專載

DOI:10.6237/NPJ.202410_58(5).0001

淺談「訊跡管理」對軍事作戰之重要性

A brief discussion on the importance of"Signature management" to military operations

海軍上校　沈育德

提　　要：

一、現代戰爭憑藉著高科技的發達技術，致使戰場迷霧越趨消散，也意謂著戰場透明度的升高；因此，要在現代戰場上提升戰場存活率，就必須從減低被發現及混淆敵人辨識來著手。

二、避免在戰場上被發現，或被發現時如何降低敵人對目標鑑別的正確度，兩者共同的前提就是要能對敵偵測手段與能力有一定瞭解，同時也要能夠掌握敵人對我軍的各式訊跡的分析能力，如此才能有效的針對敵軍偵蒐手段實施迴避、隱掩，有效降低被偵知機率。另方面，設法布散戰場迷霧，造成敵軍致茫、困惑，這都屬於「訊跡管理」的範疇。

三、儘管再周延的「訊跡管理」機制、規章或規範，值得注意的是，關鍵破口仍可能是執行或管理前述機制、規章的「人」，倘未落實管理，不僅只是違規或違紀的懲處問題，而應聚焦在軍事作戰準備上；畢竟因疏忽「訊跡管理」，輕則個人生死、重則戰場勝敗，海軍幹部確實應高度重視。

關鍵字：訊跡、訊跡管理

Abstract

1.Due to the development of advanced technology, the fog of battlefield in the modern warfare has become smaller. The implication is that the transparency of the battlefield would be relatively improved. To increase the battlefield survival rate in the modern warfare, one must reduce detection and to confuse the enemy's identification.

2.On the basis of understanding enemy's detection methods and capabilities of analyzing our signature ability is the key issue to avoid be detect-

ed or discovered on the battlefield, and also to decrease enemy's identification of targets. Moreover, we can effectively evade and conceal the enemy's reconnaissance and reduce the probability of being detected. On the other hand, spreading the fog of the battlefield to confuse the enemy, and preventing the transparency of the battlefield are within the scope of "Signature Management".

3.Nevertheless, it is worth noting that the key breach may still be related to the"person"who implementing or managing the aforementioned mechanism and regulations. In particular, the Navy cannot afford to ignore the issue of negligence in" Signature Management"that may lead to the defeat of the war and the matter of life and death.

Key Words: Signature，Signature management.

壹、前言

古代的戰爭，兩國(軍)交戰前搜尋對方兵馬的過程，就如同是一場捉迷藏，誰先被發現，就有可能先遭受到攻擊，雙方在「藏」與「找」的過程當中，依據的是對兵馬的「形」、「聲」、「光」、「煙」、「痕」等跡象判斷，靠的是人的眼、耳、鼻等基本官能，運用視覺、聽覺及嗅覺功能，以「先敵發現，先敵攻擊」。若把視角拉回現代，即使經歷長遠時間演進，惟在戰場環境中這些形、聲、光、煙、痕等線索依然存在；唯一不同的是，戰爭已隨著時間演進，增加「科技」這個關鍵元素，透過科技運用，讓查找敵人的方式變得更多元。

當前「俄烏戰爭」中就出現受到「訊跡」因素影響，導致作戰傷亡的案例，如俄羅斯士兵因為使用手機，遭到烏克蘭軍隊偵知、定位然後攻擊，[1]讓各國對於看不見的電磁波訊號及高科技的定位技術更加敬畏；或者當俄國媒體在國營電視台多次播放戰事勝利的報導，此舉動反而間接的曝光了俄軍部隊行踪，讓烏軍得以輕鬆找到這些「作戰目標」，進而展開反擊。[2]2022年3月7日，烏克蘭國防部指出，烏軍順利擊殺俄軍「第41聯兵軍團」參謀長格拉西莫夫(Vitaly Gerasimov)少將，根據事實查核、新聞調查集團「Bellingcat」以及烏克蘭國防部釋出的俄方對話，判定應是通信出現問題，讓將領不得不使用當地的SIM卡，導致行踪暴露，而遭烏軍擊

註1：〈士兵偷用手機洩密惹禍！ 俄國遭烏克蘭「跨年夜襲」釀89死〉，壹新聞，2023年1月4日，https://www.nexttv.com.tw/NextTV/News/Home/WorldNews/2023-01-04/1020134.html，檢索日期：2024年7月5日。

註2：林彥銘，〈俄國遲遲攻不下烏克蘭 外媒揭主因：「自己暴露行踪」〉，新頭殼Newtalk，2022年3月27日，https://tw.news.yahoo.com/%E4%BF%84%E5%9C%8B%E9%81%B2%E9%81%B2%E6%94%BB%E4%B8%8D%E4%B8%8B%E7%83%8F%E5%85%8B%E8%98%AD-%E5%A4%96%E5%AA%92%E6%8F%AD%E4%B8%BB%E5%9B%A0-%E8%87%AA%E5%B7%B1%E6%9A%B4%E9%9C%B2%E8%A1%8C%E8%B9%A4-095140877.html，檢索日期：2024年7月12日。

弊；甚至烏國國防部在事後釋出截獲的俄方通話，顯示俄羅斯「聯邦安全局」(FSB)官員抱怨，加密通訊系統遭到破壞、入侵，因而讓烏方得以有機會監聽俄軍命令內容，並完成斬首行動，[3]此更凸顯訊跡管理之重要。

本文透過瞭解美軍陸戰隊對於各類「訊跡」與「訊跡管理」的定義，來說明其內容及如何執行「訊跡」的管理；並進一步說明訊跡管理對軍事作戰的重要性。另對國軍而言，「訊跡管理」雖然聽起來有點陌生，但實際上「它」並不是一個創新的事物，而是經過有系統的定義與分類的作戰關鍵作為。事實上，國軍各級部隊平時都已在執行「訊跡」的管理，只是沒有針對「它」做出特別明確的分類；因此，國軍幹部對可能之疏漏，應及早預防，以避免因忽略對訊跡管理的周延性，導致任務失敗。

值得注意的是，縱使再高端的裝備，或再嚴格的規範，如果疏忽了對「人」這個關鍵要素的管理，恐怕所有作戰的努力很有可能都將「功虧一簣」。因此，撰文主要目的，即期望藉本文讓國軍重新審視對部隊軍、士官、兵，乃至於文職、聘雇人員的訊跡管理作為；畢竟如果沒有做好完整的訊跡管理，要面對的恐怕不僅僅是單純涉及的違規或違紀的懲處問題，其影響可能是聚焦在無情的戰場上，攸關國家存亡勝敗的大課題，面對此一嚴重之問題，各級管理高層確實應審慎應對。

貳、訊跡的定義與分類

「訊跡」(Signature)在新編《國軍簡明美華軍語辭典》的解釋為「徵候、特徵、信跡、訊號」等意。[4]若由2022年2月24日爆發迄今已近3年的「俄烏戰爭」觀察，部分戰況的演變發展，再次喚起美國軍方高層對於作戰中落實「Signature」的電磁波管理、部隊對「Signature」管理的作為，以及如何避免遭敵偵知等情況的高度重視，同時也針對「訊跡管理(Signature management)」(以下稱SIGMAN)進行更積極且深入的探討，此一狀況同樣值得國軍重視。我國國防部在2023年即已將「Signature」統一譯為「訊跡」一詞，不僅完整定義其內容，亦有助相關作為分類，及戰場上採取合宜行動。以下就訊跡內容介紹，分述如後：

一、什麼是訊跡

簡要的說，也就是舉凡可以看得見(徵候、特徵、跡證)、聽、聞得到的徵(跡)象，或使用科學儀器偵測得到的電磁(信)訊號都是訊跡的範疇。國人日常最常聽

註3：〈糗！俄軍毀烏克蘭基地台害到自己 洩漏行踪還賠掉高階指揮官〉，即時新聞網，2022年3月9日，https://lihkg.com/thread/2920283/page/1，檢索日期：2024年7月12日。

註4：〈訊跡〉，《國軍簡明美華軍語辭典》，中華民國國防部，頁859，https://www.mnd.gov.tw/NewUpload/files/ 國軍簡明美華軍語辭典.pdf，檢索日期：2024年7月12日。

附表：「行政訊跡」觀察及偵測手段綜整表

項　　目	觀 察 及 偵 測 手 段 說 明
人工情報(HUMINT) Human Intelligence	運用人力或者與其它情報機構聯繫來蒐集情報。
電訊情報(SIGINT) Communication Intelligence	透過偵測、截收、辨識電磁輻射，蒐集發射源訊號特性訊息，訊號情報較偏向進行長時間監聽、截收與分析。
公開資源情報(OSINT) Open Source Intelligence	從公開報告、新聞報導、網路訊息等資料分析獲得的情資，將大部分注意力集中在蒐集傳統機密情報。
攻勢網路作戰(OCO) Offensive Cyber Operation	意圖於網路空間內或透過他國網路空間展現武力，以支持作戰指揮官，藉由攻勢網路作戰實施干擾、破壞敵武器系統、指管流程、後勤節點與高價值目標。

資料來源：參考張婷，〈美軍創建人工情報單位 蒐集金正恩情報〉，大紀元，2017年5月9日，https://www.epochtimes.com/b5/17/5/8/n9120117.htm；杜貞儀，〈第七章 共軍電子偵察能力發展與評估〉，《2021國防科技趨勢年度報告-中共新世代軍事科技評估》，財團法人國防安全研究院，2021年12月22日，https://indsr.org.tw/respublicationcon?uid=16&resid=837&pid=1412；吳宗翰，〈美軍對俄「攻勢網路作戰」支援烏克蘭的意涵與對臺正面啟示〉，財團法人國防安全研究院，2022年6月13日，https://indsr.org.tw/focus?uid=11&pid=369&typeid=，檢索日期：2024年7月13日；陳韋廷，〈開源情報是什麼？美自認情蒐罩門 比不上大陸〉，《聯合報》，2023年1月18日，https://vip.udn.com/vip/story/121937/6918584，檢索日期：2024年7月13日，由作者彙整製表。

到的「凡走過必留下痕跡」，以及「蛛絲馬跡」等用語，實際上就已經是對「訊跡」做出了最簡單也最普遍的詮釋；至於「俄烏戰爭」中俄羅斯士兵因為使用手機，反遭烏克蘭定位然後攻擊，其被偵測到關鍵的訊跡，就是看不見的電磁波訊號。

二、美軍訊跡的分類

美軍陸戰隊《遠征前進基地作戰手冊》(TENTATIVE MANUAL FOR EXPEDITIONARY ADVANCED BASE OPERATIONS 2ND EDITION)第二版中，針對「訊跡」做出完整分類及定義，[5]相關「訊跡」種類說明，分述如後：

(一)行政訊跡(Technical signatures)

指個人與單位在計畫、機動、簽訂支援協定，以及執行其他行政事項時，敵軍透過不同情報方法來觀察及偵測我方訊跡，其手段包含「人工情報」(HUMINT)、「電訊情報」(SIGINT)、「公開資源情報」(OSINT)及「攻勢網路作戰」(OCO)等(如附表)。這裡所指的個人與單位，應屬廣義的從事軍事相關事務人員，除軍職人員外，當然也包括軍中的約聘人員；因為這些對象都有可能直接或間接的接觸軍事相關事務，所以都必須納入管理。

(二)物理訊跡(Physical signatures)

敵軍可透過直接觀察或地理空間情報(指有計畫的觀察、觀測)來對目標進行蒐集情資。從字義上可以很明顯地看得出來，是敵軍針對我部隊所製造出的物理訊跡，藉由觀察、刺探或調查後，再經過蒐整

註5：“TENTATIVE MANUAL FOR EXPEDITIONARY ADVANCED BASE OPERATIONS 2ND EDITION”, 9 May 2023, p.7-6,https://www.marines.mil/Portals/1/Docs/230509-Tentative-Manual-For-Expeditionary-Advanced-Base-Operations-2nd-Edition.pdf，檢索日期：2024年7月12日。

、研判而獲得敵軍所想要的情報，例如部隊位置、種類、數量等。

（三）技術訊跡（Technical signatures）

技術訊跡指敵人必須使用專用（業）裝備（電訊監聽或監測系統）實施訊跡的蒐集（如電信、電磁波）。這個部分對國軍應該不陌生，因為幾乎各作戰部隊都執行過電磁波發射管制（亦即電磁頻譜管理），其目的就是減少或禁止特定頻率的發射，這裡所指的管制，包含通信（話）及雷達波。[6]

三、如何做好訊跡管理

（一）要想做好訊跡管理，首先必須要先瞭解我方部隊可能產生的訊跡種類及性質；再來，需要知道敵軍蒐集訊跡的手段與能力。這部分涉及我方對敵軍相對敵情的研析與瞭解程度，敵軍對我訊跡蒐集能力，與其科技和作戰目的有密切的關聯性；透過對敵軍訊跡蒐集與對訊跡研析能力的瞭解，才能有利於我方研判採取何種方式（法）來隱蔽訊跡，俾盡可能的不被敵軍偵知、發現或遭受攻擊。

（二）對敵軍具備的情蒐能力分析，除了有助我隱蔽訊跡之外，進一步可以對敵軍情（偵）蒐的手段，採用投射錯誤訊跡（假目標）方式，誤導敵軍致其產生錯誤研判，藉以保護我軍及友軍兵力；如果狀況允許，希望可以更進一步誘使敵軍誤判而採取錯誤行動，或引導進入劣勢位置，[7]以獲取我方所欲之作戰效果（益）。戰場上若想要採取攻擊行動，首先必須先解決「目標獲得」這個難題，採攻擊的一方要用盡手段「尋找」敵對方的任何「蛛絲馬跡」，再從中釐出可用的線索，進而設法運用諸般手段，尋找、定位欲攻擊的目標，並在確認目標後遂行攻擊作為。

（三）被攻擊的一方則會竭盡心力的不想被發現，所以會用盡辦法隱藏、掩蔽；而若想盡辦法減低被敵對方發現的機率，那就必須對自身（部隊）所產生的訊跡實施管理。因此簡單的說，適切減少部隊產生的訊跡就是最直接的一種管理方式，但單方面的減少自身（部隊）所產生的訊跡，就可以不被發現嗎？當然不是，從被動面向來看，就是不希望先被發現；從積極面向來看，則必須透過對敵軍蒐集和分析這些訊跡的手段與能力進行分析，並有效的針對敵軍偵搜（蒐）的方式實施迴避，才能降低被敵偵知的機率。因此，為能更提高戰場存活率，必要時也應採用欺敵策略，製造錯誤訊跡，用以保護我軍及友軍部隊，就如同古代兵法家孫臏採「添兵減灶」方法，誘敵錯估情勢，進一步引導敵軍採取特定行動或是陷入劣勢被動位置（或態勢）

註6：曾怡碩，〈頻譜管理與電子戰〉，《國防情勢特刊-電子戰專題》，第30期，財團法人國防安全研究院，2023年8月15日，https://indsr.org.tw/respublicationcon?uid=13&resid=2978&pid=5146，檢索日期：2024年7月14日。

註7：同註5，頁E-7。

註8：〈添兵減灶〉，國家教育研究院網站，https://dict.idioms.moe.edu.tw/idiomView.jsp?ID=15823&webMd=1&la=0，檢索日期：2024年7月14日。

。[8]

在《孫子兵法》〈軍行篇〉中，對部隊作戰掩藏或隱蔽中提到：「善守者，藏于九地之下；善攻者，動于九天之上。故能自保而全勝也。」；[9]另外在〈虛實篇〉也寫到：「故形人而我無形，則我專而敵分。我專為一，敵分為十，是以十攻其一也。」[10]這些內容都在強調部隊在戰場多變環境下，隱藏(匿踪)行動的重要性，亦值得國軍參考。

參、淺談軍事各類訊跡

就國軍而言，對於「訊跡」的認知其實已有一定程度的概念與認識，只是對內容似乎並沒有特別進行區別或分類。透過前述美軍對訊跡定義與分類的理解後，接續檢視國軍各類軍事訊跡的態樣，用以提醒各部隊對於各類訊跡的應有注意與重視。分述如後：

一、常被忽略的行政訊跡

這類訊跡大多發生在單位或是個人執行相關行政事項或作業時的時候，有別於採取作戰行動時所產生的訊跡。一般行政訊跡態樣，分述如下：

(一)檔案轉換文字的介面

部隊或軍事相關機構(編組)在產製計畫過程，於擬定或規劃、研討計畫的各種階段當中，所有作業相關的人員，以及作業所需使用的設備(電腦、列表機多功能事務機、影印機、錄影(音)設備、傳真機)、物件(紙本、筆記)等，都是可以將書面計畫列印而以紙本呈現，此時行政訊跡就被產出。

圖一：行政訊跡態樣示意圖

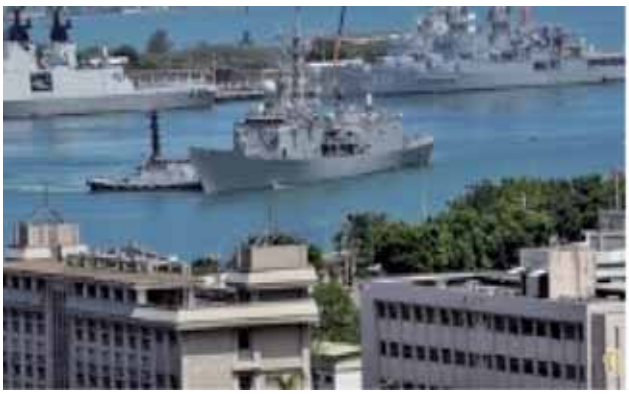
說明：羅馬尼亞國防部長參訪陸軍學院，旁邊立著一面大白板，上頭就寫下了該國陸軍網路系統的帳號密碼，簡直就是把國家機密暴露給全世界。

資料來源：參考〈羅馬尼亞部長訪問校園 白板1排字讓陸軍慌了〉，三立新聞網，2021年3月26日，https://tw.sports.yahoo.com/news/部長訪問校園-白板1排字讓陸軍慌了-231028028.html，檢索日期：2024年7月14日，由作者彙整製圖。

(二)文字記述的態樣

人員藉由口述的討論、記錄或者是透過電腦具體的轉化成文字及印列出來，意即這些透過計畫參與人員的前述動作，是可以顯露出全般計畫或是局部計畫，甚至作業過程當中，列印(記錄)計畫文字殘留作廢的紙張，也或者是在白板上用來記述或研討計畫卻未擦拭掉的殘存文字與圖表，這些行政訊跡如果沒有嚴密的管理，便可能讓敵對一方透過情報管道蒐集，並藉由分析這些蛛絲馬跡，進而獲取所要的我

註9：魏汝霖，《孫子今註今譯》(臺北市，國立編譯館，1978年)，頁109。
註10：同註9，頁130。




圖二：物理訊跡態樣示意圖

說明：敵軍可透過對營區及港口有計畫性的觀察(左圖)；或經由掌握機動部隊產生之物理訊跡來蒐集情資(右圖)。

資料來源：參考涂鉅旻，〈增艦隊存活率 海軍左營二港東側碼頭拚5年後完工〉，《自由時報》，2023年5月30日，https://def.ltn.com.tw/article/breakingnews/4317465；陳怡璿，〈269旅戰備偵巡 實戰訓練淬戰技〉，《青年日報》，2024年4月1日，https://www.ydn.com.tw/news/newsInsidePage?chapterID=1664246&type=life，檢索日期：2024年7月14日，由作者彙整製圖。

方情報(如圖一)。

(三)文件存放的空間

軍事單位或個人常常因任務調整或異動，在異動的過程當中，有可能遺落文(物)件或未將現場淨空，而讓敵對的一方(或有心人士)可藉由蒐集這些被忽略或遺落與行政事項有關之物(跡)證，推測研判出其所需要的我方情報。

(四)經常被忽視支援協定

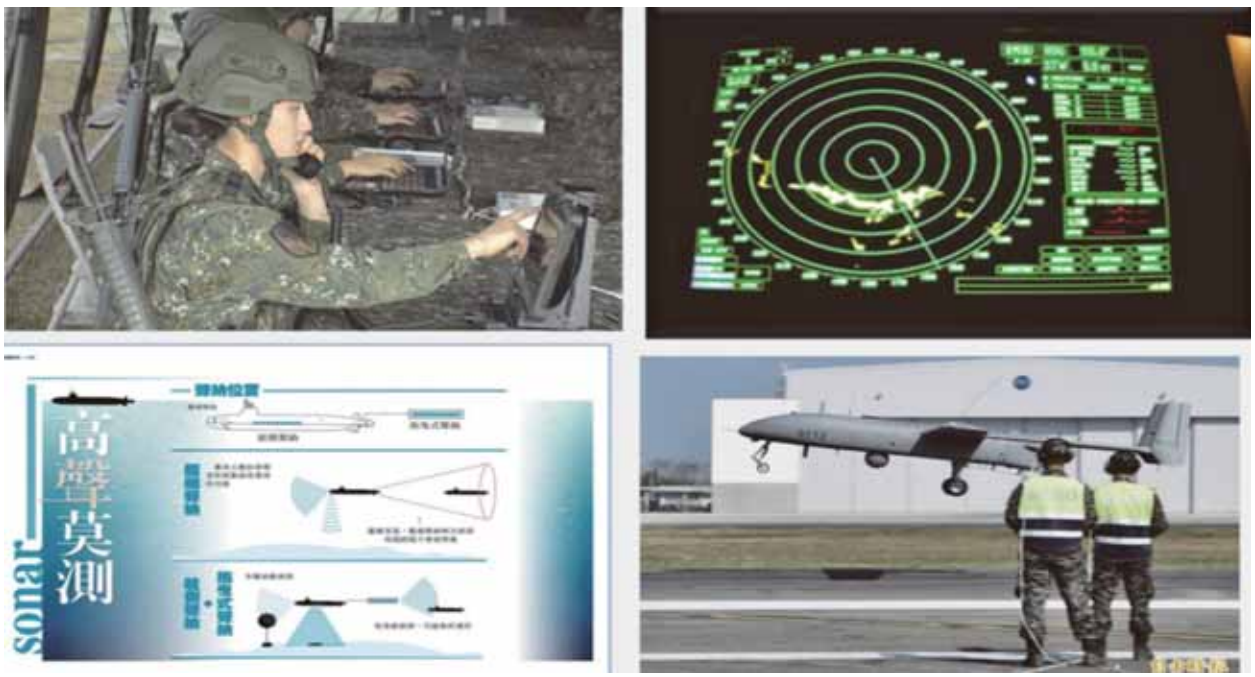
軍事單位與相關軍、民間機關，因實需而簽訂有關之支援協定(或合約)時，參與支援合作的非該單位之其他軍、民間機關人員，可能透過支援協定內容的條文，很有可能就這樣間接或直接的知悉或臆測出單位或部隊部分之軍事意圖。

二、與部隊息息相關的物理訊跡

物理訊跡是敵軍可透過直接觀察或地理空間情報(如攝錄影、偵照等得以具象化)，來對我進行情資蒐集。至於敵軍如何獲取我軍的物理訊跡，其手段或方式概述如後：

(一)敵軍平時可以透過對營區及港口有計畫性的觀察，對戰機的起降、陸軍戰、甲車及部隊的機動、海軍艦艇進出港動態及數量等觀察，都有可能研判出我軍部隊的動向或意圖；或場景延伸到戰場，透過對我軍事機場戰機起、降數量的統計，敵軍可以推研出我空軍基地還保有多少空中戰力(態樣，如圖二)。

(二)藉觀測我軍裝甲車引擎聲響，以及在路面所製造出的履帶壓痕、軍用車輛行進間所產生的引擎排煙等等，這些部隊移動所產生的「形」、「聲」、「光」、「煙」、「痕」之物理訊跡，都可能做出推算部隊動向、數量甚至作戰意圖之依據，至於媒體上面的報導，也有可能間接暴



圖三：技術訊跡態樣示意圖

說明：無線電通信(左上)、雷達示波(右上)、主動式聲納(左下)及無人機遙導控信號(右下)都是看不見的技術訊跡－電磁波(聲)訊跡。

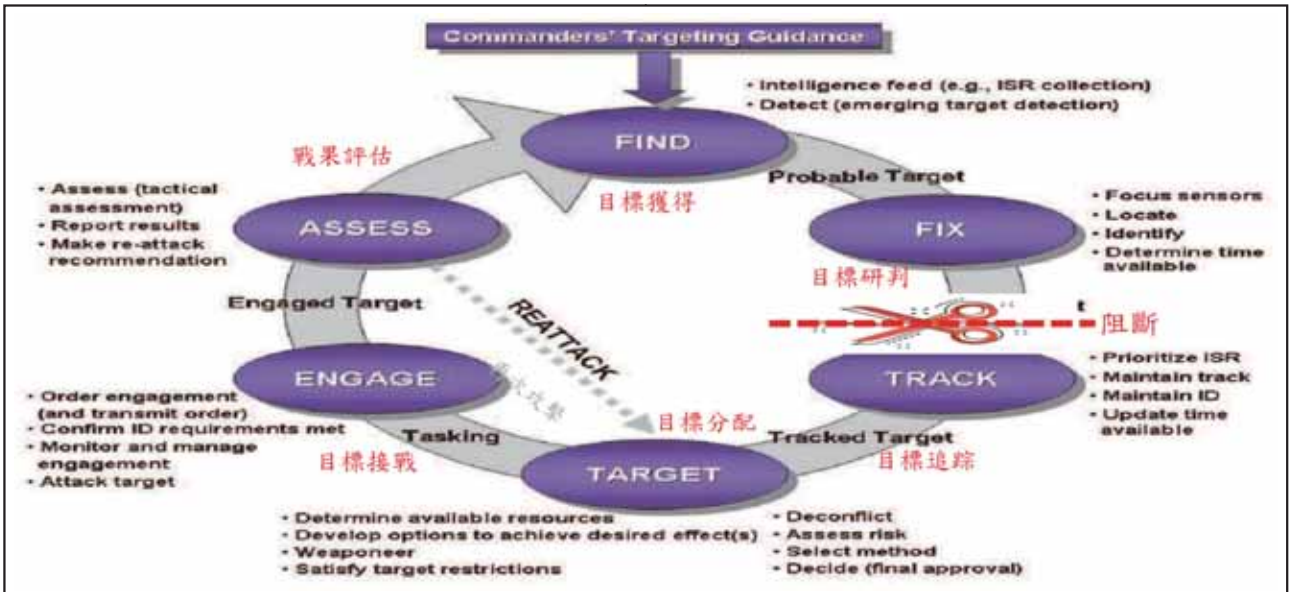
資料來源：參考涂鉅旻，〈軍事迷點進來！銳鳶無人機起降首公開曝光〉，《自由時報》，2019年1月24日，https://news.ltn.com.tw/news/politics/breakingnews/2681633；江炘杓，〈韜略談兵-高「聲」莫測 淺析潛艦水下航行與發現目標〉，《青年日報》，2022年11月3日；https://www.ydn.com.tw/news/newsInsidePage?chapterID=1543589；翁有繼、吳俊德，〈臺灣逐步強化不對稱戰力 「資通訊」導入部隊訓練〉，民視新聞網， 2024年2月9日，https://www.ftvnews.com.tw/news/detail/2024209P51M1；〈航海科技〉，國立海洋科技博物館，https://ship.nmmst.gov.tw/ship/content/148/610，檢索日期：2024年7月14日，由作者彙整製圖。

露部隊行踪。

（三）敵軍亦可能透過對港口進出軍艦數量及艦型（舷號）與動向的掌握（軍營附近高樓都可進行觀測）、在作戰海域對水面目標的偵察與夜間對船舶燈光的研判，都有可能掌握到我軍艦艇行踪；尤其在一段時間的情資蒐集後，敵軍就有可能研判出想獲得之作戰情報。

三、看不見的技術訊跡

依據「俄烏戰爭」經驗教訓，技術訊跡除電磁波外，自然也包括手機信號，而管制電磁波的目的都在避免遭敵軍電偵截獲，進而暴露部隊位置，或被研判出我軍可能之行動或意圖；若未能落實，嚴重者甚至可能遭定位攻擊（態樣，如圖三）。再就現代戰爭而言，在講究制電磁權的前提下，敵我相互針對彼此技術訊跡的偵、防，更在未開戰的平時即已無聲無息地進行著，這類專業部隊與機構不僅是資通電軍及相關國安、軍情單位，甚至一般部隊都



圖四：阻斷「擊殺鏈」示意圖

說明：與其讓敵人建立「擊殺鏈」，再來面對如何處理高端武器的致命威脅與危害，也許從做好部隊訊跡管理先著手，阻斷敵殺鏈循環裡頭最重要的源頭「目標獲得」以及「目標研判」兩個關鍵，較能夠提升戰場存活率。

資料來源：參考〈Improving the Kill Chain for Prosecution of Time Sensitive Targets〉,SEMANTIC SCHOLAR,https://www.semanticscholar.org/paper/Improving-the-Kill-Chain-for-Prosecution-of-Time-Lo-Au/0e04983abe88459841ccb45fd-2bb0422bd03e1da，檢索日期：2024年7月14日，由作者彙整製圖。

應特別注意。

肆、訊跡管理對軍事作戰之重要性

談到訊跡管理對軍事作戰的重要性，就不得不提「擊殺鏈(kill-chain)」也就是所謂的「F2T2EA」。[11]軍事作戰強調經由目標獲得(Find)、目標研判(Fix)、目標追踪(Track)、目標分配(Target)、目標接戰(Engage)、戰果評估(Assess)等循環步驟，建構一個完整的目標擊殺過程，其最終目的，無疑的是要順利接戰並摧毀目標。但整個循環過程中，最重要的兩個關鍵，就是在目標獲得及研判；如果交戰過程中無法發現目標或目標研判困難，敵人極可能無法完成「擊殺鏈」的程序。所以，掌握敵偵知的手段與能力，並減少暴露我部隊行踪，就能夠阻斷敵人的擊殺鏈(如圖四)，提高我軍部隊戰場存活率；所以完整有效的「訊跡管理」，在作戰中的重要性自然就「不言可喻」。以下就其重要性，探討分析如後：

一、國軍既有的訊跡管理機制

(一)行政訊跡管理

1. 在計畫階段，計畫擬訂與規劃過程所需使用到的電腦，國軍已採用軍網與民

註11：曾國政，〈海軍建置「協同作戰能力」(CEC)與現行數據鏈路之研究 〉，《海軍學術雙月刊》，(臺北市)，第56卷，第6期，2022年12月1日，頁93-94。

網實體隔離，[12]並要求公務電腦資料檔案均需加密、也採取限制性檔案傳輸機制（由保密督導官檢核傳送），目的就是在防範敵軍或有心人士透由網路情蒐，同時也防止作業人員因可能的疏忽或便宜行事，造成檔案濫傳而肇致洩違密情事。

2. 針對列表機（或多功能事務機）也同樣都採實體隔離方式，避免混用致可能被植入惡意程式；就連傳真機也必須採加密傳輸，機密文件的產製，除要求精準核密之外，並按規定執行登管。另在公務文件列印上，依規定都必須加註相關記號，密級以上作廢文件，必須依規定程序銷毀；一般文件則由符合規格之碎紙機碎斷，[13]再採集中水銷方式，澈底斷毀行政訊跡，以防杜洩密。

3. 軍事單位或個人的調動或職務調整，在遷移的過程當中，有可能會遺落文件或未將現場淨空，而讓有心人士刻意蒐集這些被忽略或散失的行政有關之物（跡）證，推測研判出所要的情報。所以國軍都有複式確認機制，[14]不管單位或部隊遷移，都有規範相關逐級複式檢查作為；因此必須落實對「執行人」的教育與複式「檢查人」（或督導人）的制約，方能發揮預期功能。

4. 若軍事單位與相關軍、民間機關，因有實需而簽訂有支援協定（或合約）時，參與支援合作的其他軍、民間機關或人員，也很有可能透過對支援協定條文內容的瞭解，間接或直接的知悉或臆測出部分單位或部隊之軍事意圖；因此，軍事單位在簽訂任何支援協定（或合約）時，必要時，亦應同時訂立保密條款加以制約，更要求不得與非相關人員記述支援協定有關內容，這些細節往往都是容易被忽略的保密重點，稍有不慎則影響重大。

（二）物理訊跡管理

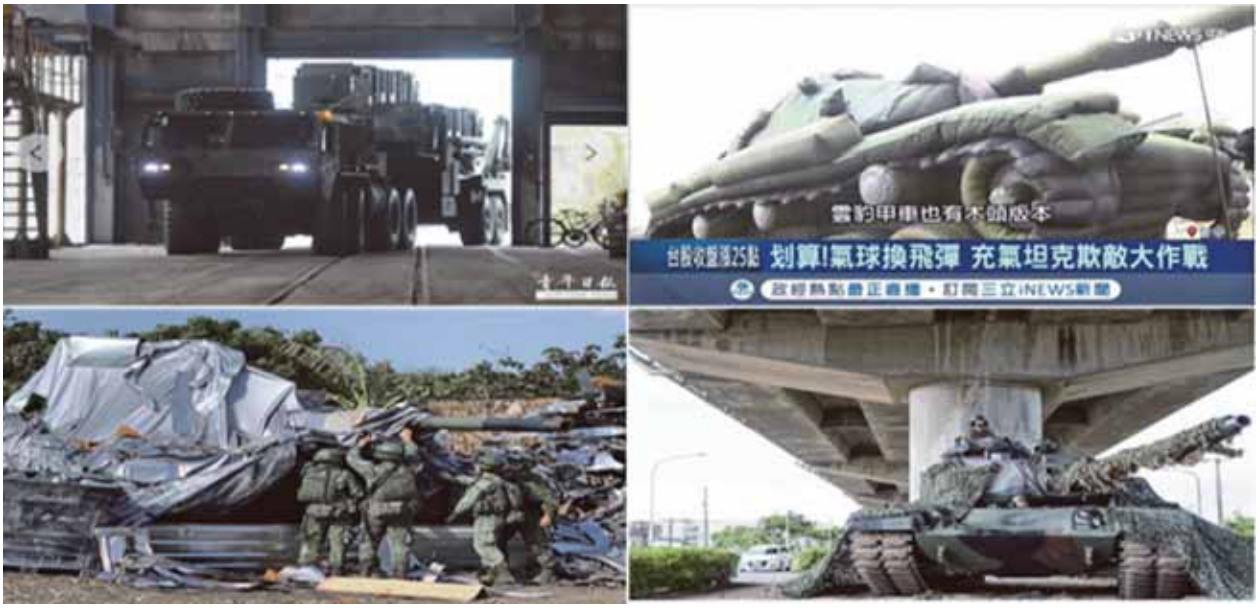
針對訊跡的管理，主要目的不外乎是減少被觀察及減少被發現，減少被觀察其深層意涵是必須對敵軍偵知手段與能力要有一定程度的掌握與瞭解；而減少被發現則意味著，必須想辦法降低及混淆敵軍對我的辨識與鑑定。作法概要如後：

1. 戰力保存階段，國軍各地面部隊會將戰、甲車、機動飛彈車、雷達車，資通電軍的干擾車、電偵車，空軍的戰機等等，適時進入車廠、車庫、機堡實施掩（隱）蔽；戰時則機動疏散，抵達各戰力保存位置，伺機轉換至戰術有利位置準備遂行後續作戰。雖然是不同的作戰進程或階段，但都有著共同努力的目標，那就是不希望

註12：〈柳營要聞 貫徹實體隔離 網域不混用〉，《青年日報》，2023年10月16日，https://www.ydn.com.tw/news/newsInsidePage?chapterID=1622543&type=military，檢索日期：2024年7月15日。

註13：〈機密文件外洩風波 國防部今直接示範如何碎紙〉，《自由時報》，2017年8月1日，https://news.ltn.com.tw/news/politics/breakingnews/2149842，檢索日期：2024年7月15日。

註14：〈避免誤射 國軍將研發防呆機制複式確認〉，中時新聞網，2016年7月4日，https://www.chinatimes.com/realtimenews/20160704002269-260407?chdtv，檢索日期：2024年7月15日。



圖五：物理訊跡管理示意圖

說明：國軍戰備演練將飛彈車機動轉移到民間廠房內(左上)、運用充氣戰車欺敵(右上)、利用橋墩掩蔽(右下)或於資源回收場加強偽裝(左下)。

資料來源：參考謝孟哲、吳承斌〈以假亂真！用氣球換飛彈 充氣坦克10分鐘變戰車欺敵軍〉，三立新聞網，2019年1月17日，https://www.setn.com/News.aspx?NewsID=486685；王臻明，〈國軍主力M60A3戰車利用高架橋墩及偽裝進行隱掩蔽〉，Ettoday新聞雲，2020年7月17日，https://forum.ettoday.net/news/1762901；洪哲政，〈中共衛星密集監看 國軍鬥法祭出偽裝欺敵三寶〉，《聯合報》，2020年10月29日，https://vip.udn.com/vip/story/121160/4971950；羅添斌，〈愛國者飛彈戰備演練 野外放列、潛入民間廠房戰力保存〉、《自由時報》，2021年3月24日，https://news.ltn.com.tw/news/Taipei/breakingnews/3477221，檢索日期：2024年7月16日，由作者彙整製圖。

被敵軍所偵蒐(觀察)，進而被識別定位(發現)。

2.國軍曾在2021年進行「愛國者防空飛彈」(PAC-Ⅲ)的戰備演練，即是將機動飛彈車轉移到民間廠房內進行戰力保存作為；[15]除此之外，橋墩底下、明隧道等都可以適切被利用做為避免被敵直接觀測的掩蔽場域(物理訊跡管理示意，如圖五)。[16]但這裡必須注意的是，軍事武裝掩蔽場域依照《武裝衝突法》(laws of armed conflict)是有一定規範的，因為該法係以人道關懷為出發點的戰爭規範；然實際戰爭中卻曾經發生，一方利用對手謹守《武裝衝突法》保護無戰鬥力平民的底線，藉此羈絆對手用兵。2003年「美伊戰爭」期間，伊拉克軍方刻意將兵力部署貼近住宅區，甚至以學校、清真寺、醫院做為武器彈藥的囤儲點，就是負面例證；而違反

註15：羅添斌，〈愛國者飛彈戰備演練 野外放列、潛入民間廠房戰力保存〉，《自由時報》，2021年3月24日，https://news.ltn.com.tw/news/Taipei/breakingnews/3477221，檢索日期：2024年7月16日。

註16：王臻明，〈漢光演習》任務尚未結束　漢光演習只是聯兵營新編裝檢討的開始〉，Ettoday新聞雲，2020年7月17日，https://forum.ettoday.net/news/1762901，檢索日期：2024年7月16日。

國際法的代價，就要承擔國際社會廣泛的譴責與事後罪責懲罰。[17]

3. 戰術有利位置即意味著隨處準備作戰並實施攻擊，既然如此，作戰部隊所處場域將與戰力保存時位置可能有所不同；因為戰術有利位置著重在火力發揚，而非隱藏實力。由於必須暴露於室外地境，這時候就必須想辦法減少部隊可能產生形、聲、光、煙、痕等物理訊跡；而想要達到預期目的，就需要透過適切的偽裝、隱蔽來欺騙敵人達到誤判效果。為降低「形」被偵知，國軍各類型地面部隊採用融入背景環境的偽裝網或塗裝、充氣式的戰車[18]、飛機，海軍艦艇也有低視度塗裝等手段；另一方面，當此類物理訊跡產生，多在部隊待機、行進或攻擊時，若實在沒辦法避免或降低這些訊跡的發生，那就必須在每一次的作戰行動後，視戰況適時、適切的實施陣地轉換，除避免部隊訊跡暴露外，另一方面的考量，就是為提高我軍部隊的戰場存活率。

(三)技術訊跡管理

1. 技術訊跡則是指敵方需要專用裝備(電訊情報或量測與訊跡情報蒐集系統)，對我實施訊跡(如電信、電磁波)蒐集。一般普遍的認知就是與電磁頻譜有關，例如雷達、通信、遙(導)控信號、微波……等；另外聲納拍發的音波、船體震動與艦艇俥葉轉動所產生的震動與聲波，都是技術訊跡範疇與態樣之一，[19]同樣必須謹慎管理(技術訊跡管理，如圖六)。

圖六：技術訊跡管理示意圖

說明：除以偽裝網布遮掩物理訊跡外，針對看不見的電磁波是類技術訊跡，則可採電磁波發射管制來執行技術訊跡管理，圖為以偽裝網覆蓋的機動雷達車。

資料來源：蘇仲泓，〈春節加強戰備！海軍「壽山雷達站」反特攻作戰罕見對外公開〉，風傳媒，2020年1月17日，https://www.storm.mg/article/2191030，檢索日期：2024年7月16日。

2. 技術訊跡管理最耳熟能詳的就是電磁波發射管制，這是依據「俄烏戰爭」中的經驗教訓，戰場上俄羅斯士兵因為使用手機，遭到烏克蘭偵知、定位然後被攻擊；因此針對手機管制方面，國軍除建置「行動裝置管理系統」(MDM)[20]或收繳手機等管理方式，以避免我軍部隊的電子參數被

註17：胡瑞舟，〈認識武裝衝突法系列三 武裝衝突法 軍事價值顯著〉，《青年日報》，2006年1月18日，https://www.youth.com.tw/db/epaper/es001001/eb0037.htm，檢索日期：2024年7月16日。

註18：謝孟哲、吳承斌〈以假亂真！用氣球換飛彈 充氣坦克10分鐘變戰車欺敵軍〉，三立新聞網，2019年1月17日，https://www.setn.com/News.aspx?NewsID=486685，檢索日期：2024年7月16日。

註19：游凱翔，〈學者：潛艦作戰是聲音戰爭 聲紋資料列為高度機密〉，中央通訊社，2023年10月2日，https://www.cna.com.tw/news/aipl/202310020109.aspx，檢索日期：2024年7月17日。

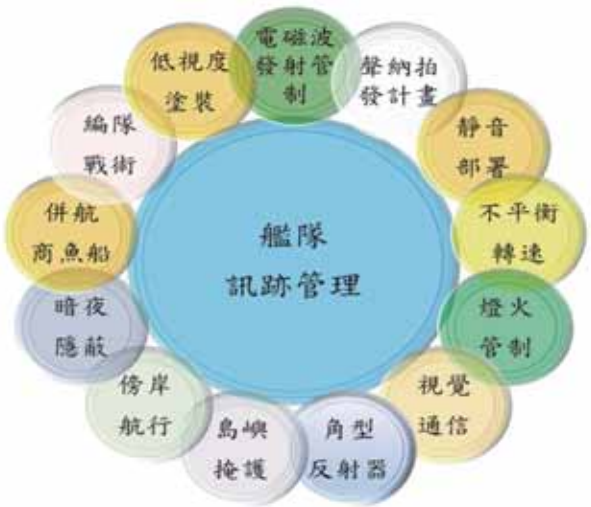
註20：〈恪遵保密規定 確維機密安全〉，國防部政戰資訊服務網，2016年1月26日，https://gpwd.mnd.gov.tw/Publish.aspx?cnid=151&p=4702，檢索日期：2024年7月17日。

截收，進而被敵軍識別、定位與攻擊；尤其，當前面對中共反輻射無人機的廣泛運用，更提醒國軍對各式武器的搜索與射控雷達進行的發射管制，不僅重要且須謹慎規劃。

3. 海軍艦隊的電磁波發射管制，比起國軍地面部隊及飛機，似乎更多元且複雜，發射管制作為除了雷達波(如停止發射、間歇性發射或各艦計畫性的輪值發射)與通信管制(無線電靜默)之外，還多了聲納及反潛作戰因應作為。聲納的禁止拍發、間歇性拍發或各艦計畫性輪值拍發，均是為了避免被潛艦發現；而啟動氣泡幕、採取各級靜音部署、或採用不平衡轉速等，都是具體技術訊跡管理的手段。其目的除避免艦艇被發現外，這些作為的深層意涵即在混淆、欺敵，最終導致敵誤判(艦隊訊跡管理多重手段示意，如圖七)。

二、中共蒐集國軍訊跡的手段

中共針對國軍各類訊跡蒐集方式，概略分為「軍事」及「非軍事」手段，「軍事手段」即是透過人員運用軍事科技裝備來蒐集我各類訊跡，例如用衛星偵照、電偵截收、雷達、無人機偵察、媒播公情蒐集、網軍等；[21]至於「非軍事手段」，也都普遍被各國情治單位所運用。由於敵我



圖七：艦隊訊跡管理多重手段示意圖

說明：海軍艦隊由於裝備及武器多元，同時又面對的是多重威脅，因此所需採取的各式訊跡管理作為，自然就顯得比陸軍或空軍複雜許多。

資料來源：由作者整理繪圖。

雙方都知道，即使訊跡管理機制、規章及規範再周延縝密，關鍵破口仍然在於「人」，所以中共常常利用人性的弱點，慣常採取設局威脅、金錢收買[22]、色誘等手段，[23]以獲取重要情報；尤其近幾年，中共蒐集國軍訊跡手段的案例，不斷在媒播中出現，再再都考驗著國軍的防杜機制是否周延縝密。

三、訊跡管理的關鍵及重要性

(一)雖說國軍都有相關的訊跡管理機制，但未必表示這類機制都是周密完備；且隨著科技的日新月異，相信敵人的偵蒐

註21：〈中共網軍？「信息支援部隊」成立 習近平：全新戰略性兵種〉，《自由時報》，2024年4月19日，https://news.ltn.com.tw/news/world/breakingnews/4646934，檢索日期：2024年7月17日。

註22：黃子杰、陳信隆，〈地下錢莊遭共諜滲透 雷達站官兵涉盜賣機密〉，公視新聞網，2024年1月2日，https://news.pts.org.tw/article/674407，檢索日期：2024年7月17日。

註23：〈國防部陸軍少將羅賢哲遭大陸吸收 長期洩漏國家機密 監察院糾正國防部及陸軍司令部〉，監察院，2011年11月18日，https://www.cy.gov.tw/News_Content.aspx?n=124&sms=8912&s=5871， 檢索日期：2024年7月17日。

裝備以及情蒐的手段，同樣會「與時俱進」。換言之，國軍對敵情的掌握與情研手段，必須隨著科技進步更上一層樓，並經常反省共諜案件教訓；更要明白不論多縝密的作戰計畫，或是多先進的武器或裝備，都還是必須仰仗「人」的參與及操作，況且不論是任何應管制的訊跡外洩，亦或是被敵偵知，追本溯源最終還是會回到「人」的因素。所以國軍在對「人」的教育、管理與制約方面，雖然已有保密查核與安全調查等機制，以及洩違密涉法懲處宣導，此外仍應重視法紀教育，[24]用以制約防範可能造成的洩、違密情事；畢竟現今軍事強權的美國，一樣重視著洩密事件的防杜，這也更凸顯出「人」在訊跡管理上的關鍵地位。

(二)國軍既有的訊跡管理機制中，規範的程度是否周延，當然是檢視完整性的重要環節；且除了嚴格限制資訊及網路使用來落實保防作為外，也必須從另一個面向思考，就是對於「人」的教育與作戰紀律管理，必須更深入且周密。此外，國軍也應該檢視更深一層的警示意涵，那就是重新務實的檢討「軍人武德」教育，亦須嚴正面對與思考此課題。面對「少子化」及軍中「人才招募」對象的新世代化(這也是全球多數國家也都會面臨同樣的問題)，加上現代社會的多樣物質誘惑、網路靜默的認知蠶食、世俗價值觀的變異等問題上，[25]都可能造成軍人武德式微；因此，謹慎面對、積極應處，才是避免「人為」因素造成訊跡外洩的最佳解方。

伍、結語

面對科技日新月異的現代戰爭，戰場透明度也隨著科技變得越來越高，尤其中共的「北斗衛星」、新世代戰機、[26]各式無人機的持續發展，加上其軍艦、飛機的擾臺已趨常態化，對我國威脅程度更是「與日俱增」。目前在兩岸懸殊的軍備與軍力態勢下，國力對比如同失衡的槓桿，此刻國軍若能從源頭將敵軍目標獲得(Find)及目標研判(Fix)程序阻斷，就可能造成敵人無法順利執行「擊殺鏈」後續追踪(Track)、分配(Target)、接戰(Engage)、戰果評估(Assess)等程序，或能在戰場上獲取部分的致勝先機。換言之，與其讓敵人先建立起「擊殺鏈」，再來面對如何處

註24：國防部，〈熟稔保密作為 防範洩密違規〉，國防部政戰資訊服務網，2016年5月19日，https://gpwd.mnd.gov.tw/Publish.aspx?cnid=151&p=4712，檢索日期：2024年7月17日。

註25：張原彰，〈中共蠶食臺灣系列(6)「結語篇」 共產主義滲透全球 學者：間接輸血給中共〉，大紀元電子報，2017年11月30日，https://www.epochtimes.com/b5/17/11/29/n9907764.htm，檢索日期：2024年7月17日。

註26：楊祖宇，〈殲 -20今年將達400架! 美重「次世代制空權」六代戰機競賽已開始〉，Newtalk新聞，2024年3月6日，https://tw.news.yahoo.com/%E6%AE%B2-20%E4%BB%8A%E5%B9%B4%E5%B0%87%E9%81%94400%E6%9E%B6-%E7%BE%8E%E9%87%8D-%E6%AC%A1%E4%B8%96%E4%BB%A3%E5%88%B6%E7%A9%BA%E6%AC%8A-%E5%85%AD%E4%BB%A3%E6%88%B0%E6%A9%9F%E7%AB%B6%E8%B3%BD%E5%B7%B2%E9%96%8B%E5%A7%8B-044733681.html，檢索日期：2024年7月17日。

理高端武器的致命威脅與危害前；部隊若能先從做好「訊跡管理」著手，阻斷敵目標獲得及研判這兩個關鍵源頭，對於提升戰場存活率，或許就可以獲得較實質的效益。換言之，嚴謹、完整的訊跡管理，對國軍而言，不失為阻斷敵人順利完成攻擊的可行方法。

有別於陸上固定的軍事設施，大多數極可能在平時即已藉由網路公開情資，都被敵人標定，很難避免遭鎖定攻擊；但是艦艇、戰車、機動飛彈車、雷達車，資通電軍的干擾車、電偵車，以及空軍的戰機等部隊而言，機動性也是一種優勢，做好訊跡管理、減少訊跡暴露，就能降低被敵發現的機率。畢竟在戰場上，缺少足夠的訊跡，對敵人來說，將無法順利、可靠的做出關鍵性的研判；且從另一個面向看來，若被敵人先發現部隊訊跡，則必須善用假訊號或偽裝來混淆、誤導敵人的鑑別與辨識。現代戰爭先要能提高存活率，才能談後續作戰；因此，「訊跡管理」是軍事作戰中不可忽視，也是戰場管理重要的一環，更可能是阻斷敵人「擊殺鏈」的重要關鍵，殊值國軍重視。 ⚓

作者簡介：

沈育德上校，海軍軍官學校85年班、國防大學海軍指揮參謀學院98年班、國防大學戰爭學院103年班。曾任海軍旭海軍艦艦長、海軍131艦隊戰隊長、海軍151艦隊參謀長、國防部作戰及計畫參謀次長室副處長，現服務於國防大學海軍指揮參謀學院。

左營軍區的故事

海軍育幼院

為照顧與安置失親遺孤，海軍於民國45年成立「海軍第一育幼院」，舊址位於明德新村35號；民國50年將院區遷往左營大路2號，更名為「海軍育幼院」。後因國防部結束三軍育幼院機構，該院併入「中華婦女反共抗俄聯合會」，更名為「婦聯會附設海強幼稚園」；其後於民國97年9月31日停辦幼稚園，目前該園區移交國防部軍備局。(取材自《鎮海靖疆-左營軍區的故事》)