因應中共多模態認知滲透作戰的新型對策：建制大型語料庫數據分析的資安語言學新取徑

摘要

有鑒於臺灣逐年受到中共「認知領域滲透作戰」的大量攻擊，本文針對資安國防概念下位的認知戰層面，提出了臺灣可以採取與建立的新型應對措施機制。本文主要係針對了中共認知滲透作戰作為評估對象，發展資安語言學政策上的方針建議，期許容或可作為未來國防資訊安全的政策建言參照。本文嘗試在較為硬理論的面向上，提供資安語言學文本探勘結合言談解構等質性與量化工具盒整合分析的概括方法論。期許本文的研究結果，往後得以使我方能組成相關跨領域專家團隊，來因應中共認知滲透作戰攻擊之挑戰。

關鍵詞：認知滲透作戰、大數據語料庫、資安語言學、文本探勘分析、敘事語言解構

壹、臺灣民主社會面臨的資安威脅：中共多模態認知滲透作戰

在臺灣這個堅守民主法治的公民社會中，當面臨來自中共的敵對勢力逐步進逼與侵略之際，我們迫切需要應對一項新型的嚴峻挑戰：即中共所發起的「多模態認知滲透作戰」。認知滲透作戰的方式不僅對我們珍貴的民主法治基石和核心價值構成了威脅，而且隨著 AI 技術的結合與應用，認知戰所帶來的威脅已演變為一種融合資訊戰與心理戰的灰色地帶攻勢，其根本目的在於瓦解臺灣的民主法治架構及政府的統治正當性，而在宏觀的數據倫理學(data ethics)考量上，中共採取這種涉及資訊與媒體來影響人們信念、價值觀和行為的認知領域滲透作戰方式，會造成整體社會和文化群體相當大的不利影響與衝擊(Floridi&Taddeo, 2016)。

在當今資訊社會的快速發展與現代第六代戰爭型態的不斷變化背景下，認知領域的滲透作戰已經成為一種新興而主流的戰爭手段，其核心目標在於影響、操控並控制對方在軍事、政治、經濟決策層面以及對社會大眾輿論的認知過程，進而達成全面戰略和具體戰術目標。King et al.（2017）指出，這種策略通常包括對社交媒體和網絡空間的大規模操控，以影響公眾輿論和政治決策。隨著 AI 技術的持續進步，無論認知滲透作戰在境內外的實施，中共的敵對勢力運用認知滲透作戰的手段和策略也在不斷地演進和更新。AI 作為當前的技術革新重大進展，不僅改變了戰爭的面貌，也為認知戰提供了新的工具和方法（Kello, 2017）。[1]

[1] Kello (2017)運用國際關係理論，探討當代技術革命在資訊戰與認知戰的影響，討論範圍主要涵蓋伊朗的 Stuxnet 行動、索尼影業遭受的資安風暴與攻擊、2016 美國大選俄羅斯的介選行動；其主要貢獻在於深入解析了當前的網絡革命，並通過案例研究來發展理解其對國際秩序影響的概念框架。

這種技術的應用使得敵對勢力能夠更加精準地定位和影響目標群體，從而提高其策略的有效性。這不僅凸顯了我國長期處於戰爭邊緣的嚴峻現實，更加迫切地突顯了制定和實施有效反制策略的重要性。本文指出，為了有效地抵禦中共的認知滲透作戰，我們必須從多個層面加強我們的防禦能力和反制能力。

第一，我們必須提高我們對中共認知滲透作戰的識別和分析能力，並及時揭露和反駁其所散佈的虛假或歪曲的資訊。這方面的研究表明，對於虛假資訊的識別和反駁是一項複雜且挑戰性的任務，需要綜合運用多種技術和方法。

第二，我們必須加強我們自身的認知安全和抵抗力，並培養我們對資訊來源和內容的批判思考能力。在這方面，研究指出，提高公眾的媒體素養和批判性思考能力對於抵禦認知滲透至關重要（Lewandowsky, Ecker, & Cook, 2017）。

第三，在「後真相（post-truth）」時代中，要研究誤導訊息和爭議訊息時，我們必須建立一個有效且協調的跨部門、跨學門、跨國際夥伴的反制機制，並將此議題放置於更宏觀的政治科技社會背景中來考慮這些問題（Lewandowsky, Ecker, & Cook, 2017）。並且需利用各種媒介和平台積極宣揚我們的民主法治理念和核心價值。而在跨學門層面，筆者將綜合心理學、語言學、社會學等方面發展一個新的跨領域研究取向，這一點可謂與 Van Dijk（2014）的研究不謀而合。[2]

---

[2] Van Dijk（2014）強調跨學科合作在對抗認知戰中的重要性；Lewandowsky et al.（2017）也強調了跨學科的技術認知（Technocognition）的重要性，不僅需要從個體心理學層

第四，我們必須持續推動科技創新和國防研究人才培育，並加強我們在 AI 技術領域的競爭力和影響力（Russell & Norvig, 2016），相關方面的研究強調了 AI 技術在提高資訊戰和認知戰能力方面的潛力。

第五，本文也建議我方參照中共與美國使用 AI 發展融合戰略與戰術目標的對策；舉例來說，中共解放軍戰略支援部隊正在發展人工智慧創新能力，並試圖將 AI 及即時語言判讀系統有效地融入武裝力量，該戰略支援部隊負責整合多種「戰略功能」，其中包括資訊領域和有效整合人工智慧，這可能決定未來衝突中的勝負（謝，2019）；又例如，美國 AI 開發商 Scale 公司已將新開發的 AI 軟體「Donovan」交付美陸軍第 18 空降軍進行情報分析測試。這套系統運用「大型語言模型」和「人類回饋強化學習」技術，可快速處理高達 10 萬則行動命令及情蒐報告等即時訊息（翟&吳，2022）。

最後，我們必須堅定不移地捍衛我們的國家主權和國防安全利益，並與國際社會共同維護區域和平與穩定（尤，2020；鄭&華，2020；河，2008）。藉由專業的研究人才，從國家安全與國防的角度評估混合戰的影響，並分析認知戰操作的層次與攻擊策略，提供相關的反制對策，惟有如此，我們才能有效地抵抗中共的認知滲透作戰（陳&徐，2021; 林，2021）；藉此來保障我們的民主法治和核心價值不受侵蝕和破壞。筆者認為，這會是我們長期戰略的核心目標。

這種認知領域作戰模型的研究，對於理解中國如何透過媒體戰爭影響其他國家，結合中共四種介選與其他模式的認知滲透攻擊，在臺灣民主政治運作下定期兩年一次的選舉中，具有重要的參考價值，筆者將其謂之為「多

面出發，考慮到個體的認知過程，也需要評估到更宏觀的政治、科技和社會背景。Lewandowsky et al.（2017）從個體心理學導向社會體制，跟本文從知覺心理學中的認知滲（cognitive penetration）的概念出發，導向更普遍針對國防敵對勢力的社會認知滲透作戰攻擊現象進行探討，在方法論的取徑上可謂是遙相呼應。

模態認知滲透作戰」。「多模態（Multi-Modal）」意指著網路科技令攻擊管道與媒介的多元性、泛用性、以及其交叉使用的多方效應，在國家政府集體層面、軍事新聞單位層面、相關企業及利益關係團體層面、乃至公民與國民個人層面，以不同傳播媒介所造成的心戰影響（沈，2009）。中共的多模態認知滲透攻擊意圖導致我國各方能動者的集體機關失靈現象或產生決策偏誤的情況發生，例如：錯估開戰的可能性、擬定錯誤或不利於我方的戰略政策或戰術目標（譚&林，2023）。

中共首先透過外宣模式（沈，2021），利用各種媒體和平台，向國際社會傳播其政策和立場，並試圖塑造一個正面的國家形象。再者，中共還利用粉紅模式，透過社交媒體上或由共青團假冒（沈，2021）、或由中共公務員偽裝（King, Pan& Roberts, 2017）的大量政治狂熱粉絲和網民，對外傳播其反分裂國家政策與不排除以任何方式解決內政問題的武統立場，對於外界的合理批評和質疑進行誣蔑詆毀性與破壞性的反擊。接著，中共還利用農場模式，透過官方渠道或非官方媒體與互聯網企業合作製造大量的網絡水軍和假新聞，對外與對內傳播其政策和立場（李，2006），試圖影響和操縱外界的輿論，並動搖臺灣的民心與士氣。

最後，中共還利用協力模式（沈，2021），讓完全無關的人自動協助散布爭議消息或假訊息，例如讓知名電影「神力女超人」女主角演員蓋兒加朵在其 Instagram 帳號上分享中國新華社的內宣新聞（信傳媒，2020），其在推特 Twitter 亦分享了方艙醫院的影片獲得大量網民和影視娛樂明星轉傳（ABC, 2022），直接擴大影響這些假訊息或爭議訊息的傳播範圍，並透過與台灣的「在地協力者」或其他國家個人和組織合作和結盟，對外傳播其一個中國政策和反分裂國家法不排除武統台灣的立場、抑或假冒海內外普通國民傳遞對臺灣執政當局的不滿（沈，2021），從而試圖獲得外界與其友邦的支持和認同。

而自臺灣全面直選施行至今的近二十多年來，中共逐年加強在介選上的認知滲透作戰，這種策略被視為有效降低對臺統一或侵略成本的滲透戰略

（松田康博，2021）。對於中共來說，能夠順利統一解放臺灣最低成本的方式，即是大幅干預臺灣的定期大選，藉由金援或招待來獲得台灣「在地協力者」的幫助，選出紅統派的總統、官員、立法委員、議會民代、里長（公視新聞網），透過改變臺灣的憲政法治結構基礎，達成「加速祖国统一的中华民族伟大复兴理想」。而即便最終中共還是需要採取有限度武力收復臺灣的手段，也可以透過影響「台湾当局」的主要政策，使我國政府大步在社會政經層面讓利中共、減少與國際聯盟的軍事合作、降低國防預算及降低軍事抵抗的意願與能力，再透過心戰與資訊戰操縱懼戰與拒戰投降的民意，進而使武力犯台的軍事成本降至最低。

中共對台進行資訊戰與認知戰的事實、以及相關認知滲透傳播過程的具體證據，在台灣資訊環境研究中心 IORG（Taiwan Information Environment Research Center）的研究下，也被美國在台協會 AIT 發言人孟雨荷在 2020 年所認證背書（李，2020）。

由此可見，對於臺灣而言，中共的認知滲透作戰對其實已構成了嚴重的潛在實質威脅。以沈（2021）提出的模型來看，中共透過外宣模式，對國際社會進行大量的宣傳和說服，試圖塑造臺灣僅是中國的一部分內政問題的國際形象。此外，中共還利用粉紅模式，對臺灣的政策和立場進行大量的批評和攻擊，試圖操縱和影響臺灣內部的輿論。再者，中共還利用農場模式，對臺灣進行大量的網絡攻擊和滲透，試圖破壞臺灣的資訊安全和網絡防禦。最後，中共還利用協力模式，透過與其他國家和組織的合作和聯盟，對臺灣進行外交上的孤立和打壓（Feldman,Dant & Massey, 2019）。

而為了應對中共的認知作戰，臺灣需要加強自身資訊安全和網絡防禦能力。意即，臺灣需要建立一個完善的資訊安全國防體系，確保政府、軍隊和企業的資訊系統不受到外部的攻擊和滲透。在資訊相關的硬體工程方面，臺灣需要加強自身的網絡防禦能力，確保我方網絡基礎設施不受到外部的破壞和攻擊。此外，在防堵中共的銳實力（sharp power）方面，除了資訊安全國防體系結合 AI 技術的應用以外，臺灣還需要加強自身的資訊安全教育和公

眾宣傳，提高民眾的資訊安全意識和防範能力，以應對中共的超限戰、認知滲透作戰和心戰攻擊（Cardenal et al., 2017; Hongzhi Qi et al., 2023）。

在粉紅模式與農場模式上，King et al.（2017）估計中國政府每年製造並發布約 4 億 4800 萬條社交媒體評論，這些社交媒體評論主要目的與意圖是分散公眾的注意力並改變話題。中共利用這種「偽裝草根」的策略，秘密發佈大量偽造的社交媒體評論，並偽裝成是普通中國網民的真實觀點，藉此來引導公眾輿論的趨勢與走向。大多數這些帖子（貼文）都是為中國、共產黨的革命歷史、或其政權符碼打氣。實際上，這些帖子的發布者實際上並非一般民眾，而是具有中共公務員身分的網軍。其行動時間點在於，重大事件發生、某個社會議題延燒、甚至引發不滿或質疑的聲浪發生時，中共就會利用「偽裝草根」的策略，發佈大量偽造的社交媒體評論。

King et al.（2017）的研究還發現，這些公務員並未收到任何「稿費」，這些發文亟可能就是他們原本的工作內容，且每年四億多的貼文有一半發表在政府網站，其他的則被送到 7 億網民活躍的社群媒體，受到五毛黨出沒影響的網站包括騰訊、新浪和百度。King et al.（2017）在數據搜集層面上首先收集了大量的社交媒體貼文。他們在 2014 年 12 月獲得了一份由匿名博主 xiaolan 發布的文檔，該文檔包含了 2013 年和 2014 年間章貢地區網宣辦賬號收發的郵件。這些郵件揭示了網絡評論員的活動，包括大量的五毛言論。由於這些文檔數量龐大、結構複雜，King et al.（2017）發展出了一種方法和流程，從大量的人工編碼，到自動化的文本分析和抓取，使得這些資料變得結構化和易於讀取。而這也正是本文建議我方政府單位與情報研究單位建置大型語料庫，進行自動化文本分析的參考依據方法之一。

值得注意的是，中共的認知滲透作戰不僅僅是針對臺灣，它還針對其他國家和地區，試圖透過認知作戰來達到其政治、經濟和軍事上的目的。為了有效地應對中共的認知作戰，國際社會需要加強合作，共同制定和實施有效的策略和措施，以確保資訊安全和網絡防禦（Hu et al., 2023）。此外，AI 技術在認知作戰中的應用也帶來了新的挑戰和機遇。例如，AI 技術可以被用

於分析和預測敵方的認知作戰策略和手段，從而提前做好防範和應對。同時，AI 技術也可以被用於加強我方的認知作戰能力，透過分析和利用敵方的認知弱點，進行有效的心理戰和輿論戰。然而，AI 技術在認知作戰中的應用也帶來了新的倫理和法律問題。例如，AI 技術可能被用於進行大規模的網絡監控和數據分析，這可能會對個人隱私和自由權利構成威脅。此外，AI 技術在認知作戰中的決策過程可能會產生偏見和歧視，這使得在認知作戰中使用 AI 技術的恰當性受到了質疑（Feldman,Dant & Massey, 2019）。因此，為了有效地應對認知作戰的威脅和挑戰，我們需要加強研究和合作，制定和實施有效的策略和措施，確保資安國防和網絡防禦。

貳、資安語言學對策：大型語料庫分析與文本語體判別

語料庫分析是一種利用大量語料庫數據來研究語言使用模式的方法。在應對認知作戰中，語料庫分析可以用來識別和分析中共宣傳材料中的語言特徵和模式。透過分析這些材料中的詞彙選擇、語法結構和話語風格，可以揭示中共在其宣傳中所使用的語言策略和技巧（Baker, 2006）。此外，語料庫分析還可以用來識別和追蹤中共宣傳材料中的主題和話題變化，從而更好地理解其宣傳的焦點和目的（Gabrielatos & Baker, 2008）。語料庫分析在識別中共認知作戰中的語言操縱方面具有重要意義，透過分析中共宣傳材料中的詞彙選擇和語法結構，可以揭示其試圖塑造的特定形象和觀點。本文發現，中共會選擇某些詞彙來強化其政策的正當性，或者使用特定的語法結構，來隱藏其認知滲透作戰宣傳的真實意圖（Partington, 2014a; 2014b）。

在反心戰層面上，臺灣還可以利用語料庫分析來發展自己的宣傳材料，透過使用更加客觀和真實的語言，來反駁中共的宣傳和提升自己的國際形象（Baker, 2010）。然而，語料庫分析在應對認知作戰中也面臨著一些挑戰和限制。首先，語料庫分析依賴於大量的語料數據，而這些數據可能難以獲取或者存在偏見和不完整性（McEnery & Hardie, 2011）。然而，雖然語料庫分析是一種基於數據的分析方法，它可能無法完全揭示宣傳材料中的隱喻和象徵意義（Sinclair, 2004）。因此，在應對認知作戰時，語料庫分析需要與

其他方法和策略（例如：語體判別）相結合，以發揮最大的效果（Biber & Conrad, 2009）。

語體判別解構（genre analysis）是一種慣用於分析文本語言風格的方法，並可被用來識別和分析中共宣傳材料中的語言特徵和風格，藉由分析文本中的詞彙豐富度、句子結構和修辭手法，可以揭露與統計分析中共在其宣傳中所使用的語言風格和表達方式（Leech & Short, 2007）。此外，透過語料庫分析與語體判別還可以用來識別和判定中共宣傳材料中的隱喻和象徵（Leech & Short, 2007），從而更好地理解其宣傳的隱含意義和意識形態（Semino & Short, 2004），這些包裝後的統戰意識形態很可能會被用來操縱目標受眾的情感和認知（Charteris-Black, 2004）。

運用語體判別解構方法的優勢是，臺灣可以透過分析中共宣傳材料的語言風格來揭露其操縱和誤導的策略。舉例來說，中共可能會使用某些修辭手法或修辭語步來強化其政策的正當性，或者使用特定的語言風格來隱藏其宣傳的真實意圖（Fowler, 1991），揭示其如何通過語言使用上的選擇來塑造閱聽人特定的社會和政治身份（Wodak & Meyer, 2009）。透過識別這些語言風格和修辭手法，臺灣可以更好地理解中共宣傳的策略和目標，藉由揭露中共宣傳中的語言操縱和偏見，我方可以制定相應針對性的事實澄清、爭議消息反駁、反心戰宣傳…等有效的反擊策略。

在探討語料庫與語體判別分析在對抗中共認知作戰方面的應用時，我們仍然必須同時考慮到資訊安全（Information Security）的重要性。資訊安全不僅涉及技術層面的保護，也包括對資訊內容的分析和管理（Pfleeger & Pfleeger, 2012）。在這方面，語料庫分析可以作為一種有效的工具，幫助識別和分析可能對臺灣民主社會構成威脅的虛假資訊和深度偽造（Deep Fake）內容。中共在其認知作戰中可能會使用深度偽造的假新聞（Fake News）、爭議訊息和虛假資訊來影響公眾輿論和操縱認知。這些虛假資訊可能被巧妙地包裝，使其看起來可信，從而對目標受眾產生不良影響（Allcott & Gentzkow, 2017）。

在這種情況下，語料庫分析可以透過分析這些資訊的語言特徵和模式，來揭示其虛假和誤導性質。例如，語料庫分析可以識別出虛假資訊中經常出現的詞彙和語法結構，從而幫助人們識別和質疑這些資訊的真實性（Conroy, Rubin, & Chen, 2015）。此外，中共可能會利用深度偽造技術來製作和傳播虛假的影片和聲音內容，以進一步操縱公眾輿論（Chesney & Citron, 2019）。在這種情況下，語料庫分析可以透過分析影片和聲音內容中的語言特徵，來揭示其虛假和操縱性質。例如，語料庫分析可以識別出深度偽造內容中不自然的語言使用和語調變化，從而幫助人們識別和質疑這些內容的真實性有多高（Tolosana et al., 2020）。

此外，文本探勘分析臺灣還需要考慮到社交媒體在中共認知作戰中的作用。社交媒體在當今時代已成為資訊傳播和公眾輿論形成的重要平台。中共可能會利用社交媒體來傳播虛假資訊和假新聞，以影響公眾輿論和操縱認知（Woolley & Howard, 2016）。在這種情況下，語料庫分析可以用來識別和分析社交媒體上的虛假資訊和假新聞的語言特徵和模式。例如，語料庫分析可以用來識別社交媒體上虛假資訊中經常出現的詞彙和語法結構，從而幫助人們識別和質疑這些資訊的真實性（Conroy, Rubin, & Chen, 2015）。此外，語料庫分析還可以用來識別和分析社交媒體上的操縱性言論和假帳號的語言特徵和模式，從而幫助防止這些操縱性言論和假帳號對公眾輿論的影響（Woolley & Howard, 2016）。透過持續的語料庫分析，臺灣可以建立一至多個可靠且被信賴的資料語料庫（例如：「臺灣事實查核中心 Taiwan FactCheck Center」即是一個可供參照的優良典範），用於追蹤和監控社交媒體上的虛假資訊和假新聞，從而更好地保護公眾輿論免受操縱。

在應對中共認知作戰的過程中，臺灣還需要考慮到國際合作的重要性。國際合作可以幫助臺灣分享和獲取有關中共認知作戰的資訊和經驗，從而更好地應對這些威脅（Nye, 2011）。在這方面，語料庫分析可以用來識別和分析不同國家和地區的中共認知作戰的語言特徵和模式，從而幫助臺灣與其他國家和地區共享和交流經驗和策略。例如，語料庫分析可以用來識別和分析中共在不同國家和地區的宣傳材料中的語言特徵和模式，從而幫助臺灣

與這些國家和地區共同應對中共的認知作戰（Nye, 2011）。此外，國際合作還可以幫助臺灣獲取更多的語料數據和分析工具，從而提高語料庫分析的效果和準確性（Biber & Conrad, 2009）。透過國際合作，臺灣可以與其他國家和地區共同應對中共認知作戰的威脅，從而更好地保護自己的民主社會和國家安全。舉例來說，我們可以使用 AntConc 進行中共假新聞，藉此來揭示假新聞中的語言特徵和模式。AntConc 是一款語言學家常用的語料庫分析工具，它能夠進行詞頻統計、關鍵詞分析、共現分析等多種功能，並可用於假新聞造謠資訊與爭議消息的分析。以下是使用 AntConc 分析步驟：

(1)收集數據：首先，需要收集一定數量的中共假新聞、造謠資訊或爭議訊息。這些文本可以來自不同的新聞來源，包括網站、社交媒體、報紙、互聯網遊戲等。

(2)預處理文本：將收集到的文本進行預處理，包括去除無關內容（如廣告、版權資訊等）、統一格式、分詞等。

(3)導入文本：將預處理後的文本導入 AntConc。可以將所有文本合併成一個大的文本文件，或者將每條爭議訊息作為一個單獨的文件導入。

(4)詞頻統計：使用 AntConc 的詞頻統計功能，分析爭議訊息中最常出現的詞語。這有助於識別假新聞中的常用詞彙和主題。

(5)關鍵詞分析：進行關鍵詞分析，找出與一般訊息相比，在爭議訊息中顯著多出或少出的詞語。這有助於識別爭議訊息的特殊語言特徵。

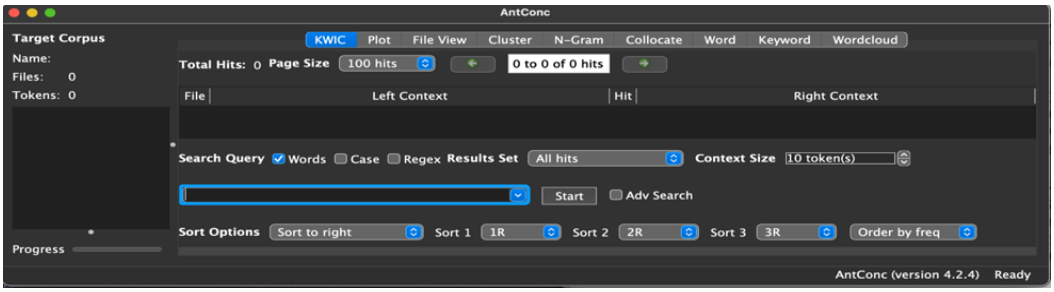
(6)共現分析：使用共現分析功能，探究特定詞語在文本中共同出現的模式。這有助於理解爭議訊息中的語境和話語結構。

(7)語境分析：查看特定詞語在文本中的具體使用情況，了解其在爭議訊息中的語境和含義。

(8)綜合分析：根據上述分析結果，進行更深入的質性分析，如話語分析、修辭分析等，以揭示境內外敵對勢力爭議訊息所包裝的隱含意義和意識形態洗腦策略。

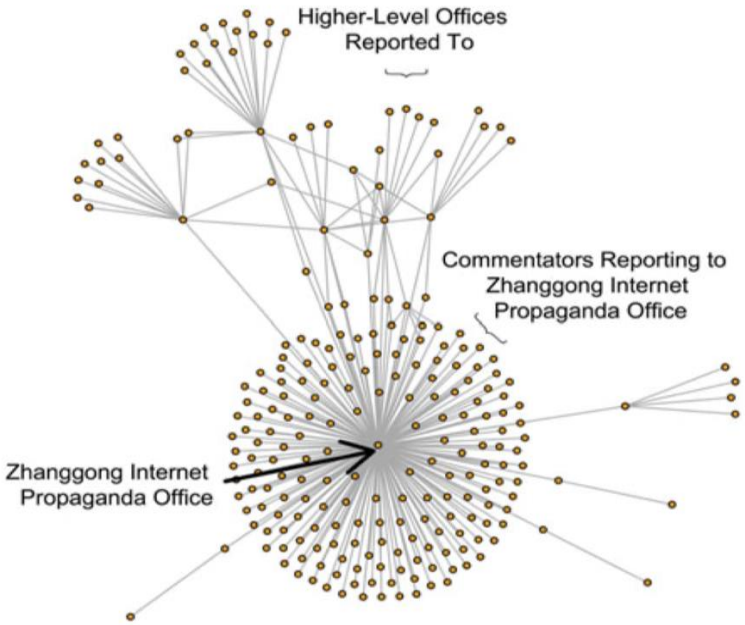
(9)結果整理與報告：可結合 R 與 Python 等編程語言將分析結果整理成報告，包括數據統計、圖表、分析解釋……等等。

圖 1 AntConc 介面使用示意圖



圖片來源： 筆者自製（使用 AntConc 軟體）

圖 2 藉由關鍵詞分析找尋傳播網路路徑示例



圖片來源：King et al.(2017) p.487

在利用 AntConc 收集中共爭議訊息或造謠資訊文本的過程中，我們可以參考下列文獻中的研究方法。

首先，可以參考 Ross& Rivers（2018）的研究，他們透過對川普推特（Twitter）言論的語料分析，揭示了川普如何作為一個連續的錯誤和假新聞的傳播者。此外，也可以參考 Chan et al.（2023）研究採用 Box-Jenkins 時間序列分析（TSA）方法，其研究中英文 COVID-19 新聞報導中的戰爭隱喻使用是否可以用 ARIMA（自回歸整合移動平均）模型來擬合，上述研究都可以提供我們在收集和分析假新聞或造謠資訊文本時的參考，採用新的基於語料庫的計算方法來處理關鍵詞排名問題，這對於我們在處理大量文本數據時可能非常有效（Chen&Chang, 2021）。此外，我們還可以參考 Li et al.（2023）使用 AntConc 3.3.5 進行符合分析，研究中美兩國新聞報導在報導 COVID-19 大流行時使用的報導動詞的分布特徵。最後，我們也可以參考袁&童（2022）在中文文獻中應用 DTA（discourse-theoretical analysis）話語分析理論工具，考察科技報導新聞中的話語框架。

而對於認知滲透作戰的關鍵詞分析，我們可以參考 King et al.（2017）的研究方法，從社交媒體上抽取包含「五毛黨」關鍵詞的貼文，並對這些貼文進行分析。King et al.（2017）運用了 Wang&Rudi（2015）和 Letham et al.（2015）的貝氏降冪規則列表（Bayesian falling rule list）的方法來區分出「普通賬戶」和「特殊賬戶」，在算法設計上加入了單調性約束，基於輸入特徵的離散化，每個特徵可以轉換為簡單的布爾向量，從而加快了運算速度。King et al.（2017）發現透過貝氏降冪規則列表，只需要運用兩個階段的步驟就能從 4 萬 9850 則貼文中區分出「普通賬戶」和「特殊賬戶」這兩種賬戶：首先，他們從章貢區政府微博賬號收集到所有對這個賬號發出的貼文進行轉發和評論的賬號，把他們當做「候選賬號」；然後，他們縮小範圍，選擇其中粉絲數小於 10 的賬號。

King et al.（2017）把篩選出來的賬號稱為「特殊賬號」，接著分析了從章貢區網信辦洩露的 4 萬 3757 則「五毛貼文」，這些貼文由大量不同的作者撰寫，來自多個不同的社群網站，包括由私人公司運營的全國性的平台，例如新浪微博、百度貼吧，以及政府運營的網站，包括全國性的、省級和區縣級的網站（King, Pan& Roberts, 2017）。本文建議參考 King et al.（2017）

的關鍵詞分析方法應用資安語言學的面向上，來反堵中共對台進行的認知滲透作戰，其主要優點在於整合 Wang&Rudi（2015）和 Letham et al.（2015）的貝氏降冪規則方法，在其解釋性可以將定性知識和機器學習(ML)結合起來，同時也能夠讓我們更加容易地將分析範圍應用到更廣泛的區域傳播路徑上。

叁、針對中共宣傳材料的大數據語料庫分析與電腦統計語言學

語言數據分析在識別和分析中共宣傳材料中的語言模式和話題和主題變化的趨勢方面都具有重要意義，且可以搭配網路議題數據流量進行交叉分析。具體來說，我們可以藉由分析與揭示中共宣傳材料中（社群網路、新聞文宣、影音(長短視頻)、輿論）的關鍵詞彙、語法結構、話語主題（參見 Baker, 2006），來推論其試圖塑造的特定形象和意識形態觀點。具體來說，在社會語言學上我們通常透過語言變體（variety）與語言變異（variation）的方式掌握相關現象（邢，2004）。粗略地說，「語言變體（variety）」是關於地域空間上的地理語言學概念（洪，2015），如東北與黃河流域的漢語習慣、長江與東南流域漢語習慣差異；「語言變異（variation）」則較著重時間演變與同一群體中不同年齡使用語言差異的跡象。而例如大陸常用的詞彙「80 后、90 后、00 后」（陈，2021），對比於臺灣三十歲以上族群常用的「六年級生、七年級生、八年級生」的名詞組漢語差異，其實並不直接反映在語意（semantic）或實質指涉意義（referential meaning）上，而是同時在「語言變體（variety）」與「語言變異（variation）」這兩個社會語言學的文化與語言變遷模式中產生此現象（张＆赵，2018）。

「名詞組」的語言變遷模式，較容易被中共敵對資訊作戰單位快速的覺察掌握與進行即時修正。然更細部來說，我方單位可以從句法（syntactic）角度上同樣觀察到上述現象的發生。理論上雖然漢語詞綴和類詞綴是詞彙意義完全虛化或部分虛化，而卻具有語法組詞功能的一種詞素（金，2006），這些詞綴、類詞綴本身不能獨立使用，但我們可以觀察到中國北方出現「的」在句中或句尾作為綴詞的比率與文法合法度都相較於臺灣高。例如：中國較常出現「总『的』来说」、臺灣則較少出現前述用法，臺灣較習於使

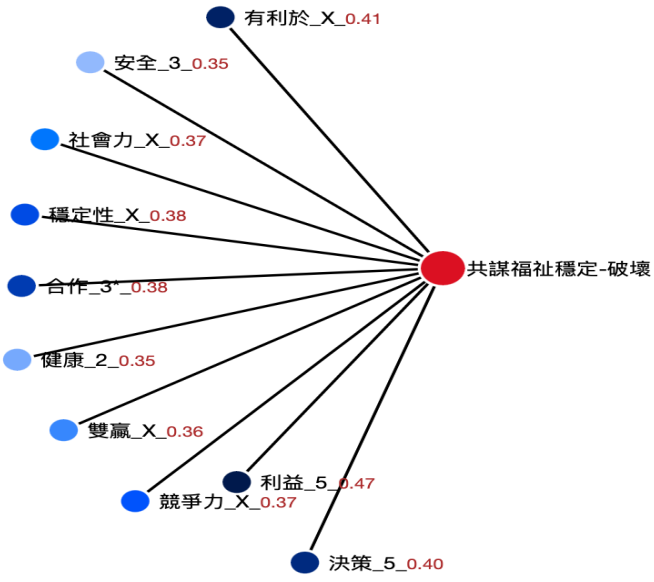
用「總體來說」或「整體來說」；另外，中國大陸境內使用「呀」或「的呀」作為句尾語助詞的頻率也相較於臺灣高出不少；臺灣常常也出現「有/了」的交替規律，例如肯定答句「她昨天有來(了)」（陳，2012）。這些細微的漢語句法區域差異，是無法只靠所謂「简体转繁体」或「专名替换」的方式，來遮掩蓋飾其發布來源是來自於非臺灣地區協力推送者的強烈語言學證據之一。

在大量的語言數據分析下，這些跡象都屬於能讓我方各層級單位判別特定資訊是否為來自境外敵方勢力的有效工具與實用對策方法（Fisher et al., 2022）。因此，本文建議政府應建置有效的人工智慧自動辨識語料庫系統與語言數據分析團隊，可參考 Shuyo（2010）的語言檢測庫以 Java 實現 xml 生成語言配置文件，並以貝氏過濾器（Bayes classifier）檢測拼寫的機率，使用 Apache License 2.0 許可證達到 99.8%的精確度；利用相似並優化的語料庫建置成為防堵中共認知領域滲透作戰的反制單位（Baughman, 2023）。這樣的系統可以透過大數據分析，提供政府機關以數據為基礎的決策依據，例如：美國國防部使用 AAF（自適應採購框架, Adaptive Acquisition Framework）簡化與加速軍武採購的流程與速度（McKernan et al., 2023），語言與大數據分析也能有效地識別和防止外國勢力透過社交媒體進行的影響操作（López & Madhyastha, 2021）。

同時，由於中共可能會選擇某些詞彙及修辭語步（rhetorical move），或者使用特定的語法結構來隱藏其宣傳滲透的真實意圖（Partington, 2014a; 2014b），來強化其政策對外的正當性，例如當涉及統一的政策時，中共官媒或外交部會偏向「團結協作」、「共維和平」、「共促發展」、「和衷共濟」、「團結向前」、「共謀福祉」、「走近走親」、「迎接回歸」、「復興解放」、「融合發展」等用詞，取代實質上是「武力併吞侵略臺灣主權」等明顯影響我國國家安全與主權事實的攻擊意圖，從而更好地包裝其宣傳焦點和目的（Gabrielatos & Baker, 2008），藉此來降低臺灣及其他國際盟友的戒心。

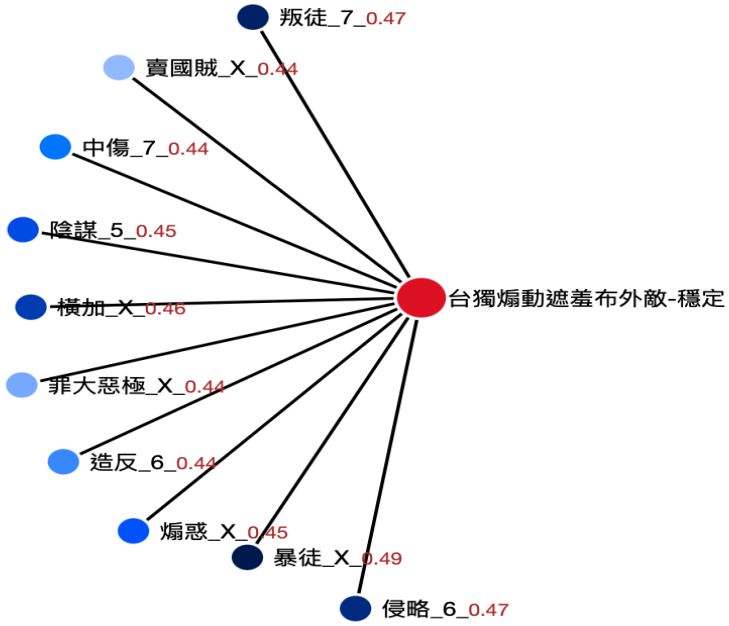
而本文建議建置良好的自動辨識語料庫逕行的語言數據分析，其可以揭示中共國台辦、外交部、官媒對外宣傳材料中所包含特定模式，e.g.「砌詞狡辯」、「拒統偏安」、「以台制華」、「頑冥不化」、「自身覆滅」、「破壞穩定」、「法理現實」、「災難深淵」、「挾洋自重」、「勾連外敵」、「煽動對抗」、「混淆視聽」、「頑固挑釁」、「告洋狀」、「遮羞布」、「五宗罪」……等等），這些夾帶統戰威懾的意識形態象徵，常被中共用來操縱目標受眾的情感和認知，從而間接促進中共的政治目標（Chilton, 2004; Charteris-Black, 2004）。以下是中國人民網與中國共產黨新聞網擷取高頻詞彙，來顯示中共在進行認知滲透戰時，所偏好選擇的詞彙其關聯語義場與共伴詞頻指數。由下列語義場關聯圖可以發現，中共媒體在其宣傳材料中，試圖用「共謀」」「福祉」、「穩定」等詞彙，導向「利益(0.47)」、「合作(0.38)」、「競爭力(0.37)」、「雙贏（0.36）」、「安全（0.36）」塑造中國統一正面形象的詞彙，來降低中共統一武嚇台灣的對人民產生的排斥觀感作用，並試圖提高臺灣民意對於統一的好感與接受度：

圖 3 語義場關聯詞分析圖：中共統戰詞彙塑造的形象



圖片來源：筆者自製

圖 4 語義場關聯詞分析圖：對於臺灣主權塑造破壞和平穩定的負面形象



圖片來源：筆者自製

反之，由上圖可見，面對臺灣執政黨堅決維護主權尊嚴與國際民主夥伴結為同盟時，中共慣於使用「台獨」、「煽動」、「遮羞布」、「外敵」，關聯到「暴徒(0.49)」、「侵略(0.47)」、「陰謀(0.45)」、「賣國賊(0.44)」等負面破壞台海穩定的形象，藉機來對外宣傳「臺灣屬於中國內政問題」的一個中國框架，並且合理化中共當局以武力恫嚇攻佔台灣與發起戰爭的可能性、與加強宣傳其環島軍演與共機侵入我方航空識別區的法理正當性（譚&林，2023）。

本文建議我方透過語言數據分析與文本判別的統計語言學方法，藉由判定特定宣傳材料的「來源域」、「目標域」、「類屬域」、「透射域」，有效的讓臺灣政府與軍情單位在應對中共的認知滲透作戰時，利用數據分析的結果來發展有效的反宣傳策略。意即，我方可以透過識別中共宣傳中的語言模式、趨勢走向、新興用詞，臺灣可以更好地理解其宣傳的策略和目的，並制定針對性的反駁和反擊策略。例如，臺灣可以透過揭露中共宣傳中的語言操縱和偏見，來揭示其宣傳的虛假和誤導性（Wodak & Meyer, 2009）。此

外，臺灣還可以利用語言數據分析來發展自己的宣傳材料，透過使用更加客觀和真實的語言，來反駁並澄清中共對外與對內的宣傳和提升臺灣自己的國際形象（Baker, 2010），並藉此建立與維繫可靠的國際盟友支持關係。

在進行語言數據分析時，臺灣可以利用各種語料庫工具和技術來進行深入的語言分析。例如，臺灣可以使用詞彙分析工具來識別中共宣傳材料中的關鍵詞彙和詞彙模式，這些詞彙可能被用來塑造特定的形象或觀點（Biber & Conrad, 2009）。此外，臺灣還可以使用語法分析工具來分析中共宣傳材料中的語法結構和句式中的語用學（Leech & Short, 2007）。除了識別和分析中共宣傳材料中語言的語意或語用特徵外，臺灣還可以利用語言數據分析來監測和追蹤中共宣傳的傳播和影響。例如，臺灣可以使用社交媒體分析工具來追蹤中共宣傳在社交媒體上的傳播和影響，並識別其宣傳的目標受眾和傳播渠道（Woolley & Howard, 2016）。此外，臺灣還可以使用輿情分析工具來監測中共宣傳對公眾輿論的影響，並識別其宣傳可能引起的社會和政治反應（McEnery & Hardie, 2011）。透過這些監測和追蹤工具，臺灣可以更有效地應對中共宣傳的傳播和影響，並及時制定相應的反應策略。

語言數據分析在應對防範認知作戰中，主要會面臨著兩項挑戰和限制：

（一）臺灣的有限經費與技術成本考量，首先，語言數據分析依賴於大量的語言數據，而這些數據可能難以獲取或者存在偏見和不完整性（McEnery & Hardie, 2011），同時，語言數據分析可能需要複雜的統計方法和演算法，這可能對分析人員提出較高的技術要求（Biber & Conrad, 2009），於此同時，語言數據分析在處理大量數據時可能面臨計算資源和處理速度的限制，這可能影響分析的效率和時效性（Leech & Short, 2007），而需要具有更高階算力的設備（如：量子電腦）。再者，語言數據分析可能受到語言多樣性和變異性的影響，不同的語言和方言可能具有不同的語言特徵和用法，這可能增加分析的複雜性和難度（Partington, 2014a; 2014b）。此外，語言數據分析可能面臨語境和文化差異的挑戰，不同的文化和社會背景

可能影響語言的使用和理解，這可能對分析的準確性和有效性構成挑戰（Charteris-Black, 2004）。

（二）中共的多模態認知滲透作戰手段工具改良與策略移轉，在應對中共認知作戰的過程中，語言數據分析作為一種重要的工具，其應用範圍和影響力不容忽視，以就是說，除了技術成本上的挑戰和限制之外，語言數據分析在應對中共認知作戰時還面臨著其他一些困難和障礙。首先，中共宣傳的語言策略可能會隨著時間和情境的變化而變化，這使得持續追蹤和分析其語言模式和趨勢變得更加困難（Baker, 2010）。中共可能會不斷調整其宣傳的語言和策略，以應對外部環境的變化和挑戰，這可能使得語言數據分析的結果失去時效性和針對性（Gabrielatos & Baker, 2008）。其次，正如昔前所述，中共宣傳會使用隱晦或含糊的語言來掩蓋其真實意圖和目的，這可能使得語言數據分析難以識別和揭露其宣傳的真實性和誤導性（Wodak & Meyer, 2009）。中共可能會故意使用模糊或雙關的語言來迷惑和誤導目標受眾，這增加了語言數據分析的難度和複雜性（Partington, 2014a; 2014b）。此外，中共宣傳可能會利用先進的技術和手段來傳播和擴散其宣傳，這使得語言數據分析變得較難以追蹤和監測其傳播和影響（Woolley & Howard, 2016）。例如：中共可能會利用新興的社交媒體、網絡平台和其他傳播渠道（如：線上互聯網即時遊戲）來加強傳播其宣傳，這可能使得語言數據分析難以全面和及時地監測其傳播範圍和影響力（McEnery & Hardie, 2011）。

在應對上述這些挑戰和限制時，臺灣可以採取一些策略和措施如下。首先，臺灣可以透過建立和維護多元化的語料庫來增加語言數據的多樣性和代表性，這可以幫助減少數據偏見和不完整性（Baker, 2006）。第二，臺灣可以透過引進和培養專業的語言分析人員來提高分析的技術水準和專業能力，這可以幫助提高分析的準確性和有效性、信度與效度（Gabrielatos & Baker, 2008）。第三，臺灣可以透過投資和升級計算資源和技術設備來提高分析的效率和時效性，這可以幫助應對計算資源和處理速度的限制（Wodak & Meyer, 2009）。第四，臺灣可以透過跨文化和跨語言的合作和交流來增進對不同語言和文化的理解和尊重，這可以幫助應對語境和文化差異的挑戰

（Woolley & Howard, 2016）。最後，筆者建議臺灣政府與企業機構也需要密切聯手關切留意中共在新興的社交媒體（抖音、小紅書）、網絡平台、和聯網型線上遊戲等其他傳播渠道實現其多模態認知滲透作戰的戰略目標。

肆、資安語言學的新對策：結合社會學、文化傳播的工具盒方法

社會語言學（Sociolinguistics）研究是一種分析語言在社會和文化背景中使用的方法，可以用來識別和分析中共宣傳材料中的社會和文化語境。透過語用學（pragmatics）分析文本中的語言使用和話語實踐，可以揭示中共在其宣傳中所反映的社會和文化價值觀（Eckert & Rickford, 2001）。此外，社會語言學研究還可以用來識別和分析中共宣傳料中的話語權力和話語霸權，從而更好地理解其宣傳的社會和政治影響（Fairclough, 2013）。

而社會語言學（Sociolinguistics）和語言社會學（Sociology of Language）是研究語言與社會之間相互作用的學科。在應對中共認知作戰中，社會語言學和語言社會學可以用來分析中共宣傳材料中的語言如何與特定的社會、文化和政治背景相互作用。透過分析這些材料中的語言使用如何反映和影響社會結構和關係，可以揭示中共宣傳的社會和文化策略（Gabrielatos & Baker, 2008）。此外，社會語言學和語言社會學還可以用來分析中共宣傳如何利用語言來構建和維護特定的社會身份和群體認同（Charteris-Black, 2004）。在應對中共認知作戰時，臺灣可以利用社會語言學和語言社會學來發展有效的反宣傳策略。透過分析中共宣傳中的語言如何與特定的社會、文化和政治背景相互作用，臺灣可以更好地理解其宣傳的策略和目的，透過分析中共宣傳如何利用語言策略與修辭技巧來構建和維護特定的社會身份和群體認同（Partington, 2014a; 2014b），並考量其在不同社會和文化背景下的複雜性和多樣性（Blommaert, 2010），揭露中共宣傳材料中的語言操縱、誤導性和虛假偏見（Wodak & Meyer, 2009），結合前一節大數據語料庫的分析方式，制定針對性的效果顯著反駁和反擊策略（Biber &

Conrad, 2009），從而更好地保護公眾輿論避免受到中共認知滲透作戰的操縱。

更進一步的，社會語言學和語言社會學的應用範圍在應對中共認知作戰方面不僅限於分析和反駁中共的宣傳，還包括了解和預測中共可能採取的語言策略，這可以幫助臺灣預測中共可能採用的新的宣傳策略和語言技巧，從而提前準備和制定有效的應對措施（Fairclough, 2013）。例如，透過分析中共過去的宣傳材料和語言使用模式，社會語言學和語言社會學可以幫助預測中共可能採用的新的語言策略和宣傳主題（Eckert & Rickford, 2001）。此外，社會語言學和語言社會學還可以用來分析中共宣傳對不同社會群體的影響和反應。透過分析不同社會群體對中共宣傳的接受度和反應，可以更好地了解中共宣傳的社會和文化影響，並制定針對性的反宣傳策略（Gabrielatos & Baker, 2008）。例如，臺灣可以透過社會學分析不同社會族群（年齡、性別、工作、地區、籍貫）對中共宣傳的反應，來制定更加精準和有效的反心戰與反滲透策略（Charteris-Black, 2004）；並運用語言社會學的理論來理解和掌握台灣社會中的語言多樣性，研究不同語言使用的異同現象，以及研究臺灣不同語言社群（如閩南語和客家語使用者）的語言態度和身份認同差異的影響（Blommaert, 2010），並利用這些語言態度與身份認同的調查結果，來設計針對性的反認知領域作戰策略，我方可在臺灣不同文化語言族群上，制定客製化的反心戰策略調整（Giles, Coupland & Coupland, 1991）。

同時，在探討社會語言學和語言社會學在應對中共認知作戰中的應用時，我們可以注意到跨學科所提供的一種獨特視角，可被用於分析和解構中共宣傳中的語言和話語結構。這種分析不僅揭示了宣傳材料的表面含義，還深入挖掘了其背後的社會結構、文化背景、意識型態、心理動機（Widdowson, 2004）、戰略目標（Van Dijk, 2008; 2017）。這些分析可以揭示中共如何透過特定的語言風格和話語範疇來進行認知作戰，並塑造其宣傳的說服力和權威性（Hyland, 2005）；設法在政治意識形態的傳播中，透過改變群體的認知過程，來達到改變社會互動的作用（Gumperz & Hymes,

1972）。例如：中共常會使用正式和權威的語言風格來增強其宣傳的可信度和影響力，企圖將「台海問題」化約成其「內政問題」。

具體來說，社會語言學和語言社會學可以結合當前的認知語言學用來分析中共宣傳中的隱喻和比喻使用當中的語言風格和話語範疇（Lakoff & Johnson, 1980），這些隱喻和比喻尤其是近年中共在習近平領導下強調的「中華民族偉大復興」的集體文化認同背景下，往往被用來塑造特定的社會現實和群體認同，我方可以透過揭示上述的方式解構中共的滲透宣傳。在應對中共認知作戰的過程中，這種取徑還可以用來分析中共宣傳中的在國際上的話語權力和話語霸權（Foucault, 1972; Van Dijk, 2008），如何對國際、對臺、對內進行操縱控制公眾輿論，尤其是解構中共在金磚國家與聯合國上的話語霸權，臺灣更可以透過民主同盟與邦交國家的協助更好地抵制中共的宣傳策略。

進一步地，運用社會語言學和語言社會學在分析中共宣傳時，我方還可以關注語言在「情感上的認知滲透」層面。語言社會學可以揭示中共宣傳如何利用語言與敘事手法來激發特定的情感反應態度和引發被限制的認知框架（Fairclough, 2013），從而影響個人乃至於公眾的集體態度和集體行為（Koller, 2008）。例如，中共可能會使用情感化的語言和修辭來激發民族主義情感，加強其國內對台進行武力統一的民族主義，從而增強其宣傳的吸引力和說服力，達到對內增兵的效益。此外，社會語言學和語言社會學還可以用來分析中共宣傳中的敘事結構和故事情節。這些分析可以揭示中共如何透過敘事和故事來塑造特定的歷史觀和世界觀（Baker, 2006），例如，中共會透過宣傳特定的歷史事件和人物關聯（孫中山→毛澤東→習近平）塑造其正統法理位階，來強調習近平領銜下共產黨統治的政治合法性和歷史正當性。雖然這種語言學分析仍很可能無法完全揭漏中共特定宣傳材料的背後是由何人或哪個統戰單位所謀劃的，但卻可以大幅增強我方的快速反應和應對中共突發宣傳時的實用性（Stubbs, 1996）。

不同的文化和語言背景可能會導致對同一宣傳材料的不同解讀和理解，這亦可以是臺灣避免被認知作戰滲透的優勢。例如，對於不熟悉台灣文化和語言的中共宣傳作戰者來說，敵方會難以準確理解和分析台灣人民主流的意識形態與特定用詞，導致做出容易被我方識破的宣傳材料（Cameron, 2001），且中共的認知滲透作戰還必須面臨著道德和倫理的嚴正譴責，尤其是涉及對個人和群體的隱私權和基本權利的侵犯，其必須對中國人民敘事偏見來進行操弄以灌輸其難以被理性大眾所接受的政治立場與意識，即便是「牆內民眾」近年來亦有許多反彈，這也給予我方透過香港與中國內部的維權人士進行「還權於民」的民主思想傳播與宣揚，瓦解中共自欺欺人的謊言與對內對外的認知滲透作戰。

伍、結論：資安語言學作為因應認知滲透作戰的新型對策建言

本文建議，在應對中共認知作戰時，社會語言學、語料庫語體判別、大數據語言分析、電腦統計語言學等對策相結合，並注意分析的客觀性和公正性，並在臺灣民主法治基礎下展現對個人和群體權利的尊重。具體來說，筆者建議了我們在面對中共認知作戰的挑戰時，可以結合上述語言學的方法，發展出一套新型態的資安語言學對策。這套對策不僅涵蓋了對中共統戰認知滲透作戰宣傳材料的深入分析，還包括了一系列的實際應用和策略，以確保有效地應對和抵制中共的認知作戰。

首先，建立一個多層次的宏觀與微觀語言分析框架是至關重要的。這個框架應該包括微觀層面的語言特徵分析，如詞彙選擇、語法結構和語用特徵（Biber & Conrad, 2009），以及宏觀層面的話語分析，如話語權力、話語霸權和意識形態（Fairclough, 2013）。此外，這個框架還應該包括對宣傳材料中情感和認知策略的分析（Koller, 2008），以及對敘事結構和故事情節的分析（Baker, 2006）。

第二，發展一套快速反應機制是應對突發宣傳攻勢的關鍵。這包括透過公私合作夥伴關係建立一個專門的語言分析團隊，迅速收集和分析新出現的宣傳材料（Stubbs, 1996）。此外，利用先進的語料庫技術和自然語言處理

（NLP）工具可以加快分析過程，提高反應的時效性和準確性（Biber & Conrad, 2009）。

第三，進行文化和語言背景教育也是不可忽視的一環。由於文化和語言差異可能導致對中共宣傳材料的誤解（Blommaert, 2010），因此進行相關的文化和語言背景教育是必要的。這可以幫助我們更準確地理解和分析中共宣傳中的隱喻和比喻。

第四，跨領域多學科的合作機制是關鍵且必要的。社會語言學和語言社會學的分析需要與心理學、政治學和媒體研究等其他學科相結合，以獲得更全面和深入的理解（Van Dijk, 1998）。這種跨學科的合作可以提高分析的全面性和深度，從而提高對策的有效性。第五，在臺灣民主法治的社會下，重視道德和倫理考量必定是不可或缺的。在進行語言分析和制定對策時，仍然必須審慎考慮到公民個人隱私和言論自由的保護（Cameron, 2001），研究者也應避免將分析純粹用於選舉意識形態，保持分析的客觀性和公正性，心繫國人國防安全是至關重要的。

綜上所述，資安語言學對策的實施需要一個多層次、快速反應、文化敏感、跨學科合作和道德倫理考量的綜合框架。本文期許，透過這樣的框架進行發展，我方可以更有效地應對和抵制中共的認知作戰，亦可結合臺灣事實查核中心（Taiwan FactCheck Center）等多樣化平台的合作管道，來保護公眾輿論免受到境內外敵對勢力的認知操縱和多模態滲透作戰影響，並容或在未來作為我方因應認知滲透作戰的新堡壘。

參考文獻

中文部分（含簡體中文）

尤正才. (2010) 我國現行法規中之 [國家安全] 概念分析. *國家發展研究*, 2010, 9.2: 27-79.

河凡植. (2008). 和平繁榮政策與韓中關係的發展. *問題與研究*, *47*(1), 127-149.

松田康博. (2021).中國對台政策及台灣總統選舉 1996- 2000 年。歐亞研究, 第十六期.

金慧蘭. (2006). 現代漢語新詞研究. 1-302.

李森永. (2006). 中共建構重點新聞網站的政策目標及其實際運作分析. *展望與探索月刊*, *4*(1), 41-55.

邢欣. (2004). 语言的社会变体及其分类. *《信阳师范学院学报 (哲学社会科学版)》*, *24*(1), 71-75.

林疋愔. (2021). 中共認知戰操作策略與我國因應作為. *國防雜誌*, *36*(1), 1-22.

沈中愷. (2009). 從網路科技探討國軍新聞媒體的整合與發展. *國防雜誌*, *24*(1), 103-118.

沈伯洋. (2021).中國認知領域作戰模型初探: 以 2020 臺灣選舉為例. *遠景基金會季刊*, *22*(1), 1-65.

张焱&赵丹. (2018).语言变异综述, *現代漢語學*, *6(2)*, 253-258.

陳津萍, & 徐名敬. (2021). 中共 [心理戰] 與 [認知域作戰] 發展之比較研究. *復興崗學報*, (118), 119-148.

陳麗君. (2012). 台, 華語語言接觸下的 [有] 字句. *台灣學誌*, (5), 1-26.

陈立. (2021). “90 后”“00 后” 青年群体特征的再审视——以湖北省为例. *中国青年社会科学*.

洪惟仁. (2015). 語言分布發展的擴散論與類型論. *Language and Linguistics*, *16*(5), 639-661.

袁靖华, & 童威楠. (2022). “影子种族主义”: 国际新闻中的话语霸权再生产. *未来传播*.

謝游麟. (2019). 共軍對於人工智慧 (AI) 之發展與政策建議. *陸軍學術雙月刊*, *55*(568), 61-80.

翟文中, & 吳自立. (2022). 論 [人工智慧](AI) 在軍事領域的運用. *海軍學術雙月刊*, *56*(4), 6-19.

鄭國漢, & 華靜泊. (2020). 以國家安全為理由以保護本土產業的論點. *香港嶺南大學經濟學系*.

譚昱涵, & 林政榮. (2023). 中共 [認知作戰] 對我國之影響-以 2022 年 [圍臺軍演] 為例. *海軍學術雙月刊*, *57*(3), 121-136.

英文部分

Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of economic perspectives*, *31*(2), 211-236.

Baker, P. (2006). Using Corpora in Discourse Analysis. *Continuum*.

Baker, P. (2010). Sociolinguistics and Corpus Linguistics. *Edinburgh University Press*.

Baker, R. S., & Siemens, G. (2014). Educational data mining and learning analytics. *The Wiley handbook of cognition and assessment: Frameworks, methodologies, and applications*, 379-396.

Baughman, J. (2023). How China Wins the Cognitive Domain. *China Aerospace Studies Institute*,1-6.

Biber, D., & Conrad, S. (2009). Register, Genre, and Style. *Cambridge University Press*.

Bishop, M. (2019). Computer Security: Art and Science (ed.). Addison-Wesley.

Blommaert, J. (2010). *The sociolinguistics of globalization*. Cambridge University Press.

Brenner, S. W. (2017). Cybercrime and the law: Challenges, issues, and outcomes. *Northeastern University Press*.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. arXiv preprint arXiv:1802.07228.

Cameron, D. (2001). Working with spoken discourse. *Sage*.

Cardenal, J. P., Kucharczyk, J., Mesežnikov, G., & Pleschová, G. (2017). Sharp power: Rising authoritarian influence. International Forum for Democratic Studies.

Chan, S. H., Guo, R., & Huang, X. (2023). Media Discourses and China's Social Mobilization at the Early Crisis Stage of the COVID-19 Pandemic. In *Comparative Studies on Pandemic Control Policies and the Resilience of Society* (pp. 287-307). Singapore: Springer Nature Singapore.

Chen, L. C., & Chang, K. H. (2021). A novel corpus- based computing method for handling critical word- ranking issues: An example of COVID- 19 research articles. *International Journal of Intelligent Systems*, *36*(7), 3190-3216.

Chilton, P. (2004). *Analysing political discourse: Theory and practice*. Routledge.

Charteris-Black, J. (2004). Critical Approaches to Metaphor. In *Corpus Approaches to Critical Metaphor Analysis* (pp. 25-43). London: Palgrave Macmillan UK.

Chesney, R., & Citron, D. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*, 107(6), 1753-1819.

Conroy, N. J., Rubin, V. L., & Chen, Y. (2015). Automatic deception detection: Methods for finding fake news. Proceedings of the Association for Information Science and Technology, 52(1), 1-4.

Eckert, P., & Rickford, J. R. (2001). *Style and Sociolinguistic Variation*. Cambridge University Press.

Fairclough, N. (2013). *Critical discourse analysis: The critical study of language*. Routledge.

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. International Security, 44(1), 42-79.

Feldman, P., Dant, A., & Massey, A. (2019). Integrating artificial intelligence into weapon systems. *arXiv preprint arXiv:1905.03899*.

Fisher, S., Klein, G. R., & Codjo, J. (2022). Focusdata: Foreign policy through language and sentiment. *Foreign Policy Analysis, 18*(2), orac002.

Floridi, L., & Taddeo, M. (2016). What is data ethics?. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *374*(2083), 20160360.

Foucault, M. (1972). The archaeology of knowledge. *Pantheon Books*.

Fowler, R. (1991). *Language in the News: Discourse and Ideology in the Press*. Routledge.

Gabrielatos, C., & Baker, P. (2008). Fleeing, sneaking, flooding: A corpus analysis of discursive constructions of refugees and asylum seekers in the UK press, 1996–2005. Journal of English Linguistics, 36(1), 5-38.

Giles, H., Coupland, J., & Coupland, N. (Eds.). (1991). *Contexts of accommodation: Developments in applied sociolinguistics*(Vol. 10). Cambridge University Press.

Goodfellow, I., Bengio, Y., Courville, A., & Bengio, Y. (2016). Deep learning (Vol. 1, No. 2). *Cambridge: MIT press*.

Goodfellow, I., Bengio, Y., & Courville, A. (2018). Deep learning for cybersecurity. In Deep Learning (pp. 751-774). *MIT Press*.

Gordon, L. A., & Loeb, M. P. (2016). Managing cybersecurity resources: A cost-benefit analysis. McGraw-Hill Education.

Gumperz, J. J., & Hymes, D. (1972). *Directions in sociolinguistics: The ethnography of communication*. Holt, Rinehart and Winston.

Hongzhi Qi, et al., Zhao, Q., Song, C., Zhai, W., Luo, D., Liu, S., ... & Fu, G. (2023). Evaluating the Efficacy of Supervised Learning vs Large Language Models for Identifying Cognitive Distortions and Suicidal Risks in Chinese Social Media. *arXiv preprint arXiv:2309.03564*.

Hu, J., et al. (2023). International cooperation in cybersecurity: Challenges and opportunities. Journal of Cyber Policy, 8(2), 210-228.

Hyland, K. (2005). Metadiscourse: Exploring interaction in writing. *Continuum*.

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.

King, G., Pan, J., & Roberts, M. E. (2017). How the Chinese government fabricates social media posts for strategic distraction, not engaged argument. *American political science review*, *111*(3), 484-501.

Koller, V. (2008). 'Not just a colour': Pink as a gender and sexuality marker in visual communication. *Visual Communication*, 7(4), 395-423.

Kruhlov, V., Latynin, M., Horban, A., & Petrov, A. (2019). Public-Private Partnership in Cybersecurity. In CybHyg (pp. 619-628).

Lakoff, G., & Johnson, M. (1980). Metaphors We Live By. *University of Chicago Press*.

Leech, G., & Short, M. (2007). Style in Fiction: A Linguistic Introduction to English Fictional Prose. *Pearson Education*.

Letham, B., Rudin, C., McCormick, T. H., & Madigan, D. (2015). Interpretable classifiers using rules and bayesian analysis: Building a better stroke prediction model.

Lewandowsky, S., Ecker, U. K., & Cook, J. (2017). Beyond misinformation: Understanding and coping with the "post-truth" era. *Journal of applied research in memory and cognition*, *6*(4), 353-369.

Lewis, T. G. (2019). *Critical infrastructure protection in homeland security: Defending a networked nation*. John Wiley & Sons.

Li, Z., Zhao, R., & Lou, B. (2023). Corpus-based critical discourse analysis of reporting practices in English news reports on public health event in China and United States. *Frontiers in Psychology*, *14*, 1137382.

López, J. A. D., & Madhyastha, P. (2021). A focused analysis of twitter-based disinformation from foreign influence operations. In *Proceedings of the 1st International Workshop on Knowledge Graphs for Online Discourse Analysis (KnOD 2021) co-located with the 30th The Web Conference (WWW 2021)* (Vol. 2877). CEUR Workshop Proceedings.

McEnery, T., & Hardie, A. (2011). *Corpus linguistics: Method, theory and practice*. Cambridge University Press.

McKernan, M., Drezner, J. A., Arena, M. V., Wong, J. P., Shokh, Y., Moore, N. Y., ... & Lewis, A. (2023). *Using metrics to understand the performance of the adaptive acquisition framework*. Acquisition Research Program.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2), 1-21.

Nye, J. S. (2011). The Future of Power. New York, *NY: Public Affairs*.

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security*, 41(3), 44-71.

Partington, A. (2014a). *The linguistics of laughter: A corpus-assisted study of laughter-talk.* London: Routledge.

Partington, A. (2014b). *The Linguistics of Political Argument: The Spin-Doctor and the Wolf-Pack at the White House.* London: Routledge.

Pfleeger, C. P., & Pfleeger, S. L. (2012). Security in Computing (4th ed.). Upper Saddle River, NJ: Prentice Hall.

Ross, A. S., & Rivers, D. J. (2018). Discursive deflection: Accusation of "fake news" and the spread of mis-and disinformation in the tweets of President Trump. *Social Media+ Society*, *4*(2), 2056305118776010.

Russell, S., & Norvig, P. (2016). Artificial Intelligence: A Modern Approach. Pearson Education Limited.

Semino, E., & Short, M. (2004). *Corpus stylistics: Speech, writing and thought presentation in a corpus of English writing* (Vol. 5). Routledge.

Shuyo, N. (2010). Language detection library for java.

Sinclair, J. (2004). *Trust the text: Language, corpus and discourse*. Routledge.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, 34(3), 503-522.

Stubbs, M. (1996). *Text and corpus analysis: Computer-assisted studies of language and culture* (p. 158). Oxford: Blackwell.

Taylor, L., Floridi, L., & Van der Sloot, B. (2017). *Group privacy: New Challenges of Data Technologies*. Springer.

Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Morales, A., & Ortega-Garcia, J. (2020). Deepfakes and beyond: A survey of face manipulation and fake detection. *Information Fusion*, *64*, 131-148.

Van Dijk, T. A. (1998). Ideology: A multidisciplinary approach. *Sage*.

Van Dijk, T. A. (2008). Discourse and context: A sociocognitive approach. *Cambridge University Press*.

Van Dijk, T. A. (2014). *Discourse and knowledge: A sociocognitive approach*. Cambridge University Press.

Van Dijk, T. A. (2017). *Discourse and Power*. Bloomsbury Publishing.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.

Wang, F., & Rudin, C. (2015). Falling rule lists. In *Artificial intelligence and statistics* (pp. 1013-1022). PMLR.

Widdowson, H. G. (2004). *Text, context, pretext: Critical issues in discourse analysis*. Blackwell.

Wirkuttis, N., & Klein, H. (2017). Artificial intelligence in cybersecurity. *Cyber, Intelligence, and Security*, *1*(1), 103-119.

Wodak, R., & Meyer, M. (2009). Critical discourse analysis: History, agenda, theory and methodology. *Methods of critical discourse analysis*, *2*, 1-33.

Woolley, S. C., & Howard, P. N. (Eds.). (2016). Automation, algorithms, and politics| political communication, computational propaganda, and autonomous agents—Introduction. *International Journal of Communication*, *10*, 9.

網路新聞專欄與報導

李柏鋒(2020)，AIT 也站台：IORG 用科學方式，找出中國對台資訊戰證據，Inside，取自 https://www.inside.com.tw/article/21268-iorg-china-information-cognitive-war-taiwan-ait。擷取日期：2023 年 12 月 4 日。

信傳媒(2020)，又是大外宣?「各國疫情失控」在推特大規模瘋傳當神力女超人也轉傳中國官媒影片 ，取自 https://reurl.cc/r6yWAy (縮網址)。擷取日期：2023 年 12 月 4 日。

ABC(2022)，分析：娱乐明星如何成为共产党宣传“一个中国”的新工具？取自 https://www.abc.net.au/chinese/2022-09-30/china-celebrity-ccp-propoganda-weibo-repost-nationalist-taiwan/101486770，擷取日期：2023 年 12 月 4 日。

網際網路平台連結

公視新聞網。兩岸/境外勢力介選，https://news.pts.org.tw/article/672234，《多縣市里長赴中遭約談 最高檢 5 認定標準》，擷取日期：2023 年 12 月 21 日。

Using Linguistics Corpus Data Analysis to Combat PRC's Cognitive Infiltration

Abstract

In light of Taiwan's extensive exposure to the Chinese Communist Party's "cognitive domain infiltration warfare," this paper proposes new response mechanisms and strategies for cybersecurity and national defense. The focus is primarily on assessing the CCP's cognitive infiltration tactics to develop policy recommendations in cybersecurity linguistics. These recommendations are intended to serve as a reference for future national defense and information security policies. Within the constraints of limited resources, this study attempts to provide an integrated analysis method combining qualitative and quantitative tools. This method involves text mining in cybersecurity linguistics, focusing on "textual content" and incorporating discourse deconstruction. The aim is to enhance the success rate in identifying and defining contentious information in cognitive warfare, thereby offering policy suggestions.

Keywords: Cognitive Infiltration, Big Data Corpus, Cybersecurity Linguistics, Text Mining Analysis, Narrative Language Deconstruction.