網路空間遂行認知作戰之研究
-以俄烏戰爭爲例

作者/蕭浩然、李建鵬

提要

一、俄羅斯於2022年2月24日對烏克蘭東部執行「特別軍事行動」，伴隨實體空間的軍事行動，有關戰爭假訊息亦於網路空間大量散傳，而烏克蘭也不斷澄清此類不實訊息，以持續爭奪戰場話語權。

二、認知作戰主要影響受眾的感知、意識、理解、意志、信念和價值觀，其標的包含軍隊與一般人民，再加以運用社群媒體大幅增強認知作戰影響力，遂使「網路空間」成為新型態認知作戰的主戰場。

三、認知作戰對民主國家之威脅更為嚴峻，利用其人民言論自由的特點，更易達成破壞或分裂社會秩序之企圖。我國軍官兵尤須了解敵對我認知作戰的目標、方法與手段，提升對訊息分析與判斷技巧，養成獨立思考與求證習慣，以反制敵之認知作戰。

關鍵詞：俄烏戰爭、認知作戰、網路空間

前言

俄羅斯總統普丁於2022年2月24日宣布，將對烏克蘭東部執行「特別軍事行動」，各國試圖通過聯合國安理會會議避免此衝突發生，同時警告此次入侵可能引發自1945年以來歐洲最大戰爭，此舉也立即引起美國及其盟國的譴責，並揚言要對俄羅斯軍事侵略實施全面制裁。[1]在衝突開始幾個小時內，在社交媒體推特上就有俄羅斯空軍在烏克蘭領空作戰的影片被多次轉發，經英國廣播公司(BBC)檢視後發現，其為俄羅斯空軍在2020年閱兵飛行表演之準備工作影片，而影片中空襲警報聲則是另外配音。[2]在俄烏戰爭中，烏國為鄰近大國之小國，而烏國為爭奪戰場話語權，以各種訊息溝通，包括外交、公共關係、資訊操作與心理作戰，甚至是假訊息、假事件及宣傳等方式，實現其戰略目標，也就是透過戰略溝通進行「認知作戰」，除成功於實際戰場驗證一場以小搏

1 “Russia launches military attack on Ukraine with reports of explosions and troops crossing border”, CNN，https://edition.cnn.com/2022/02/23/europe/russia-ukraine-putin-military-operation-donbas-intl-hnk/index.html，(檢索日期：2023年1月4日)。

2 “Ukraine conflict: Many misleading images have been shared online”, BBC，https://www.bbc.com/news/60513452，(檢索日期：2023年1月4日)。

大的戰爭外，也讓認知作戰在世界各國面前展現其影響戰局之重要性。

「認知作戰」是新的作戰型態，敵方以網路滲透及輿論操作方式，於網路空間企圖運用不實訊息影響民眾認知，瓦解戰鬥意志，將《孫子兵法》「夫用兵之道，攻心為上」概念發揮極致，此種無硝煙的作戰方式令人防不勝防，而在俄烏戰爭後，更提升了認知作戰之範圍與強度。[3]認知作戰可從不同方向進行，例如官方、非官方、軍方，甚至民間等，其特性無平時與戰時之分，且善用敵我雙方國內或國際媒播平台，強化認知作戰影響程度。

美國眾議院議長裴洛西於2022年8月初訪問臺灣後，中共立即對我國實施圍臺軍演，並同時運用認知作戰方式，散布超過272則演習假訊息在國內社群媒體流傳，[4]企圖影響我軍民士氣。內容雖為偽冒或虛假訊息，惟此類假訊息經過大量傳播後，仍可能對我社會穩定造成不小影響。本研究以分析俄烏戰爭中，雙方運用網路空間[5]執行認知作戰之手段為標的，探討國軍應如何借鏡戰爭實例，強化認知作戰之運用策略與反制作為，期可提升反制認知作戰戰力。

認知作戰涵義暨運用探討

一、認知作戰涵義

「認知(Cognitive)」乙詞始於心理學，舉凡與認知、思考、記憶、學習、決策等人類心理過程，皆為其領域。雖然作戰方式隨部隊指揮官的經驗、智慧、直覺與判斷等綜合能力有所不同，但是戰爭主體在於「人」，伴隨戰爭型態改變，掌控認知領域的資訊，也同時掌握了雙方作戰人員思維邏輯，甚至作戰方式與偏好。美國華府智庫「詹姆士頓基金會」(Jamestown Foundation)的研究指出，認知戰廣義上屬於心理戰之範疇，而「認知作戰」內涵雖為心理戰，其重點為結合新媒體來實施。[6]因此認知作戰之特殊性，已成影響戰爭的新興領域，以下茲針對世界軍事大國對認知作戰之涵義簡要探討。

(一)美國

美國國防部早在2001年向國會報告「網路中心戰(Network Centric Warfare, NCW)」的文件即指出，網路中心戰也是一種戰爭型態，要了解網路中心戰，必須關注三個戰爭領域以及它們之間的相互關係(如圖1)，這些領域包括「

3 〈強化媒體識讀 反制中共認知作戰〉，《青年日報》，＜https://www.ydn.com.tw/news/newsInsidePage?chapterID=1522591＞ (檢索日期：2023年1月5日)。

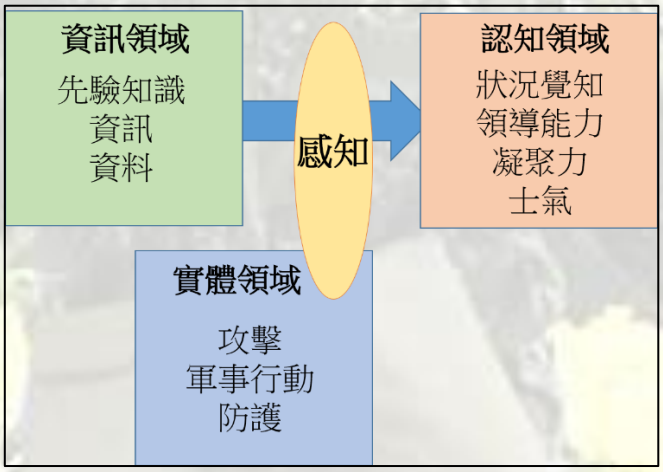
4 同註3。

5 【網路空間】（Cyberspace）：係指資訊環境中之總體領域，其組成包含網際網路、電信網路、電腦系統及其內部之處理器與控制器。《國軍軍語辭典》，頁9-2。

6 劉緯憲，〈2014年克里米亞危機中認知作戰之研究〉(國防大學政治作戰學院，政治學系碩士論文，2022)，頁7。

實體領域」、「資訊領域」和「認知領域」。[7]其中「認知領域」在所有人的腦中，為感知、意識、理解、信念和價值觀所在之處，也是形成決策之基礎。透過認知領域可了解指揮官的企圖、戰術、技術和程序，若能在此領域發揮軍事欺敵之誤導，輕則影響戰鬥行動遂行，重則改變戰爭勝敗。

圖1 戰爭領域相互關係示意圖



資料來源：作者整理，參考“Network Centric Warfare”, Department of Defense，http://www.dodccrp.org/files/ncw_report/report/ncw_main.pdf，(檢索日期：2022年11月12日)

2017年9月時任美國空軍參謀長大衛·李·戈德費因(David L. Goldfein)上將提出軍事「認知作戰」概念，強調「戰爭型態正由消耗戰過渡到認知作戰」，[8]顯見認知作戰已從過去觀念化描述轉變成理論化之實踐，開啟新的作戰型態。美軍2018年版聯戰準則《JP 3-12網路空間作戰(Cyberspace Operation)》所提出「資訊環境」[9]為蒐集、處理、傳播或處理資訊的個人、組織和系統之集合，其環境區分實體、資訊和認知領域，[10]此三種領域相互關聯也相互影響，在分析與選定網路攻擊目標時，應將目標的獨特內在或後天特徵，包含實體、功能、認知、環境和時間等因素納入考量，因此遂行網路空間的軍事活動，除網路作戰行動外，認知作戰也必須納入運作範疇。

美國國防部於2022年6月於阿肯色州小石城北部約瑟夫·T·羅賓遜基地的陸軍國民兵專業教育中心舉行了一年一度「網路之盾2022(Cyber Shield 2022)」演習，為美國國防部最大規模之非機密網路演習，由約800名國民兵網路

7 “Network Centric Warfare”, Department of Defense, 2001/7/27, pp.3-7.
8 “Goldfein delivers Air Force update”, US Air Force，https://www.af.mil/News/Article-Display/Article/1316603/goldfein-delivers-air-force-update/，(檢索日期：2023年2月2日)。
9 【資訊環境】（Information Environment）：執行資訊作業之個體、組織及系統所構成之整合環境。國軍軍語辭典》，頁9-2。
10“Joint Publication 3-12 Cyberspace Operations”, Joint Chiefs of Staff, 2018, pp.I-7.

專家和來自全國各地的法務、政府和企業合作夥伴以及美國海軍與海岸巡防隊參與。本次演習重點於因應「太陽風(SolarWinds)」的供應鏈攻擊，同時為增加演習真實性，也將社交媒體假訊息納入演習想定場景實施演練。[11]

(二)北約

北大西洋公約組織(NATO，以下簡稱北約)指出，認知是心理活動或理解過程，包括人類決策的潛意識和情感方面。戰爭最初是指國家、政府或實體之間的武裝衝突。前述兩個詞共同描繪了認知戰定義：認知戰整合了網路、訊息、心理和社交方面的能力，並與其他方式同步進行，以影響、保護或破壞個人和群體的認知來影響態度和行為以獲得優勢。[12]北約認為認知作戰是一個新的競爭領域，超越了傳統陸、海、空以及多領域空間；在認知作戰中，人的思想變成了戰場，其目的不僅在於改變人們想法，還在於改變他們之想法和行為方式，它會塑造和影響個人和群體信念和行為，以支持侵略者的戰術或戰略目標。實現認知作戰並不一定要運用假訊息或假新聞，透過令人尷尬的政府文件或從公務人員電子郵件中竊取的機敏資訊，將其披露到社交媒體或交付敵對勢力使用，都能以引起爭議與加深矛盾。[13]

北約「卓越聯合網路防禦中心(NATO Cooperative Cyber Defence Centre of Excellence, CCDCOE)」於2021年4月舉行全世界規模最大的軍事網路攻防演練「The Locked Shield 2021」，計有30個會員國逾2,000位專家共同參與。其想定為非北約國家(Crimsonia，簡稱C國)針對假想之北約成員國(Berylia，簡稱B國)發起網路攻擊，場景為B國之供水系統、行動網路及金融系統等關鍵基礎設施遭網路癱瘓攻擊，此外C國同步利用假新聞與社群網路進行認知作戰，[14]試圖混淆B國人民認知，歸咎於政府官員因貪污而造成斷水、斷網及銀行癱瘓等事件，藉以驗證B國反制作為及能力。可知，認知作戰係利用不實資訊或假訊息等方法，從官方、非官方、軍方及民間等共同攻擊，不分平、戰時，並運用敵我雙方、國際傳媒及新媒體，影響思維進而改變行為之目的。

(三)中共

11“U.S. National Guard’s Cyber Training Emphasizes Social Media, Supply Chain Protection”, Nextgov，https://www.nextgov.com/cybersecurity/2022/06/us-national-guards-cyber-training-emphasizes-social-media-supply-chain-protection/367872/，(檢索日期：2023年2月2日)。

12“Cognitive Warfare: Strengthening and Defending the Mind”, NATO’s Strategic Warfare Development Command，https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/，(檢索日期：2023年6月25日)。

13“Countering cognitive warfare: awareness and resilience”, NATO REVIEW，https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html，(檢索日期：2023年2月2日)。

14〈北約網路軍事演練首度加入認知作戰情境〉《行政院國家資通安全會報技術服務中心》，https://www.nccst.nat.gov.tw/NewsRSSDetail?lang=zh&RSSType=news&seq=16547，(檢索日期：2023年2月2日)。

中共對認知戰的相關概念源自於「三戰(心理戰、法律戰、輿論戰)」，並於2014年以「三戰」的基礎及俄國「資訊戰」[15]理論架構上，研提「制腦權」的概念，整合腦科學、心理學、語言學、傳播理論和資訊理論等跨領域研究成果，將過去以制空、制海、制陸、制電磁等作戰領域導入制腦的認知作戰領域；[16]另中共軍方劉惠燕等人建議中共當局應運用大數據及自然語言處理技術，提升主流社群媒體平台認知戰操作，進行潛意識訊息傳遞，[17]讓傳統戰場以實體空間為主的領域，因各國對戰爭認知和科技技術不斷發展，已逐步由實際戰爭行為，轉向為虛擬網路空間的交兵，企圖控制社會大眾意識形態，達成不戰而勝的戰略目標。中共在2013年時發展媒體融合，之後更結合2016年軍改成立之「戰略支援部隊」，[18]將傳統文宣心理戰進行轉型，先透過大數據分析受眾之喜好進而產製對應訊息後，於主流社群媒體發送，讓認知作戰可進行精確攻擊，也可以產生大範圍影響的效果。

(四)我國

《中華民國110年國防報告書》指出，認知作戰之目標為影響對方心理意志及改變思維，作戰場域不受地域與時間的限制。認知作戰源自於情報戰、心理戰與輿論戰，再透過現代的資訊科技、網際網路、社群媒體，企圖透過網際網路進行心理滲透、輿論操作，以擾亂目標之社會秩序、心理思維、法治觀念等價值觀。[19]為肆應中共假訊息對國軍之威脅，國防部於「漢光35號」電腦輔助指揮所演習時將反制中共假訊息納入演練課目，將情報、政戰及資通電軍指揮部等單位組成「資訊作戰小組」執行假訊息反制及欺敵之演練，以驗證國軍相關單位於反制假訊息之整合與協調。[20]

(五)小結

綜前所述，各國認知作戰的標的為受眾之感知、意識、理解、意志、信念和價值觀，所要達成的成效為藉影響受眾心理認知後，藉以影響指揮官在

15【資訊戰】（Information Operations）：軍事行動中，運用戰略溝通、聯合跨部會協調、公共事務、軍民作業、網路戰、資訊確保、電子戰、心理戰、情報、軍事欺敵、作戰安全及關鍵領導幹部接觸等手段，影響、干擾、阻絕或篡改敵決策，以達自我防護之目的。《國軍軍語辭典》，頁9-2。

16〈腦計畫：世界科技競爭新高地〉，《解放軍報》，2016年10月20日，<http://www.81.cn/jfjbmap/content/2016-10/20/content_159464.htm>（檢索日期：2020年8月24日）。

17劉惠燕、熊武、吳顯亮、梅順量，〈全媒體環境下推進認知域作戰裝備發展的幾點思考〉，《國防科技》，第39卷第5期，2018年，頁41-42。

18中共2015年以前的「七大軍區」時期僅有類似「電子對抗部隊」的戰略支援力量，但缺乏統一的領導機構，2015年底成立戰略支援部隊，並將原四大總部(陸、海、空、火箭軍)的航天、電子戰及信號情報，移轉到了戰略支援部隊，為各軍種提供網路及衛星等軍事作戰支援能力。黃郁文，〈中共軍事作戰支援能力：戰略支援部隊〉，《國防情勢特刊》，第22期，2022年，頁24。

19《中華民國110年國防報告書》（臺北：國防部，西元2021年10月），頁44。

20〈漢光演習電腦兵推 首次演練反制假新聞〉《公視新聞網》，https://news.pts.org.tw/article/429617，2019年4月22日，(檢索日期：2023年2月2日)。

戰場之決斷，進而將作戰結果導向有利我的方向進行，惟影響作戰因素除了軍隊外，亦包含一般社會大眾。在資訊科技與社群媒體發達的推波助瀾下，認知作戰戰場也從傳統實體領域轉進虛擬網路空間，在網路無遠弗屆特性的增強後，更加大了認知作戰之影響。有鑑於此，網路空間除了是惡意程式與資訊系統攻防戰之外，也是新型態認知作戰的主戰場。

二、認知作戰戰略操作層級及運用

「戰略」是針對國家安全與利益，綜合整體國力之目標、構想與執行的分析與運用，主要是建力用力、創機造勢、乘機用勢，俾得在爭取所望目標時，能獲得最大成功公算和有利效果。[21]從國家戰略與軍事戰略不同戰略層次看認知作戰內涵，分述如後。

(一)國家戰略層級

1.國家戰略層級的認知作戰主要由國家各部門和相關機構所主導，其受眾包括本國民眾及軍隊、敵國民眾與軍隊及國際友盟，主要影響國家的正常發展或造成國安危機，打擊政府威信，從認知領域打擊敵人之戰鬥意志，強化勝戰條件。

2.運用案例

(1)在2014年俄羅斯兼併克里米亞危機中，時任烏克蘭總統的亞努科維奇拒絕與歐洲聯盟簽署貿易與政治協定，此舉造成親歐盟示威者和警察發生流血衝突，也讓俄羅斯有可趁之機，使用「小綠人(配備俄國裝備的秘密武裝人員，但身上卻沒有任何識別徽章)」攻佔克里米亞政府大樓、電視台，關閉烏克蘭的電視台訊號，並以社群媒體、傳統媒體傳散假訊息，讓克里米亞民眾對烏克蘭政府產生不信任感，成功將實體空間衝突搭配認知作戰，以「民族自決」公投後「合法」併吞克里米亞。[22]

(2)美國眾議院議長南希·裴洛西於2022年8月率眾議院訪團訪問臺灣，此舉引發中共不滿，後續幾日總統府、外交部、國防部網站都有遭受攻擊，導致網站無法提供正常服務，攻擊狀況為平日的23倍，[23]雖然相關單位與部會已立即啟動防護機制，並未肇生資安事件，且網站異常狀況也迅速排除，惟此類中共網路攻擊主要在影響政府領導威信與擾亂社會秩序。

(二)軍事戰略層級

1.軍事戰略層級的認知作戰隸屬國家戰略之下，依循國家政策(戰略)

21王立申，〈戰略規劃與國軍建軍〉《海軍學術雙月刊》，(臺北)，第50卷第3期，2016年6月，頁2。
22同註6，頁ii。
23〈總統府、國防部、外交部遭網攻 政院：沒資安危機〉《聯合新聞網》，https://udn.com/news/story/6656/6511807，2022年8月4日，(檢索日期：2023年2月4日)。

與國防政策，軍事戰略層級的認知作戰由軍事部門主導，其他相關部門配合，透過展示軍事武力實況，遂行軍事作戰之認知作戰威懾作為。

2.運用案例

(1)中共解放軍自2022年8月4日至7日於我國周邊海域實施大規模軍演，除了飛彈試射、海空機艦威脅之外，亦運用「認知作戰」手段意圖擾我軍民士氣與心理。根據國防部統計，中共散布三種類型的爭議訊息，包括「營造武統氛圍」、「打擊政府威信」及「擾亂軍民士氣」，透過網路大量傳散與複製後，對我民心士氣之影響力不容小覷。[24]

(2)中共自圍臺軍演後，密集以民用小型無人機入侵金門、馬祖、東引等外離島防區，針對國軍前線陣地實施襲擾，此舉雖無立即危害，其目的為政治與軍事之針對性。[25]金防部於2022年9月1日中午，再次發現不明民用小型無人機進入獅嶼地區的禁限制水域上空後，隨即依標準作業程序，先實施示警無效後，將該無人機擊落。中共透過低成本之民用無人機實施營區空拍並上傳影片為其最新的認知作戰手法，成功執行其認知作戰作為與嚴重威脅我國軍營區安全，並造成營區駐守官兵壓力與士氣之影響。

(三)認知作戰各層級之關係

國家戰略層級的認知作戰係統合國家資源，依據政治、外交與國家利益，對敵國社會大眾遂行相關作為，其目的主要影響民眾情感、意志與意識形態，使其產生預期反應；在資訊科技發展下，網際網路的使用已經全面改變人類生活，遂行手段也多以網路空間之假訊息方式進行。

軍事戰略和戰術戰鬥層級的認知作戰以達成軍事戰略目標為主，惟仍須依循國家戰略目標遂行，其主要目的為影響軍事單位領導者的決策與判斷，也同時影響部隊士氣與戰鬥意志。雖然各層級的認知作戰之目的、對象與預期成效，略有不同，惟皆以「人」為主要對象。即使各階層目的不同，但在共同大目標下，各階層的認知作戰應相互搭配與執行，以發揮最大效益。此「不戰而屈人之兵」之用兵方式，也就是孫子「慎戰」的思想，相較傳統戰爭需要大量人力、物力和財力之損耗，甚至人員傷亡時，透過認知作戰實現國家利益為較高效的方式。

分析俄羅斯於俄烏戰爭中的認知作戰策略

24〈中共軍演也打「認知作戰」 國防部：本月已272則爭議訊息〉《自由時報》，https://news.ltn.com.tw/news/politics/breakingnews/4018471，2022年8月8日，(檢索日期：2023年2月4日)。

25〈也是認知作戰！中國無人機離島「打卡」常態化 金防部今成功擊毀一架落海〉《yahoo新聞》，https://news.campaign.yahoo.com.tw/2022-election/article.php?id=b4bac3c7-0315-31af-9953-6f7798e8b4b8，2022年9月1日，(檢索日期：2023年2月4日)。

在2022年2月24日凌晨，俄羅斯國家電視台播放了俄羅斯總統普丁講話影片，普丁宣稱因應兩天前由烏克蘭東部頓巴斯地區獨立的頓涅茨克和盧甘斯克等兩國求助，俄羅斯將派兵前往兩地執行「特別軍事行動」，其目的為使烏克蘭「非軍事化」和「去納粹化」；影片播放數分鐘之後，俄羅斯從陸地、空中和海上對烏克蘭發動了軍事攻擊，導彈也擊中烏克蘭境內的目標，普丁說明其行動是對威脅之自衛，他告訴俄羅斯同胞無佔領烏克蘭的計畫。[26]

俄羅斯入侵烏克蘭幾天後，網路上充斥著有關這場戰爭的假訊息，包含Instagram、Twitter、TikTok等都大量充斥描述烏克蘭實地情況之誤導性訊息和經過偽冒處理圖片，讓人難以分辨網路資訊的真偽。為了打擊有關烏克蘭的假訊息，Facebook於2022年2月24日下午成立了「特別行動中心」，以應對與戰爭有關的網路活動，並加速刪除違反Facebook所訂定標準之內容，而Twitter則分享了在俄烏戰爭地區使用其平台技巧。[27]顯見俄羅斯正在使用假訊息作為武器，配合實體戰場的入侵行動，同時對烏克蘭發動攻擊。

一、俄羅斯認知作戰手段運用

(一)俄羅斯假訊息生態系統

在俄烏戰爭中，俄羅斯不斷運用假訊息影響烏克蘭民眾的認知，其實在戰爭之前，烏克蘭就已遭受假新聞攻擊，尤其是社群網站，要發動認知作戰，尤其是國家級之認知作戰，需要有組織、計畫及政府的資助。依據美國國務院全球參與中心(Global Engagement Center, GEC)的報告指出，俄羅斯「假訊息生態系統(Russia’s Disinformation Ecosystem)」主要組成包含官方通訊、國家資助之全球訊息、代理來源的培養、社交媒體武器化和網路假訊息等五項，分述如後：[28]

1.官方通訊(Official Government Communications)：來源包括克里姆林宮、部會或大使館聲明、俄羅斯政府官方帳號的社交媒體貼文以及俄羅斯官員聲明，這些是最明顯和最容易與俄羅斯關聯之來源。[29]

2.國家資助之全球訊息(State-funded Global Messaging)：是由克里姆林宮直接和公開資助的媒體機構，旨在傳播具有特定目的訊息管道，包括俄羅斯

26“Putin lashes out with ominous threat to Ukrainians and other countries”, CNN，https://edition.cnn.com/europe/live-news/ukraine-russia-news-02-24-22-intl/h_1d10d8f9522910cac8758c5dbc0f7d5e，(檢索日期：2023年2月6日)。

27“Fact-checking fake videos of Ukraine conflict”, CNN，https://edition.cnn.com/2022/02/26/politics/fake-ukraine-videos-fact-check/index.html，(檢索日期：2023年2月6日)。

28“Pillars of Russia’s Disinformation and Propaganda Ecosystem”, U.S. DEPARTMENT of STATE, 2020年8月, pp.9.

29同註26, pp.9.

著名媒體如「今日俄羅斯(RT)」和「俄羅斯衛星通訊社新聞(Sputnik)」、俄資外媒及國際俄羅斯社會文化機構，其目標為國內外民眾。[30]

3.代理來源的培養(Cultivation of Proxy Sources)：第三方新聞和分析媒體有其特定地區的受眾，若透過它們協助散播假訊息和宣傳，可淡化與俄羅斯政府之間關係。[31]

4.社交媒體武器化(Weaponization of Social Media)：利用社交媒體活動可影響其他國家的國內事務，包括試圖在外國選舉中施加影響、加劇抗議、引發動亂和國內對立。[32]

5.網路假訊息(Cyber-enabled Disinformation)：這包括駭客攻擊和資訊洩漏、網站攻擊、使用偽造網站進行網路間諜活動、製作偽造品及破壞官方來源或客觀媒體的可信度。[33]

克里姆林宮在其宣傳管道及情報服務上進行了大量投資，以進行惡意網路活動來支持假訊息工作，並利用偽裝成新聞網站或研究機構來傳播這些錯誤和誤導性的報導，[34]這些平台和策略構成了一個生態系統，其中不同元素相互增強後，創造了一種加乘效應，放大了假訊息之效果。

(二)俄羅斯的攻擊手段

俄羅斯軍隊於2022年2月24日入侵烏克蘭一個月前，烏克蘭外交部、內閣和安全暨國防委員會等機構遭受網路攻擊，導致網站暫停服務並在部分網站以烏克蘭語、俄語和波蘭語等三種語言留下「你的所有個人資料都已被公開，電腦上所有資料都已被銷毀，無法恢復」等威脅訊息。此次網路攻擊正值烏克蘭及其盟友對俄羅斯可能對烏克蘭發動新一波軍事攻擊行動發出警告之際，雖無法立即證實此次網路攻擊的幕後黑手，但烏克蘭外交部發言人指出，俄羅斯過去曾是類似網路攻擊之幕後黑手，而俄羅斯外交部未回應此事件。[35]雖然未發生個人資料外洩情況，政府網站無法提供正常服務除影響政府運作外，也企圖引發人心恐慌。

關於烏克蘭及其盟友假訊息已經在網路中甚囂塵上，俄羅斯總統普丁針對說俄語的烏克蘭人正在遭受「種族滅絕」聲明，被德國總理奧拉夫·蕭茲

30同註26, pp.9.
31同註26, pp.9.
32同註26, pp.9.
33同註26, pp.9.
34同註26, pp.3.
35“Massive cyberattack hits Ukrainian government websites as West warns on Russia conflict”, REUTERS，https://www.reuters.com/technology/massive-cyberattack-hits-ukrainian-government-websites-amid-russia-tensions-2022-01-14/，(檢索日期：2023年2月8日)。

斥為「荒謬」，因為沒有證據可證實烏克蘭東部發生種族滅絕之情況。[36]此外，普丁使用了二次世界大戰「去納粹化」乙詞，該詞為戰後時代的一個特定時刻，因普丁恐懼當前烏克蘭民主政府而濫用「去納粹化」當作認知宣傳重點，[37]但這些聲明都只是俄羅斯對烏克蘭入侵的片面之詞。

俄羅斯假訊息再次顯示了它對烏克蘭和其他歐洲國家構成的威脅，(VoxCheck)統計了2022年2月24日至2022年11月15日俄烏戰爭期間，俄羅斯透過41個俄羅斯Telegram[38]頻道與18個親俄羅斯Telegram頻道發布了5,579則假訊息，這些訊息可區分為19個類別(如表1)，其論述主題皆與俄烏戰爭相關，涉及領域從烏克蘭內政、外交、人道、糧食、軍武及歷史等議題，[39]數量前三大議題依序為「烏克蘭有軍事生物和藥物實驗室」、「烏克蘭是恐怖主義國家」與「俄羅斯入侵具正當性」，其意圖無非合理化俄羅斯入侵的正當性。由於Telegram缺乏內容過濾機制和提供加密和未加密之聊天功能，已成為獨立新聞、宣傳和虛假信息的來源。其中，俄羅斯Telegram頻道主要受眾為俄羅斯民眾，而親俄Telegram頻道是指偽烏克蘭頻道，其訊息發布對象為烏克蘭民眾，並試圖展現該頻道是獨立媒體的印象，俄羅斯情報人員也涉入部分頻道。自戰爭開始以來，Telegram已成為烏克蘭人主要訊息來源，其次是YouTube，[40]這也是俄羅斯遂行假訊息時最頻繁使用Telegram的原因。

36“Ukraine crisis: Vladimir Putin address fact-checked”, BBC，https://www.bbc.com/news/60477712，(檢索日期：2023年2月8日)。

37“Historians on What Putin Gets Wrong About ‘Denazification’ in Ukraine”, TIME，\，(檢索日期：2023年2月8日)。

38Telegram是在2013年由兩名俄羅斯兄弟Nikolai Durov與Pavel Durov所創立，提供端對端加密的通訊服務，支援桌面與行動平臺，還能傳送大型檔案。Durov兄弟也是俄羅斯社交網站VK的創辦人，為了閃避俄羅斯政府的施壓，他們把Telegram的總部設在杜拜，同時標榜不會提供用戶資料予各國政府，因而成為許多民主活動的重要通訊平臺。

39〈烏克蘭VoxCheck培力全球查核組織 揭露俄羅斯19個戰爭假訊息論述〉《臺灣事實查核中心》，https://tfc-taiwan.org.tw/articles/8670，2023年1月11日，(檢索日期：2023年2月15日)。

40“Disinformation and Russia’s war of aggression against Ukraine”, OECD，https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/，(檢索日期：2023年2月15日)。

表1 俄羅斯傳散Telegram假訊息種類與數量統計表

俄羅斯2022年2月至11月傳散Telegram假訊息統計表					
項次	名稱	發布期	俄羅斯頻道	親俄頻道	小計
1	納粹主義在烏克蘭	2~11月	215	101	316
2	俄羅斯的入侵具正當性	2~11月	340	62	402
3	詆毀或嘲笑烏克蘭政府的代表性	2~11月	207	151	358
4	烏克蘭人道救援物資遭盜用	2~11月	25	53	78
5	烏克蘭人道主義的災難	2~11月	134	102	236
6	俄羅斯正在重建烏克蘭的城市	2~11月	141	24	165
7	烏克蘭轉售西方友盟提供的武器	2~3月	187	140	327
8	對俄制裁只會傷害西方國家	2~5月	100	75	175
9	烏克蘭是恐怖主義國家	2~4月 7~11月	412	123	535
10	俄羅斯軍隊未在烏克蘭犯下戰爭罪	2~3月 8~10月	196	121	317
11	抹黑烏克蘭難民	2~5月	135	59	194
12	西方國家為了已利控制烏克蘭	2~6月 8~11月	124	70	194
13	烏克蘭發生非法器官移植	2、7月	26	17	43
14	烏克蘭有軍事生物和藥物實驗室	4月	889	90	979
15	烏克蘭試圖在札波羅熱核電廠造成核災	4~5月 11月	94	101	195
16	抹黑烏克蘭的改革	5~11月	74	53	127
17	烏克蘭引發了烏克蘭和世界的糧食危機	6~11月	221	96	317
18	烏克蘭人想加入俄羅斯	8~10月	288	112	400
19	關於烏克蘭的歷史	9~10月	173	45	218
合計			3,981	1,595	5,576

資料來源：作者整理，參考 ”Disinformation about Ukraine in Russian and pro-Russian Telegram channels”，VoxCheck，https://narratives.voxukraine.org/en.html。

二、假訊息反制機制

(一)國際事實查核聯盟

在2022年2月24日俄羅斯開始入侵烏克蘭起，世界各地的事實核查人員就立即注意到有關戰爭和人道主義假訊息正在快速增加，各國出現不同錯誤訊息或影片在各大社群平台傳播。戰爭爆發後，「西班牙查核組織(Maldita.es)」聯手「國際事實查核聯盟(International Fact-Checking Network, IFCN)」建立協作計畫並創建「#UkraineFacts網站」，將來自全球68個國家、90個查核組織所彙整及查核的報告公布於網站供大眾查詢，已產製超過2,748篇查核報告。[41]該網站透過世界地圖方式顯示各國查核組織的查核報告內容與統計數量，其中有68篇臺灣地區查核報告為臺灣事實查核中心所產製。

(二)美國新聞和資訊可信度監測公司

俄羅斯透過官方媒體來源、匿名網站和帳號等方法在網路社群媒體傳播假訊息，以促進克里姆林宮的利益及破壞其敵對國家。自2018年以來，美國新聞和資訊可信度監測公司(NewsGuard)[42]一直在追蹤這些來源和方法，並將其關於俄羅斯宣傳工作的資料提供給美國國務院、美國網戰司令部以及其他政府和國防單位，截至2023年1月10日止已確定並正在追蹤329個發布假訊息或親俄宣傳網站，其中3個最有影響力的網站是官方媒體來源「俄羅斯電視台(RT)」、「俄羅斯塔斯社(TASS)」和「俄羅斯衛星通訊社(Sputnik)」。[43]

(三)烏克蘭事實查核組織

烏克蘭事實查核組織(StopFake)於2014年3月由基輔大學莫亥勒新聞學院(Mohyla School of Journalism)的老師、校友與學生所組成，並以烏克蘭文、俄文等13個不同之歐洲語言發布假訊息的查核報告，以抵擋俄羅斯假訊息活動。當時時空背景為俄羅斯併吞克里米亞，作為俄羅斯的鄰國，烏克蘭是俄羅斯假訊息之最佳試驗場，並可將試驗成果應用於其他國家。該組織的查核者冉克沃伊(Zamkovoi)指出，在俄羅斯軍隊大規模進攻之前，俄國已於2022年初即以頻繁、大規模方式進行心理戰，企圖從內部分裂與說服烏克蘭社會與人民，

41“#UkraineFacts”, IFCN，https://ukrainefacts.org/，(檢索日期：2023年2月15日)。

42NewsGuard專門評估新聞網站可信度並追蹤不實資訊，並延攬了許多訓練有素的記者替這些新聞與資訊網站以「營養標籤」（Nutrition Label）進行評分，他們根據包含涉及可信度與透明度的9項標準來判斷網站是否可靠，包括不會重覆出版不實內容、負責任地蒐集與呈現內容、會澄清錯誤、會明確處理新聞與意見的差異、避免建立欺騙性的標題、披露網站的所有權與資金來源、清楚標識廣告內容、公布網站負責人與利益衝突，以及揭露作者資訊等。〈微軟贊助、可辨識新聞網站可信度的免費瀏覽器擴充程式NewsGuard問世了〉《iThome》，https://www.ithome.com.tw/news/125499，2018年8月27日，(檢索日期：2023年7月28日)。

43“Russia-Ukraine Disinformation Tracking Center”, NewsGuard，https://www.newsguardtech.com/special-reports/russian-disinformation-tracking-center/，(檢索日期：2023年2月15日)。

自2014年以來，可歸納出俄羅斯假訊息的七大類別：「烏克蘭是一個失敗國家」、「貶低烏克蘭軍方跟地方防衛隊」、「任何條件下的和平都比對抗好」、「挑撥俄語與烏克蘭語人口的衝突」、「在烏克蘭與歐盟、北約之間挑撥，阻止合作」、「在烏克蘭各地操弄地方議題，展開地方層級的資訊操作」及「製造烏克蘭國內政治混亂」。[44]

StopFake不論晝夜，24小時查證俄羅斯媒體放出的消息，在戰爭爆發後，大量讀者向他們投訴自己看到之可疑訊息。該組織查核記者艾琳娜·莫森茲（Alina Mosendz）以「烏克蘭經驗」指出，在使用資訊時，必須要小心檢視資訊的來源，並思考誰會因為這個資訊而受益。[45] StopFake也關注尚未在國際媒體上曝光的貼文，例如該組織於2022年12月30日指出，俄羅斯Telegram頻道上最近出現一篇貼文，聲稱烏克蘭人正在購買印有納粹黨徽之聖誕樹裝飾品，這些照片實際上是在某家德國博物館所拍攝，該博物館曾經展出過希特勒時代的聖誕裝飾品，[46]這種假訊息切合普丁「去納粹化」訴求。

三、認知作戰與軍事作戰之關聯分析

為了解俄羅斯認知作戰操作方式，筆者彙整2022年2月至11月間之國際軍事行動與網路假訊息之時序對照圖(如圖2)，藉以發現兩者的關聯性與企圖達成之效益，敘述如下：

(一)發展歷程與趨勢

在戰爭初期，假訊息主題多為「俄羅斯入侵具正當性」、「納粹主義在烏克蘭」、「烏克蘭是恐怖主義國家」等類型，主要呼應俄羅斯派兵前往烏東地區執行「特別軍事行動」的必要性，以符合普丁聲明將使烏克蘭「非軍事化」和「去納粹化」之目的。

(二)合理化戰爭行為

戰爭過程常因被侵略國家非正規軍隊於民宅或非軍事設施進行攻擊而發生誤傷平民事件，因此有「俄羅斯軍隊未在烏克蘭犯下戰爭罪」的假訊息流傳。此外，伴隨戰事僵持，俄軍也開始攻擊烏國基礎設施，企圖擾亂社會民心與運作，同時開始傳散「烏克蘭試圖在札波羅熱(Zaporizhzhia)核電廠造成核災」的假訊息，以證明對民用基礎設施之攻擊是正當的。

44〈有健康的媒體才能對抗資訊戰：烏克蘭破解「假訊息犯罪現場」、抓出俄國代理人的攻守兵法〉《報導者》，https://www.twreporter.org/a/russian-invasion-of-ukraine-2022-stopfake，2022年7月18日，(檢索日期：2023年2月15日)。

45〈【烏俄戰爭】來自戰場上的聲音 烏克蘭查核組織《Stop Fake》如何反擊俄國假訊息〉《臺灣事實查核中心》，https://tfc-taiwan.org.tw/articles/7093，2022年3月16日，(檢索日期：2023年8月1日)。

46"'Deny, deflect, distract': How Russia spreads disinformation about the war in Ukraine", CBC，https://www.cbc.ca/news/politics/disinformation-ukraine-stop-fake-org-1.6721522，(檢索日期：2023年8月1日)。

(三)攻擊領導者

在「詆毀或嘲笑烏克蘭政府的代表性」類型中，烏克蘭總統比外交部長、國防部長、部隊總司令及基輔市長遭詆毀案例最多，尤其在戰爭初期，其內容為總統從基輔逃跑之相關假訊息，惟烏國總統不斷透過影片向外界澄清，並親臨戰場向官兵慰勉，以打擊假訊息的影響。

(四)假訊息相互關聯

雖然俄羅斯散傳Telegram假訊息區分為19類，但假訊息之間有相互關聯性，例如「納粹主義在烏克蘭」、「關於烏克蘭的歷史」與「西方國家為了己利控制烏克蘭」等3類，從烏克蘭是俄羅斯歷史上的一部分、烏克蘭人和俄羅斯人是兄弟國家，因此俄羅斯不能讓西方國家控制烏國，透過清除烏國納粹主義名義出兵，以完整合理化俄羅斯的入侵行動。

(五)挑戰普世價值

戰爭開始之後，軍人死傷當然是大眾關注焦點，但是更能讓各國與人道救援組織關注的就是難民相關議題，俄羅斯以「抹黑烏克蘭難民」類型假訊息，挑戰人道價值之普世概念，透過謊報烏克蘭難民抵達歐洲後搶劫商店且具攻擊性，讓歐洲各國無法接受難民，並試圖將他們驅逐出境的假新聞，企圖汙名化烏克蘭難民。

前述部分手法中共曾對臺灣進行，例如攻擊領導者，在2022年9月14日，俄烏戰爭開戰約7個月後，臺灣事實查核中心指出，中國影音平台快手發布「如果中國開始收復臺灣，蔡英文逃到美國，美國會收留她嗎問答記者會」的虛構影片，查證後，影片內容與總統蔡英文無關，是五角大廈發言人柯比針對俄國與北約的狀況答覆記者之內容；[47]在2022年8月2日美國聯邦眾議院議長裴洛西訪臺後，在中國大陸網路論壇上便出現「授權新華社向全世界通告：中華人民共和國恢復行使對臺灣主權，臺灣一切海權、空權由中華人民共和國管轄」的假新聞，企圖影響臺灣外交成果與合理化對臺灣實施各種主權之主張，[48]由此可知中共對臺灣進行的認知作戰是有組織、有目的且不斷變化進行。

47〈【錯誤】網傳影片「如果中國開始收復臺灣，蔡英文逃到美國，美國會收留她嗎 問答記者會」？〉《臺灣事實查核中心》，https://tfc-taiwan.org.tw/articles/8154，2022年9月14日，(檢索日期：2023年6月30日)。

48〈【錯誤】網傳「授權新華社向全世界通告：中華人民共和國恢復行使對臺灣主權，臺灣的一切海權、空權由中華人民共和國管轄」？〉《臺灣事實查核中心》，https://tfc-taiwan.org.tw/articles/7987，2022年8月5日，(檢索日期：2023年6月30日)。

圖2 俄羅斯網路假訊息與國際/軍事行動時序對照圖

資料來源：作者整理，參考〈2022年俄羅斯入侵烏克蘭時間軸〉《維基百科》，https://zh.m.wikipedia.org/wiki/2022%E5%B9%B4%E4%BF%84%E7%BE%85%E6%96%AF%E5%85%A5%E4%BE%B5%E7%83%8F%E5%85%8B%E8%98%AD%E6%99%82%E9%96%93%E8%BB%B8，(檢索日期：20223年1月15日)。

四、小結

俄羅斯雖已建立假訊息生態系統，也擬定各種假訊息議題遂行認知作戰，企圖重現2014年成功模式，但卻事與願違。國防安全研究院助理研究員吳宗翰博士指出，俄羅斯長期對烏克蘭進行認知作戰、分化社會，在2014年爭奪克里米亞半島中獲得成功，但在此次俄烏戰爭裡，分化沒有達到俄羅斯要的效果。此次俄羅斯攻擊親近西方與親近俄羅斯的地區，影響民眾對俄羅斯觀感，也削

弱了認知作戰效果。[49]

從俄羅斯入侵開始，親俄電視台就被烏克蘭政府停播，並由幾家電視台發起聯合電視馬拉松(United TV Marathon)為戰爭初期最重要的訊息傳播來源，以確保烏克蘭人從他們認識及信任之主持人和廣播公司獲得可靠的全天候訊息，除有助於在戰爭初期肆應來自俄羅斯假訊息，也間接讓曾經同情俄羅斯之烏克蘭人改變想法，而講俄語的人在日常生活中也轉向烏克蘭語，因為他們希望切斷與俄羅斯一切聯繫。儘管俄羅斯雖運用認知作戰沒有取得成功，俄羅斯仍將繼續散佈虛假訊息，目的是瓦解烏克蘭抵抗，播下內部分裂的種子，破壞對政府和軍隊之信任，讓人們感到冷漠和軟弱。[50]

應對認知作戰策略芻議

社交網路是全球最受歡迎網路活動之一，也是日常上網不可或缺的一部分，伴隨新媒體與行動裝置之發達，預計2023年全球社交媒體用戶數量將達48.9億人，[51]因此網路空間更能與大眾連結，也成為兵家必爭之地。再者，民主國家特點是政府需要向大眾公開許多訊息，讓民眾更了解政府施政方向及成效，以獲得更多民眾對政府支持，其方式不外乎電視、廣播、網路媒播或是網路社群等平台，且依現今資通科技發展，前述平台大多透過網路為主流媒介。

而認知作戰就是利用輿論自由及網路普及等特點，遂行其影響社會大眾的認知並可加劇衝突、破壞或分裂本來具有凝聚力之社會秩序，對民主國家的威脅較訊息被管控的共產國家更為嚴峻。伴隨愈趨繁忙的社會活動，人們只能快速獲得所需資訊，若網路媒播或意見領袖傳達之訊息有誤，將影響甚鉅，且在網路空間遂行作戰行動較實體空間的軍事行動成本更為低廉且影響範圍更大。綜合俄烏戰爭於網路空間遂行認知作戰之諸般手段及其影響，本研究就國軍未來面對敵之認知作戰因應策略，提列建議如下：

一、國際跨域交流合作，識假破假作業同步

在國際方面，「#UkraineFacts網站」有68篇在臺灣地區的查核報告，除包含臺灣事實查核中心查核報告亦包含其他在臺媒體，故應爭取友我國家之協作與共享，可透過非營利組織「臺灣事實查核中心」民間身分擴大我國在國際組織及媒體的交流合作。此外，可仿效南韓，以貢獻參與者身分加入北約卓越

49〈俄烏戰爭的第二戰場：臺灣成假訊息受害者 攻擊美國、仰賴中國成主力〉《READr》，https://www.readr.tw/post/2902，2022年3月28日，(檢索日期：2023年6月30日)。

50“A Year of Lies: Russia’s Information War Against Ukraine”, CEPA，https://cepa.org/article/a-year-of-lies-russias-information-war-against-ukraine/，(檢索日期：2023年8月1日)。

51“Number of social media users worldwide from 2017 to 2027”, statista，https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/，(檢索日期：2023年2月15日)。

聯合網路防禦中心(CCDCOE)，與北約各國交流網路安全[52]情資、研究、訓練和演練，除擴大我國際參與及經驗分享外，亦能多管道獲得網路威脅資訊，以迅速及全方位因應假訊息的威脅。

而因應資訊傳遞無疆界限制與容易大量複製的特性，訊息傳遞不但非常容易且迅速，借鏡俄烏戰爭假訊息傳遞內容可以發現，假訊息之主題包含各個面向，不管是政治、軍事、外交、法律、人道、災難甚至歷史等，都是可以是攻擊的主題，且可以同時進行，也只有國家級組織才能執行此類活動，因此政府各部會應充分協調、合作與整合，才能因應假訊息威脅。我國於2018年4月由臺灣媒體教育觀察基金會與優質新聞發展協會成立「臺灣事實查核中心」負責公布假訊息查核報告，復於2020年由國安局成立「國家安全作業中心」負責「協調整合部署執行對境外敵對勢力爭議訊息應處有關事項」，未來將國防領域納入管制，滿足同步識假、破假之作業能量，方足以應對。

二、統合國軍部隊戰力，肆應反制認知作戰

由俄羅斯執行認知作戰的方式可知，從議題擬定與製作、宣傳管道建立與維持、受眾接收方式與反應等面向，證明要執行認知作戰需要投入大量資源，才能依受眾或他國反應，調整執行內容，唯有國家級力量始能整合公私部門、社群或意見領袖，共同遂行此類活動。認知作戰是跨單位與領域的行動，除前述軍民單位合作外，國軍內部也需要深化整合心戰與資訊戰力，如心理作戰大隊製作反制文宣圖卡及影片等心戰成品後，透過心戰作業車對敵實施心戰喊話，成果較為受限，如能透過網路方式傳散，可大大增加心戰效果，而資通電軍指揮部具資通專業人才，雙方可建立協作機制，強化雙方認知心理學、資通科技、輿情分析等專業知識，並透過演習或任務方式，驗證整合成效。

兩岸雖以中文為官方語言，惟兩岸用詞用語仍有不同，孫子有云：「知彼知己，百戰不殆」，為精準掌握中國大陸地區輿論動向，應先熟悉「兩岸差異用詞」，藉以認識在中共極權統治下，現今中國大陸民眾文化特性及習性，以剖析其社會脈動，達成知敵的目標。另外在科技應用部分，應持續增進資通科技能量，除研析中國大陸境內註冊用戶數達上億之社群網站或應用程式，如微博(微型網誌社交網站，被稱為「中國版twitter」)、微信(即時通訊軟體)、小紅書(網路購物和社交App，外界稱為「中國版的Instagram」)、抖音(短片分享平台)等平台外[53]，亦需相關建立情研資料庫，透過大數據分析方式，以數據化及

52【網路安全】（Cyberspace Security）：防護及復原電腦、電子通信、有線通信之系統（含系統內之資訊）與服務，以確保其可用性、完整性、機密性及不可否認性。國軍軍語辭典》，頁9-2。

53〈內地社交平台｜認識內地4大社交App：小紅書、抖音、微博、微信 小紅書取代IG？〉《yahoo新聞》，https://hk.news.yahoo.com/%E5%85%A7%E5%9C%B0-%E7%A4%BE%E4%BA%A4%E5%B9%B3%E5%8F

趨勢判斷方式，解析中國大陸民眾對特定主題的輿論動向，先期掌握潛在對臺不利言論之發酵，藉以擬定並傳散適切利我內容，提供正確認知，化被動為主動。

三、健全自我文化意識，融入教育強化反制

在現今網際網路發達時代，網路流行語、新鮮詞、梗圖或轉載文章也不斷出現在各類媒播或網路社群，而中國大陸流行語，例如：「閨蜜」、「信息」、「網紅」、「學霸」、「視頻」、「顏值」、「老司機」等字句，[54]也隨著影劇熱播，於無形中融入臺灣人民的日常生活中。此現象為長年累積而成，這種不具立即威脅且潛移默化以電視劇、影片或社群的文化入侵，也是中共對新型態對臺統戰手段之一。因此在兩岸交流過程中，為避免過度傾向中國大陸文化，應健全我國自我文化意識，熟悉與認同我國語言、文化、歷史、土地、社會、政治、軍事等要素，如此才能在兩岸相似與共通之語言與文化中，降低被混淆或誤導的風險。

文化的影響是長期且深遠，針對自我文化意識之深根，應納入各階層軍事教育內容，惟應針對不同層級教育班隊或課程，擬定教育主題及內容，深究不同主題背後含意及目的，並同步建立數位教學內容，在由淺入深，逐步深化對不同主題的自我文化意識提升後，也能透過數位教材加深熟悉度，對我國文化有正確及深入之認知與了解。

四、增進國軍數位素養，提升虛假訊息思辨

在資訊科技發達時代，因多元數位工具及巨量網路資訊，對工具及資訊之正確使用與認知便愈顯重要，這也是數位素養的要素。面臨日趨嚴重假訊息的挑戰，我國國防部由政治作戰局軍事新聞處負責反制中共解放軍對臺實施認知作戰，也在2022年8月初美國眾議院議長裴洛西訪問臺灣之後，掌握272則演習相關假訊息，惟相關資料僅於國防部記者會上說明，未見深入分析報告於國防部首頁或政戰資訊服務網公布，以供國人或國軍官兵能進一步了解共軍對我實施認知作戰之方式，藉以強化我應處作為。建議除定期公布相關研析報告供大眾了解共軍對我認知作戰方式及手段外，亦可由國軍專責單位錄製相關宣導影片供部隊運用，並不定期舉辦講習，由國軍專業新聞人員運用實際案例向部隊說明假訊息運作方式及識假之經驗與方法，置於重點訊息辨識技巧的熟稔及推理，使國軍官兵從識假進而破假，增進思考判斷技巧，養成理性思考

%B0-%E5%B0%8F%E7%B4%85%E6%9B%B8-%E6%8A%96%E9%9F%B3-%E5%BE%AE%E5%8D%9A-%E5%BE%AE%E4%BF%A1-085414395.html，2023年6月12日，(檢索日期：2023年6月30日)。

54〈中國流行語入侵與新型文化統戰〉《Newtalk新聞》，https://newtalk.tw/citizen/view/56975，20221年4月16日，(檢索日期：2023年2月24日)。

各類報導並多方求證之習慣，避免遭敵誤導。

此外，針對遂行認知作戰技術層面也應研析與了解，現今遂行認知作戰多使用資訊科技的協助，例如：網路機器人、假帳號、社交工程攻擊、深度造假、大數據分析等技術，順應各類社群媒體蓬勃發展，人們也習慣於各類媒體分享個人資訊，舉凡生日、學經歷、電話、地址、喜好、照片、打卡、影片或評論等內容，大量增加個人在網路空間的數位足跡，為降低國軍官兵數位足跡遭敵蒐羅，在揭露個人有關資訊前，應審慎思考遭敵運用風險，建議應降低個人數位足跡，避免遭敵發展認知作戰之使用。

結論

《中華民國110年國防報告書》指出中共透過灰色地帶衝突對我國之威脅日趨嚴重且手段多元，主要包含軍事及非軍事等兩個層面。在軍事侵擾手段中，包括侵入我防空識別區、加大我周邊海域演訓力度、強化軍事威懾作為等；非軍事手段包括網路戰[55]危害與認知作戰等，中共除在實體空間不斷對我國進行武力威懾，企圖在我國人民心中植入解放軍的強大外，亦同步於虛擬空間透過各種傳媒平台的假訊息對我國進行認知作戰，以打擊我國人抗敵信心，進而改變社會大眾對中共之意識形態，最後再加上政治、經濟與外交等手段，建構出包含國家戰略與軍事戰略的對臺統戰策略。借鏡俄烏戰爭實際狀況，惟有統合國家各公私部門通力合作，始能因應此種複合式威脅。

認知作戰遊走在模糊地帶，並具備平戰不分、戰域難定、真假難辨等特性，運用現今資訊科技與新媒體，以低成本、低強度、範圍廣的非軍事手段，在高度媒體自由之國家與地區，可發揮加乘的效果。近期，生成式人工智慧（Generative AI）獲得高度討論，利用人工智慧生成內容（AI Generated Content ,AIGC）可快速、輕鬆產製大量訊息內容，如運用在假訊息產製，大大降低製作門檻，再搭配ChatGPT或深偽（Deep Fake）技術，將可增加認知作戰的效度與廣度。鑑此，除國防部持續強化與各單位合作破除假訊息之同時，國軍官兵在戮力戰訓本務之際，也須了解攻心的認知作戰之目標、方法與手段，不斷提升對訊息分析與判斷技巧，養成獨立思考與求證的習慣，並逐步降低個人數位足跡，避免在資訊時代，遭假訊息蒙蔽與遭敵利用。

55【網路戰】（Cyberspace Operations）：運用電腦系統、網際網路或通信網路之網路空間（Cyberspace），藉網路情蒐等手段，獲取軍事所需情報，並掌握敵系統弱點，適時對敵實施破壞、阻絕、衰退或摧毀存在於電腦與網路空間上之資訊，甚至是電腦及網路空間本身的相關作為，以達成軍事目的。《國軍軍語辭典》，頁9-2。

參考文獻

中文部分

一、官方文件

《中華民國110年國防報告書》（臺北：國防部，2021年10月），頁44。

二、期刊專題

(一)劉惠燕、熊武、吳顯亮、梅順量，〈全媒體環境下推進認知域作戰裝備發展的幾點思考〉《國防科技》，第39卷第5期，2018年，頁41-42。

(二)王立申，〈戰略規劃與國軍建軍〉《海軍學術雙月刊》，(臺北)，第50卷第3期，2016年6月，頁2。

三、學位論文

劉緯憲，〈2014年克里米亞危機中認知作戰之研究〉(國防大學政治作戰學院，政治學系碩士論文，2022年)，頁ii。

四、網際網路

(一)〈強化媒體識讀 反制中共認知作戰〉《青年日報》，https://www.ydn.com.tw/news/newsInsidePage?chapterID=1522591。

(二)〈北約網路軍事演練首度加入認知作戰情境〉《行政院國家資通安全會報技術服務中心》，https://www.nccst.nat.gov.tw/NewsRSSDetail?lang=zh&RSSType=news&seq=16547。

(三)〈腦計畫：世界科技競爭新高地〉《解放軍報》，2016年10月20日，http://www.81.cn/jfjbmap/content/2016-10/20/content_159464.htm。

(四)〈漢光演習電腦兵推 首次演練反制假新聞〉《公視新聞網》，https://news.pts.org.tw/article/429617，2019年4月22日。

(五)〈總統府、國防部、外交部遭網攻 政院：沒資安危機〉《聯合新聞網》，https://udn.com/news/story/6656/6511807，2022年8月4日。

(六)〈中共軍演也打「認知作戰」 國防部：本月已272則爭議訊息〉《自由時報》，https://news.ltn.com.tw/news/politics/breakingnews/4018471，2022年8月8日。

(七)〈也是認知作戰！中國無人機離島「打卡」常態化 金防部今成功擊毀一架落海〉《yahoo新聞》，https://news.campaign.yahoo.com.tw/2022-election/article.php?id=b4bac3c7-0315-31af-9953-6f7798e8b4b8，2022年9月1日。

(八)〈烏克蘭VoxCheck培力全球查核組織 揭露俄羅斯19個戰爭假訊息論述〉《臺灣事實查核中心》，https://tfc-taiwan.org.tw/articles/8670，2023年1月11日

(九)〈有健康的媒體才能對抗資訊戰：烏克蘭破解「假訊息犯罪現場」、抓出俄國代理人的攻守兵法〉《報導者》，https://www.twreporter.org/a/russian-invasion-of-ukraine-2022-stopfake，2022年7月18日。

(十)〈【烏俄戰爭】來自戰場上的聲音 烏克蘭查核組織《Stop Fake》如何反擊俄國假訊息〉《臺灣事實查核中心》，https://tfc-taiwan.org.tw/articles/7093，2022年3月16日，(檢索日期：2023年8月1日)。

(十一)〈【錯誤】網傳影片「如果中國開始收復臺灣，蔡英文逃到美國，美國會收留她嗎 問答記者會」？〉《臺灣事實查核中心》，https://tfc-taiwan.org.tw/articles/8154，2022年9月14日。

(十二)〈【錯誤】網傳「授權新華社向全世界通告：中華人民共和國恢復行使對臺灣主權，臺灣的一切海權、空權由中華人民共和國管轄」？〉《臺灣事實查核中心》，https://tfc-taiwan.org.tw/articles/7987，2022年8月5日。

(十三)〈俄烏戰爭的第二戰場：臺灣成假訊息受害者 攻擊美國、仰賴中國成主力〉《READr》，https://www.readr.tw/post/2902，2022年3月28日。

(十四)〈內地社交平台｜認識內地4大社交App：小紅書、抖音、微博、微信 小紅書取代IG？〉《yahoo新聞》，https://hk.news.yahoo.com/%E5%85%A7%E5%9C%B0-%E7%A4%BE%E4%BA%A4%E5%B9%B3%E5%8F%B0-%E5%B0%8F%E7%B4%85%E6%9B%B8-%E6%8A%96%E9%9F%B3-%E5%BE%AE%E5%8D%9A-%E5%BE%AE%E4%BF%A1-085414395.html，2023年6月12日。

(十五)〈中國流行語入侵與新型文化統戰〉《Newtalk新聞》，https://newtalk.tw/citizen/view/56975，20221年4月16日。

英文部分

一、官方文件

(一)“Network Centric Warfare”,Department of Defense, 2001/7/27,pp.3-7.

(二)“Joint Publication 3-12 Cyberspace Operations”, Joint Chiefs of Staff,2018, pp.I-7.

(三)“Pillars of Russia’s Disinformation and Propaganda Ecosystem”, U.S.DEPARTMENT of STATE, 2020年8月, pp.3.

二、網際網路

(一)“Russia launches military attack on Ukraine with reports of explosionsand troops crossing border”, CNN，https://edition.cnn.com/2022/02/23/europe/russia-ukraine-putin-military-operation-donbas-intl-hnk/index.html。

(二)“Ukraine conflict: Many misleading images have been shared online ”,BBC，https://www.bbc.com/news/60513452。

(三)“Goldfein delivers Air Force update”, US Air Force，https://www.af.mil/News/Article-Display/Article/1316603/goldfein-delivers-air-force-update/。

(四)“U.S. National Guard’s Cyber Training Emphasizes Social Media, Supply Chain Protection”, Nextgov，https://www.nextgov.com/cybersecurity/2022/06/us-national-guards-cyber-training-emphasizes-social-media-supply-chain-protection/367872/。

(五)“Cognitive Warfare: Strengthening and Defending the Mind”, NATO’s Strategic Warfare Development Command，https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/。

(六)“Countering cognitive warfare: awareness and resilience”, NATO REVIEW，https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html。

(七)“Putin lashes out with ominous threat to Ukrainians and other countries”, CNN，https://edition.cnn.com/europe/live-news/ukraine-russia-news-02-24-22-intl/h_1d10d8f9522910cac8758c5dbc0f7d5e。

(八)“Fact-checking fake videos of Ukraine conflict”, CNN，https://edition.cnn.com/2022/02/26/politics/fake-ukraine-videos-fact-check/index.html。

(九) “Massive cyberattack hits Ukrainian government websites as West warns on Russia conflict”, REUTERS，https://www.reuters.com/technology/massive-cyberattack-hits-ukrainian-government-websites-amid-russia-tensions-2022-01-14/。

(十) “Ukraine crisis: Vladimir Putin address fact-checked”, BBC，https://www.bbc.com/news/60477712。

(十一) “Historians on What Putin Gets Wrong About ‘Denazification’ in Ukraine”, TIME，https://time.com/6154493/denazification-putin-ukraine-history-context/。

(十二)“Disinformation and Russia’s war of aggression against Ukraine”, OECD，https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/。

(十三)“#UkraineFacts”, IFCN，https://ukrainefacts.org/。

(十四)“Russia-Ukraine Disinformation Tracking Center”, NewsGuard， https://www.newsguardtech.com/special-reports/russian-disinformation-tracking-ce

nter/。

(十五)"Deny, deflect, distract': How Russia spreads disinformation about the war in Ukraine", CBC，https://www.cbc.ca/news/politics/disinformation-ukraine-stop-fake-org-1.6721522。

(十六)"A Year of Lies: Russia's Information War Against Ukraine", CEPA，https://cepa.org/article/a-year-of-lies-russias-information-war-against-ukraine/。

(十七)"Number of social media users worldwide from 2017 to 2027", statista，https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/。

作者簡介

蕭浩然中校，中正理工學院電機系92年班，國管指參班107年班，曾任分隊長、資網官、課長、科長，現任國防大學管理學院戰略班學員。

李建鵬中校，中正理工學院電機系87年班、國管指參班101年班，曾任電子官、修護組長、通參官、科長、資參官、電戰官，現任國防大學國防管理學院國管中心教官。