



FOCUS

專題報導

● 作者/Christopher H. Chin, Nicholas P. Schaeffer, Christopher J. Parker, and Joseph O. Janke

● 譯者/李永悌 ● 審者/黃坤銘

中共仿效俄羅斯資訊作戰 趨勢及對美聯合部隊意涵

When Dragons Watch Bears: Information Warfare Trends and Implications for the Joint Force

取材/2023年第二季美國聯合部隊季刊(*Joint Force Quarterly*, 2nd Quarter/2023)

爲因應未達武裝衝突門檻的大國競爭，中共深入研究俄羅斯資訊戰手法，藉此強化三戰效益，而美國應重新定義非傳統戰爭、成立統一中央資訊戰機構，以及建立傳統軍事體系外的資訊戰人才培育架構。

(Source: Shutterstock)

心理因素凌駕物質因素且會帶來長遠影響，由此得知，任何戰爭理論應儘可能海納百川。

——李德哈特(B.H. Liddell Hart)，《戰略論》(Strategy)¹

過去十年，中共抱以極高興趣觀察俄羅斯資訊戰(Information Warfare, IW)運用。鑑於近期烏克蘭衝突與2014年俄羅斯併吞克里米亞(Crimea)，中共正在積極評估，若選擇以武力統一臺灣時，西方國家的反應及對全球性之影響。中共試圖改寫全球規範，意圖對臺灣與亞太地區施加最大影響力，已成為當前步步進逼的威脅。「中」俄兩大強權的相似處，以及對其分裂自治共和國的相關侵略舉措，讓美國與聯合部隊有機會瞭解



2017年9月西方聯合戰略演習重大操演科目期間，俄羅斯總統蒲亭與總參謀長格拉西莫夫(Valery Gerasimov)大將於列寧格勒州(Leningrad Region)盧日斯基(Luzhsky)訓練場視導俄羅斯與白俄羅斯部隊操演實況。

(Source: President of Russia)

中共不斷演進的資訊戰戰略，俾於未來該區域衝突發生前擬定全面因應作為。鑑於現代資訊戰的行動範圍、複雜性及規模，欲於危機與衝突期間阻擾中共資訊對抗戰術，須果斷全面整合政府機關以團結一致。為能在二十一世紀資訊環境中拔得頭籌，美國防部應整合跨部會力量，在未來聯合部隊中主導三項措施：

- 擴大非正規作戰暨資訊戰範圍與規模，俾有效適應未達武裝衝突門檻的現代競爭連續光譜(未來一至三年)。
- 提倡建立專責中央機構，負責蒐整美國整體政府資訊相關活動，以對抗外國惡意舉措(未

來三至五年)。

- 以數位時代方式報效國家，成立平民網路團(Civilian Cyber Corps)作為美國第7軍種網路軍(U.S. Cyber Force，譯註：為與時下所謂「網軍」有所區分，故譯為「網路軍」)的先驅，以保衛美國、國家網路及傳統軍事行動，以建立遂行網路效應作戰所需要的部隊能量(未來五至七年)。

中共對俄羅斯資訊戰之省思

當今俄羅斯領導人與中共領導人一樣，認為西方民主國家經濟繁榮都是建立在他們的痛苦之

上。軍事欺敵(Maskirovka)構想不僅是俄羅斯應對衝突之戰略方針，更是其控制國際社會觀感、實現國家利益、創造有利態勢的官方整體宣傳做法。² 資訊戰活動對軍事欺騙構想至關重要，旨在對敵人進行擾亂、超載、癱瘓、虛耗、欺騙、分裂、安撫、嚇阻、激怒及施壓等戰術。³ 這些戰術可以個別運用，但必須注意，俄羅斯資訊戰活動與軍事作戰密切整合，而其軍事作戰旨在先發制人、出其不意、隱匿意圖、卸責，進而延後戰略後果，讓國際統一因應作為只能向隅。⁴ 遂行軍事欺騙時最常見手段包括假旗行動(False Flag Operations)、僱用代理人散布假訊息、運用諸如瓦格納集團(Wagner Group)等私人軍事/傭兵企業，以及在東歐、非洲、中東及美國各地僱用駭客主義者而試圖規避國際社會究責。以上作為通常會同時進行，以便在演習或衝突前營造有利環境。

2008年俄羅斯陸軍入侵喬治亞共和國後，各軍區輪流舉辦四場大型演習(西方[Zapad]、東方[Vostok]、中央[Tsentr]及高加索[Kavkaz，俄羅斯南部軍區]等

演習)成為俄羅斯年度盛事。這些演習讓莫斯科得以隱藏真實意圖，同時適應作戰環境，使其得以避開《維也納文件》(Vienna Document)律定之1萬3,000人門檻，在外國觀察員不在場的情況下大幅調動兵力。⁵ 俄羅斯每次進行重大軍事演習前，幾乎都會進行資訊戰，並通常會執行俄羅斯決策者屬意的「圍城」(Besieged Castle)。2014年，俄羅斯西方演習(與俄羅斯併吞克里米亞)前的資訊活動將重點置於戰略論述，其目的在散布令人畏

懼的言論——演習想定描寫波蘭與立陶宛等北大西洋公約組織(North Atlantic Treaty Organization)會員國支持針對白俄羅斯與加里寧格勒州(Kaliningrad Oblast)等俄羅斯領土的恐怖主義。⁶ 此舉為俄羅斯併吞克里米亞提供了兩項重大優勢：一是能根據虛構演習想定，將軍事行動意圖定調為防禦性質，二是激勵民眾支持保衛克里米亞境內俄羅斯族裔。

相較之下，中共在進行戰略軍事演習前，並沒有進行規模



2022年5月1日，美陸戰隊第1遠征軍資訊群心戰連心戰士普拉多(Estefany Gomez Prado)中士，於加州二十九棕櫚村(Twenty-nine Palms)陸戰隊基地陸戰隊陸空特遣部隊3-22戰鬥演習期間，與參演人員進行意見交換。

(Source: USMC/Benjamin Aulick)



2019年12月17日，習近平於海南省三亞軍港登上山東號航空母艦進行校閱。

(Source: Xinhua/Li Gang)

媲美俄羅斯的資訊戰。但卻有相似運用「圍城」的思維，中共營造恐怖主義威脅維吾爾人，⁷並頒布「香港國安法」律定「分裂國家、顛覆國家政權、組織恐怖活動或勾結境外勢力危害國家安全者，最高可判處無期徒刑」。⁸中共已利用此種論述獲得巨大成效，目前更準備向俄羅斯多方學習，例如近期首度安排俄羅斯軍隊於中國大陸境內進行聯合戰略演練。⁹

作為威權政府，中共與俄羅斯已成功展示整合協調政府機關遂行資訊戰的意圖與能力。這兩個政權皆擁有執行周密資訊戰活動的機制，有悖於

二十一世紀文明國家義務履行的國際規範與普遍期望。美國不諳此道，應憂心俄羅斯與中共刻正相互學習，共同對抗西方在各自勢力範圍內的影響力。

中共汲取俄羅斯資訊戰經驗教訓

中共宣傳人員深入研究俄羅斯，鑽研如何將虛假論述散布於資訊空間，並希望複製俄羅斯成功在影響美國行動與觀感等成果。中共政治圈所謂的「話語赤字」構想，指的是一種根深蒂固感受，亦即中共在全球討論與辯論中遭到毀謗，甚

至遭到忽視。¹⁰而補救措施就是加強自身「外宣」，亦即對外宣傳，積極地散布中共所望傳達的訊息。為執行這項計畫，中共媒體高層將「今日俄羅斯」(Russia Today, RT)電視臺等媒體稱為「對外宣傳航空母艦」(External Propaganda Aircraft Carrier)，並將其用於影響社群媒體輿論風向，突破外國營造的媒體環境。¹¹2018年，《人民日報》一篇文章中提到，今日俄羅斯在臉書、推特及YouTube等社群媒體上的影響力日益增長，與全球媒體不斷拓展合作範疇。此外，俄羅斯媒體戰略概可分為兩個統一戰略：一是積極表達俄羅斯對世界事件的觀點與看法，二是正面宣揚俄羅斯文化與民族。儘管中共分析師指出，外宣並不會澈底改變西方觀感，但卻可反制負面論述，讓反「中」媒體產生歧見。¹²

此外，愈來愈多人公開承認，俄羅斯經驗教訓值得中共宣傳人員研究學習。自2015年起，俄羅斯與中共每年舉辦「網絡媒體雲端論壇」(Internet Media Cloud Forum)。最近一次論壇於2020年底舉行，由中共官媒《中

國日報》(*China Daily*)主編與俄羅斯數位發展、通信及大眾媒體部副部長發表專題演講。此次集會聚焦在透過諸如人工智慧、大數據及5G電信系統等全新資訊科技，加強「中」俄雙邊交流。此外，俄羅斯與中共領導人還承諾，透過設立「媒體創新研究中心」(Media Innovation Research Center)與雙邊「人才交流」(Talent Exchange)等管道——此過程普遍被視為將俄羅斯資訊科技融入中共作戰行動的方式。¹³ 雙方合作範疇雖然有限，但已建立彼此資訊溝通管道。儘管中共資訊戰專家可能無法完美複製俄羅斯行動，但不可否認的

是，中共正在學習運用俄羅斯技術，特別是今日俄羅斯電視臺成功向西方閱聽人論述與深化「另類」觀點。

中共公開研究期刊亦提到前述立場。有人撰文公開表彰俄羅斯對西方國家的資訊戰，並說明「外部傳播力」(External Communication Power)如何成為國家軟實力的關鍵。近年來，中共持續強化外部傳播能力，仿效今日俄羅斯電視臺成功滲透西方思想的模式。俄羅斯國家制度與資訊傳遞流程，打造出日益完善的獨特國際傳播體系。¹⁴ 2015年底，俄羅斯衛星通訊社中文新



中共亦步亦趨，不斷仿效俄羅斯資訊戰作為，期能掌握國際輿論方向，透過社群媒體等多元管道向國際社會渲染自身另類觀點。(Source: Shutterstock)



2022年12月20日，烏克蘭總統澤倫斯基視導頓內次克(Donetsk Oblast)巴赫姆特(Bakhmut)前線部隊時，在烏克蘭國旗上簽名。

(Source: Ukrainian Presidential Press Office)

聞服務(Sputnik Chinese News Service)正式上線，成功設立微博與微信公開帳號，加強「中」俄國營媒體的官方與非官方合作。2015年，今日俄羅斯電視臺亦與新華社簽署合作協議，就聯合採訪與新聞活動展開長期合作。

更令人憂心的是，北京認為國家正處於「戰略機遇期」，促使共軍在南海與其他地區肆意擴大軍事作為。¹⁵ 中共正採用俄羅斯的獨特手法，透過未達國際社會反彈或挑起美「中」軍事衝突門檻的行動，擴大其影響力與戰略定位。

中共媒體業以特定方式觀察俄羅斯吞併克里米亞行動並汲取相關經驗教訓。首先，今日俄羅斯電視臺在輿論戰的準備階段，以經濟術語論述相關議題，避開政治術語，避免外界將其與美歐冷戰態度相形比較。此舉可預先說明中共在南海的活動——只是在「確保貿易路線的安全」與「確保中國大陸經濟區安全無虞」。其次，在衝突升溫後，俄羅斯媒體將話題由經濟轉向政治，將反俄羅斯抗議者渲染為暴徒與恐怖分子，喚起政治與經濟危機的雙重困境。此種透過經濟正當性連結

政治目的之做法，在中共合理化國際水域擴張領土行為時也昭然若揭。第三，俄羅斯持續引用諸如「此為民之所欲」與「這塊土地長屬俄羅斯」等論點，利用歷史與民主論點降低國際干預意願，而中共宣傳人員正積極運用類似論述，為中國大陸南方沿海大規模軍事與經濟入侵辯解。作者提到，由於這些論點(通常是謬論)提出時符合民主理想與維護人民自治權的架構，因此西方領導人常啞口無言。

無庸置疑，中共已研究2022年俄羅斯入侵烏克蘭前夕及作戰全程的資訊環境。中共戰略家可能正制訂反制美國拜登政府巧妙揭露情報的論述，例如拜登政府率先駁斥俄羅斯在邊境集結兵力，預先塑造全球反對俄羅斯2022年2月入侵烏克蘭的共同輿論。¹⁶

深入理解競爭

如欲對抗此類微妙且普遍的資訊戰活動，必須更深入瞭解現代競爭延續不斷的本質，以及美國防部如何在未達武裝衝突門檻的狀況中與敵人交手。

此種理解不僅可釐清中共全面整合政府資源的競爭方法，亦能揭露當前作法分歧的聯合競爭方法之不足。當前作法不僅扼殺創造力，也約束作戰指揮官掌握先機。美軍聯戰準則通告1-19(Joint Doctrine Note [JDN] 1-19)《競爭連續光譜》(Competition Continuum)將未達武裝衝突的競爭，描述為聯合部隊或代理人與其競爭對手為達不同目標而採取的非暴力行動。¹⁷ 在認知此種競爭需要所有政府機關通力合作後，聯戰準則通告1-19將國家權力工具與聯

合部隊專屬行動進行區分。最高層級競爭包括「外交與經濟活動、顛覆政權、情報與反情報、網路空間與資訊環境行動、軍事接觸」等，而聯合部隊則剩下「安全合作、軍事資訊支援、航行自由，以及其他非暴力軍事接觸活動」。¹⁸ 前述各個領域及聯合部隊相對限縮的工作範疇，與共軍奉為主臬的全般作法與「三戰」戰略形成強烈對比。

在共軍廣泛「積極防禦」戰略中，有一項特別適用在未達武裝衝突門檻期間採取攻勢的作戰構想。作為中共全球影響力作戰

的基石，三戰戰略運用心理戰、輿論戰及法律戰宣揚支持北京言論，並為實現中共戰略目標創造有利條件。¹⁹ 此構想依靠宣傳、欺騙、威脅及脅迫等手段影響敵方決策，同時在公共論壇上宣傳針對性敘事與假訊息，洗腦主要國內與國際閱聽人。²⁰ 儘管三戰手法相對標準化，亦即構想缺乏獨創性，但卻能在中共統一行動中有效彌合黨、國家、軍隊及民眾間差距，彌補規模與範圍上的不足。中共中央統一戰線工作部、宣傳部、國務院新聞辦公室、共軍及國家安全部



共軍未達武裝衝突門檻期間，運用心理戰、輿論戰及法律戰等三戰戰略，創造後續有利國家戰略環境。

(Source: 達志/AP)



皆為致力協調影響國內、外閱聽人工作的重要參與者。²¹ 認識三戰構想涵蓋極廣、協調作業經緯萬端，即可確立聯合部隊組織調整的必要性，以及應從何處著手，才能有效與中共競爭。以下四點建議將有助於美國聯合部隊在現代戰爭中取得勝利。

建議1：進一步整合非正規作戰與資訊戰構想。

如欲於大國競爭中取勝，美國必須摒棄過往陳舊觀念，不可再將戰爭與和平視為兩個截然不同狀態，以更加瞭解未達武裝衝突門檻行動的創新方法與手段。美國防部達成此目標的關鍵，就是重新定義非正規作戰，納入資訊戰，讓聯合部隊在競爭連續光譜中採取必要行動。

目前美國國防部非正規作戰定義過於狹隘，已不再適用於大國競爭時代。美軍聯戰書刊1(Joint Publication 1)將非正規作戰定義為「國家與非國家行為者間，為取得相關民眾認同，發揮輿論影響力而進行的暴力鬥爭」。²² 非正規作戰與傳統作戰的區別，在於其具有非西發利亞式(Non-Westphalian)特質——亦即無視國家主權與內政相關規範。非正規作戰與資訊戰極為類似，通常採間接或不對稱戰法，專門用於持久衝突，其目的在「削弱敵方的實力、影響力及意志」。²³ 俄羅斯與中共皆以未達武裝衝突門檻方式，遂行非正規作戰與資訊戰，並透過控制輿論、混淆局勢及影響關鍵受眾等手段，暗中破壞競爭對手，使其行為喪失正當性。

雖然非正規作戰整體構想仍然可行，但「暴力」一詞的定義違背非正規作戰本意，需要適度調整。非正規作戰定義為暴力鬥爭，僅適用於武

裝衝突時期，這是美軍過時軍事思想遺緒，此種思維採用狹隘的和平、戰爭二分法，與競爭連續光譜所呈現的整合模式並不相融。²⁴ 應當透過合作、競爭及衝突等作為，應對將競爭視為不斷追求「安全、影響力與資源」的敵人。²⁵ 然而，在競爭連續光譜中行動必須採用適當工具，就像「小綠人」(Little Green Men)在烏克蘭製造混亂，以及「小藍人」(Little Blue Men)對南海爭議島礁宣示主權，聯合部隊亦應研擬靈活作戰方案，在競爭與衝突期間靈活運用。

儘管修改非正規作戰定義，擴大適用範圍並不困難，但卻能如實在當代準則反映戰爭不斷變化的本質，使得指揮官在未達武裝衝突門檻競爭中有更多選擇方案，並激發大國競爭中取勝所需的創造力。修改定義並不是要求改變政策或權責，而是同時改變聯合部隊理解與整合未達武裝衝突門檻的非正規作戰與資訊戰方式。近期，諸如聯戰書刊通告1-19等美軍出版品，均體認作戰本質變化與調整聯合部隊競爭方法的必要性。近期，聯戰書刊5-0《聯合計劃作為》(Joint Planning)修訂內容，凸顯競爭期間作為的重要性，並強調二十一世紀作戰中多領域戰術不可或缺。因應網路空間作戰興起，修訂諸如決戰點(Decisive Point)等關鍵詞彙；而競爭連續光譜期間範圍增加，非正規作戰亦應同樣進行更新。²⁶ 其他學者亦提出類似論點，指出必須重新定義非傳統戰爭(Unconventional Warfare, UW)——非正規作戰範疇，俾阻擾或脅迫競爭對手以取得競爭優勢。²⁷ 支持此論點者認為，非傳統戰爭應積極投入資訊環境，並挑起動亂或脅迫敵方政府，而不應將主



2023年1月10日，美空軍第18通信中隊莫瑟(Cody Moser，圖左)上等兵與萊德福德(Calvin Ledford)上等兵於日本嘉手納空軍基地裝設星鏈(Starlink)終端設備。(Source: USAF/Sebastian Romawac)

要重點放在支援叛軍。儘管這項改變與本文立場一致，卻也只是擴大聯合部隊理解競爭時必要之文化轉變。

將「非正規」定義擴大到武裝衝突之外，可提供聯合作戰司令更多行動方案。雖然前述行動方案通常限縮在聯合作戰區或聯合特種作戰區，但只要相關方案主軸是讓敵方無法採用未達武裝衝突門檻手段，在作戰區內擴大影響力，就可持

續執行且無須經國家指揮權責機構批准。此種權責的擴大，與2018年中曾根(Paul Nakasone)上將參議院聽證會期間，研討攻勢網路作戰行動權責的討論類似。仲宗根在其書面證詞中主張：「基於敵方網路能力與威脅不斷演進，美國網路司令部必須在網路空間隨時備便，透過網路空間保衛美國，如此一來可能必須在武裝衝突或公開敵對區之外展開特定網路行

動。」²⁸ 無論戰場環境整備或非傳統戰爭準備，聯合作戰司令都必須有能力進行未達武裝衝突門檻的資訊戰。隨著權限擴大，非正規作戰與資訊戰皆可納入戰區戰役計畫，而不再限縮適用於突發事件。如此一來強化先期規劃作為，為指揮官提供更多合作、競爭及衝突之作戰方案。

建議2：整合政府機關資源，復編美國新聞總署。美國從事



資訊領域活動時，不能受限於單一部門專業，也不能採取孤立做法。敵人已展現自身能力，足以產製涵蓋國家權力的戰略論述，並產生巨大效果。儘管目前美國已更加努力，但在資訊戰統一行動與統一指揮前，美國仍無法與敵抗衡或握有主導優勢。在冷戰勝利多年後，美國認為不再需要美國新聞總署(U.S. Information Agency, USIA)而於1999年將其裁撤。結果，美國失去在國家領導層級中擁有「一席之地」的單一內閣層級代表，自此無法率領各部會進行聯合行動。²⁹ 如今，美國國家安全會議(National Security Council)試圖制定「國家立場」以解決問題時，往往欠缺具有相關專長的內閣層級代表方能提供的一致說詞。隨著反制外國惡意影響力任務與日俱增，敦請國家領導階層重新審視美國新聞總署構想，並依據二十一世紀與當前大國競爭時代需求，重新調整並擴大其職掌與業務。這不能是單一部門單打獨鬥，也複製過往美國新聞總署做法——此組織必須納編武器、情報、執法及國家事務等專業背景人員。如欲臻完善，美國國防部可提供能協助制定及反制相關戰略論述的人才，這些人員瞭解論述產生三階段：形成(如何撰擬論述)、闡述(散布與澄清論述)及接收(接受論述的方式)。³⁰ 美國應著眼打造一個環境，使美國國務院承辦人能與具有境外作戰(政治或區域事務戰略家)、資訊戰、影響力作戰、公共事務、戰略、情報及網路戰等背景的軍職人員攜手合作。許多質疑復編美國新聞總署做法的人認為，該機構適用於單純兩極時代(美國與蘇聯或「西方與其他國家」)，當時世界數位化連結程度較低。然而該部門復編後，現代

化的美國新聞總署將統合國防部、司法部、國務院及國土安全部之權責與能力，密切合作整合政府機關資源，共同反制境外假訊息。

建議3：國家網路軍之編成與留營措施。1933年，羅斯福(Franklin D. Roosevelt)推行新政(New Deal)，一系列的勞動專案，目的不僅在振興國家勞動力，也試圖保持美國競爭優勢。新政其中一個施政重點是「平民保育團」(Civilian Conservation Corps, CCC)，旨在於招募、訓練、僱用及最終重振美國青年，試圖在國內動盪與全球失序時期，重建、恢復及保護國家重大基礎設施、聯邦土地及自然資源。

如今美國正處於轉捩點，相較競爭對手中共，美國的科學、數學、工程及數位化素養正以驚人的速度流失。儘管資訊科技與安全計畫湧入數十億美元資金，美國國防部仍無法產生在範圍與規模上足以全面應付大國對手間諜活動與網路攻擊的能力。

正如1933年平民保育團，美國國防部可領銜重新思考二十一世紀資訊時代(除了目前傳統軍事武裝部隊外)效忠國家部隊的樣貌，尤其在電腦工程、資訊科技及網路安全等技術領域。在此情況下，美國將投資最少資金，擬定方法，讓天賦異稟的熱血年輕公民自願從軍。就像過去平民保育團一樣，後續在第二次世界大戰成為美陸軍士官團骨幹，以資訊為中心的平民保育團，將廣納美國技術人才，承平時期於後備「平民網路團」服務，並在國家危難時接受徵召，共同強化重大基礎設施防護。由近期事件可得知，美國國防部與美國政府皆無法有效保護美國網路空間與重大

基礎設施免於網路攻擊。成立平民網路團是一石二鳥之計，不僅能迅速培養年輕技術人才，也讓青年得以報效國家。

借鑑歷史，平民網路團重點在及早培育國家技術人才，並提供傳統兵役架構以外報效國家的簡易途徑。平民網路團可強化國防能量，透過動員民事防務資源(Defense Support to Civil Authorities)支援政府機關執行任務，而其領導階層主要為後備役或國民兵，而這些部隊與民間產業關係密切，並在州與聯邦層級建立防衛與保障國家安全所需組織。該組織不僅提供技術訓練，也提供就業機會，範圍從基本資訊系統管理到惡意軟體分析與威脅試探(Threat Heuristics)等進階技術。

就結構而言，平民網路團將專注三大工作領域，包括人才招聘、發展及融入現有聯邦與州級網路安全組織。從招募與發展角度來看，平民網路團聚焦招募小學生至25歲以下年齡層，培養數位化素養與各領域技術人才。就像美國童軍(Boy Scouts of America)一樣，若參與者興趣滿滿、願意奉獻，將可獲得技術訓練機會、聯邦補助金、學術獎學金等獎勵，甚至安排就讀美國軍事學院與大學。畢業後，參與者將獲得科技公司及政府部門實習機會。若有意願，還可接受任命，成為武裝部隊後備役人員，在重大基礎設施遭受網路攻擊或視重要國家級網路計畫需要時接受徵召。整體來看，平民網路團將為聯邦、州、地方政府及潛在民營企業組織形塑最大作業能量。現代平民網路團將可當作美國聯邦與州招募與人才獲得的「數位人才儲備庫」(Digital

Bench)，並在國家安全架構上，協助遂行網路空間與資訊科技相關手段。如今，美國更須跳脫框架，運用創新手段培養與招募人才，並充分利用技術實力，俾因應二十一世紀資訊時代挑戰。平民網路團成立後將澈底改變二十一世紀部隊樣貌，同時在傳統兵役架構外激發美國青年的競爭精神，這也是美國戰勝大國競爭對手的必要條件。

最後，成立平民網路團，將有助於美國國防部促成第7軍種——美國網路軍——的成軍。此軍種專門致力於組織、訓練、整備攻勢與守勢網路部隊，以保衛國家、網路及支援傳統軍事活動。由於平民網路團在數位人才年輕時即行招募與培育，自然而然即可成為這個新軍種的兵源。此外，對於試圖短暫脫離現役身分，在軍事單位外尋求工作機會，同時為國家奉獻微薄之力者，平民網路團就成為理所當然的後備役兵役選項。此時此刻，美國國防部必須認清，自網路任務部隊(Cyber Mission Forces，美國網路司令部行動部隊[Action Arm])成立以來，該部隊戰備、能量與留營率逐漸下降，而這些部隊編制小、部隊任務要求卻不斷增加。目前，美軍各軍種組織編裝、訓練及整備網路部隊的方式雜亂無章、繁瑣、高度官僚，且最終缺乏相應制度蒐集資源，畢竟網路作戰並不是各軍種的主要任務。無數次以慰留網路專業人員為重點的國會聽證會，證明美軍現有機制——無論是文職網路專業職務或直接入營服役機制——皆不足以滿足部隊戰備要求。正如必須透過平民網路團建立專責招募與培養年輕數位人才的組織一般，美軍如欲建立一支能在資訊環境備便作



戰與克敵制勝的部隊，也必須有專責獨立軍種負責組織、訓練與整備網路作戰部隊。

結論

民主制度面臨前所未有的挑戰與威脅，美國必須準備在此國家歷史關鍵時刻採取大膽行動。俄羅斯與中共近期在資訊領域同流合汙，證明不採取行動確實風險過高。美國若在此領域喪失先制後將難以挽回，後續影響將擴及美國與世界各地民主國家數個世代。競爭連續光譜規模既龐大且複雜，遠超出美國國防部權責。

現在正是勇敢採取全新措施的時刻。美軍必須迅速改變過時思維，讓聯合部隊在現今瞬息萬變的戰場中發揚機動能力。因此，本文認為美國國防部必須擴大解釋非正規作戰，以符合現代競爭連續光譜場景，並與跨部門夥伴攜手合作，共同建立美國中央資訊機構。最後，在傳統軍事組織外建立全新國家軍事組織架構。成立平民網路團將可實現此一目標，該部隊將利用國家數位人才從事國防工作，並成為建立未來美國網路軍種的手段。總之，前述改革將使聯合部隊維持當前對敵優勢，並於未來保護美國民主核心價值。

作者簡介

Christopher H. Chin美空軍中校為美國網路司令部未來作戰處處長。

Nicholas P. Schaeffer美空軍中校為美國戰略司令部國家空中作戰中心(即E-4B空中指揮機)上的情報長。

Christopher J. Parker美陸軍少校為堪薩斯州李文渥斯堡(Fort Leavenworth)聯合參謀部聯七(J7)戰略計畫官。

Joseph O. Janke美陸軍少校為南韓韓福瑞營(Camp Humphreys)駐韓美軍第8軍團參九(G9，民事)計畫暨演習長(Plans and Exercises Chief)。

Reprint from *Joint Force Quarterly* with permission.

註釋

1. Basil Henry Liddell Hart, *Strategy*, 2nd ed. (New York: Signet, 1974), 5.
2. Conor Cunningham, "A Russian Federation Information Warfare Primer," The Henry M. Jackson School of International Studies, November 12, 2020, available at <<https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/>>.
3. Timothy Thomas, "Russia's Reflexive Control Theory and the Military," *The Journal of Slavic Military Studies* 17, no. 2 (2004), 237–256.
4. Brenna Cole and George Noel, "Nation-State Perspectives on Information Operations and the Impact on Relative Advantage," paper presented at the International Conference on Cyber Warfare and Security, February 2021.
5. Dave Johnson, "ZAPAD 2017 and Euro-Atlantic Security," *NATO Review*, December 14, 2017, available at <<https://www.nato.int/docu/review/articles/2017/12/14/zapad-2017-and-euro-atlantic-security/index.html>>.
6. Andreas Ventsel et al., "Discourse of Fear in Strategic Narratives: The Case of Russia's Zapad War Games," *Media, War & Conflict* 14, no. 1 (March 2021), 24–26.
7. Sheena Chestnut Greitens, Myunghee Lee, and Emir Yazici, "Understanding China's 'Preventive Repression' in Xinjiang," *Order From Chaos* (blog), March 4, 2020, available at <<https://www.brookings.edu/blog/order-from-chaos/2020/03/04/understanding-chinas-preventive-repression-in-xinjiang/>>.
8. "Hong Kong Security Law: Anger as China's XI Signs Legislation," BBC, June 30, 2020, available at <<https://www.bbc.com/news/world-asia-china-53234255>>.
9. Tom O'Connor, "China Hosts Russia Troops to Hold Strategic Military Drills for First Time,"

- Newsweek*, August 2, 2021, available at <<https://www.newsweek.com/china-hosts-russia-troops-hold-strategic-military-drills-first-time-1615496>>.
10. Elizabeth Chen, “China Learning From Russia’s ‘Emerging Great Power’ Global Media Tactics,” *China Brief* 21, no. 7 (April 12, 2021), available at <<https://jamestown.org/program/china-learning-from-russias-emerging-great-power-global-media-tactics/>>.
11. Ibid.
12. Kristin Huang, “Can Beijing Use Lessons Learned by Europe to Ease South China Sea Tensions?” *South China Morning Post*, November 9, 2019, available at <<https://www.scmp.com/news/china/diplomacy/article/3036788/can-beijing-use-lessons-learned-europe-ease-south-china-sea>>.
13. Chen, “China Learning From Russia’s ‘Emerging Great Power’ Global Media Tactics.”
14. Gary Rawnsley, “To Know Us Is to Love Us: Public Diplomacy and International Broadcasting in Contemporary Russia and China,” *Politics* 35, nos. 3–4 (2015), 273–286, available at <<https://doi.org/10.1111/1467-9256.12104>>.
15. *China’s Military Power: Modernizing a Force to Fight and Win* (Washington, DC: Defense Intelligence Agency, 2019), 4–140.
16. Jake Harrington, “Intelligence Disclosures in the Ukraine Crisis and Beyond,” *War on the Rocks*, March 1, 2022, available at <<https://warontherocks.com/2022/03/intelligence-disclosures-in-the-ukraine-crisis-and-beyond/>>.
17. Joint Doctrine Note (JDN) 1-19, *Competition Continuum* (Washington, DC: The Joint Staff, June 3, 2019), 4–7, available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_19.pdf>.
18. Ibid., 2.
19. *Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China 2020* (Washington, DC: Office of the Secretary of Defense, 2020), 130, available at <<https://media.defense.gov/2020/sep/01/2002488689/-1/-1/2020-dod-china-military-power-report-final.pdf>>.
20. Ibid.
21. Ibid.
22. Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: The Joint Staff, March 25, 2013, Incorporating Change 1, July 12, 2017), I-6, available at <<https://irp.fas.org/doddir/dod/jpl.pdf>>.
23. Ibid.
24. JDN 1-19, *Competition Continuum*, 4–7.
25. Blagovest Tashev, Michael Purcell, and Brian McLaughlin, “Russia’s Information Warfare: Exploring the Cognitive Dimension,” *MCU Journal* 10, no. 2 (2019), 141, available at <<https://dx.doi.org/10.21140/mcu.2019100208>>.
26. JP 5-0, *Joint Planning* (Washington, DC: The Joint Staff, December 1, 2020), IV-32, available at <https://irp.fas.org/doddir/dod/jp5_0.pdf>.
27. Otto C. Fiala and Jim Worrall, “Imposing Costs: Unconventional Warfare in the Information Environment,” *Modern War Institute*, July 6, 2021, available at <<https://mwi.usma.edu/imposing-costs-unconventional-warfare-in-the-information-environment/>>.
28. Senate Armed Services Committee, Advance Policy Questions for Lieutenant General Paul Nakasone, USA, Nominee for Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service, 115th Cong., 2nd sess., 2018, 31, available at <https://www.armed-services.senate.gov/imo/media/doc/Nakasone_APQs_03-01-18.pdf>.
29. Dr. Vivian Walker, email, July 22, 2021, following author’s presentation, “Countering Disinformation Narratives: Strategic Approaches,” Joint Combined Warfighting School, Norfolk, VA, July 16, 2021.
30. Alister Miskimmon, Ben O’Loughlin, and Laura Roselle, *Forging the World: Strategic Narratives and International Relations* (Ann Arbor: University of Michigan Press, 2017).