

數位威權主義下 中共對臺網路監控寒蟬效應之評估

孫懋嘉

(國防大學新聞學系助理教授)

摘要

本文旨在探討中共對臺網路監控是否會對臺灣民眾產生寒蟬效應（減少談論中共政治敏感議題的意願及產生自我審查現象）。透過實驗法（ $N = 294$ ），本文發現，在中共監管的網路與社群平臺上，擁有網路隱私保護技巧較好的臺灣民眾，在面對中共網路監控的威脅下，會有較高的意願來談論有關中共政治敏感的相關議題。然而，中共對臺網路監控會讓有網路隱私顧慮較高的臺灣民眾產生自我審查的傾向，顯示中共對臺網路監控會對部分的臺灣民眾產生寒蟬效應。整體來說，中共對臺網路監控寒蟬效應的強度，會隨著臺灣民眾對中共網路監控的感知程度和網路隱私外洩的風險程度而有所不同。

關鍵詞：網路監控、寒蟬效應、自我審查、網路隱私保護技巧、網路隱私顧慮

壹、前言

自 2012 年習近平上任後，網際網路空間已成為國家治理的重要領域，並由「中共中央網絡安全與信息化領導小組」和「國家互聯網

信息辦公室」負責網際網路治理的相關工作。¹ 2016年，中共將網路空間視為國家主權的新疆域，並提升網路安全為國家安全的一環，同時對網際網路進行全方面的治理，以實現網路強國的戰略目標。² 鑑於網際網路有利於社會集體動員、言論自由表達等特性，中共透過多機關、多層次和多手段的方式對網路言論進行箝制，以達到社會控制及政權鞏固之目的。³ 近年來，隨著《中華人民共和國網絡安全法》、《網絡信息內容生態治理規定》、《中華人民共和國數據安全法》及《網絡安全審查辦法》等法規相繼實施，更擴大了中共政府對網路監控的權力與合法性。從當前網路治理型態觀之，中共政體可說是已走向利用數位科技控制社會的數位威權主義(Digital Authoritarianism)。⁴

為能達到有效的網路治理，中共採取許多嚴格措施管控網路資訊。⁵ 在預防措施方面，中共當局運用新興數位科技和人工審查方式來過濾網路資訊，防止不利中共當局的資訊在網路上流通；在網路監控措施方面，中共不僅使用自動化工具審查網路言論，而且還會透過查核人員和網路管理員，以人工方式監控整個網路，同時也鼓勵網路使用者主動「舉報」；當不利中共當局的網路事件（如：官方醜聞、禁忌主題）發生後，網站營運者會被監督機關要求刪除資訊、停止使用

1. 林穎佑，〈中國近期網路作為探討：從控制到攻擊〉，《台灣國際研究季刊》，第12卷第3期，2016年9月，頁58。

2. 中華人民共和國國家互聯網信息辦公室，〈《國家網絡空間安全戰略》全文〉，2016年12月27日，《中華人民共和國國家互聯網信息辦公室》，〈http://www.cac.gov.cn/2016-12/27/c_1120195926.htm〉。

3. Rongbin Han 著，黃文啓譯，《中共掌控下的網路世界》(*Contesting Cyberspace in China: Online Expression and Authoritarian Resilience*) (臺北：國防部政務辦公室，2021年)，頁46-49。

4. 王信賢，〈科技威權主義：習近平「新時代」中國大陸國家社會關係〉，《展望與探索》，第16卷第5期，2018年5月，頁112-117。

5. 林穎佑，〈中國近期網路作為探討：從控制到攻擊〉，頁53-58。

者權限，或是警告、處罰或關閉違規網站，而個人違犯者則會遭到拘留和訊問，甚或是囚禁。⁶此外，中共採取網路實名制，藉以消除網路匿名的特性，一來對使用者有嚇阻作用；二來利於追蹤與掌握言行不當的使用者。整體來說，中共多管齊下的網路管控措施，透過監視、操縱、審查網路使用者的言行，不僅大幅縮限網路上的政治言論自由，還促使網路使用者產生自律和順從的行為。⁷

值得注意的是，中共利用數位科技不僅強化對其國內社會的控制，同時亦加強對海外人士的掌控。近年來，中共對國內大規模網路監控的手段已延伸到國際主流的社群網路平臺上。《華盛頓郵報》分析中共政府的招標文件發現，官媒、宣傳部門、軍警及網路監管單位，都在採購輿情分析的軟體與系統來蒐集臉書 (Facebook)、推特 (Twitter) 和 YouTube 等社群平臺上反共人士之言論與資訊。⁸不僅如此，中共更針對全球政商人士及其家人進行監控並建立資料庫，該監控資料庫至少有 2,900 位臺灣人的基本個資、相關文件及社交媒體

6. Rongbin Han 著，黃文啓譯，《中共掌控下的網路世界》(*Contesting Cyberspace in China: Online Expression and Authoritarian Resilience*)，頁 56-59；周嘉辰、黃佳雯，〈大眾化的網路監管與威權體制：中國大陸的網路「舉報」制度〉，《政治學報》，第 71 期，2021 年 6 月，頁 123-124。

7. Zhi-Jin Zhong, Tongchen Wang, & Minting Huang, “Does the Great Fire Wall Cause Self-Censorship? The Effects of Perceived Internet Regulation and the Justification of Regulation,” *Internet Research*, Vol. 27, No. 4, August 2017, pp. 985-990.

8. Cate Cadell, “China Harvests Masses of Data on Western Targets, Documents Show,” *The Washington Post*, December 31, 2021, <https://www.washingtonpost.com/national-security/china-harvests-masses-of-data-on-western-targets-documents-show/2021/12/31/3981ce9c-538e-11ec-8927-c396fa861a71_story.html>.

帳號，⁹並且透過駭客在臉書平臺監控住在臺灣的海外維吾爾人。¹⁰此外，中共利用網路監控打壓異議人士案例不勝枚舉，其中最值得關注的是，中共透過網路監控逮捕臺灣人李明哲。李明哲因長期關注中共人權和民主運動，故在騰訊 QQ、臉書、微信等社群網路平臺，發表許多有關評論中共政府、國家社會制度等政治敏感言論，於 2017 年 3 月 19 日從澳門入境中國大陸時被公安逮捕，法院根據他的網路言論足以煽動他人顛覆國家政權，判刑五年。¹¹這些事件均顯示中共對臺早已進行長期的網路監控。

從中共對海外網路平臺的言論監控，以及大範圍的監控全球政商人士和反共異議人士，皆凸顯了中共滲透國外網路的威脅，特別是在目前兩岸緊張的政治情勢，以及兩岸人民相對頻繁的交流與互動的情境下，中共對臺的網路監控是否會對臺灣民眾有實質威嚇的效果，是一個值得研究的現象。再者，當前網路監控的實證研究主題多聚焦於政府監控作為對其民眾之影響，卻鮮少涉及中共對海外網路監控的影響。基此，為了解中共網路監控的寒蟬效應 (Chilling Effect) 是否存在，本文嘗試以實驗方法探討中共對臺網路監控是否會影響臺灣民眾對於中共政治敏感議題的參與行為，以及是否會對臺灣民眾產生自我

9.〈中國數據庫監控 240 萬有力人士 外媒曝光「台灣名單」〉，《自由時報》，2020 年 9 月 16 日，〈<https://news.ltn.com.tw/news/politics/breakingnews/3293058>〉。

10.〈中國駭客用臉書監控在臺維吾爾人 台灣民眾恐遭殃〉，《中央通訊社》，2021 年 3 月 25 日，〈<https://www.cna.com.tw/news/firstnews/202103250337.aspx>〉。

11.〈李明哲遭指積極參加顛覆 判刑 5 年放棄上訴〉，《中央通訊社》，2017 年 11 月 28 日，〈<https://www.cna.com.tw/news/firstnews/201711285003.aspx>〉；〈李明哲：因公開受審 中國自曝違反言論自由罪證〉，《中央通訊社》，2022 年 6 月 29 日，〈<https://www.cna.com.tw/news/acn/202206290280.aspx>〉。

審查 (self-censorship) 的現象。¹²

進一步而言，中共對臺網路監控的寒蟬效應可從臺灣民眾在「非中國大陸」與「中國大陸」監管的網路空間上，參與有關中共政治敏感議題的行為來觀察。非中國大陸的網路平臺多屬西方公司的網路和社群通訊平臺，例如：臉書、推特、LINE、Google 及 YouTube 等，而中國大陸的網路平臺均為中國大陸民間企業所開發的搜尋引擎與社群通訊軟體，例如：微博、微信、抖音、百度及小紅書等。從「非中國大陸」的網路與社群平臺上觀察臺灣民眾對中共政治敏感議題的參與行為，可以作為評估中共對臺網路監控寒蟬效應的一種方式。這是因為中共法律對多數臺灣民眾並無直接約束力（除了對部分有赴陸需求的臺灣民眾外），即便直接批評中共政府，較不會擔心受到對岸網路監管機關的約談或懲罰；因此，從這樣的角度便可檢驗中共對臺網路監控的威嚇效果。

然而，從「中國大陸」的網路與社群平臺上來觀察臺灣民眾對中共政治敏感議題的參與行為，則可評估中共對內網路監管措施，是否亦會對臺灣民眾造成影響。其原因是，在中共嚴格的網路管控下，任何人使用中國大陸的網路平臺都可能會受到網路監管機關的監視，且使用中國大陸的社群與通訊軟體亦須以真實身分註冊；因此，在這樣的情境下，若有涉及政治敏感議題的言論與行為，理應會引起網路監管人員的注意，為避免不必要的麻煩，故臺灣民眾可能會約束自我的網路言行。

基此，本文將中共對臺網路監控所產生的寒蟬效應定義為：一、針對中共人權、領導人、六四天安門事件及臺灣統獨等政治敏感議題，臺灣民眾會受到中共網路監控而影響其搜尋、轉發和評論這些敏感議題的意願；二、和中國大陸網路使用者一樣，在網路監控的情境

12. 本研究經國立政治大學人類研究倫理審查委員會審查通過，送審案號：NCCU-REC-202303-E017。

下，臺灣民眾也會在網路上產生自我審查的現象。雖然目前尚未有此類實證研究，但在兩岸特殊的政治情境脈絡下，探討中共對臺網路監控的影響，將有助於了解臺灣民眾對境外勢力網路監控的反應，以及如何看待中共對網路隱私的侵犯。

貳、文獻回顧

一、網路監控與寒蟬效應

網際網路是一個可供人們自由討論、互動交流的公共空間。網際網路雖有利於促進公民的政治參與及言論自由，但國家機器也可透過在網路空間上的監控手段來強化對社會與資訊的掌控，¹³而網路監控便會產生寒蟬效應。寒蟬效應本質上是一種威嚇行爲 (an act of deterrence)，能夠影響法律所賦予人們的言論自由及自主行爲。¹⁴依據寒蟬效應理論 (Chilling Effects Theory) 觀點，寒蟬效應的產生主要源自於人們擔憂受到法律的懲罰，以及對個人隱私造成危害。¹⁵人們在考量法律訴訟過程中的諸多不確定性因素（例如：法官的個人偏見或誤判）和其中所付出的成本後，通常會選擇自我約束從事受到法律保障的言論或行爲。¹⁶此外，在面對網路監控和資料蒐集的情境中，人們也會評估並降低隱私在未來被侵犯的風險，故先行自我約束行使自身相關的權利或行爲。¹⁷

13. 王信賢，〈科技威權主義：習近平「新時代」中國大陸國家社會關係〉，頁 113-114。

14. Frederick Schauer, "Fear, Risk and the First Amendment: Unraveling the Chilling Effect," *Boston University Law Review*, Vol. 58, March 1978, p. 689.

15. Jonathon W. Penney, "Understanding Chilling Effects," *Minnesota Law Review*, Vol. 106, No. 3, April 2022, pp. 1465-1487.

16. Jonathon W. Penney, "Understanding Chilling Effects," p. 1465.

17. Daniel Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review*, Vol. 154, No. 3, January 2006, p. 487.

的確，民主社會享有高度言論自由，民眾可針對政治和公共事務暢所欲言；然而，當民眾知曉政府對網路進行監控時，卻會因此感到恐懼，而改變在網路上的行為模式。最著名的網路監控案例就是史諾登 (Edward Snowden) 於 2013 年 6 月揭發美國政府大規模監控全球網路的稜鏡計畫（後稱史諾登事件），使美國國內與國際社會皆為之譁然。自此，政府網路監控便成為各界關注的焦點，許多關於網路監控對人們行為之影響的調查亦隨之展開。在史諾登事件爆發後，「美國筆會」(PEN America) 執行一項問卷調查以了解美國政府監控對作家的影響：調查發現，528 位作家（含記者）中，高達 85% 作家對政府的監控作為感到擔憂，73% 擔心隱私權和新聞自由會受到影響，40% 會減少或避免從事社群媒體上的活動，33% 會特別避免在電話或電子郵件中談論特定議題。¹⁸ 此外，皮尤研究中心 (Pew Research Center) 的民調顯示，大多數美國民眾會在人際面對面互動的場合談論史諾登事件，但不願意在社群媒體上談論此議題；¹⁹ 超過五成的美國人對於美國政府以反恐之名來蒐集電話和網路數據保持不同意的態度。²⁰ 另一個研究調查 1,212 位美國網路使用者對網路監控的反應，結果發現，在政府監控網路的情境下，62% 的人傾向不會在網路上

18. FDR Group & PEN American Center, *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor* (New York: PEN America, 2013), p. 3, *PEN America*, <https://pen.org/wp-content/uploads/2022/08/2014-08-01_Full-Report_Chilling-Effects-w-Color-cover-UPDATED.pdf>.

19. Keith Hampton, Lee Rainie, Weixu Lu, Maria Dwyer, Inyoung Shin, & Kristen Purcell, “Social Media and the ‘Spiral of Silence,’” August 26, 2014, *Pew Research Center*, <<https://www.pewresearch.org/internet/2014/08/26/social-media-and-the-spiral-of-silence/>>.

20. Shiva Maniam, “Americans Feel the Tensions between Privacy and Security Concerns,” February 19, 2016, *Pew Research Center*, <<https://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/>>.

談論或撰寫特定的議題，78% 在網路上的言行會變得更為謹慎，60% 傾向不願意在網路上分享個人資訊。²¹此外，一項對1,202位瑞士民眾進行網路監控寒蟬效應的調查發現，多數民眾會因網路監控而產生自我約束行為，例如：民眾在網路上的言行會更為謹慎、避免在網路上引起他人關注和查找資訊，以及減少分享個人意見。²²從上述問卷調查可知，多數人會因政府網路監控而感到不安，並表達會改變自身的網路行為。

為進一步驗證網路監控的寒蟬效應，學者透過實驗方式來評估網路監控對人們網路行為的實際影響。一些準實驗設計 (quasi-experimental design) 的研究，將史諾登事件作為一個自然的刺激物，來判斷在事件前後，人們的網路使用行為是否有明顯改變。例如，潘尼 (Jonathon Penney) 以史諾登事件作為一個分隔時間點，觀察涉及「恐怖主義」主題的48篇文章閱讀量的變化，來觀測網路監控的寒蟬效應；他發現在史諾登事件後，該類文章的閱讀量明顯減少三成多，並且這樣的情況持續了數個月之久。²³另一個觀察 Google 關鍵字搜尋量的研究也發現相同的現象，在史諾登事件後，美國民眾大幅減少使用具有敏感性的關鍵字，以避免招致無妄之災。²⁴另有

21. Jonathon W. Penney, "Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study," *Internet Policy Review*, Vol. 6, No. 2, May 2017, pp. 7-12.

22. Moritz Büchi, Noemi Festic, & Michael Latzer, "The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda," *Big Data & Society*, Vol. 9, No. 1, January 2022, pp. 8-9.

23. Jonathon W. Penney, "Chilling Effects: Online Surveillance and Wikipedia Use," *Berkeley Technology Law Journal*, Vol. 31, No. 1, January 2016, pp. 140-149.

24. Alex Marthews & Catherine Tucker, "Government Surveillance and Internet Search Behavior," February 17, 2017, *SSRN*, <<https://ssrn.com/abstract=2412564>>.

研究發現，在史諾登事件爆發後，注重使用者網路隱私的搜尋引擎 DuckDuckGo 之使用流量反而有持續大幅的增加。²⁵ 此外，學者亦使用實驗設計 (experimental design) 來檢驗網路監控與寒蟬效應的因果關係。這類研究主要是以實驗操弄來觸發受試者對網路監控的感知，從而評估受試者後續的行為是否產生改變。一項研究發現，在受試者自身的意見與主流意見相左的情況下，受試者會因政府網路監控而傾向不會在社群媒體上談論有關美國攻打伊斯蘭國政府的敏感議題，這主要是害怕受到社會大眾的孤立，但同時也有可能是擔心受到政府的處罰。²⁶ 另一項調查政府大規模網路監控的寒蟬效應研究中，在實驗操弄前先評估受試者於未來從事非法行為（例如：下載盜版影片、參與網路賭博）、政治敏感議題參與行為和隱私保護行為的可能性，隔一週後再對同一批受試者進行網路監控的操弄，然後再評估相同行為的可能性；結果發現，知道政府會在網路監控的受試者，從事非法行為的可能性有顯著的降低，即使在總統候選人初選期間，政治參與行為也未大幅增加。這樣的寒蟬效應不僅出現在一般美國民眾樣本中，而且在美國回教徒樣本中亦有相同的現象。²⁷

綜合上述實證研究成果可知，多數民眾對政府進行網路監控普遍抱持不認同的態度，民眾也因網路監控而減少參與政治敏感議題的討論，主要可能是避免後續會受到政府的調查或法律懲罰，甚或是擔心隱私受到侵犯。這顯示網路監控會對人們產生無形的約束力，並直接

25. Mark Rosso, ABM Nasir, & Mohsen Farhadloo, "Chilling Effects and the Stock Market Response to the Snowden Revelations," *New Media & Society*, Vol. 22, No. 11, November 2020, pp. 1980-1982.

26. Elizabeth Stoycheff, "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring," *Journalism & Mass Communication Quarterly*, Vol. 93, No. 2, June 2016, pp. 306-307.

27. Elizabeth Stoycheff, Juan Liu, Kai Xu, & Kunto Wibowo, "Privacy and the Panopticon: Online Mass Surveillance's Deterrence and Chilling Effects," *New Media & Society*, Vol. 21, No. 3, March 2019, pp. 608-612.

影響其後續的網路行爲。值得注意的是，史諾登事件不僅對美國社會產生巨大的寒蟬效應，而且對國外民眾也產生了寒蟬效應。一個調查研究指出，史諾登事件對部分的挪威民眾產生了寒蟬效應，例如：在網路和通訊時會特別注意使用的字詞，以及停止經常使用的某些網路服務和改變他們的通訊習慣；這些民眾多數都是 15 歲至 29 歲的族群，由於他們長時間使用網際網路，故認為大規模網路監控會對他們造成一定程度的影響。²⁸ 另一個研究發現，史諾登事件後，與美國有貿易往來的 40 個國家之網路使用者，在 Google 上有明顯減少使用具敏感性議題的關鍵字；該研究還發現，被美國政府視為優先監控的國家，史諾登事件對其所產生的寒蟬效應是最小的，相反地，對被美國視為盟友的國家卻造成很大的寒蟬效應。²⁹ 從上述研究可知，縱然沒有政府公權力或法律的約束下，境外勢力的網路監控仍會產生某種程度的寒蟬效應，例如：減少搜尋或談論敏感議題。網路使用者雖較不擔憂受到其他國家法律的直接懲罰，但很可能會擔心自己的網路隱私受到侵犯，而改變原本的網路行爲，以降低被監控的機率。

值得注意的是，儘管網路監控會迫使網路使用者改變自身的網路行爲，但網路監控對個人行爲改變的影響，卻會受到個人的網路使用習慣、經驗及網路技巧等不同因素而有所差異。³⁰ 因此，從境外勢力的網路監控來說，依照根據寒蟬效應理論，網路隱私的保護很可能是

²⁸ Teknologirådet & Datatilsynet, "The Chilling Down Effect in Norway Privacy Trends 2014," November 7, 2017, *Datatilsynet*, <<https://www.datatilsynet.no/en/regulations-and-tools/reports-on-specific-subjects/privacy-reports/chilling-down-in-norway/>>.

²⁹ Alex Marthews & Catherine Tucker, "Government Surveillance and Internet Search Behavior."

³⁰ Moritz Büchi, Noemi Festic, & Michael Latzer, "The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda," pp. 5-6.

一個影響寒蟬效應大小的主要因素。網路監控基本上已侵犯到個人在網路上的隱私，對於在意網路隱私的人而言，為減少網路監控對其隱私的威脅，便可能會採取保護隱私的行為，來因應網路監控的威脅。基此，本文推測，如同史諾登事件，中共對臺網路監控可能會對臺灣民眾產生寒蟬效應，降低民眾談論中共政治敏感議題的意願，但此寒蟬效應的大小卻可能會因為個人對隱私重視程度的不同而有所差異。接下來，本文將探討網路監控、政治敏感議題參與行為和網路隱私保護之間的關係。

二、網路監控、政治敏感議題參與行為及網路隱私保護

網路監控通常會產生壓抑言論自由的寒蟬效應，進而減少網路使用者在線上談論政治敏感議題。³¹ 對一般人而言，網路監控會對被監視的人產生心理壓力，因為網路上的一舉一動都很可能會被監看著，於是就較不願意去談論具有敏感或禁忌性質的政治議題，以避免招致不必要的麻煩。然而，在面對政府網路監控時，有些網路使用者會採取一些應對作為，來保護其線上隱私和避免留下可讓人追蹤的數位足跡，以降低被監控的可能性。³² 這些防範措施通常包含：修改密碼、清除網頁瀏覽紀錄、使用虛擬私人網路 (Virtual Private Network, VPN) 來確保個人資訊不會被蒐集、更改社群網路的隱私設定，或使用資安軟體來偵測和刪除會蒐集個資和記錄網路使用行為的惡意軟體。³³ 值得注意的是，通常在重大的個資外洩或監控相關事

31. Elizabeth Stoycheff, "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring," pp. 306-307.

32. Lee Rainie & Mary Madden, "Americans' Privacy Strategies Post-Snowden," March 16, 2015, *Pew Research Center*, <<https://www.pewresearch.org/internet/2015/03/16/americans-privacy-strategies-post-snowden/>>.

33. Brooke E. Duffy & Ngai Keung Chan, "You Never Really Know Who's

件爆發後，對網路隱私和監控有顧慮的人，會提高保護個人隱私與資料的動機，進而改用能提升個人隱私安全的科技 (Privacy-Enhancing Technologies, PETs)。³⁴ 例如：在 2013 年史諾登揭發美國國家安全局的監控計畫後，能保護個人網路隱私的搜尋引擎 DuckDuckGo 和 Tor 之使用量便持續大幅增加。³⁵ 此外，一項在新冠疫情期間的調查指出，民眾對政府監控網路越感到擔心，則越會採取隱私保護行為。³⁶ 這些現象皆顯示網路使用者對隱私的重視，並採取具體的行動來保護個人網路隱私，以因應網路監控的威脅。

此外，研究指出，政府對網路的監控未必能有效阻止人們在網路上表達意見，只要人們具有一定程度的網路隱私保護技巧 (online privacy skills)，即便知覺到政府監控，仍可克服對政府監控的擔憂與恐懼，進而在網路上對政治敏感議題進行評論和分享。³⁷ 由此可知，

Looking': Imagined Surveillance across Social Media Platforms," *New Media & Society*, Vol. 21, No. 1, January 2019, pp. 124-132; Hongliang Chen, Christopher E. Beaudoin, & Traci Hong, "Protecting Oneself Online: The Effects of Negative Privacy Experiences on Privacy Protective Behaviors," *Journalism & Mass Communication Quarterly*, Vol. 93, No. 2, June 2016, pp. 416-421.

³⁴Balázs Bodó, "Piracy Versus Privacy: An Analysis of Values Encoded in the Piratebrowser," *International Journal of Communication*, Vol. 9, May 2015, pp. 819-820; Sören Preibusch, "Privacy Behaviors after Snowden," *Communications of the ACM*, Vol. 58, No. 5, May 2015, p. 54.

³⁵Mark Rosso, ABM Nasir, & Mohsen Farhadloo, "Chilling Effects and the Stock Market Response to the Snowden Revelations," pp. 1976-1995; Sören Preibusch, "Privacy Behaviors after Snowden," p. 54.

³⁶Athina Ioannou & Iis Tussyadiah, "Privacy and Surveillance Attitudes during Health Crises: Acceptance of Surveillance and Privacy Protection Behaviours," *Technology in Society*, Vol. 67, November 2021, p. 8.

³⁷Mustafa Oz & Akan Yanik, "Fear of Surveillance: Examining Turkish Social Media Users' Perception of Surveillance and Willingness to Express

在面對網路監控的情境下，網路隱私保護技巧的強弱與否，便會影響人們在網路上參與政治敏感議題討論的意願。對於熟嫻網路隱私保護措施的人來說，很可能會有較高的意願參與政治敏感議題的相關討論，但對於網路隱私保護技巧較差的人，其參與的動機和意願便可能會大幅降低。簡言之，網路隱私保護技巧可視為一種應對網路監控威脅的作為。基此，在中共對臺網路監控的情況下，網路隱私保護技巧較好的臺灣民眾理應有較高的意願涉及中共政治敏感議題參與行為。鑑於中共對臺網路監控的寒蟬效應可分別從臺灣民眾在「非中國大陸」與「中國大陸」的網路空間上參與政治敏感議題的相關行為來觀察，因此，本文提出下列的假設：

假設 1：網路隱私保護技巧對於網路監控感知與在中國大陸網路平臺上政治敏感議題參與行為之間的關係具有調節效果。當擁有較好的網路隱私保護技巧時，網路監控感知越高，則在中國大陸的網路與社群平臺上，參與政治敏感議題的行為會越高（假設 1a）；當擁有較好的網路隱私保護技巧時，網路監控感知越高，則在中國大陸的即時通訊軟體上，參與政治敏感議題的行為會越高（假設 1b）。

假設 2：網路隱私保護技巧對於網路監控感知與在非中國大陸網路平臺上政治敏感議題參與行為之間具有調節效果。當擁有較好的網路隱私保護技巧時，網路監控感知越高，則在非中國大陸的網路與社群平臺上，參與政治敏感議題的行為會越高（假設 2a）；當擁有較好的網路隱私保護技巧時，網路監控感知越高，則在非中國大陸的即時通訊軟體上，參與政治敏感議題的行為會越高（假設 2b）。

三、網路監控、自我審查及網路隱私顧慮

自我審查是一種因害怕招致不良後果而自發性避免或減少表達個人言論的行為。³⁸ 網路監控通常會讓人產生自我審查，這樣的現象容易發生在當人們認為自己正被監視，且同時認為這樣的監視是具有正當性的時候。³⁹ 在有網路監管體制的國家中，自我審查現象會更普遍。例如：中共的網路警察制度，藉由網路監控方式來杜絕任何會危害社會及不利政權的言論，⁴⁰ 而網路「舉報」制度，鼓勵網路使用者糾舉網路不當言論，⁴¹ 因此這些制度多會讓網路使用者產生自我監督、自我約束的效果，避免談論政治敏感議題。在西方民主國家，即便沒有明確的網路監管體制，但網路監控仍會產生民眾自我審查的效果。例如在史諾登揭發美國政府的大規模網路監控計畫之後，許多國家的 Google 使用者在敏感關鍵字的搜尋量有明顯下降；⁴² 多數美國民眾傾向不會在網路上談論特定的議題，在網路的發言會變得更為謹

³⁸ Andrew F. Hayes, Carroll J. Glynn, & James Shanahan, "Willingness to Self-Censor: A Construct and Measurement Tool for Public Opinion Research," *International Journal of Public Opinion Research*, Vol. 17, No. 3, October 2005, pp. 299-301; Mark Warner & Victoria Wang, "Self-Censorship in Social Networking Sites (SNSs) – Privacy Concerns, Privacy Awareness, Perceived Vulnerability and Information Management," *Journal of Information, Communication and Ethics in Society*, Vol. 17, No. 4, December 2019, pp. 376-377.

³⁹ Elizabeth Stoycheff, "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring," pp. 307-308.

⁴⁰ 黃妍甄，〈科技監控下的影響評估—以中國網路警察為例〉，《中國地方自治》，第 73 卷第 7 期，2020 年 7 月，頁 22-25。

⁴¹ 周嘉辰、黃佳雯，〈大眾化的網路監管與威權體制：中國大陸的網路「舉報」制度〉，頁 123-124。

⁴² Alex Marthews & Catherine Tucker, "Government Surveillance and Internet Search Behavior."

慎。⁴³ 實驗研究也發現，美國人在面對網路監控時，不願意在社群媒體上談論政治敏感議題。⁴⁴

除了網路監控的影響外，網路隱私顧慮 (online privacy concerns) 也是影響自我審查的一個重要因素。網路隱私顧慮意指一個人知覺其個人隱私和資料在網路上是否有外洩的疑慮。⁴⁵ 研究發現，多數人在上網時會擔心個人隱私受到威脅，且願意採取一些作為來避免隱私外洩，⁴⁶ 而且網路隱私顧慮較高的人通常較不願意在網路上留下個人資料。⁴⁷ 在調查社群媒體上自我審查現象的研究指出，網路隱私顧慮與自我審查有正向的關係，越會顧及網路隱私的人，在社群媒體上的自我審查傾向會越高，這可能是社群使用者只擔心個資是否遭到濫用，而未特別意識到其個資也會作為監控分析之用。⁴⁸ 的確，網路監控會

43. Jonathon W. Penney, "Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study," pp. 7-13.

44. Elizabeth Stoycheff, "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring," pp. 306-307.

45. Carina Paine, Ulf-Dietrich Reips, Stefan Stieger, Adam Joinson, & Tom Buchanan, "Internet Users' Perceptions of 'Privacy Concerns' and 'Privacy Actions'," *International Journal of Human-Computer Studies*, Vol. 65, No. 6, June 2007, p. 527.

46. Carina Paine, Ulf-Dietrich Reips, Stefan Stieger, Adam Joinson, & Tom Buchanan, "Internet Users' Perceptions of 'Privacy Concerns' and 'Privacy Actions'," pp. 533-534.

47. Tamara Dinev, Paul Hart, & Michael R. Mullen, "Internet Privacy Concerns and Beliefs about Government Surveillance—An Empirical Investigation," *The Journal of Strategic Information Systems*, Vol. 17, No. 3, September 2008, p. 227.

48. Mark Warner & Victoria Wang, "Self-Censorship in Social Networking Sites (SNSs) – Privacy Concerns, Privacy Awareness, Perceived Vulnerability and Information Management," pp. 387-388.

增加人們對網路隱私外洩的疑慮。過去研究發現，政府監控作為會讓網路使用者更為擔心其隱私受到侵犯，因而降低在網路上留下個人資訊的意願。⁴⁹

再者，從一項針對土耳其民眾的調查指出，網路隱私保護技巧較好的民眾，即便知道政府有實施網路監控，其談論政治敏感議題的意願會越高；反之，當民眾的隱私網路保護技巧較差時，則較不願意談論政治敏感議題。⁵⁰ 從此研究發現可以推判，面對網路監控的威脅，民眾在意的是個人隱私在網路上是否有外洩的可能性。綜合上述研究發現可知，網路隱私顧慮在網路監控和自我審查之間扮演一個重要因素。擔心個資外洩或身分曝光的人，在有網路監控的情況下，較會自我約束其網路行為。根據前述研究結果推論，對於會在意網路隱私的臺灣民眾，面對中共網路監控的威脅，可能容易產生較高的自我審查傾向，因此，本文提出下列的假設：

假設 3：網路隱私顧慮對於網路監控感知與自我審查傾向之間具有調節效果；當擁有較高的網路隱私顧慮時，網路監控感知越高，則自我審查傾向越高。

鑑於假設 3 是從隱私外洩風險感知的層面來了解中共對臺網路監控的寒蟬效應現象，因此亦有必要從隱私保護行為的層面（網路隱私保護技巧），來探討網路監控感知與自我審查之間的關係。雖然網路監控相關的實證研究鮮少探討網路隱私保護技巧、網路監控感知與

49. Tamara Dinev, Paul Hart, & Michael R. Mullen, "Internet Privacy Concerns and Beliefs about Government Surveillance—An Empirical Investigation," pp. 226-227.

50. Mustafa Oz & Akan Yanik, "Fear of Surveillance: Examining Turkish Social Media Users' Perception of Surveillance and Willingness to Express Opinions on Social Media," pp. 14-17.

自我審查三者的關係，但文獻指出，具有較好的網路隱私保護技巧，通常可減緩人們對政府網路監控的顧慮，並願意對政治敏感議題發聲。⁵¹ 由此推判，當擁有較好的網路隱私保護技巧時，人們在受到監控的網路場域中，其自我審查傾向可能會比較低。據此，網路隱私保護技巧較好的民眾，在面對中共網路監控的威脅下，應該會有較低的自我審查傾向，故本文提出下列的假設：

假設 4：網路隱私保護技巧對於網路監控感知與自我審查傾向之間具有調節效果；當擁有較好的網路隱私保護技巧時，網路監控感知越高，則自我審查傾向越低。

參、研究方法

一、受試樣本

本文利用即時通訊軟體 LINE，於 2022 年 5 月 30 日至 6 月 2 日期間，透過 LINE 好友和群組，招募實驗受試者，計有 362 位受試者參與實驗；其中，有 66 位受試者未完成作答、兩位未具中華民國國籍（中國大陸、馬來西亞），⁵² 剔除前述 68 位無效樣本後，計有 294

51. Mustafa Oz & Akan Yanik, “Fear of Surveillance: Examining Turkish Social Media Users’ Perception of Surveillance and Willingness to Express Opinions on Social Media,” pp. 14-17.

52. 檢視二位非中華民國國籍樣本在剔除前後是否會對實驗操弄效果產生干擾。獨立性檢定結果顯示，當未剔除此二位樣本時，網路監控感知在性別， $\chi^2(1, N = 290) = 1.93, p = .17$ 、年齡， $t(288) = -0.30, p = .77$ 、教育程度， $\chi^2(5, N = 290) = 0.14, p = .36$ 、平均月收入， $\chi^2(13, N = 287) = 7.84, p = .85$ 、居住地， $\chi^2(1, N = 290) = 0.02, p = .89$ 、家人朋友赴陸經驗， $\chi^2(1, N = 296) = 0.80, p = .37$ 、家人朋友在中國大陸出生長大， $\chi^2(1, N =$

位有效樣本。在有效受試者中，男性 142 人 (48.3%)、女性 146 人 (49.7%)，平均年齡為 36.5 歲 ($SD = 11.84$)，教育程度高中以下 34 人 (11.6%)、大學 / 專科 151 人 (51.4%)、碩士以上 103 人 (35%)，287 人目前現居住於臺灣 (97%)，六人未填答性別、年齡、教育程度、現居地；月平均收入 30,000 元以下 67 人 (22.8%)、30,001 元至 60,000 元 118 人 (40.1%)、60,001 元至 90,000 元 47 人 (16%)、90,001 元以上 53 人 (18%)，九人未填答月平均收入。有 210 位受試者的家人或朋友有赴陸求學、工作或生活之經歷 (71.4%)；108 位的家人或朋友是在中國大陸出生長大 (36.7%)。受試者認為我國與中國大陸之關係偏向敵對 ($M = 7.00$, $SD = 2.43$)，對中國大陸政治新聞有一定程度之關注 ($M = 2.60$, $SD = 0.83$)。

二、實驗設計

本文採單因子（網路監控感知：有 vs. 無）受試者間實驗設計，透過線上調查實驗法 (online survey experiment) 方式執行。「網路監控感知」的設計在於觸發受試者產生中國大陸對臺網路監控之感知，意即讓受試者察覺自己在網際網路及新媒體上所有的使用行為都會被中國大陸監控。過去研究顯示，網路監控的觸發操弄能讓受試者產生不同的政治敏感議題參與行為，⁵³故本文將網路監控感知區分為「有、無」兩個情境，並且藉由請受試者閱讀一段文章來加以操弄。在實驗

296) = 3.41, $p = .07$ 、對中國大陸觀感, $t(294) = 0.00$, $p = 1.00$ ，均無顯著差異。剔除此二位樣本後的分析結果（請見頁 79）與未剔除時的分析結果一致，故排除該樣本不會干擾後續的實驗操弄效果。

⁵³Elizabeth Stoycheff, “Under Surveillance: Examining Facebook’s Spiral of Silence Effects in the Wake of NSA Internet Monitoring,” pp. 301-305; Elizabeth Stoycheff, Juan Liu, Kai Xu, & Kunto Wibowo, “Privacy and the Panopticon: Online Mass Surveillance’s Deterrence and Chilling Effects,” pp. 606-611.

情境中，受試者將閱讀一篇虛構的短文，改寫自新聞媒體報導，⁵⁴ 說明中國大陸如何對臺灣民眾進行網路監控；而在對照情境中，受試者則閱讀一篇關於手機主題的網路短文。⁵⁵

本文透過 Qualtrics 網路問卷平臺進行資料蒐集，受試者點選連結後，會被告知參與一個網路使用行為調查之研究和個資保護說明，以及完成調查後可參加禮券抽獎活動。當同意參與實驗後，受試者首先填答上網與新媒體使用的頻率、政治興趣、政治新聞關注度、對中國大陸的好感度，以及家人或朋友是否有赴陸經歷和是否在中國大陸出生長大。完成填答後，每位受試者會隨機分派至兩個情境中的其中一個情境，被分派到實驗組的受試者會閱讀一篇說明中共對臺灣民眾進行網路監控的短文，對照組的受試者則會閱讀一篇關於手機充電會干擾上網速度的短文（請見表 1）。在上述實驗操弄後，受試者回答政治敏感議題參與行為、自我審查傾向、網路隱私顧慮，以及網路隱私保護技巧等量表，量表及其題項的順序皆以隨機方式排列，最後為人口變項。完成填答後，受試者自行決定是否參與禮券抽獎活動。實驗最後向受試者揭露研究真實目的和說明實驗刺激物，並顯示致謝頁面。

54. 吳介聲，〈中共在國際強化網路監控——場值得警惕的大亂鬥〉，《聯合新聞網》，2022 年 1 月 4 日，<<https://opinion.udn.com/opinion/story/120611/6008706>>。

55. 〈手機網路又變慢了？小心是被這個動作干擾電波〉，《聯合新聞網》，2022 年 5 月 24 日，<<https://udn.com/news/story/7098/6335061>>。由於此篇網路文章字數比實驗組刺激物的內容字數多，為避免閱讀量差異干擾實驗結果，故本文刪除部分內文，以使實驗組與對照組刺激物的字數相同。

表 1 實驗刺激物

實驗組刺激物	對照組刺激物
<p>中共網路監控之手伸向臺灣人民</p> <p>近年來，中共利用新科技和大數據分析來監控中國內部人民，並嚴格管制國內網路言論，追查及懲罰批評者，以維持社會穩定、鞏固政權。然而，近期中共已將網路監控的手法擴張至臺灣！</p> <p>根據國內外媒體和研究近期指出，中共透過監控科技與軟體，從國際網路、社群平臺、即時通訊軟體等多種網路平臺，來監控臺灣民眾的網路使用行為與言論，並蒐集不利中共當局的言論與情資。中共中央宣傳部、國家安全和軍警機構都是幕後黑手。可見中共不僅監控中國內部人民，對於監控臺灣人民也不遺餘力！</p>	<p>手機的網速變慢可能是充電干擾的影響</p> <p>現代科技發達，有一臺手機就能夠連上網路，想查資料、交朋友或玩遊戲都沒問題。行動網路可說是手機的一大命脈，只要網路出了問題，手機功能再好都是枉然！</p> <p>根據國外媒體報導，影響到平時網速的原因之一，很可能就在於充電線上。在使用充電線時，因為會散發出電波，所以可能會影響網路速度。這些高速、大容量的 USB，以序列通訊進行傳輸，有干擾到手機內部元件的可能，使得網路的品質下滑。如果想要保持網路暢通，最好就別在插著充電線的狀況下使用手機，以免訊號品質出問題。</p>

資料來源：作者自行整理。

三、變項測量

(一) 自變項

網路監控感知為本文之自變項，透過實驗操弄來測量受試者是否知覺到中共對臺進行網路監控。受試者 ($n = 159$) 被隨機分派至觸發中共網路監控感知之情境，其餘受試者 ($n = 135$) 則分派至對照組。

(二) 依變項

1. 政治敏感議題參與行為

參考 2019 年臺灣傳播調查資料庫之「政治參與」量表，⁵⁶ 本文

⁵⁶張卿卿、陶振超，《臺灣傳播調查資料庫第二期第二次調查計畫執行報告（計畫編號：MOST 105-2420-H-004-035-SS3）》（臺北：行政院科技部，2019年），頁 62。

發展出 12 個問題（請見表 2），測量受試者於未來幾週內，分別在「中國大陸」與「非中國大陸」的「網路及社群平臺」與「即時通訊軟體」上，進行「搜尋、瀏覽、點閱、觀看」、「轉貼、轉寄」和「發文、製作、留言、評論」，有關中國大陸政治敏感議題的新聞、訊息、影片（例如：人權、兩岸統獨、中共領導人、六四天安門事件）。回答選項為該行為發生的可能性，從 0 為一定不會發生到 100 為一定會發生。依據網路平臺是否為中國大陸公司研發及網路平臺類別，區分為四個類型，每個類型各有三題，分別加總後平均，成為四個構念，其所得分數越高，代表政治敏感議題參與行為發生的機會越高。「中國大陸的網路及社群平臺」($M = 6.54, SD = 14.49, Cronbach's \alpha = .85$)、「中國大陸的即時通訊軟體」($M = 6.16, SD = 14.75, Cronbach's \alpha = .91$)、「非中國大陸的網路及社群平臺」($M = 18.84, SD = 24.52, Cronbach's \alpha = .86$)，以及「非中國大陸的即時通訊軟體」($M = 16.59, SD = 23.31, Cronbach's \alpha = .88$)。

表 2 政治敏感議題參與行為量表

題 項
1. 在未來幾週，請問你會在中國大陸的網路及社群平臺上，進行「搜尋、瀏覽、點閱、觀看」和中國大陸政治敏感議題有關的新聞、訊息、影片嗎（例如：人權、兩岸統獨、中共領導人、六四天安門事件）？
2. 在未來幾週，請問你會在中國大陸的網路及社群平臺上，進行「轉貼、轉寄」和中國大陸政治敏感議題有關的新聞、訊息、影片嗎（例如：人權、兩岸統獨、中共領導人、六四天安門事件）？
3. 在未來幾週，請問你會在中國大陸的網路及社群平臺上，進行「發文、製作、留言、評論」和中國大陸政治敏感議題有關的新聞、訊息、影片嗎（例如：人權、兩岸統獨、中共領導人、六四天安門事件）？
4. 在未來幾週，請問你會在中國大陸的即時通訊平臺上，進行「搜尋、瀏覽、點閱、觀看」和中國大陸政治敏感議題有關的新聞、訊息、影片嗎（例如：人權、兩岸統獨、中共領導人、六四天安門事件）？
5. 在未來幾週，請問你會在中國大陸的即時通訊平臺上，進行「轉貼、轉寄」和中國大陸政治敏感議題有關的新聞、訊息、影片嗎（例如：人權、兩岸統獨、中共領導人、六四天安門事件）？

題 項
6. 在未來幾週，請問你會在中國大陸的即時通訊平臺上，進行「發文、製作、留言、評論」和中國大陸政治敏感議題有關的新聞、訊息、影片嗎（例如：人權、兩岸統獨、中共領導人、六四天安門事件）？
7. 在未來幾週，請問你會在不是中國大陸的網路及社群平臺上，進行「搜尋、瀏覽、點閱、觀看」和中國大陸政治敏感議題有關的新聞、訊息、影片嗎（例如：人權、兩岸統獨、中共領導人、六四天安門事件）？
8. 在未來幾週，請問你會在不是中國大陸的網路及社群平臺上，進行「轉貼、轉寄」和中國大陸政治敏感議題有關的新聞、訊息、影片嗎（例如：人權、兩岸統獨、中共領導人、六四天安門事件）？
9. 在未來幾週，請問你會在不是中國大陸的網路及社群平臺上，進行「發文、製作、留言、評論」和中國大陸政治敏感議題有關的新聞、訊息、影片嗎（例如：人權、兩岸統獨、中共領導人、六四天安門事件）？
10. 在未來幾週，請問你會在不是中國大陸的即時通訊平臺上，進行「搜尋、瀏覽、點閱、觀看」和中國大陸政治敏感議題有關的新聞、訊息、影片嗎（例如：人權、兩岸統獨、中共領導人、六四天安門事件）？
11. 在未來幾週，請問你會在不是中國大陸的即時通訊平臺上，進行「轉貼、轉寄」和中國大陸政治敏感議題有關的新聞、訊息、影片嗎（例如：人權、兩岸統獨、中共領導人、六四天安門事件）？
12. 在未來幾週，請問你會在不是中國大陸的即時通訊平臺上，進行「發文、製作、留言、評論」和中國大陸政治敏感議題有關的新聞、訊息、影片嗎（例如：人權、兩岸統獨、中共領導人、六四天安門事件）？

資料來源：作者自行整理。

2. 自我審查傾向

本量表採用海斯 (Andrew Hayes) 等人所研發之自我審查意願量表，⁵⁷ 由八個問題組成，分別為：(1) 如果我覺得別人不認同我的情況下，我就很難說出自己的意見；(2) 很多時候我覺得身邊的人錯了，但我沒有讓他們知道；(3) 當我不同意別人的意見時，我會順從他們

⁵⁷Andrew F. Hayes, Carroll J. Glynn, & James Shanahan, "Willingness to Self-Censor: A Construct and Measurement Tool for Public Opinion Research," p. 306.

的意見，而不是與他們爭辯；(4) 向「不同意我的人」表達意見，對我來說是件容易的事；(5) 如果有人問我的意見，但是我知道其實他／她不同意我的意見，我會感到不自在；(6) 我傾向於只在朋友或我信任的人面前表達我的意見；(7) 與其公開發表大多數人不同意的觀點，保持沉默會更安全；(8) 如果我不同意其他人的意見，我會說出來。回答選項採李克特六點量表，從 1 為非常不同意至 6 為非常同意。其中，問題 (4) 與 (8) 為反向題，經反向編碼後，八個題項加總後平均，成爲一個構念，其所得分數越高，代表越會自我審查 ($M = 3.66$, $SD = 0.72$, Cronbach's $\alpha = .76$)。

(三) 調節變項

1. 網路隱私顧慮

本量表採用馬賀拉 (Naresh Malhotra) 等人所發展之量表，⁵⁸ 由三個問題組成，分別爲：(1) 我比其他人更注意網際網路公司怎麼處理我的個人資料；(2) 我非常重視網際網路公司不會侵犯我的隱私；(3) 我會擔心個人隱私受到威脅。回答選項採李克特六點量表，從 1 為非常不同意至 6 為非常同意。三個題項加總後平均，成爲一個構念，其所得分數越高，代表越會關心自身的網路隱私安全 ($M = 4.68$, $SD = 0.90$, Cronbach's $\alpha = .71$)。

2. 網路隱私保護技巧

本量表採用奧茲 (Mustafa Oz) 等人所發展之量表，⁵⁹ 由五個問題組成，分別爲：(1) 我知道如何連接到 VPN (虛擬私人網路) 來隱藏

⁵⁸Naresh K. Malhotra, Sung S. Kim, & James Agarwal, "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research*, Vol. 15, No. 4, December 2004, p. 352.

⁵⁹Mustafa Oz & Akan Yanik, "Fear of Surveillance: Examining Turkish Social Media Users' Perception of Surveillance and Willingness to Express Opinions on Social Media," p. 12.

我的 IP 地址；(2) 我知道如何更改社群媒體的隱私設定；(3) 我能發現未經我許可安裝的侵入性間諜軟體；(4) 我會刪除電腦或手機中部分或全部的 Cookies（網站在您瀏覽網頁時儲存在您電子裝置上的資料）；(5) 我會刪除網路瀏覽器的瀏覽紀錄。回答選項採李克特六點量表，從 1 為非常不同意至 6 為非常同意。五個題項加總後平均，成爲一個構念，其所得分數越高，代表保護自身網路隱私安全的能力越強 ($M = 3.82, SD = 0.98, Cronbach's \alpha = .70$)。

(四) 控制變項

鑑於網路監控的寒蟬效應可能會因個人的網路使用頻率而有所不同，以及中共政治敏感議題參與行爲亦可能會因受試者的政治興趣和政治新聞關注的程度而有所差異，故本文將這些潛在干擾因素納入控制變項，以提高實驗內在效度。

1. 上網及新媒體使用頻率

在上網頻率方面，詢問受試者「平均每週會有幾天上網？」在新媒體使用頻率方面，分別詢問受試者「平均每週會有幾天使用社群媒體（臉書、IG、推特、微博、抖音、小紅書）？」「平均每週會有幾天使用即時通訊軟體（LINE、微信、臉書聊天室）？」和「平均每週會有幾天使用影音平臺（YouTube、嗶哩嗶哩）？」回答選項爲使用天數，從 0 爲完全沒有使用至 7 爲每天使用。12 個題項加總後平均，成爲一個構念，其所得分數越高，代表上網和使用新媒體的頻率越高 ($M = 3.04, SD = 0.81, Cronbach's \alpha = .92$)。

2. 政治興趣

詢問受試者「對政治感興趣的程度？」回答選項採李克特六點量表，從 1 爲非常不感興趣至 6 爲非常感興趣。其所得分數越高，代表對政治感興趣的程度越高 ($M = 3.94, SD = 1.90$)。

3. 政治新聞關注度

本量表由三個問題組成，分別爲：(1) 請問您多常關注臺灣政治

的新聞？(2) 請問您多常關注中國大陸政治的新聞？(3) 請問您多常關注國際政治的新聞？回答選項採李克特四點量表，從 1 為從來沒有至 4 為經常。三個題項加總後平均，成爲一個構念，其所得分數越高，代表越關注政治新聞 ($M = 2.92$, $SD = 0.68$, Cronbach's $\alpha = .76$)。

(五) 人口變項

本文人口變項爲性別、年齡、教育程度、平均月收入、國籍，以及現居地。此外，爲了解受試者對中國大陸的接觸情形與好感度。在接觸情形方面，本文詢問受試者「您家人或朋友現在或曾經在中國大陸工作、讀書或生活嗎？」「您家人或朋友是在中國大陸出生長大？」回答選項爲有、沒有。在對中國大陸觀感方面，詢問受試者「兩國之間的關係爲何？」回答選項爲李克特十點量表，從 1 爲非常友好、5 爲普通至 10 爲非常敵對，其所得分數越高，代表認爲我國與中國大陸的關係越敵對，反之則越友好 ($M = 7.00$, $SD = 2.43$)。

肆、研究結果

在驗證假設與回答研究問題之前，本文首先以獨立性檢定檢驗「網路監控感知（有 vs. 無）」在人口變項與對中國大陸接觸及好感度上是否有顯著差異。結果顯示，兩個情境在性別， $\chi^2(1, N = 288) = 0.33$, $p = .57$ 、年齡， $t(286) = -0.14$, $p = .89$ 、教育程度， $\chi^2(5, N = 288) = 2.96$, $p = .71$ 、平均月收入， $\chi^2(13, N = 285) = 8.50$, $p = .81$ 、居住地， $\chi^2(1, N = 288) = 0.51$, $p = .47$ 、家人朋友赴陸經驗， $\chi^2(1, N = 294) = 0.01$, $p = .91$ 、家人朋友在中國大陸出生長大， $\chi^2(1, N = 294) = 1.72$, $p = .19$ 、對中國大陸觀感， $t(286) = -0.94$, $p = .35$ ，均無顯著差異，此表示實驗的隨機分派程序是成功的，且各人口變項與對中國大陸接觸及好感度皆不會對研究變項間之關係造成混淆效果。

操弄檢核部分，獨立樣本 t 檢定結果顯示，在非中國大陸的網站與社群平臺上，政治敏感議題參與行爲在網路監控感知上有顯著差

異， $t(294) = -2.38, p = .02$ ，知覺到中共網路監控者（實驗組）的政治敏感議題參與行為（ $M = 21.88$ ）顯著高於未知覺到中共網路監控者（ $M = 15.21$ ）；在非中國大陸的即時通訊軟體上，政治敏感議題參與行為在網路監控感知上亦有顯著差異， $t(291) = -2.92, p = .004$ ，知覺到中共網路監控者（實驗組）的政治敏感議題參與行為（ $M = 20.15$ ）顯著高於未知覺到中共網路監控者（ $M = 12.48$ ）；然而，在中國大陸的網站與社群平臺 [$t(287) = -1.92, p = .06$]，以及即時通訊軟體上 [$t(292) = -1.17, p = .24$]，政治敏感議題參與行為在網路監控感知上皆未有顯著差異。整體而言，實驗操弄能有效區別出政治敏感議題參與行為在網路監控感知上的差異。從操弄結果可知，臺灣民眾在非中國大陸的網路和社群平臺及通訊軟體上，並未因中共網路監控而減少中共政治敏感議題的參與行為，反而有較高的意願來搜尋、觀看、轉發和評論中共政治敏感議題。但根據文獻指出，網路監控的寒蟬效應會因網路隱私保護技巧和網路隱私顧慮的程度而有所差異，且在執行獨立性檢定時並未控制潛在的干擾變項，因此，透過假設驗證方能進一步評估中共對臺網路監控的寒蟬效應。

在假設驗證部分，本文採用海斯所開發之 PROCESS 巨集 4.0 版本，⁶⁰ 其使用一般最小平方 (ordinary least squares) 迴歸分析檢視中介、調節、調節中介 (moderated mediation) 等效果，並採偏誤校正拔靴法 (bias-corrected bootstrapping)，進行 5,000 次重複取樣，提供效果估計值的 95% 信賴區間。當效果估計值之 95% 信賴區間未包含 0，表示該效果顯著；反之，95% 信賴區間包含 0，則表示該效果不顯著。因此，本文使用 PROCESS 巨集來檢驗各假設之調節效果是否存在。

⁶⁰ Andrew Hayes, *Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach* (New York, Guilford Publications, 2017), pp. 1-692.

假設 1「網路隱私保護技巧對於網路監控感知與在中國大陸網路平臺上政治敏感議題參與行為之間的關係具有調節效果。當擁有較好的網路隱私保護技巧時，網路監控感知越高，則在中國大陸的網路與社群平臺上，參與政治敏感議題的行為會越高（假設 1a）；當擁有較好的網路隱私保護技巧時，網路監控感知越高，則在中國大陸的即時通訊軟體上，參與政治敏感議題的行為會越高（假設 1b）。」採用 PROCESS 巨集模型 1 進行檢驗，以「網路監控感知」為自變項、「在中國大陸的網路與社群平臺上的政治敏感議題參與行為」及「在中國大陸的即時通訊軟體上的政治敏感議題參與行為」分別為依變項、「網路隱私保護技巧」為調節變項，並控制潛在的干擾變項（上網及新媒體使用頻率、政治興趣、政治新聞關注度、網路隱私顧慮、自我審查傾向、在非中國大陸的網路與社群平臺上的政治敏感議題參與行為，以及在非中國大陸的即時通訊軟體上的政治敏感議題參與行為）以避免研究變項間之虛假關係。

在檢驗假設 1a 時，在中國大陸的即時通訊軟體上的政治敏感議題參與行為納入為控制變項，結果顯示（請見圖 1）：「網路監控感知（有 vs. 無）」未能顯著預測在中國大陸的網路與社群平臺上的政治敏感議題參與行為 [$b = -6.81, t(294) = -1.67, p = .10$]，「網路隱私保護技巧」則顯著預測在中國大陸的網路與社群平臺上的政治敏感議題參與行為 [$b = -3.27, t(294) = -2.01, p = .05$]，「網路監控感知」和「網路隱私保護技巧」對在中國大陸的網路與社群平臺上的政治敏感議題參與行為，有顯著交互作用效果 [$b = 2.05, t(294) = 1.99, p = .05$]。進一步以詹森—內曼法 (the Johnson-Neyman technique) 檢視交互作用效果，結果顯示：網路隱私保護技巧數值 4.509 為臨界值；當其高於 4.509 時，實驗組與對照組在政治敏感議題參與行為上會有顯著差異，而當其低於 4.509 時，實驗組與對照組在政治敏感議題參與行為上則無顯著差異。換言之，在網路隱私保護技巧較強（數值高於 4.509）的情況下，有知覺到網路監控者（實驗組）會比未知覺到網

路監控者（對照組）更傾向在中國大陸的網路與社群平臺上談論政治敏感的相關議題。在本文樣本中，有 27.2% 受試者的網路隱私保護技巧數值高於 4.509（灰色區域），72.8% 受試者低於 4.509。故假設 1a 成立。

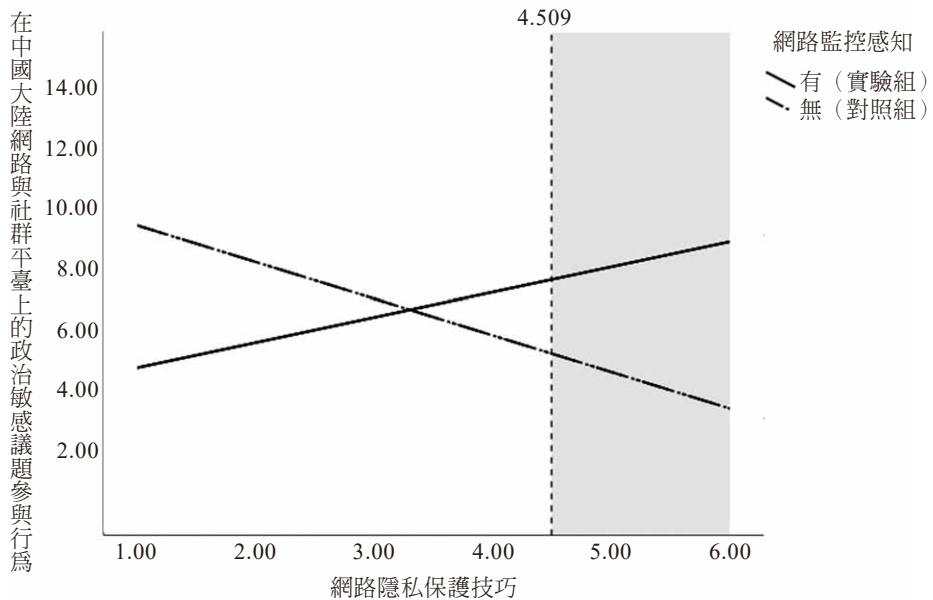


圖 1 網路監控感知與網路隱私保護技巧的交互作用效果

資料來源：作者自行繪製。

在檢驗假設 1b 時，在中國大陸的網路與社群平臺上的政治敏感議題參與行為納入為控制變項，結果顯示：「網路監控感知（有 vs. 無）」 $[b = 2.04, t(294) = 0.49, p = .63]$ 與「網路隱私保護技巧」 $[b = 1.26, t(294) = 0.74, p = .46]$ 皆未能顯著預測在中國大陸的即時通訊軟體上的政治敏感議題參與行為，「網路監控感知」和「網路隱私保護技巧」對在中國大陸的即時通訊軟體上的政治敏感議題參與行為

亦未有顯著交互作用效果 [$b = -0.75, t(294) = -0.70, p = .49$]。故假設 1b 不成立。

假設 2「網路隱私保護技巧對於網路監控感知與在非中國大陸網路平臺上政治敏感議題參與行爲之間具有調節效果。當擁有較好的網路隱私保護技巧時，網路監控感知越高，則在非中國大陸的網路與社群平臺上，參與政治敏感議題的行爲會越高（假設 2a）；當擁有較好的網路隱私保護技巧時，網路監控感知越高，則在非中國大陸的即時通訊軟體上，參與政治敏感議題的行爲會越高（假設 2b）。」採用 PROCESS 巨集模型 1 進行檢驗，以「網路監控感知」爲自變項、「在非中國大陸的網路與社群平臺上的政治敏感議題參與行爲」及「在非中國大陸的即時通訊軟體上的政治敏感議題參與行爲」分別爲依變項，「網路隱私保護技巧」爲調節變項，並控制潛在的干擾變項（上網及新媒體使用頻率、政治興趣、政治新聞關注度、網路隱私顧慮、自我審查傾向、在中國大陸的網路與社群平臺上的政治敏感議題參與行爲，以及在中國大陸的即時通訊軟體上的政治敏感議題參與行爲）以避免變項間之虛假關係。

在回答假設 2a 時，在非中國大陸的即時通訊軟體上的政治敏感議題參與行爲納入爲控制變項，結果顯示：「網路監控感知（有 vs. 無）」 [$b = -6.99, t(294) = -1.10, p = .27$] 與「網路隱私保護技巧」 [$b = -2.56, t(294) = -1.00, p = .32$] 皆未能顯著預測在非中國大陸的網路與社群平臺上的政治敏感議題參與行爲，「網路監控感知」和「網路隱私保護技巧」對在非中國大陸的網路與社群平臺上的政治敏感議題參與行爲，未有顯著交互作用效果 [$b = 1.96, t(294) = 1.22, p = .22$]。

在回答假設 2b 時，在非中國大陸的網路與社群平臺上的政治敏感議題參與行爲納入爲控制變項，結果顯示：「網路監控感知（有 vs. 無）」 [$b = 9.72, t(294) = 1.66, p = .10$] 與「網路隱私保護技巧」 [$b = 3.67, t(294) = 1.55, p = .12$] 皆未能顯著預測在非中國大陸的即時通訊軟體上的政治敏感議題參與行爲，「網路監控感知」和「網路隱私

保護技巧」對在非中國大陸的即時通訊軟體上的政治敏感議題參與行為，亦未有顯著交互作用效果 [$b = -1.96, t(294) = -1.31, p = .19$]。故假設 2 不成立。

假設 3「網路隱私顧慮對於網路監控感知與自我審查傾向之間具有調節效果；當擁有較高的網路隱私顧慮時，網路監控感知越高，則自我審查傾向越高。」採用 PROCESS 巨集模型 1 進行檢驗，以「網路監控感知」為自變項、「自我審查傾向」為依變項、「網路隱私顧慮」為調節變項，並控制潛在的干擾變項（上網及新媒體使用頻率、政治興趣、政治新聞關注度、網路隱私保護技巧、在中國大陸和非中國大陸的網路與社群平臺上的政治敏感議題參與行為，以及在中國大陸和非中國大陸的即時通訊軟體上的政治敏感議題參與行為）以避免變項間之虛假關係。

根據分析結果，「網路監控感知（有 vs. 無）」 [$b = -1.13, t(294) = -2.56, p = .01$] 與「網路隱私顧慮」 [$b = -0.37, t(294) = -2.48, p = .01$] 皆顯著預測自我審查傾向，「網路監控感知」和「網路隱私顧慮」對自我審查傾向有顯著之交互作用效果 [$b = 0.26, t(294) = 2.73, p = .01$]。進一步以詹森—內曼法檢視交互作用效果，結果顯示（請見圖 2）：網路隱私顧慮數值 3.245 與 5.232 為臨界值；當其高於 5.232 和低於 3.266 時，實驗組與對照組在自我審查傾向上會有顯著差異，而當其介於 3.245 至 5.232 之間時，實驗組與對照組在自我審查傾向上則無顯著差異。換言之，在網路隱私顧慮較高（數值高於 5.232）的情況下，有知覺到網路監控者（實驗組）會比未知覺到網路監控者（對照組）更傾向在網路上進行自我審查；反之，在網路隱私顧慮較低（數值低於 3.245）的情況下，相較於未知覺到網路監控者（對照組），有知覺到網路監控者（實驗組）則較不會在網路上進行自我審查。在本文樣本中，有 5.8% 受試者的網路隱私顧慮數值低於 3.245（左側灰色區域），94.2% 受試者高於 3.245；有 30.6% 受試者的網路隱私顧慮數值高於 5.232（右側灰色區域），69.4% 受試者低於

5.232。故假設 3 成立。

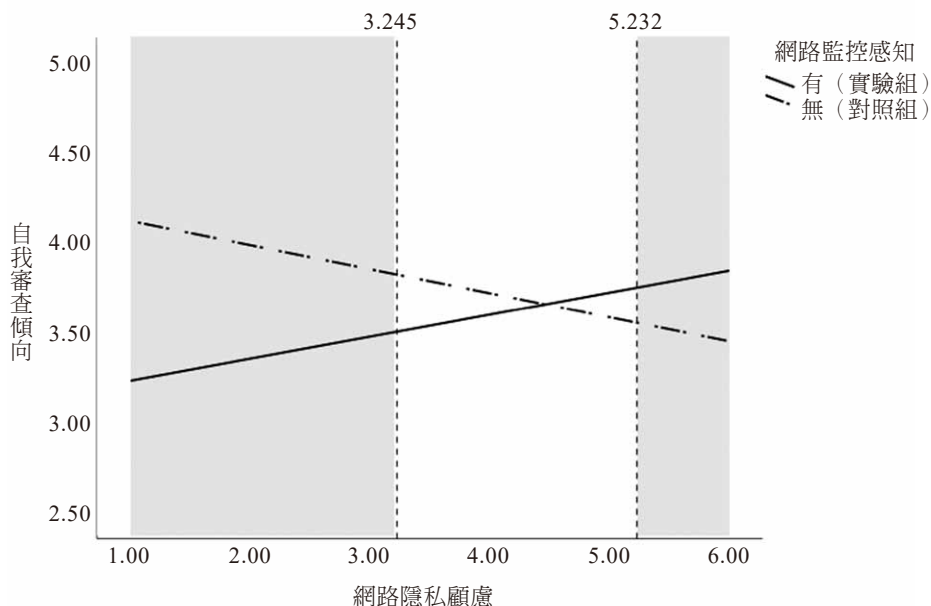


圖 2 網路監控感知與網路隱私顧慮的交互作用效果

資料來源：作者自行繪製。

假設 4「網路隱私保護技巧對於網路監控感知與自我審查傾向之間具有調節效果；當擁有較好的網路隱私保護技巧時，網路監控感知越高，則自我審查傾向越低。」採用 PROCESS 巨集模型 1 進行檢驗，以「網路監控感知」為自變項、「自我審查傾向」為依變項、「網路隱私保護技巧」為調節變項，並控制潛在的干擾變項（上網及新媒體使用頻率、政治興趣、政治新聞關注度、網路隱私顧慮、在中國大陸和非中國大陸的網路與社群平臺上的政治敏感議題參與行為，以及在中國大陸和非中國大陸的即時通訊軟體上的政治敏感議題參與行為）以避免變項間之虛假關係。

分析結果顯示，「網路監控感知（有 vs. 無）」 $[b = -0.19, t(294) = -0.56, p = .58]$ 與「網路隱私保護技巧」 $[b = -0.14, t(294) = -1.02, p = .31]$ 皆未能顯著預測自我審查傾向，「網路監控感知」和「網路隱私保護技巧」對自我審查傾向未有顯著交互作用效果 $[b = -0.75, t(294) = -0.06, p = .46]$ 。故假設 4 不成立。

伍、討論

一、研究發現與意涵

本文旨在探討中共對臺網路監控的寒蟬效應是否存在，具體言之，現居於臺灣的民眾是否會因受到中共網路監控的威脅，而影響其在「非中國大陸」與「中國大陸」監管的網路空間上涉及中共政治敏感議題的參與行為（如：人權、中共領導人、六四天安門事件及兩岸統獨），以及產生自我審查的現象。研究發現，中共對臺網路監控會讓有隱私顧慮的臺灣民眾產生自我審查的現象，顯示中共對臺網路監控會對部分的臺灣民眾產生寒蟬效應。另一方面，隱私保護能力較好的臺灣民眾，相對不會擔心中共網路監控的威脅，會有較高的傾向在中共監管的網路與社群平臺上，談論有關中共政治敏感的話題。以下本文將依照假設之順序，針對研究發現之意涵進行闡述。

假設 1 探討，在「中共監管」的網域中，網路隱私保護技巧可調節網路監控感知與中共政治敏感議題的參與行為之間的關係；假設 2 在探討，在「非中共監管」的網域中，網路隱私保護技巧可調節網路監控感知與中共政治敏感議題的參與行為之間的關係。結果發現，在中共監管的網路空間中，網路隱私保護技巧具有調節作用的效果。意即，在網路隱私保護技巧較好的情況下，面對中共網路監控的威脅的民眾，會比未面對中共網路監控威脅的民眾，更願意在中國大陸的網路和社群平臺上（假設 1a），而非即時通訊軟體上（假設 1b），

搜尋、閱讀、轉發和評論關於人權、中共領導人、六四天安門事件和兩岸統獨等中共當局視為敏感的議題。此發現亦與過往研究相呼應，隱私保護能力較好的網路使用者，會願意在社群媒體上針對政治敏感議題發表看法。⁶¹ 假設 1a 成立而假設 1b 卻不成立，可能是網路平臺特性的不同所導致。網際網路和社群平臺是屬於開放性或半開放性的網路場域，而即時通訊平臺則屬封閉性的網路場域；與即時通訊平臺相比較，網際網路和社群平臺上，資訊傳散的速度快且範圍廣，且能觸及更多的使用者，因此，民眾在此談論、轉發政治敏感議題相對容易吸引他人的關注或討論。雖然網路和社群平臺的隱私安全性可能沒有即時通訊平臺來得高，但是民眾可藉由採取網路隱私保護的相關措施，來降低隱私外洩的風險。

然而，在非屬中共管轄的網路空間中，網路監控感知與網路隱私保護技巧皆未能預測政治敏感議題的參與行為（假設 2）。從這些結果可知，在非中共管轄的網域中，臺灣民眾相對較不擔心中共網路監控所帶來的威脅。寒蟬效應理論和實證研究皆指出，⁶² 害怕受到法律制裁是引發寒蟬效應的主要因素。所以從此觀點來看，不擔心網路監控的威脅，或許是民眾較不害怕受到中共法律的制裁。這可能是由於受試者目前都現居於臺灣，且近期不會和中國大陸有直接的往來關係，因而會認為只要不進入中共法律管轄權的區域，中共政府就無法把臺灣人當作是國內執法對象來加以處罰。若民眾要搜尋、談論中共政治敏感的議題，也較不會擔憂個人網路隱私是否會受到中共網路監

61. Mustafa Oz & Akan Yanik, "Fear of Surveillance: Examining Turkish Social Media Users' Perception of Surveillance and Willingness to Express Opinions on Social Media," pp. 14-17.

62. Jonathon W. Penney, "Understanding Chilling Effects," pp. 1465-1487; Mustafa Oz & Akan Yanik, "Fear of Surveillance: Examining Turkish Social Media Users' Perception of Surveillance and Willingness to Express Opinions on Social Media," pp. 14-16.

控而有所外洩。但在中共監管的網域中，網路隱私保護技巧卻是一個影響涉及政治敏感議題的重要因素，也就是說，有能力保護個人網路隱私的民眾，相對較能克服面對被網路監控的心理壓力，而不擔心觸及中共政治敏感議題所帶來的後果。的確，過往研究也發現相同的現象：網路使用技巧 (Web-use skills) 越好的人，參與政治活動的意願相對較高。⁶³ 因此，在中共網路監控下，隱私保護技巧便成爲一個影響網路使用者自由發表言論的關鍵因素。

儘管這些發現不能直接代表中共網路監控所產生的寒蟬效應，但其代表兩種意涵：（一）數位科技雖能有利於國家政權對其社會進行大規模監控，但數位科技亦賦予民眾對抗國家機器監視的能力；（二）在面對網路監控的威脅下，擁有保護自身網路安全的能力，可爲網路使用者本身創造出相對安全的情境，進而提高政治敏感或禁忌議題的參與動機，或是更敢於表達個人真實的想法；就本文的例子來說，隱私保護能力較好的臺灣民眾，更願意在中共監管的網路及社群平臺中，論及自由民主與人權價值的議題。

假設 3 檢視網路隱私顧慮如何調節網路監控感知與自我審查傾向之間的關係。研究發現，網路隱私顧慮是一個會影響中共網路監控寒蟬效應的調節因素。具體來說，在高度擔心個人網路隱私的情況下，有察覺到中共網路監控的民眾，會比沒有察覺到的民眾，更傾向在網路空間上表現出自我審查行爲。反之，在相較不擔心個人網路隱私的情況下，有察覺到中共網路監控的民眾，會比沒有察覺到的民眾，較不會有自我審查傾向。過往關於網路隱私的研究指出，具有高隱私顧

⁶³ Eszter Hargittai & Aaron Shaw, "Digitally Savvy Citizenship: The Role of Internet Skills and Engagement in Young Adults' Political Participation around the 2008 Presidential Election," *Journal of Broadcasting & Electronic Media*, Vol. 57, No. 2, December 2013, pp. 130-131.

慮的人，通常不傾向在網路空間中透露較多的個人資訊，⁶⁴ 而網路監控經常會涉及個人網路隱私的侵犯，⁶⁵ 所以在被監控的網路空間中，高隱私顧慮者所展現出來的網路行為，會比隱私顧慮低者的網路行為，來得更為謹慎或保守。因此，在面對中共網路監視的威脅，對網路隱私顧慮較高的人，則容易產生自律行為，以避免招致後續不必要的麻煩。

假設 4 檢驗網路隱私保護技巧對網路監控感知與自我審查傾向之間的調節效果。分析結果指出，網路隱私保護技巧未能顯著調節網路監控感知與自我審查傾向之間的關係。雖然網路隱私保護技巧不是一個顯著的調節因素，但檢視三個變項之間的關係仍可發現，在網路隱私保護技巧較好的情況下，實驗組受試者（面對中共網路監控的威脅）的自我審查傾向會比對照組受試者來得低；反之，在網路隱私保護技巧較差的情況下，實驗組和對照組的受試者皆有較高的自我審查傾向。進一步比較假設 3（成立）和假設 4（不成立）的驗證結果可知，網路隱私顧慮和網路監控對自我審查現象的交互作用效果，會比網路隱私保護技巧和網路監控的交互作用效果來得更為明顯；由於網路隱私顧慮可視為人們對隱私外洩風險的一種主觀感知，⁶⁶ 所以，當

⁶⁴Tobias Dienlin & Sabine Trepte, "Is the Privacy Paradox a Relic of the Past? An in-Depth Analysis of Privacy Attitudes and Privacy Behaviors," *European Journal of Social Psychology*, Vol. 45, No. 3, April 2015, pp. 294-295.

⁶⁵Tamara Dinev, Paul Hart, & Michael R. Mullen. "Internet Privacy Concerns and Beliefs about Government Surveillance—An Empirical Investigation," p. 227；黃妍甄，〈科技監控下的影響評估—以中國網路警察為例〉，頁 21。

⁶⁶Tamara Dinev, Paul Hart, & Michael R. Mullen, "Internet Privacy Concerns and Beliefs about Government Surveillance—An Empirical Investigation," p. 218.

網路隱私外洩的風險感知越高時，民眾在面對中共的網路監控，便容易產生明顯的自我審查現象。

中共對網路空間實施不同的監控措施，其目的是讓其國內民眾產生被監視與審查的恐懼感。例如：中共會透過懲罰方式來讓意見領袖產生恐懼，進而自我審查，以達到遏止這些人的發言，而這些懲罰案例就可對一般民眾形成壓力；⁶⁷再者，中共亦透過大眾化的網路「舉報」制度，讓民眾彼此可以相互糾舉，以造成網路言論的限縮，加深自我審查的效果。⁶⁸所以民眾為減少生活與工作上的麻煩，其在網路上發言自然會謹慎許多。與此不同的是，面對中共對臺網路監控的威脅，臺灣民眾在意的是個人網路隱私，當網路隱私有「裸奔」之虞，臺灣民眾會選擇優先保護個人隱私，所以會產生自我審查的現象；而這些高隱私顧慮的人，自然很可能也會避免在網路空間上觸及中共當局認定的政治敏感議題。但對於有赴陸需求的臺灣民眾來說，避免因不當網路言論而導致工作生活上的不便，或許是一個更為優先考量的因素，而非網路隱私顧慮。從整體來看，網路監控確實會使網路使用者產生自我審查的效果，只是選擇自我審查的考量因素，會因國家政治體制與社會制度的不同，而有所差異。就本文的發現來說，面對中共的網路監控，臺灣民眾會因為個人網路隱私顧慮而產生自我審查的現象。

⁶⁷Margaret Roberts, "Testimony before the U.S.-China Economic and Security Review Commission Hearing on China's Information Controls, Global Media Influence, and Cyber Warfare Strategy," May 4, 2017, *U.S.-China Economic and Security Review Commission*, <<https://www.uscc.gov/sites/default/files/Molly%20Roberts%20May%204th%202017%20USCC%20testimony.pdf>>.

⁶⁸周嘉辰、黃佳雯，〈大眾化的網路監管與威權體制：中國大陸的網路「舉報」制度〉，頁 119-121。

二、研究限制與未來研究建議

本文運用實驗法來觀察中共對臺網路監控的寒蟬效應，但研究設計上仍有需要補強之處，在此提出說明以利後續研究者參考。第一，本文以便利抽樣 (convenience sampling) 方式招募受試者，故限制了實驗的外在效度，而無法將實驗結果有效推論至臺灣全體民眾，未來研究可使用具代表性的樣本，以提高研究結果的外推性；儘管如此，本實驗設計採隨機分派及納入控制組來消除外衍變項的影響，故研究結果具有因果推論的效度；第二，本文發現網路隱私顧慮是一個會影響臺灣民眾自我審查的調節變項，然而，可能還有其他調節變項亦會影響自我審查現象，例如：對於網路監控技術或知識的認知程度，故後續研究可進一步檢視這些調節變項對中共網路監控寒蟬效應之影響。另外，本文從個人主觀認知的角度，來測量受試者的網路隱私保護技巧，而非其實際的技術能力，故未來研究可測量網路隱私保護技巧的客觀技術等級，探討實際的網路隱私保護能力與網路監控寒蟬效應之間的關係。

第三，本文並未考量「統獨傾向」對寒蟬效應的潛在影響。在面對中共對臺網路監控的威脅下，獨立傾向比較強的人很可能會採取「對抗」的方式，而更願意談論中共政治敏感議題；反之，統一傾向的人則可能會選擇「順從」的方式，而不願意談論中共政治敏感議題，因此，未來有關中共網路監控寒蟬效應的實驗設計，應考慮統獨傾向的影響；第四，本文僅針對目前現居於臺灣的民眾進行調查實驗，因為臺灣民眾使用臉書、IG、LINE 及 Google 等網路平臺的頻率很高，而普遍較少使用微博、微信等中國企業所開發的平臺，所以這有可能導致無法在中共管轄的網路空間上發現臺灣民眾的寒蟬效應；未來研究可針對具有赴陸工作、讀書或生活的民眾作為樣本，探討其在中共網路與社群平臺上的政治參與行為；第五，本文挑選中共政治敏感議題作為評估中共網路監控寒蟬效應的方式之一，主因是這

些政治敏感議題皆屬於中共政府認定的重大禁忌話題，且臺灣民眾對其應較為熟悉，但未必是民眾感興趣的議題，故可能造成關於這些議題的參與行為意願相對偏低，未來可選取中共防疫或其他近期的敏感議題作為衡量寒蟬效應的方式。

儘管有上述的研究限制，本文仍為中共對臺網路監控的寒蟬效應提供了一個實證的發現。

陸、結論

總體言之，臺灣民眾對境外勢力網路監控的威脅，無論在中國大陸和非中國大陸監管的網路空間中，皆未產生明顯的寒蟬效應（未發現受試者有明顯避談中共政治敏感議題的現象），主要原因可能是大多數臺灣民眾尚無赴陸的需求，因而較不害怕受到中共相關法律的制裁，所以即使民眾感知到中共對臺進行大規模網路監控，也較不擔心因談論政治敏感議題而被中共當局「請喝茶」。但值得注意的是，網路隱私是臺灣民眾比較在意的因素，當網路隱私保護技巧越好時，感知到中共對台網路監控的民眾，會比較願意在中國大陸的網路空間上談論政治敏感議題，不過，對於網路隱私顧慮越大的人，面對中共的網路監控，則自我審查的現象會越明顯。顯見中共對臺網路監控寒蟬效應的強弱，會隨著臺灣民眾對網路隱私在意的程度而有所不同。

本文結果亦呼應寒蟬效應理論所主張的寒蟬效應來自於個人隱私有受侵犯之虞，特別是在境外勢力大規模網路監控、資料蒐集的情境下，人們為顧及隱私安全而選擇減少在網路上表達個人意見或提供相關個人資訊。⁶⁹此外，本文從網路隱私保護技巧（隱私保護行為）與網路隱私顧慮（隱私外洩風險感知）兩個面向，檢視其如何影響中

⁶⁹Jonathon W. Penney, "Chilling Effects and Transatlantic Privacy," *European Law Journal*, Vol. 25, No. 2, March 2019, pp. 126-130.

共對臺網路監控的寒蟬效應。根據本文的發現，做好網路隱私保護的措施，基本上可減少臺灣民眾在中共監管的網域中所帶來的不安與恐懼，顯示個人的隱私保護措施能降低網路監控寒蟬效應的影響。對於網路隱私顧慮高的人來說，中共網路監控的威脅會增強他們對個人隱私外洩的風險認知，故進而自我限制個人網路言論與行為，這反映出網路監控寒蟬效應對擔憂隱私外洩的人會產生較大的影響。

鑑於中共對臺網路監控對臺灣民眾造成寒蟬效應，反映出民眾對中共的網路入侵和非法蒐集個資的擔憂與恐懼，因此，在實務面，政府相關部門不僅應加強重視資安教育來強化國人的資安素養，更要讓社會大眾了解中共數位威權主義對國家、社會，乃至個人的資安威脅與影響（例如：中共如何透過數位科技滲透臺灣網路、如何藉由社群平臺、影音軟體、手機遊戲、網路廣告等多元的管道蒐集個人的資料和電磁紀錄），以提升國人的資安危機意識及資安防禦能力。此外，政府相關部門亦應檢視和評估現行保護個資和隱私的相關法規（如：跨境的個資傳輸），能否足以因應中共數位威權主義對國人所帶來的資安威脅，以強化保障個人資料安全，降低中共數位威權主義對我國國家安全與社會的衝擊。

收件：2022年10月11日

修正：2023年3月28日

採用：2023年3月31日

參考文獻

中文部分

專書譯著

Han, Rongbin 著，黃文啓譯，2021。《中共掌控下的網路世界》(*Contesting Cyberspace in China: Online Expression and Authoritarian Resilience*)。臺北：國防部政務辦公室。

期刊論文

王信賢，2018/5。〈科技威權主義：習近平「新時代」中國大陸國家社會關係〉，《展望與探索》，第 16 卷第 5 期，頁 111-127。

周嘉辰、黃佳雯，2021/6。〈大眾化的網路監管與威權體制：中國大陸的網路「舉報」制度〉，《政治學報》，第 71 期，頁 99-129。

林穎佑，2016/9。〈中國近期網路作為探討：從控制到攻擊〉，《台灣國際研究季刊》，第 12 卷第 3 期，頁 51-68。

黃妍甄，2020/7。〈科技監控下的影響評估—以中國網路警察為例〉，《中國地方自治》，第 73 卷第 7 期，頁 17-36。

研究計畫

張卿卿、陶振超，2019。《臺灣傳播調查資料庫第二期第二次調查計畫執行報告（計畫編號：MOST 105-2420-H-004-035-SS3）》。臺北：行政院科技部。

網際網路

2017/11/28。〈李明哲遭指積極參加顛覆 判刑 5 年放棄上訴〉，《中央通訊社》，<<https://www.cna.com.tw/news/firstnews/>

201711285003.aspx>。

2020/9/16。〈中國數據庫監控 240 萬有力人士 外媒曝光「台灣名單」〉，《自由時報》，<<https://news.ltn.com.tw/news/politics/breakingnews/3293058>>。

2021/3/25。〈中國駭客用臉書監控在臺維吾爾人 台灣民眾恐遭殃〉，《中央通訊社》，<<https://www.cna.com.tw/news/firstnews/202103250337.aspx>>。

2022/5/24。〈手機網路又變慢了？小心是被這個動作干擾電波〉，《聯合新聞網》，<<https://udn.com/news/story/7098/6335061>>。

2022/6/29。〈李明哲：因公開受審 中國自曝違反言論自由罪證〉，《中央通訊社》，<<https://www.cna.com.tw/news/acn/202206290280.aspx>>。

中華人民共和國國家互聯網信息辦公室，2016/12/27。〈《國家網絡空間安全戰略》全文〉，《中華人民共和國國家互聯網信息辦公室》，<http://www.cac.gov.cn/2016-12/27/c_1120195926.htm>。

吳介聲，2022/1/4。〈中共在國際強化網路監控——一場值得警惕的大亂鬥〉，《聯合新聞網》，<<https://opinion.udn.com/opinion/story/120611/6008706>>。

英文部分

專書

Hayes, Andrew, 2017. *Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach*. New York: Guilford Publications.

期刊論文

Bodó, Balázs, 2015/5. "Piracy Versus Privacy: An Analysis of Values Encoded in the Piratebrowser," *International Journal of*

- Communication*, Vol. 9, pp. 818-838.
- Büchi, Moritz, Noemi Festic, & Michael Latzer, 2022/1. “The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda,” *Big Data & Society*, Vol. 9, No. 1, pp. 1-14.
- Chen, Hongliang, Christopher E. Beaudoin, & Traci Hong, 2016/6. “Protecting Oneself Online: The Effects of Negative Privacy Experiences on Privacy Protective Behaviors,” *Journalism & Mass Communication Quarterly*, Vol. 93, No. 2, pp. 409-429.
- Dienlin, Tobias & Sabine Trepte, 2015/4. “Is the Privacy Paradox a Relic of the Past? An in-Depth Analysis of Privacy Attitudes and Privacy Behaviors,” *European Journal of Social Psychology*, Vol. 45, No. 3, pp. 285-297.
- Dinev, Tamara, Paul Hart, & Michael R. Mullen, 2008/9. “Internet Privacy Concerns and Beliefs about Government Surveillance—An Empirical Investigation,” *The Journal of Strategic Information Systems*, Vol. 17, No. 3, pp. 214-233.
- Duffy, Brooke E. & Ngai Keung Chan, 2019/1. “‘You Never Really Know Who’s Looking’: Imagined Surveillance across Social Media Platforms,” *New Media & Society*, Vol. 21, No. 1, pp. 119-138.
- Hargittai, Eszter & Aaron Shaw, 2013/12. “Digitally Savvy Citizenship: The Role of Internet Skills and Engagement in Young Adults’ Political Participation around the 2008 Presidential Election,” *Journal of Broadcasting & Electronic Media*, Vol. 57, No. 2, pp. 115-134.
- Hayes, Andrew F., Carroll J. Glynn, & James Shanahan, 2005/10. “Willingness to Self-Censor: A Construct and Measurement Tool

- for Public Opinion Research,” *International Journal of Public Opinion Research*, Vol. 17, No. 3, pp. 298-323.
- Ioannou, Athina & Iis Tussyadiah, 2021/11. “Privacy and Surveillance Attitudes during Health Crises: Acceptance of Surveillance and Privacy Protection Behaviours,” *Technology in Society*, Vol. 67, pp. 1-16.
- Malhotra, Naresh K., Sung S. Kim, & James Agarwal, 2004/12. “Internet Users’ Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model,” *Information Systems Research*, Vol. 15, No. 4, pp. 336-355.
- Oz, Mustafa & Akan Yanik, 2022/3. “Fear of Surveillance: Examining Turkish Social Media Users’ Perception of Surveillance and Willingness to Express Opinions on Social Media,” *Mediterranean Politics*, Vol. 27, pp. 1-25.
- Paine, Carina, Ulf-Dietrich Reips, Stefan Stieger, Adam Joinson, & Tom Buchanan, 2007/6. “Internet Users’ Perceptions of ‘Privacy Concerns’ and ‘Privacy Actions’,” *International Journal of Human-Computer Studies*, Vol. 65, No. 6, pp. 526-536.
- Penney, Jonathon W., 2016/1. “Chilling Effects: Online Surveillance and Wikipedia Use,” *Berkeley Technology Law Journal*, Vol. 31, No. 1, pp. 117-182.
- Penney, Jonathon W., 2017/5. “Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study,” *Internet Policy Review*, Vol. 6, No. 2, pp. 1-39.
- Penney, Jonathon W., 2019/3. “Chilling Effects and Transatlantic Privacy,” *European Law Journal*, Vol. 25, No. 2, pp. 122-139.
- Penney, Jonathon W., 2022/4. “Understanding Chilling Effects,” *Minnesota Law Review*, Vol. 106, No. 3, pp. 1451-1530.

- Preibusch, Sören, 2015/5. "Privacy Behaviors after Snowden," *Communications of the ACM*, Vol. 58, No. 5, pp. 48-55.
- Rosso, Mark, ABM Nasir, & Mohsen Farhadloo, 2020/11. "Chilling Effects and the Stock Market Response to the Snowden Revelations," *New Media & Society*, Vol. 22, No. 11, pp. 1976-1995.
- Schauer, Frederick, 1978/3. "Fear, Risk and the First Amendment: Unraveling the Chilling Effect," *Boston University Law Review*, Vol. 58, pp. 685-732.
- Solove, Daniel, 2006/1. "A Taxonomy of Privacy," *University of Pennsylvania Law Review*, Vol. 154, No. 3, pp. 477-564.
- Stoycheff, Elizabeth, 2016/6. "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring," *Journalism & Mass Communication Quarterly*, Vol. 93, No. 2, pp. 296-311.
- Stoycheff, Elizabeth, Juan Liu, Kai Xu, & Kunto Wibowo, 2019/3. "Privacy and the Panopticon: Online Mass Surveillance's Deterrence and Chilling Effects," *New Media & Society*, Vol. 21, No. 3, pp. 602-619.
- Warner, Mark & Victoria Wang, 2019/12. "Self-Censorship in Social Networking Sites (SNSs) – Privacy Concerns, Privacy Awareness, Perceived Vulnerability and Information Management," *Journal of Information, Communication and Ethics in Society*, Vol. 17, No. 4, pp. 375-394.
- Zhong, Zhi-Jin, Tongchen Wang, & Minting Huang, 2017/8. "Does the Great Fire Wall Cause Self-Censorship? The Effects of Perceived Internet Regulation and the Justification of Regulation," *Internet Research*, Vol. 27, No. 4, pp. 974-990.

網際網路

- Cadell, Cate, 2021/12/31. “China Harvests Masses of Data on Western Targets, Documents Show,” *The Washington Post*, <https://www.washingtonpost.com/national-security/china-harvests-masses-of-data-on-western-targets-documents-show/2021/12/31/3981ce9c-538e-11ec-8927-c396fa861a71_story.html>.
- FDR Group & PEN American Center, 2013. *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor*. New York: PEN America, *PEN America*, <https://pen.org/wp-content/uploads/2022/08/2014-08-01_Full-Report_Chilling-Effects-w-Color-cover-UPDATED.pdf>.
- Hampton, Keith, Lee Rainie, Weixu Lu, Maria Dwyer, Inyoung Shin, & Kristen Purcell, 2014/8/26. “Social Media and the ‘Spiral of Silence’,” *Pew Research Center*, <<https://www.pewresearch.org/internet/2014/08/26/social-media-and-the-spiral-of-silence/>>.
- Maniam, Shiva, 2016/2/19. “Americans Feel the Tensions between Privacy and Security Concerns,” *Pew Research Center*, <<https://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/>>.
- Marthews, Alex & Catherine Tucker, 2017/2/17. “Government Surveillance and Internet Search Behavior,” *SSRN*, <<https://ssrn.com/abstract=2412564>>.
- Rainie, Lee & Mary Madden, 2015/3/16. “Americans’ Privacy Strategies Post-Snowden,” *Pew Research Center*, <<https://www.pewresearch.org/internet/2015/03/16/americans-privacy-strategies-post-snowden/>>.
- Roberts, Margaret, 2017/5/4. “Testimony before the U.S.-China Economic and Security Review Commission Hearing on China’s

Information Controls, Global Media Influence, and Cyber Warfare Strategy,” *U.S.-China Economic and Security Review Commission*, <<https://www.uscc.gov/sites/default/files/Molly%20Roberts%20May%204th%202017%20USCC%20testimony.pdf>>.

Teknologirådet & Datatilsynet, 2017/11/7. “The Chilling Down Effect in Norway Privacy Trends 2014,” *Datatilsynet*, <<https://www.datatilsynet.no/en/regulations-and-tools/reports-on-specific-subjects/privacy-reports/chilling-down-in-norway/>>.

The Chilling Effects of Online Surveillance under China's Digital Authoritarianism: An Assessment

Mao-chia Sun

(Assistant Professor, Department of Journalism,
National Defense University)

Abstract

This study investigates whether China's monitoring of activities on Taiwan's Internet and social media may have a chilling effect (e.g., unwillingness to discuss China's sensitive political issues and willingness to self-censor) among the Taiwanese. Using an online experiment that primes participants ($N = 294$) of China's online surveillance, this study found that on China's Internet and social media platforms, when having better online privacy skills, people who were cognizant of China's online surveillance were more willing to search for and discuss China's sensitive political issues than those who were not. People with higher level of online privacy concerns tended to be willing to self-censor when facing China's online monitoring. In other words, variations in intensity of China's online surveillance' chilling effects depends on how much people perceive China's online surveillance and care about their online privacy.

Keywords: Online Surveillance, Chilling Effect, Self-Censorship, Online Privacy Skills, Online Privacy Concerns

