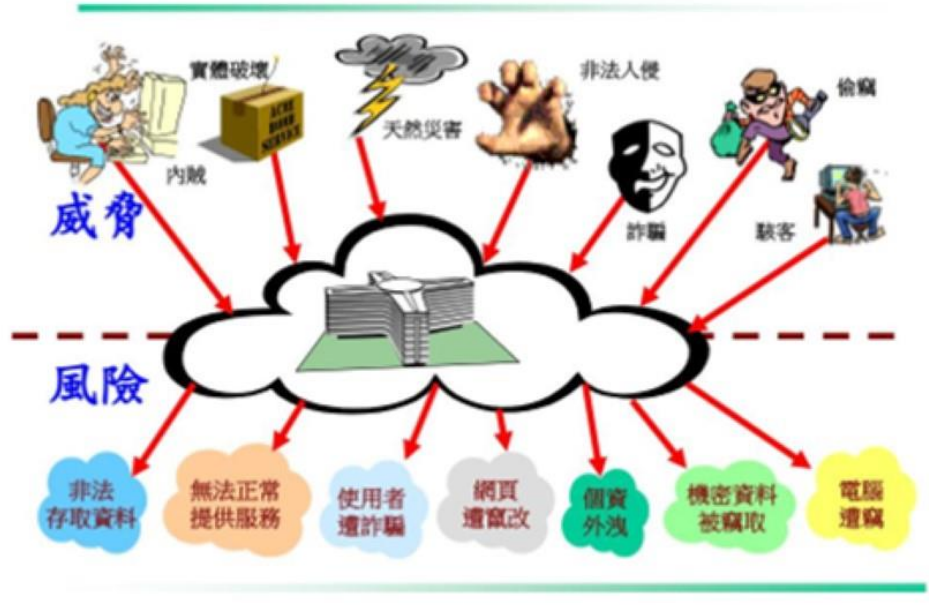
臺東林區管理處政風室
112年2月號

公務機密

資訊安全維護

網路無國界，個資須警戒。
防駭不注意，隱私落滿地。



資安時事案例

免費Wi-Fi恐遭駭客"造假" 個資全盜光!

普發6000元假網址簡訊冒用名義
數位部：已報警並註冊網址澄清防詐騙

個人資料保護法

新增團體訴訟

生活中的資安

臉-為何會被挖走?

數位學習

【個資保護】阿貴跟你說：個資提供要小心
資安防護免煩惱！

免費Wi-Fi恐遭駭客"造假" 個資全盜光！

華視新聞張庭瑜 陳建安 報導 / 台北市

不少飯店或景點都會提供免費Wi-Fi讓旅客使用，但是如果沒有仔細確認是不是官方的網域，很可能不小心連到駭客設置的假WI-FI，資安專家表示，通常駭客會設定與飯店相似的Wi-Fi名稱，民眾連線後若再使用銀行或購物網站App，個資就容易外流，若是飯店系統被駭客入侵，甚至連財務報表、房客銀行卡號都可能被竊取。

電影講述女子，在餐廳連上不明WI-FI後，開啟了一連串惡夢，個資被竊取連在家換衣服也被偷拍，但現實生活中，到處可以看到免費Wi-Fi，不少民眾出遊，到飯店第一件事，就是拿出手機打卡，但如果沒有仔細看連上的網域，可能有個資風險，許多假Wi-Fi名稱通常看不出來，資安專家表示，尤其在飯店，假設旅客住在601房，那麼駭客可能設定Wi-Fi名稱為6樓5樓等，當旅客連線假Wi-Fi後，再使用銀行或購物等App，個資就可能被上傳盜取，那麼如果是飯店系統被駭客入侵呢？

資安專家劉彥伯說：「包含飯店本身公司的內部資料，這個部分就包含像員工的個人資料，公司的財務資料，包含像旅客聯絡方式，或者是旅客的金融交易相關資料，像是信用卡或者是個人的身分證，住宿聯絡方式。」

但台灣人大多使用手機吃到飽方案，加上還有i Taiwan免費無線上網可以使用，相對被駭客使用Wi-Fi盜取機會低，但出國旅遊到機場，難免會使用當地免費網路，那麼可以怎麼避免，資安專家劉彥伯說：「防毒軟體基本上如果可以安裝，基本上一定要安裝，因為防毒軟體針對於假的軟體，如果它是假的WI-FI軟體，它是有一定性的能力可以保護(個資)，第三個就是如果有VPN的話，建議可以開啟VPN。」公共Wi-Fi有一定程度的風險，建議民眾出遊，避免使用不需要密碼的不明Wi-Fi，以防個資被盜用，還壞了出遊好興致。

普發6000元假網址簡訊冒用名義

數位部：已報警並註冊網址澄清防詐騙

Newtalk新聞 | 社會 | 謝莉慧 綜合報導　發布 2023.01.06

數位發展部今（6）日表示，有民眾收到偽冒該部名義發送的詐騙簡訊，數位部接獲訊息後，已向警方165反詐騙專線完成報案。經查由於該簡訊的網址實際上之前沒有人註冊使用，為避免日後遭有心人士利用，造成民眾上當受騙，數位部已經註冊，並設定自動導向民間事實查核單位的澄清說明網頁，以釐清事實，防止假訊息擴散。

數位部進一步指出，該詐騙簡訊所載網址首段不是gov.tw結尾，不屬於政府機關網址，顯然是假訊息，呼籲民眾若有收到這類詐騙簡訊，務請不要轉傳，造成親友誤解。

數位部同時也提醒國人注意，不會透過簡訊通知民眾領錢，普發6000元在農曆年後才會發放，發放方式一旦定案就會立即公開說明，相關申領網站的網址首段一定會是gov.tw結尾。至於數位部推出的政府縮短網址服務（https://url.gov.tw）所產生的政府網站短網址，也一定是https://gov.tw/ 開頭，請民眾認明政府機關專用網址，切勿點擊來源不明的簡訊或連結，以免上當受騙。

個資法修正重點

- **新增團體訴訟**
  - 為鼓勵民間公益團體參與保護，並方便被害民眾行使損害賠償請求權，增訂團體訴訟相關規定，**得提起團體訴訟**，以協助當事人進行損害賠償訴訟。（第 32 至 40 條）

資料來源:個人資料保護法

FaceBook 標註姓名？

◆ 調查局資通安全處　雷瑜翔

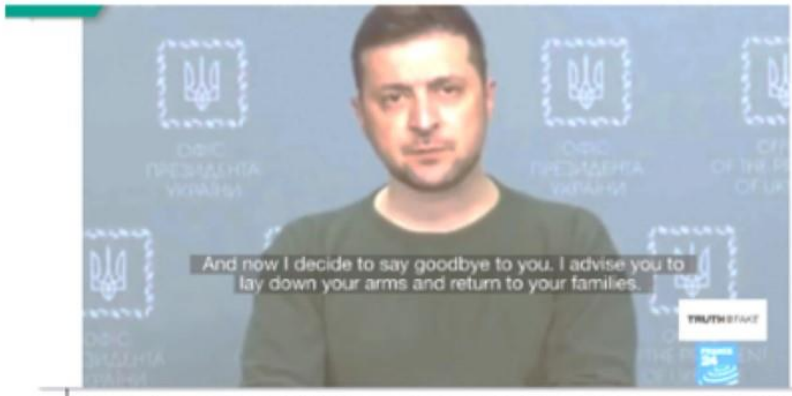
DeepFake 影片內容多半是不雅影片或假訊息，輕則傷害當事人名譽，重則危及國家安全，不可不慎。

DeepFake 影響，不容小覷

隨著科技快速發展，多媒體的傳播途徑也因此受惠，發布者自此多了一種便利且快速的傳播方式；但是一方便，就會造成氾濫，若散播內容是正確的，抑或是無關緊要的廣告，尚且無妨，但若是「惡、假、害」的不實訊息，那麼將帶來負面衝擊，甚至危及國家安全。

最明顯的例子是今年俄烏開戰初期，駭客散播烏國總統澤倫斯基勸烏軍投降的DeepFake 影片，[1]這支影片長度 1 分鐘，澤倫斯基對著鏡頭向烏軍喊話，要他們放下武器、停止與俄羅斯戰鬥。這影片不僅出現在社群媒體，更一度被駭客放到烏國新聞電視臺「Ukraine24」上，稱澤倫斯基已逃離基輔，要求民眾無需抵抗，直接投降。

[1] "Debunking a deepfake video of Zelensky telling Ukrainians to surrender • FRANCE 24 English", https://www.youtube.com/watch?v=ZtgcX5WYhr0.



以 DeepFake 技術假造烏克蘭總統澤倫斯基勸烏軍向俄羅斯投降的影片截圖；影片中，澤倫斯基的發言和嘴型尚算同步，但觀看者很快會發現他的口音不對。（Source: FRANCE 24 English, https://youtu.be/ZgqX5WVhr0）

何謂 DeepFake 技術

DeepFake 技術簡單來說，就是可以把一個人的臉，天衣無縫地置換入另個人的影片或相片中，即使他（她）從未在其中實際出現過。其實這並非新穎技術，2015 年美國電影《玩命關頭 7》就曾運用過。男主角之一的保羅・沃克，在戲未殺青前突然發生車禍意外身亡，因此製片團隊找了保羅的弟弟拍攝剩餘戲分，利用電腦動畫技術，將保羅的臉置換在弟弟身上，使保羅得以在片中復活演出；當時需動用到一整個電影團隊，且不知燒了多少資金才得以製作出該影片。而現代拜科技蓬勃發展、人工智慧（AI）快速運算優勢之賜，DeepFake 影片製作流程已相當簡化，目前不需花大筆費用，僅需要一個人操作，透過家中個人電腦即可產出。

2015 年美國電影《玩命關頭 7》男主角之一的保羅沃克因車禍意外身亡，製片團隊找保羅的弟弟拍攝剩餘戲分，再利用電腦動畫技術，將保羅的臉置換在弟弟身上，使其得以在片中復活演出。（Source: Weta Digital, https://youtu.be/ye7arp5IrAg）

DeepFake 技術之發展過程

DeepFake 的核心技術是機器學習，也是 AI 的應用之一。要製作某人的 DeepFake 影片，首先須將某人的實際影片交由類神經網路（neural network）訓練，讓程式蒐集該人物在不同角度及不同光線的資訊數據。這過程雖不需像早年的動畫技術，動輒需耗時數個月，但也需要幾個小時的時間，程式才得以完成訓練。接著便可結合訓練完的類神經網路及電腦圖學技術，取代標的人臉。

要製作某人的 DeepFake 影片，須將某人的實際影片交由類神經網路訓練，讓程式蒐集該人物在不同角度及光線的資訊數據，接著便可結合訓練完的類神經網路及電腦圖學技術，取代標的人臉；圖為國科會 2022 年發布的《認識 Deepfake 防範假訊息》宣導影片，主角為數位發展部部長唐鳳。（圖片來源：國科會科技辦公室，https://youtu.be/VEgGSbFWjb8）

類神經網路知多少

類神經網路是 DeepFake 的核心技術之一，早在 1980 年代便已被提出，然而當時因遇到技術瓶頸而沉寂了一段時間，直至 2012 年因圖形處理器（GPU）技術的進展，才讓類神經網路再次活躍於技術最前線。

簡單來說，類神經網路就是透過電腦模擬生物大腦的神經元運作方式所建立出來的數學模型。透過建置出多層的神經元，每一層神經元都會經由一個特別的函數產生輸出值，並且逐層往下傳遞，直到最後一層輸出最終結果，如圖 1 所示。輸入層及輸出層各僅有一層，而中間層可以有很多層，層級愈多，計算的複雜度也愈高，所需耗費時間也愈久，不過，相對所獲得的結果也會較為精準。

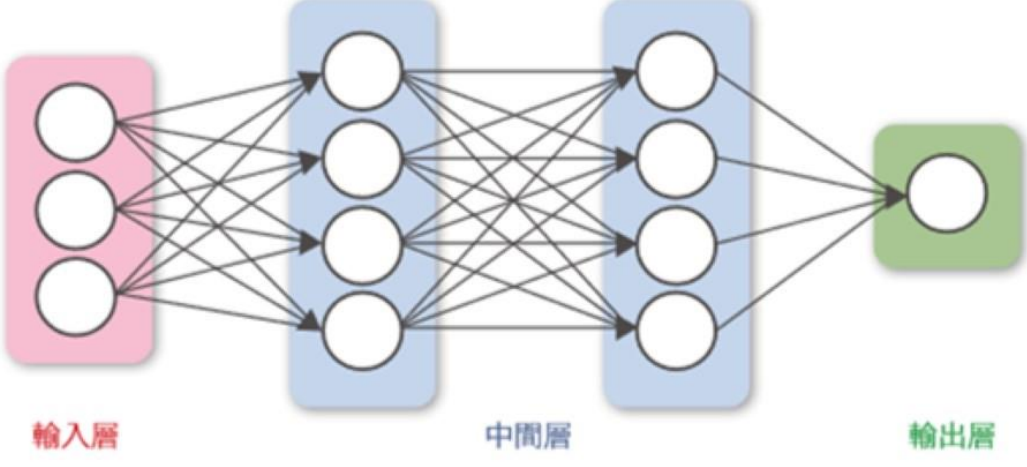


圖 1　神經元傳遞層級示意

既然是要模擬生物大腦的神經網路，那就必須建構出數千萬層的神經元網路，如此才能夠計算出最貼近真實的結果。然而，在 1980 年代，當時僅能正確地計算出 2 至 3 層的神經網路，故類神經網路這項技術並不受科學家重視；之後在 GPU 運算能力大幅提升後，解決了瓶頸，從而打開類神經網路應用的這條大道。

另個大家很常聽到的名詞是「深度學習」（deep learning），其實它的本質就是類神經網路，之所以取新名為「深度」，就是因為 GPU 使得類神經網路的多層網路不再只是紙上談兵，而是可實現的技術。一種名為「生成對抗網路」（generative adversarial networks, GANs）的深度學習演算法，便是 DeepFake 的主要開發引擎之一。

「生成對抗網路」演算法

GANs 顧名思義，是由一個名為「生成網路」及另個名為「對抗網路」所組合的演算法。「生成網路」輸出作為「對抗網路」輸入，「生成網路」輸出目的是要儘可能產出以假亂真的資料，而「對抗網路」是要判別「生成網路」傳來的資料，區分差異，然後將結果回饋給「生成網路」。與此同時，「生成網路」藉由這個回饋產出更逼真的資料。如此一個乒乓來回的過程，讓最終的產出結果幾近真實。

所以現在要製作 DeepFake 影片，不需要自己重頭到尾寫一套類神經網路程式，網路上已有許多現成應用程式或是手機 APP 可供下載（當然是要付費，開發者藉此賺些蠅頭小利），使用者僅須按照指南，便可一步一步地製作出 DeepFake 影片。

相關案例

2020 年 11 月初，韓國第一位 AI 主播金柱夏於 MBN 電視臺首次亮相，順利播報當天新聞。這位 AI 主播以該電視臺主持人金柱夏為原型，觀眾收看後幾乎分不清誰才是本尊。[2] MBN 表示，「使用 AI 主播可在突發災難狀況時，迅速向觀眾播報新聞內容，且能一天 24 小時持續工作」，並可節省大量人力、時間和費用成本。

2021 年 3 月初，一則好萊塢巨星湯姆克魯斯（Tom Cruise）開始玩抖音，在高爾夫球場開球並向網友打招呼的影片出現，立刻吸引 250 萬人觀看。該影片其實是比利時電影特效專家 Chris 所製作，其自創「一鍵生成」濾鏡，能讓任何人輕易把明星的臉移花接木到自己臉上。[3]

政客更是 DeepFake 影片製作顯而易見的標的對象。2020 年美國總統大選前，DeepFake 讓拜登（Joe Biden）打瞌睡受訪、[4] 裴洛西（Nancy Pelosi）酒醉演說、[5] 川普（Donald Trump）加入《絕命毒師》

[2] 《南韓首位 AI 主播正式上工：以當家主播為原型，本人直呼「好可怕！」》，https://www.storm.mg/article/3224466。

[3] 《「阿湯哥」變軍抖音？ 辨 deepfake 技術真假難辨》，https://news.tvbs.com.tw/world/1474034。

[4] 《【錯誤】老拜登在電視訪問時睡著打呼的影片？影片後製痕跡》，https://www.mygopen.com/2020/09/Joe-Biden-asleep.html。

[5] 《裴洛西「喝醉假影片瘋傳」200 萬人看過　神川普與律師都散播》，https://www.ettoday.net/news/20190524/1451830.htm。

左圖畫面右側為韓國首位 AI 主播，以左側的主播金杉雯為原型；工作人員只要輸入文字稿，就能讓 AI 主播自動播報新聞，如右圖播報畫面。（Source: MBN News, https://youtu.be/k8X_Em-NQn0; https://youtu.be/Fo33gOcHXSU）

男川普置入《絕命毒師》影集，該如何洗錢的 DeepFake 影片（左），與原影集畫面相較（右），幾乎沒有破綻。（Source: Ctrl Shift Face, https://youtu.be/Hc9h0uemWQ; Breaking Bad & Better Call Saul, https://youtu.be/RnsUHDJ0BPM）

陣容大談如何洗錢，[6] 以及其與國務卿蓬佩奧（Mike Pompeo）高唱「我愛你，中國」[7] 等影片，更是瘋傳全球，一天內甚至超過百萬人次轉傳。

Deepfake 影片除造成名譽與金錢損失外，透過假訊息造成的社會意見分歧，也可能產生嚴重後果，在世界各地已有先例；中非國家加彭（Gabon），甚至因此成為一起政變的導火線。[8]

---

[6] 《Breaking Bad》為美國電視影集劇，講述高中化學教師的犯罪故事，其因患上肺癌末期，龐大的醫療費用讓起家的他開始製作及販賣冰毒；本片被認為是最偉大的電視劇之一，並贏得 110 個獎項。

[7] https://www.youtube.com/watch?v=UdtcWps3jSM.

[8] 2018 年 10 月，非洲國家「加彭」的總統邦戈（Ali Bongo），在沙烏地阿拉伯訪問傳感腦，此後 3 個月除官方照片外，加彭當局鮮少釋出其他訊息，直到 2019 年新年除夕，邦戈出現在電視上向人民拜年，但螢幕上的他看似中風模樣，卻引發大眾揣測。反對黨成員跳出來，指責這是一支 Deepfake 影片；也有人懷疑，邦戈健康狀態已嚴重到不能露面，而實際掌權的是他身旁貪腐的集團。影片播出後第 7 天，武裝集團便展開政變。《總統拜年影片是 Deepfake ？被不信任催化的一場政變》，https://www.aibooksbank.com/news/content/3A34CF908C10819930420B117A13A229。

安全議題與相關法令

DeepFake 技術雖對娛樂圈與商業界貢獻不少，然經估計，93% 的 DeepFake 影片內容都是偏向色情，據悉上傳該等影片的論壇已累計超過 1.34 億次的瀏覽量，相信「獲利匪淺」。《神力女超人》蓋兒・加朵（Gal Gadot）及黑寡婦史嘉蕾・喬韓森（Scarlett Johansson）等上百位國際女星都是受害者。[9]

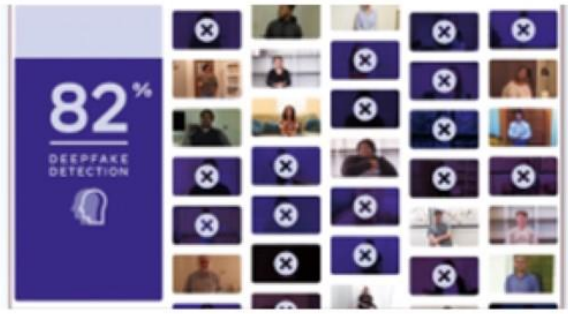
去年立委高嘉瑜被變造的不雅影片流出，引起一陣軒然大波，許多立委跳出來大聲疾呼，拋出修法議題欲嚴加防範。DeepFake 影片的危害，嚴重者將會影響金融安全、選舉公平性甚至擴大至國家存亡。行政院於今（2022）年 3 月通過修正《刑法》來遏制 DeepFake 技術亂象，草案規範若製作不實性影像並散布營利，最高可處 7 年有期徒刑。

自動屏蔽 DeepFake 影片技術

DeepFake 技術門檻的降低，讓非資訊領域出身的素人，亦可經由現成工具，在短時間內自行製作出 DeepFake 影片，且在有利可圖下，一定會有人以身試法。縱使有刑罰能遏阻其等製作散播，然若經由人工舉發後才得知，表示該影片已外流擴散，不僅效率不彰，且可能已經造成傷害，故根本解決之道，最好還是能發展出自動偵測 DeepFake 影片，並立即禁止其等轉傳的技術。

全球數間社群媒體大廠，諸如臉書（Meta）、推特（Twitter）及 YouTube 已爭相投入相關研發工作，並發展出偵測與自動屏蔽疑似 DeepFake 影片軟體的技術。概述如下：

《神力女超人》主演蓋兒・加朵（右）及《黑寡婦》史嘉蕾・喬韓森（左，圖為法國大導演盧貝松在臺灣取景的《露西》電影劇照）等女星都是 DeepFake 的受害者。（Photo Credit: Warner Bros., DC Films., EuropaCorp, Universal Pictures）



臉書（Meta）與微軟曾共同舉辦過「DeepFake 偵測競賽」，希望透過競賽收集全球專業人士針對偵測偽造影像視訊內容的演算法，以提升偵測 DeepFake 的技術；其中，最佳的演算模型偵測準確率高達 82.56%。（Source: Meta AI, https://ai.facebook.com/datasets/dfdc）

一、透過區塊鏈技術，在數位影音檔案中內建一份對應的證明書，證明該檔案是由安全且經過認證的作者所產生。當使用者要瀏覽該檔案時，經由檢查證書而確認該檔案沒有被第二手加工過，並得以瞭解作者相關資訊。採用區塊鏈技術，可以不需要中央伺服器的存在，以分散式作業的方式，能提高認證效率。

二、採用類似防毒軟體或電子郵件過濾軟體的處理方式，預先過濾所有多媒體影音檔案，並經由數位影像技術偵測是否有明顯的人為操縱痕跡，若有的話則自動將其分流至隔離區。這作法類似許多郵件處理系統會將垃圾郵件主動搬至垃圾郵件夾中，此舉能避免這類被判定為有疑慮的影片進一步散播。

「資訊戰」時代來臨，全民媒體素養為首要

雖然偵測技術持續進步，但同樣的，DeepFake 影片也會「吸取教訓」來改良既有程式碼，因此要發展出一套能夠百分之百辨識媒體內容真偽的技術仍有發展空間。

民主制度是優點但同時也是弱點，威權政體利用民主國家包容言論的特性，散播假消息，進而造成內部動亂，使這些國家不戰而敗。因此，在尚未開發出完美的偵測軟體以前，最好的方式還是仰賴所有網路使用者的自我審查，對於可疑影片不隨意散播，以避免無意中助長了惡意擴散。「資訊戰」時代已經來臨，大眾媒體素養的全面提升，才是有效杜絕 DeepFake 影片損害的最大關鍵。