酒駕修法要既見秋毫亦見輿薪

大學助理教授／趙萃文

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意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）

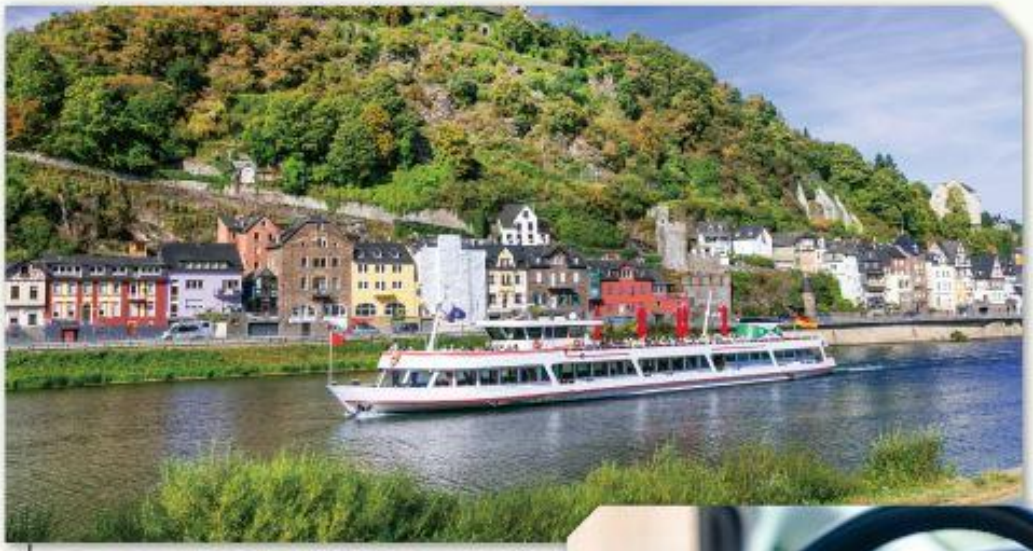
鄰近日本亦有酒駕問題，其另制定《道路交通法》特別法，加重處罰酒駕及其他重大違規行為（如超速、無視號誌、危險駕駛等），重大違規致死最高處20年徒刑，相較我國處罰上更加嚴厲，值得注意的是，該國對酒駕及各式不能安全駕駛行為一律重罰，立法上顯然更為完善。觀諸2021年其全國交通事故死亡數僅2,636人，[6]考量到日本總人口數是臺灣的5.5倍，其對酒駕及其他交通犯罪之防制經驗，值得我國修法參考。

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

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。

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。

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。

本文摘自清流雙月刊中華民國111年5月 號P64-P68

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

清流 MJIB

◆ 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

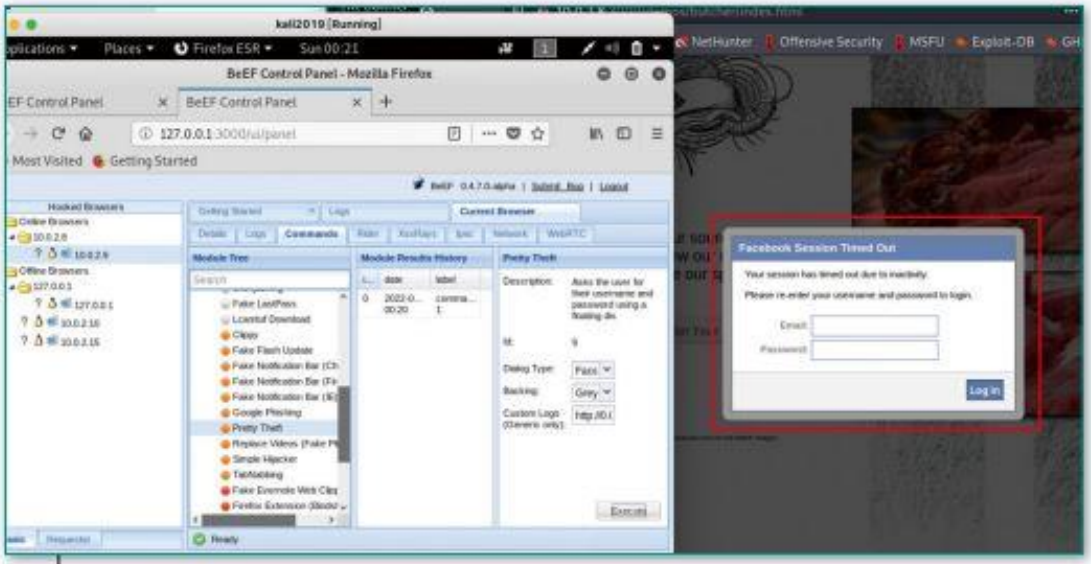
「盡信網路，不如無網路」，已成了現代人對於網路上充斥著太多假訊息，詐騙術無所不在的深沉無奈與抗議。以往享受於瀏覽網頁、沉浸在無論是文字知識的充實之樂，或是音樂影音的華麗饗宴，感受到無比的雀躍。現在卻得要處處防範、時時小心。深怕一個錯誤滑鼠的「click」，造成難以彌補的損失。在大量的影音互動所帶動的誘惑之下，詐騙的行為也因而開始升級。人們很難在多管齊下的誘騙之下能全身而退，最好的防範方式就是讓自己隔絕在這樣的威脅之外。然而，我們現今的科技足以支援這樣的服務嗎？哪些網站是有疑慮的？科技究竟能否幫我們忙，一眼就看穿惡人的把戲？

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/

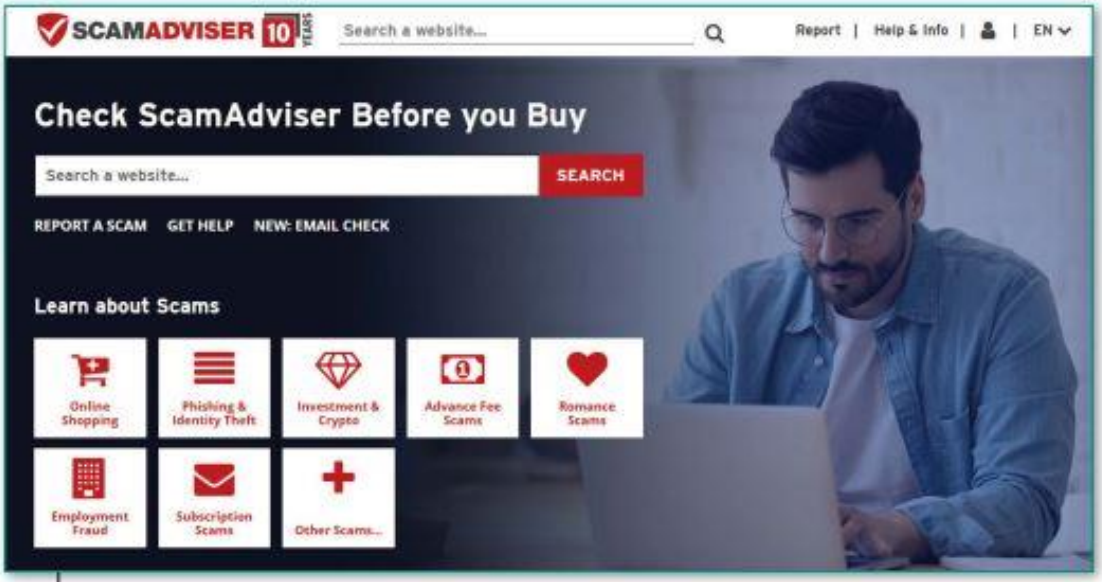
[2] https://www.scamadviser.com/

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？



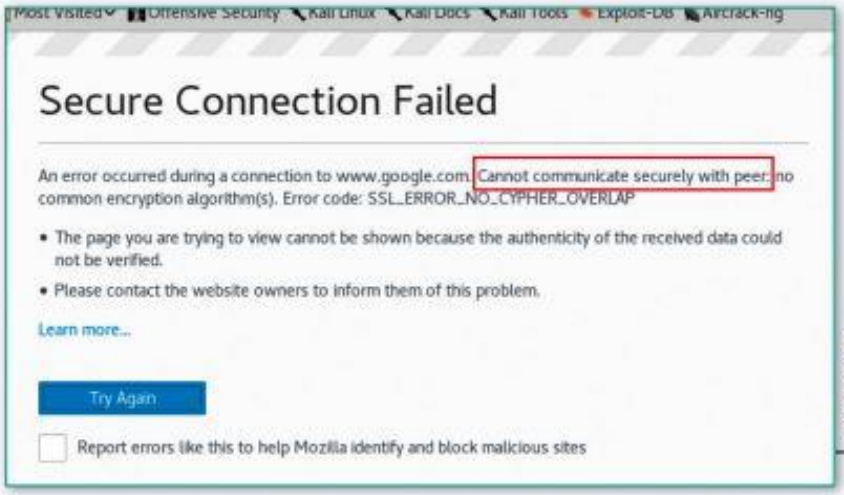
ScamAdviser 是一個免費的網站安全檢測服務，透過多種不同的指標來檢查網站是否安全可靠，使用者只要輸入網址就會顯示結果。（Source: https://www.scamadviser.com）

[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

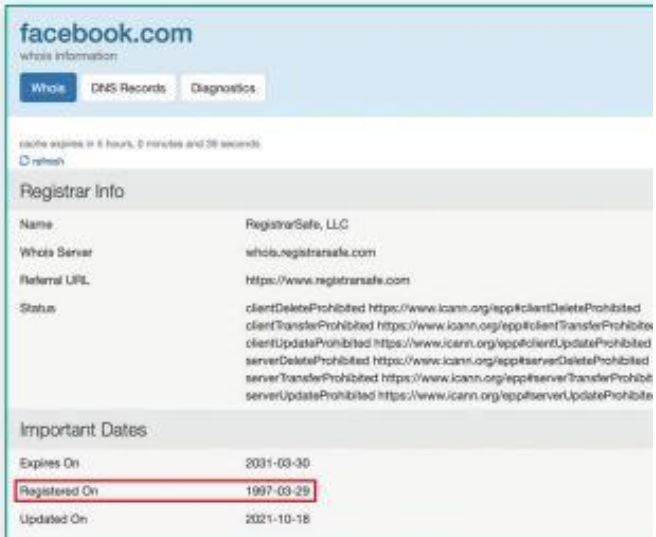
四、開網站後有問題，儘速離開

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

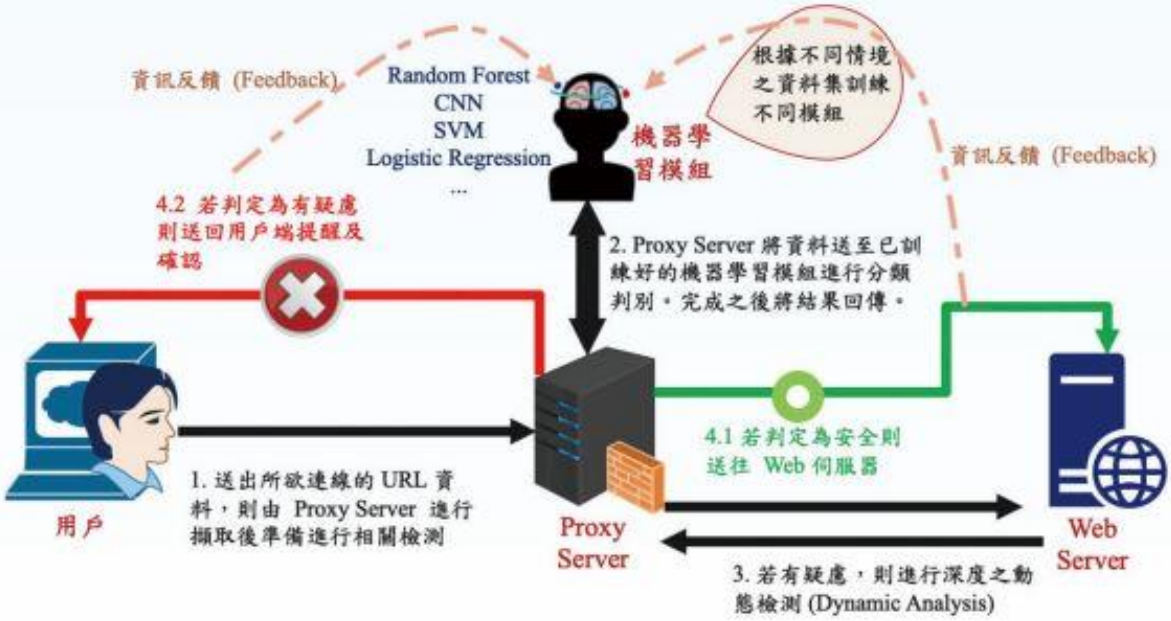


圖 1　整合機器學習的網頁安全性判別模式

[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）

本文摘自清流雙月刊中華民國111年5月 號P28-P35