● 作者/Dennis W. Katolin ● 譯者/王建基 ● 審者/黃坤銘

強化通信部隊情蒐能力

The Need for S-2s in Communications Units: Comm Formations as Maneuver Units within Global Kill Chains

取材/2022年9月美國陸戰隊月報(*Marine Corps Gazette*, September/2022)

美陸戰隊通信部隊肩負各項鏈路維管與防護作業，卻無從得知相關威脅情資，先行策擬因應作爲。本文建議陸戰隊進行組織調整、拓展通信人員專長及調整指揮官情報需求，全面提升通信部隊作戰效能。

(Source: US National Guard)

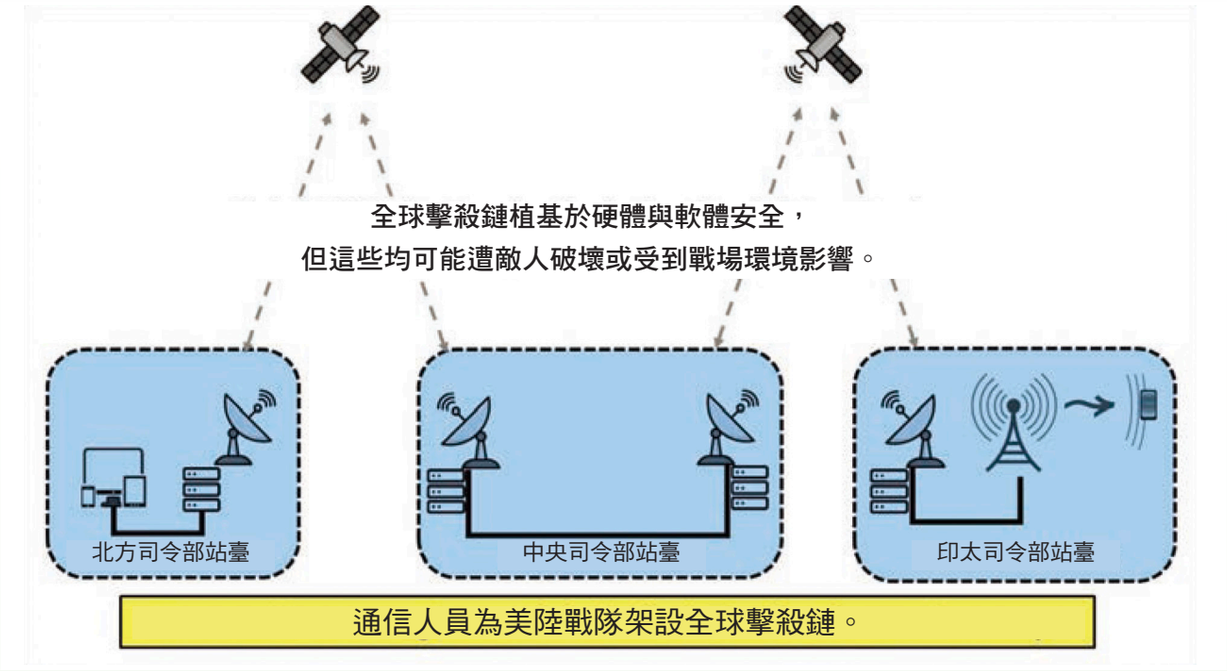


圖1：通信人員建立擊殺鏈來回答問題一。(Source: Dennis W. Katolin)

鑑於大國競爭興起，美陸戰隊提醒自己，當前已不再執行反叛亂作戰。目前焦點是意在武裝衝突門檻下與美國競逐的那些同等級對手，所造成之種種威脅——在太空、網路及電磁頻譜中均占有一席之地。雖然我們認為應對上述三個領域(本文將電磁頻譜視為一個領域)多加注重，但事實上，陸戰隊卻是遠遠落後於今天所面臨之威脅。這是因為沒人全盤探究敵人在網路、太空及電磁頻譜領域內之各項戰術、系統、編組及能力。身處這三個作戰領域的通信單位，必須為陸戰隊提供此類能力。從通信單位便可看出整個擊殺鏈。這些單位接著應注意擊殺鏈所面臨之種種威脅，俾使陸戰隊陸空特遣部隊各級指揮官訂定指揮官情報蒐集要項，推動情報蒐集與目標標定作業。這要從通信部隊建制情報人員著手。

作戰需求：指揮官該問的問題

筆者的某位學長曾說：「紅筆作業完後，再用藍筆作業。」意思是我們一直要到理解(以一種可化為行動的方式)敵人意圖後，才有辦法產生自身計畫。指揮官都該問以下三個問題，但目前通信部隊僅關切其中一個：

問題一：「如何建立指管？」(見圖1)

通信部隊未考量敵人如何攻擊自身網路，就逕行建立自身指管。美陸戰隊陸空特遣部隊各級指揮官之所以會允許這種情況發生，是因為他們大多不注重敵軍網路威脅。在通信單位開始為指揮官建立指管前，指揮官必須提出第二個問題：

問題二：「敵軍如何攻擊指管系統？」

當我方情報人員綜整陸地、空中及海上威脅時，上級只給他們少數幾種模式(簡單易懂的那幾種)，呈現來自太空、網路及電磁頻譜領域的威脅。作戰環境情報整備(Intelligence Preparation of the Operating Environment, IPOE)大多置重點於來自陸地、空中及海上威脅——主要是因為我們有既定模式呈現這些威脅。但不幸的是，這會使網路、太空與電磁頻譜領域威脅變得晦暗不明，也無法判斷前述領域情資與陸地、空中及海上情資間的關聯性。作戰環境情報整備呈現完整陸地、空中及海上威脅時，指揮官就可以據此擬定反制作為。但觸及網路領域時，情報人員就只能告訴指揮官，敵人在這方面「蠢蠢欲動」。

這些模糊不清的評估與分析報告，會使指揮官對威脅失去防備，而無法適切應處。美陸戰隊陸空特遣部隊指揮官應開始提出一些明確問題，並從需要明確答案的作戰環境情報整備相關問題著手。如果情報正確無誤，作戰環境情報整備就能促使指揮官適切分配運用情報資源，針對所獲情資採取相應手段。

作戰層次解決方案：通信情報

作戰環境情報整備並非只是情報人員的職責，每個人都責無旁貸。在資訊領域中，沒有哪一個兵科比通信官更加衡平。此類專長人員須建立美軍全球擊殺鏈，並加以監視。他們最適於將通信面向之需求告知情報部門，將這些需求納入作戰環境情報整備。但問題是，多數通信部隊是將自己視為「支援單位」，而非「受支援單位」。若欲建立起那種能結合太空、網路及電磁頻譜的全球網路，就必須對全球威脅時刻保持警覺，以防範我們遭受該威脅而無法使用擊殺鏈。通信單位應建立一種網路，預判具有特定能力、可攻擊我軍特定系統網路之行為者(硬體與軟體面向皆然)。

是否已經知道有哪些行為者，企圖在美軍進行部署之際侵入網路？該行為者是否具備那種能瞄準小型衛星地面站之干擾器？美軍衛星基準站是否有那種能阻礙該行為者接收美軍對地傳輸資料能力之干擾器？如果有，何種頻率易受到干擾？小型衛星地面站是否位於敵火射程之內？敵軍是否具備能夠滲透美軍基地、截斷電纜線與光纖電纜之特戰部隊？在美軍作戰環境中，是否有大量城鎮載臺發射電波？以上種種都需要持續不斷的情報資料，而且通信人員絕對需要！要做到這點，各通信中隊與通信營皆須設置情報參謀，確保前述單位在作戰期間能落實掌握各種威脅(見圖2)。

一旦獲得情報，通信人員(及指揮官)知曉敵人與環境對美軍網路之影響後，就能對美軍網路開始加以規劃，使其更能對抗這些威脅，而這點就能接著回答第三個問題——**問題三：「應如何確保指管安全無虞？」**

通信部隊成為感測器與機動單位

就網路空間層面而言，任何一套網路皆可能遭受實體與邏輯層面攻擊。實體層面包括電磁頻譜與太空裝備。工程設計是建構堅實防禦措施(以及從而使此防禦能力成為潛在反擊能力)的基礎。瞭解敵電磁作戰系統性能後，就能據此決定我方發射站設置地點及電磁頻譜運用頻段。此

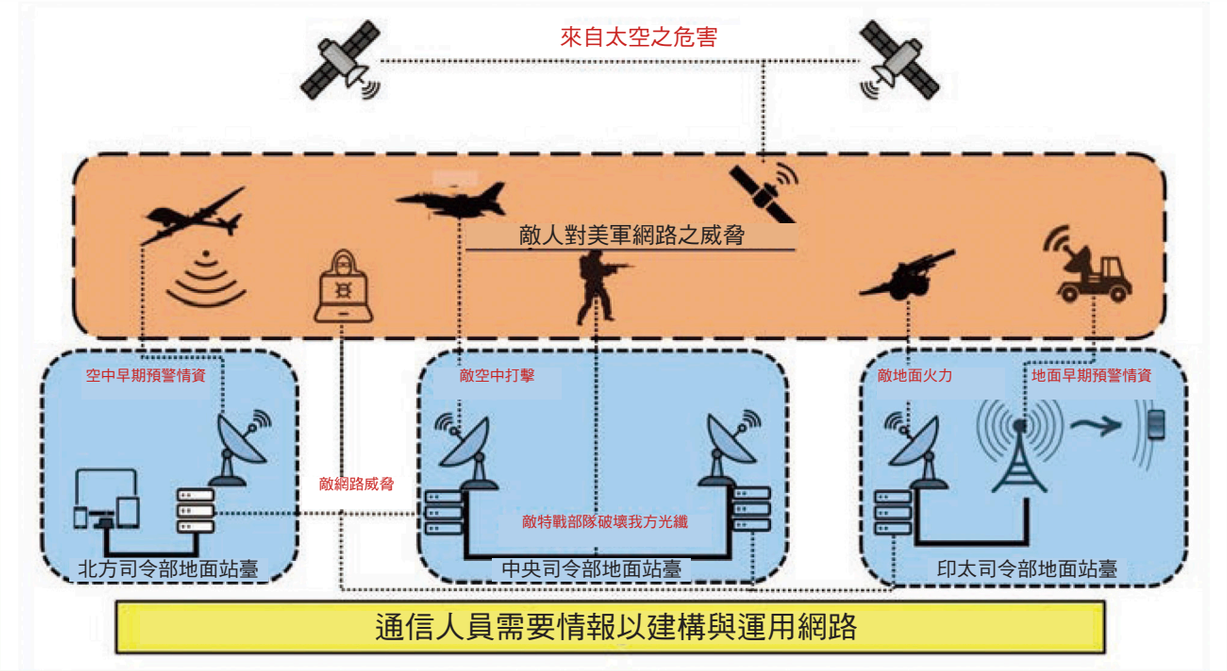


圖2：通信單位持續監控全球擊殺鏈威脅警覺，對作戰環境情報整備作出實質貢獻。(Source: Dennis W. Katolin)

外，根據敵軍火力，也可決定中繼站及天線架設地點。

瞭解敵人使我方衛星失去感測功效，或者從地面干擾我方衛星傳輸之能力後，可使我們知曉自身太空領域弱點，且有助於提升我方工程在這方面的韌性與彈性。我方所使用之光纖電纜屬何國所有，而該電纜是否易受敵特戰部隊破壞？網路空間的特定威脅應納入網路建設工程項目，以肆應可能的病毒或魚叉式網路釣魚攻擊。如此一來，亦可促使通信單位與網路使用者更加努力工作，以保證各項資訊防護作為均有所規範、均能加以落實且滿足所需，以防範敵人侵入我方網路與系統。雖然會有人認為，網路部隊致力維持我軍網路暢通，但敵人對依靠網路運作的各項系統虎視眈眈，摩拳擦掌試圖發起攻擊。這就是我方網路部隊應特別注意的。若能影響美陸戰隊先進野戰砲兵戰術資料系統(Advanced Field Artillery Tactical Data System)射擊諸元，抑或掌握共同航空指管系統(Common Aviation Command and Control System)軌跡資料時，又何必破壞伺服器？雖然執行過程極其複雜，但敵可單靠入侵與操弄網路，就可使我軍對友軍發射砲彈，或使我軍飛機互撞。

這些問題會增加通信單位作業範疇，不只建立網路，還要操控網路。通信部隊必須觀察網路上各項活動，並據以考量是否有必要轉用替代衛星、傳輸終端站臺，或者改變伺服器或路由器的數位行動。敵人一定

會有所行動。我們必須先行預測，並做好反制準備。

我們反制敵人的方式之一，就是將自己當作是資訊環境中，「火力單位」之前進觀測員(Forward Observer)。雖然通信單位負責防範威脅，但並非(也不應擔任)威脅反制單位。攻勢網路作戰、迅速電磁反制，甚或是動能火力，均應提供給美陸戰隊陸空特遣部隊，以反制敵人網路攻擊。就像其他火力，前述作戰手段也需要「偵測、決心、執行與評估」(Detect, Decide, Deliver, and Access)的3DA目標攻擊模式(見圖3)，而通信部隊必須協助進行「偵測」。是否有人攻擊美軍網路？此一資訊必須傳送至陸戰隊遠征軍資訊群(MEF Information Group)，以作為如何作出反應、採用正確火力，以及協助後續評估。通信單位如欲成為前進觀察員，就必須提高威脅警覺，立即偵知威脅，而這需要情報。

只有網路部隊不夠

有些人會說，這些問題早已交由美陸戰隊防禦性網路與內部防禦機制(Defensive Cyberspace Operations-Internal Defensive Measures, DCO-IDM)連處理。這是以管窺天，未全面看待美軍整體擊殺鏈之不足。防禦性網路與內部防禦機制連，依法僅遂行美陸戰隊所屬網路作業，而不能超出前述網路作業範圍。

該連針對敵軍砲兵或特戰部隊威脅，能提供我軍何種協助？要求協助提高我軍網路在敵電磁戰威脅或太空活動下之韌性，是否合適？答案是不合適。目前蒐集之情報，完全能輔助其進行掃描、

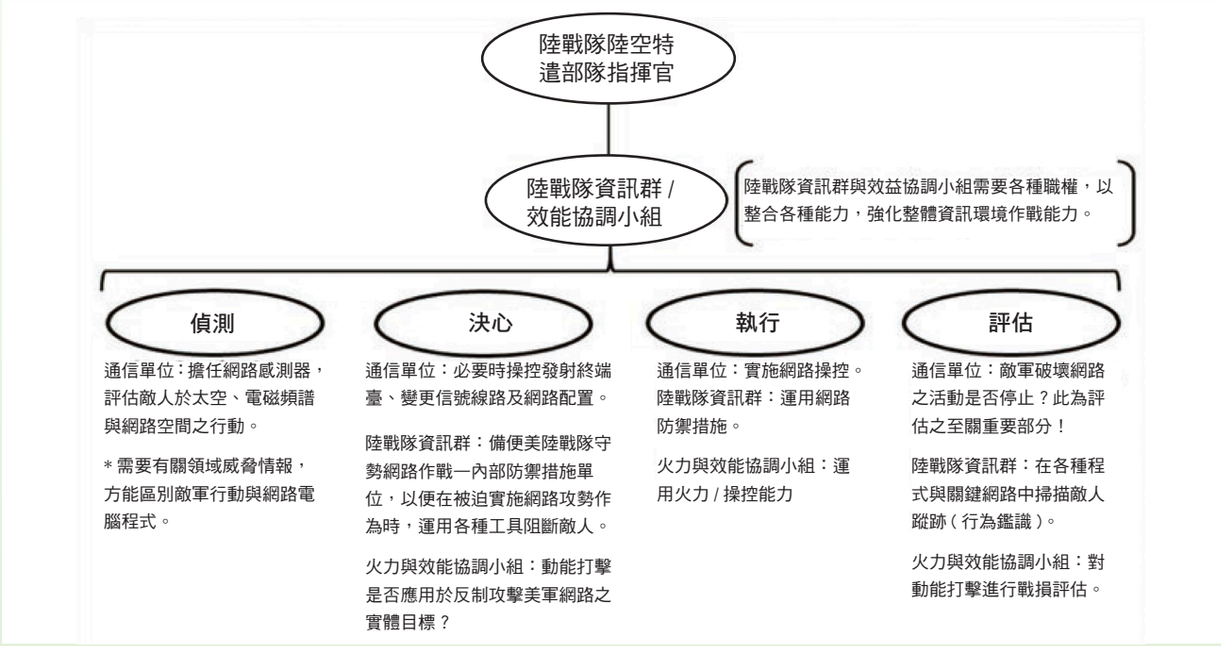


圖3：3DA架構下的通信單位 (Source: Dennis W. Katolin)

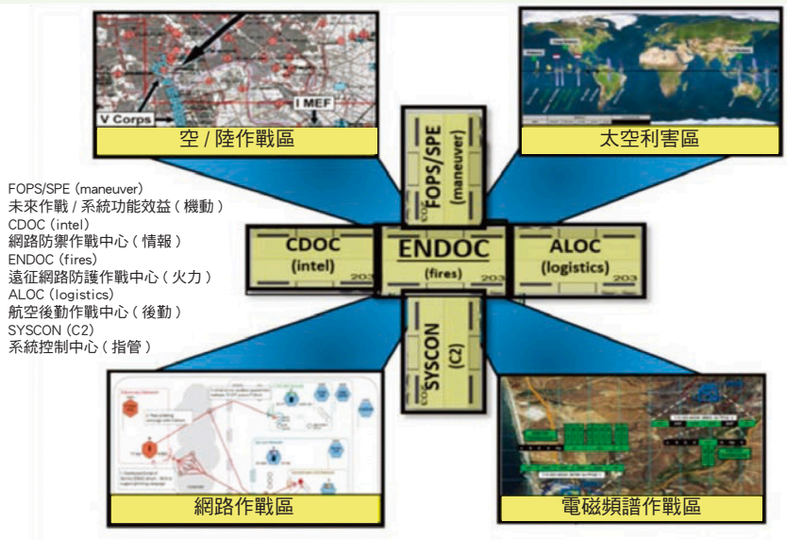
蒐集及鑑識等行動，並透過縱深防禦措施，保護我軍網路。前述連級單位確實是擊殺鏈整體防禦措施中關鍵且涉及高端技術的部分，但他們僅能防護擊殺鏈中特定鏈路。此外，如果必須運用美陸戰隊防禦性網路與內部防禦機制連在網路中追擊敵人，那麼美軍可能早就敗下陣來，因為敵人根本就不應該有辦法侵入我方網路。

接下來該怎麼做？(從低成本辦法著手)

這個問題的解決辦法並不困難，但確實須對通信兵科及陸戰隊陸空特遣部隊進行澈底改革。

1.通信單位情報人員不一定要具備情報專長：當初筆者派任美陸戰隊航空聯隊第28通信中隊隊長時，便立即爭取在中隊編制一個情報官職缺。根據編裝表，行政官為通信專長，而非人事專長。猜怎麼著？本隊行政業務辦理得極為圓滿！我決定對麾下情報官如法炮製。塔茜珂(Leanna Tacik)中尉對於網路所面臨的威脅，素來能找出許多精闢問題，也頗能運用陸戰隊遠征軍內部網路，以及整個情報部門相關情報，提供整個團隊敵人與作戰環境必要情資，以協助美軍在資訊環境中之作戰行動。任何一位具有「機密」以上接密等級的人，都能進入各種情報網站。

2.指揮官在戰場情報整備中，應提出即時資訊環境情報需求：傳統上，飛行單位一向十分關切敵飛行與防空能力，而且絕不會等閒視之。然而，敵人對美陸戰隊航空聯隊之威脅，已擴展至資訊環境，危及陸戰隊航空聯隊擊殺鏈。我們並未使指揮官充分知曉，有哪些資訊環境中的特定行動，使其無法派出戰機支援陸戰隊陸空特遣部隊。陸戰隊航空聯隊第28通信中隊與陸戰隊空管第28大隊(Marine Air Control Group 28)，早已擔負責任，協助指揮官瞭解相關威脅，並將之融入指揮官整體威脅評估。建立指管對我們而言已經不夠，我們必須讓指揮官知曉，如何能確保指管安全無虞。第一步就是取得可能危害飛行部隊指管之威脅，進



情報應融入通信單位作業，遠征網路防禦作戰中心在獲得情報後，持續關注整個擊殺鏈狀況，俾於攻擊目標過程中執行偵測、射擊及評估等步驟。

圖4：遠征網路防禦作戰中心獲取情報後，預測威脅並執行網路運作。(Source: Dennis W. Katolin)

行情報分析。

3.遠征網路防禦作戰中心(Expeditionary Network Defense Operations Center, ENDOC)：傳統上，通信單位是透過某處系統管制中心(Systems Control Center, SYSCON)接受上級指揮。該中心係一網路監視站，負責找出網路何處故障，並引導故障排除作業。這樣遠遠不足。雖然系統管制中心對作戰成敗影響甚鉅，但卻專注於行政庶務。該中心並未全盤瞭解當面威脅。各通信中隊長或營長，不應督管系統管制中心運作，這種工作交給連長執行即可。通信單位指揮官應負責作戰中心運作，掌握網路運作狀況。這需要成立一處作戰中心，彙整各單位情報與系統管制中心數據，並引導陸戰隊陸空特遣部隊與下級單位指揮官，在面對敵人威脅之際，善用此情報網路進行相關決策。我們已成立此類機制，稱為遠征網路防禦作戰中心。本中隊遠征網路防禦中心負責軍官契斯那(Daniel Chisner)中尉，已經在挪威冷反應(Cold Response)演習中，根據實況指揮該中心運作。

4.拓展通信人員本職學能：美陸戰隊所訓練出的通信人員極為優秀，均能進行網路相關計畫與建置作業。前述通信人員具備基礎網路工程相關知識，對開放式系統互聯(Open Systems Interconnection, OSI)模型有所瞭解。通信官兵所欠缺者，乃是對情報作業流程、目標標定、計畫作為或陸戰隊陸空特遣部隊特性等面向。其部分原因，是出自「我們只是支援兵科」的那種思維架構。我們該向誰索取情報？這是作戰單位的工作！通信部隊現在必須隨時掌握威脅，不斷保持戰場覺知，並建立一組情報團隊，提供敵方威脅情資。我們同時也必須能參與目標標定，並讓人知道，通信部隊成為資訊環境中的前進觀察員，必能引導陸戰隊陸空特遣部隊、聯合部隊及跨軍中火協作業。這都不須撰寫新書加以闡明，而只需要重拾老準則即可(尤其是《陸戰隊陸空特遣部隊火力》[*MAGTF Fires*]、陸戰隊作戰準則《情報作戰》[*Intelligence Operations*]，以及聯戰準則《作戰環境聯合情報整備》[*Intelligence Preparation of the Operational Environment*])。

結論

坐而言很容易。長久以來，通信人員「放棄」自身在情報環境中所該扮演之作戰角色。該是採取行動的時候了。身為一個軍種，美陸戰隊嘴上總說，要對此類威脅隨時保持警覺，而且已發展出一種依賴太空、網路及電磁頻譜的作戰模式。我們知道前述領域都不容忽視，但千萬別將這些領域一概視為整體擊殺鏈。通信人員獲准存取這些鏈路。為了善用資源進行鏈路防護，通信單位必須能從陸戰隊網路獲取威脅情資。雖然取得美國國防部內部情報須通過層層關卡，但對於通信人員而言，此一過程必須透過在通信單位設置情報人員著手，從組織內部開始做起。

作者簡介

Dennis W. Katolin中校具通信與作戰計畫專長，現為美陸戰隊航空聯隊第28通信中隊(Marine Wing Communications Squadron 28)中隊長，曾任陸戰隊副司令(資訊)計畫官，亦為陸戰隊準則第八號《資訊》(*Information*)之共同作者。

Reprint from *Marine Corps Gazette* with permission.