠港」（Cyber Pearl Harbor）的概念。[1] 懷有惡意的攻擊者，無論是否背後來自國家資助，在攻擊手法與攻擊動機兩個面向上都呈現更加複雜的狀況。攻擊者未必是出於金錢或是竊取機敏資訊為目的，更有可能是潛藏特定政治意圖，

* 吳宗翰，國防安全研究院網路安全與決策推演研究所博士後研究。

1 Elisabeth Bumiller and Thom Shanker, “Panetta Warns of Dire Threat of Cyberattack on U.S.,” *The New York Times*, October 11, 2012, https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

希望藉此影響或打擊被攻擊國家的關鍵基礎設施，削弱國民信心，以謀求對自身的最大利益。同時，基礎設施相互依存的特性，往往也使得受害者在歸因（attribution）階段需要耗費大量心力。

網路攻擊本就屬於灰色地帶，目前在國際法上也尚未有對「網路戰」形成一個一致的規範；各國在相關的接戰規則（rules of engagement, ROE）上也仍然多屬於發展中的研議階段。但無論如何，關鍵資訊基礎設施乃至關鍵基礎設施的防護已然刻不容緩，各國政府亦在規範面與實務面向做出大量努力。

貳、關鍵資訊基礎設施的定義與安全意涵

關鍵資訊基礎設施定義雖然歷時而變，但多與關鍵基礎設施定義相關；在數位社會的發展推進下兩者界線更是趨於模糊，難以釐清。隨著美國川普總統在其任內正式設立「網路安全暨基礎安全局」（Cybersecurity and Infrastructure Security Agency, CISA），將網路安全事務治理提升到聯邦層級，兩者在美國幾乎已不存在實質分別。美國「國土安全部」將關鍵基礎設施視為「對美國極為重要的實體與網路系統或資產，其無作用或損害將會對實體與經濟安全或是公眾健康有嚴重影響。關鍵基礎設施的服務支撐美國社會」。[2] 可以說，這些設施攸關政府在各方面的運作順暢，包括政府機關、道路與運輸交通、通信系統、水系統、能源系統、醫療與銀行等。[3]

歐盟雖然對兩者有做出區別，但實際上兩者內容仍有高度重疊。歐盟執委會在其第 2008/114/EC 發布的指令中（*Council Directive 2008/114/EC*），將關鍵基礎設施定義為「會員國內維護重要社會功能、人民健康、安全、經濟與社會福利等的資產或系統，其相關損害會有重大影響」。儘

2 "Critical Infrastructure Security," Department of Homeland Security, https://www.dhs.gov/topic/critical-infrastructure-security.

3 Kelley A. Pesch-Cronin and Nancy E. Marion, Critical Infrastructure Protection, Risk Management, and Resilience: A Policy Perspective (CRC Press, 2016), p. 4.

管歐盟執委會未對關鍵資訊基礎設施進一步闡述，歐盟網路資訊安全署（European Union Agency for Cybersecurity, ENISA）在其發布相關文件中指出關鍵資訊基礎設施是那些支持關鍵基礎設施的資通訊設備與服務，包括軟體、網路、衛星等。[4]

在我國，根據行政院《國家關鍵基礎設施安全防護指導綱要》指示，我國將國家關鍵資訊基礎設施定義為「涉及核心業務運作，為支持國家關鍵基礎設施持續營運所需之重要資通訊系統或調度、控制系統，亦屬國家關鍵基礎設施之重要元件（資通訊類資產），應配合對應之國家關鍵基礎設施統一納管。」[5] 根據《指導綱要》，我國關鍵基礎設施按三層架構分類：第一層為主領域，共分成能源、水資源、通訊傳播、交通、金融、緊急救援與醫院、政府機關、科學園區與工業區等 8 類；第二層為次領域，是針對主領域中的 8 種領域依照功能再細分；第三層領域為次領域的再細分。相關細節可見表 9-1。

初步比較美國、歐盟與我國對於關鍵資訊基礎設施以及關鍵基礎設施的定義看法，可以發現彼此內容雖有重疊，具體項目卻有差異。這說明在不同社會脈絡下，因產業、國家發展差異，對於「重要設施」的認定會有所不同。

表面上看起來，資通訊系統只是上述國家關鍵基礎設施中主領域的其中一類，但考量到關鍵基礎設施之間的相依性以及設施的聯網普遍性，關鍵資訊基礎設施的防護幾乎無法自外於關鍵基礎設施的防護（critical infrastructure protection, CIP）。基於此，關鍵資訊基礎設施的安全實質上同關鍵基礎設施的安全，可以從實體安全、非實體安全（特別是資訊安全）以及人員安全三個面向理解。所謂實體安全，指的就是「設施」本身

4 European Commission, “Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection,” Official Journal of European Union, 345 (2008), p. 77; “Critical Information Infrastructure,” European Union Agency for Cybersecurity, https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/cii?tab=details.

5 〈國家關鍵基礎設施安全防護指導綱要〉，《行政院國土安全政策會報》，https://ohs.ey.gov.tw/Page/1E6899A649BEF1F9。

的安全。造成設施安全出現問題的原因可能來自天災與人禍導致。非實體安全的面向則主要來自軟體系統故障，在多數實例中，這些故障往往與資訊系統或網路系統影響整體系統正常運作有關。第三個面向是人員安全，這指涉的是人員因為違反規定、不當操作軟硬體，或是惡意破壞，例如駭客（hacker）、網路恐怖分子導致設施安全受到損害。

另一方面，資安領域常見的攻擊手法亦成為相關設施防護必要重視的風險。這些包括惡意軟體（malware）、電腦病毒、木馬程式、分散式阻斷服務攻擊（distributed denial-of-service attack, DDos）、進階持續性威脅（advanced persistent threat, APT）、針對人員發動的魚叉式釣魚（spear-pishing）、針對軟體更新落差的零日攻擊（zero-day attack）等。隨著第 5 代行動通訊技術（5th generation wireless systems，下稱 5G）發展，有關資訊科技（information technology, IT）與營運科技（operation technology, OT）的更多整合以及物聯網（Internet of Things, IoT）帶來的風險更是需要高度重視。

從前述定義可知，關鍵基礎設施攸關政府與社會的整體正常運作。若然遭受侵害影響範圍可能廣大。從「混合威脅」與「不對稱戰」的角度言，攻擊關鍵基礎設施可說是低成本、高回報，又具備隱匿性的途徑。並且，在引發社會不安情緒頗能有卓越成效，因而亦是行遂認知戰的適合手法。今年由於疫情緣故，社會人心普遍焦躁不安，維護關鍵基礎設施更是政府重中之重的優先事項。

表 9-1　台灣關鍵基礎設施

主領域	次領域	業務功能	主管機關
能源	電力	負責供電服務	經濟部
	石油	供應油品與帶動石化相關工業發展之設施	
	天然氣	供應天然氣之相關設施	
水資源	供水	供水	經濟部（地方政府）
通訊傳播	通訊	支持通訓服務之重要設施，如市內／長途／國際通、行動通訊、衛星通訊及數據通訊等	國家通訊傳播委員會
	傳播	支持傳播服務之重要設施，如無線／有線廣播電視	
交通	陸運	陸上運輸服務，含鐵路、高速鐵路、大眾捷運	交通部（地方政府）
	海運	提供航運及商港、工業港、漁港之相關設施	交通部、經濟部、農委會
	空運	提供航空營運管理及航空運輸相關服務	交通部、國防部
	氣象	與氣象、地震、海象等觀測預報有關之服務	交通部
金融	銀行	財金公司、中華郵政	金融監督管理委員會、交通部
	證券	執行全國證券、期貨市場交易及結算、交割	金融監督管理委員會
	金融支付	我國支付清算系統之相關系統	中央銀行
緊急救援與醫院	醫療照護	提供醫療照護之相關系統	衛生福利部
	疾病管制	傳染病疫情監測與預警之相關設施	
	緊急應變體系	災害緊急應變中心等相關重要設施	
政府機關	機關場所與設施	支持政府核心業務運作重要設施	內政部、海洋委員會（地方政府）
	資通訊系統	支持政府核心業務運作之重要資通訊系統	中央政府機關（地方政府機關）
科學園區與工業區	科學工業與生醫園區	科學園區等	科技部
	軟體園區與工業區	軟體園區、工業區等	經濟部

資料來源：修改自〈國家關鍵基礎設施領域分類〉107 年 7 月 30 日版本，見 https://ohs.ey.gov.tw/Page/1E6899A649BEF1F9。[6]

6 〈國家關鍵基礎設施領域分類〉，《行政院國土安全政策會報》，https://ohs.ey.gov.tw/Page/1E6899A649BEF1F9。

參、美中對抗衝擊下的 5G 網路建設與網路空間

討論關鍵資訊基礎建設無法迴避網路建設。2020 年各國陸續啟用 5G 網路，有關基礎建設、應用與資安議題也隨之增加。並且，美中對抗格局與地緣政治更是使相關討論變的複雜。

歐盟在 2019 年 10 月發表《5G 網路風險評估報告》（*EU coordinated risk assessment of 5G networks security*），當時就指出，由於 5G 網路環境需要建置更多的基地台與設施，網路的便利性使得聯網裝置數量大為增加，裝置也能彼此互通，並且軟體的角色更為重要，因此面臨的資安挑戰也更加嚴峻。[7]

任一基礎建設本身就由更多更小的零件構成。從防護的角度來說，網路供應商本身與供應鏈安全就成為網路基礎建設中最優先的事項。歐盟的報告指出，來自非歐盟國家或政府干預或支持的駭客攻擊將可能造成嚴重損害。儘管該報告內容並未明確點名何者為不可靠的供應商，但一般認為字裡行間暗指中國華為。然而，報告書中所言不應過度依賴特定供應商的說法，也被視為歐盟並未排除華為參與網路建設。不過，隨著美中加劇對抗以及疫情影響，多個歐盟會員國已經在 2020 年間陸續宣布排除華為，或是採取更為嚴格的審查手段，英國也在 2020 年 7 月宣布禁止華為，自該年底不再從華為購買新設備，已經存在英國 5G 建設中的設備也將在 2027 年前移除。[8]

---

7 "Member States publish a report on EU coordinated risk assessment of 5G networks security," European Commission, October 9, 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049.

8 "Member States publish a report on EU coordinated risk assessment of 5G networks security," European Commission, October 9, 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049; "Europe brief: western Europe's stance on China hardens," *The Economist*, September 10, 2020, https://www.eiu.com/n/europe-brief-western-europes-stance-on-china-hardens/; Robbie Gramer, "Trump Turning More Countries in Europe Against Huawei," *Foreign Policy*, October 27, 2020, https://foreignpolicy.com/2020/10/27/trump-europe-huawei-china-us-competition-geopolitics-5g-slovakia/; Department for Digital, Culture, Media & Sport, National Cyber Security Centre, and The Rt Hon Oliver Dowden CBE MP, "Huawei to be removed from UK 5G networks by 2027," *GOV. UK*, July 14, 2020, https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027.

美國國務卿蓬佩奧（Mike Pompeo）在 2020 年 4 月底宣布「乾淨路徑」（Clean Path）計畫，當時該計畫旨在要求有關進出美國的 5G 網路須來自「可信任與可靠的」設備供應商，並點名排除華為與中興等企業。

在 8 月時，蓬佩奧更進一步整合川普政府近年來在 5G 網路安全的計畫，針對中國共產黨對公民隱私、企業機敏訊息以及人權的侵害，提出在全球範圍建立「乾淨網路」（Clean Network）計畫，倡議在電信業、行動應用程式、雲端儲存、海底電纜以及路徑等六個面向排除中國供應商，並尋求各國加入行列，創立理念相近國家組成的網路安全聯盟。根據美國國務院委託戰略暨國際研究中心（Center for Strategic and International Studies, CSIS），台灣的五大電信「中華電信、遠傳、台灣大哥大、台灣之星、亞太電信」均在美方定義的乾淨供應商名單內。從規模來說，「乾淨網路」計畫目前是川普政府任內試圖圍堵中國資通訊企業中採取力度最大的行動。[9]

作為反制，中國也在 9 月底提出了「全球數據安全倡議」（Global Data Security Initiative），以不具名的方式批評美方的做法是排他性質。在該倡議中，中國高調提倡國際間應該建立開放、合作、有序、安全的網路空間。[10] 在 11 月底，中國透過舉行「世界互聯網大會 • 互聯網發展論壇」的場合發布《網路主權：理論與實踐（2.0 版）》，更新其稍早前在 2020 年 6 月第六屆互聯網大會時的論述，除了堅稱任一主權國家可申張擁有「網路主權」的正當性，亦呼應「全球數據安全倡議」的內容，批判部分國家透過網路干涉他國內政，行單邊主義與霸權行動；顯然是針對美國。[11]

表面上看，這是美中夾雜國家利益、商業利益以及資安的多層次與多領域對抗，並在國際間各自尋求支持者。長遠地說，這無法排除未來網路

9 "The Clean Network," U.S. Department of State, August 2020, https://www.state.gov/the-clean-network/.

10 〈全球數據安全倡議〉，《人民網》，2020 年 9 月 9 日，http://industry.people.com.cn/BIG5/n1/2020/0909/c413883-31854708.html。

11 〈網路主權：理論與時間（2.0）〉，《中華人民共和國互聯網信息辦公室》，2020 年 11 月 25 日，http://www.cac.gov.cn/2020-11/25/c_1607869924931855.htm。

空間最終會出現聯盟化、壁壘化的網路標準的可能性。後續情況值得追蹤觀察。

肆、新趨勢下海底電纜成為重要議題

網路活動的蓬勃，使網路已不僅止於相互溝通與尋找資料，更協助商貿經濟活動、服務得以建立；疫情的到來，更影響各國網路使用者爆增的需求。而一切的基礎實有賴訊息的傳遞，作為路徑的頻寬至關重要。然而，頻寬建設並非無形，而是實體。直白地說，就是纜路。

海底電纜自 19 世紀問世而被鋪設以來，迅速地成為世界各國彼此在民用、商用甚至軍事溝通交流往來的重要設施；至今，海纜更是擔負連結跨國網路傳輸資料服務角色，國際網際網路 95% 的流量都是通過海纜運輸（見圖 9-1）。聯合國大會在 2010 年即指出海纜對全球經濟與各國國安極端重要，呼籲各國重視相關防護。[12] 然而儘管如此，由於海纜系統的建置與維護涉及高度技術門檻，[13] 又容易受到海洋天然環境以及人類海上作業影響而受損害，致使營運成本昂貴，有能力並同時有意願投入建設的國家非常少，多數交給跨國電信公司與集團獨立建造或共同投資，各國當地業者或參與投資或承租纜線。目前國際上主要的行為者有美國 TE SubCom、法國阿爾卡特集團（Alcatel）、日本電氣股份公司（NEC）及中國華為海洋（Huawei Marine）等，微軟、谷歌、臉書等國際內容業者（international content provider）則為新興的參與者。

隨著美中科技戰持續進行與疫情，海纜議題在今年變得較以往熱門，公眾尤其討論中國公司在相關產業的狀況。2020 年 5 月，中國移動（China

12 United Nations, Resolution 65/37 Oceans and the law of the sea, General Assembly, March 17, 2011, https://undocs.org/en/A/RES/65/37.

13 ITU 建議文件 G.971 指出海纜系統應有以下特點：1. 總體來說要能被長時間使用及具有可靠性；2. 機械特性上可被安裝在深海環境，且能抵抗環境的相關條件，在防護與恢復也有一定的配套措施；3. 海纜的光纖須能可靠的達到產品設計年限，具備抗老化機制。見 “G.971 : General features of optical submarine cable systems,” ITU, https://www.itu.int/rec/T-REC-G.971/en。

Mobile）因為涉及參與「2Africa」的計畫而受到注目。該計畫是目前全球最大的海底電纜項目之一，參與者除了中國移動外，還有臉書、南非電信商 MTN GlobalConnect、法國 Orange 以及英國沃達豐（Vodafone）等；該計畫主要連結非洲、歐洲以及中東地區，預計 2023 或 2024 年建成並開始啟用（見圖 9-2）。[14] 此外，在今年 7 月底華為海洋參與競爭智利政府出資興建的連結南美與亞太地區的海底電纜案失利，最後由日本電氣的方案取得勝利。有關分析也指出美國的態度扮演了重要因素（見圖 9-3）。[15] 這顯見美國川普政府對中國科技公司的圍堵封殺已從行動通訊延伸到電纜領域。

在今年 4 月，美國聯邦傳播委員會（FCC）否決了中國移動進入美國市場並同時關閉中國電信、中國聯通以及太平洋網路在美國的業務公司；在 10 月委員會更呼籲全面審查美國與中國之間連結的海纜系統。而在 6 月，美國「通訊服務業外國參與審查委員會」（The Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector），隨後向聯邦傳播委員會建議否決啟動谷歌、臉書等企業投資的「太平洋光纖電纜網路」（Pacific Light Cable Network, PLCN）中試圖連結美國與香港的路線，建議代之以「台灣 —— 馬尼拉」路線，理由是發現該電纜路線中在香港端登陸站的營運業者為中國電信在港的子公司，這可能會使北京藉此蒐集美國數據。由於時值香港國安法頒布，美國政府的聲明引發諸多揣測。[16]

14 Angelina Rascouet, Loni Prinsloo, and Thomas Seal, "Faster Internet Coming to Africa With Facebook's $1 Billion Cable," *Bloomberg*, May 14, 2020, https://www.bloomberg.com/news/articles/2020-05-14/facebook-china-mobile-to-build-1-billion-sub-sea-africa-cable; Ellen Daniel, "2Africa: New subsea cable will "greatly enhance connectivity" in Africa," *Verdict*, May 14, 2020. https://www.verdict.co.uk/2africa-subsea-cable/.

15 杜貞儀，〈南美與亞太首條海底光纜的戰略布局〉，《國防安全雙週報》，第 9 期，頁 17-21。

16 David Shepardson, "FCC commissioner calls for new scrutiny of undersea Data cables," *Reuters*, October 1, 2020, https://in.reuters.com/article/usa-trade-china-telecommunications/fcc-commissioner-calls-for-new-scrutiny-of-undersea-Data-cables-idINL1N2GR1DV；江今葉，〈美政府建議否決美港海底電纜改連結台灣菲律賓〉，《中央社》，2020 年 6 月 18 日，https://www.cna.com.tw/news/firstnews/202006180014.aspx。

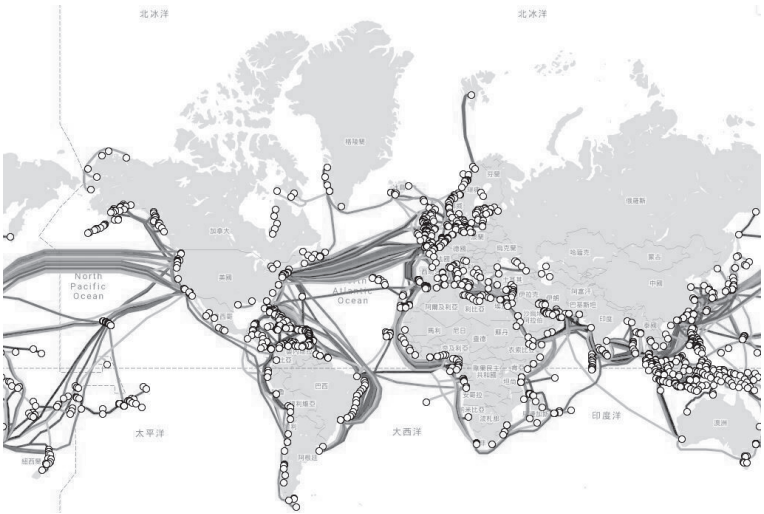

圖 9-1　全球海底電纜分布圖

資料來源：TeleGeography, “Submarine Cable Map,” reviewed December 1, 2020, https://www.submarinecablemap.com/.

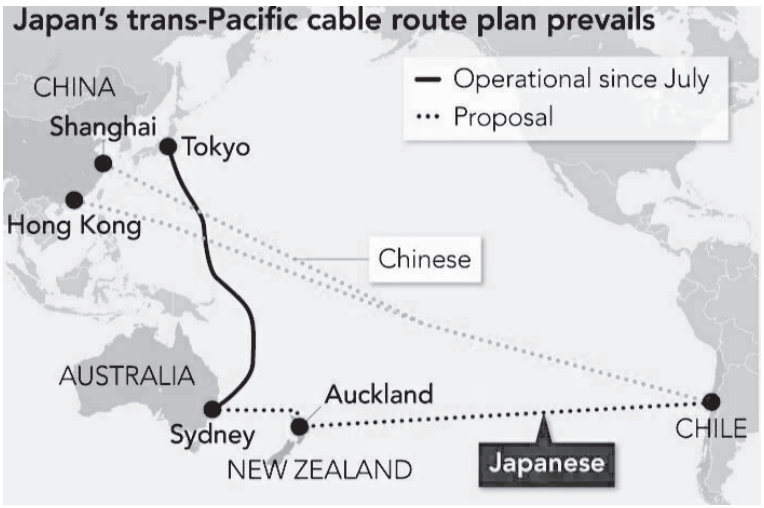

圖 9-2　日本電氣有關連結智利至亞洲的海纜方案

資料來源：Yohei Hirose and Naoyuki Toyama, “Chile picks Japan’s trans-Pacific cable route in snub to China,” *Financial Times*, August 12, 2020, https://www.ft.com/content/674557bc-13c7-4010-a7f8-7b8c06b3a32e.

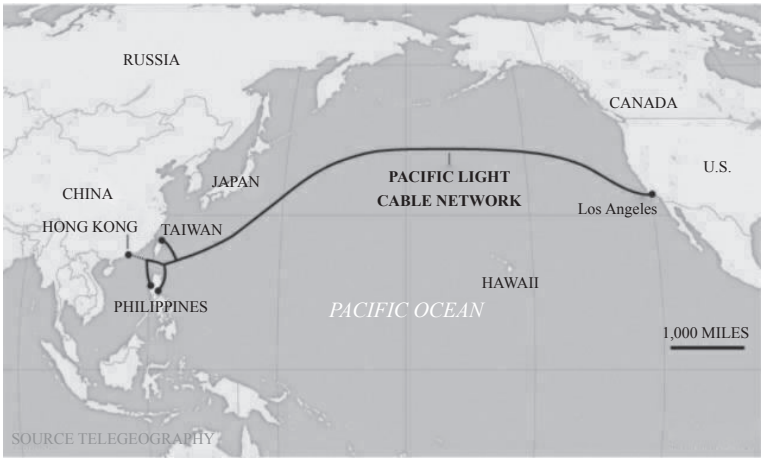

圖 9-3　太平洋光纖網路洛杉磯 —— 香港段被否決啟動

資料來源：Naomi Xu Elegant, "How Google and Facebook's 8,000-mile undersea data cable got caught in U.S.-China feud," *Fortune*, June 18, 2020, https://fortune.com/2020/06/18/google-facebook-undersea-Data-cable-us-china/.

伍、新冠肺炎接觸者追蹤程式的資訊戰

為能及早發現新冠肺炎感染者，迅速切斷傳染途徑，各國政府高度仰賴資通訊手段。各國政府並投入巨大資源開發相關手機應用程式，發展所謂的「接觸者追蹤程式」（contact tracing app）。要說明的是，該類應用程式可能看似未必符合傳統上的「關鍵資訊基礎設施」，但在防範新冠疫情的脈絡下，考量到該類程式的發展基礎其實來自多領域大型資料庫的建立與整合，涉及人民醫療、資通訊技術、交通等，目的在於建立患者的接觸軌跡，甚至在部分國家（如中國）已被用作人民出入行動與否的重要依據，可屬於廣義上的關鍵資訊基礎設施。

從途徑來說，相關應用程式可以大致區分成中心化追蹤技術與非中心化追蹤技術兩種框架（圖 9-4）。所謂中心化指的是應用程式的中央資料庫會與使用者端連線，自動更新與交換資料（Data）；反之，去中心化的

程式則不存在這樣的連線設計。這兩種途徑背後有不同的設計考量：中心化的設計旨在透過大量而自動的資料蒐集使疾病研究人員獲得更多資訊，以利後續研究；而去中心化技術則更強調使用者隱私權，在自願的基礎上提供個人資訊。在實際的程式細部設計上，多數相關程式並不是非此即彼，而是混合式；並且，因為設計原理採用藍芽傳輸方式或是其他定位方式而衍生出更多差異。

目前多數歐美國家正在發展或已投入使用的官方應用程式主要是基於蘋果（Apple）與谷歌（Google）於 2020 年 4 月宣布合作的開發程式，在其基礎上進一步發展；這是為了考量到程式在 Android 或 iOS 系統上的相容性與準確度。[17] 蘋果 —— 谷歌的設計是採行去中心化以及藍芽的方案。然而，由於諸多因素，包括政府並未強制規定民眾須要下載安裝應用程式，民眾的自我揭露程度，以及去中心化追蹤技術的缺陷等，相關應用程式的效果至今仍然有待觀察。[18]

17 Chance Miller, "Here's how Apple and Google's Exposure Notification API works while securing privacy," *9TO5Mac*, June 19, 2020, https://9to5mac.com/2020/06/19/apple-and-google-exposure-notification-api/; "Exposure Notifications: Using technology to help public health authorities fight COVID-19," Google, https://www.google.com/covid19/exposurenotifications/.

18 "UK contact-tracing apps start to talk to each other," *BBC News*, November 5, 2020, https://www.bbc.com/news/technology-54826807; Cat Fergusonarchive, "Do digital contact tracing apps work? Here's what you need to know," *MIT Technology Review*, November 20, 2020, https://www.technologyreview.com/2020/11/20/1012325/do-digital-contact-tracing-apps-work-heres-what-you-need-to-know/.

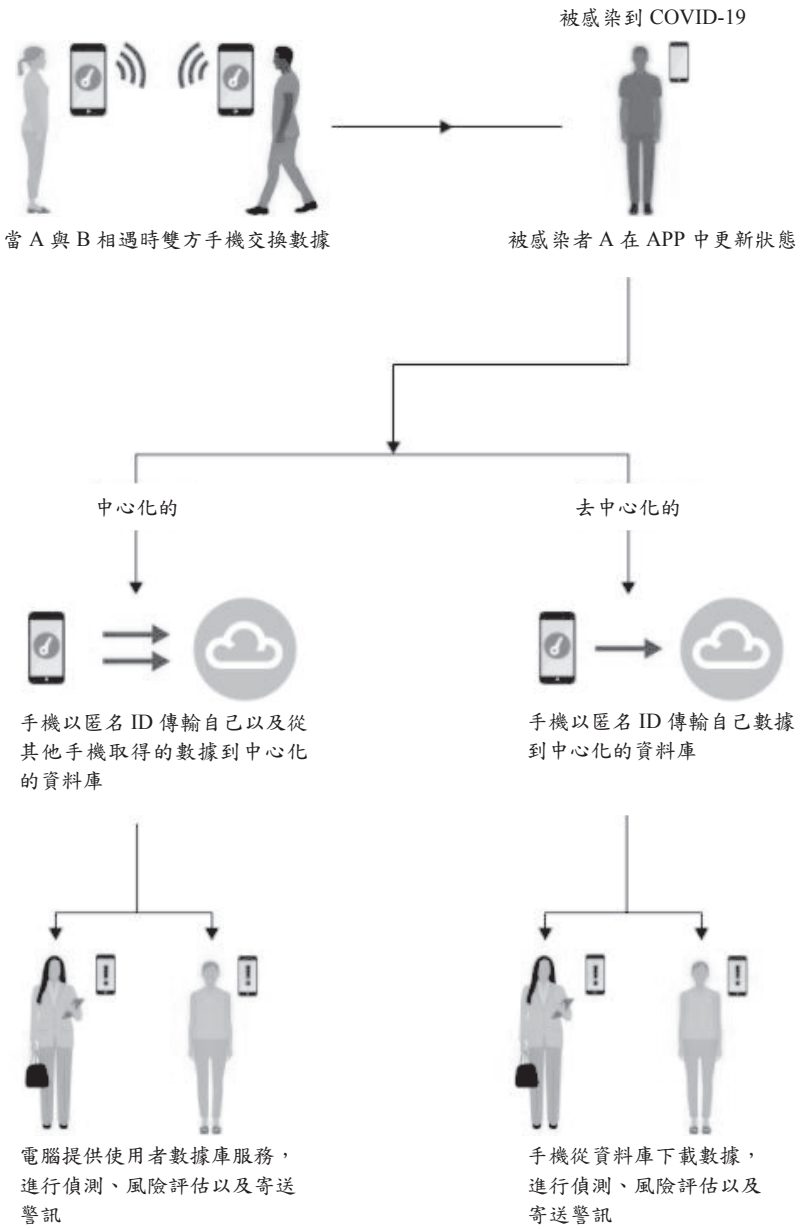

圖 9-4　中心化與去中心化追蹤程式運作架構圖

資料來源：吳宗翰翻譯自 Cristina Criddle & Leo Kelion, "Coronavirus contact-tracing: World split between two types of app," *BBC News*, May 7, 2020, https://www.bbc.com/news/technology-52355028。

另一方面，從發展時程來看，中國可以說是世界上最早推出相關程式的先驅，但其採用的程式設計原理並不同於「蘋果 —— 谷歌」的去他化設計，而是中心化的方案。疫情自 2020 年初在湖北武漢爆發並向外省地區擴散不久，中國官方與民間即著手開發出許多相關手機應用程式，並不斷更新、整合、改版；多數程式最終建立在微信或者是支付寶平台上。儘管細部名稱各有不同，但所有程式最終都設計成以能產生被統稱為「健康碼」的 QR code 二維條碼為主，以供使用者在一定範圍內移動時得以向人展示個人健康狀況。「健康碼」的原理主要是透過三角定位手機 SIM 卡而得知持有者的行動軌跡，並藉由使用者在程式中填報個人資訊健康狀況、旅遊史、居住地，及是否接觸過疑似或確診肺炎病患等問題而判斷出用戶的身體狀況，顯示結果分紅、黃、綠三種顏色標示。截至 2020 年底，中國各地區基本仍維持認定不同的健康碼程式，換言之，民眾當移動到他處時很可能就會被要求安裝使用不同於原來當地的應用程式。

由於中國日前疫情相較於歐美緩和，健康碼便被官方塑造為是中國抗疫手段中極為重要且頗有成效的利器，並預計推廣施行到澳門、香港等地。在 11 月，習近平於 2020 年的 20 國集團（G20）高峰會致詞時還刻意倡議建立以國際互認的「健康碼」機制，以恢復人員旅行和商品流通。[19] 習的說法乃是包裹其在大會上向其他參與國訴諸制定全球標準的意圖。相較於闡明當前中國的實際狀況，習近平對「健康碼」的提倡本質上是大外宣性質。會否能引起他國迴響仍有待觀察。

陸、小結

在美中對抗格局加劇以及新冠肺炎疫情衝擊下，有關「關鍵資訊基礎設施」的討論出現兩種趨勢。首先，衝突領域不斷變換戰場、延伸戰場，

19 Karen Yeung, “Coronavirus: Chinese President Xi Jinping proposes global QR code system to help free up travel,” *SCMP*, November 22, 2020, https://www.scmp.com/news/china/diplomacy/article/3110871/coronavirus-chinese-president-xi-jinping-proposes-global-qr.

有關攻擊手法的設想（同時也可能是實際上的手法）更是層出不窮，混合威脅與灰色地帶衝突不斷侵入社會領域，導致社會焦慮不安的心情瀰漫。5G 網路的建設與運作，使得供應鏈安全的資安議題更加被重視，也不斷擴大被審視的領域。這些討論反映出「關鍵資訊基礎設施」的「安全」與「安全化」是一個浮動、複雜因地制宜（situational）的概念。

此外，疫情影響下關鍵資訊基礎設施似也值得再重新定義範圍，這是因為大量數位資通訊手段被運用與取代原有的生活方式。如此，過去可能不被包含在關鍵基礎設施的項目將可能在新條件下被視為是重要設施，譬如手機應用程式、雲端資料庫，未來包括數位貨幣等。