

第十五章 中俄深化戰略合作後的數位威權與民主競逐

杜貞儀*

壹、前言

數位威權主義（digital authoritarianism）一般定義為利用數位及資通訊科技從事阻礙資訊的自由流通、鎮壓政治異議、監控公民、侵犯個人隱私、削弱人權和民主原則等一系列作為，並在國內甚至全球範圍進行惡意影響行動（malign influence operation）。藉由數位環境的虛擬網路空間以及實體設施層面，數位威權主義促使不重視個人自由的規範（illiberal norms）向外傳播，使威權主義的實踐不僅僅限於國境內，更以惡意行動直接影響自由、開放的民主社會，或使民主社會基於自身利益，不自覺採行限制個人自由的政策或措施，而對民主社會以及其注重人權、隱私等價值構成實際威脅。¹

中國與俄羅斯兩國屬數位威權的典型範例，例如中國的雙向「防火長城」，不但以封鎖境外網站、社群媒體平台以及新聞限制民眾接觸外界資訊，同時也使境外無法順利存取中國境內網站，控制訊息自由流通，並在數位科技支援下、對社會進行大規模的全面監控。² 中國後續制定與修訂的《國家情報法》、《反間諜法》，也明文規定電信與網路服務業者等有依法支持、協助政府相關工作的義務。俄羅斯的數位威權模式，除了監控

* 國防安全研究院網路安全與決策推演研究所助理研究員。

1 Doug Strub, “Brief for Congressional Affairs: Confronting the Rise of Digital Authoritarianism,” *The National Bureau of Asian Research*, April 8, 2023, <https://www.nbr.org/publication/confronting-the-rise-of-digital-authoritarianism/>.

2 John Leyden, “Exhaustive Study Puts China’s Infamous Great Firewall under the Microscope,” *The Daily Swig*, August 12, 2021, <https://portswigger.net/daily-swig/exhaustive-study-puts-chinas-infamous-great-firewall-under-the-microscope>.

網路流量以及社群媒體訊息外，亦立法要求網路服務商以及電信業者保存所有資料長達半年至3年，並提供政府存取權。

然而，在俄羅斯入侵烏克蘭後，歐美各國陸續對俄羅斯提出經濟制裁，使所屬企業陸續撤出，或關閉在俄羅斯境內的服務。中國則因提供俄羅斯重要軍民物資，而受到美國商務部的漸進式制裁施壓，對此兩國則以「全面深化戰略合作」抵禦制裁影響，但強化合作的後續如何落實，則牽涉從數位基礎建設到服務的不同層面，除官方政策外，亦需有實際的經濟效益才能從中受益，才能進一步支持其數位威權模式的優越論述。

本文將試圖分析中俄兩國深化戰略合作的數位科技與經濟層面，是否亦支持數位威權主義及其向外擴張，並在多邊國際組織持續推廣其治理模式。而印太區域面臨數位威權主義的威脅和挑戰，將如何與理念相近國家結盟，共同維護民主國家的制度、價值和規範。

貳、中俄深化戰略合作的數位科技與經濟層面

中國與俄羅斯雖然並非正式盟友，但兩國長期維持密切的「戰略夥伴關係」，而兩國間「無止境的友誼」，又因俄羅斯2022年2月入侵烏克蘭後、逐漸遭各國孤立而進一步深化。2023年3月，中國國家主席習近平與俄羅斯總統普欽在莫斯科會晤後，簽署全新的中俄聲明——《中華人民共和國和俄羅斯聯邦關於深化新時代全面戰略協作夥伴關係的聯合聲明》（以下簡稱《聲明》），視彼此為優先合作夥伴。除了重申對俄烏戰爭的立場外，《聲明》強調「各國自身歷史、文化、國情不同，都有自主選擇發展道路的權利」並反對「民主對抗威權」敘事架構、「外部勢力干涉內政」等。具體執法領域合作重點包括同意協商舉行公安、內務部部長年度會晤、加強防範「顏色革命」，打擊包括「東伊運」（東突厥斯坦獨立運動）在內的「三股勢力」（暴力恐怖勢力、民族分裂勢力和宗教極端勢力）、跨國有組織犯罪、經濟犯罪、毒品犯罪等。³ 這也顯示兩國以執

³ 〈中華人民共和國和俄羅斯聯邦關於深化新時代全面戰略協作夥伴關係的聯合聲明〉，《中華人民共和國外交部》，2023年3月22日，https://www.fmprc.gov.cn/web/gjhdq_676201/gj_676203/oz_678770/1206_679110/1207_679122/202303/t20230322_11046188.shtml。

法、反恐為由進行內部社會控制，仍是中俄兩國戰略合作的重要面向。

雖然在手段上，中國與俄羅斯同樣透過科技進行大規模社會監控強化對內控制，但兩者各自建構的數位威權主義模式，仍然同中存異。在具體落實層面，俄羅斯政府的願景與實際能力存在不小差距，以科技應用來觀察，中國以自主生產替代的方式扶植華為等國內設備廠商，但俄羅斯在基礎設施上大量採用歐美設備。例如俄羅斯首都莫斯科的數位基礎設施，主要使用歐美資通訊大廠的硬體設備，如網路設備的思科（Cisco）、伺服器系統的戴爾（Dell）以及惠普（HP）等；而作為社會控制主要手段的閉路監視器系統，影像分析核心則來自輝達（NVIDIA）以及其他美國供應商，中國供應商則提供硬碟、電源供應器等附屬設備。⁴

不過，俄羅斯入侵烏克蘭以及伴隨而來的歐美經濟制裁，也讓歐美設備商逐漸撤出俄羅斯，支援其數位威權的實體設施組成，以及後續如何維持、營運，可能仍會因此產生變化。在硬體設備部分，思科在2022年6月宣布撤出俄羅斯市場，同時摧毀價值18.6億盧布（相當於2,300萬美金）的設備與財產。⁵即使經濟制裁使思科必須先取得美國政府輸出許可，才能將網路設備出貨至俄羅斯，但根據《華爾街日報》記者比對關務資料顯示，在思科撤出俄羅斯將近1年後，未參與對俄制裁的中國與土耳其兩國，依然允許業者利用平行輸入的方式將遭制裁的商品出口至俄羅斯，從俄羅斯境內主要銷售管道亦有相當存量的思科網路設備來看，短期內應仍足以供應俄羅斯境內使用。⁶

另有觀察認為，中國的華為等公司，可能利用思科等歐美大廠離開俄羅斯市場的機會，搶占相關資通訊設備市場。⁷但已遭歐美制裁多年的華

4 Leonid Kovachich and Andrei Kolesnikov, "Digital Authoritarianism With Russian Characteristics?" *Carnegie Endowment for International Peace*, April 21, 2021, <https://carnegiemoscow.org/2021/04/21/digital-authoritarianism-with-russian-characteristics-pub-84346>.

5 "Cisco Moscow Trashed Offices as It Quit Putin's Putrid Pariah State," *The Register*, April 6, 2023, https://www.theregister.com/2023/04/06/cisco_destroyed_spares_in_russia/.

6 Alistair MacDonald and Kate Vtorygina, "Inside the Gray Market Keeping Cisco Tech in Stock in Russia," *The Wall Street Journal*, February 14, 2023, <https://www.wsj.com/articles/inside-the-gray-market-keeping-cisco-tech-in-stock-in-russia-23b60391>.

為，並未能善加利用此機會，反而逐步停止供貨至俄羅斯。自 2019 年以來，華為已是俄羅斯境內行動通訊基地台供應商，此舉引起俄羅斯政府的關切。不過，即使產品從俄羅斯市場自主下架，華為依舊利用歐美公司撤出俄羅斯的機會，大舉吸納人才至設於俄羅斯境內的研發部門。⁸ 除華為外，來自深圳，以防火牆為主力的深信服科技（Sangfor Technology）產品在俄羅斯依舊經由代理商銷售，不受制裁影響，而且持續資助雙邊資訊安全學術研究交流與人才培育，也是兩國繼續深化合作的具體事例。⁹

此外，與《聲明》同時簽署的《關於 2030 年前中俄經濟合作重點方向發展規劃的聯合聲明》中，亦指出兩國雙邊經濟合作的八大重點方向，其中將「擴大貿易規模，優化貿易結構，發展電子商務及其他創新合作模式。穩步推動雙邊投資合作高質量發展，深化數字經濟、綠色可持續發展領域合作，營造良好經商環境，相互提升貿易投資便利化水平」置於首位，顯示數位經濟仍是兩國經濟合作的重點。

雖然中共政府自 2021 年開始以「反壟斷」為由打擊私人企業投資案，一度重創阿里巴巴、騰訊等網路巨頭，然而以阿里巴巴旗下的國際跨境電子商務平台——「全球速賣通」（AliExpress）為例，其國際電商業務仍持續增長，中俄合作在俄羅斯入侵烏克蘭後依然相當穩固。阿里巴巴集團早在 2010 年即開設「全球速賣通俄羅斯」（AliExpress Russia），是俄羅斯境內最大的電子商務平台，並在 2019 年為因應俄羅斯政府的外資限制，改由與行動通訊業者 MegaFon、俄羅斯直接投資基金（Russian Direct Investment Fund, RDIF），以及俄羅斯網路公司 Mail.ru Group（目前已更

7 Iain Morris, “Cisco Exit Will Drive Russia Further Into China’s Embrace,” *LightReading*, June 24, 2022, <https://www.lightreading.com/routingswitching/cisco-exit-will-drive-russia-further-into-chinas-embrace/d/d-id/778519>.

8 Vita Spivak, “How Sanctions Have Changed the Face of Chinese Companies in Russia,” *The Moscow Times*, May 29, 2023, <https://www.themoscowtimes.com/2023/05/29/how-sanctions-have-changed-the-face-of-chinese-companies-in-russia-a81302>.

9 深信服科技在俄羅斯與獨立國家國協成員國的代理商為 Factor Group（Фактор груп），其官方網站為 <https://www.fgts.ru/collection/sangfor>；〈聚焦國際化數字人才培養 | 俄羅斯名校葉列茨基國立大學參訪深信服科技〉，《深信服科技》，2023 年 8 月 1 日，<https://www.sangfor.com.cn/news/886b7936cc6343e99257336836894378>。

名為 VK Group) 成立合資公司共同持有，凸顯其與俄羅斯企業已建立深厚的戰略合作關係。¹⁰ 即使在俄烏戰爭初期，「全球速賣通俄羅斯」曾因歐美經濟制裁而傳出裁員消息，但從 2023 年至今發展觀察，阿里巴巴顯然並無任何撤出俄羅斯市場的規劃。¹¹

近年來歐美國家逐漸對「全球速賣通」此類中國跨境電商平台所伴隨的跨境資料傳輸風險，與其銷售仿冒、盜版商品的侵害智慧財產權行為有所警覺。例如，荷蘭政府 2023 年 7 月宣布禁止公務手機安裝「全球速賣通」、「微信」等手機應用程式，美國白宮所屬的貿易代表辦公室 (U.S. Trade Representative Office) 在 1 月發布的年度報告中，再度將「全球速賣通」、「微信電商平台」等列入仿冒及盜版商品銷售平台的「惡名昭彰市場」(Notorious Markets) 黑名單。¹² 烏克蘭國家預防腐敗局 (National Agency on Corruption Prevention) 8 月 17 日發表聲明，將阿里巴巴列入「戰爭國際資助者」的名單，同時引用《路透社》(Reuters) 4 月的調查報導，指控中國公司自烏克蘭的俄羅斯占領區進口銅錠再加工，成品則在阿里巴巴的電商平台銷售。該局並在聲明中表示，阿里巴巴針對旗下電商平台進行言論審查，封鎖「全球速賣通」上發表有關俄烏戰爭評論的烏克蘭用戶。¹³ 這也凸顯中國跨境電商平台除了以往討論的跨境資料傳輸疑慮外，更可能會配合中共政府政策執行言論控制，延伸其影響範圍到境外。

¹⁰ Jing Yang, "Alibaba's Russia Venture Puts Chinese E-Commerce Giant in Awkward Spot," *The Wall Street Journal*, March 24, 2022, <https://www.wsj.com/articles/alibabas-russia-venture-puts-chinese-e-commerce-giant-in-awkward-spot-11648123931>.

¹¹ John Power, "A Year Into Ukraine War, Asia's Big Brands Sit Out Russia Boycott," *Aljazeera*, February 24, 2023, <https://www.aljazeera.com/economy/2023/2/24/asian-brands-sit-out-russia-boycotts>.

¹² "Dutch Government Bans Officials from Using Chinese Apps AliExpress, WeChat on Work Phone," *NL#TIMES*, July 14, 2023, <https://nltimes.nl/2023/07/14/dutch-government-bans-officials-using-chinese-apps-aliexpress-wechat-work-phone/>; "USTR Releases 2022 Review of Notorious Markets for Counterfeiting and Piracy," *Office of the United States Trade Representative*, January 31, 2023, <https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/january/ustr-releases-2022-review-notorious-markets-counterfeiting-and-piracy>.

¹³ "The NACP Included the Owner of AliExpress in the List of International Sponsors of the War," *National Agency on Corruption Prevention*, August 17, 2023, <https://nazk.gov.ua/en/news/the-nacp-included-the-owner-of-aliexpress-in-the-list-of-international-sponsors-of-the-war/>.

簡而言之，從硬體設備到數位經濟，中俄兩國在俄烏戰爭後的持續深化戰略合作，短期內仍能維持，甚至進一步鞏固雙方的數位威權治理模式。而目前歐美的經濟制裁，對於數位經濟發展的影響亦相當有限。不僅如此，代表數位經濟蓬勃發展的跨境電子商務平台，也可能已成為數位威權向外擴張的一個管道。

參、網路治理角力、數位威權主義擴張與印太區域安全

從更上層的網路治理政策觀察，作為數位威權主義的典型，中俄兩國均強調網路治理必須遵守主權原則，即每個國家都有權控制自己的網路空間，包括監管國內網路和對外限制外國網路公司在境內活動與營運，並主張國際網路治理政策與發展方向，應由聯合國架構的多邊國際組織主導，並應遵守包括《聯合國憲章》和其他相關條約現有的國際法和規則，而忽略各國仍有大量的網路實體基礎設施仍為私有，並非全數為國家所管轄，必須由多方利益攸關者（multi-stakeholder）共同參與。然而，對內強化網路空間監管，以此打擊網路犯罪及防止恐怖主義擴張的論述框架，對印太地區各國仍十分具有吸引力，因此，以此議題爭取區域國家支持，仍有助於中俄兩國在多邊國際組織的相關政策討論取得更大影響力，並藉此推展其數位威權模式。

舉例來說，由俄羅斯、中國、北韓等國 2019 年共同在聯合國大會提案決議設立新的國際網際網路犯罪公約，並成立委員會（即 Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes）進行討論，但直到 9 月 1 日結束第六輪討論後，就公約實際適用範圍以及網路犯罪定義依舊無法達成共識。主要的癥結點在於中俄希望將所有涉及使用資通訊科技的犯罪行為，都納入公約適用範圍，中國甚至提案建議重新定義網路犯罪，並將「在網路上散布虛假訊息」也納入，而有限縮言論自由的疑慮。越南和中國更表示希望在草案中完全排除人權有關的字眼，或限縮至僅適用於已簽訂其他人權公約的國家。實質

上來看，聯合國對於網際網路犯罪公約的一系列討論，已經成為民主與威權國家競爭在數位時代對網路、科技以及人權未來願景的外交戰。¹⁴

以印太區域而言，跨域數位經濟、基礎建設投資，以及其可能伴隨的外國經濟干預與數位威權主義擴張，依舊是未來觀察的重點。中俄兩國深化戰略合作，無論是資源還是產業面的投入，在非洲以及中東地區已有相輔相成的前例，即使現階段俄羅斯在此區域的經貿往來仍以能源、原物料出口為主，但仍有機會持續以中俄合作達成各自維持強權、搶奪話語權及推動「多極」格局的共同戰略目標。¹⁵相較於歐美對俄羅斯、中國的經濟制裁與公開譴責，東協國家如越南、馬來西亞以及印尼，仍因以往歷史因素，避免公開譴責俄羅斯的入侵行徑，或有主流輿論對俄羅斯表示同情的狀況，如同走鋼索般維持平衡。¹⁶

若進一步觀察跨境數位經濟在東協國家的發展，主要電子商務平台不

¹⁴ Rishi Iyengar, Robbie Gramer, and Anusha Rathi, "Russia Is Commandeering the U.N. Cybercrime Treaty," *Foreign Policy*, August 31, 2023, <https://foreignpolicy.com/2023/08/31/united-nations-russia-china-cybercrime-treaty/>; Jessica Lyons Hardcastle, "UN Cybercrime Treaty Risks Becoming A 'Global Surveillance Pact'," *The Register*, August 24, 2023, https://www.theregister.com/2023/08/24/un_cybercrime_treaty/; Alexander Martin, "China Proposes UN Treaty Criminalizes 'Dissemination of False Information'," *The Record*, January 17, 2023, <https://therecord.media/china-proposes-un-treaty-criminalizing-dissemination-of-false-information>; Jonathan Greig, "Global Cybercrime Treaty Could be 'Disastrous for Human Rights,' NGOs Warn," *The Record*, August 28, 2023, <https://therecord.media/global-cybercrime-treaty-disastrous-rights-orgs>.

¹⁵ Oleg Yanovsky, "Russia Looks East to Trade," *EASTASIAFORUM*, May 9, 2023, <https://www.eastasiaforum.org/2023/05/09/russia-looks-east-to-trade/>; Mercy A. Kuo, "China-Russia Cooperation in Africa and the Middle East," *The Diplomat*, April 3, 2023, <https://thediplomat.com/2023/04/china-russia-cooperation-in-africa-and-the-middle-east/>.

¹⁶ Benjamin Y.H. Loh and Munira Mustaffa, "Social Media Discourse in Malaysia on the Russia-Ukraine Conflict: Rationales for Pro-Russia Sentiments," *Fulcrum*, April 27, 2022, <https://fulcrum.sg/social-media-discourse-in-malaysia-on-the-russia-ukraine-conflict-rationales-for-pro-russia-sentiments/>; Ann Marie Murphy, "Ukraine War Highlights Differences between Indonesian and US Foreign Policy Frameworks," *EASTASIAFORUM*, August 5, 2022, <https://www.eastasiaforum.org/2022/08/05/ukraine-war-highlights-differences-between-indonesian-and-u-s-foreign-policy-frameworks/>; Maria Siow, "Asia's Russia-West Balancing Act on Show with Push for Peace in Ukraine from Indonesia's Prabowo," *South China Morning Post*, June 10, 2023, <https://www.scmp.com/week-asia/politics/article/3223563/asias-russia-west-balancing-act-show-push-peace-ukraine-indonesias-prabowo>; Olga Dror, "Weaponising Ho Chi Minh in Vietnamese Discourse on the War in Ukraine," *Fulcrum*, June 17, 2022, <https://fulcrum.sg/weaponising-ho-chi-minh-in-vietnamese-discourse-on-the-war-in-ukraine/>.

僅掌握有關用戶個人資料、消費行為等所有資訊，使「大者恆大」。即使2023年8月發布的《東協—中國強化數位商務合作倡議》（*ASEAN-China Initiative on Enhancing Cooperation on E-Commerce*）中，強調雙邊電商平台合作，以及由中國分享其電子商務政策、監管作法、電子簽章等中國居領先地位經驗，以共同與東協成員國建構相對應的能力，¹⁷但實際上，中國跨境電商已幾乎完全取得主導權，不斷加大在東協國家的投資，並快速擴張版圖。如阿里巴巴於2023年7月藉由新加坡分公司對旗下之東南亞電商品牌「來贊達」（Lazada）增資8.45億美金，以與「蝦皮」（Shopee）和TikTok商店競爭；而拚多多旗下的跨境電商平台Temu，也以菲律賓作為進軍東南亞市場的跳板等。¹⁸未來亦不排除將在東南亞地區發生類似烏克蘭用戶遭「全球速賣通」封鎖，或以服務約定條款約束用戶在平台的行為，促使用戶針對發表言論進行自我審查等情況。

而在數位基礎建設以及政策能力建構的部分，澳洲、日本與美國等國合作，持續由數位基礎建設拓展與東協及太平洋島嶼國家的合作關係，以對抗中國在東協及太平洋島嶼國家的經濟與安全影響力。東協國家的數位基礎建設合作以5G網路及網路安全為主，如日本與美國的5G網路倡議，於2022年在菲律賓開設「亞洲開放性無線接入網路（Open Radio Access Network, O-RAN）學院」（Asia O-RAN Academy）。¹⁹東協各國在5G網路以及後續智慧城市計畫推動與建設的積極程度不一。印尼即將於2024年8月17日落成的新首都努山塔拉（Nusantara）吸引大量中國企業投資，並有數項採用中國的智慧城市解決方案的計畫正在進

¹⁷ “ASEAN-China Initiative on Enhancing Cooperation on E-Commerce,” *ASEAN*, August 24, 2023, https://asean.org/wp-content/uploads/2023/08/ASEAN_China_ECommerce_Initiative_Adopted.pdf.

¹⁸ Olivia Poh, “Alibaba Injects \$845 Million Into Southeast Asia Unit Lazada,” *Bloomberg*, July 19, 2023, <https://www.bloomberg.com/news/articles/2023-07-19/alibaba-injects-845-million-into-southeast-asia-unit-lazada>; Tracy Qu, “PDD-owned Temu Enters the Philippines to Heat up Competition in Southeast Asia’s e-commerce Market Against Alibaba’s Lazada and TikTok Shop,” *South China Morning Post*, August 28, 2023, <https://www.scmp.com/tech/big-tech/article/3232584/pdd-owned-temu-enters-philippines-heat-competition-southeast-asias-e-commerce-market-against>.

¹⁹ Mayumi Hirose, “U.S.-Japan 5G Initiative Launches First Academy in Philippines,” *Nikkei Asia*, June 30, 2022, <https://asia.nikkei.com/Spotlight/5G-networks/U.S.-Japan-5G-initiative-launches-first-academy-in-Philippines>.

行；相較之下，馬來西亞則在 5G 網路建設推動強調技術中立（technology neutral），即使初期建構 5G 網路採用瑞典易立信（Ericsson）公司系統，但對其他中國設備如海康衛視（Hikvision）採取較為開放的態度，不願在美、中科技戰之間選邊站。²⁰

至於太平洋島嶼國家，由於對外通訊連結的主要管道為海底光纜，不僅網路普及率有待提升，數位基礎建設亦相當脆弱，容易受天然災害影響中斷，因此強化數位基礎建設是此區合作的重點所在。2021 年建置完成，連結印尼、巴布亞紐幾內亞各島與索羅門群島的「極樂島海底光纜網路」（Kumul Submarine Cable Network），由華為海洋建置，即有超過八成建置資金來自中國進出口銀行的貸款；因 2022 年 9 月地震導致的巴布亞紐幾內亞海纜損壞，在 2023 年 3 月揭露其後續維修工作同樣是由中國出資援助，並由華為海洋提供技術與材料支援。²¹ 澳洲、日本與美國為強化與太平洋島嶼各國合作，也於 2023 年 6 月 7 日共同簽署價值 9,500 萬美元的海底光纜計畫同意書，此計畫預計建設全長約 2,250 公里（1,400 英里）的海底光纜，連接密克羅尼西亞聯邦的科斯雷州、吉里巴斯的塔拉瓦州和瑙魯，以及位於密克羅尼西亞波納佩的現有光纜登陸點。²²

網路安全與政策亦仍為澳洲、日本等國與中國持續角力的場域。澳洲政府自 2016 年已設立針對東協及太平洋島嶼各國的「網路合作計畫」，支援開放、自由及安全的網際網路，藉由保護國家安全與強化國際穩定支援經濟成長與持續發展，並在 2021 年進一步擴大包含關鍵科技合作。²³ 但此依舊面對來自中國的挑戰，如索羅門群島政府 2023 年 7 月與中國在

²⁰ Muhammad Zulfikar Rakhmat and Yeta Purnama, “Indonesia-China: A Smart City Can Make for Clever Politics,” *The Interpreter*, April 4, 2023, <https://www.lowyinstitute.org/the-interpreter/indonesia-china-smart-city-can-make-clever-politics>; Ilaria Carrozza and Giacomo Bruni, “China’s Digital Silk Road and Malaysia’s Technological Neutrality,” *The Diplomat*, August 22, 2023, <https://thediplomat.com/2023/08/chinas-digital-silk-road-and-malaysias-technological-neutrality/>.

²¹ Donald Nangoi, “China Assists PNG to Repair Submarine Cables,” *Papua New Guinea Post-Courier*, March 8, 2023, <https://www.postcourier.com.pg/china-assists-png-to-repair-submarine-cables/>.

²² Mari Yamaguichi, “Japan, Australia, US to Fund Undersea Cable Connection in Micronesia to Counter China’s Influence,” *AP News*, June 7, 2023, <https://apnews.com/article/micronesia-japan-australia-us-cable-china-155cd017a5a3045bf5078e5df25f17d9>.

²³ “Cyber and Critical Technology Cooperation Program,” *Australian Government*, <https://www.internationalcybertech.gov.au/our-work/capacity-building>.

北京政府簽署警務合作協議，預計增強索國現有 1,500 名警官在網路安全和社區警務方面的能力，並且否認澳洲、美國、紐西蘭等國認為此協議「對太平洋地區和平構成威脅」的說法。²⁴ 日本政府則在 2023 年 8 月向媒體透露，預計將在 2024 年編列預算在印太地區強化網路攻擊訊息分享與部署反制作為，以因應來自俄羅斯、中國以及北韓的威脅。這項計畫的重點在於強化太平洋島國的應變能力，具體支援將包括設備建置以及共同訓練的能力建構，並由世界銀行提供人力資源經費，頗有與中國分庭抗禮的意味。²⁵

肆、小結

從數位科技及經濟層面來看，俄烏戰爭後的中俄深化戰略合作，兩國在技術與資源共享下，各自短期內仍能維持，甚至進一步鞏固雙方的數位威權治理模式；而在多邊國際組織參與上，中俄仍將持續透過制定新網路犯罪公約以及參與新興科技標準制定過程，推廣其數位威權模式。中國更藉由跨境電商與數位經濟的蓬勃發展，將其影響力向外延伸至東協國家，歐美經濟制裁對此的影響亦十分有限，未來「中國模式」應會持續成為東協國家數位經濟發展的主要參考對象。但在數位基礎建設以及延伸的網路安全政策上，美國、日本、澳洲等理念相近國家，為與中國抗衡而在印太區域共同推出的各項合作計畫，即使在太平洋島國碰到部分挫折，後續仍有持續爭取並擴大數位政策影響力的空間。未來印太區域面臨此數位威權主義的威脅和挑戰，仍需透過各國、公私部門及不同面向的全面合作以因應。

²⁴ Kirsty Needham, "Australia Raises Concern over Solomon Islands Policing Plan with China's Top Diplomat," *Reuters*, July 14, 2023, <https://www.voanews.com/a/solomon-islands-says-chinese-police-to-assist-cyber-community-security/7180542.html>.

²⁵ Rieko Miki, "Japan to Set up Cyberdefense Network that Includes Pacific Islands," *Nikkei Asia*, August 13, 2023, <https://asia.nikkei.com/Politics/International-relations/Japan-to-set-up-cyberdefense-network-that-includes-Pacific-islands>.