DOI:10.6915/PMSS.202308_(23).0003
軍事社會科學專刊，第 23 期，頁 23-48 (2023 年 8 月)

新型態戰爭－「混合戰」威脅之應處作為：以俄烏戰爭為例

黃志軒*

摘要

隨著資訊科技快速發展，戰爭型態變得複雜與多樣，具有正規和非正規作戰方式的「混合戰」特徵，並具體呈現在 2022 年發生的俄烏戰爭，在戰爭期間，俄國透過網路攻擊、散布假訊息、軍事威懾、操縱國家認同與經濟脅迫等方式，試圖瓦解烏克蘭抗敵意志，而烏克蘭也能適時採取反制行動，抵抗俄國的混合戰攻勢，顯見，混合戰的行為模式似乎已成為現代戰爭的重要指標。本文係採「文獻分析法」為主要研究方法，嘗試瞭解混合戰之概念、特性與目標，並歸納俄羅斯與烏克蘭運用混合戰的方式與特點。藉由探討混合戰如何應用於戰場上，進一步理解在面對混合戰之威脅時，我國須持續提升民眾防範意識及參與度，加強應對混合戰之韌性與復原力，以及深化各領域交流與合作。

關鍵詞：灰色地帶、非正規戰爭、混合戰、俄烏戰爭

* 空軍司令部政戰官、國防大學政治學碩士；E-mail: fhklovejay@gmail.com

DOI:10.6915/PMSS.202308_(23).0003
Publication of Military Social Science, No.23, pp. 23-48 (August, 2023)

A New Type of Warfare: Taiwan's Responses to the Threat of "Hybrid Warfare": Lessons from Russia-Ukrain War

Chih-Hsuan Huang*

Abstract

With the rapid development of information technology, the nature of warfare has become complex and diverse, characterized by "hybrid warfare," which involves both regular and irregular combat methods. This phenomenon was demonstrated in the Russia-Ukraine War of 2022. During the war, Russia utilized cyberattacks, dissemination of false information, military deterrence, manipulation of national identity, and economic coercion to undermine Ukraine's resistance. In response, Ukraine employed timely countermeasures to resist Russia's hybrid warfare offensive. This illustrates that hybrid warfare has emerged as a crucial aspect in modern warfare.

This article adopts the "literature analysis method" to understand the concept, characteristics and goals of hybrid warfare. It also summarizes the methods and characteristics of hybrid warfare used by Russia and Ukraine. By exploring how hybrid war-fare is applied on the battlefield, we can further comprehend the importance of enhancing public awareness and engagement in defense in our country. It is essential to strengthen resilience and recovery capabilities against hybrid warfare and foster greater collaboration across various fields in order to effectively counter this threat.

Keywords: Gray zone, irregular warfare, Hybrid warfare, Russia-Ukraine War

* Political Warfare Officer, Air Force Command Headquarters; Master of Arts in Political Science, National Defense University; E-mail: fhklovejay@gmail.com

壹、前言

隨著全球化與科技發展的日新月異，現代戰爭型態已不同以往所認知的傳統軍事武力戰，轉變為具有多樣化、多層次及高隱蔽性的「混合戰」型態，並具體呈現在 2014 年克里米亞(Crimea)事件與 2018 年敘利亞內戰，近期則以 2022 年俄羅斯(以下稱俄國)與烏克蘭發生的「俄烏戰爭」較為顯著。在俄烏戰爭期間，俄國運用政治、經濟、軍事、心理、資訊、網路及外交等手段，試圖達成主要政治目的，而烏克蘭也能夠運用混合戰方式適時給予反擊，使得混合戰更加受到關注。

2022 年 8 月，美國眾議院議長裴洛西(Nancy Patricia Pelosi)女士訪台，引起中共強烈抗議，除以一連串軍事手段來回應，亦運用駭客入侵、假訊息操控輿論，以及經濟制裁等方式，製造社會紛亂，顯見臺灣正面臨與過去不同的挑戰，混合戰的攻擊手段已不是未來式，而是現在進行式。根據我國《110 年國防報告書》，中共持續以網路媒體為平臺，輸送大量真、偽混雜的假訊息，建構臺灣民眾錯誤認知或干擾政府與人民之間的相互信任(國防部，2021：中華民國 110 年國防報告書)。

基此，為面對混合戰的挑戰，本文不同以往學界僅探討混合戰的本質及威脅特性，研究者係以 2022 年發生的俄烏戰爭為例，迄 2023 年屆滿一周年之際，嘗試探討混合戰之概念與內涵，並歸納俄烏戰爭期間，俄國與烏克蘭如何將混合戰應用於戰場上及其特點，俾供我國於戰爭發生前，盡可能完善各項法規、制度以及軟硬體設備，以應對混合戰的戰爭型態，此即為本研究之動機。

我國雖與烏克蘭同屬防衛作戰形態之國家，然而，不可諱言地，俄烏與臺海情勢在本質上仍有諸多不同，俄烏兩國所採取的混合戰態樣不見得完全適用於臺海，錯綜複雜的兩岸情勢恐增添難以預測的變數，以及目前二者平戰狀態的差異，亦須一併納入考量，即為本研究之限制。

綜上，本研究旨在瞭解混合戰之概念與內涵，並彙整俄烏戰爭採取混合戰之態樣、方式與手段，於歸納其運用特點後，再根據我國國家安全需求，提出應對新型態戰爭之建議，俾供決策單位參考運用。

貳、混合戰之概念與內涵

混合戰的概念並非至近代才萌生，中國古代兵書《孫子兵法》:「上兵伐謀，其次伐交，其次伐兵，其下攻城」，即強調「伐謀」、「伐交」的「謀攻」重要性，指

出戰爭的勝負並非完全由正規武力決定，應優先運用外交、經濟、心理、顛覆的方式挫敗敵人的戰略意圖或戰爭行為，力求以「全勝」的策略達成「不戰而屈人之兵」之目的。

一、混合戰之概念與定義

隨著資訊科技的進步，國家與非國家行為者(non-state actors)發動戰爭或衝突的方式逐漸產生變化，人類所面臨的威脅更趨複雜與多元，使得學者開始探討新型態戰爭與威脅的混合性，嘗試預先瞭解詭譎的戰場空間，以應對潛在敵人。

2007 年，美國防大學研究員法蘭克霍夫曼(Frank G. Hoffman)在其《21 世紀衝突：混合戰爭的興起》(Conflict in the 21st Century: The Rise of Hybrid Wars)著作中具體提出「混合戰」一詞，認為未來戰爭模式將融合多種樣式，同時進行且相互為用之新型態，包括正規(Conventional)能力、非正規(irregular)戰術以及無差別的暴力、脅迫等恐怖行為與犯罪活動，不同模式的行動可由不同單位或同一單位執行，通常於主戰場空間內進行作戰和戰術指導與協調，以實現協同效果(Hoffman, 2007)。

Miller(2015)指出混合戰是「在相同的戰場空間中，使用正規和非正規方式和手段，由國家和非國家行為者的任意組合。」亦有學者提出混合戰涉及正規軍隊和非正規軍隊(例：游擊隊、叛亂份子和恐怖份子)結合的衝突，其中可能包括國家和非國家行為者(Wither, 2016)。Batyuk(2017)則根據美國政界和軍事專家對中東和烏克蘭局部衝突的分析，指出混合戰是行為者將技術、能力和資源混合在一起並達成目標的衝突。

2015 年，北約(NATO)成員國在美國華盛頓舉行的轉型研討會上一致認為，混合戰及其輔助戰術能包含廣泛、複雜、適應性、投機行為(opportunistic)，且經常融合常規和非常規的方法(Caliskan & Cramers, 2018)，北約 2022 年《戰略概念》(Strategic Concept)進一步論述，未來敵人將直接或透過代理人採取「混合戰爭」破壞公民安全，包括在網路空間和太空展開惡意活動，散播假訊息，將移民作為工具，操縱能源供應，實施經濟脅迫等(NATO, 2022)。中共解放軍西部戰區司令員汪海江亦認為 2022 年的俄烏戰爭明顯展現混合戰爭的新型態，相互交織軍事、政治、金融、科技、網路與認知戰，戰爭對抗是從傳統領域延伸至非傳統領域(Doyle, 2023)。

此外，美軍對混合戰也提出相似的定義。2011 年，美陸軍正式於作戰準則內將混合戰定義為「正規部隊、非正規部隊、犯罪份子的多樣化與動態組合，共同整

合一致地去實現互惠互利的效果(Schnaufer, 2017)」。美國前海軍陸戰隊少校McGuire(2021)指出，混合戰經常應用於傳統和平與戰爭模式之間的灰色地帶(gray zone)，屬於不對稱戰術、非正規方式、傳統權力和影響力工具的協同融合，無縫存在於每個作戰領域，包含地面、空中、海上、太空、網路空間與資訊領域。美國海軍中將 Scott(2016)於《2035 聯合作戰環境(Joint Operating Environment 2035)》報告中強調，混合戰是部分「修正主義國家」(revisionist states)採用一系列強制性活動，透過直接和間接相結合的方式來促進國家利益，旨在減緩、誤導(misdirect)和削弱(blunt)目標國家的成功反應，使其變得混亂。

2014 年，俄國併吞克里米亞之後，混合戰的概念迅速成為用以幫助解釋在這場衝突中取得成功的原因，部分學者嘗試去了解俄國先前提出的軍事理論後，認為俄軍總參謀長格拉西莫夫(Valery Gerasimov)是俄國混合戰方法的代言人，他強調「非軍事工具」在衝突中已成為作戰環境的重要因素之一(Renz, 2016)。學者Clark(2020)則認為俄國的混合戰為一種透過戰略層面(strategic-level)的努力，以形塑目標國家所有行動的政府治理和地緣戰略方向，並評估戰爭逐漸變得非正規且更快速，採取措施與參與者也越來越多樣化。

二、混合戰運用之特性

Chivvis(2017)指出混合戰是莫斯科(Moscow)使用廣泛的一系列顛覆工具，以達成其國家利益，來確保遵守一些特別的政策問題，例如分裂和削弱北約影響力、顛覆親西方(Pro-Western)的政府、為戰爭製造藉口、吞併領土等。由於俄國意識到掌握民眾想法之重要性，進而試圖透過資訊操作、代理團體和其他有影響力的行動來影響目標國家，而人民與社會通常最容易受到輿論影響，俄國充分利用國家權力各個面向，將其意志加諸在另一個國家(Bratko et al., 2021)。

Cullen 與 Reichborn-Kjennerud(2017)則認為混合戰具有「不對稱」的特性，國家與非國家行為者透過垂直(強度的大小)與水平(手段多樣性)基線，同步運用軍事、政治、經濟、社會、資訊等多種權力工具(如圖 1)，逐漸增加混合戰的威脅強度與方法，以降低對手的整體能力，在不同程度上更加重視戰爭的創造力、模糊性和認知要素。

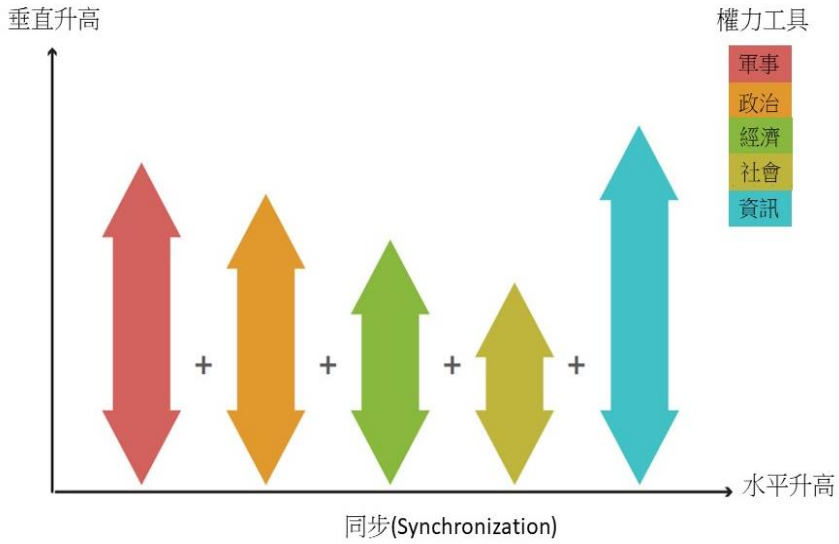

圖 1 混合戰提升模式
資料來源：Cullen & Reichborn-Kjennerud(2017, p.9)。

此外，多層面(multidimensionality)也是混合戰的特性之一。實現政治和戰略目標不再僅僅侷限於傳統的正規軍事手段，更重要的是融合政治、經濟、資訊、人道主義和其他軍事手段，且能達成預期戰略效果(Raska & Bitzinger, 2015)。Mumford(2020)提出模糊性的看法，其表示混合戰是在模稜兩可(deliberate ambiguity)的程度上為模糊性創造出條件，此種戰爭方式利用模糊手段，以低於合法反應(legitimate response)門檻的武力，秘密的將其藏匿於軍事行動中，以應用於戰略上的政治目的。

三、混合戰欲達成之目標

新科技的出現以及全球化條件下相互依賴性的日益增加，使現代戰爭融合「軟實力」和「硬實力」，雙方更加頻繁地運用政治、經濟、資訊以及多種非軍事工具與手段，向對手施加最小的軍事壓力而達到最大化的政治目的。國家或非國家行為者採取混合戰之目的，除欲達成局部作戰目標與企圖，也嘗試透過多種權力工具、語言、管道與途徑，結合隱蔽行動、破壞襲擾、網路駭客、暴力犯罪、恐怖主義、輿論干擾及獲取敵境內部反對勢力的支持等非正規軍事行動。

根據 Chivvis(2017)分析，俄國運用混合戰有三種典型目標，第一是不訴諸公開或運用正規軍事力量奪取領土；第二是為發動正規軍事行動製造藉口；第三是影響西方和其他國家的政治與政策，以尋求確保目標國家的政治結果符合俄國的國家利益。

混合戰行為者通常會故意隱瞞自己的意圖和能力，利用和平與戰爭之間、國家與國際責任之間去欺騙敵人和國際社會，試圖迫使對手實現、滿足他們的意志，主要攻擊目標在於國家、社會秩序和凝聚力(Jäger, 2021)。由於混合戰手法具有成本低、風險小、隱蔽高的特點，得以運用秘密、潛在的力量(含實體、虛擬)滲透對手進行擾亂，再捏造與事實相悖的理由，以合理化本身行為，進而影響對手的經濟體系運作與政治決策。

此外，混合戰的行為者亦運用政治、經濟、外交、資訊、網路等不易發現的權力工具和技術，試圖在未達戰爭門檻的衝突空間中，降低國際上對戰爭或衝突的理解，規避國際法與武裝衝突法的可執行性，使國際社會無法及時做出反應與處置，降低對該行為者的制裁力道，而國家隨著混合戰略的日趨完善、代理人戰爭加劇以及建立區域核威懾(nuclear deterrents)能力，將更有助於該國尋求地區的主導地位與能力(Scott, 2016)。

參、俄烏戰爭運用混合戰之方式

2022 年 2 月，俄國除了採取傳統軍事武力的方式入侵烏克蘭，也運用政治、經濟、外交、網路、資訊等非傳統戰爭方式企圖影響戰爭勝負，並試圖合理化戰爭行為、爭取國際認同以及瓦解烏國民心士氣，達「不戰而屈人之兵」之目的，然而，烏克蘭在歐美各國的援助下，同步運用俄國預料之外的抵抗能力，有效抵擋與遲滯俄軍的攻勢進展，以下針對雙方在混合戰之作為，分述如次。

一、俄國運用混合戰之態樣

(一) 資訊與網路攻擊

美國微軟(Microsoft)在 2022 年 6 月發布《捍衛烏克蘭：網路戰的早期教訓》(Defending Ukraine:Early Lessons from the Cyber War)的報告，內文研究俄烏戰爭期間，俄國主要採取三種網路攻擊策略，分別如下(Microsoft Corporation, 2022)。

1.發動破壞式攻擊：

俄國於 2 月 23 日即以惡意程式「FoxBlade」木馬病毒對烏克蘭基礎架構實施網路攻擊，並於開戰初期對烏克蘭政府資料中心發射飛彈，並對烏國境內的電腦網路環境，發動資料刪除的毀滅式(Wiper)攻擊。

2.展開網路滲透與間諜行動：

微軟統計 2022 年 2 月至 6 月，俄國駭客不僅對 48 個烏國政府組織與民間

公司發動攻擊，也企圖對全球 42 國、128 個組織發起網路滲透行動，並以美國及北約成員國為首要目標。

3.發起網路影響行動(cyber-influence operations)：

俄國善於透過輿論影響四類民眾的認知，第一是俄國人民，目的是對俄國民眾宣揚軍事行動的正當性；第二是烏克蘭人民，意圖削弱抵抗的意願與信心；第三則是美國與歐洲人民，企圖破壞歐洲國家與美國的團結，轉移對俄國犯下戰爭罪的批評；第四是其他未與烏克蘭結盟國家的民眾，欲煽動他們在聯合國等國際場合，表態支援俄國的立場。

此外，俄國的網路攻擊行動通常會與正規軍事武力協調一致地執行，當俄軍選定以飛彈攻擊烏克蘭境內目標(例：重要關鍵基礎設施)，同時間或前後幾天內，可發現俄國已增加對該目標網路攻擊的頻次與強度，試圖同步發揮實體與虛擬空間的襲擊效果，降低目標防護能力。

(二) 散布假訊息

俄國總統普丁(Vladimir Putin)以「去納粹化」及「去軍事化」為名，對烏克蘭發動特別軍事行動，並要求國內大眾傳播及社群媒體禁止使用戰爭、入侵、攻擊等用語，對內嚴格控管輿論與新聞的用詞(Roth, 2022)。另外，俄國脫口秀主持人也在節目上扭曲事實，譴責烏克蘭欲加入北約是非常不明智的行為，藉由節目娛樂效果形塑對俄國有利的輿論，使國內多數民眾對烏克蘭的好感度大幅下降(Goncharenko, 2022)。

此外，在俄國入侵烏克蘭後，主要社群媒體及影音頻道(例：Facebook、Twitter、Instagram、YouTube)出現大量的假帳號與假訊息，大肆宣傳烏國政府崩潰、總統逃亡、首都遭包圍、烏軍對民眾實施非人道攻擊等不實訊息(詹祥威，2022)。尤其是 Telegram 軟體，它是烏國最多人使用的通訊軟體，因保密性較強，政府無法隨時監控和封鎖聊天群組，使其成為俄國散播假訊息的管道(陳穎萱，2022)。

再者，紐約非營利組織「ProPublica」調查報告亦指出，俄國以「自導自演」方式產製不實影片與訊息，再以「闢謠」為名，上傳到政府網站或事實查核平台，並受到俄國社群媒體轉載分享。學者唐納凡(Joan Donovan)認為，俄國不需要於社交媒體廣泛宣傳才能達到效果，因為這些過程足以讓民眾相信烏克蘭宣傳部門極有可能會採取這些作為，且成功博得社會輿論關注，重塑有利政府的戰略敘事(Silverman & Kao, 2022)。

(三) 非正規軍事威懾與戰略欺騙

俄國善於將特種部隊偽裝成平民百姓，或是利用親俄份子，滲透目標國家製造紛亂與破壞，再將其行為嫁禍於該國。根據美國的情資掌握，俄國在入侵烏克蘭之前，已預先派兵在烏東親俄地區執行「假旗行動(false flag operation)」，並以民間保安公司名義掩護軍事介入之實，轉移國際上對軍事行動的注意(Restuccia & McBride, 2022)，直到正規部隊正式進入烏國前，普丁仍稱願意透過外交手腕解決彼此問題，使各國降低戒心。

由於戰場上的人力短缺問題，在俄國政府授權下，傭兵組織「華格納集團(Wagner Group)」協助執行監獄招募計畫，誘以高薪並承諾如果囚犯能自願服務 6 個月以上，將獲得俄國政府特赦 (Walsh, 2022)，然而實際上雙方並未有正式的合約簽署關係。上述計畫由「非國家行為者」協助政府將非正規武力的犯罪份子，招募整合後加以投入戰場，根據俄軍評估，這批囚犯的戰鬥意志更勝於正規軍隊，對烏軍可產生威懾作用。

(四) 操縱國家認同

俄國與烏克蘭存在密不可分的歷史關係，蘇聯解體後，俄國自認繼承前蘇聯的正統，希望能夠重振昔日蘇聯的光榮，而這部分與烏克蘭想脫離蘇聯陰影、「親西方」的主流立場完全相反，間接造成雙方長期衝突不斷，更導致 2014 年俄國併吞克里米亞與 2022 年俄烏戰爭的發生(Kordan, 2022)。烏克蘭東部地區以俄裔人口占多數，俄語人口比例約在 70%以上，由於語言文化的差異，烏東地區對烏克蘭的國家認同較為淡薄，屬於「親俄國」陣營，俄國即利用價值觀差異分裂社會，降低該地區人民的國家認同與歸屬感，以影響民眾選擇(況正吉、宋鎮照，2016)。

戰前，俄國持續詆毀烏克蘭政府存在的正當性，聲稱烏國境內俄裔人口面臨的風險正不斷升高，2022 年 2 月 23 日，普丁突然宣布正式承認「頓內次克人民共和國(Donetsk People's Republic)」與「盧甘斯克人民共和國(Lugansk People's Republic)」的獨立地位，並且扶植魁儡政權舉辦公投，與這兩個共和國政權建交，塑造俄、烏民眾希望加入俄國的輿論，並捏造烏克蘭「納粹化」、「北約東擴」、烏國政府對俄裔族群進行「種族滅絕」等謊言，為後續軍事行動尋找藉口(Kirby, 2022)。

(五) 經濟手段壓迫

俄國長期是歐盟最重要的天然氣、石油與煤炭供應者，根據 2021 年統計，歐

盟從俄國進口超過 40%的天然氣消費量、27%的石油和 46%的煤炭(European Commission, 2022)。戰火點燃之初，由於俄國受到歐盟的經濟制裁，普丁於是大幅降低甚至切斷對歐洲的能源及原物料供應，而材料及能源成本的上升，可預期將轉嫁到物價上，不僅對民眾生計產生影響，亦可能限制歐洲國防工業的復興與發展(Nezhyva & Mysiuk, 2022)。

此外，在各國對俄國展開經濟制裁前，緊張的戰爭威脅氛圍已對烏克蘭經濟產生重大影響。根據經濟學人(The Economist)指出，自 2014 年至 2022 年，這 8 年來因為俄烏衝突已使烏克蘭損失至少 2,800 億美元，其國內與國際市場對於戰爭的擔憂，嚴重抑制當地的投資與經濟活動，甚至在戰爭發生前幾個月，外資便撤走至少 125 億美元，使得烏國匯率嚴重縮水，經濟危機更加惡化(The Economist, 2022)。

二、烏克蘭運用混合戰之態樣

自 2014 年克里米亞遭併吞後，混合戰一度受到高度關注，為應對潛在的多重威脅，烏克蘭即與美國及歐洲等國家展開密切合作與交流，且烏國政府深知混合戰的威脅型態複雜、作戰行動模糊，必須統籌國家整體資源，發揮組織分工能量，採取綜合措施才能有效應對混合戰之威脅。基此，針對本次戰爭期間，研究者將列舉烏國採取混合戰的方式。

(一) 號召網路戰士，遂行網路反擊

烏國政府透過基輔網路安全公司創辦人奧舍夫(Yegor Aushev)的協助，在駭客論壇中徵召將近 800 位的志願者，組建一支「烏克蘭 IT 軍團」(IT Army of Ukraine)，用以抵抗俄國的網路破壞行動，除了保護國內關鍵基礎設施，也針對俄軍進行網路情蒐與間諜工作(Supruniuk, 2022)。

此外，國際駭客組織「匿名者」(Anonymous)於 2022 年 2 月 25 日透過「推特(Twitter)」宣布，將正式向俄羅斯發動網路戰，包括關閉俄羅斯石油巨頭天然氣工業股份公司、國家控制的新聞機構 RT 與眾多俄羅斯和白俄羅斯政府機構網站，以及向俄國民眾發送數百萬個電話、電子郵件和簡訊(Pitrelli, 2022)，此舉也暴露俄國網路安全防禦比想像中還要脆弱，證明網路攻擊具高度破壞性與有效性。

(二) 鞏固戰爭面，爭取國際支持

「戰爭面」之功能，即控制作戰地域包含敵、我的一切戰力要素，削弱敵人戰力，繼而爭取戰場優勢，確保作戰任務達成(謝奕旭，2007)。烏克蘭政府各部會與民眾緊密合作，全體上下一心展現強大抗敵意志，國內科技人才以創新、不對稱作

戰思維開發數種手機 APP(例：反監控、分享即時戰況、全民獵殺無人機)等，供全民下載運用並適時通報軍方，有效支援軍事作戰(Harwell, 2022)。

為爭取談判籌碼，烏國總統澤倫斯基(Volodymyr Zelensky)頻繁前往各國或利用國際會議發表演說，一方面呼籲國際夥伴共同譴責俄軍行為，並加強制裁力道，另一方面持續爭取軍事武器與經濟資源的援助。此外，美國太空探索科技公司(SpaceX)也給予烏克蘭約 2 萬套接收天線和路由器，提供星鏈(Starlink)網路服務，讓烏國在能源和通訊設施遭受導彈攻擊時，也能透過星鏈設備維持網路與通信暢通，持續遂行指揮作戰(Visit Ukraine, 2022)。

(三) 捏造英雄人物，擴大宣傳力度

2001 年的電影「大敵當前」(Enemy at the Gates)是一部以史達林格勒(Stalingrad)攻防戰為背景的戰爭片，片中將狙擊手男主角塑造為蘇聯的英雄人物，每當成功擊斃敵軍重要指揮官，蘇聯就會印製「戰報」發送各部隊進行宣傳，成功造就「狙擊之神」的美譽，有效提振官兵士氣。本次俄烏戰爭中，無論是「基輔幽靈」(Ghost of Kyiv)、或是「烏克蘭收割機」(Ukrainian Reaper)，均為烏克蘭虛構的戰場英雄，目的在於實施假訊息宣傳與爭取國際關注。華盛頓智庫「新美國」研究員辛格(Peter W. Singer)曾表示：「如果烏克蘭沒有加強宣傳他們的英勇事蹟、正義價值，以及人民的苦難，將有可能會失去這場戰爭(何蕙安，2022)。」

此外，一張基輔市長克里契科(Vitali Klitschko)身著迷彩服的照片也在網路引起討論，多數人對市長親自到前線作戰此舉感到佩服與尊敬，並視他為英雄人物，然而實際上照片是在 2021 年時，市長與烏國預備軍人一起接受訓練所拍，並由市長親自發布在 Instagram 上(Wesolowski, 2022)。由此可見，當國家陷入危難、發生戰爭時，最容易激起人民團結意識的做法，就是塑造一個共同英雄，並且透過媒體廣為宣傳，促使民眾支持與認同。

三、俄烏運用混合戰之共同特點

(一) 介於正規與非正規的灰色地帶

現代戰爭或衝突的空間環境已被重新定義，一種介於正規與非正規的灰色地帶(作戰環境)，橫跨實體與虛擬的範圍(空間)，結合國家與非國家行為者，透過政治、經濟、軍事、外交、法律、網路等途徑，使用模稜兩可性、利用非歸屬性以實現其戰略目標，同時又可有計謀地限制其他國家的反制行動，降低民眾對「基於規則體系」的信心、規則及其帶來的可預測性，並適時規避國際法律責任的追究，以

獲得具有更大算計之政治目標(汪毓瑋，2021)。

Najžer(2020)指出，正規戰通常被視為國家彼此間的對抗，而混合戰具有流動性，融合正規與非正規的因素在內(如圖 2)，利用多樣性政策工具與手段影響國際秩序的穩定，甚至可讓目標對象產生誤判，縮短反應時間，使行為者得以迅速達成階段性目標。

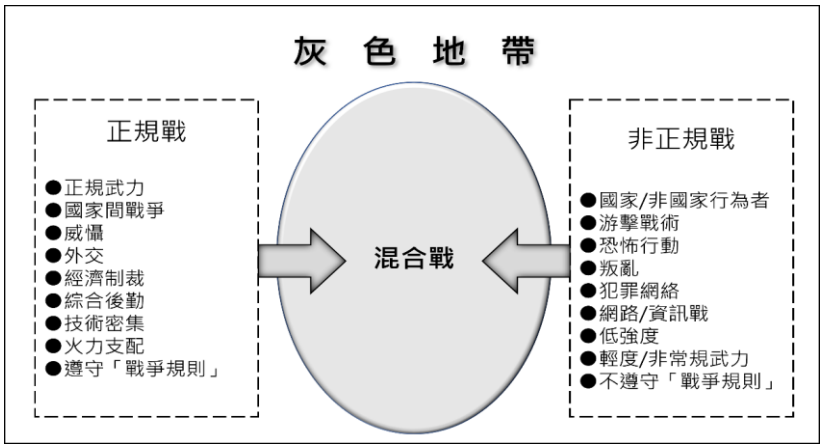

圖 2 混合戰是正規和非正規戰爭的混合體

資料來源：Najžer (2020, p. 31)。

(二) 高度依賴網路與通訊

戰爭初期，烏克蘭通訊與網路設施遭受大規模導彈與網路攻擊而中斷，連帶影響烏軍的指揮作戰與任務遂行，然而當取得星鏈衛星網路技術，能夠接收歐美國家分享的情報資訊後，烏軍迅速發揮其抵抗韌性，得以提前掌握俄軍動向，予以反制，也成為民間和軍方通聯的重要管道，美國「馬薩爾科技」（Maxar Technologies）亦提供商用衛星影像，讓俄軍動態頻頻曝光。

至於俄國也深知網路癱瘓將對國家安全產生重大影響，包含經濟、金融、輿論傳達或戰爭決策，因此基於網路防禦的需要，俄國持續建構與世界不聯通的全俄互聯網(Runet)，以降低對境外網路的依賴，擺脫西方國家的束縛，達到保護國內關鍵基礎設施的安全與維持對國內民眾認知掌控的目的(黃郁文，2022)。

當戰爭或衝突發生時，網路遭破壞已是必然會發生的情況，也不利戰況後續發展，資訊網路的暢通與否將決定其他國家提供情資共享的即時性，以及面對網路通訊遭癱瘓時，所採取之反制行動能否達到效果，甚至不分平戰時，政治活動與假訊息的宣傳也從未停止，其目的都在於對特定對象(含個人、國家)產生影響，改變目標對象的認知，至於是否可以順利達成上述目標，關鍵在於訊息必須能夠順利傳

遞，因此，未來戰場上，網路安全絕對是致勝關鍵因素之一。

(三) 重視媒體的影響力作用

科技的快速發展改變人類所處的資訊環境，資訊傳播除了透過傳統媒體(例：電視、廣播、報刊)傳遞，現今，社群媒體也運用演算法篩選閱聽眾的需求，發送特定訊息。根據臺灣人工智能實驗室研究，社群媒體的「武器化(weaponization)」已成為現代戰爭和衝突不可或缺的一部分，它以數據分析推特的社群帳號在俄烏戰爭前異常的大量創建、頻繁轉貼文以及重疊活躍使用時間，證明俄國操縱資訊的可能性，它亦認為媒體不僅是宣傳工具，還在戰略溝通和公共外交中發揮作用(Hou et al., 2023)。

再者，由於越來越多人使用社群媒體取代傳統電子媒體取得新聞資訊，俄國於是鎖定各種社群媒體 APP、Podcast 散播假訊息，甚至是媒體事實查核機制也遭俄國利用，成為另類的輿論戰場。烏克蘭事實查核組織 StopFake 自 2014 年成立以來，致力提高不同受眾族群的媒體素養水準，告知媒體宣傳和傳播虛假資訊的危險，在新聞和宣傳之間建立明確的界線，以堅守媒體專業和營造健康環境(StopFake, 2022)。Azad(2021)指出，在混合戰之中，媒體將繼續發揮改變公眾輿論和塑造戰爭氛圍的作用，而其宣傳目的主要有三個，即獲得本國、敵國和中立國的支持，尤其面對危急時刻，它宣傳訊息、塑造公眾輿論、影響國際政治和防止軍事干預，已使媒體成為混合戰的重要工具(Azad, 2021)。

綜上，俄烏戰爭徹底展現軍事與非軍事手段融合運用的混合戰，許多準軍事行動更是遊走於灰色地帶，具體呈現混合戰的隱蔽性與模糊性，藉以降低民眾警覺，喪失對戰爭認識與安全威脅認知。在俄烏戰爭期間，俄國與烏克蘭都廣為運用網路與媒體，進行情資傳遞、輿論操控與戰略溝通等作為，甚至將軍事行為進行包裝後，再透由網路社群及媒體進行宣傳。因此，我國可汲取俄烏戰爭之經驗，瞭解到混合戰已成為現代戰爭趨勢，無論是軍事或非軍事手段，抑或是介於灰色地帶的衝突，都是國家安全必須面對的威脅來源，全國民眾應具危機意識團結一心，持續完善國家政策，以及國內外、公私部門間的交流合作，以下將從俄烏戰爭探討我國面對混合戰之應處作為。

肆、從俄烏戰爭論我國面對混合戰之應處作為

從俄國與烏克蘭運用混合戰的態樣得知，混合戰係於資訊網路、訊息、政治、

經濟、軍事及社會等不同領域中，將正規與非正規武力的手段融為一體，不完全是以軍隊為主體，而是包含非國家行為者及個人，並且有系統、有組織、有目標去攻擊敵對國家，以影響其經濟活動發展、動搖社會民心，甚至顛覆政治體制，達不對稱作戰之效果。因此，為應對混合戰的多元威脅與多樣手段，我國應以主動、務實的態度展開各項措施，一是提升民眾的防範意識與對威脅的認知，並引導參與相關議題的討論；二是加強應對混合戰之韌性與復原力；最後是深化國內外於不同領域的交流與合作，以全面降低混合戰造成的負面影響。

一、提升民眾防範意識及參與度

2022 年 8 月，美國眾議院議長裴洛西女士來臺會見總統蔡英文，中共除對臺灣發動正規武力的大規模軍演，也對總統府、臺電等政府網站和國營企業發動網路攻擊，更有多達四種以上不實資訊的敘事，散布於大陸、臺灣和國際輿論環境，此外，為了貼近民眾的日常生活，超商、車站的電子看板也被更換為簡體字，秀出「戰爭販子裴洛西滾出台灣」等用語，戰時如擴大運用，將可能成為心戰和認知作戰的有效利器(曾怡碩，2022)。

上述此舉已成為 1996 年臺海飛彈危機以來，中共對臺灣發動火力最強大的武力威嚇，演習期間也結合運用混合戰手段，然而綜觀臺灣民眾及整體社會輿論反應，似乎未有普遍的撻伐共鳴，也欠缺警覺和危機意識。面對中共始終不放棄武力犯臺，且持續增加國防預算挹注於正規與非正規的軍事行為，我國必須不斷灌輸民眾正確敵情意識，建立民眾參與討論的管道或機制，提升對國防的關注敏感度。如以新加坡(Singapore)的「全面防禦(total defence)」戰略而言，其強調涵蓋軍事、民事、經濟等六大支柱，並且首重心理防禦(Matthews & Timur, 2023)。基此，研究者提出三點論述。

(一) 建立全民國防觀念

國防法第 3 條明文規定指出，「中華民國之國防，為全民國防，包含國防軍事、全民防衛、執行災害防救及與國防有關之政治、經濟、心理、科技等直接、間接有助於達成國防目的之事務(周明輝，2011)。」基此，承平時期不應僅有軍人或其眷屬才關注國防事務，甚至認為打仗是軍人的事，政府平時應藉由學校教育、政府機關（構）在職教育、社會教育等面向，落實執行全民國防教育，提高民眾對混合戰的威脅本質的認識，強化「全民關注、全民支持、全民參與」的觀念。

在俄烏戰爭中，俄國對烏克蘭採用的混合戰方式，部分與中共對我進行的文攻

武嚇行為相似，但是我國民眾普遍未有共同抗敵的意志與心態。國防部先前即公布《全民國防手冊範本》並於今(2023)年公布《全民國防應變手冊》，提供民眾面臨軍事危機與可能發生災難時相關緊急應變資訊。2022 年，獨立媒體「沃草」(Watchout)也發行民間版民防手冊《公民行動指南—保護自己、守護臺灣：遇到危機與戰爭該怎麼辦》(王先正，2022)，上述皆有助於強化全民防衛力量，增進民眾對全民國防之認知。

(二) 加強安全警覺意識

新加坡的心理支柱(Psychological Pillar)之防禦重點在於加強民眾面對危機的決心和韌性，於人際間建立特定的集體意志和承諾，能夠促進彼此的相互信任，提升對社會和政府機構的信賴度，有助於抑制會影響公眾輿論、國家利益、危及政府合法性和國家認同的假訊息(Matthews & Timur, 2023)。尤其在混合戰中，行為者會透過網路、社交媒體等途徑進行分化、煽動、恫嚇等手段，容易擾亂民眾的思維、情緒和行為。

因此，為提升民眾應對混合戰的防範意識，政府可從教育面著手，建立民眾參與討論之平臺，例如辦理講座、研討會、戰鬥營等活動，輔以教育和宣傳，增進公民參與度，共同探討混合戰的手法與可能造成之影響，亦可透過演習，使民眾瞭解混合戰的威脅來源，鼓勵民眾提出想法與建議，在提高對混合戰的認識和警惕性之餘，還可鏈結彼此情感，增進互信合作，凝聚社會向心。

(三) 提高媒體識讀(media literacy)能力

身處數位傳播時代的每位民眾，每天接收的訊息不乏存在假訊息，某些國家意識到辨識假訊息的重要，已將媒體與資訊素養教育納入學校課程，例如英國公視 BBC 自 2018 年開始對中學生進行課堂與線上教學，以及泰晤士報(The Times)在中學與大學推動媒體素養方案，或由政府向社群媒體公司徵收教育稅，作為發展數位素養教育架構的資金(胡元輝，2019)，以建立民眾批判性思考的辨別能力。

2019 年，我國將「科技資訊與媒體素養」列為十二年國民基本教育 9 大核心素養之一，以灌輸學生能夠瞭解運用媒體與資訊工具之創造性潛能，以具備媒體識讀能力，更於 2023 年 3 月頒布「數位時代媒體素養教育白皮書」，闡述未來媒體素養教育執行內容(教育部，2023)。基此，面對混合戰的威脅來源，持續提升民眾的媒體識讀能力有助於理解資訊的真實性，從而判斷其可信度，以降低假訊息的影響程度，提升社會整體防範意識和應處能力。

二、加強應對混合戰之韌性與復原力

韌性係指「能夠預測、準備、應對、適應環境持續變化的威脅以及突發性運作中斷時，組織仍能繼續生存和維持發展的能力(謝翠娟、蔡君微，2020)」，因此，一個具備韌性的政府、組織或單位，不僅能夠永續經營，還能夠在緊急情況有效率地展現修復能力。俄烏戰爭帶來的啟示之一，在於烏克蘭在政治、經濟、軍事、數位領域，以及全國人民的心理意志，都展現十足的抗敵韌性。

混合戰係利用國家的脆弱性，範圍涵蓋政治、軍事、經濟、社會、資訊和基礎設施，因此，我國應對關鍵功能和脆弱性進行自我評估，並定期進行維護。跨國能力發展行動(A Multinational Capability Development Campaign project, MCDC)的報告指出，混合戰使用協同一致的軍事、政治、經濟、民事及資訊等超出軍事領域的權力工具(Cullen & Reichborn-Kjennerud, 2017)，應從識別關鍵功能、發現脆弱性到建立具有韌性的機制，以致力提升對混合戰的自我評估能力(如圖 3)。

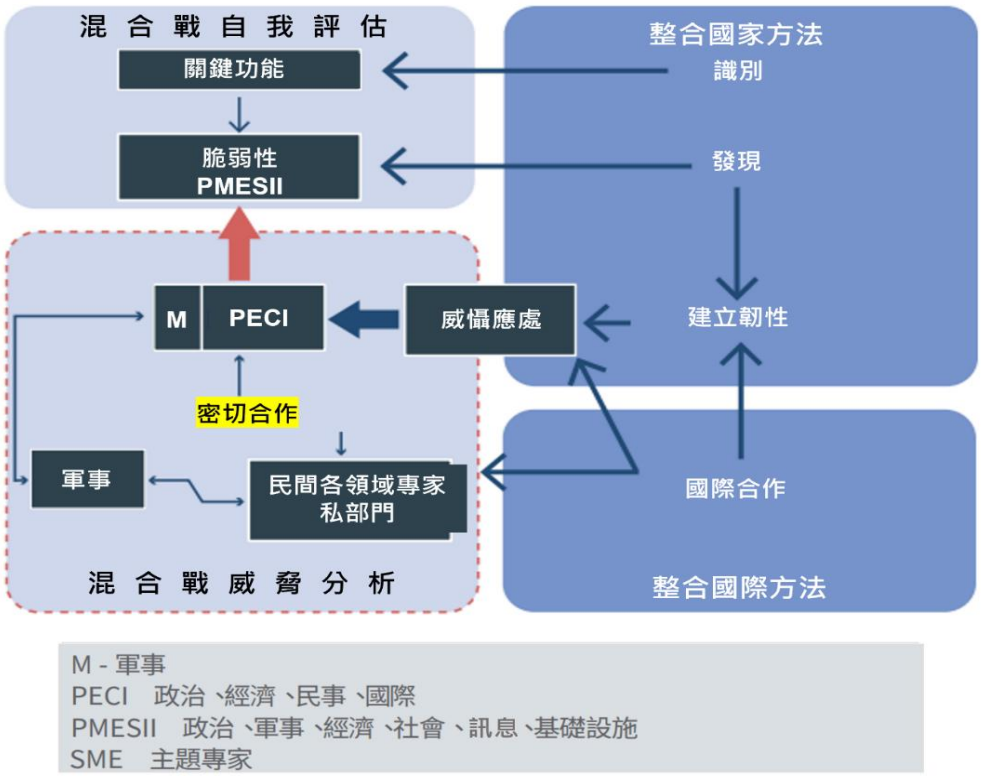

圖 3 應對混合戰的建議措施

資料來源：Cullen & Reichborn-Kjennerud(2017, p.23)。

(一) 塑造組織文化與韌性

組織文化(group culture)代表個人與組織共享的價值觀與行為規範，包含運作

策略、機制流程與領導風格。由於俄烏戰爭令人意識到社會的集體脆弱性，更瞭解到軍事韌性與社會韌性相互依存的必要性，有必要發展具備彈性與韌性的組織，能夠因應外在威脅改變適時修正核心任務，以妥善應付複雜的戰場空間與環境，並且基於信任與透明度，發展跨組織的問責管理制度，嚴守組織價值，並訂立團隊韌性與國家韌性的具體目標，以應對混合戰帶來的威脅(英國標準協會，2023)。

(二) 加強政策前瞻與應變能力

混合戰的手段具有多元與模糊的特性，且全面地透過政治、經濟、社會、外交、社會及軍事等方面影響目標對象，政府應加強對混合戰未來演化的前瞻預測能力，依據國家利益及國家戰略預先制定完善的應對策略和計畫，並納入相關變數考量，預判可能錯誤之因素，適時調整政策方向以應對各種突發狀況，確保政府和關鍵基礎設施部門服務的系統性，以增強政府的應變能力。

(三) 發展多元經濟與存儲機制

俄烏戰爭引發全球能源危機，使各國認知到經濟與能源安全的重要性，我國須建立多元化的經濟結構，避免過度依賴某一特定公司或國家，一旦這些產業或國家拒絕提供必要資源，將使我國在戰爭中處於劣勢；此外，因應戰時遭經濟制裁或脅迫，政府應確保民生、能源及衛生系統能夠因應危機發生，充實醫療人力，提升醫院備援量能，同時建立國家戰備物資儲存機制，預先儲備必要關鍵物資、資源，並慎選儲存地點與區域，以利緊急情況下的供需無虞。

三、深化國內外各領域交流合作

混合戰係同步運用各種管道，有系統地對目標對進行騷擾和破壞，政府應以指導和協調自我評估和威脅分析的方法，各部門共同合作以了解、偵測和應對混合戰的威脅。在國內方面，可建立跨層級、跨部會以及與民間組織的合作機制，在國際上，除了在現有合作的基礎上精進相關策略，應持續與理念相近及友好國家建立合作管道，發展密切的情報共享，深化多元領域的實質夥伴關係，同時增加具威脅國家的透明度，研究者提出以下建議。

(一) 完善公私部門協調合作

為應對混合戰的多元威脅，已無法單獨依賴單一公部門(public sector)處理，從國防部、外交部、經濟部等部會，各自皆有負責的安全威脅，然而在權限受限下，如何協調與溝通成為極為重要的關鍵因素，我國可參考北約成立專責機構負責指揮與管制，統籌各部會資源與能量，共同制定和執行協調一致的國家戰略或行政命

令，並區分平時行政指揮與戰時作戰指揮鏈，避免多頭馬車、步調不一，以提升公部門應對混合戰之效果。

混合戰係將正規與非正規武力的手段融為一體，在軍事政策上，我國應建立靈活且具戰鬥力的專業部隊，理解對手的混合戰並及時反應，並加強網路、資訊、電磁及認知等不對稱作戰能力，創新戰術戰法，以強化國防戰力與韌性；另可預想未來作戰環境，促進相關領域專業部隊與民間學術、研發單位交流，結合理論與實務，以應對混合戰之挑戰(黃柏欽，2019)。

(二) 爭取國際合作交流

根據北約 2022 年的《戰略概念》，分別將俄國與中國定位為「最重大威脅」與「系統性挑戰」，須透過「合作性安全」(cooperative security)以確保北約各國的安全和防禦，並首次強調印太地區對北約的重要性，承諾將透過強化與印太區域夥伴的合作與對話(鍾志東，2022)。基此，我國可學習和借鑒其他國家和地區的經驗和做法，主動表態加入制衡中共的威脅擴張陣營，並與相關國家深化交流合作，提高自身競爭力和影響力。

此外，我國應以建設性方式解決問題，不僅可與理念相近國家加強和建立基於相同利益的新關係，爭取設立「印太反混合威脅中心(Indo-Pacific hybrid threat center)」於臺灣，有助於提供更具前瞻及預測性的分析(Seebeck et al.,2022)，還可與世界各地民間社會團體、私營公司、慈善機構、地方政府和智庫，尋求更具包容性的發展夥伴關係，進而解決脆弱性、衝突和危機的根本原因。

(三) 支持透明度及反腐敗

現今，中共採用廣泛的政治、經濟和軍事工具進行全球性的力量投射，對戰略、意圖和軍力擴張依然保持不透明，且不斷深化與俄國的戰略夥伴關係，破壞基於規則為基礎的國際秩序。為秉持合作性安全的理念，我國應持續投入資源以提升自身能力，互相支持合作夥伴，以防範、嚇阻和防禦國家及非國家行為者運用政治、經濟、能源、資訊和其他混合戰的脅迫手段。

針對構成最直接威脅的國家，政府或智庫單位可定期發布相關研析報告，例如：美國蘭德智庫發布的「瞭解俄羅斯混合戰(Understanding Russian Hybrid Warfare)」(Chivvis)、美國資安公司 Mandiant 發布的中共網路活動報告(吳奕軍，2022)，亦可舉辦論壇、研討會或公開與混合戰相關的資訊，增進民眾了解現況的機會，皆有助於提高政策透明度，降低對腐敗容忍度，增加發動混合戰的成本。

伍、結論

俄烏戰爭起源於地緣政治和意識形態的分裂與衝突，發生迄今已逾一周年，烏克蘭軍民團結一致誓死反抗，加上民主陣營國家的奧援，瓦解俄羅斯速戰速決的美夢，顛覆外界對這場戰爭的最初預測。本文認為混合戰是在正規軍事力量的行動期間，同時結合非正規的各種手段，將具有影響力的工具應用於目標對象，以實現其國家利益，此種戰爭行為不僅改變傳統認知的國家安全威脅來源、威脅特性、執行方式與行為者，也成為各國檢討國家安全戰略的重要參考之一。

在混合戰的新型態威脅下，烏克蘭面臨來自俄國各種不同的挑戰，包括政治、經濟、軍事、網路、外交和假訊息的攻擊，同時，烏克蘭也以混合戰方式展開反制行動，引發的思考是「非國家行為者」的影響力與作用逐漸顯現，無論是「匿名者」等駭客組織向俄國宣戰、俄軍傭兵組織「華格納集團」協助作戰，或是兩國透過社群媒體用戶積極發布與戰爭相關的訊息，無論訊息是真或假，確實對民眾判斷造成影響，也阻礙政府決策，使俄烏戰爭與國際輿論環境更加複雜且難以控制。

其次，由於全球化的趨勢，經濟貿易結構具高度相互依賴，即使某國違反國際規範，各國對其制裁力道及效果仍有限，尤其越是大規模的制裁行動，往往使制裁者與被制裁者均受創。在俄烏戰爭中，臺灣和中共均從中學習到寶貴經驗，而中共遠比俄羅斯來得更加靈活、更具有侵略性，早已意識到戰爭的勝負關鍵在戰場之外，也就是政治、經濟、外交、輿論、媒體等領域，勢必會持續積極向外擴張，營造有利於己的輿論氛圍，以建立絕對優勢的戰場。

綜上所述，透過本文對俄烏戰爭期間運用混合戰方式的探討，未來除了有賴政府相關部門制定周延的法規外，更須思考如何落實全民國防教育，建立民眾對訊息的正確辨識與媒體識讀能力，減少不實訊息造成的負面影響，並且持續匯集政府各部門應對混合戰的能量與資源，深化國內外各領域交流合作，提升國家的韌性與彈性，以利應對混合戰的威脅與挑戰。

參考文獻

一、中文部分

BBC News(2022/3/9)。俄羅斯入侵烏克蘭：歷史學家梳理 20 世紀烏克蘭歷史上六個關鍵節點。*BBC News 中文網*。取自 https://www.bbc.com/zhongwen/trad/world-60661810 (檢索日期：2023/7/20)

王先正(2022)。從「烏俄戰爭」帶來之啟示析論我國全民國防在職教育。*民國 111 年國防大學全民國防教育學術研究論文集*。桃園：國防大學。

何蕙安(2022/3/7)。【烏俄戰事】烏克蘭全民動員的抗俄資訊戰。台灣事實查核中心。取自 https://tfc-taiwan.org.tw/articles/7040(檢索日期：2023/3/3)

吳奕軍(2022/9/1)。中國宣傳戰日新月異：假媒體、假紀錄片、假電子書席捲全球。中央廣播電臺。取自 https://www.rti.org.tw/radio/programMessageView/programId/88/id/135679(檢索日期：2023/7/8)

汪毓瑋(2021)。我國面臨新型態混合式威脅下軍事情報工作之展望。*軍事社會科學專刊*，*19*，7-32。

周明輝(2011)。我國與中共全民國防教育之比較研究－兼論我全民國防教育未來展望。*國防雜誌*，*26*(4)，117-134。

況正吉、宋鎮照(2016)。從國內政治與國際因素分析烏克蘭危機。*全球政治評論*，*53*，41-66。

胡元輝(2019/3/8)。【全民國防】強化媒體識讀 辨認假訊息。*青年日報*。取自 https://www.ydn.com.tw/news/newsInsidePage?chapterID=1135484(檢索日期：2023/4/18)

英國標準協會(2023/4/20)。組織文化。*英國標準協會*。取自 https://www.bsigroup.com/zh-TW/Our-services/Organizational-Resilience/(檢索日期：2023/4/20)

國防部(2021)。*中華民國 110 年國防報告書*。臺灣：國防部。

教育部終身教育司(2023/3/30)。面向未來關鍵能力，深化媒體素養教育—教育部發布數位時代媒體素養教育白皮書。*教育部全球資訊網*。取自 https://www.edu.tw/News_Content.aspx?n=9E7AC85F1954DDA8&s=D8DDE34F0A469662(檢索日期：2023/4/20)

陳穎萱(2022)。從俄烏戰爭看假訊息的影響。*清流雙月刊*，*39*，16-21。

曾怡碩(2022/8/8)。中共軍演驗證其資訊作戰計畫也測試台灣數位韌性。*國防安全研究院*。取自 https://indsr.org.tw/focus?typeid=16&uid=11&pid=413(檢索日期：2023/7/20)

黃柏欽(2019)。戰爭新型態－「混合戰」衝擊與因應作為。*國防雜誌*，*34*(2)，45-68。

黃郁文(2022)。淺析俄羅斯「網路戰」-以 2022 年「俄烏戰爭」運用為例。*海軍學術雙月刊*，*56*(4)，88-104。

詹祥威(2022)。俄烏戰爭中的「混合戰」運用。*國防安全雙週報*，*51*，75-81。

謝奕旭(2007)。美軍「民事」與國軍「政治作戰」之比較。*復興崗學報*，*89*，209-238。

謝翠娟、蔡君微(2020)。後疫情時代韌性智慧政府運作思維。*國土及公共治理季刊*，*8*(4)，8-19。

鍾志東(2022/7/15)。評析《北約 2022 戰略概念》。*國防安全研究院*。取自 https://indsr.org.tw/respublicationcon?uid=12&resid=1905&pid=3074&typeid=3 (檢索日期：2023/4/20)

二、英文部分

Azad, T. M. (2021). Media as an Instrument of Hybrid Warfare. *Global Mass Communication Review*, *4*(1), 12-27.

Batyuk, V. I. (2017). The US Concept and Practice of Hybrid Warfare. *Strategic Analysis*, *41*(5), 464-477.

Bratko, A., Zaharchuk, D., & Zolka, V. (2021). Hybrid warfare: a threat to the national security of the state. *Revista de Estudios en Seguridad Internacional*, *7*(1), 147-160.

Caliskan, M., & Cramers, P. A. (2018). What Do You Mean by “Hybrid Warfare”? A Content Analysis on the Media Coverage of Hybrid Warfare Concept. *Horizon Insights*, *4*, 23-35.

Chivvis, C. S. (2017). *Understanding Russian Hybrid Warfare and What Can be Done About It*. the Rand Corporation.

Clark, M. (2020). *Russian Hybrid Warfare*. The United States of America: Institute for the Study of War. Retrieved from https://www.understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf (檢索日期：2023/7/15)

Cullen, P. J., & Reichborn-Kjennerud, E. (2017). *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare*. A Multinational Capability Development Campaign project.

Doyle, G. (2023/5/16). *With eye on Ukraine, top Chinese general calls for unconventional warfare capabilities*. Reuters. Retrieved from https://www.reuters.com/world/china/with-eye-ukraine-top-chinese-general-calls-unconventional-warfare-capabilities-2023-05-16/ (檢索日期：2023/8/17)

European Commission. (2022/4/20). *In focus: Reducing the EU's dependence on imported fossil fuels*. European Commission. Retrieved from https://commission.europa.eu/news/focus-reducing-eus-dependence-imported-fossil-fuels-2022-04-20_en (檢索日期：2023/7/15)

Goncharenko, R. (2022/2/16). *Russia's TV war against Ukraine*. Deutsche Welle. Retrieved from https://www.dw.com/en/how-russian-media-outlets-are-preparing-an-attack-on-ukraine/a-60801837 (檢索日期：2023/3/20)

Harwell, D. (2022/3/24). *Instead of consumer software, Ukraine's tech workers build apps of war*. The Washington Post. Retrieved from https://www.washingtonpost.com/technology/2022/03/24/ukraine-war-apps-russian-invasion/ (檢索日期：2023/7/20)

Hoffman, F. (2007). Conflict in the 21st Century The Rise of Hybrid Wars. https://www.potomacinstitute.org/images/stories/publications/potomac_hybrid-war_0108.pdf. (檢索日期：2023/7/15)

Hou, S. M., Fu, W. C. & Lai, S. Y. (2023). Exploring Information Warfare Strategies during the Russia–Ukraine War on Twitter. *The Korean Journal of Defense Analysis*, *35*(1), 19-44.

Jäger, T. (2021). *Hybrid Warfare Future and Technologies.* Insititut für Politische Wissenschaft.

Kirby, P. (2022/2/24). *Has Putin's war failed and what does Russia want from Ukraine?* BBC News. Retrieved from https://www.bbc.com/news/world-europe-56720589 (檢索日期：2023/7/15)

Kordan, B. (2022). Russia's war against Ukraine: historical narratives, geopolitics, and peace. *Canadian Slavonic Papers, 64*(2-3), 162-172.

Matthews, R. & Timur, F. B. (in press). Singapore's 'Total Defence' Strategy. *Defence and Peace Economics*.

McGuire, V. (2021). Hybrid Warfare: Russia's strategy to alter the international balance of power. *Marine Corps Gazette.* 34-37.

Microsoft Corporation. (2022). *Defending Ukraine: Early Lessons from the Cyber War*, 1-28. Microsoft Corporation.

Miller, M. (2015). *Hybrid Warfare: Preparing for Future Conflict*. Air War College, Air University.

Mumford, M. (2020). *Ambiguity in hybrid warfare*. The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/wp-content/uploads/2020/09/202009_Strategic-Analysis24.pdf (檢索日期：2023/7/15)

Najžer, B. (2020). *The Hybrid Age: International Security in the Era of Hybrid Warfare*, Bloomsbury Publishing Plc.

NATO. (2022). The 2022 Strategic Concept. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf (檢索日期：2023/8/17)

Nezhyva, M., & Mysiuk, V. (2022). War in Ukraine: challenges for the global economy. *Foreign trade: economics, finance, law, 121*(2), 16-25.

Pitrelli, M. (2022/3/1). *Global hacking group Anonymous launches"cyber war" against Russia*. CNBC. Retrieved from https://www.cnbc.com/2022/03/01/how-is-anonymous-attacking-russia-disabling-and-hacking-websites-.html (檢索日期：2023/4/13)

Raska, M., & Bitzinger, R. A. (2015). Russia's Concept of Hybrid Wars: Implications for Small States. *RSIS Commentary*, *91*, 1-3.

Renz, B. (2016). Russia and 'hybrid warfare'. *Contemporary Politics*, *22*(3), 283-300.

Restuccia, A., & McBride, C. (2022/1/14). *White House Says Russia Planning 'False Flag' Operation as Pretext for Invading Ukraine*. The Wall Street Journal. Retrieved from https://www.wsj.com/articles/white-house-says-russia-is-planning-false-flag-operation-as-pretext-for-invading-ukraine-11642182308 (檢索日期：2023/7/15)

Roth, A. (2022/2/26). *"Don't call it a war"-propaganda filters the truth about Ukraine on Russian media*. The Guardian. Retrieved from https://www.thegua

rdian.com/world/2022/feb/26/propaganda-filters-truth-ukraine-war-russian-media (檢索日期：2023/3/10)

Schnaufer, Tad A. II. (2017). Redefining Hybrid Warfare: Russia's Non-linear War against the West. *Journal of Strategic Security*, *10*(1), 17-31.

Scott, K. D. (2016). *Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World*. Joint Chiefs of Staff Washington United States. https://publicintelligence.net/jcs-joe-2035/

Seebeck, L., Williams, E. & Wallis, J. (2022). *Countering the Hydra: A proposal for an Indo-Pacific hybrid threat centre.* Australian Strategic Policy Institute. Retrieved from https://www.aspi.org.au/report/countering-hydra (檢索日期：2023/7/15)

Silverman, C., & Kao, J. (2022/3/8). *In the Ukraine Conflict, Fake Fact-Checks Are Being Used to Spread Disinformation*. ProPublica. Retrieved from https://www.propublica.org/article/in-the-ukraine-conflict-fake-fact-checks-are-being-used-to-spread-disinformation (檢索日期：2023/4/26)

StopFake. (2023). Retrieved from https://www.stopfake.org/en/about-us/ (檢索日期：2023/7/10)

Supruniuk, L. (2022/6/30). *Yegor Aushev, CyberUnit. Tech & Cyber School "Our* mission *is to elevate the perception of Ukraine as a country of innovation"*. Techukraine. Retrieved from https://techukraine.org/2022/06/30/yegor-aushev-cyberunit-tech/ (檢索日期：2023/5/10)

The Economist. (2022/2/9). *Vladimir Putin is already battering Ukraine* economically. The Economist. Retrieved from https://www.economist.com/europe/2022/02/22/vladimir-putin-is-already-battering-ukraine-economically (檢索日期：2023/5/6)

Visit Ukraine. (2022/10/1). *Starlink: why the Internet from Elon Musk is crucial for Ukraine*. Visit Ukraine. Retrieved from https://visitukraine.today/blog/1046/starlink-why-the-internet-from-elon-musk-is-crucial-for-ukraine (檢索日期：2023/5/2)

Walsh, N. P. (2022/8/9). Russia dangles freedom to prisoners if they fight in Ukraine. Many are taking the deadly gamble. *CNN*. Retrieved from https://edition.cnn.com/2022/08/09/europe/russia-recruits-prisoners-ukraine-war-cmd-intl/index.html (檢索日期：2023/5/1)

Wesolowski, K. (2022/4/28). Fake news further fogs Russia's war on Ukraine. *Deutsche Welle*. Retrieved from https://www.dw.com/en/fact-check-fake-news-thrives-amid-russia-ukraine-war/a-61477502 (檢索日期：2023/7/16)

Wither, J. K. (2016). Making Sense of Hybrid Warfare. *Partnership for Peace* Consortium *of Defense Academies and Security Studies Institutes*, *15*(2), 73-87.

收件日期：2023 年 05 月 19 日

一審日期：2023 年 05 月 23 日

二審日期：2023 年 07 月 12 日

採用日期：2023 年 07 月 25 日

(本頁空白)