財團法人國防安全研究院
Institute for National Defense and Security Research

中華民國 109 年 7 月 10 日　　第 3 期

國防情勢特刊

不對稱戰的演變與發展特輯

⊙ NUMBER 3 ⊙ JULY 10, 2020 ⊙

Defense Situation Special Edition Vol 3

The Evolution & Development of Asymmetric Warfare

⊙ NUMBER 3 ⊙ JULY 10, 2020 ⊙

編輯報告

馬拉松賽跑起源於公元前5世紀的的希波戰爭，雅典在馬拉松戰役，放棄傳統均衡方陣，改採強化兩翼創新戰法，擊敗人數優勢的波斯軍。雅典將領的指揮藝術扭轉了兵力對比的戰場方程式，也改變希波戰爭的發展格局，在作戰與戰爭層面都展現了不對稱的效應。

而在21世紀的今日，關於「不對稱戰」(asymmetric warfare)或「不對稱作戰」(asymmetric operation)、甚至「不對稱衝突」(asymmetric conflict)等概念仍有不同的定義及論述，也就是在國家層級、戰爭層級、戰役層級、作戰層級、乃至戰術層級皆有不同論者。

同時，也有論者以為資訊戰、金融戰、乃至心裡戰等非軍事手段的運用才是屬於不對稱戰的範疇。實際而言，容或由廣義、狹義的角度來看待，以及所採取的 「途徑」(approach)為何，便可較清楚的予以區隔。

本期特題由不同的層級、途徑等面向切入，試著描繪不對稱競爭在不同層級的可能邏輯思考以及樣貌，以提供可能的觀察定位與參考。可以這麼說，不對稱是競爭雙方的相對論，基本原理就如同軍事理論所強調的節約與集中原則，強調的是在資源有限的情況下讓戰力最大化，以求取最高的成功公算。

也如同天平兩端的不對稱砝碼，可以透過支點的調節重行平衡甚至改變輕重砝碼的位置。準此，改變戰場上的支點，發揮戰略槓桿效應以改變敵我競爭的優劣元素，進而產生決定性效果。不對稱效益的發揮，就成為政軍決策菁英、以及戰場管理者在和戰經營、總體競爭力投資、風險管理等方面所需思考的藝術。

21 世紀不對稱戰思維的發展

李哲全

國家安全與決策研究所

壹、前言

「不對稱戰」（asymmetric warfare）自古有之。許多戰役並非勢均力敵，倚強凌弱、以弱勝強的戰爭或衝突所在多有。因此，「不對稱戰」反映的是對陣雙方的強弱、大小、先後、高低等差距，以及圍繞這些客觀現實的戰略、戰術、戰具各層級手段與能力的彈性與創新運用。不論強國或弱國，都希望透過「不對稱戰」的策略與行動，實現其最大利益。本文將扼要探討911事件後美國與中國有關「不對稱戰」的理論與思維發展，及其對軍事戰略與實務的影響。

貳、911 事件後美中的「不對稱戰」研究

冷戰時期的國際權力格局，是以美國為首的北約組織，和蘇聯主導的華沙集團之間的核子與傳統武力集團的對峙。雙方軍事思維在於因應單一明確的高強度威脅，不對稱的探討並非研究的主流。[1]冷戰結束蘇聯瓦解後，美國國防重心轉而關注分散且不確定的低強度威脅，其官方文件開始探討「不對稱戰」概念及其對美國海外或本土利益的可能影響，並開啟1990年代「不對稱戰」的研究風潮。[2]

---

[1] 1975 年邁克（Andrew J. R. Mack）以相對性的概念詮釋不對稱衝突的勝負，是早期「不對稱戰」研究的代表。他主張相對權力（Relative Power）較強的一方，在小規模衝突的相對利益（Relative Interest）較弱（因不會危及生存），相對決心（Relative Resolve）也較弱，但其相對政治脆弱性（Relative Political Vulnerability）則較高，政治菁英與民意通常不希望陷入持久戰與消耗戰的泥沼。而實力較弱的一方，由於戰事勝敗攸關生存，故常有非贏不可的決心。請見 Andrew J. R. Mack, "Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict," *World Politics*, Vol. 27, No. 2, January 1975, pp. 175-200.

[2] 1995 年 11 月美國參謀首長聯席會議在《美國武裝部隊的聯合作戰》（*Joint Warfare of the Armed Forces of the United States*）報告中，首度提出「不對稱戰」概念，並以波灣戰爭為例，解釋如何發揮聯合部隊的不對稱作戰能力，以武裝直升機打擊伊拉克坦克。1997 年美國的《四年期國防總檢討》（*Quadrennial Defense Review*）則指出，美國在傳統軍事領域的優越地位，可能會

一、美國的「不對稱戰」研究

911事件前，「不對稱戰」概念雖已提出，但受重視的程度仍然不高。2001年911事件的發生，讓美國政府體認到，多年來賴以維繫國家安全的嚇阻戰略並未發揮作用。華府決策者對內迅速調整國家安全優先順序、整頓國土防衛的組織架構，對外則積極建立國際反恐聯盟，並以反恐之名，發動阿富汗反恐戰爭與第二次波斯灣戰爭。美國智庫也推出許多研究報告，探討面對不對稱威脅時的因應之道。[3]

911事件是典型的不對稱攻擊。它完全符合不對稱戰「不尋常、非正規、不合法、與敵方戰力不相匹配或無法抗衡、難以回應或根本無法回應，以及以小搏大」的所有特徵。[4]恐怖主義的思考，確實符合「不對稱戰」思維；但恐怖主義不等於「不對稱戰」，二者之間仍有區別。學者陳偉華指出，「不對稱戰」多探討交戰雙方在力量不均等或軍事作為不相當的情況下，基於強弱能力不對稱的差異，運用傳統作戰範疇以外的戰略與戰術作為贏取勝利。恐怖主義則通常是弱勢的一方採取戰術運用，而形成不對稱的衝突。恐怖份子通常效命於某些黨派，往往具有強烈的政治訴求，或受宗教狂熱驅動，不但不受道德

使對手採取不對稱手段，攻擊美國在海外或本土的軍隊與利益。請見 Steven Metz & Douglas V. Johnson, *Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts*, （ CreateSpace Independent Publishing Platform, January 2001), P.5, https://apps.dtic.mil/dtic/tr/fulltext/u2/a387381.pdf.

[3] 911 事件後，美國軍方與智庫針對恐怖主義的重要研究報告包括：2002 年美國戰略與國際研究中心（CSIS）公布《防衛美國的新途徑》（*The New American Approach to Defense：The FY 2003 Program*），從不對稱戰爭、反恐行動、本土防衛與軍力轉型等角度，探討美國國家安全。2003 年布魯金斯研究院（Brookings Institution）公布《保護美國本土》（*Protecting the American Homeland: One Year On*）報告，從大戰略思考美國境內重要目標的防護、國防架構重整，及預算分配等面向，探討美國面對不對稱威脅時的因應之道。請見 Anthony H. Cordesman, *Terrorism, Asymmetric Warfare, and Weapons of Mass Destruction: Defending the US Homeland* （Washington DC.: Center for Strategic & International Studies, 2002), pp.1-6; I.M. Destler, David Gunter, James Lindsay, Michael E. O'Hanlon, Peter R. Orszag, James B. Steinberg, and Ivo H. Daalder, *Protecting the American Homeland: One Year On*, （Washington DC.: Brookings Institution, January 1, 2003), https://reurl.cc/rxjQr1.

[4] 學者藍巴凱斯（Steven J. Lambakis）認為，「不對稱性」通常具備不尋常（unusual）、非正規（irregular）、不合法（unlawful）、敵我雙方戰力不能匹敵或無法相抗衡（unmatched）、難以回應或根本無法回應（例如以大規模正規部隊應付游擊戰）及以小搏大、攻擊致命重心（center of gravity）等特質。Steven Lambakis, "Reconsidering Asymmetric Warfare," *Joint Force Quarterly*, Issue 36, December 2004, pp. 102-108.

法律限制，且經常以傷及無辜為影響對手的手段。這些都超出911事件前「不對稱戰」研究的內容。[5]

「不對稱戰」的研究雖多，但因缺乏嚴謹與一致的定義，及指涉的軍事與準軍事策略、行動與思維幾無邊際，使相關研究有詞彙濫用或標新立異的批評（將在下一節討論）。更艱難的挑戰在於，911後。美國由冷戰時期的「核子嚇阻」戰略，調整為「先制攻擊」戰略，希望在恐怖攻擊發動前，予以先制摧毀。但這種策略造成美國在不確定目標上投入大量資源，既難有效嚇阻，亦難將對手一舉殲滅；其次是「不對稱戰」的對象經常涉及無辜百姓及較具戰略意義的非軍事設施，為有效因應不對稱威脅，決策者經常被迫採取在道德文化上不恰當卻又不得不為的作法。「不對稱戰」已對民主國家構成嚴峻挑戰。

二、中國的「不對稱戰」研究

中共並未正式將「不對稱戰」納入其軍事戰略，但對「不對稱戰」相關理論十分重視並積極研究，且落實在戰略、戰術與戰法的運用及不對稱戰力的建構上。[6]中共深知，解放軍在軍事科技及武器裝備上，相較美軍仍居於劣勢。只有訴諸非常態作戰方式與手段，才有可能贏取勝利。[7]郭武君在《解放軍報》撰文指出，「在可預見的一個時期內，武器裝備敵（美）優我劣的狀況還不能從根本上改變，只有在發揮主觀能動性上高敵一籌，才有可能戰勝敵人」。[8]

1999年2月，喬良與王湘穗兩位解放軍大校合著的《超限戰》，被美軍視為典型的「不對稱戰」。該書指出，戰爭是生死存亡之事，

[5] 請見陳偉華，〈「不對稱作戰概念」與「不對稱戰力建構」關係之研究〉，《國防雜誌》，第25卷第4期，2010年，頁11-12。

[6] 陳偉華教授指出，中共在「不對稱作戰」研究上，2000年以前偏重作戰方式的討論；之後逐漸朝向戰役與戰略層次發展，但對理論化與概念化則無特別著墨。請見陳偉華，〈「不對稱作戰概念」與「不對稱戰力建構」關係之研究〉，頁12-14。

[7] 沈明室，〈評中共「超限戰」〉，《共黨問題研究》，第 26 卷第 3 期，2000 年 3 月，頁 52-56。

[8] 郭武君，〈呼喚不對稱軍事理論研究〉，《解放軍報》，2000 年 12 月 19 日。

因此要超越一切界線和限度。在「超限戰」思維下，戰場無所不在，一切武器和技術都可任意疊加，軍事與非軍事的界限要全部打破。美國學者巴奈特（Thomas Barnet）指出，「超限戰的第一條規則就是沒有規則，不受任何限制」，其內容與「不對稱戰」精神完全相符。[9]

作為科技後進國，中共也積極探討從「高技術戰爭」與「信息戰」的方向，爭取彎道超車、壓制美軍的可能性。美國國防部發布的「中國軍力報告書」自不會漏掉這些發展與思維。早在2007年，蘭德公司（RAND Corporation）即在《深入龍潭：中共拒止戰略對美國的意義》（*Entering the Dragon's Lair: Chinese Anti-access Strategies and Their Implications for the United States*）報告中明確指出，中共試圖利用網路滲透、病毒與駭客方式，侵入美國軍方電腦，並稱這是極易成功遂行「不對稱戰」的有利方式。[10]

參、「不對稱戰」研究的限制

一、缺乏普遍性定義

學界對於「不對稱戰」有各種詮釋，但迄今尚無普遍為各方接受的定義。這與「不對稱戰」強調的相對概念，及非傳統、非正規、超乎想像的特質有關，911事件打破基本的法律與道德規範，更加深定義「不對稱戰」的困難。儘管如此，我們可以參酌各方定義，歸納出「不對稱戰」的共同特點包括：（一）迴避或削弱對手的優勢，並以己方強項，選擇性攻擊對手弱點；（二）使用超乎預期、非傳統、創新手段進行攻擊或防衛；（三）在軍事或財政投資效果上，帶來超高效益。[11]

---

[9] 蔡昌言、李大中，〈不對稱戰爭相關理論及其應用於中國對鼎戰略之研析〉，《遠景基金會季刊》，第8卷第3期，2007年7月，頁25。

[10] Roger cliff, Mark Burles, Michael S. Chase, Derek Eaton, and Keven L. Pollpeter, *Entering the Dragon's Lair: Chinese Antiaccess Strategies and Their Implications for the United States* （Santa Monica, LA: RAND, 2007), p.55.

[11] 請見Franklin B. Miles, *Asymmetric Warfare: An Historical Perspective*（Carlisle, Pa.: US Army War College, 1999）, pp.3-4; Robert M. Cassidy著，國防部史政編譯室，《俄羅斯於阿富汗與車臣藏

有許多研究特別強調「不對稱戰」的操作層面，也就是如何透過上述（二）與（三），達到克敵制勝的效果。例如，不對稱威脅可來自科技與武器，如無人機或遠超乎對手的強大武器或平台，也可能來自非軍事層面，例如採取恐怖主義、人肉盾牌或種族清洗等手段。端看對陣雙方如何透過戰略、戰術、戰法的設計，以及巧妙運用有限的資源，投注到科技與武器（戰力）的研發及建構上。

二、無限組合的不對稱威脅

藍巴凱斯（Steven J. Lambakis）從科技、文化與心理三個層面進行分析，指出在「不對稱戰」思維下，強大的一方未必佔有絕對優勢，弱小的一方也未必只能俯首稱臣。戰場上高科技是優點，但也有其要害。若對手能集中資源，箝制其阿基里斯腳跟（Achilles' Heel），便可扳倒具備軍事科技優勢的敵人。例如以駭客手段癱瘓對手的電腦與通訊系統、以飽和式自殺攻擊（如無人機蜂群戰術）進襲獨重防空飛彈的現代船艦等。在文化上，西方民主國家的民意、輿論及政治人物對戰場死傷的敏感度，相對於伊斯蘭戰士視死如歸或毛澤東的人海戰術，都可能提供「不對稱戰」的施展空間。心理層面上，恐怖攻擊、宣傳戰、心理戰或拖延戰等手段，也是「不對稱戰」戰場上，特別是弱勢方可用以瓦解對手意志，消耗其耐心毅力的手段。[12]

班奈特（Roger. W. Barnet）指出，強大的西方民主國家，如美國，在實施嚇阻戰略及對敵作戰上，經常面臨作戰、組織、法律及道德等四大層面的限制。例如，美國立國以來的戰略守勢，抑制了奇襲策略的可能性；民意與媒體監督及顧慮特殊武器殺傷性的後遺症，也是讓

軍事戰略文化與不對稱衝突》〈Russia in Afghanistan and Chechnya: Military Culture and the Paradoxes of Asymmetric Conflict〉，（台北：國防部史政編譯局），頁7-8; "The Security Situation in the Taiwan Strait," Department of Defense, USA, February 1, 1999, https://reurl.cc/R4gKZ9.

[12] Steven J. Lambakis 著，黃淑芬譯，〈不對稱戰爭的再思考〉(Reconsidering Asymmetric Warfare)；蔡昌言、李大中，〈不對稱戰爭相關理論及其應用於中國對臺戰略之研析〉，《遠景基金會季刊》第 8 卷第 3 期，2007 年 7 月，頁 10。

美軍對武器系統的使用自我設限的作戰限制。行政與立法部門的戰爭決策權問題、美國對盟國動向與維繫聯盟團結的考量，及美國的外交孤立主義傳統等，都是美國在反制對手時組織上的限制。而美國接受傳統的義戰（Just War）、戰爭法（Jus in Bello）及武力使用之國際法（Jus ad Bellum），及軍備管制等國際公法與條約的指導或限制，也使美國遵循目的比例原則、區分軍事與平民目標原則、武力做為最後手段，及先制與預期性自衛（Anticipatory Self-defense），這些都是法律層面構成的限制。在道德與價值層面，關於戰爭目標與手段的關聯性、社會大眾企求和平與厭惡戰爭的傾向，也都限制了美國的作為。[13]以上因素不只適用於美國，也對其他國家構成一定程度的限制，只是影響程度因各國的軍力、科技、文化、心理與法規等條件而有不同。

卡西迪（Robert M. Cassidy）則針對俄羅斯在車臣與阿富汗戰場的案例，探討戰場上的優勢者（俄國）與其弱勢對手（車臣與阿富汗），在「不對稱戰」形態下的戰略目標、戰術手段、武器與科技、意志力與內部凝聚程度、軍事文化，及時空概念等六組二元情境，進行對比分析，作為未來美國用兵時的借鏡。[14]以下即歸納前述研究觀點，綜整「不對稱戰」下，傳統強弱兩方可能面臨的優勢與劣勢，及其可能採取的手段如下表。

[13] Roger. W. Barnet著，國防部史政編譯室譯，《不對稱作戰：當前美國軍力面臨之挑戰》（Asymmetrical Warfare: Today's Challenge to U.S. Military Power）（臺北：國防部史政編譯室，2005 年）。

[14] 卡西迪在書中針對對陣雙方實力懸殊下，在戰略目標、戰略手段、武器與科技、意志力與內部凝聚程度、軍事文化，及在時間與空間的概念等六種情勢下的優勢與劣勢分別進行分析。請見Robert M. Cassidy著，國防部史政編譯室譯，《俄羅斯於阿富汗與車臣：軍事戰略文化與不對稱衝突》（*Russia in Afghanistan and Chechnya: Military Culture and the Paradoxes of Asymmetric Conflict*)（臺北：國防部史政編譯室，2004 年），頁11。

表1、「不對稱戰」下的優劣勢分析

本質	傳統優勢方	傳統劣勢方
戰略目標	有限度的戰爭（因其相對權力較強，在較小規模衝突的相對利益與相對決心較弱，相對政治脆弱性較高，通常不會進行全面軍事動員）。	總體戰（戰爭的結果是生死存亡關鍵，願動員所有資源）。
戰術手段	相對較多，但受到作戰、組織、法律及道德等因素限制。 傾向克勞塞維茲式的正規與直接作戰手段。	相對有限，但可採取避敵之鋒、間接戰鬥、打帶跑拖延持久戰術等手段消耗對手。 傾向毛澤東間接式手段，著重游擊戰、重機動性、奇襲與彈性、政治與軍事合一、將戰力隱藏於社會之中，使敵人無法區分平民與戰鬥人員。
科技與軍備	優勢，發展新進科技與武器制敵，但存在弱點。	劣勢，但可運用不對稱策略抵消對手的優勢。例如，集中資源攻擊敵方的脆弱點，例如電腦與通訊系統，若成功則可在瞬間扳倒強大對手；或投注資源建構具備不對稱優勢的武器或裝備。
心理與精神	有條件投入戰爭。領導者與民意、輿論對死傷的敏感度高，戰場受挫承受力較弱。	相對無條件投入戰爭。願以較大代價換取勝利、社會內部對戰場死傷的忍耐程度較高。 可能採取恐怖攻擊、拖延戰等手段，消耗對手耐心、瓦解對手意志。
文化與道德	民主國家民意、輿論與政治人物對戰場死傷敏感度較高。 企求和平、厭惡戰爭的文化與價值觀。	伊斯蘭戰士的視死如歸、毛澤東的人海戰術，是可能運用的手段。
時間與空間	集中、快速。戰場上重視整體數量優勢以發動進攻，常因後勤補給，而落入集中與分散的兩難。	分散、延長。傾向以空間換取時間，拉長戰線、重視局部優勢的形成，採取分散與孤立對手、各自擊破等手段。

資料來源：作者在Robert M. Cassidy著，國防部史政編譯室譯，《俄羅斯於阿富汗與車臣：軍事戰略文化與不對稱衝突》（*Russia in Afghanistan and Chechnya: Military Culture and the Paradoxes of Asymmetric Conflict*），頁11表格的基礎上酌修，並納入其他學者見解綜整製表。

肆、結語

「不對稱戰」領域沒有絕對的贏家。就兩岸問題而言，若中共試圖以非和平方式解決台灣問題，中南海與解放軍領導人，將面臨「雙重不對稱戰」的情境。

以兩岸而言，為避免以美國為首的國際社會介入，中共可能規劃以其強大軍力，打一場強勢的「不對稱戰」，試圖在短時間內挫敗甚至奪佔台灣。但以台灣的角度而言，面對解放軍逐漸形成「以強擊弱」的「不對稱戰」格局，勢必也在思考如何避免兩岸軍力落差進一步擴大，並運用「不對稱」思維及整體防衛構想（Overall Defense Concept），推動國艦國造、國機國造、潛艦國造等國防自主計畫與全民國防，透過「印太戰略」下的台美夥伴合作，強化對北京方面的嚇阻能力。

以美中可能發生的衝突而言，解放軍是否將採取「不對稱戰」或「超限戰」思維，嚇阻美軍介入兩岸衝突？或在美軍介入後，試圖避實擊虛、以小搏大、以弱擊強，以贏得台海戰事的勝利？而相對居於軍力優勢的美國，是否可能在台海對解放軍打一場「不對稱戰」？這些都是美中台三方高度關切的議題。

本文作者李哲全為美國南卡羅萊納大學國際關係博士，現為財團法人國防安全研究院國家安全與決策研究所副研究員。

Thoughts and Implications of 21st Century Asymmetric Warfare Research

Che-Chuan Lee

Associate Research Fellow

Abstract

This paper presents a brief review of asymmetric warfare research after the 9/11 incident. The concept of asymmetric warfare was fascinating by pointing out strong powers do not always win due to its weakness in technology and weaponry and factors limiting its flexibility and innovative capability in war-fighting because of legal, organizational, cultural, and psychological reasons. The weaker opponents, on the other hand, hold opportunities to prevail if it can avoid and undermine enemy advantages, and exert its own strength against selected enemy weaknesses.

Although China does not adopt "asymmetric warfare" into its military doctrine, it treats "asymmetric warfare" seriously. The book Unrestricted Warfare written by two PLA colonels was regarded as a typical representation of Chinese way of thinking on asymmetric warfare. As a late-comers in science and technology, PLA also emphasizes the importance of "winning local wars under high-technology conditions," "information warfare," and works hard on the construction of its "Anti-access and Area Denial" （A2/AD） capabilities.

The author points out, if Beijing tries to resolve the dispute across the Taiwan Strait by non-peaceful means, the parties could face a situation of "double asymmetric warfare". PLA would probably launch a quick and positive asymmetric warfare trying to defeat or occupy Taiwan before the

U.S. and international forces were able to intervene. While Taiwan could have developed asymmetric defense capabilities to deter or frustrate PLA invasion. On the other hand, PLA would apply asymmetric warfare strategy or tactics to deter or defeat U.S. military. It is also the concern of the U.S. whether it would be able to fight a positive asymmetric warfare against the PLA.

不對稱作戰的理論與實際

歐錫富

先進科技與作戰概念研究所

壹、前言

不對稱作戰（asymmetric warfare）簡單的說，就是避實擊虛。不對稱概念以戰國時代齊威王與大臣田忌賽馬最有名。孫臏告訴田忌，三匹賽馬有上中下之別，以你的下駟對王的上駟，以你的上駟對王的中駟，以你的中駟對王的下駟，你雖有一敗，但必有二勝。齊威王擁有全國最好的馬，田忌若以上駟對上駟的對稱方式迎戰，則必有三輸。在牧羊人大衛（David）與巨人歌利亞（Goliath）的對戰中，大衛是明顯的劣勢者，巨人歌利亞是令人聞風喪膽的霸主。大衛卻以石頭擊中歌利亞眉間最脆弱部位而贏得勝利。在特洛伊戰爭（Trojan War），特洛伊王子帕里斯（Paris）用箭射中阿基里斯腳踝（Achilles Heel），這是刀槍不入阿基里斯的唯一弱點。面對美國各種制裁，具有實戰經驗與控制重要石油交通線的伊朗，不可否認地是不對稱作戰典型案例。

貳、不對稱作戰定義與特點

20 世紀英國戰略理論家李德哈特（B. H. Liddell Hart）大力支持間接路線（indirect approach），強調避開敵人優勢，尋求敵人弱點。冷戰時代蘇聯擁有數量優勢，美國則以質量優勢反制。目前中國的反介入與拒止，也是對抗美國全面優勢的不對稱戰略。不對稱思想也貫穿在戰役、戰術層級，游擊戰、閃電戰、潛艇戰、恐怖主義、信息戰等，都是有名的事例。美國參謀首長聯席會議定義不對稱作戰為企圖使用非傳統方式操控對手弱點，以規避或破壞對手力量。[1]

[1] Roger W. Barnett, *Asymmetric Warfare: today's Challenge to U.S. Military Power* （Washington D.C.: Brasseys, 2003), p. 15.

美國中央情報局（Central Intelligence Agency）將不對稱作戰定義為較弱的國家或次國家對手，面對較大或科技優越對手，企圖避實擊虛，使用創新的戰略、戰術與技術。這包括：一、國家或次國家團體使用選擇性武器或軍事資源，對抗、嚇阻或擊敗數量或技術佔優勢的對手。二、國家或次國家團體使用外交或其他非軍事資源或戰術，打消或限制優勢國家的軍事行動。[2]美國國防專家麥爾斯（Franklin B. Miles）認為，美國國防部和中央情報局不對稱作戰定義之共同特點，包括：一、發揚己長選擇性攻擊對手弱點。二、使用不預期、非傳統、創新手段進行攻擊或防衛。三、在軍事或財政投資後果上，形成不成比例的效益。四、不對稱威脅可能是文化或技術層面，前者如恐怖主義、人肉盾牌或種族清洗，後者如無人機。[3]

1999 年《聯合戰略評論》（*Joint Strategy Review*）定義不對稱路線為「企圖使用有別於美國預期的作戰手段，操控美國弱點，以規避或破壞美國力量。不對稱路線尋求重大心理衝擊，這種衝擊或混淆將對對手主動、行動自由與意志造成影響。不對稱路線使用創新、非傳統戰術、武器或技術，並應用到戰爭所有層級—戰略、戰役、戰術—跨越軍事行動的所有光譜」。[4]

梅特茲與強森（Steven Metz and Douglas V. Johnson II）指出，一個更全面的戰略不對稱定義：在軍事事務與國家安全，為了擴大本身優勢，操控對手弱點，取得主動或行動自由，不對稱在行動、組織、思維方面，與對手絕然不同。不對稱可能在政治-戰略、軍事-戰略、戰役，或者綜合上述面向。不對稱需要不同的方法、技術、價值、組織與時間，或者綜合上述因素。[5]

---

[2] Central Intelligence Agency, *Statement of Work for Asymmetric Warfare Threats to US Interests: Expert Panel Support*, May 1998, p. 2.

[3] Franklin B. Miles, "Asymmetric Warfare: A Historical Perspective," 1999, US Army War College, pp. 3-4.

[4] Steven Metz and Douglas V. Johnson II, "Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts," January 2001, US Army War College, p. 5.

[5] Ibid., pp. 5-6.

不對稱有正向與負向。美國在冷戰時期全力保持武器質的優勢是正向不對稱，對尋求美國弱點則是負向不對稱。不對稱有短期與長期。二次大戰德國的閃電戰為短期不對稱，毛澤東的人民戰爭屬於長期不對稱。不對稱有實質與心理。美國第三次抵銷（third offset）保持技術優勢是實質不對稱，中國宣稱彈道飛彈可擊沉美國航空母艦，一般認為技術上仍有困難，但有產生心理震撼不對稱效果。

不對稱之形式主要有：一、手段。必須有獨特的作戰概念與戰術準則，例如游擊戰。二、科技。在 1893-94 年馬塔貝萊戰爭（Matabele War），50 名英軍使用 4 挺馬克沁機槍（Maxim gun）對付 5 千名馬塔貝萊戰士。越南應付科技優勢的不對稱手段是持久戰（protracted war）。三、意志。意志在戰略層面，較弱的一方願意承受大犧牲與風險。意志在戰役、戰術層面，士氣高或站在正義一方，會有較強戰力。拿破崙說精神與物質是三比一。四、組織。馬其頓方陣（Macedonian phalanx）曾經在戰場上所向披靡，拿破崙的徵兵制也比當時歐洲的雇傭兵擁有更多的兵源。五、時間。一般認為優勢一方希望速戰速決，較弱一方強調持久以拖待變，認為時間站在他們這邊。[6]

麥爾斯認為，不對稱威脅或手段主要有游擊戰（包括叛亂戰、非傳統戰爭與不規則戰爭）、恐怖主義、大規模毀滅武器（核生化放）、信息戰、城鎮戰等。[7]

參、伊朗的不對稱戰力

伊朗神權政府視美國為其最大安全威脅，華盛頓無時不刻企圖推翻這個神權政府，駐伊拉克與中東美軍更是芒刺在背。為了有限嚇阻這個世界超級強國與其代理人以色列，伊朗發展不對稱作戰力量。伊朗武裝部隊分為正規軍（Artesh, regular forces）與伊斯蘭革命衛隊

[6] Ibid., pp. 9-12.
[7] Franklin B. Miles, "Asymmetric Warfare: A Historical Perspective," 1999, US Army War College, pp. 16-39.

（Islamic Revolutionary Guard Corps, IRGC），前者包括伊斯蘭伊朗共和國陸軍 35 萬人、伊斯蘭伊朗共和國海軍 1.8 萬人、伊斯蘭伊朗共和國空軍 3.7 萬人、伊斯蘭伊朗共和國防空軍 1.5 萬人，總共 42 萬人；後者伊斯蘭革命衛隊陸軍 15 萬人，伊斯蘭革命衛隊海軍 2 萬人，伊斯蘭革命衛隊空天軍 1.5 萬人，伊斯蘭革命衛隊特種部隊聖城軍（Quds Force）0.5 萬人，後備部隊 45 萬人，總共 64 萬人，若不包括後備部隊則只有 19 萬人。伊朗正規軍與革命衛隊兵力共 61 萬人，缺點為二元結構，遭受美國制裁缺乏獲得現代化武器與科技管道。[8]

德黑蘭核心不對稱戰力包括：

一、長程攻擊彈道飛彈

由於缺乏現代化空軍，伊朗依賴彈道飛彈作為長程攻擊武器。伊朗是中東地區擁有最多彈道飛彈的國家，雖然準確度不高，射程從 300 公里到 2,000 公里不等，使用固體或液體燃料，以道路機動或發射井方式發射（圖 1）。[9]伊朗短程彈道飛彈（Short-Range Ballistic Missile, SRBM）流星（Shahab）-1/2 起義（Qiam）-1，技術來源主要以飛毛腿（Scud）飛彈為基礎。中程彈道飛彈（medium-range ballistic missile, MRBM）技術主要來是北韓，例如流星-3 以北韓蘆洞（No Dong）飛彈為基礎。2017 年 6 月伊朗以起義彈道飛彈攻擊敘利亞的伊斯蘭國戰士，2018 年更數度以中程彈道飛彈攻擊葉門。伊朗另發展攻陸巡弋飛彈，以彌補彈道飛彈的不足。近年來伊朗積極發展攻擊無人機，配合彈道飛彈共同執行攻擊任務。2017 年伊斯蘭革命衛隊成立 1 個無人機師，統籌無人機研發、生產、部署與訓練。2019 年底無人機師一戰成名，以 20 多架無人機攻擊沙烏地阿拉伯石油生產設施。[10]

---

[8] Defense Intelligence Agency, *Iran's Military Power*, 2019, p. 11.

[9] Defense Intelligence Agency, *Iran's Military Power*, 2019, pp. 44-46; Stephen M. McCall, "Iran's Ballistic Missile and Space Launch Program," January 9, 2020, Congressional Research Services, pp. 1-2.

[10] "Procurement: Ready for Prime Time," *Strategy Page*, May 20, 2020, http://www.strategypage.com/htmw/htpro/articles/20200522.aspx.

征服者-110 Fateh-110	流星-1 Shahab-1	流星-2 Shahab-2	佐爾法卡爾 Zolfaghar	起義-1 Qiam-1	流星-3 Shahab-3	伊瑪德-1 Emad-1	阿舒拉節 Ashura
固體	液體	液體	固體	液體	液體	液體	固體
300-500 km	300 km	500 km	700 km	750 km	2,000 km	2,000 km	2,000 km
道路機動	道路機動	道路機動	道路機動	道路機動發射井	道路機動發射井	道路機動	道路機動

圖1、伊朗主要各型彈道飛彈

資料來源：Defense Intelligence Agency, *Iran's Military Power*, 2019, p. 47.

二、反介入與區域拒止（anti access/area denial, A2AD）

伊朗的反介入與區域拒止在遏止對手進入其近海，波斯灣（Persian Gulf）與荷姆茲海峽（Strait of Hormuz）是世界重要石油交通線遏制點，德黑蘭採取海上游擊戰，以小艇飽和攻擊對手大艦。其不對稱戰力包括艦載／岸置攻船巡弋飛彈、快速攻擊艇（Fast Attack Craft, FAC）、近岸快速攻擊艇（Fast Inshore Attack Craft, FIAC）、水雷、潛艦（3 艘基洛級）、小型潛艇、無人機、反艦彈道飛彈與防空系統（圖 2）。伊朗快速攻擊艇為裝備 C-801／802 攻船飛彈的中國 21 艇（滬東級或侯東級）；卡迪爾（Ghadir）小型潛艇為仿製北韓鮭魚級

（Yono）；將征服者-110 彈道飛彈改良成波斯灣（Khalij-Fars, Persian Gulf）攻船彈道飛彈。伊朗的反介入與區域拒止是中國的縮小版，以飛彈、潛艦、快艇為主。

圖 2、伊朗主要核心不對稱戰力

順時鐘依次為快艇、卡迪爾小型潛艦艇、流星-3 彈道飛彈與莫哈佳（Mohajer）-6 無人機。
資料來源：圖片取自伊朗梅爾新聞社（*MEHR News Agency*）。

三、非傳統作戰行動

由於傳統軍力有限、規避責任以及降低衝突升高風險的考量，伊朗傾向採取夥伴、代理人或地下活動等介入地區事務。伊斯蘭革命衛隊聖城軍是德黑蘭非傳統作戰行動的主要工具，透過經援、訓練、提供武器裝備等方式扶持盟友，打擊敵人。這些盟友通常與伊朗同樣信仰什葉派伊斯（Shia Islam），不過也有因共同利益、共同敵人等其他因素而結盟。早在 1982 年伊朗與黎巴嫩真主黨（Hizballah）結盟，近年來與敘利亞阿塞德政權（Asad regime）友好，同時成為援助真主黨的重要管道。在伊拉克，聖城軍與民眾動員力量（Popular Mobilization Forces, PMF）共同打擊伊斯蘭國（Islamic State, IS）。在葉門，伊朗援

助胡塞（Huthi）反抗軍。

肆、伊朗形成的不對稱威脅

伊朗發展不對稱戰力，造成威脅主要包括：一、聯合非國家團體、志願者，這是一種不用負責並可以否認的威脅。二、攻擊無人機、巡弋飛彈、彈道飛彈，而且越來越準確。三、潛艦、小型潛艦、導向魚雷、攻船／攻陸飛彈、智慧水雷，特別是水雷，1988 年伊朗在荷姆茲海峽部署約 150 枚水雷，其中重創美軍飛彈巡防艦羅伯特號（*USS Samuel B. Roberts* FFG-58）。四、滲透或支援鄰近或其他國家的什葉派。五、網戰。六、以宣傳、宗教為宗派武器。七、移交飛彈給黎巴嫩真主黨（Hezbollah）與葉門胡賽武裝團體（Houthi）。八、攻擊海上商船。九、攻擊關鍵基礎設施。十、發動低度、持續地有限與消耗攻擊。十一、挑釁地武器測試、軍演或其他形式的侵略。十二、目標突擊或小型攻擊。[11]

伍、結論

不對稱作戰即避實擊虛，針對阿基里斯腳踝下手。換句話說，發揚自己長處選擇性攻擊對手弱點，使用不預期、非傳統、創新手段進行攻擊或防衛，在軍事或財政成本上，造成不成比例的效果。不對稱可能在政治-戰略、軍事-戰略、戰役，或者混合以上面向。不對稱需要不同的方法、技術、價值、組織與時間，或者混合上述因素。一般將不對稱作戰都把重心擺在手段、科技方面，其實意志、組織改造、時間更為重要。德黑蘭在兩伊戰爭進行油輪攻擊戰，時間長達 8 年，因宗教熱誠支撐的作戰意志，認為時間站在他們這邊，勝利最後一定屬於他們。

[11] Anthony H. Cordesman, *The Gulf and Iran's Capabilities for Asymmetric Warfare*, January 2020, Center for Strategic and International Studies, http://www.csis.org/analysis/gulf-and-irans-capabilities-asymmetric-warfare.

面對世界超級強國美國及其代理人以色列，以及遜尼派（Sunni）的沙烏地阿拉伯，伊朗首要發展長程彈道飛彈，雖然準確度不高，射程兩千公里涵蓋整個中東地區，足以打擊地區敵國與美軍基地，形成有限嚇阻力量。伊朗為控制荷姆茲海峽及其周邊海域，發展縮小版的中國反介入與區域拒止，以飛彈、潛艦、快艇為主力，甚至擁有攻船彈道飛彈。一旦發生危機，騷擾或切斷海上石油運輸，成為伊朗的撒手鐧武器。伊朗還發展非傳統作戰行動，以伊斯蘭革命衛隊聖城軍為主力。伊朗支持黎巴嫩真主黨、敘利亞阿塞德政權、葉門胡塞反抗軍等，多為什葉派理念相同或利益相同的組織團體，團結所有反美力量，藉此騷擾或對抗美軍，分散本身壓力。

伊朗不對稱作戰個案對台灣頗具參考價值，同樣面臨敵強我弱，必須以小搏大的局面。台灣創新不對稱作戰主要在提高中國犯台成本，降低其成功機率而讓北京考慮再三。台灣版的反介入與區域拒止除了飛彈、潛艦、快艇外，還要像伊朗長程彈道飛彈一樣擁有反制打擊力量。伊朗全力發展無人機並具實戰經驗，為其不對稱戰力特色，值得台灣學習。除了武器裝備硬體創新，台灣還要重視組織、意志士氣等軟體作為。自由民主對抗威權獨裁，如伊朗宗教熱誠般地為自由民主理念而戰，才足以支撐危機的艱苦挑戰。

本文作者歐錫富為美國邁阿密大學國際關係博士，現為財團法人國防安全研究院先進科技與作戰概念研究所研究員。

The Theory and Implementation of Asymmetric Warfare

Si-Fu Ou

Research Fellow

Abstract

The key characteristics of asymmetric warfare include pitting one's strengths against selected enemy weakness; using unexpected, unconventional, or innovative methods of attack or defense; offering a disproportionate effect in terms of outcome to the military or financial investment; asymmetric threats can be either technologically or culturally based. Facing the US various sanctions, Iran adopted an asymmetric approach and its core asymmetric military capabilities are comprising of ballistic missiles, anti-access/area denial （A2/AD） and unconventional operations. Tehran has also developed several types of unmanned aerial vehicles （UAVs） and launched swam drone attacks against its enemies. Like a David and Goliath rivalry in the Taiwan Strait, Taiwan can learn a lesson from the Iranian case. An innovative asymmetric approach involves not only hardware, but also software that is the will to resist. In order to encounter Beijing's military intimidation and possible use of force, the Taiwanese will to fight for freedom and democracy is more important than weapons.

不對稱戰：認知作戰的途徑

曾怡碩

網路作戰與資訊安全研究所

壹、前言

對於俄羅斯過去針對烏克蘭與波羅的海三小國及近年來對於美國的選舉進行干預，相關研究已經陸續出爐。其手法雖借助網路空間與社群媒體，但本質上是以從事認知操縱，企圖操弄或改變選舉結果，具有不對稱戰特質。認知戰的文獻累積相當可觀，然而，對於認知戰有何不對稱特質，以及在介入操縱不同國家選舉時，認知戰需要如何因應調整作為，以達不對稱戰效果，迄今仍付諸闕如。

有鑒於此，本篇以俄羅斯干預破壞民主國家選舉安全為例，藉文獻比較分析，首先探討認知戰的脈絡、認知戰與網路戰關係，並歸結出認知戰的不對稱戰性質。其次，為了解敵意國對小國與對大國遂行認知戰之手法有否差異，藉以進一步掌握認知戰之不對稱特質，本篇將解析俄羅斯在波羅的海三小國多次選舉以及在美國 2016 年總統大選期間所遂行之認知戰，並比較手法異同。最後，在將比較結果置諸歷史與制度脈絡分析之後，歸結出認知戰在因地制宜適應調整上的實務要點。依此，本篇除積累認知戰論述資訊，並期作為後續相關比較研究的參考之一。

貳、認知戰概念與操作面的不對稱性質

一、認知戰概念

自俄羅斯以資訊作戰分別於 2007-8 年干預波羅的海國家選舉之後，認知戰（cognitive warfare）即成為熱門議題。按照曾於俄羅斯總統普欽（Vladimir Putin）身旁扮演意識形態總設計師的蘇爾柯夫（Vladislav Surkov）所言，俄羅斯介入他國選舉，是藉由操縱選民接收

的資訊，在媒體生態系灌輸假訊息與宣傳，冀能干預思維並改變意識。易言之，認知戰藉由資訊手段所要影響與改變的目標，就是「在兩耳之間的思維，以及隨之改變的行為」。[1]觀諸與認知戰相關的論述，在美國有「影響力行動」（influence campaign）、「資訊作戰」（information operations），而俄羅斯有「主動作為」（active measure）／「反射性控制」（reflexive control），中國則在「統戰」與「三戰」（輿論戰、心理戰、法律戰）之外，於 2014 年提出「制腦權」的概念。

然而，認知戰應為前述種種論述架構之一部分，而非將認知戰與影響力作戰／資訊作戰或反射性控制混為一談。鑒諸 2012 年美軍《資訊作戰》（*Information Operations*）準則中，美軍首次提出「影響資訊作用流程框架」（Information-influence relational framework），描述如何在認知向度（Cognitive Dimension）、資訊向度（Informational Dimension）、實體向度（Physical Dimension）運用各式工具以達成對目標閱聽眾之影響力。其中，認知向度指的是傳遞、接收、回應或資訊採取行動的人員思想，包括資訊處理、判斷、決策的個人或群體；資訊向度包括資訊、處理、儲存、傳播及保護的位置與方式；實體向度則是由指揮與控制（Command and Control, C2）機制、關鍵決策者、支援之基礎設施等所組成。[2]圖 1 所示即為其應用之架構，其概念類似「影響力行動」（influence campaign），而認知戰為其支柱之一。

俄羅斯的反射性控制，則考慮了人的心理特徵，並涉及對其決策模式的故意影響（intentional influence），這些特徵揭露了一種反映內部決策機制的認知模型，反射性控制可能導致從欺騙到暗示的心理影響，如表 1 所示，如果這些機制中的其中之一失敗，那麼則整體反射性控制途徑需要運用另一種機制，否則其原始效應可能會迅速降低。

[1] Oliver Backes and Andrew Swab, "Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States," Belfer Center, Harvard Kennedy School, November 2019, p. 8.
[2] "Information Operations," Joint Chiefs of Staff of US, November 27, 2012, Joint Pub 3-13, p.I-2-3.

此外，隱匿也是一種反射性控制技術，分為兩個層次，其中作戰層次的隱藏旨在使敵人對於即將進行的作戰行動之性質、概念、規模及時間上迷失方向；戰略層面的隱藏則是暗中準備一項戰略行動或運動，使敵人在行動的真實意圖上迷失方向。[3]由表 1 可見，認知戰可搭配資訊與實體領域之多重手段。因此，認知戰除具備前述資訊作戰或影響力作戰之不對稱性質，且跨越戰略、作戰，甚至到戰術層次。

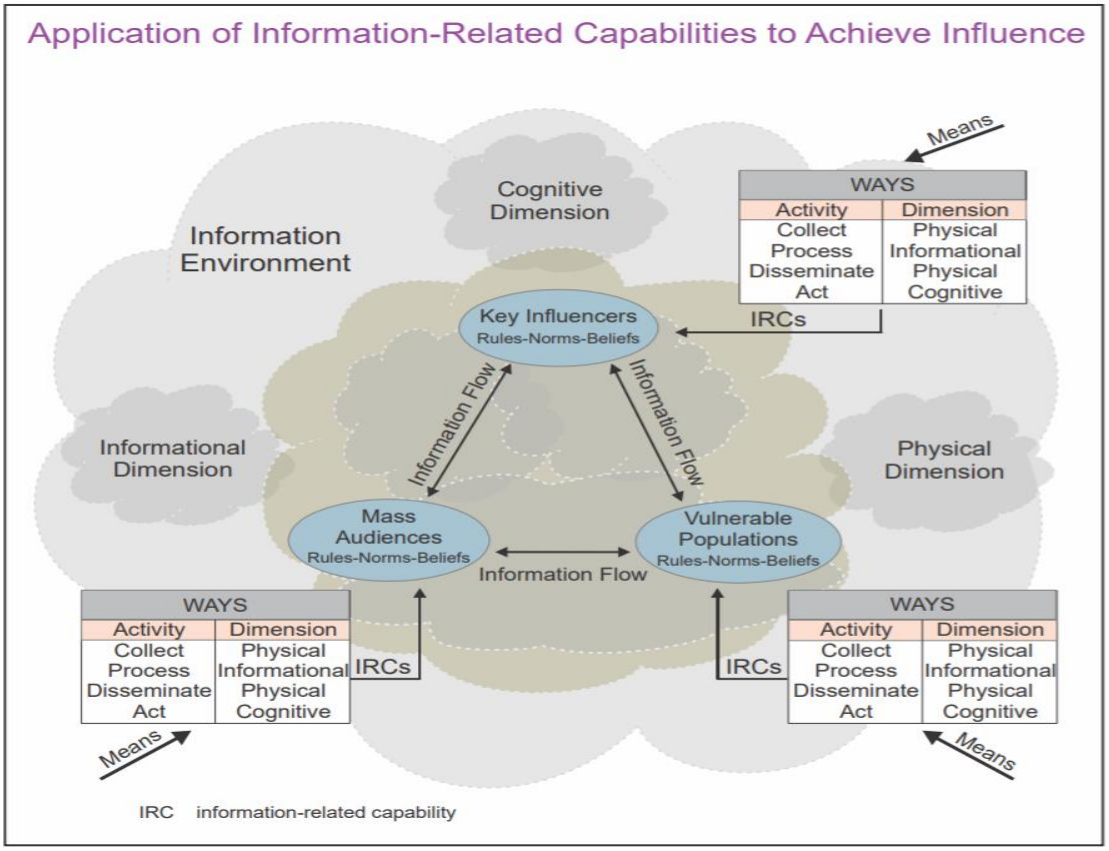

圖 1、應用資訊相關能力進行影響

資料來源：“Information Operations,” Joint Chiefs of Staff of US, November 27, 2012, Joint Pub 3-13, p.I-7, Figure1-4.

表 1、俄羅斯「反射性控制」機制

欺騙（Deception）	在戰鬥行動的準備階段，迫使敵方將部隊引導到受威脅的地區。

[3] A.J.C. Selhorst, “Russia’s Perception Warfare,” *Militaire Specrator*, 185, No. 4, 2016, pp.151-152.引自洪霽廷，《俄羅斯資訊作戰之研究》，淡江大學戰略所碩士學位論文，108 年 6 月。

威懾（Deterrence）	創造不可超越的優越感。
分散注意（Distraction）	在戰鬥行動的準備階段，對敵方最重要的地點之一造成真實或虛假的威脅，進而其重新考慮決策方向。
分化（Division ）	說服敵方必須反對同盟利益。
消耗（Exhaustion）	迫使敵方進行無用的行動，使其執行作戰時的資源減少。
超載（Overload ）	經常向敵方發送大量的衝突資訊。
安撫（Pacification）	引導敵人相信預先計劃的作戰訓練在正發生，而不是正在進行作戰準備，進而降低敵人的警覺性。
癱瘓 （Paralysis）	使敵人認為已對其重要利益或弱點造成特定威脅。
壓力 （Pressure）	製造詆毀敵方政府的不利資訊，使民眾產生不信任。
挑釁（Provocation）	迫使敵方採取有利於己方的行動。
暗示（Suggestion）	製造在法律、道德、意識形態或其他方面影響敵方的資訊。

資料來源：A.J.C. Selhorst, “Russia’s Perception Warfare,”Militaire Specrator, 185, No. 4, 2016, p.152. 引自洪霽廷，《俄羅斯資訊作戰之研究》，淡江大學戰略所碩士學位論文，108 年 6 月。

二、認知戰操作面

就操作面向而言，認知戰可搭配資訊及實體向度所發生之衝突，形成混合戰（hybrid warfare）。例如，網路戰可以形成改變認知的助力，藉由網路入侵竊取並竄改資訊，再加以散布（hack and leak），或者藉由干擾甚至破壞實體關鍵基礎設施的運作，造成目標閱聽眾的認知混淆或心生疑義、恐懼、憤怒，[4]進而付諸行動製造衝突。另一方面，認知戰也可搭配實體世界的衝突，藉以強化認知戰所欲遂行目標。若前述搭配或引發之衝突未達戰爭程度，則認知戰尚屬灰色地帶衝突（grey zone conflict）界限之內；若衝突升高引發戰爭，認知戰就超越灰色地帶範疇。

認知戰藉資訊與衝突所欲達之目的，在於改變思維並進而改變行為。若因而達到以小博大、甚至不戰而屈人之兵，進而取得對己有利

[4] Michael Cheatham, “Wars of Cognition,” *Air & Space Power Journal*, Winter 2018, pp. 18-24.

結果或因此削弱對手，均可視認知戰具備不對稱作戰的特性。有鑒於此，冷戰時期美國意圖「和平演變」共黨陣營，對於運用認知戰以宣揚民主自由與資本主義市場經濟的優越性可謂不遺餘力，最終導致共黨陣營地崩解，可說是不費一兵一卒，堪稱認知戰的不對稱作戰凱旋勝利代表作。

相對的，如今民主政體在選舉期間，反而是面對認知戰最為脆弱的時刻。民主政體的言論自由保障與開放社會特質，反倒有利於敵意國家或團體得以運用假訊息或收買媒體、政客以遂行認知戰，但敵意國家如為威權體制並遂行網路言論控制，則民主政體如欲反擊，卻少有可施力之處。有鑒於認知戰在選舉期間的不對稱優勢，以下將以俄羅斯干預波羅的海三小國選舉與 2016 年美國總統大選為例，分析俄羅斯認知戰對選舉安全的重大衝擊。

參、俄羅斯認知戰干預選舉之案例

一、波羅的海三國

愛沙尼亞、拉脫維亞及立陶宛在冷戰時期為舊蘇聯所佔領並實施蘇聯化，迄今各有 24.9%、25%及 15%俄裔／俄語人口，俄羅斯分別在 2003 年、2007-8 年以及 2018-9 年波羅的海國家選舉時出手干預，並積極透過俄國電視台、社群媒體、非政府組織以及親俄政客影響俄裔與俄語人口投票取向。

2004 年 4 月 5 日立陶宛總理 Rolandas Paksas 因授予俄羅斯犯罪頭領 Yuri Borisov 公民身分、並對其洩露調查不公開資訊而遭彈劾。據信 Borisov 在克里姆林宮贊助下，對 Paksas 在 2003 年大選金援 40 萬美金。[5]此外，立陶宛專家指控，俄語電視台在大選期間善用夾帶煽

[5] Oren Dorell, "Alleged Russian political meddling documented in 27 countries since 2004," *USA Today*, September 7, 2017, https://www.usatoday.com/story/news/world/2017/09/07/alleged-russian-political-meddling-documented-27-countries-since-2004/619056001/.

動辭語畫面以對立陶宛操作俄語民族意識。[6]

2007 年 4 月愛沙尼亞政府為了選舉考量，將蘇聯時期置於首都塔林的軍事紀念銅像移址。俄羅斯趁機炒作歷史情結，將此事件連結為愛沙尼亞政府當年拒蘇聯而屈從納粹的歷史，俄羅斯電視台與社群媒體不斷播映相關論述與影像，數百名俄裔在親俄的非政府組織鼓動下集結抗議。接下來數周，愛沙尼亞遭受大規模分散式阻斷網路服務攻擊。俄羅斯在接下來 2008 年對波羅的海其他兩國選舉也同樣採用俄語電視媒體、社群媒體及親俄非政府組織力挺親俄政客。[7]

2018-9 年在拉脫維亞與愛沙尼亞的選舉，俄羅斯同樣動用社群媒體、俄語電視媒體與親俄非政府組織力挺親俄政客，但這次打出的是族群牌。拉脫維亞被觀察團體 Kremlin Watch 列為因應俄羅斯認知戰最成功的國家之一，但在 2018 年 10 月 6 日拉脫維亞國會大選投票日，該國熱門網站 Draugiem.lv 遭駭客攻擊，並將頁面改為「俄羅斯疆界與文字文化延伸到拉脫維亞」等挺俄口號，意圖影響親俄與俄裔人口，而該次大選結果也讓該國親俄政黨「和諧黨」（Harmony Party）獲得該次大選相對最多票。拉脫維亞安全機構認為這次事件背後，親俄團體嫌疑最大，而且指控俄羅斯針對拉脫維亞長期散布網路假訊息進行影響力作戰。[8]

2019 年在愛沙尼亞首都塔林 Eesti 200 公車候車亭出現六張海報，刻意區分愛裔俄裔站不同邊，雖然其立意是為鼓吹兩邊和諧，但俄羅斯國營電台與社群媒體偕同迅速重複播放，並且不斷轉傳富煽動性內容的不實訊息，刻意將之扭曲比擬為當年南非種族隔離政策，鼓動俄裔人口出門投給親俄政客。此番俄羅斯的媒體偕同動員效率驚人，

[6] Oliver Backes and Andrew Swab, “Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States,” ibid., p. 15.

[7] Raphael Cohen and Andrew Radin, “Russia’s Hostile Measures in Europe-understanding the threat,” RAND report, 2019, pp. 41-46.

[8] Anna Udre, “Exploring Latvia's Election Day Hack,”*CEPA StratCom*, https://www.cepa.org/exploring-latvias-election-day-hack.

連愛沙尼亞官方都出面指陳，這已然是典型俄羅斯資訊作戰模式。[9]

二、2016 年美國總統大選

根據位於美國德州的事實查核公司 New Knowledge 與英國牛津大學運算宣傳計畫（Oxford University's Computational Propaganda Project）針對俄羅斯散播假訊息的調查報告指出，俄國針對 2016 年美國總統大選主要採取三種的干預形式。（一）網攻駭入美國各州的線上選舉系統；（二）由俄國總參謀部軍事情報局主導網路攻擊，竊取民主黨全國委員會相關資料，並透過「維基解密」洩漏希拉蕊陣營的電郵；（三）針對美國公民運用各類的假訊息、進行廣泛而持續的社會影響行動，旨在發揮政治影響力及加劇美國社會文化之分歧。而第三種的干預形式，主要由俄羅斯「網路研究局」（Internet Research Agency）在進行多年的假訊息活動。[10]該局利用 Facebook、Instagram、Twitter 等平台向數千萬名美國使用者進行與美國的重大政治事件、危機及國際事件等緊密相關宣傳活動，其中最關鍵影響力的宣傳多為該局所管理的假網頁，或是偽裝成關注事件的公民使用的帳號所製作的貼文。[11]

俄國「網路研究局」的活動旨在增加美國社會分歧，針對非裔美國民眾，而且同時影響著左翼及右翼的政治意識形態。例如在「黑人的命也是命」（BlackLivesMatter）社會運動中，俄國「網路研究局」在 Twitter 及 Facebook 設立假帳號，持續推文非裔民眾遭到警察槍殺的事件，企圖製造社會對立，並將美國執法機關形容為種族主義者；

[9] Oliver Backes and Andrew Swab, “Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States,” ibid., p. 11.

[10] Renee DiResta, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, Ben Johnson, “The Tactics & Tropes of the Internet Research Agency,” New Knowledge, Austin, TX, 2018; https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper.pdf, p.4.

[11] Philip N. Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly , Camille François, “The IRA, Social Media and Political Polarization in the United States, 2012-2018,” Oxford University's Computational Propaganda Project, 2018, p.7.

在 2016 年 7 月美總統大選選前，也讓俄國影響活動有了加劇社會分歧的機會，當時發生三名警察濫殺非裔男子的事件，在事後的抗議活動中即發生不滿的民眾狙擊維持活動秩序的警察，導致 5 名警察身亡，而該抗議活動為「黑人的命也是命」運動的一部分。[12]

肆、俄羅斯認知戰的差異性與不對稱性

比較分析俄羅斯干預波羅的海國家與對美國選舉安全之認知戰作為，其中最值得注意的是其效益—俄羅斯對美國這樣的大國遂行認知戰奏效，對波羅的海三小國卻未必如此。然而，認知戰的不對稱效益，不能就此簡化為「對稱戰才生效，不對稱戰反而失效」，必須在進一步結合時空背景脈絡，予以檢視分析其手法異同暨其背後意涵。

有關於兩者之共通點，首先是俄羅斯會利用並擴大既存之歧異，放大為對政府的不信任。因此，波羅的海國家的族群認同與美國的種族歧視，均成為俄羅斯運用為選戰炒作的議題。其次，網路與媒體均為俄羅斯充分利用以在選舉期間散布假訊息及放大歧異。最後，俄羅斯均曾發動網路攻擊影響選舉，但網路攻擊僅為輔助性助攻角色。在 2007 年在愛沙尼亞，俄羅斯發動網路攻擊主要是釋放警告訊號，其作用是在於影響選民認知。2016 年在美國，俄羅斯雖被證實曾網路入侵每一州的選舉機器，但並未發動癱瘓或造假，而雖曾對民主黨競選總部進行「駭入再散布」，但主要作用還是在於增強認知影響，而非侷限於網路攻防。

至於相異處，首先是兩者雖然都打族群牌，但在波羅的海國家卻涉及媒體與政界的俄羅斯代理人與俄羅斯認同問題，美國則未涉及親俄議題。其次，法西斯主義政府的歷史陰影纏繞糾結著波羅的海國家，而且俄羅斯舞動歷史與族群情結的劍，其意在動搖波羅的海國家人

[12] Suzanne Spaulding, Devi Nair, Arthur Nelson,“Beyond the Ballot: How the Kremlin Works to Undermine the U.S. Justice System,” CSIS's Defending Democratic Institutions Project, 2019, pp.24-25.

民對其政府治理能力的信任，運用俄裔人口為支點，讓這波羅的海三國脫離北約與歐盟，重返俄羅斯旗下。因此，俄羅斯在波羅的海國家的認知戰作為，一直偏重宣揚扶植俄裔或親俄團體與政客，希望複製克里米亞與烏克蘭的經驗。

只是，俄羅斯恐怕白忙一場，畢竟俄裔族群僅佔少數，而且波羅的海三國是最早加入北約的前共產國家，境內俄裔族群也未必有分離主義意識或者大斯拉夫意識，克里米亞與烏克蘭的模式，實難以套用在波羅的海三國。同理，俄羅斯在波羅的海國家大打俄裔族群牌的認知戰經驗，勢將難以適用於對西歐諸如英、德、法、荷等國。

相較於在波羅的海國家大打族群牌而一面倒地扶植特定立場團體或個人，俄羅斯在美國的目標則是讓民眾對於民主體制失望，藉由深化內部歧異矛盾，削弱美國的國力。因此，俄羅斯的認知戰是對保守與自由陣營同時兩面作戰，在共和黨與民主黨支持者兩個陣營，都運用社群媒體遂行分化手段，而非扶持特定陣營而打擊另一陣營。

以上分析顯示，對於民主多元社會，利用矛盾、各個擊破的手法，最能發揮認知戰的不對稱效益。俄羅斯對美國陷於兩極化撕裂的社會，在對立兩陣營內部均不斷製造分化。對於波羅的海國家，則因多數人基於歷史傷痛記憶，對於俄羅斯滲透破壞具有戒心，又囿於俄裔人口僅佔少數，對於不同陣營要各個擊破，相對較難奏效。即使如此，俄羅斯刻意鎖定俄裔少數族群的作為，仍可適時發揮相當的認知影響力，讓俄羅斯保有發動不對稱認知戰的威脅能力。

伍、結論

基於上述概念探討到案例比較分析，認知戰若要充分體現其不對稱性效益，必須要因循目標國特有政經軍心背景脈絡，予以客製化特定的認知戰組合作法。亦即，首先必須充分掌握目標國家之歷史文化與人口族群結構，才能利用並擴大既有之社會歧異、甚至客製化創造

出新的分化爭點。

其次，對於民主國家而言，其民主開放與保障言論自由，成為認知戰攻防的不對稱特性分界線。敵意國家或團體可充分運用此特性施以認知戰攻擊，而民主國家遂行認知戰之際，卻往往受制於敵意國家專制體制對言論的箝制與網路控制。循此，選舉安全成為民主國家在認知戰攻防中的弱點，但民主國家的開放自由卻也足以培養出因應認知攻擊的韌性。因此，因應認知戰的關鍵，在於如何一方面不會因噎廢食地將自由辯論視為認知攻擊而全面管制，另一方面又能確保不被敵意國家團體分化崩解消滅，方能讓韌性逐漸增生茁壯。

最後，認知戰往往並非單獨進行，而是混搭其他諸如網路戰或者實體衝突。因此，必須要充分體認到認知戰從戰略層次到戰術層次，從虛擬空間結合實體向度的特質，進而在認知戰攻防上靈活應處。尤其認知戰絕非新的產物，其本身類似過去的統戰應用了新的科技手法。當我國體認中共師法俄羅斯資訊作戰手法時，也必須認識到中共會將過去統戰路數傳統做出延續與針對台灣的客製創新，絕非死守俄羅斯教範準則，如此我國方能靈活而從容應處來自對岸的認知戰威脅。

本文作者曾怡碩為美國喬治華盛頓大學政治學博士，現為財團法人國防安全研究院網路作戰與資訊安全研究所助理研究員。

Asymmetric Warfare: A Cognitive Approach

Yisuo Tzeng

Assistant Research Fellow

Abstract

Cognitive warfare oftentimes falls into the category of asymmetric warfare, yet its asymmetric characteristics and the ways asymmetry operationalizes remain opaque or unknown, thereby amounting to imperative inquiry to most students of International Relations. With the employment of literature review and case study, this short essay endeavors to answer to the above research question by examining the conceptual and empirical dimensions of cognitive warfare.

Based on conceptual proximity to the U.S. information operations and Russian reflexive control, asymmetric character of cognitive warfare makes connections to virtual information warfare and physical warfare, presenting in hybrid warfare composed of cognitive, cyber and probably military attacks, thereby going through differed zones from grey to hot one, as well as various levels from strategic, to operational, and to tactic level.

With the comparisons between Russian interference in the U.S. 2016 presidential election and Baltic states' elections from 2007 to 2018, this study finds that exploiting existent societal divisions aside, what it takes to make cognitive warfare works in asymmetric way depends on how successful the adversary makes the best use of the local contextual history, culture, racial, and nationalistic elements.

Put simply, with the help of modern information and communication technology, cognitive warfare nowadays is pretty much the old wine in a new bottle. What Taiwan has been facing faces are perennial threats posed by China's long-lasting United Front Work, with growing cognitive elements going both virtual via cyberspace and physical through Chinese military harassments in the air and sea surrounding Taiwan. In order to bring Taiwanese into Beijing's reign, rest assured is that China follows the path of Russia in exercising cognitive warfare notwithstanding, there is no doubt that China will come up with something tailored to Taiwanese context.

不對稱戰：反制無人載具的途徑

舒孝煌

先進科技所與作戰概念研究所

壹、前言

無人機在「不對稱作戰」（asymmetric warfare）中的運用日益廣泛。無人機種類繁多，中大型無人機可執行長程、大酬載的複雜任務，通常為政府機關、軍事單位及商務集團使用，但小型或迷你無人機則極容易取得，具有體積小、技術層次低、容易部署、慢速且低高度飛行、難以偵測等特性，若配備武器，甚至具有潛在致命打擊能力，已成為國防安全的嚴重威脅。另外，中國已成為無人機生產大國，除商用領域，軍事上也大量運用無人機，並出口至中東國家。

反制無人機極為困難，使用無人機成本不高，但對手要增加大量成本應付無人機，傳統防空系統主要用於反制飛機或飛彈的攻擊，仍無法有效反制小型無人機，而且成本過高，因此許多國家均加快發展無人機反制系統，因應此種新興的不對稱威脅。面對中國無人機的高度威脅，國軍應強化發展無人機反制系統，整合已有指管通情能力及不同接戰方式，並發展其他技術，以利反制無人機威脅。

貳、無人機威脅

近年來無人機威脅日漸增加，不僅在作戰時，無人機被軍方用以執行精準打擊任務，而敵對國家、非國家角色如恐怖分子、游擊隊及叛軍，亦以無人機攻擊對手的政治、經及軍事設施，甚至造成重大破壞及損失。在平時，無人機對重要政經人員及關鍵基礎設施的干擾甚至攻擊，時有所聞，不但影響公共服務正常運作，威脅政府高層人員安全，甚至造成重大經濟損失。這些被用以作為攻擊手段的無人機，有些屬於中大型機種，但更多的是便宜的迷你商用機種，甚至以簡單

零組件即可組裝，極難防範。而無人機在軍事上的運用，已成一種新興的不對稱威脅。[1]

一、無人機對重要政經人員與關鍵設施威脅

無人機的威脅是全方位的，可用在軍事作戰上，也可用於攻擊重要政府高層官員，以及關鍵基礎設施，甚至用於攻擊平民，通常是一國或非國家角色，企圖影響另一國的政治、經濟穩定，製造社會動亂，以達到其政治目的。在對政府官員威脅方面，2013 年德國總理梅克爾（Angela Merkel）在發表競選演講時，一架無武裝無人機飛行至接近她面前；2015 年 1 月，一架無人機飛進美國白宮草坪的禁飛區，直到落地才被發現；[2]同年 4 月，日本一架無人機掉落在安倍首相官邸屋頂，造成維安人員緊張，經檢視無人機容器，發現有微量輻射物質「銫」。[3]2018 年 5 月，2 架無人機執行刺殺委內瑞拉總統馬多羅（Nicolas Maduro）未成。[4]

在對關鍵基礎設施或政府公共任務的干擾方面，2016 年 8 月，5 架無人機干擾洛杉磯森林大火空中消防任務，迫使直升機緊急降落以避免撞擊。[5]2018 年 12 月，英國蓋特威機場（Gatwick Airport）遭到多架無人機侵入，機場被迫關閉 3 天，由於是聖誕假期前的輸運，超過 1,000 個航班被取消，大約有 14 萬名旅客受影響，這使得英國空軍緊急部署拉斐爾無人機圓頂（Rafael Drone Dome）通訊干擾系統，

[1] " Unmanned Aerial Vehicles in Asymmetric Warfare: Maintaining the Advantage of the State Actor," *Institute for National Security Studies*, July 2017, https://www.inss.org.il/publication/unmanned-aerial-vehicles-asymmetric-warfare-maintaining-advantage-state-actor/

[2] Anthony Tingle & David Tyree, " The Rise of the Commercial Threat: Countering the Small Unmanned Aircraft System," *Joint Force Quarterly*, Quarter, 2017, p.30.

[3] 陳永全，「新興威脅—無人機惡意運用之應處防護作為」，《清流》雙月刊，法務部，106 年 1 月，https://www.nasc.gov.tw/News/news_more2?id=0edb118676da495686374791c77834ec

[4] "Venezuela President Maduro survives 'drone assassination attempt'," *BBC*, August 5, 2018, https://www.bbc.com/news/world-latin-america-45073385

[5] Anthony Tingle & David Tyree, " The Rise of the Commercial Threat: Countering the Small Unmanned Aircraft System," *Joint Force Quarterly*, Quarter, 2017, p.30.

以保護蓋特威機場。[6]之後無人機干擾機場的事件時有所傳，2019 年 6 月，新加坡樟宜機場 2 度發現無人機，該機場被迫關閉一條跑道，近 40 個航班遭延誤，而近 3 年來，樟宜機場已發生 8 次無人機非法入侵事件。[7]

而台灣也發生多次無人機干擾公共設施或政府高層的例子，2015 年 2 月，2 名英籍攝影師操作的無人機，墜落於距前總統馬英九座車僅 20 公尺的地面。[8]2019 年 12 月，無人機侵入桃園國際機場航道，使機場降落被迫暫停，12 航班轉降他處。[9]台北松山機場也多次傳出民航機目擊無人機、民眾在河濱公園施放無人機、無人機侵入限航區等事件，導致機場緊急關閉，這些事件多數均未發現施放者，僅有一次被查獲並當場制止，同時依《民航法》加以裁罰。[10]

二、無人機變身精準打擊武器

更嚴重是無人機被用於攻擊高價值的基礎設施，無需使用高成本、精密航電系統，即造的消費型無人機一樣可以成為精準武器。2019 年 9 月 14 日，沙烏地阿拉伯 Abqaiq 煉油廠及 Al Khurais 油田遭到疑似來自葉門叛軍的無人機和短程彈道飛彈攻擊，使石油產量每日減少 500 萬桶。2019 年，葉門叛軍「青年運動」（Houthis）多次以無人機攻擊葉門及沙烏地阿拉伯目標，雖然其使用低成本的無人機，但其行動經過精確協調，美國情報單位指出這並非葉門叛軍有能力實施，背後是伊朗指使，甚至親自執行。此次無人機對沙國煉油廠的攻擊，也使美製先進防空系統在面對低成本「不對稱威脅」時的弱點顯示無遺。

---

[6] "Counter UAV: High Tech Flyswatters," *Asia Military Review*, May 24, 2019, https://asianmilitaryreview.com/2019/05/counter-uav-high-tech-flyswatters/

[7] "Drone sightings at Changi Airport force closure of one runway, nearly 40 flights affected," *ChannelNewsAsia*, June 19, 2019, https://www.channelnewsasia.com/news/singapore/changi-airport-drone-sightings-one-runway-closed-11641920

[8] 余雁翔，「遙控無人機危安防制」，《清流》，法務部，2020 年 3 月，頁 31。

[9] 「無人機入侵航道！桃機航班暫停降落 12 班轉降」，《聯合新聞網》，2019 年 12 月 31 日，https://udn.com/news/story/7266/4260431

[10] 余雁翔，同前註。

11

低端技術且價格便宜的無人機攻擊，已為國家和恐怖分子用來進行攻擊行動。[12]最早的攻擊例子可能是 2006 年的第二次黎巴嫩戰爭。伊斯蘭國（ISIS）從 2014 年也開始使用消費型無人機，運用航拍功能製作宣傳影片，接著用來執行偵察任務，拍攝政府軍高解析度影像，並用以觀察迫砲目標，伊斯蘭國的據點被發現正製造即造無人機，使用木材、保麗龍組裝，另有小型攝影機及陀螺儀，韓國、日本及土耳其的電子元件，以及拆解的俄製地對空飛彈。除伊斯蘭國外，在敘利亞及伊拉克的其他組織也在使用無人機，包括真主黨，伊拉克政府也用無人機用在尋找汽車炸彈及戰術偵察任務。但除了偵察外，伊斯蘭國已用無人機裝載炸藥，改成廉價的導引武器，雖然威力不大，但問題日益嚴重。

由於無人機難以被擊落，許多組織都在利用無人機開發武器。而消費型無人機的飛行軟體也日益進步，如大疆無人機可以自動閃避樹木及建築等障礙物，精準降落功能可以透過圖像識別降落地點，無人機很快便可自動飛行，不需人員控制及衛星訊號，從而避免遭電子干擾。[13]

俄羅斯也大量運用無人機在戰場上，2015 年時就以使用無人機對付烏克蘭部隊；美國也早在中東戰場大量運用無人機，用以執行軍事任務，或獵殺恐怖分子。最近的戰例是 2020 年 1 月，美國以無人機執行斬首行動，攻擊巴格達國際機場，擊殺伊朗革命衛隊指揮官蘇雷曼尼（Qasem Soleimani），因他負責策畫及攻擊美國在伊拉克的外

[11] 賴怡忠，「沙烏地油廠攻擊事件的戰略衝擊」，《芋傳媒》，2019 年 10 月 2 日，https://taronews.tw/2019/10/02/476274/

[12] "Maneuver Air Defense: Addressing Emerging Air Threats Today," *Leonardo Drs*, February 2020, https://www.leonardodrs.com/news/news-features/maneuver-air-defense-addressing-emerging-air-threats-today/

[13] " How Islamic State is using consumer drones," *BBC*, December 9, 2016, https://www.bbc.com/future/article/20161208-how-is-is-using-consumer-drones

交及軍事人員，造成數百人喪生。[14]

中國已是無人機出口大國，中東並成為中國製無人機的試驗場，主要出口產品是翼龍及彩虹無人機，[15]2020 年利比亞內戰期間，利比亞國民軍由阿拉伯聯合大公國取得中國製造的翼龍 II 型「偵打一體」無人機，打擊對手的地面目標，另一方利比亞民族團結政府由土耳其、義大利等國支持，主要依賴土耳其軍事援助。交戰雙方均大量使用無人機，其中土耳其軍方多次擊落中國製的翼龍無人機。土耳其無人機技術也十分成熟，曾使用自製無人機攻擊土耳其境內及敘利亞的庫德族目標，也向烏克蘭、卡達出口無人機，使得利比亞衝突已成為無人機與反制無人機的戰爭。

三、無人機的類別與威脅

無人機威脅日益增長，對手使用相對較便宜的無人機對付友軍、軍事裝備、關鍵基礎設施。無人機不但可為預算不足國家提供爭奪戰場制空權的工具，不一定需要精密的作戰飛機，以及複雜的作戰指揮管制程序，甚至非國家組織，也開始選擇無人機作為武器。由於無人機技術的普及，未來無人機可能成為所有未來衝突中最普遍的武器。

在民用領域，無人機日益被用於犯罪等目的，只要簡單改裝，廉價的現成消費型無人機及業餘愛好者使用的無人機，就可能被轉用於搭載導引炸彈或其他攻擊武器，無人機大廠雖採取一些措施，防止其產品遭濫用，例如對飛行軟體施加限制，使其無法飛入機場等禁飛區，但有經驗的操作者卻可輕易關閉這項限制。因此在民用或執法機關，無人機攻擊的問題已非「如果」，而是「何時」，防範無人機攻擊也已

[14] 「無人機精準斬首 美空襲狙殺伊朗高級將領」，《中央社》，2020 年 1 月 3 日，https://www.cna.com.tw/news/firstnews/202001030212.aspx

[15] 「人類首次無人機戰爭 利比亞成中國武器試驗場」，*BBC*，2020 年 6 月 20 日，https://www.bbc.com/zhongwen/trad/world-53097510?at_custom4=61D40FCC-B308-11EA-A873-B2013A982C1E&at_custom3=BBC+Chinese&at_medium=custom7&at_custom2=twitter&at_campaign=64&at_custom1=%5Bpost+type%5D

成為維安的基本認知。

本文所指無人機威脅，意為小型、低空、飛行速度低的無人機，然其大小、酬載、飛行性能實難絕對畫分，《無人機資料庫》（Drone Datebase）將無人機分為三級：

1、第一級（Class I）無人機，本文暫稱為小型無人機，重量在 150 公斤以下，耐航時間約 1~3 小時，最大航程約 80 公里，酬載約 5 公斤，最大時速約 100 公里。此類小型無人機若為定翼式，發射方式包括由手拋擲或車載軌道彈射式，旋翼式則可直接起飛，通常不攜帶武裝。北約另將第一級再分類為微型（micro）、迷你（mini）、小型（small）等三個次類型。

2、第二級（Class II）無人機，有時被稱為戰術無人機，本文暫稱為中型無人機，耐航時間約 10 小時，最大航程約 200 公里。第二級無人機通常為固定翼，需要小型跑道起降，或是較大型的旋翼式無人機，雖然大部分為無武裝，但有些型式可以配備空對地飛彈，與直升機所配備相同。

3、第三級（Class III）無人機，本文暫稱為大型無人機，通常又分為「中高度長航程（MALE）」，以及「高高度長航程（HALE）」兩種。耐航時間超過 24 小時，酬載可達數百公斤，時速可達 300 公里以上，典型的第三級無人機通常供情監偵使用，但也有戰鬥打擊型，有固定翼及旋翼兩種，前者需使用跑道。

另外，美軍則將無人機分為 5 類，Group 1 屬迷你或微型 UAV，為重 20 磅以下的小型無人機，在 1,200 呎以下高度操作，速度低於 100 節；Group 2 為小型戰術無人機，重 21 至 55 磅，在 3,500 呎以下操作，速度低於 250 節；Group3 為戰術型無人機，重逾 55 磅，但不超過 1,320 磅，操作高度在 18,000 呎以下，速度低於 250 節，Group 4 屬持久型無人機，重逾 1,320 磅，在任何速度情況下，於 18,000 呎

以上高度操作;Group 5 為滲透型無人機,也是重逾 1,320 磅,在 18,000 呎以上操作。其中 Group 1 及 Group 2 極難被偵測，構成地面部隊的嚴重威脅，無人機可能有某種酬載，執行情監偵任務或搭載致命性武器；Group2 及 Group3 均由輕量型機體構成，主要亦集中於情監偵任務，其較小的雷達截面積有利躲避偵測；Group 4 及 5 均需較多後勤支援，Group 4 為戰術型，Group 5 則為戰略型，也是無人機中最大的一級。[16]

大型無人機較容易反制，因其飛行特性如體積、高度、速度如同一般飛機，較易加以攔截，一般防空系統即可應付。但小型或迷你無人機飛行速度慢、高度低，甚至低到樹稍高度，使得一般制式防空系統無法應付,且其價格低廉,使用精密且高成本的防空飛彈不僅浪費,甚至也無法應付。此類型無人機可能涵蓋小型及中型無人機，小型或迷你無人機威力有限，僅能用於攻擊重要政經人員或戰鬥部隊，較大型的無人機則可用於攻擊高價值目標，如前所述之煉油廠，創造更大的威脅，但同樣難以防範。

由於導引系統簡單、成本低廉，簡易式自殺無人機更成恐怖攻擊新興手段。不過更致命的是自殺攻擊無人機（kamikaze drone），防空制壓武器即為一種自殺攻擊無人機,代表產品為以色列航太工業公司（Israel Aerospace Industries, IAI）發展的「哈比」無人機,「哈洛普」（Harop）有 2 種導引模式，可執行反輻射任務及一般打擊任務，迷你哈比（Mini Harpy）也可用在廣泛作戰領域。另外，美國、土耳其等其他國家也發展類似的低成本型自殺攻擊無人機，可由迫砲、飛彈發射管、單兵攜行發射，如果其技術擴散，也將成為安全上的重大考驗。

[16] US Army, “Counter-Unmanned Aircraft System Techniques,” *Department of the Army*, April 2017, pp1-2~1-3.

參、無人機反制技術

反制無人機極為困難，傳統防空系統主要用於反制飛機或飛彈的攻擊，雖然技術層次日益精進，成本也大幅增加，然而在反制小型無人機上，為反制無人機威脅，世界各國均加快發展、測試及部署無人機反制系統的速度，以因應此種新興的不對稱威脅。

無人機的反制已成為一項重要課題。儘管可以通過現有的擊殺手段，例如裝備機砲或飛彈的遙控武器系統（RWS），反火箭及迫砲（C-RAM）系統，或是防空飛彈，這些手段通常用以保護固定和高價值目標，部署成本頗高。傳統武器在城市環境的使用也受到嚴格管制，因為其附帶損害的風險極高。[17]

一、高科技蒼蠅拍

為應付無人機威脅，美國正致力於縮小無人機反制系統（Counter Uumanned Air Systems, C-UAS）與一般機動短程防空能力間的差距，其他國家亦然，使無人機反制技術開始蓬勃發展。根據統計，至少有 95 個國家操作軍用無人機，比過去十年增加 58%，與無人機在軍用及民用領域中的運用不斷擴大有關。[18]

無人機反制系統也被視為是維護安全及執法的重要工具，因為由於無人機日益被用於危險或犯罪，因此對有效偵測及反制無人機方法的需求日益迫切。

無人機難以防禦的原因之一是，一般防空系統是設計用以防範飛機的攻擊，有人機是大型快速移動目標，較容易被偵測、追蹤及擊落。但這些防空系統無法偵測小型、移動速度慢、低空飛行的小型無人機，再昂貴精密的防空飛彈都無法對付。2016 年，1 架俄製的簡陋固定翼

[17] "Counter UAV: High Tech Flyswatters," *Asia Military Review*, May 24, 2019, https://asianmilitaryreview.com/2019/05/counter-uav-high-tech-flyswatters/

[18] Dan Gettinger, "the Drone Databook," the Center for the Study of the Drone at Bard College, 2019, https://dronecenter.bard.edu/files/2019/10/CSD-Drone-Databook-Web.pdf

無人機從敘利亞侵入以色列領空，並躲過 2 枚愛國者飛彈，以及以色列空軍戰機的獵殺。

目前在民用領域，無人機尚不需攜帶應答器，因此也無法從現有的空中交通管制系統偵測及追蹤，依賴視覺辨識效果也不佳，即使距離僅剩數百公尺，肉眼依然無法辨識無人機。

鑑於現代國防系統在防範無人機上的空白，使得無人機反制系統開始蓬勃發展，2015 年一項市場調查顯示，這年珊迪亞國家實驗室（Sandia National Laboratories）認證了 12 套無人機反制系統，僅在 5 年之後，市場已經多達 537 套類似系統，同時技術也更為先進，也更瞭解如何反制，然而仍未能解決重大挑戰。

目前反制無人機系統已成為安全裝備市場上重要產品，根據 2018 年一項統計，有 155 家公司銷售無人機反制系統，共有 235 種產品，合作夥伴包括 33 個國家。[19]

二、無人機偵測技術

小型無人機對傳統防空武器帶來極大挑戰，為增進對快速飛機、巡弋飛彈、火箭、彈道飛彈的偵測，傳統防空系統常會過濾掉鳥類、浮空器，以免對防空雷達造成混亂，[20]但這將無法有效應付無人機，因此需使用「不對稱」方式，應付小型 UAV 的威脅，並整合多重方式，以形成反制無人機的「擊殺鏈」，有效反制無人機。

首先，無人機反制系統的感測系統必須能偵測、標定、識別、定位及追蹤來襲的無人機，根據感測器型式，首先進行初步偵測，並需與第二感測器交叉辨識，確認偵測到物體為一架無人機，並確認其精確位置，及追蹤其運動。輔助感測器也可用以提供該無人機的其他訊

[19] Arthur Holland Michel, “Counter-Drone Systems,” Center for the Study of the Drone,2018, P5

[20] “ Countering the UAS Threat from a Joint Perspective,” *Military Review*, November-December, 2015, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20151231_art012.pdf

息，以協助確定其意圖，例如，長距離攝影機可以顯示其是否攜帶爆炸物；有些感測器甚至可以偵測其操作人員位置，其相關數據應可儲存，以利將來作為物證。[21]

其實發展無人機感測系統的技術層級並不高，然而因各種系統在不同作戰環境下操作，例如海上、山區或城鎮地形等，均有其不同盲點，同時可能會被其他目標欺騙，因此無人機反制系統需整合多重偵測手段，彼此互相支援，藉以全方位涵蓋需保護的目標區域，以增進無人機偵測的準確性，並確切阻止無人機威脅。[22]一般而言，一套完整或多功能的無人機偵測系統，包括雷達、無線射頻裝置、紅外線、聽音器、以及綜合式感測器：

1、雷達：需可偵測現有小型無人機的雷達反射訊號，這是無人機反射無線射頻脈衝時被偵測元件所檢知到訊號，這些系統要透過演算法來區分無人機或是其他小型低飛目標，例如鳥類。

2、無線電訊號：可透過掃瞄已知的無線電訊號來偵測無人機，大部分無人機均會在此頻段上操作。

3、電子光學系統：藉由電子光學系統偵測無人機。

4、紅外線系統：藉由熱訊號偵測無人機。

5、音響偵測系統：藉由辨識其馬達所發出的特定音響訊號來偵測無人機，音響辨識系統依賴已知無人機的音響資料庫所提供的聲音訊號，並藉在作戰環境中辨識是否匹配來加以偵測。

6、綜合式感測器：大部分無人機反制系統均整合一系列不同型式的感測器，以提供更綿密的偵測能力。

---

[21] Arthur Holland Michel, " Counter-Drone Systems," Center for the Study of the Drone, December, 2019, 2nd Edition, p.5, https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf

[22] "DRONES AN "IMMEDIATE THREAT": DoD Plans Rapid Acquisition of Counter-UAS Systems," *Breaking Defense*, March, 2020, https://breakingdefense.com/2020/03/ebrief-drones-an-immediate-threat-dod-plans-rapid-acquisition-of-counter-uas-systems/

三、結合硬殺及軟殺的反制方式

由於無人機成本低廉，相對而言使用高成本的防空飛彈攔截無人機並不划算，而且還不一定能用來對付低空、慢速的小型無人機，需結合多重反制手段，包括直接加以擊落的「硬殺」方式，及以干擾等方式使其失效的「軟殺」方式。[23]

其中，軟殺方式包括：1、無線電訊號干擾：破壞無人機與操控站間連繫，使無人機無法降落或返航；2、衛星定位訊號干擾：干擾用以導航的衛星定位訊號，失去定位訊號的無人機將無法標定目標位置，也無法返航；3、電子欺騙：藉傳遞假訊號來控制或誤導目標無人機的通訊及導航，相關方式包括網路攻擊、通訊協定操縱、無線電欺騙、衛星定位訊號欺騙等；4、致盲：以高強度雷射光束「致盲」無人機的攝影機；5、欺騙，藉向無人機提供假訊息，接手控制或將其導引至錯誤目標；6、高能微波，以高能量電磁波使其電子系統失去效用。

在硬殺方面，包括：1、使用運用傳統或特殊設計的彈藥來摧毀無人機；2、撞擊式無人機：運用另一架在空中巡弋的無人機，將來襲無人機加以撞毀；3、攔截網：用來纏住無人機的螺旋槳；4、雷射：使用高能量雷射燒毀機體，使其墜毀。

此外，許多無人機反制系統結合綜合式反制作為，以增加攔截成功的機會，許多干擾系統同時結合無線電干擾及衛星定位干擾功能，其他無人反制系統則將軟殺放在第一線，硬殺則運用在第二線。

四、成熟的無人機反制系統

防範 UAV 攻擊保護部隊、軍事基地及重要關鍵基礎設施，是目前發展反制系統的重要項目。由於各種型式的 UAV 廣泛運用在軍事及攻擊用途，使得防範 UAV 攻擊以保護部隊、軍事基地及重要關鍵

[23] 余雁翔，同前註，頁 33。

基礎設施成為當務之急，美國陸軍及海軍陸戰隊已提出多種反制措施，將用以保護前線部隊。目前已有多種成熟或發展完成的無人機反制系統，或是短程防空系統，有利於反制無人機威脅，其中包括陸軍野戰防空系統、以無人機對抗無人機方式，以及雷射系統等，也有軍火廠商提出完整的反制系統，涵蓋雷達及光電偵測，以及由干擾到飛彈，以及 UAV 反制等多種措施。

（一）雷射系統

目前雷射武器已廣泛用於短程防空，對付無人機、巡弋飛彈等低空或低成本的威脅，美歐許多軍火集團均推出雷射防空系統，同時雷射發射成本低廉，如能解決電力供應問題，發射一次的成本僅約為一美元，遠遠低於飛彈，只是目前仍需設法提升雷射的功率。以雷神的高能雷射武器系統（High-Energy Laser Weapon System, HELWS），使用一套「多光譜目標標定系統」（Multi-spectral Targeting System），以光電及紅外線偵測、辨識及追蹤無人機，並以高能量雷射加以摧毀。這套雷射裝置在一種小型的全地形車輛上，可使用標準的 220 伏特電源線充電，除供應光電偵蒐系統外，還可供雷射發射數十次。[24]

（二）以蜂群加以反制

美國陸軍發展的群集式（Swarm）自殺攻擊無人機，裝置在集束炸彈內，可攻擊多重目標。美國雷神公司發展的「郊狼」系統（Coyote）也衍生為低成本自殺攻擊無人機，即以撞擊或自爆方式攻擊目標，體型與多管火箭一般大小，也可用於監視戰場，並可以群集方式大量發射，在戰場上自動化操作。AeroVironment 的「彈簧刀」（Switchblade）戰術式自主攻擊無人機，也是以小型化無人機對即時目標發動精準打擊。

「郊狼」無人機是以撞擊或自爆方式攻擊目標，其體型像一般多

[24] "The Air Force just fielded its first high-energy laser weapon overseas," *Task & Purpose*, April 6, 2020, https://taskandpurpose.com/military-tech/air-force-laser-weapon-fielding

管火箭或是反潛機上的聲納浮標那樣大小，可用原來的發射管發射，原本是用於改善戰場監視能力，以群集（Swarm）概念大量發射，在戰場上自動化操作，無須人工控制，除戰場監測外，也可用以氣象觀察。土狼無人機曾成功用於颶風探測，此次雷神用土狼無人機在空中偵測其他無人機並加以攻擊，一發的攻擊成本低於其他武器系統，也有多種衍生型，酬載可彈性挑選，並可加裝加力器以增加航程及速度。

（三）野戰防空系統

除保護基礎設施外，野戰部隊也受到無人機嚴重威脅，因此各國軍方都較過去更為重視短程及野戰防空能力，用以保護作戰部隊，不受無人機威脅。美國陸軍發展中的「機動短程空防系統」(Mobile Short-Range Air Defence, MSHORAD)，雖然目的是補足陸軍機動短程防空能力的不足，其主要用於反制 C-RAMM(counter rocket, artillery, mortar and missile，反火箭、砲彈、迫砲與飛彈)，但對低空慢速目標也具備一定打擊能力。[25]

（四）多重反制方式

目前已有多家軍火商、科技公司及研發單位提出偵測及反制無人機的解決方案。在各大軍火集團中，雷神公司提出的措施最為完整，涵蓋雷達及光電偵測，以及由干擾到飛彈，以及 UAV 反制等多種措施。這套系統其實已開發一段時間，主要是因應陸軍野戰防空的需求，由 AN／MPQ-64 短程 3D 防空雷達、KuRFS（Ku 波段無線射頻系統）雷達組成，以標定跨光譜的威脅。

反制方式則十分多樣化，在武器方面，可以整合陸軍所有可用的防空系統，包括刺針肩射飛彈、鐵穹（Iron Dome）飛彈系統、挪威的先進飛彈系統（NASAMS）是一種分散式、網路化的中至長程防空飛

[25] " New air defense threats mean new equipment and new ways of defending," Defense News, October 20, 2019, https://www.defensenews.com/news/your-army/2019/10/20/new-air-defense-threats-mean-new-equipment-and-new-ways-of-defending/

彈系統，其實就是「陸基先進中程空對空飛彈」（AIM-120, SL-AMRAAM），由挪威康斯堡（Kongsberg）與雷神共同開發，另也包括愛國者防空飛彈，射程涵蓋短至長程。

哨兵雷達及雷射系統的實車體積小，雷達為拖曳式，可由任何陸軍車輛拖行，雷射則裝載在小型越野車上，充分展現彈性部署能力。雷神的雷達及光電系統並未架高，對低高度飛行的 UAV 效果如何就不得而知。

瑞典 SAAB 的長頸鹿雷達 AME（Giraffe AMB）為車載式、可由舉升臂升高的雷達，對付飛行高度不高的 UAV 頗具實效，具極佳目標辨視率，可接戰多重目標，具多任務能力，特別是針對小型目標，如無人機，其架高設計，可越過樹稍高度，偵測低飛目標。長頸鹿雷達可整合其他系統，如 MBDA 的強化模組式防空解決系統（EMADS）中，使用 8 聯裝共同防空模組飛彈（CAMM）或是延程型（CAMM-ER），可快速部署，在狹窄空間對付任何空中威脅，飛彈採軟射式垂直發射，減少發射位置訊號，可使用不同武器，結合任何監視系統，因採垂直發射，可涵蓋 360 度範圍。

無人機反制系統並非大型軍火集團專利，小型公司或研究團隊也都推出反制 UAV 的解決方案，主要是以小型悍馬車載運，保護基地、前進部署部隊、關鍵基礎設施，採用微波干擾方式加以中和 UAV 威脅。未來的中和威脅方式則包括高能雷射、微波及製造亂流等。

肆、結論

無人機已成為國家安全的嚴重威脅，中國不但是無人機生產大國，其大量出口至中東國家的無人機也被用於作戰中，其無人機產品大量應用在各種領域，除軍事用途，也運用在不對稱戰術戰法上。台灣未來會面對中國無人機的高度威脅，除大型無人機以偵打一體或自殺攻擊方式，在台海衝突中被運用之外，小型無人機也可能運用在灰

區衝突，或是特種任務中，用以攻擊關鍵設施或政府高層。

國軍目前擁有可涵蓋高、中、低空層的防空飛彈，例如愛國者二、三型飛彈、天弓二、三型飛彈，屬防空飛彈指揮部，短程飛彈目前為檉樹飛彈，未來將採購陸射劍二飛彈，屬陸軍砲兵指揮部，單兵發射的刺針飛彈則將編配各旅。對於應付極低空飛行的無人機，或是更小更慢的迷你無人機，除使用干擾槍外，尚無有效應付方法，防空飛彈不可能用於低價的無人機，而且若在人口密集區域，尚可能造成附加傷亡。另外，國軍目前也無有效偵測無人機的裝備。

為應付無人機威脅，國軍應將發展無人機反制系統列為國防自主的重要項目，整合偵測、指管通情能力及不同接戰方式，以國軍現有的成熟系統，並參考其他國家的發展經驗及思考模式，如結合中科院現有的蜂眼雷達或雙基雷達等系統，加上民間研發團隊發展的紅外線、被動偵測等方式，並設法使防空系統能連網，以利互相支援。在反制方面，同時結合多種干擾或擊殺無人機，如機砲、短程飛彈，並多層部署，減少應付此種不對稱威脅的成本，徹底消除無人機威脅，保護地面作戰部隊、重要關鍵基礎設施、軍事基地、政經中樞與重要軍政人員安全。

本文作者舒孝煌為淡江大學國際事務與戰略研究所博士，現為財團法人國防安全研究院先進科技與作戰概念研究所助理研究員。

Asymmetric Warfare: A Counter-Drone Approach

Hsiao-Huang Shu

Assistant Research Fellow

Abstract

Drones or Unmanned Air Vehicle are increasingly used in Asymmetric Warfare. There are many types of drones, medium and large drones can perform long-range, large payload complex tasks, usually used by government agencies, military units and business groups, but small or mini drones are very easy to purchase, with small size, low technical level , easy to deploy, flight slow and low altitude, difficult to detect and other characteristics. If equipped with weapons, it has the potential for lethal strike. Drones have become a serious threat to national defense security.

Countering drones is extremely difficult. The cost of using drones is not high, but opponents have to increase a lot of costs to deal with drones. Traditional air defense systems are mainly used to anti aircraft or ballistic missile. They still can't effectively counter small drones, and the cost is too high. Many countries are accelerating the development of UAV countermeasure systems in response to this emerging asymmetric threat.
China has become a major producer of drones. In addition to the commercial field, the PLA also makes extensive use of drones. China also exports drones to Middle Eastern countries. Due to the high threat of Chinese drones, Taiwan should strengthen the development of counter-drone systems, integrate existing command and communication systems and different engagement methods, and develop other technologies to counter UAV threats.

不對稱戰：陸基精準武器的途徑

許智翔

先進科技與作戰概念研究所

壹、前言

矛與盾的對抗，在軍事議題上向來是長時間存在的問題，「彈藥」（ammunition）與「載台」（platform）之間的選擇問題，在二戰後精準導引武器逐漸開始大量服役後，更成為軍事上經常探討的重要議題。如 1973 年贖罪日戰役（Yom Kippur War）中，以色列裝甲部隊在西奈半島遭致當時埃及部隊配備的反裝甲武器（如俄製 9M14「嬰兒」Malyutka、北約代號 AT-3「火泥箱」反戰車飛彈）迎頭痛擊的戰例，就曾引發主戰車是否能在未來戰場生存之爭論。

近年，長程精準導引武器的持續發展與擴散，使得類似的議題更成為檯面上的焦點。現代精準導引武器不論巡弋飛彈、彈道飛彈或防空系統，其性能與射程都非過去所能相比。儘管射程長短在不同武器系統上定義各異，如美國的空射反艦飛彈 AGM-158「聯合空對地遙攻飛彈」（Joint Air-to-Surface Standoff Missile, JASSM）的射程逐漸由 370 公里延伸至 JASSM-ER（增程）型的 925 公里，新式的 JASSM-XR 將進一步大型化、而射程更延伸至 1,600 公里之遠，而長程空對空飛彈的射程則約為一百餘公里。但在武器射程大幅延伸之下，陸基的精準導引武器將可在台灣海峽及台灣西半部，成為重要的不對稱作戰工具，台灣應可藉由加強陸基機動精準導引彈藥的戰力，強化對抗中共優勢海空戰力的能力，並使傳統高價載台能得到更有效的運用。

貳、精準武器發展威脅大型海空載台

一、以「彈藥」對抗「載台」的作戰方式存在已久

小型載台透過投射威力強大彈藥以對抗高價大型載台的作戰方

式，在戰史上存在已久，過往最明顯的例子，或許是 19 世紀中後期魚雷的出現。這種威力強大的彈藥，使得小型船艦（如魚雷艇、驅逐艦等）能對具備重甲及大砲的大型艦艇（如戰艦 battleship 等）形成重要威脅。

類似的威脅在精準導引武器出現、並逐漸成為主流後更進一步提升。1967 年，埃及飛彈快艇運用俄製 P-15「白蟻」（Termit）反艦飛彈（北約代號 SS-N-2「冥河」飛彈）擊沈以色列的「埃拉特」號（*INS Eilat*）驅逐艦，首開反艦飛彈擊沈船艦的紀錄，正是小型船艇透過現代精準導引武器對抗大型艦艇在近代的第一個重要例證。

精準導引武器的進步，使較弱勢的一方，得以強化其與強勢對手的大型高價載台對抗的能力。同樣以海軍作戰為例，為對抗美國海軍及北約的強大戰力，前蘇聯在冷戰時期也同樣透過海軍航空隊、運用 Tu-22M（北約代號「逆火」）等轟炸機以飽和攻擊（Saturation Attack）方式，投射大量長程反艦飛彈以對抗強大的美國海軍航艦戰鬥群。

在過往的發展中，不僅是海上兵力較弱勢的蘇聯採取類似發展方式，在兩強對抗中整體兵力數量佔據劣勢的美國及西方陣營，也採取了同樣的發展方向。冷戰期間美國的「第二次抵銷戰略」（Second Offset Strategy）核心之一，正是以精準導引武器等高科技裝備，對抗蘇聯及華約的龐大兵力優勢，[1]並藉此建構了美國及西方在後冷戰時期強大軍事實力的基礎。

二、先進彈藥帶來強大「致命性」威脅現代主戰載台

先進彈藥對於各種高價載台的威脅，近年來不僅在海上作戰方面，在陸空等方面也同樣受到重視。整合式防空系統（integrated air defense systems, IADS）並非全新的概念，然俄中在現代透過長程防空

[1] Adam J. Boyd and Michael Kimball, “The Future Operating Environment and the Third Offset: the Implications of the third Offset Strategy for the U.S. Army,” US Army War College, 2017, p.7, https://www.jstor.org/stable/pdf/resrep12117.5.pdf.

飛彈如 S-400（北約代號 SA-21）及 S-300V4（北約代號 SA-23）等，搭配各式機動中短程防空飛彈，加上包含空中預警機在內、各式感測系統與現代通聯及鏈路系統，形成一涵蓋數百公里範圍的綿密防空網、以此對抗美國及北約的空中優勢。這些先進防空火力與彈道飛彈及巡弋飛彈等火力，共同構成「反介入／區域拒止」（anti-access/area-denial, A2/AD）能力的核心。[2]此外，在陸戰領域上，先進精準導引武器也同樣對主戰載台持續造成威脅，不論美製 M1A2、德製豹 2A4 及俄製 T-90 等現代先進主戰車，都在中東地區的戰事中因反戰車飛彈的攻擊遭受損失，顯示在地面作戰中、精準導引武器對於高價裝備所同樣造成之威脅同樣龐大。

換言之，精準導引武器由於技術的進步，其「致命性」（lethality）大幅增加，使相對弱勢的一方通常可以運用具備良好「致命性」的精準導引武器，對抗敵方在質或量上的相對優勢。因此，資源較為不豐的國家，在建軍備戰時依其自身能力及安全威脅考量，將可能加強在「彈藥」上的投資。

三、長程精準武器為美國的「島鏈防禦」戰略核心

長程精準導引武器不僅在近年成為俄羅斯及中國對抗西方部隊的 A2/AD 利器，同樣的方式為美國所參考，形成其對抗中俄的利器，近期美軍的調整，不論是退出《中程核武條約》（Intermediate-Range Nuclear Forces Treaty, INF），還是美國陸軍在多領域作戰（multi domain operations）下的發展方向、及美國海軍陸戰隊的轉型上，皆可看出其將戰略重心逐漸轉移至印太地區、尤其是在西太平洋及第一島鏈等區域，並將透過精準導引武器等多種措施，將島鏈形成美國與西太平洋

[2] Justin Bronk, "Modern Russian and Chinese Integrated Air Defence Systems The Nature of the Threat, Growth Trajectory and Western Options," *Royal United Services Institute*, January 2020, https://rusi.org/sites/default/files/20191118_iads_bronk_web_final.pdf.

盟國的現代「長城」。[3]2019 年 5 月，美國智庫「戰略與預算評估中心」（Center for Strategic and Budgetary Assessments, CSBA）即建議美國採取「海上壓力」（maritime pressure）戰略，在第一島鏈上、即中共 A2/AD 能力範圍內部署陸基防空與反艦火力，配置大量精準打擊火力，並以較遠距離的海空兵力輔助對抗中共。[4]

美國此種「島鏈防禦」戰略，或可追溯至前蘇聯及中共在海軍上運用的「稜堡」（bastion）戰略。冷戰時，由於與美國在海軍實力上的差距過大，蘇聯為保護其核嚇阻力量中最重要的彈道飛彈潛艦，在己方所能有效控制的地區，透過層層海空防線及精準導引武器的輔助，形成一「稜堡」以保護彈道飛彈潛艦的。近年，中共除透過類似方式，建立強大的「稜堡」以保護其海軍重要資產外，[5]由於長程精準導引武器的蓬勃發展，中共的各個「稜堡」逐漸成為攻守能力強大的前線堡壘，並藉由長程、進攻性的火力控制附近相當面積的海域。此種情況下，美國開始加強發展其長程精準導引武器，並藉此在西太平洋前線形成美國版「稜堡」，並威脅縱深短淺的東海及黃海地區、挑戰中共的「稜堡」戰略。[6]

而儘管美軍手上擁有包含前述「聯合空對地遙攻飛彈」等，以及目前正研發將取代陸軍戰術飛彈（Army Tactical Missile System, ATACMS）的「精確打擊飛彈」（Precision Strike Missile, PrSM），還是在退出 INF 後進一步在美國陸軍在「多領域作戰」發展方向下所研發之中程彈道飛彈等，多種可用於部署在第一島鏈上的各重要據點的長程武器在

[3] James Holmes, “The Ultimate Way to Deter China: Why Island-Chain Defense Can Work,” June 10, 2019, https://nationalinterest.org/blog/buzz/ultimate-way-deter-china-why-island-chain-defense-can-work-61942.

[4] Thomas G. Mahnken, et.al., “Tightening the Chain: Implementing a Strategy of Maritime Pressure in the Western Pacific,” Center for Strategic and Budgetary Assessments, May 23, 2019, https://csbaonline.org/research/publications/implementing-a-strategy-of-maritime-pressure-in-the-western-pacific.

[5] Robert Farley, “China’s Aircraft Carriers and Nuclear Bastion Defense,” *The Diplomat*, May 11, 2017, https://thediplomat.com/2017/05/chinas-aircraft-carriers-and-nuclear-bastion-defense/.

[6] James Lacey, “BATTLE OF THE BASTIONS,” *War on the Rocks*, January 9, 2020, https://warontherocks.com/2020/01/battle-of-the-bastions/.

內，多樣化且大量的精準導引攻擊能量，然而美軍地面部隊正在為此進一步強化其能力，更展開作戰概念及組織上的轉型。除了陸軍發展的「多領域作戰」外，美國海軍陸戰隊也開始進行近年最大的變革，將淘汰所有戰車營，轉型成能快速在島嶼上部署長程精準導引武器的部隊，協助美國海軍制海、並藉由第一島鏈與中國大陸間的短淺縱深壓制中國海軍及其基地。而同樣的發展方向，或可作為台灣在同一個區域內遂行防衛作戰的重要參考。

參、陸基精準導引武器可成台灣不對稱作戰利器

一、海峽與台灣西半部成為現代「無人地帶」抵擋入侵

前述精準導引武器在現代戰場上發揮的作用來看，台灣在整體的守勢作戰上，將可進一步運用陸基的長程精準導引武器對海空目標，形成一現代版的「無人地帶」(no man's land)。

「無人地帶」意指在 1914 年至 1918 年的一次大戰的西部戰線中，德國與協約國雙方在狹窄正面透過連綿不對的戰壕、鐵絲網、機槍、地雷以及大砲等各種兵火力與防禦工事綿密交織，形成一個部隊難以通過、並需付出極大人命代價的地區。

從台海的防衛作戰需求中，儘管中共對台可能採取多種非軍事及軍事手段，然而對台灣而言最大的安全威脅，仍是海空的全面入侵，也正因此台灣目前的「整體防衛構想」也將重心置於此方面。從這個角度探討，在今日的兩岸軍事情勢上，平均寬度 180 公里的台灣海峽，儘管仍具備相當程度的屏障、能對試圖渡海入侵的敵軍，在登陸作戰上形成強大天然阻礙。然在現代具備相當射程及精準度的先進導引武器輔助下，台灣海峽扮演的傳統「天險」角色，對於在這個區域活動的大型載台而言，或許不再絕對。

就目前兩岸裝備的長程精密導引武器而言，不論中共配備的俄製 S-400、S-300 等長程防空系統，還是台灣方面裝備的「天弓」系列防

空飛彈，或是各式反艦及巡弋飛彈等，幾乎可使說雙方機艦在台灣海峽或西半部活動時，將面對同樣的風險：即在大量的長程精準武器威脅下，雙方機艦在這個地區活動時，都將遭致大量此類武器的攻擊導致巨大威脅及損失。換言之，在未來的台海戰場環境下，台灣的西半部以及海峽當面，將可能因為這類具備較長射程的先進精準導引武器，而形成一個現代版的「無人地帶」，各種高價、高性能的載台如航空器與船艦在此區中會遭遇極大生存壓力甚或承受相當損失。

二、藉「以陸制海」及「以陸制空」手段遂行不對稱作戰

從前述角度進一步推論，則在台海區域及台灣西半部的不對稱防衛作戰上，透過地面的精準導引武器「以陸制海」及「以陸制空」，對中共在數量上佔據優勢的海空兵力進行不對稱作戰。

前述的「以陸制海」及「以陸制空」在精準導引武器蓬勃發展的今日並不是全新的概念。前述中共藉由彈道飛彈等裝備對美軍艦隊形成的威脅，及前述美國的「島鏈防禦」戰略，都是此種作戰概念的實踐。就台海的作戰環境而言，由於前述的台海短淺縱深，以及雙方先進長程精準武器所造成的現代「無人地帶」，將意味著台灣的地面部隊（包含陸軍、海軍陸戰隊、海空軍的地面單位如防空及海鋒大隊等應可加強裝備各種精準導引武器，並在這個作戰環境中成為關鍵核心力量，以不對稱方式對抗中共兵力。

近年來，美國的學者或重要智庫如蘭德公司（RAND Corporation）等，在分析台灣的防衛作戰時，也多次提出類似建議。2008 年美國海軍戰院教授莫瑞（William S. Murray）提出「豪豬戰略」（Porcupine Strategy），認為在中共軍力的急速發展，台灣海空軍將可能因共軍的打擊能力而難以發揮作用，並主張台灣應強化陸基反艦飛彈、攻擊直升機、多管火箭（MLRS）及水雷等，並維持先進裝甲、火砲及反甲

武器等，[7]對陸基精準導引武器的建議也多見於其他相關報告中。2014年CSBA的《HARD ROC 2.0》報告認為台灣陸海空均須強化精準導引及機動、隱蔽的能力，因此建議台灣應強化投資包含陸基機動反艦飛彈，機動防空飛彈在內的裝備，甚至投入生產大量僅120噸的小型潛艦等。[8]2017年蘭德公司針對台灣空防能力，也提出建議認為最佳方案是僅保留50架改良後的F-16戰機、並以大量防空飛彈取代現有的機隊。[9]喬治梅森大學（George Mason University）的《時間問題》（*A Question of Time*）報告也認為，與其投注在高科技先進載台上，台灣更應強化精準彈藥在內的高致命性武器，並強化部隊的生存性及數量，以達成有效的嚇阻能力。[10]儘管諸多報告中對於台灣建軍方向的建議或許激進，然而其強化彈藥面的投資，加強數量及投射能力的共通主要目標卻顯而易見。

三、「機動性」及「生存性」為地面部隊遂行不對稱作戰關鍵要素

前述的智庫及學者建議中，可注意到機動性是另一個普遍受到重視的核心考量。由於中共在海空方面仍具備極大優勢，同時台灣西半部同樣籠罩在中共的精準火力打擊範圍內，因此儘管「以陸制海」及「以陸制空」概念應能成為有效手段，不對稱對抗可能的海空入侵。但這些裝備及其相關重要支援設備皆應具備高度機動性、以提高其生存性。這是由於中共目前的長程對地精準導引武器，主要仍以彈道飛彈或長劍系列巡弋飛彈為主，此類遙攻（Stand-Off Weapon）武器主

[7] William S. Murray, "Revisiting Taiwan 's Defense Strategy," *Naval War College Review*: Vol.61, No.3, 2008, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1814&context=nwc-review.

[8] Jim Thomas, et.al., "HARD ROC 2.0: TAIWAN AND DETERRENCE THROUGH PROTRACTION," Center for Strategic and Budgetary Assessments, December 21, 2014, https://csbaonline.org/research/publications/hard-roc-2-0-taiwan-and-deterrence-through-protraction.

[9] Michael J. Lostumbo, et.al., "Air Defense Options for Taiwan: An Assessment of Relative Costs and Operational Benefits," RAND Corporation, 2016, https://www.rand.org/pubs/research_reports/RR1051.html.

[10] Michael A. Hunzeker, et.al., "A QUESTION OF TIME Enhancing Taiwan's Conventional Deterrence Posture," Center for Security Policy Studies at George Mason University, November 15, 2018, http://cimsec.org/a-question-of-time-enhancing-taiwans-maritime-deterrence-posture/38830.

要應仍用於攻擊固定及具備有限機動能力的目標（如機場與雷達站等），而對較小、且具備高度機動力的單位（如車輛）的威脅則相對較低，因此機動性以及小型化（相對於傳統的固定大型設施）同樣是在此種不對稱作戰思維下，所必須強化的發展方向，藉以強化地面單位的生存能力。

關於在敵空中優勢下，地面部隊的生存能力，或可由 1999 年科索沃戰爭中，北約對塞爾維亞地面部隊的空中攻擊中一窺。在具備強大精準打擊支援能力的北約盟軍發動長達 79 天的空襲下，塞爾維亞陸軍藉由長時間投資的各種掩體、偽裝、誘餌等良好戰場經營，及小型機動車輛對空襲的難度等因素，成功的保存了其地面部隊主力，僅擊中賽軍 600 輛戰車中的 93 輛、600 輛裝甲運兵車中的 153 輛，[11]顯示地面機動單位仍有對抗精準打擊能力的存活空間。

四、投資不對稱戰力外仍應維持全面性作戰能力

然而，必須注意的是前述的「以陸制海」以及「以陸制空」的概念，並非將以陸基防空與反艦武器完全取代傳統的戰機及水面作戰艦艇等裝備。儘管在海峽與台灣西半部缺乏縱深的地區而言，長程精準導引武器確實可對中共的優勢海空兵力造成相當威脅，然而不對稱手段的裝備如防空飛彈等，在用途上相對單一。同時，中共對台可能的軍事威脅手段亦不僅有海空全面入侵等方式，因此為求具備全面性的作戰能力，以因應可能的各種狀況，傳統載台如戰機及較多用途的大型作戰艦在整體防衛作戰中仍能扮演一定角色。同時由於這些載台具備較高的運用彈性，在有效保存其戰力的同時，在適當運用下可進一步強化台灣取得戰略及作戰節奏上主動權的能力。

因此，就不同的戰場環境需求來看，在台灣的整體防衛作戰中，

[11] "How the Serb army escaped Nato 'They came out to burn villages when they wanted to, they hid when the weather was good'," *Guardian*, March 9, 2000, https://www.theguardian.com/world/2000/mar/09/balkans1.

西半部及海峽方面透過陸基精準導引武器，對共軍的海空優勢兵力進行不對稱作戰時，除能以有效方式對抗中國的海空優勢兵力外，亦可「釋放」原有的傳統高價海空載台能量，將其投入在其他方面的重要任務，如台灣東部及外海的制空、反艦任務等，甚至探討更有效率的任務運用，除了避免重要的高價載台在西半部的「無人區」過度消耗外，更能增加國軍整體的兵力運用彈性。

肆、小結

儘管基本戰力與不對稱戰力在實際戰場上無法偏廢任何一項，然而在面對中共絕對的數量優勢時，需進一步考量如何以不對稱手段「抵銷」中共海空優勢的方式。精準導引武器的蓬勃發展及射程的持續增加，能為台灣在防衛作戰時強化部隊的「致命性」，以有效對抗中共的龐大兵力。考量台灣海峽及西半部的短淺綜深，以及長程精準導引武器的威力，雙方部隊在這個區域活動時，面對這些武器所遇到的威脅其實是同等的。換言之，透過精準導引武器的作為西半部及海峽的主要防禦手段，將是國軍值得嘗試的發展方向。而由於台灣整體國力有限，因此在發展此類戰力的方向上，或許應進一步投注更多資源加以強化，以面對持續增加的兩岸軍力差距。

本文作者許智翔為德國杜賓根大學博士，現為財團法人國防安全研究院先進科技與作戰概念研究所博士後研究。

Asymmetric Warfare: A Ground-based Precision Weapon Approach

Jyh-Shyang Sheu

Postdoctoral Fellow

Abstract

With the development of modern weapon technologies, the precision guided munitions（PGMs）highly threaten the survivability of the large/expensive platforms such as aircrafts and surface combatants. Considering the lack of depth regarding the defense of Taiwan, large numbers of PGMs might create a “modern no-man’s land” in the Taiwan Strait and the western part of Taiwan. Activities of the naval and air units would be largely threatened and restricted in this area. Therefore, to enhance the ground-based long-range PGMs could be an effective approach for offsetting the Chinese naval and air advantages. Nevertheless, although the ground-based PGMs could be effective as an asymmetric capability, all these ground units should have high mobility in order to survive in the modern battlefield when facing the Chinese military.

不對稱戰：資訊作戰途徑

章榮明

量化分析暨決策推演中心

壹、前言

不對稱作戰的特性之一在於避實擊虛，就是迴避敵人最強之處，而集中一切力量，攻擊敵人最關鍵的弱點。也就是孫子兵法的始記篇所說：「兵者，詭道也。…強而避之…攻其無備、出其不意…。」[1]資訊戰（information warfare）在 1991 年波灣戰爭受到大量運用，使得該戰爭被稱為「第一次資訊戰」。[2]由於資訊戰的使用方式符合不對稱作戰避實擊虛的特性，因而可視為不對稱作戰的一種途徑。

貳、資訊作戰的定義與演進

首先在此釐清資訊戰與資訊作戰（information operation）。根據 1998 年版《美軍聯戰準則 3-13》，資訊戰是指「為影響敵方資訊及資訊系統，同時保護己方資訊和資訊系統所採取的各種行動。」[3]根據 2014 年 2 月 14 日發布的《參謀首長聯席會議主席指導 3210.01C》（*Chairman of the Joint Chiefs of Staff Instruction, CJCSI, 3210.01C*），資訊作戰的定義是「在軍事行動時整合運用資訊相關能力，配合其他行動，以影響、阻撓、破壞、或奪取對手與潛在對手的決策制定，同時保護我們自己的。」[4]由上可知，資訊戰停留在軍事行動的層次，而資訊作戰則包含了軍事行動及其他行動，因此範圍較廣。

---

[1] 王建東，《孫子兵法大全》，華威國際，2016 年，頁 17。

[2] Alan Campen, *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War*, （AFCEA International Press, 1992）.

[3] Joint Chiefs of Staff, Joint Pub 3-13: Joint Doctrine for Information Operations （Washington, DC: Joint Chiefs of Staff, 1998）, p. vii 轉引自葉志偉，〈美軍資訊作戰聯戰準則之演進〉，《海軍學術雙月刊》，2017 年 4 月 1 日，第 51 卷第 2 期，頁 78。

[4] "Chairman of the Joint Chiefs of Staff Instruction 3210.01C," Chairman of the Joint Chiefs of Staff, February 14, 2014, https://reurl.cc/exbRLm.

近代資訊戰概念的提出，通常認為是羅納（Thomas Rona）於 1976 年向美國國防部提出的一份名為《武器系統與資訊戰》（*Weapons Systems and Information War*）的報告。該報告主張美國的商業發展與資訊發展密不可分，導致資訊系統極可能成為未來受到攻擊的目標。[5]值得注意的是，該報告所點出的並非美國未來應如何進行資訊作戰，而是從敵人發動資訊作戰的角度，來反觀美國該如何進行防衛。

波灣戰爭結束後的十年間，是資訊戰研究蓬勃發展的時期。首先是 1992 年美國國防部所提出的《國防部指引 TS3600.1》（*DOD Directive TS3600.1*），指出資訊戰下的電腦網路攻擊必須防範。[6]隔年，美國智庫蘭德公司（RAND）提出《戰略性資訊戰》（*Strategic Information Warfare*）的報告。該報告認為未來對美國的攻擊將不分平時或戰時、軍事或民用設施、前線或後方，造成分界線的模糊化（blurred traditional boundaries）。值得注意的是，該報告的撰寫過程中，曾進行了六次兵推，每次兵推的結果都納入隔次的兵推，完善了報告的內容。[7]

根據 2000 年 5 月 30 日美國國防部所公布的《共同願景 2020》（*Joint Vision 2020*），「全光譜的支配地位」（full-spectrum dominance）是美軍在 2020 年的願景；不對稱作戰則是美軍在 2020 年所要面對的重大挑戰，而確保資訊優勢（information superiority）則是美軍達成願景的要素之一。[8]

資訊作戰具有以下特性：（1）避免短兵相接。資訊戰的優點在於避免武力的實際接觸，卻仍能達成目的。（2）破除疆界的限制。在

---

[5] 轉引自 Myriam Dunn Cavelty, Cyber-Security and Threat Politics: US Efforts to Secure the Information Age, Routledge （2008）, p.44.

[6] 《國防部指引 TS3600.1》被列為機密，並未對外公開，但其內容透過後來的發展而逐漸顯露出來。關於資訊戰的七個種類，請見 Martin Libicki, *What is Information Warfare*, U.S. Government Printing Office, （1995）, p. 7.

[7] Molander, Roger, Andrew S. Riddile and Peter A. Wilson. *Strategic Information Warfare: A New Facet of War*, （RAND, 1996）.

[8] *Joint Vision 2020*, U.S. Department of State, May 30, 2000, U.S. Government Printing Office,（2000）.

資訊作戰之下，傳統認知的前線與後方、國外與國內的意義不大。敵人不須先擊潰前線才能攻擊後方，敵人可以跳過前線而直接攻擊後方；甚至敵人可以同時攻擊前、後方。（3）虛實難辨。一個成功的訊息必然包括一些事實，先讓人信以為真，以便於接受該訊息內添加的一些非事實。經由資訊作戰的不對稱作戰特性，避實擊虛，造成對手無法可戰，無力可戰，確有可能達到孫子所說的不戰而屈人之兵。

參、資訊作戰的案例

資訊作戰案例近年來大幅增加，且使用之科技程度日新月異。以下列舉幾個資訊戰手段針對「關鍵基礎設施」（Critical Infrastructure Sectors, CIS）實施打擊，並造成實體損壞（physical damage）的實例。

一、伊朗核子研究設施病毒事件

伊朗於 2006 年重啟核計畫。三年後，伊朗位於納坦茲（Natanz）的核子研究設施的 1,000 具分離鈾的離心機突然異常加速，並因而受損，佔了該設施所有離心機數量的五分之一。其立即的影響是延後了伊朗提煉濃縮鈾的時程。[9]經過深入的調查，網路資安公司於 2010 年 6 月發現該事件是由一種叫做「震網病毒」（Stuxnet virus）的蠕蟲病毒所造成。[10]進一步的調查，發現該病毒早於 2007 年就被植入納坦茲濃縮鈾提煉廠的電腦。一般認為是美國的中央情報局與以色列的摩薩德（Mossad）聯手製造了該病毒，但由於該提煉廠控制離心機的相關電腦並未連上網路，因而如何中毒成為一個未解的謎。2019 年的新聞報導，解開了這個謎。引述四個不同的消息來源，報導指出該事件乃是由荷蘭的「情報與安全總局」（Algemene Inlichtingen- en Veiligheidsdienst, AIVD）出面，吸收了一位在該濃縮鈾提煉廠工作的

[9] 吳俊德，〈伊朗與美國之網路衝突〉，《國防安全週報》，2019 年 10 月 18 日，第 69 期，頁 31-34。

[10] 該病毒亦被稱為「超級工廠」。

伊朗工程師，並交付該工程師儲存了「震網病毒」的隨身碟，再由該工程師將隨身碟插入納坦茲提煉廠內控制離心機的電腦，順利將病毒植入電腦。[11]在該事件中，避實擊虛的原則再次獲得採用，是不對稱作戰的一個案例。

二、烏克蘭電網受攻擊事件

2015 年 12 月 23 日，烏克蘭首都基輔市部分地區與烏克蘭西部約 70 萬戶遭遇了突如其來的停電，長達 3 至 6 小時。同時，停電戶接到假電話，讓他們誤以為相關單位已經知道了停電的狀況，他們也就無須回報。根據調查，該起停電事件是由駭客組織「沙蟲」（Sandworm）以電子郵件的方式，散播 Black Energy 3 病毒給基輔電廠的高階主管。待郵件被開啟後，電腦隨即被植入病毒，駭客組織便藉由這個病毒遙控電廠內的控制電腦，導致該起停電事件。[12]2016 年 12 月 17 日，烏克蘭基輔州北部的村莊新佩特里夫齊（Novi Petrivts），因變電所的自動控制系統故障造成停電。該次停電時間持續 30 分鐘，經由電力公司的工程師切換至手動控制模式，30 分鐘後逐漸開始恢復供電。[13]2015 年負責該變電所資安的西門子（Siemens）公司曾釋出修理程式，但並非所有控制電腦均下載了該程式；未下載該程式的電腦因而成為駭客植入「當機覆寫」（Crash Override）病毒的漏洞，從而導致該起停電事件。以上兩起事件均被認為是俄羅斯境內的駭客組織所為。

---

[11] "'Dutch mole' planted Stuxnet virus in Iran nuclear site on behalf of CIA, Mossad," *The Times of Israel*, September 3, 2019, https://reurl.cc/Mvx1RL.

[12] "Hackers behind Ukraine power cuts, says US report," *BBC*, February 26, 2016, https://reurl.cc/vDO0Vo； "Hackers caused a major blackout for the first time," *Business Insider*, January 6, 2016, https://reurl.cc/AqmjgZ.

[13] 〈烏克蘭再次發生大規模停電，疑遭駭客攻擊〉,《行政院國家資通安全會報技術服務中心》, 2017 年 1 月 9 日，https://reurl.cc/ZO397A.

三、沙烏地阿拉伯油氣工廠受攻擊事件

2017 年 8 月 4 日，位於沙烏地阿拉伯的拉比格石化工廠（Petro Rabigh）出現了兩起緊急關閉的事件。該事件並未造成損失，因此受到媒體的報導較少。後續的調查發現該石化工廠所使用施耐德電機（Schneider Electric）公司出產的資安產品「安全儀表系統」（Safety-Instrumented System, SIS），受到 Triton 病毒的破壞，因而導致工廠的緊急關閉 。由於拉比格石化工廠內為高溫、高壓的環境，如果發生意外的話，將導致嚴重的爆炸。所幸該病毒只造成石化廠的緊急關閉。[14]

四、以色列水廠受攻擊事件

2020 年 4 月 24-25 日，以色列沙崙（Sharon）地區多處市立自來水廠與汙水處理廠突然停止運作。儘管備用系統很快被啟動，因此短暫的停止運作並未造成任何嚴重損害，但這些不尋常的事件都被記錄了下來。經過網路資安公司的調查，這些停水事件並非意外，而是由惡意軟體（malware）所造成。以色列情報單位的進一步調查，發現該事件由伊朗革命衛隊所發動，而且讓網路攻擊的路徑通過美國境內的伺服器。[15]5 月 9 日，以色列對伊朗境內的阿巴斯港（Shahid Rajaee Port）的電腦進行資訊戰，造成貨櫃車壅塞及船期的延誤，意在警告伊朗勿再對以色列的關鍵基礎設施進行攻擊。[16]

---

[14] "The inside story of the world's most dangerous malware," *E&E News*, March 3, 2019, https://reurl.cc/R4GWdD；"Unprecedented Malware Targets Industrial Safety Systems in the Middle East," *Wired*, December 14, 2017, https://reurl.cc/Mv5jAm.

[15] "Iran Fingered For Attack On Israeli Water Infrastructure," *Cyber Security Intelligence*, May 13, 2020, https://reurl.cc/V6v696.

[16] Ronen Bergman and David M. Halbfinger, "Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks," *New York Times*, May 19, 2020, https://reurl.cc/8GZn4j.

肆、結語

資訊作戰具備避實擊虛的特性，可清楚顯示在以上所選錄的個案。而作為不對稱作戰的一種方式，資訊作戰在科技快速進步的時代，顯得格外重要。從以上的個案來看，印證了羅納與蘭德公司分別於1976年與1996年提出的看法，也就是在資訊時代下，由外國發起的攻擊，非軍事設施也將成為目標。同樣地，隨著資訊科技的進步，資訊作戰的範疇已經從原先的軍事層次，提升到國家安全層次，包含了政治、經濟、社會等面向，也就是前文所述關鍵基礎設施的打擊，並可能跨越戰時與平時的分界，值得我們審慎應對。

本文作者章榮明為美國美國馬里蘭大學政治學博士，現為財團法人國防安全研究院量化分析暨決策推演中心博士後研究。

Asymmetric Warfare: An Information Operation Approach

Jung-Ming Chang

Postdoctoral Fellow

Abstract

One concept of asymmetric warfare is to avoid strength and attack weakness of one's adversary, and the concept has been written in Sun Tzu's Art of War. Information operation fits into this concept well and could be considered as a form of asymmetric warfare. The author starts by distinguishing the difference between information war and information operation. Then, the evolvement of information operation is explored. In the third section, four recent cases of information operation are used for illustration.

出版說明

「財團法人國防安全研究院」設立宗旨為增進國防安全研究與分析，提供專業政策資訊與諮詢，拓展國防事務交流與合作，促進國際戰略溝通與對話。現設有 7 個研究所、1 個中心，本院研究範圍涵蓋：國家安全與決策、國防戰略與政策、中共政軍、非傳統安全與軍事任務、網路作戰與資訊安全、先進科技與作戰概念、國防資源與產業、量化分析與決策推演等領域。

本刊各篇文章由本院研究人員撰擬，以 3,000 至 4,000 字以內為度，稿件均經審稿程序，其著作權為本刊所有，未經同意，請勿轉載。本特刊內容及建議屬作者意見，不代表財團法人安全研究院立場。

發行人：霍守業 ｜ 總編輯：林成蔚 ｜ 副總編輯：柏鴻輝
編輯主任：蘇紫雲 ｜ 執行主編：洪瑞閔
助理編輯、責任校對：王綉雯、蔡榮峰
出版者：財團法人國防安全研究院
院址：10048 臺北市中正區博愛路 172 號
電話：（02）2331-2360　傳真：（02）2331-2361
Institute for National Defense and Security Research
No.172, Bo-Ai Road, Chongcheng Dist., Taipei City, Taiwan（R.O.C.）
Tel:886-2-2331-2360　Fax:886-2-2331-2361

財團法人國防安全研究院

Institute for National Defense and Security Research