數據鏈路整合運作之安全性探討

作者／資訊作戰組教官 朱盈豪少校

提要

現代作戰中，以戰場情資共享實現作戰行動同步是決定戰爭勝利的關鍵，藉由通資平台技術的精進，「載台作戰」方式逐漸演進成「網狀化作戰」方式，大幅強化作戰效能。戰場中的指管系統植基於通資系統之上，因此通資系統的使用，應考慮其即時性、保密性、可靠性與抗干擾性的需求，以發揮指管系統應有效能，使 C4ISR 工作有效整合，本篇論文研究在瞭解指管通資網路運用時可能遭受的攻擊方式，以提供日後安全性提升參考。

前言

資訊科技的快速發展，帶動了軍事上的變革。1970 年代，電子技術迅速發展，電腦技術也逐步成熟，使得「情資獲得」與「戰場指管」能夠整合在一自動化系統，增進指揮管制的效率。在情資獲得上，以各種先進的監偵設備取代以人為主的「觀察」情資；而在戰場指管中，無論是上級對下級單位的命令下達或是下級對上級的狀況回報，皆隨著通資技術的進步更有效率。因此 C4ISR 的作戰指揮系統在現代化高科技戰爭中扮演著舉足輕重的角色，而指管系統的基礎建設—通資系統，更影響著整體效能的表現。

本文首先從網狀化作戰的概念切入，介紹網狀化作戰概念以及其組成；接著說明主要構成網狀化的鏈路—數據鏈路，並介紹其性能與特性，最後以軍事上常見的指管系統數據鏈路整合架構為例，探討其安全性問題。

本文

壹、網狀化作戰

一、網狀化作戰概念

網狀化作戰又稱為網路中心戰，是透過將部隊連接上網路實現軍事作戰。以網路為中心的作戰，能為部隊提供戰場情資與信息，藉以取得戰場優勢。在網路中心戰中，作戰部隊能夠藉著取得情資的優勢，大大的增加其作戰效能。2003 年波灣戰爭中，美英聯軍即以「網狀化作戰」方式取得資訊優勢，掌握戰場情資，以優勢的海、空軍對伊拉克之政治及指揮中心投擲巡弋飛彈，並以衛星導引炸彈實施精準打擊。

網狀化作戰是指將戰場空間中的各單位與戰場互相結合，以產生戰力的一種構想；係基於戰場空間高階情資的發展而據此訂定作戰行動，並透過與情資

單位的有效鏈結，以及分權式指揮，加以描述其特性。故一個具備資訊時代高科技支援的鏈結部隊，將使各級決策者都具備此種充分掌握戰場之能力。

二、網狀化作戰的作戰結構[1]

網狀化作戰係由美國海軍所提出的作戰方式，以區別於以載台為中心的作戰方式。其組成包含有資訊網格、感測器網路、接戰網路(如圖一)，分述如后：

(一)資訊網格

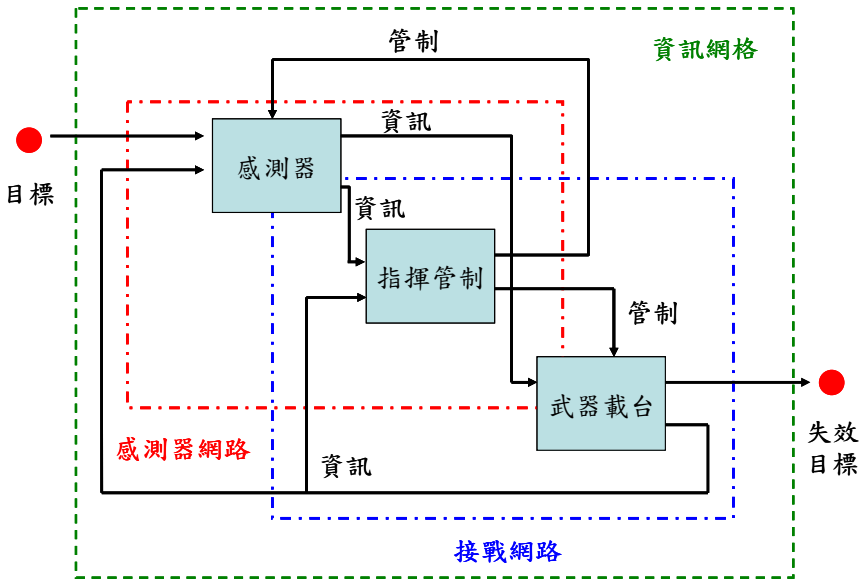
為提供計算與通信骨幹，促成網狀化作業的架構，為一實體之基礎建設。

(二)感測器網路

用以強化部隊戰場體認。透過感測器網路的部署運用，克服了單一感測器的限制，促使作戰行動同步化。感測器網路的元件包含太空、空中、海上及地面感測器。

(三)接戰網路

將感測器網路與武器載台網路結合，使資訊傳播速度與作戰節奏相配合。接戰網路的組成為指揮與管制、網際世界的動態武器載台及支援部隊，供指揮官運用並增進聯戰戰力。透過戰況體認的運用，將空中、地面、海上的「武器載台」鏈結，以產生聚能的效果。作戰網狀化的接戰模式中，其偵測、指揮、管制及接戰功能經由數據鏈路形成強固的網路，使得網路節點間傳輸的資訊內容、品質與即時性增加，增強部隊對戰場空間的體認及指揮速度的功能，從而使戰鬥部隊的戰力提昇。



圖一　網狀化作戰結構(資料來源：劉慶宏，「網路中心戰-21 世紀的作戰概念」，現代防禦技術，第 31 卷第 2 期，2003 年，頁 2。)

[1] 萬濟人，「資訊時代的作戰趨勢-網狀化作戰」，國防雜誌，第 21 卷第 3 期，頁 45-46。

貳、數據鏈路的特點

一、數據鏈路的定義

數據鏈路是採無線網路的通信技術結合通信協定，實現站台與載台間的信息交換，從而發揮戰術系統效能的系統。數據鏈路可以形成點對點數據鏈路和網狀數據鏈路，使作戰區內的各種指管系統和作戰平台的計算機系統組成戰術數據傳輸和信息處理網路，提供指揮官與作戰人員有關的數據與戰場圖像。

二、戰術數據鏈路的發展

早在四、五十年代美國與盟國部隊通信方式採用不保密的無線電通信方式，僅能提供語音連絡用，限制了除了聲音以外的戰術數據傳輸能力。隨著戰爭規模的擴大，軍種聯合作戰對於戰場信息共享的需求越來越迫切，加上裝配有射控雷達的先進戰術機的出現，戰術機群間空情的傳遞與目標的分配也加速促成戰術數據鏈路的發展。透過理論與實際的證明，具有數據通信的機群作戰效能遠高於不具數據通信的機群。

數據鏈路技術的廣泛應用還是這一、二十年的事，尤其是隨著資訊技術與網路技術的發展，它的作用才越來越被軍事專家重視。1983 年，入侵格瑞那達使美軍認識到通信能力不足所導致的影響，因通信系統不相容，陸軍部隊無法得到山另一邊的海軍支援。1991 年的波灣戰爭中，初級的數據鏈路被應用在戰場上，美軍的“愛國者”飛彈攔截伊拉克的“飛毛腿”飛彈，表現出數據鏈路的作用。當然，波灣戰爭中，美軍的數據鏈路僅運用在一些領域，並未實現在整個戰場，特別是三軍橫向通信的問題並未獲得解決，作戰命令因此不能透過通信網下達，這也是後續數據鏈路的發展被迫切需求的原因。

第一種戰術數據鏈路用於美國海軍戰術數據系統(Navy Tactical Digital System, NTDS)，於 1961 年研製成功，當時的目的在使作戰情報中心自動化，以解決空戰中指揮自動化與信息共享的問題。而後，各種類型的戰術數據鏈路相繼而生，在不同的領域中發揮了作用。

許多國家在 C4ISR 系統建設的過程中，均以數據鏈路系統作為其實現武器裝備及作戰效能的重要環節。美軍與北約國於 60 年代初開始研發數據鏈路，包含有一系列的數據鏈路 Link 4A、Link 11 與 Link 16 等，簡述如下：

(一)Link 4A 數據鏈路

Link 4A 數據鏈路與美軍的戰術數據鏈路 TADIL-C 相當，採用 FSK 調制方式，UHF 頻段，傳輸速率為 5000bps，不具有保密及抗干擾能力。以美國海軍為主研製而成，設計的原始目的在取代戰機的語音通信，其後的運用主要包含空中管制、空中攔截控制、地面控制轟炸系統與慣性導航系統校準等。Link 4A 數

據鏈路採用分時多工存取(TDMA)方式實現站台與多架飛機間的指揮管制。

(二)Link 11 數據鏈路

Link 11 數據鏈路與美軍的戰術數據鏈路 TADIL-A 相當，採用網路通信技術與標準信息格式進行數據交換的數據鏈路，半雙工的網路具加密特性，整個網路主要以「網路主控站」管理載台間信息交換，使用波段為 HF 與 UHF 兩種波段，傳輸速率一般不高於 25000bps，具有保密傳輸與超視距能力，但抗干擾性的能力較差。E-3 系列預警機上裝配有 Link 11 數據鏈路終端設備，用於預警機雷達情報傳輸。

(三)Link 16 數據鏈路

Link 16 數據鏈路為美國與北約組織國廣泛使用的戰術數據鏈路，美軍稱為 TADIL-J，伴隨著美軍聯合戰術資訊分散系統(JTIDS)的研發與應用而成為新一代的數據鏈路。Link 16 泛指採用 Link 16 標準的戰術數據傳輸系統，目前主要指聯合戰術資訊分散系統(JTIDS)與多功能資訊分散系統(MIDS)。

Link 16 數據鏈路是集合通信、相對導航與敵我識別的綜合系統，其特性為傳輸速率高(238.08kbps)、容量大，採用分時多工存取技術，組網效率與機動性高。與 Link 4 和 Link 11 比較，Link 16 採用了直接序列展頻、高速跳頻、R-S 錯誤糾正編碼和密碼加密等技術，信號在傳輸的過程中具有低截收率與高干擾特性。有別於 Link 11 的「網路主控站」，LinK 16 採用「無節點」的網路架構，不管哪個站台或載台被破壞，不致於影響到其他用戶功能，故系統具有很強的存活性。

三、數據鏈路的主要功能作用

信息化武器的一個重要特點是武器平台間實現橫向聯網，並做到戰場情資共享，從而提供武器平台的作戰效能。傳統的以坦克、戰車、火砲和導彈為代表的陸上作戰平台，以艦艇、潛艦為代表的海上作戰平台，以飛機、直昇機為代表的空中作戰平台等，都必須在火力優勢的基礎上兼具有信息優勢，才能成為高科技資訊化武器裝備。唯有透過數據鏈路的聯接，才能優化信息資源，有效調配和使用作戰能量，因此，數據鏈路是未來使軍隊結合與發揮其戰力的最佳通信工具。

四、聯合戰術信息分發系統(JTIDS)

聯合戰術信息分發系統(JTIDS)是由裝備有 Link 16 數據鏈路標準的終端設備的載台所構成的系統，其運用於作戰上的特點如下：

(一)相對導航

成員間的相互位置是聯合作戰中最為重要的戰術資訊，JTIDS 的相對導航能

力提供了此一要求。相對導航的實現是構築在網路精確時間同步的基礎上，使網路上的載台能進行相互間的距離測量以獲得位置數據。JTIDS 的導航功能還最大限度地利用了其數據鏈路大容量的交換能力。系統內各成員不僅能完成自己的定位，而且還能把自己的位置數據廣播到整個網的其他成員中間， 使網中的任何成員均不但知道自己的位置，而且有可能知道其他成員的位置。它使得在公海上或其它不能獲得地理定位源的情況下，網成員間仍能定出準確的相對位置和速度，使網成員具有相互定位和定向關係，從而任何網成員的情報系統所獲得的訊息均能以此為基礎互相交換，實現情資共享。

(二)影響作戰效能

對於飛機上的一般通信系統，駕駛員僅透過耳機獲得信息。而在 JTIDS 系統中，飛機載台能顯示目標位置、目標識別及瞄準目標的投彈點等數據，更可了解來自其他方面的威脅與我軍的狀況，且提供了近距離空中支援和攔截任務的成功率。

參、數據鏈路整合架構

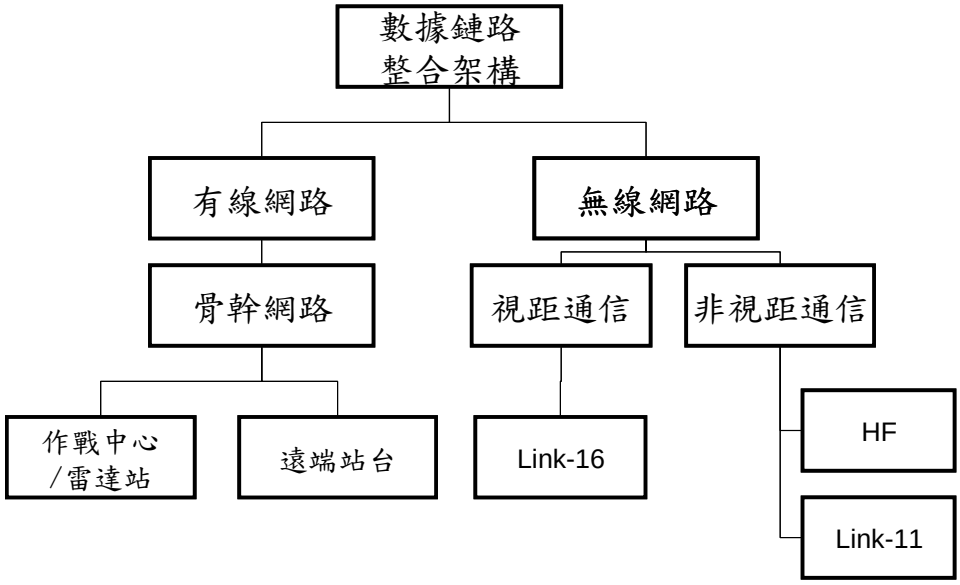
各國為發揮新一代兵力統合戰力，均逐步建置一體性指管通資情監偵系統(C4ISR)，構連各軍種指管系統與武器平台，用以同步交換即時情資，提升戰場透明度，構建看得到、聽得到、能指揮的即時指管決策系統，為日後建立資訊優勢，發揮資訊作戰能力的關鍵目標。數據鏈路整合架構如圖二，區分有線網路與無線網路，分述如下：

一、有線網路

以傳遞資訊的骨幹網路為主，連結各作戰中心、雷達站與遠端站台。作戰中心內部主要設置有指管伺服器及網路設備，用以整合監偵系統所傳遞情資。遠端站台主要設置數據鏈路終端機，為有線網路與無線網路界接之橋樑。當地面作戰中心要傳遞給機動載台之指管信息時，須藉由遠端站台終端設備方能達成。

二、無線網路

主要以 Link16 數據鏈路構連三軍的機動載台，並整合既有數據鏈路，建構成綿密的數據鏈路網。



圖二 數據鏈路整合架構(作者繪製)

肆、安全性分析探討

數據鏈路整合架構主要藉由兩種系統組成—有線網路與無線網路。各作戰中心成為國軍主幹網路上的資訊節點，彼此傳遞情資與指管命令；而作戰中心與載台間或載台與載台之間的即時戰場情資傳遞，使用各種數據鏈路架構而成，其中以 Link 16 為主，整合其它既有的數據鏈路及偵測系統。因此數據鏈路整合網路的安全性可分別從數據鏈路與資訊網路可能遭受的攻擊方式加以探討：

一、數據鏈路攻擊方式

學界有許多對於數據鏈路技術的介紹，雖然 Link 16 綜合採用直接序列展頻、錯誤糾正編碼(R-S code)與跳頻的技術，使得對其進行偵察、干擾具有相當的難度，但仍有相關研究探討對其攻擊模式，摘錄如后：

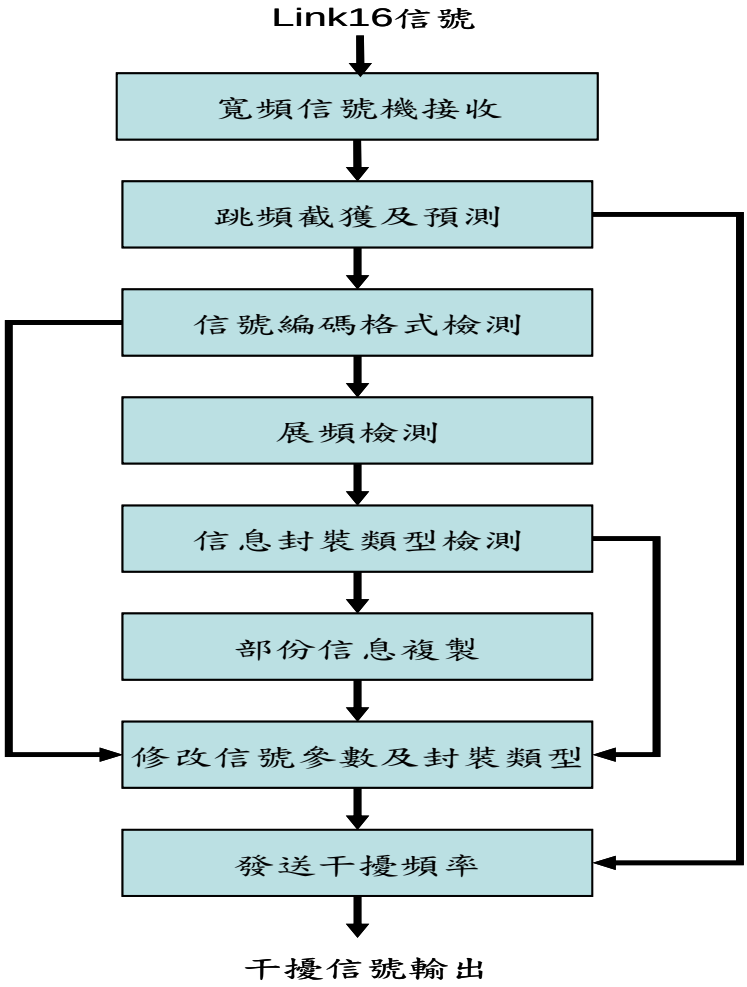
(一)欺騙式干擾[2]

對於 Link 16 進行大頻寬、大功率的壓制性干擾雖然具有一定的干擾效果，因所耗成本過大，顯然不是理想方案，且 Link 16 的網路拓樸屬無節點的通信網路，即使某些終端受到影響而失效，系統具自動組網能力使整個系統能夠正常工作，而達不到預期效果。

對 Link 16 進行干擾可以考慮採用欺騙式干擾的方式。干擾系統可以先行使用偵查機對 Link 16 網路的信號快速偵查接收，在截獲信號的基本參數後，對其進行檢測與評估。將接收到的 Link 16 信號進行部份複製並生成與原始信號具

[2]劉治國，趙新國，「基於信號分析對 link16 干擾策略研究」，艦船科學技術，第 23 卷，2007 年 6 月，頁 84~85。

高度相關性的干擾信號發射出去。這種欺騙式干擾信號由於與 Link 16 鏈路中傳輸的信號相似度較高，因而可以獲得較好的干擾效果。欺騙式干擾流程圖如圖三所示：



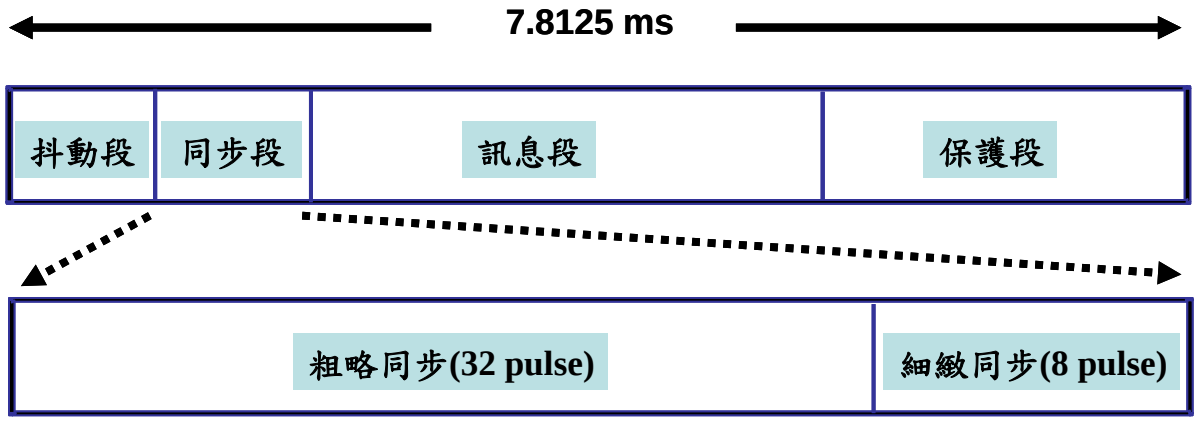
圖三 Link 16 欺騙式干擾流程(劉治國，趙新國，「基於信號分析對 link16 干擾策略研究」，艦船科學技術，第 23 卷，2007 年 6 月，頁 85。)

(二)對 Link 16 同步階段進行干擾

Link16 採用分時多工存取(TDMA)的工作方式，根據系統所使用的通信協定，其封包格式有四種分別為標準雙脈衝(STD/DP)、P2 雙脈衝(P2DP)、P2 單脈衝(P2SP)與 P4 單脈衝(P4SP)四種。

Link16 將時間劃分為一系列的時槽用以傳遞信息，每個時槽的長度為 7.825ms，包含抖動段(Jitter)、同步段(Sync)、訊息段(Message)與傳輸保護段(Propagation)。在訊息段之前是同步段，為了使接收端能正確的接收且恢復信息的編碼，Link 16 在接收端必須能處理同步段信息，否則系統無法完成後續的信息傳輸與解碼作業。

同步段又分為粗略同步和細緻同步，且同步信號均為雙脈衝，每個同步段信號共有 40 個脈衝，其中粗略同步為 32 個，細緻同步為 8 個。與訊息段不同的是，同步段僅使用 8 種偽隨機碼且只在 8 個跳頻點上作偽隨機的跳變，不同的時槽所選用的偽隨機碼也不同。



圖四 Link 16 時槽結構(作者繪製)

透過 Link16 信號時槽分析可知，同步是該系統正常工作的前提，如果能採取措施對該系統同步過程進行有效干擾，破壞 Link 16 定時信號的穩定，導致期同步過程無法順利完成，數據段信息自然無法接收，即可對數據鏈路產生有效干擾。

Link 16 信號不同時槽的數據段所攜帶的信息格式和信息內容是不同的，但用於同步的脈衝格式卻是一致的。Link 16 信號時槽的數據段和同步段跳頻的方式是有區別的，在數據段，脈衝載頻可以在所有 51 個跳頻點上作偽隨機跳頻變換，但同步脈衝卻只在 8 個跳頻點上變換。對於同步階段 40 個脈衝而言，每個頻點被重複使用的機率比較高，提供了干擾的可能性。

在 Link16 信號同步階段，根據其同步機制，接收機必須確認正確接收 16 個以上的同步信號(粗略同步)才能轉入細緻同步階段。因此，如果在粗略同步階段若有 5 個以上的頻道被干擾，則 Link16 就無法完成同步動作，即認為其被有效干擾。

二、資訊網路攻擊方式

資訊網路的安全可從中共「網軍」的威脅來探討。電腦作戰在電腦信息戰中，最直接與主要的關鍵在於電腦病毒程式的設計與執行網路攻擊的人才。基於此，中共一方面延攬海外電腦科技人才，以求電腦作戰及其他高科技作戰能力的提昇；另方面集合全國各地電腦專業人士，組成專業化的電腦作戰部隊，1999 年在中共解放軍報上首次出現「網軍」一詞，其任務即在於進行電腦網路

的攻擊或防禦的網路戰。此為中共為了因應超限戰，建軍方向朝向陸、海、空、天、電網一體化的作戰方式發展，且網軍可能繼陸、海、空之後，成為解放軍的第四軍種。

在無形的網路空間，「網軍」可憑藉有利的攻擊武器和高超的技能，入侵敵方網路系統，攻擊敵國的金融、交通、電力、航空、廣播電視及政府等網路，擾亂敵國政治、經濟和社會生活，造成社會動盪，一旦信息系統被破壞，軍事信息被截獲或篡改，整個軍事體系將陷入混亂甚至癱瘓狀態，影響力不容小覷。

網路戰技術涉及到作戰行動方面，勢必要有熟練的偵察技術，研發先進的網路入侵偵測軟體，透過此軟體從事網上偵測、破譯密碼、竊取資料及反跟蹤等。亦要有無堅不摧的攻擊技術，研發網絡攻擊軟體與技術，進而展開網上攻擊和反攻擊，包括信息癱瘓、資訊阻塞及資訊欺騙型等軟體，俾利於關鍵時刻癱瘓敵方的網絡系統。

「網軍」兵力具有「來源廣泛、行動隱蔽突然及作戰方式靈活」之特徵，對未來信息化戰爭起著舉足輕重的作用。未來信息化戰爭將會充份依賴、運用網路，而作戰型態會演變為「破網」與「護網」之對抗。所謂的「破網」即進入和破壞敵方的網路系統，一方面著重於平實的情報蒐集與網路攻防演練，另一方面則不斷以「黑客」攻擊，以癱瘓對手電腦網路功能，其作戰方式可分為「網路黑客戰、網路病毒戰、網路破襲戰」等三種：

(一)網路黑客戰

「網軍」的「黑客」部隊，對敵實施網上攻擊或竊取敵網上信息。它可穿過「防火牆」，入侵敵核心系統，達到網路制信息權之目的。

(二)網路病毒戰

「網軍」將具有大規模破壞作用之電腦病毒，利用傳播途徑，導入敵方雷達、導彈、衛星及自動化指揮中心的計算機信息情報搜集系統。並在關鍵時刻啟動病毒，藉不斷地傳播、感染及擴散，侵害敵系統軟體，致使其系統癱瘓。

(三)網絡破襲戰

「網軍」攜帶專用武器設備，在其軍兵種的配合下，摧毀敵方計算機網絡的物理設備，達到癱瘓敵指揮系統之目的。

以上三種的作戰方式中，可採用的攻擊性資訊戰武器，又可區分為資訊層與物理層兩大類

(一)資訊層武器

藉由網路或媒體的傳遞，以擾亂，癱瘓，截取，入侵資訊系統為目的。

1.病毒(Viruses)

將自己複製到電腦程式中以修改正常的電腦程式，將單機，系統或網路癱瘓。

2.蠕蟲(Worms)

不會修改正常的電腦程式，但是會大量複製，造成網路過載而癱瘓。

3.特洛伊木馬程式(Trojam)

隱藏在電腦程式裡，當電腦執行特定的工作時，木馬程式會執行未經授權的功能，讓攻擊者有機可乘。

4.邏輯炸彈(Logic Bomb)

蓄意預置在電腦程式系統內的程式碼，當執行特定指令或在特定時間下被觸發，會吞噬大量數據，癱瘓網路。

5.後門(Trap/Back door)

原先就存在電腦系統內的程式結構，讓知悉此一結構的攻擊者能進入電腦系統。

6.攔截程式(Sniffer)

對網路封包進行監視，並複製給攻擊者，讓攻擊者由獲得的封包資訊中過濾出想找的資訊，如帳號及密碼。

7. 阻絕服務攻擊(Denial of Service)

對特定網站伺服器大量索取資訊，使資訊通道壅塞，而無法提供正常資訊索取的服務。

(二)物理層摧毀武器

以機械能、生化或定向能對資訊系統的實體、人員、電力系統及網路等進行實體攻擊的武器。

1.機械能武器

包含了傳統的炸彈、炸藥、砲彈及飛彈等。

2.生化武器

以攻擊人員，影響資訊系統的物質的物理性質，使隔絕橡膠，密封劑等變質，達到破壞系統的目的。

3.定向能武器

(1)電磁脈衝武器

可以干擾電子裝備或使電子零件的電壓或電流大幅增加而燒毀，可用於對雷達、通訊及電腦等電子系統的攻擊。

(2)高能粒子武器

以高能粒子束照射目標，將能量傳遞到目標內部，使電子甚至機械零件損壞。

4.其他

(1)晶片細菌

以特殊培養的細菌啃蝕晶片基材，造成電子裝備故障。

(2)詭詐晶片

在晶片生產之初，即置入特殊電子電路，使晶片在使用一定時間後，

或接收到特定訊號時功能失常，或發送出特定訊號。

「網軍」憑藉高超的技術，侵入敵方龐大的 C4ISR 系統，隨意瀏覽、竊取、刪改有關資料或輸入假命令、假情報，破壞其整個作戰自動化指揮系統，致其做出錯誤的決策，達到「不戰而屈人之兵」的目的；亦可透過「無線注入、預先設伏、有線網路傳播」等途徑實施電腦網路病毒戰，癱瘓對方網路，達到「少戰而屈人之兵」之目的；運用各種手段施放電腦病毒直接攻擊，摧毀我高技術武器硬體系統，如巡航導彈、戰機內的電腦系統，使這些武器系統因內部的電腦系統紊亂、癱瘓而失去戰鬥力。

現代戰爭是綜合國力的較量，一旦發生戰爭，孰能於戰場上取得資訊優勢，即為取得勝利先機。能有效地動員和組織專業技術人員投入戰爭，將是資訊作戰中制勝的關鍵。中共利用「網軍」與其強大的「信息民兵」於網路戰中發揮作用，包括「駭客」攻擊、病毒傳播及集體發送郵件進行通道干擾等作為，已被喻為世界上除恐怖份子外的第二大威脅；另一方面亦鼓勵學術研究、利用專才於軍事作戰中，發展出各種取得電磁優勢的技術與策略，對我整體通資安全威脅影響甚距。

結論

第二次波灣戰爭引發現代戰爭型態變遷的新思維，當前所強調的是完全數位化的 C4ISR 技術，大幅度強化戰場即時情資與監控，嚴密控管戰爭遂行的每一進度，更提升了作戰效能。因此準確且即時掌握了戰場的指揮管制亦即掌握了作戰優勢;相反的，若戰場中指管系統遭敵破壞干擾，致不能發揮其應有效能，猶如失去耳目一般，容易遭敵擊潰。

資訊作戰是場無時空的作戰，藉由數據鏈路的整合，將有線的資訊基礎建設與無線的戰鬥數據鏈路結合在一起，構成多重情資傳遞管道，提升指管系統在戰場存活率，尤以國內資訊基礎建設於世界排名 17，位居許多國家之前[3]，將這有利環境運用於戰時，更能發揮指管效能。但「水能載舟，亦能覆舟」，多重的情傳管道所遭遇到的困難除了系統的整合、過多情資的正確性，在系統的安全方面同時也多出一些風險。

數據鏈路整合架構在中共國防科技日益精進的威脅下，可採取因應作為建議如下：

(一)要具備監偵及反偵蒐節點能力，防止指揮管制機制遭破壞。

本研究中所論述中共可能採用對無線網路攻擊技術，必須植基於對信號的

[3] 世界經濟論壇公佈網路整備度評比，http://www.weforum.org/pdf/gitr/rankings2007.pdf。

偵蒐與分析，從而提昇干擾機率以達其效能。因此，強化系統中監偵與反偵蒐能力，亦即加強我通資系統防護能量，保障指管系統作業安全。

(二)結合 C4ISR 指管通情系統，建置資訊戰反制能量。

所謂資訊戰，可以定義為對立雙方對於資訊的取得權、控制權及使用權，而展開的一種戰爭形式，目的在取得資訊優勢或是使對方失去資訊優勢。現階段以被動式的「防護作戰」為主，藉由指管通情與資訊傳輸系統的整合，強化通資戰防護能量；未來應結合監視偵察系統，建立主動式的反制作為，在戰場上發揮克敵制勝的效果。

(三)提升使用中的各項資訊防護機制，建置安全的通資作業環境。

資訊戰防護首重「安全」，敵攻擊方式日新月異，我方在資訊安全防護機制上，需妥採因應之道，諸如防護系統軟、硬體的設置、備援系統的建立、人員編組執掌與標準作業程序均應明定，且以建立自動化、系統化及資訊化之安全防護系統目標邁進，以防禦我通資系統之安全與完整，確保資訊優勢。

(四)積極培養專業科技人才，充實我國防科技戰力。

資訊科技進步愈迅速，專業人才的培養愈不易，如何打贏以高科技決定一切的戰爭，人員訓練如同武器一樣具有決定性的關鍵，任憑有再精良的武器，若作戰人員訓練不佳，則無法發揮應有效能。專業人員的運用應適才適所的分配，並鼓勵軍中與民間對國防科技的研究風氣，以充實國防戰力。

官兵個人在平時安全規定的遵守與資訊防護習慣的養成，同樣也是影響著惡意程式是否入侵我通資系統的關鍵，確遵軍民網的「實體隔離」政策及各項資安管控規定，可避免敵有可趁之機，降低我通資系統遭受攻擊機率。

參考資料

一、王薇，曾興雯，「JTIDS 最佳干擾的研究」，無線電工程，第 34 卷，2004 年，頁 27~29。

二、丁鋒，「戰術數據鏈路技術現況及發展研究」，無線電工程，第 24 卷，2004 年，頁 37~40。

三、楊曉欣，「中共網軍對我資訊安全威脅之探討」，http://www.kinmen.gov.tw。

四、陳志誠，彭彥倫，「論恐怖主義可能實施的資訊戰及其反制措施」，第二屆恐怖主義與國家安全學術研討暨實務座談會論文集，2006 年，頁 163~181。