中國大陸散播假訊息對我之影響及因應作為

空軍中校　王乾恩　空軍少校　藍聖智

提　要

隨著傳播科技發展與網路的普及，現代資訊的來源脫離不了社群網站，待查證及惡意的資訊層出不窮，由社群網站引發的威脅日益擴大，部分國家為求其利益，透過資訊戰以達到全面滲透完成目的，並以虛實混合的假消息來影響著世界各國。運用入侵Facebook、YouTube、PTT、Line、Twitter及TikTok等社群媒體，企圖獲取利益達到特定目的，並針對他國重大活動、議題釋放假消息，藉以煽動政府與人民之間的對立。

即便兩岸局勢趨於和緩，我全體國民仍然不可掉以輕心，亦不可忽略特定人士可能藉由社群媒體作為資訊戰攻擊手段，研究顯示謠言的散布平均31天才能追查到源頭，而透過法院的審理平均要78天才能將謠言者定罪，這不僅消耗了政府的能力，也考驗著人民對政府的信任。故全面檢視資訊戰手法，必須全面提升資訊安全的防護等級，並提高國人對於媒體識讀的素養，堅實共同抵禦來自對岸的無形攻擊。

關鍵詞：資訊戰、信息戰、社群媒體、假新聞

前　　言

「沒有煙硝味的戰爭」是近代各個國家致力發展的戰爭型態，相較於使用傳統的熱兵器而言，資訊戰可以在短時間內發起數以萬次的攻擊，它既可以秘密地進行駭客攻擊，更可以在不消耗人力資源的狀況下完成任務。由於不用耗費高額的國防預算，即便是小國仍有可能在資訊戰當中獲取絕對的優勢。

隨著網路科技的發展與網路的普及，現代人們所得到資訊的來源脫離不了社群網站，資訊戰已是現代化戰爭不可或缺的一環，其投資報酬率勝過於傳統戰爭的資源投入。尤其我國防經費有限，在軍備競賽上又無法與中共抗衡，故在資訊戰的投入與運用即可能成為我反制中共侵略的關鍵點之一。

1970年代末全球進入「資訊革命時代」，托夫勒(Alvin Toffler)認為資訊革命不僅造成社會的變遷，甚至影響著國家的競爭力，連帶也產生新的戰爭型態。美國學者李彼奇(Martin Libicki)認為資訊戰的手段計有：(1)指管戰、(2)情報偵蒐戰、(3)電子戰、(4)心理戰、(5)駭客戰和網路戰、(6)經濟資訊戰等六種形式。[1]本文所

關注的社群網站即屬於駭客戰及網路戰的範疇，其透過網路入侵、資料搜集、機密竊取及引導輿情等方式來進行實質的攻擊。網路戰(Netwar)最早是1993年由朗非德(David Ronfeldt)阿爾吉拉(John Arquilla)所提出的戰爭形式，其藉由心理戰、文化殖民、新聞傳播、外交、政治顛覆、網路等方式來策劃對敵對國家的反政府活動。[2]

現代資訊戰的發展呈現多元並進的樣貌，甚至成為恐怖分子、反政府游擊隊的利器，他們利用網路作為散播恐懼、宣揚恐怖主義及通信作戰的工具。例如蓋達組織即是透過網路搜集美國飛行學校的資料、設立假帳號以利劫機者登機、搜集航班資料等方式來籌劃911攻擊事件。[3]顯見網路攻擊已成為常態，恐怖主義藉此迅速發揚宗教及組織教義，增進內部凝聚力及對外號召力，成為有心人士的絕佳利器之一。中共甚至認為由於電視、報紙、廣播等媒體都逐漸「網路化」，因此資訊戰的戰略目標應以網路戰為主體，透過網路戰對敵對國家進行恐嚇威脅、擾亂社會秩序、爭取國際輿論支持等各種手段，期能達到兵不血刃的軍事目的。[4]

現代資訊戰作為分析

俄羅斯參謀總長葛雷席莫夫(Valery Gerasimov)在2013年提出的「混合戰」的概念，他認為在二十一世紀戰爭與和平的狀態漸漸模糊，國與國之間不再彼此宣戰，戰爭早已進行中。[5]葛雷席莫夫不僅點出了現代戰爭的模糊性，更凸顯了現代戰爭的不明朗與隱蔽的性質，而現代戰爭最為明顯地轉向便是資訊化的戰爭型態。現代戰爭已經進入第六個階段—「精確武器+資訊戰」(如圖1)，非接觸式的戰爭型態即將成主流。

現代資訊戰的發展不僅僅侷限在政府或軍事機關所執行的資訊戰攻防，更是逐漸朝向透過社群媒體的操作，進而去影響缺乏媒體識讀能力的人民，進而達成癱瘓市場、煽動民心、慫恿叛變等不戰而屈人之兵的目的。因此，社群媒體的經營者若是對於言論自由採取嚴格管控或是過度放縱，甚至無法維持中立態度的話，社群

1 呂爾浩、魏澤民，〈中國「資訊作戰」的類型分析〉，《遠景基金會季刊》，第七卷第三期，2006年7月，頁192。
2 呂爾浩、魏澤民，〈中國「資訊作戰」的類型分析〉，《遠景基金會季刊》，第七卷第三期，2006年7月，頁196。
3 魏曼(Gabriel Weimann)，《新一代恐怖大軍：網路戰場》(臺北：政務辦公室，2018年)，頁34。
4 呂爾浩、魏澤民，〈中國「資訊作戰」的類型分析〉，《遠景基金會季刊》，第七卷第三期，2006年7月，頁212。
5 桑格(David E. Sanger)，〈《資訊戰爭》：網路永遠改變了混合戰，讓「格拉西莫夫準則」更為切合實際〉，《The News Lens關鍵評論》，2019年12月1日＜https://www.thenewslens.com/article/127942＞(檢索日期2021年1月2日)。

圖1　第六代戰爭理論

資料來源：魯斯濱，〈解析俄軍資訊戰——給臺灣的啟示〉，《報呱》，〈https://www.pourquoi.tw/2019/11/11/russian-sixth-generation-warfare/〉。(檢索日期2021年1月15日)

媒體將成為二十一世紀最強大的資訊戰手段之一。

無論是透過社群媒體作為人才招募的宣傳工具，抑或是做為攻擊敵對國家的武器，美軍為最早投身於運用社群媒體作為資訊戰的國家。作為軍事強國的美軍自然也知道社群媒體所潛藏的危機，其制定社群媒體手冊供官兵認識社群媒體的功用及危險，除了要避免在網路談論軍事機密之外，更得防範各種潛藏的木馬程式攻擊。2015年英國軍方成立網路相關的作戰單位，該單位主要任務即是透過社群網站搜集情報、對敵發動心理戰、進行資訊攻防、宣揚政府立場等，甚至早於2008年即已頒布社群媒體的線上指南，藉以培養官兵運用社群媒體進行資訊戰的能力。[6]以下便針對幾個案例作為探討，藉以瞭解世界各國如何透過社群媒體執行資訊戰的任務。

一、俄羅斯對烏克蘭(克里米亞)的假新聞及假訊息資訊戰

克里米亞半島(Крым́ский полуо́стров)自蘇聯解體後隸屬於烏克蘭，但由於國土位於俄羅斯之西，再加上境內居民約有58%左右為俄羅斯人，[7]無論是在戰略的重要性或是民意的基礎上，使得俄羅斯積極地想方設法對烏克蘭進行攻擊藉以掠取克里米亞。

6 劉耀隆，《社群媒體對政治作戰作為影響之研究》(臺北，國防大學政治作戰學院政治學系政治研究碩士班碩士論文，2016年)，頁67-69。

7 吳凱琳，〈4大重點速解：為什麼俄羅斯出兵，選擇克里米亞〉，《天下雜誌》，2014年3月3日＜https://www.cw.com.tw/article/5056246＞(檢索日期2021年1月2日)。

《大西洋雜誌》(The Atlantic)刊載的〈烏克蘭的選舉是一場全力對抗假訊息的戰爭〉(Ukraine's Election Is an All-Out Disinformation Battle)指出俄羅斯透過假新聞的散播，藉以干涉他國的重要選舉，透過假帳號來偽造新聞報導，藉以誤導民眾的選擇及判斷。[8]尤其烏克蘭受到來自俄羅斯的攻擊最為頻繁，甚至可以說是「俄羅斯操練假新聞的練兵場」。[9]

烏克蘭政府成立了資訊政策部(The Ministry of Information Policy)來對抗及反制俄羅斯的資訊攻擊，該單位在2017年封鎖了俄羅斯的搜尋引擎及親俄的網站，但卻遭受到盟國及國民的反對聲浪。[10]烏克蘭政府所面臨的困境也正是其他飽受假新聞困擾的國家的共同遭遇——捍衛民主話語或是踐踏言論自由的兩難困境。[11]

俄羅斯的網軍日以繼夜地對烏克蘭發動數位戰爭(Виктор Фёдорович Янукович)，2014年俄羅斯企圖操盤烏克蘭總統大選便是著名的案例。親俄派的烏克蘭前總統亞努科維企圖透過民主選舉重掌政權。因此，俄羅斯在選舉日當天便已滲透烏克蘭選舉系統，在開票之際便已清除所有的計票資料，並透過網路來即時變更各家媒體的選票數。俄羅斯自然知道這僅是權宜之計，最終選舉的結果還是得由中央的計票所最後公布之資訊為主，但如此混淆視聽的做法即足以製造混亂及不安。但資訊政策部早已偵查到駭客行為，並在公布結果前修正得票數後才交由電視台播報，甚至連俄羅斯網軍都未曾察覺，其電視台還在報導親俄的候選人當選的新聞。[12]由此可見，現代戰爭跳脫於傳統的軍事作戰思維，不再只是針對重要設施進行破壞，而是企圖透過資訊戰藉以獲取先機，甚至可以兵不血刃完成任務。

二、俄國對美國大選之「拉赫塔計畫」

「網路研究社」(Internet Research Agency)是由俄國總統普丁(Vladimir Putin)所掌控的組織，其於2016年美國大選試圖購買網域名稱、Facebook、

8 〈Ukraine's Election Is an All-Out Disinformation Battle〉，《The Atlantic》，2019年4月17日＜https://www.theatlantic.com/international/archive/2019/04/russia-disinformation-ukraine-election/587179/＞(檢索日期2021年1月2日)

9 賴昀，〈俄羅斯資訊戰入侵　喜劇演員高票當選烏克蘭總統〉，《沃草》，2019年4月23日＜https://musou.watchout.tw/read/QdVEQpA9F4cebwZNMaOl＞(檢索日期2021年1月2日)

10 賴昀，〈俄羅斯資訊戰入侵　喜劇演員高票當選烏克蘭總統〉，《沃草》，2019年4月23日＜https://musou.watchout.tw/read/QdVEQpA9F4cebwZNMaOl＞(檢索日期2021年1月2日)

11 〈Ukraine's Election Is an All-Out Disinformation Battle〉，《The Atlantic》，2019年4月17日＜https://www.theatlantic.com/international/archive/2019/04/russia-disinformation-ukraine-election/587179/＞(檢索日期2021年1月2日)

12 桑格(David E. Sanger)，〈《資訊戰爭》：網路永遠改變了混合戰，讓「格拉西莫夫準則」更為切合實際〉，《The News Lens關鍵評論》，2019年12月1日＜https://www.thenewslens.com/article/127942＞(檢索日期2021年1月2日)。

Instagram的廣告及Twitter的假帳號來散播假消息，「用以促使美國政治體制分裂」，而遭到美國司法部起訴。[13]此次計畫名為「拉赫塔計畫」(Project Lakhta)，主要透過俄國網軍機構的會計庫斯亞諾娃(Elena Alekseevna Khusyaynova)追查到線索，庫斯亞諾娃所記載的開支紀錄(2016.1-2018.6)總金額高達3,500萬美金以上，試圖透過社群媒體藉以針對美國社會進行散佈假消息。[14]他們當時透過社群媒體散播是以百萬計的假消息，藉以煽動美國人民與政治團體彼此之間的敵意。[15]

俄國的「網路研究社」在過去使用社群媒體來誘導輿論時，時常使用不流利或錯誤百出的英文，甚至使用過時的流行用語，因而時常被看破手腳。但「網路研究社」從實戰中吸取教訓，除了成員能夠精準地使用美國當下的流行政治詞彙，亦能夠使用流暢的英文來進行敘事。除此之外，對於其所假扮的身分亦能夠不漏痕跡地發表精準的言論，甚至對於LGBT[16]族群還進行了深入研究，瞭解其發文的活躍時間及用語，就是為了能夠獲得美國民眾的信任。[17]其實不僅僅只有俄國企圖透過資訊戰來干預美國總統大選，美國的聯邦調查局、司法部、國土安全部和國家情報總監辦公室等四個單位共同發表聲明指出中國及伊朗等國家也影響美國選民的投票意向。[18]

三、俄烏資訊戰作為

俄羅斯自2月入侵烏克蘭戰爭，雙方傷亡快速增加的同時，另一個戰場情勢也再升高。來自美國政府、烏克蘭智庫的分析顯示，俄方正在加大資訊戰攻擊力道，烏克蘭國防部長雷茲尼科夫(Oleksii Reznikov)警告民眾，俄羅斯可能先破壞資訊傳播系統，接著發動大規模的資訊戰與心戰。隸屬烏克蘭國防委員會的「不實資訊對應中心(The Center for Counteracting Disinformation)」表示，俄羅斯民眾對於

13 蔡婠嫣，〈「境外勢力」如何干預民主國家選舉？俄羅斯花10億元再度示範　女網軍遭美國司法部起訴〉，《風傳媒》，2018年10月20日＜https://www.storm.mg/article/556077?page=1＞(檢索日期2021年1月2日)。

14 Nathan Layne，〈Russian charged with conspiring to interfere in U.S. congressional elections〉，《Reuters》，2018年10月19日＜https://reurl.cc/bznrMX＞(檢索日期2021年1月2日)。

15 〈美司法部開第一槍 俄女干預期中選舉被起訴〉，《芊傳媒》，2018年10月20日＜https://taronews.tw/2018/10/20/155730/＞(檢索日期2021年1月2日)。

16 女同性戀者(Lesbian)、男同性戀者(Gay)、雙性戀者(Bisexual)與跨性別者(Transgender)的英文首字母的縮寫。

17 蔡婠嫣，〈「境外勢力」如何干預民主國家選舉？俄羅斯花10億元再度示範　女網軍遭美國司法部起訴〉，《風傳媒》，2018年10月20日＜https://www.storm.mg/article/556077?page=1＞(檢索日期2021年1月2日)。

18 〈美國四大國安機構齊發聲：警惕中國、俄羅斯、伊朗干預期中選舉、總統大選〉，《風傳媒》，2018年10月20日＜https://www.storm.mg/article/555724＞(檢索日期2021年1月2日)。

自己國家發出的新聞內容已起疑心，在Google Search上，與戰爭相關的包括「損失」、「戰俘」、「死亡」等關鍵字搜尋次數持續上升，維基百科 (Wikipedia)上有人建立俄烏戰爭頁面，試圖提供訊息給俄國民眾，但俄羅斯政府立即警告，並在俄網域內將關閉維基百科上相關頁面，並封鎖兩家獨立媒體後頒布行政命令：散播關於俄羅斯軍方不實資訊者，將面臨最高15年罰則。這只是資訊與認知戰場上，俄烏雙方的其中一回合攻防。[19]

烏克蘭面對網路攻擊作為，得到美國微軟公司的幫助，微軟也加入封鎖俄國國營媒體的行列。微軟威脅情報中心在2月24日，偵測到一波針對烏克蘭基礎架構的「破壞性」網路攻擊，包括一隻新惡意程式，主要鎖定烏國軍事機構、政府機關及製造業等單位，微軟命名為FoxBlade，並已針對這波攻擊對烏國政府提供防禦建議。且在YouTube網站上封鎖俄國兩家官媒的廣告營收。臉書母公司Meta、推特也宣布封鎖平臺上據信散布烏克蘭相關假訊息的俄國帳號。[20]使整個作戰期間俄羅斯的網路攻擊似乎未見預期的成效。

從上述案例可以得知現代戰爭的開端，不再只是敵對國之間對彼此宣戰的那一刻開始算起，而是時時刻刻都處於準戰爭的狀態，現代戰爭的攻防早在雙方宣戰以前就已經開始運行了。由於社群媒體具有去中心化(非單向的互動傳播)、去代言化(無需透過媒體業者的審查)、透明化(訊息公開且流動快速)等特質。[21]

不僅如此，在2019年由自由之家(Freedom House)所公布的報告書《自由與媒體：向下的螺旋》認為即便是講求言論自由的民主國家，也經常透過民粹領袖來影響媒體的中立性，更遑論中共這種獨裁國家了。中共甚至將魔爪延伸至其他國家，企圖透過推動利於中共之敘述、制壓關鍵觀點及嚴格管控內容傳遞等方式向其他國家進行資訊戰。[22]顯見中共除傳統網路攻擊手段外，對於社群媒體的運用及箝制已超乎我們的想像，面對如此巨大的威脅，臺灣事實查核中心依據國際事實查核聯盟(International Fact-checking Network)的《查核準則》，在2018年11月1日首度通過審核，成為臺灣第一家、全球第53家獲得IFCN認證、符合國際標準的事

19 劉致昕、陳映妤，〈來自俄烏資訊戰前線的警告：反制假訊息，別讓絕望吞噬事實和光明〉，《報導者》，2022年3月3日＜https://www.twreporter.org/a/russia-ukraine-war-2022-information-warfare＞(檢索日期2022年4月28日)。

20 林妍溱，〈微軟移除攻擊烏克蘭伺服器的FoxBlade木馬程式、封鎖俄官媒〉，《iThome》，2022年3月1日＜https://www.ithome.com.tw/news/149594＞(檢索日期2022年4月28日)。

21 Byung-Chul Han著，程巍著，《在群眾：數字媒體時代的大眾心理學》(In Schwarm Ansichten des Digitalen)(北京：中信出版社，2019年)，頁25-32。

22 呂易儒，《假新聞還是假民主?-論假新聞與民主制度》(臺北：世新大學法律學院碩士論文，2019年)，頁168-169。

實查核組織；並於2019年10月第二度通過IFCN認證。所有認證成員遵循中立公正、消息來源的標準與透明、資金與組織透明、查核方法的標準與透明及公開與開放的更正措施等原則，參考國外具代表性的事實查核機制，並輔以我國的傳播生態需求，依循專業、透明、公正的原則，執行公共事務相關訊息之事實查核。[23]期能抑制不實資訊的負面影響，維護國家的資訊正向發展。

中共訊息戰對我國之影響

2018年瑞典V-Dem(Varieties of Democracy)跨國調查指出在全球所有國家中，其受到來自外國政府的假資訊攻擊的嚴重程度，臺灣竟是位居第一名，而全球最強大的國家美國卻僅僅位居於第13名。由此可見，資訊戰對我國的影響極大，尤其以來自中共的威脅最大。

中共自2015年起重新整編國安部、統戰部、解放軍等網軍單位合併為「解放軍戰略資源部網路系統部門」，成為對臺資訊戰之主要單位。此單位透過假訊息操弄2018年臺灣地方選舉，並企圖在2020年扶植親北京政府的政權為最終目標。[24]因此，中共所釋出假消息可謂是包山包海，小從錯誤資訊或觀念的分享，假訊息的攻擊時時刻刻出現在我們的生活當中。除了「錯誤訊息」和「不實訊息」這兩種分法，在非營利組織《初稿》(First Draft)研究中心主任Claire Wardle研究中，又將不正確的訊息做出更細的七種分類 (如圖2)[25]：

(一)揶揄模仿：無惡意但有可能誤導

圖2　假新聞的形式

資料來源：《假新聞種類分析和舉例說明》，《沃草公民學院》，<https://reurl.cc/nnD1yl>(檢索日期2021年1月6日)。

23 〈IFCN認證與申訴〉，《台灣事實查核中心》，<https://tfc-taiwan.org.tw/about/ifcn>(檢索日期2022年4月25日)。

24 李怡欣、莊麗存、賴玟茹，〈中共網攻臺灣 一張圖揭假訊息產業鏈〉，《臺灣大紀元》，2019年10月6日<https://reurl.cc/jqgQbZ>(檢索日期2020年12月20日)。

25 於下頁。

讀者。例：利用設計對白調侃公眾人物

(二)錯誤連結：標題、影像或圖說與內容不相符。例：為了吸引讀者點閱，使用聳動甚至失真的標題

(三)誤導內容：對報導對象的資料誤用。例：民調調查結果顯示某候選人民調35%，媒體詮釋為「有65%不支持該候選人」

(四)錯誤情境：真實事件被放在錯誤情境。例：以舊的水果棄置照片，放在新的農業新聞事件中

(五)偽裝新聞：偽裝成媒體或公眾人物(內容農場、假裝其他身分發言。例：為求提高影響力，假裝以匿名外交官身分發言

(六)操弄內容：真實事件但被惡意操弄以達到欺騙讀者效果。例：謠傳「蔡英文在軍人節忠烈祠活動吐口水」影片

(七)造假內容：100%造假內容(就是徹底的造假)。例：謠傳「林飛帆是李登輝的私生子」

這些不同形式的假新聞所造成的負面傷害程度及影響範圍也不一，有些看似無害的假資訊，卻在無形中造成莫大的傷害。近年來，中共對我國輿情的掌握及操控逐漸精準化，從議題的設定到輿論的引導，中共網軍整合新聞媒體與社群媒體，使假訊息幾可亂真的操作手法，[26]致使我國人民需要在主流的新聞媒體及社群媒體間去判別真假訊息。本文主要便以中共透過社群媒體散播的假新聞為研究主軸，藉以探討中共進行資訊戰的手法。

一、中共資訊戰之慣用手法

中共操作資訊戰的場域主要為Facebook、YouTube、PTT、Line及TikTok等平台，雖然上述的媒體平台大多數都為中共官方所禁止，其人民必須使用VPN翻牆軟體(Virtual Private Network，虛擬私人網路)才能使用這些社群媒體，且屬於違法行為。然而，當我們在使用這些社群媒體時卻發現了大量使用簡體字的個人帳號或是粉絲專頁，許多來自對岸的用語及影片大量湧進社群媒體，我們必須對這些現象存有疑心，因為它不僅成為散佈假消息的平台，更是企圖消弭我們對於國家認同的工具。這些網軍散播著親中的言論藉以改變我國人之認知(如圖3)，藉由外宣模式、粉紅模式、農場模式、協力模式加強宣傳的深度及廣度。

由此可見，中共善加利用各種平台進行病毒式的散播，以下便透過實例藉以分析中共資訊戰的操作：

(一)以傳遞中華文化做為包裝藉以同化／弱化國家認同

若是常使用社群媒體如TikTok(抖音)、Facebook、YouTube等平台，便可發

25 《假新聞種類分析和舉例說明》，《沃草公民學院》，<https://medium.com/watchout/fake-news-example-ec0959930e08>(檢索日期2022年4月26日)

26 蔡雨葳，《中共運用假訊息對我影響之研究》(臺北：國防大學政治作戰學院政治學系政治研究碩士班碩士論文，2020年)，頁62。

圖3　親中言論在台散布的模式

資料來源：《駛向全球的中共大外宣機器，如何把「小粉紅」與「紅色App」武器化？》，《報導者》，＜https://www.twreporter.org/a/information-warfare-business-cpc＞(檢索日期2021年1月6日)。

現幾乎充斥著中國的影片，而各式各樣的中國用語也不斷入侵我們的生活。如「立馬」、「藍瘦香菇」、「好評／差評」、「狂」、「網紅」等辭彙，不僅僅出現在我們日常的口語對話，甚至連新聞媒體都不斷地使用來自中國的詞彙。而在許多長輩的群組當中更是流傳許多與中華文化相關的影片，中共利用社群媒體散播通俗的、搞笑的娛樂影片或連續劇的片段，再來是介紹中共境內人民生活、宣揚中國興盛強大等影片，其內容多半未涉及敏感的政治議題，且甚至以閩南語作為主要語言，許多人更是誤以為是我國的影片。[27]無論是傳統習俗、旅遊風光等象徵中華傳統文化等內容，中共企圖營造兩岸一家親的假象，藉以爭取國人對於中共的好感及認同。

(二)透過內容農場散佈假消息以分裂我國人彼此之信任

2018年7月我國爆發年金改革之爭議，當時的社群平台及LINE群組便開始散佈蔡政府以退休金要脅國民出國必須申報之不實訊息，後由總統府國家年金改革委員會出面澄清。據國安情資單位表示，關於年金改革的不實謠言多半出自於微信、微博及中共所操作的網路內容農場，[28]這些假訊息以梗圖的方式重製後，最後會透過LINE的群組廣為流傳，這些不實訊息的深度及廣度實難想像，通常好發在年紀較長、缺乏媒體試讀能力的中老年人的群組，有些影片明顯是移花接木或是斷章取義，卻能在不同的平台當中廣為流傳，顯見這些不實訊息所造成的影響甚鉅。

2018年6月美國在台協會(AIT)在內湖舉行落成儀式，當時的維安情形受到媒體

27 蔡雨葳，《中共運用假訊息對我影響之研究》(臺北，國防大學政治作戰學院政治學系政治研究碩士班碩士論文，2020年)，頁64-65。

28 李怡欣，〈誰是韓流推手？中共網軍被起底〉，《大紀元》，2019年6月27日＜https://reurl.cc/9Z4GQn＞(檢索日期2020年12月20日)。

的關注。在新館落成之前，網路上即已流傳美國海軍陸戰隊從宜蘭登陸準備進駐內湖的照片，並散佈AIT新館落成典禮前，美國的陸戰隊士兵將近8千人，從宜蘭登陸並經過國道至內湖[29]等不實訊息在社群媒體上流傳。經查證後，該圖其實為國軍裝甲車移防的舊圖而已。雖然該傳言對於維安工作並無實質影響，但政府仍需去澄清不實的訊息，無形中消耗了政府的資源及能量。此外，尚有「故宮文物與日本交換展覽五十年」、「佳山基地要租借美軍」等不實訊息[30]亦在網路上掀起了反彈的聲浪，這些都還只是中共操弄假消息的冰山一角而已。

二、中共假訊息之態樣分析

經常使用社群媒體的人應該不難發現，近年來關於中共的貼文或影片——無論是輕鬆搞笑的影片、教育及科學普及的文章、健康及養生等資訊——幾乎充斥著整個平台，這些都是中共試圖透過資訊戰藉以同化國人的舉動。關於假消息的製作與傳播，儼然已成為一個龐大的產業鏈。(如圖4)

從上圖我們可以看見中共從俄羅斯操控美國大選的模式學習經驗，並且從中共官媒發佈消息改為透過第三方平台來操控輿論，經過多方的經手與轉包，執政

圖4　假訊息產業鏈

資料來源：《圖解假新聞的跨國生產鏈：中國解放軍對台訊息戰》，＜https://www.dpp.org.tw/news/contents/8402＞(檢索日期2020年12月20日)。

單位其實很難追溯到幕後黑手。《天下雜誌》便曾以「輿論戰爭@臺灣」作為專題，其訪問網路行銷公司的負責人偉恩(化名)，旗下擁有PTT近60個帳號，他的團隊在網路上操縱輿論風向的價碼為3到10萬不等，這還僅是整合行銷公司向下外包的開價。他也間接指有不肖業者承包中共的案子，無論是操作臉書社團或是製作污衊政府的梗圖等。[31]

中共藉由設立網站、收購粉專或收

29 劉榮、丁國鈞，〈【截獲假訊息戰情報】裝甲車照遭移花接木　竟變美陸戰隊進駐AIT〉，《鏡週刊》，2018年10月23日＜https://www.mirrormedia.mg/story/20181023inv021/＞(檢索日期2021年1月2日)。

30 〈【截獲假訊息戰情報】假新聞6大手法公開　瞎掰太平島、佳山基地租美軍〉，《鏡週刊》，2018年10月24日＜https://reurl.cc/9Z4WMX＞(檢索日期2021年1月2日)。

31 於下頁。

買網紅等方式，由中共官方統一提供素材，並以某傳媒或是新聞網作為包裝，「以此途徑散佈如假似真的假訊息，企圖製造我國內部對立甚至影響選舉結果。」[32]何清漣在《紅色滲透》提及中共對於境外媒體的滲透程度實在難以想像，近年來更是逐漸加強對臺灣媒體的控制。在2008年以前主要是透過「中資」的方式來持有臺灣媒體的股份；2008年以後則是透過親共的台商來併購臺灣媒體。此外，中國也將對其他國家進行大外宣的模式移植到臺灣，其手法包含以資金控制媒體、以經濟手段制衡獨立媒體、買斷獨立媒體的廣告時段等方式，企圖全方位地掌控媒體的話語權。[33]

在立法院外交及國防委員會的會議中，國安局針對假新聞進行專案報告。中共散播不實訊息的模式計有：(1)中共對新聞事件加油添醋再回銷臺灣、(2)中共變造爭議事件之事實藉以改變認知、(3)中共媒體捏造假新聞-透過通路來擴散至臺灣、(4)中共官方指導方針藉由多重平台配合以引領風向等四大模式，[34]主要皆是以新聞媒體及社群媒體為主要平台，尤其許多傳統新聞媒體也開始投身於電子媒體，使得假訊息的傳遞更為快速且即時。而社群媒體便成為傳播假消息的溫床，特別是國人對於本國所發佈的新聞訊息多半沒有戒心，而這些假新聞多以真假參半的方式來進行論述，可謂是防不勝防。

中共企圖利用社群媒體這個平台作為資訊戰的媒介，便是看中其多元性、即時性、互動性及共享性等特點。[35]當中共透過網路行銷公司、中共代理人等媒介進行假訊息的散播，不僅增加我國對於消息來源查證的困難之外，網路行銷公司透過購買廣告或大數據平台等方式，更能精準地將假消息強行推廣給目標群眾。而這些假消息透過網路媒體的宣傳，使得訊息本身更難分辨真假，並且能在不同的社群媒體平台上進行病毒式的傳播，使得影響的層面更廣。

遭遇資訊戰威脅時如何有效作為以提升反制能量

據美國麻省理工大學媒體實驗室以Twitter作為主要平台進行研究，其搜集2006至2017年數據資料發現假訊息和一般

31 李怡欣、莊麗存、賴玟茹，〈中共網攻臺灣 一張圖揭假訊息產業鏈〉，《大紀元》，2019年10月6日＜https://reurl.cc/nnD1Xl＞(檢索日期2021年1月2日)。
32 蔡雨葳，《中共運用假訊息對我影響之研究》(臺北，國防大學戰院政治系碩士論文，2020年)，頁107。
33 何清漣，《紅色滲透》(臺北：八旗文化，2019年)，頁161-171。
34 國家安全局，《中共假訊息心戰之因應對策》，＜https://lis.ly.gov.tw/lydbmeetr/uploadn/108/1080502/01.pdf＞(檢索日期2021年1月20日)。
35 劉耀隆，《社群媒體對政治作戰作為影響之研究》(臺北，國防大學政治作戰學院政治學系政治研究碩士班碩士論文，2016年)，頁62-65。

訊息的傳播速度相差將近6倍，[36]這不僅顯示社群媒體散播假新聞的效率極高，也反映了澄清假消息應成為政府的首要工作。事實上，目前政府對於假消息的反制成效並不如預期，尤其現今假消息以虛實混合的方式，使得民眾完全無法辨別其中的真偽，而在網路的隱蔽之下也不易追查來源。根據研究平均要31天才能追查到散布謠言的源頭；而平均要78天才能透過法院的審理將謠言者定罪(如圖5)，這不僅消耗了政府的能力，也考驗著人民對政府的信任。

此外，「社群媒體武器化」概念的提出也足以證明社群媒體的影響力逐漸擴大，甚至有學者將社群媒體視為「新力量」(New Power)，[37]顯見社群媒體已成為現代戰爭中不可或缺的一環。因此，本節將討論我國針對他國之假消息攻擊可以採取的反制作為。

圖5　假消息判定時程圖

資料來源：〈假訊息與它們的產地〉，〈https://www.readr.tw/project/disinformation〉。(檢索日期2021年1月15日)

一、 開發大數據資料庫

由於社群媒體蘊藏著演算法的機制，它記錄著使用者所有的數位足跡，並預測使用者偏好的資訊內容，因而失去對於訊息的真偽的判斷。此外，演算法的機制也將人們化成一個又一個的同溫層，除了接收相同的資訊之外，也會誘導使用者加入同溫層的社團群組，以致使用者失去辨明真相的察覺。人們如果都處在同溫層內相互「取暖」，接受新的意見和想法的可能性就越低；而處在開放的、多元的資訊環境當中，就能提高對於假新聞的敏感度。在同溫層的思考邏輯之下，永遠無法跳脫舊有的思維邏輯。這一切都是仰賴著龐大的大數據資料庫，因此建構及發展應對機制有其必要性。

由於科技發展的進步，對於人工智慧的需求也越來越重要，它將可能左右著新世紀戰爭的成敗。許多國家都投身於人工智慧的開發與研究，在AI時代誰先掌握資訊，誰就可以奪得先機。過去需要耗費大量人力所進行的分析，以後僅需要將指令輸入至人工智慧，便可以跨平台、跨裝置去大量搜集使用者的數位足跡、判別使用者的喜好與政治傾向，藉以投放有效之不實訊息，這些不實訊息的經過精密的設計，再也無從判斷真假。[38]我們未來要

36 "The spread of true and false news online" Science 09 Mar 2018: Vol. 359, Issue 6380, pp. 1146-1151.
37 黃柏欽，〈社群媒體武器化影響、運用與能量建構〉，《國防雜誌》，第三十五卷第三期，2020年9月，頁5。

面對的是人工智慧和機器學習的科技，它的背後即是龐大的數據庫在運作，不分晝夜地去搜集人類的數位足跡及不間斷地大量學習及訓練的模式，這兩者的結合將使假訊息更加難以辨別真偽。因此，我國應全力開發大數據資料庫，透過人工智慧及機器學習得以在短時間內過濾、分析來自境外的網路攻擊，除了可以節省人力成本之外，更可以透過每一次的攻防演練來增加資料庫的數據，藉以完善攻防策略。

二、加強監控網路訊息

我國憲法保障人民的言論自由，網路訊息的監控便成為每位執政者的燙手山芋。若採取嚴格的法律來箝制網路訊息的傳遞，這樣則無異於獨裁國家。但若對於假消息的傳播毫無作為，等於是直接放棄與敵方抗衡的重要場域。國安局即建議政府應採取「全政府」、「全社會」的對策，必須針對中共的各種滲透模式擬定反制策略，整合產、官、學、研之力來強化資訊安全之防護能量。此外，政府更得運用各種管道適時地澄清爭議的訊息，並掌握時機予以反擊。[39]

同時，政府應獎助企業、大學或研究中心成立網路緊急反應小組，當有具爭議或假訊息傳散時能夠迅速予以澄清，並且針對所使用之網路系統採取必要的防護措施，避免遭到中共網軍的病毒攻擊，藉以威脅換取我國重要產業之機密資訊。另外，政府應加重網路犯罪的罰則，除了擴增電信警察的編制及培育專業職能，更應防範我國人民的個人資料遭中共竊取，以作為不法行為之用途。[40]

我國目前已逐步建立假新聞及防治的相關法條，除了有《社會秩序維護法》、《反滲透法》、《數位通訊傳播法草案》等法案，並經過跨部會的協調後，行政院陸續通過內政部〈災害防救法第41條修正草案〉、行政院農業委員會〈糧食管理法15條之1〉等七個修法案；除此之外，國防部亦針對《陸海空軍刑法》第72條進行修正，將原先捏造軍事謠言的散播管道添增了電子通訊、廣播電視、網際網路等媒體平台。[41]政府企圖透過法規來遏止假消息的發布及二度傳播，唯對於來自境外的謠言攻擊，仍須與各個國家制定相關的法規及協議，透過世界各國的協力合作方能有效阻止來自境外的攻擊。

三、擴增網路反制戰力

今年度所公布的《110年國防總檢

38 蔡雨葳，《中共運用假訊息對我影響之研究》(臺北：國防大學政治作戰學院政治學系政治研究碩士班，2020年)，頁89。

39 國家安全局，《中共假訊息心戰之因應對策》，<https://lis.ly.gov.tw/lydbmeetr/uploadn/108/1080502/01.pdf>(檢索日期2021年1月20日)。

40 楊明芬，《中共資訊戰對臺灣資訊安全之影響》(嘉義：國立中正大學戰略暨國際事務研究所碩士論文，2012年)，頁90-91。

41 姜家涵，《假新聞現況探討及解決方案分析》(臺北：世新大學口語傳播學系碩士論文，2019)，頁40-42。

討》報告書中，明定「科技先導、資電優勢、聯合截擊、國土防衛」為我國建軍方向，此為延續著過去「資電先導、遏制超限」的戰略思維，顯見我國持續在資電發展下有著持續性的發展。在「創新／不對稱」的作戰思維下，除了持續精進資訊防禦在硬／軟體上強化之外，更應朝向增進網路反制戰力的方向發展。

一般來說，當我國境內遭受到假消息的散佈時，在資訊戰的範疇下即屬於被動的一方，當務之急便是立即澄清不實或爭議之內容並適時予以反擊。根據研究顯示，中共除了針對境外國家散佈假消息之外，更是針對本國人民頻繁地散佈假消息；而身為敵對國的臺灣無論是對內或是對外，幾乎很少製造假新聞來做為反制的工具。[42]

我國在平時就應針對中共的指揮管制及武器的系統擬定作戰方針，在戰前即使用資訊戰及輿論戰癱瘓敵之網路系統，破壞其政經及社會秩序，以求制敵機先之效果。運用社群媒體大量散佈假訊息以混淆視聽，企圖造成中共對於情勢的誤判，以擾亂其政策、命令的執行；另一方面亦可透過社群媒體爭取國際間的認同，訊息的傳遞可以無時差、無限制傳播至世界各地。同時，我國應以國家整體的資訊能力及聯合駭客來發動網路攻擊事件，使得中共無法在第一時間內回應網路攻擊及澄清假訊息。[43]

四、建立網路制裁／衡機制

一般來說，社群媒體具有言論審查機制，例如臉書會即時移除關於仇恨言論、色情、虐待兒童／動物、種族歧視、恐怖主義、暴力、自殘等內容，但由於使用者數量龐大也造成審查人員在查核上的困難，尤其是針對假新聞的判斷更是見仁見智，這也正是假新聞能在社群媒體迅速散播的原因。此外，並不是所有的社群媒體都有嚴格的審查機制，大多數更是聲稱自己僅是提供「平台」供使用者發表，再加上社群媒體也無法即時查核每一則訊息的真偽，因而成為網路的灰色地帶。

因應社群媒體放任假新聞或仇恨性言論的傳播，德國已經立法規定社群媒體應具有社會責任，並明確規範社群媒體接獲通報或投訴的24小時內，必須撤除不當的貼文，同時設立相關的關鍵字供大數據資料庫進行監控，違者將處以高額的罰款。[44]我國則可以德國的立法經驗做為參考依據，藉以健全我國網路資訊安全及抵制不實言論的傳播。

42 李怡欣、賴意晴，〈臺灣受假訊息攻擊嚴重 瑞典學者：嫌犯是中共〉，《大紀元時報》，2019年09月27日＜https://www.epochtimes.com/b5/19/9/27/n11550605.htm＞(檢索日期2020年12月20日)。

43 林宜昌，〈資訊戰對國軍防衛作戰重要性之研究〉，《海軍學術雙月刊》第五十三卷第六期，2019年12月，頁119。

44 呂易儒，《假新聞還是假民主?-論假新聞與民主制度》(臺北：世新大學法律學院碩士論文，2019年)，頁182-183。

五、建立有效假訊息查核機制

現行中共資訊戰操作已不僅同(弱)化國家認同及分裂國人彼此信任，已開始有以「先造謠再闢謠」之假反共手法,先博取部分國人信任，然假訊息傳播後，能在多少時限內完成訊息真相的查核，同時查核後的結果是否能完全根除先前接受假訊息的社群網站成員認知，是刻不容緩的。

基此，我國法務部調查局為快速提升假訊息案件之調查能量，於2009年8月8日成立「假訊息防制中心」，全力執行假訊息之溯源偵辦，務求「事件有分析、案案有結果」。[45]；另為落實我國資通安全戰略的重要環節，並持續強化民主的防衛機制，假訊息的危害已引起全世界民主國家的高度重視，甚至有境外勢力在網路上製造假消息，皆易對國家整體政策與管制造成莫大干擾，故法務部調查局於2010年4月24日將原本「假訊息防制中心」升級為法務部「調查局資安工作站」，除依法查緝網路犯罪外，也提升偵防、蒐證、鑑識的能力。[46]

結論與建議

108年所公布的國防白皮書明確指出提升我國「電子暨網路作戰能力」藉以創造不對稱作戰之優勢，主要是以電子戰及網路戰的軟硬體設備進行開發及擴充，以及建立可監控武器系統的電磁頻譜並對其信號進行分析、目標鑑識和情報分享的機制[47]為主軸。期能完善基礎建設之網路安全防護，以達成「安全之國防網路」、「精確之網路情報研究能量」與「可恃之網路攻防戰力」等目標，[48]可見我國對於網路安全防護作為的重視。

唯上述的防護作為主要針對資訊設備的強化與人才的培育，屬於國與國之間戰略層級的攻防。而本文述及的社群媒體則是直接針對國民的資訊戰作為，若是透過法律來箝制或審查社群媒體的言論，則牴觸了我國憲法保障人民的言論自由。因此，社群媒體成為網路攻防戰中的軟肋。它看似無害但卻能潛移默化地誘導我國人民的意向，制定合宜的法律及反制作為成為我國刻不容緩的重要議題。以下便提出幾點建議，期能強化我國對於社群媒體之假消息傳遞能有實質的助益。

一、強化資訊安全工作站，過濾境外惡意造謠消息

所謂「工欲善其事，必先利其器」，

45 〈假訊息查證參考資訊〉《法務部調查局》https://www.mjib.gov.tw/news/Details?Module=1&id=501(檢索日期2022年4月28日)。

46 〈調查局成立假訊息防制中心維護國家安全〉《法務部調查局》https://www.mjib.gov.tw/news/Details/1/600(檢索日期2022年4月28日)。

47 中華民國108年國防報告書編纂委員會，《中華民國108年國防白皮書》(臺北：國防部，2020年)，頁68。

48 中華民國108年國防報告書編纂委員會，《中華民國108年國防白皮書》(臺北：國防部，2020年)，頁69。

網路安全防護系統的建置有助於防制假訊息的傳播。中共無時無刻在透過網軍針對我國網路系統、數據庫等軍事、民間機構進行滲透，並針對網路系統的漏洞來植入木馬程式，藉以竊取機密資料或癱瘓網路系統。目前行政院已透過「國家資通安全會報」來整合及擬定資訊安全防護工作；國軍單位也透過多層式資安防護機制來強化資訊安全工作站。政府應整合軍事、民間、企業的資安防護能量，不僅需要鞏固資訊安全防護網，更需針對中共的網路攻擊進行監測及反偵蒐的能力，並預防指揮體系遭到滲透或破壞時的因應作為。[49]尤其須注意境外的造謠消息，中共透過VPN系統不斷轉移IP位置或創造虛擬分身，使我國資安單位不易追查來源，致使無法有效過濾不實訊息。

二、建立第三方查核機制，適時澄清來源不明訊息

我國憲法保障人民之言論自由，若因防範假消息而嚴格控管網路訊息之傳遞，則違反了憲法之精神，因此政府單位也不傾向透過立法來遏止假新聞。[50]但如今假新聞對於社會所造成的動盪與不安亦不可輕忽，因此行政院政務委員唐鳳則表示不實訊息之查核應交由法律來處置，而非由政府來插手管制，「如果政府自己設立『事實查核單位』是不妥的，因為『自己永遠不會糾正自己』，但如果是Google、臉書等民間公司來做，可以讓政府接受檢驗。」[51]

因此，直至2018年4月19日我國第一個事實查核中心才成立。「臺灣事實查核中心」成立宗旨主要是以國外的事實查核機制為學習對象，並針對我國新聞媒體傳播生態擬定方針。其秉持公正、透明、專業的原則來執行事實查核之工作。[52]該網站有「政治與政策」、「國際」、「健康」、「科技資安」、「生活」、「環境能源」等類別的假訊息查證資訊，並透過詳實的調查以辨別訊息之真偽。事實查核中心為了避免遭人誤解其公信力及中立性，不希望政府資金的挹注，其主要查核的對象為網路及社群媒體中關注度最高的新聞，無論查核的結果如何，該中心必須誠實地報告查核結果。[53]因此。建立起公正的第三方查證平台，絕對是破除假消息的最佳工具。

49 楊明芬，《中共資訊戰對臺灣資訊安全之影響》(嘉義：國立中正大學戰略暨國際事務研究所碩士論文，2012年)，頁86-87。

50 沈超群，〈如何遏制假新聞? NCC 會議代表多反對立法管制言論自由〉，《風傳媒》，2018年5月9日＜http://www.storm.mg/article/443083＞(檢索日期2021年1月20日)。

51 〈出手管控網路謠言？唐鳳：這本身就是個謠言〉，《自由時報》，2017年5月5日＜http://news.ltn.com.tw/news/politics/breakingnews/2058320＞(檢索日期2021年1月20日)。

52 〈成立宗旨〉，《臺灣事實查核中心》，＜https://tfc-taiwan.org.tw/about/purpose＞(檢索日期2021年1月20日)。

53 於下頁。

三、建立媒體識讀之能力，辨別不實內容

由於社群媒體的主要受眾為一般民眾，並不是每個人都具備對於辨明真偽訊息的素質。因此，建立良好的媒體識讀能力是刻不容緩的課題。尤其新聞媒體為了爭取收視率，常以聳動的標題來吸引民眾的注意，甚至對於消息的來源也未經確認。此外，更得提防具有中資介入的新聞媒體。我國的挑戰在於國民對於新聞識別的能力較差，許多媒體的競爭激烈，因此時常擬定聳動的標題來引起注目[54]因此，我們必須訓練民眾避免成為假消息的二度散播者。

目前我國已於108學年度起於十二年國教之課程綱要中，納入媒體素養教育之課程，並針對教職人員如國中小校長及主任實施媒體釋讀教育專班，期能培育思辨能力及判斷之素養；而政府部門及機關人員亦須建立常態性的培訓課程，並透過民間團體及社教機構共同強化媒體釋讀之能力，使每個個體都有獨立判斷的能力，不會輕易受到劣質媒體之誤導(如圖6)。此外，建立第三方查核平台也同等重要，政府必須邁向公開及透明化，而第三方組織得已在合乎法律的規範下進行資料的調閱及查核，兩者之間建立互信且平等的機

圖6　防制假訊息之因應作為

資料來源：羅秉成，〈防制假訊息危害專案報告〉，〈https://reurl.cc/ra5D4x〉。(檢索日期2021年1月15日)

53 周芸，〈「臺灣事實查核中心」成立 胡元輝：過程一律公開透明〉，《銘報即時新聞》，2018年5月8日＜https://reurl.cc/Q74pl0＞(檢索日期2021年1月20日)。

54 原文為「Part of Taiwan's challenge, experts say, lies with weak media literacy and a hypercompetitive news industry that sometimes compromises editorial standards in the race for traffic.」請見《Specter of Meddling by Beijing Looms Over Taiwan's Elections》，《The New York Times》，＜https://www.nytimes.com/2018/11/22/world/asia/taiwan-elections-meddling.html＞(檢索日期2021年1月16日)。

制。

未來我們面對假新聞／假消息的挑戰只會越來越嚴苛，自2017年起已有不肖人士透過Google公開的原始碼來進行人工智慧的訓練，並且釋出一款名為Fake的App，使用者可以將任何人的臉代換到另一個人的臉，原先只是用於將明星的臉置換到色情影片的女主角，但已有團隊使用此種技術讓歐巴馬抨擊川普的行為，[55]企圖提醒人們不能再「眼見為憑」。若不肖人士將此種影片在選前之夜用以抨擊對手，其後果則無法想像。

然而，政府不能永遠處於守勢的狀態，僅透過第三方的查核平台、事實澄清具爭議之假訊息及透過法律來嚴懲，都只是治標不治本的方法。除了全面提升國民的媒體素養之外，也得思考如何在嚴峻的資訊戰威脅下進行反擊或主動出擊，根據國安局的報告亦指出，中共對我國的攻擊手段更加多元且精細難辨」，必須以「截長補短主動出擊」作為因應之道。[56]在2008年出版的《資訊作戰：以柔克剛的戰爭》亦認為我們必須將任何網路連結都視為敵方可能的突破點，「資訊作戰不僅要保護我方資訊和資訊系統，亦須影響敵方資訊及資訊系統，俾壓制其可能對我不利之資訊能力。」[57]然而，資訊戰已不僅僅是國與國之間高端科技資訊競賽，而是透過眾人熟知的媒體平台進行滲透、分化等攻擊行為。社群媒體已逐漸朝向武器化發展，它可以說是顛覆我們對於現代戰爭的既有想像，更可「提供多元情報搜集、分析管道，輔助戰演訓效果，強化感召、宣傳力度；以及發揮明確目標、對象定位，降低戰場迷霧、減少摩擦，改善戰場模糊的效果。」[58]因此，面對這種無形的戰爭我們更不能掉以輕心，期能透過縝密的分析對岸的手法及擬定反制作為，並建立起強大的資訊攻擊及防護的能力，以捍衛我台海之安全。

作者簡介

王乾恩中校，空軍官校飛專90年班、國軍電戰班97年班、國防大學空軍指揮參謀學院105年班。經歷：情報官、電戰官。現任國防大學空軍指揮參謀學院中校教官。

藍聖智少校，空軍官校航太系99年班、空軍官校作戰參謀軍官班104年班、國防大學空軍指揮參謀學院110年班。曾任飛行官、飛安官。現任空軍第四聯隊救護隊少校飛行官。

55 黃哲斌，〈比假新聞更可惡！你聽過「深假」嗎？〉，《天下雜誌》，2019年7月15日<https://www.cw.com.tw/article/5096017>(檢索日期2021年1月20日)。

56 國家安全局，《中共假訊息心戰之因應對策》，<https://lis.ly.gov.tw/lydbmeetr/uploadn/108/1080502/01.pdf>(檢索日期2021年1月20日)。

57 里・阿米斯德，《資訊作戰：以柔克剛的戰爭》(臺北：國防部史政編譯室，2008年)，頁93。

58 黃柏欽，〈社群媒體武器化影響、運用與能量建構〉，《國防雜誌》，第三十五卷第三期，2020年9月，頁25。