其他論述

DOI:10.6237/NPJ.202002_54(1).0008

論社群媒體的安全議題及因應之道

劉宗翰　少校

提　　要：

一、我國有八成人口數為社群媒體使用者，社群媒體除了成為大眾上網的一部分外，還成為傳播訊息的最佳管道，然其中的假新聞除了影響人們的認知與立場外，其影響力也擴及至政治與軍事安全層面，相關案例時有所聞，儼然形成一種非傳統安全議題，值得有關單位引以為鑑、及早因應。

二、社群媒體目前已開始與深度偽造、人工智慧等新興科技進行結合，導致「眼見不一定為憑」，若遭到有心人士濫用，勢必造成負面效應，因此相關科技的後續發展，殊值關注。

三、社群媒體的善惡是一體兩面，目前看來是接近「與惡的距離」，本文也提出一些因應之道，希望提供防治單位參考；至於視聽大眾則應建立對不實訊息「拒看、拒聽、拒點閱」的素養，同時也應培養檢視不同觀點的能力，避免陷入認知錯誤的陷阱之中。

關鍵詞：社群媒體、假新聞、深度偽造、政治安全、軍事安全。

壹、前言

當前是網路普及化與幾乎人手一支智慧型手機的世界。根據聯合國「國際電信聯盟」(International Telecommunication Union，ITU)估計，2019年全球網路使用者將超過全球總人口數的一半，對比十年前，則僅有約二成人口連網[1]，不可同日而語；另全球也超過三分之二人口數至少擁有一臺行動裝置，行動網路的普及率逾六成五，而上網人口數平均一天連網時間已達6小時[2]，且行動裝置的網路用戶數也在2014年初時首度超過個人電腦[3]。在這種現象下，社群媒體平臺逐漸成為大眾上網的一部分，也成為人們傳播資訊的常用管道；不同類型的平臺，有其不同的特色及功能(如表一)，且我國

註1：The World in 2019: Closing the 'Digital Divide' in 2019, The Economist, https://worldin2019.economist.com/，檢索日期：2019年10月13日。

註2：We Are Social and Hootsuite, Digital in 2018: World's Internet Users Pass the 4 Billion Mark, January 30, 2018, https://wearesocial.com/blog/2018/01/global-digital-report-2018，檢索日期：2019年10月13日。

註3：Rebecca Murtagh, "Mobile Now Exceeds PC: The Biggest Shift Since the Internet Began," July 8, 2014, Search Engine Watch, https://searchenginewatch.com/sew/opinion/2353616/mobile-now-exceeds-pc-the-biggest-shift-since-the-internet-began，檢索日期：2019年10月13日。

表一：各社群功能與媒體種類

功能	社群種類	備考
發布貼文與動態	臉書(Facebook)、Instagram、QQ空間(QZone)、新浪微博(Weibo)、推特(Twitter)	受歡迎度由高至低依序為臉書、YouTube、WhatsApp、臉書Messenger、微信、Instagram、騰訊QQ、QQ空間、抖音、新浪微博、Reddit、推特、Line
影音娛樂平臺	YouTube、抖音(Tik Tok)	
聊天室	Line、臉書Messenger、微信(WeChat)、騰訊QQ、	
網路論壇	Reddit	

資料來源：Clement, "Global Social Networks Ranked by Number of User 2019," Statista, https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/，檢索日期：2019年10月13日。

有八成人口數為使用者[4]。

然而，在社群媒體上傳播資訊的行為，開始從善意的分享與交換資訊，逐漸遭有心人士濫用而變質，不實與錯誤訊息的假新聞事件層出不窮，甚至也影響到政治與軍事安全層面，成為政治利用的手段；另軍事資訊經由社群媒體洩露事件，也時有所聞。因此，本文先探討社群媒體產生的安全危機，接著探討政治與軍事安全層面的議題，以及新科技若遭濫用，將助長社群媒體的負面影響力，最後提出因應之道。此外，基於國軍官兵也是社群媒體的使用者，相關安全議題也不容忽視，唯有大家都瞭解這些安全警訊，才能進一步防範網路的安全漏洞，並管控部隊安全上的風險。

貳、社群媒體的正負評價

社群媒體的好與壞可說是一體兩面，其為人們帶來好處之餘，也引起一些負面影響，茲分述如下：

一、正面評價

(一)對軍事而言

1. 社群媒體平臺可提供軍事領導人、組織及個人一個資訊分享的機制，並能不受時間與地域限制，快速地觸及更廣泛的目標群眾，例如在現今的資訊環境中，人們往往會使用此平臺瀏覽新聞，因此軍方能適時用來發布及時與正確的新聞[5]。

2. 軍方可利用此一平臺進行資訊宣傳，而這將可節省紙本宣導資料與傳單的經費，而官兵使用者加入線上粉絲團也能主動獲得相關訊息[6]。

3. 社群媒體平臺可主動獲得直接快速的回饋，對於千禧世代的官兵(年齡介於18至25歲之間)而言，在平臺上留言表達己見是很平常的事，軍事幹部則可以從中獲得一些改進意見，進而調整現行政策不足之處[7]。

4. 社群媒體可以塑造軍人正面的形象，並訴說不為人知、犧牲奉獻的故事，像是人道援助的救災行動[8]。

(二)對政治而言

1. 善用社群媒體的政治人物，通常可打

註4：臺灣網路資訊中心，《2018臺灣網路報告》，2019年1月10日，頁3。
註5：Ryan G. Walinski, The U.S. Military and Social Media (Maxwell Air Force Base, Alabama, 2015), pp.15-16。
註6：Ibid。
註7：Ibid。
註8：Ibid。

一場漂亮選戰。2008年美國前總統歐巴馬在「推特」(Twitter)成立不久的年代，就有12萬的追踪者；8年後，美國總統川普也常利用「推特」發布消息，行銷專家認為，「臉書」與「推特」等社交媒體對川普的勝選功不可沒[9]。川普曾接受美國「福斯財經新聞網」(FBN)訪問時表示。這樣他大可對他的追隨者有話直說，而不必理會媒體對他的不公平報導；許多共和黨領袖也要求川普避免或是減少推文，並承認有些朋友建議他不要使用社交媒體[10]。但根據「推特外交」(Twiplomacy)研究，川普擁有超過5,200萬的追隨者，榮登各國領袖推特人氣王[11]。

2.在我國的案例上，2014年11月臺北市長的選舉中，無黨派的政治素人柯文哲席捲85萬票，打敗政治世家的連勝文當上首都市長，這是歷任市長選舉第二高票，而他的成功公式是6億個讚+5人小組+1,400萬人次臉書用戶=85萬張白色力量[12]。社群媒體在其中扮演的關鍵角色不言可喻。目前網路聲量的大數據分析，也常被用來評估一位候選人的支持度，這種有別於一般傳統民調的作法，即是拜社群媒體盛行所賜；另當前火紅的「網紅政治」現象，也在社交平臺盛行，這也將政治傳播與選舉形式帶往另一種新型態[13]。

二、負面評價

(一)對人們身心的影響

1.過度使用社群媒體的人，將有可能引起心理健康的問題，尤其在年輕人身上特別明顯，因為他們通常是社群媒體的愛好者。研究指出，目前社群媒體使用會對少數人產生包含焦慮、失落、孤獨、注意力不足及成癮等心理問題，所幸並未對大多數人產生心理影響[14]。不過，使用習慣確已帶來不良影響，像在餐桌上不見寒暄交流，只見人們爭相拍攝美食、上傳打卡；大眾運輸上的乘客也大多忙著滑手機，沉浸在自己的世界，這種顧著滑手機卻忽略他人動作的現象，也稱為「低頭族」(Phubber)[15]。此外，還有一種「錯失恐懼症」(Fear of Missing out，FOMO)，係看到別人不停更新動態、討論時下最熱門的事物，以及廣為流傳的網路文章、影片或照片，深怕自己沒跟上流行腳步，導致自己無時無刻都在點閱手機上的資訊[16]。

註9：陳曉莉，〈川普勝選，臉書與推特助攻？〉，iThome，2016年11月10日，https://www.ithome.com.tw/news/109533，檢索日期：2019年10月14日。

註10：〈94要用推特！川普：沒有推特就沒法贏得白宮〉，自由時報電子報，2017年10月22日，https://news.ltn.com.tw/news/world/breakingnews/2230078，檢索日期：2019年10月14日。

註11：〈逾5,200萬追隨者，川普是推特人氣最高領袖〉，TVBS新聞，2018年7月10日，https://news.tvbs.com.tw/fun/953311，檢索日期：2019年10月15日。

註12：謝明瑞，〈大數據分析：以柯P現象為例〉，國家政策研究基金會，2015年2月26日，https://www.npf.org.tw/2/14788，檢索日期：2019年10月15日。

註13：蔡孟軒，〈臺灣政界漸趨網紅政治化〉，中時電子報，2019年2月24日，https://www.chinatimes.com/newspapers/20190224000189-260301?chdtv，檢索日期：2019年10月15日。

註14：Daria J. Kuss and Mark D. Griffiths, “Social Networking Sites and Addiction: Ten Lessons Learned,” International Journal of Environmental Research and Public Health, Vol. 14 Iss. 3, March 2017, p. 311.

註15：希平方，〈你每天都在做這件事！phubbing這個字是什麼意思？〉，《商業周刊》，2014年8月27日，https://www.businessweekly.com.tw/article.aspx?id=9071&type=Blog，檢索日期：2019年10月16日。

註16：〈FOMO：臉書時代心理現象〉，中央通訊社，2012年10月30日，https://www.cna.com.tw/topic/newsworld/27/201210300004.aspx，檢索日期：2019年10月16日。

2.網路的霸凌也常出現在社群媒體中，常見作法是在社群互動中運用惡毒言語或圖像，反覆威脅、凌辱、攻擊他人。由於它比當面霸凌的行為更容易執行，且傷害經常比當面更大，造成受害者身心重創或是在逼迫下導致自我傷害[17]。更有些青少年會藉由社群網站，排擠特定某人，使之覺得沒有存在感，這也是另一種型態的網路霸凌[18]。

(二)成為假新聞的溫床

1.由於網路已成為資訊的大平臺，每個人都可以上網找到各種所需資訊，也因為網路的高覆蓋率與智慧手機的普及，使得大眾對網路的黏著度提高，而時常使用網路的人往往都是社群媒體的愛好者，也常在社交網站上點閱朋友圈所傳的新聞。然而，「假新聞」卻將之帶往「惡」的方向，尤其是在選舉活動之前，假新聞更是呈顯著攀升。中文的「假新聞」相對應的英文為「Fake News」，其所指涉的不實訊息，包括網路流傳的錯誤資訊與媒體組織的錯誤報導，該名詞雖然廣泛被人使用，但因為其涵義被賦予多重色彩，其實並無法反映假新聞的複雜性，因此有些國外學者進一步區分「Misinformation」為非故意型態的假新聞(可譯為錯誤訊息)，而「Disinformation」為蓄意製造與傳播假新聞(可譯為虛假訊息)[19]。因此，在惡意造謠與無心推手兩相結合所造成的「資訊共伴效應」下，社群媒體時代的假新聞往往更容易發生[20]。由於人的認知模式本來就容易受到新奇消息吸引而落入陷阱，因此在看到多人按讚與轉傳的資訊，就容易信以為真，失去判斷力。此外，人天生的認知缺陷也會導致「逆火效應」(Backfire Effect)：即使假訊息被澄清了，但人們並不會因為訊息更正而改變原有看法，特別是對於該議題抱持堅定立場的人，更正訊息不但無助於減弱其錯誤認知，甚至在某些情況下還會強化其錯誤認知[21]。

2.假新聞氾濫的原因，除了個人無意間的轉傳外，媒體從業者的亂象也是主要因素之一。近幾年主流媒體流行做「即時新聞」，快是第一要求，查證的新聞倫理往往被擺在一旁，反正發現有誤，再更正即可；但更正的新聞往往沒什麼人看到，或者人數遠小於看到錯誤新聞的讀者。況且，加上靠收視率和點閱率賺廣告費老闆們的不重視，所以這種亂象是難以消失的[22]。假新聞也與人力有關，畢竟記者數量有限，在網路媒體的時代，時間是關鍵，某位記者曾無奈表示，「只要一家媒體有，大家都會抄，每人每天要

註17：游梓翔(教授)，〈小心臉書上的四大惡人〉，《臺灣立報》，2017年5月1日，http://www.limedia.tw/comm/1054/，檢索日期：2019年10月17日。

註18：陳和琳，〈用社群網站孤立同儕，新型態「網路霸凌」〉，TVBS新聞，2015年10月6日，https://news.tvbs.com.tw/life/620329，檢索日期：2019年10月17日。

註19：Claire Wardle, “Fake News It’s Complicated,” First Draft, February 17, 2017, https://medium.com/1st-draft/fake-news-its-complicated-d0f773766c79，檢索日期：2019年10月18日。

註20：黃哲斌，《新聞不死，只是很喘：媒體數位轉型的中年危機》(臺北：天下雜誌，2019年3月)。

註21：胡元輝(教授)，〈克服認知缺陷，終結假訊息氾濫〉，《青年日報》，版11。

註22：關魚，〈臺灣假新聞越來越多的祕辛〉，公民行動影音紀錄資料庫，2015年2月6日，https://www.civilmedia.tw/archives/27216，檢索日期：2019年10月19日。

產生5、6則新聞、每月流量要32萬，每個人都在拚達標！」實難有充足時間查證資訊來源與正確性[23]。根據臺灣大學新聞研究所王泰俐教授指出，假新聞的來源可歸納為六類：第一是內容農場(Content Farm)[24]；第二是直接引用或再製其他媒體內容的網站，如雅虎、臉書、Line Today；第三是網路論壇，如PTT論壇；第四是政治諷刺性或批評性網站，如「卡提諾狂新聞」；第五是針對各式各樣議題，做出違背正統民調方式的民調；第六是特定名嘴[25]。因此假新聞通常夾雜在眾多真新聞之中，來源複雜，一不留意就會上當。

根據「民主指標研究」(Varieties of Democracy)近期釋出第九版資料庫的調查顯示，2018年在「遭受外國假消息攻擊」方面，我國是最嚴重的國家，自2013年就開始位居榜首，其次為拉脫維亞、巴林、卡達、匈牙利等國[26]。值得注意的是，假消息同時也會排擠真消息的存在與被信任度，甚至影響人對一件事物的認知，不可不慎。

(三)社群媒體營造回音室效應

1.「回音室效應」(Echo Chamber Effect，又稱同溫層效應)與「過濾泡泡」(Filter Bubble)也是社群媒體的負面效應，前者是比擬身處在回音室般，周遭意見都是與自己相類似的觀點；後者是將不同意見過濾在外，每個群體或個人活在自己的泡泡之中[27]。此二種現象儘管成因不盡相同，但共同結果是用戶沉浸在一個同質性非常高的內容群組中，甚至誤認為這就是社會上的主流意見[28]；此外，當新聞媒體抱持特定立場，很容易就會尋求迎合己方立場的資訊，反而忽略相反立場的蛛絲馬跡。像在2016年川普當選總統後，美國媒體圈就自我批判，認為位於東、西岸大城市的主流媒體，困在自我感覺良好的回音室裡，輕忽另一半美國人的不滿聲浪，因而誤判川普崛起的社會因素。

2.大數據演算法也強化了上述的效應，社群媒體網站紀錄了用戶的使用歷程，諸如瀏覽、按讚、分享、互動等，並利用演算法，依據使用者偏好傳送相關消息，完全阻隔無興趣與負面的訊息，一旦長時間處於認知制約的氛圍下，使用者會封閉在特定社群網站內，一旦跨出認知舒適圈，自然會產生認知衝突[29]。更令人擔憂的是，「大數據在看著你」並非未來式，而是現在進行式；諸如臉書與劍橋分析公司(Cambridge Analyti-

註23：林倖妃、伍芬婕，〈拆解內容製造生態鏈：一條假新聞背後，無奈的記者〉，《天下雜誌》，第671期，2019年4月23日，https://www.cw.com.tw/article/article.action?id=5094847，檢索日期：2019年10月19日。

註24：內容農場係指一個線上網站為了取得網路流量或影響力，而以各種合法、非法手段大量快速產生品質不良或有誤的文章。換言之，內容農場是所謂的內容分享平臺，圈養一些真假難辨，或是吸引網友點閱的內容，透過網站中所張貼的圖文點擊數，可衝流量獲取廣告利益。

註25：同註23。

註26：〈瑞典最新調查資料：臺灣受假新聞危害程度世界第一〉，自由時報電子報，2019年4月10日，https://news.ltn.com.tw/news/world/breakingnews/2754163，檢索日期：2019年10月20日。

註27：胡全威(副教授)，〈聆聽對方：同溫層效應的解藥〉，立報傳媒，2018年6月27日，https://www.limedia.tw/edu/688/，檢索日期：2019年10月21日。

註28：鄭宇君(助理教授)，〈是臉書決定動態牆內容，還是我們自己？〉，《科學月刊》，2015年8月號，https://pansci.asia/archives/85603，檢索日期：2019年10月22日。

註29：吳旻純，〈Seeing is Believing:「同溫層效應」〉，《清流雙月刊》，第20期，2019年3月，頁26。

ca)發生的洩密醜聞、中國大陸「社會信用」體系建設等都僅是大數據與人類隱私的衝突案例之一，真正原因在於當今社會已經被演算法包圍，數據、數學模型決定了人們臉書塗鴉牆優先出現誰的貼文、網頁看到什麼樣的廣告，人們發現數據愈來愈瞭解自己，知道個人的網路閱覽愛好，甚至是政治傾向[30]，這應該不是一件好事！

參、社群媒體對政治與軍事安全之影響

若從政治與軍事安全層面上解析，不難發現社群媒體的驚人影響力：

一、政治安全

(一)社群媒體雖然能協助政治候選人拉抬網路聲量與提升支持度，但也能成為抹黑與造謠的場所。2014年印度國會大選就有利用網路媒體和社群媒體操弄輿論的現象，5年後這個情況更加惡化，主要原因在於便宜的智慧型手機和網路行動數據，使得用戶數量遽增，5.6億人是臉書和旗下訊息平臺WhatsApp的最大市場，熱衷使用社交平臺的莫迪(Narendra Modi) 總理在推特上擁有4,600萬名粉絲，僅次於川普總統。2019年國會大選時，莫迪所屬的印度人民黨(BJP)與最大反對黨國民大會黨(INC)都力圖掌握多數席次，而大選也就成為假新聞的戰場，並利用社群媒體來相互對抗[31]。「臉書」網路安全政策負責人葛萊徹(Nathaniel Gleicher)曾表示，此一期間臉書已刪除和國大黨相關的687個臉書頁面和帳號，雖然散播假消息的幕後黑手利用假帳號來掩蓋其身分，但經審查後發現，這些帳號和國大黨有高度相關聯，當然臉書也撤除15個支持人民黨的粉專、社團和帳號，阻止抹黑反對黨的不實言論繼續散播[32]。

(二)政治人物也曾遭到抹黑，例如莫迪一支早期受訪影片遭到斷章取義，讓他看起來只有高中學歷，但他其實是政治學碩士；還有假新聞指聯合國教科文組織頒發「全球最優秀總理獎」給莫迪，事實是根本沒有這個獎項；前國大黨魁桑妮雅・甘地(Sonia Gandhi)也被誤傳她比英國女王還富有，雖然該指控在6年前就已被證明為不實，但大選中民眾依然熱烈轉發這項訊息，另有幾張穿著艷麗的照片遭指證，因此批評她道德低落，但事後證明與她毫無關係[33]。

(三)對心懷不軌的政治領導人而言，利用「網路誘餌與電腦自動程式」(Trolls and Bots)，或雇用專業人士以大量假帳號偽裝成一般用戶，已成為其塑造公眾言論風向的方法。俄羅斯特別擅長運用網路暴民與

註30：〈大數據在「看著你」〉，《多維TW》線上月刊，2018年，第35期，https://duoweicn.dwnews.com/TW-2018%E5%B9%B4035%E6%9C%9F/10007026.html，檢索日期：2019年10月23日。

註31：楊昭彥，〈印度馬拉松大選起跑 社群媒體假新聞陰影揮之不去〉，中央廣播電臺，2019年4月11日，https://www.rti.org.tw/news/view/id/2017355，檢索日期：2019年10月23日。

註32：陳苑婷，〈一個擁有5.6億網民的超級大國，打起選戰會是什麼樣子？莫迪粉絲數僅次川普，假新聞造成社會極化〉，風傳媒，2019年4月11日，https://www.storm.mg/article/1150836?srcid=73746f726d2e6d675f61616266383266343865343134316136_1559718437，檢索日期：2019年10月24日。

註33：洪培英，〈網軍來襲！印度大選假新聞氾濫，抹黑吹捧樣樣來〉，信傳媒，2019年4月24日，https://www.cmmedia.com.tw/home/articles/15271，檢索日期：2019年10月24日。

電腦自動程式的方法，結合不同來源的社群媒體，導致真相難明。因為，一方面資訊揭露是透過專業的網路攻擊與駭客行為，並經由像是「DC洩密」(DCLeaks)與「維基解密」(WikiLeaks)等網站平臺來公開不為人知的訊息；另一方面資訊又透過自家《RT臺》與《史普尼克新聞社》(Sputnik)傳達俄國觀點與論述[34]。此外，俄國還干預2016年的美國總統大選，「臉書」事後調查發現，期間確實有人花費10萬美元，利用近3,000則廣告與約470個假帳號及粉絲專頁，製造社會與政治分裂的內容，而帳號竟來自一個俄國境外的業者「巨魔工廠」(Troll Farm)，而該公司向來與莫斯科政府關係密切[35]。

(四)「阿拉伯之春」讓世人看到推翻極權政府的武器，不是槍砲彈藥，而是網路、智慧型手機及社群媒體平臺。2010年10月，突尼西亞一名青年攤販戲劇性地自殺，引爆該國「茉莉花」革命，這股力量也使阿拉伯世界的其他國家開啟追求民主浪潮。阿拉伯之春在埃及地區的重要推手，是谷歌中東及北非地區行銷經理戈寧(Wael Ghonim)，他表示在2011年時，自己匿名建立了一個臉書專頁，後來這個專頁引發了埃及革命，導致曾鐵腕統治埃及30年的穆巴拉克(Hosni Mubarak)被迫下臺。」由此可見，社群媒體是一把雙面刃。在之後的時間裡，埃及政治鬥爭愈演愈烈，而社群媒體卻只是放大言論、傳播錯誤的訊息、重複高喊口號及散播仇恨言論，在這種情況下，軍隊支持者和伊斯蘭教主義者逐漸兩極化，進而塑造一個容易讓人們產生這些行為的環境，並放大影響力[36]。

二、軍事安全

(一)社群媒體在軍中的使用率也逐漸普及，使用者通常會將自拍照、生活照或影片上傳分享至社群網站上，而配合自動定位系統或是打卡，這些內容能夠顯示出拍攝與上傳的地點。例如，俄羅斯軍人的貼文就曾洩漏俄國在烏克蘭和敘利亞軍事部署的位置；2014年也有位俄國軍人把在烏克蘭處理動亂中使用軍火的過程分享到社群網站上，後來被BBC的記者轉貼[37]。此外，國家的官媒報導也會基於自身立場，刻意洩漏對方的軍事資訊，例如2017年7月，在土耳其與北約成員國間緊張情勢升溫期間，土國媒體「安納杜魯新聞社」(Anadolu)竟公布美軍的秘密基地及在敘利亞的軍事據點，在這則新聞報導中同時也指出美軍與法國特種部隊的駐地[38]，這種報導透過社群媒體流傳，即對軍事層面造成一定程度的安全影響。

(二)受年輕人喜愛、全球每月活躍用戶數達5億的中國大陸手機影音APP「抖音」也

註34：Kim Taehwan, “Authoritarian Sharp Power: Comparing China and Russia,” The Asan Forum, June 18, 2018, http://www.theasanforum.org/authoritarian-sharp-power-comparing-china-and-russia/，檢索日期：2019年10月25日。

註35：〈臉書證實：俄買廣告搞分化干預美大選〉，自由時報電子報，2017年9月7日，https://news.ltn.com.tw/news/world/breakingnews/2186796，檢索日期：2019年10月25日。「巨魔工廠」是指專門在網路上散播不實言論的網路水軍，而Internet Research Agency被認為是俄羅斯最有組織的巨魔工廠。

註36：〈後悔用臉書發起「阿拉伯之春」？埃及革命推手：社群媒體讓世界更聳動、更一面倒……〉，《商業周刊》，2016年3月8日，https://www.businessweekly.com.tw/article.aspx?id=15837&type=Blog，檢索日期：2019年10月26日。

註37：王元容，〈防機密外洩，俄羅斯禁止軍人自拍上傳社群媒體〉，上報，2017年10月6日，https://www.upmedia.mg/news_info.php?SerialNo=26233，檢索日期：2019年10月26日。

註38：Leela Jacinto, “Turkey Leaks Secret Locations of US, French Troops in Syria,” France 24, July 20, 2017, https://www.france24.com/en/20170720-turkey-usa-military-leaks-french-troops-syria，檢索日期：2019年10月27日。

有安全疑慮。美國重要智庫彼得森國際經濟研究所(Peterson Institute for International Economics)的報告指出，「抖音」可能淪為中共的間諜工具，該APP會蒐集用戶的數據並傳回總部，中共能假藉協助蒐集情報為由，擷取數據並製作出辨識西方人臉孔的監控軟體，或蒐集西方軍事活動的情報，另外更有不少美國年輕軍人會穿著美軍軍服，用抖音上傳健身短片，而拍攝地點都在美國軍事設施內，因此有安全上的隱憂[39]。

(三)2011年美軍對賓拉登的秘密突擊行動，竟被一位住在巴基斯坦阿伯塔巴德(Abbottabad)的資訊顧問阿薩(Sohaib Athar)無意間在推特上進行直播，像是：「…現在是凌晨一點，發生直升機在阿伯塔巴德上空盤旋的罕見情形，我突然聽到一個爆炸聲響(其實是美軍直升機墜毀)，希望這不是一件麻煩事要來的預告…」。整個過程都被在阿薩推特上報導，同時吸引他推特上的朋友追踪，大家還在網路上相互討論。事後，美軍官員對外宣稱任務持續不到40分鐘，但阿薩卻公開表示在該事件發生後2小時都還有軍事部隊駐留[40]，明顯打臉美方的說法。社群媒體洩漏精心策劃的軍事行動事件，這是當初美軍始料未及的。

(四)川普在2018年12月閃電探訪駐伊拉克美軍，不過習慣推文的他卻不經意公布與美海豹部隊成員的合照，前海軍情報專家南斯(Malcolm Nance)就指出，在戰區執行任務的特種部隊成員，其姓名、面貌與身分都應受到保密，若讓這些人曝光，恐怕會被敵對政府與恐怖分子盯上[41]，這肯定是生死攸關的大事。而一款跑步使用的Strava APP，由於能顯示用戶在運動時的路徑或稱之為熱圖(Heat Map)，導致一些軍事基地位置遭到曝光，雖然某些基地靠著衛星地圖就可以看到，但令人擔憂之處是它能顯示人員的活動狀況，而基地外的運動軌跡紀錄，可能洩露人員常使用的路線或巡邏道路[42]。值得注意的是，雖然使用者只是單純要上傳並與人分享運動成果，但這種會顯示資訊點的APP運動程式，相關資訊將可能遭有心人士利用。

三、眞實的案例

(一)利用社群媒體發動戰爭早已開始，最知名案例莫過於伊斯蘭國恐怖組織(Islamic State of Iraq and al-Sham，ISIS)。ISIS趁著2014年敘利亞內戰和伊拉克內亂動盪之際，占領兩國一大片的土地，並在一個相當於英國領土大小的地域上成立哈里發帝國(Caliphate)，不僅實施管理，徵收雜

註39：賴瑩綺，〈美智庫：抖音恐成間諜工具〉，《工商時報》，2019年1月15日，https://www.chinatimes.com/newspapers/20190115000303-260203?chdtv，檢索日期：2019年10月27日。原文請參閱，Claudia Biancotti, “The Growing Popularity of Chinese Social Media Outside China Poses New Risks in the West,” Peterson Institute for International Economics, January 11, 2019, https://piie.com/blogs/china-economic-watch/growing-popularity-chinese-social-media-outside-china-poses-new-risks，檢索日期：2019年10月27日。

註40：“Bin Laden Raid Was Revealed on Twitter, BBC News, May 2, 2011, https://www.bbc.com/news/technology-13257940，檢索日期：2019年10月28日。

註41：馮英志，〈川普一則推文，美海豹部隊機密行蹤意外曝光〉，中時電子報，https://www.chinatimes.com/realtimenews/20181228002294-260408?chdtv，檢索日期：2019年10月28日。

註42：〈這款APP讓全球軍事基地曝光，傳臺灣飛指部也在列〉，自由時報電子報，2018年1月29日，https://news.ltn.com.tw/news/politics/breakingnews/2325912，檢索日期：2019年10月29日。

稅，乃至發起一場社群媒體運動，徵召外國聖戰分子或追隨者加入，甚至吸引孤狼式恐怖分子發動恐攻；同時藉由社群媒體宣傳，可將恐懼訊息傳播到世界各地，諸如殘忍的斬首與處決方式，當媒體爭相報導之際，更替ISIS打開知名度，進而吸引大量同類分子[43]。

（二）美國國土安全部（Department of Homeland Security）2010年的特別報告就指出，恐怖分子利用社群媒體來達成以下目標：其一做為分享作戰與戰術資訊的平臺，諸如製造應急爆炸裝置（Improvised Explosive Device，IED）手冊、調配有毒物質的化學配方及武器的保養與使用；其二做為連結極端網站及其他線上激進內容的入口，如伊斯蘭國即擅長利用臉書與推特來傳播；其三做為恐怖宣傳與極端意識形態訊息的平臺；其四用做遠端監視特定目標對象的資訊來源[44]。美軍的報告也指出，恐怖分子利用社群媒體的可能想定，第一種為在平臺上即時發布美軍部隊的動態；第二種為利用直播功能，傳送即時影像，以精準設定自殺炸彈客的引爆時間；第三種為由某網路恐怖分子鎖定一名士兵並駭入其社群媒體帳戶，竊取其身分與其他士兵互動[45]。

（三）值得注意的是，恐怖分子利用社群媒體傳播假消息，也能波及到一國的經濟。例如，一自稱「敘利亞電子軍」（Syrian Electronic Army）的團體在竊取「美聯社」（Associated Press）記者的密碼後，其駭客在該社推特帳戶推文：「突發新聞：白宮發生兩起爆炸，歐巴馬受傷。」假新聞一出，投資者的恐慌使華爾街損失了1,365億美元（約新臺幣4兆3,680億元）[46]。由此可見，社群媒體的傷害也外溢至經濟領域。

四、中共的案例

（一）2018年在美、中貿易角力如火如荼之際，中共運用官媒輿論與網路控制等手段，操控有利於己的消息，進而塑造受害者的形象，除在國內激勵民族主義愛國情操外，也讓外界認為美國是非理性的國家[47]。此外，中共空軍官方微博「空軍發布」在2017年刻意發布其轟6K轟炸機繞過玉山照片，事實證明是子虛烏有，我國國防部當下出面嚴正否認，指稱「這是假的，勿以訛傳訛」。中共刻意故布疑陣，想拿從我國西岸拍的照片，混冒共機已從東部近距離臨空，企圖營造隨時可多方位空襲臺灣的緊張氣氛，而這類以混淆視線距離從臺海中線以西上空拍的共機照片，即是共軍宣傳的技倆[48]。

註43：Jarred Prier, “Commanding the Trend: Social Media as Information Warfare,” Strategic Studies Quarterly, Winter 2017, p. 64.

註44：Department of Homeland Security, “DHS Terrorist Use of Social Networking Facebook Case Study,” December 5, 2010, Public Intelligence, https://publicintelligence.net/ufouoles-dhs-terrorist-use-of-social-networking-facebook-case-study/，檢索日期：2019年10月30日。

註45：304th Ml Bn OSINT Team, “Al Qaida-Like Mobile Discussions & Potential Creative Uses,” October 16, 2008, p. 9.

註46：〈推文稱白宮驚爆，美股短暫大跌〉，中央社，2013年4月24日，https://www.cna.com.tw/news/firstnews/201304240003.aspx，檢索日期：2019年11月1日。

註47：Matt Schrader, “Pre-suasion: How the PRC Controls the Message on a Sino-US Trade War,” China Brief, Vol. 18 Iss. 6, April 9, 2018, https://jamestown.org/program/pre-suasion-how-the-prc-controls-the-message-on-asino-us-trade-war/，檢索日期：2019年11月1日。

註48：吳明杰，〈國軍破解共機繞臺照，非臺灣東部拍攝，其實是在這裡……〉，風傳媒，2016年12月26日，https://www.storm.mg/article/204904?srcid=73746f726d2e6d675f323064386636663735656561653134 63_1556783470，檢索日期：2019年11月2日。

(二)中共操控社群媒體眾所皆知，華盛頓智庫的一場座談會中，全球臺灣研究中心執行主任蕭良其(Russell Hsiao)表示，媒體是中共用來控制和動員的重要政治工具，為實現「兩岸統一」，中共不僅通過報紙、電視、廣播等傳統媒體對我做宣傳戰，同時也利用新媒體對臺統戰、滲透臺灣公民社會，通過心理戰效果製造分化，以達到削弱我國民主、實現「一國兩制」的最終政治目標[49]。我國安單位也證實中共已建立自身的「巨魔工廠」，培養自媒體，在微博、臉書、YouTube、推特等媒體建立帳號，對臺展開「認知空間作戰」[50]；另惡名遠播的「五毛黨」(官方名稱是網路評論員)也將我國當成下手目標，散播統戰的消息。近期新的手法就是收購臺灣的臉書粉絲團，中共在「104外包網」的徵才公告，要徵求「政黨臉書粉絲專業管理小編」，案件內容主要是管理黨內粉絲專頁的發文及宣傳案件，薪水為新臺幣2-5萬元，強調執行時間不拘，在家作業亦可，不過前提竟然是「支持和平統一」[51]。

針對上述這種統戰訊息干擾，我國須做好反統戰的準備，教育民眾具備敵情意識，強化立法與社會宣導的工作，而法規制定可參考美、英、德、澳各國近期通過的規範[52]；另值得注意的是，長期觀察兩岸關係的學者寇謐將(J. Michael Cole)指出，中共現在利用聊天機器人、不同的社群媒體及內容農場，在臺散布支持北京的文宣資訊，並使民進黨和國民黨持續惡鬥。換言之，中共正運用宣傳(Computational Propaganda)的作法，介入我國民主政治的戰場[53]，國人不能掉以輕心。

肆、社群媒體與新興科技

經裁切、合成與後製的假照片與影片，對一般人而言或許是見怪不怪，可是如果是活生生的人在螢幕上講話，你或許就會上當了，在「深度偽造」(Deepfakes)科技出現後，「眼見就不一定為憑了」。這是近幾年出現的一項科技產品，其是利用深度學習的人工智慧，深度學習使用一道道簡單的數學方程式，其數學模型稱為「神經網路」(Neutral Networks)，可來推斷並複製各種圖像模式，資料來源則是從一個大量資料集內進行篩選。它主要是由生成器(Generator)與鑑別器(Discriminator)這兩種特定的演算法組成，兩者在生成對抗網路(Generative Adversarial Networks)中進行交互比對，前者是從資料集中創造經修改的內

註49：〈專家：中國利用社群媒體削弱臺灣民主〉，《民報》，2018年3月30日，https://www.peoplenews.tw/news/1bca4f0b-5f77-45d0-ba1d-73b31da71010，檢索日期：2019年11月2日。

註50：鍾麗華，〈為扶植親中政權！中國「巨魔工廠」拿臺灣選舉練兵〉，自由時報電子報，2018年11月4日，https://news.ltn.com.tw/news/politics/breakingnews/2601457，檢索日期：2019年11月2日。

註51：〈政黨徵小編高薪5萬……竟要支持和平統一！網轟：接案賣靈魂〉，三立新聞網，2019年4月4日，https://www.setn.com/News.aspx?NewsID=522363，檢索日期：2019年11月2日。

註52：張玲玲，〈中國對臺「認知空間作戰」〉，自由時報電子報，2019年5月16日，https://talk.ltn.com.tw/article/paper/1288955，檢索日期：2019年11月3日。

註53：J. Michael Cole, "Will China's Disinformation War Destabilize Taiwan?," The National Interest, July 30, 2017, https://nationalinterest.org/feature/will-chinas-disinformation-war-destabilize-taiwan-21708，檢索日期：2019年11月4日。

圖一：皮爾導演製作的深偽影片

資料來源：BuzzFeedVideo，https://www.youtube.com/watch?v=cQ54GDm1eL0，檢索日期：2019年10月13日。

容，後者是利用鑑別器來辨識人工的內容，這種技術在短時間內就已獲得迅速進展，目前已能產製出極為真實的假影音內容[54]，這種「深偽影片」也成為社群媒體傳播的最佳管道。

目前在不同領域上都可發現深偽技術的發展，「深度偽造」其實在電影界的運用已行之有年，只不過以往從業人員須花費大量時間與心力才能製成可以看的影片，但現在電腦運作很快，圖像處理器很先進，擬真度愈來愈逼真，幾達不可思議程度。在學術界上，2017年美國華盛頓大學發展出名為「深度影片肖像」(Deep Video Portraits)的人工智慧技術，偽造歐巴馬談論恐怖主義等議題的演說，並製成活生生的影片畫面[55]。在媒體業上，2018年4月，美國新媒體網站Buzzfeed與知名導演皮爾(Jordan Peele)共同製作一部歐巴馬的深偽影片，皮爾以人工智慧科技變造自己成為歐巴馬，並以假歐巴馬告訴大眾媒體識讀的重要性，正當一切看似合理時，就在影片40秒時，揭曉此為皮爾個人的言論[56](如圖一)。 雖然此一技術所產製的影片還不精細，仍有許多破綻，但這項技術已快速發展並普及，目前網路上已有類似應用程式的下載與教學，使修改影音的方式就像修圖軟體「Photoshop」處理圖片一樣並不困難。

「深度偽造」的影片雖然多數屬於惡作劇，但像是更換國家領導人臉部的惡搞影片或是將明星臉部移接到色情影片，就可能涉及某種程度的道德與法律問題。但令人擔憂之處是，這項技術若經過專業人士後製與有心人士透過社群媒體管道傳播，並以不當目的用於與政治與軍事問題上，勢必會造成相當程度的影響及恐慌。因為就心理學角度而言，深偽影片內容愈接近視聽者的立場，就愈容易讓人信以為真，許多專家也警告，如「在未來選舉中，使用深偽影片幾乎是無可避免，因為假影片可用來抹黑候選人，或是讓人們否認真實影片捕捉到的真實事件。」或「雖然我們尚未到達深偽影片武器化階段，但那一刻即將到來。」[57]幸好目前專家已研擬出兩種反制深偽影片的方法：其一為在影片中嵌入數位簽章，以證明為真，同時演

註54：Robert Chesney and Danielle Citron, “Deepfakes and the New Disinformation War,” Foreign Affairs, Vol. 98 No. 1, Jan-Feb, 2019, p. 148.

註55：陳正健，〈在美掀國安疑慮，利用AI人臉偽造政治人物影像〉，自由時報電子報，2018年7月3日，https://news.ltn.com.tw/news/politics/paper/1213456，檢索日期：2019年11月4日。

註56：〈以假打假！外媒用AI假影片讓歐巴馬告訴你假新聞問題〉，Inside，2018年4月18日，https://www.inside.com.tw/article/12601-ai-fake-news-video-from-jordan-peele-aand-buzzfeed，檢索日期：2019年11月4日。

註57：葉俐緯編譯，〈深偽影片流竄，恐加劇假新聞招致混亂〉，中央社，2019年1月28日，https://www.cna.com.tw/news/aopl/201901280290.aspx，檢索日期：2019年11月5日。

圖二：中共的新小浩人工智慧新聞主播
資料來源：黑龍江網路廣播電視臺，https://www.youtube.com/watch?v=R6l_g65eaCU，檢索日期：2019年11月6日。

算法能找出人眼看不見的數位簽章與臉部活動跡象；其二為利用偵測工具自動糾舉假影片，例如美國國防先進研究計畫局(DARPA)已在2015年推動名為「媒體鑑識計畫」(Media Forensics)，該計畫採取三種主要策略：第一種是檢查影片的數位指紋；第二種是確認影片內容遵循物理定律；第三種是查證外部資料[58]。

另一個與社群媒體息息相關的技術是新聞與人工智慧(AI)的結合。人工智慧技術目前已能被用來合成人類的新聞主播，並在螢光幕前為大眾播報新聞，中國大陸網路搜尋引擎「搜狗」與中共官媒「新華社」在2018年於烏鎮舉辦的世界互聯網大會上，以該社主播「邱浩」為原型，研發出名為「新小浩」的人工智慧合成主播(如圖二)。報導稱，人工智慧新聞閱讀機器人能模仿人類的聲音、表情和手勢，可從現場直播視訊中學習，像真人的專業新聞主播自然地閱讀文本，而這些模擬器未來可在網站或社交媒體平臺上使用，降低新聞製作成本，在即時或突發新聞播報上更具優勢[59]。

值得注意的是，人工智慧合成技術也暗藏假新聞危機，而社群媒體正好成為假新聞的最佳傳播管道，如果利用後製變臉技術、借用「名人」形象來傳遞假消息，其影響力不容小覷。因此，吾人須密切觀察此一科技的後續發展與運用[60]，畢竟科技本身並沒有善惡之分，與社群媒體相關的技術如果使用在正途上，將有助於教育與影視等產業發展。而一個技術的最後應用取決於使用者的心態和意圖，唯有使用者存乎善意，新興技術才能獲得正面的結果。

伍、因應之道

在社群媒體往「惡」的方向發展之際，我國實應針對其常見安全態樣，研擬因應之道，建議有以下幾項：

一、防範應用程式介面(API)漏洞

社群網站上會使用許多應用程式介面，但這也是其安全漏洞的來源。臉書在2018年12月14日發文承認，其圖片應用程式介面爆發安全漏洞，高達680萬用戶未發布之照片，可能已遭第三方應用程式存取[61]。換言之

註58：波瑞爾(Brooke Borel)著，鍾樹人譯，〈新聞、謊言、假影片〉，《科學人雜誌》，2018年11月號，第201期，http://sa.ylib.com/MagArticle.aspx?Unit=featurearticles&id=4150，檢索日期：2019年11月5日。

註59：〈主播未來將失業？新華社「AI主播」首度亮相〉，《今周刊》，2018年11月10日，https://www.businesstoday.com.tw/article/category/161153/post/201811100002/%E4%B8%BB%E6%92%AD%E6%9C%AA%E4%BE%86%E5%B0%87%E5%A4%B1%E6%A5%AD%EF%BC%9F%E3%80%80%E6%96%B0%E8%8F%AF%E7%A4%BE%E3%80%8CAI%E4%B8%BB%E6%92%AD%E3%80%8D%E9%A6%96%E5%BA%A6%E4%BA%AE%E7%9B%B8，檢索日期：2019年11月6日。

註60：〈中共官媒推AI主播引熱議，人假聲音也假〉，大紀元，2018年11月10日，http://www.epochtimes.com/b5/18/11/9/n10842005.htm，檢索日期：2019年11月6日。

註61：蔡亦寧，〈臉書資安漏洞爆不完！相片應用程式出包，680萬用戶私人照片外洩〉，風傳媒，2018年12月15日，https://www.storm.mg/article/714687，檢索日期：2019年11月7日。

表二：假消息網站與查證平臺

假消息網站		查證平臺	
內容農場	「看中國」、「雪花新聞」、「香港01」、「COCO01」、「琦琦看新聞」	我國	「真的假的Cofacts」、「美玉姨」、「新聞小幫手」、「MyGoPen」、「臺灣事實查核中心」、行政院即時新聞澄清專區、Line Today「謠言破解」、國防部新聞稿。
		英國	「Full Fact」
自媒體	「小五快報」、「中國臺灣網」、「臺灣那點事兒」、「江湖百曉生」、「你好臺灣」、「天朝自千五」	德國	「Correctiv」
		美國	「Politifact」、「FactCheck.org」、「Snopes.com」、「Truth or Fiction」、「First Draft News」

資料來源：〈獨家：國安局監控11造謠網媒，防假消息擾大選，列管名單曝光〉，《蘋果日報》，https://tw.appledaily.com/headline/daily/20190516/38337512/，檢索日期：2019年11月9日。

，這種應用程式介面的漏洞未來可能會成為發動社群網路戰爭的進入點，所以資安單位應將之列為管理社群網站的重點，國軍同仁使用時亦應特別注意。

二、使用者須保持警覺心

社群媒體資安問題已經浮現，受大眾歡迎的臉書、推特等都曾淪為駭客攻擊的目標，一般攻擊態樣可區分以下三種：

(一)假造社群網站通知信，誘人點閱以竊取資料。

(二)社群網站成為駭客發送垃圾訊息/惡意網址連結的跳板。

(三)在社群網站張貼有病毒的訊息，再利用聳動標題吸引使用者點閱[62]。

因此，使用者除了不應點閱社群網站上不明訊息與通知外，一經發現疑似攻擊態樣時，應及時向網站管理者反應，以利管控單位進行處置。國軍雖已完成軍民網實體隔離作業，但在民網的官方社群媒體平臺仍應留意相關態樣。

三、反制社群媒體的「認知空間作戰」

我國國安系統已發現中共對臺散布假新聞有固定操作模式：即鎖定兩岸關係、國防軍事、政府政策推行等議題，由《環球時報》、「今日海峽」、「臺海網」等中方媒體先發動，接著報導再經由網路水軍、五毛黨剪輯製成影片，最後透過PTT、臉書、LINE、Youtube等社群媒體轉傳[63]。這種「認知空間作戰」延續中共過去對臺實施「入島、入戶、入腦」[64]的統戰工作，現在更進一步結合社群媒體的「入心」型態，這種「溫水煮青蛙」的統戰方式讓人不易察覺，所以我國須做好這種新型態統戰的因應之道，逐一檢視相關工作，並教育我國民眾具備足夠敵情意識[65]。

四、反制社群媒體上的假新聞傳播

註62：〈面對社群網站資安威脅與其禁用，不如有效管理〉，科技網，2010年10月27日，https://www.digitimes.com.tw/tech/dt/n/shwnews.asp?cnlid=13&id=0000203166_26324CM85LOQQT7XC506E，檢索日期：2019年11月7日。

註63：宇妍，〈國安單位證實：中國「巨魔工廠」拿臺灣選舉練兵〉，臺灣英文新聞，2018年11月4日，https://www.taiwan-news.com.tw/ch/news/3567865，檢索日期：2019年11月7日。

註64：2004年中共領導人胡錦濤要求「中央人民廣播電臺」對臺廣播時要做到「入島、入戶、入腦」的統戰目標，演變至今，當前社群媒體之運用將可達到「入心」，因為網路資訊真假難辨，況且中共網軍水軍或五毛黨常在社群媒體上對臺散播假輿論或假消息。

註65：張玲玲，〈中國對臺「認知空間作戰」〉，自由電子報，2019年5月16日，https://talk.ltn.com.tw/article/paper/1288955，檢索日期：2019年11月8日。

由於人的認知模式本來就容易受到新奇消息吸引而落入假新聞的陷阱，不過假新聞通常會有一些徵兆出現：

(一)誇張聳動、讓人忍不住想點閱的標題，而這可能為惡意點擊誘餌。

(二)冒充真實新聞網站的可疑網址。

(三)內容出現拼字錯誤或網站版面不正常。

(四)經過刻意修圖的照片或圖片。

(五)來源不明，像是沒有發布日期或未註明作者、資料來源或相關資料[66]。

因此，吾人可以透過這些徵兆來提醒自己，閱聽者要有對假新聞「拒看、拒點閱、拒轉載」的態度。

我國國安單位已列管來自中國大陸具爭議性或假消息的內容農場與自媒體，而找尋事實真相或是澄清消息最佳之處，亦可參考事實查核組織所設立的網站平臺(如表二)，避免以訛傳訛，甚或遭到誤導。

閱聽者一方面要培養媒體識讀(Media Literacy)能力，意即在接收資訊的同時，也能查核資料來源、確認內容的正確性，另一方面還要有檢視正反立場觀點的能力，因為即便消息來源是出自於可靠的新聞媒體網站，但因報社政黨偏好不同，其報導的立場也會有所偏頗，考驗個人的判斷分析能力。

五、軍方應有的態度與作為

軍事概念中常提及要掌握制空權、制海權，但在社交平臺蓬勃發展之際，軍人的軍事思維應加入所謂的「掌控社群媒體趨勢」(Command of The Trend)[67]，因為運用社群媒體手段的戰爭，是一場無煙硝味的戰爭，敵人無須攻擊實體設施，透過平臺上的網路訊息即能影響大眾認知與行為，這種戰爭型態將成為未來的戰爭趨勢之一，吾人須審慎面對。再者，軍方應對社群媒體的危害有所警覺，因為官兵無意間上傳至平臺的生活資訊，都可能成為敵人情蒐的目標，甚至官兵在平臺上接觸的朋友，就有可能是敵人假裝的，這些都不乏相關案例。鑑此，社群媒體安全應列入軍方的教育訓練之中，並以跨部門共同合作的方式來因應，才是最佳防範之道。

陸、結語

社群媒體在有心人士的操弄下，正不斷侵蝕這個資訊洪流的世界，許多人可能正成為其幫兇而不自知。國軍官兵除了不助長這些不實訊息的傳播外，也要積極配合相關單位的防範作為，一同遏止這種另類的非傳統安全威脅型態。畢竟在科技的助長下「眼見不一定為憑」，社群媒體的影響力可大可小，身在社群網路世界裡的我們，都有可能被趁虛而入，因此國軍弟兄更應保持警覺性，時時關注相關社群媒體的安全議題，才能擁有分辨網路資訊真偽的能力。

社群媒體逐漸增長的影響力已成為一種資訊媒介，正受到國家與非國家行為者的操弄並用以達成不法之目的，甚至淪為間接戰爭的一種手段。它可以是心理戰之一環，可

註66：陳竹梅、吳冠輝，〈國軍人員運用社群媒體應有的素養〉，《社群媒體與軍事傳播》(臺北：國防大學政戰學院，2017年10月)，頁132。

註67：Jarred Prier, “Commanding the Trend: Social Media as Information Warfare,” pp.51-86。

用來進行宣傳活動，擾亂人心；也可以是資訊戰的一部分，可用來傳播不實訊息；更可以是「假新聞」最佳的傳播媒介，我國相關單位應及早因應這種未來的安全趨勢，國人也應培養檢視正、反觀點的能力，方不致陷入認知錯誤的陷阱之中。 ⚓

作者簡介：

劉宗翰少校，國防大學管理學院93年班、政治大學外交系戰略所碩士104年班，曾任排長，現服務於國防部政務辦公室、《國防譯粹月刊》主編。

老軍艦的故事

廬山軍艦 PF-836

廬山軍艦原為美海軍BULL號，編號APD-78，由美國丹佛造船廠建造，1943年8月12日成軍服役。

民國55年美國依據軍援政策將該艦售予我國，於同年12月19日拖抵左營港，12月22日由總司令馮啟聰中將主持升旗典禮，命名為「廬山軍艦」，隸屬驅逐艦隊。

廬山軍艦成軍後，主要執行海峽偵巡及外島運補護航，民國57年曾與壽山軍艦納編敦睦遠航支隊，前往關島、中途島、夏威夷及沖繩等地訪問，於民國84年10月1日功成除役。

(取材自老軍艦的故事)