後疫情時代之闇黑勢力入侵

網路闇黑勢力入侵，伴隨假訊息流竄等危機，
政府資安鐵三角聯防機制已啟動，
秉持人權與安全並重，繼續大步前行。

捍衛網域國境 腳步從不停歇

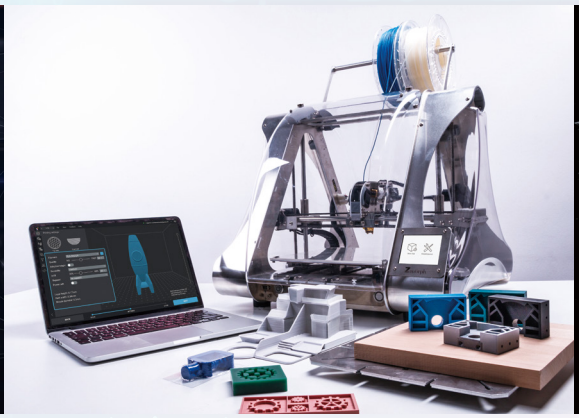
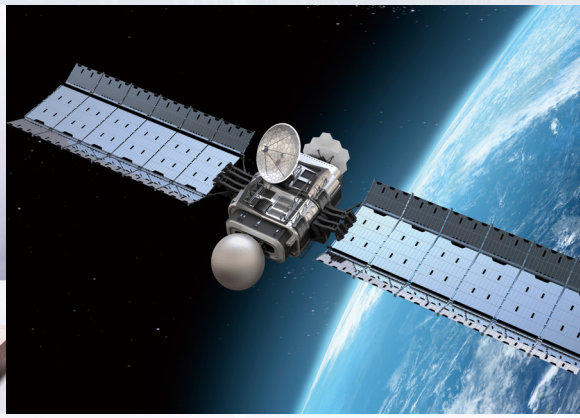
／調查局資通安全處　蘇　羣

資訊科技發展日新月異，多元資安威脅與日俱增，不法駭侵犯罪邁向產業化，調查局力抗駭侵狂瀾。

如果您佇立門外仔細聆聽，有個聲音在耳邊悄悄迴盪，彷若手法純熟的演奏家正此起彼落敲著琴鍵，奏鳴出未曾聽聞的旋律，您可能會疑惑，這篇樂章截至目前為何始終在細膩鋪陳著前奏，潛藏的思緒與情懷卻難以捕捉，是刻意按捺？是意境延伸？突然一聲動人心魄的重音，將樂章瞬間畫下句點，回歸瀰漫著詭異的寧靜。

如果您佇立門內睜大雙眼，原來有個人影在螢幕前映著藍光，彷若全神貫注的演奏家，敲的卻是鍵盤，在螢幕上奏出一行又一行的指令及程式碼，而非耳中輕快跳動的音符，您會驚覺方才的綿長鋪陳竟是潛伏的惡意，待萬事即將俱備、大功即將告成之際，眼前人影突然使勁敲下「Enter」鍵，螢幕中滿布駭侵而得的戰利品，嘴角的訕笑無情地諷刺著彼端的血淚。

或無能為力，或力不從心嗎？這般景象恐愈發頻繁地在世界各地上演，但大多數的人往往無所知覺已然受駭，資安技術與防護概念似如一扇高聳冷冽的大門，不得其門而入，今天就讓我們一起試著推開這扇門吧。

未來 5G 網路將全面布建，萬物皆可聯網，虛擬貨幣、自動駕駛、太空開拓、3D 列印生產技術等事物，流通串聯的是難以計數的資訊流，然而其中的黑暗面值得引起我們的思考與重視。

新資訊時代蓬勃發展

網路科技數十年來席捲了整個世代的變革，為人們的生活帶來無窮的便利與品質的提升，然而網路等資訊科技的影響真正開始從資訊業巨幅外溢、甚至更為深入地滲透人們生活中所行所為，則在近幾年來愈發顯著；根據 FRED 數據，資訊產業中數據儲存處理分析相關服務及其他新興資訊服務從業人數，在近十年來成長至少一倍以上；尤其在今年新冠肺炎疫情爆發以來的這段期間，實加速了諸多產業的數位轉型，甚至擴及農業、製造業、服務業。

與此同時，我們似乎已可望見未來世界的藍圖逐漸清晰，5G 網路的全面布建、萬物皆可聯網、區塊鏈技術帶來零信任交易基礎的智慧合約及虛擬貨幣、普及的自動駕駛車輛與飛行器、太空開拓與衛星網絡的建構、跳脫人力框架的 3D 列印生產技術、自線上愈趨落地的社群網絡；在不遠的未來，你會發現身處的世界、手邊之物，彼此緊密的串聯著，流通的是難以計數的資訊流，然而在與嶄新未來接軌的此時此刻，有些黑暗面令我們不得不開始思考與重視。

資安威脅與日俱增

一、全球發生資安事件之產業分布

根據 Statista 針對全球產業機構去（108）年發生資安事件之統計（來源：Verizon），3 萬 2 千餘件中即有約 6 成以

上，集中於資訊產業、公共部門、專業技術服務產業（如研究室、管理顧問等），均係科研技術密集、持有機敏資料之單位；大型規模之機構受駭案例則有約 7 成集中於公部門，而小型規模之機構受駭案例則有 5 成集中於金融、醫療、資訊、公部門等產業。

Incidents:	Total	Small	Large	Unknown
Total	32,002	407	8,666	22,929
Accommodation (72)	125	7	11	107
Administrative (56)	27	6	15	6
Agriculture (11)	31	1	3	27
Construction (23)	37	1	16	20
Education (61)	819	23	92	704
Entertainment (71)	194	7	3	184
Finance (52)	1,509	45	50	1,414
Healthcare (62)	798	58	71	669
Information (51)	5,471	64	51	5,356
Management (55)	28	0	26	2
Manufacturing (31–33)	922	12	469	441
Mining (21)	46	1	7	38
Other Services (81)	107	8	1	98
Professional (54)	7,463	23	73	7,367
Public (92)	6,843	41	6,030	772
Real Estate (53)	37	5	4	28
Retail (44–45)	287	12	45	230
Trade (42)	25	2	9	14
Transportation (48–49)	112	3	16	93
Utilities (22)	148	5	15	128
Unknown	6,973	83	1,659	5,231
Total	32,002	407	8,666	22,929

Table 1. Number of security incidents by victim industry and organization size

我們可以初步研判，小規模但提供重要服務的機構可能因資安防護的能量較為不足，易成為駭侵犯罪得手的目標；而大規模機構通常擁可觀預算及人力，能夠實施較高的資安防護水平，因此一般較不易成為駭侵目標；但是大規模的公部門機構，可能因內部資料較為機敏、資料結構品質完整、運用價值高，甚至可藉其獲利或以攻擊遂行政治上的訴求及目的，而遭到不法人士的鎖定。

二、 社會矚目案件

我們已可在新聞報章媒體上看到，電腦、網路的駭侵犯罪已經不僅止於資料遭竊，而是搭配服務阻斷及勒索、社交工程及詐騙等複合式攻擊手法，諸如「第一銀行詐領案」、「銓敘部個資遭駭案」、「臺大醫院病歷遭駭案」、「衛福部及醫療院所遭植入勒索病毒案」、「全球殭屍網路 Necurs 不法案」、「政府機關遭 DDoS 攻擊案」、「某

根據統計資料顯示，全球產業機構 108 年發生的資安事件中，3 萬 2 千餘件中即有約 6 成以上，集中於科研技術密集、持有機敏資料之單位；大型規模機構受駭案例則有約 7 成集中於公部門，而小型規模機構受駭案例則有 5 成集中於金融、醫療、資訊、公部門等產業。（Source: Statista, Verizon, https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf）

新聞上常見的電腦、網路駭侵犯罪不僅止於資料遭竊，還搭配服務阻斷及勒索、社交工程及詐騙等複合式攻擊手法，鎖定目標集中於擁有機敏資料、提供民眾關鍵服務的機構及企業。（圖片來源：截自東森新聞，https://youtu.be/sd1vugUHhqU，https://youtu.be/Z8RK5w2MmWw）

公司遭植入勒索病毒」、「某公司營業秘密遭竊」……等案例不勝枚舉。

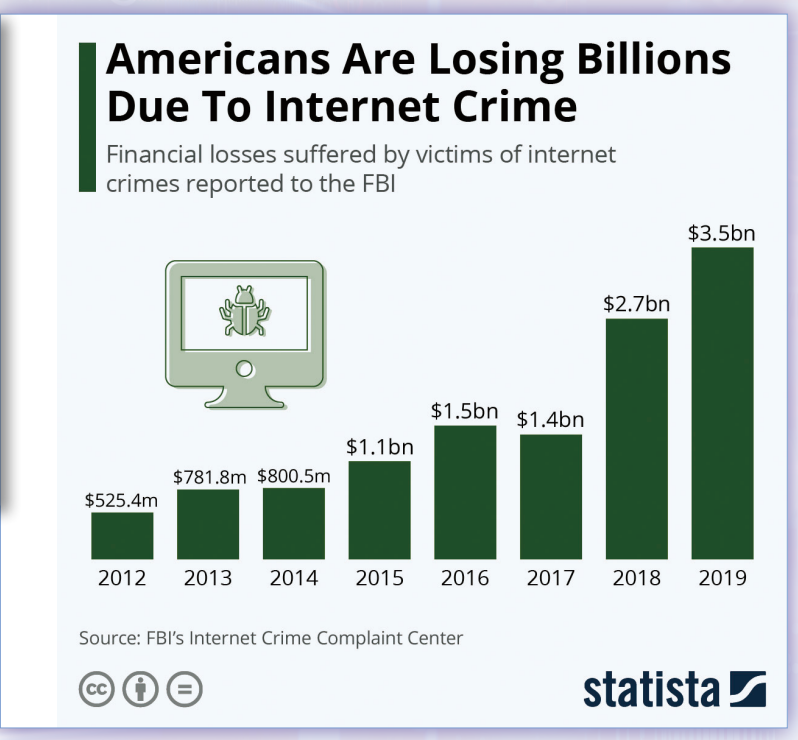
對於一般人或企業來說，最為迫切相關的大概就是個資遭竊、信用支付遭盜用、各種服務癱瘓、商業匯款郵件詐騙、勒索病毒損失等狀況，除影響生活所需及便利性外，更造成實質上的損害。同時我們也可以看到，惡意駭客鎖定的目標，確如統計所述的集中於擁有機敏資料、提供民眾關鍵服務的機構及企業。

三、駭侵犯罪規模及肇生損害顯著攀升

根據 Statista 針對近年來的網路犯罪（來源：FBI 所屬 IC3 的網路犯罪報告）損失金額統計，僅去（108）年即高達至少 35 億美元，相較於 8 年前水準竟有將近 6 倍之漲幅，且連年呈現高度成長的態勢。

經綜合多項統計資料，我們可以發現，近年來資安事件除數量顯著增加外，相應的損失更為驚人攀升，可見網路駭侵犯罪隨著時間的演進，其商業模式、產業鏈、獲利手法已然成形且組成龐然的分工結構，同時更具有針對性、目的性，只要有利可圖，不論是個人、法人、公部門均可能成為駭侵的目標。

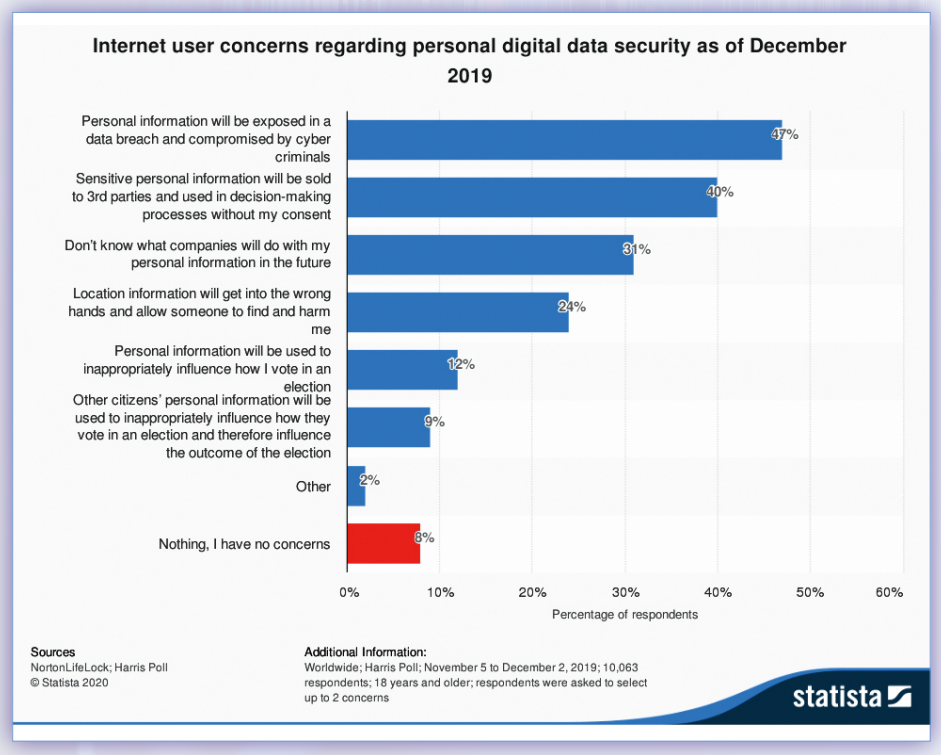
根據 Statista 針對全球網路使用者進行抽樣調查（來源：NortonLifeLock; Harris



Poll），約有 5 成的人擔心個人資訊遭駭客違法取得利用，約有 2 成多的人擔心位置遭暴露致遭人不當利用及出現安全疑慮，約有 1 成的人擔心個人資訊遭利用於影響政經決策傾向。

在現代資安事件層出不窮的背景下，民眾開始逐漸意識到，原來資訊安全是如此的重要，小則危害個人身家安全，中則影響企業經營運作，大則撼動政經體制平衡。

據 FBI 所屬 IC3 的報告統計，2019 年美國因網路犯罪損失的金額高達至少 35 億美元，相較於 8 年前水準竟有將近 6 倍之漲幅。（Photo Credit: Statista, https://www.statista.com/chart/20845/financial-losses-suffered-by-victims-of-internet-crimes）



由全球網路使用者抽樣調查來看，在現代資安事件層出不窮的背景下，民眾開始意識到資訊安全小則危害個人身家安全，中則影響企業經營運作，大則撼動政經體制平衡。（Photo Credit: Statista, https://www.statista.com/statistics/296700/personal-data-security-perception-online）

駭侵犯罪攻擊趨勢

近期的駭侵犯罪及攻擊的型態與未來趨勢將是如何呢？我們可以想像有一間賣餅乾的公司，專長就是做餅乾，在上市開賣前的第一步當然就是先調查看看消費者喜歡吃什麼口味，再針對能引發消費者食慾又難以抗拒的口味進行開發，除了巧妙精緻的包裝外，少不了專業的行銷宣傳，不論是廣發傳單、置入性行銷，甚至是強迫推銷都在所不惜，接著利用像是便利商店般的廣大通路送到每位消費者的手上，如果不夠還可以雇用狂熱的業務員，甚至租用攤販、自動販賣機 24 小時營業。

如果有人拒吃這家公司的餅乾，可能會被業務員盯上，以各種花言巧語騙稱吃了會瘦，同時為取信消費者自己還吃上一口……消費者荷包因此被掏空也就算了，但他們還可能在你停車的時候偷偷上車輪鎖，留下紙條表示不付錢就不解鎖，嚴重的話還可能被一群凶神惡煞包圍到無路可逃，最後只得被迫付錢買餅乾。

是不是覺得這間餅乾公司很惡質？讓我們換個情境，這間公司其實就是駭客不法集團，專長撰寫惡意程式，在做案之前，會先偵測檢閱看看哪些系統、軟體、機構有資安漏洞，再針對這些漏洞開發破解的駭侵手法，或將惡意程式碼巧妙包裝、隱匿於看似無害的文件或檔案裡，透過廣發垃圾郵件、惡意連結、包裹在民眾常用的網路服務裡，散播到大家的手機及電腦，有時更針對系統漏洞強行將惡意程式注入到設備中，如同強迫推銷一般；再者，還可以操控為數眾多的殭屍網路，不夠的話甚至還能找其他駭客租借，以各種通路散布出去，24 小時不間斷，若是有人具備不錯的資安觀念，拒病毒於門外，亦可能被駭客盯上以社交工程、假造郵件鎖定詐騙，一不留神恐損失慘重，還可能被注入勒索病毒，將電腦檔案加密無法使用，不付比特幣就無法解鎖，嚴重者可能還被 DDoS 阻斷式攻擊，癱瘓網路服務，甚至遭到鉅額勒索。

現在的電腦、網路駭侵犯罪已經形成穩固的地下產業結構，擁有清晰的商業模式及獲利方法，高度組織化、多層次分工，只要有利可圖，不論是販售個資、機敏政府資料，詐騙勒索，取得市場競爭優勢等，都能接受委託或主動出擊，即使目標資安防護固若金湯也無法阻擋其駭侵意圖，有些駭客不法團體背後甚至有國家那雙看不見的手，意圖撼動國際政經情勢。

調查局力抗惡意駭侵狂瀾

為了應對這場沒有煙硝的嚴峻戰爭，調查局在今（109）年成立資安工作站，集結資通專業人力、整合司法調查能量，在資安事件、駭侵犯罪發生之際，即能迅速發動偵辦，遏止犯罪行為持續擴散，有效減輕損害及後遺，發揮「主動偵查、打擊犯罪」的能力，為落實我國資通安全戰略立下一個新里程碑。

蔡總統在「國家資通安全戰略報告」提出「資安即國安」，甚至在今年公開表示「資安成為新政府重點核心戰略產業」，就是為了建立並完備「國家資安聯防架構」，在國安單位及政府各部會的合作下，提升「早期預警、緊急應變、持續維運」的能量及效率。

調查局將本於資安專業技術，成為我國資安執法先鋒，擔任我國網域國境安全

電腦、網路駭侵犯罪已形成穩固的地下產業結構，擁有清晰的商業模式及獲利方法，且高度組織化與多層次分工，有些駭客不法團體背後甚至有國家撐腰，意圖撼動國際政經情勢。

調查局在 109 年 4 月成立資安工作站，集結、整合資通專業人力與司法調查能量，有效遏止駭侵犯罪發生與擴散，為我國資通安全戰略立下新的里程碑。（圖片來源：總統府）

維護之「資安尖兵」！只要民眾、企業、公家機關察覺到有可疑駭客行為，不論是收到夾帶可疑檔案的電子郵件、商業匯款電郵詐騙、偵測到可疑來源駭侵攻擊，甚至是發現有大筆不法個資或政府機敏資料遭到販售及利用，都可以向調查局檢舉通報，共同協力杜絕不法駭客。

結語

大家平時除了須培養良好的資安觀念外，更要在生活與工作中實踐，注意使用的手機、電腦應用程式版本是否都有即時更新，網路連線（尤其使用 WIFI）時是否安全，點閱郵件及瀏覽網站時，是否有謹慎確認來源、排除可疑風險；企業及公部門亦要全面檢視自身的資安威脅，以風險為導向進行評估，建立符合需求的資安防護體制。

同時，本局的每一位成員必將竭盡所能，讓正義的輝芒照映駭客門內的黑暗，打擊惡意的潛伏、終止無情的訕笑，誓言劃下駭客不法樂章最後的句點。

後疫情時代的雲端資料安全管理

／科技大學講師　魯明德

2020年是企業對內部資訊管理的一個轉捩點，受到新冠病毒（COVID-19）疫情的影響，人們的工作模式也有了另類的思考。

疫情的衝擊

有些公司為了降低辦公室的人員密度，規劃輪流上班，甚至推動員工異地上班、在家上班等措施，以避免可能的感染對公司的營運造成衝擊；各級學校為了讓教學能順利進行，開始超前部署，規劃停課時的遠距教學方案。

但是，不論是異地上班、在家上班還是遠距教學，所要面臨的都是「從外部存取資料」的安全問題，因此，如何建置一個安全的系統，就成了當務之急。

雲端平台的趨勢

以往的觀念為了資訊的安全，最好是把所有的資料建在自己能控制的平台上，當面對異地存取資料的需求時，這個方法就面臨挑戰了。雲端運算（cloud computing）是近年新興的技術，使用者只要透過網路登入伺服器（server），就可以操作各項工作。而雲端平台的服務就是一個基礎建設，未來它就像水、電等公共系統一樣，只要接上就可以使用服務。

因應疫情衝擊，各公司、學校規劃在家上班、遠距教學等方案，均面臨從外部存取資料的安全問題，因此建置安全的系統成為了當務之急。

圖 1　雲端架構

（圖表內容：作者提供）

雲端安全聯盟（Cloud Security Alliance, CSA）針對雲端運算所面臨的資訊風險，提出建立雲端運算安全架構的方法，包括了雲端架構（cloud architecture）、雲端治理（governing in the cloud）及雲端營運（operating in the cloud）層面。

在雲端治理方面，主要關注在以下 5 項資訊安全領域的問題：企業治理與風險管理、法律上的契約與電子證據、法規遵循與稽核管理、資訊管理與資訊安全、相互運作與可攜性。

而大多數使用者所關切的雲端營運在技術面上的安全議題不外乎是：業務持續與災害復原、資料中心營運、資安事件應變、應用程式安全、加密與金鑰管理、權限識別與存取管理、虛擬化、安全即服務。

資料放到雲端是否安全？

雲端運算的概念已提出多年，相關的技術、服務均已趨成熟，然而，雲端運算仍是架構在既有的資訊科技（information technology, IT）之上，因此，傳統資訊系統所面臨的資訊安全議題，在雲端依然會出現。

企業導入雲端運算之後，在資訊管理上面對的問題，將會從企業內部延伸到利害關係人，資料放上雲端的目的在共享，因此，存取的使用者變多，所衍生的資訊安全問題也變多。

圖 2　雲端資料存取方式

（圖片來源：作者提供）

雲端資料所產生的資訊安全風險可歸納為 3 方面：網路、資料安全、資料管理，網路風險可透過防火牆、實體隔離等技術予以解決，以下將探討資料安全與管理上的問題。

一、雲端資料安全

資料放上雲端，可方便利害關係人下載閱讀，如企業的產品或零件設計圖可以放在雲端，讓供應商可以直接下載，以評估內容進行報價。法院的訴訟資料，也可以放在雲端，讓兩造的律師自行下載，以減少人員奔波。

但是，資料的擁有者可能會擔心：雲端資料是不是會被不相干的人下載、閱讀、重製、散布？當然，資料存在雲端，它占有一定的空間，既然占有空間，就不可能不被不相干的人看到，因此，在資訊安全上要做的不是不被看到，而是看到也看不懂。

當資料擁有者要將資料存放到雲端時，並不是存放明文（plain text）資料，而是存放一個經過加密後的檔案，明文資料經由一個加密函數以使用者的金鑰加密才能上傳，因此，雲端上存放的產品或零件圖、訴訟文件都是加密後的亂碼，不相干的人即使下載了也看不懂。

當利害關係人下載後，必須要有文件擁有者所給的解密金鑰及當初的加密函數，才能把所下載的資料打開，也就是說，

供應商從雲端下載了產品或零件圖，也同時會拿到解密金鑰；律師在接受委託、申請閱卷時，也會取得一個授權的解密金鑰，以便日後下載訴訟資料時可以閱讀。

文件的使用者在每次打開文件時，解密金鑰都會自動由金鑰伺服器確認有效期，因此，文件擁有者可以控制文件使用者的閱讀時間與權限，如報價期間如果設定為 5 天，則 5 天後供應商就打不開下載的零件圖了；同理，律師在解除委任關係後，金鑰伺服器就會停止金鑰的權限，其下載的檔案亦無法開啟。

二、雲端資料管理

在談資訊安全時，大家都會專注於外部的攻擊，所以要設防火牆、避免弱點被攻擊，但是，往往會忽略內部的合法使用者，所謂外賊易擋、家賊難防，除了教育訓練、管理制度、定期稽核外，雲端資料除了要加密外，每一次的存取都要留下紀錄。

系統建置時，都會設置 log 檔，log 檔會記錄檔案每次存取的資料，如是誰在什麼時候存取了哪個檔案，系統可以定期把異常存取的資料列出，進行檢討、追蹤，可以提早發現問題，防範於未然。

結論

後疫情時代改變了人們的工作模式，資料放到雲端管理已經是未來的趨勢，對於資料放在未知的雲上，很多人都對其安全心存疑慮，然透過加密技術讓資料不被無關的人存取，並記錄每次存取的事件，將可提升使用者對雲端資料存取的信任度。

透過金鑰加密與解密，讓雲端資料的共用與存取更加安全，但除了重視外部攻擊，更別忽略內部的教育訓練、管理制度及定期稽核系統，否則易導致外賊易擋、家賊難防的窘境。

淺談資安風險管理：以遠距視訊為例

／金門縣政府政風處專員　陳大中

資安風險管理為資安防護之基礎，唯有完善的風險管理，方能逐步建構更臻妥適之資通安全防護網。

全臺上網人數已突破 2 千萬

依據財團法人臺灣網路資訊中心「2019 臺灣網路報告」，推估民國（下略）108 年全國 12 歲以上曾上網人數達 1,898 萬人，而全國上網人數（包含未滿 12 歲）已達 2,020 萬，整體上網率高達 85.6%，為歷年最高[1]。換言之，我國各項資訊科技及網際網路不僅日益普及，更有快速發展之趨勢。

公私部門因資安破口，遭受鉅大損害

然隨著網際網路及其他資通科技之迅速發展，亦帶來資訊安全危機，如：銓敘

[1] 109 年 7 月 3 日引用於財團法人臺灣網路資訊中心「2019 臺灣網路報告」，網址：https://report.twnic.tw/2019/assets/download/TWNIC_TaiwanInternetReport_2019_CH.pdf。

107 年台積電設備遭電腦病毒 WannaCry 感染，造成產線停擺，損失慘重。（圖片來源：截自中視新聞，https://www.youtube.com/watch?v=D0ud9d6C2S0）

銓敘部於 108 年 6 月公告接獲外部情資知悉國外網站揭露歷史個資，經確認後掌握外洩資料內容，並下架舊系統，補強現行系統之可疑弱點，全面檢視資安防護。（圖片來源：截自銓敘部官方網站，https://www.mocs.gov.tw/pages/detail.aspx?Node=489&Page=6145&Index=0）

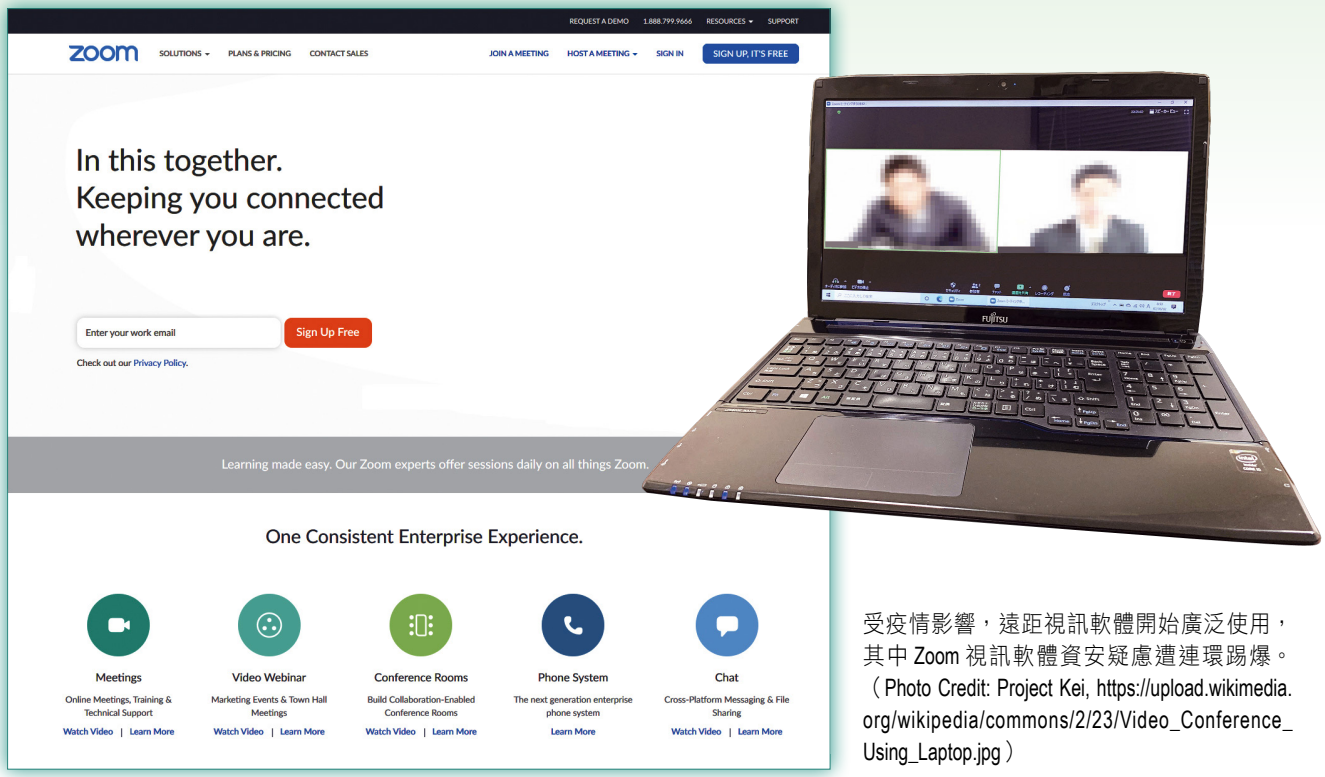
部 108 年 6 月間經報導指出超過 24 萬筆個人資料遭外洩，台積電於 107 年 8 月初設備遭電腦病毒 WannaCry 感染，該次中毒事件影響台積電營收估計新臺幣 25.96 億元（依台積電 107 年第三季財報數據），足堪為我國史上損失最大的資安事件。今年 5 月間不僅國內多家重要能源及科技公司接連遭勒索軟體攻擊，甚至爆發位列資通安全責任等級最高級 A 級之總統府電腦也遭駭客入侵事件。

視訊軟體 Zoom 之資安隱憂

全球因受新冠病毒蔓延影響，遠距視訊軟體開始廣泛使用，其中 Zoom 視訊軟體資安疑慮遭連環踢爆，先是該視訊軟體將加密金鑰存放位於中國大陸的伺服器，有遭駭客竊聽之虞。隨後爆發英國金融時報記者藉由竊聽其他報社運用 Zoom 視訊軟體召開的會議，刺探其他報社之新聞訊息。不僅如此，香港中文大學使用 Zoom 視訊軟體進行遠距考試，系統被不明人士駭入，考試時透過該軟體分享個人電腦螢幕，播放色情成人片、舞曲 MV 等，Zoom 的各種資安事件接踵而來地發生。因此，電動車大廠特斯拉、美國國家航太總署及英國國防部等機構陸續宣布禁用 Zoom 軟體。

資安風險管理步驟

為免更多公、私部門或個人因資安破口，遭受鉅大損害，我國亟待正視資安防



受疫情影響，遠距視訊軟體開始廣泛使用，其中 Zoom 視訊軟體資安疑慮遭連環踢爆。（Photo Credit: Project Kei, https://upload.wikimedia.org/wikipedia/commons/2/23/Video_Conference_Using_Laptop.jpg）

護問題，然資安防護沒有百分之百，不同資通環境，都存在不同的弱點與威脅，只有透過不斷精進，確實做好風險管理，才能將資安風險降到最低，因此，無論是公、私部門或個人，都應確實認識強化資安風險管理，管理步驟有四：

首先，應先識別風險，不論是公務機關、私人機構或個人，均應對其本身及所屬部門之資安風險全貌確實掌握，雖然各部門業務、作業差異甚鉅，可能潛存的風險因子不盡相同，然仍應審酌不同業務屬性，做出可識別的異質性資安風險因子，做好風險識別，是管理的基礎，也是最重要的一個步驟。

其次，進行風險評估，針對資訊資產可能存在的每個資安風險，逐一分析，分析要項包含評估曝險係數、發生可能性、發生時之影響程度、損失預期範圍及處理之優先順序等，確實風險分析與評估，以為後續有效之管理與因應。

第三，深入檢視風險成因，瞭解可能之外在威脅與本身潛存之弱點，透過確實認識可能造成資訊設備、系統危害或威脅之外在影響因素，如系統內容遭駭或遭植入惡意程式，致機密資料遭竊取、竄改，或造成原有之服務不得不中斷等；以及掌握資訊系統或資訊設備本身可能存在的弱點，例如硬體設計存有缺陷、無防火牆設

備、軟體測試不足、內部控制未確實等，唯有全方位檢視風險成因，清楚分辨外在可能危害之威脅與內在潛存之弱點，才能進行有效之相應安全管控或對策，避免損害發生或擴大。

第四，提出最適切之風險因應，當風險經識別出來及評估後，須提出相應之處理計畫，**處理方式大致上可區分為避免風險、轉移風險、降低風險及接受風險**。我們須先思考有無方式避免風險，如無法避免，退而考慮能否轉移風險，若無法避免又無法轉移，就審酌有沒有辦法降低風險可能帶來的影響與衝擊，最後，如果無法處理或需處理成本過於巨大，接受風險，也算是一種選擇。

使用遠距軟體之風險管理

以遠距軟體為例，使用前應提前做好風險管理，其一，選購本身較無資安疑慮之產品，不論公、私部門在使用遠端視訊產品前，均應由資安管理單位或請專業之資安人員，協助全面盤點遠端視訊之同質性產品，了解產品是否符合《資通安全管理法》等相關規定，是否存有將資料回傳

圖 1　資安風險管理步驟

至特定地區之伺服器的疑慮，汰除有資安風險之產品，擇優選用符合規定之遠端視訊產品。

其二，進行遠端視訊會議或教學前，應修改密碼，**避免使用弱密碼，更不得便宜行事，取消密碼**。進行安全性及相關環境設定，落實人員管控，**非屬該次會議或教學之第三人，未經同意，不得進入**。

其三，針對遠端視訊產品之操作人員做好教育訓練，以利視訊之正常進行，遇有狀況，方得以迅速處置。

其四，**凡機密、敏感議題或資料，均不宜於遠端視訊會議或教學使用**，避免不慎洩漏，造成重大損害。透過完善資安防護措施，減少外在威脅及內在弱點，讓風險因子降到最低，持續落實資安風險管理，讓遠距辦公或遠距教學，更加安心踏實。

資安即國安

資訊安全不僅是安全與便利的取捨，更關係整體國家安全與國家利益，近年政府為強化資安工作，陸續完成相關法制作業，然徒法不足以自行，若要達到有效資安防護，就須做好妥善之資安風險管理，並逐步落實資安環境的改善，減少風險的存在，並培養資通使用者之資安觀念及敏銳度，提升其資安防護之素養與能力，如此方能建構更臻完妥之資通安全防護網。

無聲的國安危機——深度偽冒詐騙技術

／勤業眾信風險諮詢服務部門

人工智慧（Artificial Intelligence, AI）演進至今的深度學習（Deep Learning, DL），逐漸地貼近人類最根本的核心需求。然而，商業自動化與智慧化引入資訊與通訊科技，資安威脅自然也隨之而來。根據 2020 資安預測報告[1]，利用 AI 技術進行深度偽冒詐騙（下簡稱「Deepfake」）之手法將大幅提升。或者，遠距工作及連網家庭設備興起，增加駭客竊取企業情資與網路釣魚勒索機會，皆是 AI 技術被不當使用或濫用。尤其，新型冠狀病毒（COVID-19）疫情蔓延全球，連帶提升企業、學校及行政機關對遠距工作的需求，駭客組織將此視為無聲地發動 Deepfake 攻擊的好時機。

[1] 趨勢科技公布 2020 資安預測報告（2019/12/13）。iThome。取自：https://www.ithome.com.tw/pr/134797。

美國各大社群媒體瘋傳裴洛西（Nancy Pelosi）的變造影片，影片中她的說話速度被放慢，因此聽起來含糊不清，像喝醉酒且更顯老邁，之後美國總統川普及其律師朱利安尼皆轉發並評論了這段影片。（Photo Credit: Donald Trump's Twitter）

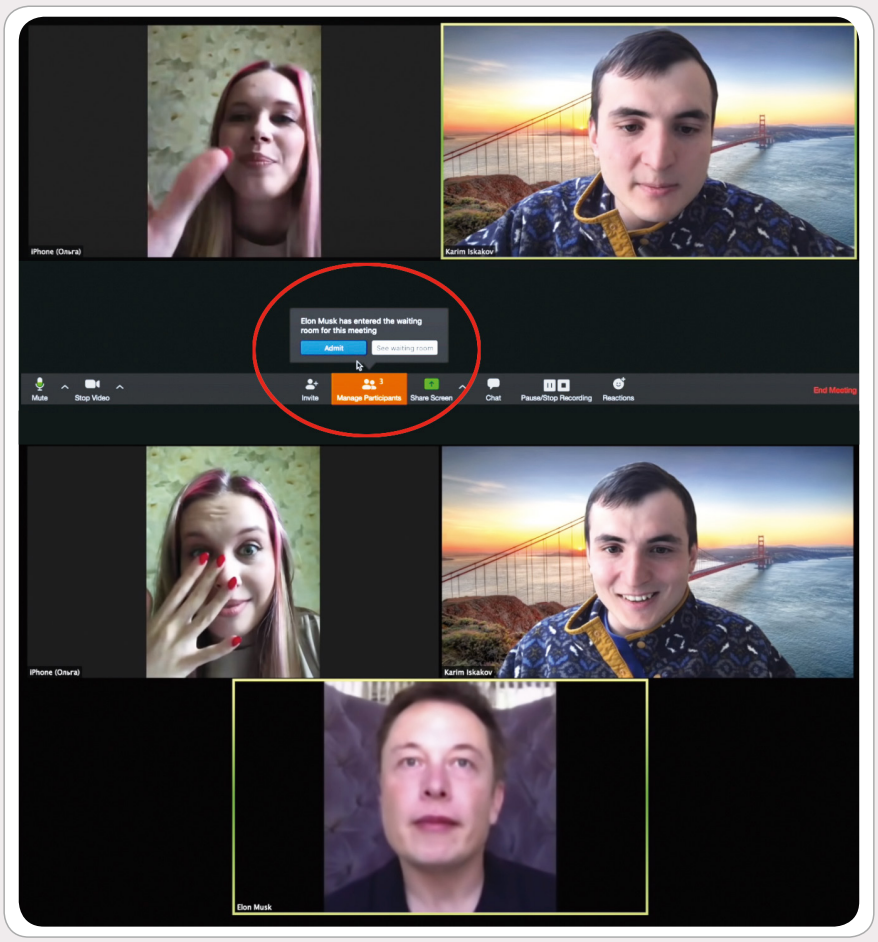
深度偽冒詐騙的崛起及威脅

從 2017 年第一起開始，美國社群（Reddit）上「deepfakes」的用戶透過 AI 技術，將好萊塢女星蓋兒加朵（Gal Gadot-Varsano）的臉移花接木到色情影片中[2]，到 2018 年美國演員運用 AI 換臉技術，合成美國前總統歐巴馬並對著鏡頭說出：「川普總統完全就是個笨蛋」[3]。

另外，2019 年 5 月，美國各大社群媒體瘋傳裴洛西（Nancy Pelosi）的一段變造影片，影片中她的說話速度被放慢，因此聽起來含糊不清，好像喝醉酒且顯得更加老邁。美國總統川普（Donald John Trump）及川普個人律師朱利安尼（Rudolph W. Giuliani）分別前後在 Twitter 轉發裴洛西（Nancy Pelosi）的一段變造影片。朱利安尼推文寫道：「南西．裴洛西怎麼了？她的語言模式很古怪。」然而，川普轉貼影片後還寫道：「裴洛西整場記者會都在結巴。」[4,5]

2018 年美國演員喬登皮爾運用 AI 換臉技術，合成美國前總統歐巴馬說出：「川普總統完全就是個笨蛋」。（Photo Credit: BuzzFeed Video, https://youtu.be/cQ54GDm1eL0）

[2] AI 假色情終究來臨：神力女超人 Gal Gadot 臉被移花接木到 A 片中（2017/12/13）。INSIDE。取自：https://www.inside.com.tw/article/11386-gal-gadot-fake-ai-porn。
[3] 黃貞怡（2018/08/13）歐巴馬罵川普笨蛋？　AI 換臉製造假新聞。TVBS 新聞網。取自：https://news.tvbs.com.tw/world/973044。
[4] 川普 PO 變造影片打對手　裴洛西變老說話結巴 [影]（2019/05/25）。中央通訊社。取自：https://www.cna.com.tw/news/firstnews/201905250194.aspx。
[5] 何蕙安（2020/03/09）因應美國總統大選，YouTube 拿出辦法對付選戰亂象。台灣事實查核中心。取自：https://tfc-taiwan.org.tw/articles/2943。



2020 年初，有人在視訊會議軟體「偽裝」特斯拉 CEO 馬斯克，並在 Github 上提供原始碼。（Photo Credit: Ali Aliev, https://youtu.be/IONuXGNqLO0）

2019 年 9 月，不肖人士透過語音合成方式，冒充英國能源公司德國母公司的 CEO 進行詐騙，金額高達 22 萬歐元，這也是第一起 Deepfake 的 CEO 詐騙[6]。2020 年初，有人在視訊會議軟體「偽裝」特斯拉 CEO 馬斯克，並在 Github 上提供原始碼，皆是 Deepfake 的運用情境[7]。

淺談深度偽冒詐騙型態

根據 AI 法論評論網，Deepfake 種類可以歸納出四種型態[8]，分別為臉部替換、人臉生成、臉部再製、聲音合成，各類型 deepfake 皆有極限，臉部再製可以保持一個人臉部的特徵不變而使照片看起來更加

[6] 愛范兒（2019/09/05）AI 語音模仿老闆聲音要求轉帳，成功騙走近 770 萬元。科技新報。取自：https://technews.tw/2019/09/05/fraudsters-voice-ai/。

[7] 【Deepfake 入侵視訊會議】工程師推出最新假冒馬斯克濾鏡，Github 上已開源（2020/04/20）。科技橘報。取自：https://buzzorange.com/techorange/2020/04/20/deepfake-fun-effect/。

[8] 你所見不一定為真— AI 與 DeepFakes（2019/12/29）。AI 法論評論網。取自：https://www.aili.com.tw/message2_detail/54.htm。

逼真。臉部替換則需要分別取得目標和素材兩個人各種不同角度的影像。在聲音合成技術成熟以前，臉部再製和臉部替換都需要有專人配音。

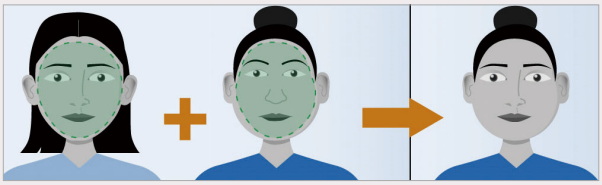
隨著網路上越來越多製作各種型態詐騙應用程式的出現，即使是對 AI 一竅不通的外行，只需要一個 GPU 和一些訓練數據，再通過按部就班的操作也能製作出影片，其影響面向除了對個人的影響，甚至包含至國安、金融與政治領域。

深度偽冒之核心技術

Deepfake 主要使用了生成對抗網路（GAN）與自編碼器（Autoencoder）的技術與概念[9]。首先，有一組編碼器模型（Encoder）需要從人臉中提取表情的

臉部替換

使用某人臉部的影像，替換掉另一個目標人物的臉，目標人物的臉被覆蓋了，重點在換上去的臉



臉部再製

主要是透過修改目標人物的臉部表情，例如移動他們的嘴巴、眉毛和眼睛，臉部再製的目標並不是取代他們的臉部特徵，而是更改他們的面部細節來使照片傳達的訊息不同。

（Source: Government Accountability Office, https://www.gao.gov/products/GAO-20-379SP#summary）

人臉生成

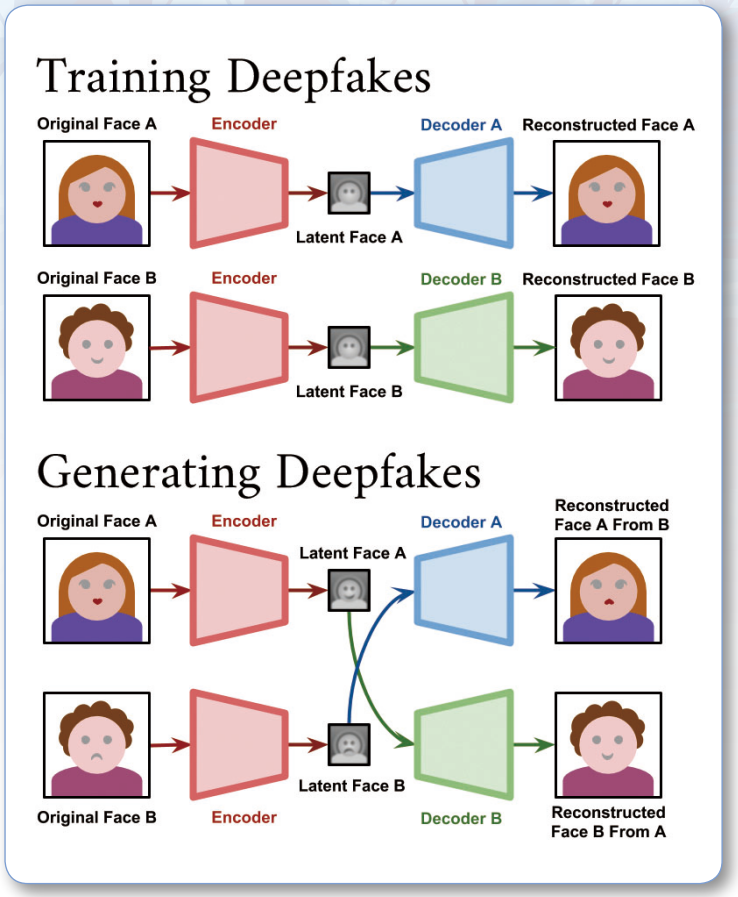
這項技術能夠創造一個全新的臉，是利用一種新興的生成對抗網路（Generative Adversarial Network, GAN）的深度學習技術，這種技術使用兩個神經網路相互對抗，其中一個生成影像，另一個負責判斷生成的影像是否夠好。

圖中男女均為使用 GAN 技術合成之影像，非實際存在之人物。

聲音合成

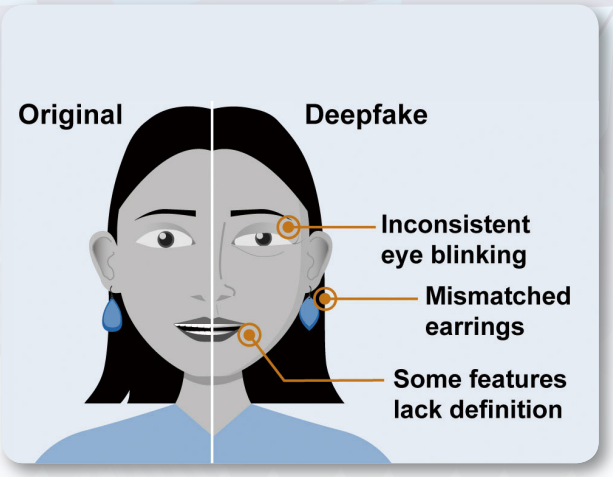
Deepfake 的分支，可以合成出一個人的聲音且使用特定人的說話方式和語調唸出文字。另有的聲音合成產品，例如 .ai，則是能讓使用者挑選聲音的年紀和性別，而非模仿某個特定人的聲音。

[9] 王淳中（2020/01/09）讓臉書忍不住出手封鎖的 Deepfake 影片，是什麼技術？台灣人工智慧學校。取自：https://aiacademy.tw/what-is-deepfake/。



Deepfake 主要使用了生成對抗網路與自編碼器的技術與概念，有一組編碼器模型（Encoder）需要從人臉中提取表情的特徵，另外一組解碼器（Decoder）則需要將表情特徵還原成某個人的人臉。（Photo Credit: Alan Zucconi, https://www.alanzucconi.com/2018/03/14/understanding-the-technology-behind-deepfakes）

特徵，另外一組解碼器（Decoder）則需要將表情特徵還原成某個人的人臉。在訓練階段時，會有另外一個分辨器（Discriminator）協助解碼器作訓練，分辨器則會盡量正確分辨真實的人臉與合成的人臉，而解碼器則會盡量產生出分辨器分不出來的合成人臉，因此兩者會互相對抗且逐漸變強。在訓練完成後我們就可以



可從四大方向判斷是否為 Deepfake 影片，其中包含眨眼的頻率與模糊的痕跡等。（Source: Government Accountability Office, https://www.gao.gov/products/GAO-20-379SP#summary）

將一張新的人臉透過編碼器提取表情特徵，再透過解碼器還原成特定人的人臉。

一般來說，就目前生成對抗網路成像技術之成熟度而言，「正面」的「大頭照」是較容易成像的條件，側臉照或有非臉部器官入照將會大幅增加訓練的難度與降低準確性。

對於 Deepfake 影片，根據白金漢大學數學與電腦教授 Sabah Jassim 及 Spectre 聯合創辦人 Bill Posters 建議，可以注意四大方向[10]：(1) 眨眼率：深度偽冒影片所生成之目標對象其眨眼率少於正常人；(2) 語音和嘴唇運動的同步狀況；(3) 影片情緒不吻合及 (4) 模糊的痕跡、畫面停頓或變色。

[10] 什麼是 Deepfake（深偽技術）？ A 片女主角也可以造！（2020/03/03）。資安趨勢部落格。取自：https://blog.trendmicro.com.tw/?p=63452。

政府及社群平台合力打擊深度偽冒詐騙

由於深度偽冒影片造成之政治、國安、經濟、輿論等各方面影響甚鉅，社群媒體平台亦設立各項措施及行動，打擊Deepfake。

除社群平台大力打擊外，各國亦透過立法防範，希望藉國家手段遏止不實或不當行為。Deepfake 影響範圍及權利甚廣，以我國律法言，Deepfake 若涉及毀損他人名譽，可主張〈刑法〉第 310 條誹謗罪，當事人亦可依《民法》第 184 條請求損害賠償，及同法第 195 條回復名譽。

YouTube

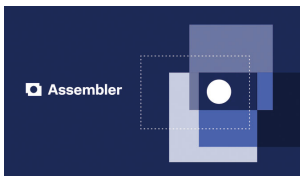
YouTube 在其現行社群準則內的垃圾郵件、欺詐行為和詐騙政策裡就有禁止變造媒體資訊的規定。他們的官方部落格「YouTube 如何支持選舉」文章中，對於會誤導選情的內容採取零容忍態度，例如可能誤導使用者和散播不實資訊的變造過影片，包括 Deepfake（深度偽冒詐騙）。關於候選人或投票過程的不實內容，無論是否變造過都不允許。

（Source: https://blog.trendmicro.com.tw/?p=63452）

twitter

Twitter 關於合成和變造媒體資訊的規則更新中也包括了 Deepfake（深度偽冒詐騙），並未具體提到即將舉辦的美國大選。它單純宣布禁止「可能造成傷害」的合成或變造媒體資訊。

（Source: https://blog.trendmicro.com.tw/?p=63452）



Google 旗下子公司 Jigsaw（原 Google Ideas）與 Google Research 合作開發 Assembler 工具，目的就是為了幫助新聞媒體與事實查核人員辨別圖片影像是否經過變造修改，進而防止假訊息傳播。

（Source: https://udn.com/news/story/11017/4334873）

facebook

Microsoft

2019 年 9 月，微軟和臉書發起 Deepfake Detection Challenge 大賽，以高額獎金鼓勵外界開發出能辨識惡意偽造影片的偵測模型。

（Source: https://www.ithome.com.tw/news/132917）

各社群平台打擊深度偽冒詐騙方式

結語

我國政府於 2016 年宣示「資安即國安」的戰略目標[11]，於 2018 年推動「3x3x3 國家級資安戰略」[12]，2019 年加速研擬「資安即國安 2.0 戰略」，不斷地提高資安人才培訓能量，開發資安產業創新技術，鞏固資訊安全，打造臺灣成為堅韌資安之國。另外，政府也以「集結防制假訊息」、「電腦犯罪」及「網路犯罪」等 3 大目標，於法務部調查局設立資安工作站，強化政府打擊各類網路犯罪的能力。

而面對網路威脅與資安事件，除情資蒐集與運用的重要性日益彰顯外，應透過擘劃戰術與技術的策略，在戰術上，分析資訊安全威脅的戰術、技術、程序，及規劃對應的防護措施並精準投入相對應的防護資源。技術面上，透過掌握資訊安全威脅的相關資訊，進一步定義更精準的威脅指標；透過確保數位安全、建立資安體系、推動資安自主研發等相關量能，將侷限轉化為超越，進而為組織挹注足夠強度的防禦能力和應變能量。

因此，「掌握資安威脅態樣、擘劃堅實防護戰略」，已然成為在資安防護的策略擬定上依循的方向，亦可使機關、企業能更全面因應可能出現的資訊安全威脅。

[11] 黃彥棻（2018/09/14）臺灣首部國家資安戰略報告出爐，總統蔡英文：資安是國家重要戰略選擇。iThome。取自：https://www.ithome.com.tw/news/125913。

[12] 蔡總統：加速研擬資安即國安 2.0 戰略（2019/11/11）。中央通訊社。取自：https://www.cna.com.tw/news/aipl/201911110143.aspx。