

2024年美國大選的 虛假訊息操作

◎ 羅世宏／中正大學傳播系教授、台灣事實查核中心董事長

2024年美國總統選舉被視為資訊戰的高峰，讓我們看到數位時代如何改變民主選舉的本質。在社交媒體演算法的不當設計、人工智慧（AI）驅動的假訊息，以及美國內外影響力操控的夾擊下，虛假訊息不僅影響選民對於正確資訊的接收與判斷，亦可能更動搖了選民對選舉制度的信任。

在這次選舉中，川普（Donald Trump）和賀錦麗（Kamala Harris）皆成為虛假訊息的攻擊目標。正如德國之聲（DW）報導指出¹，針對賀錦麗的攻擊包括毫無根據的謠言，例如她曾從事性交易或在車禍中撞死小孩。而針對川普的虛假訊息則例如他在電視節目中使用尿失禁護墊的荒謬謠言等。

虛假訊息的擴散與 社交媒體的影響力

社交媒體在虛假訊息擴散中扮演著關鍵角色。以X平台（前Twitter）為例，其演算法和高知名度的用戶加速了虛假訊息的傳播。據英國廣播公司（BBC）的報導指出²，在X平台上有諸多關於賀錦麗的虛假資訊，特別是關於她具有「共產主義」傾向的謠言。以及流傳一張AI生成的賀錦麗身穿共產黨軍服的圖片，並宣稱她「從一開始就想當共產主義獨裁者」。該偽造圖

1 <https://www.dw.com/en/fact-check-what-role-did-disinformation-play-in-the-us-election/a-70729575>

2 https://www.bbc.com/news/articles/cn8jg11ynj7o?conesso_link_tag=5f7972354&utm_campaign=Disinformation%20Watch%2018%20Sep%20-%201%20Oct%202024%20-%20SOCIAL&utm_medium=email&utm_source=Conesso。



台灣事實查核中心
Taiwan FactCheck Center



台灣事實查核中心官網



片迅速在拉丁美洲流亡者群體之間傳播，引發在有反共經歷的古巴和委內瑞拉移民社區，對美國變成專制國家的恐懼。美國選舉中常見的策略之一，是透過虛假訊息來挑起特定群體的情緒，而社交媒體平台擔負著巨大的責任，尤其是演算法的選擇性推送，使一些虛假訊息的影響遠遠超過正確資訊³。

外國勢力干預： 俄羅斯的假訊息操作

俄羅斯長期以來被認為在干預美國選舉，這次也不例外。根據微軟威脅分析中心（Microsoft Threat Analysis Centre）的報告，俄羅斯的網路特工組織 Storm-1516 和 Storm-1679 針對賀錦麗及其副手明尼蘇達州州長沃爾茲（Tim Walz），製作和散布了許多虛假影像，試圖詆毀賀錦麗的形象⁴，

企圖製造混亂。事實上，俄羅斯的影響操作並非針對某個候選人，而是在削弱美國民眾社會的凝聚力和對民主制度的信任。從某種程度上說，這場選舉成為俄羅斯實現其長期戰略目標的舞台。

俄羅斯的影響力操控策略也包括利用虛假新聞網站和社交媒體帳號，並透過這些平台來持續擴散對美國民主的質疑。例如，美聯社的調查報導指出⁵，俄羅斯在選舉前夕製作的虛假影像宣稱喬治亞州發生選民舞弊事件，該影像迅速在網路上傳播並引發熱議，但很快就被美國聯邦執法

3 <https://www.dw.com/en/fact-check-what-role-did-disinformation-play-in-the-us-election/a-70729575>

4 https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/MTAC-Election-Report-4.pdf?conesso_link_tag=972354a39&utm_campaign=Disinformation%20Watch%2018%20Sep%20-%20201%20Oct%202024%20-%20SOCIAL&utm_medium=email&utm_source=Conesso

5 <https://apnews.com/article/election-2024-security-voting-cybersecurity-misinformation-5fc1f17a888ac25855a9feda62d9be50a>

機構識破並公開闢謠。然而，即使謠言被揭穿，它所產生的負面影響仍有可能已不可逆，因為一旦虛假訊息被選民接受，會進一步增強他們對整個選舉過程的懷疑。

AI技術的應用與 未來挑戰

AI工具不僅能夠快速生成具有誤導性或操控性的內容，還能利用社群媒體的力量迅速傳播，對選民的心理與投票行為產生直接影響。根據2024年兩份關鍵報告——OpenAI的《影響力與網路作戰更新報告》（Influence and Cyber Operations: An Update）與數位仇恨反制中心（The Center for Countering Digital Hate, CCDH）的《AI選舉虛假訊息》（AI Election Misinformation）——AI技術在選舉期間被廣泛濫用，成為隱蔽影響力作戰的利器。

這些報告揭示AI驅動的虛假資訊活動如何影響選舉，特別是針對美國、歐洲及非洲等地的選舉過程。CCDH的報告強調了AI圖像生成工具在選舉假資訊中的角色。根據報告，AI圖像生成器在41%的測試中成功生成了與選舉有關的誤導性圖像，特別是關於選舉舞弊與投票恐嚇的圖像。這些圖像中，一些展示了被丟棄在垃圾桶中的選票，另一些則顯示選票機被破壞或暴



AI技術在選舉期間被廣泛濫用，成為隱蔽影響力作戰的利器。

Data source: https://cdn.openai.com/threat-intelligence-reports/influence-and-cyber-operations-an-update_October-2024.pdf
<https://counterhate.com/>

力場面，這類圖像對選民心理的影響不容小覷。

AI在2024年的選舉中被廣泛應用，並創造大量深度偽造內容。德國之聲的報導指出，AI生成的拜登音頻和假造的賀錦麗影像成為選舉操控的工具。這些技術雖未大規模影響選舉結果，但它們對資訊可信度的侵蝕令人相當擔憂。

由於AI技術的進步，未來選舉面臨的挑戰會更加複雜。美國政府與各大科技公司亟需制定政策來應對這種新型威脅。正如德國外交關係協會的研究員卡蒂亞·穆諾茲（Katja Munoz）所言，虛假訊息的長期目標是削弱民眾對新聞媒體與民主制度的信任，讓許多人質疑主流新聞的價值。這也意味著，即使事實最終勝出，民主制度的脆弱性已經顯露無遺。

■ 美國民主的挑戰

美國選舉制度面臨的這些挑戰，絕不會隨著選戰結束而結束。在這次選舉期間，美國國土安全部、聯邦調查局等機構迅速回應俄羅斯等國家的介選干預行為，但這些措施是否能持久有效，尚待進一步觀察。儘管美國政府在這次選舉中展現打擊虛假訊息的能力，但這種跨國虛假資訊的介選干預已成為常態，而且正在逐年升級。

美國這場選舉的經驗提醒我們，社會對虛假訊息的耐受性正在下降，但虛假訊息的破壞性卻在加劇。面對如此龐大的虛假資訊挑戰，政府、企業、媒體和公民都必須共同承擔起保護民主的責任。正如本次選舉所顯示的，當人們的信仰基石被持續削弱，虛假訊息的影響便不僅是誤導，而是對整個社會信任與民主體制的傷害。●



淺談公開來源情資技術 有效辨識爭議訊息

◎ 藍啟源／法務部調查局認知戰研究中心



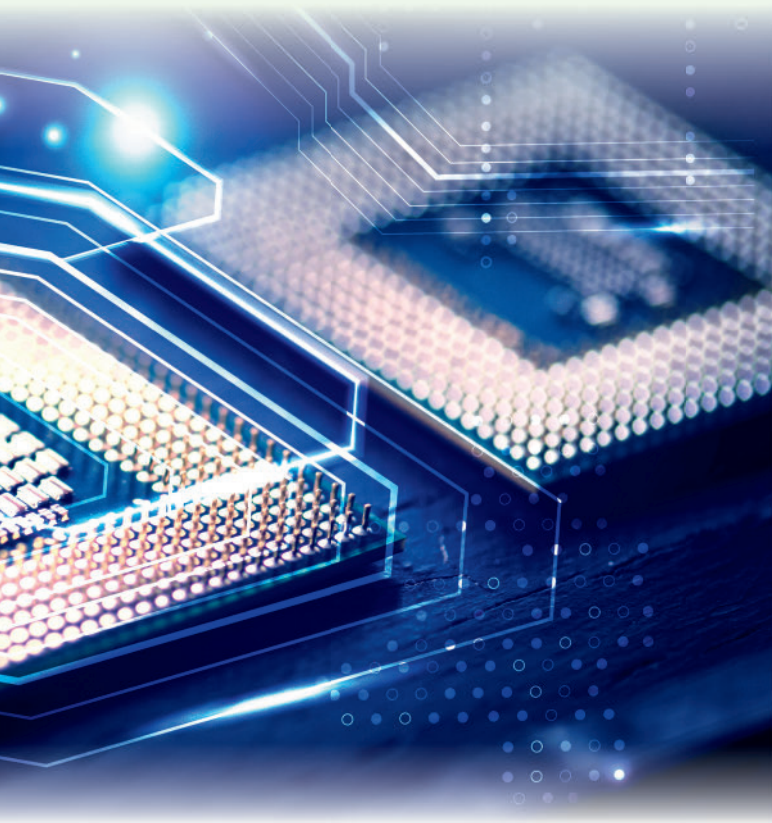
在資訊爆炸的時代，公開來源情資技術（Open Source Intelligence Technology，下稱：OSINT）不僅在日常生活中扮演重要角色，更在國家安全和國際衝突中發揮關鍵作用，換言之，OSINT正悄然改變著人們的生活。

什麼是 OSINT

在情報學領域，OSINT被定義為「透過對公開資訊分析後所得情報或從半公開資料或消息中獲取情報」¹。美國國家情報總監（Director of National Intelligence，

1 李修安，111年9月30日，《情報學理論與實務》，一品出版，第61頁。

2 Director of National Intelligence，113年3月8日，《The IC OSINT Strategy 2024-2026》。網址：<https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2024/3785-the-ic-osint-strategy-2024-2026>



DNI) 則定義為「專門從公開或商業可用資訊中獲取的情報，目的在解決特定的情報事項或要求」²。

拋開生硬的用詞，OSINT技術就是指通過公開可得的資料收集和分析情報的技術與方法；包括網際網路、社交媒體、新聞報導、政府公開文件、商業數據等，都可能是這些資料的來源。隨著數位時代來臨，大量資訊在網路儲存且易於獲取和分析，更加重OSINT的重要性。

網際網路時代，個人數位足跡與公開資訊能拼湊出行為模式和事件全貌，但面對巨量資料，OSINT技術的核心在於知道所欲了解的資訊有哪些網路資源，並且如

何查找。與其說OSINT是新技術，不如說它是一種思維方式。關鍵在於熟悉數位時代下取得證據的來源、建構事實的方式，並在正確的方向上尋找答案。

日常生活中 OSINT 的應用

在日常生活中，OSINT的應用無處不在。例如肇事逃逸案件，過去往往難以追查；但現今已可以透過路口監控、商家監視器，甚至社群媒體徵集行車紀錄器影像，迅速找出肇事車輛。

在商業領域，OSINT同樣發揮著重要作用。企業可通過多方面的公開資料，例如檢索公司商業登記資料、登記票據信用交換所的信用紀錄、環保署的汙染紀錄、智慧財產局的商標註冊情況，甚至是上市公司的財務報表及營收情況等，來評估合作夥伴或競爭對手。這些資訊不僅能幫助評估公司的現況，還能預測其未來發展趨勢。



個人數位足跡與公開資訊可以拼湊出一個人的行為模式。
Photo Credit: 達志影像

在一般民事交易，OSINT也扮演著助手角色。例如買房或租房時，民眾可藉查詢建築物第二類謄本，了解房產歷史和所有權變更情況，避免誤向人頭或二房東承租，亦可透過新聞媒體資料查詢建物是否曾發生「非自然死亡案件」。在車輛交易中，則可利用監理系統查詢驗車里程數，降低誤購變造里程車輛的風險。

OSINT在 突發事件中的重要性

在突發事件中，OSINT同樣能發揮關鍵作用。國外已有專業的OSINT人員及組織（如 Trace Labs）³，專門協助調查綁架、失蹤和無名屍等案件。他們通過分析各種公開資料，包括分析失蹤者的社交媒體活動、金流活動、監視器畫面等公開資訊，幫助執法部門追蹤失蹤人口，提供關鍵線索和證據。這些看似零散的資料，經過專業分析後，往往能為案件帶來突破性進展。

在地點未知的大規模衝突事件中⁴，OSINT技術也被用來分析視覺資料。例如，通過影片逐幀慢放可以觀察地景地貌或特殊建物，幫助確定拍攝地點；影像中的影子則可用來推估拍攝時間和緯度。這



OSINT在網路犯罪的應用上也日益廣泛。
Photo Credit: 達志影像

些細節往往被普通人忽視，但對於專業分析人員來說，卻能提供大量有價值的資訊。

OSINT在 案件偵辦中的應用

OSINT在案件偵辦中的應用也日益廣泛。最近一則引起廣泛關注的案例，是國人林睿庠在暗網化名法老（Pharoah），經營名為「匿名市場（Incognito Market）」的販毒平台，最終遭美國逮捕⁵；起訴狀中當地檢警以諸多公開情資提高證據證明力⁶，例如林男透過Linkin等社群帳號公開

3 Trace Labs, 《what we do》。網址：<https://www.tracelabs.org/about/what-we-do>

4 何蕙安，111年3月9日，《【網路上的烏俄戰爭】「開源情報」社群大顯身手鍵盤調查改變戰事資訊生態》。網址：<https://tfc-taiwan.org.tw/articles/7056>。黃哲斌，111年3月28日，《眾包戰爭時代—從抖音到匿名者》。網址：<https://www.wealth.com.tw/articles/d58926d0-e502-4495-a3c8-4a1673755701>

5 商業周刊，113年6月1日，《〈資安快報〉23歲台大菁英，為何淪32億販毒平台首腦、恐被終身監禁？》。網址：<https://infosecu.technews.tw/2024/06/01/he-trained-cops-to-fight-crypto-crime/>

6 Southern District of New York, 113年5月20日，《"Incognito Market" Owner Arrested For Operating One Of The Largest Illegal Narcotics Marketplaces On The Internet》。網址：<https://www.justice.gov/usao-sdny/pr/incognito-market-owner-arrested-operating-one-largest-illegal-narcotics-marketplaces>



透過無人機攝影，亦是OSINT資訊的重要來源。
Photo Credit: 達志影像

貼文，佐證其熟稔區塊鏈、虛擬貨幣及暗網技術；透過軟體代碼服務平台GitHub帳號佐證其高度熟悉程式撰寫等。這個案例突顯OSINT在跨國犯罪調查中的重要性，縱使其透過暗網及虛擬貨幣製造大量斷點，也可能在公開資訊中尋得蛛絲馬跡。

OSINT在 戰爭中的應用

戰爭中，OSINT的價值更為顯著。自敘利亞內戰以來，許多獨立記者及研究者利用OSINT技術，揭露戰爭罪行和反

人類罪行。如烏克蘭東部親俄叛軍擊落馬來西亞航空17號客機事件中，縱使叛軍竭力否認，但隨著各調查團隊調查揭露，事實逐漸浮現。敘利亞使用化學武器砲擊反政府軍占領區事件，亦是在眾多研究者共同協力下，終而拼湊出不能否認的真相。

在俄烏戰爭中，OSINT的作用更加突顯。鄰近接戰區的民眾經常將影像上傳至社群平台，這些影像成為俄羅斯、烏克蘭官方及各研究機構分析戰事進程的重要線索。烏克蘭官方甚至研製DELTA⁷和DIIA⁸系統，將OSINT納入軍事指揮管制鏈，提升作戰效率，不僅提升情報分析能力，還能將相關資訊即時納入指揮管制鏈，大大增強戰場上的決策支持能力。

美國情報社群如何 看待 OSINT

傳統情報單位著重人員情報，然而數位時代下追蹤數位足跡可獲巨大效益，強化OSINT技巧，並輔以傳統人員情報分析始可全面達成情蒐目標。基此，美國於95年啟動國家公開來源事業計畫（National Open Source Enterprise, NOSE）⁹專注於公開來源資訊蒐集研析。

7 許智翔，111年6月6日，《烏軍活用民間無人機能量強化戰力》。網址：<https://indsr.org.tw/focus?typeid=30&uid=11&pid=362>。

軍傳媒Bryan，112年3月20日，《商用天基系統將能協助北約建立新指管系統》。網址：<https://mmedia.com.tw/商用天基系統將能協助北約建立新指管系統/>

8 穗禾，112年10月26日，《IG 影片如今也是重要軍情！開源情報（OSINT）為何在現代戰爭中不可或缺？》。網址：<https://www.inside.com.tw/article/33163-what-is-osint>。

9 中央社綜合報導，111年3月24日，《俄烏戰爭爆發「推特間諜」順勢崛起》。網址：<https://www.cna.com.tw/news/aopl/202203240268.aspx>

李修安，111年9月30日，《情報學理論與實務》，一品出版，第63頁。



United States Intelligence Community

美國情報體系明確制定OSINT戰略，確立其在提升國家安全和情報的關鍵作用。Photo Credit: The IC OSINT Strategy2024-2026, <https://www.state.gov/open-source-intelligence-strategy/>

美國國家情報總監（DNI）於113年3月公布2024至2026年的公開來源情報戰略¹⁰，更加確立OSINT在提升國家安全和情報的關鍵角色。此外，美國命中央情報局為OSINT秘書單位，亦在各情報單位內設立OSINT單位業管主管。美國國務院轄下情報及研究局（INR）也遵循發布戰略方案措施略以，制定明確OSINT政策和操作程序、投資技術和獲取數據、強化人員培訓、加強國際、跨部門合作及民間參與。

我國OSINT發展的現狀與未來展望

在我國，OSINT發展雖然起步較晚，但卻有高度的發展潛力。我國目前爭議訊息查核工作已有眾多且堅實的民間團隊參與。未來可以持續強化民間協力，推動OSINT工作的發展。同時，政府應積極強化官方OSINT人才培訓，就像現今對無人

機飛手的重視一樣，我們需要培養足夠的OSINT人才來應對潛在的戰事和安全威脅；另應該建置通用研究方法及架構，發展配合韌性骨幹網路的系統，將OSINT納入指揮管制鏈。從承平到戰爭，OSINT不僅能提升戰時應變能力，還能在平時保障社會安全和穩定。

而人工智慧和機器學習的應用，將進一步提升OSINT技術的效率和準確性。例如AI可以輔助分析大量視訊和圖片

資料，迅速找出關鍵線索。大數據技術則能整合來自不同來源的資訊，提供更全面的分析和預測。

結語

隨著技術的不斷發展，OSINT應用範圍從日常生活擴及國家安全，在未來將扮演更加重要的角色。然而，在運用OSINT技術時，必須注意保護個人隱私和遵守相關法規。OSINT能帶來巨大的便利和安全保障，但如果使用不當，也可能侵犯個人隱私。我們需要在利用這項技術的同時，建立相應的規範及框架。

隨著OSINT技術的不斷發展和應用，我們可以預見，它將在未來的社會中扮演愈來愈重要的角色，值得我們持續關注和深入研究。

10 同前揭註2