21世紀聯合作戰的網路力量
Cyber Power in 21st-Century Joint Warfare

譯者簡介

鄧炘傑備役少校，管院專9期、國防大學政治作戰學院英文正規班、中原大學企管研究所碩士；曾任排長、連長、地區補給庫分庫長、教準部編譯官，現任特約翻譯、華語／英語專業領隊／導遊。

In 2008, Russian military forces, supported by cyber attacks, rapidly defeated opposing Georgian forces and seized territory later traded in exchange for Georgia's granting greater autonomy to pro-Russian governments in South Ossetia and Abkhazia. Cyber power is the ability to exploit cyberspace to create advantages and influence events, and cyberspace is the interdependent and interconnected networks of electronics and the electromagnetic spectrum where information is created, stored, modified, exchanged, and exploited.[1]The 2008 Russia-Georgia war marks the only public incidence of cyber power integrated with traditional kinetic military operations. To date, however, little attention has been paid regarding how to integrate cyber power into conventional military operations. Rather, research has tended to focus on the independent use of cyber power for espionage and as a means of strategic attack to punish and/or compel a state to do one's will.

2008年，俄軍在網路攻擊支援下，迅速擊敗敵對的喬治亞部隊，並占領其領土；之後喬治亞予親俄的南奧賽提亞和阿布哈茲政府更大的自治權。網路力量是指運用網路空間，創造優勢與影響的能力；而網路空間則是指可以創造、儲存、修改、交換與運用資訊，彼此互通、互連的電子與電磁頻譜網路。[1]2008年俄羅斯－喬治亞戰爭，即是網路

1　於下頁。

力量與傳統軍事作戰僅有的整合案例。然直至今日如何將網路力量納入傳統軍事作戰仍未受到重視；反而研究比較著重於將網路力量用於間諜活動之中，以及作為戰略攻擊的手段，以懲罰或迫使其他國家屈服其意志。

This article addresses this research gap by focusing on how cyber power can best be integrated into joint warfare to fight and win the Nation's wars. Using the Russia-Georgia war as an illustrative case, this article argues that the principal value of integrating cyber power into a joint military campaign is that it compels the enemy to make mistakes by performing three main warfighting tasks: reconnaissance, superiority, and interdiction. It begins with a description of how cyber power's main warfighting tasks support kinetic operations by degrading/disrupting the enemy decision cycle. The cyber aspects of the Russia-Georgia war are then analyzed to show how pro-Russian forces employed cyber power to degrade the Georgian decision cycle in support of kinetic military operations. Finally, implications for present and future integration of cyber power into joint warfare are discussed.

本文指出這方面研究的不足並如何將網路力量有效融入聯合作戰，來打贏國家層級的戰爭。以俄羅斯－喬治亞戰爭為例，本文認為將網路力量與聯戰戰役整合的主要價值，是網路力量將迫使敵人在「偵察、優勢及阻絕」三項主要作戰任務犯下錯誤。論述首先闡明網路力量如何藉由抑制或打亂敵人的決策圈支援軍事作戰。然後分析俄羅斯－喬治亞戰爭的網路交鋒發現，親俄軍的部隊運用網路力量，降低喬治亞部隊決策效能，以致無法充分支援其軍事作戰。最後則討論目前及未來將網路力量納入聯合作戰之議題。

Reconnaissance, Superiority, and Interdiction
偵察、優勢及阻絕

Cyber power has evolved similarly to early airpower and will likely make contributions to joint warfare now and into the foreseeable future, namely to conduct cyber reconnaissance, gain and maintain cyber superiority, and conduct cyber interdiction.

網路力量與早先的空中武力相同，對當前及可預知的未來聯合作戰有所貢獻，就是執行網路偵察、獲得與確保網路優勢以及實施網路阻絕。

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.

In World War I, the advantages of aerial reconnaissance gave birth to the battle for air superiority. Aerial reconnaissance "warned of any movement or change in the enemy camp, and with few exceptions it foretold the enemy's offensive and helped guarantee that it would fail."[2] As a result, the requirement emerged to gain and maintain air superiority, thereby securing the information advantage flowing from aerial observation. Despite its value to effective land operations, aerial reconnaissance could not directly degrade or defeat enemy operations.

第一次世界大戰，空中偵察之利益催生了爭取空優之戰鬥。空中偵察「警報敵營任何行動或改變，預先警示敵方攻勢，確保作戰勝利」。[2]結果是產生獲得與保持空中優勢的需求，而確保資訊優勢的手段，就從空中觀測開始。空中偵察雖對地面作戰極具價值，卻無法直接削弱或瓦解敵方的作戰。

In the same manner, cyber power's military development can trace its roots to reconnaissance. As the recent Mandiant report about Chinese cyber espionage highlights, much of the impetus to develop cyber power arises from the advantage that accrues to the side that can conduct more effective cyber reconnaissance operations.[3] In turn, effective cyber reconnaissance and the information advantage that comes with it depend on possessing at least a degree of cyber superiority. Like airpower, cyber reconnaissance and cyber superiority can make friendly operations more effective, but they cannot directly degrade or defeat enemy operations.

同樣的，網路力量在軍事方面的發展，追溯其源頭是偵察。近期Mandiant公司對中國網路間諜報告特別強調，發展網路力量的原動力，大多是因為執行越多有效的網路偵察行動之一方，就越能累積作戰優勢。[3]換言之，有效的網路偵察與資訊優勢，是視掌握住至少某種程度的網路優勢而定。就像空權，網路偵察與網路優勢可以讓友軍行動更有效率，但卻無法直接削弱或擊敗敵方的作戰。

In 1936, 18 years after World War I ended, Sir John Slessor of the Royal Air Force described how airpower could be integrated with land operations to directly and substantially degrade or defeat an adversary's warfighting capability in airpower and armies. Using evidence from British military operations in the Middle East, Slessor deduced that in addition to aerial reconnaissance, airpower's main warfighting tasks in a joint air-land campaign were to gain

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〉.

and maintain air superiority and to interdict enemy land lines of communication and supply. Air superiority continues to provide friendly forces with the ability to exploit airpower for reconnaissance, mobility, and attack without prohibitive enemy interference.[4] Air interdiction destroys or interrupts those elements of an enemy's system of supply or communication for a sufficient time that the degradation will immediately or in due course prove fatal to his continuance of effective operations.[5]

1936年，第一次世界大戰結束後18年，英國空軍施雷瑟(John Slessor)爵士描述了如何整合空中武力與地面作戰行動，以直接、實質的手段削弱或挫敗敵人空中武力與陸軍戰鬥能力。舉英軍在中東的軍事作戰為例，施雷瑟爵士推論除空中偵察外，空中武力在地空聯合戰役的主要任務是獲取並維持空中優勢，切斷敵人地面的通訊軸線和補給路線。空中優勢有利於友軍空權在不受敵軍干擾下執行偵察、機動與攻擊[4]。空中阻絕可摧毀或阻滯敵人補給或通訊體系，而使我軍有充足時間可立即或採取連續而有效的致命行動[5]。

Cyber superiority and cyber interdiction can also be described in terms akin to air superiority and air interdiction. Cyber superiority provides friendly forces with the ability to exploit cyber power for reconnaissance, communication (that is, information mobility), and attack-in addition to orientation (that is, information/ computer processing) and command and control-without prohibitive interference by the enemy. Cyber interdiction interrupts, destroys, or otherwise neutralizes electronic information lines of communication and electronic information systems of supply (that is, cyberspace) used by enemy land, sea, air, and space forces for a sufficient length of time that they will immediately or in due course prove fatal to his continuance of effective operations. Unlike today, World War II bombers lacked the precision attack capability to substitute for the lethality of land forces to destroy an enemy army. Hence airpower's primary offensive contribution was air interdiction. Like air interdiction in Slessor's time, cyber interdiction is the principal contribution of cyber attack operations in joint warfare today.

網路優勢與網路阻絕，也可以描述近似空中優勢及空中阻絕。網路優勢提供友軍有能力運用空中力量來偵察、通信(即資訊機動)和攻擊－除了定位(亦即資訊運算)和指揮與管制外－不遭致敵之阻礙。網路阻絕可干擾、摧毀，或制壓敵人用於陸、海、空及太空通訊的電子資訊線路，及備援的電子資訊系統(亦即網路空間)，使我軍有充裕時間可立即或採取連續而有效的致命行動。第二次世界大戰時轟炸機缺乏精準攻擊能力，無法

4 JP 1-02, 16.

5 John C. Slessor, Air Power and Armies (Tuscaloosa: The University of Alabama Press, 2009), P16, 17.

致命性摧毀敵地面部隊。因此，空中武力主要的攻擊貢獻是空中阻絕。如同施雷瑟爵士那個時代的空中阻絕，網路阻絕是今日聯合作戰中網路攻擊作戰的主要貢獻。

In the air and cyberspace domains, offensive operations to destroy or neutralize the adversary's air and cyber forces are the primary means of establishing superiority within each domain. Cyber reconnaissance, however, plays a much greater role in gaining cyber superiority than aerial reconnaissance plays in establishing air superiority. At the tactical level in cyberspace, the speeds of action and of observation both approach the speed of light. In other words, cyber defenders do not have the benefit of the warning time that observation at the speed of light via radar gives air defenders. Consequently, tactical defenses are unlikely to have sufficient warning to react against a cyber attack and prevent significant negative effects. Tactical defense in cyberspace is more akin to battle damage repair, recovery, and reconstitution than to any analogous effort to parry a physical blow. Effectively defeating cyber attacks thus largely depends on fielding a set of defensive measures that one knows in advance an adversary cannot overcome. That is, the most effective way to achieve cyber superiority is to field cyber defense and cyber attack capabilities that render potential corresponding enemy cyber attacks and defenses impotent a priori.

在空中和網路空間領域，以攻勢作戰摧毀或制壓敵方空中或網路武力，是在其每一領域建立優勢的主要手段。然網路偵察在獲取網路優勢所扮演的角色比空中偵察獲取空優的角色重要。在網路空間的戰術階層，行動與觀測的速度猶如光速；換言之，網路防禦者不會有充裕預警時間的好處，如空中防禦者透過快如光速的雷達來觀測。結果是，戰術防禦不太可能有充分預警來反制網路攻擊，及防範重大的的負面效應。在網路空間的戰術防禦，比較類似於戰損修復、恢復與重建而非致力避開實體損壞。要有效擊敗網路攻擊極有賴於建置一套早期預警及敵人無法壓制的防禦措施。也就是說，達成網路優勢的最有效方式，是建立好網路防禦及網路攻擊能力，以因應敵人潛在的網路攻擊和防禦網路弱點。

The critical requirement for neutering potential enemy cyber attacks and defenses without known precedents, and thus the key to cyber superiority, is technical intelligence about enemy cyber attack and defense capabilities, as well as tactics, techniques, and procedures. Although all-source intelligence contributes to developing this foreknowledge, the principal way of gathering the requisite intelligence is cyber reconnaissance. Unlike orders of battle, cyber capabilities only exist in cyberspace and cannot be observed except from within cyberspace. Thus, those who win the cyber reconnaissance competition in peacetime will likely win the battle for cyber superiority in wartime.

制壓敵人潛在的網路攻擊，防範於未然，是為獲得網路優勢之要件，也就是掌握敵人網路攻擊、防禦能力，以及戰術、技術及程序等技術情報。雖然多重情資對於發展預

知能力有所貢獻，但蒐集必要情資的最主要方式還是網路偵察。不同於其他的作戰，網路能力僅存在於網路空間，只有在網路空間才能觀測到這種能力。因此，平時能在網路偵察勝過對手，戰時就能在網路優勢勝出。

To gain and maintain cyber superiority, peacetime cyber reconnaissance operations should prioritize intelligence about enemy cyber reconnaissance and attack capabilities (for example, enemy malicious code development), followed by enemy cyber defense capabilities. With intelligence about these activities, one can develop and field cyber defenses that negate adversary cyber attacks prior to their use as well as develop cyber attack capabilities impervious to enemy cyber defenses. Possessing cyber attack capabilities that are relatively impervious to anticipated defenses is a critical requirement for cyber interdiction. The kinetic corollary to this set of cyber reconnaissance activities might be more commonly described as intelligence preparation of the battlespace. Therefore, it is during the intelligence preparation of cyberspace, which should be constantly ongoing during peacetime, when cyber superiority is won or lost.

想獲取或保持網路優勢，平時網路偵察作戰，應優先於掌握敵人的網路偵察與攻擊能力情資(如敵人惡意程式碼的發展)，緊接著是敵人的網路防禦能力。有了這些情資，我們便可在敵人使用網路攻擊前，發展或建構網路防禦能力；或發展網路攻擊能力，以突破敵之網路防禦。對網路阻絕而言，擁有網路攻擊能力較純粹之防禦更為重要。就戰場情報整備而言，網路偵察活動引起更多重視。因此，在網路空間的情報整備期間，不論有無網路優勢，在平時都必須持恆進行。

Cyber interdiction is made possible by, and complements, cyber superiority. Interdiction in general is a network warfare concept applicable to any domain. An electronic information network is simply a transportation network, but rather than physical supplies, information is the commodity. The objective of any transportation network is to deliver accurate, relevant, and timely supplies (that is, the right stuff to the right place at the right time)-or information in the case of cyberspace.[6] Regardless of whether an interdiction campaign chooses to target a network's capability to deliver supplies with accuracy, relevancy, or timeliness, the objective is the same: to introduce friction and uncertainty into the decision cycle so it becomes increasingly difficult for the enemy to conduct effective operations in comparison to friendly forces. Interdiction is not about the impact of any one attack on an enemy network, but rather the cumulative effects of a stoppage.[7]

網路阻絕倚賴網路優勢，並與網路優勢相輔相成。阻絕通常是一種網狀作戰概念，適用於任何領域。電子資訊網路只不過是一種運輸網路，但不是實體運補，資訊才是其

6、7 於下頁。

載體。所有運輸網路的目標是準確、適切、即時的遞送物資(就是將對的貨物在對的時間送到對的地點) ── 在這裡是網路空間的資訊。[6]只要選定阻絕戰役的目標，不論其傳送如何準確、適切、即時，其目標是相同的：將阻礙與不確定性導入決策迴圈，以增加敵對友軍遂行有效作戰的困難度。阻絕無關攻擊敵網路的影響，而是阻滯的累積效能。[7]

A successful interdiction campaign accounts for a network's capacity-how much (flow volume) and how fast (flow rate) supplies can travel through the network to meet user demand. In air interdiction campaigns, air attacks and land operations complement each other to overwhelm the enemy's supply network. Air attacks destroy, disrupt, or degrade nodes and links in the enemy's land transportation/supply network (for example, rail and roads), reducing its capacity. Simultaneously, land combat operations create demand for a high volume of supplies to flow through the network at a high rate. Land combat operations place timeliness requirements on an enemy's supply network that air interdiction prevents the network from meeting. For example, when combat was at a fever pitch in the phase of the Korean War spanning the Inchon Landing to China's entry, both sides consumed supplies voraciously, demanding a high volume and a high rate flow from their respective networks.

成功的阻絕戰役，在於要計算網路的負載量 ── 多少(流量)和多快(流速)的資訊流通速率才滿足用戶需求。在空中阻絕戰役中，空中攻擊與地面行動作戰相互配合，以瓦解敵人的補給網路。空中攻擊能摧毀、干擾或削弱敵人地面運輸／補給網路的節點與連結(如鐵路與公路)，以降低其能力。同時，地面戰鬥要求以更大流量運送更多的補給品。地面戰鬥敵人要求補給網路須及時運補，空中阻絕行動則阻滯其達成。例如韓戰時美軍在仁川登陸對付中共參戰的白熱化階段，雙方補給品消耗快速，都要求各自的補給網路能大量快速運補。

However, the North Korean army had to rely on a low capacity rail and road network to meet its tremendous needs. American air interdiction ensured that North Korean forces could never accumulate enough supplies or resources in sufficient time to mount a successful counterattack, and U.S. forces rapidly moved north to the Yalu River. At precisely the time when the enemy needs the most from its supply network, interdiction makes it capable of providing the least.

然而，北韓軍隊必須仰賴運能很低的鐵路及公路網，以滿足其大量需求；美軍的空中阻絕，從未讓北韓軍隊有足夠時間獲得足夠補給或物資以發動反擊，這讓美軍能快速

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 C[4]ISR Cooperative Research Program, 1999), 32.

7 Slessor, 122, 123.

向北移動到鴨綠江。當敵人必須適時從補給網獲得物資時，阻絕將讓敵人期望落空。

A cyber interdiction campaign- where cyber interdiction is the destruction, disruption, or degradation of nodes, links, and data in an enemy information network to interrupt it and reduce its capacity-functions similarly to an air interdiction campaign, with one critical exception. Unlike air interdiction, cyber interdiction can make portions of cyberspace inaccessible for other operations such as reconnaissance. Air attacks do not prevent the use of the air domain for mobility and reconnaissance. Because cyberspace is composed of information networks, cyber interdiction, which by definition will disrupt enemy information networks, will probably hinder the ability of cyber reconnaissance to gather intelligence data from targeted networks. As a result, tension exists between cyber interdiction and cyber reconnaissance.

網路阻絕戰役－如果網路阻絕用於摧毀、干擾或破壞敵人資訊網路中的節點、連結與資料，以阻滯或削弱其能力－其功用就類似於空中阻絕戰役，但有一很大的不同。不像空中阻絕，網路阻絕會讓網路空間部分資源無法再去執行其他工作，如偵察。空中攻擊不會阻止空域用來機動和偵察。因為網路空間是由資訊網路構成，網路阻絕顧名思義是阻斷敵人的資訊網路，但也可能會妨礙網路偵察對目標網路的蒐集情資能力。結果就是網路阻絕和網路偵察間處於緊張狀態。

If one anticipates a long conflict, or if use of a specific cyber attack in one conflict would significantly decrease one's cyber advantage in more vital potential contingencies, one should favor the decision advantage created by cyber reconnaissance over cyber interdiction. For example, the United States in World War II, in what it anticipated to be a long conflict, protected the information advantage it gained from breaking German and Japanese encryption rather than taking actions that might compromise this invaluable intelligence source. This critical intelligence advantage allowed U.S. forces to decimate Japanese convoys as well as choose the time and place of battle in a war that lasted more than 3 years.[8] Commanders going forward must weigh the costs and benefits of sacrificing intelligence gained from cyber reconnaissance over the long term against the effects created by cyber interdiction in the near term.

假如預期是一場長期衝突，或是在一場衝突中使用特定的網路攻擊手段，重大的潛在意外將會明顯抵銷其網路優勢，網路偵察應比網路阻絕更有利於決策優勢。以美國在第二次世界大戰為例，因預期會是一場長期衝突，保護破解德國及日本的密碼情報所獲

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.

之資訊利益，將比採取冒險行動而危及情報資源來得好。此關鍵情報優勢，使得美軍得以超過3年於預想殲敵區殲滅日本護衛艦隊。[8]各級指揮官必須在犧牲長期網路偵察所獲的情報，或短期網路阻絕所得效益間權衡其價值和利益。

Cyber interdiction compels an enemy to make a mistake. Like the complementary relationship between air interdiction and land operations, high intensity kinetic operations create information demands that can overwhelm an information network whose useful capacity has been reduced by cyber interdiction. To limit the effects of cyber interdiction, an opponent could concentrate his information supplies, which would place them at greater risk for destruction from cyber or kinetic attack. Additionally, cyber attacks that alter, reroute, or delay data present a choice to an opponent. If a cyber attack alters or reroutes an enemy's data, he can act on the information he has, increasing the likelihood that he will make a mistake, or submit additional requests in an attempt to acquire the missing data, thus reducing his network's useful capacity and hindering timely information development. If he chooses the latter, he will compound the effects of cyber attacks that add extraneous data into the network, further impeding timely information development and potentially depriving him of new information altogether. Cyber interdiction thus compromises an enemy's decision cycle by placing him on the horns of a dilemma. Should he yield superiority in decision speed or yield superiority in decision quality? Either way the cumulative effect of yielding decision superiority over time will inevitably lead to mistakes.

網路阻絕會迫使敵人犯下錯誤。高強度的地面作戰會創造資訊需求，網路阻絕可降低敵使用容量，其資訊需求將使整個資訊網路當機。為拘束網路阻絕效應，敵可集中資訊容量，但可能讓他們陷入網路毀滅或實體攻擊的更大危險。此外，網路攻擊可選擇讓敵人接收資料被竄改、繞道或延遲。假如網路攻擊改變敵人的接收資料或接收路徑，敵人會依手中已有的資訊採取行動，增加犯錯可能性；或提出額外要求試圖找回散失的資料，因此降低網路的可使用容量，有礙即時資訊的掌控。假如敵人選擇資訊延遲，將因增加額外資料進入網路而使網路攻擊複合化，更進一步防礙即時資訊的掌握，可能使其喪失整合新資訊之能力。網路阻絕因而危及敵人的決策程序，使其陷入兩難困境。此時究應考量決策速度或是決策品質？不論是哪一種，決策結果都因為錯過最佳時機，而無法避免導致錯誤。

Cyber Power in the 2008 Russia-Georgia War
2008年俄羅斯－喬治亞戰爭中的網路力量

The 2008 Russia-Georgia war helped focus attention on cyber power and its utility in war in a way that previous cyber power uses had not. That conflict's high profile caused it to become

the subject of much study, so it is a rich source of information for analyzing the dynamics of cyber power in a joint military campaig.

2008年的俄羅斯－喬治亞戰爭，引起聚焦網路戰力在戰爭中運用的關注。這場衝突的獨特性引起很多研究，因它有豐富訊息可用來分析聯合軍事戰役中網路戰力的效能。

Following Georgian independence in 1991, secessionists seeking to remain part of Russia seized control of the majority of Abkhazia and portions of South Ossetia before cease-fire agreements were reached in 1992 and 1994.[9] These conflicts remained unresolved and formed the roots for the 5-day war between Russia and Georgia in 2008.[10]

1991年喬治亞獨立後，主張續留在俄羅斯的分離主義者，在1992和1994年兩次停火協議前，已控制了阿布哈茲大部分地區和南奧賽提亞部分地區。[9]這些衝突的擱置未決，成為2008年俄羅斯與喬治亞5日戰爭的導火線。[10]

On the surface, cyber power would not appear to be particularly useful in a war with Georgia. Only 7 percent of the citizens used the Internet daily,[11] which might cause one to overlook Georgia's critical cyber vulnerability-more than half of 13 connections to the outside world via the Internet passed through Russia, and most of the Internet traffic to Web sites within Georgia was routed through Turkish or Azerbaijani Internet service providers, many of which were in turn routed through Russia.[12] Georgia's Internet infrastructure suffered from a dearth of internal connections known as Internet exchange points.[13] Consequently, a Georgian user's request for a Georgian Web site would likely be routed through Russia, analogous to having to travel through Mexico to get from Los Angeles to San Francisco.[14] As a result, pro-Russian forces could employ cyber power to affect a large percentage of Georgia's access to, and use of,

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-attackedfrom-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/p01s05usmi.htm〉.

14 Ibid.

the portion of cyberspace known as the Internet. Lacking control of the infrastructure required for external or internal Internet use, Georgia could neither disperse network traffic nor cut Internet connectivity from abroad as defensive measures without ceding the cyber advantages of Internet access if the state came under cyber attack.[15]

表面上，這場戰爭網路力量對喬治亞並無顯著影響。每日僅有7%人民使用網際網路，[11]這會讓人誤以為喬治亞網路的脆弱性並不嚴重 ── 但是喬治亞與外界聯繫的13條網際路線，有一半以上是透過俄羅斯，而喬治亞境內大部分網站的網際網路流量，都經過土耳其和亞塞拜然的網路服務供應商；其中許多網路會經過俄羅斯。[12]喬治亞的網際網路基礎設施，苦於境內連結過少，就是一般所謂的網路交換節點不夠。[13]結果是喬治亞的網路使用者要在境內使用網站，必須繞道由俄羅斯連線。好比洛杉磯人去舊金山，還得繞道墨西哥一樣。[14]如此親俄羅斯的部隊，就可以運用網路力量去影響喬治亞網際網路空間的大部分存取和使用。因為在基礎設施方面無法有效掌控國內外的使用，喬治亞不是分散網路流量，就是乾脆切斷從外國連接進來的網路，作為一種防禦手段；這樣即使遭到網路攻擊，也不致因為被敵方全盤掌握網路優勢而遭受太大損失。[15]

The Russia-Georgia war officially started on August 7, 2008, after Georgian military forces responded to alleged Russian provocation with a massive artillery barrage on the town of Tskhinvali in South Ossetia.[16] Moscow seized the opportunity to further solidify South Ossetia's and Abkhazia's independence from Georgia. It immediately deployed troops to South Ossetia and initiated aerial bombing raids on Georgian territory. It also deployed its navy to blockade the Georgian coast and landed marines on the coast of Abkhazia. After Russian mechanized forces and South Ossetian militia defeated the lightly armed Georgian military around Tskhinvali, they invaded Georgian territory uncontested.[17] Georgia was not able to offer even a modicum of additional resistance because of the advantage cyber power created for the Russian forces.[18]

俄羅斯－喬治亞戰爭公認肇始於2008年8月7日，之後喬治亞軍隊對位於南奧賽提亞

15 Tikk et al., 6.

16 David Hollis, "Cyberwar Case Study: Georgia 2008," Small Wars Journal, January 6, 2011, 1, available 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-CyberCampaign-Overview.pdf〉.

的塔斯金村(Tskhinvali)遭俄羅斯大規模的砲擊展開反擊，宣告正式開始。[16]莫斯科以此為契機，進一步強調南奧賽提亞和阿布哈茲應從喬治亞獨立出來。俄羅斯立即調派部隊到南奧賽提亞，並開始對喬治亞領土實施空中轟炸；同時俄羅斯也部署海軍封鎖喬治亞海岸，並派遣陸戰隊登陸阿布哈茲。在俄羅斯機械化部隊和南奧賽提亞民兵，於塔斯金村擊敗輕裝的喬治亞部隊後，他們明目張膽入侵喬治亞領土。[17]喬治亞完全沒有抵抗能力，因為網路優勢完全被俄軍部隊壟斷。[18]

The concentration and advanced preparation of cyber attacks in the war suggest that cyber superiority and cyber interdiction operations against Georgia were the product of cyber reconnaissance and intelligence preparation of cyberspace well in advance of the conflict. The cyber interdiction campaign against Georgia included both Web site precise in scope and concentration, never exceeding 11 targets, and the same Web sites continued to be attacked throughout the war.[19] Most of the cyber attacks were customized for Georgian targets with at least one Web site defacement prepared more than 2 years prior to the conflict.[20] The cyber attacks were also sophisticated in their targeting. Government and news media Web sites were struck first, helping sow confusion by hindering Georgians and their officials from determining what was actually happening and delaying any international response. In addition to Georgia's two major banks, cyber attacks targeted commercial entities that could have been used to communicate or help coordinate a response to Russian forces writ large and the cyber attack specifically.[21] The concentration of botnet cyber attacks on 11 targets, the years-long cyber attack development, and the sophisticated appreciation of how Georgia would likely use the Internet to operationally respond all indicate that the cyber superiority the pro-Russian cyber forces held over Georgia was the product of excellent pre-conflict cyber reconnaissance and intelligence preparation of cyberspace.

這場戰爭中網路攻擊的集中與先期準備，俄羅斯針對喬治亞的網路優勢與網路阻絕作戰，在衝突發生之前就已展開網路偵察與網路空間情報準備。針對喬治亞的網路阻絕作戰，包含精準掌握網站範圍和集中程度都不超過這11個目標，亙戰爭全期持續對這些網站實施攻擊。[19]大部分的網路攻擊都是專以喬治亞為目標，早在戰爭發生兩年前，至少將一個網站外貌加以變造。[20]網路攻擊時對目標的設定煞費苦心，首先是癱瘓政府和新聞媒體的網站，製造混亂，阻擾喬治亞人民和政府官員無法正確判斷情勢，並遲滯國際的任何反應。除喬治亞的兩家主要銀行外，網路攻擊鎖定用來溝通的商業實體或幫助

19 Ibid.

20 Ibid., 4-5.

21 Ibid., 5.

協調的機構，俄軍都特別將其列為網路攻擊目標。[21]針對11個目標的網路殭屍攻擊，是經過數年的網路攻擊整備，以及精確評估喬治亞會如何使用網際網路回應的跡證，這些在衝突前卓越的網路偵察和網際網路空間情報準備等，使俄羅斯網軍的網路優勢足以宰制喬治亞。

To assert cyber superiority, pro Russian cyber forces suppressed Georgia's cyber defenses through diversion and direct attack. Educational institutions devoted to science, technology, and medicine were among the initial 11 botnet cyber targets struck.[22] At the time, Computer Emergency Response Team Georgia (CERT Georgia) was chartered solely to provide cyber security for higher education institutions within the Georgian Research and Educational Networking Association (GRENA).[23] By attacking educational institutions, cyber attackers focused CERT Georgia on its charter mission of protecting GRENA's cyberspace and away from responding to the larger national crisis. By attacking what the opponent must succor-the GRENA-pro-Russian cyber forces used CERT Georgia's natural response against it to divert and suppress the state's best cyber defenses. Also, a popular Georgian Internet hacker forum was among the initial 11 cyber attack targets, impeding some of Georgia's more capable cyber experts from coordinating an organized response.[24] Pro-Russian forces achieved cyber superiority using the method Slessor described to gain command of the air-through disruption, dislocation, and disorganization of the opposing force.

維護網路優勢，親俄羅斯網軍藉由牽制和直接攻擊壓制喬治亞的網路防禦，喬治亞之科學、技術和醫療等教育機構，被列入殭屍網路首波攻擊的11個目標。[22]當時，喬治亞電腦緊急應變小組(CERT)是唯一專責維護喬治亞研究與教育網路協會(GRENA)內，高階教育機構的網路安全。[23]俄羅斯對喬治亞教育機構採取的攻擊，聚焦於CERT保護GRENA網路空間所負的任務，目的是要讓喬治亞的CERT無法對國內大規模網路危機做出即時反應。GRENA是CERT必須保護的首要目標，親俄羅斯網軍就利用這種關係，來箝制和壓制喬治亞防護最好的機構，而且將著名的喬治亞網路駭客論壇也列在首波11個攻擊目標中，讓喬治亞的網路專家們，無法協調出有組織的反擊作為。[24]親俄軍隊所達成的網路優勢是使用施雷瑟爵士制空的概念，透過分裂、混亂與瓦解反抗武

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/2008/081208russian-hacker-militia-mobilizes-to.html〉; Tikk et al., 12.

力。

Pro-Russian cyber power maintained cyber superiority throughout the conflict, and as a result Georgia never mounted a successful cyber defense or cyber counterattack. For example, Georgia attempted to maneuver around the cyber atacks by filtering them out based on their origin (that is, their originating Internet protocol [IP] address). However, the cyber attackers' intelligence preparation allowed them to easily defeat this tactic. Cyber attackers routed their assault through foreign servers to mask their real IP addresses and created false IP addresses to spoof Georgia's cyber defense filters.[25] Still, Georgia preserved the use of some government Web sites by moving them to U.S.-based servers.[26] Despite the failure of Georgia's cyber defense, it did attempt at least one major counterattack, but it also failed. Georgia posted cyber attack tools and instructions in Russian language Internet forums to deceive pro-Russian cyber forces into unwittingly attacking Russian Web sites instead of Georgian sites.[27] This Georgian counterattack appears to have had a negligible effect on the Russian Web sites targeted.[28] Overall, the cyber defense efforts were too little too late.

親俄網軍在衝突全期都掌握網路優勢，使得喬治亞從未發動有效的網路防禦或網路反擊。例如，喬治亞企圖採取來源過濾方式，從網際網路協定位址清查網路攻擊的源頭；然而，網路攻擊者的情報準備作為，輕易破解了這個戰術。親俄網軍運用轉址功能，藉由國外伺服器隱藏他們真的網際網路協定位址和建立假的位址，欺騙喬治亞的網路過濾器。[25]然而，喬治亞還是把一些政府網站移到美國伺服器上以維持運作，[26]儘管喬治亞的網路防禦沒能成功，但至少試圖打算奮力一擊 ── 雖然還是失敗了。喬治亞在俄語網站論壇張貼網路攻擊工具與操作指南，以誘騙親俄網軍在不知情狀況下攻擊俄羅斯網站。[27]喬治亞的這個反擊，對俄羅斯網站的影響微乎其微。[28]總而言之，喬治亞網路防禦的努力，規模太小也太晚。

With cyber superiority in hand, pro-Russian forces used cyber interdiction to choke Georgian communications by leveraging the generic properties of transportation networks. After the first wave of botnet cyber attacks on the initial 11 targets, an ad hoc cyber militia joined the assault. Cyber attack tools and a list of suggested targets were posted on Web sites for Russian supporters to launch their own strikes. The instructions were simple enough for

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.

people with limited computer skills to follow. This ad hoc cyber militia was so effective that it shut down or defaced 43 Web sites beyond the 11 original botnet targets.[29] In total, 54 Georgian Web sites related to communications, finance, and government were struck, and Georgians could not access these sites for information or instructions.[30] The cyber attacks thus denied Georgian forces access to a key portion of their information network, the Internet, reducing their overall information network's useful capacity.

親俄網軍挾其對通用屬性傳輸網路影響的優勢，使用網路阻絕窒息喬治亞的通訊。在第一波以殭屍網路攻擊11個初始目標之後，特設網路民兵也參與攻擊。網路攻擊工具與建議攻擊名單張貼在親俄網站上，讓俄羅斯支持者發起各自的攻擊行動。指示簡單易行，只要具備基礎電腦技術就可以照辦了。這些網路民兵除殭屍網站攻擊的11個初始目標外，又很有效率的關閉或破壞43個網站。[29]總共有54個與通訊、金融及政府相關的網站遭到癱瘓，導致喬治亞人無法運用這些網站存取資訊或指令。[30]這些網路攻擊阻斷喬治亞軍隊在網際網路上傳遞資訊，降低了他們整體資訊網路的使用能力。

As a result, the cyber attacks dislocated Georgian data flows, shunting data that normally would have traveled over the Internet into more traditional conduits such as telephone and radio communications. Additionally, land, sea, and air combat operations created a dramatic spike in the data volume and data rate demands on Georgia's overall information network. For example, in the town of Gori, government and news Web sites were disabled with DDoS attacks just prior to a Russian air attack, which would predictably drive information demands up.[31] A subsequent spike in information communication demands combined with the dislocation of Internet communications to more traditional forms-such as cell and land phones-appear to have created a bottleneck.

其結果，網路攻擊打亂了喬治亞的資料流通，分流資料通常會經由網際網路到許多傳統的管道，如電話和無線電通訊。此外，陸、海、空作戰行動使得喬治亞整體資訊網路資料流量和流速大增。例如，在戈里鎮的政府和新聞網站，於俄羅斯空襲前遭到分散式阻斷服務攻擊(DDoS)而失能，達到激增資訊的預期要求，[31]隨之而來的資訊流

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〉.

通尖峰需求由網際網路通訊移動至更多傳統通訊系統－如手機和家用電話－因而產生瓶頸。

Georgians were trying to transmit more data at a higher rate than the useful capacity of their information network could accommodate because a large proportion was being consumed by cyber attacks injecting extraneous data into the network. The cyber attacks effectively jammed Georgia's overall information network during the early stages of the war when rapid and organized action by Georgian defenses, cyber and kinetic, could have had the greatest impact.[32] Cyber interdiction created a Russian military advantage at the operational and tactical levels by hindering the Georgian military's ability to organize and conduct effective operations to thwart kinetic Russian military operations. Cyber interdiction created conditions such that Georgian forces could not help but to act mistakenly.

喬治亞企圖在他們資訊網路可用容量中，以較高速率傳送更多資料，但極大部分通達率已被網路攻擊灌入的無關資訊用罄。在戰爭初期階段，網路攻擊很有效地阻塞了喬治亞整體資訊網路，當時喬治亞若在網路或實體面採取迅速且有組織的防禦措施，將有強大的反擊。[32]網路阻絕在作戰及戰術階層替俄羅斯創造出軍事優勢，係藉由阻礙喬治亞軍事力量去組織及執行有效作戰阻止強大的俄羅斯軍事作戰。網路阻絕創造的條件，讓喬治亞部隊不由自主地採取錯誤行動。

Furthermore, cyber interdiction likely multiplied the effectiveness of cyber attacks conducted to achieve cyber superioity by interfering with CERT Georgia's ability to gain situational awareness and orient itself to more effectively respond. Slessor describes the problem of air superiority as "how to deprive the enemy the ability to interfere effectively by the use of his own air forces."[33] Because all Georgian information communications were essentially jammed by the cyber interdiction attacks, CERT Georgia would have had an extremely difficult time simply gathering enough data to understand the cyber attacks' effects, much less mitigate them. By jamming all Georgian communications, cyber interdiction not only interrupted Georgia's traditional military response but also likely stifled Georgia's cyber defenses, prolonging pro-Russian cyber superiority.

再者，網路阻絕因為阻礙了喬治亞電腦緊急應變小組(CERT)瞭解戰況並即時有效反應，而加乘了網路攻擊的戰果。施雷瑟爵士描述空優問題時表示：「如何使用其自身空中武力剝奪敵人干預效能」。[33]因為所有喬治亞的資訊通聯都已經被網路攻擊阻塞，

32 Tikk et al., 6.

33 Slessor, 31.

CERT甚至連蒐集足夠資訊以準確評估網路攻擊遭受多少損失都困難重重，遑論設法降低損失。藉由阻塞喬治亞所有通訊，俄羅斯的網路阻絕不但打亂了喬治亞的傳統軍事頻率響應，同樣也壓制了喬治亞的網路防禦，延長了親俄部隊之網路優勢。

In that war, cyber attacks for cyber superiority and cyber interdiction were mutually reinforcing. The result was a situation where Georgian communications-its system of information supply-were gummed up, preventing timely delivery of data and commands to Georgian forces. The Georgians had to choose whether to yield superiority in decision speed or decision quality. The effect with either option was an unqualified Russian military advantage that Georgia could not overcome.

這次戰爭中，網路優勢及網路阻絕的網路攻擊，彼此相輔相成，結果是喬治亞的通訊狀況－其資訊供應體系－被搞得一團亂，即時傳遞資料及指揮部隊陷入停滯。喬治亞部隊被迫只能在決策速度和決策品質間選擇，然不管選擇哪一樣，喬治亞都無法克服俄軍的軍事優勢。

Implications
啟示

As in the early days of airpower, cyber power today is critical to victory, but it probably cannot win wars alone if for no other reason than its inability to create much violence, although this shortcoming will likely fade in the future. Consequently, it is imperative to understand how best to employ cyber power in concert with land-, sea-, and airpower. Airpower theory suggests two principles to guide cyber power strategy at the operational level: securing the enemy's freedom of action, and confronting him with a choice between at least two bad options. Cyber superiority satisfies the first principle, while cyber interdiction satisfies the second. The example of the 2008 Russia-Georgia war demonstrates the truth of these principles, but how should one go about gaining and maintaining cyber superiority and conducting cyber interdiction?

如同早期的空中戰力，網路戰力是今日的致勝關鍵；但若不能藉其他理由來創造更多暴力，單靠它大概無法贏得戰爭，儘管這種情況在未來越來越式微。所以，瞭解如何妥善運用網路力量與陸、海、空戰力協同配合，是非常勢在必行。在作戰階層，空權理論建議兩個原則以指導網路力量戰略：拘束敵人行動自由，以及迫使其在至少兩個不利選項中做出抉擇。網路優勢滿足了第一個原則，網路阻絕則滿足了第二個。以2008年俄喬戰爭為例，論證這兩個原則真實性。但該如何獲得並確保網路優勢，同時又能進行網路阻絕？

With securing cyber superiority being the first priority for military cyber power, initially

focusing on neutralizing the adversary's capability to prohibitively interfere with friendly operations via cyberspace seems most logical. Consequently, the enemy's cyber attack, cyber reconnaissance, and cyber defense capabilities should be among the highest priority targets for cyber reconnaissance and all-source intelligence preparation of cyberspace, as well as among the highest priority targets for suppression or destruction (via cyber or kinetic attack) once hostilities begin. Second, cyber attacks directed at those portions of cyberspace irrelevant to the war but which an opponent must succor, such as the cyber attack on the GRENA that diverted CERT Georgia from the larger conflict, are valuable in that they focus the enemy's cyber defense forces away from decisive points. Third, cyber attacks should be used to interdict data required by enemy cyber repair, recovery, and quick reaction defense forces to disrupt the adversary's ability to effectively parry cyber strikes. Together, these actions should neutralize, divert, and disorganize an opponent's cyber power to gain and maintain cyber superiority.

對軍事網路力量而言，確保網路優勢安全無虞是首要優先；初期聚焦於抵銷敵人的能力，使其無法經由網路空間干擾我友軍行動。因此，在敵對行為初始時，敵人的網路攻擊、網路偵察與網路防禦能力，應是網路偵察和網路空間多重情資情報準備的優先目標，以及列為壓制和摧毀的最優先目標(經由網路和動能攻擊)。其次，將網路攻擊目標指向與作戰無直接關聯卻是對手必要保護的部分，如俄羅斯攻擊喬治亞研究與教育網路協會(GRENA)，將網路攻擊轉向其電腦緊急應變小組(CERT)，就是因為在大規模衝突中，CERT是喬治亞移除敵人網路防禦能力的決定點價值。第三步，網路攻擊應該用來阻斷敵人網路修護、復原與快速反應防衛所需資料，以避免敵人採取有效的網路反擊。綜前所述能力就能壓制、箝制及瓦解對手的網路力量，贏得和維持網路優勢。

Cyber interdiction targets are the next most important cyber objectives in joint military operations, first at the operational level and then the tactical and strategic levels. At the operational level, analogous to the rail marshaling yards that were the primary air interdiction targets of World War II, data marshaling yards (also known as data fusion centers) are the logical focal points for cyber interdiction. Data fusion centers are few in number compared to the combat systems they support (for example, fighters, tanks, and submarines), and they are the nodes where raw materials (data) are marshaled and transformed into information, a coherent understanding of the situation to be shared military forces. Data fusion centers are centers of gravity in cyberspace because they are where orientation happens.

聯合軍事作戰下一個最重要的目標是網路阻絕，先在作戰階層，然後是戰術和戰略階層。在作戰階層，第二次世界大戰時最主要的空中阻絕目標就是鐵路調度中心；如今

邏輯上的網路阻絕目標，就是資料調度中心，又稱為資料匯流中心。資料匯流中心在數量上，比戰鬥系統少(如戰機、坦克或潛艇)，他們是原始數據(資料)整理或轉換成資訊的節點，整合瞭解當前狀況，並轉發給各部隊。資料匯流中心是網路空間的重心所在，因為所有行動指引都要靠它匯流。

Fusion centers at the operational level include enemy command and control nodes and intelligence, surveillance, and reconnaissance processing, exploitation, and dissemination nodes. By destroying, degrading, or neutralizing these data marshaling yards, cyber interdiction caps an adversary's operational effectiveness by limiting his ability to orient and concentrate effects in time and/or space. Regardless of an enemy's camouflage, concealment, and deception capability to foil kinetic strikes, data fusion centers must advertise their location in cyberspace (for example, IP address) to some degree to receive data and distribute information. Data fusion centers are almost certain to be vulnerable t o cyber attack because their utility heavily depends on their connectivity-the power of a network grows exponentially with the number of users.[34] If these nodes are not widely connected, they are irrelevant to the enemy's warfighting effort and can be ignored. Degrading data fusion capabilities creates greater uncertainty at the operational level and compels an adversary to rely more on his ability to adapt at the tactical level. In turn, an enemy's ability to adapt at the tactical level depends on the effectiveness of his tactical network and communication/data links. Thus, cyber interdiction at the operational level magnifies the significance and impact of cyber interdiction and electronic attacks to disrupt data links at the tactical level.

在作戰階層，匯流中心包括敵人的指揮管制節點和情報、監視、偵察處理、運用、傳送節點。經由破壞、摧毀和制壓這些資料調度中心，網路阻絕可以遮斷敵人的作戰效能，在時間和空間方面限制其定向和集中的效果。不管敵人如何以偽裝、隱匿或欺騙等方式隱匿行動，資料匯流中心都必須在網路空間標示其位置(如網際網路協定位址)，以利我方某些單位得以接收資料及傳送資訊。資料匯流中心必然非常容易遭受網路攻擊的危害，因為它的運作，完全要依賴資訊的相互連結 —— 使用人數越多，網路成長指數的力量越發強大。[34]假如這些節點沒有廣泛的連結，將因無涉及敵人的戰鬥作用而被忽略。降低資料匯流能力，可在作戰階層製造更多不確定，而迫使敵人必須依賴戰術階層能力。質言之，敵人的能力適應了戰術階層後，就會依賴戰術階層網路和通訊／資料連結的有效性。如此一來，網路阻絕即在作戰階層擴大其重要性和網路阻絕的衝擊，以及電子攻擊，進而瓦解戰術階層的資料連結。

34 Carl Shapiro and Hal R. Varian, Information Rules: A Strategic Guide to the Network Economy (Cambridge: Harvard Business School Press, 1999), 184.

An opponent's tactical data links are the next most important cyber interdiction target set after data fusion centers. At the tactical level, each node (for example, fighter plane, platoon, and destroyer) on the tactical network has some level of data fusion capability, so information is rarely concentrated to the point that attacking those nodes in cyberspace will have widespread effects. However, tactical data is so perishable that even temporary disruptions to the data link network can have significant negative impacts on the ability of each tactical unit to derive information before the data are no longer a valid basis for decisions. As a result, disrupting tactical network data links, not disabling nodes, is the appropriate objective of cyber interdiction at the tactical level. Interrupting these links can cause brief but meaningful delays and misperceptions in an opponent's decision cycle to create or magnify a "first look-first shot-first kill" tactical advantage. By focusing military cyber power on gaining and maintaining cyber superiority and cyber interdiction at the operational and tactical levels, joint forces can maximize their capabilities and gain a significant decision advantage difficult for an opposing force to overcome.

繼資料匯流中心之後，下一個網路阻絕的最重要目標就是對手的戰術資料連結。在戰術階層，每一節點(如戰機、排和驅逐艦) 在戰術網路中都具備某種程度的資料匯流能力，所以資訊很少會集中在這些點，在網路空間攻擊這些節點將會分散效果。無論如何，戰術資料是脆弱的，在它成為決策的重要根據前，即使是對個別的戰術單位實施暫時性破壞，也會對資料連結造成嚴重衝擊。因此，在戰術階層，網路阻絕適當的手段是瓦解戰術網路的資料連結，而不是使其節點失效。對這些網路連結破壞過程雖短，卻能使敵人決策程序延遲及喪失洞察力，可創造或擴大我初期之觀測、射擊和獵殺等戰術優勢。藉由聚焦於軍事網路力量，在作戰及戰術階層獲得並保持網路優勢及網路阻絕，聯合部隊能最大化作戰能力，並獲致敵人難以匹敵的重大決策優勢。

In joint warfare, it is the air campaign that can benefit most from the effects of cyber superiority and cyber interdiction against enemy data fusion centers and tactical data links. Although cyber power supports land and sea operations, the air campaign is typically the leading effort in joint warfare. Beginning with World War II, airpower has formed the vanguard of every U.S. military operation whether based on land or sea. Additionally, the ability of modern air forces to conduct parallel warfare in the style first used during the 1991 Persian Gulf War critically depends on the exploitation of cyber power for situational awareness, communication, and reconnaissance. Furthermore, enemy capabilities to defeat stealth aircraft have at their heart data fusion to overcome stealth's ability to hide from air defense radars. Cyber power puts the integrated in integrated air defense. With cyber power knitting air defense sensors and shooters together, an opponent could generate an airspace picture with fewer

weaknesses.

在聯合作戰，空中戰役的利益大部分來自於以網路優勢、網路阻絕對抗敵人的資料匯流中心和戰術數據鏈路。雖然網路力量支持地面和海上作戰，空中戰役仍是主導聯合作戰的典型。第二次世界大戰初始時，每一場美國軍事作戰，不管是陸戰或海戰，都以空中武力為續戰。此外，現代的空中武力平時作戰，首次運用係於1991年波斯灣戰爭期間，當時就非常依賴利用網路力量來執行戰況掌控、通訊與偵察。而且，敵方能力想擊敗隱形戰機，其資料匯流中心就必須具備足夠能耐，讓隱形戰機在雷達上無所遁形。網路力量可以將這些能力整合到空中防禦，以網路力量整合空中防禦感測器和射擊武器，一個對手能建立一個較少弱點的空中空間圖像。

However, without a data network to fuse multiple sensors, surface-to-air missile batteries become individual defenders in a one-on-one engagement, a scenario that stealth aircraft have proved they can dominate since 1991. Cyber interdiction applied in support of air forces can dramatically ease the dangerous task given to air forces-to penetrate the teeth of an enemy's defenses at the outset when the defenses are most lethal. The price of air warfare without a cyber advantage is steep. The last time U.S. airpower fought through an enemy air defense without the benefit of cyber superiority in World War II, American aircrews had a lower probability of survival than Marines fighting in the Pacific.[35] In addition, air operations can unfold much more rapidly than land or sea operations. Surface forces move at tens of miles per hour compared to air forces, which move at hundreds of miles per hour. Land and sea forces-much like the foot soldiers of World War I who were too slow to convert a breakthrough into a breakout-will in all likelihood be too slow to exploit the fleeting advantages created by cyber interdiction as effectively as air forces.

無論如何，沒有數據網路來匯流多重感測器，地對空飛彈營將變成個別防衛者而陷入一對一的接戰劣勢；自1991年起，證明隱形戰機足以支配戰局。網路阻絕應用在支援空中武力，因使危險任務容易執行而能引人注目 ── 突入敵防衛網的空隙時大幅減少任務危險性。在無網路優勢的空中作戰，代價是很高的。上一次美國空軍在沒有網路優勢飛越敵人領空進行作戰是在第二次世界大戰時，美國的空中機組員傷亡比在太平洋上作戰的陸戰隊還高。[35]此外，空中作戰的進展比地面和海上作戰快；水面部隊每小時移動10哩，相較於空中部隊，每小時可移動數百哩。陸地和海上部隊－就像第一次世界大戰時的步兵，因速度太慢而無法將突破轉換為包圍突破－網路阻絕如同空中武力效力，所有反應速度太慢者將無法利用稍縱即逝戰機。

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.

Conclusion
結論

Cyber power is critically important in joint warfare. Military cyberspace operations should have as their priority the attainment and maintenance of cyber superiority and cyber interdiction in support of kinetic operations with a focus on supporting the air campaign. Additionally, operations to gain and maintain cyber superiority should concentrate on neutralizing enemy cyber attack and cyber reconnaissance capabilities, followed by suppressing enemy cyber defenses. Cyber interdiction attack operations should focus on the cyber equivalent of rail marshaling yards-data fusion centers-and tactical data links. Together, cyberspace superiority and cyber interdiction yield a powerful decision-making advantage in joint warfare, the cumulative effect of which is to compel an enemy to make mistakes that will likely prove fatal in due course.

網路力量在聯合作戰中確實重要。軍事網路空間作戰必須獲取並維持網路優勢與網路阻絕，以支援機動作戰如同聚焦於支援空中戰役；此外，獲取並維持網路優勢應集中於削弱敵人的網路攻擊與網路偵察能力，接下來是壓制敵人的網路防禦。網路阻絕攻擊作戰應聚焦於網路的鐵道調度場－資料匯流中心－以及戰術數據鏈路。總體而言，在聯合作戰，網路空間優勢與網路阻絕產生決策優勢，累積效應可迫使敵人犯錯進而導致失敗。

作者：E. Lincoln Bonner III

文章出處：《聯合作戰季刊》74期，2014年第三季