雙月刊

網路資訊攻防，戒備深入日常。

清流

No.39
2022.5月號

從俄烏戰爭
看假訊息的影響

關鍵基礎設施
之資安防護

酒駕修法
要既見秋毫亦見輿薪

數位時代防護術

俄烏啟示 全境戒備

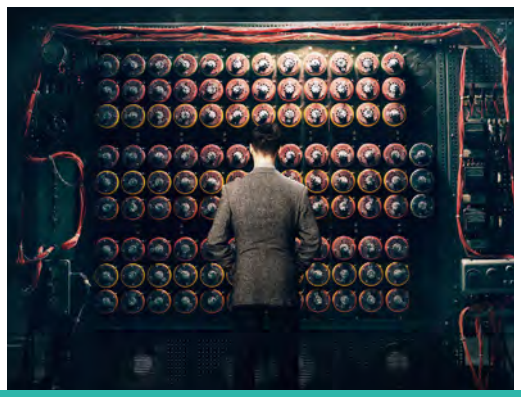
法務部調查局　編印

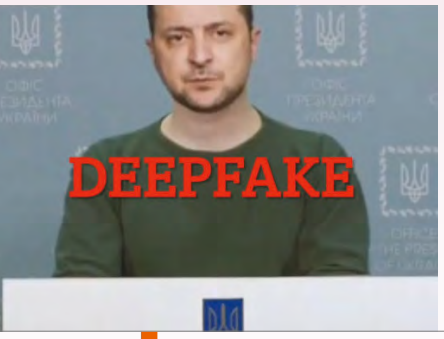
雙月刊 2022.5月號 NO.39

清流 MJIB

Contents

目錄





封面
NO.39 MAY 2022

發 行 人：王俊力
副發行人：黃義村、文瀚、吳富梅
社　　長：宋樂怡
副 社 長：凌文興
主　　編：許淑珍、黃日萱
文字編輯：魏男烜、黃增雄
出 版 者：清流雜誌社
發 行 所：法務部調查局
社　　址：新北市新店區中華路 74 號
傳　　真：（02）2911-2314
法律顧問：劉紀翔律師
美編印刷：加斌有限公司
地　　址：臺北市大安區復興南路二段 210 巷 30 號 1 樓
電　　話：（02）2325-5500
每本工本費新臺幣 30.8 元

歡迎點閱電子書
http://www.mjib.gov.tw
e-mail: 2d40@mjib.gov.tw

GPN: 2010500577
ISSN: 2415-4970

中華郵政板橋雜字第 224 號登記證
登記為雜誌交寄

掃描 QR Code 閱覽電子書版本，可快速連結至其他資料來源，閱讀更多資訊！

數位時代防護術

俄羅斯入侵烏克蘭後，
從國家層級的 CI 到個人社群媒體
Twitter、Facebook 等，
都成為攻防的戰場；
假訊息、深偽技術、勒索軟體
如何深入日常生活？

俄國入侵烏克蘭——這場虛假訊息充斥的資訊戰，我們該學到什麼？

◆ 中正大學傳播系教授、臺灣媒體觀察教育基金會董事長、臺灣事實查核中心董事 ── 羅世宏

有心人刻意散播利用深偽技術（Deep Fake）的造假影片：片中，烏克蘭總統澤倫斯基呼籲烏克蘭士兵放下武器投降！

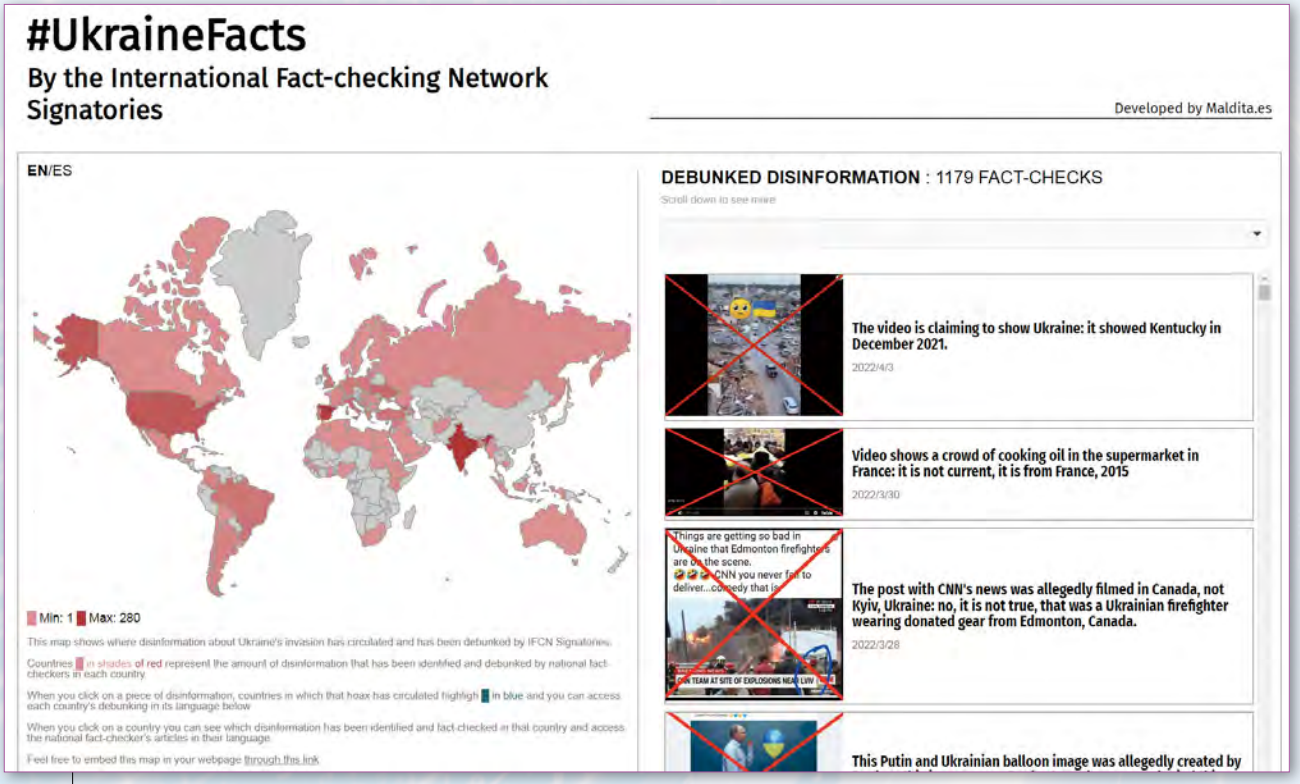
全球事實查核組織共襄盛舉 查核與俄烏戰爭相關虛假訊息

俄羅斯於今（2022）年 2 月 24 日揮軍入侵烏克蘭；毫無意外，正如很多專家所預測的，這場戰爭已成為虛假訊息資訊戰的溫床。西班牙一家事實查核組織 Maldita.es 有先見之明，在戰爭爆發之際，立即倡議結合各國事實查核組織，致力於共同合作查核與這場戰爭有關的虛假訊息。很快地，有來自全球各地的 70 多家事實查核組織共襄盛舉，其中也包括台灣事實查核中心。

在他們的共同努力下，設立了一個與烏克蘭這場戰事相關的事實查核網站（ukrainefacts.org），[1] 公開分享最新的事實查核成果，並且彼此交流專業經驗，以發揮事實查核組織的跨國合作力量。截至 4 月 18 日為止，他們已經查核了近 1 千 3 百條與俄烏戰事有關的虛假訊息！

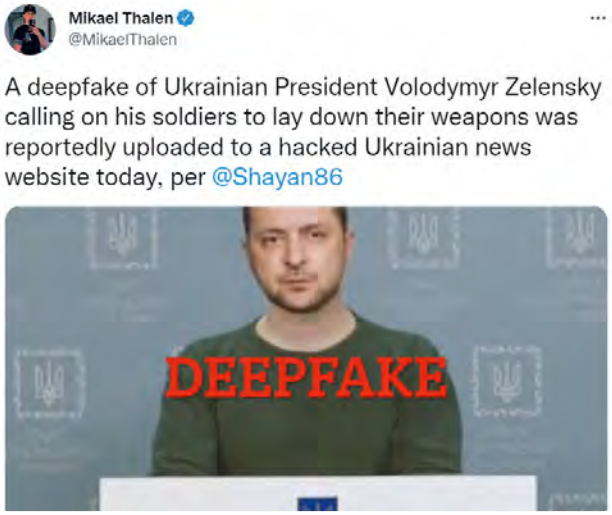
虛假訊息五花八門，往往真假難辨

這些虛假訊息五花八門，往往真假難辨，一般人很容易誤以為真，並透過分享轉傳而協助擴散了虛假訊息的傳播。其中，一個經典案例是有心人刻意散播利用深偽技術（Deep Fake）製作的造假影片：片中，烏克蘭總統澤倫斯基呼籲烏克蘭士兵放下武器投降！



西班牙事實查核組織 Maldita.es 在戰爭爆發之際，立即倡議結合各國事實查核組織，設立一個與烏克蘭戰事相關的事實查核網站，公開分享最新的事實查核成果。（Source: #UkraineFacts, https://ukrainefacts.org）

[1] "#UkraineFacts, By the International Fact-checking Network Signatories," https://ukrainefacts.org/.



烏克蘭戰略通訊和資訊安全中心在臉書貼文警告各界注意，俄國可能會使用深偽技術來冒充澤倫斯基呼籲軍隊投降；而後果然出現深偽技術製作的造假影片。（資料來源：台灣事實查核中心，https://tfc-taiwan.org.tw/articles/7099；Mikael Thalen twitter, https://twitter.com/MikaelThalen/status/1504123674516885507?）

台灣事實查核中心資深國際事務專員何蕙安指出，這支刻意製作的造假影片，被發布在多個烏克蘭新聞網站。所幸人們對於深偽影片有所警覺，該影片很快就被揭穿。在第一時間，澤倫斯基本人也在 Telegram 頻道上傳影片闢謠。他說，他如果要呼籲投降的話，該放下武器回家去的應該是俄羅斯軍隊。[2]

烏克蘭媒體遭駭客入侵 播放總統下令停止抵抗之跑馬燈

值得注意的是，虛假訊息不僅嘗試在社群媒體及即時通訊軟體等平臺上散播，也試著結合駭客網路攻擊手段入侵烏克蘭主流新聞媒體。例如，這次烏克蘭新聞頻道《Ukrayina24》的直播節目裡，字幕跑馬燈顯示澤倫斯基已下令烏克蘭人停止抵抗，並說自己已經離開基輔。這當然不是《Ukrayina24》發布的字幕跑馬燈！據該新聞媒體事後聲明可知，當時該媒體遭到不明網路駭客入侵。

值得慶幸的是，這支深偽造假影片散播的虛假訊息最終沒有得逞，因為烏克蘭政府早已為全民打了「預防針」，事前即已判斷俄羅斯可能利用深偽造假影片混淆民心士氣，而且在臉書等社群媒體平臺積極把關下，讓這支造假影片無法如願廣傳。同樣的，中文臉書平臺也未被有心人成功地用來流傳這支深偽影片。

這只是眾多有關俄侵烏戰爭虛假訊息的案例之一，更多案例可參考台灣事實查核中心有關俄侵烏戰爭的事實查核最新動態。[3] 過去一個多月來，烏俄雙方除了硬碰硬的戰爭攻防，也有時時刻刻進行著的資訊戰。

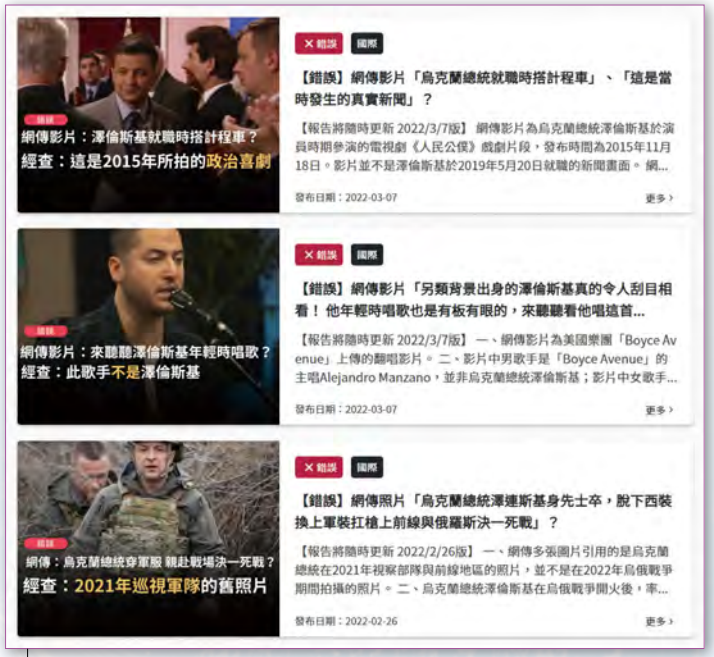
[2] 《【烏俄戰爭】深偽影片首在烏俄資訊戰現身 冒充澤倫斯基要求烏軍投降》，https://tfc-taiwan.org.tw/articles/7099。

[3] 烏俄戰爭當中，假訊息成為戰爭攻擊的一環，「台灣事實查核中心」收集國際最新的查證訊息，供民眾與媒體專業工作者參考。https://tfc-taiwan.org.tw/articles/6988。

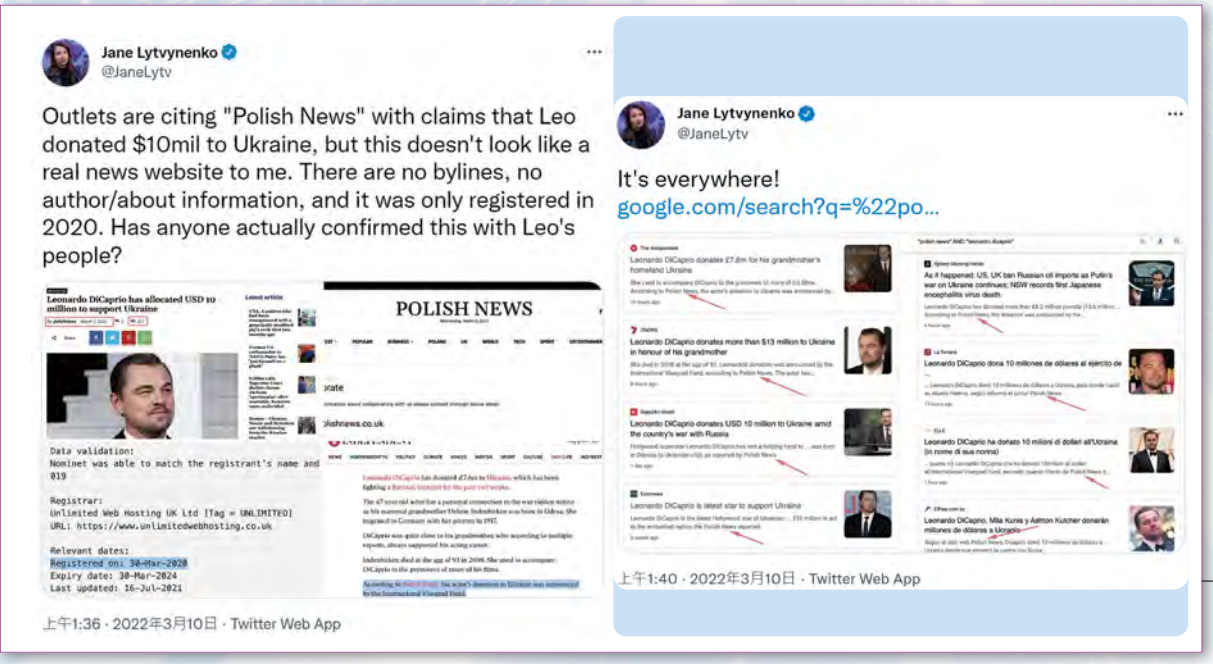
資訊戰的戰時宣傳目標

這場資訊戰所為何來？依據研究宣傳而馳名於世的傳播研究大師拉斯威爾，戰時宣傳有以下四大目標，包括：一、使民眾仇敵恨敵；二、保持盟邦的友誼；三、與中立者保持友好，可能的話，拉攏中立者，使其加入我方陣營;四、瓦解敵方的民心士氣。而宣傳的這四大目標，正是我們當下看到各式烏俄戰爭假訊息想要達成的目標。比方說，這次有各種與烏克蘭總統澤倫斯基本人的虛假訊息，有意塑造其親民、討喜、無畏、堅毅與身先士卒的英雄形象，為原先孤軍抗俄的烏克蘭贏得不少國際奧援與網路聲量支持……等。

此外，一度傳遍全世界的另一則錯誤訊息是「李奧納多捐款 1 千萬美元給烏克蘭」，包括英國、法國、印度、美國及臺灣新聞媒體都做了跟進的錯誤報導。事後，經美國有線新聞網 CNN 進行事實查核後發現，李奧納多（Leonardo DiCaprio）確實有捐款，但並非捐給烏克蘭政府，而是捐給國際關懷協會、國際難民組織、救助兒童會，以及聯合國難民署等國際人道組織。他的捐款金額不是 1 千萬美元，而且他也不具烏克蘭血統，因為他的外婆並非假訊息所宣稱的是烏克蘭奧德薩人。



各種與烏克蘭總統澤倫斯基本人有關的資訊，雖已被證實是假訊息，但也已成功塑造其親民形象。（資料來源：台灣事實查核中心，https://tfc-taiwan.org.tw）



宣稱李奧納多因祖母是烏克蘭人而捐款 1 千萬美元的消息傳遍網際網路，錯誤資訊研究者 Jane Lytvynenko 指出此新聞很可疑，而後 CNN 進行調查，證實為假消息。（Source: Jane Lytvynenko twitter, https://twitter.com/JaneLytv/status/1501612840624562179?s=20&t=_BlOkLH33pvGx7y4b1aEeg）

俄羅斯為侵略烏克蘭找藉口而造假影片，後經媒體與事實查核組織查證，其為 10 年前芬蘭軍方實戰演習影片音訊。（資料來源：胡元輝臉書，https://m.facebook.com/story.php?story_fbid=10221405358186730&id=1332827914）

以上這些案例，可以讓我們從中密集觀察，與軍事戰爭同時發生的，而且實際「參戰方」可能更多的虛假訊息資訊戰。涉及製造、傳播這些虛假訊息的，可能包括交戰雙方的政府、人民，也可能是其他國家關注此事發展的各種力量，其中有刻意為之的虛假訊息（例如，宣稱澤倫斯基已宣布投降、逃離首都基輔的惡意造假影片或訊息），也有動機良善或是無心失誤造成的錯誤訊息（例如，宣稱澤倫斯基是搭計程車前往就職典禮的照片，或是李奧納多捐款支持烏克蘭且具烏克蘭血統的錯誤訊息）。

俄羅斯替侵略找藉口之造假影片

誠如中正大學傳播學系教授胡元輝所說的：「俄羅斯入侵烏克蘭，又是資訊戰一個重要的觀察案例。」胡教授說得完全正確！他舉了一個特別重要的案例，亦即俄羅斯為了替侵略找藉口而造假的影片，俄羅斯官方媒體大肆散播指控烏克蘭挑釁、陰謀破壞與攻擊烏東地區的虛假訊息。所幸，很快地，美國媒體《Newsy》與國際事實查核組織 Bellingcat 聯合查證發現，這些影片是人為偽造與惡意栽贓的影片，其畫面與聲音都不是基於發生在烏克蘭境內的真實事件，而是移花接木自 10 年前一支芬蘭軍方實戰演習影片的聲音！

面對虛假訊息充斥的資訊戰，我們該學到什麼？

面對虛假訊息充斥的資訊戰，我們從俄烏資訊戰中應該學到的重要一課是應提升全民不輕信來路不明訊息的媒體資訊素養，政府則應力守民主價值與誠信形象，並且努力健全並支持打造我國具有公信力的新聞資訊生態系統。雖然未來資訊戰必然會愈激烈，各種造假技術會更高明，但若我們做好防患未然的全民心防，未來終必可以克服資訊戰帶來的挑戰，免於淪為資訊戰的受害者。

防範 Deepfake 技術遭濫用

◆ 行政院環境保護署政風室科長— 李志強

網紅小玉涉嫌以 Deepfake 技術製作換臉影片，引發各界開始關注私密影片外流以及該技術的犯罪問題。

Deepfake 製作虛偽影像 動搖人類互信基礎

隨著數位科技及人工智慧（Artificial Intelligence, AI）高度發展，民眾使用網路已是稀鬆平常，然而近年來利用電腦合成之 Deepfake 技術，不僅侵害他人之隱私與名譽，也使普羅大眾難以辨識其真實性，進而動搖人與人之間互信基礎，危及社會安定。甚可猜想，俄羅斯若動用 Deepfake 技術，散布烏克蘭總統宣布投降的影片，將讓烏克蘭軍民被絕望吞噬掉事實和反擊機會，或散播敵國將使用核武等假訊息，恐將爆發第三次世界大戰—核子大戰。因此，Deepfake 技術能動搖國家安全，甚至攸關全人類存續，影響力實在不容小覷。

Deepfake 正面價值

Deepfake（深偽技術）係英文 deep learning（深度學習）與 fake（偽造）混合而成的單字。簡言之，是透過人工智慧（AI）中的深度學習技術將一個人肖像替換成另一個人。作法首先需要目標的人像、語音或影片，再與被插入目標的人身、語音或影片合成，主要係運用 AI 從各種角度和條件研究其等共同特徵，再進行合成動作。

Deepfake 有其娛樂性與正面價值，例如 2015 年美國電影《玩命關頭 7》（Furious 7）的男主角之一保羅（Paul Walker）在影片未殺青前發生車禍意外身亡，劇組人員即運用 Deepfake 技術，讓已逝世的明星重返大螢幕。[1] 導演李安的 2016 年《雙子殺手》（Gemini Man），[2] 為「複製人」科幻電影，由奧斯卡獎得主威爾·史密斯（Will Smith）主演，中年退休特務與年輕的自己在同一畫面中進行殊死較量，傳達「只有自己能超越自己」亦或者「最大的敵人是自己」等意涵，讓電影更具可看性。Deepfake 除運用於電影外，2021 年美國基因公司（My Heritage）的「深度懷舊」計畫，推出一款名為「Deep Nostalgia」的線上工具，[3] 只要簡單操作，一鍵就讓逝去親人的照片「動起來」，不僅能轉頭、能眨眼，還能微笑，讓親友再次目睹離世家人栩栩如生的動態相片，以解思念之情。然今日 Deepfake 被多用來偽造名人不雅影片，或用來製造假新聞及惡作劇，負面效應持續增強。

Deepfake 負面案例

2017 年，美國社群網站 Reddit 上，一名帳號為「deepfake」的用戶上傳一系列色情影片，就是透過 Deepfake 將色情影片中的人臉更換為名人。2018 年，媒體以 Deepfake 變造美國前總統歐巴馬的演說內容，藉以調侃川普總統。2019 年，有人利用 Deepfake 的語音合成方式，模仿英國能源公司德國總公司執行長的聲音，與該公司出納人員通話，竟然順利騙得 22 萬歐元。2020 年，時任美國總統參選人拜登，外流一段在家中接受記者電訪時竟打瞌睡的影片，也是使用 Deepfake 合成。

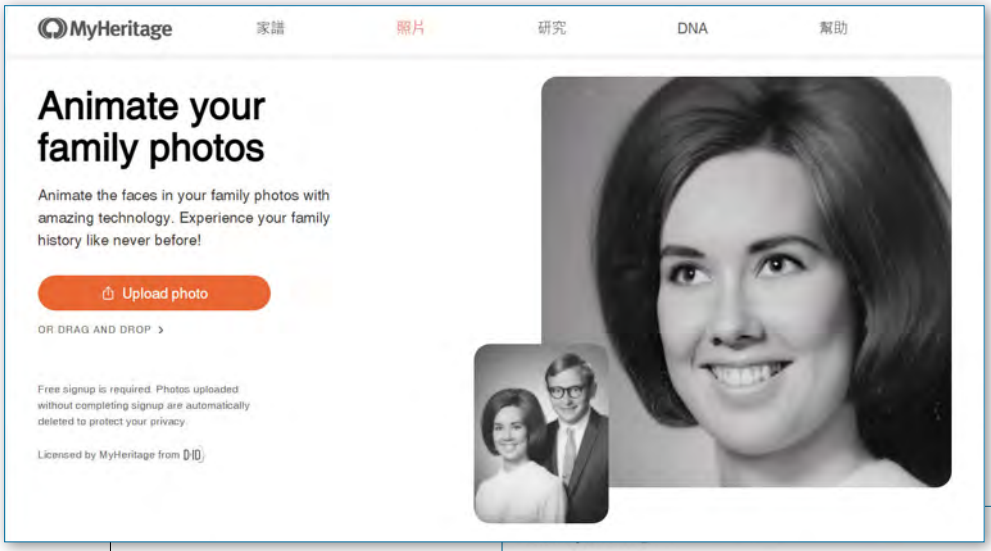
國內近期矚目案件是 2021 年網紅小玉涉嫌利用 Deepfake 技術，將名人臉部圖像，移植到成人影片上販售得利。他還設立會員制度，只要繳交數百元不等費用，就可以加入私密聊天群組，線上瀏覽完整版的換臉影片，讓會員票選某位知名人物，

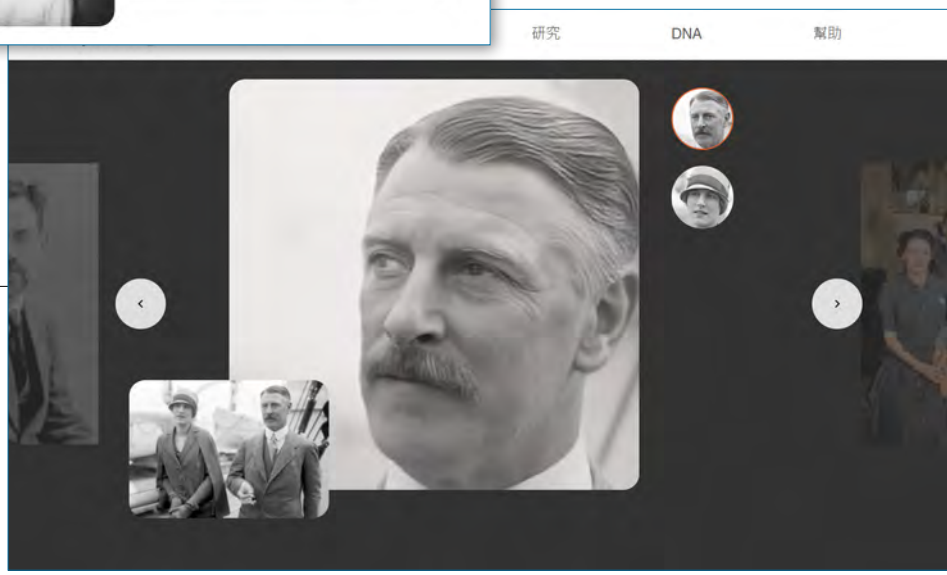
[1] 《〈玩命關頭 7〉如何讓已故的保羅沃克重獲新生》，https://www-hollywoodreporter-com.translate.goog/movies/movie-news/how-furious-7-brought-late-845763/?_x_tr_sl=en&_x_tr_tl=zh-TW&_x_tr_hl=zh-TW&_x_tr_pto=op,sc。

[2] 內容描述中年退休特務，遭到有著自己樣貌的年輕複製人追殺的故事。有趣的是，這個複製人並非替身所飾演，而是由電影特效製成。《動員 500 人搞技術！李安 20 年力作解鎖新技術，〈雙子殺手〉打造極致寫實的觀影體驗》，https://www.bnext.com.tw/article/55089/ang-lee-will-smith-gemini-man。

[3] "My Heritage", https://www.myheritage.tw/deep-nostalgia.

2015 年美國電影《玩命關頭 7》的男主角之一保羅沃克，在影片未殺青前發生車禍意外身亡，劇組人員運用 Deepfake 技術，讓已逝世的明星重返大螢幕。（Source: Weta Digital, https://youtu.be/ye7arp5IrAg）





美國基因公司 My Heritage 推出一款名為「Deep Nostalgia」的線上工具，只要一鍵的簡單操作，就能讓逝去親人的照片「動起來」。（Source: My Heritage, https://www.myheritage.tw/deep-nostalgia）

2020 年，美國總統競選期間，網路流傳一段拜登在家中接受記者電訪時打瞌睡的影片，後經查核證實，此影片之影像、聲音皆為合成。（Photo Credit: MyGoPen, https://www.mygopen.com/2020/09/Joe-Biden-asleep.html）

2021 年網紅小玉涉嫌利用 Deepfake 技術，將名人臉部圖像移植到成人影片上販售得利。（圖片來源：刑事警察局）

再由其換臉合成影片上傳，本案一經媒體報導後即引發各界撻伐。

Deepfake 技術容易操作，有心人士有機可乘；若法律制度跟不上科技進程，人們無法確知何謂真、何謂假，將讓假訊息本已紛飛的網路時代變得更加混亂。由於我國過往無規範數位性暴力之法令，[4] Deepfake 影片便成為法律灰色地帶，充其量僅能以散布猥褻物品罪及妨害名譽罪等論斷，最後大多易科罰金了事，實在難以發揮嚴懲或嚇阻效果。被移花接木的受害者們，有苦說不出，更何況，為什麼無辜的受害者要拚命去澄清從未做過的事，而讓自己再次受到二度傷害？

[4] 行政院院會於 2022 年 3 月 10 日通過《刑法》、《兒童及少年性剝削防制條例》、《性侵害犯罪防治法》、《犯罪被害人保護法》等 4 項修正草案，送立法院審議。攸關 Deepfake 部分，未來「意圖散布而製造不實性影像／散布不實性影像」，處 5 年以下有期徒刑；意圖營利而犯之者，處 7 年以下有期徒刑。《遏制網紅小玉「變臉謎片」再生 政院通過性暴力犯罪防制 4 法》，https://tw.news.yahoo.com/遏制網紅小玉 - 變臉謎片 - 再生 - 政院通過性暴力犯罪防制 4 法 -033037896.html。

國內外相關法令

立法院於 2021 年底，三讀通過國家通訊傳播委員會（NCC）組織法修正條文，在掌理事項增加網際網路傳播相關業務，例如通訊傳播監理及網際網路傳播政策與法令之訂定、修正、廢止及執行；通訊傳播網路設置之監督管理；通訊傳播傳輸及網際網路內容分級制度等。

針對數位網路新興犯罪，政府從被害人的需求角度進行修法，透過專章保護、加重罪責等方式，完善民眾的人格權、名譽權及性隱私權之保障。（資料來源：行政院，https://www.ey.gov.tw/Page/448DE008087A1971/e35b242f-4c35-4fbf-8731-c2832666bca5）

因應網路性暴力事件層出不窮，行政院 2022 年通過〈刑法〉等防制性暴力四項修法，其中為遏止 Deepfake 技術亂象，草案規範，製作或散布不實性影像並意圖營利，最高可處 7 年徒刑；散布強暴脅迫攝錄的性影像並營利，得加重其刑 1/2，最高可關 10 年 6 個月。

據報載，韓國訂定《性暴力犯罪處罰特別法》，其中第 14 條規定「意圖散布，以可能誘發性慾或羞辱的形式進行編輯、合成或加工編輯人臉、身體或聲音者，處 5 年以下有期徒刑、5 千萬韓圓以下罰金」等；此外，美國維吉尼亞州《復仇式色情法》（Revenge Porn Law）也將偽造他人照片或影像等 Deepfake 技術納入適用範圍。[5]

[5] 《因應深偽技術犯罪手段 法務部：參考美韓完成立法》，https://today.line.me/tw/v2/article/Gggq8ry，2022 年 2 月 4 日。

由上可知，透過法律規範 Deepfake 技術已然是趨勢。為保護個人隱私，防範 Deepfake 技術淪為犯罪工具，政府廣泛徵詢各界修法意見及蒐集外國立法例，研議〈刑法〉增訂「散布性私密影音罪」等內容。說明如下：

一、加重處罰竊錄性影音罪。[6]

二、增訂散布性私密影音罪。[7]

三、增訂製作或散布他人不實性影音罪。[8]

四、修正〈刑法〉第 28 章章名為「妨害秘密及性隱私罪」。[9]

五、增訂製作或散布他人不實活動、言論、談話影音罪。[10]

可行作法— SQR

2020 年 2 月 11 日，歐盟發起、全世界超過 130 個國家共同響應之全球網路安全日（Safer Internet Day, SID），針對 Deepfake 技術提供「停、問、報」（SQR）三招，呼籲民眾觀看影片時考慮以下三點，藉此遏止 Deepfake 技術氾濫。

首先是停（Stop），一旦發現影片有任何疑慮，不要立刻回應、評論或者分享。接著是問（Question），此影片原始出處？影片中人的言行舉止是否有異？為何這個人或團體要在線上分享此影片？最後是報（Report），在網路上看到任何可疑內容時，若懷疑或認定屬 Deepfake，就向該社群網站或平臺舉報。[11]

先查證不轉傳，避免無辜人受傷害

由於 Deepfake 影片主要是透過社群媒體轉傳，所以臉書已建立辨審核機制，防堵換臉影片流傳，同時推特（Twitter）也跟進，明確標示換臉影音為假訊息，而 YouTube 則是在社群準則中明訂禁止變造媒體影音資訊之規範。

---

[6] 修正〈刑法〉第 315 條之 1 規定，增列竊錄之內容為他人之性影音予以加重處罰之規定。若有竊錄性影音之行為，最重處 4 年 6 個月有期徒刑，若有散布竊錄性影音之行為，最重處 5 年有期徒刑。

[7] 增訂〈刑法〉第 315 條之 4 規定，亦即增列未經他人同意，而散布、播送、交付或以他法供人觀覽其性影音或電磁紀錄之處罰規定，最重處 2 年以下有期徒刑。

[8] 增訂〈刑法〉第 315 條之 5 規定，亦即增列意圖散布而以電腦合成或其他科技方法製作關於他人不實之性影音或其電磁紀錄，以及散布、播送、交付或以他法供人觀覽之處罰規定，並增列意圖營利之加重處罰規定。於製作或散布不實性影音之情形，最重處 5 年有期徒刑，若有意圖營利之情形，最重處 7 年有期徒刑。

[9] 因應上開增訂條文，將刑法第 28 章章名「妨害秘密罪」予以修正，以彰顯性隱私權之保護。

[10] 於〈刑法〉第 36 章「妨害電腦使用罪章」，增訂第 362 條之 1 修正草案，亦即增列意圖散布而以電腦合成或其他科技方法製作關於他人不實之活動、言論、談話之影音或其電磁紀錄，以及散布、播送、交付或以他法供人觀覽之處罰規定，並增列意圖營利之加重處罰規定。本罪為以電腦合成或其他科技方法製作或散布他人不實影音之基本犯罪類型，最重處 3 年有期徒刑，於意圖營利之情形，最重處 5 年有期徒刑。

[11] 《響應 SID 全球網路安全日，趨勢科技發布 Deepfakes 防禦三招》，https://blog.trendmicro.com.tw/?p=63390，2022 年 2 月 6 日。

看到來路不明的影片、消息，應提高警覺，「先查證、不轉傳」，提升自身媒體素養，避免人人受到 Deepfake 危害。

另從國際趨勢來看，管制 Deepfake 影片已是必然，如世界智慧財產權組織早在 2019 年就指出，Deepfake 技術可能會危及人權，如侵犯隱私權及個人資料等，故當 Deepfake 技術內容侵犯前述權利時，其著作權即不應受到保護。

展望未來，我國對 Deepfake 技術課責條款雖尚未三讀通過，仍奉勸國人切勿心存僥倖以此侵害他人權益。誠如行政院唐鳳政委提醒社會大眾，若看到來路不明之影片，就應提高警覺，並做到「先查證、不轉傳」，只要養成主動查證之習慣，提升自身媒體素養，即能避免人人受到 Deepfake 危害。

從俄烏戰爭看假訊息的影響

◆ 國防安全研究院政策分析員 ── 陳穎萱

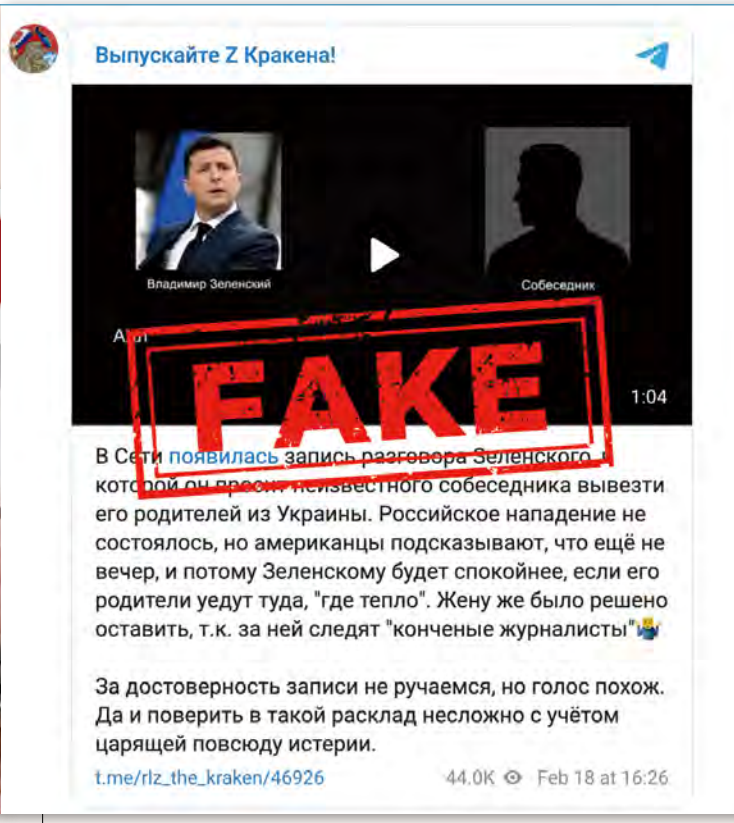
近期俄烏戰爭，雙方除在軍事、外交上短兵相接外，同時也在網路社群媒體進行一連串的資訊攻防。

假訊息成為戰爭利器

早在戰事開打之初，Twitter、Facebook 等社群媒體上就多次傳出烏克蘭總統澤倫斯基（Volodymyr Zelensky）已經逃離首都基輔的假訊息；Telegram、WhatsApp 也有多個冒名帳號，冒充澤倫斯基要求烏克蘭軍隊投降。[1]

[1] "Lacking oversight, Telegram thrives in Ukraine disinformation battle," *The Citizen*, March 14, 2022, https://www.thecitizen.co.tz/tanzania/oped/lacking-oversight-telegram-thrives-in-ukraine-disinformation-battle-3746840.

Telegram 是烏克蘭最盛行的通訊軟體，烏克蘭政府與民眾利用其公布俄羅斯攻勢與共享疏散路線等資訊，卻也成為俄羅斯假訊息散播的溫床。



2 月時網傳烏克蘭總統安排家人出國的錄音檔，後經查證出現自傳播假訊息的俄國 Telegram 頻道，隨後又在其他社群平臺流傳。（圖片來源：台灣事實查核中心，https://tfc-taiwan.org.tw/articles/7018）

在本次俄烏戰爭的認知戰中，有兩個值得注意的現象：

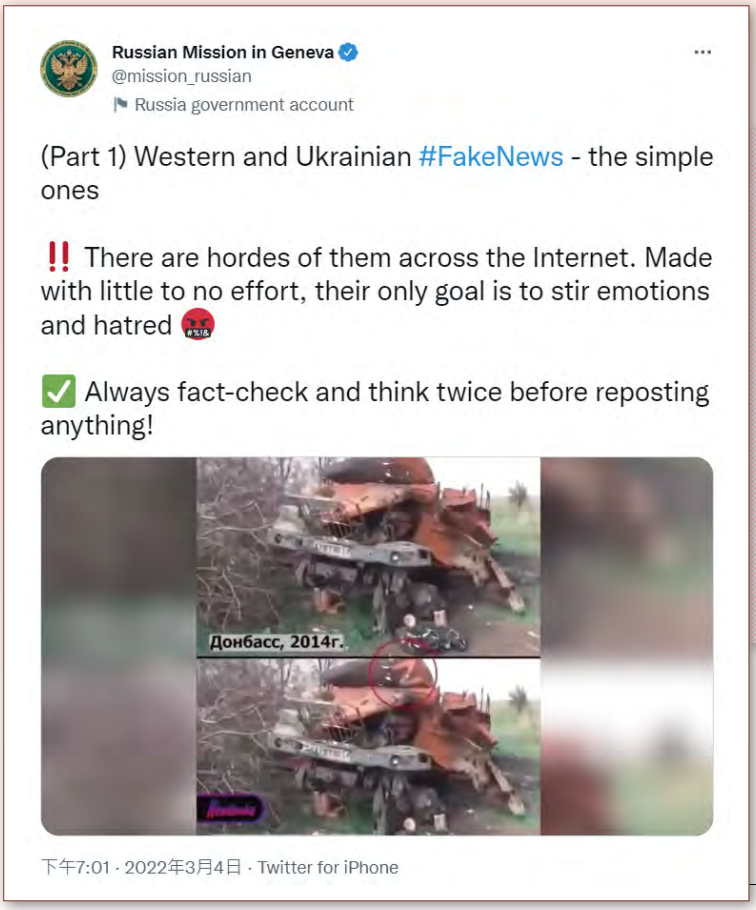
一、加密應用程式成為兩面刃

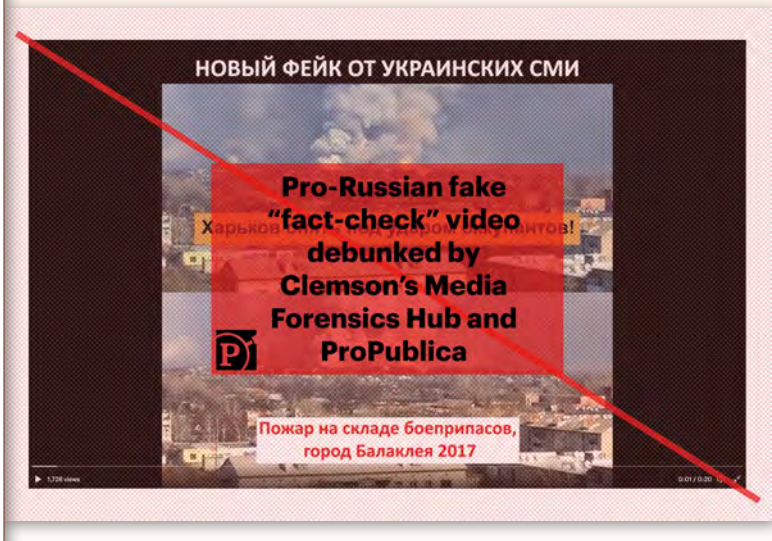
Telegram 作為烏克蘭最受歡迎的通訊軟體，成為俄烏雙方戰時傳播場域的兵家必爭之地。烏克蘭軍方及政府官員透過 Telegram 即時更新俄羅斯的攻擊情形，並傳達政府政策，民眾更利用 Telegram、WhatsApp 組織自發性團體共享疏散路線等資訊。然而，Telegram 亦成為假訊息的溫床。烏克蘭危機媒體中心（Ukraine Crisis Media Center）資深研究員 Oleksandra Tsekhanovska 接受採訪時提到，由於 Telegram 保密性較強，政府無法即時監督和封鎖聊天群組，使得假訊息在各聊天群組間大量轉發。更有甚者，有心人士冒充烏克蘭公民，創設或加入聊天群組，套取與傳遞錯誤訊息，或是以「金援烏克蘭」為由，進行加密貨幣詐騙等犯罪活動。

二、攻擊方利用查核平臺公信力進行假訊息宣傳

根據位於紐約的非營利組織「ProPublica」2022 年 3 月 8 日發布之調查報告，本次俄烏戰爭中出現一項新型態的認知作戰攻擊手段—俄羅斯以「自導自演」的方式，產製影片或訊息，並上傳到查核平臺「打假」。[2] 雖然影片內容宣傳意味濃

[2] Craig Silverman and Jeff Kao, "In the Ukraine Conflict, Fake Fact-Checks Are Being Used to Spread Disinformation," *ProPublica*, March 8, 2022, https://www.propublica.org/article/in-the-ukraine-conflict-fake-fact-checks-are-being-used-to-spread-disinformation.





根據 ProPublica 報導指出，俄方自製不實影片，上傳至查核平臺，反控為烏克蘭所製，並透過俄羅斯政府官方推特與媒體宣傳。（Source: Russian Mission in Geneva, https://twitter.com/mission_russian/status/1499701438821326852; ProPublica, https://www.propublica.org/article/in-the-ukraine-conflict-fake-fact-checks-are-being-used-to-spread-disinformation）

厚，但由於其「事實查核」的性質，仍多次被俄羅斯媒體引用以反駁烏克蘭方的論述，甚至連俄羅斯外交部也曾轉推過相關內容。俄羅斯採取該手法的目的不在於說服受眾內容的真實性，而是讓觀眾相信烏克蘭宣傳部門「有可能」會採取這些作為。事實上，中共的事實查核平臺也曾出現過類似地「作賊喊抓賊」手法，北京當局一方面製造似是而非的假新聞，另一方面以「闢謠」為名成立「事實查核」平臺，博得社會輿論關注，並重塑有利政府的戰略敘事。

民眾是否受到假訊息影響？

在討論「認知作戰」與「假訊息」時，除關注攻擊方的手段與特徵外，更重要的是評估認知作戰與假訊息是否會對受眾產生影響？影響的方式與程度為何？首先，關於民眾接收假訊息的動機，美國非營利組織「保衛民主聯盟」（Alliance for Securing Democracy）資訊操縱部門主任謝佛（Bret Schafer）認為，民眾之所以會選擇接收假訊息，肇因在於其迫切想獲得資訊，但可靠資訊太少，因此使得許多片

段資訊得以填補空缺。[3] 而這些未經證實的資訊，通過民間社交媒體帳戶、或是不可靠的新聞平臺，以及受眾本身的人際網絡，像病毒一樣快速地傳播，甚至被官方媒體、政府宣傳平臺等利用和放大，產生更大的影響力。為何民眾容易相信並傳遞假訊息？心理學家認為，相比與自身立場牴觸的訊息，人們更傾向接受與自身價值觀相符的論述，以避免認知失調帶來的負面情感。另外，資訊爆炸的時代讓民眾產生疲乏，缺少批判性思維（analytic thinking）而易相信錯誤資訊。同時，假訊息較容易帶給受眾新鮮感，聳動與煽情的內容也促使受眾更願意轉發。

臺灣民眾同樣受到假訊息氾濫的影響。根據台灣事實查核教育基金會 2022 年 2 月發布的調查報告顯示，超過 75% 的民眾在最近一年曾經收到過假訊息，但 58% 的民眾認為「自己不會受到假訊息影響」。[4] 不過，國防安全研究院在 2021 年「台灣國防安全民意調查」第二波網路民調中，將受訪者隨機分為三組進行實驗。[5] 實驗組 1 接受有關國軍漢光演習正面報導影片的刺激，實驗組 2 接收有關國軍漢光演習負面報導

民眾會接收假訊息，在於迫切想獲得資訊，但可靠資訊太少，因此使許多片段資訊得以填補空缺；同時，資訊爆炸時代，讓民眾產生疲乏，致缺少批判性思維而輕易相信錯誤資訊。另外，聳動與煽情內容也促使民眾更願意轉發。

[3] "Propaganda, fake videos of Ukraine invasion bombard users," *AP*, February 25, 2022, https://apnews.com/article/russia-ukraine-technology-europe-media-social-media-123c7975a879b89b85c06877f1f12908.

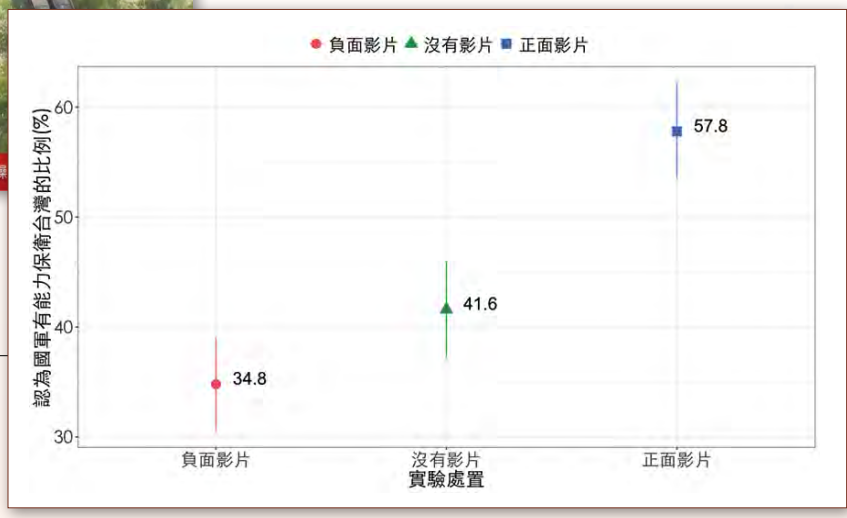
[4] 《【假訊息年度大調查】臺灣首次針對假訊息現象與事實查核成效大調查 學術報告出爐》，台灣事實查核中心，2022 年 2 月 18 日，https://tfc-taiwan.org.tw/articles/6953。

[5] 卡方檢定顯示三組在性別、年齡、教育程度和政黨認同等特徵上無顯著差別，表示三組具有同質性，不同組別認知國軍保衛臺灣能力的差異來自於實驗處置（treatment）的差異。

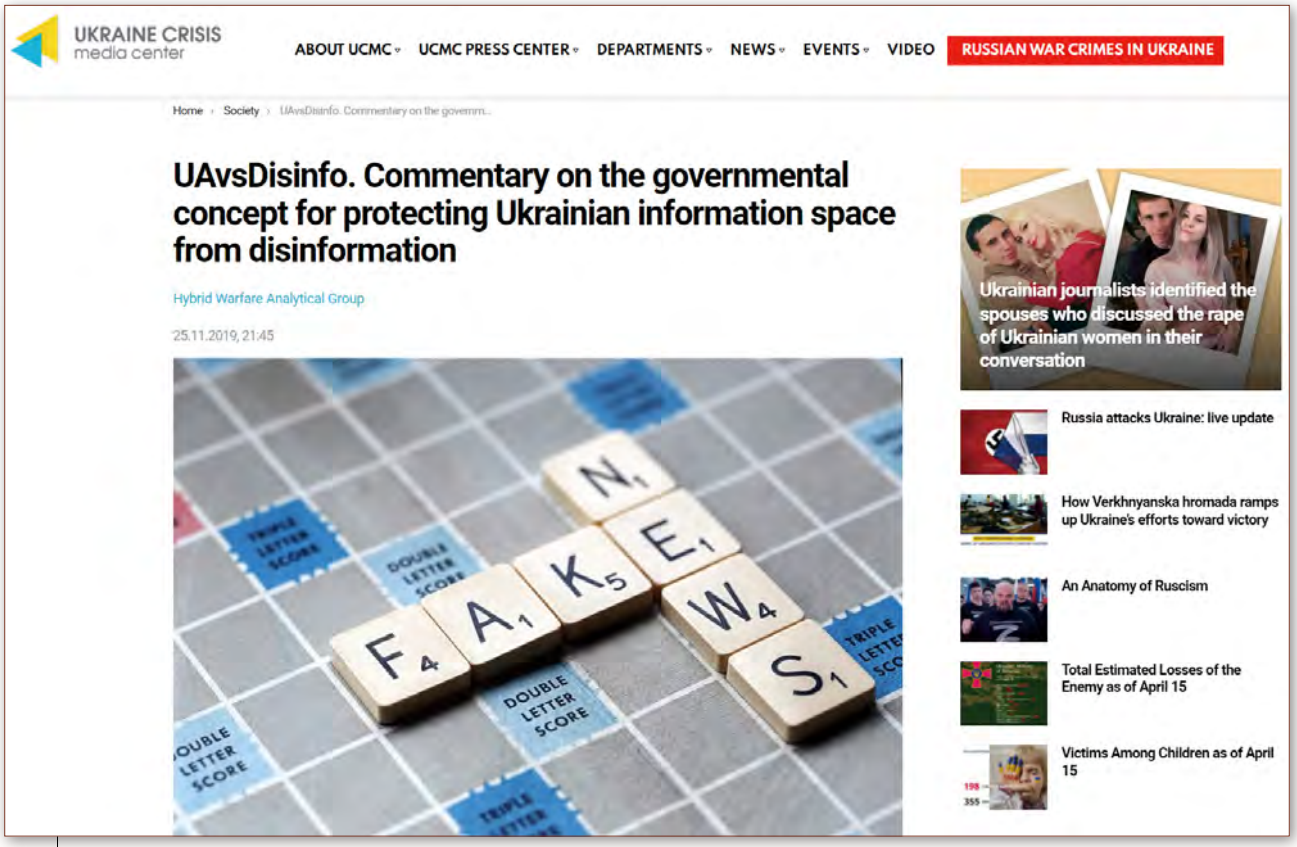
影片的刺激，控制組則不受到任何刺激。觀看完影片後，三組受訪者皆被詢問國軍有沒有足夠的能力保衛臺灣。研究結果顯示，接受漢光演習正面報導影片刺激的受訪者中，接近六成（58%）認為國軍有足夠的能力保衛臺灣；沒有觀看影片的控制組中，認為國軍有足夠能力保衛臺灣的比例占四成二；而受到漢光演習負面報導影片刺激的受訪者中，只有三成五左右認為國軍有足夠的能力保衛臺灣。顯示民眾的認知評估確實會受到訊息內容的影響，且更傾向於關注漢光演習出現事故、國軍軍紀不佳等負面訊息，也更容易轉發。

解方：強化媒體識讀與增加假訊息傳遞成本

從相關研究與民意調查可以發現，為快速獲取資訊，民眾並不會逐一審視資訊來源與內容正確性，且受到個人特質與心理因素影響，傾向於接收與自身立場一致、負面情緒的訊息。再加上面對龐大而雜亂的資訊，個人對單一訊息的注意力有限，即便事後得知澄清資訊，但假訊息散布已覆水難收，民眾對轉發澄清訊息的動機亦相對薄弱。



透過報導國軍相關影片播放畫面進行實驗調查（左），發現正、負面影片對民眾認知國軍保衛臺灣能力造成影響（右）。（資料來源：國防安全研究院，台灣國防安全民意調查）



烏克蘭在2014年克里米亞危機後，積極透過公民社會發展與媒體識讀教育，以及成立烏克蘭危機媒體中心（Ukraine Crisis Media Center）等組織培養民眾分辨真偽及查證的習慣。（Source: Ukraine Crisis Media Center, https://uacrisis.org/en/uavsdisinfo-commentary-on-the-governmental-concept-for-protecting-ukrainian-information-space-from-disinformation）

故此，培養民眾「媒體識讀」（media literacy）的能力就顯得格外重要。本次俄烏戰爭中，善於認知作戰的俄羅斯並未完全主宰戰時傳播場域，部分原因在於烏克蘭在 2014 年克里米亞危機後，積極透過公民社會發展與媒體識讀教育，以及成立烏克蘭危機媒體中心（Ukraine Crisis Media Center）等組織培養民眾分辨真偽及查證的習慣。烏克蘭總統與政府高層也善於運用社群媒體，獲得國內民眾與國際社會支持。故如何在平時培養民眾思辨能力，戰時提供即時且正確的資訊與查核管道，對政府而言是當務之急。

然而，從俄烏戰爭發展過程也可以發現，認知作戰的攻擊方也可能利用事實查核平臺的公信力散布假訊息，或是透過社群媒體的弱點來進行認知作戰與犯罪活動。故增加散布的成本也應納入假訊息防制體系中，如加重散布假訊息的刑事責任與強化執法，或建立認知作戰的人工智慧監控與警報系統等。然而，目前國際社會對於打擊假訊息的最佳模式仍莫衷一是，故臺灣仍應借鏡各國作法，逐步構建有效且符合民主法治的「打假臺灣 style」。

假訊息及認知作戰之態樣與趨勢

◆ 調查局資安工作站 ── 蘇　羣

「假訊息」及「認知作戰」形成之威脅及肇生之危害已不容小覷，與境外勢力介選、各國疫情、俄烏戰爭、兩岸情勢均息息相關。

假訊息已成全球重視議題

現代網路科技蓬勃發展，每個人觸手可及的資訊量及範疇均已大幅擴展，與過去不可同日而語，同時人與人之間的溝通聯繫亦更為即時而緊密，雖然身處現代的我們受益良多，但背後卻有層層隱憂於近年漸漸浮上檯面，甚至已成為全球各國重視的議題之一，「假訊息」即是其中一環。

學者指出中共「認知作戰」目的，在壓縮我國際活動空間、渲染擴大對我軍事威懾、擾亂我社會秩序，造成國人心理紛擾，削弱抗敵意志，奪取輿論主導權，對我民心士氣影響十分巨大。（Source: Innovation Hub, https://www.innovationhub-act.org/sites/default/files/2021-01/20210122_CW%20Final.pdf）

國防部學者指出，中共對我進行「認知作戰」對象不僅限於國軍，而是臺灣社會整體，所以在各領域都可發現其遂行認知戰的痕跡。此「溫水煮青蛙」方式，一般民眾不易察覺，不可不防。

由於我國位居特殊地理位置，面臨複雜之國際關係、兩岸情勢，應運而生的潛在國安威脅除了陸海空戰等傳統戰爭型態、經濟戰、網路戰，甚至是未來的太空戰之外，其實威脅的場域亦已拓展至非實體範疇，例如：你我的大腦。「認知作戰」於是自此衍生而成，試想若境外勢力透過投放「假訊息」，而具有撼動、操弄社會大眾認知、思想的能力，自然可不戰而屈人之兵，不必耗費軍火發動實體戰爭，即能以相對較低的成本達成其目的。

在 109 年 228 連假期間，時值全球新冠肺炎疫情正啟，國內上下無不嚴陣以待之際，我們面臨來自境外的三波假訊息攻擊，不實訊息充斥於各方社群及通訊軟體之中；在 110 年間，我們再度面臨來自境外的大量假訊息及爭議訊息，境外勢力利用網路的匿名性創建數以百計甚至更多的網路身分，如臉書帳號，以少數人即可進行操作並有計畫地跨平臺層層傳遞，如槓桿般營造出大宗網路聲量，散布層面對我國社會而言可謂滲膚入骨，致使社會大眾

於閱聽網路資訊時，可能誤信其傳遞之虛假訊息，基於錯誤的認知作出判斷及行動。調查局鑒於其衍生之危害實不可小覷，已積極關注應處並針對不法加以偵辦。

近年境外勢力操弄假訊息案例

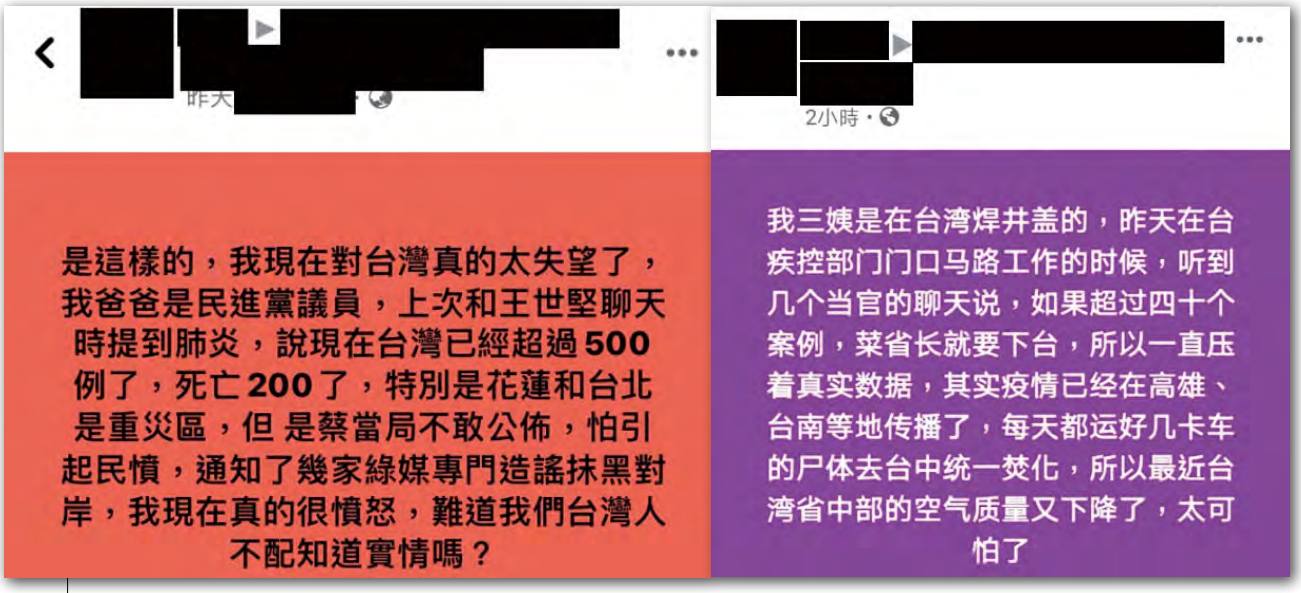
一、109 年 228 連假期間，境外勢力發動三波假訊息攻擊

約於 109 年 2 月底至 3 月中，中國大陸網民因「不滿我國禁止口罩出口政策」及「認定我國網民潛伏於大陸社群伺機批判防疫不力」而心生不滿，於是基於報復心態，群起串聯在我國民眾習慣使用的社群平臺上發動假訊息攻擊，意圖製造恐慌、架空我國行政及司法資源，並在干擾防疫政策之餘順帶破壞政府公信力。

這些中國大陸網民在微博社群集結、相互討論，除了蒐集製作假訊息的題材、研析兩岸語法差異，甚至擬定散布策略，以提升假訊息辨認難度及擴散成效；在這個案例中，他們製作出一個版本的假訊息後，即透過臉書人頭帳號到我國民眾常瀏覽之臉書社群及媒體專頁進行散布，甚至偽裝成本土網民進行發文、留言及與人互動，就是為了混淆及規避我國司法查緝，並使民眾誤信進而轉載至個人臉書頁面或 LINE 社群，達成更深更廣的擴散效果。

調查局在這期間察覺異狀，特別組建專案小組加以應變，經過完善的溯源調查，剖析出境外勢力運用的假訊息態樣及手法有三：

（一）**模組化文字訊息攻擊**：套用假訊息模板，利用我國時事、公眾人物、地名等進行套換，加速假造及散布效率。



境外勢力運用的假訊息態樣之一：模組化文字訊息攻擊。（圖片來源：作者提供）

境外勢力運用的假訊息態樣之二：客製化圖文訊息攻擊，右圖為偽造公文。（圖片來源：作者提供）

（二）**客製化圖文訊息攻擊**：擷取我國新聞媒體畫面、政府機關公文，假造不實圖文訊息，再搭配我國政府或公眾人物名義散布，增加誤導成效。由於遭偽造之新聞畫面、公文甚有行政院關防及院長簽名章已至足以亂真程度，這類假訊息極易陷民眾於錯誤，讓眾人誤認假訊息內容是客觀事實。

（三）**反制澄清抹黑攻擊**：擷取我國官方澄清或宣導防範假訊息之圖文，加工製成「假澄清」及「假宣導」訊息，讓國人錯認政府發布的真訊息是網路假訊息，混淆國人視聽。

在境外勢力發動前述三波假訊息攻擊的期間，調查局即時應變溯源研判，除了針對以上各種態樣的假訊息進行公開說明，更將其手法揭露予社會大眾知曉，並提出具體預警，供民眾預先防範。

境外勢力運用的假訊息態樣之三：反制澄清抹黑攻擊，左圖為假訊息，右圖為真訊息。（圖片來源：作者提供）

二、110 年境外勢力手法升級，對我國大量散布不實訊息

110 年間調查局發現境外敵對勢力藉創建無法識別真實身分的人頭帳號，利用結構化、流程化的手法，將不實圖文訊息迅速、大量地投放到我國社群，意圖操弄疫情、政治輿論，進行認知作戰。

最初境外勢力先於具網路聲量的卡提諾論壇註冊帳號，接著頻繁發布有關疫情及政治的爭議訊息，甚至利用網頁瀏覽器開發者模式，編輯竄改 PTT 既有文章內容進行造假，再藉由境外人士管理的數個臉書粉絲專頁如「茯苓有點兒甜」進行第一層傳貼及散布，再利用數以百計的臉書假帳號進行第二層轉傳分享，廣泛散布至本土在地社團、宗教、生活娛樂等各類臉書社群，促使社群成員如我國民眾因誤信而再度轉發；於是，這些假訊息、爭議圖文便透過此般計畫性分工層層轉傳散布，深入我國社會各階層，不斷地投放有所意圖的訊息，激化對立、加深矛盾，並讓其意圖型塑的認知在我們的社會中持續蔓延。

調查局剖析釐清網路上此類跨平臺製假、布假的手法後，隨即發動偵辦，並針對前面所提的不實訊息傳遞結構揭曉予社會大眾，讓民眾在閱聽網路資訊時，能意識到獨立思辯、確認訊息真確性的重要，進而遏止危害的擴散。

獨立思辯與多加查證 方能抑制假訊息流傳

隨著時間的演進及民眾識別訊息能力的提升，網路社群上流傳之假訊息已有質的變化，從較為粗糙夾雜境外習慣用語、簡體字、模板化的型態，轉變成使用我國習慣用語、結合順應在地時事、以第一人

境外勢力最初於具網路聲量的卡提諾論壇頻繁發布有關疫情及政治的爭議訊息（左），甚至編輯竄改 PTT 文章內容進行造假（右），再藉由境外人士管理的數個臉書粉絲專頁進行第一層傳貼及散布，後又利用數以百計的臉書假帳號進行第二層轉傳分享，廣布至本土各類臉書社群，促使民眾因誤信而轉發散播。（圖片來源：作者提供）

當社會大眾在網路上閱聽資訊時，假訊息如同現實中俯拾即是的廣告訊息，以似真亦假、真假參半的言辭，誤導群眾、引起爭端、發酵輿論，進而肇生社會混亂與危害。

稱或第三人稱視角訴諸情緒之辭，遊走在現存法律規範的灰色地帶；策略從直接灌輸目標群眾錯誤認知，轉變成間接觸發目標群眾負面情緒及激化立場；散布模式從境外公開製假再直接投放至境內社群，轉變成隱匿製假流程並改採以大量人頭帳號模仿境內社群用戶，跨多重平臺進行轉傳分享，有如藉人頭帳號為媒介在社群間建構起訊息流通樞紐及通路。當社會大眾在網路上閱聽資訊時，這些背後有所意圖的訊息通路就會像現實中俯拾即是的便利商店投放有如咖啡半價般的廣告訊息，以似真亦假、真假參半的言辭，誤導群眾、引起爭端、發酵輿論，進而肇生社會混亂與危害。

有鑑於此，根本解決之道即為培養獨立、邏輯、思辯的能力，調查局呼籲社會大眾在接收來自網路上的訊息時，務先謹慎思考查證，不輕易隨之起舞，為自己發布、轉傳的訊息內容負起責任，共同維護網路環境與秩序；調查局亦將積極查辦在網路上肆虐的假訊息，並即時揭露境外勢力、有心人的操弄手法，供民眾提高警覺、預先防範，有效遏止假訊息危害之擴散與發生。

當網頁愛上人工智慧

◆ 社團法人台灣 E 化資安分析管理協會、嘉義大學資訊工程系教授 — 王智弘

要在多管齊下的誘騙中全身而退，最好的防範方式就是讓自己隔絕在威脅之外；而人工智慧是否能幫忙，一眼就看穿惡人的把戲？

原來是場騙局

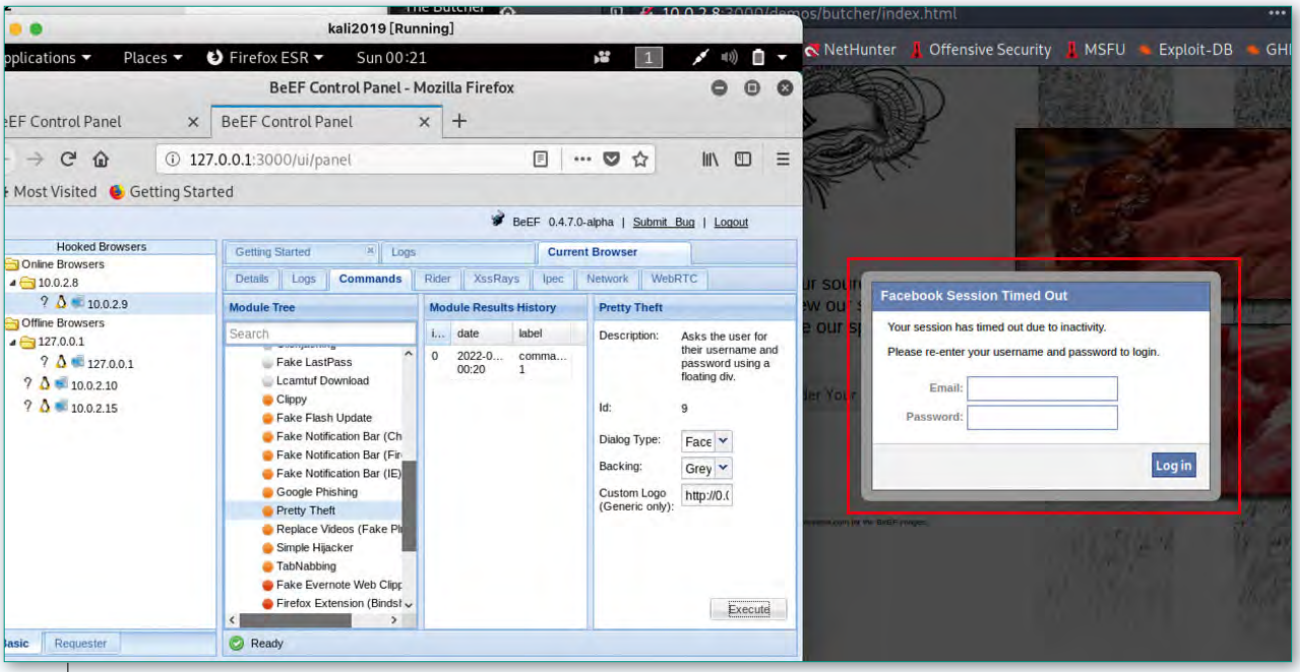
「盡信網路，不如無網路」，已成了現代人對於網路上充斥著太多假訊息，詐騙術無所不在的深沉無奈與抗議。以往享受於瀏覽網頁、沉浸在無論是文字知識的充實之樂，或是音樂影音的華麗饗宴，感受到無比的雀躍。現在卻得要處處防範、時時小心。深怕一個錯誤滑鼠的「click」，造成難以彌補的損失。在大量的影音互動所帶動的誘惑之下，詐騙的行為也因而開始升級。人們很難在多管齊下的誘騙之下能全身而退，最好的防範方式就是讓自己隔絕在這樣的威脅之外。然而，我們現今的科技足以支援這樣的服務嗎？哪些網站是有疑慮的？科技究竟能否幫我們忙，一眼就看穿惡人的把戲？

現今網路上充斥著大量假訊息，詐騙術無所不在；然而，亦有許多網站可能本身沒有惡意，但卻因為具有漏洞而遭駭客利用犯罪。

我們常聽到有一種駭客攻擊方法稱作「跨站腳本程式碼攻擊」（Cross-site Scripting, XSS），讓你看似網站是正常的，但卻是潛藏危機。這些網站可能本身是沒有惡意的，但卻因為具有漏洞（Vulnerability）而遭受了駭客栽贓的禍害。網路上種種迷幻的效果，讓人目不暇給，也讓人覺得眼見的內容竟然也非事實。譬如社交工程裡的釣魚（Phishing）手法，甚至是復刻整個網站內容以達到欺騙的目的。近期新聞便有關犯罪者製作假的銀行網站並傳送簡訊給被害者，由於太過仿真，使得好幾十人以上受騙，損失竟逾千萬元。在數位包圍下生活，我們對於實與虛、真與假、正本與副本的界線判定已退化，尋求外力協助是可以理解的想法。**「以科技解決科技所製造的問題」，看來是當前可能的藥方**，否則當有一天你發現了所有背後隱藏的攻擊程序，才驚覺，原來之前看到的那些亮麗的網路資訊，都只是個騙局。

欺騙花樣層出不窮

當你連上了惡意或是有漏洞的網站，它所能搞欺騙的花樣可謂千奇百怪。大家可能會想到的是，假的網站可能會盜取使用者的密碼。因此現在防範的方式類似透過一次性密碼（One-time Password, OTP），傳送簡訊到手機或 email 信箱。然而，實際上，駭客透過腳本程式碼，如 Java Script，可以變出許多不同的花樣，令人防不勝防。例如透過跳出式視窗（Popup Window）的社交工程方式，於網頁瀏覽



利用在 Kali Linux 中的 BeEF 工具進行漏洞利用（Exploitation）測試，出現 Session 過期的通知，誆騙使用者鍵入正確的密碼。（圖片來源：作者提供）

的時期跳出類似 Session 過期的通知，誆騙使用者鍵入正確的密碼。此外，還有多種不同型的攻擊運作，例如，透過啟動自動重新導向（Redirection）的方式或是修改 HREFs 的連線網址，讓使用者不自覺中連線到具有 Hook 的惡意網站；也有其他的手法像是開啟相機（Webcam）、播放聲音、偽造虛假的通知欄（Notification Bar）等。每個人在長期地接受這些攻擊，不禁要問，如何能還我一個乾淨的瀏覽空間，告訴我哪些網站可連，而哪些網站有安全疑慮呢？

黑名單與白名單

網站的安全評分是一直以來許多專家建議的方式。安全評分的方式透過許多綜合的指標來評估一個網站的安全性，也透過一些回報機制來登錄部分問題網站。我們可以從網路上查到許多這類的服務，包括像是針對釣魚網站的檢查，如趨勢科技。[1] 此外，Google 的「安全瀏覽」（Google Safe Browsing）每天也都會進行數十億個網站檢查，以找到可能的威脅。而像是 ScamAdviser [2] 則能夠檢測可能的釣魚及詐騙網站，相當具有準確性。另外，也有針對網站聲譽（Reputation）

[1] Trend Micro, https://global.sitesafety.trendmicro.com/

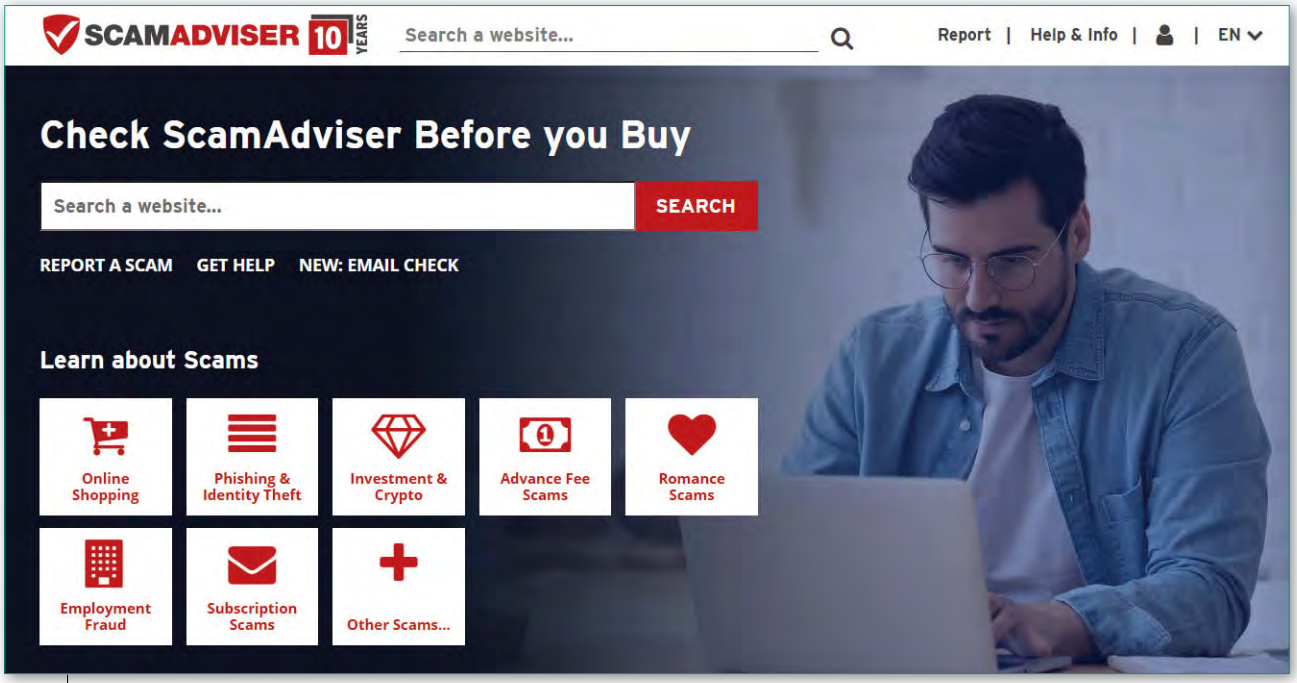
[2] https://www.scamadviser.com/

進行評分，如 URLVoid，[3] 能夠透過超過 40 個以上眾多不同的黑名單報告（Blacklist Report）資訊進行評估；亦有提供網域註冊（Domain Registration)， 從 whois 查詢網域資訊、Reverse DNS、ANS 以及位置資訊等。此外，著名病毒檢查網站 VirusTotal [4] 也可對於 URL 是否為惡意的情況進行檢查；而像是 Cisco Talos Intelligence [5] 也是一個相當知名的網站威脅分析工具。

上述的檢測服務，需要定期更新名單或是評估規則。因此雖基本上足夠使用，但難免也會有一些漏網之魚。此外，使用黑名單方法比較擔心的是因為檢測錯誤而導致用戶誤入有威脅的網站。另外一種方式則是建立白名單（Whitelist），只有被允許的網站或網域才能夠連上，其餘則進行攔阻。這樣做法安全性高，但對於用戶的限制也相對多，造成使用經驗與感受不佳。我們其實可以透過簡單的自救的方法，初步排除這些駭客的陷阱。

簡單自救方法

一、是否為安全加密連線？[6] 憑證（Certificate）是否有疑慮？



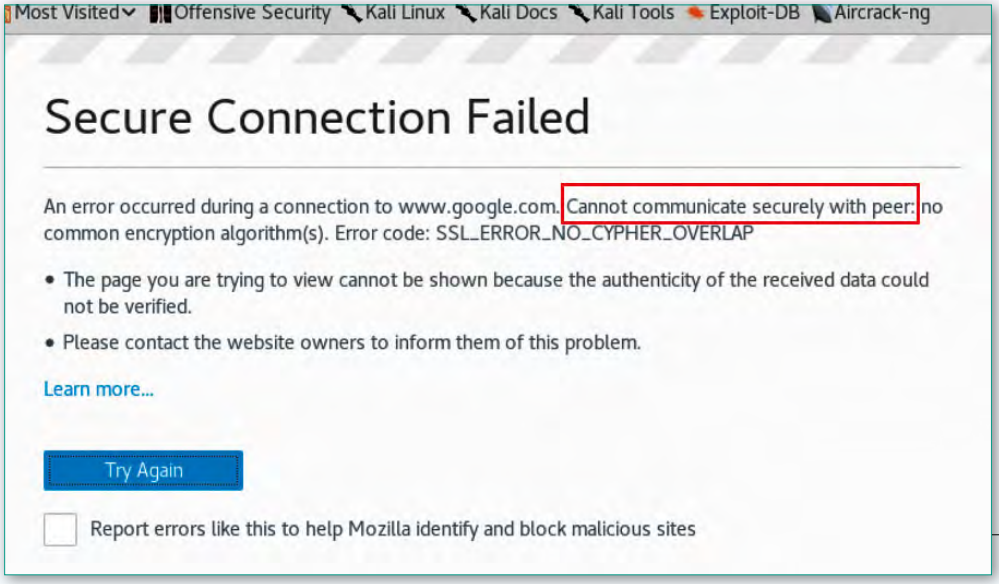
ScamAdviser 是一個免費的網站安全檢測服務，透過多種不同的指標來檢查網站是否安全可靠，使用者只要輸入網址就會顯示結果。（Source: https://www.scamadviser.com）

[3] https://www.urlvoid.com/

[4] https://www.virustotal.com/gui/home/url

[5] https://talosintelligence.com/

[6] 建立安全加密連線是保障資料的絕佳方案。我們連線的網站是否具備 TLS（Transport Layer Security）的安全機制雖然不是惡意網站判定的唯一方式，然而如果你的連線是正在進行帳號密碼的登錄，或是類似於購物網站要處理訂單或是信用卡資料的填寫，那加密與否就成了相當關鍵的問題。



Google 網站有強制安全傳輸的機制，連線若受到攻擊，會出現連線失敗的回應。（圖片來源：作者提供）

我們鍵入網址時，可能不會加上 https:// 或是 http://，但安全網站會將其轉換成 https 的安全連線。然而有項駭客的技術稱為 SSLStrip，可透過中間人攻擊，將原來要連線至 https 的重導向而映射到 http 連線，駭客因此能夠擷取重要的傳輸機密。而目前最新技術加上強制安全傳輸的機制（HTTP Strict Transport Security, HSTS），不允許跟網站之間進行無安全加密的傳輸，如此應可避免這類攻擊。此外，若遇到安全連線時憑證有問題的情況，如類似「您的連線不是私人連線」，或者是「網站的安全性憑證不可靠」等警告頁面，也請勿按下「仍要繼續」，以免引來隱藏風險而不自知。

二、睜大眼睛注意網址

我們在連線網站之前，通常將游標放在連線處，會出現連線的 URL 資訊。[7] 建議要注意 URL 的內容，以下有幾個簡單的判斷方式：

（一）故意與某些知名網站類似，但卻有一些差異，如 go0g1e，或是 rnicro.soft.com 之類的，讓使用者產生錯亂。

（二）縮短網址（Short URLs），例如，bit.ly、TinyURL 所提供的縮短網址服務，能夠取代長網址而使得連結的交換較為便利。然而由於這類短網址掩蓋了真正網址的諸多資訊，譬如真正的域名以及隱含的參數或檔名等，因此判斷良善或惡意並不容易。[8]

（三）網址前放置令人信賴名稱，如 google 後面再加上擴增的網域名。例如 http://login.google.com.

[7] 注意有些惡意透過 XSS 攻擊，其連線實際上是 Submit 按鈕以及一大串的填入資料，此時要避免與其連線。

[8] 基於過去許多安全的事件也因縮短網址而起，建議連線時仍要特別留意。

myphishing.com/welcome.html，上述顯然不是 google 的網站，但前面的域名卻又與 google 登入的名稱相同，藉以混淆視聽。[9]

（四）注意特殊字元，例如是否有類似 email 的 @ 符號，或是很多的點（dot）或斜線（/, slash）。譬如一般的網址其 dot 的數量大概為 3 個，如果過多，那麼可能會是有問題的網站，如上述 google login 的例子。

（五）查詢網域名稱註冊時間是否最近才建立；若是最近註冊，應考慮駭客為釣魚而建立的新網域。

（六）要特別留意連線的 URL 是否為 IP 而非網域名稱。

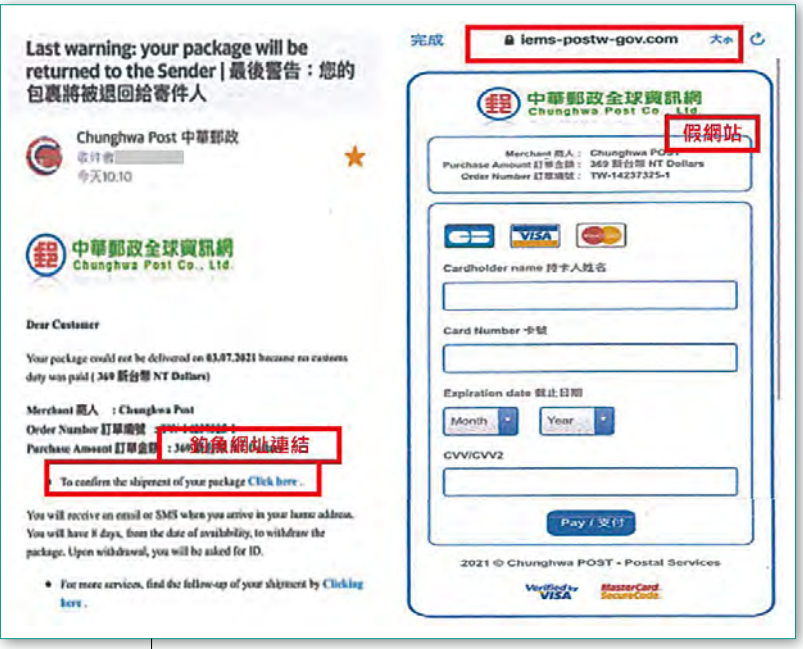
三、透過評分網站檢查後再連線

四、開網站後有問題，儘速離開

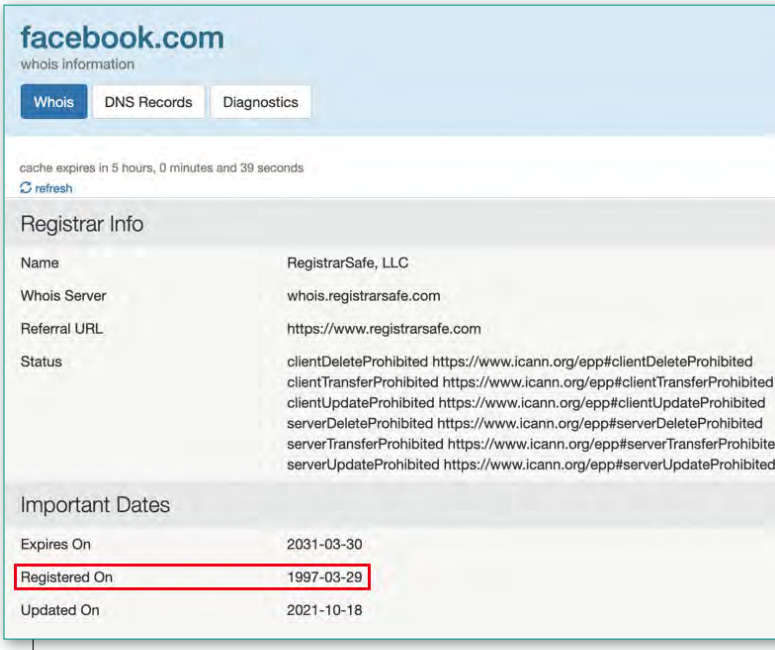
打開網站後要注意觀看內容，若有疑問，請儘速離開；然而有太多類型的攻擊是在一連線便進行，而且在極短時間內完成。

機器學習的可能與不可能

從上述的網址判別方法，可以思考透過更為自動的方式來進行。雖然目前已經有許多網站評分的服務，但若要找到潛藏的惡意網站，仍力有未逮。**透過機器學習（Machine Learning）的機制，以資料訓**



釣魚網站會故意採用與官方網站類似的網址，誘騙使用者登入，藉此竊取帳密資訊。（圖片來源：新北市政府警察局蘆洲分局，https://www.luzhou.police.ntpc.gov.tw/cp-1087-82938-23.html）



透過網域名稱註冊時間，可考慮是否為駭客為釣魚而建立的新網域；圖為 facebook.com 在 whois 所查詢的網域名稱註冊資訊。（圖片來源：作者提供）

[9] 注意 URL 長度，若過長，除了可能是上述的情況或是名稱編碼問題外，也可能是有一些惡意的參數輸入資料。

練方式替代人工制定規則，可能是對抗目前不斷激增且變異的惡意與釣魚網站的一個可選方案。

透過特徵（Feature）的篩選以及資料集的訓練，將會產生一個模型，[10] 該模型可儲存於雲端服務或是架設一臺代理伺服器（Proxy Server）以作為攔截檢查惡意連結，以及進一步深度檢測之用。圖 1 為可能的架構想法，表 1 則說明可能的特徵類型。

可以思考透過不同環境的訓練資料以強化情境分析。譬如有些惡意的連結來源是經由 Email，有一些是透過社群平臺，如 Facebook、Twitter 等，有些則是即時通訊如 Line、IG、Messenger 等，因此透過不同的訓練集或是模型參數，可以讓判斷更為精準，而若是對於網站有疑義，仍可經過一些深入的檢測模式（透過代理伺服器進行以避免用戶端身處險境）進行更為精準的判斷，提供用戶更好的安全監控及過濾服務。

網路安全與人工智慧之競合

面對科技，我們常會悠遊於它所帶來的便利，但也始終擔心它的負面效應。網

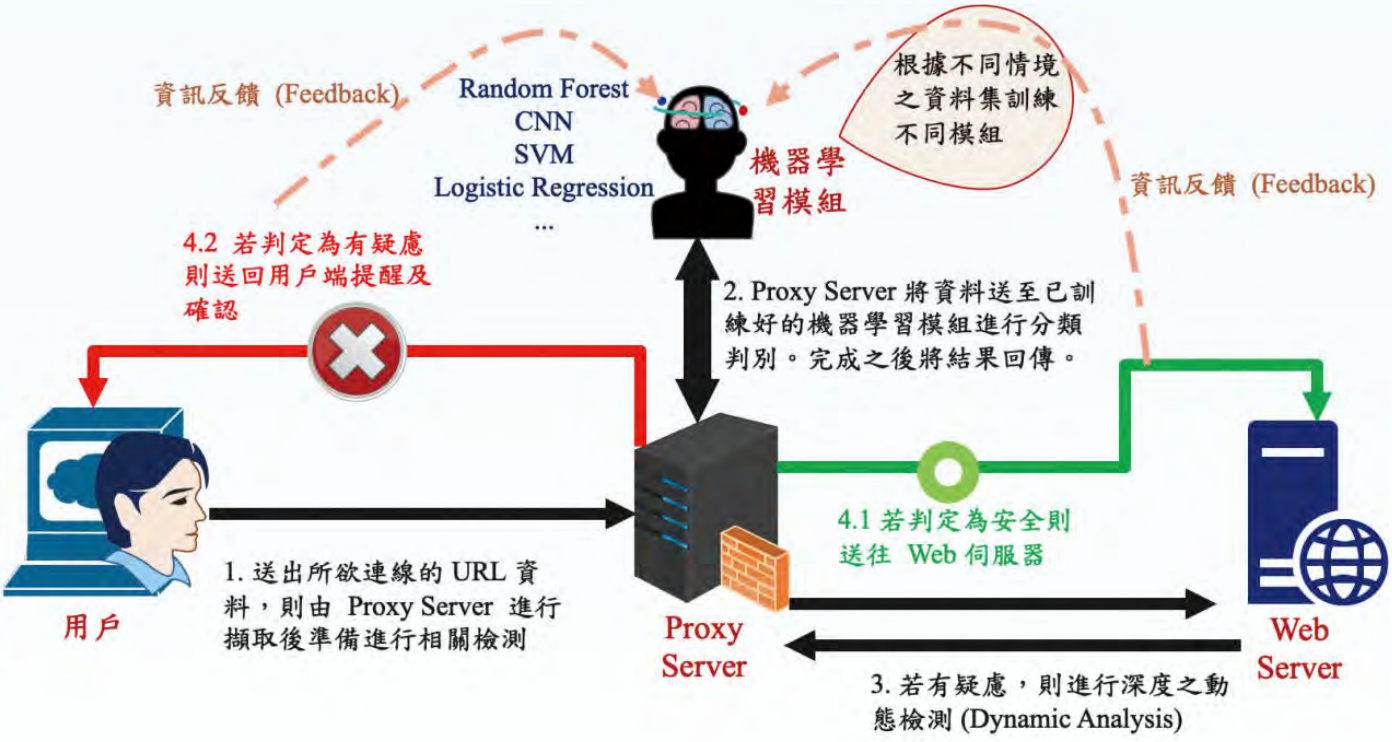


圖 1　整合機器學習的網頁安全性判別模式

[10] 如採用隨機森林（Random Forest）、卷積神經網路（Convolutional Neural Network, CNN）或其他機器學習模式。

表 1　網頁連結之安全性特徵例舉

安全性特徵	舉　例
從 URL 字面上所取得的特徵	URL 的長度、是否使用 IP 位址、是否使用縮短網址、是否有 @ 的符號、URL 中出現‘.’（dot）及‘/’（slash）次數、是否有前綴（Prefix）及後綴（Suffix）、是否使用 https 開頭、是否使用特殊的埠號（Port）等
URL 連接之網頁內容或行為	回傳網頁具有內部或外部連結的數量、是否使用跳出式視窗（Popup Window）、服務表單處理程序 Server Form Handler（SFH）是否為空白或是指向不同網域、是否啟動電子郵件服務傳遞資訊、是否載入大量外部網域之圖片、是否重導向等
網域及網站排名之相關特徵	網域名稱註冊距離現在時間、網站的名聲或排名、網站的流量大小等

路成癮、健康損害以及安全隱私的破壞都是我們所熟知的問題。然而，作為新一代科技人，我們要能夠掌握科技的脈動，要能駕馭科技而不是被科技所支配。當安全問題能夠假人工智慧之手而獲得更好的保障，這將是對抗惡意、詐欺等行為最佳的良藥解方。然而人工智慧也面臨自身系統被攻擊的問題，如最近非常熱門的研究議題—深偽技術（Deepfake），把深度學習（Deep Learning）與偽造（Fake）結合在一起，這讓依賴人工智慧為安全判斷依據的防衛方法面臨不小的威脅。「道高一尺，魔高一丈」，看來這場網路安全與人工智慧之間的競合勢必還有一大段長路要走。

社團法人台灣 E 化資安分析管理協會（ESAM）

AI 時代的網路安全

英美電影《模仿遊戲》（The Imitation Game）曾介紹圖靈於二戰期間協助盟軍破譯德軍密碼的真實故事，而圖靈當時所發明的密碼機即為現代電腦雛形。（Photo Credit: The Weinstein Company）

◆ 中興大學國際政治研究所副教授 ── 譚偉恩

英國數學家圖靈（Alan Turing）於 1950 年經由測試發現，計算機在特定條件下可以和人類的心智思考相比擬，進而提出「人工智慧系統」（artificial intelligence system）的概念。[1]

隨著數理計算機的相關技術日臻成熟，人類社會的經濟、教育、醫療、托育長照、環境保護、交通運輸，以及公共行政和執法等，無不在一定程度上與圖靈提出的人工智慧（AI）鑲嵌在一塊兒。

[1] Alan Turing, "Computing Machinery and Intelligence," *Mind*, Volume LIX, Issue 236 (October 1950): 433-460.

AI 可以概分為兩種亞型：一種是與人類有互動的輔助型智能系統，旨在幫助人類更快更好地完成工作（左）；第二種亞型的 AI 不直接與人互動，多數是工廠中自動化生產的智能系統（右）。

AI 的應用及其問題

市場上目前 AI 技術的開發主要是以創建「像人類一樣思考」的優等高階 AI 為主軸，藉由將計算機智能化，來分析客觀環境、學習特定事物，然後產出近似人類的理性判斷，但結果上更為精準。根據普華永道（PwC）的研究，大部分的 AI 可以概分為兩種亞型（subtype）：一種是與人類有互動的輔助型智能系統，旨在幫助人類更快更好地完成工作（例如停車）；此種類型的 AI 有時包括自我調適能力，可以配合使用者的實地需要做出情勢判斷，並在與人互動時進行自我學習和調整。第二種亞型的 AI 不直接與人互動，多數是工廠中自動化生產的智能系統；這種 AI 的工作範疇是固定的，很少會被增設新的工作項目，但在既有的工作內容中，其生產效率會透過自我學習而不斷提升。[2]

無論上面哪一種 AI 技術及其應用，計算機的功能與效率都會漸漸超越原始設計的智能水平，因此有可能對它的設計者、使用者，甚至是不特定的人群構成風險。詳言之，AI 在執行任務過程中的自我學習與資訊累積，讓它的適應能力與技術效能越來越純熟精準，以致有可能發生排除人類而獨自行動的風險。一個引起關注的例子是「AI 自動履歷篩選」；在美國已有高達 75% 以上的企業採用 AI 技術招募新人，

[2] 如果搭配物聯網系統，還可以輔助工廠生產線的管理事務。

取代傳統耗時的人資部門面試。然而，純熟精準的 AI 欠缺彈性，會將有額外才能或極具創意的求職者判定為資格不符，甚至有些企業的 AI 篩選系統會將主管核可的應聘者從名單中移除，導致企業最終痛失良才。[3]

AI 在應用上的另一個問題就是對於數據資料的取得和分析，這一部分與網路安全密切相關，有越來越多的犯罪是在網路上利用 AI 進行侵權和獲利。該如何因應，讓 AI 的總體效益大於潛在損害的結果，是 AI 技術與應用普及化的同時，難以迴避之挑戰。舉例來說，蒐集、分析和處理不特定多數人的某些資料是應用 AI 的關鍵環節。企業需要這些資料來進行 AI 的培訓，進而應用於廣告行銷和線上商務；國家需要這些資料作為政策擬定時的參考，或與人民互動交流意見，落實政策的風險溝通和施政彈性。由於透過 AI 蒐集和分析大數據變得越來越頻繁，掌握這些數據資料的使用者便取得了不對稱的資訊優勢，一旦用於犯罪，後果往往不堪設想。然而，對這些數據取得或使用的嚴格規範會減緩 AI 的發展，兩者間要如何平衡是各國正面臨的兩難困境。

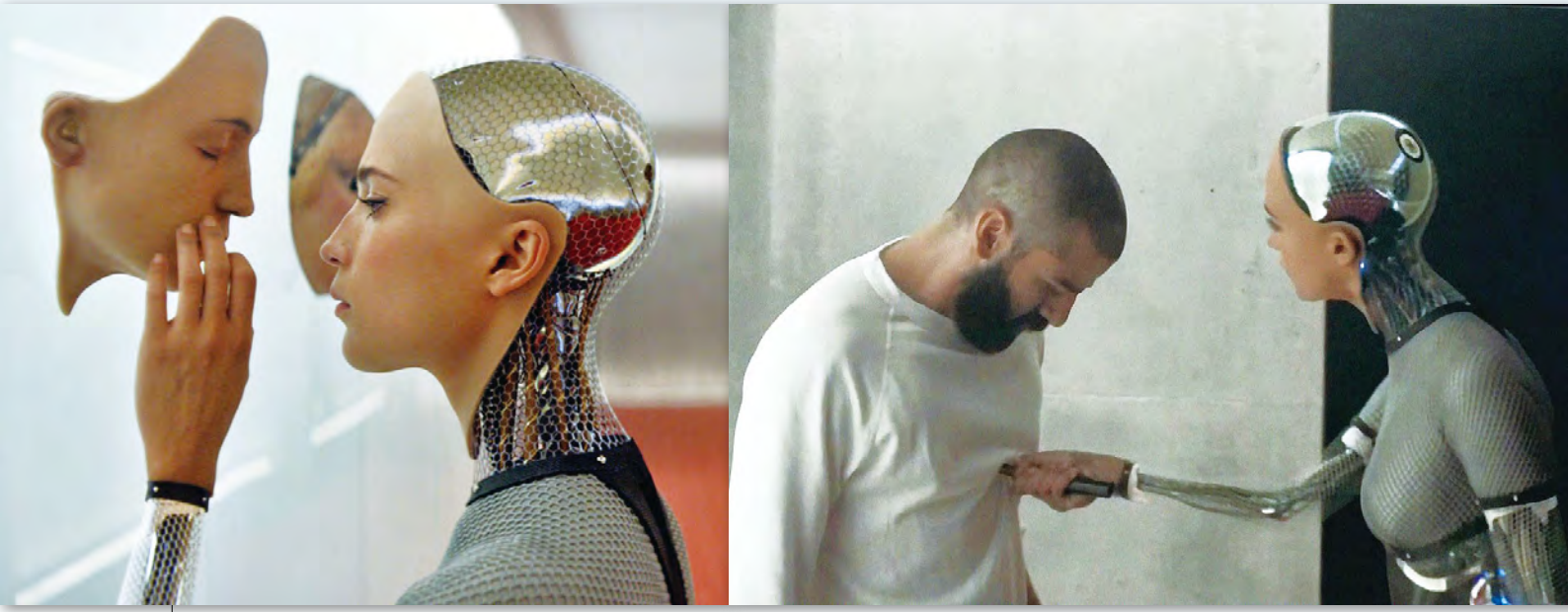
AI 對網路安全造成的威脅

AI 對網路安全的影響大約從 2017 年被各國正視，[4] 美國的 FBI 甚至針對犯罪組織使用 AI 的問題召開過專門會議。由

透過 AI 蒐集和分析大數據變得越來越頻繁，掌握這些數據資料的使用者便取得了不對稱的資訊優勢，一旦用於犯罪，後果往往不堪設想。

[3] Sarah K. White, "AI in Hiring Might Do More Harm than Good," *CIO*, (September 17, 2021), via at: https://www.cio.com/article/189212/ai-in-hiring-might-do-more-harm-than-good.html

[4] 一篇非常具有參考價值的論文是：Alex Wilner, "Cybersecurity and Its Discontinuities: Artificial Intelligence, the Internet of Things, and Digital Misinformation," *International Journal*, Vol. 73, No. 2 (June 2018): 308-316.



無論哪種 AI 技術，AI 功能都會漸漸超越原始設計的智能水平，因此有可能對它的設計者、使用者，甚至是不特定的人群構成風險。英國電影《人造意識》（Ex-Machine）即描述完美的 AI 機器人，最後卻殺掉設計者之情節。（Photo Credit: Universal Pictures）

於網路是一個虛擬空間，讓侵害權利的犯罪行為得以隱身其中，並藉助科技帶來之轉換效果對真實世界的秩序造成破壞。英國倫敦大學學院的報告指出，犯罪者透過 AI 技術破解密碼、複製人類語音，以及其他諸多的非法侵權技術。其中深偽技術（deepfake）被列為犯罪結合 AI 後對網路安全的首要威脅之一，因為這有可能讓人們對任何影音或視頻資訊的傳遞失去信任感，嚴重妨礙人類社會資訊交換與傳播的現狀。此外，上述報告也指出，運用 AI 的犯罪與傳統犯罪不同之處在於，它的犯罪效能可以在網路上被快速分享、重製與再現，甚至在犯罪組織的包裝下成為一種「服務」來銷售，以致國家司法機構難以有效抑制。[5]

此外，COVID-19 疫情爆發後，各國遠距工作人數大增，導致網路端點之間的聯繫暴露在風險中。許多企業或是智庫的分析報告均指出，資訊科技（IT）與營運科技（OT）已成為網路犯罪者的主要侵權對象，特別是數位支付及加密貨幣的攻擊事件或竊取行為明顯增加。由於犯罪者可以透過 AI 的協助來生產惡意軟體或非法取得個資，再將之出售給其他犯罪者來營利，暗網交易變得越來越熱絡。[6] 相較於過去，網路侵權犯罪多半是由專業的駭客為之，

[5] 詳見：“AI-enabled Future Crime,” https://www.ucl.ac.uk/jill-dando-institute/sites/jill-dando-institute/files/ai_crime_policy_0.pdf。

[6] Wytske van der Wagen and Wolter Pieters, “From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks,” *The British Journal of Criminology*, Vol. 55, No. 3 (May 2015): 578-595.

英國倫敦大學報告指出，犯罪者透過 AI 技術破解密碼、複製人類語音，以及其他諸多的非法侵權技術。美國電影《關鍵報告》（Minority Report）即描述凶嫌透過 AI 技術，將責任移花接木嫁禍予無辜者之情節。（Photo Credit: FOX）

但 AI 與暗網交易結合之後，資訊科技與營運科技會面臨更多元與廣泛的網路攻擊。顯然，AI 技術的普及化增加了我們正規生活中面臨威脅之風險，而這些風險在網路世代可歸類為兩大類：一、惡意軟體攻擊；二、涉及社交工程（social engineering）的技術性攻擊。

第一類可以說是犯罪者受惠於 AI 的最佳證明；由於 AI 在速度和效率方面的突出表現，讓犯罪者得以將之用以強化勒索軟體的破壞性，升級病毒避開防火牆、深入企業計算機網路，癱瘓運作並竊取重要資料。第二類是藉由 AI 技術編寫縝密的「故事」進行社交詐騙；犯罪者透過 AI 有系統地分析特定人士的網路使用慣性，再設計個人化的「故事」進行網路詐騙。數據安全專家 George Dvorsky 及 Brian Wallace 等人曾經指出，AI 是兩面刃，對駭客或有心犯罪人士而言，是絕佳的新一代武器。[7]

犯罪與相關風險之因應

許多國家已經發現，既存的法律規範很難對網路上的 AI 犯罪行為進行有效管制。或許也因為如此，私人性的網

[7] George Dvorsky, "Hackers Have Already Started to Weaponize Artificial Intelligence," *Gizmodo*, (September 11, 2017), via at: https://gizmodo.com/hackers-have-already-started-to-weaponize-artificial-in-1797688425

路安全措施相繼推出，例如較具代表性的阿西洛馬人工智慧原則（Asilomar AI Principles）。[8] 這個原則已獲得諸多業界人士的廣泛支持，在總共 23 項的原則性內容中，有幾個面向值得吾人注意。

首先，AI 研發之目的與使用可能在不久的將來會成為立法時的考量。研發者有義務對自己 AI 系統承擔責任；由於 AI 的自主性是透過海量數據資料的學習而來，但 AI 對什麼樣的資料感到興趣卻是研發者「價值觀」的反映。鑑此，在設計之初就應明確化與公開 AI 的目的，並同時在手段（means）與目標（goals）上給予清楚的說明。根據此原則，具有攻擊性或使用目的不明確的 AI 或相關應用，日後在立法上就應受到高密度審查，若研發者無法清楚交代此類資訊，政府就不應核可。

第二，因為 AI 一定會建立屬於自己的獨立性，所以「未來的不可控」必然是會存在之風險，研發者與使用者都應該預見且提早預防此類風險。第 7 項原則中特別提到 AI 如果出現意外也必須要有透明性，即對於釀成損害的因果關係要明確呈現並客觀上歸責。此外，第 8 項的審判透明性強調「司法性的決策」不能逸脫人類社會合理之解釋範疇，並且最終要由人類的監管機構保留審核權。

圖 1　阿西洛馬人工智慧 23 條原則內容

[8] 此原則的製訂背景與詳細內容可見：https://futureoflife.org/2017/08/11/ai-principles/。

AI 的治理不妨思考以法律賦予 AI 適當之權利與義務，使其對可能致生的風險或實害承擔責任。

最後，是因 AI 而產生的利益應予開放及盡可能公有化。在原則的第 23 項提及「公共利益」，認為 AI 的問世及應用要符合全人類的利益，而不是某一個國家或特定組織之利益。然而，「利益」的定義是什麼？這個問題的爭議性幾乎是不可能解決的，而定義不清楚的規範，無論是私人機構或公家部門，在執行上都會有困難，其最終的結果就是法律漏洞。

結語

不久的將來，人類社會現行的法律制度就會因為 AI 技術的發展和相關網路應用而大幅修正，其中網路犯罪的防治和相關侵權行為的歸責與賠償機制極需被處理。鑑於 AI 自我學習及自我調適後所可能產生的不確定風險，本文建議對於 AI 的治理不妨思考以法律賦予 AI 適當之權利與義務，概念上類似透過立法擬制給予 AI 有限或準法人的資格，使其對可能致生的風險或實害承擔責任。有別於傳統以自然人或法人為中心的立法，保障因 AI 的應用或商業化使用而發生之權利受損並提供救濟，是新一代治理規範的主旨。

金牌至上！中國大陸積極向各國運動員招手

◆ 調查局兩岸情勢研析處 ── 楊宗新

冬奧最受關注的歸化運動員谷愛凌與朱易，均以外貌兼具實力著稱；後者因中文程度與賽事結果不佳，最後竟慘遭中國大陸網民無情批評。

中國大陸外籍歸化運動員比例之高令人咋舌

在甫落幕的北京冬季奧林匹克運動會（下稱冬奧）中，中國大陸因主辦者身分，獲得所有項目的自由參賽權，共派出 174 名運動員參與 109 項比賽項目，其中有 31 項是首次參與。引發外界議論的，是這些運動員中，竟有數十人是外籍歸化運動員，包括知名滑雪運動員谷愛凌、花式滑冰運動員朱易，在冰上曲棍球代表隊男、女合計 48 人中，更有高達 28 人是歸化者，比例之高，令人咋舌。

中國冰上曲棍球代表隊男、女合計 48 人中，有高達 28 人是歸化者，比例之高，令人咋舌。（圖片來源：路透社／達志影像）

伴隨中國大陸歸化措施的不斷放寬，未來是否會進一步吸收我國運動員代表出賽，值得關注。

近年逐步放寬運動員歸化限制

中國大陸雖在意參與運動賽事的獲獎牌數，但過去仍以自身培訓之運動員為參賽主體，對外國運動員的吸收，則是近十年才開始盛行。

早期對吸納外國運動員不積極的原因，可從制度、心理兩層面觀之。就制度面而言，是中國大陸在國籍法上的自我約束。依據《中華人民共和國國籍法》第 3 條：「中華人民共和國不承認中國公民具有雙重國籍」、第 8 條：「申請加入中國國籍獲得批准的，即取得中國國籍；被批准加入中國國籍的，不得再保留外國國籍」規定，但凡不願放棄原國籍的運動員，均無法歸化。

就心理層面而言，中國大陸境內雖有 56 個民族，然在漢族人口占絕大多數的情況下，長期具有漢族沙文主義，認為漢族能透過文化同化其他少數民族，一旦面對不同文化者，即產生強烈的群我意識，使得大陸民眾最多只能接受華裔運動員歸化，而不能認同由非華裔之白人、黑人代表出賽。

促使其逐漸放寬歸化措施的原因，可能與經濟水平提升，大眾有更多時間關注全球體育賽事、文化素養提高後對「非我族類」之運動員有更多包容、目睹他國運動員歸化措施有成、運動員逐漸能接受放棄原國籍歸化中國大陸，以及政府高層支持運動員歸化態度有關。

足球是第一個改變的項目，2011 年在習近平支持下大幅引進歸化者，自此中國大陸歸化風氣大開。其他發展不佳的運動項目，都開始對外延攬人才。然因中國大陸國籍法並未配合修正，使得對於不願放棄原國籍的運動員，採取「規範上不承認雙重國籍，但事實上默認」的方式處理。

吸收外國運動員衍生的爭議

中國大陸現行對外籍運動員採取表面禁止雙重國籍、事實上卻默許的權宜歸化措施，無論在中國大陸境內或國際社會都引發爭議。

以谷愛凌為例，谷女父親為美籍，母親為陸籍，自出生開始即為美國公民，2019 年取得中國大陸國籍，開始代表陸方參賽，陸媒對外聲稱渠已放棄美國國籍，然而谷女對此始終不願正面回應，僅表示：「我在中國時是中國人，在美國時是美國人。」加以依據美國法律規定，但凡放棄國籍者，姓名會被公布在聯邦政府相關單位網站上，然而在網站上卻始終不見谷女之名（Eileen Feng Gu），使得幾乎所有媒體都認為其擁有美、「中」雙重國籍。

另一位被認為擁有雙重國籍者，是前美國冰上曲棍球職業聯盟球星瑞米史密斯（Jeremy Smith），渠於 2019 年轉赴大陸「崑崙紅星隊」打球，本屆冬奧前入籍大陸。近日《美聯社》向其求證是否放棄美國國籍時，他表示從未被要求放棄美國國籍。類似谷愛凌、瑞米史密斯等事實擁有雙重國籍者，在本次中國大陸冬奧代表隊中，可能不在少數，只是知名度不如前兩人高，因此沒有遭到媒體追逐探究。

至於心理層面的爭議，主要與歸化運動員的血統及是否會說中文有關。儘管北京當局近年逐漸對歸化運動員敞開大門，

但受限於文化，主要仍以接受具華裔血統者為主，基本上只要父母一方，甚至祖父母、曾祖父母中有華裔血統者，對中國大陸民眾而言都可接受，但如果毫無華裔血統，純粹憑藉技術卓越而歸化者，則難以被認同。

除血統外，另一評價歸化運動員的要素是—中文說得是否流利。據悉，外籍運動員歸化入籍前，必須會唱《義勇軍進行曲》，俾能在賽場演奏國歌時跟唱，因此，中文能力也是中國大陸社會評價歸化運動員的標準之一。以本屆冬奧最受關注的歸化運動員谷愛凌、朱易而言，兩人均以兼具實力及外貌著稱，前者雖是混血，但中文流利，賽前就已廣告代言不斷；後者是純華裔血統，但中文不佳，賽前雖備受關注，但卻慘遭網友出征。[1]

誠然，接受歸化運動員的原因，原本就是因為本國在該領域發展不佳，才會產生向外國優秀選手招手的需求，因此期待歸化運動員在賽場中奪得佳績，也是理所當然。然而相較於西方社會傾向在運動員

谷愛凌自出生開始即為美國公民，2019 年取得中國大陸國籍後代表陸方參賽，陸媒對外聲稱渠已放棄美國國籍，本人卻不願正面回應。（Photo Credit: Martin Rulsch, https://w.wiki/532g）

前美國冰上曲棍球職業聯盟球星瑞米史密斯在本屆冬奧前入籍中國大陸，曾向媒體表示從未被要求放棄美國國籍。（Photo Credit: Lisa Gansky, https://w.wiki/53JA）

[1] 甚有網友痛斥朱易講不好中文，要他「先學好中文，再談愛國」。《同為棄美轉中 北京冬奧 2 運動員媒體待遇大不同》，https://today.line.me/tw/v2/article/Kw0Z5Er。

歸化後即視為本國人看待，中國大陸社會更傾向把運動員當做奪牌的工具，能奪牌即為其歡呼，不能奪牌則揮之即去。

這種將奪牌視為唯一評價依據的做法，在本次北京冬奧體現無疑：奪得金牌的谷愛凌，頓時成為最具知名度的運動員，而原本預期有望奪牌但最後卻墊底的朱易，則猶如過街老鼠般地遭到網民無情批評。

我國運動員可能成為吸收目標

中國大陸近年積極吸收優秀運動員，我國也成目標之一。2019 年 11 月 4 日，國臺辦公布《關於進一步促進兩岸經濟文化交流合作的若干措施》，有關體育部分為第 25、26 條，[2] 均明確載明歡迎我方運動員以「內援身分」參加陸方聯賽與報考其體育院校等。

〈26 條措施〉公布後，國臺辦發言人朱鳳蓮進一步表示：「中國國家體育總局正在著手修訂相關辦法，預計 2020 年初可出爐，符合資格的臺灣運動員、教練和裁判等體育從業人員未來可在大陸持證上崗」，並指出臺籍運動員在中國大陸發展現況。[3]

由此可知，北京當局對我國運動員的吸收，係採漸進式做法，先改變運動員身分，將長期在中國大陸訓練、參賽的運動員視為「內援」而非「洋將」，享受與當地公民同等的「國民待遇」，未來這些人當中若有表現出眾者，則很有可能直接被陸方納入代表團參加國際比賽。

朱易是純華裔血統，但中文不佳，賽前備受關注，但卻因為在賽中失利而慘遭中國大陸網友出征。（Photo Credit: David W. Carmichael, https://w.wiki/53JL）

2005 年代表我國奪得世界撞球賽冠軍的吳珈慶，在 2009 年宣布轉籍新加坡，

[2] 第 25 條：歡迎臺灣運動員來大陸參加全國性體育比賽和職業聯賽，積極為臺灣運動員、教練員、專業人員來大陸考察、訓練、參賽、工作、交流等提供便利條件，為臺灣運動員備戰 2022 年北京冬奧會和杭州亞運會提供協助。第 26 條：臺灣運動員可以內援身分參加大陸足球、籃球、乒乓球、圍棋等職業聯賽，符合條件的臺灣體育團隊、俱樂部亦可參與大陸相關職業聯賽。大陸單項體育運動協會可向臺灣同胞授予運動技術等級證書。歡迎臺灣運動員報考大陸體育院校。

[3] 朱鳳蓮表示，截至 2019 年底，共有 4 位足球員、7 位籃球員、45 位桌球員在大陸參加職業或業餘賽事，並有 3 支桌球隊、3 支圍棋隊、1 支象棋隊在大陸參加聯賽，另有 39 位臺生就讀於北京體育大學。

我國目前有數名運動員長期在中國大陸訓練、參賽，圖為籃球名將陳盈駿，日前在陸比賽表現傑出；陸方第 26 條措施明定臺灣運動員為「內援」而非「洋將」。（資料來源：截自龍獅籃球俱樂部微博，https://weibo.com/u/1859597684?tabtype=feed）

我國競賽滑冰運動員、同時也是北京冬奧掌旗手黃郁婷，在賽前訓練時因身著中國大陸國家隊服，被認為言行不當，已遭懲處。（圖片來源：截自公視新聞，https://youtu.be/WRMvtYGa9u0）

據悉因條件沒談妥而作罷，卻因此遭我國撞球界抵制，乃選擇於 2011 年入籍中國大陸，成為第一位、同時也是迄今唯一一位入籍中國大陸的我國運動員，目前仍代表中國大陸參與各項國際賽事。此外，日前我國競賽滑冰運動員、同時也是本次我國北京冬奧掌旗手黃郁婷，在賽前海外移地訓練時身著中國大陸國家隊服的照片流出，甚至被網友發現在個人 Instagram（IG）中標註「BEIJING」並貼上五星旗圖樣，遭致輿論批評，賽事結束後，體育署認為其言行不當，做出停止補助 2 年專案培訓及參賽經費的懲處。[4]

我國運動員受限於體育資源、舞臺不足，前往中國大陸訓練、發展已成為另一選擇。近年我國體育人才輩出，在 2021 年東京奧運中奪牌數創下歷史新高，未來若有實力到位者，陸方勢必積極吸收，藉此作為對臺宣傳樣板，實不可不防。

[4] 《黃郁婷選手備戰及參賽北京冬奧期間言行失當 體育署停止補助2年經費》，https://www.sa.gov.tw/News/NewsDetail?Type=3&id=3625&n=92。

如何降低 OT網路 遭受勒索軟體攻擊的風險

◆ 華梵大學特聘教授 — 朱惠中

俄烏開戰，戰場的攻防由地面延燒至網路，許多證據顯示國家級（Nation-State）的攻擊者，已逐步將攻擊目標轉移到運營技術（OT）網路。

OT 網路成攻擊標的，造成災難性後果

歷史上最具破壞性的網路攻擊可追溯至 2017 年，NotPetya 勒索軟體攻擊烏克蘭的 IT 網路，除烏克蘭的政府機構、銀行（包括軍方銀行的 ATM）和地鐵系統均受到影響外，更發現當 OT 網路成為攻擊標的時，可能造成災難性後果，例如烏克蘭車諾比核電廠的輻射監測系統無法正常運行（在 1986 年災難後，核電廠周圍仍然是一個活躍且危險的區域）；此外，NotPetya 亦蔓延至許多國家的關鍵基礎設施，影響擴及丹麥航運巨頭 Maersk、英國 WPP 等

2017 年 NotPetya 勒索軟體攻擊烏克蘭的 IT 網路，烏克蘭的政府機構、銀行和地鐵系統均受到影響。（圖片來源：路透社／達志影像）

丹麥航運巨頭 Maersk 遭勒索軟體 NotPetya 攻擊，嚴重影響船務運作並造成鉅額損失。（Photo Credit: kees torn, https://flic.kr/p/oZx7nF）

跨國公司，包括醫療保健、能源和交通運輸等領域陷入停頓，估計造成約 100 億美元的損失。

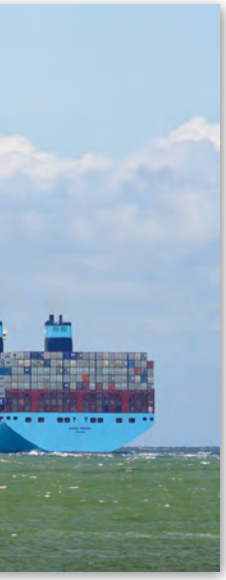
攻擊者鎖定工控系統下手，企圖竊取企業帳密

過往攻擊者可能從企業員工的電腦下手，進而橫向移動，以便更進一步掌控整個企業網路，但近年來智慧工廠、智慧製造的導入，使得工業控制系統（ICS）與企業內部網路的界線更加模糊，攻擊者很可能透過工業控制系統作為跳板，進而入侵受害企業。電腦緊急應變小組（Computer Emergency Response Team, CERT）列舉了攻擊者常見的策略和技術，如透過魚叉式網路釣魚以獲取對 IT 網路的存取權限，然後轉向 OT 網路，或直接連接到無需用戶或設備身分驗證的互聯網可存取控制器。由於這些網路上的安全控制數量有限，攻擊者可以潛伏於 OT 網路數月甚至數年而不會被發現。

勒索軟體攻擊行為與趨勢

美國、澳洲與英國的網路安全部門觀察到 2021 年網路犯罪分子的行為趨勢如下：

一、透過網路釣魚、遭竊取之遠端桌面協定（RDP）憑證或暴力破解以及利用漏洞來存取網路。



二、使用網路犯罪服務出租，例如勒索軟體即服務（Ransomware as a Service, RaaS）、協助受害者付款以及仲裁付款糾紛等服務。

三、全球勒索軟體組織彼此共享受害者資訊，例如，出售對受害者網路的存取權限，進而使其他網路威脅行為者能夠進行後續攻擊。

四、勒索金錢的方式多樣化，使用三重勒索（triple extortion），威脅要：1. 公開發布被盜的機敏資訊；2. 破壞受害者的網際網路存取；3. 通知受害者的合作夥伴、股東或供應商關於勒索事件。

五、攻擊對象逐步由具高價值或提供關鍵服務的組織，如 Colonial Pipeline Company 及 JBS Foods 等，轉向中型受害者，如慈善機構、法律界及公共服務部門。

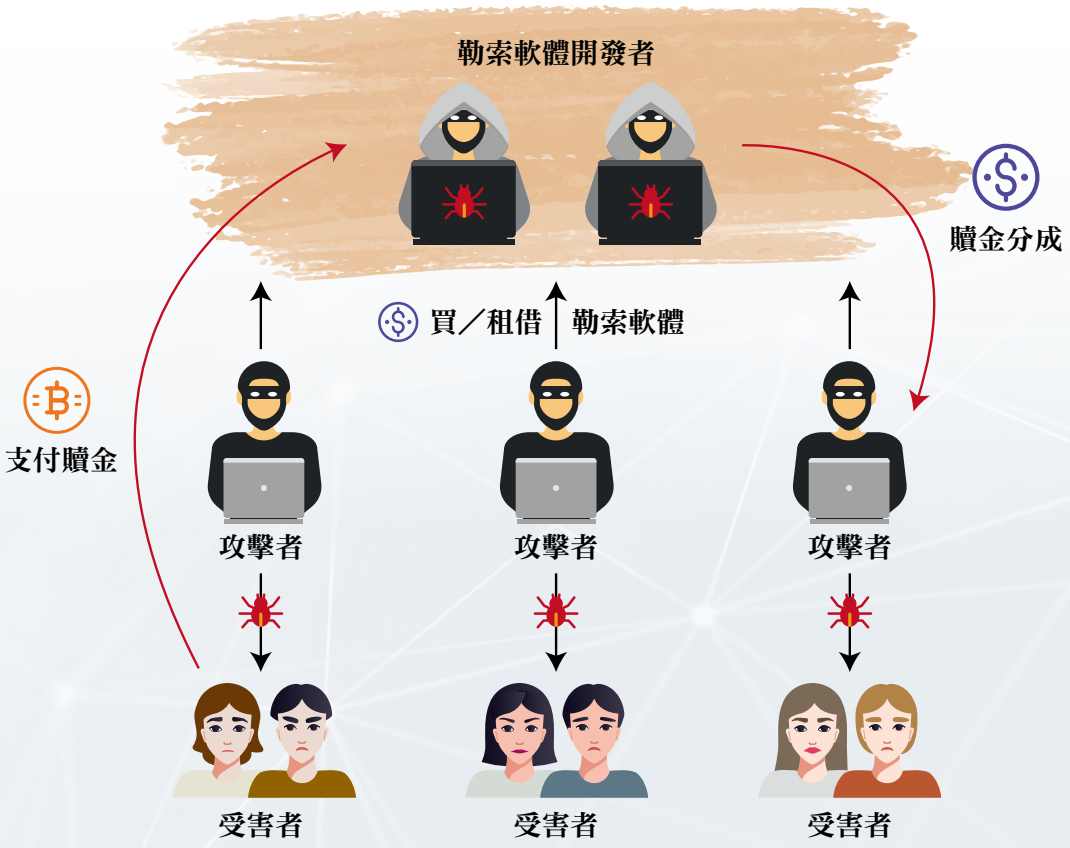
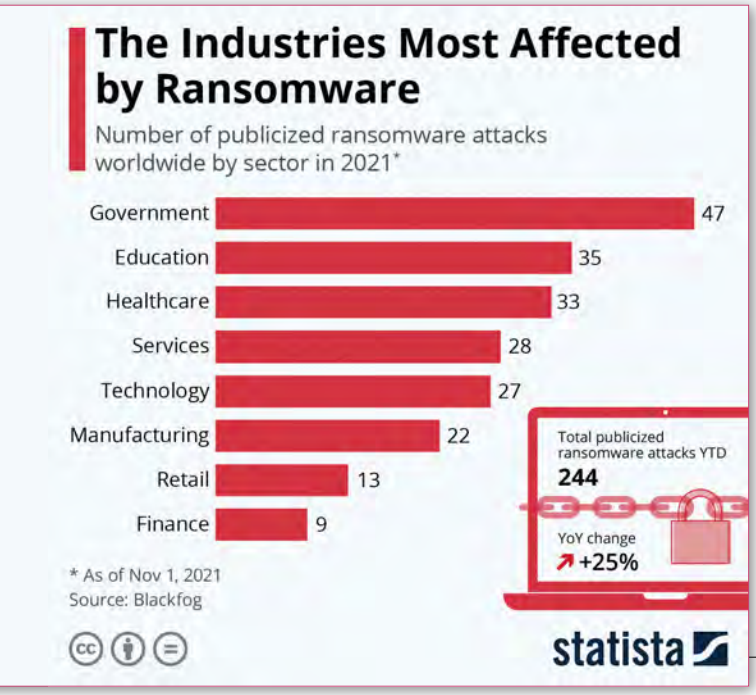


圖 1　勒索軟體即服務（RaaS）的營運模式

隨著數位轉型和遠距工作的加速，基礎設施已面臨前所未有的考驗和壓力。復因組織需要提高業務效率和盈利能力，故 IT 與 OT 網路相聯將是一個趨勢，當務之急是讓這種連接更加安全。



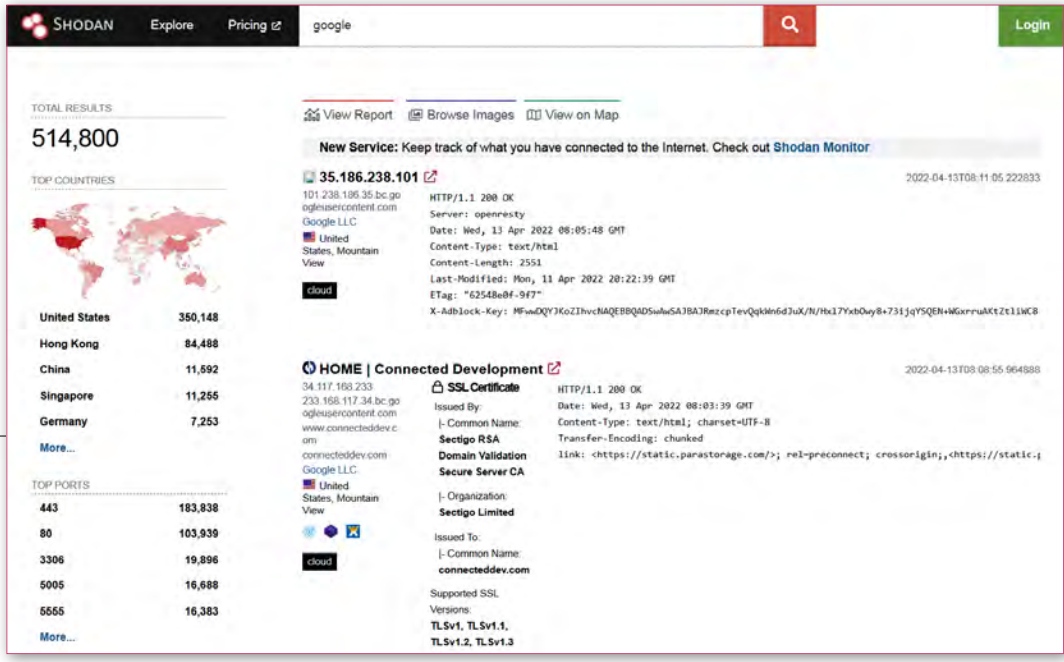
2021 年勒索軟體攻擊對象逐漸轉向公部門、教育、醫療、科技等中型受害者。（Photo Credit: Statista, https://www.statista.com/chart/26148/number-of-publicized-ransomware-attacks-worldwide-by-sector）

如何降低遭受勒索軟體攻擊的風險

於此新環境中，防禦者如何強化其 OT 環境的安全態勢，以降低遭受勒索軟體攻擊的風險？將是每位資安長（CISO）的首要任務，提出下列七項建議，以供相關組織及負責人員參考：

一、擴大風險治理的範疇

包括所有工業物聯網（IIoT）、工業控制系統（ICS）和企業物聯網（Enterprise IoT）的實體設備及軟硬體。當然，這對許多組織來說是一個具有挑戰性的步驟，因為識別這些資產不是一件容易的事。技術



Shodan 搜尋引擎可搜尋全球的物聯網設備，得知 IP 位址、運行服務、系統資訊等，有助於發現未在資訊財產清冊上的資產，分析其暴露風險；圖為搜尋「google」出現之相關內容。（Source: Shodan, https://www.shodan.io/search?query=google）

抵禦網路威脅及在線安全問題可使用包含強密碼、密碼庫和多因素身分驗證等方法。

方面，例如可利用 Shodan 搜尋引擎，搜尋全球的物聯網設備並擷取其相關資訊，可得到 IP 位址、運行的服務、系統資訊等，找出在 Internet 上可直接存取 Intranet 資料的設施或點，這有助於發現未在資訊財產清冊上的資產，並分析其暴露之風險。

二、確保在 IT 和 OT 網路之間進行適當的劃分

除了 IT/OT 分段之外，亦可將虛擬分段（virtual segmentation）部署到 OT 環境中來協助檢測 OT 網路中的橫向移動。另如遠距操作需要直接存取 OT 網路的資產，則須確保通過對用戶、設備和會話進行嚴格控制的安全遠距存取連接來完成。

三、養成良好的網路安全思維模式

隨時將抵禦網路威脅及在線安全問題列為考量的主軸，可使用包含強密碼（而不是在不同用戶之間共享密碼，這是工業運營中常見的做法）、密碼庫和多因素身分驗證等方法，來確保防禦者能將上述之主軸落實到 OT 和 IoT 設備上。某些過程，例如修補遺留系統（Legacy System），可能更具挑戰性或不可能。美國網路安全和基礎設施安全局（CISA）擁有許多免費的工具，包括掃描和測試，可協助找出網路的弱點及防禦機制的不足。

四、實施健全的系統監控

監控系統必須同時注意來自 IT 和 OT 的威脅，以及任何可能跨越 OT/IT 邊界的威脅。專為 OT 環境設計的無代理（Agentless）[1] 持續性監控系統有以下 3 個特色：

1. 可以快速被建置起來。
2. 可以輕易整合進 OT 和 IT 的系統及工作流程。
3. 可以讓 IT 和 OT 人員共同監控 OT 的環境。

另，若 IT 和 OT 人員能持有同一組資訊，他們將能對已知和未知的威脅做出相對應的措施。

[1] 凡是監控 server A 的系統不是裝在 server A 上，此監控系統就是 Agentless。以防毒軟體為例：所有防毒軟體都不是 Agentless，而用 SSH/SFTP 去撈別臺電腦 log 的系統就是 Agentless。

核心業務系統之備份數據或副本在一段時間內不可更改，以防止任何網路攻擊者加密機敏數據。

五、演練並落實緊急應變計畫

模擬勒索軟體攻擊的桌面演習（桌推）可以幫助防禦者了解自己的組織和技術準備情況。

六、隨時更新作業系統及應用程式

如果使用的是舊版本的軟體，將容易受到勒索軟體攻擊—就像 Wannacry 攻擊。

七、妥善管理核心業務系統之備份數據

因應勒索軟體攻擊復原之保護機制，設定核心業務系統之備份數據或副本在一段時間內不可更改，以防止任何網路攻擊者加密機敏數據，如此，復原後，防禦者可以用乾淨的副本或備份來進行復原工作，無需向攻擊者屈服並支付費用。

結論

勒索軟體已經開始攻擊運輸業、加工廠以及食品分銷系統，甚至開闢了國家戰爭中的新戰場。他山之石可以攻錯，做好基礎性的防護處理，我們就能減少勒索軟體對 OT 環境的影響。

關鍵基礎設施之資安防護

◆ 淡江大學國際事務與戰略研究所博士候選人 ── 陳永全

俄羅斯入侵烏克蘭後，美國政府近期持續發出勒索軟體對關鍵基礎設施（CI）的攻擊警告。[1]

俄羅斯將對美國 CI 發起網路攻擊

2022 年 2 月，美國官員警告政府機構和 CI 營運商，[2] 俄羅斯可能會在對烏克蘭發動軍事攻勢的同時，對烏克蘭和美國發起網路攻擊。聯邦調查局（FBI）和國土安全部（DHS）警告執法人員、軍事人員和 CI 營運商，要特別留意俄羅斯在網路上的行動，因為他們發現俄羅斯掃描美國網路次數增加，且其製造的假訊息也越來越多。

CI 為國家命脈

CI 提供一個國家的國家安全、社會民生、經濟發展、政府運作等持續營運所需要之基本功能或各項服務，一旦遭受天然災

[1] 在俄羅斯入侵烏克蘭後，美國持續發出關鍵基礎設施的勒索軟體攻擊警告，其中包括政府、金融以及食品和農業等目標。“Feds Warn About Critical Infrastructure Ransomware Attacks, Vulnerabilities”，https://www.esecurityplanet.com/threats/critical-infrastructure-ransomware-attacks-vulnerabilities/。

[2] “FBI and DHS Warn of Russian Cyberattacks Against Critical Infrastructure”（聯邦調查局和國土安全部警告俄羅斯對關鍵基礎設施的網絡攻擊），https://www.natlawreview.com/article/fbi-and-dhs-warn-russian-cyberattacks-against-critical-infrastructure。

由於科技的快速發展及全球化的概念，使人類活動大量仰賴網路互動，舉凡政治、能源、金融、交通等均包含在內，未來如何整合串聯虛、實兩個不同的領域，對國家的穩定運作極其重要。

害、人為破壞，都可能造成政府及企業運作中斷，形成骨牌及擴大效應，衝擊經濟發展與民心士氣，甚至嚴重影響政府運作。

全球化的概念將人與人的實際接觸邁向虛擬空間的交流，舉凡政治、社會、能源、商業、物流、金融與交通運輸等，均大量仰賴網路互動。未來如何整合，串聯虛、實兩個不同的領域與世界，對國家的穩定運作極其重要。

網路攻擊事件倍數增長

2021 年統計數據顯示，勒索軟體攻擊頻率呈倍數成長，在威脅持續提升下，政府及資安業者呼籲企業組織需更強化資安機制，以避免重要關鍵基礎設施的運作系統遭癱瘓或機敏資料遭竊，同時更需強化人員的資安防護意識與技能。

2021 年網路威脅趨勢，以勒索軟體利用資安漏洞和供應鏈入侵攻擊為主，駭客趁 COVID-19 疫情，政府企業分工分流、異地或居家辦公、遠端工作等時機大舉實施。據統計，勒索軟體攻擊在 2021 年 6 月至 12 月間內飆升 93%。另據全球知名網路安全公司最新報告指出，2021 年全球的網路攻擊量創下歷史新高；[3] 臺灣受攻擊次數遠高於亞太地區平均值，每週平均被攻擊 2,644 次。[4]

[3] Check Point Software 公司的《網路攻擊趨勢：2022 年安全報告》指出，與 2020 年相比，2021 年教育／研究部門每週被攻擊次數為 1,605 次（增加 75%），緊隨其後的是政府／軍隊每週被攻擊 1,136 次（增加 47%）和通信每週被攻擊 1,079 次（增加 51%），https://www.checkpoint.com/press/2022/check-point-softwares-2022-security-report-global-cyber-pandemics-magnitude-revealed/。

[4] 《中共網軍壓境！台灣去年遭網路攻擊大增 38% 遠高亞太平均值》，https://news.ltn.com.tw/news/politics/breakingnews/3815742。

新興攻擊態樣

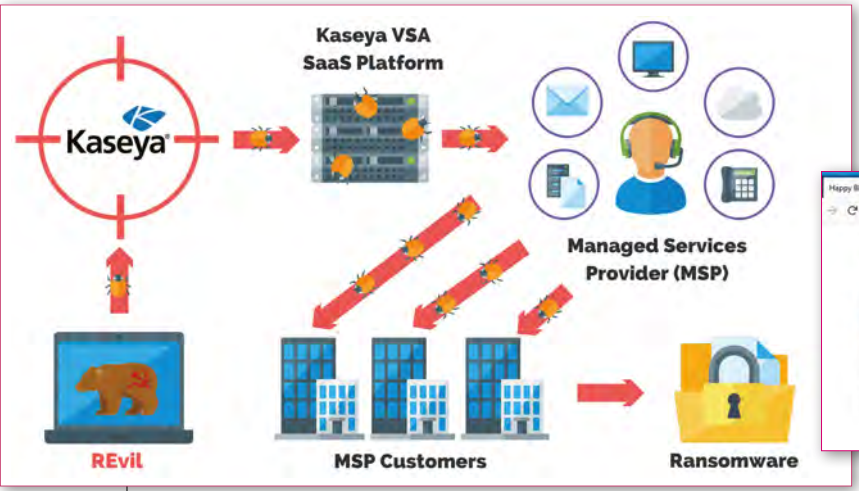
新興的勒索軟體攻擊，例如 “Triple Extortion”（三層勒索），其攻擊方式，係從企業網路中竊取機敏數據、威脅受害對象、要求付款、否則將公開發布其所竊取之機敏寶貴資訊，尤有甚之，攻擊者針對該受害組織的客戶、協力廠商、合作夥伴，亦要求給付高額贖金。

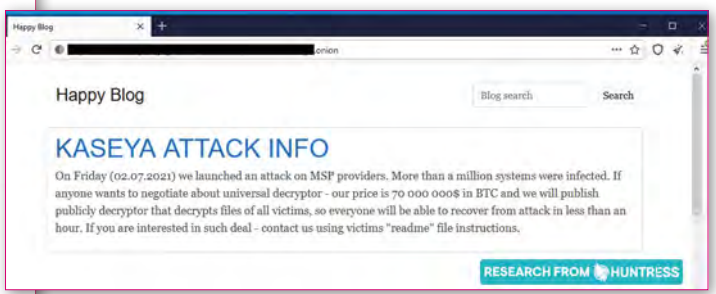
供應鏈攻擊案例，以 2021 年的 SolarWinds 攻擊最著名，其他複雜的供應鏈攻擊尚有 2021 年 4 月份的 Codcov，以及 7 月初的 Kaseya 攻擊，規模與影響均不容小覷。

另有許多惡意軟體正迅速擴展中，例如：Trickbot、Dridex、Qbot 和 IcedID 等；網路駭客正採取更具滲透力的軟體工具，使其攻擊更有威力與效力；儘管各國執法部門加強取締，但勒索軟體增長速度卻未因此而減緩。這種虛實之間的攻與防，日益變化的攻擊手段與趨勢，將對 CI 營運商造成極大的損害，需採取更嚴密的防範策略來因應。

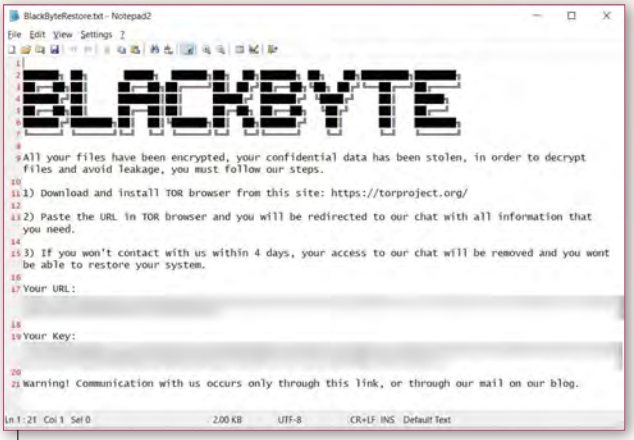
美國關鍵基礎設施頻傳遭駭客攻擊

美國聯邦調查局（FBI）發出警告，曾於 2021 年 7 月首次現身的 “Black Byte” 勒索軟體服務組織（RaaS），已再次活躍於網路世界中，截至 2022 年 3 月為止，美國至少已有三個關鍵基礎設施部門遭 Black Byte 入侵攻擊，分別是：政府部門設施、金融服務機構和食品農業設施等。此外，該組織同時鎖定全球多個企業目標，準備針對各大企業資訊安全漏洞發起攻擊行動，進而竊取並將文件加密進行勒索。





Kaseya 是一家為管理服務商（MSP）和 IT 公司提供 IT 管理軟體的公司，遭到俄國駭客團體 REvil 勒索威脅，其聲稱已感染超過 100 萬臺設備，並要求支付價值 7 千萬美元的比特幣作為贖金。（Photo Credit: PurpleSec, By Josh Allen, https://purplesec.us/kaseya-ransomware-attack-explained; Huntress, By John Hammond, https://twitter.com/_JohnHammond/status/1411868939903246338）



截至 2022 年 3 月為止，美國至少已有 3 個關鍵基礎設施部門遭 Black Byte 入侵攻擊，其同時鎖定全球多個企業目標，準備針對各大企業資訊安全漏洞發起攻擊，並竊取文件加密進行勒索。（Photo Credit: SOCRadar, https://socradar.io/who-is-the-blackbyte-ransomware-group-and-how-does-the-decryptor-works）

Ragnar Locker 在網站宣稱他們駭入 ADATA 的系統，並已盜出 1.5TB 機密資訊。（圖片來源：竣盟科技，https://blog.billows.com.tw/?p=1137）

FBI 另發現至少有 52 家橫跨十大關鍵基礎設施領域的企業組織，遭到 Ragnar Locker 勒索軟體入侵，[5] 涵蓋製造、能源、金融服務、政府及資訊科技等領域企業；可怕的是，Ragnar Locker 在執行加密過程中，電腦仍可正常執行而不會被受害者發現。[6] Ragnar Locker 2020 年曾攻擊全球第四大貨櫃船運業者—達飛海運集團公司（CMA CGM），[7] 臺灣記憶體大廠威剛公司在 2021 年也遭到 Ragnar Locker 攻擊。[8]

整合 3T 科技

當 CI 營運商為了強化自身資訊安全防護能力，布署添購多項的資訊安全監控與管理工具，例如入侵偵測防護系統、防毒軟體系統、防火牆之後，資訊系統管理人員是否就可無後顧之憂？資訊安全設備每日產出的記錄檔，少則數千筆，多則上萬筆甚至千萬筆，是否能妥切分類並且進行正確分析？統計分析完成後，是否確定哪些是相關聯的？哪些是個別的事件？又有哪些是緊急的事件需要即刻進行處置？一旦緊急事件被資訊管理人員歸納出來後，是否能夠立即確認該事件之攻擊手段？

上述問題精髓，均在於虛實環境的認識與整合，CI 營運商必須有效整合資訊科

[5] Ragnar Locker 犯罪組織主要對大型企業發動攻擊，並在加密前先行取走檔案，以迫使受害單位支付贖金。《全球第四大貨櫃船運業者 CMA CGM 遭 Ragnar Locker 勒索軟體攻擊》，https://www.ithome.com.tw/news/140261?fbclid=IwAR279_IVLDPG2hpep1aSmpucGcHfKSTsM_ma8Ibzx9Z1SyzG8RYUMGpdZ6k。

[6] FBI 除提供該勒索軟體的入侵指標（IOCs Indicator of compromise security）外，也督促受害者主動向主管機關舉報並提供相關細節以追蹤駭客，避免其他組織再度受害。

[7] https://www.cma-cgm.com/local/taiwan-agencies。

[8] 《威剛遭勒索軟體 Ragnar Locker 攻擊》，https://www.ithome.com.tw/news/144910。

技（IT, Information Technology）、操作科技（OT, Operation Technology）與通訊科技（CT, Communication Technology），再進一步結合開放式數據平臺，形成智慧企業整合架構，據以鏈結雲端資料分析應用，把設備控制層、現場管理層、企業營運層及協同商務層整合，一路貫通串接，使上下各類型資訊皆趨向透明化且能即時呈現；循此，CI 營運商便可建構出智慧型戰情監控室，採全天候、全時段、即時根據運作生產狀況，傳送資訊至雲端進行大數據分析，可迅速作出反應，確保運行順利。

CI 營運商必須有效整合 IT、OT 與 CT，再進一步結合開放式數據平臺，鏈結雲端資料分析應用，建構出智慧型戰情監控室，採全天候、全時段、即時根據運作生產狀況進行大數據分析，確保運行順利。

CI 營運商之資安防護作法

揆諸過往，有別於傳統軟體病毒攻擊都是由具備專業技術的駭客組織發起，然隨著 RaaS 勒索軟體服務這類新興組織的崛起，其背後集結來自不同專業領域的技術人員，包含開發者、測試人員及談判人員等，以專業分工團隊的型態，提供向買家出售或出租勒索病毒的服務，從中抽取佣金與租金的非法獲利，此行為被視為是促使勒索病毒攻擊迅速擴散的主因之一。

因此，CI 營運商在面對虛實的網路世界與實體世界環境中，如何落實資安防護，有效降低遭攻擊的風險，可遵循下列六點：

一、使用獨特且高強度的密碼。

二、執行多重身分驗證。

三、操作系統和軟體需保持在最新版本。

四、刪除對管理網路共享不必要的訪問。

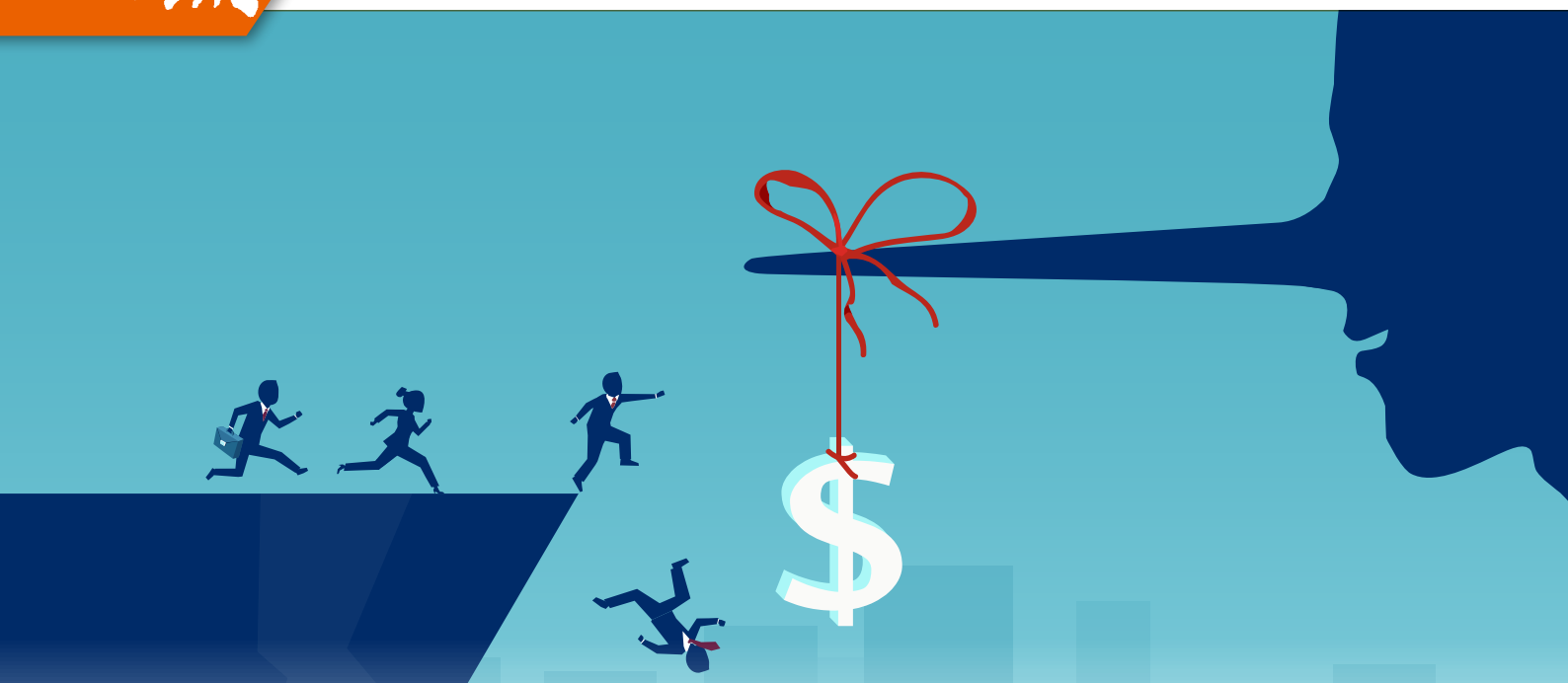
五、使用基於主機的防火牆。

六、為搭載 Windows 系統的電腦啟用文件受保護的檢視機制。

在 IT、CT 及 OT 與設備之相依性位置圖建置版本管理、維護協力廠商緊急連絡電話等相關訊息方面，均須符合資通安全管理等相關規範。[9] 另輔以運用「政府組態基準」（Government Configuration Baseline, GCB）規範的一致性安全設定（如密碼長度、更新期限等），以降低資安風險。上述資訊在「行政院資通安全會報技術服務中心」中可獲得解答。[10]

[9] 「有效運用資安弱點通報機制」（Vulnerability Alert and Notification System, VANS），結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實資通安全管理法之資產盤點與風險評估應辦事項。

[10] 政府組態基準目的在於規範資通訊設備（如個人電腦、伺服器主機及網通設備等）的一致性安全設定（如密碼長度、更新期限等），以降低成為駭客入侵的管道，進而引發資安風險。該專區提供 GCB 說明文件、相關資源及常見問答，能協助各機關進行導入規劃與實作。https://www.nccst.nat.gov.tw/GCB。



我被詐騙了！

◆ 教育工作者 — 陳宏煇

現在這個年頭，最好賺的莫過於「詐騙」這個行業了。

你被詐騙過嗎？或許你曾被詐騙過，但卻不敢說出來，因為礙於面子、害怕會被別人當做是笑話。像我就曾經被詐騙過2次，事後心有不甘，故希望開誠布公個人的親身遭遇，以讓各位減少受騙機會！

第一次被詐騙：購買未上市股票

第一次被詐騙在民國90年，那時已在軍中服務5年，當時有位要好的學長跟我說，對他很好的老長官退伍後在證券行工作，有內線消息說未來TFT-LCD面板將會

成為主流，這家公司正準備要增資興建廠房，一旦上市後，獲利相當可觀，他問我要不要先購買該公司的未上市股票，等到上市後、股價漲了再脫手，就可以大賺一筆，也可以把剩下的房貸還清，就不用再辛苦地過日子。

學長看我猶豫許久，就拿出份報紙上的報導給我看，報紙上有相當大篇幅報導，並且指出該公司的董事長是由剛卸任的某部會首長擔任，而且還有開工動土剪綵的照片，再加上許多退休政府官員都名列其中，不疑有他且相當有自信的我，便以僅有的積蓄，加上小額信用貸款，以 1 股 50 元價格買了 10 張、合計 50 萬元的未上市股票，希望能夠以小搏大、一夜致富，然後把房貸還清。

過了 3 年，該公司突然召開記者會宣布破產，瞬間股票變成「廢紙」，50 萬元就像丟入水裡，全部泡湯！事後檢討，發現自己過於自信，相信報紙上的報導，殊不知那是一家人頭公司，先以高薪聘請卸任官員當董事長，製造破土動工的場面，以假亂真，接著再向報社買廣告，由報社代筆並報導，結果一堆人相信了！購買未上市股票後，沒多久公司「人去樓空」，公司高層「遠走高飛」，而人頭董事長則早就離職，最後只有投資的股民倒楣，錢永遠討不回來！

第二次被詐騙：我中獎了

第二次被詐騙在民國 91 年，那時因為購買未上市股票而向銀行信用貸款，接著又因工作關係而有了車貸、房貸，貸款常常壓得我喘不過氣來，每個月都在想辦法籌錢還錢，生活過得更加辛苦。

有天撿到張刮刮樂，沒想到竟然刮中 50 萬元，被高額獎金沖昏頭的我，馬上按照指示打電話給對方，對方自稱是「香港馬會」的在臺代理商，因為中獎需要先扣抵 20%（也就是 10 萬元的稅），不過要先匯款到「香港馬會」，等審核確認後，一個星期後才會將 50 萬元匯到我的帳戶。

當時手機雖然已漸普遍，然資訊流通並不普及，加上當時相當缺錢，便將僅有的 10 萬元匯到「香港馬會」，匯完後還開心地和對方確認是否收到稅款及中獎款項匯進時間，並且滿心期待地等著 50 萬元匯進戶頭內。

等啊等地，一個星期終於過去了！趕緊去郵局刷存摺，但存摺紀錄卻是空空如也，中獎的 50 萬元並沒有入帳。趕緊打電話問代理商，但電話卻變成空號，這才驚覺自己被騙了！

第三次識破詐騙：遭重複刷卡

第三次被詐騙發生在最近，有天接到來電顯示是國內號碼的電話。（交談內容請參照右頁圖示）

其實，我早就知道這是詐騙電話，原因很簡單，因為當天刷卡的是內人不是我，所以要退錢也是退給內人，最重要的是對方口音怪怪的，而我和詐騙集團周旋許久，所以想知道對方使用何種方式詐騙。當然，我也就沒有被騙囉！

只是，好朋友卻因此詐騙方式而被騙了 6 萬元，他告訴我時還一臉懊惱，我問他當時不覺得是詐騙電話嗎？他說對方提供的資料不但詳實而且正確，等到錢匯出去時，才發現被詐騙，但已經來不及了！

這是一般人被騙的心態，被騙後只能自己懊惱、咒罵對方，但匯出去的錢卻很難再回來了！有人說，「一朝被蛇咬，十年怕草繩」，被騙一次，或許以後就不會再被騙，但多數人卻是一再受騙，原因很簡單，被騙過後總覺得自己不會那麼笨，但往往就是這種心態，才讓詐騙集團一再得逞。

現今詐騙方式百百種，更是無所不在、無孔不入的，唯有小心才能駛得萬年船，時時提防、隨時查證，才能避免受騙。

「請問是陳 XX 先生嗎？」

「我是！」

「請問您是不是在 X 月 X 日到淡水 XX 餐廳消費，並用信用卡刷卡 1,513 元。」

「沒錯！有問題嗎？」

「不好意思！您那天付款時因為店員不小心重複刷卡了一次，也就是刷了 3,026 元，幸好我們稽核時發現，現在要將 1,513 元退還給您，但因為銀行關門了，不知道您有沒有網路銀行？我們可以馬上退款給您。」

「眞的嗎？我有網路銀行。」

「好的，那請您先開啟網路銀行，不要掛斷電話，照我說的步驟一步一步操作就可以了！」

「好的，那您等我一下！我先開網銀……。」

酒駕修法 要既見秋毫亦見輿薪

◆ 大學助理教授 — 趙萃文

立法院於今（2022）年 1 月通過「酒駕三法」，未來將公布酒駕累犯姓名與照片；酒駕致人於死者，最高將處 10 年徒刑與新臺幣（下同）2 百萬罰金。

「來不及說再見」[1] 酒駕又造成家破人亡

高雄去（2021）年底發生一起因酒駕而釀成一家 4 口 1 死 3 重傷的悲劇，[2] 和樂家庭突然破碎，經濟無以為繼。立法院火速於今（2022）年 1 月 24 日通過〈刑法〉修正案，加重酒駕刑度，增訂加重結果犯與再犯之罰金刑，延長再犯加重處罰之年限，將單純酒駕刑責，從現行 2 年調

[1] 《聯合報》的《來不及說再見，5 個被酒駕撞碎的生命故事》，以插畫記錄酒駕受害者 32 歲臺大醫師曾御慈、32 歲烘焙坊老闆兼主廚陳育邦、15 歲資優學生陳詩云的生命瞬間停格、28 歲剛通過碩士班論文口試詹庭豪變成植物人迄今尚未醒來，以及交通警員陳昭宏在執行勤務時遭二度酒駕者撞擊，致雙腿粉碎性骨折，截肢後才能保命的悲慘遭遇等等；該報並統計 10 年來，臺灣有近 3 千人於酒駕車禍中喪命，逾 10 萬人因而全身癱瘓、截肢或終生不良於行。https://udn.com/upf/newmedia/2019_data/DUI_victim_stories/?utm_source=&utm_medium=related&utm_campaign=7-39。

[2] 37 歲母親當場傷重不治、父親重傷；大女兒雙腳及顏面多處骨折，牙齒脫位；小女兒頭部受重擊、顱內出血。家中經濟支柱一夕間倒下，未來復健路更不知道有多長。《高雄 3 度酒駕男撞一家 4 口 爸爸及大女兒多處骨折手術中》，https://www.chinatimes.com/realtimenews/20211227003492-260402?chdtv；《高雄酒駕釀一家四口 1 死 3 傷 BMW 男殺人罪起訴》，https://news.ltn.com.tw/news/society/breakingnews/3798371。

立法院於今年 1 月 24 日通過〈刑法〉修正案，加重酒駕刑度與罰則，期望藉此杜絕憾事再發生。（圖片來源：交通部道路交通安全督導委員會，交通安全入口網，https://168.motc.gov.tw/theme/ndd/publish）

高為 3 年以下徒刑，酒駕累犯認定加重其刑的年限從 5 年拉高至 10 年，最重並得併科 300 萬元罰金。《陸海空軍刑法》亦一併修正，相較於〈刑法〉再加重罰金額度，嚴懲酒駕之決心昭然若揭。

「酒駕」為修法最頻密之〈刑法〉犯罪

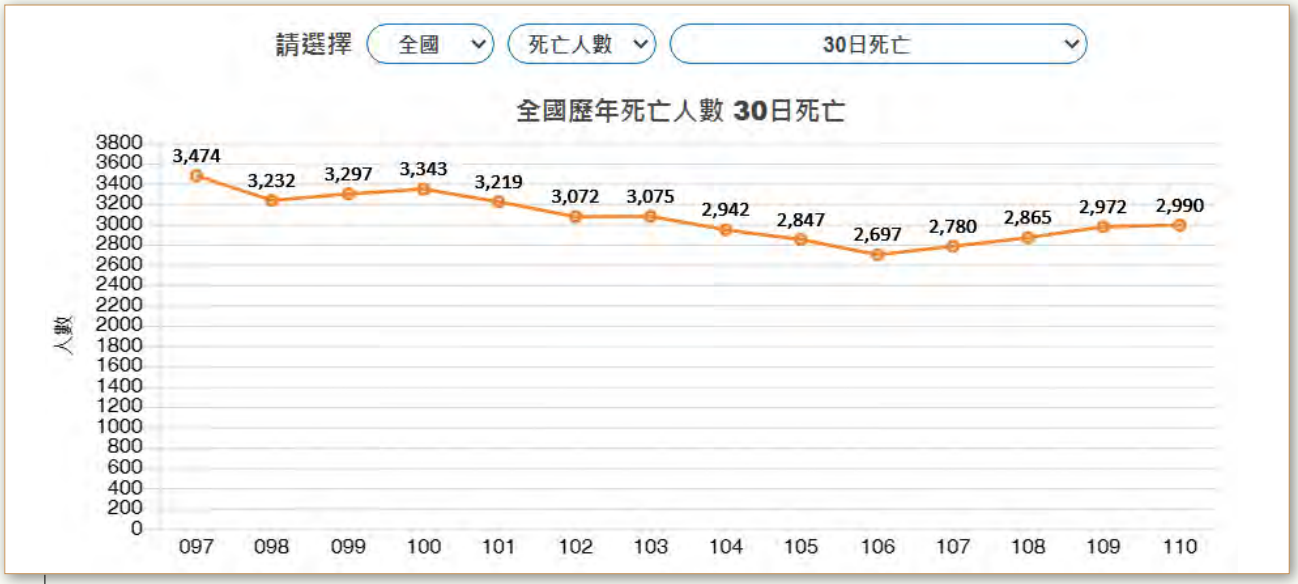
我國對酒駕處罰始於 1968 年，當時規定於《道路交通管理處罰條例》第 35 條，處 100 元以上 300 元以下罰鍰，屬單純行政不法。1999 年我國模仿〈德國刑法〉增訂現行〈刑法〉第 185-3 條酒駕罪，旋因部分酒駕案件造成重大傷亡，在媒體推波助瀾下，於 2007、2011、2013 [3]、2019 [4] 年接連修法，2021 年法務部又提出修正草案，希望完善吸毒駕駛處罰，惜未能完成修法。酒駕成為我國刑法典裡修法最頻密之犯罪，而相較我國〈刑法〉長期模仿國德國及日本，此不能不說是我國刑事司法之新奇蹟。

事實上在歷任政府強力宣導下，我國酒駕案件統計上確實有顯著下降，但整體交通事故死亡人數依然居高不下，以去（2021）年為例，截至 12 月底止有 2,990 人死亡，[5] 此數字著實令人怵目驚心。

[3] 2013 年 5 月，臺大醫師曾御慈返家途中，遭酒駕者詹震山闖紅燈撞上，搶救 5 天仍宣告不治；立法院當年即將〈刑法〉酒駕致人於死的條款，從最重 7 年有期徒刑提高到 10 年，法界稱之為「曾醫師條款」。

[4] 新增「酒駕特別累犯」規定，曾犯酒駕經有罪判決確定或經緩起訴處分確定，於 5 年內再犯酒駕因而致人於死者，最高處無期徒刑或 5 年以上有期徒刑。臺灣酒駕防制社會關懷協會秘書長林美娜直言「大大不滿意」，她指出，被首次酒駕撞到導致重傷殘的被害人，就已經家破人亡了，不該只有第二次才重罰。https://www.cna.com.tw/project/20190719-drunkdriving/article5.html。

[5] 2022/2/17《道安資訊查詢網》之查詢資料，https://roadsafety.tw/Dashboard/Custom?type=%E7%B5%B1%E8%A8%88%E5%BF%AB%E8%A6%BD。



我國酒駕案件統計上確實有顯著下降，但整體交通事故死亡人數依然居高不下。（資料來源：道安資訊查詢網，https://roadsafety.tw/Dashboard/Custom?type= 統計快覽圖表 #dash_item_1876）

鄰近日本亦有酒駕問題，其另制定《道路交通法》特別法，加重處罰酒駕及其他重大違規行為（如超速、無視號誌、危險駕駛等），重大違規致死最高處20年徒刑，相較我國處罰上更加嚴厲，值得注意的是，該國對酒駕及各式不能安全駕駛行為一律重罰，立法上顯然更為完善。觀諸2021年其全國交通事故死亡數僅2,636人，[6]考量到日本總人口數是臺灣的5.5倍，其對酒駕及其他交通犯罪之防制經驗，值得我國修法參考。

日本酒駕罰則嚴厲，且針對其他各式不能安全駕駛行為亦一律重罰，立法上更為完善。

不同風險酒駕行為刑罰應有重輕

動力交通工具雖本身即屬足以造成公共危險器具，且依據交通工具種類、載客量或載重量、速度等之不同，而有不同的潛在公共危險性，惟我國〈刑法〉酒駕罪條文並未細分，這自然會發生情重罰輕之弊。〈德國刑法〉對於因飲酒或服用藥品

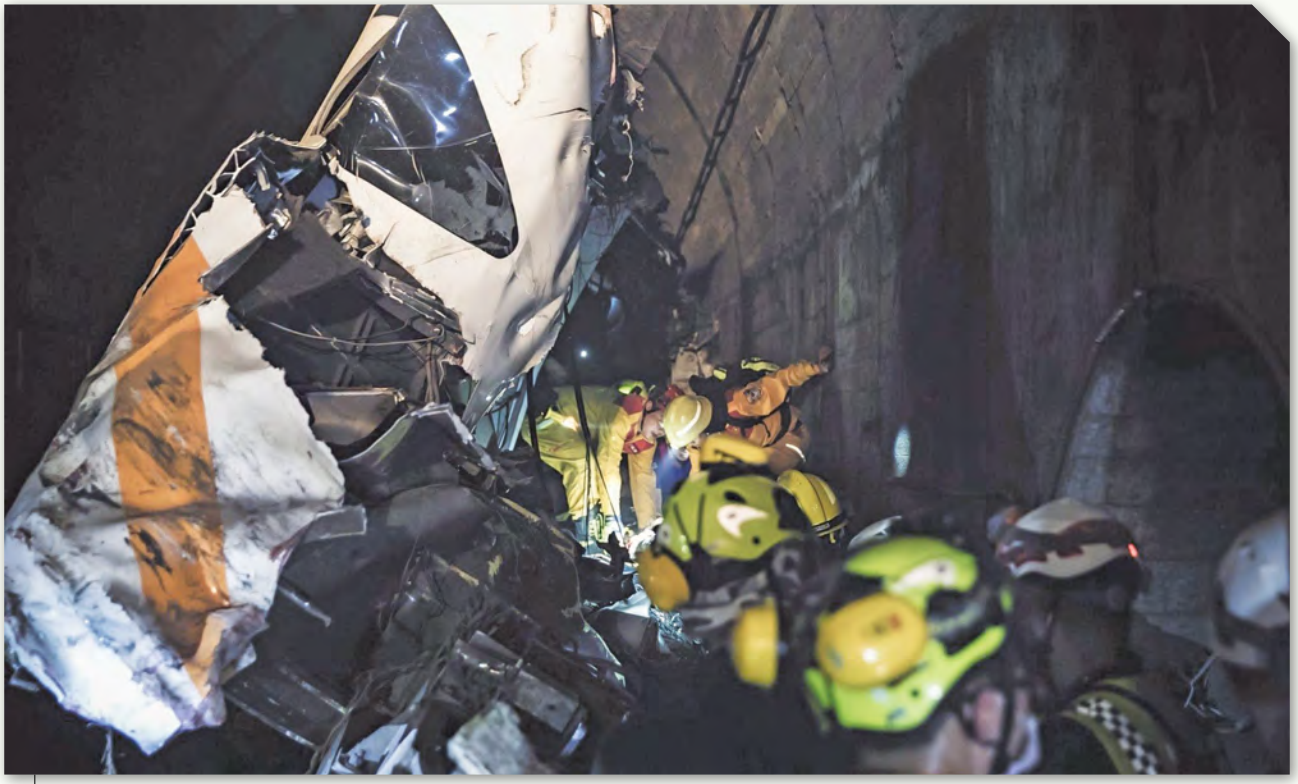
[6] 曾兩度獲得金鼎獎的作家陳柔縉，於110年10月在新北市淡水區騎單車遭機車追撞，頭部重創，搶救3天無效，宣告不治。住在臺灣的日本女作家田中美帆對她表示哀悼並蒐集資料指出，2020年日本交通事故總數30萬9,000件，死亡數為2,839人，臺灣交通事故總數36萬2,393件，死亡數為2,972人；臺灣人口約日本1/6，但交通事件死亡人數卻比日本還多。《日本女作家批台灣交通事故多　超速、無視號誌、不打方向燈等現象不勝枚舉》，https://tw.appledaily.com/life/20211118/YJ7VGVA7YNABVHPFJDL7SJAU3I/。

〈德國刑法〉對於因飲酒或服用藥品致不能安全駕駛，依交通工具種類及具體危險犯或抽象危險犯分別規定罰則，交通工具種類包含火車、纜車、船舶或航空器及其他交通工具等。

致不能安全駕駛，依交通工具種類及具體危險犯或抽象危險犯分別規定，其第 315a 條規定：由於飲酒或服用麻醉藥品，或由於精神上或肉體上缺陷，在無法安全駕駛火車、纜車、船舶或航空器及其他交通工具者，處 5 年以下自由刑或罰金。第 316 條規定，若其行為未能依前條規定處罰者，仍可處 1 年以下自由刑或罰金。將酒醉駕駛火車或航空機等大眾交通工具加重處罰，尤具參考值得。

另外，〈德國刑法〉第 315c 條酒駕罪，除了罰及酒駕、毒駕外，對其他出於精神上或肉體上缺陷、嚴重違反路權或交通規則、毫無顧忌超速等，**皆一律重罰**，而非如同我國僅加重處罰酒駕，對其他開車時滑手機、看影片、打瞌睡，甚或男女朋友嬉戲等，足以造成分心且具有高度危險故意的駕駛行為卻並未加重處罰，體例上並不衡平。事實上我國早有〈刑法〉學者指出，若有對情侶，女友替正在開車的男友口交，男友心神恍惚之際撞死人，此一適例其可罰性絕不亞於酒駕致死，而行為人卻僅能依〈刑法〉第 276 條過失致死罪至多判處 5 年徒刑，其中之不合理，不言可喻；因此，〈刑法〉第 185-3 條酒駕罪較理想修法，應係直接以行為人不能安全駕駛動力交通工具為要件即可，至於為何不能安全駕駛，無需再作限制。

對其他開車時滑手機、看影片、打瞌睡或男女朋友嬉戲等，足以造成分心且具有高度危險故意的駕駛行為，我國〈刑法〉未加重處罰，體例上並不衡平。



2021 年「太魯閣號出軌」事故造成 49 死，然被告李義祥已羈押期滿獲釋，其所犯〈刑法〉第 276 條過失致死罪，最重僅能處 5 年有期徒刑，罪與刑明顯不成比例。（圖片來源：花蓮縣消防局，蔡哲文攝，https://www.hnfa.gov.tw/News_Content.aspx?n=5624&s=84872）

風險社會下〈刑法〉之危機控管

我國現行〈刑法〉承繼自 1911 年《欽定大清新刑律》，歷經百年滄桑，行為可罰性基礎所立基之經濟發展水準，已無法對應當代社會快速變異及社會活動危險源擴大之現況。科技進步，生活機能升級，交通逐漸成為現代人生活的重要部分，讓現代人風險無所不在。以去（2021）年「太魯閣號出軌」造成 49 死一案為例，被告李義祥因羈押期滿，於今年 1 月獲釋，其所犯〈刑法〉第 276 條過失致死罪，最重僅能處 5 年有期徒刑，罪與刑明顯不成比例，不符國民法律情感。

〈刑法〉宜另訂交通犯罪之專章

〈刑法〉是與人民生活最密切相關的法律，隨著經濟、科技條件發展的變動，本應隨時準備修調。我國〈刑法〉一向模仿德國，該國針對普通殺人、放火、過失致死等罪，構成要件增訂「情節特別嚴重」，用以涵蓋某一行為造成多人死傷之同種想像競合情形，特別加重處罰，足堪我國借鏡。期望立法者能將目光穿透個案，慎思〈刑法〉背後時空，同時扣準現代科技進步、動力快速的交通實況，將傾覆交通工具罪、損壞交通設備罪、損壞公共通路罪及酒駕罪等獨立出來列為專章，設計相應寬嚴程度之規範要求，建構一個更符合生命權保障的規範機制，護守國人安全，則全民幸甚。

南沙太平島：史地篇

◆ 清華大學榮譽退休教授 — 鍾　堅

美國印太司令部表示，中國大陸已軍事化南海的三座人工島礁，正把太平島包圍在中間。

國境之南

疫情橫掃下全球旅遊窒息，國內趴趴走正夯，連外島、離島都成為國民旅遊的熱門去處。但是有一處南海天堂，民眾絕少有機會踏訪，那就是行政區劃屬高雄市的南沙群島太平島。它距高雄市的航程約 1 千 6 百公里，作者有幸曾公訪登島多次，特從史地、接收、建設、戰略面向，分期與讀者分享這寧靜無華的熱帶島嶼風貌。

（Photo Credit: CSIS, Asia Maritime Transparency Initiative, https://amti.csis.org/itu-aba-tracker/?lang=zh-hant）

太平島是鄭和群礁中面積最大的島，初始由珊瑚礁岩形成。（圖片來源：彭錦珍堤供；內政部，https://www.moi.gov.tw/News_Content.aspx?n=2&s=9649）

史前時代

太平島現在的位置，在 3 百萬年前的「新近紀」地質年代，還是茫茫大海；不過，珊瑚蟲在大海下方的海底山錐頂端開始大量繁殖，消亡後的骨骸，堆積在錐頂，讓它慢慢增高，每萬年增高約 1 米。

10 萬年前，海底山錐頂終於冒出海面，環狀海底山錐頂的邊緣繞行一圈約 120 公里，圈成的潟湖海域面積約 6 百餘平方公里，水深達百米，現今稱為鄭和群礁。陸續露出海平面，遭高約一層樓的鳥糞覆蓋之珊瑚島礁有 8 個，其中面積最大的，就是擁有近 50 甲地的太平島。

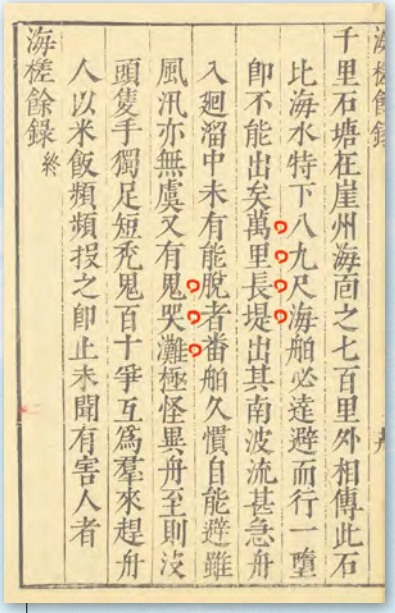
躍上歷史舞臺

約 1 千年前，人類乘漁舟橫渡大海找到太平島。由於它周邊還有很多水下覆蓋珊瑚的岩塊尚未冒出海面，探險的漁舟屢屢觸礁沉沒，所以，來探訪珊瑚島嶼的人類不多。島上匯集的雨水遭鳥糞汙染，喝了就身體不適；故人類把踏查這座珊瑚島嶼視為畏途，嫌島上的環境惡劣，不宜長居久留。率先踏訪的是廣東海南島瓊州人，他們在驚濤駭浪中迷航，涉水登島暫時棲

息；島外沒有天然的避風塘，他們的漁舟不能久留，摘了椰子裝滿漁舟就揚帆而去，故瓊州人無法在島上形成聚落。

約在 17 世紀初，瓊州人在《更路簿》手稿中描述他們來往南海的航海記事，用瓊州語稱太平島為「黃山馬峙」，這是珊瑚島嶼第一個非官方的名字。其實，漢人早於三國東吳赤烏 11 年（公元 248 年）朱應出使南洋返國後，就撰寫《扶南異物志》，記載扶南（今日的柬埔寨）諸邦及航途見聞筆記。

自漢唐以降，漢人即持續揚帆經過南海諸島，古籍均詳加記載；如 16 世紀明朝顧岑撰寫的《海槎餘錄》就記載漢人航經「萬里長堤」在「鬼哭灘」的見聞。清康熙 49 年（公元 1710 年），清國水師副將吳陞率艦巡守「昆侖」海域的南海諸島，返航後呈奏摺將其納入大清版圖，清國遂正式將南海諸島繪入「江海險要圖」內，但未派官吏駐島設治，清國遂成為首個聲索黃山馬峙與所有南海諸島主權的國家。


海槎餘錄 終

千里石塘在崖州海面之七百里外相傳此石比海水特下八九尺海舶必達避而行一墮即不能出矣萬里長堤出其南波流甚急舟入迴溜中未有能脫者番舶久慣自能避難風汛亦無虞又有鬼哭灘極怪異舟至則沒頭隻手獨足短禿鬼百十爭互爲羣來趕舟人以米飯頻頻投之即止未聞有害人者

明朝顧岑撰寫的《海槎餘錄》就曾記載漢人航經「萬里長堤」在「鬼哭灘」的見聞。（資料來源：哈佛大學圖書館，寶顏堂秘籍，https://nrs.lib.harvard.edu/urn-3:fhcl:25595537?n=1666）

清道光 18 年（公元 1838 年）嚴如煜彙編的《洋防輯要》，就將南海「萬里長沙」繪入清國海防巡守範圍；繪圖內的萬里長沙，泛指「萬里」石塘（今日的南沙群島）與千里「長沙」（西沙群島），此為清國最早將南海諸島正確位置納入海防的明證。又過半個世紀的清光緒 9 年（公元 1883 年），光緒皇帝以清國過往百餘年繪製的「江海險要圖」與《洋防輯要》，向全球宣告此為聲索南海諸島主權憑證。

清朝嚴如煜彙編的《洋防輯要》即將南海「萬里長沙」繪入清國海防巡守範圍。（資料來源：香港中文大學圖書館，洋防輯要，https://repository.lib.cuhk.edu.hk/tc/item/cuhk-730505#page/41/mode/2up）

1895 年之後

日本取臺後，關注「南支諸島」（今日的南海諸島）豐沛的海洋資源及日益重要的戰略地位，在「南進」的政略指導下，日本在黃山馬峙進行繪測，向天皇建議將部分南支諸島更名為新南群島，重新命名黃山馬峙為「ながしま」（日本漢字為長島）；日本從此採用新名稱，沿用至太平洋戰爭結束止。

昭和 14 年（公元 1939 年）3 月 1 日，日本帝國海軍馬公要港部編成中隊（連級）規模的「新南群島派遣隊」駐守長島，並設置海軍病院。4 月 28 日，臺灣總督府以「告示 122 號」，宣布新南群島歸高雄州高雄市設治管理，併入日本版圖，還在長島新設庄役所，派遣庄長治理，轄有警察官吏派出所，負責治安兼辦港口防疫。因此，歷史上這座珊瑚島嶼首次有國家設治，行使主權管轄。

日本是歷史上首次在黃山馬峙進行設治管理的國家，並將島嶼重新命名為「長島」；太平洋戰爭結束後，由我國接收南沙群島，再將長島改名為「太平島」。（圖片來源：外交部，https://www.roc-taiwan.org/uschi/post/1388.html；國家發展委員會檔案管理局，https://www.archives.gov.tw/alohasImages/54/search.html#）

民國 79 年內政部報奉施行，太平島自此屬高雄市行政轄管，並於民國 99 年定編為高雄市旗津區中興里 18 鄰南沙 1 號，成為我國南疆極南的戶政地址。（圖片來源：行政院，https://www.ey.gov.tw/state/4447F4A951A1EC45/094b1d53-de8d-4393-bde6-ab092969cce4；海洋委員會海巡署東南沙分署，https://www.cga.gov.tw/GipOpen/wSite/ct?xItem=81470&ctNode=10472&mp=9994）

日軍敗亡後，我海軍接收南沙群島，內政部重新命名長島為太平島，政府委請海軍設置「南沙群島管理處」代管，替政府行使治權。政府再於民國 45 年 6 月將南沙群島管理處晉名為「海軍南沙守備區指揮部」。

比照日本取臺期間首次在太平島設治時，係將新南群島的長島劃歸高雄州的高雄市行政管轄，民國 78 年高雄市政府建請將南沙群島的太平島以行政託管模式，納入高雄市政府管理。於民國 79 年核定內政部報奉施行，從此太平島屬於我國高雄市行政轄管。

民國 88 年底「海軍南沙守備區指揮部」撤銷編制，兩個月後行政院「海岸巡防署」（海巡署）立銜運作，復編「南沙指揮部」，改隸海巡署海岸巡防總局，海域執法由具海洋警察身分的海巡人員執行，並代替國軍守島。

民國 99 年 1 月，「南沙指揮部」的行政區劃門牌，定編為高雄市旗津區中興里 18 鄰南沙 1 號，成為我國南疆極南的戶政地址。民國 107 年 4 月，行政院新設海洋委員會，所轄之南沙指揮部連同門牌納編入海巡署整編之東南沙分署內。

漫漫歲月，太平島始終於國境南疆綻放其熱帶風華。

知彼知己 才能規避高風險

◆ 臺灣警察專科學校前校長 — 陳連禎

司馬楚之看見驢的耳朵被人割下，當下預判「大敵將至」，可說是「一葉知秋」最佳範例。

阻絕災禍於門前　境外決戰能躲劫

決戰境外，阻絕禍害於家門前是危機預防的上策。而危機預防之成敗，常繫於當事人能否立即反應「明哲保身」。「明哲保身」除了要有過人的洞察力，遇事不慌不亂的修養外，更要有知己知彼的功夫，才能防範未然。南北朝司馬楚之因深具危機意識，而能躲過一劫。

軍中驢耳朵被割 將軍立馬下令築城

劉裕篡廢晉朝而建立劉宋，據《資治通鑑》記載，劉裕上位後第一件大事就是「誅翦宗室之有才望者」。司馬宗室有才望的多沒能躲過政治追殺之災，唯獨司馬楚之一人倖免於難。

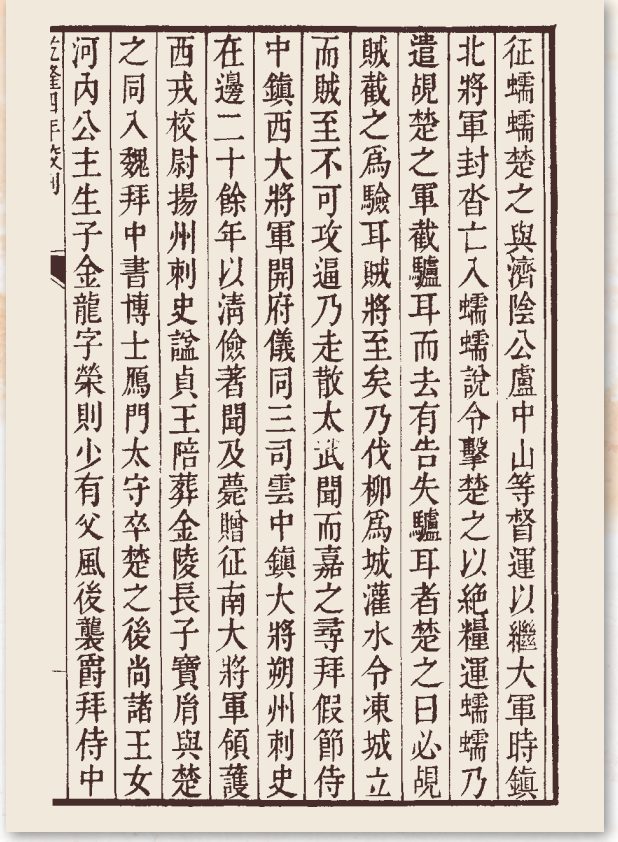
司馬楚之是司馬懿四弟的八世孫，能力強、聲望高，成為北魏大將，被派任征討柔然汗國，並負責後軍押運糧草重任。司馬楚之親自督考軍糧運輸，檢查柳樹林附近行軍情況；這時士兵來報，發現有隻驢子少了一耳朵。司馬楚之親自到現場檢查，思考片刻，神情瞬間凝重。他迅即下令三軍原地待命，稍後又命令就地築城。[1] 司馬楚之讓士兵砍下柳樹，再用柳條和著泥巴築城，化為一座被冰凍的堅固城池，其實就是座冰牆。

過了不久，柔然騎兵果然撲天蓋地殺來，而司馬楚之好整以暇備戰。騎兵在冬天遇到堅硬而滑溜的冰牆，根本無法躍起入城。柔然騎兵一時無法得逞，又唯恐北魏大軍支援圍剿，只好悵然撤退。

事後兵眾對司馬楚之的神預判嘆服不已，並問他如何得知內情？司馬楚之解釋，驢的耳朵被割，判斷必是柔然前來偵蒐、刺探軍情的間諜，他回去為了取信當局而割下驢耳當作證物，這是柔然人習俗。司馬楚之知彼知己，研判對方將會很快侵犯，所以當機立斷，要早做準備。[2] 司馬楚之親

[1] 《北史》記載：「即使軍人伐柳為城，水灌之令凍，城立而賊至。冰峻城固，不可攻逼，賊乃走散。」

[2] 《北史》記載：「蠕蠕乃遣奸覘入楚之軍，截驢耳而去。有告失驢耳者，諸將莫能察。楚之曰：『必是覘賊截之以為驗耳，賊將至矣。』」


征蠕蠕楚之與濟陰公盧中山等督運以繼大軍時鎮北將軍封沓亡入蠕蠕說令擊楚之以絕糧運蠕蠕乃遣覘楚之軍截驢耳而去有告失驢耳者楚之曰必覘賊截之爲驗耳賊將至矣乃伐柳爲城灌水令凍城立而賊至不可攻逼乃走散太武聞而嘉之尋拜假節侍中鎮西大將軍開府儀同三司雲中鎮大將朔州刺史在邊二十餘年以清儉著聞及薨贈征南大將軍領護西戎校尉揚州刺史謚貞王陪葬金陵長子寶肩與楚之同入魏拜中書博士鴈門太守卒楚之後尚諸王女河內公主生子金龍字榮則少有父風後襲爵拜侍中

自督導勤務的時候，見微知著，既熟悉對手的風俗習性，又有高風險敏感度的反制作為，實深具危機意識。

華人首富李嘉誠 具危機意識而安然無恙

2008 年全球金融危機，各國哀鴻遍野，災情慘重。喜愛中華文化具憂患意識的華人首富李嘉誠，則有備無患。李嘉誠是一個危機感很強的人，從早年創業至今，一直保持著兩個習慣：一是睡覺之前一定要看書；二是晚飯之後一定要看十幾二十分鐘的英文電視，不僅要看，還要跟著大聲說，因為怕落伍。

華人首富李嘉誠有每天閱讀、自省的好習慣，時時具憂患意識，因而順利熬過全球金融危機。（Photo Credit: EdTech Stanford University School of Medicine, https://flic.kr/p/8FAs6A）

李嘉誠有每天閱讀、自省的好習慣。他總是在內心不停地給自己提問題，然後不斷設想如何解決問題。由於李嘉誠平時未雨綢繆，準確預見金融危機發生，並已備傘防禦，因此 2008 年的全球金融危機，李嘉誠集團不僅安然無恙，還從中獲利得以擴張事業版圖。

1996 年，李嘉誠長子李澤鉅被世紀大盜張子強綁架，對方單槍匹馬到李嘉誠家中，開口就是要 20 億，李嘉誠當場同意。李嘉誠的鎮靜，連張子強都很意外，張子強問他：「你為何這麼冷靜？」

李嘉誠答道：「因為這次是我的錯。我們在香港知名度這麼高，但是一點防備

都沒有，比如我去打球，早上五點多自己開車去新界，在路上，幾部車就可以把我圍住，而我竟然一點防備都沒有，我要仔細檢討一下。」

當時他勸告張子強：「你拿了這麼多錢，下輩子夠花了，趁現在遠走高飛，洗心革面，做個好人；如果再犯錯，就沒有人可以再幫到你了。」據李嘉誠透露，後來張子強又打電話給他；李嘉誠說：「你搞什麼鬼，怎麼還有電話？」張子強說：「李先生，我自己好賭，錢都輸光了，你教教我，還有什麼是可以投資的？」李嘉誠：「我只能教你做好人，但你要我做什麼，我不會了。你只有一條大路，遠走高飛，不然，你的下場將很可悲。」張子強沒有危機感，下場不問可知。

李嘉誠將這種冷靜功夫，歸功於他喜歡看書，「我喜歡看書，什麼書都看，這對我都有用，今天有用，明天也有用。所以，很多大事來的時候，我也能解決。」

安不忘危，存不忘亡，治不忘亂

孔子曾說：凡是招致危險的人，都是因為他安逸於他的職位上；滅亡的國家，是因為自以為國家可以長存；敗亂的國家，是因為自以為已經治理穩定。因此君子安居而不忘傾危，生存而不忘滅亡，整治而不忘敗亂，自身則可常安，而國家可以永保。[3]《易經》也說：心中時時警惕著，將滅亡了！將滅亡了！天下的治安，就能像繫在堅固的桑樹根上一樣安穩。以上皆為先賢提醒我們平時就要具備憂患意識，司馬楚之、李嘉誠等二人生於憂患，具有「知己知彼」的用心覺察、能細膩觀察周遭環境變化的特質，才能過著天清地寧的日子，順利避開「黑天鵝」天翻地覆般的災難襲擊。

李嘉誠（左圖右）的長子李澤鉅（左圖左）曾被世紀大盜張子強（右圖）綁架，李嘉誠理智面對。（圖片來源：Province of British Columbia，https://flic.kr/p/d9vVNQ；截自中天新聞，https://youtu.be/pumFJA9myaM）

[3] 孔子好學《易經》、好問問題有成。子曰：「危者安其位者也，亡者保其存者也，亂者有其治者也。是故君子，安不忘危，存不忘亡，治不忘亂，是以身安而國家可保也。《易》曰：『其亡其亡！繫于苞桑。』」https://www.facebook.com/QunshuZhiyaoTW/posts/3075336335885630/。

東港海鮮美食

（Photo Credit: Johnson Wang, https://flic.kr/p/7KMhiM）

◆ 菱　怡

黑鮪魚是壽司中的極品，油花媲美和牛，口感猶如冰淇琳，入口即化。東港不僅只有黑鮪魚，國寶級的櫻花蝦，在這裡也吃得到。

東港三寶—黑鮪魚、櫻花蝦、油魚子

以「迎王祭」聞名全臺的東港鎮，是臺灣三大漁港之一，全鎮有超過半數人口都仰賴漁撈和養殖為生，是個不折不扣的「漁鄉」。其出產的海鮮，有口皆碑，尤其是有東港三寶之稱的「黑鮪魚、櫻花蝦、油魚子」，更是老饕們絕不能錯過的特產美食。

黑鮪魚品質優

最懂門道的海鮮饕客，絕不會錯過每年 4 至 6 月黑鮪魚最肥美的季節，[1] 屏東東港為臺灣黑鮪魚的主要捕獲地，2021 年捕獲量不但是全臺第一，更是全世界第一！[2] 只要吃過黑鮪魚生魚片，就會對那充滿豐富油脂、入口即化的口感驚豔。

[1] 2022 年「屏東黑鮪魚文化觀光季」於 4 月 7 日至 7 月 24 日舉辦。

[2] 2021 年黑鮪季捕獲量創新高，總數突破 4 千尾。《屏東黑鮪季 4371 尾創 14 年新高，疫情衝擊價格低迷》，https://news.ltn.com.tw/news/life/breakingnews/3605212。

東港為臺灣三大漁港之一，漁撈業奠定了東港經濟發展的基礎。（圖片來源：黃昱峰，https://flic.kr/p/2jiJMfM）

屏東縣政府每年會在黑鮪魚最肥美的季節舉辦「黑鮪魚文化觀光季」，其中「第一鮪拍賣」的活動享譽全臺，拍賣金額大多能超過百萬元以上。（圖片來源：屏東縣政府傳播暨國際事務處，https://www.pthg.gov.tw/plantou/cp.aspx?n=21C9C568BBDD7864）

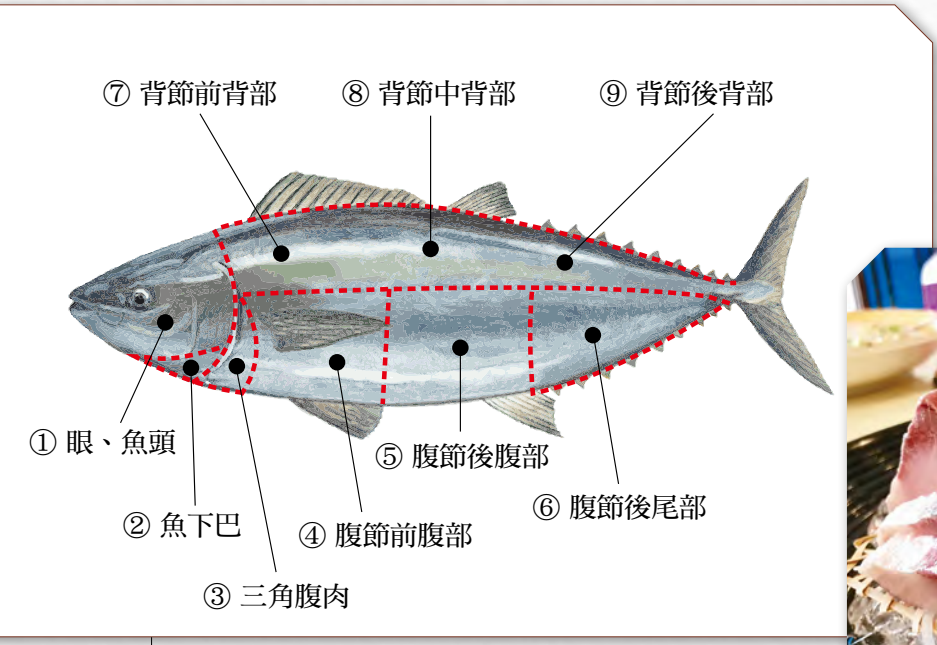
黑鮪魚是鮪類中體型最大的一種，其肉質鮮美，油脂豐厚，不論做成生魚片或各式料理，皆非常美味，膽固醇不高且富含 DHA，營養健康。黑鮪魚最高級的肉質，是從鰓到腹部的部位，稱為「上腹」，為生魚片中的極品，呈淡粉紅色，脂豐肉嫩；其次，是中腹到尾部，俗稱「中腹」，油脂稍少，屬中上等級，肉質也極為鮮美。油花美得像和牛的「金三角」，則位於黑鮪魚頭鰓下到上腹之間，號稱是魚界的松阪牛，肉質與香味最棒，入口後輕輕化開完全不用咬，淡淡油脂香在脣齒間流竄，更是東港的金字招牌，價格卻只有臺北的一半、日本的十分之一，因此，吸引了不少觀光客到此嚐鮮、大飽口福。

櫻花蝦鈣質豐

每年 11 月至隔年 5 月是東港櫻花蝦的捕撈期，俗名為「花殼仔」的櫻花蝦，屬群聚性浮游生物，因身上布滿紅色素及發光器，讓外觀粉紅透明，在海洋中群體游動時像櫻花繽紛落下，因而得名。

早年櫻花蝦被認為僅分布於日本靜岡縣沿海，[3] 直到 1980 年代，東港櫻花蝦才

[3] 日本早已將櫻花蝦列為國寶級水產品，http://gustavechang.blogspot.com/2017/06/blog-post_18.html。



黑鮪魚因部位不同而價格有異，然從頭到尾皆美味。

東港黑鮪魚生魚片各部位皆肉質鮮美、油脂豐厚。（Photo Credit: OZ & SUSAN, https://flic.kr/p/26W4MA6）

被日本學者大森信確認其與日本的櫻花蝦同種。在日本櫻花蝦產量逐漸缺少，日人開始向臺高價收購後，東港漁民才感受到櫻花蝦的經濟價值；由於稀有，櫻花蝦在臺亦被稱為「國寶蝦」。櫻花蝦是上天特別眷顧予東港的禮物，平時潛藏深海，迴流到東港後，因洋流浮起而易被捕獲。

早期的競爭濫補，讓櫻花蝦曾面臨枯竭，討海人自發守護，成立產銷班，[4] 將所有捕蝦船納入公約，限定捕撈期間與捕撈數量，[5] 一方面不會因捕撈太多而讓價格崩跌，另方面漁民也可休養生息，讓櫻花蝦繼續繁衍。沒想到的是，限制捕撈數量後，櫻花蝦售價因此攀升，[6] 漁民收入明顯提高。產銷班每艘船遵守規定，為永續經營海洋資源樹立典範，堪稱是團結自律的「臺灣之光」漁業傳奇。近年宜蘭頭城龜山島櫻花蝦漁業興盛，[7] 頭城亦成立產銷班來控管漁獲量，再度成為另一個自主漁業管理的典範，現每年產值逾 1.5 億元，成果相當耀眼。

[4] 早年漁民為了生活，只能靠不斷捕撈才能養家餬口，櫻花蝦因此面臨枯竭，且因大量撈捕而價格崩跌。「東港櫻花蝦產銷班」成立於民國 81 年，建立自律公約，規範定時、定量捕捉並嚴禁私賣，不僅讓櫻花蝦價格上升數十倍，櫻花蝦資源因此也得到保護。《櫻花蝦之光 01—誰說漁業和保育不能並重？東港漁民嚴格自律，寫下櫻花蝦護漁傳奇》，https://www.newsmarket.com.tw/blog/162672/。

[5] 捕撈期間為每年 11 月至翌年 5 月，週休二日強制為停捕日；捕撈數量因 2020 年起收獲量減少，產銷班下修每船每航次捕撈上限，從 12 箱（每箱 15 公斤）改成 10 箱。《櫻花蝦變少了？東港櫻花蝦產銷班下修捕撈上限保護蝦資源》，https://www.agriharvest.tw/archives/11213。

[6] 櫻花蝦每箱（15 公斤）均價可達 7 千元，估算每艘漁船年收入約在 2、3 百萬，甚可高達 7 百萬。

[7] 國內另一個櫻花蝦產地在宜蘭龜山島海域，捕撈時間是每年 2 月至 8 月，https://www.agriharvest.tw/archives/33697。

櫻花蝦外型小巧玲瓏，成蝦約 5 公分，外殼細薄柔軟，肉質鮮甜，[8] 其鈣質特別適合人體吸收，[9] 且含有鉀、鎂和蛋白質等營養成分，加以深海不受汙染，被日本人視為珍饈與補品。不過，日本櫻花蝦供不應求，更加大對臺採購，目前東港 9 成的櫻花蝦都銷往日本。

櫻花蝦是大廚名菜與家常料理的絕配，可以快火炒香，當作小菜下酒，或炒飯、炒蛋、炒高麗菜與滷白菜等，亦可製成櫻花蝦米糕等傳統美食。由於櫻花蝦殼柔嫩，肉質鮮美，頗受消費者好評，業者更開發出各種櫻花蝦即食零嘴，每一口都能讓人吃到健康與美味。

油魚子口感佳

油魚子外表，看起來很像烏魚子，呈橢圓形（烏魚子為菱形），但比烏魚子大，色澤較暗，不透光，也較為罕見，價格較烏魚子便宜。油魚子製作過程，和烏魚子加工類似，但難度卻比烏魚子更高，製作更耗工費時。

櫻花蝦俗稱「花殼仔」，因身上布滿紅色素及發光器，外觀看起來粉紅透明。（Photo Credit: michelle.khuu, https://flic.kr/p/4Dinx5）

櫻花蝦外型小巧玲瓏，外殼細薄柔軟，肉質鮮甜，日人習慣生食。（Photo Credit: Miyuki Meinaka, https://w.wiki/4$Pt）

[8] 櫻花蝦是少數人類可以直接攝食的浮游動物。《海洋生物資源永續發展課程》，https://smbrcourse.wordpress.com/sergestidshrimp/。

[9] 營養師表示，櫻花蝦鈣質是蝦米的 2.8 倍，而且營養多元豐富。《日本吃客最愛！ 台灣櫻花蝦營養加倍，老人、小孩、孕婦都能補》，https://health.tvbs.com.tw/nutrition/316028。

櫻花蝦是大廚名菜與家常料理的絕配，可以快火拌炒各樣食材，亦可當作下酒的小菜；左圖為櫻花蝦炒飯，右圖為櫻花蝦零嘴。（圖片來源：Sunline Liu, https://flic.kr/p/6gefe4；江虹興，https://flic.kr/p/DKATo4）

油魚是在遠洋海域所捕撈到的魚類，更顯彌足珍貴。油魚卵巢含豐富油脂，鹽醃加工製成油魚子後，肉質纖細豐腴，香且甘甜。食用方式與烏魚子相似，[10] 食用前可先用火燻烤，或用高粱酒浸煮後，再切成薄片，搭配水梨、蘋果等水分多且質地爽脆的果物，吃起來鹹香順口。在東港各家海產店中，皆可嚐到此道料理。

「那個魚」肉質嫩

特別推薦東港特產「那個魚」，由於其肉質鮮嫩，油炸後口感軟綿，吃起來像果凍或豆腐，入口即化，許多遊客到東港，都會特地點「那個魚」來品嚐一下。

「那個魚」學名為「小鰭鎌齒魚」，屬東港地區獨有的海水魚，其頭部長得像鰻魚，全身軟趴趴，烹煮後，全身變透明狀，又名「水晶魚」。由於「那個魚」的名字太難念了，消費者在購買時就直接用手指，點名要買「那個魚」，後來約定成俗，現在已成為東港特色美食。

「那個魚」因含水量高，捕撈上岸後，若放置過久，魚身會像水般融化掉，只剩下魚頭。由於魚體多刺，又沒有很多肉，整條軟軟的模樣，賣相不甚理想。過去漁民捕撈上船後，都是自己帶回家吃；但風水輪流轉，現在「那個魚」身價翻紅好幾倍，是老饕們的最愛，在東港每家海產餐廳，都可以點到這道菜。「那個魚」因為沒有鱗片，料理方式大多由廚師先切成塊狀，再裹粉油炸，快炸起鍋，外酥內嫩，肉質鬆軟鮮甜，總能令吃貨們食指大動。

[10] 《臺灣烏金—烏魚》，http://mjib-ebook.com/MJIB/no37/index.html#p=81，本刊第 37 期頁 81 至 86。

逛魚市嚐小吃

東港魚市場遠近馳名，不僅漁獲種類多，品質高檔，價格也很實惠；最受外地客歡迎的當屬「華僑市場」，[11] 為生猛海鮮的大本營。很多去小琉球玩的遊客，搭船回東港後，都會來此買新鮮魚產回家，當地人稱這些出手闊綽的貴賓為「華僑」，因而得名。

有人說，到東港看魚、買魚、吃魚，會讓您年年有「餘」。不只華僑市場，附近光復路更是海鮮餐廳匯聚地，各種海鮮美食琳瑯滿目，從中式快炒料理到充滿日式風情的壽司應有盡有。坐在港邊看海景、大啖海鮮，品味豪爽奔放的漁港風情，絕對是最道地的東港體驗！

油魚子外表看起來很像烏魚子，形狀為橢圓形，食用方式和烏魚子相同。（圖片來源：東港鎮農會，https://www.dgpa.org.tw/product.aspx?PNo=9）

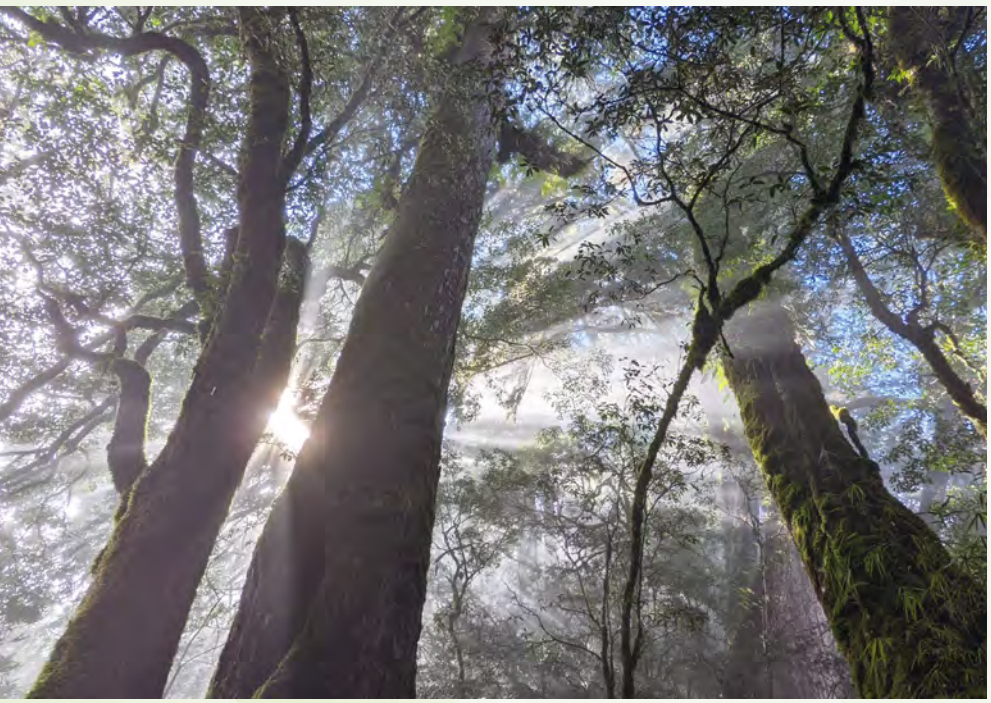
因為名字太難念而被取名為「那個魚」的小鰭鎌齒魚，現已成為東港特色美食，經油炸後外酥內嫩，肉質鬆軟鮮甜。（Photo Credit: Sunline Liu, https://flic.kr/p/6gefVV）

東港魚市場遠近馳名，漁獲種類多、品質高檔且價格實惠，圖為東港華僑市場魚類的現撈區。（Photo Credit: Kun-chia Wu, https://flic.kr/p/XY6u5z）

[11] 為黃昏市場，每天中午營業至晚上 7 點結束。華僑市場因老舊而重建，2012 年全新啟用，更名為「東港漁港漁產品直銷中心」，成為新穎且具地方特色的觀光休閒魚市。占地 1,500 坪，攤位 4 百個，提供各式各樣現撈且價廉之魚貨與新鮮現作美食而遠近馳名。《東港漁產品直銷中心 (華僑市場) 導覽手冊》，https://www.pthg.gov.tw/film/Photo_Content.aspx?n=1635F69C7777535B&s=D47B46EF27BF1D0D。

可以是天堂 也可以是地獄的中級山

◆ 文字、攝影／行政院農業委員會林業試驗所—徐嘉君



攀爬豬股山這天一開始天氣很陰鬱，登山客狼狽的身著雨衣，在雨中疾行，撥開滿是水珠的箭竹林掙扎前進，林下的枯木上，有如纳斯卡線般昆蟲啃蝕的痕跡，有一種詭異的美麗。

倏地從樹冠層射入一道溫暖的陽光，原來是爬升突破雲霧層來到清朗的秋陽下了，走在稜線上的時候，從森林間隙看到一座座好似飄浮在海上的山頭，這就是攀登臺灣雲霧帶中級山的魅力，先把登山客重重摔落到濕冷地獄，再高高舉起賜予你天堂般的美景。

111 年法務部調查局調查人員特考（三等考試）

報名日期：111 年 5 月 3 日至 12 日（網路下載報名表／紙本寄件）
考試日期：111 年 8 月 13 日至 14 日（第一試筆試）
考試主辦機關：考選部（02-22369188 轉特考司）
報名書表（應考須知）：請於報名期間利用考選部網站下載報名　　（法務部調查局）

組別	第一試		第二試	第三試	備註
	普通科目	專業科目	體能測驗	口試	
調查工作組	一、國文（作文、公文與測驗） 二、綜合法政知識與英文	三、社會學 四、政治學 五、刑法與刑事訴訟法 六、外國文（詳附註）	心肺耐力測驗 1,200 公尺跑走 ※ 及格標準 男性： 5 分 50 秒以內 女性： 6 分 20 秒以內	個別口試	1. 考試預定錄取名額以考選部正式公告為準。 2. 有關年齡、兵役及學歷等應考資格及應繳文件，可至考選部網站應考人專區下載本年度應考須知，內已詳載。 3. 相關法規：公務人員特種考試法務部調查局調查人員考試規則。 4. 本項考試錄取人員，由法務部調查局幹部訓練所訓練 1 年，成績及格者，分發該局及所屬各機關服務，從事反制敵諜滲透、檢肅貪污、防制重大經濟及洗錢犯罪以及查緝毒品等國家調查官工作，無分男女性別、報考組別或從事之調查工作類型，必須服從命令，接受任務指派；該局鼓勵調查人員接受各項職務歷練，以豐厚完整調查工作資歷。 5. 進一步瞭解相關工作內容請參閱法務部調查局全球資訊網：
法律實務組		三、刑法 四、刑事訴訟法 五、行政法 六、商事法			
財經實務組		三、經濟學 四、財務管理 五、中級會計學 六、證券交易法與商業會計法			
化學鑑識組		三、生物化學 四、有機化學 五、分析化學 六、儀器分析			
醫學鑑識組		三、生物化學 四、有機化學 五、分子生物學 六、遺傳學			
電子科學組		三、電子學與電路學 四、計算機概論 五、工程數學 六、通信與系統			
資訊科學組		三、系統分析與設計 四、資料庫應用 五、資通網路 六、資訊安全實務			
營繕工程組		三、結構分析 四、營建法規 五、施工法 六、政府採購法			
附註：外國文選試科目（英文、日文、德文、西班牙文、阿拉伯文、法文、俄文、韓文）。					

各項考試資訊請參考考選部（https://www.moex.gov.tw）或法務部調查局（https://www.mjib.gov.tw）網站特考資訊專區，並以考選部正式公告為準。

邀稿說明

一、 清流雙月刊是法務部調查局所發行之「全國安全防護」宣導刊物，邀稿完全對外公開，歡迎踴躍投稿。

二、 本刊宗旨為宣導國家安全，投稿方向可參閱本刊的單元類別 ，或至法務部官網電子書櫃「清流雙月刊徵稿說明及訊息公告」查詢。

三、 本刊刊載以白話且易讀的文章為主，來稿字數以 2,000 字內為限，並請加註 60 字內摘要；若投稿為**主要業務**相關的文章，字數限制可調整至 3,000 字以內。本刊對來稿保有修改與增刪之權力。

四、 文章一經發表，其著作財產權即授權本刊，並同意經本局再行授權第三人利用，但作者仍保有著作人格權，保有該著作未來自行集結出版與教學等個人使用之權利。

五、 由於本刊為政府出版品，投稿文章需同時授權予政府出版品主管機關— 文化部以及文化部所授權之對象刊載。

六、 投稿文字請寄送至電子信箱：2d40@mjib.gov.tw，並留下聯絡電話及住址（未留聯絡方式、非電子檔形式之稿件及圖片，不予採用，亦不主動退回）由於本局信箱有單信最大容量上限（8MB），若投稿內容包括圖片等較大容量之檔案，請分封寄送。

七、 清流雜誌社聯繫電話為：02-29112241 轉 3332 或 3333

八、 本刊發行層面廣泛，致文章內容難以兼顧各界需求；若有價值觀或理念不同者，敬請讀者見諒。

電子書連結說明

今年 4 月，中共遼寧號結束南海訓練後，航經巴士海峽續向東航行，被我國防部全程監控的畫面。（圖片來源：軍聞社，https://mna.gpwb.gov.tw/post.php?id=8&message=98515）

電子書版本提供自動連結，點選後可連線至資料或影像來源，閱讀更多相關資訊。

友情陣線

海巡季刊

移民雙月刊

警光

讀者意見表

一、請問您從何處取得本刊？

☐ 我是訂戶　☐ 親友熟識推薦　☐ 公共場所、圖書館

☐ 其他 _____

二、您閱讀本刊的原因是？

☐ 訂戶定期閱讀　☐ 被封面吸引　☐ 喜歡某位作者或文章

☐ 其他 _____

三、您喜歡哪些美術編排？

☐ 封面　☐ 封底　☐ 目錄　☐ 主題文章

☐ 內文排版與圖片，頁數：_____

四、本期喜歡的單元是：

☐ 數位時代防護術　☐ 生活中的資安　☐ 西進停看聽　☐ CI 學堂

☐ 詐欺實錄　☐ 法令天地　☐ 時代故事　☐ 風險管理歷史課

☐ 餐桌上的臺灣旅行　☐ 絕美臺灣

☐ 其他：_____

五、您的基本資料：

姓　名：　　電話 / E-mail：

住　址：

年　齡：○ 20 歲以下　○ 21-40 歲　○ 41-60 歲　○ 61 歲以上

學　歷：○ 國中以下　○ 高中職　○ 大學（專）以上　○ 碩士　○ 博士

職　業：○ 上班族　○ 軍公教　○ 學生　○ 家管　○ 已退休　○ 其他_____

※ 本刊依個人資料保護法及相關法令規定，所蒐集之個人資料僅做聯繫及相關合理應用。

其他建議：

_____

_____

_____

_____

電子版讀者意見表

※ 感謝您耐心填寫，若意見獲得採用將有機會獲得精美小禮。

傳真：02-29112314

法務部調查局檢舉專用電話一覽表

機關名稱	地址	檢舉電話
法務部調查局	231209 新北市新店區中華路 74 號	(02) 29177777 (02) 29188888 (傳真)
臺北市調查處	106229 臺北市大安區基隆路二段 176 號	(02) 27328888
新北市調查處	220075 新北市板橋區漢生東路 193 巷 2 號	(02) 29628888
桃園市調查處	330026 桃園市桃園區縣府路 19 號	(03) 3328888
臺中市調查處	403012 臺中市西區英才路 525 號	(04) 23038888
臺南市調查處	708008 臺南市安平區永華路二段 208 號	(06) 2988888
高雄市調查處	801612 高雄市前金區成功一路 428 號	(07) 2818888
航業調查處	435059 臺中市梧棲區臨港路四段 390 號	(04) 26560555
福建省調查處	893017 金門縣金城鎮西海路一段 65 號	(082) 322888
基隆市調查站	201005 基隆市信義區崇法街 220 號	(02) 24668888
宜蘭縣調查站	260023 宜蘭市津梅路 52 號	(03) 9288888
新竹市調查站	300075 新竹市香山區經國路三段 126 號	(03) 5388888
新竹縣調查站	302099 新竹縣竹北市光明五街 56 號	(03) 5558888
苗栗縣調查站	360017 苗栗市玉清路 382 號	(037) 358888
南投縣調查站	540019 南投市民族路 486 號	(049) 2228888
彰化縣調查站	500034 彰化市卦山路 12 號	(04) 7248888
雲林縣調查站	640013 雲林縣斗六市鎮南路 67 號	(05) 5328888
嘉義市調查站	600011 嘉義市東區維新路 321 號	(05) 2778888
嘉義縣調查站	613016 嘉義縣朴子市朴子一路 1 號	(05) 3628888
屏東縣調查站	900044 屏東市合作街 51 號	(08) 7368888
花蓮縣調查站	970064 花蓮市中美路 3-33 號	(03) 8338888
臺東縣調查站	950254 臺東市中興路二段 731 號	(089) 236180
澎湖縣調查站	880010 澎湖縣馬公市新明路 77 號	(06) 9278888
馬祖調查站	209001 連江縣南竿鄉介壽村 15 號	(0836) 22258
北部地區機動工作站	235028 新北市中和區永和路 33 號	(02) 22482626
中部地區機動工作站	407003 臺中市西屯區福順路 500 號	(04) 24615588
南部地區機動工作站	812003 高雄市小港區平和南路 129 號	(07) 8122910
東部地區機動工作站	970018 花蓮市瑞美路 7 號	(03) 823-3712
國家安全維護工作站	231206 新北市新店區中生路 40 號	(02) 22177211
航業調查處基隆站	202007 基隆市中正區中正路 303 號	(02) 24633633
航業調查處高雄站	806041 高雄市前鎮區佛公路 167 號	(07) 8134888

調查局免付費「檢舉專線電話」— 0800-007-007

設定直接轉接至調查局北、中、南、東四個地區機動工作站及外島處站，值日人員 24 小時接聽受理

一水之隔的民主與威權

英國「經濟學人資訊社」（EIU）公布 2021 年全球民主指數，臺灣在 167 個受評比國家排名第 8，高居東亞之首，被歸在「完全民主」（full democracy）的級距中；中國大陸則落居全球第 148 名，被歸類為「專制政權」（authoritarian regime）。