無人機——新興科技還是威脅？

◆ 社團法人台灣 E 化資安分析管理協會、輔仁大學人工智慧與資訊安全學程、台南應用科技大學資管系教授 — 李俊達

2022 年臺灣燈會在高雄，其中最吸睛的當屬在愛河灣展區由 1,500 架空拍機展演的「聚光台灣 · 虎星高照」。適逢虎年，臺灣民俗中虎爺有為人民除煞、抗疫、祈福之用，結合臺灣重金屬樂團，讓無人機展演的虎爺，以飛行巨吼之姿震撼全場！

無人機的運作

無人駕駛的航空器（unmanned aerial vehicle, UAV），或稱 Drones，是一種能藉由遠端或車載電腦進行控制的飛機。Drones 可以自主導航無需人類控制，由數種 IoT 的智能設備所組成，如光脈衝距離感測器（雷射）、無線電檢測和測距感測器（radio detection and ranging sensor）、磁場變化感測器（magnetic-field change sensor）、聲納距離感測器（sonar-pulse distance sensor）、飛行時間（Time of Flight, ToF）感測器、熱感測器（thermal sensor）、化學感測器（chemical sensor）及方向感測器（orientation sensor）等。隨著無人機內部各種設備（處理器、微控制器、感測器、無線收發器）的小型化，許多物聯網技術也隱含於其中，使得無人機網路（Internet of Drones, IoDs）也成為 IoTs 的一部分。一般而言，無人機網路是由 4 種不同的

2022 年臺灣燈會展演主題之一「虎嘯迎春　威武除煞」，透過 1500 臺無人機主燈呈現在地民俗文化。（圖片來源：高雄市政府 FB 粉絲專頁，https://m.facebook.com/bravo.Kaohsiung/photos/pcb.5016013738460216/5015840491810874）

工作角色所組成，分別為地面站伺服器（ground station server, GSS）、遠端無人機（remote drone, RD）、控制室（control room）及具授權之使用者（authorized user）。

無人機除了實現即時影像截取外，也能進行飛行與運輸貨物的能力，甚至可在特定人多的區域作為無線寬頻存取的熱點使用。因此，近年內已有超過百萬架無人機被投入商業使用。由於無人機結合 IoTs 各式的感測元件、定位服務、無線傳輸讀取、內容服務等技術，衍生出許多不同型態的無人機應用。

無人機的應用範圍

一、民間用途

1. **攝影用途**：讓電視／電影製作人透過無人機以前所未有的方式進行空中攝影，從而將鳥瞰圖提升到另一個新的高度。

2. **自然災害評估與控制用途**：2005 年卡崔娜颶風侵襲美國後，無人機就被用於災害控制與評估，可掌握何處的道路被倒

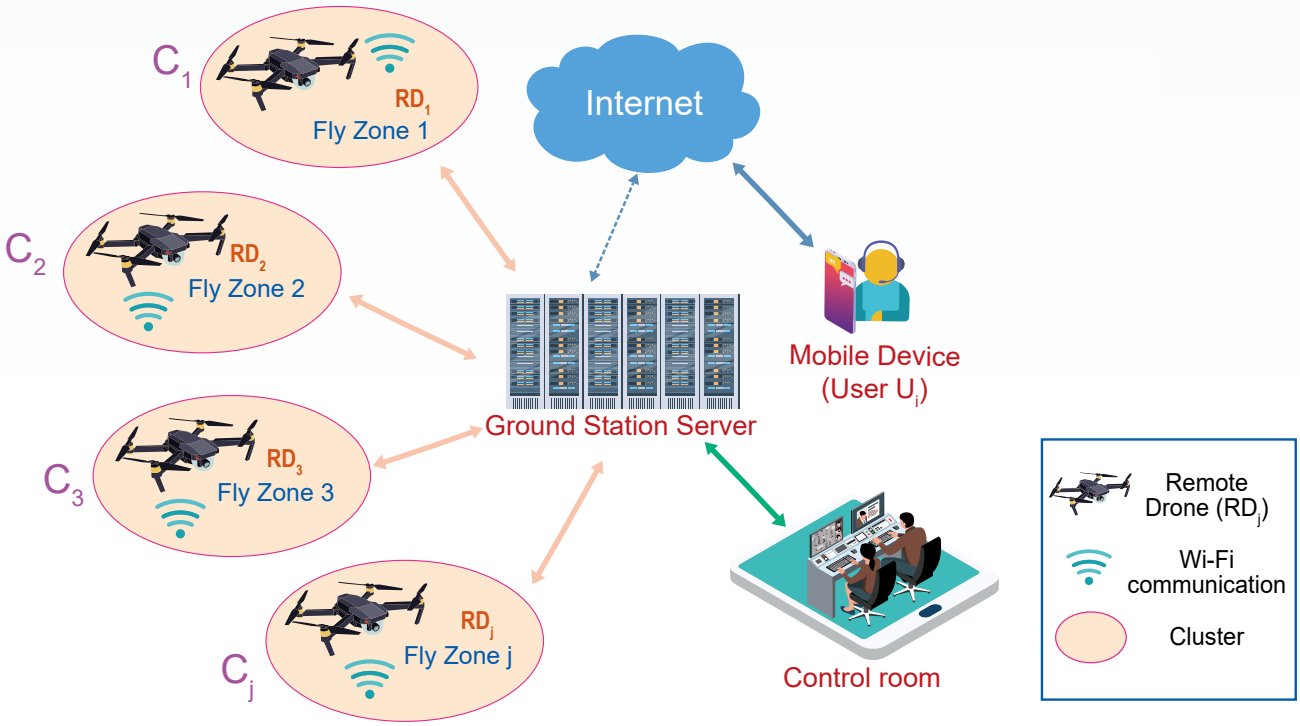


圖 1　無人機網路運作圖

2004 年敏督利颱風降下豪雨造成嚴重土石流，使位於臺中的松鶴部落大量民宅被毀；2009 年 8 月莫拉克颱風在臺灣造成半世紀以來最嚴重的水患；兩者的山體崩塌、災害情形及周遭環境，皆可從空拍影像探知。（圖片來源：水土保持局，https://photo.swcb.gov.tw/Repository/ViewEvent?eventid=637813996118950097；https://photo.swcb.gov.tw/Repository/ViewEvent?eventid=636779791187354519）

下的樹木、汽車、道路障礙等阻塞，或被用來檢視失蹤情況、受傷及受困的民眾等。

3. **搜尋與救護用途**：無人機可被用於搜尋失蹤、散落或滯留的人，尤其是當人們處在危險或受限無法動彈的環境時。

4. **旅遊用途**：無人機可被用於捕捉令人驚嘆的美景，如風景鳥瞰圖，以吸引遊客並促進旅遊景點及名勝古蹟的觀光。

5. **商業廣告用途**：無人機可被用於拍攝商業廣告，因它們可在特定的時間拍攝具有高清（HD）質量的場景，也能減少對昂貴設備和人機互動的需求。

6. **危機管理用途**：當發生恐怖攻擊或自然災害的情況下，無人機可被充當成熱點或基站（base station），進一步地收集受影響人員所發送之訊息或用於向特定人員發出警報。

不同於傳統登山或乘坐直升機的拍攝方式，無人機能捕捉令人驚嘆的空拍美景，猶如俯瞰世界的上帝之眼。

7. **緊急應變用途：**就像救護車一樣，無人機也可作為行動醫療包，發送醫療物資給現場急救單位，尤其當現場車輛無法通行的情況下。此外，無人機還能用於提供受困者食物，或減少在大型傳染病流行期間的人與人接觸。

8. **環境監控用途：**無人機可被用於執行環境汙染測量的任務，如空氣品質測量與分析；農業任務，如土壤分析、農作物／牲畜管理／病患害防治；動物保護任務，如自然／野生動物保護／反盜獵／瀕危物種保護等。

無人機可作為行動醫療包，發送醫療物資給現場急救單位，或遠距離提供受感染患者食物及藥物，減少人與人的接觸。

9. **水下及海事用途：**水下無人機或無人海洋飛行器（Unmanned Ocean Vehicles, UOV）可被使用在水下搜尋與救援行動，另外也能針對海洋或沿海環境進行數據收集，以檢測或監控海洋動植物之數量。

二、警界用途

1. **交通監控用途：**無人機可被用於監視交通和事故現場，如自 2015 年來，被西班牙政府用於監視交通瓶頸點的情況。

2. **罪犯追蹤用途：**可被用來監視犯罪現場和監獄逃犯，如 2016 年，美國俄亥俄州警局使用無人機追蹤一名逃脫的囚犯，並將他追捕到案。

3. **法醫搜救用途：**可被用於解決犯罪事件，如 2015 年 Tara Grinstead 女士的失蹤謀殺案，喬治亞州的警察使用一款名為 Spectra 的固定翼無人機來搜尋她的下落。

無人機在農業任務領域具有優勢，不僅作業資源成本低，防治效率高，亦可遠距離遙控操作，增強安全性，經濟效益非常顯著。（圖片來源：行政院農委會農業試驗所，https://www.intelligentagri.com.tw/xmdoc/cont?xsmsid=0K303431216608203659&sid=0L207556862169758218）

以色列國防軍和警察使用小型無人機，向抗議群眾投擲催淚瓦斯以驅散示威者。（圖片來源：路透社／達志影像）

4. **防暴動用途**：可被用於反抗議活動中，如 2015 年印度警方考慮使用配備胡椒噴霧的無人機；2018 年以色列國防軍和警察使用攜帶催淚瓦斯的無人機從以色列和巴基斯坦的邊界驅散抗議示威者。

三、軍事用途

1. **空中監視／偵察**：無人機可被部署在空中進行情報與訊息的收集，進一步地識別和追蹤恐怖分子的營地、車輛、武器、工廠、簡易爆炸裝置位置等資訊。

2. **空襲**：早在 2002 年美國即利用無人機進行空襲任務並將其發展在全球反恐戰爭中使用。此外，以色列也依靠無人機對西岸伊拉克和敘利亞的軍事設施／關鍵目標／人物等進行空襲。

各國多會依靠無人機進行高空偵察及空襲任務；圖為美國於阿富汗執行作戰任務的 MQ-9 收割者無人機。

3. **無人機劫持**：主要是透過 GPS 干擾／欺騙來劫持另架無人機，曾用於抵抗伊斯蘭國威脅。

4. **躲避雷達探測**：無人機另一個軍事目的是避免雷達探測，如英國「火影」無人機，能夠逃避雷達檢測系統，並攜帶自毀彈頭進入主要的目標區。

四、犯罪攻擊用途

1. **實體攻擊**：若有意或無意地將無人機撞入人們的財產，會造成對方嚴重損失。例如：2015 年，觀光客的無人機直接撞擊臺北 101，幸好未造成破壞；2016 年，

一架從瑞士飛回倫敦的英國班機，在降落前高度 5 百公尺處，遭到無人機撞擊，所幸平安降落，無人員傷亡。

2. **網路攻擊：**無人機能偽裝成行動 Wi-Fi 網路的熱點，讓使用者連接後，竊取其如帳號密碼與信用卡等敏感資訊，或將惡意軟體植入到已連接至此惡意熱點的智慧型手機與行動設備。此外，透過樹莓派（Raspberry Pi，平價單板電腦）連接到無人機也能對它進行惡意編碼植入，以攔截或劫持附近其他的無人機。

是助益還是威脅？

從安全和威脅分析的角度來看，本文針對無人機網路系統之 5 項組成元素（使用者、無人機平臺、無線連接、雲端服務、應用層）歸納出各別可被利用之安全缺口及安全保護策略，詳如表 1。

新興的無人機技術對人類而言是助益還是威脅呢？這個問題就如同「水」一樣，水能載舟，亦能覆舟。將新興科技用於「對的事」，那就是一種助益；反之，若應用於「錯的事」，那就是一種威脅。

表 1　無人機網路系統之安全缺口及保護策略

系統元素	安全缺口	安全保護策略
使用者 User	· 非授權之存取 · 弱認證 · 社交工程 · 逆向工程 · 無意的錯誤	· 點對點加密 · 實體安全保護 · 較強的授權機制 · 較強的認證（多因子） · 設備識別
無人機平臺 Drone Platform	· 惡意病毒與軟體 · Rootkits 隱藏碼及後門 · 字典及暴力猜測攻擊 · 埠掃描（port scanning）	· 實體保護 · 關閉不需要的埠 · 較強的密碼保護策略 · 三 A 安全機制
無線連接 Wireless Connection	· 中間人攻擊 · 監聽 · 通訊流量分析 · IP/MAC 位址欺騙 · ARP 欺騙	· 加密機制 · 雜湊保護 · 防火牆 · IPS/IDS · 存取控制的更新
雲端服務 Cloud Services	· 勒索軟體 · 間諜軟體 · 缺乏 accountability · 缺乏 security 機制 · 明文密碼	· 提高認知 · 維護資料機密性 · 維護資料完整性 · 簽署保密協議 · 簽署使用者隱私協議
應用層 Application Layer	· 應用劫持 · 偽裝的應用 · 弱 account 安全性 · 弱 authentication 機制	· 多因子認證 · 已驗證／已測試應用 · 用戶意識 · 系統更新與補丁修補

烏克蘭為了抵抗俄羅斯的攻擊，利用無人機空拍偵察，再將其掛載炸彈，鎖定俄國部隊進行飛彈攻擊。（圖片來源：烏克蘭武裝部隊作戰戰術組官方臉書，https://www.facebook.com/otusumy/posts/pfbid041smt87y6cgk9EeEicUzL7D2Mw7g6hrosy8ZweRtysc1bNuz5j8L2hBdAYvDeD9Ml）

在戰場上，烏克蘭為了抵抗強權俄羅斯的攻擊，利用無人機的特性，對地面進行空拍與情資的偵察，了解俄軍的一舉一動，最終再將無人機掛載炸彈，鎖定俄國地面部隊及海面上的艦艇進行飛彈攻擊，造成俄軍人員及戰鬥裝備巨大損失。在此，無人機技術對烏克蘭來說是助益，因為他們利用新興技術有效阻礙俄羅斯的入侵。

由於無人機已快速且全面地融入現今社會，因此，臺灣在發展無人機各式應用的過程中，除了應積極開發更安全成熟的無人機模組與易於操作的飛行控制技術外，也需針對無人機各種不同的服務應用模式，擬定其相對應之管理機制，以避免無人機墜落傷人、撞上建築及毀損私人財產、威脅航空安全等事件發生。

另一方面，當在擴展無人機應用服務市場時，如何保護民眾安全及隱私亦是一項重要議題，建議相關權責單位應建立完備的納管及監理機制，如：制定無人機飛行安全規則及飛行管理處罰條例、建立禁航及限航區、適航路線申請、無人機操作員技術考核、無人機機體安全檢驗機制、無人機專屬頻段設置、民眾安全及隱私權保護等。最終，讓無人機的各式應用發展能有效地改善人民的生活品質，而不是成為人民生活中的威脅。

社團法人台灣 E 化資安分析管理協會（ESAM）

臉，為何會被挖走？深度偽造（DeepFake）介紹

◆ 調查局資通安全處 ── 雷喻翔

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=2tgqX5WVhr0.

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/2tgqX5WVhr0）

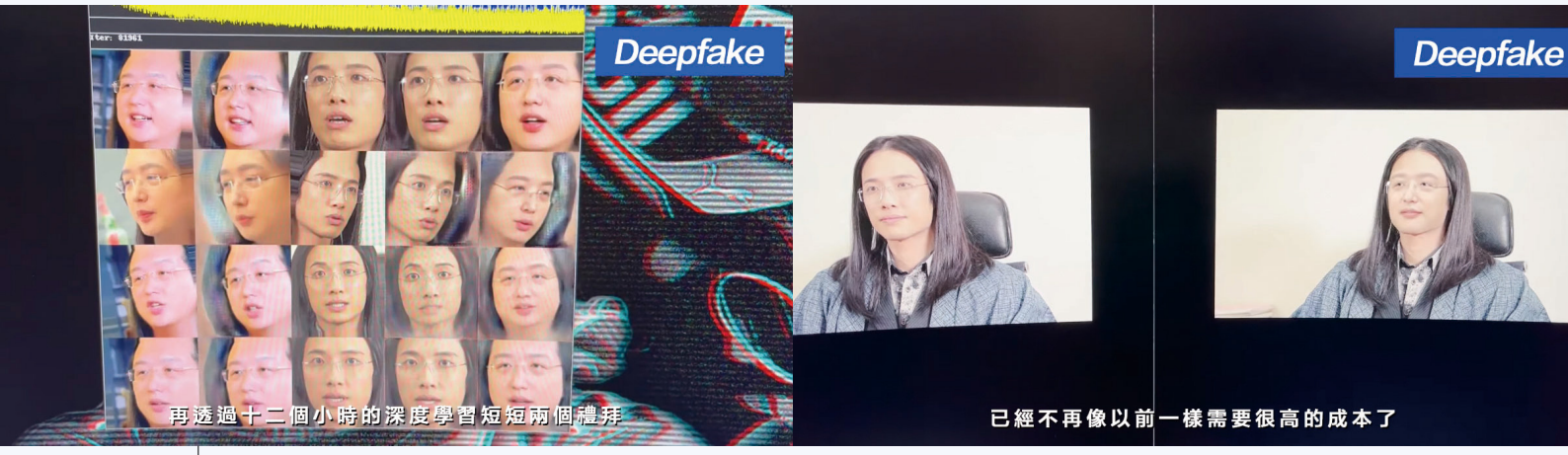
何謂 DeepFake 技術

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。

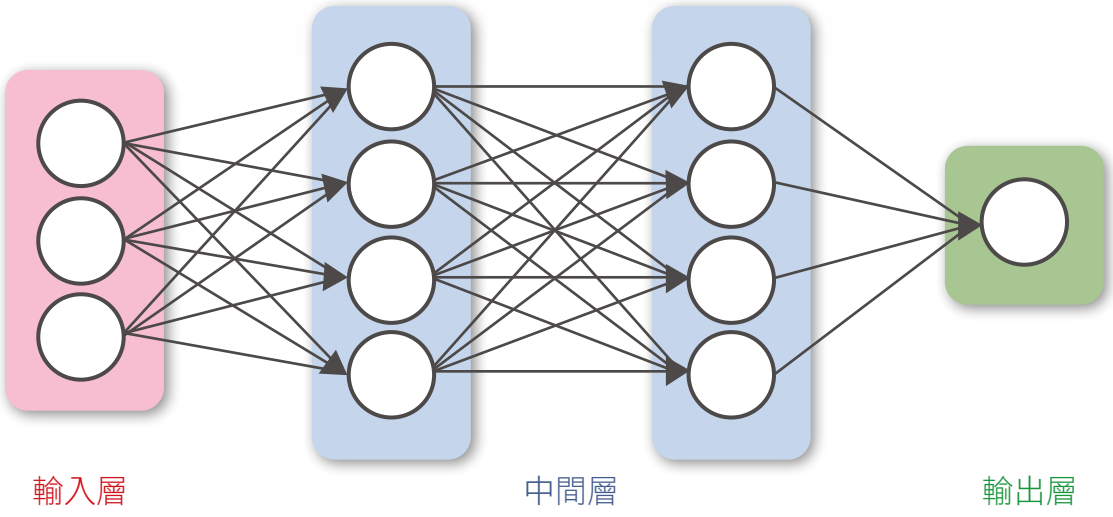


圖 1　神經元傳遞層級示意

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」進軍抖音？　靠 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？影片後製謠言》，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　連川普與律師都散播》，https://www.ettoday.net/news/20190524/1451830.htm。

左圖畫面右側為韓國首位 AI 主播，以左側的主播金柱夏為原型；工作人員只要鍵入文字稿，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/Fo33gOcKKSU）

將川普置入《絕命毒師》影集，談如何洗錢的 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/Ho9h0ouemWQ; Breaking Bad & Better Call Saul, https://youtu.be/RhsUHDJ0BFM）

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》為美國電視連續劇，講述高中化學教師的犯罪故事。其因患上肺癌末期，龐大的醫療費用讓絕望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），在拜訪沙烏地阿拉伯時驚傳就醫，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。

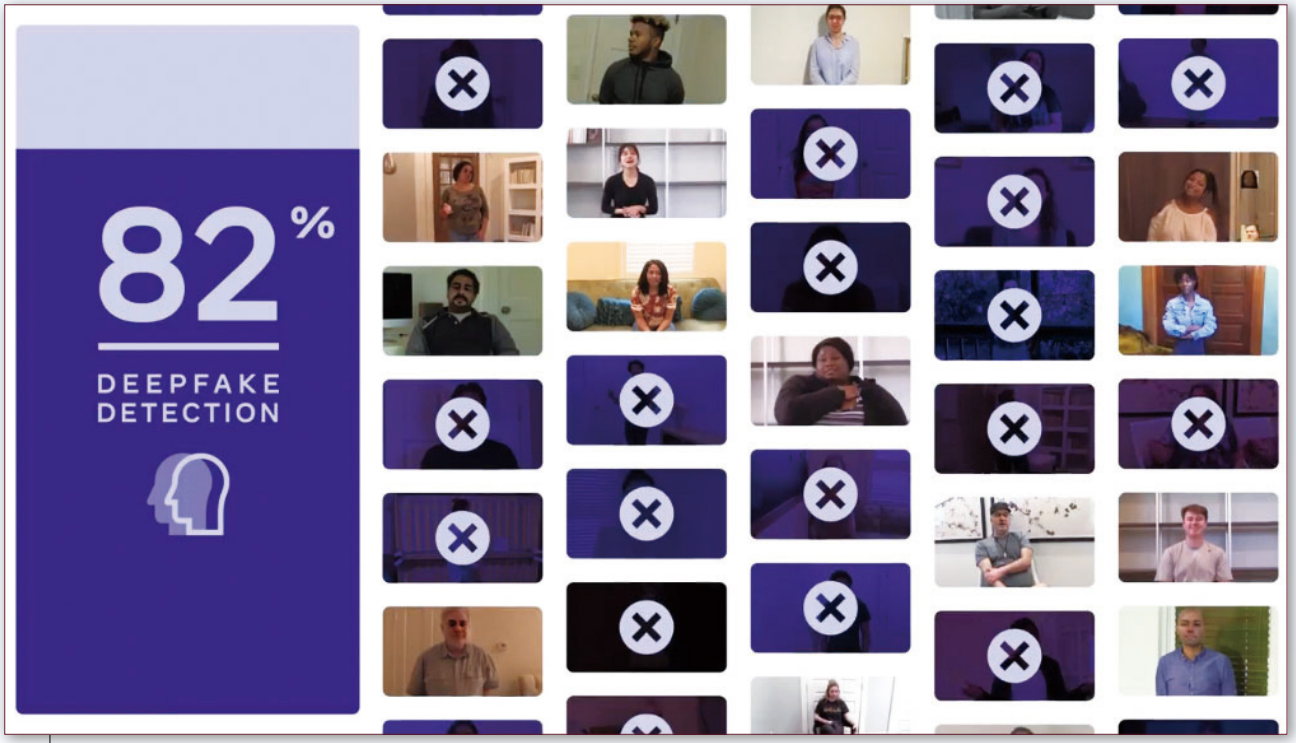
自動屏蔽 DeepFake 影片技術

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）

[9] 《逾 9 成明星 A 片都是假的，「深偽色情」一般人更難防》，https://www.aibooksbank.com/news/content/3A34CF908C10819930420B117A13A229。



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。