中國認知領域作戰模型初探：以 2020 臺灣選舉為例

沈伯洋

（臺北大學犯罪學研究所助理教授）

摘　要

為深入研究中國認知領域作戰之意涵，本研究使用網路攻擊常見的鑽石模型，試圖描繪出資訊作戰「發動者」，以及其「攻擊模式」。首先，本研究整理 2019 年 5 月至 2020 年 1 月的數據約 32 萬筆，列出 2020 臺灣大選期間資訊的異常現象，並比照現有研究及訪談資料，找尋可能的認知領域作戰痕跡。根據本研究整理，認知領域作戰有四種完全不同的模式：外宣模式、粉紅模式、農場模式，以及協力模式。面對四種不同型態的威脅，臺灣應立即針對各威脅建立防禦機制與法制，以抵擋中國的認知作戰。

關鍵詞：資訊作戰、認知領域作戰、鑽石模型、進攻模式、統戰

壹、前言

根據瑞典哥德堡大學政治系多元民主計畫的數位社會研究資料庫(Varieties of Democracy Institute)顯示，臺灣是全世界受「境外爭議訊息」攻擊的第一名。[1] 然而，此命題有四項不得不解決的問題：第

1. Degital Society Project, "Foreign Government Dissemination of False Information," April 9, 2019, *Degital Society Project*, <http://digitalsocietyproject.org/foreign-intervention-on-social-media/>.

一，境外訊息的進攻來源在哪裡？第二，爭議訊息如何擴散？第三，爭議訊息的內容是什麼？第四，誰才是被爭議訊息影響的受害者？若此四項問題無法解決，最後只能流於把與自己立場不同的假新聞視作爭議訊息，則無法聚焦並解決此一現象。受限於篇幅，本文僅先嘗試回答前兩個問題，關於進攻內容及受害者的分析，將留待日後發表。

本文於第二節先介紹現有的資訊作戰與認知領域作戰理論，並使用 2020 大選資料在第三節做進一步驗證。除了將臺灣的數據異常指出之外，並於第四節探討是否可將異常現象歸責於中國，並描繪四種不同進攻模型的圖象，試圖回答上述「發動者」與「進攻方式」的提問。作為結論，本文於第五節提出根據此模型的截斷(disturbance)與標示(labeling)方案，目標是在藉由一定程度的資料探勘或截斷嘗試，[2] 還給受害者乾淨的訊息判斷空間，同時保障言論自由。[3]

貳、文獻回顧與分析架構

一、混合戰、資訊作戰與認知領域作戰

混合戰為資訊作戰的上位概念，而資訊作戰為認知領域作戰的上位概念。本文將依次介紹，進而選擇認知領域作戰的理論基礎。

---

2. 資料探勘可見 Kai Shu, Amy Sliva, Suhang Wang, Jiliang Tang, & Huan Liu, “Fake news detection on social media: A data mining perspective,” *ACM SIGKDD Explorations Newsletter*, Vol. 19, No. 1, September 2017, pp. 22-36；截斷嘗試可見 Kai Shu, Suhang Wang, & Huan Liu, “Beyond news contents: The role of social context for fake news detection,” paper presented at the Proceedings of the Twelfth ACM International Conference on Web Search and Data Mining (Melbourne: WSDM, February 11-12, 2019), pp. 312-320。

3. International Commission of Jurists, “Dictating the Internet: Curtailing Free Expression, Opinion and Information Online in Southeast Asia,” April 6, 2020, Accessed pp. 5-6, *International Commission of Jurists*, <https://www.icj.org/southeast-asia-icj-launches-report-on-increasing-restrictions-on-online-speech/>.

斯里普琴科(В.И.Слипченко)於 2002 年所提出的第六代戰爭理論，即為後人所熟悉的「混合戰」(Hybrid warfare)。[4] 前美國陸軍參謀總長凱西(George W. Casey)亦提出「傳統，非正規，恐怖和犯罪能力的各種動態組合」的定義。[5] 赫爾辛基的反混合戰中心對此的定義則為「故意針對民主國家或機構系統性的弱點作攻擊，並使用政治、經濟、軍事、公民運動或資訊等手段，混淆戰爭與和平的偵察與歸因界線」，最後再「攻擊不同層級（國家、區域、機構等）的認知體系，產生錯誤判斷。」[6] 其中，所謂「資訊的手段」即為資訊作戰的原始型態。而「認知體系攻擊」即為本文欲探討的認知領域作戰。

在前述定義之下，混合戰包含外交作戰、軍事作戰、經濟作戰、貿易作戰、金融作戰與資訊作戰，因此資訊作戰乃混合戰之一環；而在資訊作戰當中，又包含網路間諜活動、竊取技術、攻擊基礎設施、數位極權輸出及認知領域攻擊等等。因此，認知領域作戰為資訊作戰的一種型態。[7] 近年來有其他類似對於此類作戰的研究但卻使用不同語詞，如影響作戰(influence operation)、認知戰(cognitive warfare)或者銳實力(sharp power)等；影響作戰的定義常與認知戰一語交替使用，

4. Vladimir Slipchenko, *Voina Budushchego* (Moscow: Moskovskii Obshchestvennyi Nauchnyi Fond, 1999), pp. 23-50.
5. George W. Casey Jr., "The army of the 21st century," *Army Magazine*, Vol. 59, No. 10, October 2009, pp. 25-40.
6. Center of Excellence, "Hybrid Threats," April 6, 2020, Accessed, *Hybrid CoE*, <https://www.hybridcoe.fi/>.
7. Christopher S. Chivvis, *Understanding Russian Hybrid Warfare* (California: Rand Corporation, 2017), pp. 3-4; Heidi Reisinger & Alexandr Golts, "Russia's hybrid warfare," *NATO Defense College*, Vol. 105, November 2014, p. 4; Mario Silvino Brazzoli, "Future prospects of information warfare and particularly psychological operations," in Len Le Roux ed., *South African Army Vision 2020* (Pretoria: D&V, 2007), pp. 217-232.

但皆為混合戰的一環；而銳實力的概念較偏向社會學解釋現象所用，難以直接與軍事概念作搭配，故本文仍舊使用傳統軍事之混合戰→資訊作戰→認知領域作戰三層次的概念來作為本文的理論基礎。

論者有謂在分析中國攻擊時，應使用中國的分析架構，較能理解中國攻擊。在中國的語境下，較為相近的則是「超限戰」或「三戰」（法律戰、心戰與輿論戰）。[8] 超限戰概念與混合戰相去不遠，而三戰的概念皆可包含於資訊作戰當中（中國稱之為信息戰）；早期中國內部文件所指出的「電子作戰、網路作戰、心理作戰、基礎設施作戰」，並再細分為進攻與防守的面向，共計八種，[9] 皆與資訊作戰的概念相去不遠。然而，這種分類方式又忽略了中國近幾年來的數位極權（如華為的輸出），以及海外個資蒐集（輸入），反而形成理解的限制，因此本文仍舊以原本的「認知領域作戰」當作「資訊作戰」之一環來理解，進而找出中國攻擊的模式。

關於認知領域作戰的定義。西方較為傳統的定義為「利用媒體、網路等資訊改變人們之意識、認知、作為或決策」；[10] 中國在網路電子戰中亦有類似說法，[11] 包含「破壞敵對國家的政治、經濟、軍事，乃至整個社會的資訊基礎設施及其運轉……運用心理戰和戰略欺騙等手段，動搖軍心、民心和政府信念」。近期較受到關注的為美國國家民主基金會之定義：「利用爭議訊息，破壞社會既有網絡、並加深原本

8. 喬良、王湘穗，《超限戰：兩個空軍大校對全球化時代戰爭與戰法的想定》（北京：解放軍文藝出版社，1999 年），頁 156-157、205-213。
9. 王高成，〈中共不對稱作戰戰略與臺灣安全〉，《全球政治評論》，第 6 期，2004 年 4 月，頁 19-33；林中斌，《核霸：透視跨世紀中共戰略武力》（臺北：臺灣學生書局，1999 年），頁 37-41。
10. Martin C. Libicki, *What is Information Warfare*? (Washington, D.C.: National Defense University Press, 1995), pp. 35-45.
11. 蔡輝榮、吳宗禮，〈面對資訊作戰之準備、發展與落實〉，《資通安全專論》，第 T96019 期，2007 年 1 月，頁 16。

之對立」。[12] 無論是哪一種說法，可知認知領域攻擊的要素有二：一為利用爭議訊息做為管道，二為混淆或破壞敵方的認知，並造成對立。過往相關文獻多是探討集權政府中的網軍對內為維穩所製造的假象，[13] 但近年來的發展已漸漸進入了這些網路軍隊對敵作戰的研究。

俄羅斯對美國 2016 年的選舉即示範了上述的認知領域攻擊。[14] 俄

12. Juan Pablo Cardenal, et al., *Sharp Power: Rising Authoritarian Influence* (Washington, D.C.: National Endowment for Democracy, 2017), pp. 103, 118.
13. Kevin Munger, Rich Bonneau, John T. Jost, Jonathan Nagler, & Joshua Tucker, "Elites Tweet to get Feet off the Streets : Measuring Elite Reaction to Protest Using Social Media," *Political Science Research and Methods*, Vol. 7, No. 4, October 2019, pp. 815-834; Sergey Sanovich, Denis Stukal, & Joshua Tucker, "Turning the Virtual Tables: Government Strategies for Addressing Online Opposition with an Application to Russia," *Comparative Politics*, Vol. 50, No.3, April 2018, pp. 435-82; Blake Miller, "Automated detection of Chinese government astroturfers using network and social metadata," April 21, 2016, Accessed, *SSRN*, <https://papers.ssrn.com/sol3/papers.cfm? abstract_id=2738325>; Gary King, Jennifer Pan, & Margaret E. Robert, "How Censorship in China Allows Government Criticism but Silences Collective Expression," *American Political Science Review*, Vol. 107, No. 2, May 2013, pp. 326-343.
14. Christopher A. Bail, Brian Guay, Emily Maloney, Aidan Combs, D. Sunshine Hillygus, Friedolin Merhout, Deen Freelon, & Alexander Volfovsky, "Assessing the Russian Internet Research Agency's impact on the political attitudes and behaviors of American Twitter users in late 2017," *Proceedings of the National Academy of Sciences*, Vol. 117, No. 1, January 2020, pp. 243-250; National Intelligence Council, "Assessing Russian activities and intentions in recent US elections," January 6, 2017, *Director of National Intelligence*, <https://www.dni.gov/files/documents/ICA_2017_01.pdf>; Renee DiResta & Shelby Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019* (Stanford: Internet Observatory, 2019), pp.

羅斯網際網路研究中心(Internet Research Agency, IRA)透過創造虛假專頁的方式在臉書(Facebook)、IG (Instagram)，以及推特(Twitter)針對爭議議題散布文章。針對種族的敏感性問題，IRA 創建非裔美國人專頁，以受到歧視等論述之文章與影片吸引其注意，並在信任節點之後，以其喜好分受眾，[15]再投其所好地於選前投放爭議訊息（含假新聞但不限於假新聞），而最終非裔美國人投票率顯著下降。[16]

同樣的情形在臺灣也出現：例如從 2017 年至 2018 年，位於中國秦皇島市的無為科技公司，即以臉書蒐集個人資料，並大量製造爭議訊息於「歡享網」，其同時於臉書對臺灣建立粉專，同步歡享網的爭議訊息。而爭議訊息不是只有在境外，臺灣境內亦有可能大量製造爭議訊息，如內容農場「密訊」，以及新媒體「芋傳媒」等，都可能形

7-9; Andrew Guess, Brendan Nyhan, & Jason Reifler, "Selective exposure to misinformation: Evidence from the consumption of fake news during the 2016 US presidential campaign," *European Research Council*, Vol. 9, No. 3, January 2018, pp. 1-10.

15. Ahmer Arif, Leo Graiden Stewart, & Kate Starbird, "Acting the part: Examining information operations within #BlackLivesMatter discourse," *Proceedings of the ACM on Human-Computer Interaction*, Vol. 2, Issue CSCW, November 2018, p. 20; Leo G. Stewart, Ahmer Arif, & Kate Starbird, "Examining trolls and polarization with a retweet network," paper presented at the Proc. ACM WSDM, Workshop on Misinformation and Misbehavior Mining on the Web (Los Angeles: ACM, February 9, 2018).

16. Renee DiResta, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, & Ben Johnson, *The Tactics & Tropes of the Internet Research Agency* (Annapolis: US New Knowledge 2019), pp. 7-10; Andrew Guess, Benjamin Lyons, Jacob M. Montgomery, Brendan Nyhan, & Jason Reifler, "Fake news, Facebook ads, and misperceptions: Assessing information quality in the 2018 US midterm election campaign," February 2018, pp. 16-21, *Dartmouth College*, <https://www.dartmouth.edu/~nyhan/fake-news-2018.pdf>.

成爭議訊息散布的溫床。而據研究指出，此類訊息的散布，可比正常訊息快達數倍，[17] 造成莫大傷害。

由於民主國家有其多元開放性，其內部意見衝突反而容易形成認知領域作戰的溫床。[18] 當然，混淆大眾認知體系的發動者，並不限於境外勢力，[19] 大公司利用個資和分群投放不同的廣告，早已成為日常生活的一部分，[20] 而這種技術若被應用在影響投票行為之上，由於此攻擊在民主機制之下隱而不顯，[21] 加上人民對認知領域攻擊的概念並不熟悉，

17. David M. J. Lazer, et al., "The science of fake news," *Science*, Vol. 359, No. 6380, March 2018, pp. 1094-1096; Zilong Zhao, et al., "Fake news propagate differently from real news even at early stages of spreading," April 16, 2019, *Cornell University arXiv*, <https://arxiv.org/abs/1803.03443>.
18. Vidya Narayanan, Vlad Barash, John Kelly, Bence Kollanyi, Lisa-Maria Neudert, & Philip N. Howard, "Polarization, partisanship and junk news consumption over social media during the 2018 US Midterm Elections," April 23, 2020, Accessed, *Cornell University arXiv*, <https://arxiv.org/abs/1803.01845>; J. B. Vilmer, Alexandre Escorcia, Marine Guillaume, & Janaina Herrera, "Information manipulation: A challenge for our democracies," August 2018, Accessed, *France Dipolomay*, <https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf>.
19. Claire Wardle & Hossein Derakhshan, "Information Disorder: Toward an interdisciplinary framework for research and policy making," *Council of Europe Report*, Vol. 27, September 2017, pp. 29-38.
20. Robert Epstein, "Why Google Poses a Serious Threat to Democracy, and How to End That Threat," April 6, 2020, Accessed, *Mercatornet*, <https://mercatornet.com/why-google-poses-a-serious-threat-to-democracy-and-how-to-end-that-threat/24598/>.
21. Insikt Group, "Beyond Hybrid War: How China Exploits Social Media to Sway American Opinion," April 23, 2020, Accessed, *Recorded Future*, <https://www.recordedfuture.com/china-social-media-operations/>; Peter Pomerantsev & Michael Weiss, *The Menace of Unreality: How the Kremlin*

並不會使人們有所警惕；[22]加上現今政府多與公司合作，將造成更大的威脅。

二、新鑽石模型的提出

在以上的攻擊架構中，有所謂的發動者（如國家與公司）、擴大訊息散布者（如網站與粉專），以及終端的受害者。過往多有學者探討早期中國信息作戰的理論基礎，[23]但必須進一步追問，該如何「類型化」、「理論化」認知領域攻擊？

本文認為，由於認知領域作戰為資訊作戰的一環，因此不妨回過頭去參考一般資訊作戰的理論基礎。比如說，早期資訊作戰強調駭客作戰，而駭客的網路作戰形式即可做為參考指標：如與網路狙殺鏈(Cyber-Kill Chain)密切相關的鑽石模型(Diamond Model)中，即將網路駭客攻擊分成四個面向：發動者(Adversary)、基礎設施(Infrastructure)、

Weaponizes Information, Culture and Money (New York: Institute of Modern Russia, 2013), pp. 14-24; Melanie Scheidt, "The European Union versus External Disinformation Campaigns in the Midst of Information Warfare: Ready for the Battle?" April 6, 2020, Accessed, *University of Pittsburgh*, <http://aei.pitt.edu/100447/>.

22. Murat Caliskan, *Modern Political Warfare: Current Practices and Possible Responses* (California: Taylor & Francis, 2018), pp. 255-272; Martin Svárovský, Jakub Janda, Veronika Víchová, Joey Gurney, & Sami Kröger, "Handbook on Countering Russian and Chinese Interference in Europe," April 23, 2020, Accessed, *European Values*, <https://www.europeanvalues.net/vyzkum/handbook-on-countering-russian-and-chinese-interference-in-europe/>.

23. 沈偉光，《新戰爭論》（杭州：浙江大學，2003 年），頁 105-118；彭錦珍，〈資訊時代中共國防現代化之研究－解放軍信息戰發展及其對台海安全之衝擊〉，《復興崗學報》，第 82 期，2004 年 12 月，頁 187-218；林宗達，〈中共軍民信息技術的聯合發展〉，《展望與探索》，第 3 卷第 10 期，2005 年 10 月，頁 34-52。

技術能力(Capability)，以及受害者(Victim)。藉此研究資訊攻擊的類型。[24] 所謂基礎設施包含網際協定位址(Internet Protocol Address, IP Address)、電子郵件、電話、假帳號、USB裝置等，[25] 而技術能力則包含木馬等駭客工具。在延伸的鑽石模型(Extended Diamond Model)當中，專家亦指出：發動者與受害者必須存在社會與政治的關係，這方面必須由犯罪學、政治學、經濟學等補充；而技術能力與基礎設施則與科技有關係，必須由科技相關學科補充（請見圖 1）。[26]

24. Hamad Al-Mohannadi, Qublai Mirza, Anitta Namanya, Irfan Awan, Andrea Cullen, & Jules Disso, "Cyber-attack modeling analysis techniques: An overview," paper presented at the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (Vienna: IEEE, August 22-24, 2016), pp. 69-76; Sergio Caltagirone, Andrew Pendergast, & Christopher Betz, "The diamond model of intrusion analysis," July 2013, pp. 8-18, *DEFENSE TECHNICAL INFORMATION CENTER*, <https://apps.dtic.mil/sti/citations/ADA586960>; Tarun Yadav & Arvind Mallari Rao, "Technical aspects of cyber kill chain," paper presented at the International Symposium on Security in Computing and Communication (Kerala: SSCC, Augest 10-13, 2015), pp. 438-452.

25. 另外要包含現下流行的機器人(bots)，該技術在法國大選中即被廣泛運用。請見 Emilio Ferrara, "Disinformation and social bot operations in the run up to the 2017 French presidential election," *First Monday*, Vol. 22, No. 8, July 2017, p. 1。

26. Sergio Caltagirone, Andrew Pendergast, & Christopher Betz, "The diamond model of intrusion analysis," pp. 19-24.

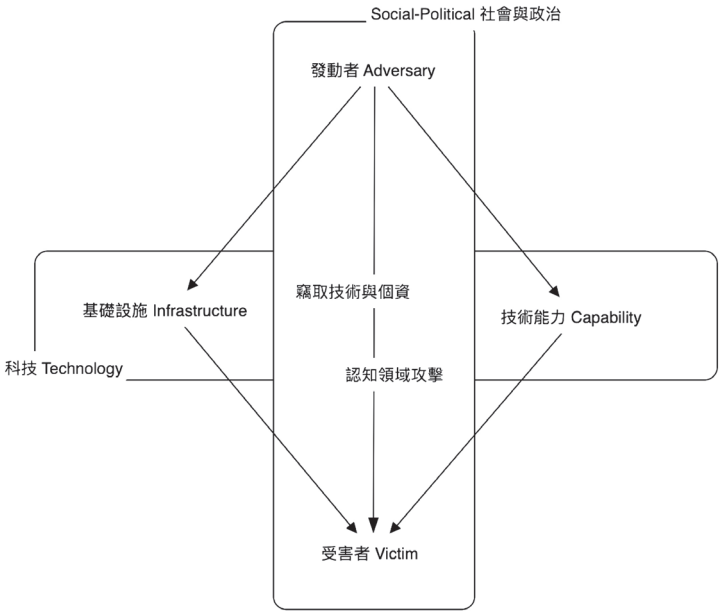

圖 1　認知領域作戰的鑽石模型

資料來源：改編自延伸的鑽石模型，請見 Sergio Caltagirone, Andrew Pendergast, & Christopher Betz, “The diamond model of intrusion analysis,” p. 19。

說　　明：本文僅先處理發動者與基礎設施問題。

此一模型原本是針對駭客攻擊的分析模型，然而若將其應用於認知領域攻擊亦可，原因在於：認知領域攻擊發動的組織與條件與一般的網路攻擊一致。以俄羅斯為例，其作為認知領域作戰發動者，經常依靠假帳號作為基礎設施（俗稱管道），並以各國內部矛盾作為其技術來做分化。[27]

雖然現行研究並未將鑽石模型直接應用在認知領域攻擊上，但假消息等研究已有類似雛形，例如，有學者即將內容產製包含在「技術

27. Jessikka Aro, “The cyberspace war: propaganda and trolling as warfare tools,” *European view*, Vol. 15, No. 1, May 2016, pp. 121-132.

能力」層次（創造與選擇爭議訊息）。[28] 國際爭議訊息指數(Global Disinformation Index, GDI)亦將認知領域攻擊分成來源(Source)、場域(Domain)、訊息(Message)和效應(Impact)，與上述分類極為類似。[29] 因此，本文將認知領域攻擊與鑽石模型結合，將駭客攻擊與認知領域繪製如圖 1。其中駭客攻擊或者數位極權輸出（如華為 5G 及中譯語通 GTCOM 等案例）乃以大數據蒐集個資或竊取技術，[30] 並藉由人工智慧以及被害者輪廓分析(Profiling)決定認知領域攻擊的受害者。而認知領域攻擊即針對此特定之受害者，進行認知領域的侵害。

對此，傳統資訊戰的軍事攻擊與防守模型已經無法完整描述現況，[31] 犯罪學、經濟學與科技等學科皆必須納入，方有可能描繪出現代資訊戰爭的實況。新的鑽石模型的四個分析維度不但可解釋駭客攻擊、電子脈衝干擾、電網攻擊等，亦可解釋認知領域攻擊、情報資訊戰、數位極權輸入與輸出，顯然較為完整。[32] 故本文將利用延伸的鑽石

28. Guy Duczynski & Charles Knight, "Strategic-Intelligence Analysis: Contributions from an Operational-Design Orientation," *Journal of Information Warfare*, Vol. 17, No. 1, Winter 2018, pp. 16-30.

29. Ben Decker, "Adversarial Narratives: A New Model for Disinformation," August 2019, *GDI*, <https://disinformationindex.org/wp-content/uploads/2019/08/GDI_Adverserial-Narratives_Report_V6.pdf >.

30. Samantha Hoffman, "Engineering global consent: The Chinese Communist Party's data-driven power expansion," October 2019, pp. 9-18, *ASPI*, <https://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion>.

31. 呂爾浩、魏澤民，〈中國資訊作戰的類型分析〉，《遠景基金會季刊》，第 7 卷第 3 期，2006 年 7 月，頁 187-229。

32. 竊取技術與個資和認知領域攻擊為兩大不同犯罪類型範疇，基於篇幅，本文僅就認知領域攻擊分析。關於竊取技術與個資等研究可參考林宜昌，〈資訊戰對國軍防衛作戰重要性之研究〉，《海軍學術雙月刊》，第 53 卷第 6 期，2019 年 12 月。頁 116-126。

模型的四個維度（發動者、受害者、基礎設施和技術能力），探討認知領域攻擊中發動者與基礎設施的關係。

三、中國化的鑽石模型

過往研究對於中國各單位對臺工作雖有詳盡介紹，但並非以認知領域作戰作為介紹基礎。[33]對此，有學者曾以實證方式，對發動者做出分類，並分析不同單位的生產內容。[34]此分類的邏輯來自於孟沛德(Peter Mattis)對於中俄網路攻擊的比較。其認為，相較於俄羅斯，中國的情報單位並不是主要的領導者，且不同的部門擔任不同的角色。[35]因此，此種網路攻擊反而常常大量依賴民間人員或公司的活動。中國這種去中心化的網路攻擊，使得追查不易，也形成一個中國式的攻擊特色。但所謂的去中心化，並沒有一個完整的描述，而臺灣學者提出的模型（請見圖 2），即回應了所謂去中心化的理論宣稱。

首先，發動者與受害者必定在社會與政治地位上占據不同的位子，而其位子本身會決定其行為方式與策略。依照社會學中重要的主觀與客觀的取徑，可將發動者與受害者之間的關係，分成客觀的資本累積，以及主觀的動機兩大部分。

個人或組織作為能動者，必須在其位置上做出符合其利益的行為。在其行為模式當中，則必須要有足夠資本才能夠進入相對位置。正如布迪厄(Pierre Bourdieu)指出的社會資本、文化資本、經濟資本等

33.寇健文，《中國大陸對臺工作組織體系與人事（計畫編號：107A107089）》（臺北：行政院大陸委員會，2019 年），頁 90。

34.沈伯洋，〈初探資訊戰攻擊節點〉，發表於「解構銳實力」研討會（高雄：中山大學，2019 年 12 月 12 日），頁 269-283；類似論述亦可見 Larry Diamond & Orville Schell, *China's Influence and American Interests: Promoting Constructive Vigilance* (Stanford: Hoover Institution Press, 2019), pp. 5-15。

35. Peter Mattis & Matthew Brazil, *Chinese Communist Espionage: An Intelligence Primer* (Annapolis: US Naval Institute Press, 2019) , p. 15.

等，[36]在認知領域作戰中亦有所謂的「作戰資本」。在歷史軌跡中累積資本的人，方有機會發動有效攻擊。其有可能是從政治與人脈中獲得資本，亦有可能是從經濟利益得到資本，或以自身特殊的認同與經濟位置獲得資本的中間人。綜上所述，從其累積的資本而論，即有所謂資本擁有者與資本追求者的差別（請見圖 2 的 Y 軸）。

主觀而言，有時訊息的散布者係為政治動機而散布消息，亦有可能是經濟動機而散布（請見圖 2 的 X 軸）。但，亦有可能散布者在被脅迫的情況下，或為了建立起自己在中國的地位而幫助有政治動機者發散訊息。雖然其帶有一定商業動機，但亦有可能是在無奈之下做出的決定，故在政治與動機的光譜中間，尚有中間型這種特殊角色，併予說明。[37]

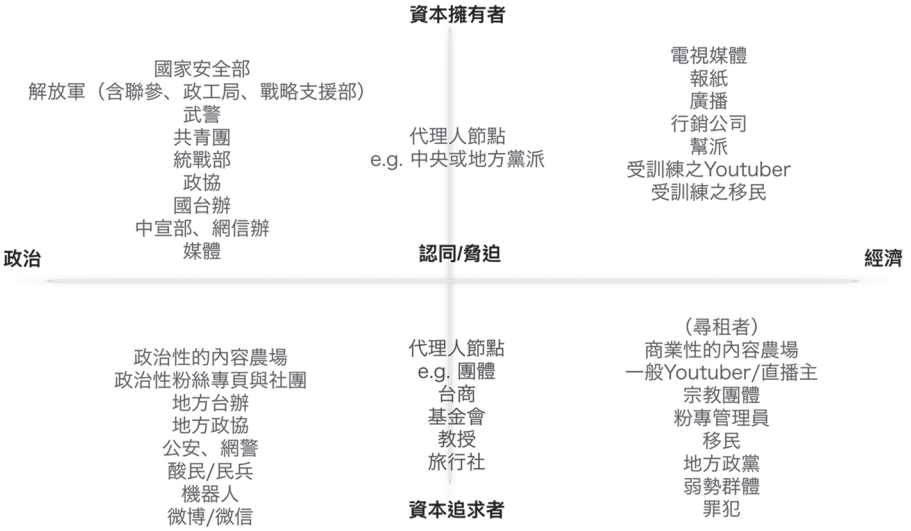

圖 2　鑽石模型發動者圖象

資料來源：沈伯洋，〈初探資訊戰攻擊節點〉，頁 269。

36. Pierre Bourdieu, *Practical Reason: On the Theory of Action* (Stanford: Stanford University Press, 1998), pp. 1-35.

然而，單單指出發動者的多元樣貌，無法得知認知領域作戰的「戰術」。亦即，必須再進一步由鑽石模型的基礎建設出發，條列出在基礎建設中可疑的爭議訊息，並指出其與發動者之間的關係，方能得知中國的進攻樣貌。本研究基於此架構，以 2020 大選備份之資料為例，試圖回答：在鑽石模型中基礎設施的異常為何（第三節）？以及相對於這些異常的中國攻擊樣貌為何（第四節）？

參、基礎建設之異常跡象

關於基礎建設的部分，主要就是爭議訊息從什麼「管道」而來。一般來說，管道可以分成線上(online)與線下(offline)。由於人的認知領域與資訊來源息息相關，其可透過一般媒體、社群媒體吸收資訊，但亦可透過一般的交談、耳語等等。也因此，本研究依據臺灣線上聲量的排名，[38] 備份資料約千萬筆（含微博、微信公眾、貼吧、博客、臺灣與中國新聞網站、中文農場、PTT 資料，Facebook 公開粉專與社團，以及部分 YouTube 頻道），[39] 並另循管道蒐集線下的耳語，歸類選舉期間的基礎建設異常 [40] 如下：

---

37. 吳介民，〈以商業模式做統戰：跨海峽政商關係中的政治代理機制〉，李宗榮、林宗弘主編，《未竟的奇蹟：轉型中的台灣經濟與社會》（臺北：中央研究院社會學研究所，2017 年），頁 675-720。

38. 計算流量以 Alexa 為基準，日期為 2019 年 5 月 1 日至 2020 年 1 月 31 日。

39. 總共約千萬個微博號，約百萬個微信公眾帳號，著名的貼吧、博客，1,431 個中國與臺灣新聞網站，35 個中國、臺灣、馬來西亞、新加坡、美國等中文內容農場，PTT 熱門看板資料（2014 年至今），370 個粉絲專頁與社團（使用工具為官方授權的 CrowdTangle），以及 62 個 YouTube 頻道。粉絲專頁、YouTube 的蒐集對象為曾經在 10 月至 1 月在 LINE 群組傳月超過 10 次，並且超過 2,000 追蹤／訂閱為標準，LINE 資料則來自於可信任的國際認證來源。中國資料每日約五萬筆；Facebook 方面，有所有粉專與公開社團皆有備份，但僅觀察特定的粉專與社團；LINE 每日約 3,000-5,000 筆。

40. 標準為 DFRLab 曾提出的 3A：Activity, Amplification, Anonymity。尚有其

一、線上基礎建設之異常

(一) 整體數據異常

根據本研究蒐集之新聞資料及社群媒體的數據，單一政治人物或議題通常會有所謂的「新聞熱度」。以新聞為例，單一政治人物在單一文章中被提及的機率如果單日 10%即為高熱度，社群媒體則約 30%，但這種現象大概只會維持一兩天。事實上，在 2019 年 10 月以前，沒有單一政治人物在 Facebook 的聲量超過 30%。[41] 然而，韓國瑜的聲量在 2019 年 10 月以後，穩定地超過 60%（蔡英文平均約 30%，郭台銘約 10%）。新聞媒體方面也出現了異常，每天約 10,000 則報導之中，平均有 850 則在討論韓國瑜，在三個月當中長期地維持 8-9%左右。作為對照，蔡英文 2016 年當選當天，聲量也不過 5%而已，並只維持一天。總結來說，無論是新聞還是網路媒體，臺灣都出現「量」的異常。[42] 新聞異常只出現在韓國瑜身上，但社群媒體的異常則是藍綠皆有，相差約兩倍左右。

表 1 為根據本研究之資料所製成之Facebook公開社團聲量圖，[43] 將提及蔡英文和韓國瑜（限繁體中文）的文章數和互動數（包含按讚、分享、留言、影片觀看數）分列如下：提及韓國瑜的文章中，YouTube 連結的數量是提及蔡英文的文章的三倍，而其他影片（如抖音、Kan-

---

他輔助標準請見 DFRLab, “Human, Bot or Cyborg?” December 23, 2016, *DFRLab*, <https://medium.com/@DFRLab/human-bot-or-cyborg-41273cdb1e17>。

41. Gene Hong，〈從新聞與社群來看韓流現像的典範轉移？〉，2019 年 12 月 31 日，《Medium》， <https://link.medium.com/ByM6wBSUu4>。

42. 此現象在 2018 年亦發生過。2018 年 11 月 12 日，YouTube 及 Google 搜尋都出現異常，當天晚上，在 YouTube 和 Google 搜尋「韓國瑜」三個字的人，臺灣連前 15 名都排不上。亦即，全世界超過 15 個國家比臺灣還關心韓國瑜。

43. 藍綠雙方的粉絲專頁主要是以官方粉絲專頁為主，但粉絲專頁的聲量遠遠不及社團（約為 7-8 倍的差距），故本數據呈現以社團為主。

Watch）或原生影片的量也有約兩倍。而提及韓國瑜文章底下的互動數，更遠遠超過蔡英文以下的互動數，可高達三倍以上。再以 Facebook 影片為例，蔡英文相關的有七萬多篇，韓國瑜相關的有 17 萬左右，但是底下互動數蔡英文約 280 萬，韓國瑜卻是 780 萬。從總數來說，韓國瑜的相關文章有 150 萬，蔡英文為 98 萬（相差約 1.5 倍），互動數蔡英文為七千萬，韓國瑜卻逼近一億八千萬（相差約 2.5 倍）。[44]

亦即，互動數在 Facebook 社團中，在特定候選人身上出現了不自然的數據，而文章中，YouTube 相關影片及 Facebook 原生影片的分享也出現了高度不合比例的現象。[45]

表 1　Facebook 公開社團提及韓國瑜與蔡英文之文章數和互動數（2019 年 5 月 1 日—2020 年 1 月 12 日）

	蔡英文 文章數/互動數	韓國瑜 文章數/互動數
YouTube	**36,551 / 2,033,492**	**89,850 / 6,279,917**
連結	177,645 / **16,173,480**	243,260 / **34,137,838**
其他影片	**27,704 / 1,587,242**	**58,076 / 4,674,521**
原生影片	**76,305 / 2,804,475**	**179,111 / 7,818,579**
照片	117,584 / 7,908,100	178,821 / **18,109,810**
純動態	55,385 / 5,922,475	119,116 / **18,247,847**
總數	982,348 / **72,858,528**	1,517,468 / **178,597,024**

資料來源：作者自製。
說　　明：異常部分以灰底表示。

44.由於文章可能提及對手陣營，所以互相之間也會製造聲量。然而本研究隨機抽樣兩政黨候選人各一千篇文章，韓國瑜相關文章中，提及對手的次數是蔡英文文章提及韓國瑜的兩倍；亦及，本數據所呈現的，蔡英文的聲量甚至有一部分是韓國瑜製造的（多過於蔡英文為韓國瑜製造的）；再者，本研究挑選兩邊社團互動數最高的 10 個社團，皆為以各自陣營支持者名義所成立的社團，而非對方的社團。

45.這樣的數據還不包含簡體中文的文章，也不包含已經被 Facebook 在選舉期間刪除的社團（99 個皆為韓國瑜社團，其中三個社團有超過 10 萬的成員）。

（二）Facebook 數據異常

為何上有大量的異常聲量？依據本研究備份之 370 個粉專與社團當中（來源為上述高互動數的社團與粉專），共有 202 個泛藍及 168 個泛綠社團，而兩者聲量的提升大部分都來自於連結、影片等分享。泛藍社團主要分享泛藍新聞媒體及內容農場，而泛綠社團則主要分享泛綠新聞媒體及新媒體（如「芋傳媒」、「放言」等），而聲量高低的關鍵在於內容農場的涉入與否。

圖 3 與圖 4 為農場與粉絲專頁之關係：左側為本研究蒐集之農場網站，右側為臉書的粉專與公開社團，每一條線代表一次的分享次數，分享次數越多則線越粗。由此圖可發現特定專頁和社團只會分享特定農場的文章（例如，世界華人系列只會分享「琦琦看新聞」），而此並不符合一般網路粉絲專頁的行為模式。「世界華人」系列粉專，加起來約有超過 25 萬的追蹤者，其選舉前六個月，分享固定連結（如 YouTube 或一般文章連結）的比重是 100%（不會分享其他），而知名泛綠粉專「打馬悍將」，雖然也是爭議消息來源，但分享固定連結的比例不到 2%。而從其分享的「琦琦看新聞」為例，甚至可達單日上傳超過 500 篇文章；簡言之，此模式乃藉由大量成立粉絲專頁和社團來提高特定政治人物的網路聲量。因此，前述的異常網路聲量（藍為綠的兩倍到三倍），除了傳統新聞以外，大部分來自於此種異常分享模式，至於其原因，詳見第四節分析。

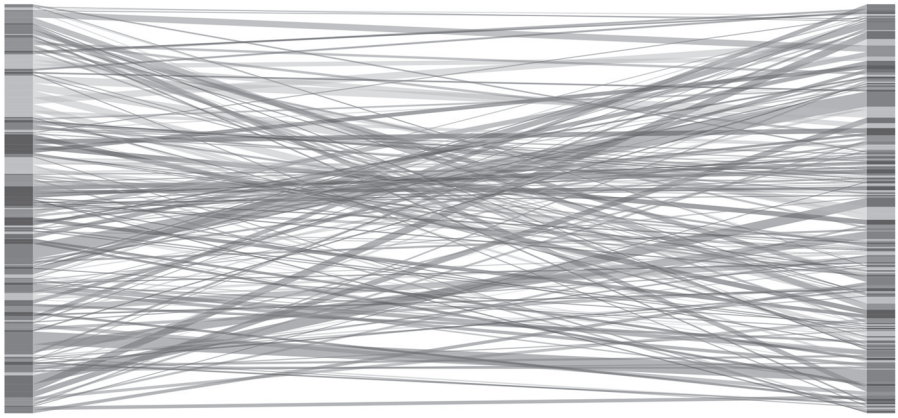

圖 3 本研究範圍內流量前 122 名之內容農場（左）與粉絲專頁、社團（右）的流量關係圖（2019 年 5 月—2020 年 1 月）

資料來源：作者自製。

說　　明：細部查詢請見以下連結：<https://plotdb.io/v/chart/24879>。

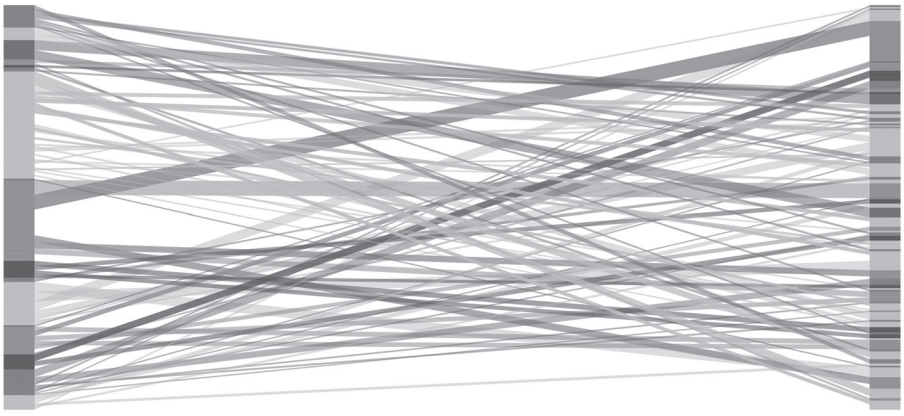

圖 4 本研究範圍內政治相關的內容農場（左）與粉絲專頁、社團（右）的流量關係圖（2019 年 5 月—2020 年 1 月）

資料來源：作者自製。

說　　明：細部查詢請見以下連結：<https://plotdb.io/v/chart/25161>。所謂政治並不局限以網頁本身宣稱為斷，例如好運加油讚看似算命頁面，卻會分享解放軍相關之外宣，則亦歸類在政治類別。

舉例而言，關於陳菊收賄的謠言，最早出現在中國的「鳳凰新聞社」（其乃著名的政治內容農場，但由於其名稱，讓人容易誤認為真實新聞），於 2019 年 4 月 9 日晚上 7 點左右發布，10 月之後，被改寫出現在「兩岸頭條」這個中國產製的農場，並同步於 Facebook 與 LINE 中。這些文章在改寫之後，並不是「原文被分享」，而是同樣的內容「被複製貼上」在不同的 115 個社團當中，而在加總有 418 萬讚的專頁與社團中，加起來竟然不到 7,000 個讚，留言加總更不到 700。[46] 這種大量複製貼上的散布，與一般單一訊息被大量分享的模式完全不同。[47] 除了散布模式之外，這些粉專的互動率亦出現與中國官方專頁（《人民日報》、「你好臺灣」）具備高度一致性（請見圖 5），證據都不斷地指向 Facebook 的數據異常。

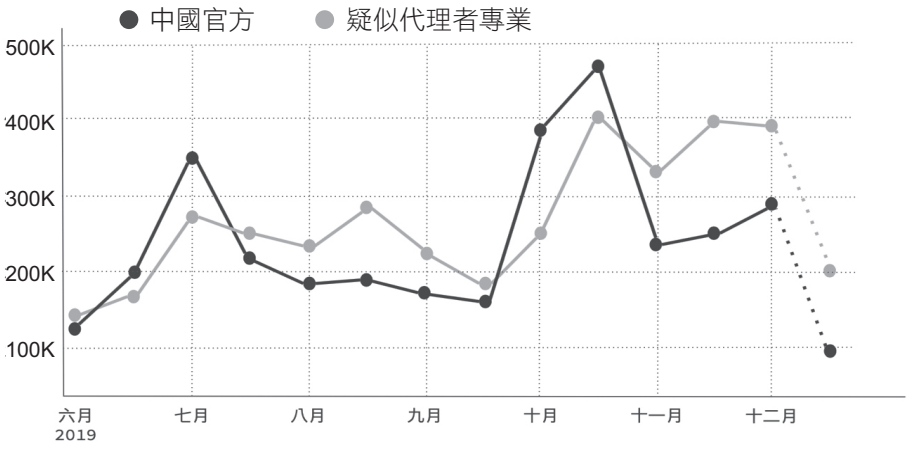

圖 5　192 個專頁平均互動率與官方（人民日報、你好臺灣）互動率之比較

資料來源：作者自製。

46. 由此可知，表 1 所述之韓國瑜異常的互動數，可能不是來自於單一文章的高互動，而是過多文章的少量互動相加而成。

47. 作為對照組，一般訊息乃是由單一來源發散，而分享會來自於單一來源。

（三）YouTube 異常

YouTube 頻道的異常可以從幾個面向觀察：觀看數、訂閱數、捐款連結、留言，以及讚數。本研究將 2,000 訂閱做為基底，掃過三個月內異常訂閱增加的中文頻道如下圖，而幾乎所有的異常增加都發生在同樣日期（2019 年 10 月 15 日）。

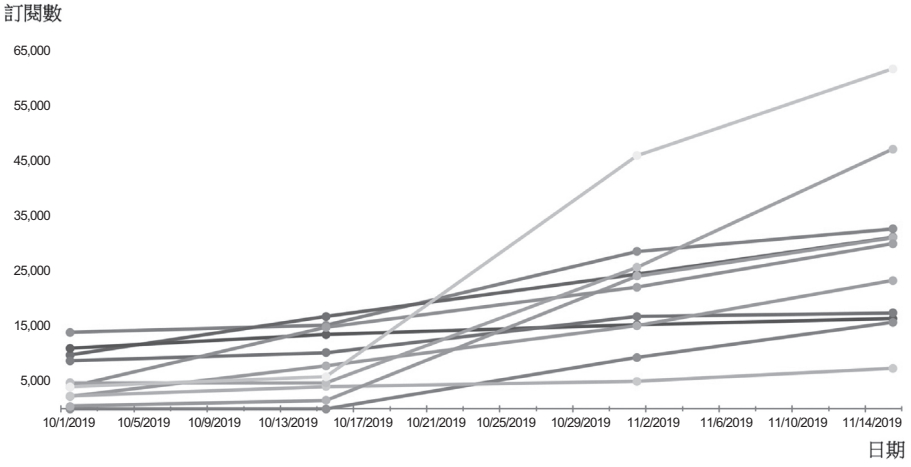

圖 6 YouTube 頻道訂閱數同時增加圖

資料來源：作者自製。

說　　明：頻道列表：邪影、趴客畫黑白、高雄媳婦、韓加青年、傾訴琳聲、偉鴻青年、索哥們、團長小魚兒、真像五則天、陳品宏。惟需注意，此類頻道並不代表跟中國有直接經營關係。中國可介入的方式有衝人數、海外捐款、透過公關公司操作等等。故此圖僅指出異常現象，進一步的連結將以第四節做說明。

此類頻道大量散布選舉相關爭議訊息，且在讚數出現異常現象，有時影片會有上千個讚，有時候一個讚都不會有。若將全部 62 頻道的按讚／按倒讚的總數每日相加，可得圖 7，可發現頻道間有固定四個空窗期（影片讚數特別少），為明顯之異常現象。此異狀同時發生在直播。許多影片訂閱數可能未破千，但直播觀看卻可破萬，不符合一般

訂閱數與直播的比例。

從流量來看，史丹佛大學網路觀測中心亦發現頻道「高雄林小姐」流量出現異常，[48] 但本研究認為，其觀看流量上上下下乃屬正常現象，因此未必表示有認知領域作戰之痕跡；但與下列各頻道比較，即可知其他頻道的流量過於「穩定」，甚至出現訂閱數「穩定增加固定數字」[49]，或每個禮拜都會固定增加一定數量的粉絲，這種現象才是真正的異常指標。本研究中所收錄之 YouTube 頻道，前 10 名訂閱當中有七名出現此類異常，而其中五個頻道為簡體中文。[50] 相關資料可見圖 8。

由於 YouTube 直播可以捐款，因此有大量的直播者可以藉此管道有所收入。但可疑之處在於：第一，部分直播者提供的捐款連結為支付寶與微信支付，但這並非臺灣慣用的支付方式；第二，根據網路平臺 Playboard 之資料，臺灣直播主 2019 年 YouTube 內建捐款排行榜中，前九名有六名為支持韓國瑜的直播主，兩名為批判執政黨之直播頻道，一名為財經頻道。第十名為著名網紅「館長」，而其他臺灣百萬級以上的 YouTuber 皆榜上無名。第一名的高雄林小姐，訂閱數也不過十萬而已。這些數據搭配前述之觀看數、訂閱數等等，皆難謂為網路自然之現象。

48. Stanford Internet Observatory, "Taiwan Election: Disinformation as a Partisan Issue," January 21, 2020, *Stanford Internet Observatory*, <https://cyber.fsi.stanford.edu/io/news/taiwan-disinformation-partisan-issue>.

49. 由於 YouTube 改變其訂閱數顯示方式，故固定增加數字不代表異常，而是「固定頻率增加」才為異常。

50. 其中一個頻道觀看數／粉絲數比例竟然每支影片都達到 100%，亦即，每部影片的觀看數都遠遠超過其訂閱人數。

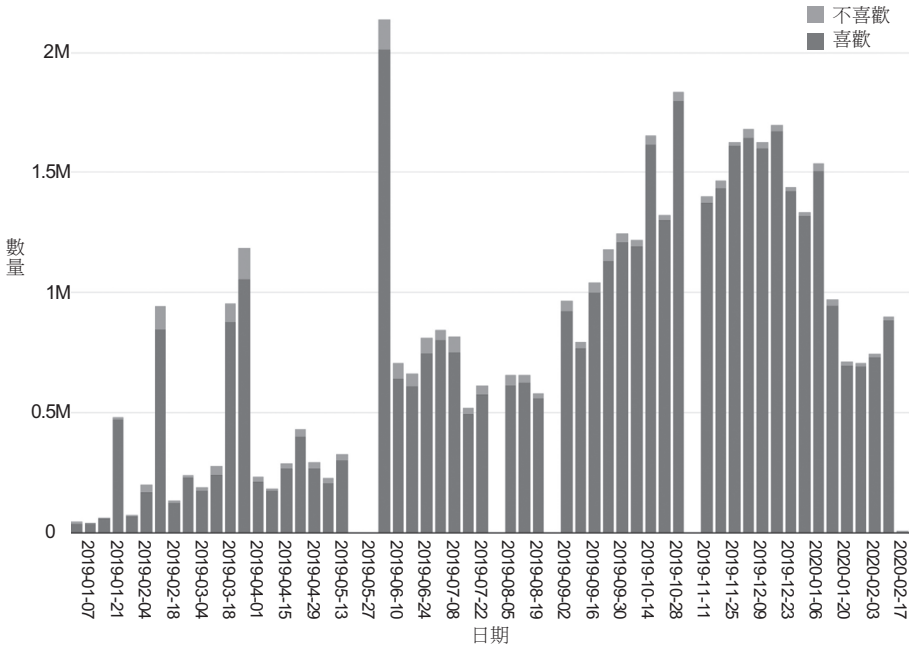

圖 7 前十頻道每日按讚累積圖

資料來源：作者提供資料，Michael Jensen (University of Canberra)繪製。
說　　明：圖中明顯出現四個特定空窗期。

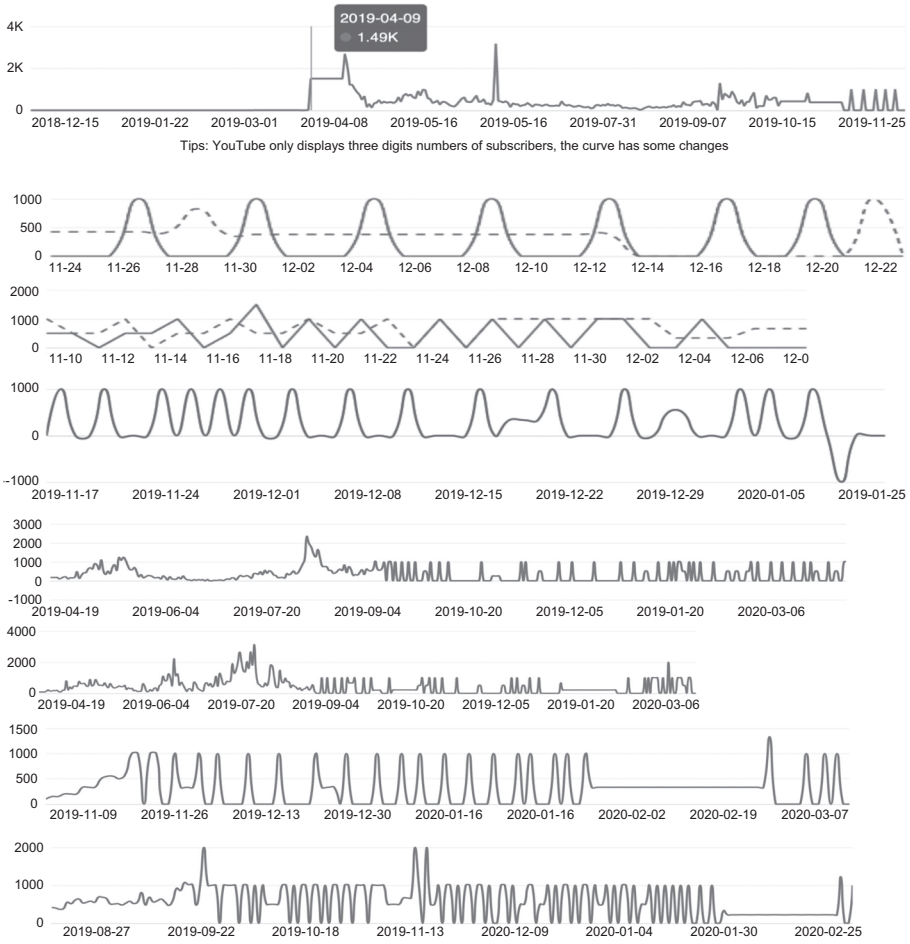

圖 8　各頻道比較圖

資料來源：Noxinfluencer，〈全方位分析提升網紅影響力〉，2020 年 4 月 23 日（檢索），《Noxinfluencer》，<https://tw.noxinfluencer.com/>。

說　　明：X 軸為時間，Y 軸為粉絲增加數。由上而下分別為高雄林小姐、寒國人、鈞鈞、點亮歷史、江湖白曉生、更新台灣、108 演播室。

（四）Instagram 與 Twitter 異常

Instagram 曾在選舉前突然大量出現「宣告我的投票意志」文章，內文討論失業率，以及政府無能，並使用相同標籤，在一小時之內大量散布。然而此些帳號在此之前從未討論過政治，並在被揭露之後大量刪除。[51] 相關截圖請見圖 9。而「宣告意志」亦非臺灣慣用語言。

圖 9「宣告我的投票意志」截圖

資料來源：作者自製。

二、線下基礎建設之異常

（一）LINE 流量與內容的異常

根據 LINE 公司報告，LINE 的流量在臺灣平均一日為 93 億則訊息，[52] 是臺灣人民主要的訊息來源之一。其中，以 2020 選舉為例，本

51. 相同的情況亦出現於現今社群上肺炎的討論，由大量的直播主在 Instagram 和 Twitter 平臺上散布肺炎與愛滋病、流感的關係，藉此弱化疫情嚴重程度。

研究資料庫回報數量約為 2018 九合一選舉的兩倍，且在 10 月之後出現大量政治類訊息。與之前顯示的新聞數量類似，皆出現不合比例的高峰。而以 2019 年 12 月 30 日為例，文字類訊息約占 76%，圖片與影音約占 24%。影音中約 60%為中國內容農場影片或抖音影片。若比對現有闢謠組織 Mygopen 資料，45.44%為假新聞（尚不包括有爭議的政治資料）。簡而言之，LINE 群組已成為國人吸收假訊息的重要來源。

通常 LINE 所散布的訊息，應該會有漸漸趨緩的趨勢，例如詐騙的謠言，會緩慢增強，甚至陡坡上升，再因為政府闢謠而漸漸趨緩。再過一段時間，又會開始廣傳，以兩個月或三個月為周期散布[53]。然而從 10 月開始出現的政治類謠言卻完全不同。首先，它不會因為闢謠而減緩，亦不會突然增加，而是跟 YouTube 頻道相同，穩定地在特定日期散布，亦即，許多簡體字政治類謠言會「自行爆發」，然後「突然中止」，而缺少穩定增加或減少的跡象。由於 LINE 會散布 YouTube 相關連結，因此互相之間又會呈現拉抬現象。關於政治類與非政治類的散播比較，請見圖 10；而其內容分布可見圖 11。

52. 相關數據請見 TH Schee，〈關於 LINE 的一些數字—從 SEC Form 20-F 開聊起〉，2019 年 8 月 3 日，《TH Schee blog》，<https://blog.schee.info/2019/08/03/line-form-20f/>。

53. 偶而會有逐月都瘋傳的假消息，比如「這個月一日開始交通要開始裁罰 XX 現象」，就會以一個月為周期散布。

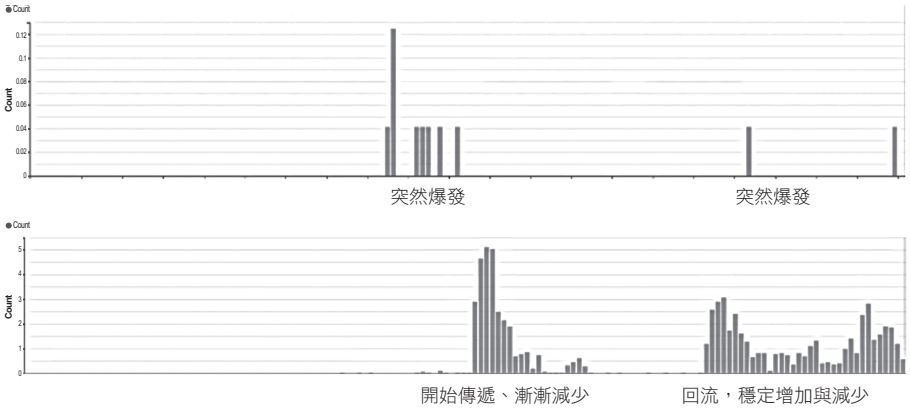

圖 10　政治與非政治類的謠言路徑比較

資料來源：作者自製。

說　　明：上圖為簡體字的民進黨收賄謠言，下圖為一般貼圖詐騙。期間為選舉前六個月，Y 軸為實際謠言回報次數，回報人數母體約 19 萬。

若觀察內容，則可進一步證實上述「突然爆發」的問題。如前所述，一般謠言的散布雖然會因為事件產生差異，但不會突然停止，除非其散布係人為刻意為之。政見發表會之前明顯有大量凝聚仇恨和網路軍隊相關的文章，卻在之後瞬間消解，隨後出現大量批評執政黨的文章，並同步出現於前述的 Instagram。例如在反滲透法過後，中國的內容農場觀察者網所做的反滲透法假新聞一日內爆量流傳，定調「執政白色恐怖」。[54]

另外，圖 11 所列主題當然有可能是臺灣政治公關公司相互攻擊的結果。然而，資訊作戰的攻擊方未必需要製造議題，而是可以單純地

54.〈為配合「反滲透法」過關 臺當局一天抓 10 多名臺灣共產黨成員〉，2019 年 12 月 31 日，《觀察者》，<https://www.guancha.cn/politics/2019_12_31_530036.shtml>；其後由聯合報報導，其引述來源為「人民政協報微信公眾號」。而此議題在 12 月 Facebook 上互動超過 40 萬次。

將議題「激化」，並加以散布。若將圖 11 所列主題與中國微博、微信公眾號做比對，可知中國試圖見縫插針的主題有新南向灑錢與能源政策失敗（執政黨議題）、媚日仇臺、楊蕙如網軍議題、民進黨倒戈（裂解議題）、蔡英文侮辱國軍（陰謀論）等。至於軍人、軍眷、教育改革等議題，中國著力甚少，可以說是臺灣內部內鬥議題；而同性戀議題較為有趣，中國並沒有主打同性戀摧毀倫理、同性戀霸權等議題，但卻不斷地散布同性戀疾病問題，此可能與中國國內維穩有關：同性戀屬於敏感議題，而主打疾病問題較不易出現維穩危機。

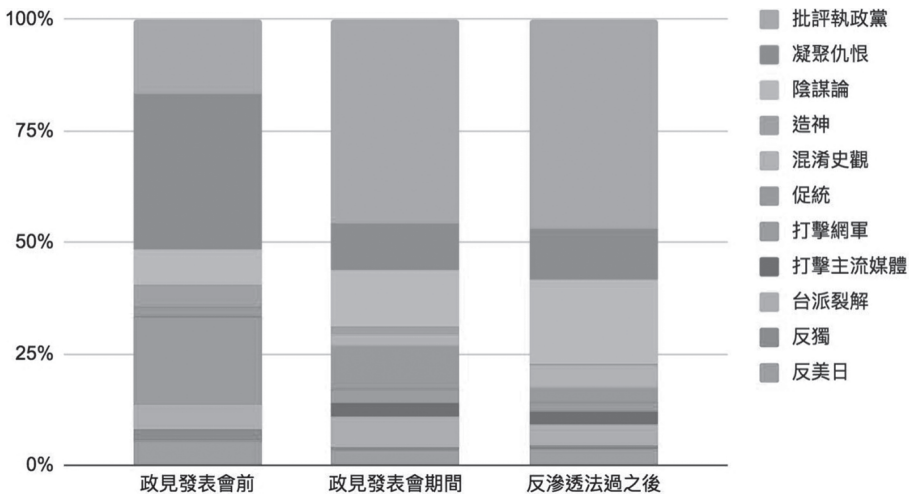

圖 11　LINE 謠言的內容落差

資料來源：作者自製。

最後的 LINE 異常現象是在選舉之後，Facebook 出現大量「作票」影片，並在 LINE 群組以 YouTube 或 Facebook 影片瘋傳，然而，在選舉過後一個禮拜內，這些群組亦出現大量退潮現象。例如作者參與的一個政治群組，在選舉過後，200 人群組瞬間退成剩 40 人。而本研究溯源之後，發現選舉作票的陰謀論並非在選後才由支持者群組出現，而

是在 12 月 13 日至 12 月 18 日時，以微信、微博的文字類形式呈現，並出現「做票」（中國謠言使用「做」而非「作」）、「大曝光」、「大暴光」、「沒收選舉」等非臺灣用語之關鍵字（見圖 12），並為中評社、人民日報、鳳凰新聞引用，最終以影片或文字形式散布至 LINE、YouTube、Telegram 和 Facebook。亦即，此類謠言早已在選舉一個月前做好準備，並在選後當天直接爆發。截至 2020 年 8 月 18 日，此類謠言已成為主要的陰謀論，並在罷韓、高雄市長補選等選舉時不斷出現。

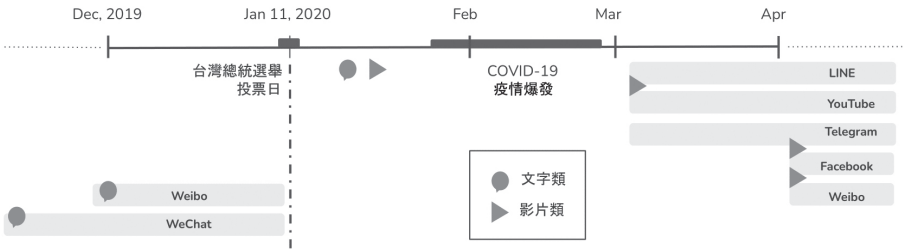

圖 12　作票陰謀論流程圖

資料來源：作者自製。

（二）地方謠言的異常

與 LINE 不同的是，地方上謠言的散布有時僅是口耳相傳，並未「數位化」於 P2P 社群當中。其中引人注目的是地方上所散布的小冊子與地方報紙，例如免費發放的農民曆，即出現「韓國瑜是奇才」、「中國武力統一臺灣」等論述。此與地方廣傳的謠言，例如「簽署和平協議，存款即可從臺幣變成人民幣」等等互相搭配，屬於傳統中國「文攻武嚇」之進攻；此類謠言族繁不及備載。

肆、攻擊模式與可歸責性

以上為各個基礎設施（管道）在選舉期間的異常狀況。問題是，這樣的異常狀況有可能是各個陣營的網路操盤手直接造成，未必與中國有關。因此，我們必須藉由其他證據，討論中國發動者的攻擊態

樣，方能確認中國與認知領域作戰之間的關係。因此，本節延續先前政治／經濟與認知領域作戰的作戰資本角度出發，根據本研究蒐集之資料，[55] 將不同資本的攻擊分述如表 2，而與前述基礎建設異常之對應呈現於圖 13。

表 2　認知領域作戰的中國進攻模式

模式	製造 指示	代理	散布	受眾	資本相關	製造者與散播者的脫勾
外宣模式	中國官方	兩岸掮客	傳統媒體	傳統媒體閱聽者	大	完全脫勾
粉紅模式	中國地方 共青團相關	無	水軍	不特定民眾	小	無脫勾
農場模式	中國網站 境外網站	無	盈利者 演算法	特定民眾	中等	漸漸脫勾
協力模式	相互合作，製造者與散布者同步。			特定民眾	里長、學生等，以統戰為主。	彼此合作

資料來源：作者自製。

55. 訪談兩個網路公司、三位網紅，以及三位 LINE 群組的發起人。其餘資料為公開來源情報(Open-source intelligence, OSINT)之搜尋。沈伯洋，當面訪談，受訪人 A，臺北市，2018 年 12 月 20 日；沈伯洋，當面訪談，受訪人 B，臺北市，2018 年 12 月 20 日；沈伯洋，當面訪談，受訪人C，臺北市，2019 年 1 月 18 日；沈伯洋，當面訪談，受訪人 D、E，臺北市，2019 年 1 月 22 日；沈伯洋，LINE 訪談，受訪人F、G、H，2019 年 1 月 1 日至 2019 年 5 月 3 日。

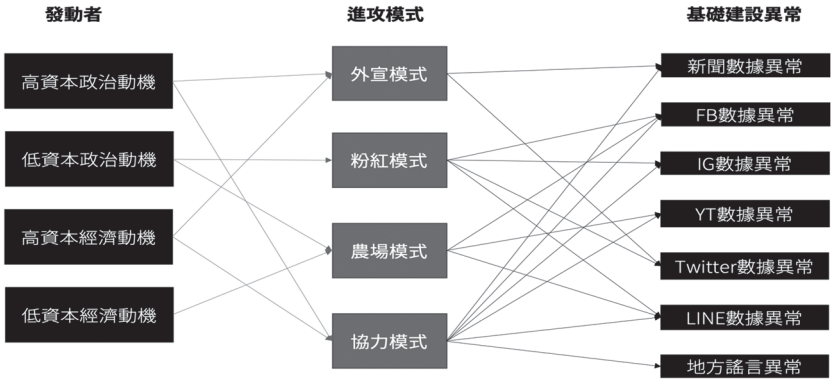

圖 13 發動者攻擊模式與基礎建設異常的對應

資料來源：作者自製。

一、外宣模式

根據《路透社》及《金融時報》報導，中國官方經常性指示臺灣媒體報導方向，媒體離職員工亦證實此事，[56]甚至蔡衍明本人都直言不諱有與國臺辦實質的交流[57]，《路透社》亦報導了「兩篇文章臺幣 13 萬」的價碼。而臺灣亦有學者訪談媒體記者如何「抵抗」上頭的親中報導指示。[58]此種外宣模式主要提供的是「替代性事實」來呈現中國觀點。而在中國市場具備致命的吸引力之下，任何有經濟動機和資本的企業，都有可能以經營媒體的方式幫忙中國進行外宣。因此，觀察《人民日報》與臺灣報紙，或者《央視》與臺灣媒體的同步性，即為觀察此外宣模式的方式。

56.蘇穩中，〈中時記者離職前沉痛告白〉，2019 年 6 月 21 日，《放言》，<https://reurl.cc/nzZRr1>。

57.何清漣，《紅色滲透》（臺北：八旗文化，2019 年），頁 191-198。

58.黃兆年，〈紅色滲透下台灣媒體人的日常抵抗〉，發表於「解構銳實力」研討會（高雄：中山大學，2019 年 12 月 12 日），頁 177-203。

依照資本的排列，中國官方具備雄厚的資本，其對口在資本的分配上，不易接觸無資本者，反而容易接觸有資本，且有經濟動機的利害關係人，如臺灣媒體或中國商業媒體。從中國官方報導及臺灣報導的相似性及同步性，[59] 不難看出部分臺灣電視與平面媒體在報導上曾產出大量特定政治人物的訊息，可合理解釋第三節所述之臺灣新聞數量異常。

除了同步報導之外，這些企業亦與中國合辦各式各樣的活動，讓更多利害關係人能夠進入場域，並獲取認知領域作戰資本。著名的「海峽青年節」，就是由中國華藝廣播公司和臺灣的主流媒體合辦之活動，但華藝廣播前身即為解放軍的心戰單位福建前線廣播電臺。國臺辦、統戰部、宣傳部等，都可藉由這樣的方式見面培養並接觸能夠加入外宣的傳媒，甚至培養統戰樣板之直播主；[60] 如由《北京日報》報業集團主辦、旺旺集團協辦的「第四屆兩岸媒體人北京峰會」，也是類似交流的延伸，並培養出更多的傳媒作為發散訊息的觸角。[61] 這也是

59. 根據台灣民主實驗室 Niven 及成功大學 Kao 之研究，《中國時報》特定種類新聞與中國官媒寫作風格相似性最高，其次為聯合報，而蘋果日報最低，比對日期為 2020 年 1 月至 2020 年 5 月。請見 Timothy Niven & Hung-Yu Kao, “Measuring Alignment to Authoritarian State Media as Framing Bias,” paper presented at the ACL Anthology (Barcelona: ICCL, December 12, 2020), pp. 11-21。

60. 如非凡音聯播網已經與海峽之聲簽訂新聞合作協議，而參與這些論壇的臺灣單位則有中國青年發展聯合會、亞太通訊社、台灣傳統倫理文化發展協會、中華時報、真晨報、中華自媒體暨部落客協會與臺灣 ETtoday 東森新聞雲等。這並不代表這些交流媒體就是外宣計畫的一部分，但這卻是未來可能合作的象徵。

61. 類似案例尚有國臺辦新聞局主辦、海峽之聲與一點資訊共同承辦的「首屆海峽兩岸網絡新媒體大陸行」，參與者有國臺辦新聞局長馬曉光、深圳市委常委、天津市委常委、市委統戰部部長、廣東省委常委、宣傳部長等人，以及中華時報、真晨報、中華自媒體暨部落客協會等。請見〈兩岸新媒體大陸行，難說再見〉，《華廣網》，2018 年 11 月 5 日，<http://www.chbcnet.com/

為何外宣模式對於臺灣新聞數據出現異常現象，提供了合理解釋。[62] 此模式與中國對美國之資訊作戰多有雷同之處，例如在大量的夾報、置入性行銷等，皆為外宣所慣用之手法。較為不同地是，中國媒體在各國大外宣的媒體（如新華社）並沒有特定隱藏其背後為中國一事，但在臺灣，由於中國媒體較難開設「直營店」，因此必須透過隱而不顯的手法來散布爭議訊息，這也是後兩者模式（農場模式與協力模式）在臺灣的特殊之處，也是臺灣得以成為其他國家借鏡之原因：臺灣是中國資訊作戰試驗的實驗場。

二、粉紅模式

外宣模式或許可以解釋新聞量的暴增，卻無法解釋本論文提出的社群媒體異狀。以關西機場事件為例，其源頭僅為幾個海南電視臺的帳號，甚至在中國國內沒有輿論的出現（故亦非維穩的一環），雖然在幾小時之內出現大量造假（協同性造假）行為，但與前述中央單位

---

normal/content/chbcnet/hgbd/content/2018-11/05/content_1346613.htm>。福建省廣播影視集團亦有類似案例。若配合統戰，此管道亦可作為重要的選舉延伸，例如曾經加入兩岸媒體人北京峰會的莊子富（原名莊曜埕），一方面接待貴州、河南、廣東、山東等交流團，會見統戰部人士，另一方面經營臺中廣播電臺與旅行業務，並製作韓國瑜造勢的礦泉水，最後由顏家協調出面競選 2020 立委等。

62. 中共中央亦常有購買 Twitter 帳號做外宣的傾向，請見 ProPublica 之研究，以及 Twitter 於反送中事件的官方聲明。Jeff Kao & Mia Shuang Li, “How China Built a Twitter Propaganda Machine Then Let It Loose on Coronavirus,” March 26, 2020, *ProPublica*, <https://www.propublica.org/article/how-china-built-a-twitter-propaganda-machine-then-let-it-loose-on-coronavirus>； Twitter Safety, “Information operations directed at Hong Kong,” August 19, 2019, *Twitter*, <https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong.html>。然而由於臺灣使用 Twitter 人口較少，故不在本文討論範圍。

發動有所不同，難以確認其為中央的攻擊。[63] 這種大量由地方性愛國人士或小粉紅製造的訊息，沒有官方的定調，亦無代理人的存在，故本文將其歸類於第二種攻擊模式：粉紅模式。

這些地方性的小粉紅，未必完全跟政府無關。例如，除了解放軍戰略支援部的網路軍隊之外，各地原本就有所謂「民兵」與「武警」的角色。在 2006 年的文獻即已指出中國民兵對訊息戰的學習，[64] 並指出 150 萬的人民武警曾在 2004 演習如何安放信息地雷、釋放信息炸彈、傾倒網路垃圾、分發網路傳單、信息欺騙、散布虛假信息、組織信息防禦、建立網路間諜站等。[65] 以作者搜尋之資料為例，在微信或 Telegram 的群組之中，不少群組有武警加入，甚至有「教戰守則」，包含低級黑、高級紅、反串等教程。有時會直接將訊息傾倒在臺灣的 Facebook 留言或者 LINE 群組當中；[66] 有時會先在微博試水溫，再將訊息加以改製，放入粉絲專頁或社團散布，甚至自己經營粉專。與外宣模式不同地是，此類粉紅模式並沒有所謂的臺灣在地代理者，而是很純粹的中國網路攻擊。但若觀察，則可發現仍有母雞與小雞的操作痕

63. 共青團曾經承認其與帝吧的關係，若此關係可以確認，則可定義為中央的攻擊。第一個發布的帳號「洪水猛獸 baby」假新聞中有標註共青團，但目的不明，本文先作保守解釋。

64. Vinod Anand, "Chinese Concepts and Capabilities of Information Warfare," *Strategic Analysis*, Vol. 30, No. 4, October 2006, pp. 781-797.

65. Tim Thomas, "China's technology stratagems," *Jane's Intelligence Review*, Vol. 3, December 2000, pp. 33-37；林宗達，〈中共信息戰之網軍作戰初探〉，《展望與探索》，第 5 卷第 9 期，2007 年 9 月，頁 60-84。

66. 作者曾經訪談過 LINE 群組的揪群者，發現其無法理解注音文，此種現象，都有可能有民兵或武警介入的痕跡。沈伯洋，LINE 訪談，受訪人 F、G、H。

67. Felix Wu 於 2019 年 11 月，中國資訊作戰研討會之發言。其以空污議題為例，即可找出約兩千個 Facebook 中國帳號之母雞，帶著多位小雞做訊息傾倒攻擊。

跡。[67]

舉例而言，2019 年 12 月 6 日中國群組中即開始討論如何製造關於香港市民要跟臺灣政府求救的假新聞，其始於微博帳號（攻擊者），並在中國各論壇散布（擴散者），最後進入LINE群組成為我們資訊接收的來源（受害者），12 月 9 日微博再度製造我國法務部拒絕香港請求的假公文（攻擊者），並透過臺灣帝吧的粉絲專頁散布（擴張者），最後進入各政黨的粉絲專頁下留言（受害者），並有少數流到LINE群組。這與小粉紅製作關西機場蘇處長的假遺書手法可謂如出一轍。 Facebook、Instagram 在 2020 年亦與作者為相同之認定，並刪除特定社團帳號（如「中國解放軍武統臺灣省支持群組」和「帝吧」群組）。

此類粉紅模式對聲量的製造十分在行，並貢獻了不少社群媒體的垃圾資訊，舉例而言，作者觀測的 72 個在社團中高度互動的「境外帳號」中，有六個帳號在選舉六個月之內，平均「一人」在「單一社團」就留言了 1,370 次；其中一個為馬來西亞帳號、一個是印尼帳號，四個是中國帳號。而且也擔任大型社團（超過九萬人）的管理員，社團名稱本身與政治無關，但內容全部是政治。另一群（無重疊）之 55 人，2019 年 1 月到 5 月在 Facebook 上總共只留言 38 次，但是選舉期間（2019 年 6 月至 2020 年 1 月 11 日），留言高達 7,268 次，根本不是常人使用網路的方式（甚至偶而切換角色），也傾倒了大量網路垃圾至一般社團以及臺灣新聞粉專，並大量加入臺灣好友，試圖影響輿論。舉例而言，一般一群中國帳號彼此間之共同好友主要應為中國人自己，若有其他國家之共同好友，比例不會超過 5%；然而在選舉期間，大量中國與美國華人帳號，共同好友是臺灣人的比例皆超過20%，明顯為操縱輿論之帳號。而在 PTT 方面，此類大量發文、推文，在 2018 年 8 月開始來自於貴港市、桂林市、柳州市和蘇州。

由於粉紅模式的訊息並不精準，因此若他們自為散布，對臺灣的影響可謂不高；造成巨大影響的關西機場事件，可能臺灣自己要負更

多的責任（如政論節目的煽動、政府不當處置等）。然而，若粉紅模式的主導者(Adversary)有相關預算，並將製造與散布脫勾，仍可觸及百萬以上的臺灣使用者（如肺炎期間幫忙散布中國謠言的直播主，皆來自於兩家中資行銷、遊戲公司）。

此類模式之運作亦不限於臺灣，例如中國小粉紅在 Reddit 上面的行為，或者在國際組織 Twitter 帳號出征，在國外大學進行言論審查等等，皆為粉紅模式的體現。然而有所不同者在於：第一，除了外文程度之外，小粉紅在海外不易辨識，而在臺灣，由於語氣上的差別，很容易被辨識出來；第二，小粉紅訴求的對象多為海外華人，並加強外宣力道（與第一模式配合），因此其在海外的行動與在臺灣的行動並不一致。例如在疫情期間，好萊塢明星蓋兒加朵(Gal Gadot)在 IG 分享了新華社製作的大外宣影片，即得到大量小粉紅的跨海支持；針對塞爾維亞，中國則是動用了外宣加上小粉紅的攻勢，先是在塞爾維亞地方上出現感謝習近平的看板，然後動用機器人操作了 70%的親中推特貼文；[68]但在臺灣，小粉紅經典著作則是在臺灣大量製造虛假訊息，如臺南疫情失控，浮屍滿河；北市大巨蛋下面，埋了上千具武漢肺炎死者屍體等負面假訊息。此種訊息與正面訊息不同，目的是要造成恐慌，然而，若小粉紅要造成傷害，仍須藉助較為優良的內容製造，或者在地協力者的協助。這也是以下兩種模式特別重要之原因。

三、農場模式

農場模式是所有模式中最複雜的一種。如果把外宣模式當作是一種資本擁有者之間的合作或私相授受，粉紅模式是無資本者的亂槍打鳥，而農場模式則是介於中間，由追求認知領域作戰資本的角色互相

68. DFC, “A Bot Network Arrived in Serbia along with Coronavirus,” April 13, 2020, *Digital Forensic Center*, <https://dfcme.me/en/dfc-finds-out-a-botnet-arrived-in-serbia-along-with-coronavirus/>.

競爭，並在商業利益與統戰利益掛勾之下，呈現的一種認知領域作戰複合體。其主要攻擊手段就是透過網站之設置及爭議訊息的產製，並大量傳到臺灣閱聽者的眼前。

根據本研究備份資料，農場模式在一年半以來轉變了三次，分述如下。

（一）直營模式

此類模式最有名者為中國的無為科技公司，其在 Facebook 上蒐集個資，並創立農場之後，大量在 Facebook 散布臺灣政治性相關爭議訊息。前述所謂網路社團異常的高聲量，大部分由此而來，他們經常經營中性社團的方式吸引臺灣受眾，之後再更名為政治社團，例如「韓國瑜總統網軍後援會」社團，原本的名字是「華人聊天」。此類模式在 2019 年中漸漸式微，由下一模式取代；部分農場仍有自己官方的 LINE 帳號，追蹤人數可達 40-80 萬之譜，仍不失為有效率的傳播方式。

（二）盈利模式

由於農場經營粉專的風險過高，容易被平臺刪除，盈利模式在 2019 年 5 月之後變成最主要的農場散布模式，也是此次選舉的重心模式。由於有些農場完全沒有廣告，其如何營利即成為最大問題。而所謂的盈利模式就是將農場設立登入機制，吸引有粉專或社團者自行登入，其只要幫忙散播文章連結，即可獲利。

作者亦曾加入此類群組「大榴槤群」，其以新加坡幣做為獎勵發放，只要將連結與自己經營的粉絲專頁結合，則可獲取相當利潤。此類「在家賺錢」的廣告亦在群組內流傳。此種模式的好處為，即使粉絲專頁或社團被 Facebook 刪除，也不會影響到政治性網站的經營，農場只需要灑錢與製造內容即可。在內部群組的討論之中，有些散布者可以達到單日 14 萬的觸及數，而單月收益可達六萬臺幣。2019 年 11 月之後，Facebook 開始對此類農場的連結予以限制，而粉專經營者則開始紛紛出走，根據作者自行加入群組並假意購買之經驗，八萬追蹤

的粉專約以兩千美元的價碼售出，十五萬追蹤約以三萬五美金賣出（殺價後）。此亦可證明，散播者本身並沒有強烈政治傾向，而是「沒錢賺我就走人」的心態。

本研究於 370 個Facebook粉絲專頁和社團中，根據其分享的 2,440 個網域(Domain)，可找到約 26 萬 7,818 個網址，幾乎全是此類農場訊息，且集中在泛藍粉專與社團，部分並以寵物、算命等包裝，但參雜歌頌解放軍的訊息。其分享亦會躲避 Google 索引(Google Index)，無法以搜尋引擎搜尋其內文（亦即，有連結與編號才能夠看到文章），此類方式有兩個目的，一個是用特定連結計算各文章的分享營利；第二個目的是，藉由此方式，可以達到大量的 P2P 散布（如 LINE），卻無法被 Google 察覺。

本研究根據約 26 萬多個被 Facebook 分享的網址中，選出單日分享超過 250 次的粉專（共 89 個），並製作下圖。與圖 3 相同，左邊為網域，右邊為粉專，分享次數越多，線越粗，顏色則是根據不同粉專標示，從此圖亦可發現單點擴散特性：「一個網站同時由多個粉專轉發，而該粉專又只會分享特定網站。」（請見圖 14 及圖 15）若只單看作者加入的大榴槤群（圖 16），其特性更為明顯；而其社團的管理者，除了中國人之外，亦包含統促黨黨員。[69] 本文前述反滲透法的假新聞（用與反滲透法無關的案件包裝成白色恐怖報導），即是由中國農場製作之後，以此種方式大量散布於 Facebook（一個月互動約 40 萬），並於LINE廣傳，甚至出現「錄音」，表達自己正要被蔡政府敲門抓走。

69. Jason Liu, Ko Hao-hsiang, & Hsu Chia-yu, “How A Content Farm In Malaysia Turned Fake News Directed At Taiwan Into A Moneymaker,” *The Reporter*, March 12, 2020, <https://www.taiwangazette.org/news/2020/3/10/fake-news-in-taiwan-comes-from-a-trans-national-content-farm-in-malaysia>.

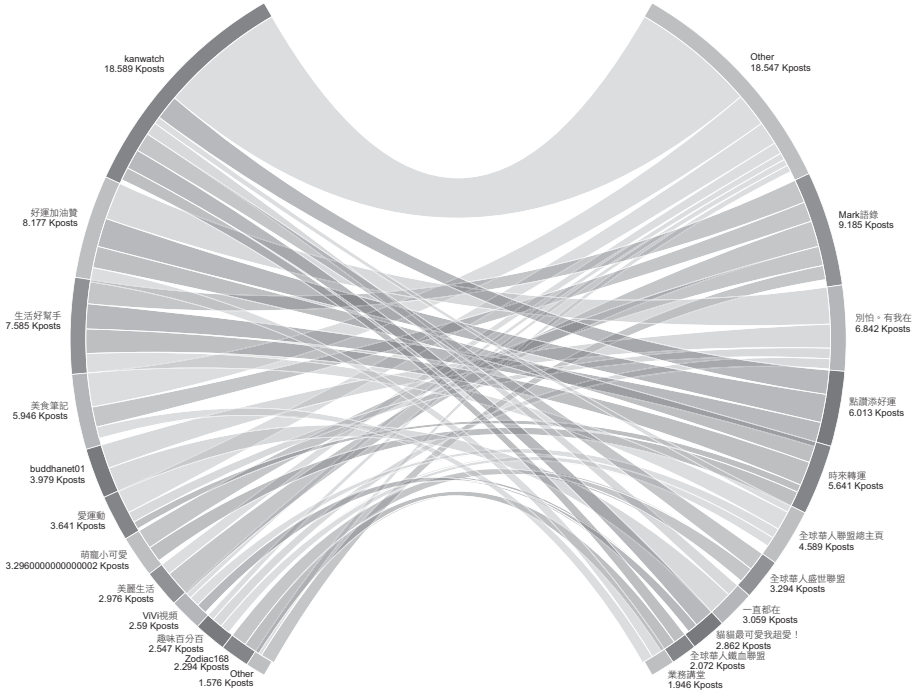

圖 14 網域與粉專關係圖(Top 89)

資料來源：作者自製。

說　　明：左側為網域，右側為粉專。另可見<https://plotdb.io/v/chart/25171> 。

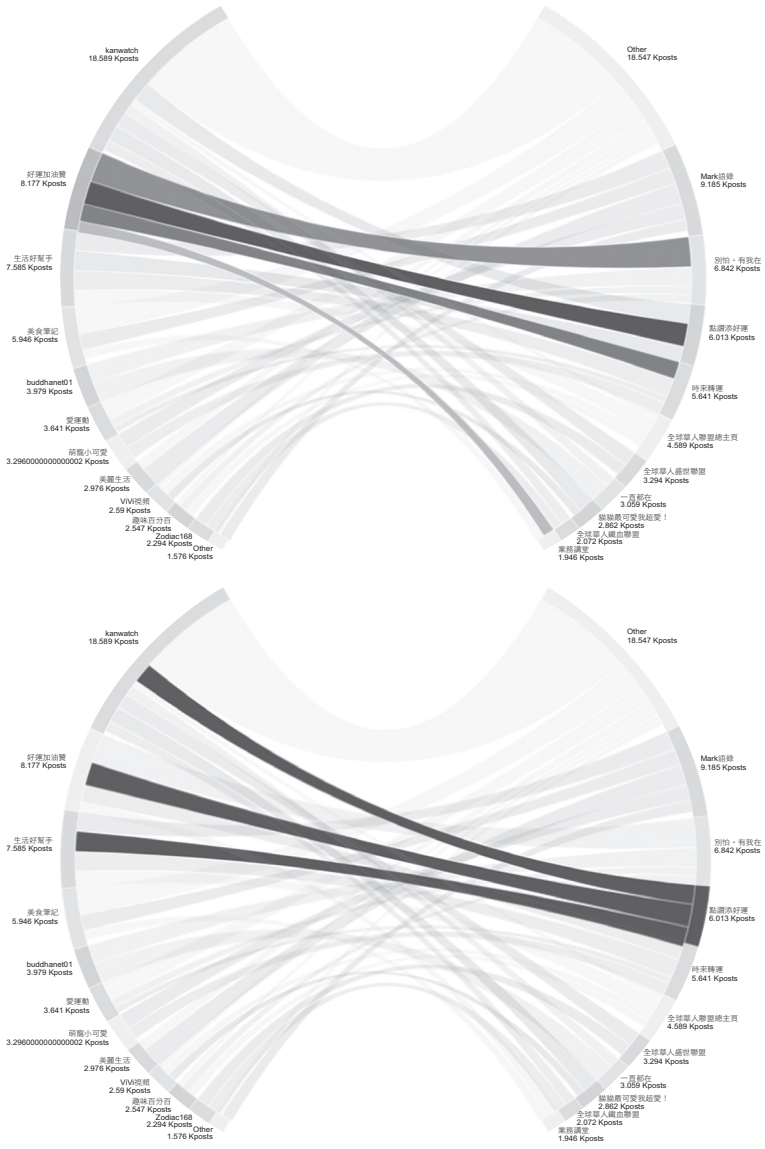

圖 15　「好運加油讚」及「點讚添好運」為例的分享特性

資料來源：作者自製。

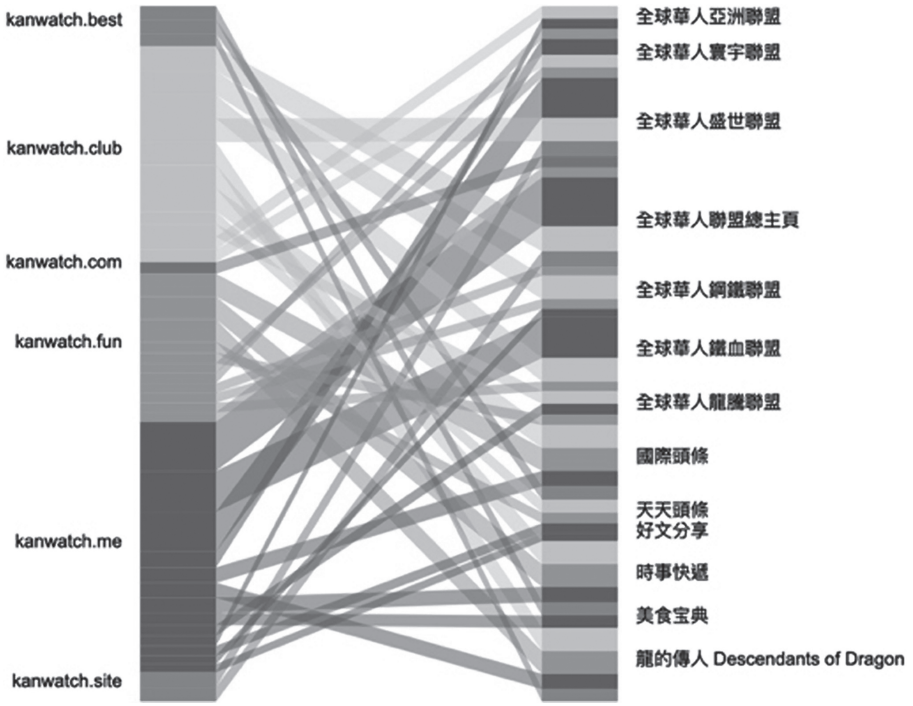

圖 16 「大榴槤群」的 Facebook 散布圖

資料來源：作者自製。

說　　明：左側網域皆為同一經營者，Evan Lee 右側為對應之臉書粉絲專業。Evan Lee 資料請見劉致昕、柯皓翔、許家瑜，〈LINE 群組的假訊息從哪來？跨國調查，追出內容農場「直銷」產業鏈〉，《報導者》，2019 年 12 月 26 日，<https://www.twreporter.org/a/information-warfare-business-disinformation-fake-news-behind-line-groups>。

（三）影片模式

在 2019 年 11 月之後，由於 Facebook 的強力取締，大量農場移往 YouTube 或 LINE 社群繼續經營。很多農場原本就有 YouTube 頻道，但觀看者通常不多，然而到了 11 月之後，許多 YouTube 相關頻道開始大量增加，並使用機器人複誦內容農場的文章，插入照片與圖片以利

影片製作；截至 2020 年 8 月，甚至出現以臺灣政論節目聲音作為基礎，並利用人工智慧方式模仿臺灣人說話來散布爭議訊息的新方式。2020 年 2 月之後，由於肺炎的疫情，頻道影片增加的速度擴增到三倍左右（從一日一更變成一日三到四更），即使頻道因為政治性內容被黃標（無法營利），亦完全無損於其製造與散布，變成主流的農場模式。亦即，從原本用「營利」的方式散布，改成用「演算法」的方式散布（用 YouTube 的演算法觸及群眾，而不用營利者的加入）。形成製造者與散布者完全脫勾的狀態。[70] 而第三節所述的異常影片連結分享，皆與此有關。

（四）與 LINE 的互動，以及與外宣、粉紅模式的差異

在營利與影片模式出現之後，由於在地協力者及演算法的協助，使得消息在LINE群組的散布倍增。但以陳菊貪污謠言為例，由圖 17、18 可知，Facebook 與 LINE 的散播高點相隔將近一個月，與一般訊息散布的速度不同。雖然中國新聞亦有報導陳菊相關事項，但從 2019 年 5 月 1 日至 2020 年 1 月 31 日，陳菊相關的中國境內報導和社群貼文僅有 1,272 篇。[71] 觀察其起落，高點是在 12 月 17 日，有 105 篇（請見圖 19），且新聞內容主要是在報導柯文哲與陳菊之間的恩怨。從此觀之，Facebook 的爭議訊息甚至比中國媒體還早出現，且小粉紅的活躍（微博）也在此之後，從此研判屬於農場的對外攻擊，而非由中國官媒主導的外宣模式或由粉紅發動的粉紅模式（亦即，發動不在中國，而可能為在地協力者）；亦即，中國更有可能只是在「見縫插針」，這就是一種製造者與散布者的脫勾，而中國可以有時扮演製造者，有

70. 典型頻道如「臺灣新聞 Today」，在美國註冊，另外連結兩個臺灣註冊的頻道，一個是醫療保健（五萬訂閱），一個是快速更新臺灣（六萬訂閱），內容雖是繁體中文，但有大量中國用詞，且政治性一面倒都是用農場轉譯的爭議訊息，跟新聞扯不太上關係。

71. 其中報導有 357 篇，微博 114 條，微信 551 篇，論壇兩篇。

時「只」扮演散播者。這也呼應了資訊作戰的指導原則：不問立場、只為分裂。

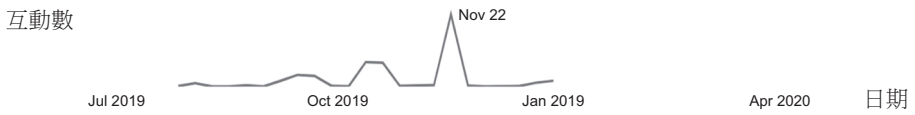

圖 17　Facebook 內爭議訊息的散播數量，以陳菊為例

資料來源：作者透過 CrowdTangle 製作。
說　　明：高點為 2019 年 11 月 17 日至 23 日。其中 22 日之互動數達 6,500 次。

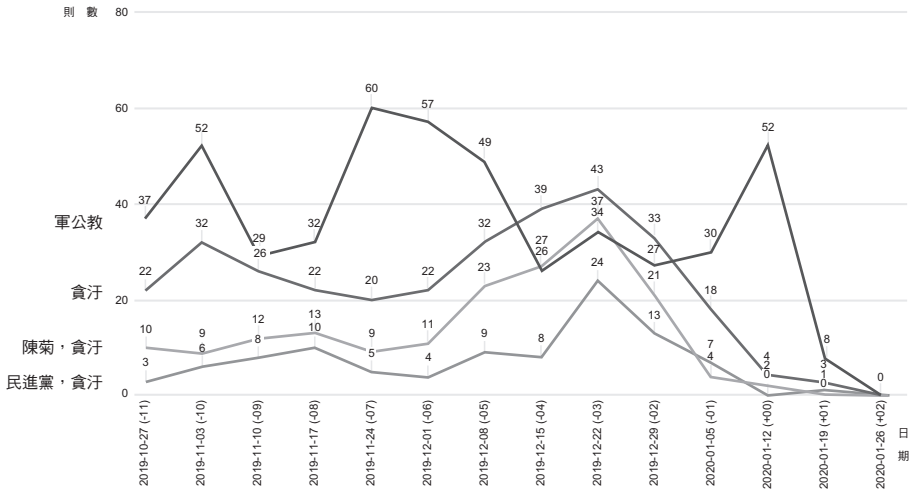

圖 18　LINE 內爭議訊息的散播數量，以陳菊為例

資料來源：作者自製。
說　　明：貪污與陳菊貪污的高點（43 則與 37 則）為 2019 年 12 月 22 日至 29 日。

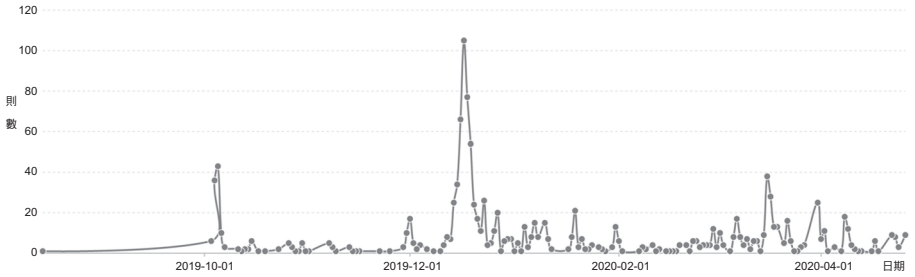

圖 19　中國國內陳菊相關貼文數量變化圖

資料來源：作者自製。
說　　明：高點為 2019 年 12 月 17 日。

農場模式在與 YouTube 結合之後，其成本理論上提高不少。長文的寫作通常更耗時費力，也因此，本研究推斷農場模式較少是個體戶；其必須有一定資本方可進行，[72] 甚至可能是專案進行，[73] 或有可能與官方有關。又由於影片較能吸引注意，加上盈利模式曾經與 Facebook 大量配合，因此本研究所指出的 YouTube、Facebook，以及 LINE 的異常分享現象，皆有可能是農場模式所導致，在本研究稿件截止前，YouTube 上針對臺灣的簡體中文農場，單一頻道平均即可單日破 40 萬次觀看。

四、協力模式

前幾種模式皆由政治動機者所發動，透過商業或中間人尋找散播者，或利用演算法做出無協力者的散播模式，然而，第四種的協力模式，卻不依循此種路徑：其製造者一開始就不在境外，形成了一個製

72. 更不要說許多農場歸屬同一集團，請見 Kayue，〈內容農場不想你知道的事〉，《關鍵評論網》，2019 年 10 月 26 日，<https://www.thenewslens.com/article/126592>。
73. 因為許多農場出現過「斷炊」狀況，一段時間完全不更新內容。

造者與散布者「無脫勾」的現象，此為最容易被忽略的認知領域作戰面向。

在臺灣的協力者中，不乏許多親中社團、政黨、政治人物或教授。如退休將領、宗親會、中華致公黨、光彩協會等等。協力模式會製造、綜合前三者的資訊，並進到臺灣的基層一線，此亦符合中國從 2017 年開始的「一代一線」的計畫：從接觸基層到透過中間的代理人，以頻繁地方交流的模式，達到統戰的目的。例如透過中華致公黨（代理人）接觸全國村里聯誼總會，或透過光彩協會接觸政治人物、又或者透過學校教授成立協會等等，都讓臺灣在地組織與中國處於統戰模式下的協力關係。然而統戰由來已久，其未必與認知領域作戰有關，因此，本文所關注的，是在統戰原本的結構下，所誕生的新的認知領域作戰模式。例如，統戰部在新北市舉辦的智慧社區論壇，推廣科技監控，降低國人戒心；又或者村里長直接接受中國補助，言談中美化和平協議，才是本研究所要關注之資訊攻擊方式。

選舉過程當中，此模式從製造到散布，都是由臺灣藉由協力者完成。例如與光彩集團有關之中國夢促進會，即在選舉期間製造小三通假新聞並散布到主流媒體。有趣地是，其最主要的散布對象可能是中國而非臺灣；亦即，對協力者來說，能夠製造此類新聞可能是為了達標或表態，也因此大力報導假新聞的反而是中國媒體而非臺灣媒體。由於光彩與統戰部有直接關係，此類模式可說是「中國資助，臺灣製造」的資訊攻擊，其對臺灣的影響僅取決於在地協力者的散播能力。同樣類型亦發生在中華致公黨，例如在反送中事件時，由中華致公黨所發布的「以香港今日之禍敬告天下洪門昆仲書」，看似中國警察製作，但原作卻是致公黨，然後再接受環球時報的專訪；再對中國人民發送假訊息。

所以真正對臺灣影響較大的，應是在對「臺灣」群眾散布的部分，而非上述中國國內報導。此攻擊可能是由較具資本的政黨進行（如新黨、致公黨），亦有可能透過臺商、教授或協會（如光彩）進

行之。舉例而言，光彩集團中的「臺灣光彩中辦青年股份有限公司」的董事長卓金鎊，同時即經營冠騰傳媒（指傳媒），專做兩岸新聞，並使用大量中國臺灣網（屬國臺辦）之爭議訊息，並與另外 22 家傳媒同時轉發國臺辦相關新聞，是資訊攻擊的明顯節點，亦會形成新聞與社群的異常數據；[74] 類似這種以地方小報和網站做攻擊的還有「互聯警政新聞網」，其發動的節點正與地方政黨有關，而其中擔任採訪的趙唯寧，也成為致公黨底下「青世代領航協會」的顧問。其餘協會例如明易協會等製作這種地方發送的農民曆爭議訊息（如武力統一臺灣），似乎已經是此等協力模式之常態了。另外，中國亦可採取較為間接的付款方式，例如本文第三節所列之頻道當中，有超過半數使用綠界等捐款支付方式，並在直播當中提供微信或支付寶的捐款連結。而啟人疑竇的，是臺灣極少有人使用此類方式捐款。

然而，本文認為，協力模式散播的方式最終仍舊必須回歸前述三種模式，並透過臺灣人慣用的新聞頻道、直播平臺、YouTuber、農場、LINE 或微信等來散播，方能有所成效。例如邱毅透過中國的「西瓜視頻」生產的選舉爭議訊息，終究必須透過 YouTube 來散布；若要影響選舉，最終仍需透過直播主等才能接觸到更多的年輕人（如 Instagram 的宣告投票意志事件，以及中國記者希達親自操刀的「玉山腳下」YouTube 頻道和其他電臺節目的製作），較簡單的方法，也有如擔任過北京政協顧問的徐正文，一方面擔任和平統一促進會常務理事的身分，一方面直接經營微信公眾號和韓國瑜粉專，散播爭議訊息。

74. 其中有民生新聞網、華民通訊社、民生導報、兩岸時報、城鄉新聞報、慈善新聞報、若水傳媒、兩岸好康報、海峽連線報導、村裡新聞網、藝傳媒、台中生活大小事、台灣省新聞記者協會新聞網、中華時報、亞傳媒、冠騰傳媒、亮點新聞網，當時全部共同貼出「今日蔡當局霸道拔『管』，明年民眾輕鬆拔『蔡』」的新聞，內容如出一轍。請見我心飛揚，〈今日蔡當局霸道拔「管」，明年民眾輕鬆拔「蔡」〉，《中國臺灣網》，2019 年 7 月 9 日，<http://big5.taiwan.cn/plzhx/wyrt/201907/t20190709_12182194.htm>。

較複雜的方式，則是將上述小報電子化之後，透過 Facebook 前述的粉專、社團手法予以散布。

其中最成功的，當屬與新黨密切相關的「密訊」內容農場。[75]其曾經在 2019 年 4 月創下最多分享次數的紀錄，分享數在當時是自由時報的五倍。2018 年九合一選舉之時，密訊甚至是新聞分享的第一名，但其包含大量爭議訊息，並與「怒吼」等農場，以及中時電子報等主流媒體互相拉抬，其中作者之一也不避諱使用「海峽導報」等新聞與中國媒體互相製造聲量。

由上可知，此大量生產文章並獲得成效的方式，首先是由協力模式「發起」，透過國臺辦、統戰部等先建立與臺灣政黨與地方團體、創業青年等的管道，並嘗試發動各種訊息，到最後「採用」了不斷進化的農場模式，與外宣模式的大媒體互相拉抬，形成了鋪天蓋地的資訊攻擊，可說是「集各模式之大成」。如果農場模式如上述不斷進化，那麼在這種「臺灣自製」的農場，可能是最成功的案例。如此一來，例如中國在臺灣收買 YouTuber，[76]以及四川基地想找網紅訓練等，[77]相比之下都是在「另闢協力蹊徑」。而由於協力模式多數由臺灣人製造，與傳統的粉紅、農場模式已有不同，其能造成的影響更為巨大。故，統戰部所能夠帶來的威脅，可能不下於管理網軍作戰和一般金流

75.經《報導者》追查，其顧問為方行商務整合行銷公司負責人林正國，也是新黨青年委員會委員。行銷公司代表人亦為新黨青年委員會委員。林正國同時亦經營「觸極者」農場，主要分享「兩岸青年派」的官方統戰節目。

76.在作者的訪談中，中國願意以一個月 150 萬臺幣價碼，換取臺灣 YouTuber 的親中論述。其他案例有肺炎期間的「搞個小小肺炎」，請見沈伯洋、曾柏瑜，〈疾病下的中國資訊作戰〉，《台灣民主實驗室》，2020 年 3 月 11 日，< https://medium.com/doublethinklab-tw>。

77.李秉芳，〈「買台灣比打台灣便宜」中國疑買粉絲頁、招募「支持統一」小編？陸委會：屬實將開罰〉，《關鍵評論網》，2019 年 4 月 6 日，<https://www.thenewslens.com/article/116816>。

的解放軍系統。[78]

同樣深受中國統戰的澳洲，其雖然亦受到中國資訊之攻擊，但程度相當不同。[79]首先，澳洲的統戰組織或解放軍相關組織從事間諜相關活動居多，並不是直接的認知領域作戰；雖然澳洲統戰組織也會試圖控制澳洲當地對中國歷史的解讀，除了小粉紅的出征外，仍舊偏向「講好中國故事」，而非像臺灣一般有系統地直接經營農場和負面爭議敘事。另外，中國在澳洲的行為，多半仍舊針對海外華人作為影響對象，然而在臺灣，由於並沒有所謂華人族群之異同，因此臺灣協力者亦與海外華人行動不同，主要是重新製造、生產與散布資訊。亦即，配合前述的農場，臺灣的特色在於「製造者與散布者的脫勾」，甚至出現「製造者與散布者皆不是中國」的奇特狀況。亦即，在統戰與資訊作戰的結合上，臺灣狀況可說是十分特殊；反觀澳洲，統戰組織多半仍舊以滲透工作為主，更多的工作內容仍聚焦於資料竊取、監控海外華人等態樣，與認知作戰並不完全重疊，而爭議訊息的製造者與散播者仍以中國為主，此點與臺灣有極大差異。

伍、結論

目前針對基礎設施的異常，研究訊息的「擴散行為模式」已成為主流，[80]其中一些數位追查標準，如低頻率發文、高產出、交互發表相

78. 尤有甚者，長期與中國交流的退休群組中，作者也看見疑似解放軍的帳號，並散布爭議訊息。群組內不乏臺灣退休高官，造成之資訊攻擊可謂嚴重。

79. 相關文獻可參考 Clive Hamilton & Alex Joske, *Silent Invasion: China's Influence in Australia* (Melbourne: Hardie Grant Books, 2018), pp. 113-142.

80. Richard Gunther, Paul A. Beck, & Erik C. Nisbet, "Fake news did have a significant impact on the vote in the 2016 election: Original full-length version with methodological appendix," April 23, 2020, Accessed, *OSU*, <https://cpb-us-w2.wpmucdn.com/u.osu.edu/dist/d/12059/files/2015/03/Fake-News-Piece-for-The-Conversation-with-methodological-appendix-11d0ni9.pdf>;

同圖文、情境比對、竊取圖或分享一樣的頭像、亂數生產之名稱、多語言、大量廣告、特定的縮網址服務、集中效應等等，部分方式已為本文所用。而以流量與特定族群的比對來計算是否有操作之嫌疑之「流量計算法」(Coefficient of Traffic Manipulation, CTM)為現今通用之作法。[81] 各大平臺如 Facebook 和 Twitter 則是專注在「協同性造假」(Coordinated Inauthentic Behavior, CIB)來偵測網路軍隊，並使其下架。[82] 本研究已應用其中幾種方式提出異常圖象，但未來需以更細緻的檢驗標準觀察之。況且，光是指出異常，卻無法歸責，則沒有意義。[83] 因此，本文提出了四個模式（表 2 與圖 13），希望有利於往後

S. Mo Jang, Tieming Geng, Jo-Yun Queenie Li, Ruofan Xia, Chin-Tser Huang, Hwalbin Kim, & Jijun Tang, "A computational approach for examining the roots and spreading patterns of fake news: Evolution tree analysis," *Computers in Human Behavior*, Vol. 84, July 2018, pp. 103-113; DFRLab, "Human, Bot or Cyborg?"

81. Ben Nimmo, "Measuring Traffic Manipulation on Twitter," January 2019, *OII*, <https://comprop.oii.ox.ac.uk/research/working-papers/twitter-traffic-manipulation/>.

82. Fabio Giglietto, Nicola Righetti, & Giada Marino, "Understanding Coordinated and Inauthentic Link Sharing Behavior on Facebook in the Run-up of 2018 General Election and 2019 European Election in Italy," January 15, 2019, *OII*, <https://doi.org/10.31235/osf.io/3jteh>; Jen Weedon, William Nuland, & Alex Stamos, "Information operations and Facebook," April 27, 2017, *Facebook*, <https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf>.

83. GB Dobson, A. Rege, & KM Carley, "Informing Active Cyber Defence with Realistic Adversarial Behaviour," *Journal of Information Warfare*, Vol. 17, No. 2, Spring 2018, pp. 16-31; Ke Wu, Song Yang, & Kenny Q. Zhu, "False rumors detection on sina weibo by propagation structures," paper presented at the 2015 IEEE 31st international conference on data engineering (Seoul: IEEE, April 15-17, 2015), pp. 651-662.

認知領域作戰的研究。

然而，對於內容(capability)的分類，以及被害狀況(victim)等，礙於篇幅，需留待日後分析，尤其是被害者部分，必須確認臺灣可能的受害者是哪些族群，以及被影響的方式等等，方可確認認知領域作戰的規模。[84]至於在內容方面，許多的爭議訊息並不是假新聞，而是有認知框架的敘事(narrative)。[85]例如，中國喜歡製造大量的「中國贏了中美貿易戰」的偏頗新聞，美國也喜歡大量製造「美國獨強」的敘事，如果只聚焦在假訊息、假新聞，則無法看出爭議訊息攻擊的全貌。

本研究在初步編碼 2,000 篇農場文章下，暫時的「敘事」主題分類有：軍事、外交、基礎建設、經濟金融、健康疾病、醜聞、商業、民生、LGBT、世代差異、移民、能源議題、美中關係、勞資議題、轉型正義、身分認同等。由於俄羅斯在選定議題時，研究指出其會對特定敘事的分類來做分眾攻擊，甚至分享大量真實、科學新聞作為「矯正」，[86]這些議題或多或少都會引發一些情緒（包含希望、愛、不喜

84. 目前作者根據 3,752 份問卷，已有對受害者初步的四個歸類，將留待日後解析。

85. Juan P. Cardenal, et al., *Sharp Power: Rising Authoritarian Influence*, pp. 7-13.

86. David A. Broniatowski, Amelia M. Jamison, SiHua Qi, Lulwah AlKulaib, Tao Chen, Adrian Benton, Sandra C. Quinn, & Mark Dredze, "Weaponized health communication: Twitter bots and Russian trolls amplify the vaccine debate," *American Journal of Public Health*, Vol. 108, No. 10, September 2018, pp. 1378-1384; Mark Davis, "Globalist war against humanity shifts into high gear: Online anti-vaccination websites and anti-public discourse," *Public Understanding of Science*, Vol. 28, No. 3, December 2019, pp. 357-371; Darren L. Linvill, et al., "'THE RUSSIANS ARE HACKING MY BRAIN!' investigating Russia's internet research agency twitter tactics during the 2016 United States presidential campaign," *Computers in Human Behavior*, Vol. 99, October 2019, pp. 292-300.

歡、恐懼、憤怒、焦慮、討厭、同情、驚喜等），[87] 並利用爭議訊息攻擊的常見手法來觸動認知偏誤（如可用性偏差、確認偏差、諧振、認知失調、信託稀釋、中和、寧可相信等等）。[88] 因此，中國如何選擇內容及其戰術為何，必須留待日後專文分析。在目前主流文獻當中，對於爭議訊息攻擊主要聚焦在 4D (Distract、Distort、Dismay、Dismiss)，[89] 但在作者初步研究當中，發現臺灣面臨的手法遠多於 4D，此亦值得於未來深入關注。

而國人最關心的，當屬中國資訊作戰到底有無「效果」。此問題可拆解成兩個部分，一個是有無攻擊，另一個是有無受害。針對前者，由於攻擊模式眾多，各模式是否有互相配合並造成傷害即變成重要之課題。例如，當粉紅模式與農場模式結合，即可擴大打擊點，造成不實訊息廣泛散布。然而擴大打擊點不代表有人會受害。台灣民主實驗室在選舉當天的出口民調即發現，傳播太廣的陰謀論，反而沒有效果。真正有效果的是小範圍、負面訊息的散布。[90] 因此，當如果粉紅

87. Xiaolei Huang, Lei Zhang, David Chiu, Tianli Liu, Xin Li, & Tingshao Zhu, “Detecting suicidal ideation in Chinese microblogs with psychological lexicons,” paper presented at the 2014 IEEE 11th Intl Conf on Ubiquitous Intelligence and Computing (UIC: IEEE, November 4, 2014), pp. 844-849; Elvis Saravia, Hsien-Chi Toby Liu, Yen-Hao Huang, Junlin Wu, & Yi-Shin Chen, “CARER: Contextualized affect representations for emotion recognition,” paper presented at the Proceedings of the 2018 Conference on Empirical Methods in Natural Language Processing (Brussels: EMNLP, November 4, 2018), pp. 3687-3697.

88. A. Lemay & SP Leblanc, “Iterative Analysis of Competing Hypotheses to Overcome Cognitive Biases in Cyber Decision-Making,” *Journal of Information Warfare*, Vol. 17, No. 2, Spring 2018, pp. 42-44.

89. Jon White, “Dismiss, distort, distract, and dismay: Continuity and change in Russian disinformation,” *Institute for European Studies Policy Brief*, No. 13, May 2016, pp. 1-3.

模式與農場模式大量地在網路製造聲量，卻沒有與在地協力者合作之時，則會形成網路聲量的「虛胖」，無法與真實狀況做出對應，自然難以拉抬選票；反之，如果協力模式與其他模式相配合之時，小群組的謠言、LINE 群組的散布等等，即會形成小範圍、但是有效的「精準打擊」。

亦即，資訊攻擊在選舉過程中是否成功的條件，與地面統戰息息相關：例如是否有記者、電視臺、里長等等的配合，即成為關鍵。如果地面的資訊流動與空中的資訊流動不一致，則效果有限。作者認為，2018 年縣市長選舉中，協力者與空中資訊的配合較為綿密，因此對於選舉結果影響甚鉅；2020 年總統大選雖然仍有影響，但協力者因為民意轉向（反滲透法通過、反送中運動及反紅媒運動出現）難以大量配合，使得資訊攻擊雖然廣泛，卻顯虛胖，最後僅有分裂效果，無法再往上升級成大量選民意向之轉變；對此，2020 年中國的資訊攻擊效果可說是「CP 值略低」。疫情時期亦然，雖然中國有廣泛的資訊攻擊，卻因為每日疾管署記者會使得不實訊息難以發酵（無地面配合），最終僅造成部分恐慌與不信任。不過，這類資訊攻擊雖不會立即發生效應。但仍舊會造成深遠的影響：因為部分僅以線上資訊接收為主的臺灣人，仍會因各式不同的陰謀論而分裂、敵視，並可能在不遠的將來產生「質變」。

因此，2019 年通過之反滲透法在法制上自有其意義，但遠遠不足。就法制而言，由於每一個發動者的動機、資本與模式皆有不同，自應有不同對應方案，無法以單一法案處理之：外宣模式由於資本龐大，且與投資有關，必須由限制中資之立法應對，且因為其打擊點廣，應由官方回應處理；粉紅模式和農場模式因為涉及海外發動者，故與社群平臺合作較能處理（如以 CIB 標記）；最後的協力模式，因

90. 曾柏瑜、陳韻如，〈假訊息對選民的影響分析〉，2020 年 4 月 29 日，《台灣民主實驗室》，<https://medium.com/doublethinklab-tw>。

為牽扯到國內在地協力者，應予以揭露，使用代理人法(Foreign Agent Registration Act)應為適切方案。亦即，未來需對每一個模式的資本與動機予以歸納，並給予不同的「強弱分數」，以資應對；針對不同的發動者與散播者做出不同程度的法律規範，亦可避免一體適用單一法律。而使用代理人法制作為「揭露」，遠比針對內容作真偽審查來得有效，亦可保障國人之言論自由。

（收件：2020 年 5 月 6 日；修正：2020 年 10 月 20 日；採用：2020 年 11 月 5 日）

參考文獻

中文部分

專書

喬良、王湘穗，1999。《超限戰：兩個空軍大校對全球化時代戰爭與戰法的想定》。北京：解放軍文藝出版社。

何清漣，2019。《紅色滲透》。臺北：八旗文化。

沈偉光，2003。《新戰爭論》。杭州：浙江大學。

林中斌，1999。《核霸：透視跨世紀中共戰略武力》。臺北：臺灣學生書局。

專書論文

吳介民，2017。〈以商業模式做統戰：跨海峽政商關係中的政治代理機制〉，李宗榮、林宗弘主編，《未竟的奇蹟：轉型中的台灣經濟與社會》。臺北：中央研究院社會學研究所，頁 675-720。

期刊論文

王高成，2004/4。〈中共不對稱作戰戰略與臺灣安全〉，《全球政治評論》，第 6 期，頁 19-33。

呂爾浩、魏澤民，2006/7。〈中國資訊作戰的類型分析〉，《遠景基金會季刊》，第 7 卷第 3 期，頁 187-229。

林宜昌，2019/12 月。〈資訊戰對國軍防衛作戰重要性之研究〉，《海軍學術雙月刊》，第 53 卷第 6 期，頁 116-126。

林宗達，2005/10。〈中共軍民信息技術的聯合發展〉，《展望與探索》, 第 3 卷第 10 期，頁 34-52。

林宗達，2007/9。〈中共信息戰之網軍作戰初探〉，《展望與探索》，第 5 卷第 9 期，頁 60-84。

彭錦珍，2004/12。〈資訊時代中共國防現代化之研究－解放軍信息戰發展及其對台海安全之衝擊〉，《復興崗學報》，第 82 期，頁 187-218。

蔡輝榮、吳宗禮，2007/1。〈面對資訊作戰之準備、發展與落實〉，《資通安全專論》，第 T96019 期，頁 1-27。

研討會論文

沈伯洋，2019/12/12。〈初探資訊戰攻擊節點〉，「解構銳實力」研討會。高雄：中山大學。頁 269-283。

黃兆年，2019/12/12。〈紅色滲透下台灣媒體人的日常抵抗〉，「解構銳實力」研討會。高雄：中山大學。頁 177-203。

研究計畫

寇健文，2019。《中國大陸對臺工作組織體系與人事（計畫編號：107A107089）》。臺北：行政院大陸委員會。

網際網路

2018/11/5。〈兩岸新媒體大陸行，難說再見〉，《華廣網》，<http://www.chbcnet.com/normal/content/chbcnet/hgbd/content/2018-11/05/content_1346613.htm>。

2019/12/31。〈為配合「反滲透法」過關 臺當局一天抓 10 多名臺灣共產黨成員〉，《觀察者》，<https://www.guancha.cn/politics/2019_12_31_530036.shtml>。

Gene Hong，2019/12/31。〈從新聞與社群來看韓流現像的典範轉移？〉，《Medium》，<https://link.medium.com/ByM6wBSUu4>。

Kayue，2019/10/26。〈內容農場不想你知道的事〉，《關鍵評論網》，<https://www.thenewslens.com/article/126592>。

Noxinfluencer，2020/4/23（檢索）。〈全方位分析提升網紅影響力〉，

《Noxinfluencer》，<https://tw.noxinfluencer.com/>。

TH Schee，2019/8/3。〈關於 LINE 的一些數字—從 SEC Form 20-F 閒聊起〉，《TH Schee blog》，<https://blog.schee.info/2019/08/03/line-form-20f/>。

我心飛揚，2019/7/9。〈今日蔡當局霸道拔「管」，明年民眾輕鬆拔「蔡」〉，《中國臺灣網》，<http://big5.taiwan.cn/plzhx/wyrt/201907/t20190709_12182194.htm>。

沈伯洋、曾柏瑜，2020/3/11。〈疾病下的中國資訊作戰〉，《台灣民主實驗室》，< https://medium.com/doublethinklab-tw>。

曾柏瑜、陳韻如，2020/4/29。〈假訊息對選民的影響分析〉，《台灣民主實驗室》，<https://medium.com/doublethinklab-tw>。

李秉芳，2019/4/6。〈「買台灣比打台灣便宜」中國疑買粉絲頁、招募「支持統一」小編？陸委會：屬實將開罰〉，《關鍵評論網》，<https://www.thenewslens.com/article/116816>。

劉致昕、柯皓翔、許家瑜，2019/12/26。〈LINE 群組的假訊息從哪來？跨國調查，追出內容農場「直銷」產業鏈〉，《報導者》，<https://www.twreporter.org/a/information-warfare-business-disinformation-fake-news-behind-line-groups>。

蘇穩中，2019/6/21。〈中時記者離職前沉痛告白〉，《放言》，<https://reurl.cc/nzZRr1>。

訪談資料

沈伯洋，2018/12/20。當面訪談，受訪人 A，臺北市。

沈伯洋，2018/12/20。當面訪談，受訪人 B，臺北市。

沈伯洋，2019/1/18。當面訪談，受訪人 C，臺北市。

沈伯洋，2019/1/22。當面訪談，受訪人 D、E，臺北市。

沈伯洋，2019/1/1-5/3。LINE 訪談，受訪人 F、G、H。

英文部分

專書

Bourdieu, Pierre, 1998. *Practical Reason: On the Theory of Action*. Stanford: Stanford University Press.

Caliskan, Murat, 2018. *Modern Political Warfare: Current Practices and Possible Responses*. California: Taylor & Francis.

Cardenal, Juan P, et al., 2017. *Sharp Power: Rising Authoritarian Influence*. Washington, D.C.: National Endowment for Democracy.

Chivvis, Christopher S., 2017. *Understanding Russian Hybrid Warfare*. California: Rand Corporation.

Diamond, Larry & Orville Schell, 2019. *China's Influence and American Interests: Promoting Constructive Vigilance*. Stanford: Hoover Institution press.

DiResta, Renee & Shelby Grossman, 2019. *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019*. Stanford: Internet Observatory.

DiResta, Renee, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, & Ben Johnson, 2019. *The Tactics & Tropes of the Internet Research Agency*. Annapolis: US New Knowledge.

Hamilton, Clive & Alex Joske, 2018. *Silent Invasion: China's Influence in Australia*. Melbourne: Hardie Grant Books.

Libicki, Martin C., 1995. *What is Information Warfare?* Washington, D.C.: National Defense University Press.

Mattis, Peter & Matthew Brazil, 2019. *Chinese Communist Espionage: An Intelligence Primer*. Annapolis: US Naval Institute Press.

Pomerantsev, Peter & Michael Weiss, 2013. *The Menace of Unreality:*

How the Kremlin Weaponizes Information, Culture and Money. New York: Institute of Modern Russia.

Slipchenko, Vladimir, 1999. *Voina Budushchego*. Moscow: Moskovskii Obshchestvennyi Nauchnyi Fond.

專書論文

Brazzoli, Mario Silvino, 2007. "Future prospects of information warfare and particularly psychological operations," in Len Le Roux ed., *South African Army Vision 2020*. Pretoria: D&V. pp. 217-232.

期刊論文

Anand, Vinod, 2006/10. "Chinese Concepts and Capabilities of Information Warfare," *Strategic Analysis*, Vol. 30, No. 4, pp. 781-797.

Arif, Ahmer, Leo Graiden Stewart, & Kate Starbird, 2018/11. "Acting the part: Examining information operations within # BlackLivesMatter discourse," *Proceedings of the ACM on Human-Computer Interaction*, Vol. 2, Issue CSCW, pp. 20-46.

Aro, Jessikka, 2016/5. "The cyberspace war: propaganda and trolling as warfare tools," *European view*, Vol. 15, No. 1, pp. 121-132.

Bail, Christopher A., Brian Guay, Emily Maloney, Aidan Combs, D Sunshine Hillygus, Friedolin Merhout, Deen Freelon, & Alexander Volfovsky, 2020/1. "Assessing the Russian Internet Research Agency's impact on the political attitudes and behaviors of American Twitter users in late 2017," *Proceedings of the National Academy of Sciences*, Vol. 117, No. 1, pp. 243-250.

Broniatowski, David A., Amelia M. Jamison, SiHua Qi, Lulwah AlKulaib, Tao Chen, Adrian Benton, Sandra C. Quinn, & Mark Dredze, 2018/9. "Weaponized health communication: Twitter bots and Russian trolls

amplify the vaccine debate," *American Journal of Public Health*, Vol. 108, No. 10, pp. 1378-1384.

Casey, George W. Jr., 2009/10. "The army of the 21st century," *Army Magazine*, Vol. 59, No. 10, pp. 25-40.

Davis, Mark, 2019/12. "Globalist war against humanity shifts into high gear: Online anti-vaccination websites and anti-public discourse," *Public Understanding of Science*, Vol. 28, No. 3, pp. 357-371.

Dobson, GB, A. Rege, & KM Carley, 2018/Spring. "Informing Active Cyber Defence with Realistic Adversarial Behaviour," *Journal of Information Warfare*, Vol. 17, No. 2, pp. 16-31.

Duczynski, Guy & Charles Knight, 2018/Winter. "Strategic-Intelligence Analysis: Contributions from an Operational-Design Orientation," *Journal of Information Warfare*, Vol. 17, No. 1, pp. 16-30.

Ferrara, Emilio, 2017/7. "Disinformation and social bot operations in the run up to the 2017 French presidential election," *First Monday*, Vol. 22, No. 8, pp. 1-33.

Guess, Andrew, Brendan Nyhan, & Jason Reifler, 2018/1. "Selective exposure to misinformation: Evidence from the consumption of fake news during the 2016 US presidential campaign," *European Research Council*, Vol. 9, No.3, pp. 1-10.

Jang, S. Mo, Tieming Geng, Jo-Yun Queenie Li, Ruofan Xia, Chin-Tser Huang, Hwalbin Kim, & Jijun Tang, 2018/7. "A computational approach for examining the roots and spreading patterns of fake news: Evolution tree analysis," *Computers in Human Behavior*, Vol. 84, No. 103-113.

King, Gary, Jennifer Pan, & Margaret E Robert, 2013/5. "How Censorship in China Allows Government Criticism but Silences Collective Expression," *American Political Science Review*, Vol. 107, No. 2, pp.

326-343.

Lazer, David M. J., et al., 2018/3. “The science of fake news,” *Science*, Vol. 359, No. 6380, pp. 1094-1096.

Lemay, A., & SP Leblanc, 2018/Spring. “Iterative Analysis of Competing Hypotheses to Overcome Cognitive Biases in Cyber Decision-Making,” *Journal of Information Warfare*, Vol. 17, No. 2, pp. 42-44.

Linvill, Darren L., et al., 2019/10. “‘THE RUSSIANS ARE HACKING MY BRAIN!’ investigating Russia’s internet research agency twitter tactics during the 2016 United States presidential campaign,” *Computers in Human Behavior*, Vol. 99, pp. 292-300.

Munger, Kevin, Rich Bonneau, John T. Jost, Jonathan Nagler, & Joshua Tucker, 2019/10. “Elites Tweet to get Feet off the Streets: Measuring Elite Reaction to Protest Using Social Media,” *Political Science Research and Methods*, Vol. 7, No. 4, pp. 815-834.

Reisinger, Heidi & Alexandr Golts, 2014/11. “Russia’s hybrid warfare,” *NATO Defense College*, Vol. 105, pp. 1-12.

Sanovich, Sergey, Denis Stukal, & Joshua Tucker, 2018/4. “Turning the Virtual Tables: Government Strategies for Addressing Online Opposition with an Application to Russia,” *Comparative Politics*, Vol. 50, No. 3, pp. 435-82.

Shu, Kai, Amy Sliva, Suhang Wang, Jiliang Tang, & Huan Liu, 2017/9. “Fake news detection on social media: A data mining perspective,” *ACM SIGKDD Explorations Newsletter*, Vol. 19, No. 1, pp. 22-36.

Thomas, Tim, 2000/12. “China’s technology stratagems,” *Jane’s Intelligence Review*, Vol. 3, pp. 37-39.

White, Jon, 2016/5. “Dismiss, distort, distract, and dismay: Continuity and change in Russian disinformation,” *Institute for European Studies Policy Brief*, No. 13, pp. 1-3.

研討會論文

Al-Mohannadi, Hamad, Qublai Mirza, Anitta Namanya, Irfan Awan, Andrea Cullen, & Jules Disso, 2016/8/22-24. “Cyber-attack modeling analysis techniques: An overview,” paper presented at the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops. Vienna: IEEE. pp. 69-76.

Huang, Xiaolei, Lei Zhang, David Chiu, Tianli Liu, Xin Li, & Tingshao Zhu, 2014/11/4. “Detecting suicidal ideation in Chinese microblogs with psychological lexicons,” paper presented at the 2014 IEEE 11th Intl Conf on Ubiquitous Intelligence and Computing. UIC: IEEE. pp. 844-849.

Niven, Timothy & Hung-Yu Kao, 2020/12/12. “Measuring Alignment to Authoritarian State Media as Framing Bias,” paper presented at the ACL Anthology. Barcelona: ICCL. pp. 11-21.

Saravia, Elvis, Hsien-Chi Toby Liu, Yen-Hao Huang, Junlin Wu, & Yi-Shin Chen, 2018/11/4. “CARER: Contextualized affect representations for emotion recognition,” paper presented at the Proceedings of the 2018 Conference on Empirical Methods in Natural Language Processing. Brussels: EMNLP. pp. 3687-3697.

Shu, Kai, Suhang Wang, & Huan Liu, 2019/2/11-12. “Beyond news contents: The role of social context for fake news detection,” paper presented at the Proceedings of the Twelfth ACM International Conference on Web Search and Data Mining. Melbourne: WSDM. pp. 312-320.

Stewart, Leo G., Ahmer Arif, & Kate Starbird, 2018/2/9. “Examining trolls and polarization with a retweet network,” paper presented at the Proc. ACM WSDM, Workshop on Misinformation and Misbehavior

Mining on the Web. Los Angeles: ACM.

Wu, Ke, Song Yang, & Kenny Q. Zhu, 2015/4/15-17. “False rumors detection on sina weibo by propagation structures,” paper presented at the 2015 IEEE 31st international conference on data engineering. Seoul: IEEE. pp. 651-662.

Yadav, Tarun & Arvind Mallari Rao, 2015/8/10-13. “Technical aspects of cyber kill chain,” paper presented at the International Symposium on Security in Computing and Communication. Kerala: SSCC. pp. 438-452.

官方文件

Wardle, Claire & Hossein Derakhshan, 2017/9. “Information Disorder: Toward an interdisciplinary framework for research and policy making,” *Council of Europe Report*, Vol. 27, pp. 29-38.

網際網路

Caltagirone, Sergio, Andrew Pendergast, & Christopher Betz, 2013/7. “The diamond model of intrusion analysis,” *DEFENSE TECHNICAL INFORMATION CENTER*, <https://apps.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf>.

Center of Excellence, 2020/4/6(accessed). “Hybrid Threats,” *Hybrid CoE*, <https://www.hybridcoe.fi/>.

Decker, Ben, 2019/8. “Adversarial Narratives: A New Model for Disinformation,” *GDI*, <https://disinformationindex.org/>.

Degital Society Project, 2019/4/9. “Foreign Government Dissemination of False Information,” *Degital Society Project*, <http://digitalsocietyproject.org/foreign-intervention-on-social-media/>.

DFC, 2020/4/13. “A Bot Network Arrived in Serbia along with Coronavirus,”

Digital Forensic Center, < https://dfcme.me/en/dfc-finds-out-a-botnet-arrived-in-serbia-along-with-coronavirus/>.

DFRLab, 2016/12/23. "Human, Bot or Cyborg?" *DFRLab*, <https://medium.com/@DFRLab/human-bot-or-cyborg-41273cdb1e17>.

Epstein, Robert, 2020/4/6(accessed). "Why Google Poses a Serious Threat to Democracy, and How to End That Threat," *Mercatornet*, <https://mercatornet.com/why-google-poses-a-serious-threat-to-democracy-and-how-to-end-that-threat/24598/>.

Giglietto, Fabio, Nicola Righetti, & Giada Marino, 2019/1/15. "Understanding Coordinated and Inauthentic Link Sharing Behavior on Facebook in the Run-up of 2018 General Election and 2019 European Election in Italy," *OII*, <https://doi.org/10.31235/osf.io/3jteh>.

Guess, Andrew, Benjamin Lyons, Jacob M. Montgomery, Brendan Nyhan, & Jason Reifler, 2018/2. "Fake news, Facebook ads, and misperceptions: Assessing information quality in the 2018 US midterm election campaign," *Dartmouth College*, <https://www.dartmouth.edu/~nyhan/fake-news-2018.pdf >.

Gunther, Richard, Paul A. Beck, & Erik C. Nisbet, 2020/4/23 (accessed). "Fake news did have a significant impact on the vote in the 2016 election: Original full-length version with methodological appendix," *OSU*, <https://cpb-us-w2.wpmucdn.com/u.osu.edu/dist/d/12059/files/2015/03/Fake-News-Piece-for-The-Conversation-with-methodological-appendix-11d0ni9.pdf>.

Hoffman, Samantha, 2019/10. "Engineering global consent: The Chinese Communist Party's data-driven power expansion," *ASPI*, <https://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion>.

Insikt Group, 2020/4/23(accessed). "Beyond Hybrid War: How China

Exploits Social Media to Sway American Opinion," *Recorded Future*, <https://www.recordedfuture.com/china-social-media-operations/>.

International Commission of Jurists, 2020/4/6(accessed). "Dictating the Internet: Curtailing Free Expression, Opinion and Information Online in Southeast Asia," *International Commission of Jurists*, <https://www.icj.org/southeast-asia-icj-launches-report-on-increasing-restrictions-on-online-speech/>.

Jeff Kao, & Mia Shuang Li, 2020/3/26. "How China Built a Twitter Propaganda Machine Then Let It Loose on Coronavirus," *ProPublica*, <https://www.propublica.org/article/how-china-built-a-twitter-propaganda-machine-then-let-it-loose-on-coronavirus>.

Liu, Jason, Ko Hao-hsiang, & Hsu Chia-yu, 2020/3/12. "How A Content Farm In Malaysia Turned Fake News Directed At Taiwan Into A Moneymaker," *The Reporter*, <https://www.taiwangazette.org/news/2020/3/10/fake-news-in-taiwan-comes-from-a-trans-national-content-farm-in-malaysia>.

Miller, Blake, 2016/4/21(accessed). "Automated detection of Chinese government astroturfers using network and social metadata," *SSRN*, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2738325>.

Narayanan, Vidya, Vlad Barash, John Kelly, Bence Kollanyi, Lisa-Maria Neudert, & Philip N. Howard, 2020/4/23(accessed). "Polarization, partisanship and junk news consumption over social media during the 2018 US Midterm Elections," *Cornell University arXiv*, <https://arxiv.org/abs/1803.01845>.

National Intelligence Council, 2017/1/6. "Assessing Russian activities and intentions in recent US elections," *Director of National Intelligence*, <https://www.dni.gov/files/documents/ICA_2017_01.pdf>.

Nimmo, Ben, 2019/1. "Measuring Traffic Manipulation on Twitter," *OII*,

<https://comprop.oii.ox.ac.uk/research/working-papers/twitter-traffic-manipulation/>.

Scheidt, Melanie, 2020/4/6(accessed). "The European Union versus External Disinformation Campaigns in the Midst of Information Warfare: Ready for the Battle?" *University of Pittsburgh*, <http://aei.pitt.edu/100447/>.

Stanford Internet Observatory, 2020/1/21. "Taiwan Election: Disinformation as a Partisan Issue," *Stanford Internet Observatory*, <https://cyber.fsi.stanford.edu/io/news/taiwan-disinformation-partisan-issue>.

Svárovský, Martin, Jakub Janda, Veronika Víchová, Joey Gurney, & Sami Kröger, 2020/4/23(accessed). "Handbook on Countering Russian and Chinese Interference in Europe," *European Values*, <https://www.europeanvalues.net/wp-content/uploads/2020/01/Handbook-on-Countering-Russian-and-Chinese-Interference-in-Europe.pdf>.

Twitter Safety, 2019/8/19. "Information operations directed at Hong Kong," *Twitter*, <https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong.html>.

Vilmer, J. B., Alexandre Escorcia, Marine Guillaume, & Janaina Herrera, 2018/8. "Information manipulation: A challenge for our democracies," *France Dipolomay*, <https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf>.

Weedon, Jen, William Nuland, & Alex Stamos, 2017/4/27. "Information operations and Facebook," *Facebook*, <https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf>.

Zhao, Zilong, et al., 2019/4/16. "Fake news propagate differently from real news even at early stages of spreading," *Cornell University arXiv*, <https://arxiv.org/abs/1803.03443>.

The Chinese Cognitive Warfare Model: The 2020 Taiwan Election

Puma Shen

(Assistant Professor, Graduate School of Criminology, National Taipei University)

Abstract

This research paper applies the extended diamond model in an attempt to illustrate Chinese cognitive warfare waged against Taiwan during the 2020 election. The paper is informed by 320,000 pieces of data, collected between May 1, 2019 and January 31, 2020, that demonstrate abnormalities on the Internet and the attribution of these abnormalities to possible players in China. According to the data collected, four different attack models existed during the 2020 election: the propaganda model, the pink model, the content farm model, and the collaboration model. This paper suggests that we need different defensive mechanisms to counterattack information operations from China.

Keywords: Information Operation, Cognitive Warfare, Diamond Model, Attack Model, Political Warfare