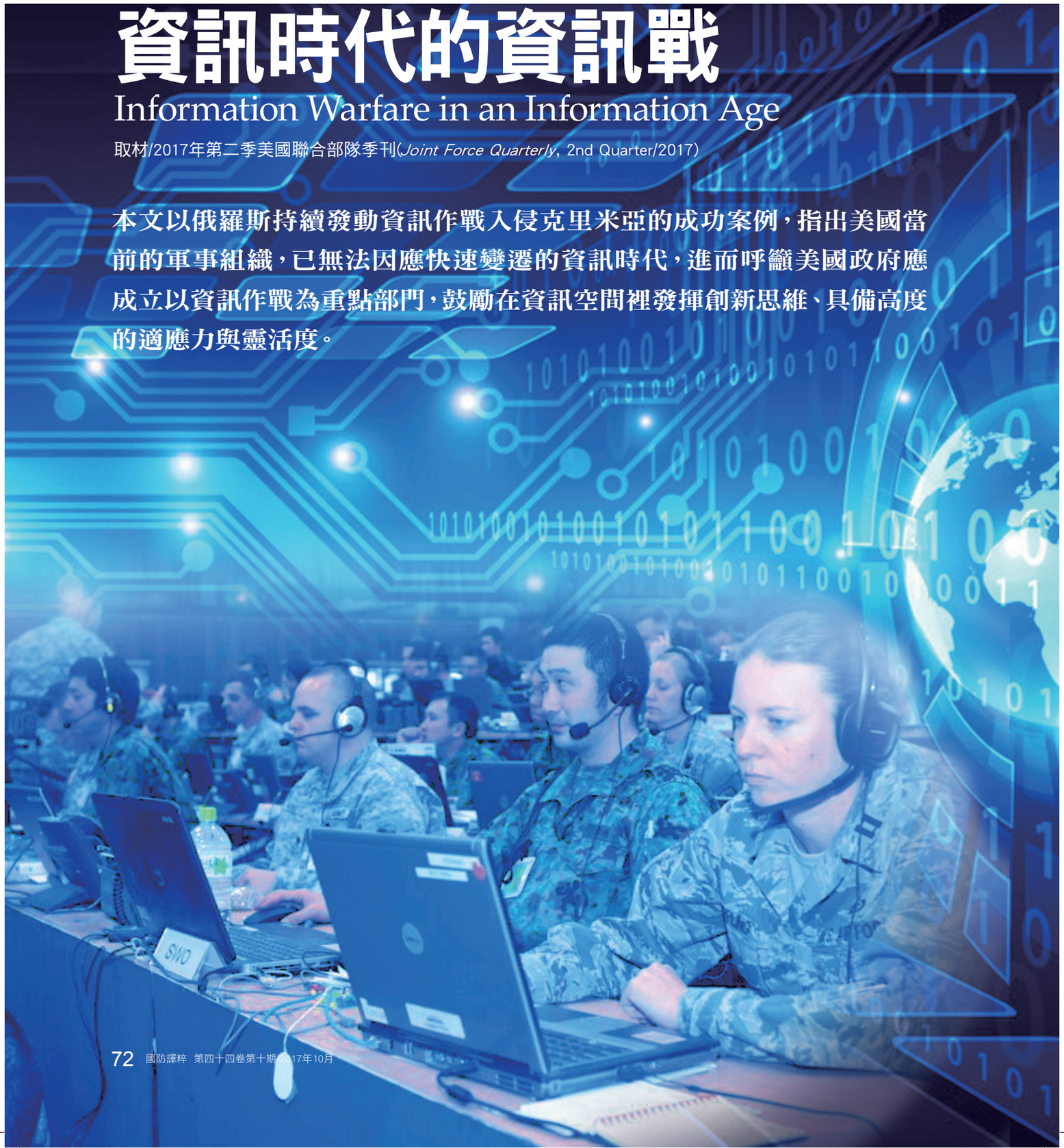
● 作者/William R. Gery, Se Young Lee, and Jacob Ninas ● 譯者/王建基 ● 審者/馬浩翔

資訊時代的資訊戰

Information Warfare in an Information Age

取材/2017年第二季美國聯合部隊季刊(*Joint Force Quarterly*, 2nd Quarter/2017)

本文以俄羅斯持續發動資訊作戰入侵克里米亞的成功案例，指出美國當前的軍事組織，已無法因應快速變遷的資訊時代，進而呼籲美國政府應成立以資訊作戰為重點部門，鼓勵在資訊空間裡發揮創新思維、具備高度的適應力與靈活度。



資訊系統遭攻擊次數逐年攀升，顯示出當前是透過資訊科技在資訊空間中作戰。

(Source: U.S. Pacific Command/David Chapman)

在過去一週中，你所曾使用的裝置裡有多少個會連上網路，或用某套演算法完成一項工作？數量可能會上看10到15個，而且就算不是每小時，也是每天使用這些裝置，可能包括運動手環、手機、個人電腦、工作電腦、居家監視系統、汽車、網路電視、印表機、掃描器及地圖，如果你真是個科技達人，甚至你的咖啡壺或電冰箱也可能包括在內。

所謂「物聯網」(Internet of Things, IoT)是由一套逐漸與我們生活各層面相結合的網路相互連結起來，而且上述裝置間也更加相互依賴，以發揮其功能。[1] 採用先進演算法的計算裝置，正邁入機器學習階段，而所謂機器學習乃屬於電腦科學的一項分支領域，旨在探討電腦如何「學習」環境，並根據已獲得之數據與條件提出預測結果。[2] 這方面的趨勢包括機器自主及自我學習。「互聯」(interconnectivity)的概念並不僅有物聯網而已，還包括改變網際網路的資訊，以及資訊如何影響我們日常決策。全球「網狀網路」(mesh-network)的趨勢

正在發展，加諸資訊科技領域的建構，使我們對所處環境更加瞭解。自1965年提出摩爾定律(Moore's Law)以來，即廣為大眾接受。如果未來摩爾定律仍被奉為圭臬，將會有更多應用程式、運算法及日常所需功能，把我們生活的各部分鏈結起來，提供更強的處理能力，也能為人類創造最大效能的無限資訊流。

《西發利亞條約》(Westphalia Treaty)設計下的社會與秩序，滿足了人類要在一套邏輯模式中運作的需求，然而國際法以及有秩序地劃分國家的原則，也創建了對於領土與國內事務的主權。若欠缺高速率資訊傳遞全球化便不可能發生，而全球化未來將扮演重要角色，也許會改變世界秩序。如果一定要有資訊優勢才能達成民族國家與軍事目標，而且因為物聯網的高複雜度導致無法保證獲得資訊優勢，美國政府該如何展現有效且整合的資訊戰能力？此外，如果要在資訊空間作戰，單靠資訊就能獲勝嗎？換言之，資訊作戰能否提供作戰的方法與手段，乃至於目標？此外，美國政府是否有需要投資成立某個組織，負責協調並整合資訊戰的能力與效果？

為提升美國政府的能力與能量，應在美國政府內創設一個新組織，並以一種全然不同於現行階層式的政府結構，專司資訊戰。美國政府尤需採用外交、資訊、軍事與經濟的模式，而不是專門設立一個組織領導此一模式的資訊職能。國務院負責協調外交角色、國防部負責協調軍事角色，而財政部則負責協調經濟角色。由物聯網所形成的二十一世紀各項挑戰，需要一個更具創新力的組織，來提倡在資訊空間的適應力和靈活度，類似谷歌、臉書或蘋果等企業所採用的模式。

2015年3月16日，「德國電信股份公司」(Deutsche Telekom)在以物聯網為主題的「2015年德國漢諾威電腦展」中，展示以機械手臂擺置陽傘的情形。
(Source:Mummelgrummel)

《資訊戰》(*Information Warfare*)乙書作者、知名資訊戰理論家斯瓦淘(Winn Schwartau)，將資訊時代形容為「無處不電腦。」[3]資訊年代的最終事實就是資訊科技的普及，而資訊科技「兼採資訊系統與資源(硬體、軟體與濕體[wetware])，而這些都被軍民決策者用於傳送、接收、管制，以及運用所需資訊達成二十一世紀的決策事項。」[4]此外，資訊科技的發展，使資訊能以近乎即時、極高速率、匿名、保密的方式進行分享。這些發展固然能作為資產，但也對

美國及其盟邦，以及敵人形成一個潛在弱點。[5]只需要短短幾秒鐘，即能將圖片或評論上傳至社交媒體網路。敵人同時也可運用這些系統獲取重要資訊。《紐約時報》的一篇專文中曾指出，「2015年7月，因政府電腦系統遭受大規模侵犯，有多達2,150萬人受到影響，所造成的傷害遠高於初期判斷，其肇因為竊取寶貴的個資，包括社會安全號碼及若干指紋。」[6]政府電腦系統遭受網路攻擊次數統計如下。[7]資訊系統遭攻擊次數逐年攀升，在在顯示出當前是透過資訊科技在資訊空間中遂行作戰。

- 五角大廈傳出每日內遭受1,000萬次攻擊。
- 美國能源部所屬「國家核子安全局」(National Nuclear Security Administration)，每日亦遭受1,000萬次駭客攻擊。
- 英國傳出每日發生12萬次網路攻擊事件，幾乎等同密西根州所面對的數量。
- 猶他州指出，2年前每日面臨100萬起網路攻擊，如今則驟增為2,000萬起。[8]

為肆應資訊時代之挑戰，必須進行組織變革。現代構想加諸工業概念，或可成為遨遊資訊空間，為未來衝突創造優勢的一種方法。

在物聯網中，各種活動均在奈秒(nanosecond，十億分之一秒)內完成，每天則有數十億次活動。大數據的概念，是要駕馭大量資訊，並從這些資訊中提取出一些人們能據以決斷的東西。在不久的將來，要在資訊上超敵勝敵的關鍵，可能就在於誰能擷取資料、找出資訊空間中的重心，並且透過一套規則與計算標準(均根據定義明確之「交戰規則」所訂)，自動採取作為。現在的確具備駕馭大數據的能力，而且此一能力還不斷提升中。各消費者產品公司，都在臉書、谷歌及其他資料中進行資料探勘，以瞭解消費者取向、全球趨勢，以及對重要事物的想法。就軍事面而言，瞭解與潛在敵人相關之資訊形勢，對軍事作戰全程之資訊作戰而言，乃是基本考量因素。運用於商界的大數據概念可能有其優點，並可用於資訊作戰。資料探勘以及因而獲得之資訊優勢，唯有透過資訊戰才有可能達成目標。

美國運用諸多資訊戰戰略、機構及專業人員，迄今已獲致程度不等的成果。「美國新聞署」(US Information Agency, USIA)自1953年成立，嗣後於1999年裁撤，其職責為整合各項資訊作為：

> [美國新聞署]職責範圍為原屬國務院「國際新聞局」(International Information Administration, IIA)、「技術合作局」(Technical Cooperation Administration)，以及「共同安全局」(Mutual Security Agency)所執行之一切外國資訊活動。在海外，既有之美國新聞署各辦事處，均成為新成立單位的外勤業務辦公室。由國際資訊局所執行的人員交換計畫，仍繼續由國務院業管，但美國新聞署則負責管理該計畫的海外部分。國務院負責提供政策指導。[9]

資訊戰在過去被認為對國家安全至關重要，而且冷戰期間美國新聞署也奉命破壞對蘇聯的支持。[10] 今天，我們通常將資訊戰當作一種手段，有時則當作一種方法，以達成目標。但現在我們

很少認為資訊戰是一種目標，即便我們活在每天受資訊環境影響的資訊時代。〈美國軍事契機〉(U.S. Military Opportunities)乙文作者尼奇波魯克(Brain Nichiporuk)，對資訊戰之構想與假設論述如后：

> 攻勢資訊戰旨在拒止、破壞，以及摧毀敵人戰場資訊來源，或降低其效果。落實並同時維持自身資訊來源安全，係達成「資訊優勢」之關鍵——亦即在戰場上見敵人所不能見。[11]

在當前及未來戰爭中，資訊優勢可能是單一決定性因素。以當前臺海局勢為例，中共刻正對中華民國政府施以強固的資訊戰戰略，使中華民國受制於中共，而無須發動實體(kinetic)戰爭。他們將同時對美國進行資訊作戰以遲滯美國介入，使美國的外部介入來得太晚而無法影響結果。[12]當今此一作戰構想業因集中發展資訊戰戰略、組織與能力而得以完全實現，正體現孫子「不戰而屈人之兵，善之善者也」的戰略思想。[13]另一個例子是俄羅斯入侵克里米亞的行動，這起事件為資訊戰的原則與如何直接獲致戰果等，提供了一個當代個案研究的題材。

資訊作戰：俄羅斯入侵克里米亞

2014年俄羅斯入侵東烏克蘭，並最終兼併克里米亞，乃是當前持續性資訊戰的一個模式，當中也有諸多資訊戰成敗案例。俄羅斯的資訊戰稱為「反身控制」(Reflexive Control)，係源自於蘇聯準則，是其「混合戰」(hybrid warfare)行動的關鍵要素。[14]反身控制「是靠……俄羅斯利用敵人既定的傾向，選擇所欲之行動方案。」[15]在烏克蘭作戰期間，俄羅斯主要障礙包括西歐各國與美國。俄羅斯採取諸般措施，獲致敵人既定的傾向，俾於烏克蘭成功執行作戰，並同時避免與西方進行大規模對抗。

做為反身控制的一部分，俄羅斯運用一套密切協調的拒止及欺敵計畫，稱為「馬斯其洛夫卡」(maskirovka)，透過運用「小綠人」建立檢查哨，並掌控烏克蘭鎖鑰地形。這些小綠人既迅速又有效率，身上未有身分標示或單位臂章。這種使他人無法辨別身分的作法，使得俄羅斯否認與這些部隊的關係，之後才發現他們就是俄羅斯部隊。由於在衝突初期能夠控制資訊，並否認參與佔領烏克蘭行動，因此俄羅斯被國際社群視為利益關係方——而不是交戰方。這使俄羅斯馬上體認到，西歐及美國不希望有直接衝突，也不會報導俄羅斯介入相關議題，即便被發現也是如此。

在作戰期間維持相當保密程度，亦使俄羅斯成功掩飾其真正意圖。藉由作戰保密，使敵人與外界觀察家基本上認定，幾乎所有俄羅斯採取的行動都會成功，其原因在於不瞭解俄羅斯企圖。這亦使俄羅斯的磨刀霍霍與威脅未引起北約組織及西方的質疑，而俄羅斯還故意將西歐及美國刻劃成紙老虎，尤其在發展中國家的眼中更是如此。除了在烏克蘭的地面行動外，俄羅斯也整合運用電視、平面媒體與社群媒體轉移焦點，在隱藏其佔領、兼併作為之際，同時降低西方介入的可能性。[16]俄羅斯成功運用資訊戰，使其部隊能夠在西方未出現大規模反應的情況下，佔領烏東地

區，兼併克里米亞。

正當世界持續邁向資訊時代之際，民族國家與非國家行為者成功地將資訊作戰戰術融入其整體戰略的能力，無疑地必然會增加。為成功嚇阻這些威脅並做出回應，美國必須採取創新作為，並發展具備防範與落實此類專業行動能力的組織。

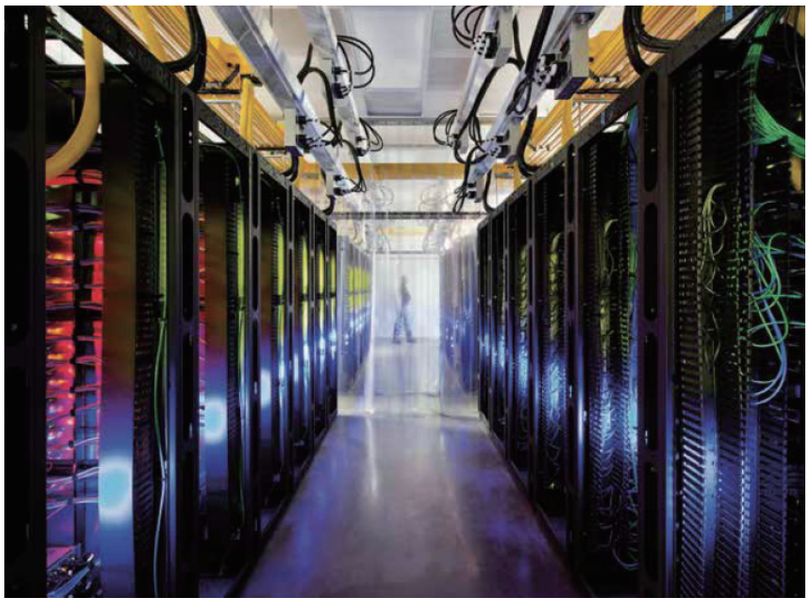
2016年10月18日，美國國防部副部長沃克(Robert Work)，以及參謀首長聯席會議副主席塞爾瓦(Paul Selva)上將，赴夏威夷史密斯營(Camp H.M. Smith)會晤美國太平洋司令部司令哈里斯(Harry Harris)上將，就「第三次抵銷戰略」(Third Offset Strategy)及其對印亞太地區之影響進行討論。

(Source: USN/Jay M. Chu)

俄羅斯在烏克蘭的資訊戰，固然使其達成兼併克里米亞的目標，但這絕不是個完美無瑕的戰略。其中一個瑕疵，就是俄羅斯領導人否認派遣部隊進入烏克蘭的作法。即便鐵證如山，包括在社群媒體公布的地理標籤相片，以及在烏克蘭境內查獲的俄羅斯部隊，但俄羅斯總統普丁仍矢口否認。這些過多且持續的否認，只是使俄羅斯領導人信用受到質疑，並使外界有更多理由相信，俄羅斯軍隊就是在烏克蘭境內作戰。[17]此外，未展開大規模攻勢的網路行動，使人質疑這種混合戰成效是否言過其實。俄羅斯應該可以算是世界上最強的民族國家網路行為者之一。[18]欠缺2007年對愛沙尼亞與2008年對喬治亞共和國所施展的一種全面性攻勢網路戰，易使人質疑俄羅斯的資訊戰與反身控制戰略是否有效。雖然這或許顯示出俄羅斯無意激怒潛在敵人，但也可能指出俄羅斯無法全面控制其網路攻擊行動，而這可能導致大規模的無預期後果[19]。這些結果也導致俄國無法否認牽涉其中，抑或將強敵引入爭端。如上所述，從反身控制準則中所提及的缺陷可看出，無論目前還是未來，在資訊時代中要控制攻擊行動結果並實施資訊戰有多麼困難。在更深入瞭解潛在敵人能力與意圖、學習他們的經驗教訓，並將之化為美方的優勢時，美國政府必須確保當前資訊戰能力及戰略規劃組織，擘劃出一套全般整合的國家安全戰略。

從戰略規劃指導至戰術執行？

在聯合計畫程序階段，資訊戰計畫作為通常是扮演支援角色。如果我們認為所有戰爭都要在認知面上進行，至少在某種程度上是如此，則假設



愛荷華州康瑟爾布拉夫斯(Council Bluffs)谷歌園區網路室內的路由器與開關，透過光纖網路，以一般家用網際網路連線速度20萬倍的高速運作，將各個資料中心相互串連。(Source: Google Inc.)

資訊戰行動方案有時應扮演支援角色即合乎邏輯。此外，「資訊戰應支援主軸，」有時是在實體軍事行動方案完成後才開始發展。[20]雖然當前計畫程序及傳統計畫作為架構，已將國家戰略與戰術階層相互鏈結，但並未規範如何在未來衝突中獲致資訊優勢。或許從國家的角度來看，資訊戰略應能啟動後續行動，並將從總統到每位官兵結合在一起。資訊戰略應與美國政府的各項戰略溝通作為相整合。然而，正如「國防科學委員會」(Defense Science Board)2008年的報告所指出，「戰略溝通係一動態過程，由政府最高層──總統與政府高級領導人──負責執行……雖然已就此採取若干措施，但仍不足夠，需要做出更多承諾。」[21]事實上，該報告建議成立一個非營利、不具政黨色彩的「全球交往中心」(Center for Global Engagement)，作為戰略溝通活動的中心。

2010年，時任美國副總統拜登(Joseph Biden)向總統提交一份有關戰略溝通的報告，籲請採取一致行動，並對整體構想進行說明。[22]同時建議成立一個由國家安全參謀所領導的跨部會政策委員會，作為解決方案；然而，此一委員會卻是由忠於所屬組織、且可能各自負有其他職責的個人所組成，他們並非完全將心力投注在整合性戰略溝通之上。現有微不足道的資訊戰能力，是植基於當前及過去遺留下來的組織架構，而這些都成了資訊作戰計畫作為與執行的障礙。

如果資訊空間能被視為一種勝出方式與手段，那就要有一套架構協助排定順序與計畫作為，以及提出可透過資訊戰達成的目標。計畫人員應根據指揮官意圖、作戰環境，以及專為解決該問題而設計之方法，說明為何要採取某一特定行動，以及該行動應何時執行。數十年來對作戰的反覆試驗，形成了制度化的準則與一套規則。雖然有人認為這些規則均應適用於實體及非實體戰，但切記仍有若干特殊因素與這兩者有關。例如，目標選定的基本要件，大體上依照攻勢實兵對抗作戰而設定，但這些目標選定理論有必要為資訊戰

而調整嗎？

有人認為，伊斯蘭國的作戰重心是網際網路。如果我們接受此一想法，那美國應如何選定伊斯蘭國的目標？由美國政府關閉伊斯蘭國所使用的網際網路服務提供者(這就是目標)？由政府對某些網站實施一種分散式阻斷服務攻擊？由政府將具影響力的訊息貼上伊斯蘭國網路留言板？所有選項看起來都不錯，但大多皆因耗時或計畫不同步而無法落實。美國政府中無人主導、也沒有工作重點，無從闡述資訊作戰的二級與三級效果，也往往造成無所作為的結果。由於沒有主導機關，瞭解資訊空間未來將如何受美國行動所影響的能力也不彰。

除了戰術層級的資訊效果外，要如何審查戰略溝通、選定目標？兩者的程序相同或相異？如果對此一程序的觀點需要改變，而且目標選定將成為一種將資訊目標置於不利處境的程序(例如，上述的網際網路服務提供者的例子，或製造一種嚇阻敵人的戰略武器)，那麼務實的選項就可能在危機行動中，提交給作戰指揮官。為落實美國將資訊目標置於不利處境的構想，必須要能接觸目標。取得經由資訊空間所傳遞的資訊相關效果，無異於那些經由飛機或船艦所傳遞的實體效果。傳遞方法可以是新聞、某種網路能力、某種軍事能力，甚至是總統的一篇評論。如欲運用「資訊相關能力」(information-related capability, IRC)，就要使發訊者能達到收訊者，而且目標選定路徑也要能長久維持。若無法保持接觸，便無法將目標置於不利處境，因為要接觸收訊者需要很長時間，而時間長短則是與作戰息息相關。

此外，此一能力須可以獲得。軟體的發展可作為一種潛在戰略優勢。將軟體發展的教育訓練向下延伸至戰術層級，可使年輕的官兵創造出與目標相關的能力、降低成本、創造效率。例如，在教導士兵如何使用步槍時，首先是施以訓練打好基礎，然後他便能根據戰場狀況，運用各種不同的戰術、戰技與程序，精熟該項武器。如果狀況有所改變，他也會按照敵情立即調整。從資訊戰觀點看來，軟體只是個工具，就像步槍一樣。在基礎建立、戰技純熟之後，就全靠戰術層級的培養，以確保相關能力能根據目標加以「調校」，因為戰術層級作業人員應對該目標有最準確的瞭解。再者，在接觸路徑改變之際，戰術與作戰階層應確保對目標保持持續、可靠的接觸。當然，官兵不是戰略制定者；國安團隊、總統及作戰指揮官才是。但哪個組織負責在整個國安體系中協調整合戰略訊息？此外，哪個組織負責對總統提交各種資訊作戰行動方案，尤其是專門設計成戰略目標？

對於向下發展至作業人員層級(也就是官兵)則有不同觀點，那就是權責無法與能力相匹配。這的確是事實。戰術層級單位不應有權在資訊空間作戰，就像步槍兵未接獲命令是不會開槍一樣。我們應該要有一套戰略，對作戰與戰術層級之目標選定，提出明確指導。這並不需要「執行授權」，但確實需要國家層級就此議題給予指導。換言之，由於技術精密度不可或缺，所以美國政府不能冒險在一個支離破碎的資訊戰戰略下，讓過度複雜、層級森嚴的結構，將整個進度拖慢。欠缺一致的作為會危及任務執行，並提高兵力的風險。發展人員、作業人員及分析人員，都應該

具備高度彈性與靈活度，以創新技術與基於對資訊時代的瞭解迅速解決問題，和官兵在戰場上所作所為一樣。

世界是否正在進行組織變革？

自公元前400年的古希臘組織及裝備武力迄今，各國通常依循階層模式建立軍事組織。面對未來全球資訊科技趨勢，美國政府需要以全然不同的思維模式組織資訊相關能力，方能與快速的資訊發展並駕齊驅。大體而言，從古希臘時代到當今的美國政府，各國都是以階層體系為核心籌建軍隊。鑒於資訊戰對政府作為與軍事作戰日趨重要，一種「格狀」(lattice)結構或體系，或許是組織資訊戰(立基於能力與人員)的一種合邏輯方式。

此一構想需要基本指導與一套規則(也就是職權)，但授權每個人得以發展出不因不熟悉技術狀況而減低效力的解決方案。該構想的原則是以英才教育為基礎，並置重點於聯盟策略與軍隊內部專用的「群眾外包」(crowdsourcing)解決方案，甚或請私人企業提出解決之道。在美國政府內部格狀組織不可能全面整合；然而，在全球化與資訊科技逐漸整合我們的世界之際，能同時掌握法律與階層架構價值，並且瞭解格狀組織潛在利益的一種混合式構想，才會有所助益。此外，格狀架構將從概念上與我們所處的「群眾網路」(mass-network)資訊科技環境更加緊密結合。商業界所提出的各種理念，都是能加以採用，或拿來改良美國政府內複雜資訊戰構想的可能解決方案。《富比士雜誌》(*Forbes*)的本柯(Cathleen Benko)與安德孫(Molly Anderson)，從商界角度針對格狀組織架構所提出的主要優點如后：

> 鑒於員工均編組分散在各地理區域，過去的溝通方法再也行不通了。採用格狀方式，可使組織朝向更加互動且更加透明的溝通方式邁進。例如，財務部將一個傳統上留給管理階層的角色——找出成長優先順序——給了員工，其方法是啟用「痛點」(painpoint)入口網頁，讓員工在此對每個人所見的當前挑戰發表意見。公司則另指派若干小組處理優先順序排在前幾名的事務。
>
> 在德勤公司(Deloitte)，我們的年度員工調查顯示，九成經歷過所有三種格狀方式的員工曾參與討論。而韜睿公司(Towers Perrin)在2007至2008年所做的一項大型全球勞動力研究結果顯示，接受調查的公司中，只有六成員工曾參與討論。[23]

不僅是格狀架構促成內部整合與理念分享，其概念亦提倡從外部資源獲得解決方案。在諸多案例中，格狀形態組織的員工，均被鼓勵針對棘手問題尋求非標準解決方案，甚至這意味著跳脫組織既有之規範。

最近美國加州聖伯納迪諾(San Bernardino)恐攻中的iPhone密碼事件，便是聯盟策略解決問題方式的例證，即便蘋果公司不願提供協助，聯邦調查局也有能力解開iPhone密碼。蘋果公司之所以如此，是擔心倘若提供所需協助，那麼政府便擁有解開全世界iPhone加密安全措施的鑰匙。[24]

2015年4月28日，美海軍自由號(USS *Freedom*)近岸作戰艦以及史坦尼斯號(USS *John C. Stennis*)航艦參加「獨立部署者認證演習」(Independent Deployer Certification Exercise)，執行水面作戰、防空、海上攔截作戰、指管/資訊作戰、指管通資系統情報與水雷作戰等課目。(Source:USN/Ignacio D. Perez)

當國際媒體對此事加以報導，並對此公開辯論之際，聯邦調查局接獲許多個人及公司來電，表示他們擁有破解密碼所需之工具。事實上，隨便一家公司就能破解密碼，並讓聯邦調查局從恐怖分子的手機中取得所欲資料。這個例子展現出資訊的多重力量；第一，政府沒有能力透過傳統方法，從私人企業獲得支援。第二，作為主要驅動力的媒體，讓問題受到注意並促成公眾討論，而此種方式有利於政府。對此正反雙方均有其論點，但應假設內部與自身挑戰應多到能激發出解決方案，無論對錯。此一案例的重點在於資訊的普及激發出解決方案，無論蘋果公司的觀點、聯邦調查局的職權，甚至公眾支持或反對聯邦調查局的意見亦然。如果資訊的力量能輕易主導上述案例的結果，那對作戰的長遠意涵又將是如何？美國政府現在即能針對組織採取行動，俾掌握資訊戰構想，並在瞬息萬變的資訊時代佔據有利位置、維持資訊優勢。

未來資訊戰的解決方案，亦需從各種不同背景的個人引進跨領域技能。在當今軍隊中，官兵一旦被認定具備某種專業，便很難將他(她)與該專業社群分離、進行跨社群運作，並同時維持向上動力。為提升資訊戰的計畫與執行成效，跨領域與多樣資訊相關能力事業，應是未來領導人最理

想的職涯發展。

當亞馬遜遇見美國政府

為駕馭資訊時代，並讓資訊戰協助美國在未來衝突中獲勝，應在美國政府內成立一個新組織。冷戰已不復在，美國新聞署也已裁撤多年；然而，時值俄羅斯持續測試其國力極限之際，成立一個新型的美國新聞署可能有其必要。正如烏克蘭、喬治亞共和國及愛沙尼亞的案例所揭示的經驗教訓，和打擊伊斯蘭國等恐怖團體所需，美國必須重新整頓資訊戰。不斷發展、瞬息萬變的環境，需要一個與當前階層式政府組織架構全然不同的組織，俾彈性處理且更加適應二十一世紀所面對的問題。此外，正當邁向資訊時代之際，我們的生活將與資訊系統更加密不可分且環環相扣。這種資訊環境，必然對美國政府與軍方，在所有作戰領域中與盟國、夥伴及敵人的互動方式，持續扮演關鍵角色。

為形塑此一環境以達成所欲目標，我們必須體認資訊戰的重要性，並採取行動以確保資訊戰構想能適切地與所有行動、作戰相結合，而非將之視為目標。我們亦須尋求各種創新方式，建立且

註釋

1. 「網狀網路是一種運用全狀拓樸(Full Mesh Topology)或部分拓樸(Partial Mesh Topology)分散式連結協議之區域網路(Local Area Network, LAN)、無線區域網路(Wireless Local Area Network, WLAN)，或虛擬區域網路。在全狀拓樸中，各個網路節點直接與其他節點連結。在部分拓樸中，某些節點與其他所有節點連結，但僅連結至交換最多資料的那些節點。」請參閱“Mesh NetworkTopology (Mesh Network),” *IoTAgenda.com*,available at <http://internetofthingsagenda.techtarget.com/definition/mesh-network-topology-mesh-network>.
2. 「機器學習」是電腦科學的一門分支，從人工智慧之「型態識別」(pattern recognition)與「計算學習理論」(computational learning theory) 研究發展而來。機器學習旨在建構及研究那些能從資料中學習並做出預測的各種演算法。
3. Richard M. Crowell, *War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare* (Newport, RI: U.S. Naval War College, 2010).
4. Ibid.
5. Joint Publication (JP) 3-13, *Information Operations* (Washington, DC: The Joint Staff, November 27, 2012), I-1.
6. Julie Hirschfeld Davis, “Hacking of Government Computers Exposed 21.5 Million People,” *New York Times*, July 9, 2015.
7. Brian Fung, , ow Many Cyberattacks Hit the United States Last Year?tersExpol Journal, March 8, 2013, 請參閱<www.nextgov.com/cybersecurity/2013/03/how-many-cyberattacks-hit-united-states-last-year/61775/>.
8. Ibid.
9. U.S. Information Agency, 請參閱<www.archives.gov/research/foreign-policy/related-records/rg-306.html>
10. Alvin A. Snyder, *Warriors of Disinformation: American Propaganda, Soviet Lies, and the Winning of the Cold War* (New York: Arcade Publishing, 1995).
11. Brian Nichiporuk, “U.S. Military Opportunities: Information-Warfare Concepts of Operation,” in *The Changing Role of Information in Warfare*, ed. ZalmayKhalilzad and John White (Santa Monica, CA: The RAND Corporation, Project Air Force, 1999), 181.
12. Eric A. McVadon, “Systems Integration in China’s People’s Liberation Army,” in *The People’s Liberation Army in the Information Age*, ed. James C. Mulvenon and Richard H.Yang (Santa Monica, CA: The RAND Corporation,1999), 請參閱

運用資訊作戰構想。我們的資訊戰專家，必須接受所需訓練與專業，以符合戰略指導之要求。作業人員必須將彈性與敏捷性，透過格狀組織架構融入道德之中，而此一架構就是邁向多領域事業的康莊大道。落實資訊戰所有需求之能力，必須以即時且簡明的方式養成，俾在最短時間內以最彈性方式執行各項作為。如果無法達成上述目標，我們便會被發展快速、瞬息萬變的資訊科技與資訊戰世界遠遠拋在後面，還可能無法有效地找到並打擊敵人作戰重心，諸如伊斯蘭國的作戰重心就是依賴資訊科技。要把握時間即刻落實那些業界已有的理念，並在無法跟上時代變遷的腳步前大力推動變革──透過美國政府內的一個永續且可重複的程序與組織。

作者簡介

William R. Gery美空軍少校現擔任美國空軍作戰司令部「空軍武器系統研判計畫」協調官。

SeYoung Lee少校現於南韓陸軍服役，就讀南韓陸軍總部軍史研究院。Jacob Ninas陸軍中校現擔任第704軍事情報旅分部主任。

Reprint from *Joint Force Quarterly* with permission.

<www.rand.org/content/dam/rand/pubs/conf_proceedings/CF145/- CF145.chap9.pdf>.

13. Sun Tzu, *The Art of War* (Oxford: Oxford University Press, 1963), 77.
14. Maria Snegovaya, *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare*, Russia Report 1 (Washington, DC: Institute for the Study of War, September 2015), 7, 請參閱<http://understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare>.
15. Ibid.
16. Ibid.
17. Dimitry Gorenburg, "Crimea Taught Us a Lesson, But Not How the Russian Military Fights," *War on the Rocks*, May 19, 2014, 請參閱<http://warontherocks.com/2014/05/crimea-taught-us-a-lesson-but-not-about-how-the-russian-military-fights/>.
18. LookingGlass Cyber Threat Intelligence Group, *Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare*, CTIG-20150428-01 (Reston, VA: LookingGlass Cyber Solutions, Inc., April 28, 2015), 請參閱<https://lookingglasscyber.com/wp-content/uploads/2015/08/Operation_Armageddon_FINAL.pdf>.
19. David Talbot, "Watching for a Crimean Cyberwar Crisis," *MIT Technology Review*, March 4, 2014, available at <www.technologyreview.com/s/525336/watching-for-a-crimean-cyberwar-crisis/>.
20. JP 5-0, *Joint Operation Planning* (Washington, DC: The Joint Staff, August 11, 2012), II-9.
21. *Report of the Defense Science Board Task Force on Strategic Communication* (Washington, DC: Department of Defense, January 2008), available at <www.acq.osd.mil/dsb/reports/ADA476331.pdf>.
22. *National Framework for Strategic Communication* (Washington, DC: The White House, 2010).
23. Cathleen Benko and Molly Anderson, "The Lattice that Has Replaced the Corporate Ladder," *Forbes.com*, March 16, 2011, 請參閱<www.forbes.com/2011/03/16/corporate-lattice-ladder-leadership-managing-hierarchy.html>.
24. Pierre Thomas and Mike Levine, "How the FBI Cracked the iPhone Encyption and Averted a Legal Showdown with Apple," ABC News, May 29, 2016, 請參閱<http://abcnews.go.com/US/fbi-cracked-iphone-encryption-averted-legal-showdown-apple/story?id=38014184>.