10.6326/NDJ.201912_34(4).0001

混合性威脅下的軍事任務思維：我國國家安全新挑戰[1]

The Thinking of Military Missions under the Hybrid Threats: New Challenges for Taiwan's National Security

吳嘵芳(Liang-Fang Wu)

空軍軍官學校學員生指揮部上尉輔導長

摘　　要

後冷戰時期，動態複雜的安全環境挑戰過去傳統的國家安全意識。國家或非國家行爲者利用光譜上傳統與非傳統間的手段，使戰爭與和平的分界模糊不清。2014年烏克蘭危機加深學界對於「混合性衝突」的重視。本文解析國際安全環境威脅型態的演化，解析混合性威脅的概念，並探究其如何將過去傳統的攻擊手段進行組合運用，借鏡美國、北約應對方針，分析出我國軍事任務發展所須調整之思維及調整後可能面臨的問題，以供政府決策參考。

關鍵詞：後冷戰時期、安全環境、混合性威脅、軍事任務、全面性途徑

Abstract

In the post-Cold War era, the complexity of this dynamic security environment challenges the conventional national security awareness. State or non-state actors have leveraged the traditional and non-traditional means to blur the boundary between war and peace. In 2014, the Ukrainian crisis triggered academic debate over “hybrid conflict.” The hybrid threats utilize unconventional ways. This paper analyzes the evolution of the threat patterns in the international security environment, in order to clarify the concept of hybrid threats, and explore the attack methods used in combination. Then, the author refers to the United States and NATO policy responses, and analyzes the thinking of adjustment for development of Taiwan's military missions and the problems that Taiwan may face after the adjustment. The entire report will serve as a policy recomendation for government decision making.

Keywords: post-Cold War period, security environment, hybrid threat, military mission, comprehensive approach

1 「Hybrid Threats」多譯為複合性或混合性威脅，因考量文章一致性及清楚理解原文因素，全文統一為混合性威脅。

壹、前　　言

全球化下，戰爭不再是國家行為者間用來解決衝突的方法，因為戰爭成本考量，國家行為者不願被捲入其他區域的長期軍事衝突，然跨國組織、企業、犯罪份子以及非政府組織等非國家行為者卻在安全領域佔有一席之地，多樣化行為者已跳脫傳統威脅的模型框架，引發難以被普遍定義新形態威脅模式。另一方面，隨著大規模戰爭爆發機率降低，傳統軍事手段在國家安全與國際安全所扮演功能下降。為了因應面對威脅變化與爭取足夠經費等諸多因素之下，許多西方國家已對軍事組織展開大規模調整與轉型，武裝力量重新執行過去被界定為非軍事性的任務為主。

後冷戰時期，當代威脅行為者在新技術協助下，操作同步性和組合戰爭類型的複雜程度日益提高，以致對於傳統大國軍事優勢造成嚴重威脅。自2006年以色列與真主黨之間的衝突以來，「混合性威脅」似乎成為表現威脅行為者日益複雜的非線性(non-linear)手段。[2] 混合性威脅透過傳統和非常規武力結合，或在兩者間迅速轉換，以產生戰略效果。然而，此種令人驚訝的轉換手法及其展現之效果，使得新興混合性威脅概念引發學界的爭論。

2014年3月俄羅斯佔領克里米亞以來，學界又再次引發有關「混合性戰爭」(Hybrid Warfare)的辯論，俄羅斯利用極小損失影響烏克蘭，對歐盟、北約及鄰國構成複雜挑戰。[3] 未來也不再僅限於非國家行為者才會使用非對稱性攻擊，所涉及範圍從原有軍事戰略主題，進入更廣泛的政策領域。透過國家力量得以未受限操縱，產生更大綜合效應。[4] 2015年5月，歐盟對外發布了一份關於〈應對混合性威脅〉(*Countering Hybrid Threats*)的報告，重申需認識混合性威脅的整體影響，並透過增強抵禦能力以因應新興威脅。

綜上所述，混合性威脅儼然成為當前全球須嚴陣以待的威脅型態。然而，各國學者對混合性威脅的定義尚模糊不清，且我國對於混合性威脅的研究尚未廣泛，面對中共利用各領域灰色地帶對我國所施以新興威脅手法，我國更應正視衝突型態的轉變，並調整軍事任務發展之思維模式，以有效打擊混合性威脅，維護我國國土安全。本研究從概念性基礎建構而起，藉分析混合性威脅的背景演化與手段，提出中共正對我國施以混合性威脅例子，促使政府與國人重視混合性威脅重要性，呼籲各層級的政府單位必須提高警覺，甚至私營部門或民間團體亦須相互配合，以情報脈絡為主軸，發展「全面性安全途徑」。

貳、威脅多樣及混合之演化

混合性威脅反映出國際安全性質重大變化，安全環境從過去單一的、線性的、規

2 「線性衝突」定義為對手計畫戰略的連續進展，反之，「非線性衝突」則是同時部署多種互補的軍事和非軍事戰術。當一個國家將傳統和非常規軍事力量與心理、經濟、政治和網路攻擊結合起來時，即會發生非線性戰爭。

3 Gjorgji Veljovski et al., "The Danger of 'Hybrid Warfare' from a Sophisticated Adversary: The Russian 'Hybridity' in the Ukrainian Conflict," *Defense & Security Analysis*, Vol. 33, No. 4, 2017, pp. 292-306.

4 Gjorgji Veljovski et al., *Defense & Security Analysis*, p. 307.

律的模式，轉變為複雜的、多層次的(multi-layered)、多面向的(multi-dimensional)狀態，隨之帶來的威脅也更加難以預期，成為21世紀各國面臨的新安全挑戰。以下就威脅、型態、行為者、空間等四大因素進行分析，以瞭解當前安全環境本質的核心。

一、國內威脅界線與國外模糊威脅界線

隨著現代通訊技術的進步，人們能夠以前所未有的方式進行溝通，高度互聯全球的個人與團體，以致過去實體或政治邊界逐漸消弭。但是，資訊革命的迅速蔓延，進一步加速破壞力的擴散，國內或區域衝突迅速「外溢」至全球，為潛在對手提供更大機會，造成整體安全環境之不穩定結果。

㈠跨國犯罪集團與恐怖主義的擴張

跨國犯罪集團對於相互關聯的貿易、運輸系統造成威脅，利用失敗國家或有爭議領域威脅對手利益，與腐敗外國政府官員和情報部門建立聯盟，利用網路技術和其他方法進行複雜的欺詐行為，進而破壞脆弱國家的政治、金融和安全機構；亦可透過黑市交易將大規模毀滅性武器(Weapon of Mass Destruction, WMD)轉讓給恐怖份子，擴大毒品販運和人口及武器走私網路。恐怖份子和叛亂團體轉向藉由犯罪網路籌集資金，並獲得後勤支持。[5] 例如在2008年12月～2009年1月期間，以色列國防軍在「鑄鉛行動」(Cast Lead Operation)期間將目標鎖定在加薩走廊的哈馬斯(Hamas)組織。[6] 在2009年1月18日停火之後，走私管道立即得到修復，持續向加薩地區哈馬斯提供武器和貨物。

㈡反移民與極端右派的意識形態崛起

交通運輸的革新帶來的全球化，大幅消弭人類移動的地理障礙，儘管外移人口大幅彌補已開發國家勞動市場人力不足的問題，然在媒體負面渲染下，移民人口成為各國當前眾多問題的代罪羔羊。此種反移民情緒促使極右派主義浪潮再次崛起，加劇歐洲與美國內部社會分化，其中在歐洲的狀況更為顯著。例如，法國國民聯盟(Rassemblement National, RN)、德國另類選擇黨(Alternative Für Deutschland, AFD)，在各國選舉中均擁有強勁勢力，這些政黨的核心政策主張就是反對外來移民和歐洲的一體化。[7]

同時，反移民和反歐洲整合是一體兩面，當反移民政黨在各國累積足夠聲勢後，勢必加劇該國在歐洲的分離情緒。透過媒體渲染及選舉政治動員及話語操作，使得潛在種族和族群的排斥心理不斷放大，容易造成偏激的社會行為，引發更多社會問題。

㈢武器與技術普遍流通

隨著武器與技術發展，雖然國際法律和社會規範將會對國家軍事行動或暴力衝突形成限制，但非國家行為者不會受到如此

5 Joint Irregular Warfare Center and US Joint Forces Command, *Irregular Adversaries and Hybrid Threats. An Assessment-2011* (Washington, DC: Government Printing Press, 2011), p. 21.

6 加薩戰爭開始於2008年12月27日，以色列國防軍對巴勒斯坦加薩走廊的哈馬斯目標，執行代號「鑄鉛行動」(Cast Lead Operation)的空襲。

7 王中原，〈觀察：為何歐洲難民危機是一場政治危機？〉，《BBC中文》，2015年9月15日。

8 軍民兩用物品是可用於民用和軍用應用的物品、軟體和技術。

9 Ralph Thiele,“Hybrid Threats: And How to Counter Them,”*ISPSW Strategy Series: Focus on Defense and International Security*, Vol. 448, 2016, pp. 10-11.

約束，依然得以恣意地操作新技術與新型武器。叛亂份子和暴力極端主義組織等非國家行為者能夠藉由日益緊密的貿易管道取得各式各樣具有軍民兩用(Dual-Use)的工具和技術，[8] 再搭配新興資訊技術，大幅減少部隊與指揮機構間距離，以及時間和訊息間停頓的差距，使非國家行為者能夠更快且更有效的執行精準打擊，將使其軍事行動變得更加活躍且具有破壞力。[9] 2009年，美國「政府責任署」(*Government Accountability Office, GAO*)得出結論，敏感軍民兩用物品得以自美國製造商與分銷商輕鬆合法地購買，且在沒有檢測到情況下，非法出口到流氓國家和恐怖份子供應商。[10]

㈣國際規範的效能限制

隨著全球化發展，國際情勢轉變，加劇國家行為者獲得必要國際合法性與採取行動的迫切性。國家行為者必須擁有客觀證據，才能使用軍事手段，為「師出有名」提供堅實基礎，但是出兵議案的通過，必須經過國會審理，接著送交聯合國安理會決議，完整審理合法性過程需要時間，加上安理會審議涉及複雜國際關係，變得越來越難以實現。以致在未來的衝突中，將造成守勢國家行為者在軍事主動的劣勢。

例如，在烏克蘭危機中，俄羅斯雖身為侵略者，卻主張遵循《聯合國憲章》(United Nations Charter)行事，使得國際社會更難定義俄羅斯的侵略行為。俄羅斯利用對《聯合國憲章》形塑對自己有利的解釋權，以「自衛」為藉口，以保護人民為名，行干預烏克蘭之實。[11] 聲稱《聯合國憲章》第五十一條明確同意國家的「自衛」行為，且國會已同意維護在克里米亞的俄羅斯國民，並執行「自衛」的權力，故意模糊軍事和非軍事行動之間的界限。[12] 因此，儘管北大西洋公約第5條(Article 5)聲稱對一個盟友攻擊是對所有人的攻擊，但面臨更顛覆且模稜兩可的俄羅斯戰術，難以引發援引第5條等升級措施。[13]

二、傳統威脅與非傳統威脅的混合

學界對於安全環境的認知之轉變大致以冷戰做為分界。冷戰以前，傳統安全觀概念著重於國家；自1980年代開始，許多學者開始批判以軍事與國家安全為中心的安全研究。[14] 冷戰結束之後，對現實主義傳統安全觀的批判變得更為激烈，隨著非國家層次因素加入，出現更多與過去政治、軍事、經濟不同的傳統安全威脅，衝突領域也擴大到環境、資源、宗教種族甚至政治社會運動等，所影響程度與範圍隨著科技革新，威脅到多數國家生存與發展。[15]

10 Joint Irregular Warfare Center and US Joint Forces Command, *Irregular Adversaries and Hybrid Threats. An Assessment-2011*, pp. 26-27.

11 Nicholas Fedyk, "Russian 'New Generation' Warfare: Theory, Practice, and Lessons for US Strategists," *Small Wars Journal*, 2016, p. 2.

12 Patryk Pawlak, "Understanding hybrid threats," *European Parliamentary Research Service Blog*, 2015/6/24, <https://epthinktank.eu/2015/06/24/understanding-hybrid-threats/.>（檢索日期：2019年4月26日）

13 Alexander Lanoszka, "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe," *International affairs*, Vol.92, No. 1, 2016, pp. 190-192.

14 Ole Wæver, *On Security* (Chichester, New York: Columbia University Press, 1993), p. 5.

然而，動態安全環境及採用戰爭方法的革新技術，使得戰爭本質在沒有改變的狀況下，戰爭型態不斷地發生變化。混合性威脅所帶來的「混合性戰爭」包含一系列對敵行為，不僅是傳統大規模軍事入侵，而透過各種行為，包括顛覆性情報行動、破壞行為、駭客攻擊以及代理叛亂者授權來破壞對手，也可能傳播假消息（在目標國和第三國），施加經濟壓力，並威脅能源供應。[16]

混合性威脅展現在使用多種包含傳統武器、化學、生物、放射和核(Chemical, Biological, Radiological and Nuclear, CBRN)材料、恐怖主義、間諜、網路攻擊和犯罪等手段與方法的融合，搭配惡意資訊操作和合法商業組織的支持，能夠同時由經濟、法律、政治、社會和軍事等多個領域共同組成及運作。因混合性威脅可以迅速擴展和收縮，並透過這些手段實現其目標。例如利用貿易聯盟(trade unions)和非政府組織作為隱蔽戰線，或使用虛假網站(false websites)和植入報章資訊。[17]

此外，複雜的混合性戰爭無法輕易切割，且戰爭與和平之間不存在二元對立，而在任何時候、在任何地方和所有資源都是在進行作戰。現代戰場是一個涵蓋政治、經濟、訊息、技術和生態手段的全面作戰空間，必須在衝突開始前就建立「有利的政治、經濟和軍事環境」。[18] 混合型對手充分利用所有可能的方法，將符合自己的戰略文化、歷史遺產、地理現狀以及用經濟和軍事手段的方法結合起來，在衝突的各個層面上，藉由國家行為者和各種非國家行為者（有或沒有國家贊助）發揮作用。以非傳統戰爭形式靈活地使用各種手段將政治或意識形態資訊傳送至全球，而不必考慮國際法律或規範，甚至不用提出替代方案。

三、國家行為者與非國家行為者交錯

過去戰爭是國家行為者間所產生衝突。21世紀初期，出現了「影子衝突」(shadow conflicts)的非傳統戰爭。[19] 在沒有明顯的狀態歸屬的蒙面戰士(masked warriors)戰鬥下，非常規組織(irregular groups)採用熟練不對稱手段(asymmetrical means)以爭取勝利，這種衝突很快成為未來最常見戰爭類型。顯示能夠威脅國際聯盟的對手不一定是國家行為者；非國家和匿名行為者可以構成重大威脅，[20] 儼然對傳統的20世紀模式和國際衝突與行為規範提出了難以解決的挑戰。

根據北大西洋公約組織(North Atlantic Treaty Organization, NATO)最新最高作戰指導構想(Capstone Concept)指出，混合性威脅是「對手」提出的威脅，擅長能夠同時且採用傳統和非傳統手段的能力以達到追求目標。[21] 其中，並沒有指定「對手」來源為

15 黃秋龍，《非傳統安全的理論與實踐》（臺北：法務部調查局，2004年），頁23。
16 Nicu Popescu,“Hybrid Tactics: Neither New nor Only Russian,”*EUISS Issue Alert*, Vol. 4, 2015, p. 1.
17 汪毓瑋，《情報、反情報與變革》（臺北：元照出版有限公司，2018年），頁22-23。
18 Jānis Bērziņš,“Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy,”*Policy Paper*, Vol. 2, 2014, p. 5.
19 David Barno,“The Shadow Wars of the 21st Century,”*War on the Rocks*, 2014/7/23, <https://warontherocks.com/2014/07/the-shadow-wars-of-the-21st-century/>（檢索日期：2019年5月16日）
20 汪毓瑋，《情報、反情報與變革》（臺北：元照出版有限公司，2018年），頁17。
21 IMSM-0292-2010,“Hybrid Threats Description and Context,”*NATO Capstone Concept*, 2010/5/10, pp. 2-3.

何，因此承認敵人模糊性(Ambiguity)，以及威脅本身和組合傳統與非常規性質。英國智庫「開發概念和準則中心」(Development Concepts and Doctrine Centre)將「模糊性」定義為「在來源、動機、意圖或威脅方面故意不明確的行動或一系列行動，但其目的是破壞穩定、詆毀或以其他方式削弱對手」，[22] 簡而言之，被用來使對手決策過程複雜化或破壞，旨在使對手軍事反應（甚至是政治反應）變得艱難。可從兩種角度分析其目的性：

㈠從軍事角度來看

目的在藉由低於戰爭的門檻，合法化其軍事力量。模糊不清原則可透過多種方式實施，旨在避免傳統戰爭，針對對手已知「紅線」或門檻，在其「下方」運作的「灰色戰爭」(Gray Warfare)。這些紅線沒有明確表示，並利用這些不明確空間，透過使用代理人（例如小綠人、傭兵公司、網路）來隱藏和否認代理，以實現合法化之模糊性。[23]

㈡從廣泛層面來看

混合性戰爭刻意「混合」以模糊隱蔽與公開行動之間界限，使得國家行為者與非國家行為者在身分能夠輕易轉換，模糊戰爭與和平以及敵對行動開始和結束之間的區別。軍隊藉由取消制服和徽章以及其他階級指標，與當地居民融為一體，叛亂組織能夠放下武器、躲進人群，成為抗議不法行為的無辜民眾。犯罪份子也穿上當地警察部隊人員，以便進入關鍵基礎設施(Critical Infrastructure)。[24]

四、威脅空間擴大—實體空間與虛擬空間

由於資訊革命的影響，現代社會知識和資訊與技術發展相互結合，擴及政治、經濟、法律或社會等範疇，不僅帶來人類生活的改變，也促使並造成軍事衝突之轉變，以致動態的國際安全環境變化跳脫出原有的物理空間。1997年美國海軍陸戰隊司令克魯拉克(Charles C. Krulak)提出「三街區戰」(Three Block War)的概念，描述典型的21世紀戰場，分別是全面性軍事行動、人道主義援助與維和行動。[25] 但馬蒂斯(James N. Mattis)和霍夫曼則辨析，這概念應增加新維度—第四區塊涉及心理或資訊操作，其中所形成之戰場，並非傳統實體空間，而在溝通或訊息傳播的虛擬空間。[26]

網路空間是由相互依賴的資訊網路所構成，可被視為資訊環境的共同全球領域(common global domain)，[27] 伴隨而來新型態的軍事衝突，將傳統軍事力量與惡意網路攻

22 United Kingdom Ministry of Defence's Development Concepts and Doctrine Centre, "Future Security Challenges: Baltic Sea Region," 2015, p. 20.

23 Ibid., p. 19.

24 United Kingdom Ministry of Defence's Development Concepts and Doctrine Centre, *Strategic Trends Programme: Future Character of Conflict*, 2010, p. 22.

25 Charles C. Krulak, *The Three Block War: Fighting in Urban Areas* (Washington, DC: National Press Club, 1997), p. 139.

26 James N. Mattis and Frank Hoffman, "Future Warfare: The Rise of Hybrid Wars," *Proceedings-United States Naval Institute*, Vol.131, No. 11, 2005, p. 12.

27 Mihai Marcel Neag, "A New Typology of War-the Hybrid War," *Land Forces Academy Review*, Vol. 21, No. 1, 2016, p. 15.

擊的破壞性和致命性結合，並透過得以作為武器的資訊以及關鍵基礎設施進行破壞。從而影響人民生活，並剝奪整體作戰規則，儼然形成「戰爭的新時代」(new era of warfare)。[28]

資訊會因為不斷增加的互聯性(Interconnectivity)而呈指數的(Exponentially)擴散，行為者得以進一步利用全球化環境和媒體週期普遍性、資訊系統即時性和網路支持，以創建更大傳輸效果。[29] 混合性攻擊者能夠透過網路進行資訊控制，使其能夠在國內及國際論壇塑造（甚至創造虛構）有爭議的話語，以便對各種活動執行近似合理的否認，保護自己免受戰爭的真正代價。然而，在虛擬環境中，不論是友軍或敵軍都使用相同的節點(nodes)，這些節點難以被識別或保護。[30] 因此，混合性威脅能夠在承擔很小風險下，有效地塑造有利的敘事戰場。[31]

在混合性威脅脈絡下，形塑敘事的目標包含所屬人民、敵人軍隊和敵人平民以及國際輿論，其目的作為可以分為下列三種：

㈠情報作為

情報部門透過向全球新聞界「洩漏」(leaking)虛假文件和訊息，企圖欺騙目標國家的公眾或政治精英，破壞國家在國際社會的信譽和信任。[32] 如今的「沉默偽造」(silent forgeries)轉為主要透過網際網路的管道進行傳播，[33] 發布資訊的來源通常是一些「秘密理想主義舉報者」(secret idealistic whistleblower)或是「善意的舉報者」(well-meaning whistleblower)。[34] 然而，事實上，可能只是混合性對手所營造的虛假情境。

---

28 Agence France Presse,“US, Britain Blame Russia for‘Notpetya’Ransomware Attack,”*Agence France Presse*, 2018/2/16, <https://www.straitstimes.com/world/europe/us-britain-blame-russia-for-notpetya-ransomware-attack>（檢索日期：2019年4月26日）

29 Herbert Saurugg,“Hybrid Threat Potential in the Light of Networking and Systemic Thinking,”in Anton Dengg and Michael Schurian, ed., *Networked Insecurity-Hybrid Threats in the 21st Century* (Vienna: Schriftenreihe der Landesverteidigungsakademie, 2016), p. 81.

30 United Kingdom Ministry of Defence's Development Concepts and Doctrine Centre, *Strategic Trends Programme: Future Character of Conflict*, 2010, p. 12.

31 Emirates News Agency,“Hybrid Warfare Poses a Serious Threat to National Security, Say Defence Experts,”*Emirates News Agency*, 2018/6/7, <http://wam.ae/en/details/1395302693450>（檢索日期：2019年4月26日）

32 Alan Malcher,“KGB Active Measures and Russian Hybrid Warfare: A Brief Comparison,”*LinkedIn*, 2016/5/14, <https://www.linkedin.com/pulse/kgb-active-measures-russian-hybrid-warfare-brief-alan-malcher-ma?trk=aff_src.aff-lilpar_c.partners_pkw.10078_net.mediapartner_plc.Skimbit%20Ltd._pcrid.449670_learning&veh=aff_src.aff-lilpar_c.partners_pkw.10078_net.mediapartner_plc.Skimbit%20Ltd._pcrid.449670_learning&irgwc=1.>（檢索日期：2019年5月16日）

33 「沉默偽造」是指冷戰時期的一種傳播錯誤資訊的技術，將偽造的文件私下傳遞給外國政府但不向媒體提供。在最好的情況下，目標政府（偽造的政府旨在影響）接受偽造的文件是真實的，且不調查此事。政府偽造的文件聲稱從未瞭解它，因此無法否認其真實性。來源：Abram N. Shulsky and Gary James Schmitt, *Silent Warfare: Understanding the World of Intelligence* (Nebraska, Lincoln: Potomac Books, 2002), p. 15.

34 Horbulin Volodymyr,“‘*Active Measures*’ *of the Ussr against USA: Preface to Hybrid War: Analytical Report*”(Kyiv: The National Institute for Strategic Studies, 2017), p. 40.

㈡宣傳作為

混合性戰爭視「人民」為關鍵重心，為追求軍事目標，媒體在政府宣傳資訊上，扮演越趨重要的角色。在軍事單位上，政府透過控制資訊以保護部隊；在民間單位，媒體為追求訊息產出速度，不太審查官方來源，也不會核實報告中所述事實，使政府更加容易透過媒體推出虛假或誤導性敘述。混合性對手透過控制傳統媒體、社群媒體及偽造的網站，使資訊散播具有主動性，且增加人為可信度。

㈢影響民主進程

民主價值即在尊重不同的意見、價值觀與政策方針，採取開放的政黨競爭，由人民選擇支持政治理念與所屬黨派，最後以民意為基礎的狀況下組成政府。然而此體制卻在混合性威脅下成為脆弱性的關鍵因素。尤其國家內部遭遇社會或經濟產生變化時，爭議性議題引起人民意見相左，且難以取得雙方的共識，容易擴張社會的不和諧。[35]混合性威脅利用民主國家體制賦予人民的自由權，透過偽裝網站或「巨魔工廠」(troll factory)，製作並散佈虛假消息和照片，以加深政治分歧及煽動民族情緒，試圖顛覆及破壞遭鎖定的組織和國家，導致原有民主政體受到打擊。然而混合性攻擊者卻能利用網際網路的「匿名性」(anonymity)撇除責任關係。

參、演化中之混合性威脅對軍事任務影響

「混合性威脅」是一種複雜的混合體，混合性攻擊者透過強化一個或多個工具（垂直升級）或同步增加操作多種工具（水平升級），以實現更大綜合效果（如圖1）。[36]

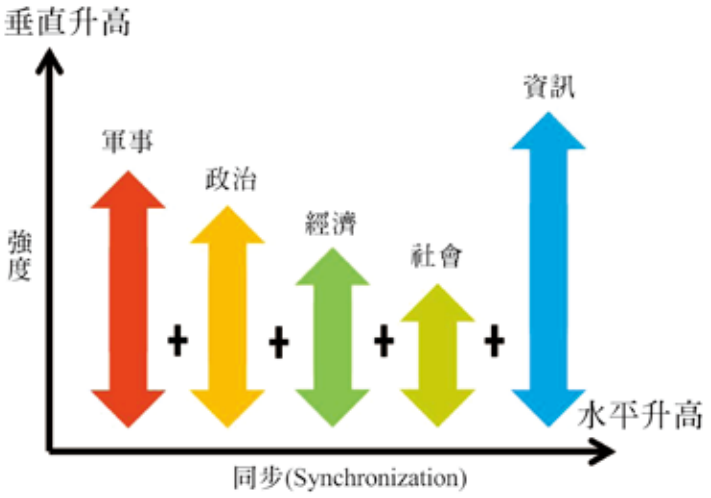

圖1　混合性威脅升高模式

資料來源：Patrick J. Cullen and Erik Reichborn-Kjennerud, *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare* (Oslo: Multinational Capability Development Campaign, 2017)

35 Christopher S Chivvis,“Hybrid War: Russian Contemporary Political Warfare,” *Bulletin of the Atomic Scientists*, Vol. 73, No. 5, 2017, pp. 4-5

36 Gregory F. Treverton, Andrew Thvedt, et al., *Addressing Hybrid Threats* (Stockholm: Swedish Defence University, 2018), p. 45.

然而，事實上，有些混合性威脅手段並非新穎，卻由網路空間賦予新工具，也創造新的機會。

此外，美國及北約比我國更早感知威脅之轉變，也因為面對「修正主義國家」的多樣化攻擊，轉變對於混合性威脅之態度與作法。本文參據美國與北約對於混合性威脅之認知及作法，供以我國面對威脅轉變後軍事任務調整之思考。

一、混合性威脅手段的演化

隨著安全環境的改變，混合性威脅的戰略目標在反對社會而非戰鬥人員，操作手法刻意模糊戰鬥人員和公民間界線，同時使用各種可能手段，從戰爭威脅到宣傳，以及介於兩者之間一切活動。再者，在動態資訊環境中，受眾不只是被動的閱聽者。反之，是參與其中並創造、傳播和放大的積極代理傳播者，往往在無意中推進宣傳者的想法。宣傳者透過廣告、操縱網際網路以及瞄準和煽動線上的群組，當消息（不論真實性）形成的漩渦夠大，即有機會吸引傳統媒體報導。一旦資訊透過人造草根(astroturfing)或殭屍網絡(botnest)放大模糊，[37]「看起來」像普通用戶的真實參與時，即成功模糊了真實與非真實之間的界限。

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。儘管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。

㈠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，使其能在許多國家塑造政治話語(political discourse)和民間敘事(popular narrative)，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。

㈡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。[38] 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」的文揭露，美國中央情報局(CIA)擁有龐大的

37 「人造草根」意旨偽造出一般民眾自動發出的評論來包裝，提出精心策劃的營銷或公關活動的欺騙行為；「殭屍網路」意旨受害電腦遭植入可遠端操控該電腦的惡意程式，即會像傀儡一般任人擺佈執行各種惡意行為。

38 C^4ISR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。

駭客武器庫，包括惡意軟體、病毒、木馬程式等，可用於攻擊手機、電話和其他數位設備。[39]

㈢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。

㈣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。[40] 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」。[41]

㈤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。[42] 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。

二、美國面對混合性威脅之回應

第二次世界大戰後，美國位居世界霸權的地位。隨著冷戰結束後，面臨日益混亂的全球安全環境，新興威脅挑戰出現及衝突原則大幅度改變，促使美國意識到其原有傳統軍事優勢正逐漸淡化，更須正視，並調整其應對的方針。

㈠美國實務上對混合性威脅之認知

美國國防部在選定戰略規劃文件中使用「混合」術語來闡明當前威脅。[43] 除了「混合」術語之外，有些美國國防部的單位採用「全頻譜作戰」(full spectrum operations)，例如《2010年陸軍野戰手冊第3-0號行動》

39 WikiLeaks,“Vault 7,” *WikiLeaks*, 2017, <https://buzzorange.com/techorange/2019/01/11/pdf-translation/>（檢索日期：2019年4月26日）

40 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.

41 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-south-china-sea>（檢索日期：2019年4月26日）

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

43 汪毓瑋，《情報、反情報與變革》（臺北：元照出版有限公司，2018年），頁43-44。

(Army Field Manual No. 3-0, Operations)將「全頻譜作戰」定義為一種作戰概念，在此概念下，陸軍部隊同時具有攻擊性、防禦性、穩定性或民事支援行動能力，作為相互依存的聯合部隊的一部分。[44]

2016年，美國《2035聯合作戰環境》強調混合性戰爭是一些「修正主義國家」(revisionist states)採用一系列強制性活動，[45]透過直接和間接方法的組合，減緩、誤導(misdirect)和鈍化(blunt)目標國，以促進其國家利益。其國家混合戰略的核心屬性將是物理和心理、動能和非動能、戰鬥員和非戰鬥員融合以及傳統和非常規方法的組合。[46]

㈡美國因應混合性威脅攻擊

在因應混合性威脅之攻擊，美國尤其側重於網路攻擊與防禦。例如，為了使國家更能應對所有網路威脅，必須促進夥伴關係，建立雙向資訊共享管道，聯邦調查局建立「全國網路調查聯合專案組」(National Cyber Investigative Joint Task Force)之平台，[47]鼓勵私營部門與當地聯邦調查局駐地辦事處建立關係，以有效分享情報。[48]

此外，美國也強調透過全球夥伴的網絡共同警覺、嚇阻與應對。2016年4月，美國為打擊國際恐怖組織與外國宣傳和假消息，建立「全球參與中心」(Global Engagement Center, GEC)，工作主要圍繞在研發、機構參與、合作夥伴參與及內容製作等四個核心領域。

三、北約因應混合性威脅之回應

北大西洋公約組織是20世紀成效最顯著的集體安全例子，成功對前蘇聯產生威懾作用。然而，冷戰結束已改變當前威脅性質，使北大西洋公約組織整體作用和使命發生變化。2010年，阿拉伯之春震撼中東世界的政治格局，[49]同時產生包含失敗國家、內亂、高端武器（甚至大規模殺傷性武器）的擴散，以及大規模難民潮等各種混合性威脅元素。2010年11月，北約重申新的「戰略概念」(strategic concept)，承諾制止與防範任何新興威脅，應對個別盟國或整個聯盟基本安全挑戰。[50]此種戰略概念被視為21世紀北約

44 Loretta Sanchez, *Hybrid Warfare* (Washington, DC: United States Government Accountability Office, 2010), p. 14.

45 在報告中，說明修正主義國家將越來越不滿意當前西方國家的國際秩序概念，並將俄羅斯、中國列為修正主義國家。其中，俄羅斯有可能通過自身作為首選安全合作夥伴，擴大其在東歐和中亞的影響力和控制力。在亞洲，中國可能會試圖削弱聯盟，並迫使鄰國承認其在該地區的霸權。

46 Frank G. Hoffman, *Hybrid Warfare and Challenges* (Washington, DC: National Defense University for National Strategic Studies, 2009), p. 39.

47 Amanda Ziadeh,“FBI Is Fighting Hybrid Cyberattacks,” *Government Cio Media*, 2018/3/1, <https://www.governmentciomedia.com/fbi-fighting-hybrid-cyberattacks>（檢索日期：2019年5月22日）

48 全國網路調查聯合專案組為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伴的機構。

49 2010年末至2011年初於北非突尼西亞所爆發的「茉莉花革命」(Jasmine Revolution)，為阿拉伯國家中第一場因人民起義導致推翻現政權的革命。接著，革命的情緒蔓延至其他阿拉伯世界國家，一些國家民眾紛紛走上街頭，要求推翻該國專制政體，而西方主流媒體稱之為「阿拉伯之春」。然而，截至2016年，只有一開始的突尼西亞成為阿拉伯之春中，唯一成功時線民主轉型的國家，其於國家則陷入長期動亂和戰爭。

50 NATO, *NATO 2020: Assured Security; Dynamic Engagement*, (Brussels: NATO Public Diplomacy Division, 2010), p. 8.

的戰略地圖。

為了做好準備因應混合性威脅，北約透過內部聯合情報和安全部門(the joint intelligence and security division)不斷收集、分享和評估資訊，以檢測和找尋出任何正在進行的混合性活動，改善聯盟國對於混合性威脅的理解和分析。此外，集體防禦仍然是北約最大責任，「威懾」是北約總體戰略的核心要素，其中包含防止衝突和戰爭、保護盟國、維護決策和行動自由等行動，保持靈活性，以最低限度的武力採用適當和專屬的方法應對各種挑戰。如果威懾失敗，北約也隨時進行「防禦」以保衛所有盟友，為此，北約部隊必須能夠以快速且靈活的方式回應新挑戰。

面對複雜挑戰的分析，歐盟和北約制定全面性途徑的戰略方針，融合所有相關行為者與現有工具：軍事力量、外交、人道主義援助、政治進程、經濟發展和技術。然而，對抗混合性威脅行動必須依賴非軍事政府和政府間機構、私營部門和國際非政府組織共同完成，歐盟的聯合溝通(EU's Joint Communication)與歐盟手冊均承認需與志同道合的夥伴進行對話和協調，以應對混合威脅。因而確立歐盟與北約在情勢警訊、戰略溝通、網路安全以及危機管理等領域有更加密切的合作（如圖2）。

混合性威脅同時操縱不同領域，以及橫跨實體與虛擬空間，較不易察覺。尤其在虛擬的網路空間，因難以驗證其歸屬，以致目標狀態複雜化。然而，每種手段功能及其使用程度，取決於行動者狀態的目標和目標所存在脆弱性。因此，在設想如何因應難以預測的混合性威脅時，現今的軍事任務必須有所調整。從美國及北約的作法中可歸結以下三點：

第一、透過即時共享訊息以及部門間的情報分享，在戰略溝通和回應方面進行合作。

第二、進行打擊混合性威脅的平行協調演習，提升網路安全和防禦。

第三、建構合作夥伴網絡，增加國防安

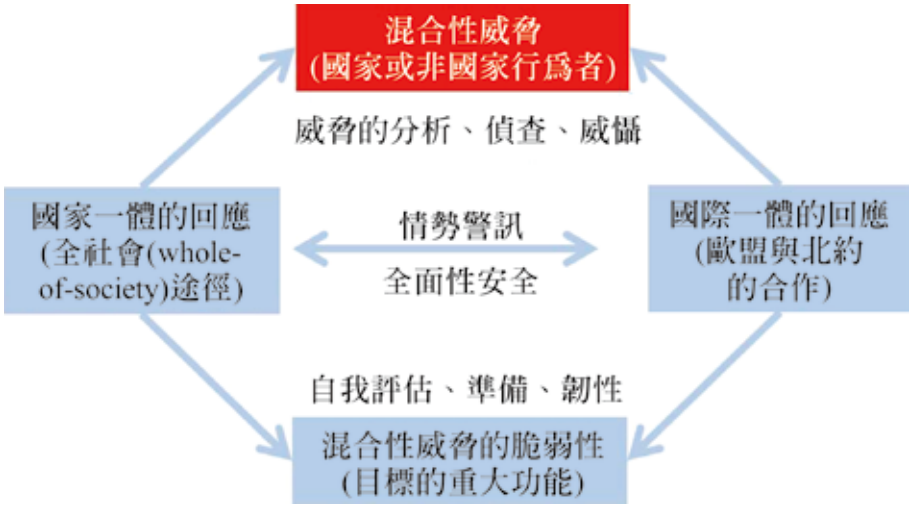

圖2　北約與歐盟應對混合性威脅的全面性途徑

資料來源：引用Axel Hagelstam and Kirsti Narinen, "Cooperating to Counter Hybrid Threats," *NATO Review Magazine*, 2018, <https://www.nato.int/docu/review/2018/also-in-2018/cooperating -to-counter-hybrid-threats/EN/index.htm>（檢索日期：2019年5月16日）

全能力。

肆、我國面對混合性威脅之思考

從過往經驗得知，目前國際環境單純施以傳統戰爭的機率降低的原因有二：第一，直接進行軍事干預，易被冠上「侵略者」之名而引起他國反感。在國際輿論的撻伐聲浪中，所施以制裁亦使侵略國在政治、經濟、社會等層面受到衝擊。第二，在衝突過程中，一旦原政權在遭受明顯可見的武力壓迫下，會激發國內人民的愛國情緒，採取激烈的對抗行為。兩相衝突下，引發重大人員傷亡，不僅在國際人權議題易受撻伐，且若不得民心，未來政權將會後患無窮。此外，對於屬於開放民主社會的我國而言，採用「混合性威脅」將會比非常規戰爭單一主題式的攻擊效果更佳，且攻擊成本更低。另外，我國與中共在族群、地理、文化、語言等方面相當接近，再加上之間存有長期的特殊對立關係，因此中共將我國作為施以影響工具的實驗場，再將其推廣至其他國家，成為攻擊美國等主要競爭對手的實驗場。[51]

一、我國所面對之混合性威脅

2015年11月，習近平更對軍事改革提出指導，於2016年1月，逐步落實軍委機關改制，且成立超越陸、海、空軍之新的「戰略支援部隊」。[52] 其扮演中共解放軍體系的「資訊傘」，負責支援其他軍種戰場作戰，在網路空間也能更有效率且更集中的對外展開「三戰」。[53] 因此，中共對於資訊運用的態度一改過去的網際網路封鎖策略，在許多領域技術優勢的基礎上，發起輿論戰，透過官方和非官方渠道在國際社會中宣傳其形象。[54] 在中共19大工作報告中更指出「強化戰略科技力量」且「將更加注重軍民融合，實現黨在新時代的強軍目標」。[55]

儘管中共施以混合性威脅橫跨多種領域，然而為清楚分析與說明，大致分為下列五個攻擊面向：

㈠假新聞

中共將原有人、時、地，加入虛構不實的內容，進而改變原本新聞內容的本意，在經過社群媒體的資訊分散性傳回我國，旨在對我國民主體制之運作帶來巨大傷害。另刻意操弄社會議題，加深政治分歧，同時煽動想法的分裂，分化我國社會凝聚力。其中，最常見的「數位輿論戰」手法是使用「內容農場」(Content Farm)散佈假消息。[56] 若

51 Chris Horton,“China Uses Taiwan as R&D Lab to Disrupt Democracies,” *Nikkei Asian Review*, 2018/12/27, <https://asia.nikkei.com/Politics/International-relations/China-uses-Taiwan-as-R-D-lab-to-disrupt-democracies>（檢索日期：2019年5月22日）

52 倪光輝，〈揭秘我軍首支戰略支援部隊〉，《人民日報》，2016年1月24日。

53 林穎佑，〈中共戰略支援部隊的任務與規模〉，《展望與探索》第15卷，第10期，2017年，頁102-122。

54 Ying Yu Lin,“China's Hybrid Warfare and Taiwan,” *The Diplomat*, 2018/1/13, <https://thediplomat.com/2018/01/chinas-hybrid-warfare-and-taiwan/>（檢索日期：2019年5月22日）

55 新華社，〈習近平：決勝全面建成小康社會—奪取新時代中國特色社會主義偉大勝利—在中國共產黨第十九次全國代表大會上的報告〉，《中華人民共和國中央人民政府》，2017年10月27日，<http://www.gov.cn/zhuanti/2017-10/27/content_5234876.htm>（檢索日期：2019年5月22日）

56 所謂「內容農場」是藉由吸引大量頁面瀏覽量，以獲取利潤的網站或公司。其先架設網站後，撰寫大量標題聳動、吸睛的文章，再經由其控制的帳戶透過通訊社群軟體進行宣傳，發送給廣泛的應用程序用

依攻擊目的，大致可分類為分化社會凝聚力、操弄政治敏感議題與干預選舉等三種。然而假新聞的流竄往往並非單一目的，可能同時包含多重目的性，或者僅是為增加假新聞的數量，使我國人民對於社會不再感到信任。例如：2018年9月4日，燕子颱風豪雨使關西國際機場被迫關閉，斷掉對外的聯繫。《人民網》6日指出「中國的大阪總領事館安排專車，將中國旅客與部分臺灣旅客優先送出機場」的消息，[57] 該報告在批踢踢(PTT)上流傳，輿論迅速發酵，有類似「讚嘆祖國強大」、「只要臺灣旅客承認自己是中國人也可以上車」等說法。[58] 引發我國民眾痛斥臺灣駐日代表處毫無作為。然關西機場發言人後來證實為「假新聞」。

㈡經濟影響

中共以經濟議題為籌碼換取政治、軍事利益已非新穎手段。然而，近年隨著資訊傳播快速，網民透過微信等社群平台，在商業行為上，鼓動中國大陸人民發起「抵制」不利中國大陸發展的企業。雖然沒有證據直接顯示中國大陸政府是否介入指導作為，然不可否認的是此種以民間發起的「經濟影響力」，以及新聞渲染力所造成的後果，往往會成功逼迫企業做出某些讓步，卻不會打擊到中國大陸政府對外的形象。例如2018年8月17日蔡總統過境美國洛杉磯期間，順道至當地「85度C」買咖啡，讓該品牌被標註為「臺獨企業」，遭大陸網友連聲抵制，使兩岸議題成功綁架商業。

㈢外交孤立

中共在外交上持續打壓我國生存空間，另配合假消息的散播，動搖我國與邦交國間的關係，以及引發我國民眾人心惶惶。2018年8月我國與薩爾瓦多斷交後，宏都拉斯遭網友點名是下個斷交國。雖然宏都拉斯駐臺大使謝拉(Rafa Sierra)一再表示「兩國雙邊關係穩定」闢謠。但如此接連斷交消息，仍引發我國民眾人心惶惶，憂慮是否將有「雪崩式斷交」的出現。

㈣軍事威懾

在傳統手段上，中共會藉由「文攻武嚇」方式，展示「不排除武力犯臺」之意圖，或在實施演訓時，故意去掉部分資訊，以沒有官方完整資訊的「半」假新聞，在特定時間釋放，使我國人民瞬間陷入高度緊張。例如：2018年4月12日中共透過官媒《環球時報》指出，本月18日早上8時～晚間12時，將在臺灣海峽進行實彈射擊軍事演習，引發關注。然事實上該公告的禁航區位於福建石獅靶場沿海，研判為中共解放軍部隊年度例行性火砲射擊訓練。

㈤秘密行動

中共直接對軍方情報招募外，亦可能資助和支持我國內部團體，包括親中政治團體或組織型犯罪集團，在議題上支持親中論

戶，再透過更多不經查證之閱聽者繼續轉發，吸引更多的「粉絲」進入該網站「按讚」。內容農場便可從Google、Facebook的廣告系統收取更高的廣告費，同時也掀起更大的「假新聞」共伴效應。

57 臺灣事實查核中心，〈【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救受困之中國旅客？〉，《臺灣事實查核中心》，2018年9月15日，<https://tfc-taiwan.org.tw/articles/150>（檢索日期：2019年4月26日）。

58 Keoni Everington,“Beijing-Based Ptt Users Spread Fake Osaka Airport Bus Story,” *Taiwan News*, 2018/9/17, <https://www.taiwannews.com.tw/en/news/3531772>（檢索日期：2019年4月26日）

述，或秘密吸收黨員，擴大其勢力，進而執行滲透、竊取機密資料之計畫。然而因為資助金流難以追查，不易確定中國大陸政府所扮演角色。例如2018年9月，《半島電視台》(Al Jazeera)發布調查紀錄片，內容描述我國內部遭到中共滲透的危機，其中「愛國同心會」坦承間接收受中國大陸資金。[59]

上述五類攻擊行為可得知，混合性威脅的不易歸屬性，使得原本看似單一領域的攻擊行為，卻同時與其他手段並行，採取針對對手量身訂製的全面性途徑之攻擊行為，接著透過網際網路的傳播效果加以渲染，使得全面性攻擊的效果能夠又深又廣。

二、我國軍事任務之未來發展

隨著威脅的不斷演化，應對混合性威脅的首要條件非僅限於新武器或硬體之研發與購置，而必須對威脅有新的理解，以及創新使用現有功能以應對新挑戰。2017年，《解放軍報》提出「致腦作戰」的想法，表明軍事對抗已從物理戰場擴展到認知戰場，從有形戰場擴展到無形戰場，有效影響對手認知，達到「不戰而屈人之兵」。[60]

儘管如此，「並非」意味著傳統軍事不再重要，傳統軍事武器是最基礎的力量，但軍隊應跳脫出過去傳統的防禦思維，不僅在內部進行合作，更需要跨領域的專家、智庫或組織進行合作，更甚者與國際間的合作夥伴共同面對，透過持續戰略風險評估，察覺混合性威脅的發展，於危機發生前予以適當對策或回應。因此軍事任務調整可分為三部分：

㈠以情報脈絡分析混合性威脅

面對混合性威脅同步且廣泛的操作手段，意味著我國政府必須採取「全面性途徑」感知威脅，然而其必須以有效的「情報」作為基礎。混合性威脅藉由同步操控多種工具，以達到更大的效果。所涉及工具橫跨多種領域且會相互影響。因此，需要全面性情報以利決策者在一系列潛在民事和軍事活動中，決定透過硬實力或軟實力予以回應（如圖3）。[61]為有效管理並整合情報，採取動態的「單一情報環境」(The Single Intelligence Environment)相當重要。

單一情報環境是一種支持「合作環境」(collaborative environment)的態度，因此不受環境或海上、陸地、空中、太空和網路等地理的限制。意味透過軍隊情報結構(military intelligence structure)與其他國家和國際間資訊及情報進行連接(interface)和應用，所構成整體空間、條件和環境，以此協助所有層級的決策者。簡言之，即將情報界的內外網路聯繫起來，以便有效地運作各種能力。[62]

此環境需要所有成員共同努力，充分利用傳統情報、監視和偵察(Intelligence, Surveillance and Reconnaissance, ISR)和資訊

59 中央廣播電臺，〈臺灣面臨中共全面滲透　外媒臥底揭露〉，《中央廣播電臺》，民國108年1月18日。

60 朱雪齡、曾華鋒，〈致腦作戰：未來戰爭競爭新模式〉，《解放軍報》，民國106年10月17日。

61 Herbert Saurugg, "Hybrid Threat Potential in the Light of Networking and Systemic Thinking," in Anton Dengg and Michael Schurian, ed., *Networked Insecurity-Hybrid Threats in the 21st Century* (Vienna: Schriftenreihe der Landesverteidigungsakademie, 2016), pp. 217-220.

62 Development Concepts and Doctrine Centre, *Understanding and Intelligence Support to Joint Operations* (London: United Kingdom Ministry of Defence, 2011), pp. 1-12.

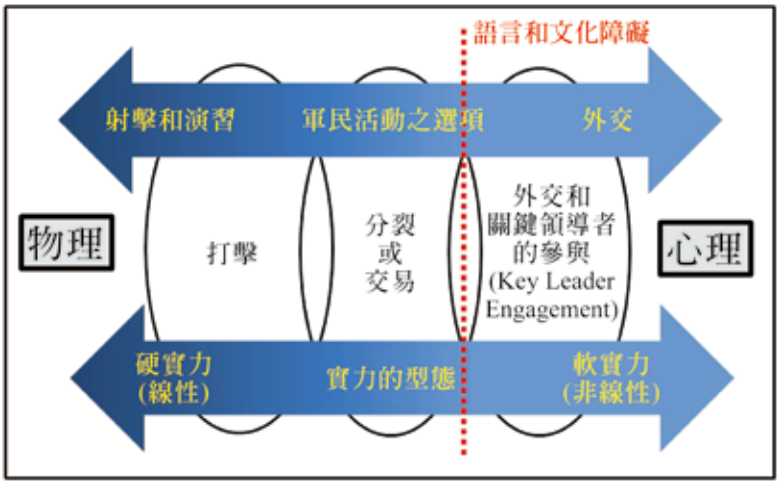

圖3　情報影響決策之光譜

資料來源：引用Herbert Saurugg, "Hybrid Threat Potential in the Light of Networking and Systemic Thinking," in Anton Dengg and Michael Schurian, ed., Networked Insecurity-Hybrid Threats in the 21st Century (Vienna: Schriftenreihe der Landesverteidigungsakademie, 2016)

系統，維持跨政府與多國聯繫，透過協調情報過程所有要素，包括情報專家、機構、資源和活動，以達最大成效。

㈡全面性途徑—全政府、全社會之概念

凡事一體兩面如同硬幣的正反概念，應對新興威脅採取「全面性」的混合攻擊模式。另一端最佳解決方法正是「全面性安全途徑」，即「全政府」[63] (whole-of-government)、「全社會」[64] (whole-of-society)之概念。

非政府組織(Non-Governmental Organization, NGO)和產業界在處理問題的經驗比起政府部門更豐富。事實上，商業界已經能成功有效打擊混合性威脅離散因素，且開發出創新技術因應具體的威脅和風險，然而這些技術並未得到廣泛共享。在這方面，民營企業的經驗對政府部門是非常具有價值的，且可以從這些專門科技中獲益匪淺。因此，軍事部門需要透過規劃和外界整合，以促進更多實質性的合作，而民間部門應是最須儘早被納入規劃範圍，規劃才會有加成的成果。軍方應儘早對外合作，給予民間部門

63 「全政府」是指公共服務機構在正式和非正式的跨組合邊界上工作，以實現共同目標和政府對特定問題的綜合響應。旨在實現政策一致性，以提高效率和效率。此方法是對部門主義的回應，不僅關注政策，還關注計畫和項目管理。資料來源：World Health Organization, *Contributing to Social and Economic Development: Sustainable Action across Sectors to Improve Health and Health Equity* (Geneva: World Health Organization, 2015), p. 3.

64 「全社會」是指承認所有相關利益攸關方，包括個人、家庭和社區、政府間組織和宗教機構、民間社會、學術界、媒體以及私營部門和工業界，在適當情況下所作的貢獻和重要作用，並認識到有必要進一步支持加強這些利益攸關方之間的協調，以提高這些努力的有效性。資料來源：United Nations General Assembly, *Political Declaration of the High-Level Meeting of the General Assembly on the Prevention and Control of Non-Communicable Diseases* (New York: United Nations General Assembly, 2012), p. 5.

必須的時間進行預算和其他準備工作，而非危機發生時才開始找尋可能需要的非軍事能力和夥伴。屆時情勢可能遠水救不了近火。[65]例如軍方協同資訊科技公司或電信業者，不僅能夠建立軍民雙方的良好溝通平台，更將民間業者如何防範網路攻擊之因應策略，或如何面對競爭對手進行黑函攻擊之危機處理模式等資訊藉由專業人才交換的方式帶回軍方。

在傳統威脅分析上，軍方除關注軍事層面的混合性威脅，更與民間專家和私營部門進行密切合作，協助處理政治、經濟、民用、資訊等層面的非傳統威脅分析，同時利用設立「假想敵」，設想混合性攻擊者將如何針對目標之軍事、政治、經濟、民用與資訊等領域的不同脆弱性訂製攻擊（紅色箭頭）。因此，透過分析可得知這些攻擊手段如何針對目標的特定脆弱性，制定出同步攻擊的組合（如圖4）。

從應對流程圖中可得知，所有步驟都環環相扣，國家必須採取全面性途徑「預為準備」、「建立韌性」，而「建立韌性」必須回到軍事、政治、經濟、民用與資訊等工具中，在這整個流程中，有效「情報」網路扮演著關鍵性重要角色。軍事部門必須向外發展，與民間專家及私營部門緊密合作，以假想敵的角度瞭解國家之脆弱性。

㈢提升韌性

「韌性」(resilience)意味著社會的不同層面，包括個人、家庭、社區、國家或地區，具有能力可承受、適應並迅速從壓力和衝擊中恢復，如自然災害、暴力或衝突。其

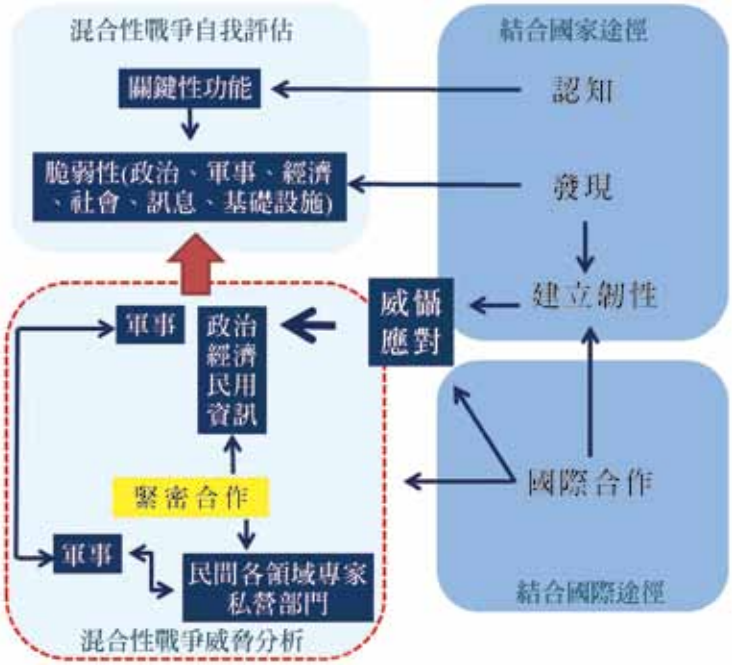

圖4　應對混合性威脅之流程圖

資料來源：參考Patrick J. Cullen and Erik Reichborn-Kjennerud, *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare* (Oslo: Multinational Capability Development Campaign, 2017)，內容部分修改。

65 Jens Stoltenberg, North Atlantic Treaty Organization, *Secretary General's Annual Report*, 2015, p. 18.

中，風險評估應透過威脅評估、脆弱性評估、影響評估等三個方法強化戰略情報：

1.威脅評估：此為戰略情報的主要角色。能夠透過全危害風險分析，找出關鍵資產清單中有興趣的潛在行為者。[66] 一旦確定那些角色構成威脅，接著必須衡量其動機和意圖與技術及分析能力，執行「假想敵」(Red Teaming)演習。[67]

2.脆弱性評估：國家內部具有一系列易受攻擊條件或系統運行中產生可被利用的弱點之處：為確保安全，須透過與各領域專家討論，進而瞭解現有關鍵性功能與其脆弱性，鑑定出可能行使這些脆弱性的威脅事件以及發生漏洞的後果，進而實現風險評估。

3.影響評估：採用先鑑定關鍵性資產受到衝擊後所產生的任務和業務成本，並評估可能尋求這些衝擊或後果之威脅來源。[68] 因為影響範圍廣泛且快速，關鍵基礎設施及運輸和通訊樞紐（如港口、機場等）控制將成為新衝突的重中之重。[69]

然而，提升韌性須不同的部門共同努力，且確保各自架構與資源是能夠互補與避免相互衝突。因此，政府須採取整合途徑(Integrated Approach)之緊急回應，緊急管理(Emergency management)又區分為準備、回應及恢復等三個階段。

軍方以「全政府途徑」為基礎，透過有效提供軍事能力和資源，增強國家防禦能力，協助各種破壞性事件的回應和復原。當國防部為保護國家免受外部軍事威脅以及應對國內危險和威脅，將擔任政府主管部門，由其他政府部門予以支持。反之，在應對國內韌性和安全挑戰時，國防部將定期為其他部門提供支持。舉例而言，一旦發生緊急情況或危機，當地緊急服務機構(Local Emergency Services)會做出第一回應；接著政府部門尋求軍事援助，協調其作為多機構回應的一部分，為當地回應者提供強而有力的支持。[70]

三、調整後所面臨之挑戰

混合性威脅是利用政府與社會的衝突或不信任感，同時透過政治與軍事指揮進行操作，不僅在處理危機的途徑有所調整，過去情報手段也隨之改變。然而在調整後仍有許多挑戰尚待克服。

㈠跨部會合作之適法性

民主國家相關的制衡機制(checks and balances)、官僚體制(bureaucracy)與各自為陣的機構(separated institutions)將使打擊混合戰爭行動複雜化，由於利益相關者多樣性及其各自的權益考量，統一指揮難以達成。[71] 此外，許多非政府組織拒絕以任何形式納入協

66 汪毓瑋，《恐怖主義威脅及反恐政策與作為》（臺北：元照出版社，2016年），頁389。

67 汪毓瑋，《情報、反情報與變革》（臺北：元照出版有限公司，2018年），頁38-39。

68 John Negroponte, *Strategic Cyber Intelligence* (Commonwealth of Virginia: Intelligence and National Security Alliance, 2014), pp. 9-10.

69 Björn Fägersten, "Forward Resilience in the Age of Hybrid Threats: The Role of European Intelligence," *Center for Transatlantic Relations*, 2017, <https://archive.transatlanticrelations.org/wp-content/uploads/2017/02/resilience-forward-book-fagersten-final-version.pdf>（檢索日期：2019年4月26日）

70 Development Concepts and Doctrine Centre, *Global Strategic Trends-out to 2045* (London: United Kingdom Ministry of Defence, 2014), pp. 165-168.

調戰略，特別是涉及軍方時，將違反在衝突時嚴格中立的原則。公部門機構也和民間企業參與者之間經常缺乏信任，國家對於聯盟層級之互動亦常有敏感之限制。[72]

㈡政策制定者不熟悉混合性威脅

決策者目光被社交媒體和趨勢描述吸引，以致無法在更深層次問題集中投入資源，無法有效解決問題。然而，當問題浮出檯面後，政策決定者希望情報部門在短時間提供全般的狀況，以供其作為決策判斷，或對選民大眾負責。由於難以評估對國家利益的損害和攻擊性網路的頻繁使用，情報部門要及時找到、相稱、合法和有識別性的答案變得更加複雜。[73]

㈢情報與媒體間的矛盾關係

長久以來，情報與媒體之間似乎存有微妙的矛盾關係。就廣義而言，情報和媒體工作雖都是負責收集、分析和傳播訊息，但在所有權（公共與私人）、接收者（政策制定者與民眾）和運作方式（封閉與開放）方面，兩個機構之間存在「關鍵性差異」，不過兩者功能仍存在彼此依賴。[74] 然而，隨著資訊時代所產生的「24小時新聞循環」(24 Hour News Cycle)，更多播出時間不等同於更周到或更準確的報導。此種追求「腥、羶、色」的報導趨勢，以致媒體未能更好地覆蓋情報或國家安全，反而讓新聞機構繼續關閉外派記者、削減預算、放棄經驗豐富的工作人員，較少關注情報和國家安全問題。與此同時，情報部門在充斥假消息的環境執行任務時，也遭遇挑戰。

㈣面臨情報執法相關問題

在打擊混合性威脅的各個面向，不斷強調情報之重要性，然而從程序和證據機制而言，「預防性戰略」要求現存的合法偵查和證據機制，必須在危機發生之前，就能夠採取檢控、干預的措施。然而，雖然為了有效打擊混合性威脅，必須制定相關情報蒐集立法，不能過分限制人民自由權，包括監視、線民、扣押、搜查、竊聽、逮捕、審問、拘留等在內的偵查活動。[75]

㈤動態的威脅環境變化

現今的威脅是動態的，隨著科技的進步或是各種不同的發展趨勢，將會改變原有的情報評估結果。在情勢警覺階段，感知威脅存時在應保持高度敏感性。

伍、結　　論

對我國而言，過去中共的「三戰」手法可歸類於非常規戰爭，但在新技術的發展下，非常規戰爭開始進行轉換為混合性威脅。雖然手段類型並非首見，在操作上卻有所不同。心理戰、輿論戰及法律戰同時相互運用於包含經濟、社會、軍事、外交等層

71 Gregory F. Treverton, Andrew Thvedt, et al., *Addressing Hybrid Threats*, p. 80.

72 Michael Miklaucic,“NATO Countering the Hybrid Threat,”*NATO Review Magazine*, 2011/9/23, <https://www.act.nato.int/nato-countering-the-hybrid-threat>（檢索日期：2019年4月26日)

73 Tobias Feakin,“*Developing a Proportionate Response to a Cyber Incident*,”*Council on Foreign Relations*, 2015/8, <https://www.cfr.org/report/developing-proportionate-response-cyber-incident>（檢索日期：2019年5月22日）

74 Robert Dover and Michael S Goodman, *Spinning Intelligence: Why Intelligence Needs the Media, Why the Media Needs Intelligence* (London: Hurst Publishers, 2009), p. 53.

75 汪毓瑋，《情報、反情報與變革》（臺北：元照出版有限公司，2018年），頁39-40。

面，更藉由資訊技術的發展，擴大三戰運用的效能。

此外，毛澤東思想核心之一的「人民戰爭」使用人民力量共同打擊對手。中共善用此種概念，透過更廣泛人民動員行動，在網際網路的意識形態，保護中共的決策與觀點，成為中共實施混合性威脅時最有利的手段。

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。

㈠混合性威脅發展之脈絡

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，混合性衝突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。但是，混合性攻擊者雖在削弱其對手能力時，不會超過可能引發軍事反應的既定門檻，卻可透過同步多個層面之手段進行升級，展現出比起傳統戰爭或非常規戰爭更大的效果。

㈡混合性威脅促使軍事任務調整之必要

混合性攻擊者得利於身分的轉化，使其所施以行為活躍於「紅線」以下灰色區塊。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。

（收件：108年6月10日，接受：108年10月28日）

參考文獻

中文部分

專書

汪毓瑋，2016。《恐怖主義威脅及反恐政策與作為》。臺北：元照出版社。

汪毓瑋，2018。《情報、反情報與變革》。臺北：元照出版有限公司。

黃秋龍，2004。《非傳統安全的理論與實踐》。臺北：法務部調查局。

期刊論文

林穎佑，2017/10。〈中共戰略支援部隊的任務與規模〉，《展望與探索》第15卷，第10期，頁102-122。

報紙

王中原，2015/9/15。〈觀察：為何歐洲難民危機是一場政治危機？〉，《BBC中文》。

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》。

倪光輝，2016/1/24。〈揭秘我軍首支戰略支援部隊〉，《人民日報》。

網際網路

新華社，2017/10/27。〈習近平：決勝全面建成小康社會—奪取新時代中國特色社會主義偉大勝利—在中國共產黨第十九次全國代表大會上的報告〉，《中華人民共和國中央人民政府》，<http://www.gov.cn/zhuanti/2017-10/27/content_5234876.htm>。

外文部分

官方文件

Development Concepts and Doctrine Centre, 2010. *Strategic Trends Programme: Future Character of Conflict*. London: United Kingdom Ministry of Defence, pp. 12, 22.

Development Concepts and Doctrine Centre, 2014. *Global Strategic Trends-out to 2045*. London: United Kingdom Ministry of Defence, pp. 165-168

Development Concepts and Doctrine Centre, 2015. *Future Security Challenges: Baltic Sea Regio*n. London: United Kingdom Ministry of Defence, p. 20.

IMSM-0292-2010, 2010/5/10. "Hybrid Threats Description and Context," *NATO Capstone Concept*, pp. 2-3.

North Atlantic Treaty Organization, 2010. *NATO 2020: Assured Security; Dynamic Engagement*. Brussels: NATO Public Diplomacy Division, p. 8.

Sanchez, Loretta, 2010. *Hybrid Warfare*. Washington, DC: United States Government Accountability Office, p. 14.

Stoltenberg, Jens, 2015. *Secretary General's Annual Report*. Brussels: North Atlantic Treaty Organization, p. 18.

United Nations General Assembly, 2012. *Political Declaration of the High-Level Meeting of the General Assembly on the Prevention and Control of Non-Communicable Diseases*. New York: United Nations General

Assembly, p. 5.

World Health Organization, 2015. *Contributing to Social and Economic Development: Sustainable Action across Sectors to Improve Health and Health Equity*. Geneva: World Health Organization, p. 3.

專書

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

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

Hoffman, Frank G., 2009. *Hybrid Warfare and Challenges*. Washington, DC: National Defense University for National Strategic Studies.

Joint Irregular Warfare Center and US Joint Forces Command, 2011. *Irregular Adversaries and Hybrid Threats. An Assessment-2011*. Washington, DC: Government Printing Press.

Krulak, Charles C., 1997. *The Three Block War: Fighting in Urban Areas*. Washington, DC: National Press Club.

Negroponte, John, 2014. *Strategic Cyber Intelligence*. Commonwealth of Virginia: Intelligence and National Security Alliance.

Sari, Aurel, 2018. *Blurred Lines: Hybrid Threats and the Politics of International Law*. Helsinki: Hybrid CoE.

Shulsky, Abram N. & Schmitt, Gary James, 2002. *Silent Warfare: Understanding the World of Intelligence*. Nebraska, Lincoln: Potomac Books.

Treverton, Gregory F., Thvedt Andrew, Chen, Alicia R., Lee, Kathy & McCue, Madeline, 2018. *Addressing Hybrid Threats*. Stockholm: Swedish Defence University.

Volodymyr, Horbulin, 2017. *'Active Measures' of the Ussr against USA: Preface to Hybrid War: Analytical Report*. Kyiv: The National Institute for Strategic Studies.

Wæver, Ole, 1993. *On Security*. New York: Columbia University Press.

專書論文

Saurugg, Herbert, 2016. "Hybrid Threat Potential in the Light of Networking and Systemic Thinking," in Anton Dengg and Michael Schurian, ed., *Networked Insecurity-Hybrid Threats in the 21st Century*. Vienna: Schriftenreihe der Landesverteidigungsakademie, pp. 81, 217-220.

期刊論文

Bērziņš, Jānis, 2014. "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy," *Policy Paper*, Vol. 2, p. 5.

Chivvis, Christopher S., 2017. "Hybrid War: Russian Contemporary Political Warfare," *Bulletin of the Atomic Scientists*, Vol. 73, No. 5, pp. 4-5.

Cilluffo, Frank J. & Clark, Joseph R., 2012. "Thinking About Strategic Hybrid

Threats-in Theory and in Practice,” *Prism*, Vol. 4, No. 1, p. 49.

Fedyk, Nicholas, 2016. “Russian ‘New Generation’ warfare: Theory, Practice, and Lessons for Us Strategists,” *Small Wars Journal*, p. 2.

Lanoszka, Alexander, 2016. “Russian Hybrid Warfare and Extended Deterrence in Eastern Europe,” *International affairs*, Vol. 92, No. 1, pp. 190-192.

Mattis, James N. & Hoffman, Frank, 2005. “Future Warfare: The Rise of Hybrid Wars,” *Proceedings-United States Naval Institute*, Vol.131, No. 11, p. 12.

Neag, Mihai Marcel, 2016. “A New Typology of War-the Hybrid War,” *Land Forces Academy Review*, Vol. 21, No. 1, p. 15.

Popescu, Nicu, 2015. “Hybrid Tactics: Neither New nor Only Russian,” *EUISS Issue Alert*, Vol. 4, p. 1.

Thiele, Ralph, “Hybrid Threats: And How to Counter Them, 2016.” *ISPSW Strategy Series: Focus on Defense and International Security*. Vol.448, pp. 10-11.

Veljovski, Gjorgji, Taneski, Nenad & Dojchinovski, Metodija, 2017. “The Danger of ‘Hybrid Warfare’ from a Sophisticated Adversary: The Russian ‘Hybridity’ in the Ukrainian Conflict,” *Defense & Security Analysis*, Vol. 33, No. 4, pp. 292-306.

網際網路

Agence France Presse, 2018/2/16. “US, Britain Blame Russia for ‘Notpetya’ Ransomware Attack,” *Agence France Presse*, <https://www.straitstimes.com/world/europe/us-britain-blame-russia-for-notpetya-ransomware-attack>.

Barno, David, 2014/7/23. “The Shadow Wars of the 21st Century,” *War on the Rocks*, <https://warontherocks.com/2014/07/the-shadow-wars-of-the-21st-century/>.

Emirates News Agency, 2018/6/7. “Hybrid Warfare Poses a Serious Threat to National Security, Say Defence Experts,” *Emirates News Agency*, <http://wam.ae/en/details/1395302693450>.

Everington, Keoni, 2018/9/17. “Beijing-Based Ptt Users Spread Fake Osaka Airport Bus Story,” *Taiwan News*, <https://www.taiwannews.com.tw/en/news/3531772>.

Fägersten, Björn, 2017. “Forward Resilience in the Age of Hybrid Threats: The Role of European Intelligence,” *Center for Transatlantic Relations*, <https://archive.transatlanticrelations.org/wp-content/uploads/2017/02/resilience-forward-book-fagersten-final-version.pdf>.

Feakin, Tobias, “Developing a Proportionate Response to a Cyber Incident,” Council on Foreign Relations, 2015/8, <https://www.cfr.org/report/developing-proportionate-response-cyber-incident>.

Hagelstam, Axel and Kirsti Narinen, 2018. “Cooperating to Counter Hybrid Threats,” *NATO Review Magazine*, <https://www.nato.int/docu/review/2018/also-in-2018/cooperating-to-counter-hybrid-threats/EN/index.htm>.

Horton, Chris, 2018/12/27. “China Uses Taiwan

as R&D Lab to Disrupt Democracies," *Nikkei Asian Review*, <https://asia.nikkei.com/Politics/International-relations/China-uses-Taiwan-as-R-D-lab-to-disrupt-democracies>.

Lin, Ying Yu, 2018/1/13. "China's Hybrid Warfare and Taiwan," *The Diplomat*, <https://thediplomat.com/2018/01/chinas-hybrid-warfare-and-taiwan/>.

Malcher, Alan, 2016/5/14. "KGB Active Measures and Russian Hybrid Warfare: A Brief Comparison," *LinkedIn,* <https://www.linkedin.com/pulse/kgb-active-measures-russian-hybrid-warfare-brief-alan-malcher-ma?trk=aff_src.aff-lilpar_c.partners_pkw.10078_net.mediapartner_plc.Skimbit%20Ltd._pcrid.449670_learning&veh=aff_src.aff-lilpar_c.partners_pkw.10078_net.mediapartner_plc.Skimbit%20Ltd._pcrid.449670_learning&irgwc=1>.

Miklaucic, Michael, 2011/9/23. "NATO Countering the Hybrid Threat," *NATO Review Magazine*, <https://www.act.nato.int/nato-countering-the-hybrid-threat>.

Pawlak, Patryk, 2015/6/24. "Understanding hybrid threats," *European Parliamentary Research Service Blog*, <https://epthinktank.eu/2015/06/24/understanding-hybrid-threats>.

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

WilkiLeaks, 2017. "Vault 7," *WilkiLeaks*, <https://buzzorange.com/techorange/2019/01/11/pdf-translation/>.

Ziadeh, Amanda, 2018/3/1. "FBI is Fighting Hybrid Cyberattacks," *government Cio Media*, <https://www.governmentciomedia.com/fbi-fighting-hybrid-cyberattacks>.