國防大學政戰學院政治學系

政治研究所碩士班

碩士學位論文

中共對臺施展混合性威脅之探討

Discussion on the Possibility of Chinese Communist Party Exerting Hybrid Threats

研　　究　　生：王彥鈞 撰

指　導　教　授：汪毓瑋 博士

中　華　民　國　一　〇　九　年　六　月

謝辭

「夫讀書將以何為哉?辨其大義，以修己治人之體也，察其微言，以善精意入神之用也。」讀書要達到融會貫通、活用自如的境界，必須將學習到的知識、理論基礎付諸實踐，並能夠解決生活及工作上遭遇的各種難題。

這一年八個月的研究所時光得以讓我好好檢視自己的不足，重新充電再出發，因此，我格外地珍惜；把握校外研究及假日的時光，好好投資自己的外語能力、參加外交部國際青年大使甄選、長風基金會海外交流暨企業參訪、教育部全球趨勢論壇、亞太事務青年培訓營……等校外活動。也逐一完成了部分人生夢想清單選項，如:利用寒暑假出國旅遊，造訪奧地利、捷克、美國、俄羅斯、澳洲……等國家；挑戰 101 大樓登高賽、參加白陽大道全國聯合徵文比賽獲第一名，遍訪台北地區的博物館、美術館及各類展覽，為短暫的研究所時光增添些許色彩。

本論文得以順利完成，要感謝指導教授汪毓瑋老師在撰寫過程，不辭辛勞的教導，從理論架構之啟蒙、研究方法到內容撰寫過程中逐一指導、啟迪與匡正，使本論文得以更臻完善嚴謹。

此外，要感謝家人的支持，讓我無後顧之憂，全力在學業上衝刺；以及語婷的陪伴、鼓勵，讓我持續不懈地向前努力，在人生的旅途上很慶幸有你們的加油打氣，謹以此論文獻給我最親愛的人。

2020 年 6 月 於復興崗

國防大學

National Defense University

摘要

21 世紀的「混合戰爭」已經變得更加明顯。「全球化時代」開闢了更多的新技術和通訊選擇，並縮短了距離，而使「混合戰爭」更易實施且不易被明確定位及揭露。實施者可能是國家和非國家行為者的組合，而不是單一實體；且針對社會全光譜系功能的特定脆弱性，在整體的戰略規劃下，會透過運作民間機制而使用非暴力手段，通過電子和社交媒體、電視頻道和出版物進行大量宣傳等諸多影響方法混合到常規戰爭、非正規戰爭、資訊戰、宣傳戰和網路戰之中，同時掌握高度適應性和韌性戰場空間的靈活和複雜的動態情勢，以達到協同效應及顛覆目標國之效果。

本文的目的在於探討混合性威脅（hybrid threats）與混合戰（hybrid warfare）在理論上的相關概念、意涵及其對於我國國家安全的影響，並討論近年以來，中共運用在混合威脅手法之思維發展，以及臺灣的因應之道。本文研究認為，對抗混合威脅的根本之道在於，必須改變舊有的「戰爭」傳統觀念與思維，從計畫性、線性、規則性的常規戰爭思維，轉變為突變性、同時性、不規則、非對稱及混用常規與非常規的思維，應是當前我國國安戰略的重點。

關鍵字：灰色地帶、混合威脅、混合戰、國家安全

Abstract

The “hybrid warfare” of the 21st century has become more evident. Globalization has opened up more new technologies and communications options and shortened distances, making hybrid warfare easier to implement and less easily targeted and exposed. The implementers may be a combination of state and non-state actors rather than a single entity; And for the specific vulnerability of full spectrum of society function, under the overall strategic planning, through the operation mechanism of folk use nonviolent means, through electronic and social media, television channels, and a large number of propaganda, and many other publications mixing effect method to conventional war, irregular warfare, information warfare, the propaganda war and network war, at the same time grasp the high adaptability and resilience of battlespace flexible and complex dynamic situation, in order to achieve synergy effect and subvert the target.

The purpose of this paper is to explore the theoretical concepts and implications of hybrid threats and hybrid warfare and their impact on Taiwan's national security, and to discuss the development of hybrid threat tactics applied by the communist party of China in recent years, as well as the countermeasures for Taiwan. In this paper, we must change the traditional war concept and thinking, from linear and regularity conventional war thinking into respectively、simultaneity、irregular、asymmetrical and combination of conventional and unconventional thinking, will should be the focus of the current the national security strategy.

Keywords: Gray area、 Hybrid threat、Hybrid warfare、National security

目錄

第一章、緒論

第一節 研究動機與目的

壹、研究動機

近年來由於全球化的快速變遷與衝擊，使得許多原本單純涉及資訊、商業、媒體、環境、人口與疾病擴散等非軍事議題的社會經濟問題，也逐漸與軍事因素交互影響、整合，而擴散、滲透到「傳統安全」領域以外的趨勢。

儘管兩岸情勢在不同的時空背景存在不同變化軌跡，但事實上中國從未放棄以武力侵犯臺灣的意圖。在此情況下，兩岸在經濟與軍事科技整體實力逐漸失衡，以及在國際政治影響力日漸擴大情況下，如何有效防範並因應中國對臺灣實施的混合威脅?乃成為近年來探討臺灣國家安全日益重要的課題。

中國解放軍在2015年成立新軍種「解放軍戰略支援部隊」，任務內容包括情報、技術偵察、電子對抗、網絡攻防、心理戰等領域。而從近期的攻擊樣本分析來看，目前中共對我國進行網路攻擊的組織，與過去有所不同，配合情報體系進行網路攻擊。在網路、新媒體及新傳播科技影響下，大量假訊息的散播對我社會產生影響，持續性的網

路攻擊指向我國政府及產業，資訊與網路安全成為我國家安全重要防線。

俄羅斯總參謀長格拉西莫夫（Valeri Vasilyevitch Gerasimov）將軍指出：21 世紀的戰爭與和平界限已經日趨模糊且逐漸淡化，戰爭將不再宣布便開始，並根據與過往不同、以及傳統上並不熟悉的戰略模板（Template），透過混合與時俱進的戰術來設計實踐[1]。

當代威脅行為者在新的科技與技術輔助之下，操作同步性與組合戰爭類型的複雜程度均日益提高，以致對於傳統的軍事強權國家優勢逐漸削減。為洞悉新型戰爭型態的發展趨勢，瞭解混合戰的內涵與衝擊、挑戰，以及掌握對混合戰的防制與反制作為，以作為我國因應混合戰威脅型態與建軍備戰的參考，即為本文的動機。

貳、研究目的

根據上述的研究動機，本論文旨在瞭解當前中共運用之「混合性威脅」對臺灣國內造成的影響；且為防止中共進而運用「混合戰」，必須著力發展反制手段與防護措施，以因應未來的挑戰。「混合戰」呈現當前資訊、科技時代的新型「準」戰爭模式，運用混合與創新、

1 汪毓瑋，《臺灣視野之下世界安全局勢與持續努力方向》(清流月刊，2018 年)，頁 27。

不對稱的戰術、戰法，破壞目標國政經穩定與城市發展，攻擊新聞及言論自由弱點，造成受攻擊目標的挑戰。

簡言之，未來的衝突環境不僅只是傳統戰爭或非常規戰爭的區別，而是具有各種組合變化的概念。威脅本身具有不同危害類型之「同時發生」和「結合」的本質，以實現作戰和戰略優勢。

因此，期盼透過本研究思考我國政府在國家安全政策上應有之努力作為。而主要目的有以下三點：

第一、如何詮釋混合性威脅之內涵?

第二、中共對臺混合威脅之探討?

第三、我國應對中共混合性威脅之策略?

第二節 文獻回顧

文獻檢閱之目的，在於參閱過去的研究文獻，使研究者了解過去在相關領域中的研究狀況，並且藉此過程修正自身可能面臨的同樣問題，並且找出對於研究有益的地方。本研究文獻探討分為二類。第一類側重於混合性威脅的概念與定義，藉以理解混合性威脅並為其出現提供基礎。第二類包括解釋、討論和建構混合性威脅概念的文獻，從概念上理解中共對臺施展混合性威脅的有關作為。

壹、混合性威脅的起源與定義

回顧歷史，威脅行為者結合戰爭類型以實現其戰略目標早有脈絡可循。然而，新興的混合性威脅更有更大程度的組合能力，利用傳統和非常規手段形成混合性作戰之力量，以實現戰略效果。目前學者對於混合性威脅的看法不一致，缺乏普遍共同接受的定義。

第一、北約的「拱頂石概念」(Capstone Concept):對當前或潛在的「對手」所構成的威脅，這些對手具有能力同時採用傳統(conventional)和非傳統(non-conventional)的手段，以實現其戰略目標。

第二、霍夫曼(Frank G.Hoffman):在戰場上，任何對手同時且適應地以融合性的組合，使用傳統武器(conventional weapon)、非常規戰術(irregular tactics)、恐怖主義(terrorism)和犯罪行為(criminal behavior)，來實現其政治

目標。[2]

第三、美國《陸軍作戰手冊》(Army Field Manuals):常規武力(regular forces)、非常規武力(irregular forces)、犯罪份子的多樣化和動態(dynamic)組合，或是這些力量和要素都同時組合與結合，以實現互利的效果。[3]

混合性威脅難以清晰列舉所有組合的型態，因此不易訂定所有學者均能一致認同的定義，然而，應對混合性威脅的關鍵並非精確定義，而是不斷的因應外在環境變化，調整其防禦機制，以適應外部安全的條件。

軍事理論的源起與發展，往往由於戰爭經驗的累積或隨著科技的進步、重大突破，從而改變戰的型態與方式。然而，軍事理論的發展，亦有出於軍事理論家或學者對當前各種戰爭要素的本質，不管是有形物質（武器、裝備、糧秣、科技、經濟、財力），無形精神（士氣、意志、勇氣、毅力、民族精神、尚武精神）、素質與智慧（指揮、將道）和組織（領導、指揮、制度、體制、政策）等等[4]的變化，或針對戰爭要素的運用方式洞察與先見，提出創新的思維與觀點，從而成為指導下一場戰爭的藝術與規範，亦有此前相關理論的逐次發展與演化。[5]

[2] Frank G.Hoffman, "Hybrid Vs.Compound War,"Armed Forces Journal,2009, Vol.1,p.2.

[3] United States Army,Fm3-0 Operations(Washington,DC:United States Department of the Army,2008)

[4] 談遠平、康經彪，《戰爭哲學》（臺北市：揚智文化，2004 年），頁 214。

[5]胡敏遠，《貫徹國軍軍事戰略－『防衛固守、重層嚇阻』作為之研究》，(陸軍學術雙月，2018

混合性威脅即是在軍事人員、軍事理論家對當前幾次衝突，就戰爭參與者雙方偶然地或蓄意所作出的「類」戰爭行為、作戰行動、戰術變化的整理與探討，提出創新的軍事理論內涵。

此外，接續混合性威脅思考而來的混合戰亦具有第四代戰爭、複合戰爭、超限戰……等理論特徵，成為混合戰理論發展的基本原理。

「混合戰」概念的源起，最早可溯源至威廉・聶梅(William J. Nemeth)在2002年所撰寫的《未來戰爭與車臣：一個混合戰案例》(Future War and Chechnya: a Case for Hybrid Warfare)論文。論文透過對車臣分離主義運動的個案研究，探索混合型社會和混合型軍事的理想典型。在假設混合戰型態越來越普遍下，希望能夠提供如美國等的軍事強權，未來在因應混合戰時的相關建議。[6]

其後，2005年美國海軍陸戰隊詹姆士・馬提斯(James N. Mattis)中將與法蘭克・霍夫曼(Frank G. Hoffman)中校共同發表的一篇〈未來作戰：混合戰的興起〉(Future Warfare:The Rise of Hybrid Wars)文章提到，阿富汗和伊拉克的寶貴經驗，使人們開始反思，不僅不能再準備打上一場的戰爭，也不能再準備打一場自己想像的、自己想要的戰爭。近幾場軍事衝突使

年)，頁 17。

[6] 倪一峯，《俄國對克里米亞混合戰的運用：兼論對我之啟示》，國防雜誌 33 期 (2018 年 12 月 1 日)，頁 45。

我們必須銘記未來的敵人會是一個富有創造力的敵人，未來的戰爭將不會依照我們的規則進行。[7]我們應對未來可能面臨的非傳統對手作準備，尤其是以下不規則挑戰者—恐怖主義、叛亂、超限戰、游擊戰或毒梟的脅迫，未來將可能面臨此種挑戰者和敵人運用各種新穎作戰方法的挑戰—不同戰爭模式和戰爭手段的合成與組合，這就是所謂的混合戰。

法蘭克・霍夫曼復於2007年出版《二十一世紀衝突：混合戰的興起》(Conflict inthe 21st Century: The Rise of Hybrid Wars)乙書，提出當前面臨的主要混合威脅包括正規作戰能力、非正規戰術，暴力、脅迫等恐怖行動，以及犯罪失序等等，並認為已進入新的戰爭型態。[8]

隨後的幾場戰役實踐，混合戰新型戰爭型態與作戰方式，漸受各界重視。歐、美研究人員普遍認為，蘇聯在冷戰時期所使用的顛覆、隱蔽行動、宣傳與假消息等手法，早已具混合戰的特質，俄羅斯在車臣戰爭、俄喬衝突、入侵克里米亞與烏東情勢中，以及近年影響歐美選舉，將混合戰發揮的淋漓盡致。然而，相較於歐美論述混合戰或混合性威脅時，總以俄羅斯近年的幾次軍事衝突作為混合戰發展與運用的例證，並指責俄羅斯對其之混合攻擊。俄羅斯也認為，美國與西方國

[7]汪毓瑋，《情報、反情報與變革》(台北:元照出版有限公司，2018年)，頁22-23。

[8] Frank G. Hoffman, "Conflict inthe 21st Century: The Rise of Hybrid Wars" (Virginia:Potomac Institute for policy studies Arlington,2007),P.5.

家才是發展與運用混合戰攻擊、影響他國政權的始作俑者。[9]

俄羅斯總參謀長格拉西莫夫(Валерий Васильевич Герасимов)於2013年2月參加軍科院全體大會的一篇題為〈科學的預見價值〉(Ценность наукив предвидении)報告中就認為，美國與西方國家在北非和中東所推動的顏色革命、阿拉伯之春，是21世紀的戰爭新典型，戰爭規則遭到改變，非軍事手段在實現目標上的作用性增加，甚至超越傳統武器的力量。[10]

雖然文中沒有使用混合戰的名稱，但所指的內涵即意指西方運用混合戰方式，來推動民主浪潮。此後，格拉西莫夫於2016年3月的另一篇〈混合戰需要高科技武器和科學論證〉文章，則直接指出「顏色革命」是混合方法、混合戰的主要手段。[11]因而，混合戰緣起於何處？究竟誰最先發展運用混合戰？呈現各說各話的情形。

不論是否這些混合性戰爭系統的效果有無被誇大，但融合了現代化軍事技術和資訊系統、網路空間的廣泛與方便利用、情報作為的革新、不同性質參與者之多樣化結合等之變

[9] 同註1。

[10] Валерий Васильевич Герасимов, “Ценность науки в предвидении（科學的預見價值；The Value of Scientific Foresight）” ВПК, 2013/2/26, <https://www.vpk-news.ru/articles/14632>.（檢索日期：2019年10月17日）。

[11] Валерий Васильевич Герасимов, “По опыту Сирии（依敍利亞的經驗；The Lessons Learned from theExperience of Syria）,” ВПК, 2016/3/9, <https://vpk-news.ru/articles/29579>.（檢索日期：2019年10月15日）Frank G. Hoffman, p. 14.。

化仍正當化了此新的概念，且使其有新的內容而能更佳的詮釋當下之威脅實質及所引發之衝突，對手模糊不易鑑定以及困難回應等的事實。

相關定義還包括了:是一個國家除了執行混合了經濟、政治、外交等必要手段，同時亦對其他國家或非國家行為者公開使用武裝力量的情況。[12]

是經由裁製而同時在一個戰爭空間，混合了傳統武器、非常規戰術、恐怖主義和犯罪行為，以獲得(一個集團)的政治目標。[13]

「混合性戰爭」是很複雜的，因為他不可能遵守「適用一切方法」(one size fits all)的模式。而是要最佳的使用所有可能的途徑，結合那些適應自己的戰略文化、歷史繼承(historical legacies)、地理現實(geographic realities)、及經濟與軍事手段。它們很複雜，且在衝突光譜系的每一個層次中或跨域施展，從戰術層次到戰略層次。可以由國家也可以由各式不同的非國家行為者執行，不論是有國家或是沒有來自於國家的支援，是可以調整及有彈性的，使用廣範圍系列的手段從戰場傳達政治或意識形態訊息到世界各個想要影響的每一個角落。而不需要國際法或規範的制約，甚至無須提出必要的「可取代性模性」而不容易被看穿。

例如俄羅斯對於東烏克蘭與克里米亞發動的戰爭，以及「伊斯蘭國」對於伊拉克與敘利亞的恐怖主義戰鬥，均是兩種混合行動方向。兩

[12] Patryk Pawlak,op.cit..
[13] Frank G. Hoffman,Conflict in the 21st century:The Rise of Hybrid wars

者均混雜了致命而執著的國家衝突及延長的「非正規戰爭」，俄羅斯對於戰爭採行的混合性途徑就是使用一切的工具，透過其軍事工具以激起可以利用的問題。混合途徑的事實特徵，就是國家與非國家行爲者使用所有的手段、非正規的、傳統的、網路、核子、戰略通訊、其至更模糊與航髒把戲（dirty trick）之結合，以達成其政治目標。[14]

也由於混合性戰爭大概都包含了一個控制主軸，並採用一系列工具及設計來實現針對打擊對手目標的觀念，因此，建立明確的責任和行動的意圖是必要的，以確保政策反應是合法和相稱的，然而，相對的，由於國際法的局限性，技術限制，權力向非國家行爲者擴散等等之因素制約，因此要實踐此等戰爭型態並不容易，作爲目標之對手可能也不易感受到，因而也增加了「可否認性」的機會，例如由於技術上的限制和非國家行爲者的參與，很難將網路攻擊歸結爲某個國家所爲，但儘管如此，美國政府過去會起訴中國官員涉嫌對其電腦網路進行網絡攻擊，並在索尼影視娛樂公司被襲擊後對北韓實行制裁。2017年1月，因爲民主黨遭受「重大惡意網路活動」而對俄羅斯個人和實體實行制裁。[15]

貳、中共對臺混合性威脅

2019年中共持續升高對我國威脅，首先是「外交打壓」，南太平洋島國索羅門群島，9月16日宣布與臺灣斷絕外交關係，並同時宣布與北京建立外交關係。與此同時臺灣與索羅門群島斷交、全面停止雙邊合作、關閉大使館。9月20日，台北宣布終止與南太平洋島國吉里巴斯的

[14] Guillaume Lasconjarias and Jeffery A. Larsen eds., NATO's Response to Hybrid Threats, op.cit..
[15] 汪毓瑋，《情報、反情報與變革》(台北:元照出版有限公司，2018年)，頁22-23

外交關係。這兩國與台灣斷交後，使得台灣目前的邦交國只剩下十五個國家；另外中共也在國際間施壓，要求遵守「一中原則」，矮化我國名稱，並於聯合國、「國際民航組織」(ICAO)、「國際刑警組織」(INTERPOL)、「聯合國氣候變化綱要公約」(UNFCCC)等打壓支持臺灣的國際行動。其次是「經濟施壓」，可能手段包括進一步限縮陸客、陸生、陸資來台，擴大縮減兩岸航班、暫停兩岸貨幣清算及限縮金融往來、要求代表性台商及重量級企業人士政治表態，或是威脅終止海峽兩岸經濟合作架構協議(ECFA)。第三是「激化對立的政治操作」，北京可能會配合對臺灣社會的加強滲透及其代理人加大各種政治操作，全面激化藍綠對立或是製造可能影響選情的危安事件。最後是「軍事威懾」北京對臺灣進行針對性軍事威嚇，旨在打擊我軍民士氣；軍機、艦頻頻巡弋台海及繞行臺灣周邊海空域，更意在造成臺海「內海化」的事實，並對美國、日本等發出警告。未來可能逐步升高的軍事行動還包括藉十一大閱兵擴大對台威嚇、持續實施對臺針對性演訓、中共海軍作戰艦船刻意駛進我鄰接區海域或於臺灣周邊海域劃設演習禁航區。

上述亦即現代與傳統武器的併用，軍事與非軍事手段的結合。為了取得勝利，除了正規軍事戰法外，還可運用恐怖戰、金融戰、心理戰、媒體戰等，以達到擾亂敵方社會及群眾心理的目的。中共使用非正規作戰的目的，不是運用懲罰性的傳統方法擊敗對手，而是要將衝突的利害關係，提高到敵人無法接受的水準並促使對手減少敵對行動或完全避免衝突。

第三節 研究途徑與研究方法

壹、研究途徑

研究途徑(Research Approach)是在說明研究者如何去研究、觀察、歸納、分析與分類的架構的方式；[16]本研究採「歷史研究」作為研究途徑，而歷史研究是一種將過去的史料作為研究對象，對某個事件作詳實敘述[17]，在政治學研究上，運用相關歷史資料與方法，進而描述一種制度的建立與發展，來說明及解釋與其他制度之間關係，[18]並透由歷史資料的收集，按時間順序來觀察中共透過各種有形、無形的非武力手段，影響臺灣的政治或決策發生的過程與結果，所產生的因果關係，推測其政策發展方向，是否有脈絡規則可循?是否有政策的延續性?

貳、研究方法

本文是以「文獻分析法」(Documentary Analysis)為主，將先大量蒐集國內外之相關文獻，包含專書論著、期刊論文、學位論文、與北京對臺政策相關之研究報告以及報章雜誌等資料。進行比較性的分析研究，加以深度研析、縱深討論、並以圖表、表格方式整理呈現，如此能有助於理解本論文所探討問題之全貌，便能夠進一步對本論文加強論述。透過文獻的蒐集、分析、研究來提取所需資料後，對文獻作客觀而有系統地描述，用以解釋社會現象甚至推測未來的一種研究方法。因

[16] 朱浤源，《撰寫碩博士論文實戰手冊》(臺北市：正中書局，2010 年 10 月第 5 版)，頁 182。
[17] 呂秋文，《如何撰寫學術論文：以政治學方法論為考察中心》(臺北市：臺灣商務印書館，2007 年)，頁 19。
[18] 魏鏞，〈行為研究法、制度研究法、歷史的研究法〉，輯於羅志淵主編《雲五社會科學大辭典，第三冊》(臺北市：臺灣商務印書館，1971 年)，頁 389。

為廣泛涉及前人在各領域的調查結果，已超越自己調查研究的侷限性，發揮站在巨人肩膀上看世界的能力，提供了解相關的概念。期望透過此方式做有系統地描述，確實掌握本論文之核心內容及撰寫主軸。

第四節 研究範圍與研究限制

一、研究範圍

本論文主要在研究探討中共對臺政策，分為時間及空間為研究主軸，故研究範圍概分二部分:

(一)時間範圍

本論文時間設定主要自習近平接任中共國家主席迄今，並置重點於2013 年至 2020 年之間兩岸政治、經濟、外交等互動情形。

(二)內容範圍

本論文主要研究範圍係為中共政治層面之對臺政策，將著重於探討中共如何運用「混合性威脅」，以分析未來對臺有關作為之方向。

二、研究限制

(一)混合性威脅已有國內外學者在各層面實施研究及論述,但未有一致定義,且議題寬窄不同,因此本研究必須探討關於混合性威脅的現有文獻和政府報告等公開資料分析。

(二)另限於目前國內混合性威脅研究者不多,因此經大量外文資料篩選後難免產生掛一漏萬之憾。

(三)中共官方文件常受該政府當局的嚴格管制,出版及發表內容亦受修飾、控制與不實等情,故在資料引用與參考上,希均盡以官方文件、政策報告、期刊、專書為主,新聞與網路資料為輔彙整運用分析,期資料引用上能經多方比對,獲得研究資料正確性,避免研究成果產生偏頗問題。

(四)混合性威脅為美國與西方國家所創立的名詞,因此在文獻上較容易受到西方觀點所影響,且有些案例相關調查結果尚未完全呈現,若隨意引用西方報導將有失偏頗。為求客觀,筆者以不帶批評的寫作方式進行歸類，僅以還原事情或案例分析。

中共官方所公布的軍事戰略中，並未將混合性威脅的詞語納入。中國國防部在今年的國防白皮書中提出新時代解放軍的使命任務「四個戰略支撐」[19]中，將捍衛國家主權、統一領土完整列為排名第二優先順序，更強調反分裂鬥爭形勢較過去更加地嚴峻。明顯可以看出中國在臺灣問題的用詞及態度越來越強硬，敵意也一再升高。在此次的白皮書中，儘管明白表示將增加對臺灣的繞島威嚇作為，更重申不承諾放棄使用武力，「保留採取一切必要措施」的選項，將「不惜一切代價」捍衛統一。這裡所提到的「一切必要措施」，便是本論文想探討的混合性威脅。

本論文預期能分析中共未來對臺方向，若仿照俄國混合戰方式侵略我國，就風險評估與可能景況，預判我國可能應處思維與方法。提供我國能防範於未然，從歷史的脈絡、角度去合理推斷、解釋中共政策背後動機，能夠提前爭取更多時間，迅速做出最佳因應之道。因此，為有效因應混合戰的威脅型態，需提高對混合威脅的互信合作與厚實遭受混合攻擊的復原能力，強化訊息管理與查證能力，以調整、建立適應混合戰的打擊能力。軍事事務革新不斷再變革，中共「混合戰」手段與方法也在不斷轉變，在未來戰場中佔有的地位將會越來越重要，國軍必須要正視此一趨勢，從全新的思考方向切入，並且依據《國防法》精神，結合國防戰略思維與軍事戰略構想，結合理論與手

[19]「四個戰略支撐」分別為:「為鞏固中國共產黨領導和社會主義制度提供戰略支撐」、「為捍衛國家主權、統一、領土完整提供戰略支撐」、「為維護國家海外利益提供戰略支撐」、「促進世界和平與發展提供戰略支撐」。

段因應戰場的實務發展，方能找出戰略的制高點，掌握化被動為主動的轉捩點，開啟化危機為轉機的機會與提前規劃應對之道，因應爾後有形、無形戰場瞬息萬變的狀況，以確保國家安全。

第二章、混合性威脅與混合戰概念、定義之比較

第一節 戰爭型態的轉變

以往美國軍事戰略設計之要打兩場主要戰區戰爭之可能性,似乎已經不太可能:而接續設計的所謂在一個主要戰區戰場、與在另一個地區之因應緊急事件回應之戰鬥與準備,可能性仍存在。此等情勢之發展,彰顯於目前美軍面臨與以往冷戰時期不同之三項挑戰:亦即何有效對付回教恐怖分子?如何因應伊朗等美國所稱謂之流氓國家核子武裝的預期發展?及如何與潛在浮現為美國軍事對手之中國交往?

因此,未來將要面對之兩種戰爭型態,一種仍是延續以往傳統之「正規戰爭」(Conventional War),另一種則是已進行多年之多樣化的「非戰爭軍事行動」(Military Operations Other Than War)。[20] 且必須關注隨著戰爭或衝突情勢發展,亦可能同時要協助其他國家建立其自己的安全能力、支持國內民事當局、協助遭遇地震等自然災難國家之人民、[21]準備嚇阻與擊敗新的威脅等之可能性,凡此均是軍方必須思考而盼能更佳應對之重要方向。亦即面臨了如何有效的平衡在什麼時候、在什麼地方及如何參與動態與不確定世界之行動需求,同時又要面對國內重要應對威脅優先事項之間的困難與挑戰。

---

[20] 有關非戰爭軍事行動動專論,請參考汪毓瑋,「從美、中等國陸軍非戰爭軍事行動發展趨勢探討我國陸軍應有作為」,中華民國99年陸軍年會專家學者論文集(龍潭),2010年9月28日,頁2-1～2-27。

[21] 有關軍方因應自然災難與緊急事件之專論,請參考汪毓瑋,「從國土防衛與民事支援探討危機管理範時下應有之全民防衛動員」,99年全民防衛動員新思維與展望學術研討會論文集(北投),99年8月26日,頁55-93。 汪毓瑋,「國軍災害防救能力之探討」,99年第三季國防大學陸軍學院學術研討會(八德),2010年9月23日,頁38-52。

(一)軍事戰略下之趨勢評估

1.發展不平均之威脅

一些全球性的趨勢,也會持續形塑國際安全環境與國家面對之衝突。 誠然「全球化」可能會增加繁榮,但也會擴散不穩定之不利影響。不公平的福利分配,創造了「富人」(Haves)與「窮人」(Have Nots)分離的社會。此等分離可能會被極端主義的意識型態利用,且導致嚴重衝突。而當社會努力調整以走向現代化與更大互賴時,反映出長期競爭與摩擦之錯誤分界,可能會爆發不可預測之事件。

1. 先進科技之負面利用

增強可用性與可負擔性之「科技」有助人類更好的發展,也能增加人類的生活福址;但相對的,也提供了不滿現狀的對手更加精緻的科技工具,並且促成一種網絡途徑之科技效率可以更強的運作,而增加被剝奪公民權的人利用來出口恐怖威脅的機會。

3.人口成長與流動之影響

改變的人口分佈與快速的「人口成長」所增強的城市化,可能會持續打破傳統、地方性規範治理、行為、認同,且會進一步限制已有壓力的政府。特別是對於經濟機會缺乏的地區,會造成潛在的不穩定與極端主義成長的可能。對於那些心存不滿的人,可能會反對已發展國家介入,挑戰傳統價值及沒有效率的政府。

4.資源稀少性競逐之衝突

增加之「資源需求」,特別是能源、水與糧食,是增加繁榮與人口

之結果。不斷成長之全球資源競爭，將會持續產生摩擦與增加軍事爭鬥的機會。同時，在此環境之下，經由「氣候變遷與自然災難」所點燃之人道危機，將會結合發展中國家本已困難的條件，而造成不穩定人口移動及提高潛在的傳染病。

5. 毀滅性武器擴散與失敗國家結合之威脅

目前各國最關切的問題，就是大規模毀滅性武器之擴散，及「已生敗」或「正在失敗」的國家之危及安全的擴散效應。利用大規模毀滅件武器之災難性攻擊，已是全球不穩定之潛在來源：已失敗或正在失敗的國家缺乏意願或能力去維持有效的領土控制，將會持續造成區域的不穩定與提供恐怖主義團體規劃與出口攻擊行動之理想環境。而這兩個趨勢的結合，將會構成一種重大與強制性的威脅。[22]

（二）持續性衝突之特徵

1. 多樣化行為者發起之衝突

在國家、非國家與個別行為者之間的長期對立，會增加使用暴力以達成其政治與意識型態目的之意願，也成為全球安全環境之特徵。與安全有關之危機會不定期的發生，其強度與範圍將會是各式各樣，且延續多久也不能確定。這些挑戰會在所有之陸上、空中、海上、太空與網路空間等場域發生。自然災難與人道緊急事件也會持續成為頻繁與不可

22 John M. Mchugh and George W. Casey Jr., Statement before the committee on armed services, Feb. 23, 2010, pp.2-4. (http://armed-services.senate.gov/ statemnt/2010/02 %20February/McHugh-Casey%2002-23-10.pdf) ,accessed on Feb. 23, 2020

預期之任務,而需要軍方與資源加以因應。在如此動態的環境下,軍方執行之行動橫跨了衝突之全光譜系，從人道與民事支援、到反暴動（Counter-Insurgency，COIN)、到正規戰爭，且經常是同時發生。

國家與非國家行為者其動機、目的以及這些行為者鑑定經常很難加以辨別,當部分行為是隱蔽性、或使用代理人[23],手段方式可能加以轉變,使其難以捉摸。而這些戰鬥是要獲得對於人民之影響力及取得他們的支持,因此任何國家想要成功的中心因素就是人民,但不同人民之間的衝突是很難避免的。且衝突之引發可能性、地點、持續性與強度,已更加的具有不可預測性。亦即在一個互賴的世界,衝突已更加的傾向於有潛在「外溢」之趨勢，造成了區域與全球之不穩定結果。

這些事情均會引發網路與全球媒體之24小時循環播報。衝突的細節與錯誤的資訊,也會經由社會通訊與網絡而流傳。而敵人將會利用這些地方性與全球性之媒體與通訊資源。

(1)國家行為者之衝突

從目前所面對之系列多元安全挑戰之複雜戰略格局方面思考,例如之前在中東之伊拉克,黎巴嫩;歐洲之喬治亞;南亞之阿富汗等戰爭。而部分國家之戰事所涉及之美軍與北約盟國,除了因應此等地區之作戰需求外，同時又要準備因應國家安全可能面對之未來挑戰。

而在中東地區之軍事戰略目標,是對付暴力極端主義與不穩定之威脅，且關切飛彈與大規模毀滅性武器擴散之威脅。在歐洲與歐亞地

23 「代理人戰爭」是指用第三者來代替自己打仗的戰爭。代理的第三者可以是政府、非國家武裝力量，或是僱傭兵。代理人戰爭的目的是打擊對手，但又不會引起全面戰爭。

區，則關注能源與跨國組織犯罪之安全挑戰與未解決的之領土等衝突。從長期美國與中國之競爭言，美國視中國將浮現為區域強權，且會以各式不同的方式造成經濟與安全之潛在衝突。因此要求中國軍力的成長，必須澄清其戰略企圖以避免引起地區摩擦。[24]

(2)非國家行為者之衝突

評估在可見的未來，暴力極端主義運動，例如「蓋達組織」與其他恐怖主義組織所構成之威脅仍存且短時間內不可能消除。

2.混合性威脅（Hybrid Threat）之衝突

正規的(Conventional)、非常規的(Irregular)、恐怖分子與罪犯能力之結合，使用不對稱性來付大國的優勢。混合威脅需要混合性的解決方案，有適應力的部隊才可以在各式不同情勢下，與不同類組之國家、聯盟與在地夥伴們一起發揮功能。因此，在既有之戰略環境，持續的全球趨勢、與二十一世紀衝突特徵下，部隊必須是聯合、跨部門、政府間、及多國團隊之一環，才能履行其全球承諾。[25]

（三）相互重疊之四大安全挑戰

未來衝突模式若從行為者之角度檢視，有多樣化行為者之衝突：若衝突樣式之角度檢視，則是混合性威脅之衝突，並可以歸納為四項挑戰：即非常規挑戰(Irregular Challenges)，主要是如何能夠擊潰恐怖分子的網絡；災禍式挑戰(Catastrophic Challenges)，主要是預防

24 Department of Defense, Sustaining US Global Leadership: Priorities For 21th Century Defense, Jan. 2012, p. 2. (http://www.defense.gov/news/Defense_Strategic_Guidance.pdf),accessed on March 20, 2020

25 John M. Mchugh and George W. Casey Jr., op.cit., pp.4-5.

流氓國家或是非國家行為者取得大規模毀滅性武器，並要能夠深度的進行國土防衛；傳統性挑戰(Traditional Challenges)，主要是因應堪與匹敵對手可能之敵對作為；及破壞性挑戰（Disruptive Challenges)，主要是形塑處於戰略十字路口之治理不良或脆弱國家，可以進行正確之發展選擇。

此等相互重疊之四大挑戰，不會立即的全部發生，但會是持續變化過程的一部分，且均具有短期與長期意涵，因此，軍方必須以其文件夾式能力(Portfolio of Capabilities)來因應，且要有立即性的措施來處理此等風險，同時也要發展其他的措施來增加未來選項的範圍。同時聚焦於此四個領域，亦可以協助評估國防戰略與檢討武力規劃結構，並找出聯合部隊（Joint Force）所需要的能力。[26]

（四）國家安全挑戰下之衝突模式

1.持久性的非常規衝突（Persistent，Irregular Conflict）

例如阿富汗與伊拉克之戰事，及全球性的對付回教恐佈主義團體之戰鬥。此外，非洲、中東、中亞、南亞與拉美的部分國家，也可能不穩定且甚至走向國家失敗。而因應此等衝突之軍事行動計有「穩定軍事行動」(Stability Operations)，「外國的內部防衛」(Foreign Internal Defense)，內部防衛與發展，穩定、安全、過渡與重建行動，「反暴動」、或「非常規戰爭」(Irregular Warfare)。[27]

26 Christopher Bolkcom, Statement Before the Senate Armed Services Committee, April 30, 2009. (http://armed-services.senate.gov/statemnt/2009/ April/Bolkcom%2004-30-09.pdf),accessed on March 20 , 2012. Department of Defense, Quadrennial Defense Review Report, Feb. 26, 2006, pp.19-20. (http://www.globalsecurity.org/military/library/policy/dod/qdr-2006-report. pdf) ,accessed on March 20, 2020.

27「非常規戰爭」定義為：國家與非國家行為者之間，向相關人民爭取合法性與影響力之暴力鬥

同時,部隊也必須能夠防阻國家之對手可能的再次挑戰,並欲主導更傳統(Traditional)或正規(Conventional)形式之戰爭。簡言之,必須有兩種部隊之匯合,一是能夠執行正規軍事行動;另一是能夠執行非常規戰爭之能力,例如直接針對「蓋達組織」與其分支,及「真主黨」(Hezbollah)之打擊作為;又如在阿富汗之戰事,是混合了直接的軍事行動與安全部隊協助之模式,目標是要能夠摧毀,解構與擊潰「蓋達組藏」,並避免阿富汗再一次成為彼等之安全天堂。[28]

2.傳統侵略式之衝突模式

迄今仍有可能發生侵略式之戰爭,例如敵人雖是在一個區域之侵略行動,但卻是經由一個整合所有層面之武力運動,包括了陸上、海上、空中、太空與網路。 因此,防範之戰略目標是在有限的時間內,使用常備部隊(Standing Forces)保護小範圍領土與人民之安全,及促進穩定政府的過渡;且必要時,也要以機動部隊(Mobilized Forces)來延長時間。且既使承諾在一個地區之大範圍軍事行動,也要有能力在第二個地區,挫敗機會主義侵略者之目標,或施以無法承受之代價。

3.反進入(Anti-Access)/區域拒止(Area Denial)之衝突挑戰

敵人可能會使用不對稱能力,包括電子與網路戰,彈道與巡弋飛彈,先進之空防、佈雷與其他方法,使採取軍事行動之計算更加的複雜

爭。 雖然可能運用全範圍的軍事與其他能力,但採取的是一種間接與非對稱性的途徑,以侵蝕對手的權力,影響力與意志。

28 Andrew F. Krepinevich, The Future of US Ground Forces, Testimony Before Senate Armed Services Committee, March 26, 2009, pp.2-4.
(Http: // armed- services.senate.gov/statemnt/2009/March/Krepinevich /2003-26-09.pdf), accessed on March 20, 2020

與提高難度。例如從美國的角度言，會認為中國與伊朗將會持續尋求非對稱手段，以對付美國的武力投射能力；同時複雜武器與科技也會擴展到非國家行為者手中。因此，美國目前因應反進入與區域拒止環境之考量，係履行聯合軍事行動進入概念、維持水面下能力、發展新的隱形戰機、改善飛彈防衛，及持續強化關鍵太空基地之復原與效率之能力。而能投射武力：對於進入與自由行動受到挑戰之地區能夠投射武力。

第二節 混合戰及政治戰之比較

烏克蘭與俄羅斯的衝突，挑戰了傳統的西方戰爭觀念。從克里米亞之危機顯示，在某種意義上，兩國的衝突像是一場內戰（civil war），也像是一場代理戰爭（proxy war）。目前有學者試圖將這兩個國家的衝突（conflict）分成非常規（Irregular）和傳統的（conventional）的兩個框架。亦有觀察者指出，這場危機就是「影子戰爭」（shadow war）的一個例子。因此，戰爭正超越我們目前的觀念，這些衝突演變的特徵提出了一個智力上的挑戰，而使安全分析者感到困惑亦使學者必須詳加思索。

也有學者簡單化與方便化的將此系列的行動，就稱之爲「政治戰」（political warfare），且以往被封爲西方兵聖的克勞塞維茨在和平時期理論的邏輯應用，就是「政治戰」。使用這個名詞來描述我們歸於「戰爭」（war）知識架構之外的含糊（ambiguous）和模糊的衝突（nebulous conflicts），且此過程之中，涉及了必須贏得民心，且要整合秘密行動（covert actions）以針對重要的外國機構；或是涉及

了減少暴力作爲和最大化國家影響力的手段等之思考與實踐。

在最廣義的定義中,政治戰是在一個國家的指揮下,爲了實現其國家目標而採取的一切手段。這些運作(operations)都是公開(overt)和隱匿的(covert)。他們的範圍從政治聯盟、經濟制裁措施和「白色宣傳」[29]等之秘密操作(covert operations)或隱蔽支持「友好」的(friendly)外國因素,例如運用「黑色心理戰」[30](black psychological warfare),鼓勵敵對國家的地下抵抗運動(underground resistance)。[31]

但是若戰爭的自身目的本來就是政治性的,則與政治戰爭的內涵有什麼不同呢?其次,對於軍事學者而言,「戰爭」(warfare)這個詞是描述解決戰爭的實體行爲(physical conduct)或是戰爭的暴力(fighting)和戰鬥(violent)方面。但是沒有暴力或致命武力的「政治活動」(political activity),藉以創造與運用有利狀況之藝術,在爭取國家目標的同時,能獲得最大成功概率之計算與追求利益最大化。就二者的目標與手段關係來說,政治戰應為其手段,因此,了解政治戰的定義後,會發現其層次上的差異。政治作戰雖然可利用社會內部的緊張關係或操弄群眾的不滿情緒,但這種影響力不僅需要仰賴目標本身的弱點,且還要考量發動者的自身實力。總之,政治作

29 「白色宣傳」是心理戰的一種技巧,它是指通過公開並且正確的來源來發布信息的方式,它通常是單邊觀點的闡述。

30 「黑色心理戰」是指將訊息來源偽裝成敵方發布的方式,只在擾亂目標國內部力量,達到分化團結的效果。

31 George F. Kennan, The Inauguration of Organized Political Warfare (Washington, DC: Central Intelligence Agency, 1948).

戰在某些經濟和社會條件下可以很有效，但也不是簡單的工作，更不是萬靈丹；是需要慢慢地及有條不紊地整合多方面的手段作為。

成功的政治作戰必須有環境的條件配合，如政局不穩、經濟崩跌、民心浮動及內部勢力爭鬥不斷等都是其成功的要件。當今政治作戰的特點如以下十點：

(一)非國家行為者可以進行前所未有的政治作戰。現代化技術和全球化的出現已大幅降低非國家行為者運用此種作戰手段的門檻。

(二)政治作戰涉及所有的國力要素（外交、資訊、軍事與經濟)。

(三)政治作戰的執行必須大幅依賴代理人和手段。代理人包括民兵組織、武裝團體、友好的政黨、非政府組織、企業公司及忠誠的民族團體。

(四)資訊領域是日益重要戰場，成功的覺知能力具決定性的影響。當今社群媒體的便利性讓政治作戰有更大操作空間，同時也更不易揭露幕後的操縱者。

(五)資訊戰的運作方式多樣化，包括誇大、混淆和勸說，以及時提供令人信服的證據是消除假消息的最佳方法。

(六)偵察早期的政治作戰需要大量地投入情報資源。要知道何種政治訊息能夠引發國內外民眾的共鳴，是一項極大的挑戰工作。

(七)政治作戰會導致意想不到的後果。如美國支持阿富汗聖戰士導致後來塔利班政權的崛起。

(八)經濟槓桿手段愈來愈成為強國的首選工具。經濟手段包括制裁與援助，兩者需要投入大量的資源但不能保證一定成功。

(九)政治作戰往往會利用相同的種族或宗教關係或其他內部關係的裂縫。

(十)政治作戰的延伸不是取代傳統衝突，而是以更低的成本來獲致戰果。[32]

這些因素或許很容易與正規作戰聯結在一起，然其任務重點主要是聚焦那些較不顯著，且模棱兩可的衝突事件。這些事件的發展可以讓決策者毫無察覺，當對手充分運用政治作戰手段時，可以透過慢慢散播衝突、削弱反對勢力、製造政局不穩及破壞團結，並在條件成熟時獲致更大的戰果。就如同俄羅斯在沒有訴諸戰爭手段的情況下快速併吞克里米亞的做法一樣，值得我國政府當局參考借鏡。

「混合性威脅」一詞，是針對「對手」採用複雜（complex）和暴力(violent)結合的威脅與行動的描述，這是由美國海軍陸戰隊建構發展的，並見於2006年及2010 年《四年期國防檢討報告》之中。 這個

32 青年日報，〈寰宇韜略-新戰爭形態 政治作戰運用與對抗〉，民國 109 年 4 月 24 日。

概念源於歷史的分析和參考了外國文學中關於有意混合和模糊「戰爭模式」(modes of warfare)之思考，因此，使用這個術語來描述衝突的複雜（complex）和不斷變化（evolving）的特質。[33]

且在過去十年中所學到的最昂貴的課程之一：就是要如何應對「混合性戰爭」(hybrid warfare)的挑戰。軍隊在「正規軍事」(regular military)和「非正規準軍事 」(iegular military)或潛在之涉及恐怖主義、犯罪行爲之平民對手(civilian adversarics)的環境中，不得不介入且將會運作的越來越普遍。

而前述之「混合性威脅」定義已充分說明了俄羅斯人及其車臣僱傭軍和奧塞梯民兵於2008年在格魯古亞的行動，且懷疑與俄羅斯在烏克蘭的「戰鬥」操作吻合，又如在敘利亞戰場上，美軍和他們的當地夥伴面對了來自阿薩德(Bashar Al Assad)部隊及來自俄羅斯軍事人員或承包商組成的瓦格納(Wagner)僱傭軍公司發動攻擊。有俄羅斯介入的證據之一，就是在2018年2月8日，曾在烏克蘭克里米亞地區戰鬥的俄羅斯老兵基爾金(Igor Girkin，亦名Igor Strelkov)通過模擬臉書之在線俄語社交網路Vkontakte表示，美國的反擊已經摧毀了兩個瓦格納「戰術單位」。且與其他有爭議的私營軍事公司，例如「黑水」(Blackwater)和DynCorp不同，在保安領域中普通認爲瓦格納就是俄羅斯政府的掩護，或者雖然獨立運作但仍然是處於俄羅斯政府的直接

33 Frank G Hoffman, On Not-So-New Warfare: Political Warfare vs Hybrid Threats, July 28, 2014. <https://warontherocks.com/2014/07/on-not-so-new-warfare-political- warfare -vs-hybrid-threats/>, accessed on Sept. 12, 2020

監督之下。[34]

因此，北約秘書長拉斯穆森（Anders Fogh Rasmusscn ）就曾經指責俄方所進行的就是「混合性戰爭」。雖然到目前爲止，鳥克蘭情勢複雜發展的犯罪方面並不是很具體明顯，但是伊爾-76軍用運輸機被擊落似已造成被指控的類似恐怖主義情節的傷害：亦有指稱俄羅斯的新形式戰爭 ，就是「蒙面戰爭」(maskcd warfare)，是其「聯邦安全局」（KGB）或「總參謀部情報局」(GRU)在背後運作與支撐所表現之傳統情報技巧的一部分。

同樣的，北約也指控伊朗和「真主黨」(Hezbollah)所造成的威脅，亦是朝向如此的方向演進，不但融入更多的暴力和致命性的國家傳統能力(conventional capabilities)，也融合了恐怖分子或「非常規衝突」（iregular conflict）的有關戰術。[35]

第三節 混合戰實際運用案例

(一)美國面對之混合威脅攻擊與回應

根據美國國防部和學術文件的分析，混合性戰爭（hybrid warfare）在整個衝突範圍內，混雜了常規(conventional)和非正規戰爭(iregular warfare)的途徑。而在美軍《非正規戰爭聯合作戰概念》(Irregular War-fare Joint Operating Concept)中，將常規戰

34 Joseph Trevithick, Russian Mercenaries Take The Lead In Attacks On US And Allied Forces In Syria, The Drive, February 15, 2018. <http://www.thedrive.com/the-war-zone/18533/russian-mercenaries-take-a-lead-in-attacks-on-us-and-allied-forces-in-syria>, accessed on February 15, 2020

35 Frank G. Hoffman, On Not-So-New Warfare: Political Warfare vs Hybrid Threats, July 28, 2020

爭(conventional warfare)定義爲各國之間的戰爭形式,這種作戰採用直接的軍事對抗以打敗對手的武裝力量,摧毀對手的作戰能力,或奪取或保留領土以迫使對手政府或政策的改變。

常規戰爭也可能被稱爲傳統戰爭(traditional warfare),但在《聯合出版物1-02》(Joint Publication 1-02)中卻沒有定義常規戰爭。將非常規戰爭定義爲國家和非國家行爲者之間對相關人群的合法性和影響力的暴力鬥爭。非常規戰爭有利於間接和不對稱途徑,儘管它可能會使用全方位的軍事和其他能力,以侵蝕對手的力量,影響力和意志。

美國在2014年6月之《四年期國土安全戰略檢討》報告中,就基於之前已經提出的各項國土安全戰略報告的基礎上,警告混合性威脅之發展趨勢及必須及早因應的論述。[36]此外,負責國內安全與反情報之聯邦調查局亦指出美國早已經處於混合性威脅之網路安全環境,亦即混合了傳統的國家安全威脅與含電腦駭客和掠奪者等在內之各式非國家行爲者不同形、態威脅的混合。

(二)美國面對之混合威脅

2018年2月27日,聯邦調查局犯罪網路,回應和服務執行助理局長保羅阿巴特(Paul Abbate)在AFCEA網路安全高峰會(Cyber Security Summit)上指出,今天面臨的大多數威脅與我們一直看到的大部分威脅相同,仍然可以分爲三個部分:亦即恐怖主義,外國情報和傳統的犯罪威脅。但是現在網路已被用來作爲從不同角度犯下這些罪行的工具,且

36 汪毓瑋,國土安全,上冊,第二版(台北北:元照出版公司,2015年10月),第五章

幾乎是匿名的,也加強了民族國家行爲者正在做的犯罪事情。更讓人難以預測、發現、難以歸因到底是誰在做這件事。

在與恐怖主義的鬥爭中,像「伊斯蘭國」(IS)等恐佈組織正在利用網際網路和網路手段,在全球範圍內激化和招募暴力傾向的個人,從而導致全球危機。來自外國對手的俄羅斯、伊朗、北韓和中國等之外國反情報威脅,包括經濟間諜,竊取國家機密,外國影響力介入選舉等。而網路只是在我們爲保護這個國家所做工作增加挑戰的動態性。且在過去幾年中,即使有傳統的犯罪威脅,企業電子郵件危害和勒索軟件犯罪也大幅增長,阿巴特強調這些均是面臨的更常見威脅,也造成最大的經濟損失:就是一種混雜(blended)或混合威脅(hybrid threat),亦即傳統的犯罪組織和駭客聚集在一起,民族國家和非民族國家的行爲者作爲一個團隊而進行攻擊。

這種「混合」的涉及網路安全例子,例如 2015年,一位名叫費力吉(Ardit Ferizi)的被告,被控通過駭入和竊取美國軍方和聯邦人員的資訊來支持「伊斯蘭國」,通過私營部門公司的報告,聯邦調查局能夠偵查這個重大違規事件,其中包括利用個人身份資訊(personally identifiable information,PII)。聯邦調查局追查到在馬來西亞的費力吉,經由分析將其與一名「伊斯蘭國」在敘利亞領導人的關係聯繫起來,在有了更進一步的情報後,聯邦調查局了解到「伊斯蘭國」利用費力吉竊取個人身份資訊並將該資訊轉交給「伊斯蘭國」。該組織使用社交媒體公佈了這一份「殺人名單」,就是爲激進人士彙編的攻擊目標清

冊。這些與外國恐怖組織結合在一起，就是利用普通駭客進行全球範圍的暴力和恐怖襲擊行動，聯邦調查局通過與國防部、私營部門夥伴以及馬來西亞當局等國際夥件的合作，在該組織針對名單進行任何傷害之前確定了此威脅且預爲防範。[37]

此外，在雅虎網路（Yahoo's network）的違規行爲，也是2014年開始的混合型攻擊（hybrid-type attack），俄羅斯「聯邦安全局」（Federal Security Service）官員與犯罪駿客合作，鎖定雅虎作爲目標並竊取了5億多戶之帳戶資訊，這些駭客爲了自己的犯罪目的將這些資訊提供給俄羅斯府處理資訊的人員，而能夠將其用於外國情報之用途，以影響行動，最終四名被告因爲電腦駭客入侵、經濟間諜罪和其他刑事犯罪被起訴，包括了兩名「聯邦安全局」官員。

2018年3月15日，美國國土安全部指責俄羅斯遠程瞄準美國電網（power grid），作爲美國對俄羅斯製裁措施回應攻擊的一部分，此等涉及不同人員與管道之混合攻擊情事以往也會發生過，例如2015年，島克蘭的電網也遭受了前所未有的據稱是俄羅斯政府造成的網路攻擊而導致大面積停電。

俄羅斯政府是先將惡意軟體植入安全性較低的小型商業第三方網路。然後再間接進入了美國政府的網路，且自2016年3月以來，俄羅斯就不斷試圖攻擊包括能源，核能，商業設施，水資源，航空和關鍵製造業部門。「賽門鐵克安全回應中心」（Symantec Security Respose）的技術總庫爾（Vikram Thakur）表示，想要進入與美國關鍵基礎設施

[37]汪毓瑋，2018年。《情報、反情報與變革》，頁43-47，臺北市：元照出版。

各方面相關網路非常困難,國土安全部所描述的網路攻擊有可能造成重大損失,而這種攻擊者與僅僅是在尋找資訊的攻擊者完全不同,其攻擊背後的唯一因就是政治動機。這次襲擊也引發了美國政府對於關鍵基礎設施有關系統漏洞的擔憂。[38]

(三)美國面臨混合威脅之回應

爲了應對此等不斷變化的感脅發展趨勢,聯邦調查局已努力改進一些領域,一個是網路人才招聘,讓學生儘早參與並開展在線網路培訓,以補充與提升該局已有的人才能量;另一個領域就是擴大資訊分享。聯邦調查局已經不斷的與其他機構和組織合作偵查(detect),預測(predict)和打擊網路威脅,其中的主要合作平台就是「全國網路調查聯合專案組」(National Cyber Investigative Joint Task Force),這是一個負責協調和分享網路威脅調查資訊之多機構的網路合作中心,涉及了20多個來自執法部門、情報部門、國防部以及州和當地合作夥件的機構。且爲了促進更多的資訊能夠有機會分享給夥伴,該局亦鼓勵私營部門與當地的聯邦調查局駐地辦事處建立關係以有效的分享情報,爲了更佳的定位國家應對所有網路威脅必須雙向的進行資訊共享,面臨危機時才能共同合作解決。[39]

2018年2月27日,在國土安全部與其他情報部門不斷的提出警告

38 Russia accused of cyber attacks on US power grid, CNN, Mar 16, 2018. <https://edition.cnn.com/2018/03/15/politics/dhs-fbi-russia-power-grid/index.html> , accessed on Mar 16, 2020

39 Amanda Ziadeh, FBI is Fighting Hybrid Cyber attacks: Terrorism, foreign intelligence threats and traditional crimes are coordinated with hackers, Government Cio Media, March 31, 2018. <https://www.governmentciomedia.com/ fbi-fighting-hybrid-cyberattacks>, accessed on April 11, 2020

之後,國務院和國防部門發起了一項耗資4,000萬美元的舉措以打擊俄羅斯的錯誤資訊運動(disinformation campaigns)。首筆100萬美元的種子資金(seed money)將匯集到國務院於2016年建立用以打擊恐怖主義網路推動伊斯蘭主義宣傳之「全球交往中心」(Global Engagement Center,GEC),以激勵公司和非營利組織在2018年年中的時候提出有效的解決方案。在「資訊進入基金」(Information Access Fund)之下,市民社會團體、媒體內容提供者、非政府組織、聯邦資助的研發中心、私人公司和學術機構均有資格從「全球交往中心」爭取經費,以推動對付宣傳與假訊息的重要工作。負責公共外交和公共事務的副國務卿史蒂夫,德斯坦(Steve Goldstein)也強調,美國不僅應該採取防禦姿態,也需要發起攻勢。[40]

能源部長里克佩里(Rick Perry)也回應了國土安全部對於混合威脅的關切,指出能源部與政府夥伴和能源部門資產所有者密切合作,以幫助確保嘗試此等針對有關鍵基礎設施攻擊之失敗或是被阻止,而此事件也說明了能源部爲什麼要創建一個「網路安全和緊急回應辦公室」(Office of Cyber Sccurity and Emergeney Response,CESER)的原因。[41]

第三章、中共對臺混合性威脅之探討

隨著中國在國際上的快速崛起,周邊區域國家幾乎都已經感受

40 State Department Launches $40 Million Initiative to Combat Russian Disinformation, Observer, Feb. 27, 2018. <http://observer.com/2018/02/state -department-launches-40- million-initiative-to-combat-russian-disinformation/>, accessed on Mar 16, 2020

41 Russia accused of cyber attacks on US power grid, CNN, Mar 16, 2018.

到了中國政治經濟的影響力與滲透力，緊鄰中國大陸僅海峽之隔的臺灣當然也不例外。近年來，北京當局正以的「混合性威脅」的方式來滲透我國的政治、經濟與社會，因此也引起臺灣對北京的行動提高警覺性，面對中國無所不用其極的滲透與干預手段，本章節將建立參考指標說明中共混合威脅可能之演化。辯證唯物論的認識論是把「實踐」提到第一的位置[42]，因此問題不只在於懂得客觀世界的規律性來「解釋世界」，而在於拿此規律性的認識去能動的改造世界。因此，認識與探討混合性威脅是從實踐開始的，經過實踐得到了理論的認識，還必須再回到實踐去。因而當認識到西方大國對中國之「戰略遏制和圍堵」態勢不會因為必須加強彼此合作以應對共同關切安全議題而被稍微減損，且三不五時就拿西方標準來檢驗中國的國內、外之各項行事時，就必須善於運用新情況而進行實踐認識上的轉移。

第一節 混合威脅之參考指標

威脅如何快速的因應必須是賦予現實性的具體意涵，且涉及相對應之反制作為，亦即必須有效的被處理及有適當的部門去管理，因此，嘗試從非傳統安全之可用角度思考，其中所關切之非傳統安全威脅包括了多樣化的議題，若要挑選出目前最關切者，同時又不希望涉及到其他既定領域之主題，或者已經是有明確部門列管之事項，也就是若其他領域已有之主題則在該等領域自行解決即可，例如人口販運、洗錢、毒

42辯證唯物主義（dialecticalmaterialism）是一種以馬克思和恩格斯學說來研究現實的哲學方法，是用「辯證的觀點」和「唯物論的觀點」解釋和認識世界的理論。《辯證唯物主義和歷史唯物主義原理》，李秀林主編，中國人民大學出版社，2017 年 10 月 27 日。

品、武器擴散等主題早已在跨國組織犯罪之領域內被有效處理，實不用再冠以非傳統安全之前置詞才會被重視或被處理，致無需畫蛇添足;又若是已有部門且進行常態之處理，亦不需要凸顯非傳統安全之跨領域合作特徵，因為此主題無須跨部門之合作而由單一部門解決 即可。因此，論證台灣面對之混合性威脅之標準有二:

第一、該等主題必須有新的發展，而具有以往所沒有的內涵。

第二、該等主題之複雜演化，已非以住透過既有主管部門的單獨處理即可。

基於前述兩項標準而進行眾多主題之檢視，發現目前必須關注之混合性威脅議題，最主要的至少有以下三項，但也不排除隨著時空的演化選有其他主題有待檢討：

1. 恐怖主義威脅：恐怖主義威脅在「九一一事件」之前，概是單純的國內執法議題，因為之前的恐怖主義組織訴求大概均是一國之內可以滿足，例如「愛爾蘭共和軍」只是要求北愛爾蘭獨立而已，但是目前之恐佈主義組織，特別是「伊斯蘭國」或是「蓋達組織」之訴求則非一國之內可以滿足，因為彼等之終極目標是建立從地中海到東南亞廣大地區之回教律法治國而要推翻目前之回教世俗政權。同時，因為該等組織之經費來源已被限縮，因此以往不可能與組織犯罪團體或是跨國組織犯罪團體合作之現像也改變了，而有與人口販運、毒品走私及武器販賣集團某種不同類型與不同程度之合作，以致於已非任一執法部門或是情報部門可以單獨因應而必須結合應對;甚至

在某些情況下，軍方也應介入。

然而目前我國仍不是非傳統安全威脅之認知，而是以美國推動之國土安全概含範疇來思考因應，且對應之負責機關是「國土安全辦公室」，並以新設計之國安與行政雙軌體系與運作去反制。

2.海事安全威脅：海事安全基本上涉及瞭如何處理自然災難與海上非法行為等兩個範疇，在自然災難方面：相關威脅包括大海嘯、海水倒灌、颱風等；海上非法行為方面；則包括海上之武器走私、毒品走私、人口販運、有毒廢棄物傾倒，非法釣漁等之海上犯罪；及展現出人為攻擊行動的海盜、海上恐佈主義、海盜綁架漁民等不法行事，而近幾年已發生之案例顯示，海盜與走私毒品，武器與人口販運等之組織犯罪團體已有更多的結合，因為兩者「取財」與「低調」之目標 與行事風格一致，然而亦有一些案例顯示，海盜與恐佈分子也可能進行某種程度之結合或有更多可以互動之灰色地帶，例如曾經發生海盜要不到贖金而將人質轉賣給恐怖主義組織之現象。因此，海事安全之維護，已非傳統之單一漁政或是交通部門能夠處理，而更多涉及了執法、情報、外交、漁政及船運企業等之公私部門的合作。而檢視曾經獲釋的我國被綁架漁民，亦論證了此等威脅的變化與多部門介入之必要。

3.網路空間威脅：隨著資訊科技與各項含加密等在內之應用軟

體的快速發展及更方便之取得與使用，已加劇了網路空間的各式樣攻擊事件，而經由已經發生過的案例顯示，從事網路犯罪或是進行網路攻擊的行為者至少可以分成7種類型，亦即駭客、駭入行動主義者、電腦罪犯、企業間諜、內鬼、契約商及恐佈分子，並至少有12種類型以進行攻擊之工具。而展現出不僅作為恐怖主義組織等之非國家行為者之洗錢、訓練、攻擊之平台，或是作為攻擊國家關鍵基礎設施之中介而有「網路恐佈主義」之新型態威脅，或是發動「網路聖戰」；恐佈主義組織亦與網路犯罪進行結合：同時也是國家行為者施展間諜行為的重要場域 。因此，駭客攻擊、網路犯罪、網路戰、資訊戰、電子聖戰等傳統內涵與分類已更模糊，相互滲透及更新。且行政院、國安會、國安局、軍方等雖各有相對應之資訊安全與管理單位但必須合作處理：此外，擁有此等資產之私部門也應配合才可能更有效解決。[43]

第二節 中共影響臺灣手法、工具之探討

儘管21世紀的混合性威脅確實帶來難以防備的新挑戰，大多數方法並非全然新穎。然而，隨著新技術革新，加上虛擬(Virtual)或數位(Digital)空間降低宣傳使用成本，不僅為新工具提供新的途徑，同時擴張戰鬥空間，使混合性威脅能夠將過去傳統與非常規武力相互組合運用，創造出比起過往非常規戰爭更有成效的戰略手段。混合性威脅的攻擊手法相互交織難以區隔，然而手段的演化，大致可分為五

[43]李明總編輯，汪毓瑋著，2018 年。《國際關係》。台北:前程文化事業股份有限公司。

大類別：資訊操作、網路工具、經濟影響力、軍事武力（代理人）、法律規範。

(一)資訊操作

不論是外交或戰爭，最終均旨在試圖影響領導人及其人民的意志，而其他一切行為都是達到這個目的之手段。所謂「資訊操作」(information operations)是對戰略目標資訊武器化，使其能達到在許多國家之間塑造政治話語(political discourse)以及民間敘事(popularnarrative)目的，產生比傳統武力更深層且強大的效果，同時在原有實體空間之外，擴大至虛擬空間。此外，混合性威脅在和平時期，資助相關菁英或團體，藉此發揮「代理人」之主體合法性，因難以被查證與威脅之關聯，而更有彈性的傳達其意志，使混合性攻擊者在未來衝突能展現其優勢條件。

(二)網路工具

此為最新也是最難概念化的混合性威脅手段，未來戰爭都會伴隨著針對指揮管理系統的網絡攻擊。[44]網路作戰風險低、成本少，卻能產生很好的效果。因為在虛擬空間中，難以追查操控者身分來源，以致混合性攻擊者藉此特點發揮進攻優勢。例如，2017年，維基解密(WikiLeaks)代號為「Vault 7」的文本中揭露，美國中央情報局(CIA)擁有龐大的平駭客武器庫，包括惡意軟體、病毒、木馬程式

44 C4ISR是一個軍事指揮作業系統的概念，它以資訊與通訊技術為核心，將作戰中所涉及的指揮、管制、通訊、電腦、情報、監視及偵察，以自動化的方式加以整合。

等，可用於攻擊手機、電話和其他數位備。[45]

（三）經濟影響力

自經濟全球化後，國際間形成統一的市場，彼此間相互依賴、相互共存。如對目標對象施加經濟壓力，影響其社會、軍事、外交等決策，可達成戰略利益。然而，與過往不同的是，除了透過援助、制裁以及借貸等傳統經濟影響力方式之外，混合性攻擊者透過結合不同領域，達成其經濟影響力。例如能源、影視和旅遊等其他行業，且為降低國與國之間直接性衝突所產生的成本，會更傾向於人民自行發出的抵制活動，採取「非官方」的制裁，以模糊空間，閃避對手有機會進行正面反擊。

(四)軍事武力（代理人）

隨著傳統戰爭頻率降低，混合性威脅多利用「代理人」(proxies)，以「未經承認」(unacknowledged)戰爭模式，避免國際法律的規範。委託者藉由非國家行為者易遊走於國際規範之特性，且不公開承認代理人身分，順利的閃避國際間究責。[46]例如俄羅斯的「小綠人」或「分離主義者」，以及具有「小藍人」之稱的中共「人民武裝海上民兵」。[47]

---

[45] WikiLeaks, “Vault 7,” WikiLeaks, 2017, <https://buzzorange.com/techorange/2019/01/11/pdf-translation/>

[46] Frank J. Cilluffo and Joseph R. Clark,“Thinking About Strategic Hybrid Threats-in Theory and in Practice, " *Prism*,Vol. 4, No. 1, 2012, p. 49.

[47] Simon Tisdall,“Little Blue Men: The Maritime Militias Pushing China's Claims, " *The Guardian*, 2016/5/16, <https://www.theguardian.com/world/2016/may/16/little-blue-men-the-maritime-militias-pushing-chinas-claims-in-southchina-sea>

(五)法律規範

從制度層面來看,《聯合國憲章》明確指出,和平是國際事務的正常狀況,戰爭是例外。各國有義務以和平方式解決爭端,只有在發生「武力攻擊」(armed attack)時才允許使用武力進行自衛。[48] 儘管現今威脅環境不斷在改變,越來越多國家行為者或非國家行為者利用各式各樣的手段來爭奪權力,戰爭與和平早已模糊不清。然而「國際法律」規定跟不上變化萬千的威脅環境,使得混合性攻擊者更能「善用」國際法對於交戰規則約束力,以操弄「合法性」的定義,例如,俄羅斯併吞克里米亞、中共之南海人工島礁擴建。

第三節 中共混合威脅可能之演化

混合威脅通常運作於低於戰爭界限之灰色地帶,是發生在整個衝突頻譜中的每一個「區間」,而不是頻譜上獨立的衝突類型。可以被定義為:「模糊性」的國家或是非國家行為者,不受以往遠近「地理」或主權「疆界」概念的限制,而「同時」在不同的戰場與市民社會之含實體與虛擬的多樣化「空間」中,混合採用了「單方面」或是結合「可調適」和「系統性」之「量身定製」的傳統武器、非常規戰術、恐怖主義和犯罪行為等之既「不易歸類屬性」、又能夠悠遊於合法與非法之「灰色地帶」的隱而不顯作為,以追求具有更大算計之政

[48] Aurel Sari, *Blurred Lines: Hybrid Threats and the Politics of International Law* (Helsinki: Hybrid CoE, 2018), p. 3.

治目標。[49]

《自由之家》2019 年時發布的一個新報告〈北京的全球揚聲器〉[50]描述了中共媒體影響的一系列策略，並提出了證據呈現其日益增加的影響力，以及這些影響所引發的來自各國政府、獨立媒體、科技公司或是公民社會的反制行為。該報告追蹤了中共自 2017 年以來的策略及其效應的演化過程，以下為三個在 2019 年最為顯著的趨勢：

第一、動員對他國的國營媒體以打擊中共的敵人

長久以來，中國的主要國營媒體在國際上一直具有一定的聲量。但是最近，其中的大多數媒體在中國國內被封鎖的國際社群媒體平台上愈漸活躍，並且吸納了數以百萬計的粉絲。面向外國觀眾的內容主要為中國和其政權做正面宣傳，並著重報導中國的經濟和科技實力，同時洗白中共的對於人權的侵犯。然而在 2019 年，隨著香港的民主抗議和新疆維吾爾人在集中營被羈押受到國際的關注，針對中共鎖定的敵人、越來越具有攻擊性和負面的內容，開始被散布在關於一般日常的內容當中。

例如，2018 年中國環球電視網（CGTN）的英文臉書頁中共國家電視台的海外國際分支針對其逾七千萬的粉絲發布了幾則影片，或把香

49汪毓瑋，清流月刊， 2020 年 1 月《灰色地帶與混合威脅虛與實》。
50《自由之家：中國共產黨影響國際媒體的行動正在迅速擴張！》，風傳媒，
https://www.storm.mg/article/2238504 (2020/01/31)

港抗議者比作恐怖份子，或重複傳播已被證明是捏造的內容。[51]去年十二月，中國環球電視網英文、西班牙文和法語版的臉書頁面張貼了一系列令人不安的「紀錄片」，內容為所謂新疆維吾爾人帶來的恐怖主義威脅。在數小時內，其中一則影片便吸引了 2 萬 5 千多次的瀏覽量，對中國環球電視網的內容來說這是相對高的流量。[52]

第二、在全球社群媒體平台上展開傳播假消息的行動

在全球社群媒體平台上展開傳播假消息的行動：過去一年來，以有組織的網路帳號假扮作是普通用戶張貼信息的俄羅斯式假消息宣傳，成為在中共海外傳播中共敘事的新手段，儘管這一現象早在 2017 年中期就已開始。先前，根據牛津大學互聯網研究所（Oxford Internet Institute）的調查，大多數的證據顯示這類隱密政治宣傳只出現在中國國內的平台上。然而在 2019 年，該機構報導，中國政府展現了「積極使用臉書、推特和 YouTube 的興趣」。這三家公司都宣布大量刪除其認定被動員於中共假消息行動的帳號。[53]

51《2019 年主要趨勢 - 全球媒體影響、意識形態推行》，中國媒體快報 https://freedomhouse.org/zhhant/report/zhongguomeitikuaibao/zhongguomeitikuaibao2019nianzhuyaoqushi。

52 《時評:中共為何反維權》，PChome 網路新聞平台，2019 年 2 月 23 日，http://mypaper.pchome.com.tw/souj/post/1320313893。

53《New report reveals growing threat of organised social media manipulation》，Oxford Internet Institute，2019 年 12 月 8 日，https://www.oii.ox.ac.uk/news/releases/new-report-reveals-growing-threat-of-organised-social-media-manipulation-world-wide/。

針對這些被移除帳號的詳細資料分析顯示，中共他們學習的速度很快。在台灣，其針對中文社群媒體的操作比其在全球範疇下的行動更加成熟，關注的專家們注意到假消息變得更難以查明。[54]還有，雖然推特採取各種措施來移除與中國相關的帳號網絡，與中國政權有關聯的網軍顯然在該平台仍相當活躍。這一點，從休士頓火箭隊總經理莫雷（Daryl Morey）在10月份發推文支持香港抗議後，所引發的威嚇式宣傳攻勢可見一斑。親北京的網軍也被懷疑正以行動操縱中國以外的主流資訊平台的內容排名，包括在Google搜索引擎、Reddit和YouTube上的內容排名。

第三、中國媒體平台上的政治審查擴展至海外

隨著中國的社群媒體公司及其主打的應用程式在全球逐漸大受歡迎，它們也為中共創造了新的管道以影響海外的新聞傳播。其中一個引人注目的例子是便是微信。微信是一款結合即時通訊、群聊、商業服務和電子支付於一體的應用程式。該應用程式為騰訊所擁有，並稱在中國國內有十億活躍用戶。根據估計，微信在海外，特別是亞洲地區，擁有約一到兩億的用戶。在微信的全球用戶中，數百萬人是身在如加拿大、澳洲和美國的海外中國僑民。在這些民主國家中，微信越來越頻繁地被政治人物用來和他們的中國裔選民溝通。

[54] 《人人都是傳播者，深陷盲人摸象囧境》，立報傳媒，2018年10月6日，http://www.limedia.tw/comm/5557/。

隨著中國國內的網路審查日益箝緊，報導聲稱微信員工正在刪除外國用戶張貼的政治敏感信息[55]，甚至關閉他們的帳戶。2019 年 4 月，研究人員發現證據指出微信有系統地監控海外用戶的通話，並標示政治敏感的內容作為某種形式的監視，即便他們並未阻擋此類訊息的傳輸。另外，中國公司字節跳動（ByteDance）旗下的應用程式抖音在 2019 年成為全球被下載次數最多的應用程式之一，特別是在美國的青少年用戶中大受歡迎。如微信一樣，有報導說抖音已在審查被中國政府認定敏感的內容，或是更大範圍地將政治性內容降低關注度。[56]

第四章、臺灣應對中共混合性威脅之策略

目前臺灣面臨的威脅是陰險的、不容易定義或鑑定的。它在國家之間的縫隙以及治理不良或薄弱的軟弱環境中蓬勃發展。新的威脅包括不同、有爭議的元素而構成了「混合性威脅」，此威脅遠遠超過現有安全挑戰的合併，其原因是由於在充滿活力的國際安全環境中，這些構成要素之間的不易切割且相互關聯性，打擊他們所需活動的複雜和相互依賴的性質，涉及了具有既得利益的利害相關者之多樣性，以及要關注傳統軍事解決方案可能不是最好的，但仍然有必要的。

混合性威脅定義之所以因難，在於它聚焦於與「 暴力」和「戰

[55]《微信上的中國：每年「被消失」的一萬篇文章都在說些什麼？》，關鍵評論網，2019/06/25，https://www.thenewslens.com/article/121165。
[56] 同註 48。

爭」之戰術結合，亦可能涉及了一些犯罪行爲的組合，但無法掌握其他非暴力行動（non-violent actions）。因此它也可能涉及了包括經濟和金融行在內的手段、顛覆性的政治行爲，例如創造或隱藏的利用貿易聯盟（trade unions）和非政府組織作爲戰線，或使用虛假網站（false websites）和植入報章資訊；也可能涉及了包括外交和金融和資訊工具等在內之所謂「超限戰」等之更大的戰爭概念的某些部分。[57]

第一節 政府在實體與網路空間之作為

儘管革新的技術帶來人類生活的便利性，卻也加速非國家行為者操控非常規戰爭的能力。現代技術的軍民兩用技術不僅限於實體的攻擊能力，也通用於虛擬的通訊和情報工作。

由於網際網路和廣泛使用的加密技術(Encryption Tcchnology)，任何擁有幾千美元的團隊都可以以創建一個安全的全球通訊系統，可以從世界各地的任何網咖或公共圖書館連結。同樣，商業化技術已經允許非國家行為者收集與傳播有關目標及其敵人之情報，例如伊拉克反叛分子利用Google地圖協助，並以簡易爆炸裝置策劃伏擊和襲擊。[58]

雖然突破性的科技成果利於人類的生活，卻也使戰場更顯得無所不在，例如AlphaGo的技術可能被駭客用來蒐集資料或查找程式漏洞，臉孔識別技術的用途就更加危險，這過人工智慧的編碼就可以配置無人機、無人駕駛汽車或者清潔機器人上使之成為暗殺武器。[59]因此，《超

[57] Frank Hoffman, On Not-So-New Warfare: Political Warfare vs Hybrid Threats-July 28, 2014
[58] 張錫模，《全球反恐戰爭》（臺北：東觀出版社，2006），頁56-64。
[59] Miles Brundage, et al., The Malicious Use of Artificial Intelligence : Forecasting, Prevention, and

限戰》一書形容，「相信人們會在某一個早上醒來時吃驚地發現，許多溫良和平的事物都開始具有了攻擊性和殺傷性」。[60]

除了實體空間受到的威脅，虛擬空間的操控，目標對象不只針對傳統的軍事和關鍵基礎設施，更重要的是發展成具有戰略意涵的惡意網路效應。隨著網際網路快速傳播資訊，雖使所有人均能享有平等的發言權，部落客（Blogger）和善於使用社群媒體者更能在其中獲得商機，然而卻也賦予具有意識形態或犯罪目的之個體得以散播思想的能力。因此，臺灣政府可以朝幾個可能之方向努力：

（一）重視安全教育，鞏固全民心防：古典戰略「心戰論」講求在先聲奪人前須先「不奪於人」，面對中共網路活動鋪天蓋地的威嚇宣傳，及渲染、分化所冀獲得的震撼效應，應從教育大眾建立正確認知開始，建立對國家安全體系、社會生活價值的信心，進而排除混合威脅所欲產生的負面影響。

（二）建立相應機構、完善網路管理：因應混合威脅造成的心理層面影響，台灣政府應成立足以執行維護資訊安全、評估輿情狀態的專業機構，既可保護網路、資料庫及各項關鍵基礎設施免於遭受攻擊，亦應針對威脅來源、複雜資訊，及有心人士刻意釋放的恫嚇資訊等進行調查、分析、駁斥與反制。

Mitigation (San Francisco: Electronic Frontier Foundation, 2018)

[60] 喬良和王湘德，《超限戰》（北京：解放軍文藝出版社，1999 年），頁 13。

（三）加強國際合作，建構聯防體系：網路無遠弗屆，面對中共混合威脅，國際社會須相互合作、交流相關資訊與經驗，才能在訊息追查、安全預警、事實查核等方面事半功倍。例如: 由美國國務院贊助、美國在台協會（AIT）及美國國務院全球參與中心（GEC）共同主辦的「美台科技挑戰賽」，該中心負責帶領美國政府對抗惡意外國政治宣傳和不實資訊，於2017年成立，並促成聯邦政府間的訊息分享與科技應用，這場資訊戰役，民間企業早已採用規避審查工具、網路識讀工具、區塊鏈驗證、暗網監控、社群聆聽、數據分析或線上廣告投放等方式遏止假訊息。透過GCTF媒體識讀工作坊、TechCamp資訊科技培訓營等方式與印太地區夥伴分享他國抵禦虛假訊息的經驗。也希望透過競賽，找出更多解決方案。[61]

第二節 私部門可以發揮的作用

失敗或失敗國家之成功穩定的唯一最重要的因素，就是經濟發展。反過來，這取決於對投資者的經濟激勵，基礎設施（數位和物理）的改善，獲得能源和熟練的勞動力等。雖然經濟發展在大多數情況下顯然是至關重要的，但是我們應該牢記，西方對發展的物質主義（materialistic）定義可能並不是被其他民族或地區所普遍接受而願意探納的共同標準，或是用來測量福利或幸福之共同必要指標。[62]

值得注意的是，宗教和遵守宗教習俗之籲求與必要性正在上升，

61〈力抗中共資訊戰，美國務院/AIT舉辦「美台科技挑戰賽」〉，《大紀元日報》，民國109年2月12日，https://www.epochtimes.com/b5/20/2/19/n11879322.htm(瀏覽日期:2020年4月1日)

62 Michael Miklaucic et al., "NATO Countering the Hybrid Threat," (Washington, DC: National University, 2011), pp. 121-122.

特別是在穆斯林世界,已作爲人類進步最重要的指標。易言之,並非只是通過改善有關人們的物質條件就能夠消除混合威脅的所有根本原因。今天穆斯林世界許多人對西方的不合理常常感到憤怒,因爲它可能或可能不會解決本國政府的無能和腐敗產生的條件且持續下去。因此,要能夠精確地了解混合威脅的根本原因的非物質層面。

事實上,混合性威脅要素對於私營部門,個別公司和行業所造成的傷害更爲密切,例如仿造網路(Counterfeiting networks)竊取了合法公司的知識產權和潛在收入。網路攻擊者可以使資訊和使通訊公司無法運作而導致他們喪失業務。 金融機構也經常受到洗錢和其他非法金融交易的影響而損失慘重。 這些對手攻擊他們的底線,這些私部門就越直接地了解混合性威脅的非法網路和其他離散因素,也就越能對混合性威脅的鑑定,方法和範圍提出更細概的評估。

事實上 ,商業界不斷開發出創新技術來對付具體的威脅和風險,但是並沒有進行廣泛的分享,在這些方面,私營部門的經驗對於公部門來說是非常有有價值的,而且可以從這種專門技術中獲益匪淺。 因此,聘請私營部門之專家參與是值得的,且政府應該鼓勵與工商企業界主動接觸。應該考慮如何外展和應對行業的參與,必須聽取真誠的意見和協商。 例如軍方和其他他行業成員定期在防務,技術進行接觸,提供有關部門活動和目標的見解,可能適用於工業的經驗教訓的「戰爭故事」作爲交換,公部門獲得了前所未有的高層管理和專業知識,甚至不

同於來自私營部門組織的援助。[63]

另外在規劃上，亦能搭配非政府部門（私營企業或非營利組織）增加戰略溝通的能力，其中非營利經織也能在確保「資訊正確」的工作上發揮重要作用。例如由「媒體觀察教育基全會」建立的「台灣事實查核中心」旨在通過提高媒體素養和事實核查主要新聞報導和謠言，為協助台灣社會提供長期的非政府解決方案。或是由台灣工程師組成的 GOV 零時政府發起的「Cofacts 專案」，開發「美玉姨」的 Line 帳號，可用於自動查詢謠言、即時回覆，並將找到的資料加入謠言資料庫，進而幫助更多人釐清真相。[64]

與此同時，也需增強公民的危機意識強化社會韌性，使人民感知有惡意的方式正在影響生活，並培養良好的媒體素養時刻察覺虛假訊息的存在也鼓勵新聞界高品質的媒體共同挺身面對惡意的挑戰。政府也呼籲進一步提高公民意識，以及與美國等志同道合的國家在媒體素養方面進行合作。

第三節 應對混合性威脅的戰略作為

混合性威脅不僅僅是其組成部分的總和，打擊這些威脅除了思考新的能力之外，更重要的是要與時俱進的加入新的合作夥伴、新的進程以及最重要的新思維。

63 NATO, NATO Countering the Hybrid Threat.
64 陳冠榮，〈即時釐清已知的謠言，快把美玉姨加入 Line 群組〉，《科技新報》，民國 107 年 12 月 25 日。

應對混合性威脅的全面性途徑，就好像是概念問題的如何更佳的制度。事實是所有的行爲者很少會期待一個單一的總體目標。因此，最好承認同一情況下的不同行爲者有不同的觀點和目的，以尋求確定可以形成合作基礎的共同點。這個戰略應該包括六個主要的努力：

1. 創建一個聚焦於對手國的「情報中心」

例如北約、歐盟在實踐或理念上，都努力建立一個專注於俄羅斯等國家可能威脅的「情報中心」(inteligence hub)，以評估這些具有威脅國家的意圖、能力和活動，因而期盼可以提供必要關注的議程。且參與的成員國之間可以透過有關資訊的蒐集和分享，增加西方集體認識和回應的能力。

2. 加強和擴大應急規劃（contingency planning）

這對於處理例如俄羅斯等對手之「低層次武力」(low-level force)、網路攻擊和資訊戰(information warfare)的前景尤其重要。例如北約已在波羅的海國家和波蘭設立了「多國戰鬥營」(multinational battalions)。要求這些部隊應該與當地警察和其他的國內安全機構一起進行規劃，並在可能的情況下要由「歐洲憲兵部隊」(European Gendarmeric Foree)進行補充，這些部隊包括來自七個歐洲國家的軍警，例如意大利的「卡賓槍騎兵隊」(Carabinieri）和西班牙的「國民警衛隊」(Guardia Civil）等。

同樣的，亦要求應該擴大對於應對網路攻擊的規劃，包括北約、歐盟和政府機構及重大關鍵基礎設施結構，例如電網運營商、電信系

統 、網際網路服務提供商和金融機構等。

3. 使用法律工具以應對外國達反國內法的行為

例如美國起訴了俄羅斯情報部門駭入「民主黨全國委員會」(Democratic National Committce)有關成員之案件。又如在愛沙尼亞國家邊防部隊被俄羅斯部隊綁架的情況下,愛沙尼亞當局也應該向有關部門起訴。

更廣泛而言,當一個國家被一個如俄羅斯等對手之混合性行動最嚴重侵犯時,要求跨大西洋社區也應酌情考慮多國制裁(multinational sanctions)。美國在「民主黨全國委員會」被襲擊之後利用單方面的制裁,但其他國家採行或通過歐盟之多邊制裁,對未來行動的反應和威脅將會更加的強大,也應該是未來的努力方向。

4. 限制對手國家或其支持實體之任何政治融資

作爲後續行動,現有的歐洲國家審查外國投資或其他金融交易機制將會更加的聚焦於作爲對手之實體的政治融資(political finance)行動,因爲這些行動可能會對一國的國家安全、經濟和或民主功能造成不利影響。將有助於破壞該對手的具有影響力的網路脈格,並因而建立更具韌性的社會(resilient societies)

5. 對於對手國介入的選舉干預作出全面性的回應

這可能包括在選舉背景下爲媒體提供資訊的(自願標準守則》(voluntary code of standards),可以在歐盟的《線上打擊非法仇SU)(Code of Conduct on Countering Illegal Hate Speech On-line)基礎上,借鑒有關誹謗、隱私和客親性的國家法律,例如德國和

英國已經實施。根據現行仇恨言論行爲守則，政府與私營網路公司必須合作才能阻止和或限制仇恨言論。且應採取可比較性途徑，以限制對手國旨在影響外國選舉而不符合自願守則標準的資訊工作影響力。

6. 建立「協調委員會」(Coordinating Couneil）來處理這些問題

爲了促進這種協調，應該有超越北約與歐型現有的限制及非正式的努力，跨大西洋社區應該要努力建立一個「協調委員會」的新實體，而能夠在自願的共識基礎上運作，而若與「金融穩定理事會 」（Financial Stability Board）相比，該委員會應該可以在北約、歐盟之國家和私營部門間提供協調一致的外交、經濟、資訊、安全和軍事行動。[65]

中國大陸確實透過各種手段，包括網路、媒體、政治、社會運動或非營利組織，以「模糊不清」的方式引誘台灣人民到「母親」的懷中國大陸採用的「混合性威脅」並非單一面向的傳統或非常規戰爭，而是一種「多型態」，透過「整體性」(Holistic）途徑，結合國家行為者的傳統和非傳統手段，產生灰色的衝突區域。

然而，在混合性衝突中，「民主體制」確實較「專制體制」更容易受到攻擊，然而民主仍有其捍衛的價值，因此，台灣作為一個以信任為基礎的民主社會，面對深具複雜性的混合性威脅，必須採取「全

[65] Franklin D. Kramer and Lauren M. Speranza, Responding to Russia's'Hybrid 'Threat: 6 ways the EU and NATO can head off Russia's many-pronged attack on Western democ- racy, April 24, 2017. <https: // www .usnews.com / opinion / world-report / articles / 2017- 04-24 / 6-ways-the-us-eu-and-nato-can-meet-and-defeat-russias-hybrid-threat>, accessed on Sept. 12, 2017.

面性」途徑與以防禦，透過政府間的跨部門以及私營部門的合作能夠藉助其所掌握的關鍵能力與設備，以針對威脅進行有效的打擊。

但是「全面性途徑」須由強大的情報網絡作為後盾，因此可藉由情報機構分析國家安全的決策能力，確定哪些部份的關鍵基礎設施最有可能成為目標，再加上基礎的政治要素，評估整體動態的依賴性和安全性。

由於決策者需要完整、正確、及時、及有做爲行動基礎能力之情報，故在國家安全政策當中，特別是戰爭與危機管理時期，情報均是進行決策所不可或缺之要素，任何主要的國家政策工具，例如外交、軍事力量，經濟壓力、宣傳、心理戰，或秘密的政治行動，或是彼等之結合使用等，要能發揮成功效用，主要就是依賴於精確分析之情報，特別是在複雜之國際情勢中此種需求更加重要。

良好的情報，不必然會導致明智的政策選擇，但是若沒有完善的情報，則國家政策的決定與行動就不可能有效的回應真實的情況，也不可能天時反映出最佳的國家利益、或適當的保護國家安全，而此在處理危機過程中亦特別凸顯。

然而需注意的是決策者盼獲得包括情報圈之永久官僚體系的支持，而能繼續順利執政，就必須讓情報圈瞭解其政策優先事項，但此可能會造成情報政治化之危險。又情報官員自身傾聽要求之既定立場認知，可能會有意或無意間造成取悅決策者之分析結果。不論那一種

結果，情報與決策官員間良好關係之欲求，均可能會造成對情報客觀性之直接傷害，但良好關保之保持又是危機時作出良好決策所必需的前提條件，故其分寸需拿捏得宜。

又雖然危機時，決策活動不會如正常時期而經常涉及部門間互動之過程，而「藐視機制」(override mechanism）或可能存在而使決策順利，[66]但是對於危機後之情報效益評估，不可免的可能又會陷入多方利益交涉之談判機制中。結果決策者批判情報分析之不完整性，而要求更佳之情報分析產品：而情報分析官員批判蒐情單位之功能不彰，致無法產生更佳之產能，而要求擴大更多之蒐情來源與資產。故有必要回歸結合情報之危機特殊機制的框架，而能持續情報與決策在危機管理作爲中之良性互動。

在危機管理過程中，從戰略層次思考，情報之最大作用在於發揮「預警」機制之功能：而從戰術層次思考，情報之作用在於發揮對於決策過程之「支援」功能，然而情報與政策之固有「不平等」特性，而必須注意決策者可能有「情報政治化」之影響，因此在保證客觀情報的要求下，應該克服情報與決策在追尋國家安全過程中可能之潛在摩擦與問題，從而發揮情報在危機決策中之最大作用。

[66]「藐視機制」指的是強迫之協定及排除相關單位之可能，所強調的不是交易與談判，而是依據主要規定行事。

混合性攻擊的主要特徵是製造社會的不確定性，同步使用各種手段，使人民對於所屬產生因惑與懷疑，尤其是在資訊爆炸的時代，透過否認或扭曲事實，輕易地操控人民，進而分化內部政治及社會凝聚力。因此，採用良好的戰略溝通，在政治層面迅速作出決策仍是成功預防和防禦未來混合威脅的關鍵。透過提供正確訊息、建立溝通管道、澄清謠言、阻止傳播訊息。政府應定期公佈其政策取向和相關資訊，同時建立反駁謠言的管道，在訊息控制中佔據有利地位。相關政府機構應發展其發言人的危機管理能力，並與傳統媒體和社交媒體建立溝通管道，以便他們能夠立即作出澄清陳述、阻止誤傳傳播，並防止台灣被外部勢力操縱，因為外部勢力要製造內部動盪。

此外，宣傳同時擴及內部與外部受眾，雖然能夠藉由「事實」打擊混合性攻擊者的宣傳手法，但要有效的戰略溝通必須謹慎且深思熟慮，並反映內部和外部受眾的不同需求與敏感性。[67]

另外，亦可採取「進攻性戰略溝通」(offensive strategic communications）首先建立有效的反敘事」(counter- narrative)，透過交外交(diplomatic)、訊息(informational)、經濟（economic）和軍事（military）工具結合起來，並且制定有效的反敘事戰略（counter-narrative strategy)。以此戰略試圖滲透對手封閉的媒

[67] European Extemal Action Service, "Food-for-Thought Paper'Countering Hybrid Threats," (Brussels: Council of the European Union, 2015), p. 6.

體空間，並破壞對手與其移伴的訊息傳遞。 然而，這必須建立在良好且全面性的情報基礎。

第五章、結論

第一節 研究發現

中共對臺灣已呈現出更有耐心，且在可以影響的公共與私領域上亦展現出更有區隔性對待之細緻性操作，並深入日常生活各層面。此外，對於之前的九合一大選，儘管臺灣有抨擊中國大陸以金錢與網路介入之反彈聲浪，但中共深知舉證困難，故都能穩住而不起舞；中共方面將會更加小心地避免成為臺灣民眾指責焦點。中共認為，只要掌握臺灣經濟發展之軟肋，則時間一久將有利於中國大陸統一。因此，在混合威脅浮現之下台灣應有認知：

一、國際關係層面的認知

（一）對於美國及其盟國

1. 重新從地緣戰略與國際安全角度檢視臺灣利益與改變的風險。
2. 思考創新而改變既有之美國主導及必然之行動限制框架。
3. 順應國際趨勢與議題，翻轉臺灣一味有求他國的具體價值。
4. 「共贏」而非「對抗」角度，進行與時俱進之政策規劃與調整。
5. 逆勢時，善於運用矛盾以進行損益管控及減緩成為被動棋子影響。

（二）對於中國大陸

1. 基於內部之不同意識型態脈絡，回歸臺灣國家利益之最大考量。
2. 從臺灣主體的角度去認識，而非完全依據美國單方面政策行事。
3. 深入瞭解中共的思維、理論，以正確掌握其意圖與政策變化。

4. 極大化與美國及其盟國互動，以緩解中國大陸等之不友善作為。

5. 基於風險之政策設計，釐清「求同存異」可能運作之實質空間。

綜上所述，由於混合威脅概念本身的模糊化，導致混合戰的概念、構成元素不斷擴張，其原因主要係因科技的進步，以及混合運用常規與非常規手段的各種新式組合手法不斷出現所致。中共施以混合威脅得以奏效，主要因臺灣新聞媒體、社群網絡的發達與近幾次的經驗逐漸累積、塑造有利於中共的環境。

透過相關文獻的探討，本文研究發現，混合威脅的發展與盛行主要係因以下因素所致：

(一) 民主、自由、多元社會本身的弱點。

(二) 低強度、低成本的軍事、外交手段與工具成為有利與有力工具。現代戰爭花費高昂，以及在以經濟發展為主流的國際環境中，致低成本的混合戰手段盛行。

(三) 地緣、種族親緣等環境因素，給予實施混合戰更佳場域。

(四) 混合戰呈現當前資訊、科技時代的戰爭模式，運用混合與創新、不對稱的戰術、戰法，破壞目標國政經穩定與城市發展，攻擊新聞、言論自由弱點，及造成備戰目標的挑戰。

為此，需提高對混合的互信合作與強化遭受混合攻擊的復原能力，避免失敗因素。發揮總體力量（國際、同盟之間，政府與民眾之間，軍民之間，民政部門與軍事部門之間），強化訊息管理與查證能力，調整、建立因應混合威脅的能力。

綜整歐美各國及此議題研究學者們所提出的防止、對抗混合對手的建議與作法，歸納如下：一、提高互信合作與厚實復原能力由於並非所有單獨、個別的恐怖行為、極端行為或犯罪行為，就是混合威脅，必須清楚認知混合威脅的本質為何。[68]歐盟的因應作為，首先在提高各會員國對混合威脅本質的認識，及理解增進彼此互信合作的重要性，以共同、協調行動加以因應。[69] 其方式是鑒於混合威脅主要係針對一個國家的脆弱性入手，故各會員國先行進行廣泛的脆弱性風險調查，透過監測與評估各種可能的脆弱性風險，建立混合威脅指標，將之納入早期預警和風險評估機制，再透過情報交流、合作，共享混合威脅情資。[70]如此，才能針對後續因應對策與作為，作出妥適的選擇。如歐盟就建立「歐盟混合融合小組(EU HybridFusion Cell)」，以接收和分析來自不同利害關係有關混合威脅的分類、公開的情資來源，定期發布分析當前混合威脅問題的公告，提供歐盟內部與各成員國情報分享。強化互信合作的面向包括國內部分，以及國際間的聯盟間合作。國內部分，主要在各部會的部際協調，以發揮整體國力因應混合威脅，達到聯合作戰的效能；[71]另軍事與民政單位間的合作，以

68 European Commission, "Joint Report to the European Parliament and the Council on The Implementation of TheJoint Framework on Countering Hybrid Threats-a European Union Response," EUR-Lex, 2017/7/19, JOIN(2017)30 final, p. 3.

69 Jan Joel Anderson & Thierry Tardy, pp. 1-2.

70 European Commission, "Joint Report to the European Parliament and the Council on the implementation of the JointFramework on countering hybrid threats-a European Union response," EUR-Lex, 2017/7/19, JOIN(2017) 30 final, p. 3.

71 U.S. Department of Defense，國防部史政編譯室譯印，《2006 美國四年期國防總檢討報告》，頁149-156。

適切回應、妥處各種混合威脅危機；最後以軍、民間的合作，以擴大因應混合威脅的基礎與能量。

在國際間方面，則強調聯盟間的廣泛合作，以及與潛在敵對同盟間的互信合作。德米特里・特列寧(Дмитрий Витальевич Тренин)提出三項可避免導致混合衝突升級的方法：事故預防、建立信任、軍備控制。三者共同點在於透明度的建立，及建立可靠溝通管道與平臺。如政治上的北約—俄羅斯雙邊定期會、軍事上戰場緊急通信、以及重大演習前的通報與觀察員的邀請等等，都在強化互信措施。[72]

由於全球化的影響，人員、資金、訊息流通無國界，任何混合威脅徵候或措施，都可能擴及第三地或更大區域。因此，藉由前述的政治、經濟、金融、戰略安全、軍事合作，以及情報、訊息交流與分享等等，都是促進互信合作的有效方式。除了思維與態度上提高對混合威脅的認知和合作，亦應發展與厚實對混合威脅的具體因應措施與抵禦能力。混合威脅主要在運用一個國家的脆弱性，以及運用自由、開放社會生活方式，所進行破壞與攻擊。尤其是針對關鍵基礎設施、供應鏈與社會的潛存脆弱點。因此，如何強化爾等壓力承受能力與遭受破壞後的迅速恢復能力，就成為對抗混合威脅攻擊的重要方向。[73]麥

[72] Дмитрий Витальевич Тренин, “Смягчение конфликта в условиях гибридной войны（混合戰情勢下的衝突緩解；The Mitigation of the Conflict under the Influence of Hybrid Warfare）

[73]European Commission,“Joint Framework on Countering Hybrid Threats-A European Union Response, " p. 5.

可・米勒曾提出預防混合戰和制止、擊潰混合敵人的戰略框架：經濟上，揭露國家對叛亂分子、恐怖分子或革命團體的支持，對該支持國家實施經濟和金融制裁，以及凍結非國家行為者的資金；政治上，透過外交手段，為遭受混合戰的國家（盟國）建立國際支持，促使國家改革與建立國際同盟，運用外交談判手段，解決、消弭內、外部政治衝突，以及揭發混合對手的暴行和戰爭罪行；軍事上，加強軍事安全合作，如情報合作、人員培訓、聯合演訓、軍售等軍事技術合作項目，目的在確保該國能有足夠力量穩定內部衝突局勢，抵禦外部侵略。[74]歐盟「向歐洲議會和理事會關於打擊混合威脅聯合框架的執行情況—歐洲聯盟的回應聯合報告」就敦請歐盟各會員國考慮建立對抗混合威脅的卓越中心，以研究混合戰略如何被操作、運用，以及鼓勵在民間企業發展新概念和技術，協助會員國建立復原力。

無論是政治上軍事存在或經濟上合作，目的都在建立民眾對政府的信心，安撫民眾心理，確保政府機關運作與維護社會穩定，避免給予混合對手藉以製造政治、經濟、社會、心理混亂，達成其混合戰的目標。此外，由於混合戰的模糊性質，致使國際法與武裝衝突法的條款出現有效性與可執行性的問題，已經無法解決當前戰爭型態的各種法律問題。[75]諸如：混合戰模糊平戰時的時空區隔，致使宣戰與最後通牒的程序無法明確執行；及需具有反侵略的自衛戰爭或人道干涉的

[74] Michael Miller, *Hybrid Warfare: Preparing for Future Conflict* (Maxwell Air Force Base, AL: Air War College,February 2015).

[75]胡明霞、張卉媛，〈混合戰背景下法律戰發展問題探究〉，《牡丹江大學學報》，第23卷第7期，2014年7月，頁8。

正義理由，以和平為目標的正目的；與由國家或聯合國國際組織等合法權威進行開戰正義的道德基礎與權利；以及混合戰中充斥平民參與者所引起的戰鬥人員非戰鬥人員區分原則，及爾等運用民用科技與平臺遂行混合戰之軍事目標與非軍事目標區分原則等問題。

第二節 研究建議

混合性威脅模糊戰爭與和平的界線，帶來一種橫跨戰時與平時的聯合作戰，所採用的是「平戰一體」、「多領域作戰」、「軍民融合」等概念，旨在利用國家在政治、軍事、經濟、社會、資訊和基礎設施不同領域之脆弱性，進行專屬式攻擊。因此，認知混合性威脅特徵與發展脈絡為首要之急，並須以此審視軍事任務發展之思維與脈絡。

安全環境變化與技術革新，帶來便利性與優點的同時，也為衝突提供新的途徑。社群媒體出現後，非國家行為者能夠更輕易觸及主流媒體和一般大眾。各領域間相互依賴且難以獨立分割，新興戰場由不同卻相互糾結的元素所組成。組成要素的關聯性、複雜性和相互依存性以及既得利益者的多樣性，造就不斷演化的國際安全環境。

因此，混合性威脅得利於此種混雜凌亂、相互糾葛之安全環境特徵。針對對手之脆弱性，利用各種手段進行「模糊」的攻擊，以達戰略目的，使混合性攻擊者在任何地方都能進行破壞、中斷或停止目標對手的社會運作，且不知道攻擊何時發動、何時發生以及如何發動

攻擊。混合性攻擊者得利於身分的轉化，使其所施以行為活躍於灰色地帶。表面上以國家行為者的角色與他國共同呼籲，達成合作協議，實則利用各種資訊操控或代理人等隱蔽方式，獲其核心戰略目的。

簡言之，即在針對關鍵的脆弱性，試圖製造模糊性，使決策者難以做出迅速且有效的判斷。因此，執著於武器技術的發展不足以贏得戰爭，而必須透過採取全面性途徑之預防和應對手段。採取「全面性途徑」，進行協調政府、軍事和私營部門的專業知識，監測情況的變化、評估影響，再透過將蒐集程序制度化，以供各層級都能協助加強混合性戰爭之預警，以建立韌性、增加威懾效果，提升整體國家安全。再加上，混合性威脅屬全球性議題，能增進與國際間合作，共同協助打擊混合性戰爭。我國可以透過如此全球安全防衛趨勢，與國際其他各國達成合作協議，共同應對中共施以的混合性威脅。

未來我國應該利用長期以來針對中共的研究能量，加以蒐集、分析、探討更多中共在國際間可能或正在操弄的混合性手段（例如「小藍人」之稱的海上民兵），以加強與國際間合作關係，共同應對中共施以的混合性威脅。其次，囿於我國對於混合性威脅之認知與準備尚未有共識，應著重瞭解衝突演化下，混合性威脅所操作手段與工具改變，應對軍事任務必須隨之調整，僅著重於思維層面，而未針對戰略、戰術等層面進行研究，因此該如何在因應不同的威脅場景，執行與操作不同的戰略方針將成為未來研究之方向。

透過本文對混合戰的探討，對於我國建軍備戰最大的啟示在於，既然混合戰反映當前國際權力格局與資訊、科技發展下的戰爭模式，

那麼就不能、也不應忽視敵人運用混合戰對我造成的威脅，應重新檢視我建軍備戰的方向與作為。如同霍夫曼在其著作之結論中所述：「我們不能再忽視社會的脆弱性，專注偏好能力的展現，低估挑戰者的想像力。在混合戰的世界裡，精神僵化或自滿只會付出更高的代價」。[76]因此，對抗混合戰的根本之道在於，必須改變舊有的「戰爭」傳統觀念與思維，從計畫性、線性、規則性的常規戰爭思維，轉變為突變性、同時性、不規則、非對稱及混用常規與非常規的思維。最重要的是，作戰計畫、指揮人員應有「容許變」、「採取變」之「變」的認知與思維，於演習、訓練中逐漸檢視、調整部隊指揮、管制與組織、編制，以及戰術、戰法、教育訓練，始能有效因應混合性威脅。

[76] Frank G. Hoffman, pp. 46-51.

參考文獻

一、中文文獻

(一)專書

朱浤源，2010 年。《撰寫碩博士論文實戰手冊》。臺北市：正中書局。

呂秋文，2007 年。《如何撰寫學術論文：以政治學方法論為考察中心》。臺北市：臺灣商務印書館。

李明總編輯，汪毓瑋著，2018 年。《國際關係》。台北:前程文化事業股份有限公司。

汪毓瑋，2013 年。《國土安全》。臺北市：元照出版。

汪毓瑋，2016 年。《恐怖主義威脅及反恐政策與作為》。臺北市：元照出版。

汪毓瑋，2018 年。《情報、反情報與變革》。臺北市：元照出版。

陳偉華，2003 年。《軍事研究方法論》。桃園：國防大學。

喬良和王湘穗，1999 年。《超限戰》。北京：解放軍文藝出版社。

黃秋龍，2004 年。《非傳統安全的理論與實踐》。臺北市：法務部調查局。

葉志誠，2000 年。《社會科學概論》。台北：揚智文化。

趙干城，鮑世奮，1988 年。《史學方法論》。台北：五南圖書出版公司。

談遠平、康經彪，2004 年。《戰爭哲學》。臺北市：揚智文化。

魏鏞，1971 年。《行為研究法、制度研究法、歷史的研究法》。臺北市：臺灣商務印書館。

(二)期刊

朱鋒，2004 年。〈非傳統安全解析〉,《中國社會科學》，第 4 期，頁 8-10。

汪毓瑋，2018 年。〈臺灣視野之下世界安全局勢與持續努力方向〉,《清流月刊》，第 18 期，頁 26-27。

林穎佑，民 2017 年。〈中共戰略支接部隊的任務與規模〉,《展望與探索》，第 15 期，頁 10-15。

俞晚秋、李偉，2002 年。〈非傳統安全論析〉,《現代國際關係》，第 5 期，頁 20-

26。
胡敏遠，2018 年。〈貫徹國軍軍事戰略－『防衛固守、重層嚇阻』作為之研究〉，《陸軍學術雙月》，頁 17-20。
倪一峯，2018 年。〈俄國對克里米亞混合戰的運用：兼論對我之啟示〉，《國防雜誌 》，33 期，頁 45-47。
謝雪屏，2008 年。〈試析中共歷代領導人對台政策的基本思路〉，《湖北省社會主義學院學報》，第 4 期，頁 20-24。
黨朝勝，2018 年。〈習近平對臺工作重要思想芻議〉，《特區實踐與理論》，第 2 期，頁 108-114。

(三)新聞

中央社，2019/7/8。〈中國打壓台灣國際參與的統戰手法：讓台灣畏懼，以為不依賴中國就活不下去〉，《中央社》。
中央廣播電台，2019/10/3。〈臺灣民意拒絕「一國兩制」、反對北京當局對臺軍事威脅及外交打壓的不友善作為〉，《中央廣播電台》。
中華民國大陸委員會，2019/9/18。〈從中共對我外交打壓論我朝野應有之立場與作法〉，《中華民國大陸委員會》。
中華民國國防部，2019/3/18。〈針對媒體報導「阿根廷聖胡安號潛艦失事乙情〉，《國防部即時新聞專區》。
王中原，2015/9/15。〈觀察：為何歐洲政民危機是一場政治危機？〉，《BBC中文網》。
王揚宇，2018/6/13。〈新室青年軍王炳忠等人沙達國安法遭北檢起訴〉，《中央通訊社》。
朱雪齡、曾華鋒，2017/10/17。〈致腦作戰：未來戰爭競爭新模式〉，(解放軍報》。
林俊良，2018/8/7。〈北檢搜索中華統一促進黨追查金流〉，《聯合報》。

林庭瑞，2018/12/26。〈中共成功試射s400地對空飛彈足以封鎖台海中北部〉，《經濟日報》。

侯姿瑩，2018/8/21。〈薩日瓦多斷交中華民國邦交國降至17國〉，(中央社》。

姚旭東，2014/1/6。〈海上後備動旅路浪行廣西北海軍分區加強海上民兵建設紀實〉，《解放軍報》。

洪哲政，2018/7/29。〈國軍建特種飛彈營區兩岸軍事對抗升高〉，《聯合晚報》。

風傳媒國際中心，2018/9/21。〈中國真的派車進關西機場接人？日方發言人給正解：沒有這回事〉，《風傳媒》。

倪光輝，2016/1/24。《揭密我軍首支戰略支援都隊》，《人民日報》。

崔慈悌，2018/1/17。〈記者被跟監？府：已要求國安局立即調查〉，《中時電子報》。

(四)網路資料

台灣事實查核中心，2018/12/27。《【錯誤】網傳台灣防疫首傳破洞，花蓮縣爆發疑似豬隻感染非洲豬瘟》，〈https://tfc-taiwan.org.tw/articles/335〉。

台灣事實查核中心，2018/9/15。《【錯誤】媒體報導：日本關西機場因燕子颱風重創而關閉後，中國優先派巴士前往關西機場營教受田之中國旅客？》，〈https：//tfc-taiwan.org.tw/articles/150〉。

超級大本營軍事論壇，2018/4/26。《超級大本營軍事論壇 agentbear 個人資料》，〈https://lt.cjdby.net/space-username-agentbear.html〉。

薩拉·庫克，2020/2/19。〈自由之家：中國共產黨影響國際媒體的行動正在迅速擴張！〉，《風傳媒》，〈https://www.storm.mg/article/2238504〉。

二、 外文文獻

(一)官方文件

Dempsey, General Martin, 2015. The National Military Strategy of the United States of America 2015 Washington D.C: United States Joint Chiefs of Staff.

Development Concepts and Doctrine Centre, 2010. Joint Doctrine Publication 04. Understanding. London: United Kingdom Ministry of Defence.

Development Concepts and Doctrine Centre, 2010. Strategic Trends Programme: Futre Character of Conflict. London: United Kingdom Ministry of Defence.

Development Concepts and Doctrine Centre, 2011. Understanding and Intelligence Suppor to Joint Operations. London: United Kingdom Ministry of Defence.

Development Concepts and Doctrine Centre, 2014. Global Strategic Trends-out to 2045 (London: United Kingdom Ministry of Defence.

Developement Cocepts and Doctrine Centre, 2010. Strategie Trends P'rogramme: Futuy Chrowr of Caye London: United Kingdom Ministry of Defence.

Develpment Concepts and Doctrine Centre, 2011. Understanding and Intelligence Support Operations .London: United Kingdom Ministry of Defence.

Develpment Concepts and Doctrine Centre, 2014. Global Strategic Trends-out to 2045 .London: United Kingdom Ministry of Defence.

Development Concepts and Doctrine Centre, 2015, Future Security Challenges: Baltie Sea Region. London: United Kingdom Ministry of Defence.

Development Concepts and Doctrine Centre, 2017. Joint Doctrine Publication 02. UK Operations: The Defence Contribution to Resilience and Security. London: United

Kingdom Ministry of Defen ce. DHS Press Office, 2016. Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security, Homeland Securiy.

European Commission, 2012. The EU approach to resilience: Learning from food security crises. Brussels: European Commission .

European Extemal Action Service, 2015. Food-for-Thought Paper Countering Hybrid Threats. Brussels: Council of the European Union.

Europcan Parliament, 2016. "Resilience in the EUs Foreign and Security Policy,"

European Parliament, 2016. Europe of Defence? Views on the Future of Defence Cooperation. Brussels: Europcan Parliament.

European Union, 2015. "Action Plan ba Strategic Communication.

Gates, Robert Michael, 2010. Quadrennial Defense Review Report. Washington DC: Unitcd States Department of Defense.

Heads of State and Government at the NATO Summit, 2010. Active Engagement, Moderit Defence . Lisbon: Heads of State and Government at the NATO Summit.

(二)專書

Frank G. Hoffman, 1998. Conflict in the 21st century :The Rise of Hybrid wars

Guillaume Lasconjarias and Jeffery A.Larsen eds., New York:Pantheon Books.

Cullen, Patrick J and Erik Reichborn-Kjennerud, 2017. MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare. Oslo: Multinational Capability Development Campaign. Michigan Press.

Dover , Robert and Michael Goodman, 2009. Spinning Intelligence: Why Intelligence Needs the Media, Why the Media Needs Intelligence. London: Hurst Publishers.

Dupont, Alan, 2001. East Asia Imperilled: Transnat Professional Challenges to Security. Cambridge: Cambridge University Press.

Gray, Colin , 2012. Another Bloody Century: Future Warfare. London: Hachette .

Hermes, 2010. Managing Within Constraints: Balancing US Army Forces to Address a Full Spectrum of Possible Operational Need. Alexandria, Virginia: Institute for Defense Analyses.

Huber, Thomas M, 2002 . Compound Warfare: A Conceptual Framework, in General, ed., Compound Wirfare: That Fatal Knot. Fort Leavenworth, Kansas: US Army Command and General Staff College Press.

And Hybrid Threats. An Assessment- 2011. Washington, DC: Govemment Printing Press. Krulak, Charles C., 1997. The Three Block War: Fighting in Urban Areas.

Washington, DC: Joint Irregular Warfare Center and US Joint Forces Command, 2011. Irregular Adversaries National Press Club.

Kuzio, Taras and Paul D'Anieri, 2018. The Sources of Russia's Great Power Politics: Ukraine and the Challenge to the European Order. Bristol, England.

(三)期刊

Aoi, Chiyuki, Madoka Futamura, 2019. “Introduction Hybrid Warfare in Asia: Its

Meaning and Shape”.The Pacific Review. pp.15-26.

Aro, Jessikka, 2016. “The Cyberspace War: Propaganda and Trolling as Warfare Tools”. European View, pp.75-82.

Bachmann, Sascha-Dominik and Andres B Munoz Mosquera, 2015. “Hybrid Warfare and Lawfare,” Operational Law Quarterly, Vol.82, No.4, pp.72-76.

Baldwin, David A, 1995. “Security Studies and the End of the Cold War,” World politics ” pp.48-51

Berzinš, Janis, 2014. “Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy,” Policy paper,Vol. 2 ,pp.214-216.

(四)新聞

Burgess, Matt, 2017/11/10. "Here's the First Evidence Russia Used Twitter to Influence Attack, "Agence France Presse. Brexit, " Wired

Chen, Adrian, 2015/6/2. "The Agency, " The New York Time Magazine.

Chen, Yu-Hua, 2018/12/11. "China's Meddling in the 2018 Taiwan Local Election," Tahwan Insights

Emirates News Agency, 2018/6/7. "Hybrid Warfare Poses a Serious Threat to National Security, Say Defence Experts, " Emirates News Agency.

(五) 網路資料

William J. Nemeth, 2002.Future War and Chechnya: a Case for Hybrid Warfare . Monterey, CA: Naval Postgraduate School. <https://www.vpk-news.ru/articles/14632>.

James N. Mattis & Frank G. Hoffman, 2005. “Future Warfare: The Rise of Hybrid Wars ” Proceedings Magazine, Vol.132.

<http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf>.