● 作者/E. Lincoln Bonner III ● 譯者/高一中 ● 審者/劉宗翰

網權在21世紀聯合作戰的角色

Cyber Power in 21st-Century Joint Warfare

取材/2014年第3季美國聯合部隊季刊(*Joint Force Quarterly*, 3rd quarter/2014)

2008年俄羅斯與喬治亞的戰爭，網權首次被整合至軍事戰役中，藉由實施網路偵察、獲取並維持網路優勢及遂行網路阻絕，網權的累積效應可迫使敵人犯錯而終致潰不成軍。

戰爭中迫使敵人犯錯，往往可使戰局扭轉。

—李德哈特(B. H. Liddell-Hart)
《戰略論：間接路線》(1941年)

2008年俄羅斯部隊在網路攻擊的支援下，迅速擊潰喬治亞軍隊，奪取了該國領土，其後並以此領土作為交換條件，要求喬治亞給予親俄的南奧塞梯(South Ossetia)和亞布卡薩(Abkhazia)政府更大的自治權。網權(*cyber power*)乃利用網際空間創造優勢及發揮影響事件的能力，而網際空間(*cyberspace*)則為相互依存且相互連結的電子網絡與電磁頻譜，吾人於此一空間內創造、儲存、更改、交換及利用資訊。[1] 2008年俄羅斯與喬治亞的戰爭，係目前唯一整合了網權與傳統動能軍事作戰(kinetic military operation)的公開案例。然而，迄今為止，鮮有人重視應如何將網權整合至傳統軍事作戰中。一般的研究傾向聚焦於單獨運用網權進行間諜活動，以及遂行戰略攻擊以懲處並/或強迫一國依我方意志行事。

本文則著手處理這種研究上的罅隙，而聚焦於探討如何最有效地將網權整合至聯合作戰中，以利遂行戰爭

美空軍部長辦公室作戰整合主任兼資訊長在巴克斯岱爾(Barksdale)空軍基地的研討會中討論網路安全問題。
(Source: USAF/Chad Warren)

並贏得國家勝利。本文以俄羅斯與喬治亞的戰爭為例，指出將網權整合至聯合軍事戰役的主要價值在於，可藉由實施偵察、獲取優勢及遂行阻絕等三項主要作戰任務，迫使敵人犯錯。文內首先描述網權的主要作戰任務如何削弱/破壞敵人的決策週期，以支援我方的動能作戰。接著分析俄羅斯與喬治亞戰爭中的網路面向，並說明親俄部隊如何運用網權來削弱喬治亞的決策週期，以支援其動能軍事作戰。最後，將討論目前與未來網權整合至聯合作戰之意涵。

實施偵察、獲取優勢及遂行阻絕

網權的演進模式與早期空權相似，將可能在目前及可見的未來對聯合作戰有所貢獻，亦即可實施網路偵察、獲取並維持網路優勢，以及遂行網路阻絕。

第一次世界大戰時，空中偵察優勢引發了爭奪空優的戰鬥。空中偵察能提供「敵陣營活動或敵改變部署的預警，而且除少數例外之外，還能預判敵人的攻勢，並有助於確保不讓敵人得逞。」[2] 因此，獲取並維持空優的需求應運而生，期能確保從空中觀測中獲得資訊優勢。儘管空中偵察對

有效遂行陸上作戰極具價值，但其本身卻無法直接削弱或擊潰敵人作戰行動。

同樣地，網權的軍事發展根基於偵察作業。誠如曼迪安特(Mandiant)公司最近一份有關中共網路間諜活動的報告強調，能進行更有效網路偵察作業的一方可獲得相當大優勢，這點是促成發展網權的主要動力。[3]其次，有效網路偵察及伴隨而來的資訊優勢又取決於擁有最起碼的網路優勢。和空權的情形一樣，網路偵察與網路優勢可促使友軍遂行更有效的作戰，但無法直接削弱或擊潰敵人作戰行動。

1936年，即第一次世界大戰結束後的18年，英國皇家空軍斯萊塞爵士(Sir John Slessor)描述了如何將空權整合至陸上作戰，直接大幅削弱或擊潰敵空中與陸上戰力。他以英軍在中東的作戰情形為依據，其推論道，空權在空地聯合戰役中的主要作戰任務除空中偵察外，還包括獲取並維持空優，以及阻絕敵陸上交通線與補給線。目前，空優依然使得友軍能在不受敵嚴重干擾的情形下，利用空權遂行偵察、機動與攻擊。[4] 空中阻絕則可摧毀或破壞敵人補給體系或通信系統的組成要素，使其在相當長時間內難以順利運作，敵人這方面的能力立即或逐漸降低的情況，勢必使其無法維持有效作戰。[5]

網路優勢與網路阻絕的功能和空中優勢與空中阻絕類似。網路優勢可提供友軍利用網權遂行偵察、通信(亦即資訊機動)及攻擊的能力，同時還能不受敵人的阻礙干預而執行定向作業(即資訊/電腦處理作業)及指揮管制。網路阻絕可破壞、摧毀或癱瘓敵人陸、海、空與太空部隊所使用的電子資訊傳輸線和電子資訊補給系統(即網際空間)，使其在相當長時間內難以順利運作，因而立即或逐漸喪失有效作戰的能力。第二次世界大戰的轟炸機缺乏目前可取代陸上部隊的殺傷力，俾用以消滅敵軍的精準攻擊能力。因此當時空權的主要攻勢作為在於空中阻絕。如同斯萊塞爵士的時代一般，網路攻擊行動在今日聯合作戰中的主要貢獻即在於網路阻絕。

在空中與網際空間領域內，用以摧毀或癱瘓敵空中和網路部隊的攻勢作戰，乃在這兩個領域內建立優勢的主要手段。然而，網路偵察在獲取網路優

用以摧毀或癱瘓敵空中和網路部隊的攻勢作戰，乃是空中與網際空間領域建立優勢的主要手段。(Source: USAF/Jeremy T. Lock)

美陸戰隊員於「標槍刺擊」(Operation *Javelin Thrust*)演習期間監控飛機與地面部隊，俾將資訊傳送至作戰單位。

(Source: USMC/Chelsea Flowers)

勢上所扮演的角色，遠比空中偵察在建立空優上所扮演的角色來得重要。於網際空間的戰術層級，行動與觀測的速率都接近光速。換句話說，因為觀測係以光速進行，所以網路防衛者無法享有雷達給予防空者的預警時間優勢。因此，戰術防衛將不會有充分預警作為，以因應網路攻擊並防止重大負面效應。網際空間內的戰術防衛作為將比較像戰損修護、恢復運作及重建工作，而非迴避類似的實質攻擊。因此，有效擊潰網路攻擊主要靠的是採行一系列我方事先了解敵方所無法克服的防衛措施。亦即，達成網路優勢的最有效方法是，動用使敵方可能採行相對應網路攻擊與防衛作為失效的網路防衛與攻擊能力。在沒有已知先例的情形下，癱瘓可能的敵網路攻擊與防衛，乃至關重要的需求，也是掌握網路優勢的關鍵。而欲達此目的，必須獲取有關敵網路攻擊與防衛能力、戰術、戰技與程序的技術情報。雖然全方位情蒐(all-source intelligence)有助於建立這種預知情資，但蒐集必要情資的主要方法仍在於從事網路偵察。不像一般的戰鬥序列，網路能力只存在網際空間內，故除了在網際空間內進行觀測外，別無他法。因此，平時在網路偵察中獲勝者，也可能在戰時的網路優勢爭奪戰中勝出。

為獲取並維持網路優勢，平時的網路偵察作業應律定有關敵網路偵察與攻擊能力(如敵惡意程式碼發展狀況)及敵網路防衛能力等情資之優先順序。獲得有關這些活動的情資後，將可發展並部署網路防衛能力，俾事先使敵人的網路攻擊喪失效用，以及發展讓敵人網路防衛無力招架的網路攻擊能力。擁有讓預期中的敵網路防衛束手無策的網路攻擊能力，係從事網路阻絕的必要條件。這一系列網路偵察活動的動能結果，可能比較類似戰場情報整備。因此，平時應不斷持續進行網際空間情報整備，此將決定網路優勢的成敗。

擁有網路優勢方得以遂行網路阻絕，而後者又補強了前者的效能。一般而言，阻絕是可運用於任何領域的網路作戰構想。電子資訊網路只是種傳輸網路，但其所傳送的不是實體補給品，而是資訊。任何傳輸網路

的目的都是在傳送正確、適當及適時的補給品(亦即在正確的時間將正確的物品送達正確的地點),在網際空間,這種補給品就是資訊。[6] 不論阻絕行動是否要阻止某一網路傳送正確、適當或適時的補給品,其目的都是相同的:要把摩擦與不確定性帶進敵人決策週期中,使得和友軍部隊相較之下,敵部隊愈來愈難以遂行有效作戰。阻絕作為講求的不是任一次對敵網路攻擊所產生的影響,而是阻滯敵行動的累積效應。[7]

成功阻絕行動可影響一個網路的能量──有多大數量(流量)的補給品,能以多快速率(流速)通過網路以滿足使用者的需求。在空中阻絕戰役中,空中攻擊與陸上作戰能相輔相成,合力破壞敵人的補給網路。空中攻擊摧毀、破壞或損害敵人陸上運輸/補給網路(如鐵公路)的節點與連接路線,以削弱其能量。同時展開的陸上作戰則造成大量補給品以高速率流經網路的需求。陸上作戰使敵人補給網路面臨時效性要求,而空中阻絕則阻止敵人網路達成此一要求。舉例而言,韓戰期間,從仁川登陸(Inchon Landing)到中共介入的鏖戰階段,交戰雙方都消耗龐大數量的補給品,故各自要求能有高流量與高流速的補給網路。然而,北韓軍隊必須依賴低能量的鐵公路網來滿足其龐大需求。美國的空中阻絕使得北韓部隊一直都無法及時積存充分補給品或資源,以發動成功的反攻作戰,美軍部隊遂能迅速向北方推進至鴨綠江。在敵人最需要充分補給品時,阻絕行動可使補給網路無法發揮作用。

網路阻絕行動──亦即摧毀、破壞或損害敵資訊網路的節點、連接路線和資料,以阻礙其運作及削弱其能量──與空中阻絕行動的功能類似,但有一項截然不同的特點:不像空中阻絕,網路阻絕將使部分網際空間無法再進行諸如偵察等其他作業。空中攻擊不會阻礙使用空域進行機動與偵察。因為網際空間是由資訊網路組成,故網路阻絕顧名思義將會破壞敵資訊網路,如此一來可能將會妨礙我方網路偵察能力,以蒐集目標網路之相關情資。職是之故,網路阻絕與網路偵察之間存在某種緊張關係。

假若吾人預判衝突將曠日持久,或者假設在某一衝突中動用特定的網路攻擊,將大幅降低我方於更重要的應急作戰中之網路優勢,那麼吾人從事網路偵察的優點將勝過網路阻絕。例如,第二次世界大戰期間,美國預判戰事將持續許久,因此保護其破解德國與日本密碼而獲得的資訊優勢,而不採取可能會破壞這項極具價值情資來源的行動。這項至關重要的情報優勢使美軍得以殲滅大量日本護航艦隊,並可選擇長達3年多戰爭中的作戰時間與地點。[8] 向戰場前進的指揮官必須衡量利弊得失,妥善決定是要犧牲長期網路偵察所獲情報,還是要短期網路阻絕所產生的效應。

網路阻絕可迫使敵人犯錯。如同空中阻絕與陸上作戰之間有相輔相成的關係,高強度動能作戰產生的資訊需求,使得有效運作能量已遭網路阻絕削弱的資訊網路無力因應。為限制網路阻絕的效應,敵人可能會將其資訊補給集中起來,但可能因此增加其遭網路或動能

為獲取並維持網路優勢，應發展讓敵人網路防衛無力招架的攻擊能力。(Source: US Army/Larry Simmons)

攻擊摧毀的風險。此外，旨在更改資料、改變資料流動路線或遲滯資料流動的網路攻擊，將提供敵人一個選項。如果網路攻擊更改敵人的資料或改變資料流動路線，則敵人可能根據其所擁有的資訊採取行動，如此將增加其犯錯的可能性，或者敵人可提出額外請求，企圖獲得遺失的資料，如此將減少其網路的有用能量並阻礙資訊適時發展。如果敵人選擇後者，將使外來資料置入其網路的網路攻擊效應變得更複雜，而進一步阻礙資料適時發展，並可能使其完全無法獲得新資訊。網路阻絕將因此使敵人處於進退維谷的困境，進而危害其決策週期。敵人究竟應放棄決策速度的優勢或決策品質的優勢？不論如何，時間一久，放棄決策優勢的累積效應勢必導致犯錯的情事。

2008年俄羅斯—喬治亞戰爭中展現的網權是分析網權動態在聯合軍事戰役中的一個豐富資料來源。

2008年俄羅斯—喬治亞戰爭中展現的網權

2008年俄羅斯與喬治亞戰爭有助於吾人將注意力集中在網權及戰爭用途，而以往運用網權的事例則前所未見。該次衝突係屬高規格，使其成為許多研究的對象，因此也是分析網權動態在聯合軍事戰役中的一個豐富資料來源。

喬治亞於1991年獨立後，想要繼續成為俄羅斯一部分的分離主義分子奪取了亞布卡薩大部分與南奧塞梯某部分的控制權，其後交戰雙方於1992年及

1994年兩次達成停火協議。[9] 但衝突仍未獲得解決，導致俄羅斯與喬治亞於2008年進行了為期5天的戰爭。[10]

表面上看來，網權在這次與喬治亞戰爭中的角色似乎不是特別突出。喬治亞只有7%的人民每天使用網際網路，[11] 吾人可能因而忽視了喬治亞的網路極為脆弱的事實——其網際網路與外部世界的13個連結點中，有半數以上必須通過俄羅斯，而且通往喬治亞境內網站的大部分網際網路流量須繞經土耳其或亞塞拜然(Azerbaijani)的網際網路伺服器，這些伺服器中許多又須繞過俄羅斯。[12] 喬治亞的網際網路基礎設施深受缺乏名為網際網路交換點(Internet exchange point)的內部連結點所苦。[13] 因此喬治亞使用者欲在喬治亞建立網站的申請可能要繞經俄羅斯，這種情形如同從洛杉磯出發繞經墨西哥前往舊金山。[14] 結果，親俄部隊可運用網權來影響大部分的喬治亞使用者進入，以及使用網際網路內的部分網際空間。喬治亞無法掌控使用內部或外部網際網路所需的基礎設施，若國家遭受網路攻擊時，也無法在不放棄網際網路連線優勢的情形下，採取分散網路流量或切斷網際網路與國外的連結等防衛措施。[15]

在喬治亞軍隊於南奧塞梯的次欣瓦利(Tskhinvali)鎮以大規模砲擊回應俄羅斯挑釁後，雙方戰爭於2008年8月7日正式開打。[16] 莫斯科趁機進一步促成南奧塞梯與亞布卡薩脫離喬治亞獨立，並立即派兵前往南奧塞梯並對喬治亞領土展開空中攻擊。俄羅斯還部署海軍封鎖喬治亞海岸並派陸戰隊員登陸亞布卡薩海岸。俄羅斯機械化部隊與南奧塞梯民兵在次欣瓦利鎮附近擊潰喬治亞的輕裝部隊後，便勢如破竹地攻進喬治亞。[17] 俄羅斯部隊挾其網權的優勢，喬治亞連基本的抵抗能力都付諸闕如。[18]

在戰爭中，俄羅斯的網路攻擊集中且經過精心準備，顯示其對喬治亞的網路優勢與網路阻絕行動，乃早在衝突前就展開的網路偵察及網際空間情報整備之產物。對喬治亞所進行的網路阻絕活動包括網站篡改及分散式阻斷服務(distributed denial of service, DDoS)攻擊。而殭屍網路攻擊(botnet assault)的範疇與集中度都相當精準，亦即只專注攻擊11個目標，且自始至終持續攻擊相同的網站。[19] 大部分網路攻擊都是專門針對喬治亞的特定目標，其中至少有一次網路篡改行動是在戰爭爆發的2年多前就已準備就緒。[20] 此外，網路攻擊目標的標定作業也十分講究。政府與新聞媒體網站係首波被攻擊的目標，如此可使喬治亞人民與官員渾然不知究竟發生何事，藉以散佈混亂狀況，並遲滯任何國際因應行動。除了喬治亞的兩家大銀行外，網路攻擊還標定某些商業實體。這些商業機構可被用來連絡或協調用以對付俄羅斯部隊，尤其是網路攻擊的諸般作為。[21] 從殭屍網路攻擊集中於11個目標上，此次網路攻擊歷經多年發展，以及對喬治亞可能如何採取網際網路因應作為瞭若指掌等事實可看出，親俄網路部隊比喬治亞部隊擁有更大的網路優勢，實乃衝突前卓越的網路偵察作業及網際空間情報整備所致。

親俄的網路部隊透過牽制

作為與直接攻擊來制壓喬治亞的網路防衛，以取得網路優勢。喬治亞境內初期遭到殭屍網路攻擊的11個目標中，包括從事科學、技術與醫療等教育機構。[22] 當時，「喬治亞電腦緊急應變小組」(Computer Emergency Response Team Georgia, CERT Georgia)受僱專門負責為「喬治亞研究及教育網路協會」(Georgian Research and Educational Networking Association, GRENA)所屬高等教育機構提供網路安全。[23] 網路攻擊者攻擊喬治亞的教育機構，導致喬治亞電腦緊急應變小組只聚焦於保護喬治亞研究及教育網路協會的網際空間，而忽略了對更大規模的國家危機做出反應。親俄的網路部隊藉由攻擊敵人必須加以援救的目標──即喬治亞研究及教育網路協會──利用喬治亞電腦緊急應變小組的自然反應來對付喬治亞，以牽制及制壓該國最有效的網路防衛能力。此外，初期11個網路攻擊目標中包括喬治亞的一個熱門網際網路駭客論壇，因而得以阻礙喬治亞某些能力較強的網路專家合力研擬出有系統的因應作為。[24] 親俄部隊使用斯萊塞所描述獲取制空權的方法──即破壞、擾亂及瓦解敵部隊──以達成網路優勢。

親俄網權在整個衝突過程中一直保有網路優勢，以致喬治亞從未能遂行有效的網路防衛或網路反攻。例如，喬治亞曾試圖根據攻擊源(亦即其原始IP位址)資料加以濾除，以達到迴避網路攻擊目的。然而，網路攻擊者的情報整備工作使其得以輕易瓦解此一戰術。網路攻擊者藉由通過外國伺服器來採取攻擊行動的方式，可以隱藏其真正IP位址，並製造假IP位址來欺騙喬治亞的網路防衛過濾器。[25] 儘管如此，喬治亞仍得以使用某些政府網站，因為這些網站已被遷移到美國境內的伺服器上。[26] 喬治亞的網路防衛雖然失敗，但最少試圖遂行一次大規模反擊，只是最終以失敗收場。此外，喬治亞曾將網路攻擊工具與指令置入俄語網際網路論壇，期能誘騙親俄網路部隊在不知情的情況下攻擊俄羅斯網站而非喬治亞網站。[27] 喬治亞此次反擊對俄羅斯網站所造成的損害似乎微乎其微。[28] 整體而言，喬治亞的網路防衛作為力道太弱，開始的時間太遲。

親俄部隊在掌握網路優勢的情況下，利用傳輸網路的一般屬性，遂行網路阻絕以阻滯喬治亞的通信。在初期11個目標遭到首波殭屍網路攻擊後，又有一支特別的網路民兵加入了攻擊行動。此時，網路攻擊工具和一份攻擊目標建議清單被貼在網站上，以利俄羅斯的支持者自行展開網路攻擊。相關攻擊指令可說簡單明瞭，連只具備有限電腦技能的人都可遵照指示行事。這支特別的網路民兵展現甚佳效能，除了先前曾對11個目標進行殭屍網路攻擊外，另還關閉或篡改了43個網站。[29] 總計喬治亞境內有54個與通信、金融及政府有關的網站遭到攻擊，使得喬治亞人無法進入這些網站獲取資訊或指示。[30] 這些網路攻擊使喬治亞部隊無法使用其資訊網路的關鍵部分，也就是網際網路，因而降低了其整體資訊網路的使用量。

因此，網路攻擊擾亂了喬治亞的資訊流量，使得資料無法像平常那樣從網際網路傳輸到諸如電話與無線電通信等較傳

統的管道。此外，陸、海、空的作戰行動，造成對喬治亞整體資訊網路的資料流量與流速的需求劇增。例如，就在俄羅斯即將發動空中攻擊之前，哥里(Gori)鎮的政府與新聞網站遭到分散式阻斷服務攻擊而癱瘓，可想而知資訊需求將因此大增。[31] 隨後資訊通信需求的劇增，加上網際網路與諸如手機與地面電話等更多傳統形式的通信受到擾亂，似乎因而造成了瓶頸現象。

因為有一大部分資料被經由網路攻擊注入網路的外來資料消耗掉，所以喬治亞人嘗試以超過其資訊網路使用量所能容許的更高速率來傳送更多資料。在戰爭初期階段，即喬治亞若採取迅速而有系統的防衛作為(不論是網路或動能防衛作為)將可發揮最大效用之際，其整體資訊網路卻遭受敵網路攻擊的嚴重干擾。[32] 網路阻絕削弱了喬治亞軍隊組織及遂行有效作戰以瓦解俄羅斯軍隊遂行動能作戰的能力，使俄羅斯軍隊因而擁有作戰與戰術層級的優勢。網路阻絕創造了一個使喬治亞部隊會不由自主地犯錯的環境。

再者，敵人藉由干擾喬治亞電腦緊急應變小組獲得狀況覺知及設法進行更有效因應作為的能力，以達成其網路優勢。網路阻絕可大幅增加這種網路攻擊的效能。斯萊塞將空優問題描述為「如何剝奪敵人運用本身空中部隊，以遂行有效干擾作為的能力。」[33] 因為喬治亞的所有資訊通信基本上都受到網路阻絕攻擊的干擾，喬治亞電腦緊急應變小組連要蒐集充分資料以了解網路攻擊的效應都極度困難，更別提要減輕此等效應。網路阻絕行動干擾了喬治亞的所有通信作業，因此不僅阻礙了喬治亞的傳統軍事反應，也可能扼殺其網路防衛能力並延長親俄部隊的網路優勢。

該次戰爭中，為獲取網路優勢所遂行的網路攻擊與網路阻絕行動有相輔相成的關係。兩者合力造成喬治亞通信──其資訊供應系統──的癱瘓，使得喬

美陸戰隊兩架F/A-18「大黃蜂」(Hornet)戰機護航一架F-35「閃電二型」(Lightning II)戰機前往佛羅里達州艾格林(Eglin)空軍基地的情形。

(Source: USAF/Joely Santiago)

治亞部隊無法適時接獲資料與命令。喬治亞被迫在放棄決策速度優勢與決策品質優勢之間抉擇。無論如何選擇，其結果都將是喬治亞所無法克服的完全俄羅斯軍事優勢。

今日網權攸關戰爭勝負，因此，了解如何妥善協同陸、海、空權以對網權做最佳運用，實乃當務之急。

意涵

如同空權問世之初的情況，今日網權攸關戰爭勝負，但其本身可能無法獨力打勝戰，因其顯然缺乏產生強大暴力的能力，雖然未來此一缺點可能會漸漸變得無關緊要。因此，了解如何妥善協同陸、海、空權以對網權做最佳運用，實乃當務之急。空權理論的兩個原則可用來指導作戰層級的網權策略：掌控敵人行動自由；迫使敵人至少在兩個壞的選項中抉擇。網路優勢滿足了第一個原則，而網路阻絕則滿足了第二個原則。2008年俄羅斯與喬治亞戰爭的案例顯示這兩個原則的正確性，但吾人應如何著手獲取並維持網路優勢，以及遂行網路阻絕呢？

由於確保網路優勢乃軍事網權的首要任務，故起初聚焦於癱瘓敵人透過網際空間大肆干擾友軍作戰的能力，似乎是最合理的作為。因此，敵人的網路攻擊、網路偵察與網路防衛能力，應被列為從事網路偵察與網際空間全方位情蒐整備的最優先對象，也是一旦戰爭開打後，我方必須加以制壓或摧毀（不論是透過網路或動能攻擊）的最優先目標。其次，對網際空間內與戰事無關但敵人必須加以救援的部分遂行網路攻擊，諸如攻擊喬治亞研究及教育網路協會，俾使喬治亞電腦緊急應變小組無法分身投入更大規模的衝突，乃甚有價值的作為，因如此一來，可促使敵人將網路防衛部隊聚焦於決戰點以外的目標。第三，網路攻擊應用來阻絕敵人從事網路修理、復原及快速反應防衛部隊所需的資料，以破壞敵人有效抵擋網路打擊的能力。結合此等作為應

確保網路優勢是軍事網權的首要任務。(Source: USN/K. Ashley Lawrence)

可癱瘓、牽制及瓦解敵人的網權，以獲取並維持網路優勢。

在聯合軍事作戰的作戰、戰術與戰略層級，接下來最重要的網路目標為網路阻絕目標。於作戰層級，其情形與第二次世界大戰時類似，當時係以鐵路調車場(marshaling yards)為空中阻絕的主要目標，因此資料調配整備場(又稱資料融合中心)乃為合理的網路阻絕焦點。資料融合中心及其所支援的戰鬥系統(如戰機、戰車與潛艦)相較之下，數量可說少之又少，但卻是原料(資料)進行集中整備進而轉化為資訊──即可供各軍事部隊分享戰場狀況覺知──的重要節點。資料融合中心係網際空間的重心，因其乃調配整備的所在地。作戰層級的資料融合中心包含敵人的指管節點，以及情監偵處理、運用與分發節點。網路阻絕可摧毀、削弱或癱瘓這些資料調配整備場，進而限制敵人調整與集中在時間與/或空間中的效應，而達到抑制敵人作戰效能的目的。儘管敵人有能力採行偽裝、掩蔽與欺敵措施，以挫敗動能攻擊，但資料融合中心必須在某種程度上宣告其於網際空間內的位置(例如IP位址)，以利接收及分送資訊。資料融合中心勢必很容易遭受網路攻擊，因為其用途主要取決於其連結性(connectivity)──一個網路的功能隨著其使用者數量之增加而大幅增強。[34] 如果這些節點並未廣泛連結，則將與敵人的作戰行動無關，故可予以忽視。削弱敵人的資料融合能力，將在作戰層級產生更大的不確定性，迫使敵人更依賴其於戰術層級的調適能力。而敵人於戰術層級的調適能力又取決於其戰術網路與通信/資料鏈路的效能。因此，於作戰層級的網路阻絕可擴大於戰術層級運用網路阻絕與電子攻擊，以破壞資料鏈路所產生的效應與影響。

敵人的戰術資料鏈路網是僅次於資料融合中心的重要網路阻絕目標。於戰術層級，戰術網路上的各節點(例如戰機、排、驅逐艦)都具有某種程度的資料融合能力，因此資訊過度集中的情形十分罕見，故攻擊網際空間內的這些節點，並不會產生廣泛效應。然而，戰術資料通常很快就失效，故即便資料鏈路網只遭到短暫的破壞，都可能嚴重危害各戰術單位在資料仍可作為決策的有效依據之前，取得所需資訊的能力。因此，於戰術層級，網路阻絕的適當目標在於破壞戰術網路資料鏈路，而不在於癱瘓節點。中斷這些鏈路的運作可在敵人決策週期內造成短暫但有意義的遲滯效應與誤判，從而創造或擴大我方「先發現、先射擊、先擊殺」(first look-first shot-first kill)的戰術優勢。於作戰與戰術層級，使軍事網權聚焦於獲取並維持網路優勢及遂行網路阻絕，則聯合部隊將能發揮最大戰力，並獲得敵人難以克服的重大決策優勢。

在聯合作戰中，能從網路優勢及對敵資料融合中心與戰術資料鏈路進行網路阻絕中獲得最大助益者，非空中戰役莫屬。雖然網權也可支援陸上與海上作戰，但在聯合作戰中，空中戰役通常扮演打頭陣的角色。從第二次世界大戰開始，空權已成為美國軍事作戰的先鋒，不論戰事發生在海上或陸上。此外，現代空軍在遂行首見於1991年波灣戰爭中的平行作戰

(parallel warfare，譯註：指同時對敵展開戰略、戰術與作戰層級作戰，以癱瘓其戰力)時，將至為依賴運用網權以獲得狀況覺知及從事通信與偵察。再者，敵人的防空雷達必須借助於資料融合能力，方可使匿蹤戰機無所遁形。網權把「已整合」的能力置入統合防空作戰中。敵人可運用網權使其防空作戰達到偵攻一體的程度，以減少其空域所存在的弱點。然而，缺乏資料網路將多重偵測器結合起來，則面對空飛彈陣地將成為一對一接戰模式中的個別防衛者，自1991年以來，匿蹤戰機顯然能充分宰制這種狀況。運用網路阻絕以支援空軍，將可大幅降低在戰爭伊始敵防空武力威脅最強大之際，空軍部隊穿越敵防空網所面臨的危險。在沒有網路優勢的情形下，空中作戰是要付出重大代價的。前次美國空權在欠缺網路優勢下與敵防空兵力交手是在第二次世界大戰期間，當時美國空勤人員的存活率比在太平洋作戰的陸戰隊員還低。[35] 此外，空中作戰的展開速度遠比陸上或海上作戰來得快。地面部隊的運動速率每小時數十哩，相較之下，空中部隊達到每小時數百哩。陸上與海上部隊——像極了

註釋

1. Daniel T. Kuehl, "From Cyberspace to Cyber Power: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry Wentz (Washington, DC: NDU Press/Potomac Books, Inc., 2009); Joint Publication (JP) 1-02, *DOD Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, November 8, 2010, as amended through October 15, 2011), 92.
2. Lee Kennett, *The First Air War: 1914-1918* (New York: The Free Press, 1991), 220.
3. Mandiant, *APT 1: Exposing One of China's Cyber Espionage Units*, available at <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>.
4. JP 1-02, 16.
5. John C. Slessor, *Air Power and Armies* (Tuscaloosa: The University of Alabama Press, 2009), 16-17.
6. David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd ed., rev. (Washington, DC: DOD C4ISR Cooperative Research Program, 1999), 32.
7. Slessor, 122-123.
8. Thomas E. Griffith, Jr., *MacArthur's Airman: General George C. Kenney and the War in the Southwest Pacific* (Lawrence: University of Kansas Press, 1998), 244-246.
9. U.S. Department of State, "Background Note: Georgia," available at <www.state.gov/outofdate/bgn/georgia/index.htm>.
10. Ibid.
11. Eneken Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified* (Tallin, Estonia: Cooperative Cyber Defense Centre of Excellence, 2008), 5; Kertu Ruus, "Cyber War I: Estonia Attacked from Russia," *European Affairs* 9, no. 1-2 (Winter/Spring 2008), available at <www.europeaninstitute.org/Winter/Spring-2008/cyber-war-i-estonia-attacked-from-russia.html>.
12. Tikk et al., 6.
13. Ben Arnoldy, "Cyberspace: New Frontier in Conflicts," *The Christian Science Monitor*, August 13, 2008, available at <www.csmonitor.com/USA/Military/2008/0813/p01s05-usmi.htm>.
14. Ibid.
15. Tikk et al., 6.
16. David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, January 6, 2011, 1, available

第一次世界大戰時的步兵，因行動過於緩慢，而無法將突破變成突圍──很可能因為行動太緩慢而無法像空中部隊那麼有效地運用由網路阻絕所創造、稍縱即逝的優勢。

結語

網權在聯合作戰中至關重要。軍事網際空間作戰的優先目標應在於獲取並維持網路優勢及遂行網路阻絕，以支援聚焦於空中戰役的動能作戰。此外，獲取並維持網路優勢的作戰應聚焦於癱瘓敵網路攻擊與網路偵察能力，進而制壓敵網路防衛。網路阻絕行動應聚焦於攻擊功能相當於鐵路調車場的資料融合中心及戰術資料鏈路。在聯合作戰中結合網際空間優勢與網路阻絕行動，將可產生重大的決策優勢，其累積效應可迫使敵人犯錯而終致潰不成軍。

作者簡介

E. Lincoln Bonner III中校係科羅拉多州美空軍太空作戰中隊航太資料設施作業主任。

Reprint from *Joint Force Quarterly* with permission.

at <www.smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf>.
17. Ibid.
18. John Bumgarner and Scott Borg, "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008," in *Cyberwar Resources Guide*, Item #138, 2-3, available at <www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf>.
19. Ibid.
20. Ibid., 4-5.
21. Ibid., 5.
22. Ibid.
23. Georgian Research and Educational Networking Association, available at <www.grena.ge/eng/cert.html>; Tikk et al., 14-15.
24. Greg Keizer, "Russian Hacker 'Militia' Mobilizes to Attack Georgia," *NetworkWorld.com*, August 13, 2008, available at <www.networkworld.com/news/2008/081208-russian-hacker-militia-mobilizes-to.html>; Tikk et al., 12.
25. Bumgarner and Borg, 7.
26. Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters* 38, no. 4 (2008), 66-67.
27. Bumgarner and Borg, 7.
28. Ibid., 7.
29. Ibid., 4.
30. John Oltsik, "Russian Cyber Attack on Georgia: Lessons Learned?" *NetworkWorld.com*, August 9, 2009, available at <www.networkworld.com/community/node/44448>; Bumgarner and Borg, 2.
31. Joseph Menn, "Expert: Cyber-attacks on Georgia Web sites Tied to Mob, Russian Government," *Los Angeles Times*, August 13, 2008, available at <http://latimesblogs.latimes.com/technology/2008/08/experts-debate.html>.
32. Tikk et al., 6.
33. Slessor, 31.
34. Carl Shapiro and Hal R. Varian, *Information Rules: A Strategic Guide to the Network Economy* (Cambridge: Harvard Business School Press, 1999), 184.
35. W. Murray and A. R. Millett, quoted in Paul Kennedy, *Engineers of Victory: The Problem Solvers Who Turned the Tide in the Second World War* (New York: Random House, 2013), 142.