自選題類

美軍資訊作戰聯戰準則之演進

海軍中校　葉志偉

提　　要：

一、美軍自上世紀80年代起開始發展資訊作戰理論研究，同時著手資訊作戰能力建設，美軍資訊作戰思想開始萌芽。

二、美軍「聯戰準則—資訊作戰(JP3-13)」自1998年10月頒布之後，歷經數次海外軍事行動後，讓美軍在資訊作戰方面有更多的實戰經驗，也正好藉此修訂原本不足及需改進之處，使美軍更加重視資訊作戰在軍事行動中的應用。

三、美軍並非將資訊作戰作為一種獨立的戰爭形態實施，而是將資訊作戰中定義的各種能力貫穿於整場戰爭之中，大幅度的提高作戰能力，也顯示出美軍已將資訊作戰作為一種核心能力並應用於戰場之中。

關鍵詞：資訊戰、資訊作戰、美軍聯戰準則—資訊作戰(JP3-13)

壹、前言

資訊戰的概念，可追溯至1976年由羅納博士(Dr. Thomas P. Rona)任職於波音公司期間，向美國國防部高級官員馬歇爾的一篇研究報告「武器系統與資訊戰爭」中出現[1]；他認為美國商業資訊基礎設施已成為其經濟發展不可或缺的要件，但卻也是在平、戰時中，極易遭受到攻擊的目標。在80年代初美國對資訊戰的研究開始醞釀，提出了資訊戰鬥、資訊戰爭、電腦病毒對抗、網路戰等新觀念，從此美國資訊作戰思想開始萌芽[2]，但直到1991年波灣戰爭後，美軍才肯定與相信：「資訊時代正在改變著軍事，並將從根本上改變戰爭的形態」[3]，同時用此一作戰行動證明他們的軍隊是一支無法戰勝的力量。從此之後，美國的現代化軍隊與作戰方式成為世界上其他國家的範例，並且向世人展現了戰爭的新面貌及一種全新的作戰力量，而其他國家在美國所進行的軍事行動背後，亦可清楚體認到一個事實，就是資訊作戰已不再僅僅只是輔助戰爭或軍事行動的行為，或是塑造戰場環境的工具；事實上，它本身已成為一種獨特的戰爭形式，在許多方面

註1：轉引自里・阿米斯德(leigh Armistead)，《資訊作戰--以柔克剛的戰爭》(國防部譯印)註11。

註2：里・阿米斯德(leigh Armistead)，余佳玲譯，《資訊作戰－以柔克剛的戰爭》(Information Operations:Warfare and the Hard Reality of Soft Power)(臺北：國防部，2008年8月)，頁31。

註3：蔡輝榮、吳宗禮，〈面對資訊作戰之準備、發展與落實〉，《資通安全專論》，2007年。

，發展出其獨特的目標、手段與工具，也就是已逐漸地形成一種新的「類型作戰」[4]。

貳、資訊作戰的定義

主管美國指管通情電腦業務的前國防部助理部長沛吉(Emmet Paige)對資訊戰的定義：「為獲得支持國家軍事戰略所需之資訊優勢，美國除藉諸般手段以癱瘓對方的資訊系統與情報作業能力之外，更應妥善採取防衛與反制措施，以鞏固其情報作業能力與資訊系統安全」。其後，馬格席格(Daniel E. Magsig)認為美國陸軍對資訊戰的定義除了攻擊和防衛資訊戰外，更應該整合民間和軍方資訊系統，不該僅從國家安全和軍隊觀點來定義資訊戰[5]。

上述定義都在1990年代中期前被美國軍方所提出[6]，但都屬於較狹義的定義，其多半侷限在軍隊戰時的「戰術」或「作戰」層面上，運用資訊環境和工具進行攻擊和防衛的行動。然而，對於「資訊戰」的定義還是缺乏完整和一貫性。隨著資訊科技影響軍隊層面加深，「資訊作戰」乙詞的出現，逐漸取代「資訊戰」。

到了90年代中後期，美軍逐漸以「資訊作戰」來取代「資訊戰」一詞，並釐清兩詞彙之間在理論上的差異。美國國防部參謀聯席會議(Joint Chiefs of Staff)在1998年給予「資訊作戰」非常完整和清晰的定義：

圖一　資訊作戰關係時序圖

資料來源：Joint Pub3-13, Joint Doctrine for Information Operations, 9 October, 1998, page I-4, Fig1-2.

「包括戰時和平時任何用來影響敵方資訊系統、資訊作戰應用在所有作戰步驟、所有軍事行動範圍和每一層級戰爭。……資訊作戰是聯合軍種作戰指揮司令官達成和維持資訊優勢所需決定性聯合作戰的關鍵因素」[7]。

但是，對於資訊作戰的定義，在現行的各項準則教範中仍存在著許多模糊甚至相左的情形，一般人對於美軍「資訊作戰(Information Operations)」與「資訊戰(Information Warfare)」[8]間的差異與分別有不同的認知，因此首先要釐清的問題就在於：資訊作戰與資訊戰何者為大？

就美軍的論點而言，從美軍聯戰準則3-13資訊作戰1998年版(JP3-13 Joint Doctrine for Information Operations)中，資訊作戰(IO)的定義為「為影響敵方資訊及資訊系統，同時保護己方資訊和資訊系統所

註4：郁瑞麟，〈資訊作戰定義探討與釋疑〉，《國防雜誌》，第24卷，第3期，2009年6月，頁50。
註5：Daniel E. Magsig，國防部史政編譯局譯，《資訊時代的資訊戰》(臺北：國防部史政編譯局，1997年)，頁250-252。
註6：1992年12月21日，《國防部指令3600.1－資訊戰》、1993年3月8日，《第30號參謀首長聯席會會議主席政策備忘錄「指管戰」(Command and Control Warfare)》。
註7：Joint Chiefs of Staff, Joint Pub 3-13, Joint Doctrine for Information Operations(Washington, DC: Joint Chiefs of Staff, 1998),p.7.
註8：依循我國軍翻譯的習慣來說，Operations翻譯為作戰，而Warfare則翻譯為戰。

採取的各種行動。」[9]而資訊戰(IW)則是定義為「當危機或衝突發生時，為了達到或促成對敵的特定目標，所進行的資訊作戰。」[10]因此，有不少軍事理論家認為，資訊戰是資訊作戰失敗之後所採用的作戰方法，在圖一中可以很清楚看出資訊作戰(藍色)與資訊戰(紅色)的相互關係，同時資訊作戰還包含了資訊確保(Information Assurance)與特種資訊作戰(Special Information Warfare)。

另一方面來看，資訊戰是達成資訊作戰特定目的的行動作為，兩相比較之下，後者在時間上跨越平時和戰時，戰略思想上包含戰略層面(Strategic)的嚇阻戰爭、摧毀大規模毀滅性武器(Weapon of Mass Destruction, WMD)、維護和平行動(Peace)和保護全球指管系統(Global Command and Control System, GCCS)等；在戰術層面(Tactic)上係指摧毀敵方指管和防空系統；於作戰層面(Operation)上，則以發現敵方的軍事欺騙、孤立敵方政府和軍隊指揮官與其他部隊聯繫為主要目的；故「資訊戰」包含的要素大多與實際戰鬥中執行作戰之行動有關。而「資訊作戰」除了上述要素外，更包括整合的軍事思想與行動[11]，包含軍事組織變革、戰略、戰術和作戰層面，顯然比「資訊戰」更能描述當代軍事資訊科技的運用層面。不僅已超越軍事和非軍事目標，也不侷限於平時和戰時之特性；因此，資訊戰可說是資訊作戰的一部分。而從圖二中亦能看出資訊作戰與資訊戰的範圍，其中資訊戰僅著重於軍事衝突中的攻擊與防禦的作戰行動機制；然而資訊作戰則涵蓋軍事競爭下，國家於經濟、政治或資訊環境等基礎建設的整備性，這與前述提及的概念具有一致性。

圖二　資訊作戰概念示意圖

資料來源：里・阿米斯德，《資訊作戰－以柔克剛的戰爭》(臺北：國防部，2008年8月)，頁30，圖表1-7。

參、美軍聯戰準則3-13資訊作戰1998年版

1998年10月，美軍參謀長聯席會(Joint Chiefs of Staff，JCS)頒布的聯戰準則—資訊戰(Joint Pub 3-13, Joint Doctrine for Information Operations)對資訊戰給予定義，同時也為美軍聯合作戰中實施資訊戰提供了準則基礎，而在這之前美軍也經歷過一段各軍兵種、專家對資訊戰概念各自表述的混亂時代，但美軍很快意識到統一資訊戰概念的重要性。因此美軍從高層以國防部指令的方式律定資訊戰的一些基本術語，並要求各軍種後續發展的準則、教令不得與這

註9：同註7，p.7.
註10：同註7，p.23.
註11：同註2，頁29-30.

些指令相違背。而此之後，美軍也多次對資訊戰的定義進行修訂。

占有「資訊優勢」意味著能夠不間斷的實現對資訊流的收集、處理與分發，同時也能阻止敵方進行此類行動，在JP3-13中對資訊優勢的定義堪稱完美，其核心思想是「己方占據不間斷的資訊流，並切斷敵方的資訊流」，並由資訊系統、相關資訊與資訊行動等3個部分組合而成。

所謂的資訊作戰是影響敵方的資訊與資訊系統，同時保護己方的資訊與資訊系統所採取的行動，包括了攻擊型資訊作戰與防禦型資訊作戰兩個主要子部分以及相關行動[12]。

攻擊型資訊作戰是指通過干擾敵方決策者(或指揮官)，以期達到或促成特定目標的行動，其在軍事行動中的適用範圍相當廣闊，涵蓋各層級(戰略、戰役及戰術)戰爭，它在和平時期與衝突的開始階段都能發揮更大的作用，包括了「作戰安全(Operations Security，OPSEC)」、「軍事欺騙(Military Deception)」、「心理戰(Psychological Operations，PSYOP)」、「電子戰(Electronic Warfare，EW)」、「實體攻擊/摧毀(Physical Attack/Destruction)」、「特種資訊作戰(Special Information Operations，SIO)」及「電腦網路攻擊(Computer Network Attack，CNA)」；相關能力則是包含了公共事務(Public Affairs，PA)及公民事務(Civil Affairs，CA)活動，這兩項也是資訊作戰中的主要分支[13]。

防禦型資訊作戰是指通過整合與協調政策、程序、作戰、資源及技術，來保護己方的資訊與資訊系統；而由於聯合部隊的作戰和目標的達成，依賴於資訊與資訊系統，因此他們必須確保對資訊與資訊系統進行必要的保護和防衛，包括了「資訊確保(Information Assurance，IA)」、「作戰安全(OPSEC)」、「實體安全(Physical Security)」、「反欺騙(Counterdeception)」、「反宣傳(Counterpropaganda)」、「反情報(Counterintelligence，CI)」、「電子戰(EW)」及「特種資訊作戰(SIO)」[14]。

然而防禦與攻擊是相輔相成的，因此攻擊型資訊作戰可以透過「資訊環境保護」、「偵測攻擊」、「能力恢復」及「應對攻擊」來支撐防禦型資訊作戰[15]；而鑒於兩者之間的緊密聯繫，整合所有的攻擊與防禦作戰因素顯得至關重要，即便這兩者在理論上是可以分別運用的，但實際上仍必須共同策劃與執行；另一方面也定義了「特種資訊作戰」，但由於其敏感性、作用力與對美國國家安全的潛在影響，這種資訊作戰方式必須經過詳細審查及一系列的批准才得以執行[16]。

根據1998年版本的JP3-13，資訊戰只被定義為在危機或衝突時期，針對一個或多個特定對手，並為實現特定目的而採取的一系

註12：同註7，p.I-2、I-9-10.
註13：同註7，P.I9-10、PII-2-7.
註14：同註7，P.I10、PIII-1-7.
註15：同註7，PIII-7-15.
註16：同註7，P.I-11

列作戰行動，因此資訊戰只是資訊作戰的中的一部分，即在危機或衝突時期採取的常規行動，在和平時期則不提資訊戰概念。但事實上，我們卻是一直處於資訊戰的狀態當中，美國及其他許多國家的資訊空間都是被不斷持續攻擊的目標，因此也被迫進入長期防禦的狀態，儘管潛在的敵人無法預知，但仍必須落實各樣的防禦措施，因為我們正處於一個和平、危機與衝突交織的時期。

因為資訊作戰具有可預測的威懾特性，其貫穿和平與和平恢復時期，同樣在衝突時期可使敵方對其自身的初步行動猶豫不決，而資訊作戰的終極目標是持續干擾敵方或是潛在的敵人，以制止他們威脅美國國家安全利益的行動，然而1998年版本的JP3-13很顯然並未考慮到恐怖主義的威脅，近20年來，各類組織對美國境內網路的攻擊驟增。有些攻擊來自於個人、有些則是激進分子、外國軍事單位、恐怖分子，甚至於國家。從資訊的觀點來看，大量病毒、世界各地的重大軍事行動，及2001年的911事件，這些事件本身都凸顯出不僅美國國防部，甚至美國政府在面對這些新形態戰爭時的脆弱無力。

在1998年版本中的最後一章則是提到資訊作戰的訓練(Training)、演習(Exercises)、模組化(Modeling)及模擬(Simulation)。在資訊作戰的訓練中區分為攻擊型及防禦型的訓練，前者應該包含所有可能及潛在可能的一體化攻擊能力用以引導資訊作戰，而後者則是應該包含所有可能的一體化防禦能力[17]。在聯合演習部分則是應納入資訊作戰適當的範圍及演習的持續時間，並包含資訊作戰的三種訓練方式：獨立執行(資訊作戰是用來影響敵方的唯一戰略)、被支援性(資訊作戰是一種被其他聯合作戰所必須支援的工作)及支援性(在傳統戰役中資訊作戰可用來做為武力的放大器)[18]。

在模組發展的最早執行階段中，資訊作戰應被所有的計畫、模組化及模擬納入，對其他的作戰區域而言，也只有資訊作戰的模組化與模擬必須被適當的整合[19]。最後在附錄A的部分則是補充了資訊作戰指導，惟此部分美軍仍列為機密，無法得知[20]。

肆、美軍聯戰準則3-13資訊作戰2006年版

2006年2月13日，JCS發布了被稱為「資訊作戰」的新版聯戰準則(JP3-13，Information Operations)。此版本與1998年版本最大的不同之處在於重新對「資訊作戰(IO)」給予定義：完整的運用電子戰(EW)、電腦網路作戰(Computer Network Operations，CNO)、心理戰(PSYOP)、軍事欺敵(Military Deception，MILDEC)及作戰安全(OPSEC)等能力並配合特定的支援與相關能力，用以影響、瓦解、破壞或奪取敵人人工及自動決策，並且保護己方[21]，另一方面則刪除了「資訊戰(IW)」的說法，同時不再將「攻擊型資

註17：同註7，p.VI-1.
註18：同註7，p.VI-2.
註19：同註7，p.VI-4.
註20：同註7，p.A-1.
註21：Joint Chiefs of Staff, Joint Pub 3-13, Information Operations(Washington, DC: Joint Chiefs of Staff, 13 Feb, 2006), p.9.

圖三　標示五大核心能力(電子戰、網路戰、心理戰、軍事欺敵及作戰安全)、支援能力(資訊確保、實體安全、實體攻擊、反情報及戰鬥照相機)與相關能力(軍民作戰、公共事務及公共外交)的聯戰行動、目標、手段、主計畫整合過程及權責歸屬等相關事項

資料來源：Joint Publication 3-13,Information Operations,13 Feb,2006,page I-7, Fig1-3.

訊作戰」與「防禦型資訊作戰」有所分割，並認為在資訊作戰的行動中，通常同時包含了攻擊及防禦的兩個面向，不易清楚的分割成兩個區塊，於是決定不再分類探討[22]。

在2006年版本的資訊作戰聯戰準則將資訊作戰劃分成五大核心能力：心理戰、軍事欺敵、作戰安全、電子戰及電腦網路作戰，結合這五種能力，再加上支援及相關能力，並透過使聯合部隊在資訊作戰中自由作戰的方式來提供聯合部隊指揮官影響敵人及其他特定目標的重要手段；支援能力則包括資訊確保(IA)、實體安全(Physical Security)、實體攻擊(Physical Attack)、反情報(CI)及戰鬥攝影(Combat Camera)，這些作為會直接或間接環繞在資訊環境中並造成有效的資訊作戰，除了應與核心能力整合與協調外，也可用在更多的其他目的；相關能力則區分為：公共事務(PA)、軍民作戰(Civil Military Operations，CMO)及公共外交(Public Diplomacy)[23]。相較於1998年版本的六種能力(作戰安全、軍事欺騙、心理戰、電子戰、實體攻擊/摧毀及電腦網路作戰)劃分的更加明確與清楚[24]，從圖三中即可明顯看出。

而在電腦網路作戰中區分為攻擊、入侵與防禦行動，其中，網路攻擊包括了癱瘓、中斷、延遲、摧毀資訊與(或)資訊系統；網路入侵則包含了收集、監測及編造資訊；網路防禦則是由保護、偵測與恢復等組成，這是首度在公開的資料中將網路戰分類，但是有關細節部分仍列為機密[25]。

在2006年版本中，我們可以看出美軍對非軍事資源利用的重視，資訊作戰行動不能在真空中進行，它需要一個環境來操作，而此一環境就是美軍所提出的「資訊環境」的概念，即軍事活動與資訊作戰必須在三維(Dimension)空間中進行。實體維(Physical Dimension)由指揮控制系統、基礎設施、網路與電腦組成；資訊維(Informational Dimension)則是進行資訊收集、加工、存儲、發布、顯示與保護的空間，也就是資訊駐留與流動的空間；認知維(Cognitive Dimension)則包含決策者與目標對想思想的空間[26]，在這三種維度中，沒有任一個維度是由軍

註22：同註4，頁54。
註23：同註21，p.10.
註24：同註4，頁54。
註25：同註21，p.II-4-5.
註26：同註21，p.I-1-2.

事資源單獨形成的，相對而言，非軍事資源則是占有重要位置；另一方面，資訊作戰中相關能力的公共事務與軍民作戰也充分顯示出美軍在資訊作戰行動中對非軍事資源的利用。美軍認為公共事務有助於資訊作戰行動的完成，公共事務對聯合部隊獲取及保持資訊優勢是至關重要的。在當今資訊化的時代，廣大民眾能接觸到的資訊量越來越多，而且在資訊環境中實施軍事行動也越發頻繁，這使得軍民作戰對達成資訊作戰目的的重要性也在增加。

綜觀近25年來美軍所發動的軍事行動，從1991年的波灣戰爭，到1999年的科索沃戰爭，再到2001年的阿富汗戰爭，直到2003年的伊拉克自由行動，無一不是由美國發起的，但美國並非獨立作戰，在每場軍事行動中，都有盟國並同作戰。在1998年版本中，就明確的表示資訊作戰的主要目標是使美國及其盟國獲取並保持資訊優勢；到了2006年的版本更特別增加了一個章節來說明在資訊作戰中多國部隊的注意事項。美軍認為，各盟國有不同的資訊戰概念，且某些國家有完整的教則、程序及能力來計畫及執行資訊戰，因此擔任多國聯合部隊指揮官必須解決各國資訊作戰的計畫與聯盟的目標與計畫的可能衝突。並且儘早將所有盟軍及聯合部隊的資訊作戰計畫整合在一起是非常重要的，而此一整合包含釐清盟軍的資訊作戰目標，瞭解其他國家的資訊作戰，以及打算如何執行資訊作戰，同時可以早期發現聯合部隊的弱點及對敵人可能運用這些弱點的對策[27]。

除了新增第六章來說明聯盟資訊作戰的注意事項外，另外新增的一個章節是第三章—資訊作戰中的情報支援。在資訊環境的軍事行動之前情報支援是可以事前計畫的，同時必須蒐集、分析動態資訊環境的當前狀態，並提供給指揮官及其參謀；同時為瞭解敵人或其他目標群組(Target Audience，TA)的決策過程，並決定達成作戰目標所需的適當能力，指揮官及其參謀必須有即時的資料，這些資料包含了資訊環境中的實體、資訊及認知特性，以及對現行資訊作戰行動的評估。而在計畫資訊作戰時的情報考量時必須有所認知：情報資源有限、蒐集行動受到法律限制、支援資訊作戰的情報通常需要很長的前置時間、資訊環境是動態的、資訊環境的特性會影響情報等五大項[28]。

最後則是新增了附錄C論述通信系統如何支援資訊作戰[29]。

伍、美軍聯戰準則3-13資訊作戰2012年版

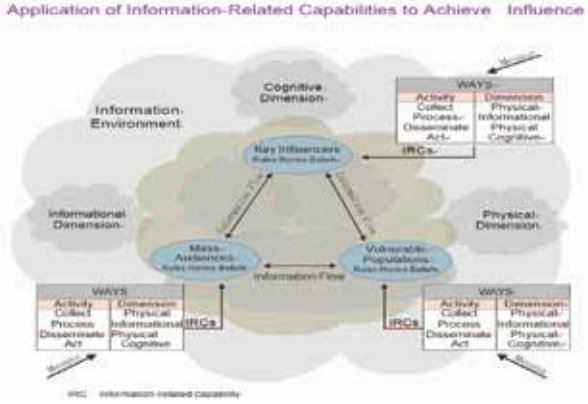
JCS在2012年11月27日發布了JP3-13資訊作戰的修訂版本(下稱2012年版)，在此版本中對資訊作戰相關核心概念作了新的闡述，並且首次提出了「資訊相關能力(Information-Related Capabilities，IRCs)」的概念[30]，明確的律定在資訊作戰中各執行單

註27：同註21，p.15、p.VI-1-4.
註28：同註21，p.11-12.
註29：同註21，p.C-1-2.
註30：Joint Chiefs of Staff, Joint Pub 3-13, Information Operations(Washington, DC: Joint Chiefs of Staff, 27 Nov, 2012),p.3.

位的職能分工與需考慮的法律因素，規範了資訊作戰計畫流程及主要任務，並對多國聯合背景下，如何實施資訊作戰與協調作了闡述，同時對作戰能力集成、組織管理建設、計畫與執行流程等諸多方面提供了更貼近現實、更具有執行力的準則以供各級人員運用[31]。

2012年版的JP3-13主要區分為「資訊作戰」、「資訊環境」及「資訊相關能力」等核心概念，並且修改了對資訊作戰的定義－「在軍事行動中，綜合運用資訊相關能力，與其他作戰方式共同作用、影響、擾亂、破壞或竄改敵人或潛在敵人的決策，同時保護己方」[32]；同時仍然沿用2006年版本中對「資訊環境」的定義[33]，但在這三個領域的內涵表述上更為具體及全面。

接著是放棄2006年版本中對資訊作戰能力的層次劃分，將重新確定的14種應用於資訊作戰的能力，統一稱之為「資訊相關能力」，並將其定義為「對資訊環境的三個領域產生影響的工具、手段或活動」。這些能力包括：戰略通聯(Strategic Communication)、聯合跨機構協調小組(Joint Interagency Coordination Group)、公共事務(Public Affairs)、軍民聯合行動(Civil-Military Operations)、網路空間作戰(Cyberspace Operations)、資訊確保(Information Assurance)、太空作戰(Space Operations)、軍事資訊支援作戰(Military Information Support Operations)、情報(Intelligence)、軍事欺騙(Military Deception)、作戰安全(Operations Security)、特種技術行動(Special Technical Operations，STO)、聯合電磁頻譜作戰(Joint Electromagnetic Spectrum Operations，JEMSO)及關鍵領導交戰(Key Leader Engagement，KLE)等[34]。



圖四　Application of Information-Related Capabilities to Achieve Influence

資料來源：Joint Publication 3-13,Information Operations,13 Feb,2012, page I-7, Fig1-4.

最後，則是首次出現的「影響資訊作用流程框架(Information-influence relational framework)」的概念，用以描述資訊作戰的作用原理，即透過資訊相關能力的應用、融合與同步，用以影響、破壞和竄改目標群組的決策，以達成作戰目標，這一框架包含了資訊(Information)、數據(Data)、知識(Knowledge)、影響行為或能力(In-

註31：同註30，p.3、p.7-12.
註32：同註30，p.7.
註33：同註30，p.7-8.
註34：同註30，p.II-5-13.

fluence)、方法(Means)、手段(Ways)、資訊相關能力(IRCs)、目標群組(TA)等諸般因素[35]，而圖四便可看出如何應用資訊相關能力以達成影響的目的。

而為了將資訊作戰貫穿於聯合作戰的各個階段，以及達成作戰目標，必須將資訊相關能力與其他作戰行動與手段綜合交互使用，為此，在2012年版本中，專門用一個章節來說明資訊作戰的組織與協調，並強調所有資訊相關能力的綜合運用，而在此章節中表達最重要的一個觀念是一達成資訊作戰目標的關鍵不在於擁有多少種能力，而在於這些能力的運用；在制定作戰計畫時，必須全面考量所有資訊相關能力並綜合使用[36]。

在第三章則是明確律定資訊作戰中，各相關指揮管理機關、人員及其職責，並闡述在資訊作戰計畫在制訂時必須考慮的法律因素。因此，制定聯合資訊作戰計畫的人員應就四個面向法律顧問進行諮詢：「資訊相關能力的實施是否會被視為故意行為」、「其他國家的安全、隱私或資訊交換；犯罪或其內部事務的法律是否適用」、「有無適用於資訊相關能力的國際條約、協議或是敵方認可的慣例」以及「聯合部隊應怎樣與美國情報機構和其他跨機構實體進行互動或得到其支持」等[37]。

在2006年的版本中雖已有提到多國聯合部隊在執行資訊作戰時，所應注意的事項，但到了2012年的版本時，更進一步的律定了在多國部隊聯合作戰中，資訊作戰的協調流程、機構建設需求，計畫制定與指揮參謀人員組成等內容。在聯合作戰中，多國聯合部隊的指揮官必須解決各國家間可能會出現的衝突與矛盾，以形成統一、可行的資訊作戰；另一方面，則是要求美軍在擔任多國部隊指揮官時，應將其他國家軍隊的相關資訊人員及領域專家，一併納入制定資訊作戰計畫，並依據美軍及其他國家部隊的準則、需求、資源及資訊相關能力來進行訓練，但也應考慮各個國家的特殊需求與不足之處，以充分利用所有可用技術與能力[38]。

陸、美軍資訊作戰聯戰準則的演進

美軍自1991年第一次波灣戰爭後，正式打響了資訊作戰的第一砲，除了向世界各國展示一種新形態的作戰力量與方式，也正式宣布了資訊作戰時代的到來，從1992年的《國防部指令3600.1－資訊戰》及1993年的《第30號參謀首長聯席會會議主席政策備忘錄「指管戰」》開始，可以發現美軍逐步正視資訊作戰在軍事行動中的重要性。也正因如此，各軍種亦開始發展適用的資訊戰教範、準則。到了1998年，JCS在綜合了各軍種資訊作戰的準則條文後，正式頒布了第一本資訊作戰的聯戰準則，這本聯戰準則是美軍在資訊作戰準則發展的一個重要里程碑，也確定了聯合部隊該如何運用資訊作戰以支持美

註35：同註30，p.I-3-5.
註36：同註30，p.II-1-5.
註37：同註30，p.III-3.
註38：同註30，p.V-1-5.

軍軍事戰略，同時也為指導聯合作戰中的資訊作戰提供了理論基礎。

8年之後的2006年，美軍再次頒布了新版本的資訊作戰聯戰準則，而在這8年中，美軍經歷了1999年的科索沃戰爭、2001年的阿富汗戰爭及2003年的伊拉克自由行動，也讓美軍在資訊作戰方面有更多的實戰經驗，也正好藉此修訂原本不足及需改進之處。從2006年到2012年間，雖然美軍僅在2011年有較大型軍事行動(利比亞戰爭)，但其在全球的駐軍及零星的軍事衝突，使美軍更加重視資訊作戰在軍事行動中的應用。而在這些戰爭中可以看出，美軍並非將資訊作戰作為一種獨立的戰爭形式實施，而是將資訊作戰中定義的各種能力貫穿於整場戰爭之中，大幅度的提高美軍的作戰能力，也顯示出美軍已將資訊作戰作為一種核心能力並應用於戰場之中。

自1998年頒布了第一本有關資訊作戰的聯戰準則到2012年最新版本的公布，在這三個版本之間，2006年的第二版本與1998年的第一版本有最多的不同與最大幅度的修訂。首先是對「資訊作戰」重新給予定義，並且刪除了「資訊戰」的說法，同時不再將資訊作戰分割為「攻擊型」與「防禦型」，另一方面則是加入了一個章節來說明資訊作戰中多國部隊的注意事項。到了2012年的版本，再次重新定義「資訊作戰」，並首次提出「資訊相關能力」與「影響資訊作用流程框架」的概念，前者是將2006年版本中對資訊作戰能力的層次劃分，統合為14種應用於資訊作戰的能力，後者則是透過資訊相關能力的應用、融合與同步，用以影響、破壞和竄改目標群組的決策，以達成作戰目標。

與1998年及2006年版本相比，2012年版本重新修訂資訊作戰的核心概念，並提出新的概念與理論，並進一步闡述資訊相關能力的綜合運用及貫穿作戰全程的全方位協調，在各方面呈現出新的特點與思維，使得資訊作戰更具有實用性及可操作性。而此一重要的資訊作戰聯戰準則，有以下數點特點：

一、對資訊作戰能力涵蓋範圍的界定更爲科學

長久以來，對於如何界定資訊作戰能力涵蓋範圍就是困擾美軍的一個重要問題，在2006年版本中，將應用於資訊作戰的13種能力劃分為三個層次，也就是核心能力、支援能力及相關能力。但這種層次劃分一直缺乏令人信服的標準，也很可能會有能力發展不均衡的情形，但事實上，許多支援能力或相關能力在資訊作戰的應用中卻常能發揮出意想不到的重要作用。而2012年版本中取消了這種層次劃分，並將其統一稱為「資訊相關能力」，其用意在避免人為區分各種能力的主從或重要性，有利於所有能力的綜合運用，發揮出最大效用。同時還特別說明，這列舉的14種能力並無法囊括可用於資訊作戰的所有能力[39]，這表示美軍已充分意識到隨著未來科技的演變與作戰需求的發展，資訊相關能力的範疇會持續的擴展與變化。

另外，「資訊相關能力」的概念也避免出現「作戰」字眼，也在在顯示美軍日益重

註39：同註30，p.II-13.

視資訊作戰的軍民界線模糊的特點，同時也是進一步強調「軍隊與政府、民間共同進行協調，綜合運用所有資訊相關能力以實現作戰目標」的重要依據。

二、對資訊作戰作用條理的描述更爲清晰

近年來，美軍已經意識到在資訊環境中，難以保持絕對的技術優勢，因此，正逐步從「發展技術能力」轉變為「技術能力的綜合應用」，強調在資訊作戰中，重要的不是擁有能力與技術，而是在於如何綜合運用。故在2012年版本中創新的提出了「影響資訊作用流程框架」的概念，此一概念定義了資訊的目標群組是「被選擇施加影響的個體或群體」[40]，此外這框架概念最重要的功能在於直接說明了由「選擇目標群組，到確定施加影響的方法，再到應用資訊相關能力實現影響」的連續過程中，涉及哪些要素與條件，要採取何種方法與手段，才能使資訊相關能力發揮整體效用[41]。更重要的是，這框架概念的應用，可為資訊作戰的計畫與執行提供更具針對性的理論依據，有效提升美軍資訊相關能力的作用效能。

三、對資訊作戰協調的要求更加全面

在2012年版本中用了較大的篇幅來說明，在作戰過程中需要協調的內容以及怎樣協調，除了對2006年版本中有關的內容作了保留或調整，還增加了對資訊作戰與其他作戰形式的協同要求[42]，無論在協調的深度及廣度都有明顯的提升，使得「全程、全方面的協調」成為2012版本最為突出的特色之一。

在這版本中不僅說明了每一種能力的定義與功能，還對各種能力應用過程中與其他能力的協調提出了具體要求，詳細的描述協調範圍與方法，更進一步強調資訊相關能力綜合運用的重要性。接著依據相關法規，在明確資訊作戰主要職能單位與人員職責的基礎上，詳細說明了各單位與人員的指揮協調關係，使其職責確定更為明瞭。在對「資訊作戰」的定義從2006年版本中「與其他支持及相關能力的共同作用」修訂為「與其他作戰形式共同作用」，進一步凸顯出資訊作戰必須與其他類型作戰協同執行的本質要求，並要求儘早計畫、協調及統一各類作戰行動，以有效同步資訊相干能力，而這也是首次明確要求資訊作戰必須與其他作戰行動的協同一致。

四、對資訊作戰計畫的指導更具有操作性

相較而言，在資訊作戰計畫這一部分是變化最大的，雖說2006年版本也對資訊作戰計畫的制定流程有所論述，但並未充分考慮資訊作戰在各方面的協調，而在2012年版本中，將資訊作戰計畫作為聯合作戰計畫不可分割的一部分，並從6個方面來說明為何資訊作戰計畫考量的重點[43]。同時也詳細律定了，在聯合作戰計畫制定的初始階段(Planning Initiation)、任務分析(Mission

註40：同註30，p.3.
註41：同註34。
註42：同註30，p.IV-1-12.
註43：同註30，p.IV-1-2.

Analysis)、行動方針發展(COA Development)、行動方針分析與作戰模擬(COA Analysis and War Gaming)、行動方針比較(COA Comparison)、行動方針批覆(COA Approval)及計畫或命令發展(Plan or Order Development)等7個步驟中[44]，同步進行的資訊作戰計畫所涉及的具體行動，以及在資訊作戰中與其他作戰行動的相互關係。

柒、結語與建議

美軍近年來所頒布的一系列戰略指導，愈加強調綜合運用外交、資訊、軍事及經濟手段，處理面臨的危機與衝突，並且要求未來不再參與曠日持久、大規模、消耗性的軍事行動，改以更靈巧、更講求效益的攻擊方式。這一戰略思維的轉變，必將對未來美軍作戰形態運用的著重點產生重要的影響。資訊作戰「不戰而屈人之兵」的本質，無疑將使其成為美軍未來軍事行動所倚重的重要作戰方式之一。

再者，美軍認為，要在資訊環境中綜合運用外交、資訊、軍事及經濟能力，處理全球範圍內的各種危機，對即時安全傳輸、接收、存儲及處理資訊能力需有極高的要求。當然，各類敵人亦同樣會在資訊環境中運用這些能力，圖謀資訊優勢。而作為戰略環境的重要組成部分，資訊環境正隨著戰略環境的不斷變化而變化，再加上資訊技術的日新月異，因此資訊作戰的內涵也不斷拓展，可供選擇的資訊作戰方式也在增加。

另一方面，新形態作戰概念的出現，也需要資訊作戰理論的更新。近年來，美軍先後提出的「網路空間戰(Cyberspace Warfare Operations，CWO)」、「空海一體戰(Air Sea Battle)」及「聯合作戰介入(Joint Operational Access Concept，JOAC)」等新型作戰概念，其核心思想在許多方面都與資訊作戰緊密相關，甚至重合。但美軍內部一度出現「網路空間戰應包含資訊作戰」、「資訊作戰已經過時」等爭議，且「空海一體戰」及「聯合作戰介入」也對資訊作戰提出了新的需求，「資訊作戰理論是否需要調整」、「如何與新型作戰方式相互協調」等問題也都需要有權威性的共同準則教範予以律定。

而在近年來對中東及北非多個國家內部衝突的介入行動中，美軍也頻頻的利用資訊作戰手段，間接影響了各國的政權更迭或對其執政當局造成巨大威脅，這些手段包含使用推特(Twitter)、臉書(Facebook)等網路工具及電視、報紙與廣播等傳統媒介，網路戰、媒體戰及心理戰在一定程度上影響了戰爭走向。在這些軍事行動中，美軍不僅驗證了傳統的資訊作戰手段，還融入了「戰略通聯」等多種新形態手段，進一步豐富與完善其資訊作戰的能力，也為2012年版資訊作戰聯戰準則的修訂提供了實踐基礎。

在探討完美軍資訊作戰的演進之後，對比我國的資訊作戰仍有許多可以再精進之處，以下提出數點建議，提供本軍未來資訊作戰發展的參考：

一、正確認識資訊戰

註44：同註30，p.IV-2~7.

資訊戰做為資訊化作戰條件下的熱門名詞經常被引用，因此資訊戰、資訊作戰及資訊化作戰也常常被混為一談。從美軍對資訊作戰的應用中可以看出，資訊作戰不僅僅是一種戰爭手段，更是一種作戰能力。資訊作戰不是獨立存在的一種戰爭形態，而是貫穿於戰爭當中的各種與資訊相關能力的展現。因此美軍強調，資訊作戰是各種資訊相關能力的整合，唯有將這些能力整合並與其他作戰行動相互配合，才能達成作戰目的，但可惜的是，部分指揮官仍然抱持傳統的作戰思維，在作戰前根本從未思考過「資訊作戰」此一選項。

二、制定明確完善的資訊戰準則

從1998年版本的本軍中譯版本中，就可以發現對資訊戰及資訊作戰的翻譯相當混亂且未一致，相當容易造成讀者曲解相關含義，另方面，在此之後對於美軍2006年及2012年版本也並未再有中譯本可供參考運用，在現行教範中雖有《國軍資訊戰要綱》，但後續卻未再有發展，相較美軍而言，自1992年起幾乎每年都對資訊作戰有不同的見解並修訂發布。因此，首先應再次檢視我國資訊作戰的相關準則教範，對部分不合時宜的內容加以調整及編修，並作有系統的延伸，使資訊作戰的概念能與現今科技及實際作戰相結合，才能有效發揮資訊作戰的功用。

三、重視資訊作戰人才的培養

相較於其他形式的戰爭，資訊作戰對於人員的能力要求較高，因此培養資訊作戰的人才極其重要。而這些人員應具有高度的學習能力，以適應快速、更新的各種資訊技術，同時要有創新能力，以應對敵方資訊技術的不斷創新。另一方面，真正能結合軍事與學術領域的專業軍官在國軍資訊作戰領域中顯得非常欠缺，這也是國軍極需培養人才的重點。

資訊作戰在現代戰爭中佔有相當的重要地位，提高軍隊資訊作戰能力，是打贏未來高科技戰爭的重要保障，在資訊化高度發展的今天，戰爭的目的已經不僅僅是對敵方進行物理摧毀，而是透過資訊攻擊，征服敵方領導者的意志，最終達到控制敵方的目的。因此將資訊作戰從一個熱門名詞轉變為務實具體的作戰能力，是打贏未來戰爭的必經之路！

作者簡介：

葉志偉中校，海軍官校91年班，國防大學海軍指揮參謀學院103年班，現服務於國防大學海軍指揮參謀學院。