

● 作者/Zi Yang ● 譯者/趙炳強 ● 審者/劉宗翰

中共的電子戰發展概況

Blinding the Enemy:
How the PRC Prepares for Radar Countermeasures

取材/2018年4月9日美國詹姆斯頓基金會網站專文(*China Brief*, April 9/2018)



研究中共出版品《雷達對抗原理》乙書，應可對中共電子戰有進一步理解。

中共的電子戰能力始終蒙上一層神祕面紗，外界難以一窺究竟；然而，若透過研究中共所使用的公開出版品《雷達對抗原理》乙書，或許就能對其戰術戰法有更進一步的理解。

資訊戰與資訊作戰構成了共軍準則中所謂「資訊化戰爭」的勝利基礎(編按：共軍以「信息」代表「資訊」)。¹ 作為資訊戰五大支柱之一的電子戰，已在共軍的戰爭準備進程中走到了最前沿，共軍現在所有的大型演習也都大規模地納入了電子戰部隊。

這些發展對於世界現況產生了影響：2018年1月底，中共媒體披露了西安轟-6G長程重型轟炸機上所裝載的新型空中干擾系統，並大張旗鼓宣告其將在南海中扮演強化電磁頻譜優勢的角色(環球網，1月24日)。該武力展示彰顯了中共對於電子戰技術的信心漸豐，並擴大了中共與鄰國之間的電子戰能力差距。

儘管如此，共軍電子戰能力仍一直是一個為人

忽略的議題，主要是因為缺乏高品質的資訊來源。不過，本文所要檢驗共軍分析的新資訊來源，卻能讓吾人以獨特眼光來檢視過去未曾驗證過的課題。為了簡化討論，本文將擱置諸如感測器、通信裝備及武器系統等議題，並置重點於電子戰此一面向，亦即中共如何針對「雷達反制」(radar countermeasure, RCM，編按：共軍以「雷達對抗」代表「雷達反制」)所進行的概念化與準備。² 電子戰在現代戰爭中是不可或缺的，電子戰設備對敵雷達的屏蔽，可在戰鬥中為友軍提供明顯的優勢；因此，在本文分析中所指出的共軍思維，以及包含針對敵航艦戰鬥群的模擬攻擊等，都值得未來進行深入檢驗與評估。

文本分析

本文分析主體借鑒《雷達對抗原理》(以下簡稱「原理」)乙書，該書由中共中央軍事委員會「2110工程」資助，國防工業出版社發行，並於2016年1月進行最新一次更新印製，以及由中共「國防科技大學電子對抗學院」與來自五大軍種頂尖的雷達和電子戰專家所共同編著。

該書根據電子對抗學院的內部教科書，揭示中共頂尖電子戰學府的雷達反制教育，以及中共學者如何將雷達反制進行概念化。因此吾人可以很肯定地說，這本書是一本具備該

領域可靠資訊的權威性文本，以往只能從一些官方、公開性的英文出版品取得這些資訊，而此書的出版則讓外界得以更深入的研究這門課題。³

美「中」對電子戰的認知差異

值得注意的重點是，中共正在快速地向其頭號敵人美國學習電子戰事務，中共學者也不斷密切關注著美國所發展出的新思維。在最近一次的「錢學森論壇」中，共軍頂尖科學家和工程師齊聚一堂，其中一位共軍戰略支援部隊專家做了一場「人工智慧與電磁頻譜戰」的主題報告，並對中共在2015年時首次公開電子戰構想及當前作為進行擴大補充，惟某些想法尚未被美國國防部完全採納(軍橋網，2月22日)。

由於雙方見解不同，也使得中共與美國學者使用不同的術語來描述各種電子戰領域事務，但大



中共正快速地向其頭號敵人美國師法電子戰事務。

(Source: DoD/Seaman Edward Gutierrez III)

部分概念卻是重疊的。美國專家將電子戰細分為三種領域：電子支援、電子攻擊及電子防護；對照中共術語，這三項則分別為：電子對抗偵察、電子進攻及電子防禦(原理，頁2-3)。

此處須注意兩點關鍵差異：首先，中共術語「目標電子防護」係專指目標防護，而美軍用語中的電子防護則涵蓋範圍較廣。其次，美軍視干擾(jamming)與欺騙(deception)為兩種獨立概念，但中共專家則將此二者視為一整體概念(原理，頁3-4)。

中共對「電子戰」兩字的用語為「電子對抗」；至於對「雷達

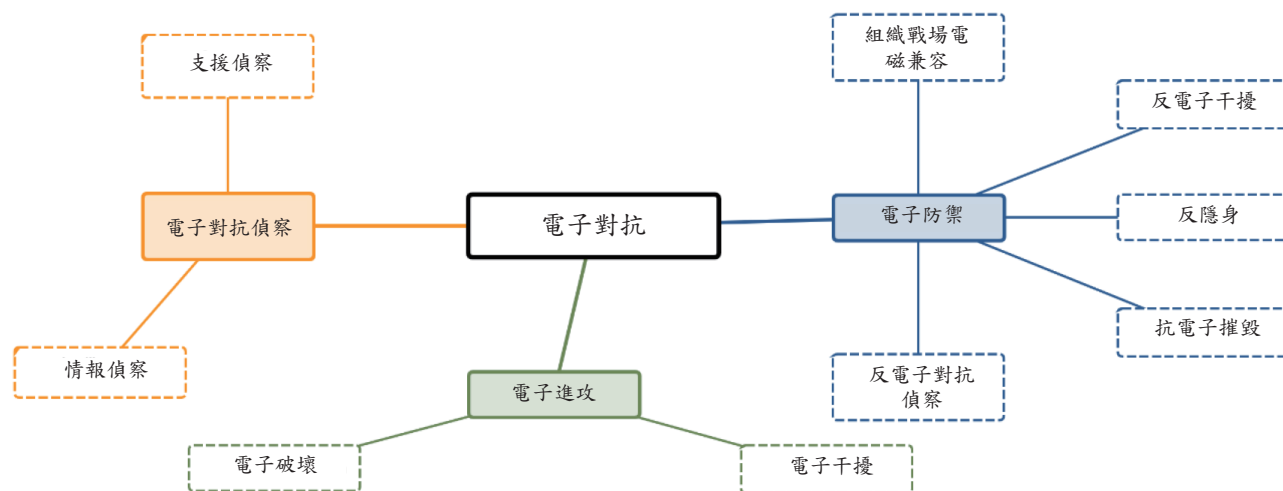
反制」則稱為「雷達對抗」，且進一步將該詞定義為「一種旨在保護友軍雷達，並破壞敵方雷達(包括雷達對抗設備)效能的電子對抗措施」(原理，頁4)。

中共的雷達反制「硬殺」

「硬殺」意指對敵裝備的實質性破壞。中共學者認為反輻射飛彈、無人機、炸彈與高功率微波武器，是對敵雷達系統執行實質破壞的主要工具。《雷達對抗原理》詳述了以上各種破壞手段的優缺點，以及在戰場上的應用方式。

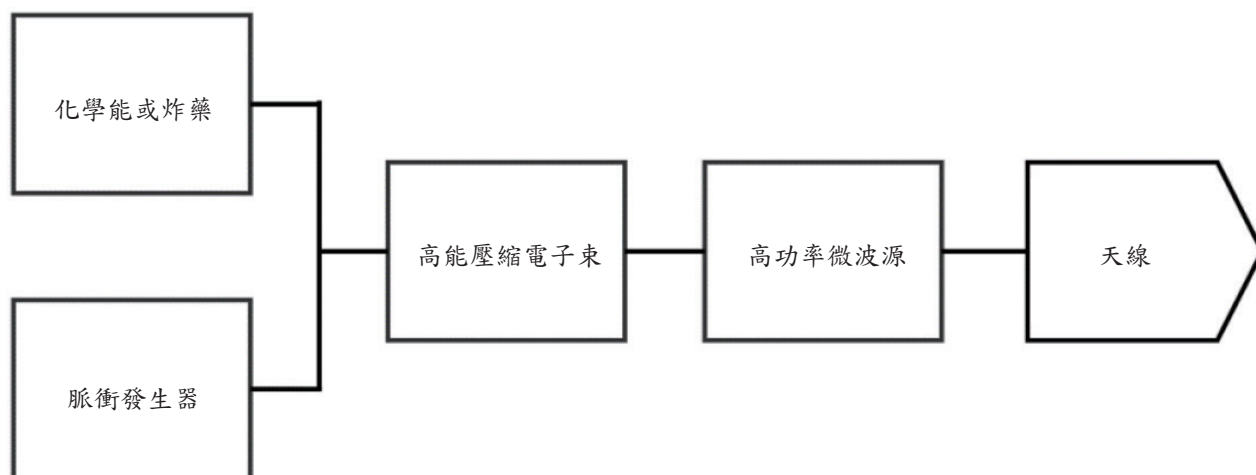
反輻射飛彈一般使用被動式雷達歸向，此種飛彈爆炸範圍

通常為20至60公尺，通常具有高匿蹤性與智能性，但某些飛彈能力則因配備的被動式雷達尋標器而有所限制。中共擁有四種型式的反輻射飛彈，分別是CM-103、鷹擊-91(YJ-91)、雷電-10(LD-10)和飛騰-2000(FT-2000)(The National Interest, November 30, 2017)。在這些飛彈中，最值得注意的是飛騰-2000，其為一種獨特的地對空反輻射飛彈，目的在攻擊空中預警與管制機和電戰機。飛騰-2000採用冷發射與主動式雷達歸向，可在12至100公里外，海拔高度在3至20公里之間攻擊目標(中國網，2015年8月21



中共電子戰作為概念圖

資料來源：賀平主編，《雷達對抗原理》（北京：國防工業出版社，2016年），頁3。



中共高功率微波炸彈示意圖

資料來源：賀平主編，《雷達對抗原理》（北京：國防工業出版社，2016年），頁243。

日)。

反輻射無人機的重量通常在200公斤(或更輕)，它們可對預定目標執行自殺式攻擊，爆炸範圍較反輻射飛彈大50至100公尺。此種無人機的最大優勢是可作為滯空彈藥(原理，頁241-243)。2017年8月，共軍在「朱日和聯合戰術訓練基地」所舉行的一場閱兵典禮上展示了ASN-301型反輻射無人機。該型機與以色列的哈比(Harpy)無人機有驚人相似之處，並擁有288公里的作戰半徑、20公尺的破壞範圍，以及4小時的續航力(Israel Defense, March 1, 2017)。

即使《雷達對抗原理》書中

提到了反輻射炸彈，但該書作者們也承認，由於這種炸彈需要空中優勢，所以鮮少在戰鬥中運用。

高功率微波武器雖然還沒有成為正式裝備，但中共專家仍將其視為重要的未來電子戰武器。高功率微波脈衝能透過各種途徑(例如天線與目標上的任何罅隙)進入電子裝備(原理，頁244)。高功率微波可依其輻射強度，使敵電子裝備失效或完全摧毀。

高功率微波也會對雷達操作人員造成傷害。在低強度(3至13毫瓦/平方公分)時，高功率微波可造成意識混亂、記憶力衰退、行為異常、失明、失聰、失

去意識，甚至心臟衰竭。當微波在最高強度(80瓦/平方公分)時，則無異於暴露在「死光」之下，可在一秒內殺死敵戰鬥人員(原理，頁245-246)。

關於那些能透過火炮、火箭、空用炸彈與飛彈投射的小型高功率微波炸彈，《雷達對抗原理》的作者們似乎透露出了較多資訊，但對於高功率微波武器設施則較少著墨。這可看出中共在前者的技術成熟度，或者是意圖掩蓋其在後者發展上所取得的進展。⁴

中共的雷達反制「軟殺」

「軟殺」意指使用電子戰反制裝備來阻擾或混淆敵人。《雷



欺敵干擾為使用假訊號來誤導敵雷達，所謂「主動欺敵干擾」也有一系列技術。(Source: USN/Richard Doolin)

達對抗原理》書中指出了兩種雷達干擾方式：制壓和欺騙。這兩個主題都各自探討了主動與被動兩個面向，並進一步細分出了十餘種不同的干擾技巧。

主動式制壓干擾使用噪音或脈衝，以抑制並干擾敵雷達接收器的運作，而這種干擾技巧的其中一個例子，即是使用隨機脈衝干擾，這是以不規則參數的方式來運用脈衝，以掩蓋目標反彈回來的雷達回波(原理，頁167)。被動式制壓干擾，則是指干擾絲和雷達波反射器在實體戰場上的運用。

欺敵干擾為使用假訊號來誤導敵雷達。所謂的「主動欺敵干擾」(有源欺騙性干擾)也有一系列的技術。舉例來說，地表反跳干擾用於對付主動或半主動歸向飛彈是相當有效的。在此狀況中，

空中電子戰系統向地面發射一個高功率的模擬雷達回波，並以相同反射角反射至來襲的飛彈。如果成功，該飛彈將會改變路徑並朝向地面反射的模擬回波方向飛行(原理，頁198)。被動欺敵干擾則是指無人機和火箭推進的誘標。誘標的雷達截面反射能力必須比真正目標要來得好，卻又不能太過明顯，否則也會提高誘標暴露的風險。

中共的雷達反制防禦面向

《雷達對抗原理》書中表示，保護友軍裝備以對付敵軍雷達最重要的方式，便是偽裝和匿蹤。這些技術同樣也區分為「天然」和「人為」兩種。

舉例來說，《雷達對抗原理》指出地球表面曲度所造成的雷達死角，讓友軍可以把部隊和裝備安置在敵雷達視線之外，諸如森林、山地、丘陵

和谷地等崎嶇地形，也有利於隱藏友軍資產，而降雨也能降低雷達回波強度(原理，頁219-221)。不過，天然偽裝是可遇不可求的，所以也不是最佳選項。

複合光譜迷彩是一項防護友軍資產免於雷達偵測的便利工具，但如果手邊沒有此種裝備，《雷達對抗原理》建議使用樹枝、蘆葦及乾草等替代方案，但這些替代品厚度也必須足以偏轉電磁波的方向(原理，頁222-

223)。

另一方面，匿蹤技術則是著重於透過極小化裝備邊緣、稜角的平滑外部設計來減少雷達橫截面。

除了這些被動式措施外，《雷達對抗原理》建議自衛式干擾也可透過干擾敵雷達的主波束，達成目標掩蔽之目的。

針對反輻射武器的防禦，《雷達對抗原理》認為可使用誘標和欺敵干擾來混淆進犯的

武器，或讓其提早引爆(原理，頁255)。針對高功率微波武器，該書特別主張加裝濾波器、使用抗燃材質的電子零件、增加自動關閉機制，以因應預期的高功率微波攻擊，並採用能吸收高功率微波的材質，來彌封裝備上的所有孔隙(原理，頁257-259)。

整合運用

《雷達對抗原理》最後特別

保護友軍裝備以對付敵軍雷達最重要的方式，即是偽裝和匿蹤。這些技術也區分為天然與人為兩種。(Source: USN/Eric Coffey)



介紹了一系列的雷達反制狀況模擬，揭示中共如何在戰術層面上整合各種雷達反制工具與技術的思維；然而，值得注意的是，這些範例是根據共軍對國外軍演和狀況模擬的觀察而來。

其中一場針對航艦戰鬥群的空中打擊模擬案例，對未來亞太地區衝突具有極大的相關性。

該案例的攻擊方是由超過20架裝備電子戰反制措施的飛機所組成；包括16架轟炸機、1架空中預警與管制機、1架雷達反制支援機、3架空中遠距干擾機，以及2架掛載反輻射飛彈的電戰機。

攻擊開始時，先由雷達反制機識別並定位敵方雷達，接著將此資訊傳遞至整個攻擊編隊。3架遠距干擾機開始對航艦戰鬥群雷達進行截斷，2架電戰機則以反輻射飛彈開始攻擊敵雷達，同時領隊的轟炸機群施放干擾絲走廊，以利在友軍轟炸機接近目標時提供防護。每架轟炸機上的自衛干擾系統亦同時啟用。

當轟炸機接近目標時，干擾絲施放機進行大坡度急彎。轟炸機開始以精確導引彈藥對敵攻擊。友軍遠距干擾機接著轉移目標，對敵火控雷達、飛彈導引接收器、監視雷達及指揮導引鏈路進行干擾，直到攻擊結束(原理，頁282-283)。

該狀況模擬預期整場攻擊可在10至15分鐘內結束。

結論

相較於對俄羅斯新興電子戰能力的理解(ICDS, September 2017)，外界對中共實際的電子戰、雷達反制能力實在知之甚少。在中共嚴格的資訊控管制度背景下，從《雷達對抗原理》內容所推斷出

的訊息，讓吾人得以一窺中共如何將雷達反制概念化，以及渠等教育電子戰專業人員的方式。本文簡要的概述及分析無法完整囊括該書所有內容，有興趣的讀者可再詳閱此書，就能以全面、權威性視角來了解共軍如何在整體電子戰準則的架構下，將雷達反制作為概念化。

作者簡介

Zi Yang係新加坡南洋理工大學拉惹勒南國際研究學院(S. Rajaratnam School of International Studies)中國大陸項目的高級分析師。

Reprint from *Jamestown Foundation* with permission.

註釋

1. 據美國傳統基金會(Heritage Foundation)資深研究員成彬(Dean Cheng)表示，「2011年版的《中國人民解放軍軍語》將資訊化戰爭(信息化戰爭)描述為在陸、海、空、太空、電磁領域，以及認知領域中，廣泛的將資訊化武器及設備和網路化資訊系統，共同運用於聯合作戰中。在資訊化戰爭中，系統體系(systems-of-systems)之間的對抗構成了衝突主要形式。在系統體系的架構下，對資訊化戰爭的設想即是資訊化部隊，後者可透過網路化的戰鬥系統、指管系統與後勤支援系統遂行作戰。」請參閱，成彬著，《網路巨龍：探討中共資訊戰與網路行動》(Cyber Dragon: Inside China's Information Warfare and Cyber Operations [Santa Barbara, California: Praeger, 2016])，頁39。
2. 雷達反制(雷達對抗)、通信反制(通信對抗)、光電反制(光電對抗)與水下音響反制(水聲對抗)組成了中共電子戰(電子對抗)的四個子領域。
3. 即使是最權威、深入的美國國防部年度中共軍力報告，也幾乎無法對此題材多所著墨。有興趣的讀者，可在2014年的年度報告第66頁找到目前針對中共電子戰最詳盡的因應作為。
4. 關於中共高功率微波武器的最新發展，請參閱，2017年3月11日的外交家(The Diplomat)網站專文。