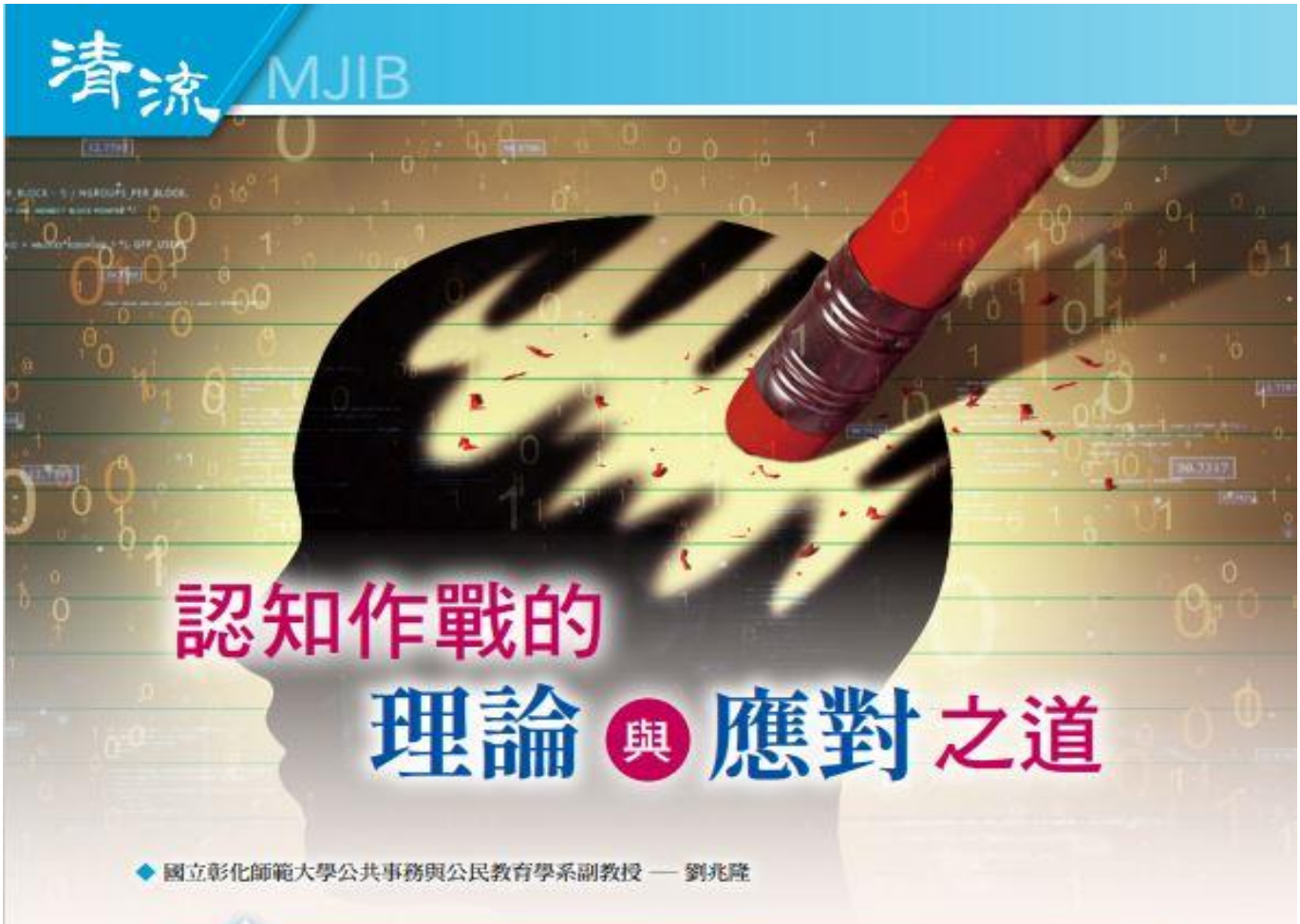
認知作戰的理論與應對之道

/國立彰化師範大學公共事務與公民教育學系副教授－劉兆隆

清流 MJIB



認知作戰的理論與應對之道

◆ 國立彰化師範大學公共事務與公民教育學系副教授 — 劉兆隆

不斷出現的假新聞使行政系統功能受阻，讓人對政府失去信任，甚至引發仇恨與戰爭。

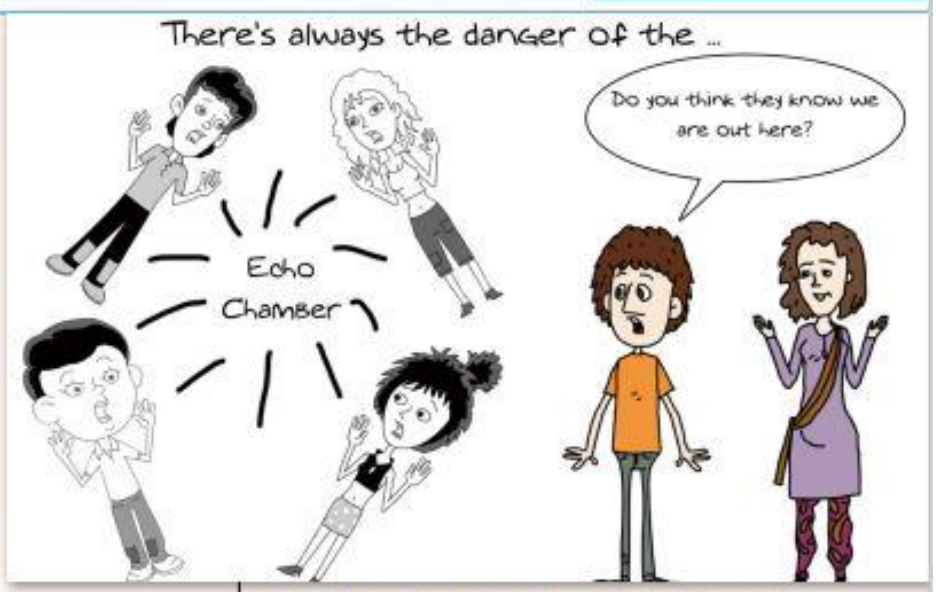
台灣事實查核教育基金會（台灣事實查核中心）於 2022 年 3 月發布針對臺灣社會的第一份《假訊息現象與事實查核成效大調查》，調查結果顯示有超過 9 成的受訪民眾認為，臺灣社會假訊息猖獗並嚴重影響社會。有近 6 成（58%）的受訪民眾認為自己受假訊息的影響不大，卻擔憂別人會上假訊息的當。

假訊息為何會如此大量與快速的激增，除了特定政治勢力的操控外，有更多的是對岸信息農場的大量偽造與惡意投送，這也形成對臺灣的認知作戰核心原因。

假訊息的成因與影響

Bhaskaran 等學者發現，民眾之所以傳播這些假新聞，其中一個原因在於缺乏媒體素養。由於民眾較習慣接觸傳統媒體，當他們使用社群媒體時，並無法分辨真實與虛構。另一原因為迴聲室（echo chamber）的存在以及缺少資訊來源等因

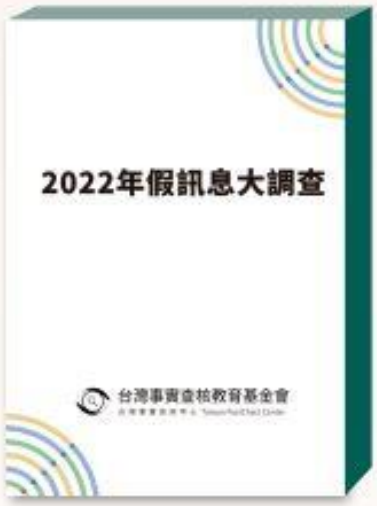
素導致。[1] 社群平臺上的假新聞所進行的認知作戰，在選舉期間更因各種政治策略考量，不但影響選舉，也影響了民主政治。不斷出現的假新聞使政治系統失去功能，更導致疏離感（alienation），並且對所有機構失去信任，甚至導致仇外與戰爭。[2]



迴聲室效應指媒體社群裡，意見相近的聲音重複出現，讓受眾更容易接觸到和自己價值觀相符的資訊，故得到的訊息越來越趨單一化，進而驅使此環境中的大多數人將這些意見認定為事實的全部。（Photo Credit: Kevin Hodgson, https://flic.kr/p/poFw67）

假訊息的類型與傳播方式

美國在2016年大選後，政治欺騙類型的假訊息也最常見，學者Allcott與Gentzkow分析認知作戰的假新聞內容，可分為六個等級：一、非故意的錯誤報導；二、非源自新聞報導的謠言；三、民眾特別相信某事為真的陰謀論；四、被當成事實的諷刺文；五、政治人物製造的錯誤陳述；六、報導有誤導傾向，但事實未必全部為假。輿論在意的也是假新聞的政治意涵。[3] 另一項研究則列出2003至2017年間，有關假新聞的字辭應用，並就真實和欺騙的不同等級歸納六種假新聞類型，包括：新聞諷刺（news satire）、新聞模仿（news parody）、捏造（fabrication）、操控（manipulation）、廣告（advertising）

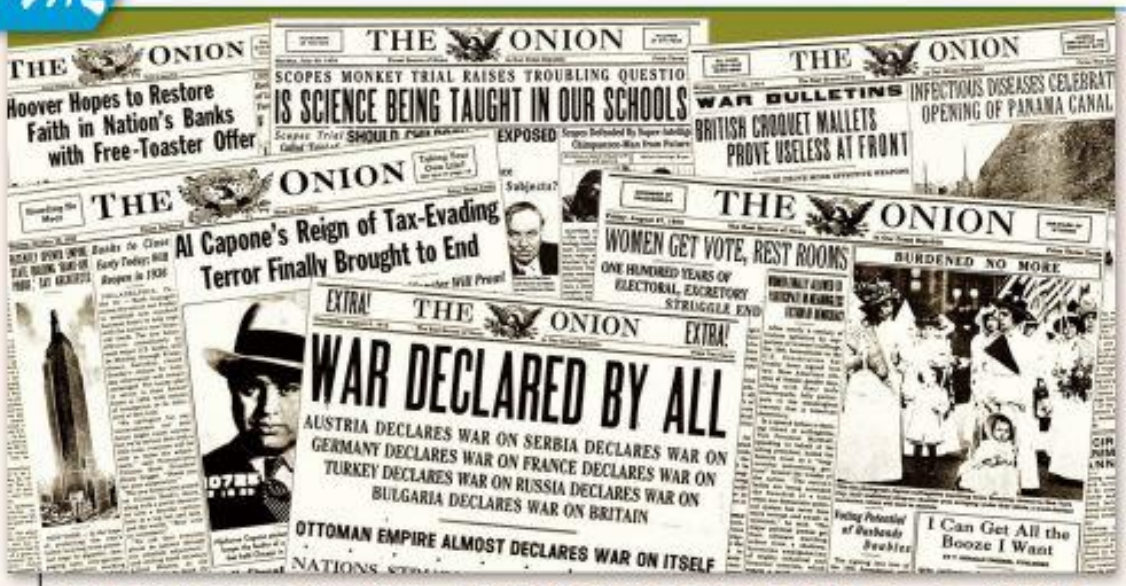


臺灣首次針對假訊息現象與事實查核成效的學術調查報告出爐；調查發現，臺灣有超過9成受訪民眾認為假訊息猖獗、嚴重影響社會，且受訪民眾普遍認為自己受假訊息的影響不大，卻擔憂別人會上假訊息的當。（資料來源：台灣事實查核中心，https://tfc-taiwan.org.tw/articles/7702）

[1] Bhaskaran, H., Mishra, H., & Nair, P. (2017). Contextualizing fake news on post-truth era: Journalism education in India. *Asia Pacific Educator, 27*(1), 41-50.

[2] Brummette, J., Distaso, M., Vafeiadis, M., & Messner, M. (2018). Read all about it: The politicization of "fake news" on twitter. *Journalism & Mass Communication Quarterly, 95*(2), 497-517; Mihailidis, P. & Viotty, S. (2017). Spreadable spectacle in digital culture: Civic expression, fake news, and the role of media literacies in "post-fact" society. *American Behavioral Scientist, 61*(4), 441-454.

[3] Allcott, H. & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of Economics Perspectives, 31*(2), 211-236.



現代人生活中充斥著各式各樣的媒體資訊，也使得民眾愈發難辨資訊真偽，諷刺新聞即屬其中一種。《洋蔥報》是美國一家新聞機構，以刊登諷刺文章著名，一貫以嚴肅的筆調報導杜撰的「新聞」，因此讓部分讀者信以為真，以訛傳訛，成為假訊息的來源。（Photo Credit: NiemanLab, https://www.niemanlab.org/2019/08/maybe-you-know-that-article-is-satire-but-a-lot-of-people-cant-tell-the-difference）

和宣傳（propaganda）。[4] Borel 則認為假新聞並不是為了告知，而是希望散播懷疑的種子，讓人分心，並且提供矛盾的、讓人困擾的新聞訊息。[5] 從臺灣 2018、2020 年兩次選舉來看，也可明白國內選舉中，不斷操作的假新聞與運用認知作戰，正在改變社會思辨的習慣。由於社群團體形成的同溫層與封閉性，選舉也形成極端的世仇（feud）陣營，世仇團體只和自己人對話，更進一步放大自己的憤怒與對特定事物的看法。[6]

從國內層面來看，政治人物或特定人士散布假新聞，主要是為了宣傳、邀功、轉移注意力以逃避更重要的問題等。散布的方式，除了透過傳統媒體之外，也會在社群媒體大量製造假帳號，大量寄送不實資訊，並藉由假帳號間的相互轉傳，增加按讚與分享的次數以營造網路聲量，讓資訊本身看起來很受重視，甚至很有公信力。美國史丹佛大學的一份研究報告顯示即使出身於網路世代，從小接觸網路、熟悉網路生態的學生族群，同樣也會被網路上的假訊息所誤導。[7]

「假新聞」已經從訊息是否虛假的問題，轉變成政治控制的問題了，這也是認知作戰討論的核心議題。事實上在認知作戰之下，這時假新聞已經無關真假，是意在權力與宰制，將衝突正當化的手段。假

[4] Tandoc, E. C. Jr., Lim, Z.W., & Ling, R. (2018). Defining "fake news": A typology of scholarly definitions. *Digital Journalism, 6*(2), 137-153.

[5] Borel, B. (2017, January 4). *Fact-checking won't save us from fake news.* FiveThirtyEight. https://fivethirtyeight.com/features/fact-checkingwont-save-us-from-fake-news.

[6] Brummette, J., Distaso, M., Vafeiadis, M., & Messner, M. (2018). Read all about it: The politicization of "fake news" on twitter. *Journalism & Mass Communication Quarterly*, 95(2), 497-517.

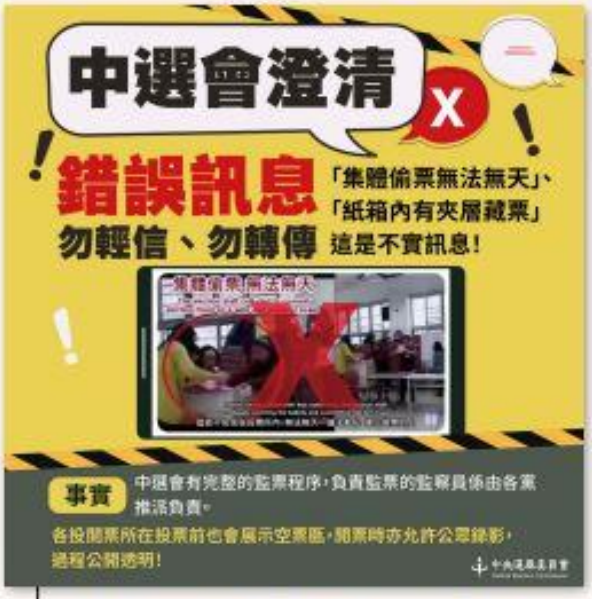
[7] Brooke Donald. (2016, November 22). *Stanford Researchers Find Students Have Trouble Judging the Credibility of Information Online.* Stanford Graduate School of Education. https://ed.stanford.edu/news/stanford-researchers-find-students-have-trouble-judging-credibility- information-online.

新聞不僅可以用來進行政治鼓吹，也可以藉著散布假新聞進行操控，以合理化自己的負面行為。[8] 社群媒體形成高同質性的社群，在選舉、公投等政治活動展開時，伺機導演各式政治攻擊，仇外與憎恨的言論日增，因此陷入極端政治，[9] 這些對民主政治的發展都是一種傷害。[10] 特別是公民如果接收一定程度的假新聞會對政治判斷產生負面的影響。[11]

從國內層面來看，政治人物或特定人士散布假新聞，主要是為了宣傳、邀功、轉移注意力以逃避更重要的問題。

假訊息的特色

如果散布假訊息要達到有效與影響力，就必須提高點閱率，引起閱讀者的注意，所以在標題的用詞上，通常會比正常的訊息來的聳動與誇張，利用釣魚式標題，來吸引讀者興趣，這類假訊息寫作風格和內容可作為辨識方法之一。特別是這類假訊息常涉及政治、種族、國家等敏感性議題，舉例圖西機場事件，當時假新聞標題使用「覺得自己是中國人就能上車！」來引發民眾的不滿，產生不適當的批評與輿論壓力，這類假新聞影響力相當大，可能造成人員傷亡或國家內部衝突。其次是為挑起閱讀者的情緒，某些假訊息在用字遣詞上會挑選較偏激詞彙，甚至人身攻擊的詞彙，例如「狼狽為奸」、「厚顏無恥」、「殘暴」、「怒斥」、「怒罵」、「胡搞」、



「假新聞」已從訊息是否虛假轉變成政治控制的問題，在選舉、公投等政治活動展開時，伺機展開各式攻擊，對立的言論日增，社會因此陷入極端政治，對民主政治的發展造成傷害。（圖片來源：中央選舉委員會 FB，https://www.facebook.com/photo/?fbid=431237392530020）

[8] 林照真（2022）。假新聞政治：台灣選舉暗角的虛構與欺騙。聯經。

[9] Mihailidis, P. & Viotty, S. (2017). Spreadable spectacle in digital culture: Civic expression, fake news, and the role of media literacies in "post-fact" society. *American Behavioral Scientist, 61*(4), 441-454.

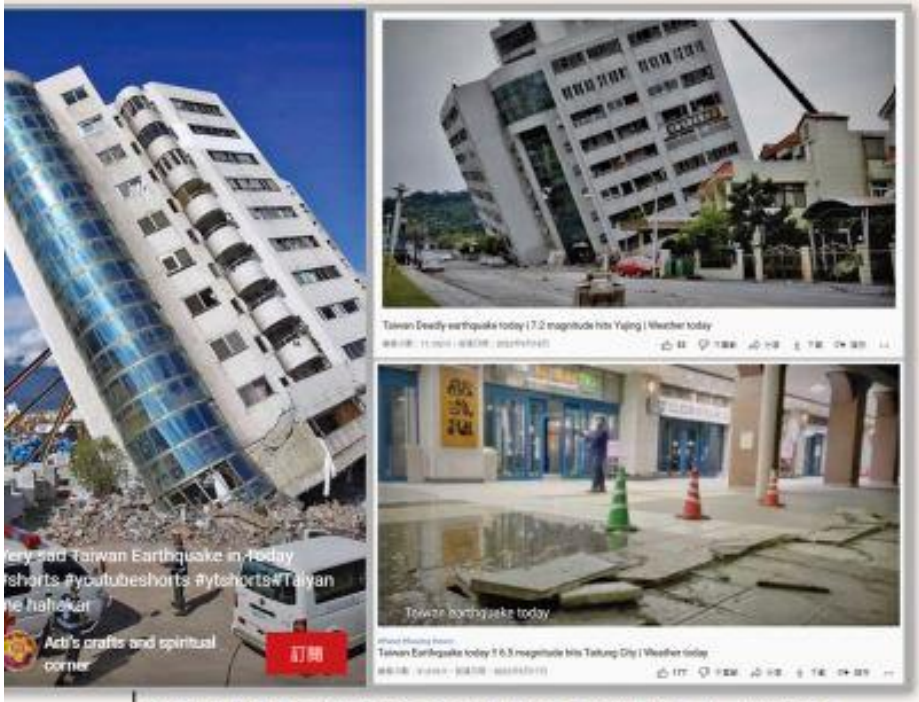
[10] Howard, P. (2016, November 23). *Is social media killing democracy?* Medium. https://pnhoward.medium.com/is-social-media-killing-democracy-ebce00776dde

[11] Guess, Andrew, Benjamin Lyons, Jacob M. Montgomery, Brendan Nyhan, and Jason Reifler. (2018). *Fake News, Facebook Ads, and Misperceptions Assessing Information Quality in the 2018 U.S. Midterm Election Campaign*. European Research Council (ERC) under the European Union's Horizon 2020 Research Report. http://www.dartmouth.edu/~nyhan/fake-news-2018.pdf

「無賴」等，都帶有負面的情緒用語。這類假訊息常發生在災情時的報導，利用改變真實新聞中的傷亡人數、發生時間與地點、災害損傷程度與數字等面向，加大災情的嚴重程度以吸引民眾點閱，如颱風侵臺時，改變真實新聞中的淹水高度、改變土石流造成的道路中斷時間或地點、捏造人員傷亡數字等。

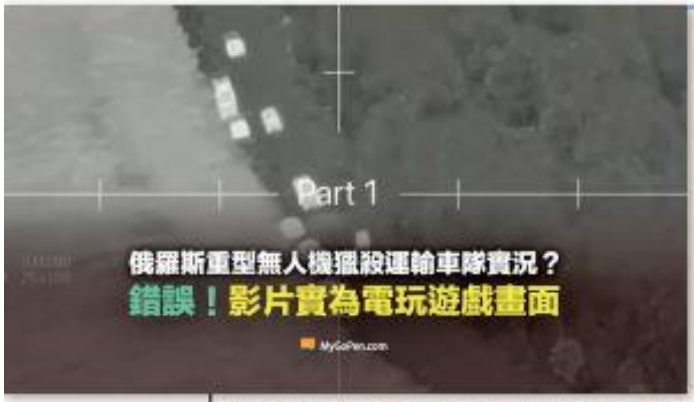
特別是當訊息是以「小道消息」、「口耳相傳」的形式在聊天群組、社交媒體等特定政治立場的選民中出現時，聽過愈多次愈容易相信、被激起的負面情緒愈強愈容易相信。但當訊息廣泛被主流媒體傳播和討論時，選民則更有可能被其他因素（既有政治立場、更多不同說法等）而影響。因此，廣泛傳播事實查核、對謠言的澄清，或許能降低謠言的可信度。

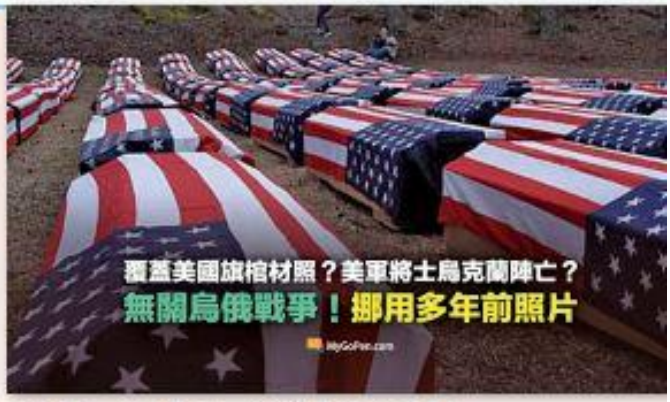
但是這些事實要查證需要時間，而且有部分真實部分虛假，因此在辨別上難度頗高。長此以往的結果便是民眾對於社會上資訊的不信任程度逐步增加。由牛津大學路透社新聞研究所發布的報告發現，我國於該調查 2017 年首度進行時，對於新聞信任度便僅有 31%，更在 2020 年進一步降至 24%。該份 2020 年的報告同時顯示，即使為使用者自行選擇的新聞媒體，使用者對於該新聞媒體的信任度也僅有 31%，透過社交媒體獲得新聞的信任度更僅有 16%。報告認為我國國民如此不信任新聞，是因為無論是社群媒體或傳統新聞媒體均充斥著假新聞。[12]



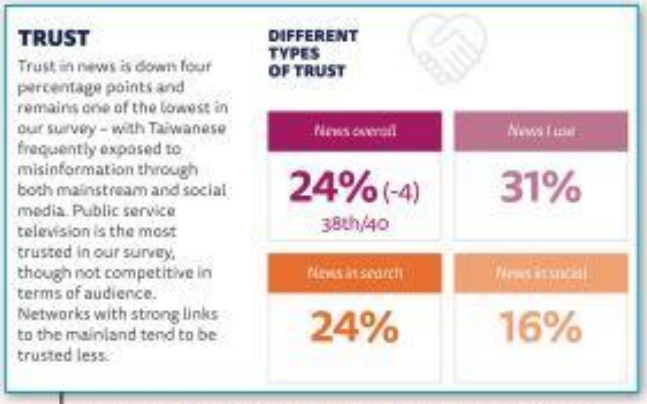
假訊息亦經常流竄於災情報導，移花接木各種類似災害影像，加大災情嚴重程度，吸引民眾點閱。（圖片來源：MyGoPen，https://www.mygopen.com/2022/09/earthquake.html）

[12] Nic Newman, Richard Fletcher, Antonis Kalogeropoulos, David A. L. Levy & Rasmus Kleis Nielsen. (2017). Reuters institute digital news report 2017, *Reuters Institute for the Study of Journalism*, p.129, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital%20News%20Report%202017%20web_0.pdf





面對認知作戰最重要的手段就是事實查核，廣泛傳播事實查核、對謠言澄清，即能降低謠言的可信度；圖為臺灣網站平臺 MyGoPen 澄清俄烏戰爭相關不實資訊的主題畫面。（Photo Credit: MyGoPen, https://www.mygopen.com/2023/02/Gunship-video.html; https://www.mygopen.com/2023/04/war-photo.html）



牛津大學的研究報告指出，2020 年我國民眾對新聞信任度僅有 24%，對社交媒體的新聞信任度更僅剩 16%；民眾如此不信任新聞，是因為媒體充斥著大量假新聞。（Source: Reuters Institute for the Study of Journalism, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2020-06/DNR_2020_FINAL.pdf）

認知作戰成為攻擊民主的武器

另外許多公共政策被片面傳遞又難以查證，就已經達到了帶風向的目的。例如，質疑美國會拋棄臺灣的「拋棄論」、美國無法保護臺灣的「實力論」與美國是世界亂源的「亂源論」，也一直是對臺灣認知作戰操弄的主軸。特別是萊豬的議題除了與食安有關，更容易連結「反政府」、「反美」的情緒，試圖傳達政府以萊豬換疫苗、換武器、換取國際關係的因果關係。萊豬議題也是中共官媒與官方社群媒體的著力點，帶有陰謀論的企圖。特別是近年國際關係的訊息也與疫情結合變異，與疫情緊密相關的是疫苗，「缺疫苗」、「疫苗有問題」、「疫苗沒有用」的論述都與捐贈疫苗的美、日兩國結合，也都有中共官媒與對臺機構的影子，試圖塑造「反美」、「反日」情緒，影響臺灣與友邦的關係。

中共官方媒體與部分媒體與臺灣的媒體經常互相引用內容，匿名華語臉書粉專內容也有所連動，因而可以持續擴大對臺影響力；目前觀察到國際新聞假訊息是隨時事而起，沒有任何證據足以證實與選舉的關聯，但要留意的是部分來自中國大陸發起的資訊操弄。

面對認知作戰最重要的手段就是事實查核

臺灣在假新聞查核相對落後的大環境下，針對公眾進行的資訊識讀教育也顯得格外重要，這部分目前也是大型社群平臺可以再為假新聞防制做出的貢獻。重懲之下是否對言論自由產生寒蟬效應，則是政府務須三思之處。

本文摘自清流雙月刊中華民國112年5月 號P4-P9

運營技術(OT)系統所面臨的挑戰與保護策略

/華梵大學特聘教授-朱惠中

運營技術（OT）系統所面臨的挑戰與保護策略

◆ 華梵大學特聘教授 — 朱惠中

運營技術（OT）系統對於工業和關鍵基礎設施的運營至關重要。然而，此類系統通常由可能已有數十年歷史（上世紀所開發製造的軟硬體）且缺乏現代安全功能的設備所組成，使得 OT 系統容易受到新型態的網路攻擊。[1]

OT 系統面臨的挑戰

歸納國內外相關文獻及我國國情後，綜整 OT 系統所面臨的挑戰及其可能造成之衝擊，如次說明：[2]

一、OT 系統之發展與沿革略可分為人力時代、電氣化時代、自動化時代及智慧時代等四個階段，各階段的主要控制機制分為機械及電子電力（類比）控制、電腦（數位）控制，及整合與智慧控制等，至於其相對應的時程，除智慧時代外，餘均早於 20 世紀初期，故負責操作與規劃人員大多數普遍欠缺資訊（安）技能。

[1] 對 OT 與 IT 的更多認識，請參閱本刊第 42 期頁 11 至 16，〈如何降低 CI 遭網路攻擊的衝擊〉，https://mjib-ebook.com/MJIB/no42/index.html；本刊第 45 期頁 56 至 61，〈如何縮小 CI 資安防護人才缺口〉，https://mjib-ebook.com/MJIB/no45/index.html。

[2] Cabrera, E (2016). *Critical infrastructure under attack: The vulnerability of converged IT-ICS networks.*

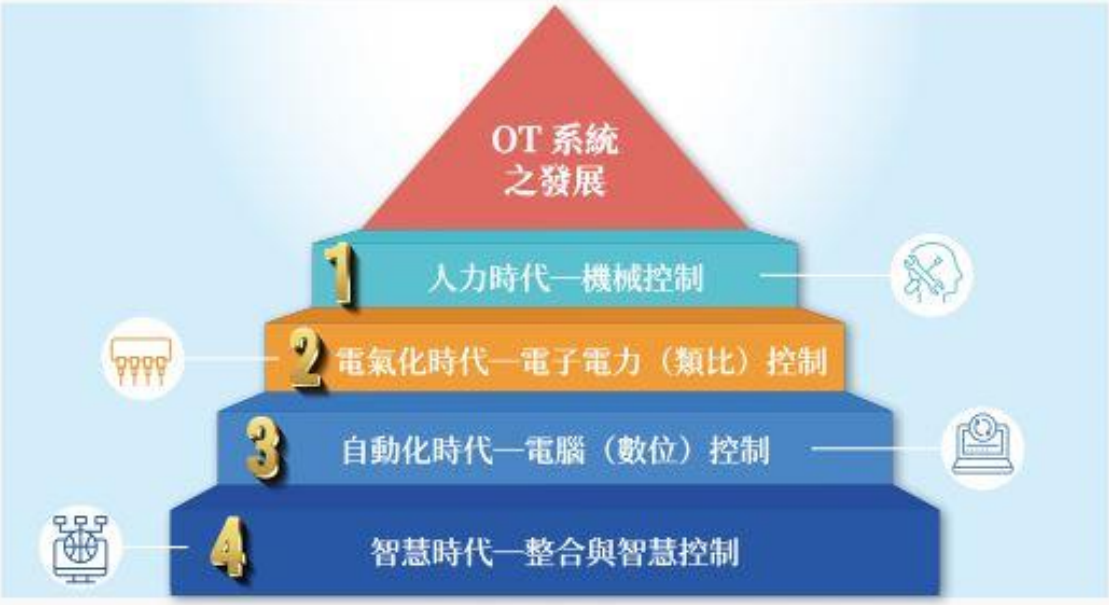


圖 1　OT 系統之發展與沿革

二、大多數的 OT 系統係由歐、美、日等地輸入，終端使用者在應用軟體（如 OT 之邏輯控制、系統的架構與安全標準等）及硬體操作介面的自主性均較低，因此資安問題更顯得重要。

三、基礎防護觀念與經驗薄弱，諸如安全防護不足、介入控制不嚴格、外包服務管理缺失（易受供應鏈攻擊）、教育力度不夠及應變能力不足等，均是需要強化處。

四、人員缺乏安全意識，管理 OT 系統的操作員和技術人員因可能缺乏安全意識和培訓，使他們容易受到社交工程攻擊。基本上成功的社交工程攻擊將可透過從業人員的輕忽，獲取對機敏資料或系統的存取控制。

五、資安工具疊床架屋的情況嚴重，這是因為觀念錯誤導致，認為工具越多越安全。事實上，工具太多會因增加複雜性，導致資安團隊疲乏、過勞，實際上反而會增加誤判風險。故新的工具應該是為了協助資安團隊，而非讓他們工作更加沉重。

六、OT 網路設備的基本精神是經久耐用而不是更新，許多工業設備對正常運行時間的嚴格要求（如無法隨時停機），迫使更新或更換變得困難、成本高昂或存在風險。

七、IT-OT 融合以及新技術將增加風險，隨著數位化轉型打破 IT-OT 障礙，以及嶄新複雜網路攻擊的出現，均使得 OT 網路框架的適應速度相對過慢。

八、許多 OT 網路所有者因對採用零信任機制的猶豫不決及對停機導致收入損失、基礎設施中斷甚至危及人員安全的擔憂，即使零信任仍然是保護現代網路的最有效策略，但工業運營商仍無法確定或權衡成本和複雜性的潛在危機。

九、普渡（Purdue）模型是否仍然適用於現代 OT 網路？傳統 OT 係使用區域概念以上下文為基礎（context-based）來進行分段（segmentation），但因 Level 0 感測器（sensor）所蒐集的資訊可以直接發送到雲端，並通過蜂巢網路（cellular networks）直接與雲中的監控軟體通信（亦即 OT 網路的分段框架通常被擱置一旁），復以蜂巢網路其本質上是扁平的，故 Purdue 模型似無法落實於蜂巢網路。

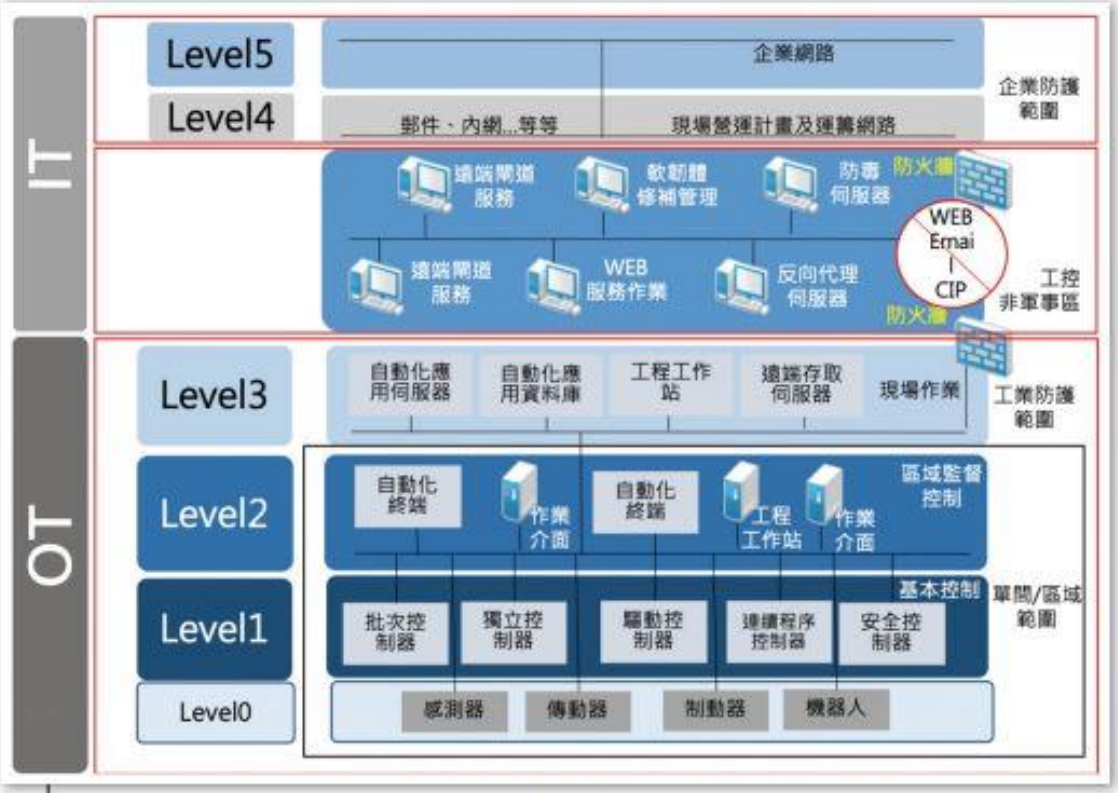
十、企業營運比以往更加仰賴即時數據提供收費依據，此外也需要遠端存取提供支援，因此，OT 網路必須與企業網路和網際網路連接。而原本跟外界 IT 網路隔離的 OT 網路對逐漸與 IT 網路整合的情況，尚未做好妥善準備。

十一、不安全且含有漏洞的 IT 網路一旦與 OT 網路直接相連，將使得控制系統（Purdue 模型中 L2 及 L3）暴露在網路攻擊的危險當中。歹徒可利用不安全的企業網路設備當成跳板，經由彼此依賴的複雜網路，一點一滴逐漸移轉到最容易攻擊的工業控制系統（ICS）設備和資料庫。

十二、OT 系統缺乏加密機制；加密對於保護現代工業和關鍵基礎設施流程中的機敏數據和通信至關重要。然而，運營技術 OT 系統因可能不支援現代加密演算法，使它們容易受到攻擊。復以系統缺少終端使用者行為紀錄，亦無法歸責或追溯被洩露的使用者帳號行為。

十三、因 OT 系統使用不安全的通信協議，故攻擊者較易入侵 OT 系統。

「零信任機制」是一種網路資安的架構和目標，它的假設前提是任何交易、個體與身分在獲得信任並持續維持信任之前，全都不可信任。



普渡模型為 OT 與 IT 網路環境整合的參考模型，共分為 6 個層級，但至今是否仍適用於現代 OT 網路已引起疑慮，且不安全並有漏洞的 IT 網路一旦與 OT 網路直接相連，將使控制系統（L2 及 L3）暴露在網路攻擊的危險中。（資料來源：經濟部，https://www.acw.org.tw/UpFiles/05- 網通產業工控物聯網資安實務指南 .pdf）

保護 OT 系統的策略[3]

一、進行風險評估

風險評估是針對「識別潛在危險」並「分析危險發生時可能發生的情況」的過程，其目的是識別、評估對 OT 系統所存在的風險並確定其優先等級的過程。組織將根據風險的潛在影響和發生的可能性及機率，對風險進行優先排序；並依據風險評估的結果，制定並實施降低風險的策略，以減少網路遭受入侵的機率。

二、實施網路分段

實施網路分段的目的為降低 OT 系統的風險，將網路劃分為更小、更安全的子網或網段，以縮小網路受攻擊的範疇，並為每個子網路提供獨特的安全控制機制和服務，保護關鍵資產遭受駭客攻擊或降低網路攻擊可能造成的損害。此外，組織應識別關鍵資產和系統，並將它們與非關鍵系統區分開來。依據最小授權機制精神，從外部連線之用戶，應配置於專屬網段，

[3] Abhay, S. K. (2023, April 24). *Securing legacy OT systems: Challenges and strategies*. Sectrio. https://sectrio.com/securing-legacy-ot-systems-challenges-and-strategies

網路分段係將網路劃分為更小、更安全的子網或網段，以縮小網路受攻擊的範疇，並為每個子網路提供獨特的安全控制機制和服務，保護關鍵資產遭受駭客攻擊或降低網路攻擊可能造成的損害。

並搭配防火牆予以隔離；不同類型用戶與不同類型資源，皆應以不同網段予以區隔，才能在發生攻擊事件時，將災害縮減至最小範圍。

三、實施存取控制

應控制對 OT 系統的存取，其機制應包括強大的身分驗證、授權和問責機制。組織應將對關鍵系統的訪問限制為僅允許有合法存取需求的授權人員進行存取。實施存取控制的第一步是確定需要保護的資產以及需要存取的個人或軟、硬體資產。接著應制定存取控制政策，來定義授予和撤銷對這些資產存取權限的規則。在授予系統存取權限之前，應使用強大的身分驗證機制，例如雙因子身分驗證（2FA）或生物識別身分驗證來確認用戶的身分。

四、實施系統強化

系統強化（systems hardening）通常是通過減少攻擊面（attack surface）來保護系統的過程，當系統能執行的功能增加時，漏洞面會隨之變大；原則上，單一功能系統的安全性比多功能系統來的高。減少可用的攻擊方式（attack vector）通常包括更改預設密碼、刪除不必要的應用軟體，以及禁用不必要的端口（port）或刪除不必要的服務、協議和應用程序等。此外，建置防火牆、入侵檢測（Intrusion Detection System, IDS）和入侵防禦（Intrusion Prevention System, IPS）系統、限制利用遠端桌面協定（Remote Desktop Protocol, RDP）對 OT 系統和組件進行存取，亦可降低網路攻擊成功的可能。惟須注意的是系統強化固可降低網路攻擊成功的風險，但任何錯誤配置可能導致意外後果或停機。

五、實施安全監控

包括實施網路和系統監控工具、入侵偵測系統以及安全資訊和事件管理（Security Information and Event Management, SIEM）解決方案，以檢測潛在威脅。同時，組織應同步建立緊急應變的復原計畫與程序。重要的是，安全監控應該是一個持續的過程，組織應該定期審查和更新監控策

在授予系統存取權限之前，應使用強大的身分驗證機制，例如雙因子身分驗證或生物識別身分驗證來確認用戶的身分。

系統強化是通過減少攻擊面來保護系統的過程，減少可用的攻擊方式包括更改預設密碼、刪除無需的應用軟體、服務、禁用無需的端口等；此外，建置防火牆、入侵檢測和入侵防禦系統、限制遠端桌面協定存取，亦可降低網路攻擊。

略，以確保在面對不斷變化的網路威脅時保持有效。

六、實施安全意識培訓

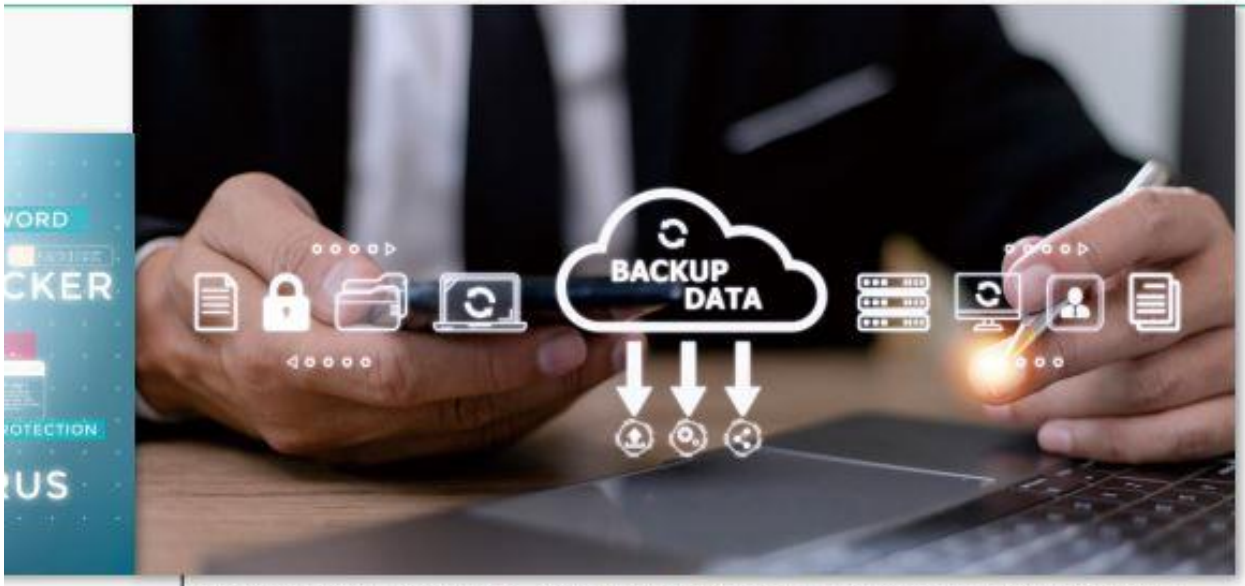
此培訓對於降低人為錯誤或疏忽導致的網路攻擊至關重要，應包括定期網路安全意識培訓以及通報潛在安全事件或威脅的明確程序。

七、定期更新和修補

OT 系統的使用壽命通常很長，並且可能運行在過時的軟體和硬體上，這使它們容易受到網路攻擊，定期更新和補丁（patch）將有助於解決這些漏洞。組織宜制定補丁管理程序，包括定期審查軟體和硬體更新、部署前測試補丁以及跟蹤和報告補丁部署的流程。同樣重要的是，要確保任何 OT 系統仍持續從製造商或供應商接收到安全更新，並擬定計畫來解決可能出現的任何安全問題。但是，由於傳統的定期更新和修補會造成關鍵運作中斷，使得更新和修補 OT 系統可能具有挑戰性。一般而言，更新和修補 OT 系統會配合關鍵系統大修時程進行。

八、實施數據備份和恢復計畫

OT 系統通常處理對業務運營至關重要的關鍵數據，這些數據的丟失或損壞可能會造成嚴重後果。組織應制定資料備份和恢復計畫，包括定期計畫的關鍵資料備份、備份和恢復程序測試，以及監控和報告備份和恢復狀態的流程。重要的是要確保安全地存儲備份並定期測試備份數據以確保在數據丟失或損壞的情況下可以恢復。此外，組織應考慮實施冗餘備份系統，如備份 3 份資料、2 種儲存媒體及 1 份異地備份的方式，以提供額外的保護層，防止資料遺失或損毀。



OT 系統通常處理至關重要的關鍵數據，組織應制定資料備份和恢復計畫，確保安全地存儲備份並定期測試以確保在數據丟失或損壞的情況下可以恢復。

九、實施災難復原計畫

包括識別關鍵系統和數據的過程、制定在發生災難時恢復這些系統和數據的計畫，以及測試和培訓人員執行該計畫，並定期測試和更新災難復原計畫以確保其有效。此外，組織亦應考慮實施冗餘系統或備份設施（High Availability, HA），以防主要系統或設施受到損害。

十、實施事件緊急應變計畫

事件的範圍從網路攻擊和系統故障到人為錯誤和自然災害，亦即須由天然災害、人為疏失及資訊安全等三個面向來規劃，並須考量當上述三個面向同時發生時的 SOP。組織應先確定最有可能發生的事件類型，例如網路攻擊或系統故障。然後，制定一個計畫概述應對每種類型的事件單獨或同步（兩種類型或三種類型）發生時應採取的步驟，計畫內容應包括檢測、遏制、根除和復原程序。

事件的範圍從網路攻擊和系統故障到人為錯誤和自然災害，亦即須由天然災害、人為疏失及資訊安全等三個面向來規劃，並須考量當上述三個面向同時發生時的 SOP。

結語

資安防護不難，難在如何落實。此外，針對不同關鍵基礎設施的 OT 之客製化，及作業疏失所造成的問題，均是本主題的關鍵成功因素。

本文摘自清流雙月刊中華民國112年9月 號P33-P39