雙月刊

享受網路便捷，留意資安風險。

清流

No.32
2021.3月號

5G 的
風險與國安

智慧城市中的
5G 運用

美國會大廈暴動
赤裸揭露極右翼之國安威脅

5G網路 引爆萬物互聯

需要全面性的 安全防護

法務部調查局　編印

雙月刊 2021.3月號 NO.32

清流 MJIB

目錄

5G 網路引爆萬物互聯

04 5G 的風險與國安 李忠憲

10 臺灣資安布局—由「布拉格提案」談起 陳永全

17 智慧城市中的 5G 運用 雷喻翔

21 5G 時代的網路安全：以對華為施行禁令的妥適性為例 譚偉恩

28 潛藏的潘朵拉魔盒 馬維駿

放眼國際

33 美國對承包商之網路安全認證 蔡裕明

38 美國會大廈暴動 赤裸揭露極右翼之國安威脅 陳能鏡

生活中的資安

46 5G 與 PK：不可不知的神奇密碼 王旭正

風險管理歷史課

53 至聖之後的至慎先生－絕口不談人事、不說禁中樹 陳連禎

人生戲院

57 由「班恩回家」電影 看戒毒辛酸史 顧崇平

懷舊行旅

63 懷念的老戲院 若　水

聽那山林裡的傳唱

68 走讀塔塔加 林文和

看那藍色大海

74 藍眼淚的奧祕：夜光蟲 蔣國平、蔡昇芳

絕美臺灣

80 桃山神木 徐嘉君

飲膳札記

82 大城小麥新故鄉 周　朝

其他

87 邀稿說明 本　社

88 讀者意見表 本　社

89 法務部調查局檢舉專用電話一覽表 本　社

封面
NO.32 MAR 2021

發 行 人：呂文忠
副發行人：劉復興、吳富梅
社　　長：宋樂怡
副 社 長：歐陽泓、凌文興
主　　編：許淑珍、黃日萱
文字編輯：朱美音
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！

5G 網路 引爆萬物互聯

生物學家威爾森（E. O. Wilson）提出三合一矛盾：認為人類仍處於舊石器時代的情緒、中世紀時期的制度、但卻擁有神般的技術。

5G 網路帶來「心之所向即身歷其境」之神般體驗，然在人性掣肘、政治角力的暗潮洶湧下，民主社會該如何接招？


5G

5G 的風險與國安

◆ 成大電機系教授暨資通安全研究與教學中心主任 — 李忠憲

5G 世代來臨，人類所有行為幾乎全在其覆蓋服務下，若系統建置、零件供應和服務營運所託非人，輕則 24 小時受到嚴密監視，重則隨時被敵人癱瘓。

美國封殺華為主因

5G 通訊設備是現代化國家必備的關鍵基礎設施，5G 建置或營運商是誰，便攸關國安問題，若系統建置、零件供應和服務營運所託非人，輕則 24 小時受到嚴密監視，重則隨時被敵人癱瘓，整個國家將陷入嚴重危機。

美「中」這場貿易戰，表面上是為平衡貿易逆差，實質上是美國希望中共能有結構性轉變。在中共進入世貿組織（WTO）後，利用自由世界得到很多好處，但其持續對出口補貼、嚴格管制市場不准外資自由進出、利用國企壟斷市場，加上「不求所有、但求所在」的政策，強迫外企轉讓

美國封殺中共的華為、中興等公司，不只是爭奪 5G 主導權，也不單純是資安問題，而是國安考量。

技術等措施，讓美國認為這些問題若未改善，貿易戰很難落幕。5G 世界，人類一舉一動難逃監視，美禁止華為與中興等公司，不止是爭奪 5G 主導權這麼簡單，更著眼於國安考量。

中共與俄羅斯、朝鮮向來關係密切，在非洲大幅投資與同地盟友組成同一陣線，在南海問題以金錢拉攏菲律賓、巴基斯坦、柬埔寨等，最近更在美國後院的委內瑞拉背後支持反美勢力。種種跡象顯示，中共試圖在各種戰場上對抗美國，這也是美國朝野兩黨對中共政策有共識的主因。因此，美國對華為或中興的作法，不單純是資安問題，而是國安考量，關係國家生死的 5G 基礎建設，讓美國封殺華為成為必然結果。

「數位獨裁」VS.「社會維穩」

筆者在擔任國家高速網路與計算中心副主任兼資安長時，曾帶隊參加世界超級電腦年會，看到大陸展示多種電腦，每個攤位我都會去問一下，他們到底應用在那方面？據說很多都用在監控人民上面，例如影像辨識、人臉追蹤、人工智慧情緒判斷等等，真的令人感到害怕。

華為研發的高品質攝影機，能即時辨識臉孔，並根據表情推測使用者有無說謊，這將使極權政府可藉此「數位追蹤」，獲得「涉嫌人」的情緒狀態與心理意圖，認定其有影響國安之虞。（圖片來源：Kárlis Dambráns, https://www.flickr.com/photos/janitors/46931581075；路透社／達志影像）

民主臺灣不管任何人，聽到「數位獨裁」，全都感到非常害怕，其實「數位獨裁」在中共已經算是非常成熟的技術，也已經過時，最新版本就是在新疆施行的人工智慧恐怖統治，這是「數位獨裁」的進階版，又可稱為「數位恐怖」。

華為等高科技公司，在半導體製程進步後，所發展出來的超高畫質的攝影機，可在受控制的區域，進行即時的臉孔識別，不僅可以判斷這個人是誰，還能根據表情、眨眼頻率與瞳孔放大情形，來推測這個人的心理狀態，如果與之對談，甚至可以判斷其是否說謊。

利用這些高科技的設備與技術，可以鎮壓所有對政府不滿之運動，即使這些反抗運動都還只是存在於某些人心裡而已。因為在「數位恐怖」時代，極權政府可依「數位追蹤」獲得「涉嫌人」之情緒狀態與心理意圖，而認定其等有影響國安之虞；因此，當大規模抗議運動開始前，幾個抗議領袖可能就會被抓起來，這就是極權政府使用人工智慧來進行「社會維穩」時的可怕之處。

我國政府禁止機關同仁使用華為等陸製手機，惟恐這些手機於機關內部收集資料，再利用沒有管制的電信網路服務傳送予中共管理者。（圖片來源：截自公視新聞，https://youtu.be/Q8oUV6EObos）

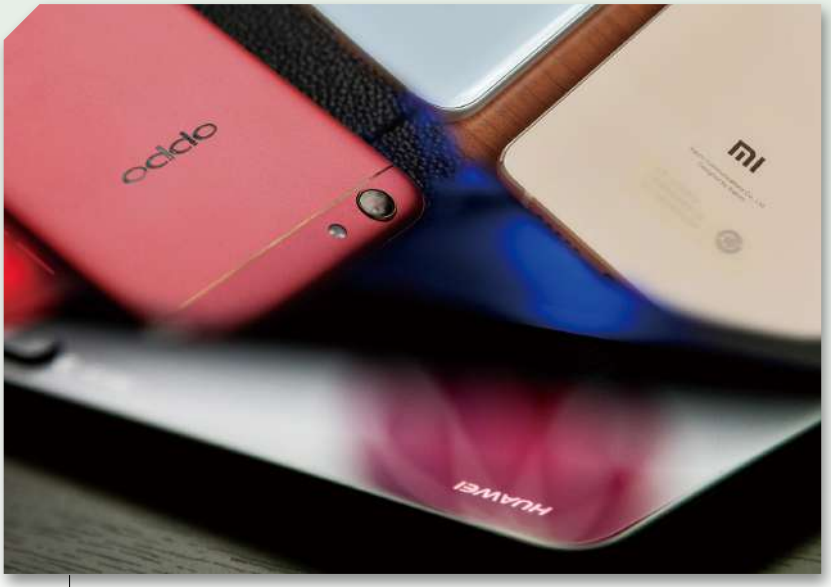
為何政府機關員工不能使用華為手機

很多資安研究者發現，華為手機裡有很多莫名其妙的東西，就是手機隱藏的後門程式，沒觸發時像大海撈針般難以發現。例如房子內如果發現一隻蟑螂，就能推測整棟房屋內應該也有很多蟑螂潛伏其中，但卻很難直接看到蟑螂們出現在屋內的各個角落，手機的後門程式也是如此。

華為手機暗藏後門，然後傳到中共管理者之終端設備。基本上政府不會自找麻煩，儘量不會去限制一般民眾使用華為手機。然為何要禁止我政府機關員工使用華為等陸製手機？因為依據過往之分析經驗，縱使對機關內部使用華為手機的員工進行嚴格的網路管控，這些手機一樣有可能在機關內部裡面收集資料，然後再利用沒有管制的電信網路服務傳送予中共管理者。這就是網路技術的基本特性，應用層可向下多工，利用不同網路層的連線傳送資料，因此，若只管理機關內部之資安設備，還是沒辦法完全防止洩密，所以機關必須嚴格管制員工使用華為手機。而且現在的手機功能非常強大，不管運算能力、儲存空間、網路傳輸速率與各種不同介面，完全可以成為一個分散式資料庫來源，所以要防止洩密，除管制外，很難有其他技術上的辦法更適用。

「陸牌」與「陸製」通訊設備之安全性比較

以國安而言，理論上應禁止使用敵製通訊設備，但因臺灣處境特殊，且資訊戰爭中，戰時和平之定義困難，所以政府處理此問題有相當難度。個人認為，以盤點「陸牌」和「陸製」通訊設備之安全性為優先考量。「陸牌」通訊設備在設計流程開始，能夠加入後門的機會較多，而「陸



「陸牌」通訊設備在設計流程開始，就有很高的機會加入後門，因此「陸牌」的資安威脅遠大於「陸製」。

製」通訊設備則是在製造過程後才有加入後門機會，因此，「陸牌」的資安威脅遠大於「陸製」。

資安防護並不在能杜絕所有安全威脅，亦即世界上沒有絕對安全，也沒有絕對資安，政府應做風險高低的優先順序表，再依可執行的資源配置由上往下嚴格管理。理論上臺灣是面對中共威脅的第一線國家，資安考量應最嚴格，然實際上因臺灣現階段政治局勢，施行較為困難，但至少應該比國際作法更嚴格一點。

人工智慧時代，「資料比錢更有用」

一般民眾在乎的是個人隱私，包括個人行蹤、拍攝的影片及照片，各種應用服務的帳號密碼，尤其銀行的資金往來，甚至自己感興趣的東西，或在網路及社群媒體瀏覽及發言的內容，都不願意讓別人知道；這些連對親屬都要保密的隱私資料，若外洩到國外的資料庫，變成別人茶餘飯後的八卦話題，您不會感到毛骨悚然嗎？

駭客攻擊中有一種稱為「進階持續性威脅」（Advanced Persistent Threat，下稱 APT 攻擊）的手法，就是針對個人或組織所做的複雜且多方位的網路攻擊，潛伏攻擊時間可能長達數週、數月甚至數年，不過，內藏後門的手機比 APT 攻擊更簡單方便，手機上任何資料，都可備份經由後門傳送到遠端，甚至直達敵方的國安單位。

之後，敵方的國安單位不僅知道您是誰、電話號碼、住哪裡、通訊錄內有誰，還可知道您跟他們的關係、長相、和誰吃飯、在手機上聊天內容、傳什麼新聞故事病毒給你最有用等等。人工智慧時代，「資料比錢更有用」，因此，呼籲大家不要貪小便宜，一定要慎選手機品牌。

「乾淨網路計畫」

德國是世界上與中共最友好的西方國家之一，然在西藏抗暴 60 週年之際，原先非常支持西藏的德國，也因受中共經濟誘

惑而有相當大的退讓。惟德國第一電視臺最近在討論華為 5G 問題時，也開始提到其可能讓國家機密被監聽，甚至政府運作遭癱瘓等問題。

坦言之，華為技術還算不錯、也很認真經營，但華為是中共企業，得聽從國家政策指示；而中共又不是民主政體，且其法律早規定企業要配合國家蒐集情報，這就是華為安全性的關鍵所在。

中共 5G 建置帶來的風險，已經引起全球警覺，因此，2020 年 8 月間，美國發起「乾淨網路計畫」（The Clean Network），之後英國、波蘭、澳洲與瑞典等國家也陸續跟進。

面對始終不放棄以武力併吞臺灣的對岸，我們真的不能不小心因應 5G，或使用「陸牌」及「陸製」通訊設備所可能帶來之風險。

2020 年 8 月美國發起「乾淨網路計畫」，英國、波蘭、澳洲與瑞典等國家也陸續跟進，與美國簽署備忘錄，共同抵禦中共 5G 建置帶來的風險。（Source: U.S. Department of State, https://2017-2021.state.gov/the-clean-network/index.html; https://2017-2021.state.gov/the-transatlantic-alliance-goes-clean//index.html）

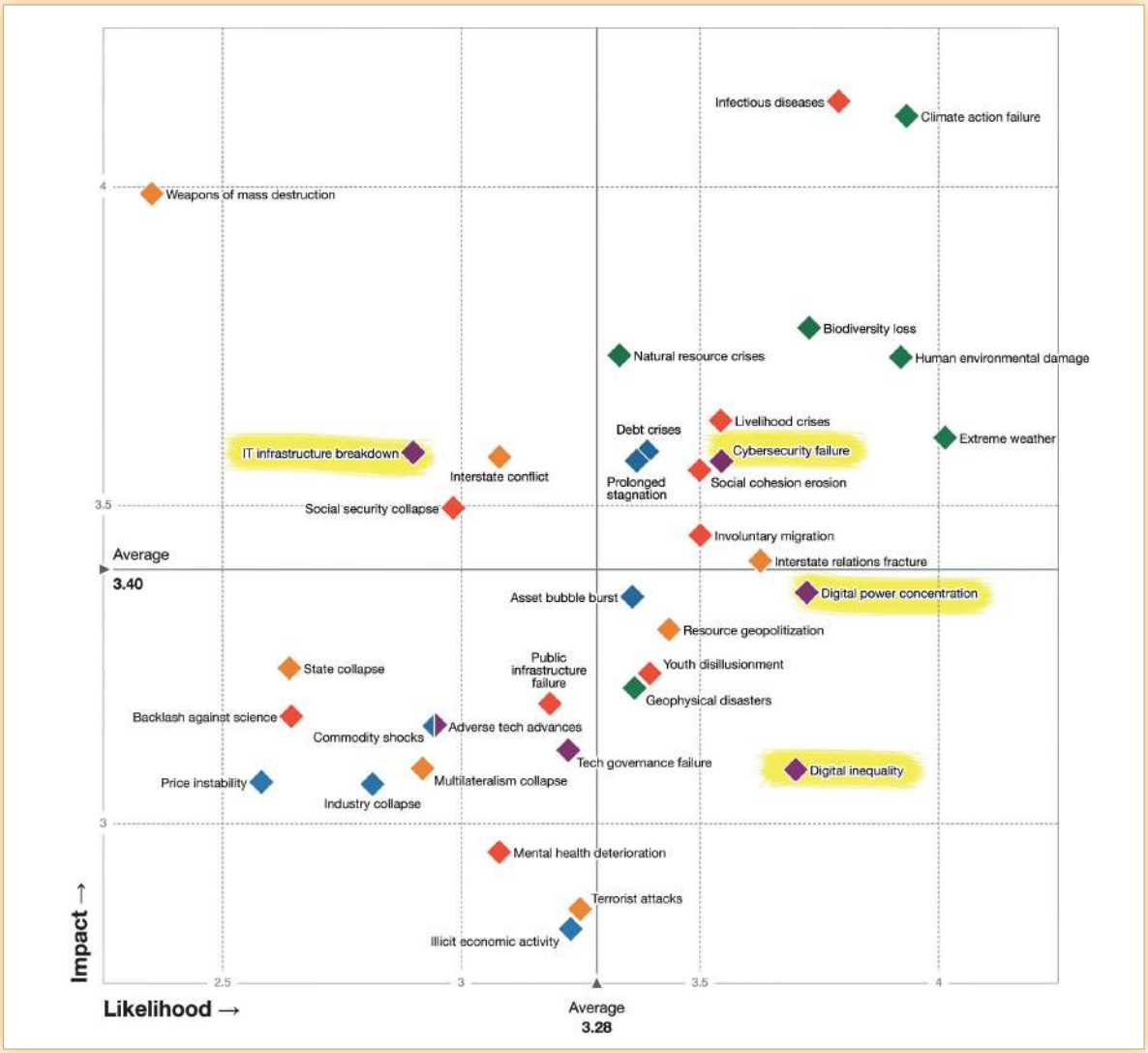
臺灣資安布局——由「布拉格提案」談起

◆ 淡江大學國際事務與戰略研究所博士候選人 — 陳永全

2019 年 5 月，全球 32 個國家齊聚捷克布拉格並公布「布拉格提案（The Prague Proposals）」，這是因應 5G 時代網路安全威脅的首次國際會議。

網路攻擊，已躍升為全球前十大風險

世界經濟論壇（World Economic Forum，下稱 WEF）每年都會發表「全球風險報告」（The Global Risks Report）。過去 15 年來的風險前 5 名都與環境有關。惟根據 WEF 2021 年「全球風險報告」（16 th Edition）顯示（如下圖），「資訊科技基礎設施故障」（IT infrastructure breakdown）已躍升為 2021 年全球風險具影響力的第 10 名；「數位權力集中」（Digital power concentration）、「數位不平等」（Digital inequality）及「網路安全失效」（Cybersecurity failure）則晉升為 2020 年風險加劇的第 6、7 及第 9 名。



2021 年全球風險報告，橫座標由左至右代表風險發生的可能性，愈右側，加劇的可能性愈高；縱座標代表風險發生的影響力大小，愈上方，影響力愈大。紫色菱形為科技類型的風險。（Source: World Economic Forum, The Global Risks Report 2021, 16th dition, http://reports.weforum.org/global-risks-report-2021）

「布拉格提案」超過 30 個國家參與，強調各國於發展 5G 時，應考慮國家安全、經濟、法治與設備商不法行為等因素以及後續的管理問題。（Photo Credit: NUKIB, Czech Republic, https://nukib.cz/en/infoservis-en/conferences/prague-5g-security-conference-2019）

我國與美國於 2020 年 8 月共同發表「臺美 5G 共同宣言」，深化臺灣與美國在 5G 資安上的合作關係。（圖片來源：外交部，https://www.mofa.gov.tw/News_Content.aspx?n=8742dce7a2a28761&s=1baaa18886648d2f）

「布拉格提案」

歐盟、北大西洋公約組織、美、德、日、韓、澳等代表，於 2019 年 5 月齊聚於捷克布拉格，為 5G 安全召開國際會議。會議中強調各國於發展 5G 時，應考慮國家安全、經濟、法治與設備商不法行為等因素，以及後續的管理問題。會議成果經主辦國捷克彙整，成為「布拉格提案」。

「布拉格提案」為首次探討 5G 議題之國際會議，其強調 5G 網路的開發、部署與商業化，必須建立在自由與公平競爭、透明以及法治基礎上，並提出 5G 安全及關鍵基礎設施防護等面向需進行國際交流與合作。參與國期望此提案內容能成為世界各國之資安防護共識。

「臺美 5G 共同宣言」延續「布拉格提案」精神

基於「布拉格提案」精神，我國與美國於 2020 年 8 月共同發表「臺美 5G 共同宣言」（Joint Declaration on 5G Security），臺美雙方宣示承諾在自由、公平競爭、透明及法治的基礎上，對 5G 通訊安全重要性的認知，通過加強對 5G 供應鏈的把關，確保 5G 通訊網路的安全，同時深化臺灣與美國在 5G 資安上的合作關係。

此項臺美 5G 安全共同宣言，代表美國與我國政府均認同 5G 通訊服務安全的重要性，為確保 5G 軟硬體供應商與供應鏈安全，應評估供應商是否可信賴，具體做法包括評估 5G 供應商是否在沒有獨立

司法審查下，受外國政府控制；資金來源是否公開；還有供應商的所有權、管理結構、採購、投資等資訊是否透明；是否尊重智慧財產權等。共同宣言中也倡議透過定期的更新與評鑑，將現有不受信任的軟硬體供應商，移轉為可信賴的供應商，提升雙方的資訊安全，善用 5G 通信網路提供的各項服務，同時確保提供一個更安全、具韌性與可信賴的 5G 行動通訊網路生態系統，並為民間提供創新的機會，在自由公平的環境中，促進數位經濟發展。

他山之石，可以攻錯

蔡總統在 2020 年就職演說中提出 6 大核心戰略產業，其中一項就是「發展結合 5G 時代、數位轉型及國家安全的資安產業」。在「資安即國安」的戰略指導前提下，保持高度的資訊安全意識。在 5G 布設建置過程中，臺灣應竭盡所能，想方設法，完全排除具有資訊安全疑慮的軟硬體設備及相關供應服務。

基此，我國可參考以下先進國家之資安戰略：

一、英國 2016 年 11 月「國家網路安全戰略」（National Cyber Security Strategy 2016 to 2021），內容聚焦網路資安防禦、嚇阻、發展，並期望達成：1. 政府網路及關鍵基礎設施防護、2. 遏制網路犯罪、3. 發展網路安全相關科學研究等目標。

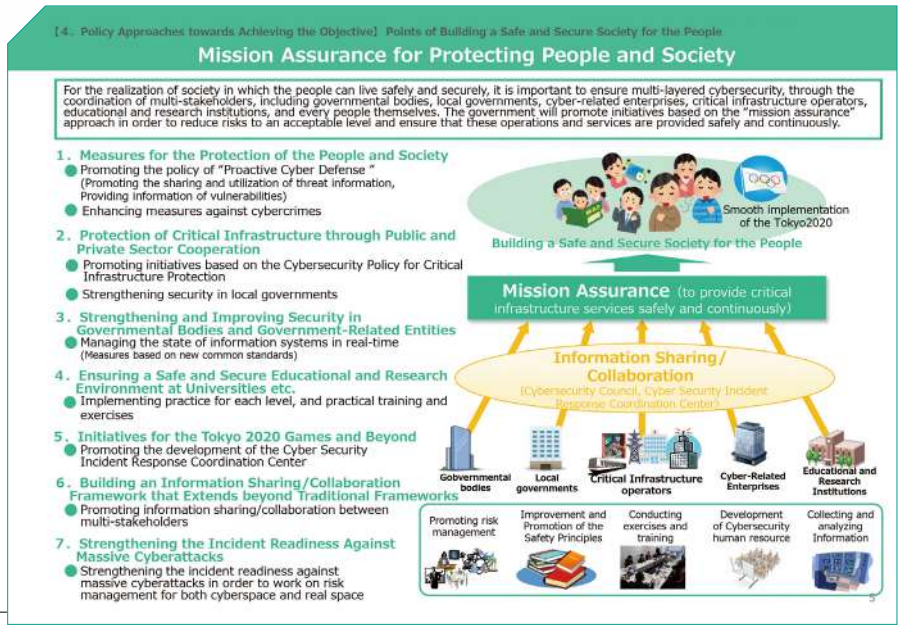
蔡總統在 2020 年就職演說中提出 6 大核心戰略產業，其中一項為「發展結合 5G 時代、數位轉型及國家安全的資安產業」。（圖片來源：國家發展委員會，https://www.ndc.gov.tw/Content_List.aspx?n=9614A7C859796FFA）

二、新加坡 2018 年 3 月「網路安全法」（Cybersecurity ACT 2018 (No.9 of 2018)），置重點於網路空間安全防護，包含關鍵基礎設施安全防護、網路攻擊反制與偵蒐、資訊、網路安全情資共享及建制資安服務供應商之管理機制。

三、日本 2018 年 7 月「網路安全戰略」（Japan's Cybersecurity Strategy），包含以下策略：1. 實現網路安全供應鏈及架構安全物聯網系統。2. 建構大學院校之資訊與網路安全教學研究環境。3. 制定網路犯罪之因應對策。4. 強化政府網路防禦應變、反制網路攻擊與應變大規模網路破壞之能力。

四、美國 2018 年 9 月「國家網路戰略」（National Cyber Strategy），置重點於採取主動防禦作為，保護國家資產

英國 2016 年 11 月「國家網路安全戰略」內容聚焦網路資安防禦、嚇阻及發展。（Source: Ministry of Housing, Communities & Local Government, UK, https://www.local.gov.uk/sites/default/files/documents/Building%20resilience%20together%20-%20William%20Barker,%20MHCLG.pdf）



日本 2018 年 7 月提出「網路安全戰略」，包含架構安全物聯網、制定因應網路犯罪有效策略、強化政府網路防禦應變，並建構大學院校資訊與網路安全教學研究環境。（Source: National center of Incident readiness and Strategy for Cybersecurity, https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-shousaigaiyou-en.pdf）

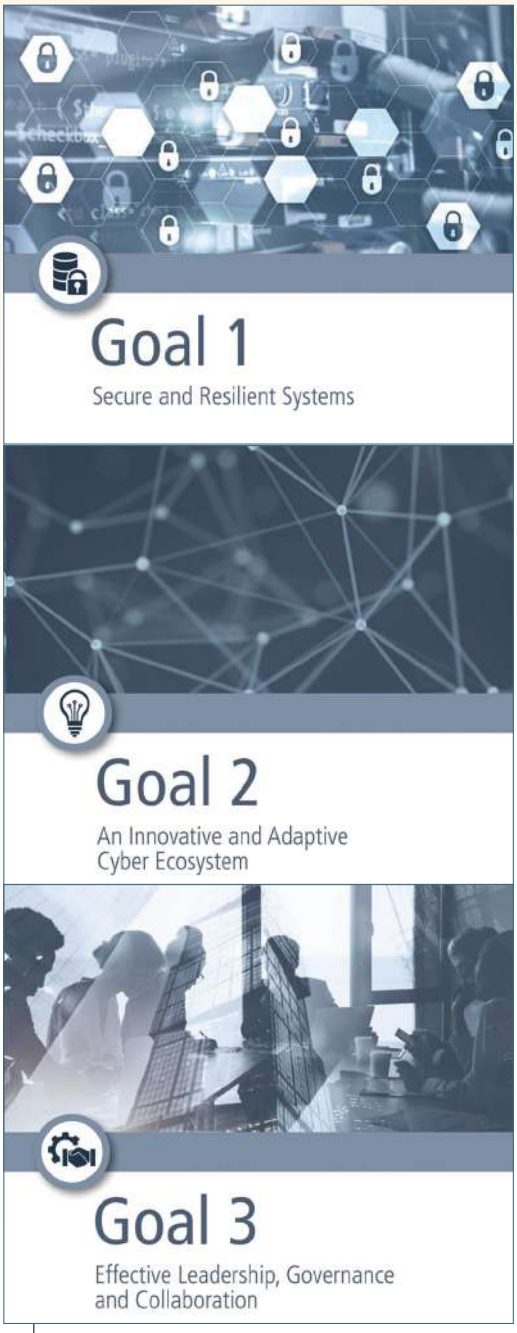
及民眾隱私安全，並提高惡意攻擊破壞者代價。

五、韓國 2019 年 4 月「國家網路安全戰略」（National Cyber Security Strategy），內容重點包括：1. 加強國家關鍵基礎設施安全、2. 提高網路攻擊應變與復原能力、3. 建立具信任的網路治理能力、4. 奠定網路安全環境、5. 培養網路安全文化、6. 領導國際網路安全合作。

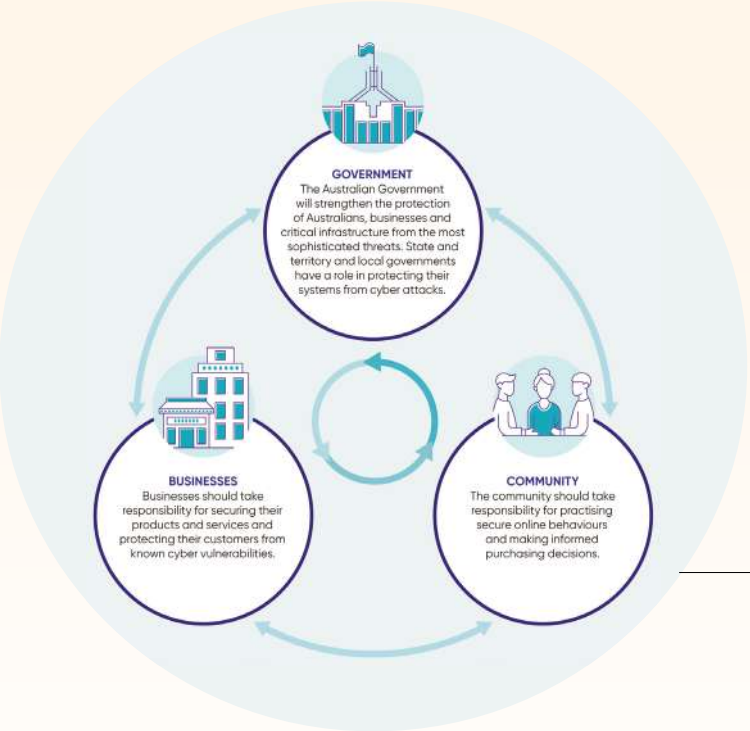
六、加拿大 2019 年 5 月「國家網路安全行動計畫」（National Cyber Security Action Plan 2019-2024），內容有 3 大目標：1. 強化關鍵基礎設施防護並增強網路犯罪偵查能力、2. 支持前瞻研究並協助創新企業發展、3. 國內、地方與民間具體合作，結合國外盟友共同塑造網路防護環境。

七、歐盟 2019 年 6 月「網路安全法」（The European Cybersecurity Act），重點為：1. 強化網路環境治理權限，2. 挹注更多人力與財務資源，3. 建立「歐盟網路安全驗證框架」驗證計畫，4. 評估網路資通訊產品、供應商服務及製程是否符合國際安全規範。

八、澳洲 2020 年 8 月「網路安全戰略」（Australia's Cyber Security Strategy 2020），重點為澳洲政府預計將於 10 年內投資 16.7 億澳幣，投資要項：1. 強化對人民、企業及關鍵基礎設施的具體防護能力，2. 保護企業產品和相關資通訊服務免受威脅或防護弱點的侵害，3. 透過公、私部門通力合作，促進網路安全。



加拿大 2019 年 5 月「國家網路安全行動計畫」包含 3 大目標。（Source: Public Safety Canada, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/ntnl-cbr-scrt-strtg-2019-en.pdf）



澳洲 2020 年 8 月「網路安全戰略」指出，期望透過公、私部門通力合作，促進網路安全。（Source: Department of Home Affairs, Australia, https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf）

綜合上述各國資安戰略，歸納重點：國家應於初始規劃階段，即建置安全的網路環境、建構國家網路資安聯防體系、培養大量優質的資安人才及尋求跨國合作之可信賴供應商等作為，方能超前部署，防範未然。

共同構建綿密的國家資安防護網

我國於 2019 年 1 月正式施行《資通安全管理法》，成為我國首部「資安專法」；調查局旋即於 2020 年 4 月成立「資安工作站」，具體落實了我國資通安全戰略的重要關鍵作為，持續強化網路安全的具體防衛機制，構建綿密的國家資安防護網。

未來更應**在戰略層級規劃**：賡續推動政府網路資安集中共享，擴大國際參與及深化跨國情資分享，制敵機先阻絕境外攻擊，提升科技偵查能量，防制新型網路犯罪。**在政策面向考量**：輔導企業強化數位轉型之資安防護能量提升，強化供應鏈安全管理具體作為，建構智慧國家網路資訊安全環境。**在教育面向推動**：擴增高等教育網路資安師資員額與教學資源，挹注資源投入高等網路資安科研，培育頂尖網路資安實戰及跨域人才。**在執行面向具體**：建立各領域公、私部門協同治理運作機制，增強人員網路資安意識與安全防護能力建構，公、私部門合作深化平、變時情資交流與相關預防、應變、復原演習演練等；建立各層級持續營運能力，及強韌、相依、可靠的網路資通訊安全環境。

備註：本文中 Cyber Security 均翻譯為網路安全，涵括資訊、通訊與網路部分。

智慧城市中的5G運用

◆ 調查局資通安全處 ── 雷喻翔

4G 與 5G 之間的差距，比起前幾代之間的應用鴻溝更為巨大，它幾乎實現了早年人們對於未來世界擘劃的景象。物聯網（Internet of Things, IoT）便是在 5G 技術下所達成的萬物皆可連網的境界，裝置連上網路進行通訊已不再侷限於桌上型電腦、筆記型電腦或是智慧型手機，家庭中的空調、掃地機器人，或是日常馬路上所見的路燈、紅綠燈等都將是物聯網世界參與者。智慧城市（Smart City）是物聯網最重要的應用之一，藉由物聯網的架構，智慧城市將可大幅改善公眾設施的運用、提升公眾設施所帶來的服務品質，而且還得以同時降低日常維運的成本，營造出有效率的政府並提升民眾的生活品質。

以下可由下列 4 個面向討論智慧城市：

智慧個人及家庭空間

雖然蘋果公司及安卓陣營已推出許多的智慧型穿戴式裝置，例如 Apple Watch 或健康手環等，但是其普及率相較於智慧型手機仍有一段距離。隨著 5G 的發展，穿戴式裝置將可預期地逐漸流行，而且不像目前的穿戴式裝置通常是以藍芽與手機搭配使用，在 5G 的環境，它將是獨立的上網個體，裝置可以依據它所感測的身體資訊做出對應的活動建議，並且可以即時地將資料傳送到雲端，讓醫療專家作為保健評估之用，不再需要透過手機當作中轉。

在 5G 的環境中，穿戴式裝置無需透過手機中轉，可直接轉送資料至雲端，讓醫療專家據此為保健評估；而智慧家庭更可讓使用者藉由快捷、安全的遠端監控，對家中家電發出開關、調節等指令。

智慧家庭則將提供一個更為舒適、安全的居住環境，藉由遠端的安全監控，可對家中的任一家電發出開關或調節指令。

智慧公共設施

智慧公共設施可藉由廣布感測器監測城市中公共設施的使用情形，像是路燈、交通號誌、路口監視器等，讓政府有效率地蒐集相關資料，進而做出對應的決策。除了經濟效益之外，智慧公共設施的另一個目的則是在急難發生的當下，讓政府可以在第一時間作為，避免民眾遭遇急難所帶來的損傷及災害。

智慧產業

近年來幾近爆炸式成長的資訊技術（包含大數據、雲端計算、人工智慧及 5G 等），吸引了許多公司極欲在其工廠或辦公環境中導入相關應用，用以提升產能、降低成本、建構友善且具吸引力的工作環境。資訊業或半導體產業無須贅言，傳統產業反倒是最有潛力的受益者。舉例而言，農業便是一個相當適合導入資訊技術的產業之一。原本廣大的農地僅靠人力及機械工具不懈地運作，所能發揮的效益有限，若能布下大量的智慧感測裝置藉以輔助農業開發，在農作物種植採收的過程中，對於農藥、肥料或水資源使用進行監測，不僅事半功倍，且能有效地節省開發成本。

智慧交通

繁忙的都會交通一直都是許多國家頭痛的難解題目，如果車輛及交通號誌也開始變得有智慧了，那會是如何的場景呢？理想的情境將是讓所有的大小車輛規律地遵守交通號誌，減少了不必要的繞路、不必要的塞車，更重要的是自駕車也將帶來

更少的汙染及更舒適的乘車環境。當然智慧交通不可能毫釐無錯地運行，難免會有偶發狀況，但是在車禍發生的當下，智慧交通系統可以立即協調並規劃出救護的路線，即刻排除車禍現場。以上由成千上萬車輛交織而成的複雜場景，若非借助 5G 技術，將很難實現。舉凡像是自駕車煞車所需的緩衝時間或是車輛接收車流量交通訊息的網路覆蓋率等，都需要藉由 5G 的低延遲、高覆蓋率的特性才得以實現。

安全議題

5G 固然便利，但也如雙面刃般面臨更多的資安挑戰。尤其隨著上網的裝置大量地增加，如何在便利的使用 5G 技術之餘仍能保持資安的要求，將是智慧城市的最大挑戰之一。以下簡介兩種 5G 應用於智慧城市可能發生的資安議題。

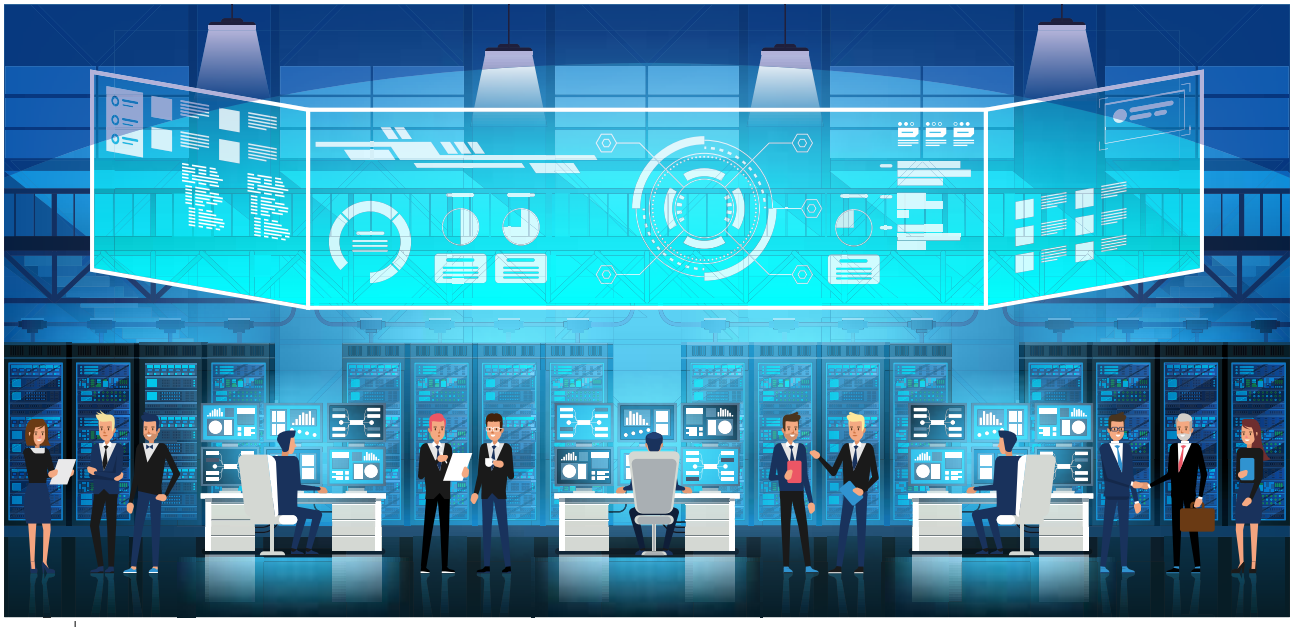
一、分散式阻斷服務（Distributed Denial of Service, DDoS）攻擊

DDoS 並不是一種新興的網路攻擊模式，最早可回溯至 2000 年左右已有網路駭客使用此攻擊手法。由於此手法相對簡單、有效，且成本也不高，故攻擊案例層出不窮。DDoS 是利用大量受控制的電腦同時對目標伺服器發出連線請求，藉此癱瘓目標伺服器原本所能提供的正常服務。無論是網路層的 TCP 協定或是應用層的 HTTP 協定，在開始一個資料連線傳輸之前都需要先配置一部分的系統資源，然而伺服器的系統資源是有限的，一旦被無意義的連線消耗殆盡後，將無法正常使用。

5G 網路由於本身的特性，無線通訊資源也同樣會受到上述 DDoS 的攻擊，智慧城市的物聯網既然是萬物皆可連，可能連路邊馬路上不起眼的灑水器皆可連上網

透過 5G 網路，布下大量智慧感測裝置輔助農業開發，亦可對農藥、肥料或水資源使用進行監測，有效節省開發成本。

借助 5G 技術實現自駕，能讓所有車輛規律地遵守交通號誌，即便發生車禍，智慧交通系統也可立即協調並規劃出救護的路線，順利排除車禍現場。



由於 5G 網路的特性，無線通訊資源也同樣會受到 DDoS 的攻擊，若其中一個監控節點遭到惡意操控，整個網路將不再安全，因此異常行為的監測將是智慧城市極具挑戰的任務。

路，一旦大量的裝置被駭客惡意劫持後，即可透過同時發送網路連線要求進行DDoS攻擊。舉例來說，攻擊若是發生在智慧城市原本運作良好的車輛自駕網路中，若其中一個監控節點遭到惡意操控，整個網路將不再安全且有效率地引導車輛流向，交通安全岌岌可危。

異常行為的監測將是智慧城市正常運作下重要的一環，也是極具挑戰的任務。在某個設施的流量發生異常的當下，若能緊急切斷與該設施的資料傳遞，則能緩解系統遭受癱瘓的可能。

二、自攜電子設備（Bring Your Own Device, BYOD）的衝擊

所謂的自攜電子設備是指在工作的場域中攜帶自身的行動裝置（諸如智慧型手機、筆電或行動裝置等），在經過核准後透過自己的帳號連上工作網路。此種模式在現今新創產業蔚為流行，一方面公司可以降低硬體維運成本，另一方面員工可以更自由地連網工作。但與此同時，公司的敏感資料也將曝露在風險之中。智慧城市的物聯網設備過於多元，某個裝置上運行的作業系統、應用軟體等都不盡相同，且資料流也更為複雜，一旦資料流中的某一個裝置被有心人士遠端利用，機敏的企業資料將面臨洩漏的可能。因此，在 BYOD 盛行之下，安全性的多重認證將變得更加重要。機關必須嚴格落實資料安全性分級，並在對應的認證身分下允許對應的資料流在自攜電子設備中流動。

結論

智慧城市帶來了令人期待的生活遠景，但與此同時，它所帶來的衝擊若無法事前提出有效的因應，那麼事後的修補可能必須付出加倍的代價。

5G 時代的網路安全：以對華為施行禁令的妥適性為例

◆ 中興大學國際政治研究所副教授 ── 譚偉恩

網路安全（cybersecurity）的維護工作在 5G 時代更加不易，因為需要更多的資源、更早的預防、更快的反應、更好的復原。

前言

全球現在除了臺灣與美國之外，很多民主國家都在思考與抉擇是否該禁止中國大陸的華為技術有限公司（下稱華為）參與自己國家關於 5G 的相關基礎建設，禁或不禁之間既有「網路安全」的考量，亦有「政治選邊」的壓力。5G 已被公認是許多國家未來 10 年內在社會與經濟發展上必須要走的方向，它是人類現有文明與通訊科技深度交織的成果。正因為事關重大，不少人認為應該禁止華為的產品，理由是這間公司與威權色彩濃厚的中國共產黨有關，基於合理的懷疑或推論，北京當局極可能利用華為及其研發的相關產品來從事諜報情蒐工作。因此，開放與華為貿易將無異於是自招風險，把網路安全置於中共的虎口之中。

上述對於中共政權的顧慮雖然是合理的，但對華為的禁令是否就是有效維護網路安全之方法？通訊科技在帶給人們更多便利性的同時，也必然增加更多的風險，[1] 從技術層次來說，5G 時代的網路安全需要的是分散與管理這些風險。

[1] Paul Mee and Rico Brandenburg, "Digital Convenience Threatens Cybersecurity," *MIT Solan Management Review* (April 14, 2020), via at: https://sloanreview.mit.edu/article/digital-convenience-threatens-cybersecurity/.

5G 的使用意謂著國家更加依賴行動網路的相關功能，像自動駕駛、遠距教學、視訊醫療、健康即時監測及許多跨時空地理的業務活動，而一旦 5G 網路無法正常運作，損失與損害將難以想像。

5G 的特點及優勢

5G 的使用意謂著一個國家將更加依賴行動網路和它所帶來的相關功能，像是自動駕車、遠距教學、視訊醫療、健康狀況的即時監測，還有許多跨越時空與地理因素限制的業務活動。其結果是，經濟與日常生活的效率變高，但過程中也變得更加脆弱，因為一旦 5G 的網路無法正常運作，損失與損害將難以想像。

當大家都在網路中相互聯繫，也就自然在網路中相互影響。相較於過去的網路只是聚焦在人與人的即時聯繫，5G 進一步讓人可以與許多設備即時聯繫，甚至做到遠端操控。同時，人工智慧的應用讓設備與設備之間也可以相互自動化聯繫，因此是一個史無前例的網路環境。

5G 時代下華為引發的安全疑慮

目前已在進行中的 5G 之爭並非只是幾間科技大廠於全球市場上較量市占率，[2] 而是同時涉及主權國家間（特別是美國與中共）下一個 10 年的權力消長。北京當局近幾年在科技研發這一塊越來越積極，而中國大陸的公司在 5G 相關設備生產上已

[2] 5G 通訊晶片的爭奪戰中，主要都來自國際的晶片大廠，如高通、英特爾、華為、三星等，皆為晶片專利的搶奪競爭者。在通訊網路規範與標準的爭奪戰中，主要則是以 Nokia、Ericsson 和華為 3 大通訊設備供應商（NEP、Network Equipment Provider）為主要競爭者。

是全球舉足輕重的行為者，其中最赫赫有名的供應商就是華為。[3] 文獻指出，高度的人事重疊存在於公部門的國安單位與華為公司。而華為創辦人任正非的背景也一直成為關注的議題，他曾在解放軍工程部門任職，然後以上校軍銜退役，於 43 歲創立華為。他的女兒曾任華為副董事長兼財務長，但在加拿大接受司法調查時被發現持有多年的中國大陸公務護照。[4]

華為引起的爭議不單只是與中共官方的關係，還包括其在共產黨的決策下輸出相關的電子監控設施給不少第三世界威權體制國家。有論者因此認為，中共是在全球推行數位威權主義（digital authoritarianism）。從許多消息來源觀之，華為不像是一般的民間企業，而是北京當局一項很重要的工具，[5] 而 2017 年中共施行《網路安全法》後，這樣的懷疑被更進一步確認，因為《網路安全法》明文要求中國大陸的企業應將資訊交給情資與安全部門進行管理，並遵守相關規定。[6]

至於在政府相關的補助方面，華為收到優惠待遇不單是一般貸款上的便利，還包括來自中共的中國發展銀行和中國進出口銀行給予總金額約 98 億美元的資助。除了上述與中共官方的聯繫外，用戶隱私權和軍民兩用科技的問題也是讓民主國家憂心華為的原因之一，畢竟這些資訊一旦淪為諜報工具，將對使用國造成嚴重的國安威脅。

華為公司的創辦人任正非（上圖）曾在解放軍工程部門任職，他的女兒（左圖）曾任華為副董事長兼財務長，在加拿大接受司法調查時被發現持有多年的中國大陸公務護照。（圖片來源：cellanr, https://www.flickr.com/photos/rorycellan/14101800091；路透社／達志影像）

[3] 中華人民共和國在全球資／通訊科技的價值鏈（the global value chains of information and communications technology, ICT）已是相當具有影響力的行為者，而華為又是之中 5G 設備與基礎建設的領先供應商。由於各國政府都很看重 5G 這一塊市場的前景，所以其實不少國家的相關產業都在一定程度上接受國家的資助，華為是特別受到北京當局支持的科技公司，與中共的國安部門聯繫甚深。參考：Mark Wu, "The "China, Inc." Challenge to Global Trade Governance," *Harvard International Law Journal*, Vol. 57, No. 2 (2016): 261-324; Douglas Black, "Huawei and China: Not Just Business as Usual," *Journal of Political Risk*, Vol. 8, No. 1 (2019), via at: https://www.jpolrisk.com/huawei-and-china-not-just-business-as-usual/; Scott Bicheno, "Huawei is Still the Leader on 5G Commercial Contracts," *Telecoms* (February 20, 2020), via at: https://telecoms.com/502562/huawei-is-still-the-leader-on-5g-commercial-contracts/.

[4] Christopher Balding, "Huawei Technologies Links to Chinese State Security Services"；此外，Huawei's ownership structure is not transparent, raising suspicions of effective party-state control over the company.

[5] Rick Umback, "Huawei and Telefunken: Communications Enterprises and Rising Power Strategies," ASPI Strategic Insights 135. Barton: ASPI, 2019.

[6] 相關資訊可詳見：「《網絡安全法》施行前夕國家互聯網信息辦公室網絡安全協調局負責人答記者」，網址：http://www.cac.gov.cn/2017-05/31/c_1121062481.htm.

上述顧慮讓臺灣和美國成為全球最先對華為採行禁令的國家，避免華為參與自己的 5G 建設，後來有些國家（例如：澳洲和日本）也相繼跟進。由於中國大陸的許多企業很難區分是黨營還是民營，臺灣早在 5 年多前就全面禁止中國大陸製造的通訊零組件進入臺灣的 4G 系統。所以在臺灣的公家機構、關鍵基礎設施，以及任何可能危及國安的地方，都一律禁用中國大陸製造或生產的電信物件（devices）。[7] 相較之下，美國在川普任職總統期間，開始對華為施行禁令，而 2020 年 8 月更進一步限制華為取得美國的通訊設備和軟體，美國商務部同時將 38 家華為的子公司或關係企業列入禁止與美國公司合作的名單中。[8]

有別於臺灣和美國，歐洲國家在禁止華為的立場並不鮮明，甚至還帶著猶疑或不確定性。以英國為例，[9] 首相強生曾表示允許華為有限度地參與英國的 5G 建設，但這個決定引來美國的政治壓力，也同時讓首相面對自身政黨的質疑。隨著〈港版國安法〉生效，英國漸漸調整立場，強調

美國和臺灣為全球最先對華為採行禁令的國家，後來澳洲、日本等國也相繼跟進，圖為 2019 華為在全球的禁用情形。（Source: statista, https://www.statista.com/chart/17528/countries-which-have-banned-huawei-products）

美國商務部在 2020 年 8 月將 38 家華為的子公司或關係企業列入禁止與美國公司合作的名單中。（Photo Credit: U.S. Department of Commerce, https://www.commerce.gov/news/press-releases/2020/08/commerce-department-further-restricts-huawei-access-us-technology-and）

[7] 我國行政院自 2019 年 1 月起即宣布，所屬之中央部會、國營企業、國家研究機構，還有具官股性質的中華電信、中華航空和兆豐金控等公司，全面禁止使用華為所生產的手機和電腦。此外，針對中國大陸籍公司所生產的硬體、軟體、網站，也皆加以禁用。不過，對於非公務以外的民間經濟活動或消費，則沒有禁止。

[8] USDOC, "Commerce Department Further Restricts Huawei Access to U.S. Technology and Adds Another 38 Affiliates to the Entity List," via at: https://www.commerce.gov/news/press-releases/2020/08/commerce-department-further-restricts-huawei-access-us-technology-and.

歐洲國家多半在華為問題上陷入兩難困境，很多電訊業者都和它有業務往來，且歐洲市場也是華為在中國大陸以外成長最快速之區域。（Photo Credit: Matti Blume, https://zh.wikipedia.org/wiki/File:Huawei,_IFA_2018,_Berlin_(P1070188).jpg）

妥善保護國家安全為首要，並在去（2020）年 7 月中旬，英國政府宣布自 2021 年起禁止採購華為的 5G 設備，且要求本土的電信業者在 2027 年以前移除所有的華為設備。（參考英國 2020 年 11 月公布之《電信安全法案》）

英國以外的其他歐洲國家也多半在華為問題上陷入一個兩難困境；一方面在安全事務上已和美國有很長時間的合作，是關係緊密的同盟，雖然川普執政期間，雙邊合作不甚愉快，但終究要比跟北京當局來得好。然而，在另一方面，華為已是 5G 科技的領導者，很多歐洲國家的電訊業者都和它有合作及業務往來；同時，歐洲市場也是華為在中國大陸以外成長最快速之區域。在上述進退維谷的兩難下，持續來自美方的政治壓力，還有歐洲國家本身對於威權共黨體制的憂心，讓它們開始認真思考是否應禁止華為。事實上，歐洲國家的問題也是國際社會很多其他民主國家的問題。

禁止華為或另尋它途？

當具體分析一國的通訊網路會不會因為禁用華為設備，或是斷絕和華為的貿易往來後，就得以避免破壞和癱瘓，便會發現其因果關聯並不若想像中的那般必然。直言之，由於中共的國際形象不佳，世人很容易會擔心華為會透過各種後門程式竊取自己的穩私或國家機密。舉例來說，電信商沃達豐（Vodafone）公司在 2009 年和 2011 年的網路安全報告中，兩次提到華為提供之通訊網路裝置在軟體系統方面有漏洞，可能會導致未經授權的網路惡意攻擊連上 Vodafone 的相關網路系統，導致數百萬家庭和企業用戶的資訊安全受到侵害。又如 2019 年，波蘭官方以間諜罪名逮捕華為在波蘭分公司的員工王偉晶，因為他進行的情蒐工作已危害波蘭的國家安全。[10] 這些事證似乎與許多民主國家對於華為的擔憂相呼應，因此強化了禁用華為的必要性與正當性。然而，美國的微軟

[9] 除了英國以外，不少歐洲國家也陷入抉擇的兩難，以目前市場上的使用情況和普及率來看，歐洲要在短期間內移除華為的通訊設備並不容易。以 2008 年至 2020 年的情況來看，歐洲國家的 4G 建設中有半數以上和華為或中國大陸籍的科技公司有關。因此，在商討是否要禁止中共的 5G 通訊設備進入歐盟國家的市場時，會員國的立場是分歧的。

[10] Bloomberg News, How Huawei Became a Target for Governments, Bloomberg, January 23, 2019.

2019 年，波蘭官方以間諜罪名逮捕華為在波蘭分公司的員工王偉晶，因他進行的情蒐工作已危害到波蘭的國家安全。（圖片來源：截自三立新聞，https://youtu.be/X4tswF_3j48）

（Microsoft）也同樣被發現在程式設計上有類似「後門」的瑕疵。[11] 同時，俄羅斯也曾發現美國政府長期安插於普丁總統身邊的間諜。[12] 顯然，民主國家和與官方無涉的私人性企業並非沒有危害網路安全的可能。

科技總是為人類帶來新的挑戰，5G 在帶來便利性的同時也因為它技術上的創新而讓人們對其依賴性增加，從而提高安全上的風險。首先，由於物聯與互聯而開放之多種網路連接方式，導致受攻擊面明顯增加，讓 5G 的脆弱性變高，資料的控制與取得變得相對容易，但這並非禁止華為及其產品後就不會發生之問題。其次，隨著物聯網的發展，彼此相連的設備數目增加，提升了分散式阻斷服務攻擊（Distributed Denial of Service）的機會。然而，此種攻擊形態的來源國並不只有中共，美國、德國、英國、荷蘭，甚至越南、印度在量上都不亞於中共。[13] 第三，5G 網路著重軟體的特性讓其必須與更多軟體開發和更新程式的業者合作，一旦其中一個環節設定不當或是成為安全防範上的破點時，風險都會升高。最後，在可預期的未來，因為 5G 建設持續發展，一定會有許多問題相繼出現但又缺乏 5G 專業人員來解決，此種科技升級與轉型的過程本來就是必經的脆弱期與調適期。

安全應優於價格

對華為及其產品施行禁令，排除這間中國大陸籍科技公司參與一國的 5G 基礎建設是有憑有據的做法，但並不是有效確保網路安全的策略。事實上，中共如果利用華為或其他法律註冊上並非中國大陸的科技公司來行使情報監控或網路攻擊，民主國家依然會面對網路不安全的風險。有鑑於此，讓本國 5G 市場多樣化，其實

[11] Ellen Nakashima, "NSA Found a Dangerous Microsoft Software Flaw and Alerted the Firm," *Washington Post* (January 15th, 2020), via at: https://www.washingtonpost.com/national-security/nsa-found-a-dangerous-microsoft-software-flaw-and-alerted-the-firm--rather-than-weaponize-it/2020/01/14/f024c926-3679-11ea-bb7b-265f4554af6d_story.html.

[12] "US Spy Worked in Russian President's Office," *France 24* (October 9th, 2019), via at: https://www.france24.com/en/20190910-usa-russia-spy-cia-asset-putin-office-intelligence-elections-extracted-clinton-trump.

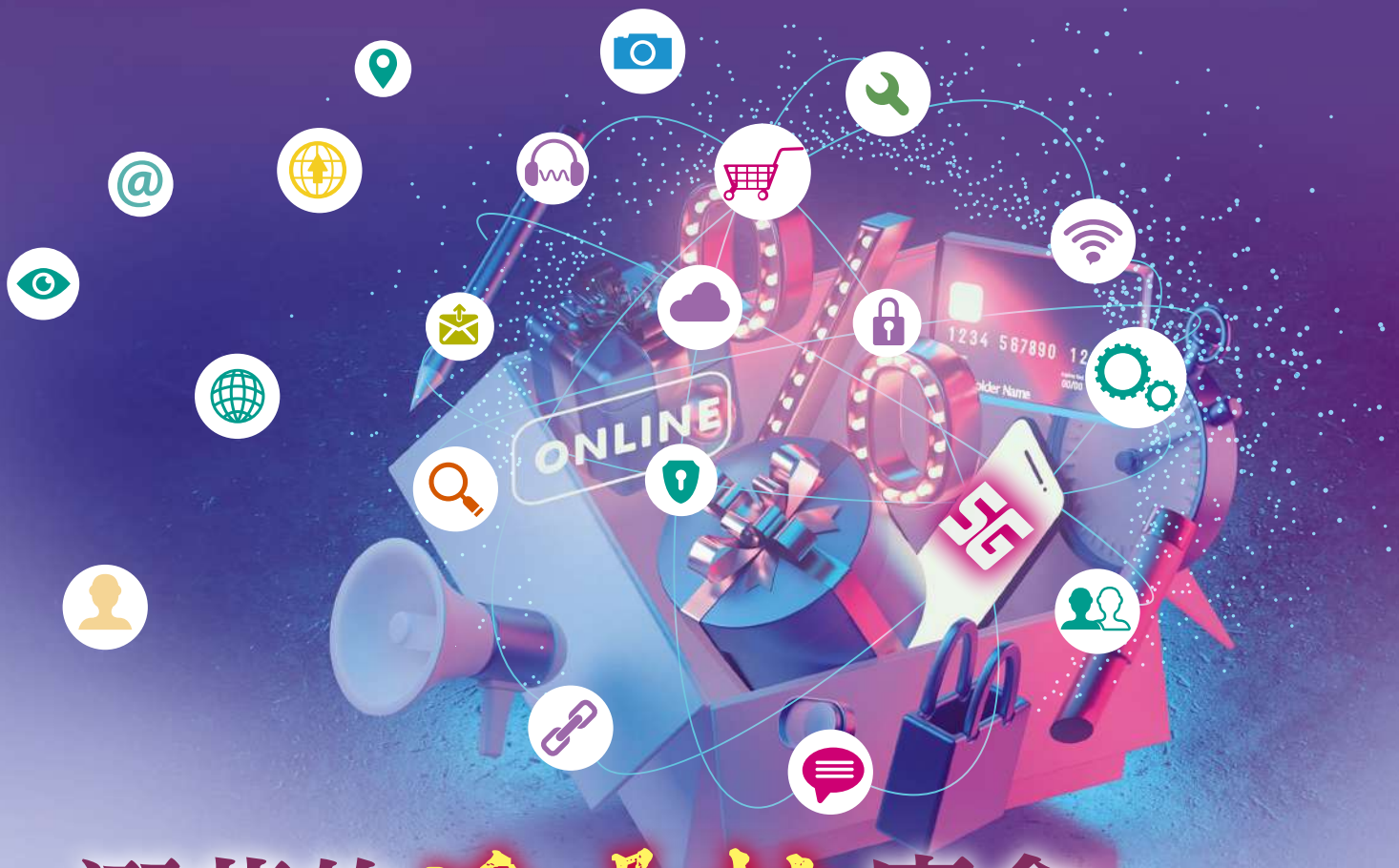
[13] 詳見：Digital Attack Map, via at: https://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=16466.2&view=map.

Ericsson 已在十多國完成 5G 網路的鋪設，而在華為被美國施行禁令後，Qualcomm、Intel 亦成為市場上具有產品競爭力的新手。（Photo Credit: Ericsson, https://www.ericsson.com/en/5g; Linux Foundation, https://www.flickr.com/photos/linuxfoundation/albums/72157680650576335）

也是一種另類的民主化和開放市場的策略應用。**只是開放給業者的資格應以安全品質為最優先的考量，而非價格**。華為之所以有如今通訊科技霸主的地位，是因為從 2015 年開始在全球市占率一直穩居第一，2018 年的 3G 或 4G 設備市占率幾乎已占全球 30%。但當時多數國家並不重視華為與中共的聯繫，只在乎產品的價格，等到開始發現一些可能存在的安全疑慮，還有漸漸受到美國施加的政治壓力時，才考慮是否要對華為施加禁令。

5G 是未來 10 年攸關國家發展的重大項目，相關基礎建設的布局不能只從價格考量。事實上，愛立信（Ericsson）已在十多國完成 5G 網路的鋪設，而高通（Qualcomm）、英特爾（Intel）也都是華為在被美國施行禁令後，浮出市場的新手，但產品的競爭力未必較差，都是民主國家在營造自己 5G 相關環境時可以考慮的合作對象。

民主寶貴的價值之一就是多元，而開放市場讓 5G 服務業者多樣化，彼此維持良性競爭，才是管理 5G 時代網路安全的較佳方法。雖然這個方法不能全然避免網路攻擊或是相關的風險事件出現，但全面禁止華為也同樣無法避免。相較之下，多樣化的管理策略在網路危機發生時可以控制災損，並有替代方法可以即時提供救援。如果一國的經濟與科技水準不差，還可以再配合提升備用設備的儲量、端到端的加密（end-to-end encryption）、以及網路流量的監管等措施來優化自己的網路安全。



潛藏的潘朵拉魔盒

◆ 政風室主任 — 馬維駿

5G 通訊速度將比現況快 10 倍以上，帶來便利也隱藏危機，若惡意運用數位足跡，將在不自覺下引發難以預估的危害，如同「潘朵拉之盒」。

九頭蛇組織已非虛構劇情

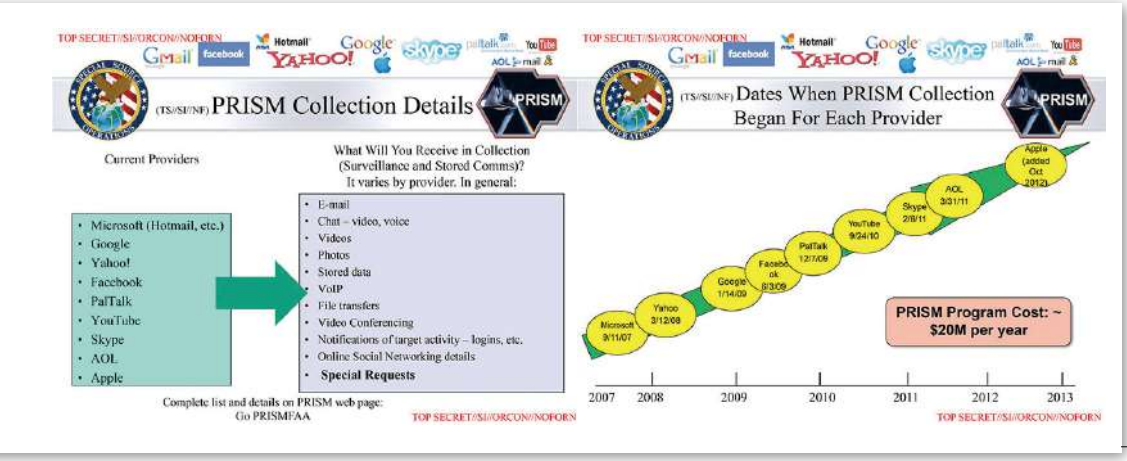
我們如今身處於第三波數位革命時代，正在全面推廣的 5G 網路傳輸技術具有「高速傳輸」、「信號低延遲回應」、「同時連結多樣裝置」等特性，配合更快速的「雲端計算」，遠端操控各項智能產品發揮更大效能，「生活與網路更加密不可分」，然而卻也因為「密不可分的智能產品」，留下更多的訊號傳輸紀錄—「數位足跡」。「數位足跡」具有危險性或機敏性？電影「美國隊長 2 —酷寒戰士」劇情，九頭蛇組織科學家索拉發明「索拉演算法」，將世界視為電子書，透過個人的

電影「美國隊長 2 ─酷寒戰士」中之九頭蛇組織科學家索拉發明「索拉演算法」，將世界視為電子書，透過個人的投票慣性、會考分數、銀行紀錄、病例、通聯紀錄、電子郵件等過去行為模式預測其未來行為。「索拉演算法」已非虛構劇情，而是現在進行式的真實！（Photo Credit: Marvel Studios, Walt Disney Studios Motion Pictures）

投票慣性、會考分數、銀行紀錄、病例、通聯紀錄、電子郵件等過去行為模式預測其未來行為，若該人隱含危害九頭蛇組織的風險，就發動航空母艦將其消滅。然而「索拉演算法」已非虛構劇情，而是現在進行式的真實情境！

著眼國家層次─網路監察蒐集數據作為戰略資源

現實中「索拉演算法」確有其事。閱覽維基百科，美國國家安全局（NSA）外包人員─愛德華·史諾登，在英國《衛報》和美國《華盛頓郵報》揭露 NSA 的「稜鏡計劃（PRISM）」。該計劃網羅眾多資訊公司參與，而參與公司包含「facebook、youtube、apple、skype 等知名企業」。該計畫自 2007 年發動網路監察，受監察之人員標的包括前揭公司的非美國客戶，或是任何與他國人士聯絡的美國公民；受監察之資訊標的包含電子郵件、視訊、語音、影片、相片、社群網路動態等「即時及既存訊息」，並透過操作智能產品攻擊特定目標。依據 2012 年統計，美國有 1,477 個情報工作計劃使用來自該計劃的資料。細思極恐！曾經網路是「保護面具」，如今我們每個人的「數位足跡」卻被未知眼睛窺探，並建構「真實的行為軌跡」及搜尋「可被攻擊的弱點」。



NSA 的「稜鏡計劃（PRISM）」網羅眾多資訊公司，監察電子郵件、視訊、語音、影片、相片、社群網路動態等「即時及既存訊息」，並透過操作智能產品攻擊特定目標。

廠商 Target 之所以比報導中的父親更早知悉女兒有孕，原因在於顧客刷卡消費後，電腦系統將自動記錄顧客的購買資訊，廠商以此建構「分析顧客喜好與需求的資料庫」，從中預測顧客需求，進而推薦商品。

無法察覺的侵略性銷售—運用數位足跡人格側寫，針對行為慣性誘導消費

如何運用「數位足跡資料庫」？不妨參閱 2012 年 2 月 16 日《紐約時報》這篇報導，題為《這些公司是如何知道您的秘密（How Companies Learn Your Secrets）》。某父親氣沖沖地向連鎖店—Target 投訴，質疑該廠商竟然郵寄嬰兒用品和孕婦服裝的優惠券給他尚為高中生的女兒！直到這位父親與女兒溝通後，始知女兒確有身孕。何以廠商比親生父親更早獲得相關訊息？在於每位顧客刷卡消費時都會自動予以識別編號，嗣後電腦系統將自動記錄顧客購買商品、時間等行為訊息，配合其他統計資料，建構一個「用於分析顧客喜好與需求的資料庫」。復以廠商分析人員開發數種預測模型分析前開資料庫，即可預測女孩可能懷孕，進而推薦相關需求商品，即為「關聯規則及預測推薦」技術。

相類技術不僅美國採用，各國企業同樣行之有年，對於企業來說，顧客偏好、生活習慣等相關資訊極具價值，而且這些

顧客偏好、生活習慣等相關資訊欠缺法令保護，經蒐集分析後可對顧客側寫，察覺顧客行為模式並誘導消費，使「數位足跡」成為可轉換成貨幣的資產。

資訊在通常認知非屬隱私，欠缺法令保護，經蒐集分析後，即可對顧客人格進行側寫，策劃相應銷售手段。企業如同獲得預知能力，機先察覺顧客行為模式，誘導消費，準確賺取營業額，「數位足跡」不再是某種指標或參數，而是一種可以轉換成「貨幣」的資產，隱私將因數據預測而被探知，不復存在。

新的壟斷者—掌控「數位足跡」的資本家

「數位足跡」能夠泛起波瀾？確實如此！關注兩岸新聞者，勢必知悉 2020 年的大事，11 月 2 日，中共金融權管機關約談「螞蟻金服集團」實際控制人馬雲等人，翌日由中共領導人直接下令阻止該集團公開募股，官方並於該年 12 月強力介入調整該集團金融商品，在這期間，各種官方媒體發聲，強調「制約壟斷者破壞國安」之正當性。姑且不論是否肇因馬雲言論引發政治打壓，平心而論，渠等創辦「阿里巴巴集團」，透過旗下「淘寶」、「天貓」等購物網累積豐富「顧客資訊」、又推動「支付寶」、「餘額寶」等數位金融商品，配合「花唄」、「借唄」等「借貸 APP」，建構引以為傲的「大數據（數位足跡資料庫）」。

該集團透過「關聯規則及預測推薦」技術誘導民眾過度消費、借貸，累積鉅額債權，再以鉅額債權做抵押向公營行庫取得資金，等同把撼動國家安全的「金融危機」「轉賣」給政府，再企圖以「轉賣金融危機」所得資金炒作股市，其影響不僅加劇貧富差距，更將兩個世代的民眾禁錮於低薪無尊嚴的勞動之下！

借鏡「保護規範原則」權衡資訊蒐集及運用

誠如前言，運用 5G 網路傳輸技術，遠端操作智能產品，有效「縮短時空侷限」，例如遠端醫療系統、遠端數位教學等，可

馬雲控制的阿里巴巴集團串流旗下「淘寶」、「天貓」、「支付寶」、「餘額寶」、「花唄」、「借唄」等金融商品及購物網，建構數位足跡資料庫。（圖片來源：Foundations World Economic Forum, https://www.flickr.com/photos/49344088@N04/39008130265；Leon Lee, https://www.flickr.com/photos/leondel/albums/72157594567186859；中新社／達志影像）

以拉近城鄉差距；全區域地理生態監控、全系統即時交通安全管制等，全面提高管理效能；然而，各機構從中獲得蒐集「數位足跡」作為背景資料使用，勢必無法阻擋。不論是國際戰略判斷或犯罪防治人格側寫，甚或民間企業的「關聯規則及預測推薦」銷售技術，對於「數位足跡」蒐集只會越加依賴、更為全面。

曾經「科技始終來自於人性」，現今「人性受科技刺激而改變」，吾輩究應如何看待這「潘朵拉魔盒」？管見以為：一、善用資安專才，研發核心技術以因應，誠屬必要。二、科技發展迅捷，則成文法恐有不及，或可運用司法判例及行政裁定之彈性，與時俱進，先行框列「資訊蒐集及運用範疇」。三、框列「資訊蒐集及運用範疇」，應受「保護規範原則」檢視、權衡，務求符合「立法意旨所保護價值」，更係維護「人性價值」的具體彰顯。

美國對承包商之網路安全認證

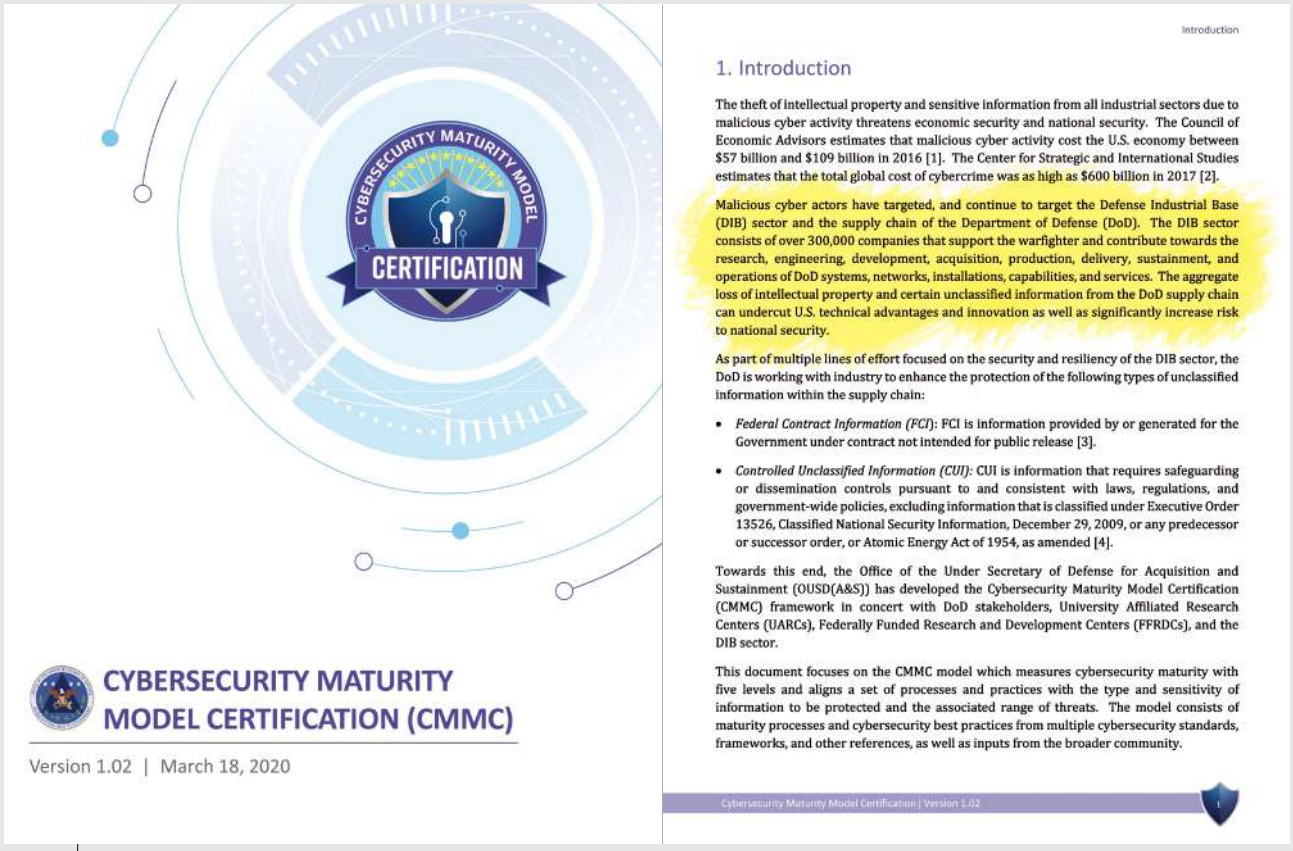
◆ 實踐大學副教授 — 蔡裕明

美國國防部於 2020 年 2 月宣布，要求競標國防部合約的承包商，需符合《網路安全成熟度認證》（Cybersecurity Maturity Model Certification, CMMC）資格，且每 3 年需更新一次認證。未來，廠商必須取得不同等級之安全驗證，才能承包美國國防部的業務。

CMMC 介紹

CMMC 是美國國防部正在實施於規範國防工業基礎（defense industrial base, DIB）網路安全工作之標準。認證主要目的是在評估國防部承包商在網路安全領域的能力，適用於與國防部有直接接觸的主要承包商、執行合約的分包商和外國供應商。這將涵蓋國防部 30 萬家承包商。

由於美國每年平均因網路安全損失超過 6 千億美金，且執行國防部合約的分包商通常都是小型企業，大部分沒有完善的網路安全措施；且對駭客而言，攻擊第二線承包商比攻擊第一線的更具吸引力。由於承包商數量極多且計畫相當艱鉅，國防部要求由第三方評估組織來執行 CMMC 認證，國防部並會對該評估組織進行認證。



《網路安全成熟度認證》（Cybersecurity Maturity Model Certification, CMMC）主要目的是在評估國防部承包商在網路安全領域的能力。（Source: Office of the Under Secretary of Defense for Acquisition & Sustainment, https://www.acq.osd.mil/cmmc/draft.html）

CMMC 的認證級別

CMMC 有 5 項認證級別，各項級別彼此相依，即每項級別需遵守較低級別之規定，以驗證對網絡安全標準的遵守情況；另承包商須通過較低級別後，才能升級到下個級別。包括：[1]

級別 1：基礎防護（Basic）—保護「聯邦合同資訊」（Federal Contract Information，下稱 FCI）。例如公司必須使用防毒軟體或確保員工定期更改密碼，以保護 FCI。

級別 2：中等防護（Intermediate）—保護「受控非機敏資訊」（Controlled Unclassified Information，下稱 CUI）。CUI 為美國法規要求保護或傳播措施之任何資訊，但不包含機密資訊。例如，承包商需通過美國商務部國家標準技術研究院的 NIST 800-171，來保護 CUI。

[1] Abigail Stokes, M. C. (2020). The cybersecurity maturity model certification explained: What defense contractors need to know. CSO (Online), Retrieved from https://search.proquest.com/docview/2387511629?accountid=13838.

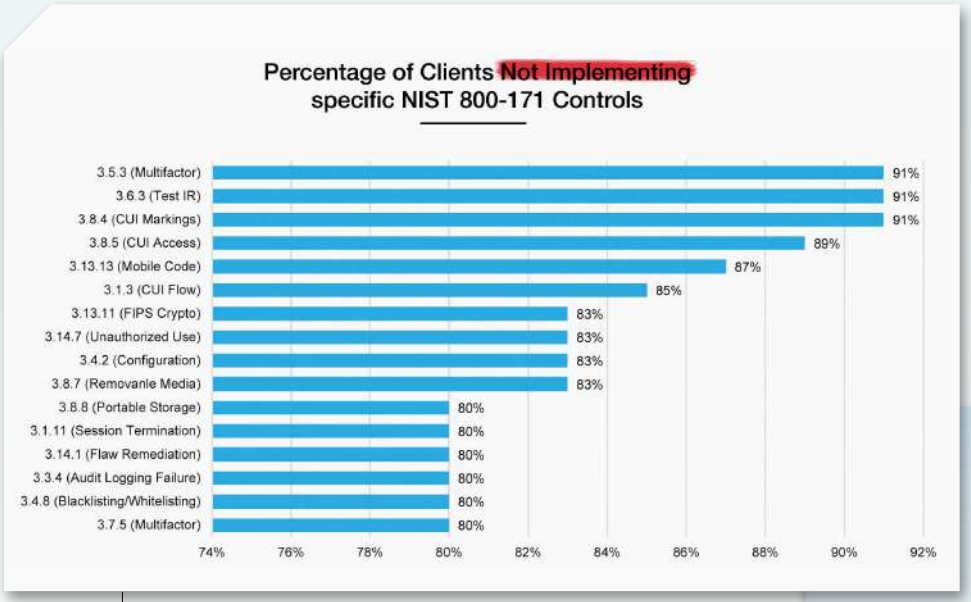
級別 3：良好防護（Good）—增加 CUI 之保護。公司必須制定制度化的管理計劃，以保護 CUI，包括所有 NIST 800-171 r2 安全要求以及附加標準。

級別 4：主動防護（Proactive）—能防範「進階持續性威脅」（advanced persistent threats，下稱 APT）。APT 被定義為具有先進水平的專業知識和大量資源的對手，對手會使用多種媒介攻擊。公司必須實施審查與評估有效性之流程，並且建立其他強化作法，可以檢測並回應不斷變化的策略、技術和程序以及持續性的先進威脅。

級別 5：進階防護（Advanced）—具備檢測和回應 APT 攻擊之優化流程。公司必須在整個組織中採用標準化和優化的流程，以及其他強化資訊安全作法，以能夠回應 APT 攻擊等更為複雜的功能。

美國國防部強調，CMMC 為改變國防單位承包商內部網路安全文化（cyber-security culture）的開始，並需要對於不斷發展的威脅進行準備，而非僅是獲得 CMMC 的認證。國防部門的承包單位除要獲得 CMMC 的認證外，還得在組織內培養靈活性的網路安全文化，以確保在市場上獲得更佳競爭力。

圖 1　CMMC 的 5 項認證級別



美國網絡風險管理公司 Sera-Brynn 在 2019 年報告提及，國防部許多承包商未實施控制措施來保護國防部在網路上的機敏情報。（Source: DEFENSE TECHNICAL INFORMATION CENTER, https://ndia.dtic.mil/2020/2020manufacturing.html）

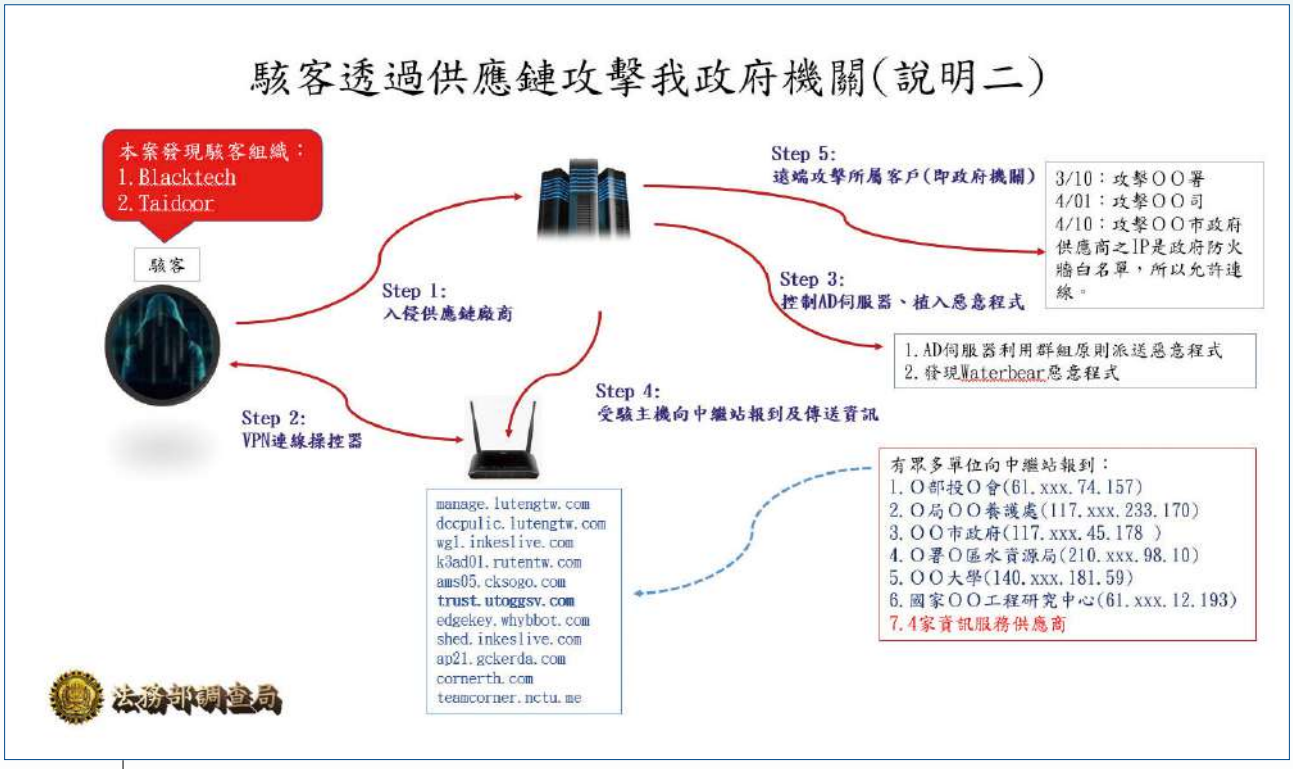
美國國防部負責採購的副部長洛德（Ellen Lord）表示，國防部注意到認證成本對於中小企業可能成為沉重的負擔，所以國防部將對小型承包商提供培訓機會，未來再擴及中型與大型國防承包商。

美國建置 CMMC 之必要性

美國網絡風險管理公司 Sera-Brynn 在 2019 年報告提及，國防部許多承包商未使用多重要素驗證（Multi-factor authentication）、通過事故應變測試等控制措施，以及僱用未經訓練的員工，或運作較差的修補程式管理（patch management），來保護國防部在網路上的機敏情報。

2018 年 6 月美國海軍承包商遭駭客入侵，導致飛彈研發之機密細節外洩。（此照片為示意圖，非當事潛艦）

此外，近年美國許多機構歷經多次網路入侵，從美國五角大廈到國土安全部，駭客甚至進入「氣隙網路」（air-gap network）機密系統或關鍵基礎設施的工業控制系統（Industrial control system, ICS）等。例如：2018 年 6 月美國海軍承包商遭駭客入侵，致美國潛艦所使用的超音速反艦飛彈之研發細節外洩。2018 年 10 月，駭客入侵外包商系統，借道進入國防部網路，導致 3 萬名員工的差旅資料外洩等事件。這些事件讓美國國防部意識到，不僅



去年 8 月調查局發現政府部門及其資訊服務供應商有遭滲透之問題。（圖片來源：法務部調查局）

需要慎選國防部門的承包商，也應同時注意這些公司僱用的二級和三級分包商。

他山之石　可供借鏡

我國曾於前（2019）年破獲新北市某間工程公司利用承包國防工程機會刺探機密，去（2020）年 8 月調查局新聞發布，發現政府部門及其資訊服務供應商有遭滲透之問題。是以，我國現階段應盤點國防部門之網路承包商，並要求或輔導其等符合國際相關網路安全規範與程序，亦可要求承包商定期報告遭受網路威脅與攻擊狀況，或仿效美國國防部所提出之 CMMC 網路安全認證標準，要求國防部門的承包商注意其網路安全與加強人員培訓，並防範承包商內部可能的「內賊」問題。

現今全球正戮力抵抗新冠肺炎之際，駭客也將攻擊重點轉向醫療院所或疫苗等研究機構。未來我國除應持續關注國防單位承包商的網路安全能力外，更需要留意駭客針對醫療院所或疫苗研發單位承包商之可能攻擊或竊取資料等行動。

美國會大廈暴動 赤裸揭露極右翼之國安威脅

◆ 調查局專門委員 ── 陳能鏡

一場暴動，摧毀美國民主基石與傳統價值，更揭露極右翼激進主義正帶來直接且立即之國安威脅。

（Photo Credit: The deadly Capitol Hill riots, https://www.flickr.com/photos/30478819@N08/50818647218）

美國國會大廈暴動案定調為恐怖攻擊事件

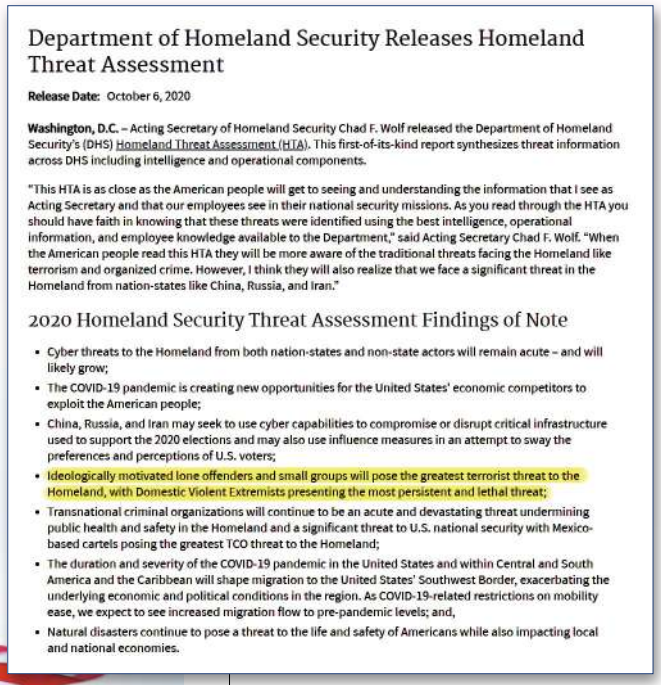
1 月 6 日在美國前總統川普、前紐約市長朱利安尼等人鼓動下，上千川迷攻占美國國會，中斷總統大選結果認證程序，破壞設施機具，甚至有人偷走眾院議長手提電腦，企圖轉賣俄羅斯情報機關等。事後經美國執法機關調查發現，極右激進民兵團體、陰謀論網路運動，如布加洛（Boogaloo Bois）、驕傲男孩（Proud Boys）、匿名者（Qanon）等團體高度介入本案，隨即定調為恐攻案，並擴大偵辦。

美國國土安全部於去（2020）年 10 月發布的年度「國土安全威脅評估」報告指出，內部暴力激進主義者正帶給美國國土安全最持續、最致命的威脅。此次國會恐攻案只是更赤裸揭露，極右恐怖主義不但澈底摧毀民主價值，更已帶給國家安全直接且立即的威脅。

川普的部分支持者認為美國大選不公，於是闖入美國國會，中斷國會認證總統大選結果的程序，試圖反轉選舉結果。（Photo Credit: Tyler Merbler, https://www.flickr.com/photos/37527185@N05/50821278936）

極右恐怖主義在歐美威脅日增

恐攻死亡人數自 2014 年起，已連續 5 年呈下降趨勢，但西歐、北美、紐西蘭與澳洲等西方民主國家，極右翼恐攻案件數



Department of Homeland Security Releases Homeland Threat Assessment

Release Date: October 6, 2020

Washington, D.C. – Acting Secretary of Homeland Security Chad F. Wolf released the Department of Homeland Security's (DHS) Homeland Threat Assessment (HTA). This first-of-its-kind report synthesizes threat information across DHS including intelligence and operational components.

"This HTA is as close as the American people will get to seeing and understanding the information that I see as Acting Secretary and that our employees see in their national security missions. As you read through the HTA you should have faith in knowing that these threats were identified using the best intelligence, operational information, and employee knowledge available to the Department," said Acting Secretary Chad F. Wolf. "When the American people read this HTA they will be more aware of the traditional threats facing the Homeland like terrorism and organized crime. However, I think they will also realize that we face a significant threat in the Homeland from nation-states like China, Russia, and Iran."

2020 Homeland Security Threat Assessment Findings of Note

- Cyber threats to the Homeland from both nation-states and non-state actors will remain acute – and will likely grow;
- The COVID-19 pandemic is creating new opportunities for the United States' economic competitors to exploit the American people;
- China, Russia, and Iran may seek to use cyber capabilities to compromise or disrupt critical infrastructure used to support the 2020 elections and may also use influence measures in an attempt to sway the preferences and perceptions of U.S. voters;
- Ideologically motivated lone offenders and small groups will pose the greatest terrorist threat to the Homeland, with Domestic Violent Extremists presenting the most persistent and lethal threat;
- Transnational criminal organizations will continue to be an acute and devastating threat undermining public health and safety in the Homeland and a significant threat to U.S. national security with Mexico-based cartels posing the greatest TCO threat to the Homeland;
- The duration and severity of the COVID-19 pandemic in the United States and within Central and South America and the Caribbean will shape migration to the United States' Southwest Border, exacerbating the underlying economic and political conditions in the region. As COVID-19-related restrictions on mobility ease, we expect to see increased migration flow to pre-pandemic levels; and,
- Natural disasters continue to pose a threat to the life and safety of Americans while also impacting local and national economies.

美國國土安全部於 2020 年 10 月發布的「國土安全威脅評估」，報告中提到具意識形態的犯罪者和小團體最可能對本土構成恐怖威脅，而國內暴力極端分子則是最持久和致命的威脅。（Source: U.S Department of Homeland Security, https://www.dhs.gov/news/2020/10/06/department-homeland-security-releases-homeland-threat-assessment）

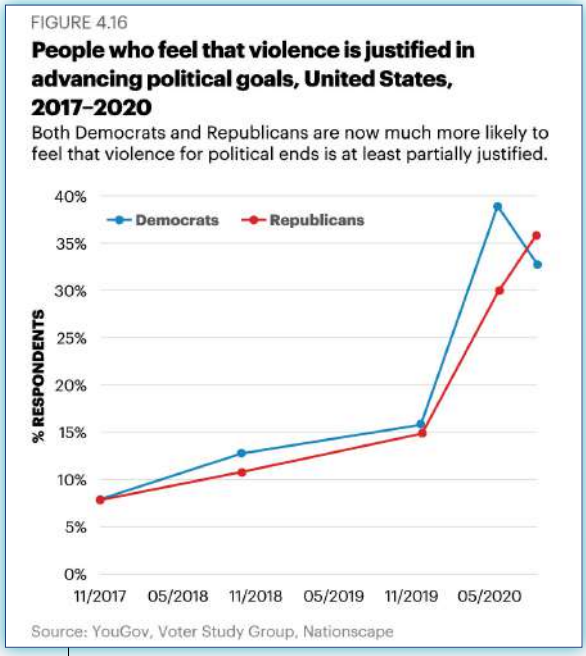
及死亡人數反現成長趨勢，右翼恐怖主義威脅是否高於伊斯蘭聖戰主義威脅，近年來已成熱門討論議題。

依據「經濟與和平研究所」（Institute for Economic & Peace）統計資料，自 2002 至 2019 年，全球死於恐攻案人數為 23 萬 6,422 人，其中 1,215 人死於發生在西方國家之恐攻案，僅占 0.51%；這 1,215 人中，814 人死於聖戰恐攻案，286 人死於極右翼恐攻案，其餘則死於民族自決、分離主義、環保、動保、極左翼等恐攻案。

另 2019 年西方國家所發生的恐攻案，63% 為極右或極左恐攻案，其所造成的死亡人數占死亡總數的 90%，其中右翼恐攻案共 49 件，其造成死亡人數占比為 82%。前述統計數字說明，極右翼恐怖主義對西方國家之威脅已超過伊斯蘭激進主義。

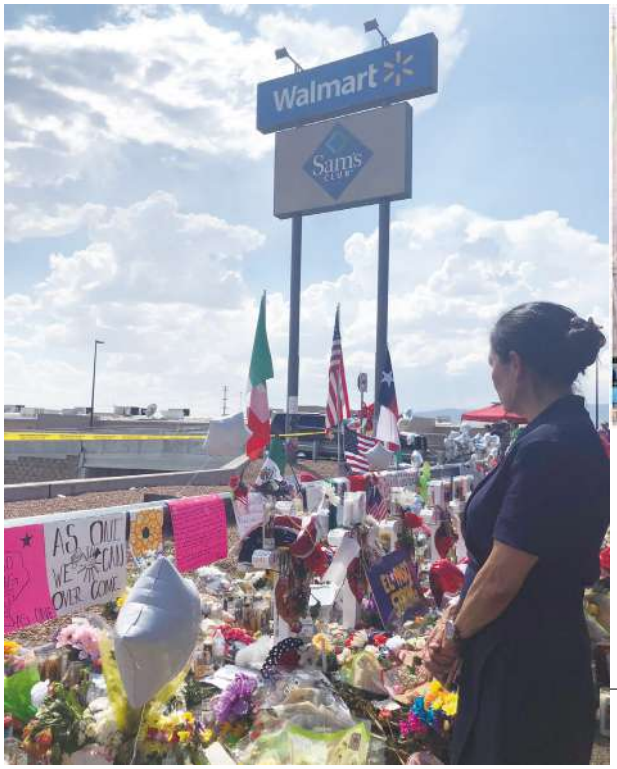
美國政客對以暴力行為來達成政治目的之接受度提高

美國近年由於資源分配不均、政府治理不彰、資訊流通不自由、他人權利不尊重、貪瀆盛行等負面因素，讓美國政治氣候發生重大變化：政治對立加深、政治暴力加劇，甚至政治人物對以暴力行為來達成渠等政治目的之接受度提高。民調顯示，共和及民主 2 黨對於以政治為最終目的之暴力接受度，在 2019 年 11 月底均約為 15%，而至 2020 年 9 月止，民主黨已達 33%，共和黨更高達 36%。

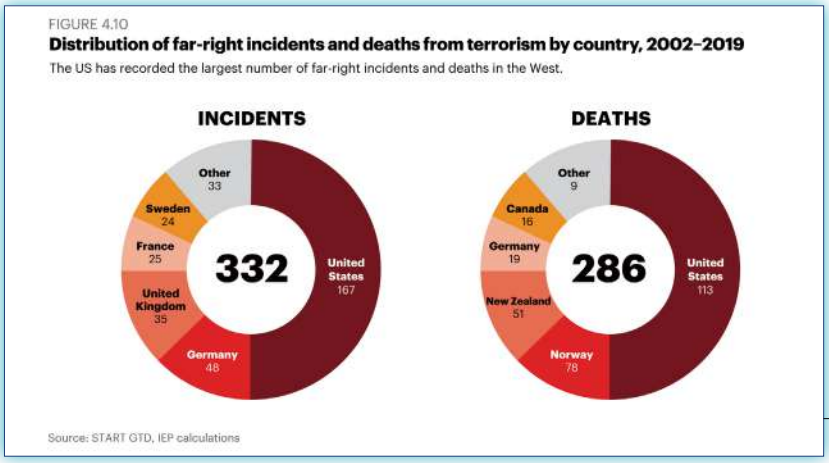


民調顯示，共和及民主 2 黨對於以政治為最終目的之暴力接受度整體提高。（Source: Institute for Economics & Peace, GLOBAL TERRORISM INDEX 2020, https://www.visionofhumanity.org/resources）

近年來激進分子增加並以強硬的暴力手段表達訴求，導致無辜民眾傷亡。圖為 2018 年匹茲堡猶太教堂槍擊案地點，槍手為白人至上主義，此事件造成 11 人罹難，6 人受傷。（Photo Credit: David Fulmer, https://www.flickr.com/photos/daveynin/45013855725）



2019 年 8 月發生在德州埃爾帕索 Walmart 賣場的槍擊案，美國司法部定調為本土恐怖攻擊。該案導致至少 20 人死亡，數十人受傷。（Photo Credit: Walmart Video Surveillance Camera, https://en.wikipedia.org/wiki/File:Patrick_Crusius_Video_Surveillance_Shooting.png; Deb Haaland, https://twitter.com/RepDebHaaland/status/1159227783513612291）



自 2002 至 2019 年，美國是西方國家中遭遇極右翼恐攻案件數及人民死亡數最高的國家，占比分別為 50% 及 40%。（Source: Institute for Economics & Peace, GLOBAL TERRORISM INDEX 2020, https://www.visionofhumanity.org/resources）

當黨政人物不排斥暴力，甚至縱容激進分子以暴力手段表達訴求或不滿時，恐攻事件將層出不窮。例如 2018 年 10 月賓州匹茲堡生命之樹猶太會堂槍擊案、2019 年 4 月加州聖地牙哥猶太會堂槍擊案、2019 年 8 月德州艾爾帕索賣場槍擊案、2020 年 10 月密西根州長惠特曼刺殺未遂案，以及 2021 年 1 月國會大廈暴動案等等。

根據「經濟與和平研究所」資料，自 2002 至 2019 年，美國是西方國家中遭遇極右翼恐攻案件數及人民死亡數最高的國家，占比分別為 50%（167/332）及 40%（113/286），在國會大廈暴動案後，更重創其國際形象，美國絕對是極右翼恐怖主義的最大受害國。

布加洛是近年來被公認為最危險的反政府、反威權暴力團體，其服裝特徵為夏威夷襯衫和軍服，以武裝推翻政府及主張擁有槍權是其兩大基本信念。（Photo Credit: Becker1999, https://www.flickr.com/photos/becker271/50284558387）

驕傲男孩是一個支持法西斯主義的右翼組織，成員基本為男性，組織宗旨為無政府、反毒品、反戰爭、反移民、反種族主義等，因為川普在總統辯論會上的認證，將此視為川普對他們的認同與激勵。（Photo Credit: Anthony Crider, https://www.flickr.com/photos/acrider/50658866101）

美國極右翼恐怖組織簡介

國會大廈暴動案後，美國執法機關盡全力追緝涉案者，發現民兵團體、陰謀論運動等極右組織為排名第二的重大罪犯，僅次於總統川普。依據知名民權團體「南方貧窮法律中心」（Southern Poverty Law Center）資料顯示，現今全美各地民兵團體超過 180 個，他們雖各有各的理念，然共同特色都是反政府組織，尤其是反對聯邦政府的槍枝管制，雖不宣揚暴力，但經常全副武裝，甚至參與暴力示威，包括美國總統大選後的 MAGA（讓美國再次偉大）示威活動。現簡單介紹其中 3 大罪犯。

一、布加洛

於歐巴馬就任總統後成立，公認為最危險的新興反政府民兵團體，美國司法部形容其是個鬆散的個人連結團體，成員們大都懷有暴力反政府情緒。人權團體「反毀謗聯盟」（Anti-Defamation League）指出，布加洛本質上就是反政府、反威權及反警察，武裝推翻政府及堅決主張擁槍權是其兩大基本信念。自 2019 年起，參與過擁槍權、反疫情封鎖、黑人的命也是命等示威活動。部分成員甚至仿效伊斯蘭激進武裝分子「mujahideen」（意謂自由戰士），自稱為「boojahideen」，利用抗議從事反公權力之武裝活動。2020 年 7 月 3 名成員企圖引發暴力示威，在內華達州以恐怖主義罪被起訴；2020 年 12 月司法部發布新聞稿，指布加洛成員共謀提供巴勒斯坦恐怖組織「哈馬斯」（Hamas）物資，並已認罪。美國總統大選後，布加洛線上論壇平臺「自由之樹」（Tree of Liberty）

匿名者 Q 屬極右翼陰謀論網路運動，其認為美國政府內部存在一個反對川普的深層政府，以擁護川普為目標，他們散布假訊息吸引民眾認同。（Photo Credit: Elvert Barnes, https://www.flickr.com/photos/perspective/50693880817; Anthony Crider, https://www.flickr.com/photos/acrider/49416341132）

貼文，號召支持者於 1 月 17 日在國會大廈及全美 50 個州州議會集結並武裝抗議，企圖阻止拜登就任總統。

二、驕傲男孩

於 2016 年由加拿大裔英國右翼分子 Gavin Mclnnes 主導成立，成員以西方沙文主義為傲。驕傲男孩是反移民的白人男性極右團體，「南方貧窮法律中心」稱其是仇恨團體，過去即有街頭暴力對抗左翼的歷史，特別是「反法西斯主義運動」（antifa），2 名成員因在紐約毆打反法西斯運動人士於 2019 年被判有罪並入獄服刑。2020 年 9 月 29 日的首場總統電視辯論會上，主持人問到是否譴責到處製造動亂的白人至上主義時，針對拜登點名驕傲男孩，川普公然答稱：「驕傲男孩，後退待命」。川普的認證激勵，讓驕傲男孩無役不與，當然包括國會大廈暴動案。

三、匿名者 Q

屬極右翼陰謀論網路運動，沒有真正的領導人，2017 年 10 月首度在美國出現，其聲稱美國政府內部有一個「深層國家」（deep state），由民主黨的歐巴馬、希拉蕊等政治人物夥同比爾蓋茲等社會精英組成的撒旦集團來領導，密謀向川普展開鬥爭，川普則是救世主。該組織以刻意製造的謠言（disinformation）或假訊息（misinformation）來吸引信徒，不但已全面滲透進入美國民眾日常，更藉新冠疫情而蔓延全球，其信徒或支持者已涉及多起暴力事件。2019 年美國聯邦調查局將其列為「國內恐怖主義潛在威脅」，西點軍校

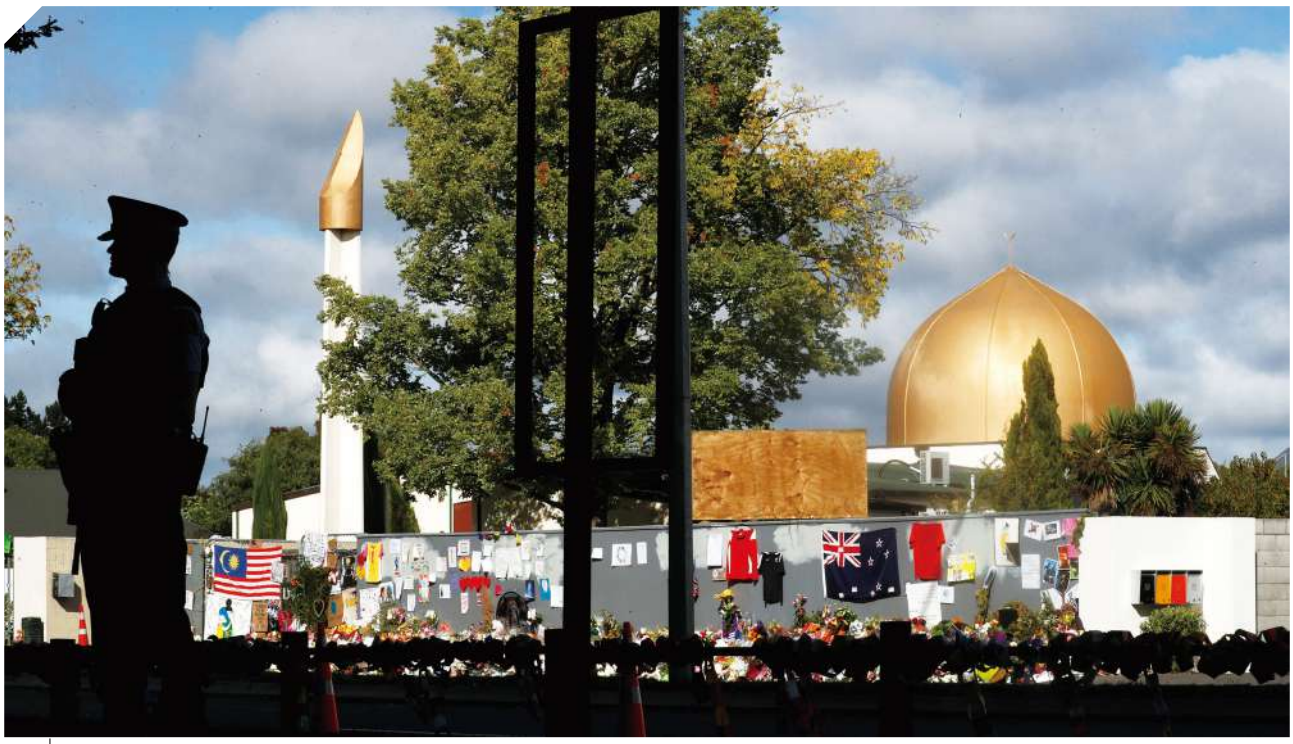
打擊恐怖主義中心亦形容其為「公共安全的全新挑戰」。在 2020 年 8 月白宮記者會中，當記者提到匿名者 Q 時，川普如是說：「我對這個運動不是很了解，只知道他們非常喜歡我，我很感激，而且他們還是愛這個國家的人民」。有了「愛國者」的加持，匿名者 Q 當然勇於衝鋒陷陣，攻占國會大廈。

極右翼恐怖主義特性

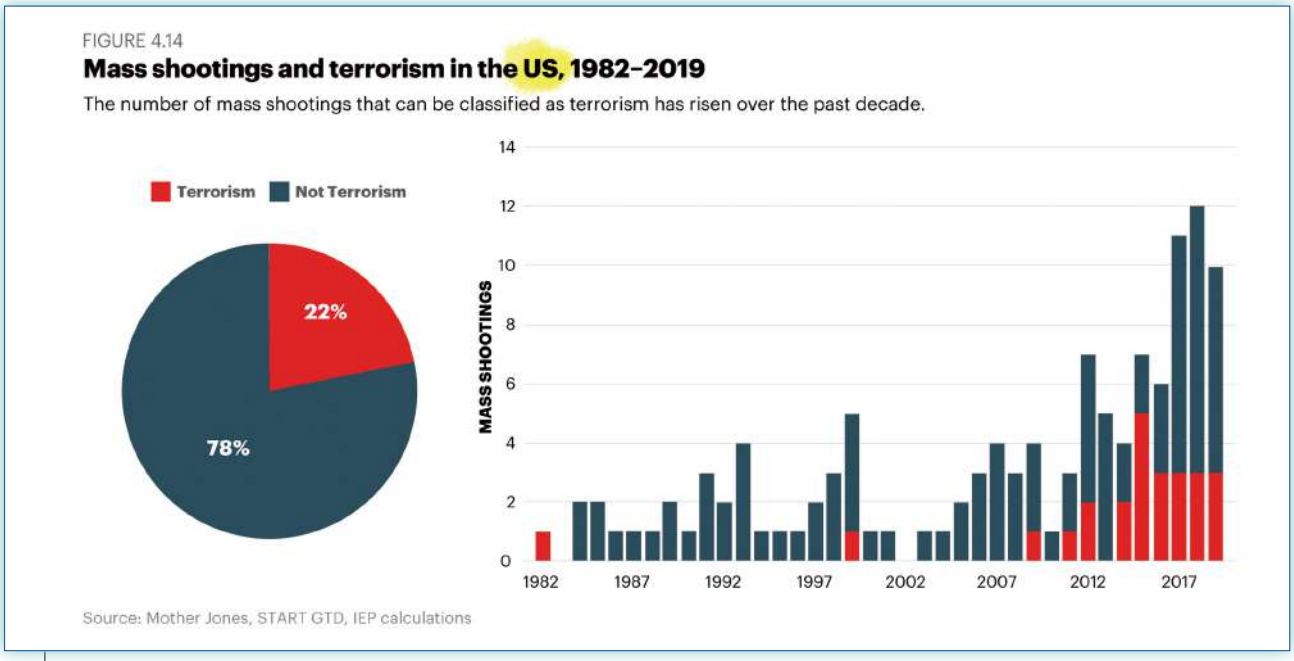
極右翼恐怖主義的崛起，已讓過去 5 年西方國家的極右翼恐攻案成長 250%，死亡人數增加 709%，極右翼恐怖主義已成為西方國家安全及民主價值的重大挑戰，其特性值得瞭解。僅依「經濟與和平研究所」2020 年 11 月發布之「2020 全球恐怖主義指數」統計資料，摘述於後：

一、致死率

西方國家過去 20 年，伊斯蘭恐攻案仍屬最致命，每案造成 4.49 人死亡，其次是極右的 0.86 人，極左則是 0.11 人。過去 5 年死亡人數超過 10 人的重大恐攻案共有 13 件，其中有 6 件屬極右恐攻案。1995 年 4 月美國奧克拉荷馬市聯邦大樓爆炸案死亡 168 人及受傷近 700 人，犯案者為極右團體主權公民運動者（Sovereign Citizen Movement）；2019 年 3 月在紐西蘭基督城的反穆斯林移民恐攻案更造成 51 人死亡。



在過去 20 年間的西方恐攻案件，伊斯蘭恐攻仍是造成最大的傷亡。圖為 2019 年發生的基督城清真寺槍擊案，當時造成 51 人死亡，引起全球嘩然。（圖片來源：路透社／達志影像）



2009 至 2019 年期間，恐攻槍擊案在大規模槍擊案之占比由 4.2% 成長到 30%，槍械成為恐怖分子重要的作案工具之一。（Source: Institute for Economics & Peace, GLOBAL TERRORISM INDEX 2020, https://www.visionofhumanity.org/resources）

二、作案者

大部分之極右翼恐攻案由孤狼所執行，孤狼並未加入任何恐怖組織或極右激進團體，但他可能曾與某極右分子接觸或受某極右恐攻案所激發。統計發現，6 成以上之右翼恐攻案由不附屬於團體的恐怖分子所為。例如 2002 至 2019 年期間，西方國家共發生 52 件造成死亡之極右翼恐攻案，其中只有 7 件由團體所為，而 2010 年以後，更是全由孤狼一人作案。

三、槍擊案

若將發生在公共場所、造成 4 人以上死亡及無確定受害對象之大規模槍擊案或瘋狂濫射案，歸類為恐攻案，則 2009 至 2019 年期間共發生 67 起槍擊恐攻案，恐攻槍擊案在大規模槍擊案之占比，由 4.2% 成長到 30%。過去極右恐怖分子以炸彈及爆裂物為主要作案工具，近年則愛用槍械，特別是高殺傷力作戰武器，例如紐西蘭基督城恐攻案恐怖分子即持用半自動霰彈槍及半自動步槍。

別讓民粹傷害民主

臺灣亦為民主國家，然近年來政黨對立面升高，民眾批判更加尖銳，為反對而反對，將民主變為民粹。觀看美國在政黨紛爭下，民粹凌駕民主後之慘況，臺灣人應戒之慎之，避免讓仇恨滲透進入你我日常，讓臺灣永遠成為居處全球動盪局勢中之最和平宜居的平行時空。

5G與AI不可不知的神奇密碼

◆ 社團法人台灣 E 化資安分析管理協會（ESAM）理事長、中央警察大學資訊管理學系專任教授 ── 王旭正

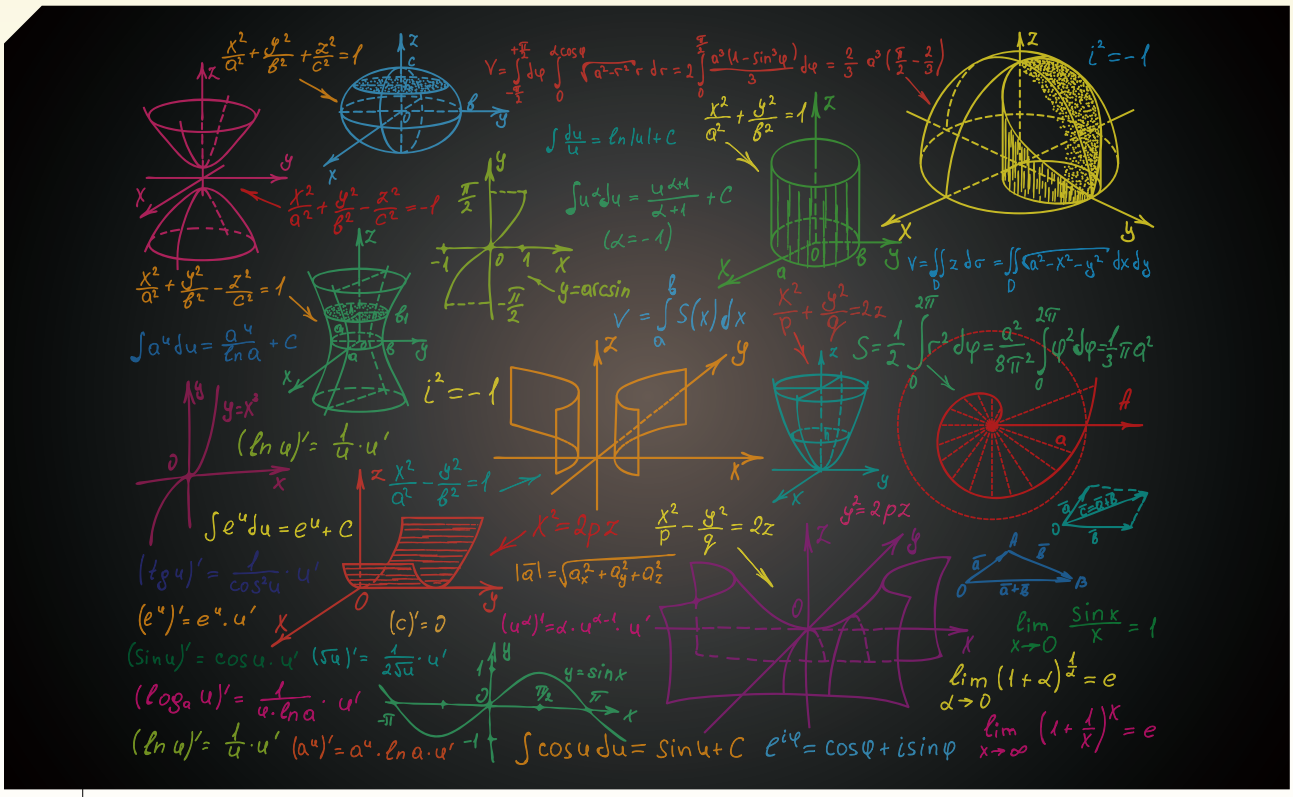
網路的興起，改變了人們溝通的方式，不再有面對面的必要性，不再有「一日不見，如隔三秋」之吟頌，也不再有傳統生活作息一天「二十四小時」的不可分割性。

拜科技、網路之賜，讓人們生活開始跳脫傳統的模式。相隔兩地的相思情，在網路裡，迅速縮短實際距離，讓影像的視訊互動升了溫；而時間的枷鎖藉網路的活化作用，在不知不覺中竟也神奇微妙地得以切割，以分工處理生活中的各式需求。網路媒介喚醒了人心深處的渴望—「快」與「準」，即有著 5G「快」的通訊速度、與 PK「準」的訊息正確性。

「快」5G

網路裡，訊息的傳遞讓通聯的雙方得以快速地分享資訊，1G、2G、3G、4G 通訊技術讓網路不斷地進化。近年，我們不斷聽到一個有點新又不是很新的英文詞：「5G」。其為 4G 通訊技術成熟後，下一個世代的通訊網路環境泛稱名詞。事實上，「G」世代的發展皆是建構在前一代的基礎，慢慢經營，而得以茁壯。1G 可語音通話；2G 開始數位訊息傳遞；2.5G、2.75G 的過渡時期；再到 3G 時代、3.5G、3.75G、3.9G，一直演進到現階段較為成熟的 4G。

而 5G 除了速度快、連通強，還有結合人工智慧的各式開發應用於 V2X（Vehicle to Everything）、遠距醫療系統、製造業市場等琳瑯滿目的網路應用，怎不令人心動呢！您是否也想到 1、2、3、4、5 後頭還有嗎？當然有，現在的 4G、10 年間的 5G、2030 年的 6G，再來的 7/8G 網路通訊技術的開發，那不是夢，是一代傳一代逐步建構上去的網路，得以符合人們心中的想像空間。那「安全」呢？接續前期的資安生活之旅，我們再次前進 PK（Public Key）的神奇戲法—密碼。



數學為科學之母，是記錄規律、整理順序、推演過程最重要的科學工具。

「準」PK

談了網路的「快」，是否還記得「準」？5G 通訊技術的確加快了網路的訊息傳遞速度，但還得準確地判斷訊息真實性，若一味搶快，失去了準真性，倒也可惜，是白費力氣地做虛工呀！在資安生活之旅中，我們曾說過法國的費瑪（Fermat, 1601-1665）對密碼「安全」的啟蒙，開啟了科技領域裡密碼與安全機制的新歷史。在業餘數學家費瑪的生活裡，他自行找出了許多自然界、生活中的規律。數學是科學之母，是記錄規律、整理順序、推演過程最重要的科學工具。藉由一項項的科學觀察與紀錄，費瑪的規律整理為「安全」奠定了深厚與重要的里程碑。讓我們看看「$a^{p-1} \bmod p=1$」，上一期介紹公開金鑰時留下的足跡，其中 p 為質數，此算式即為 a^{p-1} 除以 p 取餘數的結果會等於 1。舉例而言：

若讓 $a=5$、$p=11$，我們可知 $5^{11-1} \bmod 11=1$。

若讓 $a=6$、$p=11$，我們亦可立即知 $6^{11-1} \bmod 11=1$。

若讓 $a=7$、$p=11$，我們馬上可知 $7^{11-1} \bmod 11=1$。

是否覺得神奇？是的，這就是規律。

法國的業餘數學家費瑪對密碼「安全」的啟蒙，開啟了科技領域裡密碼與安全機制的新歷史。

歐拉為費瑪的規律繼續加碼，是網路公開金鑰得以實務運作的重要基礎。

一百年過後，瑞士的歐拉（Euler, 1707-1783）為費瑪的規律繼續加碼，有著新規律，「$a^{\emptyset(n)} \bmod n=1$」，其中 $\emptyset(n)$ 為歐拉函數，數學家歐拉找出規律，給了這樣的含意：$\emptyset(n)$=「小於 n 且與 n 互質的所有正整數個數」（例如 $\emptyset(7)$ 為小於 7 且與 7 互質的數為 {1, 2, 3, 4, 5, 6}，個數共有 6 個；$\emptyset(12)$ 為小於 12 且與 12 互質的數為 {1, 5, 7, 11}，個數共有 4 個），這可是網路裡經典的公開金鑰得以實務運作的重要基礎。在歐拉的此一規律下，網路的「密碼安全」得以強而有力，阻擋任何非法企圖的訊息破壞者與偽造訊息的散播者，保障網路安全訊息傳遞的正確性、值得信任的真實性。

5G 中的資安風險

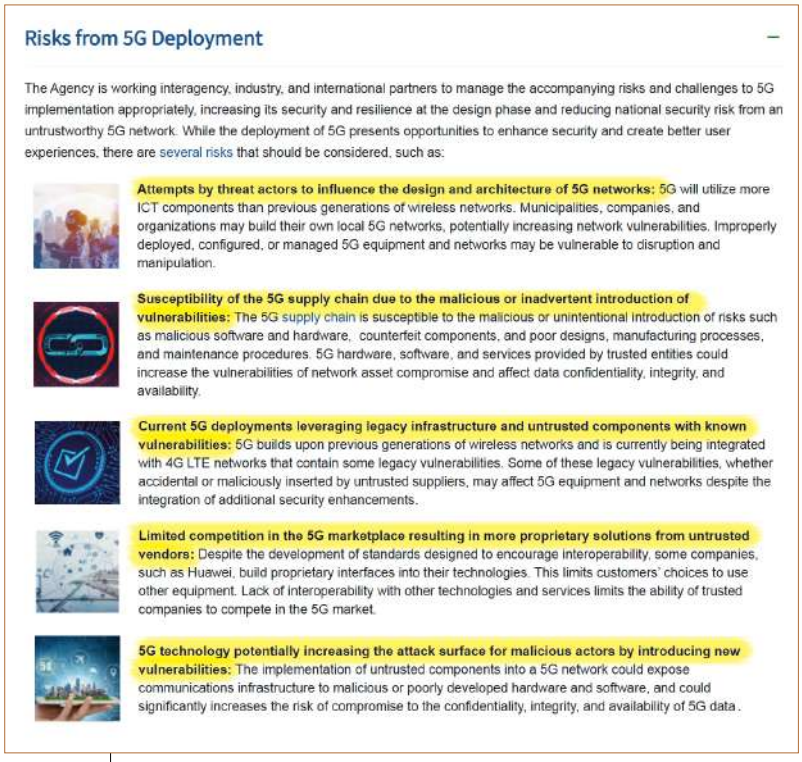
回顧我們的公開金鑰系統，「安全」有兩個目標，一者是「祕密性」、另一者是「真實性」。5G 裡所有的基礎來自前世代的通訊架構，是得以延伸而發展出來，所有 G 世代的安全問題如出一轍，卻也隨著資訊生活的普及，使得資安生活的安全意識更顯得重要。近年來網路通訊技術 5G 的推動，科技大國美國早已有所警覺並「超前部署」。根據美國負責「安全」的國土安全部與國家情報總監於 2019 年 5 月執行「保護資通技術及服務之供應鏈的行使命令」，藉此國土安全部緊接著發布「美國採用 5G 引發的風險概述」（Overview of Risks Introduced by 5G Adoption in the United States），列舉 5G 網路風險的脆弱性包含：供應鏈公司製造 5G 組件未經妥當的認證、傳承先前世代所承受的「網路安全」風險、5G 未來普及化部署實施過程安全配置、市場競爭機制不恰當、5G 技術操作標準等因素將增加 5G 執行的風險。

藉此，其中的「網路安全」，延續世代交替的密碼基礎，即 5G 系統的訊息正確性傳遞，需為通訊雙方所認可。若以密碼機制的公開金鑰系統來看此部分，也就是傳送方的訊息經網路傳遞的資訊，得被接

收方能正確的判斷訊息來源真實性。在公開金鑰系統的運作下，此一目標可以用傳送方的祕密 key 對訊息先做「驗證碼」的提供，而接收方將以傳送方的公開 key，對所接收的「驗證碼」進行檢驗，即可清楚判斷訊息來源真實性。

傳承費瑪與歐拉的密碼原理

我們再以孫悟空與牛魔王的通訊模式說明如下：老孫的「驗證碼」，是以老孫的「祕密 key」對訊息做加密得到「驗證碼」。當老孫傳送訊息給老牛時，「驗證碼」也將一併送出。接收方的老牛即以小猴的「公開 key」來解密「驗證碼」，再比對傳送訊息與解密「驗證碼」運算的結果，得為辨識真假訊息的依據。在公開金鑰系統下，若非老孫的小猴公開 key，是無法對網路所傳遞的「驗證碼」做正確解密運算，以得到吻合的比對結果。因為唯有同源（即代表老孫分身的



Risks from 5G Deployment

The Agency is working interagency, industry, and international partners to manage the accompanying risks and challenges to 5G implementation appropriately, increasing its security and resilience at the design phase and reducing national security risk from an untrustworthy 5G network. While the deployment of 5G presents opportunities to enhance security and create better user experiences, there are several risks that should be considered, such as:

Attempts by threat actors to influence the design and architecture of 5G networks: 5G will utilize more ICT components than previous generations of wireless networks. Municipalities, companies, and organizations may build their own local 5G networks, potentially increasing network vulnerabilities. Improperly deployed, configured, or managed 5G equipment and networks may be vulnerable to disruption and manipulation.

Susceptibility of the 5G supply chain due to the malicious or inadvertent introduction of vulnerabilities: The 5G supply chain is susceptible to the malicious or unintentional introduction of risks such as malicious software and hardware, counterfeit components, and poor designs, manufacturing processes, and maintenance procedures. 5G hardware, software, and services provided by trusted entities could increase the vulnerabilities of network asset compromise and affect data confidentiality, integrity, and availability.

Current 5G deployments leveraging legacy infrastructure and untrusted components with known vulnerabilities: 5G builds upon previous generations of wireless networks and is currently being integrated with 4G LTE networks that contain some legacy vulnerabilities. Some of these legacy vulnerabilities, whether accidental or maliciously inserted by untrusted suppliers, may affect 5G equipment and networks despite the integration of additional security enhancements.

Limited competition in the 5G marketplace resulting in more proprietary solutions from untrusted vendors: Despite the development of standards designed to encourage interoperability, some companies, such as Huawei, build proprietary interfaces into their technologies. This limits customers' choices to use other equipment. Lack of interoperability with other technologies and services limits the ability of trusted companies to compete in the 5G market.

5G technology potentially increasing the attack surface for malicious actors by introducing new vulnerabilities: The implementation of untrusted components into a 5G network could expose communications infrastructure to malicious or poorly developed hardware and software, and could significantly increases the risk of compromise to the confidentiality, integrity, and availability of 5G data.

美國國土安全部超前部署，列舉 5G 網路風險的脆弱性。（Source:CISA, U.S., https://www.cisa.gov/5g#risks）

在公開金鑰系統的運作下，可以用傳送方的祕密 key 對訊息做「驗證碼」的提供，而接收方將以傳送方的公開 key，對所接收的「驗證碼」進行檢驗，即可清楚判斷訊息來源真實性。

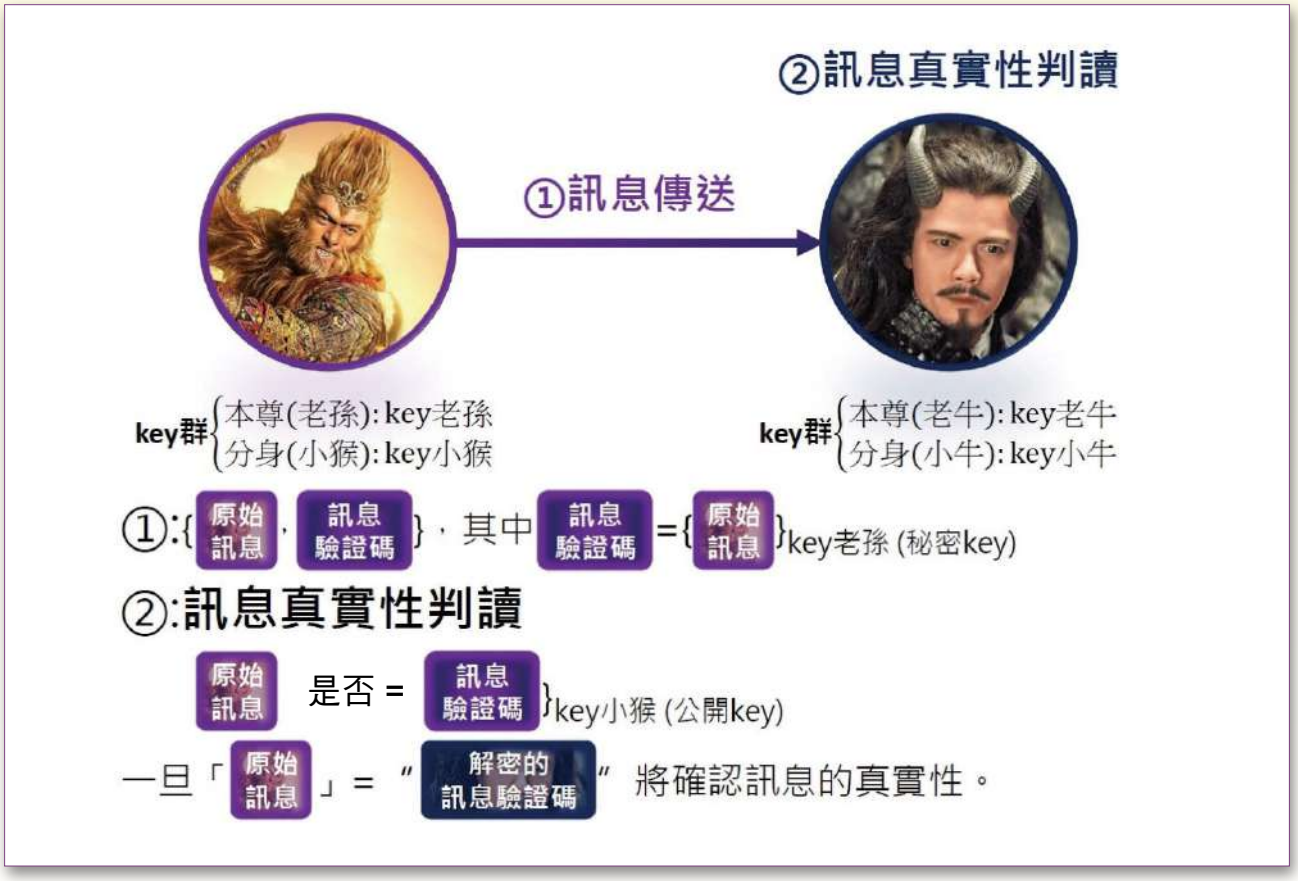


圖 1　公開金鑰驗證訊息真實性的通訊模式

小猴）的公開 key，才能與本尊老孫所採用的祕密 key 搭配，正確加解密，「還原真相」，得以做正確比對而檢驗出訊息真實性。（參考圖 1 說明）

這裡讓我們玩一個小戲法，讓老孫有著祕密 key，key 老孫 =3；公開 key，key 小猴 =7。另外再用一些數字當作訊息傳遞過程是否能判斷真實訊息的依據。

【範例】

讓訊息（數字）=「19」，老孫用祕密 key 老孫 =3 進行運算如下：$19^3 \bmod 33=28$（19 的 3 次方，再除 33，會餘 28），其中數字 33 為密碼環境中的微妙條件，戲法裡我們先賣關子，後續將陸續說明神奇卻簡單規律、得以創造強而有力密碼的安全系統。運算結果的數字「28」即是代表老孫為傳送訊息「19」過程中，所一併產生的驗證碼。老孫將一起傳送訊息「19」與檢驗用的驗證碼「28」，即傳遞｛「訊息 19」，「驗證碼 28」｝給老牛。老牛接著用老孫分身小猴的公開 key 小猴 =7，進行運算如下：$28^7 \bmod 33=19$。此結果將神奇地得到一個似曾相識的數字 "19"。是的，過程所傳遞的原訊息「19」與老牛運算得到的 "19"，竟是一樣的。這可不是偶然的發生，而是費瑪與歐拉這些科學先驅者所留下的智慧寶藏。

5G 基礎建設的發展需各領域技術相互依存、搭配與結合應用，加碼「安全」保障下的資安科技才能近乎「完美」。

科技不只來自人性 資安科技加持　更能深得人心

5G 通訊技術，是延續先前世代的所有基礎，我國行政院自 2019 年核定「臺灣 5G 行動計畫」，由國家通訊傳播委員會執行推動 5G 資安防護計畫。另外 2019 年開始實施的《資通安全管理法》，使得資通安全成為資訊生活裡必然得瞭解的科技基礎常識。而公開金鑰基礎建設（Public Key Infrastructure, PKI），讓 5G 承接各世代資通安全裡「網路安全」的重要技術與管理架構，得以具體實現資安科技。5G 未來十年的布置，結合我們已導入的 PKI 機制，5G — PK（5 Generation with Public Key）基礎建設利用公開金鑰系統的密碼技術、安全協定、鑑識判讀等相關資安技術，才得完善 5G 時代的「快」與「準」。科技的發展需各領域技術相互依存、搭配與結合應用，加碼「安全」保障下的資安科技才能近乎「完美」。資安生活的放心，不只廣告用語：「科技始終來自人性」；我們想說：「科技不只來自人心，以資安科技加持更是深得您我心」。

至聖之後的至慎先生

——絕口不談人事、不說禁中樹

◆ 臺灣警察專科學校前校長 — 陳連禎

居家不談人事，閒聊不涉公事，是公務員的基本素養。漢朝孔光稟性周密，典守樞機多年，時有上書，輒削稿銷毀，此因畏懼公事外洩。休假在家燕語，始終不及半句宮中政事，或問長樂宮溫室殿中樹，孔光則選擇沉默不應，答非所問。他事事至慎，故能終身無過，成為歷史保密美談。

禁中—皇帝駐蹕處所及論政宮殿之統稱

自古以來，皇宮內有論政的宮殿、官署，還有帝后皇家居住的地方，後者通稱禁中；後人將警衛森嚴的宮中、府中以及皇帝駐蹕處所，都稱禁中。置身禁中人員必須絕對保密，禁止對外感言發聲，如果洩漏了禁中談話內容，就是死罪。《史記》曾記載有人洩漏始皇帝的行蹤給丞相李斯，而引發始皇帝強烈不滿，致禁中隨扈全遭殺害之史事。

國政興革都在禁中密商 置身禁中必須絕對保密

廁身禁中者必須絕對保密，否則會闖大禍。主因是為了維護最高領導者的神祕色彩，不能讓臣民窺見其真面目或知道他的底細，就可讓人心存畏懼，不敢造次。其次，為了鞏固領導中心的萬全，帝王須與人保持距離，才不會受到任何危害與驚擾，因此帝王行蹤，必須列為最高機密，以防出現危安漏洞。最後，當然是因為國政興革都在禁中密商，禁中關涉國家安全，當然要嚴防外洩，以免暴露維安破口。職是之故，不是經過精挑細選的忠誠之士不能接觸禁區。因此，凡入出禁中者，無不以口風緊、不洩密為工作倫理的最高美德。

《漢書 · 孔光傳》記載孔子十四代孫的孔光廁身禁中，於公於私都能嚴守口風，為漢史留下一道難得好風景。

孔光保密工夫到家 連禁中之樹都絕口不提

孔光品學兼優，當過議郎、僕射、尚書令等職；他嫻熟典章制度，法規命令如數家珍。孔光思慮周密、行事謹慎，未嘗有任何過失，多次受到表揚。孔光後來升為九卿的光祿勳，參贊中樞機密十餘年，遵守法度，仍不斷學習漢法的精義，很得漢元帝的信任。

孔光工作態度認真外，更有同理心，處處為人設想，因而得到上下的敬重。例如他時有建言，每次奏書核批下來，立即銷毀草稿。孔光認為個人留下底稿，恐會有外洩機會而暴露上級長官的過失，而且又有沽名釣譽而想博得忠直美名的私心之虞；這樣的心機是為人部屬的罪過。又如每逢休假，孔光經常和家人閒話家常，但是話題始終不會觸及朝廷禁中的事務。就有人好奇地探問孔光：「溫室殿上種的都是那些樹呢？」孔光保持沉默不應，立即改用其他話題支開。溫室殿是何等機敏重地，孔光連禁中之樹都絕口不提，遑論其他機敏人事政務，真是保密到家。

由於孔光是皇帝師傅的兒子，飽讀詩書，很早就服公職，難免有很多官員想接近而有所他圖；但孔光為官低調，既不結黨交遊，也沒有養賓客、培植私人勢力的習氣。歷史人物中，如孔光從政經歷如此完整，幾乎前所未見。他歷任漢家 3 代皇帝，為官前後擔任御史大夫、丞相各 2 次，又曾任大司徒、太傅、太師等要職，服公職 17 年，而身後備極哀榮。王莽陳請太后以最高規格辦理喪事，博士護駕行禮。太后派遣謁者持節視喪。公卿百官聚集弔唁

送葬。羽林孤兒四百人輓送，禮車萬餘輛送行，經過道路的居民無不舉音悲痛。

孔光居高位多年，而能善始善終，歸根究柢是他深具高度的風險意識：身為至聖先師孔子的後代，懷有強烈的責任感，不能有辱先祖家風的信念。其次是終身學習經典又嫻熟法制，與時俱進，處事嚴謹而受到上下的尊敬。再其次是為人具有同理心，上書後銷毀草稿，不留底稿的用意，除了不矜己能之外，也嚴防草稿外流而洩密。功歸長官，沒有私心，當然讓人放心。

至於為國推薦舉才，他都唯恐人知而增加人情負擔；不誇己功，更受尊重而屢受重用。最後也是最難得的是，參贊國家機要多年，都嚴守口風，即使是家居生活，人或問起宮殿上所植的樹木，隨時隨地心存危機警覺，已經成為工作習慣，斷然不肯鬆口。

吉人辭寡　最好無言

常人好奇探問，又喜愛爆料以為先知。然而吉人辭寡，最好無言，唯有懂得自律以保護自己，魔鬼就無法藏在細節裡作祟。孔子至聖，而後代子孫孔光至慎，慎處禁中事，無不憂患全身。孔光一生具有高度危機意識，已成公務員守密的典範。

唐太宗時期接任魏徵的宰相楊師道為人謹慎，從未洩漏禁中語。他常說：「年幼的時候，我讀過《漢書》，上面說孔光不言溫室之樹，我非常欽佩他的保密素養。」於公於私有高度的危機意識，絕口不談人事、不說禁中樹的保密素養，就能阻絕「黑天鵝」意外事件發生。

由「班恩回家」電影 看戒毒辛酸史

◆ 顧崇平

盼「班恩回家」這部影片，讓曾徬徨於人生十字路口的朋友及協助戒毒的親友們，拾回重塑生命的力量。

根據我國食品藥物管理署針對民國108年物質濫用的統計，除了常見菸、酒及檳榔等成癮性的物質外，最嚴重的即是藥物濫用，是類通報個案高達3萬6千餘件，又以海洛因、安非他命與愷他命高居前3名，不少人生尚未起步的青少年，在懵懂無知下誤涉毒害，甚而失去寶貴的生命。

毒品不僅對人體產生危害，亦衍生諸多社會犯罪的問題。然而因勒戒或是毒品案入獄重返社會者之心路歷程卻鮮少人留意；而要讓其等順利地重新融入社會，實應需要我們多多給予支持及協助。

「毒」與「獨」的夾擊

電影「班恩回家」（Ben Is Back）中，故事的主角班恩，因國中的一場滑雪意外，逐漸成癮於醫師開立的止痛藥物中，終因吸食毒品而多次出入勒戒所。聖誕節前夕無預警地回到家中，對於重組家庭而言，「班恩」是不速之客，再次回來，又成為家人們的頭痛問題。繼父、親妹妹對他不

班恩回家（Ben Is Back）探討主角班恩因為吸毒從勒戒所返家後，受到除了母親以外的家人、朋友與鄰居的排斥，在和毒品搏鬥與外界的紛擾中，他要如何遠離誘惑、回到正軌。（Photo Credit: Black Bear Pictures, 30West, Color Force）

班恩的「回家」，成為家人們的頭痛問題，繼父、親妹妹對他不抱持信心，認為他仍會因毒品再次回去勒戒。（Photo Credit: Black Bear Pictures, 30West, Color Force）

抱持信心，認為他仍會因毒品再次回去勒戒。社區居民的子女曾因班恩販毒而失去寶貴的生命，至今對他仍無法諒解，故同班恩家人一樣，不希望看到他的出現。家人與鄰居的冷漠及排他舉動，讓想要重新融入社區的班恩，倍感孤寂無力。

「善」與「惡」的距離

班恩再次回到熟悉的社區，卻不時受到毒品的誘惑。在意志動搖初期，班恩隨即告知母親要到社區的互助會尋求協助，盼透過戒毒成功夥伴的經驗，彼此加油打氣，以堅定其遠離毒品的力量。

然而在光譜的另一端，曾因班恩陷入毒品控制的受害與關係者依舊存在，憎恨班恩將自己帶到不歸之路，並表明如果要她戒毒，她希望跟班恩再吸最後一次。昔日的「毒」友史賓賽及毒販在得知班恩回來後，並不想放過班恩，甚至藉由侵入其家中搞破壞等威脅手段，希望他能重操販毒舊業。

母親的「呼喚」

回顧從前，母親荷莉在前夫拋下班恩與妹妹之後，開始身兼父職，由於過於忙碌而忽視班恩狀況，因此，荷莉對班恩染上藥物毒癮的事情一直深感愧疚。

當班恩受不了誘惑想吸毒時，母親荷莉將班恩帶到墓地旁，給予班恩當頭棒喝。（Photo Credit: Black Bear Pictures, 30West, Color Force）

再次與班恩發生爭執的荷莉知道，如果連她都放棄了，班恩將永遠深陷泥沼，無法逃離毒品。（Photo Credit: Black Bear Pictures, 30West, Color Force）

在家人都不願接納班恩之時，母親是班恩最大的精神支柱，她更展現母親堅定的力量。為了不讓班恩有接觸毒品的機會，開始緊迫盯人，包含了驗尿、衣物檢查等措施。當班恩想再次吸毒時，她將班恩帶到墓地旁，大聲斥責「想要在哪一區躺下，我覺得你應該快了」，給予班恩當頭棒喝，目的無他，就是希望兒子有朝一日可以克服毒品的誘惑，重新回到正常的生活。

當荷莉逐漸知道班恩染毒如此深且曾做過的種種荒唐行徑後，頓時感到無力而潸然淚下，荷莉深知如果她也放棄，班恩將更無法由痛苦深淵脫離，於是決定無論如何都會與班恩一起面對任何挑戰。

如果能重來

對於母親無私的關懷，班恩感到自己並不孤單，更瞭解昔日乖誕的行徑讓母親操碎了心，也希望能有所改變。然而環境的不友善，讓班恩與母親求助無門。最後，班恩心力交瘁，不想再造成大家無比的困擾，於是選擇用毒品結束了自己的生命。母親聲聲呼喚，試圖將班恩救起，然此時畫面戛然而止……

本片所要傳達的核心主軸就此浮現—如果能重來一次，「你是否還會輕易嘗試毒品？」。

身體脫毒後　心癮更難戒

電影片名採用「回家」，有其特殊意涵；對於一般人而言，「回家」或許是簡單不過的事，然對於曾因毒品案件想要重返社會的人，卻是一條荊棘之路。回顧吸毒者的家庭背景，大都是缺乏家庭的溫暖與關懷，而想要尋求同儕認同，因此在同伴慫恿或是好奇心的驅使下，致誤陷於毒海之中。

因此，「毒品防制」工作，應從最核心的「家庭」開始做起。或許是一開始的疏忽，而讓家人不小心染上毒品；但當發現家人染毒之後，全家人更應齊心協力，共同凝聚面對困難的信心及勇氣，重啟安定與愛的力量，讓家人的關愛與時刻提醒，成為脫離心癮的最大助力。

另外的作法是發揮學校與社區的力量。近年來新興毒品在毒販的包裝下已轉換成日常生活中隨時可見的物品，引誘人在不經意間掉入其陷阱中。因此，若能透過防毒宣導，讓每位民眾知道新興毒品的種類及包裝手法，並瞭解吸毒後將造成之不可逆的危害，絕對是首要工作。再者，每個人應培養正向的休閒習慣，多參與白天戶外運動，遠離聲色場所，不讓周遭損友及毒販有任何可趁之機，並牢記「不接觸、不好奇、不逞強」的 3 不口訣，防範毒品戕害，掌握自我人生。

近年來毒品的包裝花樣百出，為讓民眾了解毒品的偽裝與危害，彰化縣首創「行動反毒箱」呈現各種新興毒品模型，強化民眾對毒品的觀念與警覺。（圖片來源：彰化縣政府，https://www2.chcg.gov.tw/main/main_act/main.asp?main_id=28142&act_id=383）

最後，發揮守望相助的精神也是很重要的，正如片中居民對周遭環境的漠不關心，因此助長了販毒者為所欲為的囂張氣焰；如每個居民均能注意肇生毒品犯罪的熱點，再與治安單位密切聯繫，將能讓人知道在此社區吸毒、販毒有極高被查獲的風險，不要心存僥倖。若人人皆可高度覺察並即時伸出援手，毒品方能遠離親愛家人及周遭生活領域，利己更能利人。

盼「班恩」們都能順利回家

當前的毒品防制工作，是項艱鉅的工作，依靠單方面努力，無法與毒品犯罪鏈長期抗戰，因此，建立「無毒有我，人人都是反毒尖兵」的正確認知，並保持「勿以惡小而為之，勿以善小而不為」的心態，將防毒的觀念帶至家庭、社區與學校，如此所凝聚起來的，就是一股在社會中不可撼動的反毒力量。期許我們都能勇敢地散播光與愛，共同消弭因毒品所衍生的憾事，讓每位迷途羔羊都能順利「回家」。

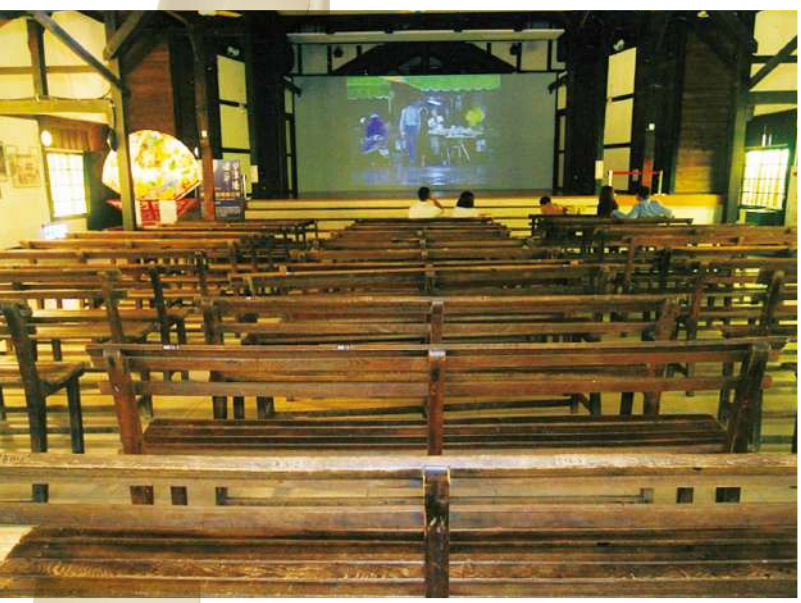
「無毒有我，人人都是反毒尖兵」，全民共同認識毒品，遠離毒害。（圖片來源：法務部，國立自然科學博物館，https://antidrug.moj.gov.tw/lp-26-1.html）

懷念的老戲院

◆ 若　水

據媒體報導，全臺的二輪戲院近年間紛紛吹起了熄燈號，讓忠實影迷們難掩落寞，深深感到不捨。這些戲院面對現實經濟壓力，不得已宣布停業，令人不勝唏噓。

（圖片來源：國家電影及視聽文化中心，https://openmuseum.tw/muse/digi_object/51b4f70385ee6c761cc080bce2ddd517；https://openmuseum.tw/muse/digi_object/d44df3d817b7d087c5d92f55f1c3a5cb）



坐在木造長椅欣賞老電影，體會 50 年代村民聚集在大廣場觀影的感受。

50 年代　星空下的布幕電影

物換星移，歲月遞嬗，科技愈昌明，物質生活愈富裕，一些懷舊產業卻紛紛湮沒在歷史的洪流之中。想當年物資匱乏，凡事講求簡約克難，生活艱辛刻苦的年代，老戲院提供不少歡樂的影片戲劇，慰撫了大眾沉悶的心靈，忘卻了他們心中的空虛寂寞，重拾生活的色彩，那真是一段難忘的黃金時光。

50 年代，那時沒有電腦及手機，只有每週放映 1 至 2 次的黑白電影，在村子裡頭的大廣場播放。一大片潔白的布簾掛在場中央，周遭擠滿了人群，小孩們坐在板凳上觀賞，大家聚精會神地盯著螢光幕，只有換片空檔，大人們才會竊竊私語，興奮地討論劇情的發展。這場景直到鎮上的戲院隆重開幕，才結束這種引頸盼望電影團來鄉下公演的「追星熱潮」。

60 年代戲院　萬人空巷追星熱潮

當時的戲院不算氣派，裝潢也不考究，簡陋中略帶著古色古香氣息。最醒目的是掛在戲院四周的招牌，色彩繽紛，畫風細膩，把電影劇情及男女主角的帥氣與高雅氣質，紛紛表露無遺。當年還流行著讓大名鼎鼎，紅遍半邊天的電影明星隨片登臺，一時萬人空巷，大家爭相慕名而來，要一睹其廬山真面目；當下戲院前人潮如織、大排長龍，那種熱烈氣氛簡直比今日追星族更為瘋狂呢！

老戲院為臺灣早年經濟注入活水

60 年代，黑白影片興起，帶動全臺興建戲院的熱潮，那時無論是男女老少，最想去的休閒場所就是戲院。當年偷看戲（看白戲或撿戲尾）的時候比較多，大都是小孩子趁虛而入，或緊跟著大人們鑽隙偷溜進戲院。當然也有被識破悵然而返的時候，戲院則是大大方方地讓大家進場觀賞最後的結局，讓其等在意猶未盡、徒留回味之後，企盼明日再來一償宿願。

老戲院可說是早年臺灣經濟起飛的搖籃之一，除了滿滿的人潮，戲院內外還有許多可以促進消費的小吃零食，小攤販甚至利用換片空檔時刻兜售零食，讓觀眾們一邊欣賞劇情，同時大快朵頤，體會感官雙重享受，簡直讓人樂翻天。

老戲院—超靈驗月老廟

當年戲院更是熱戀中情侶約會的最好去處，尤其是來自國外、名聞已久的「舶來品」影集，更吸引忠心的影迷們迫不及待地購票觀賞，如《亂世佳人》（Gone with the Wind）、《吾家有女初長成》（Light in the Piazza）、《蝴蝶夢》（Rebecca）等。也有本國自製的文藝愛情片，如《窗外》（林青霞主演的首部電影）、《幾度夕陽紅》（江青主演，她亦藉此作品獲得金馬獎最佳女主角）、《星星月亮太陽》等，均是名震一時、叫好又叫座的電影。拜戲院之賜，促成許多男女結緣，造就出不少對佳偶。

60 年代的戲院不算氣派，但色彩繽紛、畫風細膩的電影海報卻成為最醒目的招牌。

老戲院可說是早年臺灣經濟起飛的搖籃之一，戲院內外有許多兜售零食的攤販，大大促進當時的消費。

「電姬戲院」採巴洛克式建築風格，外牆有 7 隻石獅，寓意天天放映、全年無休，右圖為戲院的售票窗口。（Photo Credit: Pbdragonwang, https://w.wiki/32Nb, https://w.wiki/32Na）

老戲院建築風格　見證歷史軌跡

日治期間，正是世界建築史上的黃金時代；建築可說是城市的精神標誌，當時很多臺灣戲院揉合歐洲與日本新古典主義的美學觀念，重資興建戲院，其中最醒目的是臺南麻豆中山路的「電姬戲院」（姬在日語中是公主的意思），興建至今已有 80 年的歷史。就建築結構而言，「電姬戲院」採用當時最流行的「巴洛克」式建築風格，加上日本東洋風味的造型，再配合西洋裝飾，所採用之建築材料、工法與風格，更是與當時世界各地戲院建築同步，見證當時的歷史足跡。戲院外牆上有 7 隻西方石獅，寓意天天放映、全年無休，其與日本「福神」浮雕神情十分吻合，以笑臉迎接著絡繹不絕的觀眾。

「電姬戲院」為鋼筋混凝土建築，堅固耐震，內部座椅為長條狀；一樓可坐 300 人，樓上則可容納 100 人，最特別的是舞臺下埋有幾個甕缸，具備立體回音之特殊效果。戲院裡有位重要的靈魂人物—放映師，其職責重大，需長時間擠在狹小高溫的環境內，且播放中途片刻不能離席，顯示三百六十行，行行各有辛苦面。

老戲院的轉型與沒落

60 年代中期，歌廳秀及錄影帶興起，戲院榮景漸漸不再，部分戲院轉型成二輪

戲院（指電影在首映戲院下檔後，以優惠價格放映該電影之電影院），其以低價吸引預算有限的民眾以及學生，讓觀眾能以百元左右價格，來觀看多部剛下檔的首映片，是很經濟又實惠的休閒選擇。當然，這些戲院的裝潢、音響設備、座椅都遠不及豪華影院來得高級舒適。二輪戲院礙於經費有限，環境衛生無法好好維護，時日一久，建物及座位破損率增高，又因門票低廉吸引許多素質不佳的觀眾，一般民眾因此望之卻步，讓老戲院經營更加困難，紛紛走上荒廢、歇業、轉業經營的命運。

期老戲院風華重現 喚醒全民遙遠美好的共同記憶

戲院不僅是城市進步的標誌，也是文化傳輸的殿堂。當年，老劇院除了放映電影、進行戲團表演，也是舉辦大型活動、宣導政令、灌輸愛國意識的重要場所；協助臺灣經濟起飛，凝聚民眾向心力，老戲院實在功不可沒。

政府已積極協助輔導一些老戲院重新修繕，從北到南計有新北市九份「昇平戲院」、新竹「內灣戲院」、嘉義「萬國戲院」及臺南鹽水「永成戲院」等等，期能恢復老戲院往昔風華，再現榮景樣貌，喚醒全臺民眾那段遙遠又美好的共同記憶。

政府已積極輔導部分老戲院重新修繕，從新北市九份「昇平戲院」（左上圖）、新竹「內灣戲院」（上圖）到嘉義「萬國戲院」（左圖）等，期能恢復老戲院往昔風華。

（本文圖片除標示來源者外，其餘皆由作者提供。）

走讀塔塔加

◆ 玉山國家公園副處長 ── 林文和

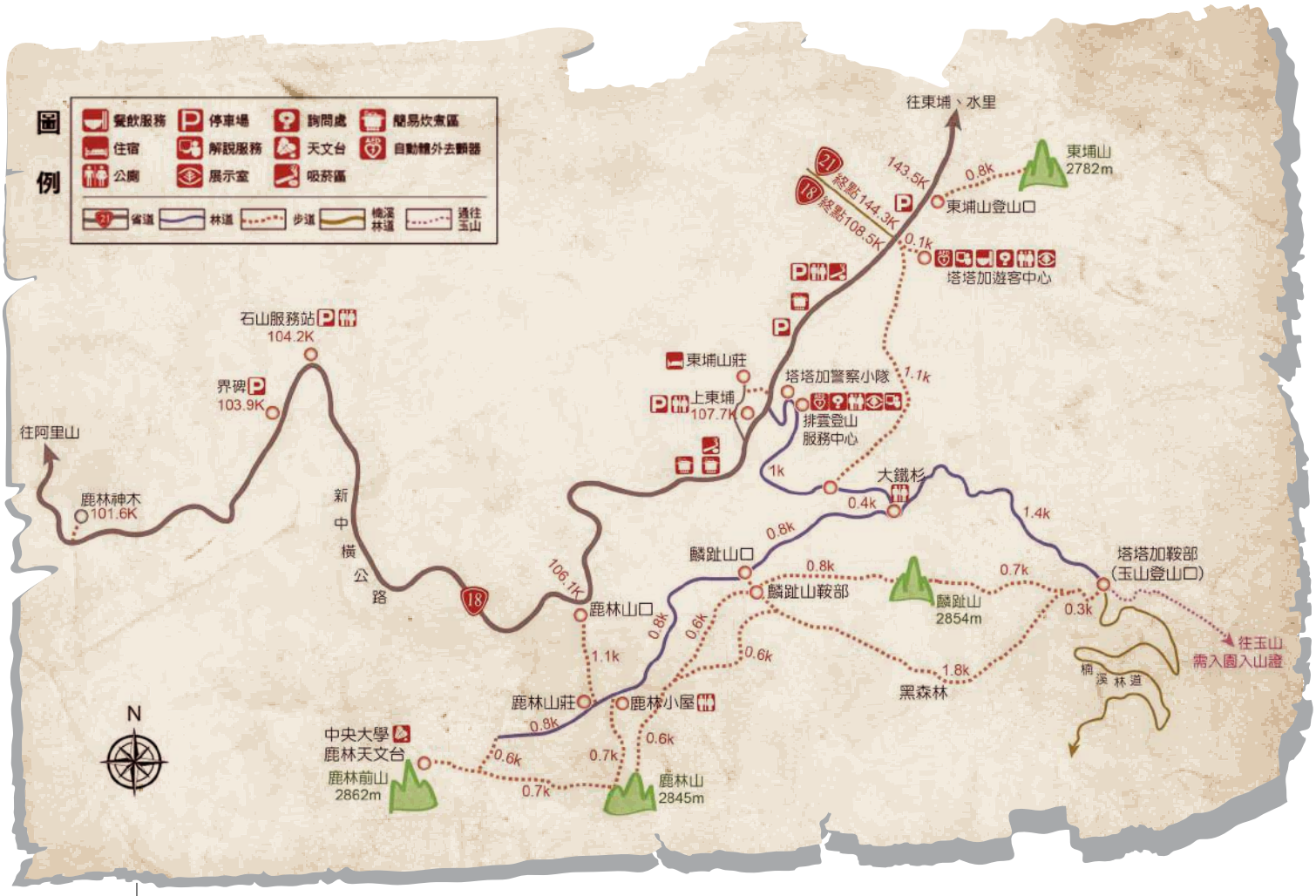
（Photo Credit: Yada Liao, https://www.flickr.com/photos/yada/29419278931）

塔塔加位於新中橫景觀公路最高點，也是攀登玉山登山口的所在地，生態資源與自然景觀相當豐富，是遊客探索玉山國家公園的最佳地點。

演進歷程訴說歷史

「塔塔加」是譯音自鄒語的「Tataka」，在鄒族人語意是指寬闊、平台草原的地方，是鄒族相當重要的獵場。記載中，塔塔加最早的開發是從 1932 年開始，日治時期的臺灣總督府鐵道部因伐木需求，將阿里山森林鐵路自沼平車站延伸至哆哆咖（即現在的塔塔加）。這也讓當時登玉山的山友可以坐火車到哆哆咖，再步行到塔塔加鞍部登山口後開始攀登玉山，而位於玉山林道上的鹿林山莊就是在此時期建造的，當時為日警駐在所，是作為管理登玉山的檢查哨。

之後國民政府遷臺，1956 年後因保育緣由停止伐木，並拆除哆哆咖線鐵道展開造林；後來政府就循該路線的路基興建新



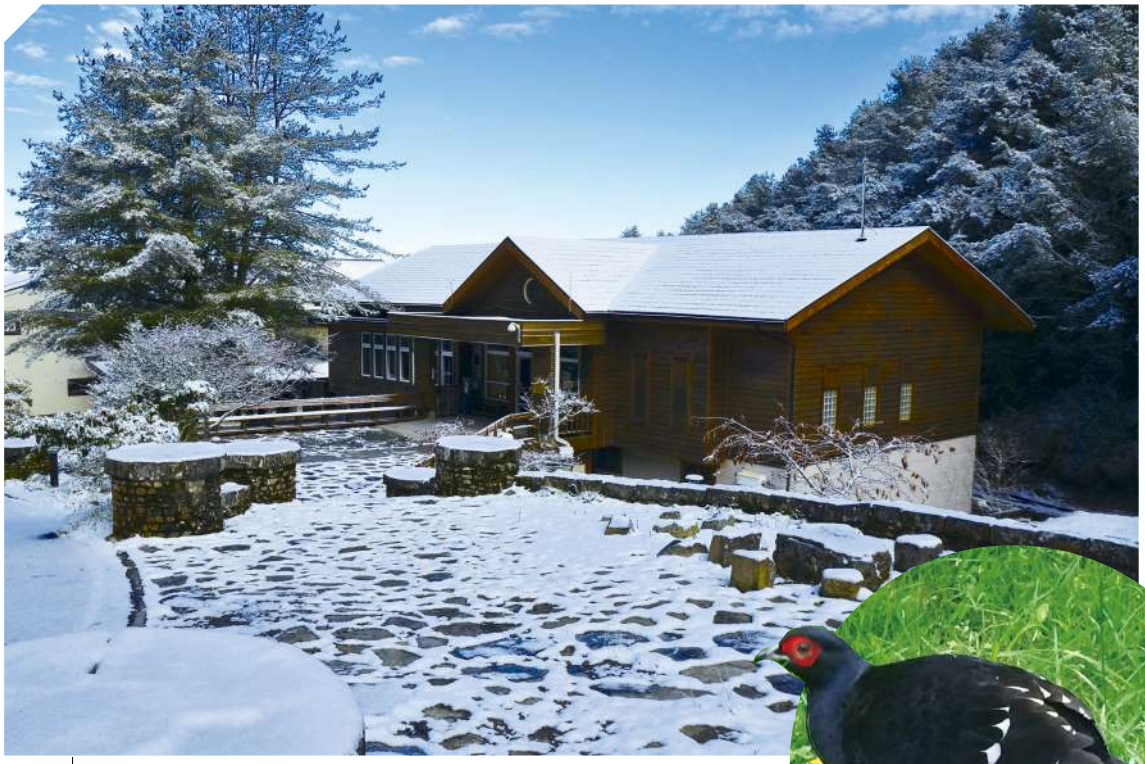
塔塔加遊憩區步道景點地圖。

中橫公路；1985 年玉山國家公園成立，將塔塔加地區劃為遊憩區，並設置遊客中心、餐飲部、步道等相關設施，目前每年約有 80 萬人次的遊客造訪，成為玉山國家公園西北園區相當知名的遊憩景點。

生態資源多樣豐富

塔塔加海拔 2,610 公尺，位處新中橫公路嘉義—玉山段（台 18 線）與水里—玉山段（台 21 線）的交界點，也是新中橫公路的最高點。塔塔加地區植物呈現以玉山箭竹與高山芒為優勢的草原景觀，但在森林火災的影響下，已逐漸演替形成雲杉、紅檜、臺灣二葉松、臺灣赤楊等次生林景觀。

在塔塔加向東可眺望玉山連峰之高山景觀，往西隔神木溪與阿里山山脈的祝山、塔山相望，清晨、傍晚在山壑間常有雲海、山嵐形成；在深秋之際，附近山區臺灣紅榨槭變紅時，楓紅景色在翠綠森林中，更顯得嬌豔美麗；在春分季節，山間林中盛開的玉山杜鵑以其白裡帶紅的花朵為大地添了彩衣；隆冬時節，如溫度過低與水氣適合，也會結霜甚或下雪，形成一片銀白色世界。



隆冬時節的塔塔加，也有機會看到美麗的雪景。

走在步道間，可能會偶遇各種野生動物，圖中動物為帝雉。

近幾年，由於國家公園的保育有成，動物資源相當豐富，清晨或黃昏漫步在步道間，偶而還會與帝雉、黃喉貂、山羌、水鹿等動物相遇，甚至連珍貴稀有的臺灣黑熊也曾在塔塔加地區出沒，這也引發大眾探討人類如何與野生動物互動、相處的相關議題。

開車遍賞高山美景

遊玩塔塔加有兩種方式，其一是開車沿新中橫公路欣賞玉山群峰及阿里山山脈等高山景色，遊客可在公路的觀山、觀峰據點駐足休息，眺望臺灣第一高峰—玉山北峰的雄姿；也可在夫妻樹據點觀賞兩棵檜木相偎相依、至死不渝的淒美故事，雖夫樹不久前因年久倒地，但妻樹仍守護在旁，讓人更加感念；而在石山服務站附近，深秋時可以觀賞神木溪谷的高山紅榨槭紅葉美景，也有國家公園志工駐點，進行環境解說及禁止餵食臺灣獼猴的勸導服務。

步道健行休閒愜意

除開車賞景外，還是以步道及林道的登山健行為主要休閒活動，塔塔加遊憩區共有 5 條登山健行步道及 2 條林道串聯相關景點。

東埔山步道

步道口位於新中橫台 21 線公路 143.5 公里處，步道雖僅長 0.8 公里，海拔落差約 300 公尺，走起來還是有些挑戰性，登上海拔 2,782 公尺的東埔山，玉山主北峰雄偉的稜線一覽無遺，同時也是塔塔加觀賞玉山日出的絕佳地點。

麟趾山步道

步道口位於玉山林道上，處處可見獸徑、啃食樹皮、腳印等動物出沒痕跡，尤其在高山小水池，更是觀察野生動物的最佳場所，幸運的話也可遇到野生動物在此喝水、泥浴打滾；登上海拔 2,854 公尺的麟趾山，玉山群峰西南稜各山頭盡在眼前，坐在山頂的木製椅上，環看四周高山深谷，是登山客的最愛。

鹿林山步道

步道口位於鹿林小屋附近，鹿林山海拔 2,845 公尺，早年因水鹿群生得名，民國 80 年的一場森林火災，使原本蓊鬱的森林現已變成白木林，並演化成以箭竹、馬醉木、假沙梨等為主的次生林，走在鹿林山區步道可見證森林火災對於自然生態環境的破壞與影響。

麟趾山擁有廣闊的步道草原。

東埔山頂是觀賞玉山日出的絕佳地點。

東埔大草原步道

步道口位於塔塔加遊客中心附近，可與楠溪林道形成一條環狀步道到達排雲登山服務中心，1.1 公里的步道隱藏在臺灣二葉松林內，夏日走在其中聞著淡淡的松脂味，聆聽臺灣噪眉清脆的鳥聲，以及感受黃喉貂偶然竄出步道的驚喜，是塔塔加最受歡迎的步道。

黑森林步道

位於麟趾山的腰部，1.8 公里的步道可到達塔塔加鞍部玉山登山口，為日治時期登玉山的舊步道，步道上有一處以高大紅檜所組成的黑森林，樹形高大、茂密鬱鬱，生態完整，是野生動物最佳的棲息庇護所。

從東埔大草原步道可清楚眺望玉山主峰。

可愛的黃喉貂偶爾會竄出步道，給遊客一個驚喜。

廢棄林道風華再現

另外還有楠溪林道及玉山林道，這 2 條林道原來是作為載運自林場伐下木材的道路，但在 1982 年結束伐木後就不再維護使用，玉山國家公園成立後將林道列為專用道路，僅提供遊客健行使用，禁止一般車輛進入，以有效管理塔塔加地區的環境遊憩資源。

楠溪林道、玉山林道

楠溪林道是登玉山的聯外道路，遊客沿著林道可先造訪 8 百多歲的大鐵杉神木，再抵達塔塔加鞍部登山口；而循著玉山林道則可參訪鹿林山莊及鹿林天文台，鹿林天文台由中央大學設置，是觀察彗星的極佳場所。

在楠溪林道巧遇山羌。

由中央大學設置的鹿林天文台是觀察彗星的極佳場所。

守護臺灣山林演進史 感受塔塔加的靜與美

塔塔加歷經原住民時期的狩獵利用，日治時期的山林開發，國民政府的交通建設，到現在設立國家公園推動保育與生態旅遊，走讀塔塔加猶如閱讀一部臺灣山林的演進史。遊客到塔塔加旅遊時，不妨放慢腳步，細細感受山林的靜與美，遇到動物時也記得不要干擾牠，更不要餵食牠，離開時請別忘了帶走不屬於山上的垃圾，讓青山常在、綠水長流。

（本文內文圖片皆由作者提供。）

藍眼淚的奧秘：夜光蟲

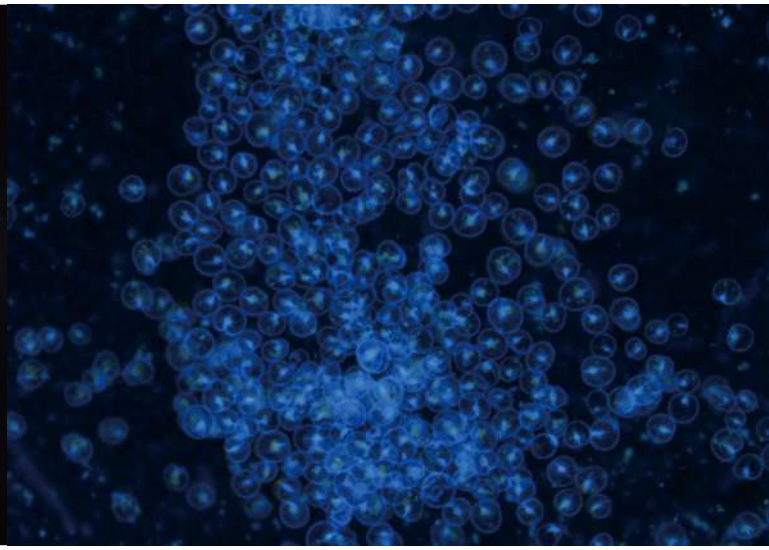
◆ 國立臺灣海洋大學海洋環境與生態研究所 — 特聘教授蔣國平、助理教授蔡昇芳

馬祖沿海在春末夏初（3～7月）偶而會出現如李安電影「少年PI」中整個海面發藍光的場景，此一海洋生物發光現象被稱為「藍眼淚」。

馬祖「藍眼淚」是一個旅遊熱門話題，2018 年大約就超過 40 萬觀光客到馬祖「追淚」。「馬祖藍眼淚」廣為人知，主要是因為兩件事，一為 2014 年 4 月，美國電視媒體 CNN 介紹馬爾地夫法度島（Vaadhoo Island）的夢幻藍色海灘，將夜光蟲發藍光奇景（藍眼淚）列為全球最壯觀的 15 個奇景的第一名。2015 年 4 月「馬祖藍眼淚」因為一名攝影師的作品而揚名國際！這位「不小心」成為臺灣觀光大使的攝影師是安德列歐（Rogelio Bernal Andreo），他在馬祖南竿拍下以銀河為背景的「藍眼淚」，絕美的畫面立刻獲選為 NASA 官網中「每日天文照片」類別的作品，讓國際人士看見「馬祖藍眼淚」的美。

「藍眼淚」由何種生物所造成，國立臺灣海洋大學（下稱海大）進行研究之前眾說紛紜，一般最常見的有兩種說法，一為介形蟲（*Ostracod*），另一為夜光蟲（*Noctiluca scintillans*）。為解開這些謎團，海大研究團隊由 2016 年 4 月開始在馬祖海域利用單離培養法及次世代定序技術，找出發光相關蛋白基因，兩種方法均證實

海洋上的「藍眼淚」奇景。（圖片來源：作者提供）



藍眼淚的形成有一說是介形蟲（圖左），但經海大研究團隊實驗證實「馬祖藍眼淚」主要是由夜光蟲所造成，圖右為顯微鏡下的夜光蟲。（圖片來源：Anna Syme, https://commons.wikimedia.org/wiki/File:Ostracod.JPG；作者提供）

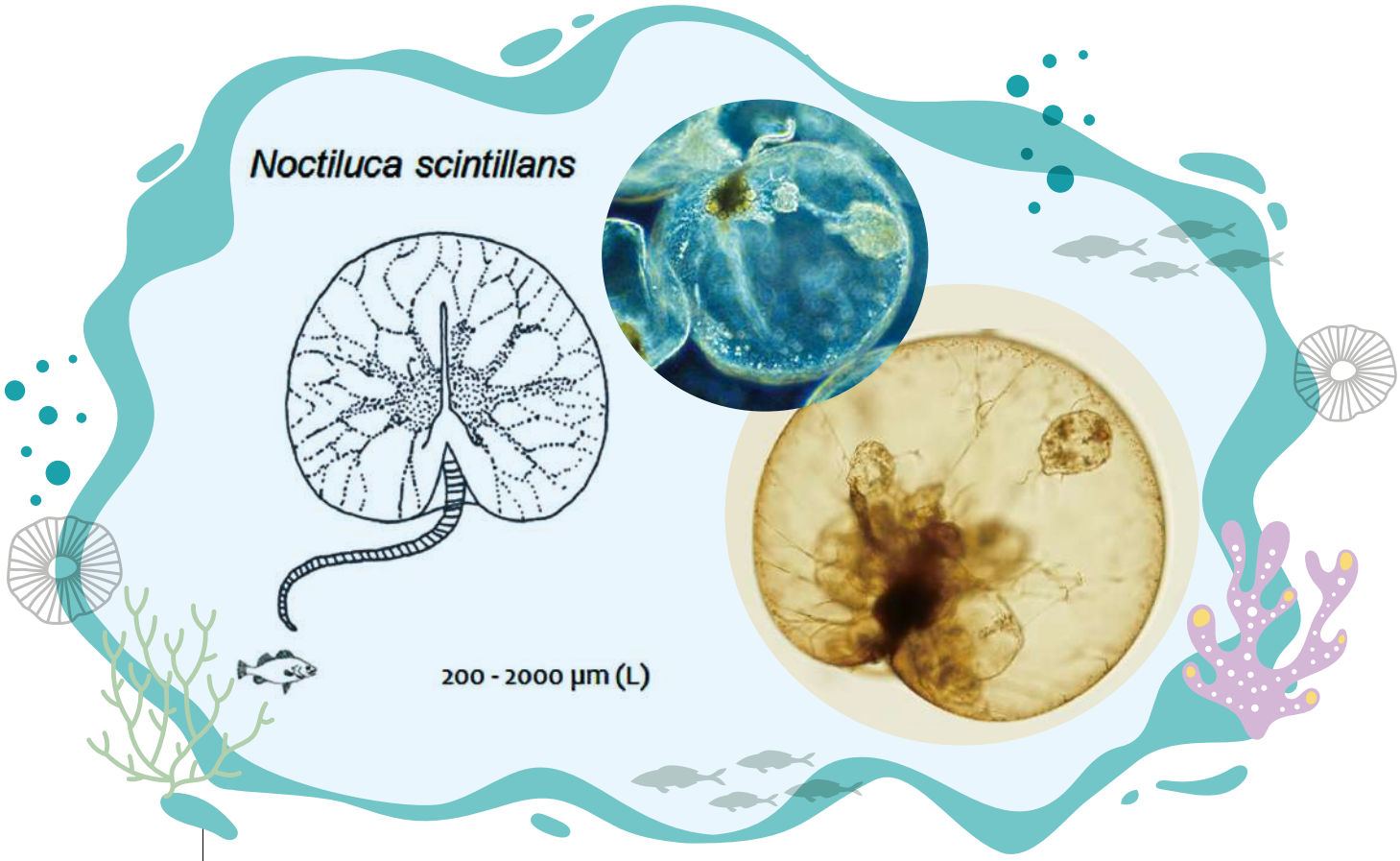
「馬祖藍眼淚」主要是由夜光蟲所造成。夜光蟲分類上屬於異營性渦鞭毛藻或雙鞭毛藻，為一種不具有色素、不行光合作用之赤潮（red tide）生物，全世界不同海域的夜光蟲均屬於同種生物。

馬祖列島濱臨福建省閩江口外，其海洋環境主要受到閩江影響，夜光蟲大量出現與閩江有密切關係。每年 4 月到 6 月底為閩江豐水期，此時閩江水帶入豐富之陸源性無機營養鹽，特別是矽酸鹽進入馬祖周遭水域，這些營養鹽造成矽藻大量快速成長，而這些矽藻為夜光蟲主要餌料，豐富之餌料引發夜光蟲成長形成「藻華」現象（指微細藻類短期間大量增加的狀態）。當豐水期結束，河水注入減少，帶入營養鹽也跟著減少，矽藻成長因此受到限制，連帶造成夜光蟲餌料不足，成長受到抑制，所以也跟著自然消失。

以下針對一直被大眾混淆的幾個問題進行解說：

1. 夜光蟲是藻還是蟲？

生物分類已經跳脫以往以營養方式簡單分為自營（光合作用，將無機物變成有機物）與異營（攝食，攝食有機物呼吸作用變成有機物）之二分法。目前分類較常使用為五界說，將單細胞（2 界）與多細胞（3 界）分開，在單細胞生物中再分為如細菌細胞般之原始構造的「原核單細胞生物界」及如高等生細胞般的「真核單細胞生物界」，以夜光蟲分類所屬之渦鞭毛藻來說，屬於真核單細胞生物。渦鞭毛藻有一半具色素能行光合作用，有一半不具色素需靠攝食行異營生活。然而，夜光蟲雖然分類屬於渦鞭毛藻，但它不具色素、無法行光合作用，靠攝食行異營生活。所



夜光蟲細胞呈透明球形，腹面有一縱溝，在此形成口部，口部之前有一小鞭毛，鞭毛前有一大觸手，觸手上具有黏膜，用來抓取食物；其無游泳運動能力，但可藉由浮力在水表層生活。（Photo Credit: GTM NERR, https://www.flickr.com/photos/gtmnerr/24485415252; Maria Antonia Sampayo, https://commons.wikimedia.org/wiki/File:Noctiluca_scintillans_varias.jpg; FWC Fish and Wildlife Research Institute, https://www.flickr.com/photos/myfwc/5808181396）

以不應該單純憑藉「藻」此一名詞，對其生態行為有錯誤之想像。

夜光蟲細胞呈透明球形，直徑 200 ～ 2000µm。腹面後端有一凹下縱溝，在此形成口部，口部之前有一小鞭毛，鞭毛前有一大觸手，觸手上具有黏膜。觸手用來抓取食物，再將食物送入口部並在體內形成食泡，食泡會分泌消化酶，食物在其內進行消化。夜光蟲雖然缺乏游泳運動能力，但可藉由浮力在水表層生活。其攝食餌料範圍非常寬廣，由細菌到魚卵或仔稚魚。早期研究認為其非常貪吃，遇到什麼吃什麼，不具餌料選擇性，但目前了解比較愛吃矽藻與綠藻。

2. 藍眼淚是否只有馬祖有？

首先「藍眼淚」名稱是由何而來，一直沒有可靠的說法，依據筆者在網路搜尋了解，「藍眼淚」最初出現於 2012 年 5 月網友臉書票選結果，該票選活動也曾被馬祖日報和國語日報報導。但事實上「藍眼淚」並未列入此次票選名單，可是不在名單中的「藍眼淚」後來卻因網友大量使用而異軍突起、聲名大噪。所以，「藍眼淚」是網友創造出來的名稱。從此網路上認定的「藍眼淚」就是指在馬祖附近海域，因夜光蟲大規模發光，使海面呈現藍色螢光幻影的現象。

藍眼淚不是只有馬祖有，比利時港口城市澤布呂赫的碼頭也有發現夜光藻的發光現象。（Photo Credit: Hans Hillewaert, https://commons.wikimedia.org/w/index.php?curid=10711494）

夜光蟲發光的現象存在於許多熱帶與副熱帶富營養鹽之沿岸水域，但只有馬祖稱此種現象為「藍眼淚」。（圖片來源：左邊口袋，https://www.flickr.com/photos/94035812@N04/17422747483）

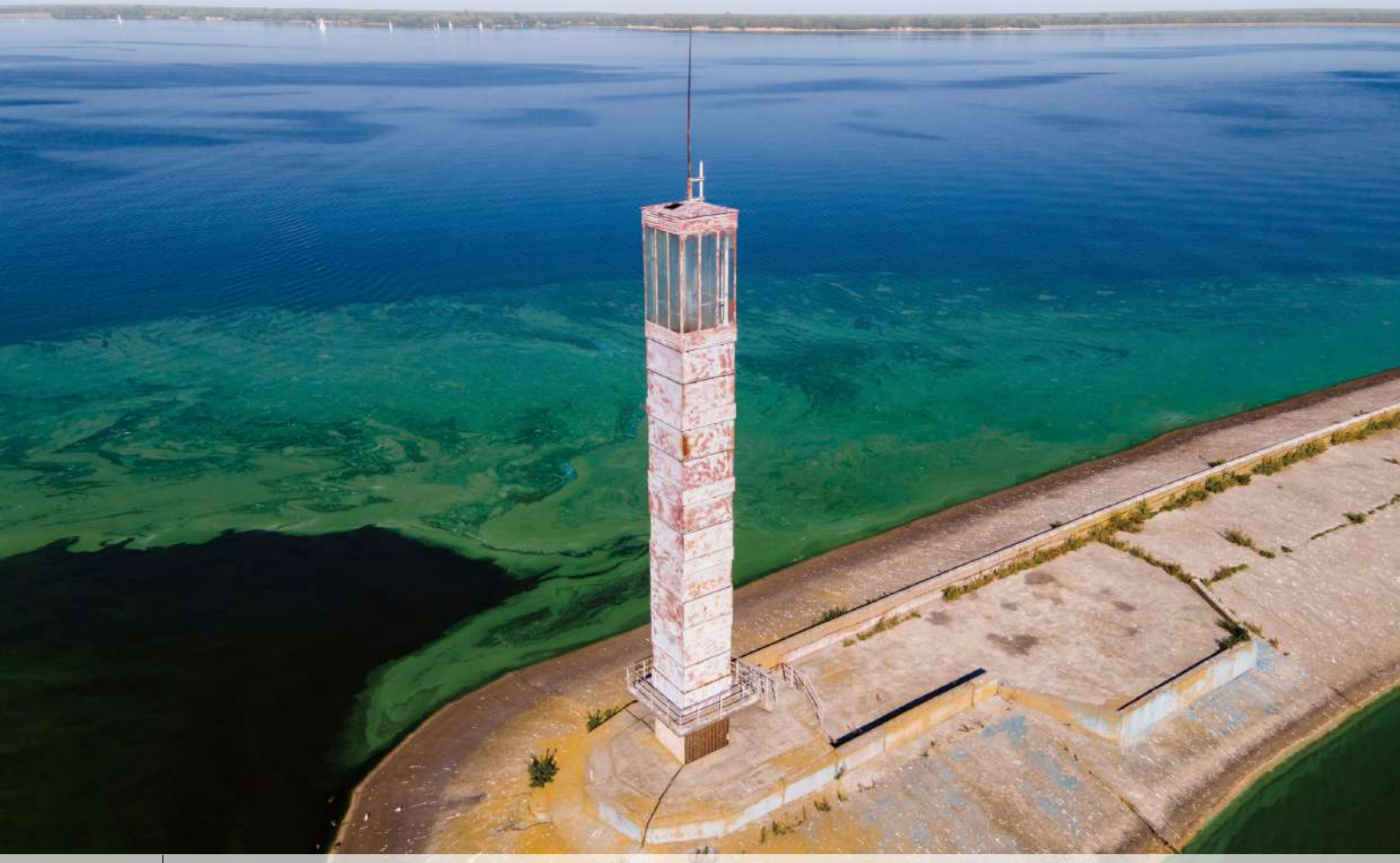
在生物界的分類上，全世界夜光蟲只有一種，但依其體內是否有共生藻分為兩群，一為體內不存在共生藻的紅夜光蟲，馬祖發現之夜光蟲屬於此類。另一種為具有共生綠藻（Protoeuglena noctilucae）的綠夜光蟲，其營養來自攝食及共生藻光合作用所提供的能量。除此兩種之外，在美國西岸加州洋流水域存在一種不發生物冷光之特殊夜光蟲。

紅、綠兩種夜光蟲分布區域不同，紅夜光蟲廣泛分布在溫帶與副熱帶沿岸海域，一般產生在鹽分較低，以矽藻為主之高基礎生產力水域，分布海域溫度由10℃～25℃。綠夜光蟲侷限於水溫25℃～30℃的南亞熱帶海域，包括孟加拉灣、阿拉伯海和紅海。綠夜光蟲體內共生綠藻推估產生於13億年前地球剛形成時期，此時海洋中溶氧量遠遠低於目前海洋，屬於低氧狀態，造就綠夜光蟲可以藉共生綠藻適應此種低氧環境，適合生長在其他生物無法成長之低氧狀態，所以許多比較高汙染之水域容易發現綠夜光藻的存在。

對於「藍眼淚」是否只有馬祖有？此一問題應該說夜光蟲發光現象存在於許多熱帶與副熱帶富營養鹽之沿岸水域，但它們都不叫做「藍眼淚」，只有馬祖稱此種現象為「藍眼淚」，所以夜光蟲發光之此種自然現象到處都有，但「藍眼淚」一詞僅存在於馬祖。

3. 夜光蟲是否為破壞環境之有害藻華生物？

一般有害「藻華」生物，造成環境危害最主要有兩個原因，一為生物本身會排放有毒物質，一為「藻華」結束後，因為細菌大量分解死亡藻類，耗盡水中氧氣，造成魚類因缺氧而大量死亡。「馬祖藍眼淚」為夜光蟲所形成，夜光蟲為無毒渦鞭毛藻，所以不會產生任何有毒物質。其次，馬祖夜光蟲「藻華」是矽藻刺激誘發所造成，當矽藻被攝食耗盡後，夜光蟲也跟著消失，目前為止也未發現夜光蟲「藻華」結束後，魚類缺氧死亡之現象。最後需特別強調的是，矽酸鹽是造成馬祖海域矽藻「藻華」最主要原因，矽之主要來源為陸上砂石，砂石中矽酸鹽溶入河水，最後被帶入海洋，所以矽酸鹽基本上與都市生活廢水或農業施肥無關。馬祖是一個富營養河口生態系的地區，發現夜光蟲出現或形成「藻華」為一正常海洋生態現象，不能以出現夜光蟲即將其視為海洋環境、生態惡化的指標。



藻華現象涉及到的藻類有綠藻或矽藻等，自然形成的藻華現象很快就會消失，並不會為環境帶來影響。

桃山神木

◆ 文字、攝影／行政院農業委員會林業試驗所 — 徐嘉君

桃山神木是一株樹高 79.1 公尺的臺灣杉，目前是臺灣島上（也是東亞）的樹高冠軍，2019 年底我們在光達圖像上看到它，離百岳桃山的直線距離 3 公里，垂直落差 1,300 公尺。

看似容易抵達，結果「找樹的人」團隊花了半年時間、共 3 次探勘才找到它，第 4 次出隊才成功測量樹高，桃山神木生長在避風平坦的肥沃谷地之中，應該再幾十年就可以突破 80 公尺紀錄了吧！（祈）

大城小麥新故鄉

◆ 文化工作者 — 周　朝

每到小麥成熟季節，在彰化縣大城鄉的小麥田，飽滿的金黃麥穗隨風搖曳起舞，此起彼落的金黃麥浪，美得如詩如畫。現今在政府和民間配合下，已透過金黃小麥，讓更多人認識大城鄉。

彰化大城—小麥新故鄉

50 年前，彰化縣濱海的大城鄉，曾經是栽種面積為全臺之冠的小麥產地。每年冬季水稻收割後的休耕期間，沿海地區農田都種滿小麥。當農曆春節過後，農家利用收成的小麥加工，製作手工「麥仔餅」，是老一輩人都會的絕活，後來，在外國廉價麵粉進口後，小麥逐漸走入人們的回憶。

回首從前，大城人決定找回過往輝煌的歲月，開始採用友善環境耕作方式播種小麥，很幸運地，獲得很好的成績。連農委會都讚嘆，大城鄉是全臺灣最適合栽種小麥的地方，不僅與自然生態和諧共存，為下一代留下乾淨無汙染的土地，且能把舊昔的記憶找回來，讓好久不見的綠繡眼、青蛙、鵪鶉，都逐一出現身影！

小麥植株特點

小麥原本是溫帶地區的栽培作物，由於臺灣是亞熱帶國家，理論上，是不太適合種植小麥，但由於臺灣早期種小麥是拿來釀酒用，所以不以小麥筋性高低為目的來選種，而是選擇容易栽種、抗病力佳、高產量的品種。

過去每當農曆春節過後，農家利用收成的小麥加工，製作麥仔餅（麥仔煎），是老一輩人都會的絕活。
（圖片來源：嘉義市政府，https://www.chiayi.gov.tw/News_Content.aspx?n=455&s=366144）

1950 年代，臺灣接受美國援助麵粉，開始推廣「麵食運動」。（圖片來源：國家發展委員會檔案管理局，國家檔案精選照片，https://www.archives.gov.tw/NationArc/NationalArcImageDep.aspx?cnid=1456）

早年臺灣種小麥的另外目的是為了對抗病蟲害，因為與水稻輪作，病蟲在頻繁更動的環境中會適應不良，就是「一直換門牌號碼，讓仇家找不到的概念」，能降低農藥使用量，並減少對環境的破壞。

美援改變臺灣人的飲食習慣

臺灣種植小麥的歷史，可溯源自日治大正時期（約1912年）開始有大規模種植，惟總生產量低於 1 千公噸。二戰結束後，臺灣出現短期糧食不足，政府鼓勵農民廣泛種植雜作，使小麥成為重要作物。

1949 年，麵食文化由大陸移民傳入臺灣。1954 年，挾美援之勢，臺灣接受美國援助麵粉，開始推廣「麵食運動」。嗣後政府為將價格較高的稻米銷售日本，爭取外匯，而成立「麵食推廣委員會」，國人漸漸習慣食用麵食，所以，小麥製品躍升為臺灣人的第二主食。1960 年代，本土小麥栽培來到史上最高峰。之後美國糧食過剩，低價小麥大舉銷臺，本土小麥種植面積一路下滑，從此一蹶不振。

保住小麥命脈的金門高粱酒

小麥為紹興酒釀造之成分，因兩蔣緣故，紹興酒深受當時黨政軍高層喜愛，讓 1980 年代本土小麥種植曾短暫回春，最盛況時期，年銷量甚至可以超過 2 百萬打。然 1995 年政府開放酒類進口，本土酒不敵進口酒，農友紛紛轉種其他作物，小麥幾乎休耕。

金門高粱酒向來遠近馳名，然金門當地缺乏足夠小麥種籽可供製麴，因此 1997 年，政府讓停耕的小麥恢復種植，並以契作保價收購臺中大雅小麥給金門酒廠。經數年研發，金門酒廠推出從製麴到釀製均為 100% 國產、全球第一且以臺灣小麥為唯一原料的「金門純麥酒」，其酒體純淨、入口清爽又帶有糧香，可謂是延續小麥新生命的臺灣之光。建議民眾如需喝酒，請多喝正港本土精心釀造酒，讓臺灣更好！

金門酒廠推出從製麴到釀製均為國產，且以臺灣小麥為唯一原料的「金門純麥酒」。（圖片來源：行政院農業委員會，https://www.coa.gov.tw/theme_data.php?theme=photo_news&id=790）

海口小鎮重返麥鄉之路

大城鄉位在彰化縣西南角，處濁水溪出海口北岸，西鄰臺灣海峽。由於大城鄉位於「風頭水尾」地帶，每年秋冬時節，東北季風狂颳強勁，因此，有很多人口外移，留下來的，大都是不捨家鄉的老人家。

鑒於國內小麥 99% 仰賴進口，加上歐美國家生產的是基改小麥，恐對人體健康有不良影響。大城地方人士自 2011 年送走國光石化後，便決定將先民在日治時期及戰後初期，種植小麥的榮光回憶找回來。之後，鄉民們胼手胝足、努力耕耘，於 2014 年，大城鄉種植小麥的面積竟超越臺中大雅，儼然成為臺灣小麥新故鄉。

吃在地、吃當季　就能救環境

小麥除能供作各式各樣麵類原料，亦可作醬油、醋及酒麴原料等，其副產品麥麩可作為家禽飼料。另外，小麥苗榨汁及胚芽更為近年流行之健康食品。因此，小麥是臺灣現階段應該特別重視培栽之作物。

「吃在地、吃當季」，是愛護地球的最佳表現。比如現在盛產蓮霧，就好好地去吃蓮霧，能補貼農民收入，對環境也有幫助。如果去吃進口舶來品，運送時消耗

大城鄉採用友善環境耕作方式播種小麥。

陣陣北風吹拂下形成的麥浪。

大量石化能源，會造成暖化問題。同樣道理，吃非當季水果，除營養成分恐流失外，水果冰在冰箱，亦得消耗不少能源來保存。

大城鄉的農田，藉水圳導引濁水溪灌溉。由於濁水溪水挾帶厚重的淤泥，含有豐富的有機質，土壤十分肥沃，是上天賜予作物的最好禮物，這亦是「濁水溪米」品質冠全臺的主要因素，溪水也為小麥提供最佳的天然有機肥。另外大城半砂土的土壤，排水性佳，十分適合耐旱的小麥種植。此外，秋冬季節的強勁東北季風，雖不利於稻米生長，然對小麥卻是利多，因為小麥不怕風，強勁的風勢，還能讓害蟲無法侵害，是最自然的「驅蟲良方」，因此，大城鄉小麥成為無毒農作。

黃金麥浪節　邀請大家一起來同樂

每年元宵節前後，是小麥成熟收割的季節，視野遼闊的小麥產區，黃金麥田耀眼璀璨，尤其於黃昏夕照時刻，在陣陣北風吹拂下，金黃波浪翩翩起舞，壯觀景象令人心曠神怡。

為迎接大片黃金麥浪，大城鄉公所每年都會舉辦「黃金麥浪節」，讓民眾得以一覽麥田風光，並認識臺灣本土小麥產業，現場也準備小麥麵包供遊客品嚐，適合闔家大小前來同樂。

黃金麥田的美麗景象。

活動現場烘焙的小麥麵包。

（本文圖片除標示來源者外，其餘皆由作者提供。）

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**

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=88&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：

☐ 5G 網路引爆萬物互聯　☐ 放眼國際　☐ 生活中的資安

☐ 風險管理歷史課　☐ 人生戲院　☐ 懷舊行旅

☐ 聽那山林裡的傳唱　☐ 看那藍色大海　☐ 絕美臺灣　☐飲膳札記

☐ 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	23149 新北市新店區中華路 74 號	（02）29177777 （02）29188888（傳真）
臺北市調查處	10675 臺北市大安區基隆路二段 176 號	（02）27328888
新北市調查處	22066 新北市板橋區漢生東路 193 巷 2 號	（02）29628888
桃園市調查處	33053 桃園市桃園區縣府路 19 號	（03）3328888
臺中市調查處	40358 臺中市西區英才路 525 號	（04）23038888
臺南市調查處	70848 臺南市永華路二段 208 號	（06）2988888
高雄市調查處	80143 高雄市前金區成功一路 428 號	（07）2818888
航業調查處	43541 臺中市梧棲區臨港路四段 390 號	（04）26560555
福建省調查處	89346 金門縣金城鎮西海路一段 65 號	（082）322888
基隆市調查站	20151 基隆市崇法街 220 號	（02）24668888
宜蘭縣調查站	26053 宜蘭市津梅路 52 號	（03）9288888
新竹市調查站	30056 新竹市經國路三段 126 號	（03）5388888
新竹縣調查站	30295 新竹縣竹北市光明五街 56 號	（03）5558888
苗栗縣調查站	36057 苗栗市玉清路 382 號	（037）358888
南投縣調查站	54058 南投市民族路 486 號	（049）2228888
彰化縣調查站	50074 彰化市卦山路 12 號	（04）7248888
雲林縣調查站	64072 雲林縣斗六市鎮南路 67 號	（05）5328888
嘉義市調查站	60049 嘉義市東區維新路 321 號	（05）2778888
嘉義縣調查站	61363 嘉義縣朴子市朴子一路 1 號	（05）3628888
屏東縣調查站	90087 屏東市合作街 51 號	（08）7368888
花蓮縣調查站	97061 花蓮市中美路 3-33 號	（03）8338888
臺東縣調查站	95065 臺東市中興路二段 731 號	（089）236180
澎湖縣調查站	88050 澎湖縣馬公市新明路 77 號	（06）9278888
馬祖調查站	20941 連江縣南竿鄉介壽村 15 號	（0836）22258
北部地區機動工作站	23558 新北市中和區永和路 33 號	（02）22482626
中部地區機動工作站	40764 臺中市西屯區福順路 500 號	（04）24615588
南部地區機動工作站	81242 高雄市小港區平和南路 129 號	（07）8122910
東部地區機動工作站	97058 花蓮市瑞美路 7 號	（03）823-3712
國家安全維護工作站	23151 新北市新店區中生路 40 號	（02）22177211
航業調查處基隆站	20248 基隆市中正區中正路 303 號	（02）24633633
航業調查處高雄站	80666 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

320 國際幸福日

——讓我們在一起

幸福

International Day of Happiness

20 March —— Happiness For All, Together

什麼是國際幸福日？

2012 年 6 月 28 日聯合國通過決議，將每年的 3 月 20 日訂為「國際幸福日（International Day of Happiness）」。國際幸福日的標誌「Helios（在希臘語中的涵義為太陽）」，象徵著每個人都有帶給世界各地人們幸福的無限潛能。