論恐怖主義可能實施的資訊戰及其反制措施

陳志誠

大同大學資訊經營所教授

彭彥倫

戰略與產業研究中心(CSIS)執行長

摘要：自從「911 恐怖攻擊事件」之後，資訊技術已成爲恐怖攻擊的新武器，各國也積極探討如何利用資訊技術進行反恐，資訊技術儼然成爲實施恐怖主義與反恐的新戰場。恐怖主義的存在，可能使現行的架構與運作出現許多例外。本文除闡明恐怖主義對資訊戰的影響外，也說明各國反恐作法的重點，並著墨於我國對於資訊戰的準備。此外，在資訊反恐具體作爲上，主要包含：發現恐怖資訊、資訊之安全防護以及反恐資訊戰的未來發展，完整進行恐怖主義情蒐作爲，必能多方抑制恐怖主義蔓延。

關鍵字：911 恐怖攻擊事件、網軍、資訊戰、資訊作戰

綱要

壹、前言

近代戰爭的模式已逐漸趨向資訊及電子化，因此資訊戰（Information Warfare）等相關議題不斷廣爲討論。近年來各國政府不斷提出對資訊安全等相關法案，證實了政府對於電子化及資訊化安全的重視，2002 年美國 911 攻擊事件後，國內除嚴格要求檢查出入境人員的身分及違禁品外，更制定了《美國愛國法案》(USA PATRIOT Act)[1]，使現存的安全機制更能有效運作，防範意外再度發生；除此之外，聯合媒體強力的譴責恐怖攻擊，並終結國家對恐怖主義的支持及物資支援，期建構反恐怖主義(Anti-Terrorism以下簡稱「反恐」)的全球安全防禦網絡。

在各國積極的反恐行動當中，我們觀察到：隨著網際網路的發達，資訊戰正悄悄來臨，且已成爲恐怖份子所利用的策略與工具。資訊戰爭具有持續且無孔不入的特性，其威脅除政治層面外，對於整個社會、產業界也將都高度受到影響。恐怖份子將網路視爲間接武器，並能具備「存取個人電腦、善用文書處理電子郵件及視訊設備等工具、以及

[1]美國愛國法案，2001/10 立法通過，其內容：降低執法人員監視罪犯或恐怖份子的監視門檻/手段，強化部門之間的資訊交流，擴大恐怖份子的定義，並增加幹員可向ISP要求出示的資訊範圍。參考 http://taiwan.cnet.com/news/special/0,2000064597,20052561-3,00.htm， 存取日期 2006/12/09。

掌握資料庫系統」等基本技能，達到其犯罪目的。911 事件對於資訊化社會提供了許多省思：恐怖攻擊發生後，世界貿易中心(World Trade Center)崩塌，該建築物內的公司(如美林證券)如何快速恢復正常營業？藉由世貿中心雙塔頂的電視廣播天線，如何利用替代基地台迅速恢復正常作業？地區性電信交換系統、郵局及網際網路等基礎設施，遭破壞後如何恢復正常營運？在資訊時代裡，資訊系統受攻擊後，如何因應的問題，值得吾人深思。

此外，恐怖主義的存在，會使現行的架構與運作出現許多例外。當現存的體系無法處理許多重要的新問題時，將因其歷史包袱而崩潰，而被一個新的、更簡單、更令人信服的典範所取代。這就是近代社會學家孔恩(Thomas Kuhn)在其經典名著"The Structure of Scientific Revolution"中所揭示並闡揚的「典範轉移(Paradigm Shift)」的概念。所謂典範是指「思想概念如何與其他個體交流的一種普遍被接受的模式，科學研究得以在它的形成的概念架構下運作執行」[2]。本文也將以此爲哲學思考基礎，討論資訊技術與反恐作爲的關係。

實質上，IT已成爲恐怖攻擊與反恐(Anti-Terrorism)的新戰場[3]。它的意涵包括：

(一) 資訊系統(硬體、軟體、資料)可能是駭客、病毒攻擊的目標，使被攻擊者造成損害。如何防制這類擾亂不能只視爲傳統的資訊安全課題，因爲恐怖主義者對資訊系統的攻擊，除了竊取機密外，旨在製造駭人聽聞的效果，因此強化資訊安全，也是反恐的重要工作之一。

(二) 在某些情況下，攻擊會發生在電腦支援系統如電話交換中心、股市交易所或飛航控制系統等，造成嚴重的傷害，以收恐怖攻擊的震撼效果。這是我們亟應防範的。

(三) 資訊戰的基本態勢是所有「開放的」使用者對「隱匿的」攻擊者的鬥爭。因此，強化整體的系統安全是至關重要的；另外，如何利用資訊技術，找到隱形的攻擊者並加以監控，也是反恐的重要作爲。

(四) 企業及政府的反恐作爲必須兼顧預防(Proactive) 與反應(Reactive)。在預防性作爲中，應以「典範轉移」對 IT 的發展與運用，重新作思考；另外，在重大資安事件發生時，如何預備萬全的應變措施更是要務。

[彭錦珍 2004]指出:「一國的資訊戰力不但是現代化國防的第一道屏障，也是國家安全的防衛後盾」。其實，資訊戰並不是一個全新的事物，煙霧信號也是資訊密碼，通信有時也是進行欺騙的一種手段。早在戰國時代，愛國商人弦高退敵的故事，就是打了一場漂亮的資訊戰。在古希臘時代，若非特洛伊人（The Troy）疏漏情報資訊，希臘士兵們豈能木馬屠城呢？今天的資訊戰由於網路的出現，更是開啓了新的局面：世界資訊系統互聯性的增強，敵人可能提出更出奇的、更可怕的資訊電子攻擊。例如，敵人並非利用戰鬥機向的機場塔台或作戰中心發射導彈，而是坐在遙遠的地方發起數位攻擊，用電腦病毒或所謂的"邏輯炸彈"[4]使我方設備失效。這樣的敵人可以直接把戰鬥引入國內，而無須通過國家邊境。如 1991 年沙漠風暴戰雲密布之際，因爲有「電子統帥」坐鎮指

[2]參照[凱文 2002]，第 19 頁。

[3] Edward Yourdon語，見[凱文 2002]第一章。

[4] 邏輯炸彈(Logic Bomb)是按一定條件設計的、蓄意埋置在系統內部的一段特定程式或程式代碼。在一定條件觸發下，它可以釋放病毒、蠕蟲或其他攻擊形式，造成系統混亂。

揮，美國最高統帥布希總統照常渡假；再如 2003 年美伊戰爭期間，網路尖兵們運籌帷幄，讓美軍照樣決勝千里之外。

我國首次由政府提出的《國家安全報告》於 2006 年 5 月 20 日公布，其中對國家的安全環境、內外在威脅等均有深入的分析，最令人注意的部份，就是將「資訊安全」的威脅，列爲「國家安全的內外在威脅」項目，其中更指出中國大陸對我國採取組織性網路攻擊，已成爲我國國家安全的一大威脅。因此，國家安全的多元性，已是新世紀國家安全與國防威脅的共同的題目。[5]

目前大多國家基本上多仍延用 1980~1990 年美軍對資訊戰與資訊作戰的定義，將資訊作戰(Information Operations, IO)界定爲廣義層面的資訊攻防運用，而將資訊戰(Information Warfare, IW) 界定爲專業的軍事行動。事實上，美國國防部在 1998 年頒布的「空軍資訊作戰準則」，對「資訊作戰」及「資訊戰」的定義，仍如下述：[6]

- **資訊作戰：**「不分平時、戰時，任何用來影響敵方資訊與資訊系統，並防護我方之資訊與資訊系統的行動。」
- **資訊戰：**「在危機或衝突期間，針對特殊的敵人，爲達成特定目的，所採行的資訊作戰。」

依據上述定義，資訊作戰作爲，具通稱性與整體性；資訊戰行動，則具指向與指標性。不過，進入 21 世紀，在歷經自 2003 年起延續迄今（2006 年）都未能完全結束的美伊軍事衝突後，美軍對新世紀的戰爭模式，已愈益重視資訊作戰，並自 2006 年 2 月 13 日正式頒布的聯合作戰中，修訂資訊作戰(Information Operations)的定義，就是將過去納爲資訊作戰一部分的資訊戰(Information warfare-IW)名詞去除，改爲一元化的資訊作戰(IO)。自此，資訊戰已不再是軍事術語，而是一般對戰爭類型通稱的用語。至於資訊作戰，應已明確界定爲軍事作戰類型的主軸之一，而不再只是一般網路或資訊安全技術的運用而已。

本文將對以上幾方面作深入之探討，其餘的內容分述如下：第二節是相關文獻與研究探討。第三節是恐怖主義對資訊戰的影響。第四節則是提到各國反恐的具體對策。第五節闡述資訊反恐的作爲；最後一節是結論。

貳、相關文獻及研究探討

本文主要基於筆者先前研究如[陳志誠 2005]、[陳志誠等 2006]和[曾章瑞等 2006]加以深入探討而成，細節可參考上述論文。本節將先對恐怖主義作正式的定義，然後藉由統計瞭解恐怖攻擊的現況。其次我們將探討資訊戰相關的資料及文獻，提供讀者參考。

2.1 恐怖主義

根據美國反恐中心統計，2004 年全球共發生了 3912 件恐怖攻擊事件，而 2005 年全球發生恐怖襲擊事件將首次超過一萬起，恐怖事件劇增的主要原因是伊拉克在舉行憲法公投和議會選舉期間武裝襲擊和綁架事件大幅增加，2005 年僅伊拉克就發生了約 3500

[5] 2006 國家安全報告，民國 95 年 5 月 20 日

[6] 美國空軍資訊作戰聯戰準則，USAF, Information Operations ,Aug,1978.

起恐怖襲擊事件，而 2004 年該國僅有 866 起。這是相當可觀的增幅，可見恐怖主義有急劇擴大興起的趨勢。

2.1.1 恐怖主義的定義

根據"牛津英語辭典"對於恐怖主義有兩種定義，第一個定義是：「如同法國一七八九至一七九七年大革命當權者實行的威脅一樣」，這是政府公權力的濫用，藉以鎮壓人民，這是政府恐怖主義；而第二個定義是「意圖以恐怖手段打擊異己的政策，威脅方式的使用，引起恐怖的事宥或者使人恐怖的情況」，這是吾人一般理解的恐怖主義。根據"簡明不列顛百科全書"對恐怖主義的詮釋是：「恐怖主義是對各國政府、公眾或個人，使用令人莫測的暴力、訛詐或威脅，以達到某種特定目的之政治手段。各種政治組織、民族團體、宗教狂熱者、革命者和追求社會正義者，以及軍隊和秘密警察都可以利用恐怖主義」，當前各國政府對恐怖主義的解釋也大致與此一致。而"美國傳統大學英語辭典"對恐怖主義的解釋是：「對武力或暴力的非法使用或威脅使用，一個人或一個有組織的集團以威脅或脅迫社會、政府爲目的而危害人類或財產，其常具有意識形態或政治原因」。

總而言之，恐怖主義者常會利用攻擊無辜的民眾，讓大眾產生恐懼意象（Terror Image），以達成他們政治目的的行爲。對於恐怖主義的定義，目前還缺乏一個完善標準的共識，這也將導致在消除反恐戰爭中出現「多重標準」，使各國打擊恐怖主義的步調不一，尤其是在處理恐怖嫌犯的引渡上。在資訊安全攻防中，例如中國大陸即區分駭客(Hacker)爲黑客及紅客(Honker)[7]，對系統攻擊者甚至於加以表揚，在在影響資訊反恐作爲。因此要實施反恐鬥爭，當深入了解恐怖主義的意涵及特性是至關重要的。

2.1.2 恐怖主義的意涵與特性

恐怖主義的特性，可歸納如下：

(1)計劃性：恐怖行動一般會像戰爭的發生一樣，恐怖份子會尋求最理性的選擇，把施予攻擊的對象設定一個極大化的戰略價值，期盼能用最小的犧牲，達到最大化的目的。

(2)政治性：恐怖主義的存在跟一般犯罪最大的不同點，就是它有特定的政治目的，例如尋求民族解放[8]、建立政權、要求釋放被囚的同伴[9]，也或許是敵視美式的資本主義[10]。這之間以尋求民族解放被認爲正義性最高。大部份的恐怖主義者，大都自許站在正義的一方。

(3)意象性：一般的恐怖攻擊行動中，恐怖份子並不要求馬上實現他們的目的，反而是透過暴力行爲的傳播，製造一種恐怖意象，讓受害的國家人民生活在恐怖的陰影中，以便對政府構成壓力，進而檢討他們對外擴張或殖民的政策。

---

[7] 黑客即一般人概念中的駭客；而紅客則是具有民族意識、愛國情操的駭客。

[8] 例如俄國境內的車臣武裝叛亂份子。

[9] 例如 2006 年 7 月以色列進攻黎巴嫩事件，即由於巴解組織挾持兩名以色列士兵要求釋放被關的一千多名巴勒斯坦人。

[10]例如近年來凱達(Al Kaeda)組織的各項作爲。

2.1.3 恐怖主義的戰略

恐怖主義者所採取的戰策，大抵有三：

(1)自許是「以小搏大」，是「弱勢者對抗強權」，是犧牲最少的戰爭。

(2)恐怖分子往往不是把受害者當成直接目標，而是要造成一種恐怖意象(Terror Image)，讓強權的人民產生焦慮或恐懼，並間接壓迫政府對恐怖份子妥協。

(3)恐怖份子的目的不同於一般的國際犯罪，他們預設政治目的，希望重建政權或國家。

2.1.4 恐怖主義的戰術

基於前一小節的戰略，恐怖主義者所採行的戰術多樣化。過去在美國中情局的統計中，最常被使用的恐怖戰術，包括武裝攻擊、縱火、暗殺、綁架、劫機與爆炸等超過十八種之多。武裝攻擊主要是在農村革命中實施；暗殺則是最古老的，也是綿延不斷的方式，在農村或城市的戰鬥中經常被使用；其他的則是在「城市游擊戰」中被廣泛的當成一種戰術。過去恐怖攻擊中最常被使用的幾種如劫機行爲、自殺炸彈則是最激進的行動，由於很少能安全脫身，類似第二次世界大戰時日本的「神風特攻隊」之所爲，只有視死如歸的恐怖份子才會使用。至於一般恐怖攻擊戰術如爆炸、暗殺、綁架的手段，可以不須把自己置身在危險的火線上。資訊戰則可藏身遠處，遠離危險，算是最安全的戰術。

在九一一的攻擊行動中，恐怖份子把劫機、爆炸、自殺性行動結合在一起，是前所未見的攻擊行爲。因此，可以把它視做是「新恐怖主義」的誕生，也就是一種連結性的攻擊行動、超越傳統的攻擊模式，以及是一種有計畫的集體謀殺行爲。[11]

2.2 資訊戰

現代戰爭全面結合了速度、指揮、通訊、資訊及電子戰等作戰範疇，開啓了所謂「資訊戰爭」的新型態作戰，因此若要探討對未來戰爭之因應之道，資訊戰是不可忽視的重要一環。

2.2.1 何謂資訊戰

所謂資訊戰，可以定義爲：「對立雙方爲爭奪對於資訊的取得權、控制權及使用權，而展開的一種爭戰形式，其目的在於利用這些資訊優勢使對方屈服，或是使對方喪失這些優勢而達到干擾對方之作用。」美國陸軍對資訊戰的定義爲：「藉由採取影響敵人資訊、資訊相關程序、資訊系統和電腦網路等行動，以奪取資訊優勢；同時，亦須對己方資訊系統採取防護措施。」

[陳志誠 2005]從廣義上來說，資訊戰是敵對雙方在政治、經濟、社會、科技和軍事等各個領域裡，以資訊技術手段，爲爭取戰略（或競爭）優勢而進行的對抗和爭戰。從狹義的軍事領域來說，資訊戰的內容包括：(1)使用資訊技術向對方進行的試探、偵測、

[11] 資料來源：美國的反恐戰爭與台灣的戰略選擇，王崑義，中興大學全球和平與戰略研究中心 參考http://cgpss.nchu.edu.tw/modules/wfsection/article.php?articleid=358, 存取日期 2006/12/09

以及對上述活動所進行的偵察、干擾、破壞和反利用等反制行動。(2)爲對抗敵方的偵察、引導、指揮、控制、通信、資訊分析、僞裝欺騙和打擊殺傷等作戰行動。(3)對敵方干擾、破壞和反利用而採取的防範措施等。

由上述定義可知，資訊戰的範圍實包括：凡涉及敵對雙方之資訊干預、干擾、破壞、破解、反制、反反制等，都可以列入資訊戰的範圍。至於資訊戰中所使用的主要手段與武器，是各種資訊技術及資訊設備，若由主動與被動的觀點來區分，亦即攻擊性及防禦性的資訊系統。

最明顯的例子算是空中預警機的電子戰爭，敵方可能會透過干擾性的資訊傳遞或是電波干預，以期造成雷達系統或是溝通系統的影響，讓我方對於敵軍走向或相關資料造成誤判或無法辨識，讓他可以在進行軍事行動時保有隱密性或威脅性。而另一個最簡單的舉例就是密碼戰，只要破解敵方密碼，就能掌握正確的情資，所以我方可能會出現多重編碼，或是擾亂性密碼，以期造成敵方誤判，而掩飾自己的軍事企圖。

2.2.2 資訊戰的目的

在波灣戰爭中，超過三千台的戰區電腦連接回美國本土處理戰務。因此，新世紀的戰爭裡，電腦與通訊及電訊，已是戰場指、管、通、資、情的命脈。這些戰場所應注重的問題，也是後方內部的問題。如何挫傷或癱瘓敵人的作戰中樞與作戰神經及作戰能量，是資訊戰的主要課題。

資訊戰的目的，在於以最小成本，來達致對敵人最大的破壞力。資訊戰所耗費的成本，遠低於傳統戰爭的軍費，所造成的破壞力，卻可超越傳統戰爭所帶來的破壞力。由敵人內部來瓦解敵方戰力。資訊戰不僅僅只是戰場問題，可直接傷害後方電腦與通訊及電訊，將造成整體後勤系統、ＣＡＬＳ系統、後方金融體系、醫療體系，與所有跟電腦與通訊及電訊相關系統，使得後方人心動亂，內部失去作戰意識。推動不流血的戰爭。核子彈對人物同時破壞；中子彈殺人但不傷物；資訊戰人物並存，但失去作戰能力，使敵人自動投降，並可順利接收敵方人力物力資源。建構安全的防護堡壘。資訊戰的能量建構完整，能有效的嚇阻敵方侵襲，爲己方築起一道安全防護牆，讓敵方了解資訊作戰能量下，不輕易發動戰爭。所以資訊戰如同戰略武器一般，是有效的防護堡壘。兼具攻擊與防禦效能。資訊戰係運用資訊技術與武器，攻擊敵方資訊與系統，以取得資訊控制；並防護我方資訊與系統之安全與完整，以確保資訊優勢。[12]

2.2.3 資訊戰的特性

有別於傳統戰爭，兵不血刃的資訊戰具有如下特點[陳志誠 2005]：

(1) 資金與科技水準的跨入門檻低：資訊戰場上的攻擊者無需具備龐大的資金、或購買昂貴的設備，甚至於不需是個資訊專家。只要他會利用/操作攻擊工具（如木馬程式），即可作爲資訊戰的攻擊方，也有可能讓對方嚴重挫傷。

(2) 傳統的界線，如戰爭與和平、軍事與非軍事、國家與地方，甚至於進攻與防禦等，都變得模糊。由於網路的建置，前方與後方的區別，因而泯滅。資訊戰的攻擊，往

[12] 參考http://www.ccit.edu.tw/~bcc/mu_Pi_e_V/___T__.html，存取日期 2006/12/09。

往都是直搗黃龍，直接中傷對方政府、組織或企業的神經中樞。

(3) 平時與戰時的分野泯滅：只要政府機關（甚至於民間機構）一有資訊安全上的漏洞，即可以引來資訊戰的攻擊。例如近年來，國防部發現每當兩岸局勢緊張之時，就有有心人士利用網際網路，假冒「中央社」及國防部新聞稿名義以虛構的「台海空戰」發布不實新聞，企圖以「心理戰」、「宣傳戰」打擊我民心士氣破壞金融穩定，其流傳速度很快，戰爭意味至爲明顯。資訊新科技的確帶來新的弱點。在過去，攻擊對方時必須派遣特戰人員才能達成的任務，在不久的將來可能在彈指之間便可完成。假如我們平素不提高警覺的話，敵人的確有可能造成國家的嚴重的干擾與破壞。

(4) 資訊系統既是資產也是負債；既是資訊戰中的武器系統也是攻擊目標。就防禦角度而言，由於攻擊隨時可能發動，且其戰線可能無限拉長，遍地烽火，似乎防不勝防。此外，資訊系統不斷演變，變得更爲複雜，管理難度也加大。因此資訊安全必須是一個動態的觀念。系統複雜化雖然可使攻擊者較難下手，但是也會使防禦者難以了解與控制潛在的弱點與威脅。這是科技的特性，沒有任何一種技術可以百分之百保證是完美的。

(5) 資訊能力是資訊戰決勝的基礎：在傳統戰爭中，軍隊素質、武器精良程度、國家經濟力、作戰指揮決策等所構成的綜合戰力是決勝基礎；但在資訊戰中，勝負有時簡化爲一場鬥智。曾經有一位退休的聯邦調查局電腦犯罪組的負責人吉姆・塞特爾，在他所做的資訊威脅評估中更加直接了當地說：「給我精選 10 名駭客，組成個小組，90 天內，我將使美國趴下。」他的話並非危言聳聽，資訊能力往往是資訊戰決勝的基礎。資訊可以制人，卻也可能制於人，愈是依賴資訊的社會，戰爭所造成的損害還可能愈大。以 2001 年「911 恐怖攻擊事件」爲例，儘管美國軍力獨霸全球，卻在錯失資訊情報下，導致華府的經濟與軍事要脈遭受重創。此例正好說明了未來戰爭的可能情況：疏漏了資訊防衛，軍事大國不見得穩居上風；相對地，若能攻擊對方資訊要穴，武力弱勢者還可能扭轉劣勢，反敗爲勝。 由此可知，在資訊社會裡，擁有能攻能守的資訊戰力，不但是大國的重要權力，更是小國最佳的防衛策略，因爲以小搏大是可能的。

(6) 資訊戰的指揮管理難度大、節奏快，因此決策模式與決策體系亦將隨之改變。決策所需考量的範圍大幅擴增，各因素之間的交互關係變得複雜，這些即是資訊戰決策應注意之情事。從決策角度而言，資訊戰的目的就是在影響甚至瓦解敵人的決策機制。

2.3 我國整體資通安全與資訊作戰作爲

我國政府及軍方因應資訊安全威脅的綜合作爲，依據政府「2006年國家安全報告」，並參考學者曹邦全[13]與彭錦珍[14]的研究，我國因應資訊安全威脅的作法，應可朝「整體策略」、「基礎建設」與「總能運用」等三個面向繼續努力：

[13] 曹邦全，中共信息戰之研究，2002

[14] 彭錦珍，資訊時代中共國防現代化之研究－解放軍信息戰發展及其對台海安全之衝擊，2004

（一）整體策略

(1) 美國在國家安全策略的制定時，區分爲「國家安全策略(NSS)」、「國家軍事策略(NMS)」、「國防政策指引(DPG)」及「軍種執行指令」各種不同層級的文件，自國家高階的發展性策略，到中階的規劃性指引，最後到低階的執行性指令均已發展完備，並成爲確保資安策略能夠一致性貫徹執行的基礎。我國應參考其作法，訂定具體的政策及戰略指導、規劃指引及執行指令，以落實強化資訊安全因應措施的執行。

(2) 目前我國由行政院資通安全會報負責規劃與執行各項資訊安全工作，各單位亦多以任務編組或兼辦方式執行資訊安全業務，美國於在白宮設置「總統關鍵基礎設施保護辦公室」、「總統網路安全顧問」、「聯邦科技政策辦公室」等資通安全專責單位，負責高階政策指導及整合；另設置「國土安全部」整合所有國土安全工作之作法，均值得我國參考借鏡。

(3) 我國現有災變應變中心及電腦緊急應變中心(NCERT)等不同類別之國家級危機處理中心，惟並未整合。各中心多爲臨時性任務編組，對日趨複雜之緊急情況之處理應變及預警情資分享，可能因權責不清、疊床架屋、協調費時之情況，導致處理時效延宕之情況。我國應考量建立整合性國家級危機處理中心，統籌處理各種情況，以因應未來狀況。

(4) 隨著科技進步，戰略思維改變，中共威脅我國家安全的手段亦不斷演進，包括傳統軍事威脅與非傳統威脅的手段。面對新型態的威脅，傳統的作法已不足以防衛國家的安全。而政府與全民必須共同承擔保衛國家安全的責任。我國應針對威脅型態的變化，定期進行全面性的推演，針對缺失不足之處，調整策略並立即進行補強及精進作爲；另應利用全民國防教育的宣導，凝聚向心力、以提升保家衛國的抗敵意志。

(5) 我國的國防預算在爭取多年之後，在2007年終於提高至國家GDP的百分之三，國軍必須配合國家的整體考量，妥慎規劃運用，並確實將資源作最佳化的運用。

（二）基礎建設

(1) DII是NII的組成元素，兩者必須整體規劃發展、整合運作，方可發揮最大效果。我國具有優秀的資訊基礎產業及資訊人才，必須藉國家基礎建設(National Information Infrastructure, NII)與國防基礎建設(Defense Information Infrastructure, DII)的推動，將此股力量誘發出來，發揮競爭優勢。目前我國行政院已將相關資源運用進行整體規劃及推動，並每年納入國家安全國防軍事演訓中演練。我國應重視國家、軍事及民間資訊的傳輸交換，以利在戰時發生戰損時，在安全前提下，迅速銜接運作。

(2) 國家各級單位建置系統或執行業務資訊化同時，應同步列入資訊安全需求，並於系統完成建置後確實驗收及執行資訊安全測式，俾於推動資訊化時，同步精進資安防護作爲；另應由中研院、中科院等專業機構參考國際資安驗證標準，針對現行資訊安全防護設備進行驗測，並提供各單位作業選用參考，以確保資訊安全。

(3) 國家各公務機關，應就公務資訊之產生、機密等級、保存、傳遞方式、網路分級及人員管理等程序，制訂標準作業程序，以維持作業安全，並強化資安事件之即時通報及處理。另應律定資安稽核週期及方式，以定期及無預警方式至各級機關實施檢

查，瞭解各項資安管制工作實際執行情況。

（三）總能運用

(1) 資訊安全工作須具備高技術能力方可勝任，資安人力亦應格外受到重視。惟國家各級機關人事任用規定僵化，使民間的資安人才，無法進入政府服務，導致資安工作推動事倍功半。我國應儘速調整公務機關人事運用制度，並考量將國際資安證照比照高普考資格，以擴大引進民間資安人才，另應採取較彈性的任用與薪給制度，以吸引優秀人才貢獻專長。

(2) 資訊作戰具有高科技、低成本之特性，我國應儘速規劃一套強化資訊安全科技自主發展的有效機制，建立我國資訊安全核心技術發展之體系，並將其納入國防科技關鍵發展項目，結合民間能量，以掌握核心能量。

(3) 我國應考量成立資訊作戰的研究中心，與各大學術機構一起研究資訊作戰理論、戰術戰法、技術等。另可考量扶植資訊安全重點產業，以專業社群的力量，加速發展的速度。

參、恐怖主義對資訊戰之影響

在九一一恐怖攻擊之後，人類世界鑑於電腦已成爲現代國家的重要基礎建設，所以紛紛研究如何加強資訊安全，以防衛恐怖攻擊可能帶來的國家社會癱瘓。在這方面的研究，系統分析大師Edward Yourdon所著”Byte War: The Impact of September 11 on Information Technology”[15]一書，有值得參考的內容。Yourdon認爲恐怖主義已迫使我們必須作「典範轉移」，對現行資訊技術及系統作結構性的改變。[Merritt et al. 2004]對安全資訊學(Security Informatics)之在學校授課中亦應順應新的變化，作典範轉移，而不只是固守原有的IT技術課程之教學方式。

3.1 認識恐怖份子可能利用的資訊戰法

知己知彼，方能百戰百勝。恐怖份子所可能利用的資訊戰術與一般的電腦犯罪者大抵相同，但是兩者之間卻有不一樣的地方：

(1) 一般的電腦犯罪者於犯罪之後會力圖滅跡，以圖全身而退；資訊恐怖攻擊者的目的，若是在造成震撼效果，往往在癱瘓對方系統，主導聳動視聽。

(2) 一般的電腦犯罪者許多是以圖利爲意圖；資訊恐怖攻擊者往往自居於正義的一方，較少以圖利爲目的，以免落人口舌。但恐怖份子者卻可能利用網路來洗錢。

(3) 一般的電腦犯罪者，除非是挾怨報復，很少摧毀電腦及其它支援設備爲攻擊目的；資訊恐怖攻擊者則可能作實體的攻擊破壞。

瞭解了以上攻擊方式之異同，資訊恐怖攻擊可想見的方式有下列幾種：

(1) 竊取機密資料：利用網路入侵、社交工程、人身接觸等方式竊取重要機密資料。此種攻擊形式表現是越權存取。入侵時，必須突破身份驗證的第一道防線。僞裝(Masquerade) 、連線截奪(Hijacking)、竊聽(Eavesdropping)等是常用的手段。

[15] 中文版”驚爆資訊戰”，見[凱文 2006]。

(2) 癱瘓系統：利用惡意程式(Malicious Code)如病毒(Viruses)、木馬(Trojan Horses)、網蟲(Worm)等，或讓系統癱瘓、或讓資料消失、或使系統拒絕服務(Denial of Service)。惡意程式往往藉由郵件傳送或是網頁下載而傳播。爲使攻擊迅速奏效，分散式攻擊是常見的手法。
(3) 實體破壞：對資訊系統，尤其是政府(軍事、經濟、國防、外交等)重要資訊系統，進行破壞(Sabotage)，以癱瘓政府運作機能。另外，對電腦支援系統如電訊、交通、廣播電視、航空航海等指揮系統進行摧毀，以收震撼效果。

3.2 面對恐怖主義應有之心態改變

瞭解資訊恐怖攻擊方式及其可能產生之強大破壞作用之後，吾人應思考如何因應。依循 Yourdon 建議的「典範轉移」，具體的說，即是面對恐怖主義，吾人應有的認知及改變，因應無形的恐怖攻擊威脅，Yourdon 建議的思考步驟如下：

(1) 重新評估優先處理事項：以前認爲重要的，今日是否仍是最重要的？很多事項必須作適度調整，IT 人員必須做得的事，而不是只按「利潤」等法則在工作。
(2) 將要務重新審議：以 IT 人員來說，可能代表著重新強調工作的品質，尤其是優良的專案管理，以實作優良的系統。
(3) 協調個人、企業及國家的優先處理事項：由於系統的互連，任何一塊的塌陷，都可能造成整體的崩潰。
(4) 發展個人網路，以爲任何災變預作準備：利用多點互連的方式，提高整體的安全性。

基於以上的思考模式及恐怖攻擊可能發生的客觀事實，人人必須知道：

(1) 認清世界的不可預測性，及早作準備；
(2) 建置預警系統，對即將發生的變化，及早提出警告；
(3) 認清資訊資產的重要性及其安全弱點。狹義的資訊資產包括硬體、軟體及資料。

Yourdon 認爲資訊安全，人人有責。他對個人、公司主管、資訊專業人員，以及政府領導都提出具體的建議。就風險管理的角度來說，

(1) 政府主管：應考慮長期性、制度性的風險管理系統之建置；且必須誠實的將可能資安威脅告知民眾。
(2) 公司主管：不可短視近利，而忽視對強化系統安全的投資。
(3) IT 人員：秉持良知，做好資訊安全工作，從系統設計到建置及運行，均應將安全列爲重要議題。
(4) 一般民眾：配合政府的安全措施，舉報任何安全危疑事物。

爲免於恐怖攻擊所可能造成的全面癱瘓，Yourdon 建議今後系統應朝向彈性系統、適用性系統來開發。另外，緊急應變系統是不可或缺的，備援系統是至關重要的。最後，萬一問題發生時，應當拿出「死亡行軍」的精神，在極有限的時間及資源下，完成不可能的(復原)任務。

3.3 情報/資訊管理與反恐作爲

誠如 B. W. Dearstyne 所說，恐怖份子利用情資處理手段得知美國安全上的弱點，得

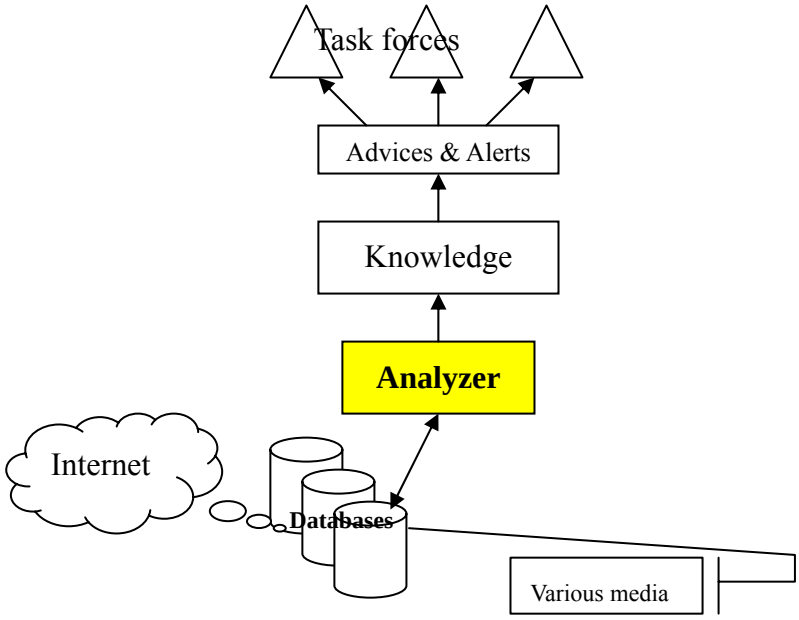
以遂行九一一攻擊，而美英兩國卻因情資研判錯誤而誤作攻打伊拉克的決策。可見國家的安全倚重良好的情資管理。在反恐鬥爭的作業中，情資工作反應了以下的缺失[Dearstyne 2005]：

- 情報領導與管理上有瑕疵；
- 對行動情報(Actionable Information)之蒐集、組織及表達有障礙；
- 有明顯可見的端倪卻無法做出及時的結論。

這些缺失與挑戰給我們的啓示是：

(1) 情報工作與資訊處理工作有共通處；但情報工作本質上是不可論斷的(Inconclusive)；
(2) 優良的領導是情報工作成功的關鍵；
(3) 組織文化是情報處理工作成功的重要因素；
(4) 人的因素是優良的情報處理最重要考量；
(5) 不確定性及資訊落差將累積錯誤，而造成武斷結論；
(6) 情資處理上的缺失將造成嚴重的後果。

有鑑於此，不少研究者便提出各種在恐怖主義時在的資訊管理架構，例如 Atrium 主張反恐知識系統之主要考量不應側重在精確的打擊[Demchak 2003]，而是在於何事吾人應該預先知道。利用組織互連概念，表現資訊系統的社會性，產生各種作業所需的知識及應用。一個反恐資訊系統架構，大抵如圖四所示：其中資料庫藉由特殊蒐尋引擎鉅細靡遺收集資料，經過分析之後，產生報告或預警，提供各專業機構(如國防或警察機關、民間企業)運用。



圖四：反恐資訊系統之架構

肆、各國反恐怖主義的具體對策

目前國際上進行反恐行動之目標概可歸結爲四個重點，即第一、終結國家對恐怖主義之支持；第二、建立與維持一種打擊恐怖主義之負責任的國際標準，以確認地方性之努力、提供行爲之評估基礎、擴大資訊交流及持續追尋互惠政策；第三、強化與維持打擊恐怖主義之國際努力，因此除了要與有意願與有能力之國家一起合作外，要持續談判「引渡暨相互法律協助條約」（Extradition and Mutual Legal Assistance）與擴大國際支持反恐戰爭之聯盟，並勸服與強制沒有意願之國家改變；第四、制止與破壞對恐怖主義之物質的支援等，特別是關於大規模毀滅性武器與飛彈擴散等方面，並且強調打擊恐怖主義組織需要直接與持續之「四D」行動，分別是「擊潰」（Defeat）、「拒絕」（Deny）、「消除」（Diminish）及「防衛」（Defend）。而支持恐怖主義的國家雖可以藉由政治施壓與經濟制裁改變其行爲，但是若要對付個別之恐怖主義組織與個別之恐怖份子，則這些戰術大部份都沒有效果。而必須經由設計之步驟，即先鑑定出恐怖份子，其次找出其藏匿地點，然後摧毀其計劃與行動之能力。[16]

資訊技術突飛猛進，這種資訊化、網絡化的趨勢已對政治、經濟、文化、軍事等不同的社會領域發生重要的影響。目前各國也競相投入相關方面的研究與發展，以在未來戰爭中搶得先機。本文將美國、中共、日本及我國的資訊作戰發展近況，以國防體系的作爲爲主，提供簡單的參考比較[17]。

4.1 美國

美國政府高度體認資訊作戰對國家安全的重要性，美軍在 2010、2020 聯戰願景中，均將資訊優勢視爲聯合作戰的基石，並持續性推動資訊基礎建設、作戰理念、機制、攻防技術與聯戰準則等的研究與發展。其發展重點包括：IO Cell 的運作、作戰理念與機制制訂；技術發展如目標網路的偵察能力、靈活準確的攻擊能力、對攻擊效能的評估能力；以及聯合作戰或政府部門協同資訊防護等近即時的情資共享等，都持續進行。爲因應未來的資訊化戰爭，美國加強推動的主要作爲，包含：

(一) 提昇人員資訊作戰素質：面對資訊時代的挑戰，美軍已把培養「資訊作戰勇士」納爲訓練重點，開設了專業培訓班，強化有關資訊軟、硬體的知識，期望全面提昇作戰人員的資訊素養，並建立「網路作戰部隊」。目前美國各軍種均已成立了資訊作戰應急反應部隊。

(二) 組建資訊作戰指揮機構：美國安全局已率先成立網路中心、國家安全委員會亦成立了國家保密政策委員會和資訊系統安全保密委員會，前者負責制定軍事安全保密政策及數位化戰場設計方案；後者負責軍事資訊傳輸主幹及數位戰場機敏資訊之安全保密管理。美國國防部則成立了聯合參謀部指揮與控制中心、聯合參謀部資訊戰局、資訊系統安全中心、國家保密局資訊戰處、國防大學資訊資源管理學院等機構。

---

[16] 資料來源：國際反制恐怖主義作爲，汪毓瑋，中興大學全球和平與戰略研究中心
參考 http://cgpss.nchu.edu.tw/modules/wfsection/article.php?articleid=357，存取日期 2006/12/09。

[17] 本小節，參考曾章瑞、陳志誠、張榮鋒，認識資訊戰、資訊作戰及政府應有軍政作爲，資通安全分析專論，2006/11/23。

(三) 組建資訊作戰專業部隊：美軍為了提高網路情報戰能力，特別成立專業網路作戰部隊，進行獲取其他國家的政治、經濟及軍事情資等任務；另亦成立了資訊作戰應變小組，以確保美軍網路正常運轉。

(四) 組建資訊網路保護特別小組：美國國防部已成立資訊網路保護特別小組，與各聯合司令部、軍種及其他機構協同工作，負責保護國防部計算機網路和系統免受入侵和攻擊。該小組負責將監控突發事件以及察查國防部各級組織系統的潛在威脅。同時，它還透過國家基礎設施保護中心與其他聯邦機構建立管道，以便透過基礎設施共享行動資訊。

前述美國國防部在 2006 年 2 月 13 日所發行的聯合資訊作戰準則顯示，美國對資訊作戰的運用，已完整發展結合各軍種的兵力，組合成可以執行不同作戰目的的資訊作戰小組（IO Cell），例如作戰安全(OPSEC)、軍事欺敵(MILDEC)、心理作戰(PSYOPS)、電子作戰(EW)以及電腦網路作戰(CNO)等五種的作戰模式，另以合縱連橫的方式，結合軍兵種實施可以高效支持核心聯合作戰之目的。

此外，美國目前亦投入微電機系統科技之研發，開發如指甲大小的微機械人，並具備自由行動與攻擊能力，將其置入敵方重要組織系統後，可自行潛爬進入敵方電子裝備中，等待作戰命令發揮作用。另外，美國也積極開發方向性能量武器，包括雷射和高能微波發射器，這些武器可摧毀電子裝備或是迫使系統失去功能。美國的研究人員甚至正在研究如何藉通訊將隱藏的指令送進敵方的電腦，未來這些指令可以負載在資料流上，藉由光纖管線傳送到電腦系統上，伺機進行系統破壞動作。由此可知美國政府及軍方的資訊作戰發展，具備多元、全向、硬軟體發展、略術一致、防護攻擊一體等特性。

4.2 中共

為了因應資訊戰的來臨，中共已多年積極致力於建立資訊化部隊，中共自稱網軍，以及相關的配屬支援能力整備。分析目前中共已執行的作法，約可歸納如下：

(一) 組建資訊作戰部隊：1999 年中共首創「網軍」一詞，此亦中共為了發展整體戰利，將建軍方向朝向「陸、海、空、天、電、網」一體規劃與發展的作戰思維。目前解放軍已陸續設置了若干專業資訊作戰部隊、資訊作戰武器及戰略研究等專責機構。基本上，中共已透過計畫性、步驟性的作為，整合與組建可支援戰資訊力發展的軍民教育單位、學術研究機構與信息作戰部隊。

(二) 調整軍隊規模結構：為了符合高科技戰爭的作戰需求，中共解放軍朝向「信息化條件的精兵路線」發展。目前解放軍正積極進行部隊調整，以建置小型、多功能、組織網狀化、指揮層級扁平化的高度整合型部隊，以因應「信息化聯合作戰」的需求。

(三) 培養資訊作戰基層幹部：誠如中共軍事戰略家彭光前上將所言：「專業化是解放軍未來的趨勢…我們尤其需要更多高教育水準的常備人員，以知識為基礎的高技術戰爭需要進行現代化。」為了達成上述目標，目前解放軍已開始招募大學生，並有計畫地甄選、補充與培訓部隊資訊作戰人才。

(四) 增加資訊作戰預算投資：自 1989 年起，中共的國防預算年年維持二位數成長。根據 2004 年美國國防部在《中共軍力報告》中的評估：目前中共一年的實際軍費支

出應高達 500 億美元以上，僅次於美國與俄羅斯，高踞世界第三。中共甚至已開始利用國家資源，擴大投資於解放軍的指管通情等資訊作戰能力上。

(五) 發展精密制導武器：根據美國公布的資料，近年中國已大幅擴張軍備，包括遙控感應衛星、先進造影系統、電子偵察衛星、利用低能量雷射「干擾」低地球軌道衛星的感應偵察能力、可攻擊地面目標的巡航導彈等。中共採購大批高新技術的武器裝備，再搭配精準制導式武器，已可有效提升打擊敵人資訊弱點的精準性。

4.3 日本

日本自衛隊在對未來資訊戰及其可能帶來的威脅進行了全面且深入的研究，也提出了多項加強措施。

(一) 成立資訊作戰專責機構:日本自衛隊在日本防衛廳內設置專門負責指揮和規劃資訊戰的「課」，三軍自衛隊也建立對應機構；自衛隊情報本部內設立緊急事態部，能即時彙總和處理各情報機關彙報之情資，以及美軍提供的情報，以提高情報的實效性及應變能力。

(二) 制定資訊作戰發展戰略：日本防衛廳在 2000 年發表的《關於信息軍事革命》研究報告，是指導日本自衛隊提高資訊戰能力的綱領性文件；而《2001-2005 年中期防衛力量整備計劃》則較爲詳細地規劃提高資訊作戰能力的方針、措施及所要達到的目標。根據未來資訊作戰和日本軍事力量的特點，日本自衛隊還制定了資訊作戰的七大基本原則，即「資訊化、一致化、迅速化、效率化、機動化、防護化以及互通化」，俾能達成順利與美軍實施聯合作戰。

(三) 擴大投入資訊作戰準備：日本已將武器裝備研製和獲得的重點將放在資訊作戰，內容上將包括製造軍用偵察衛星、研制戰區導彈防禦系統等。

(四) 加速整合 C4I 系統：日本防衛廳總部已成功整合中央資訊系統、陸上自衛隊參謀部、海上自衛隊參謀部、航空自衛隊參謀部及情報支援等五大系統，將可即時彙整三軍自衛隊的情資，以作爲戰略決策的參考依據。

4.4 我國

我國軍事體系的資訊作戰發展擘劃，係由參謀本部通信電子資訊參謀次長室負責。自民國 90 年迄 95 年間，歷經統一通信指揮部、通信資訊指揮部與資訊作戰指揮部三階段轉型發展，目前已正式以資訊作戰爲主軸，持續經營與發展資訊作戰戰力。現階段，國軍通信電子資訊的整體規劃與發展，係依「有效嚇阻、防衛固守」之戰略指導及聯合作戰需求，達成爭取「資電優勢、鞏固國防、制敵機先」目的。同時，也本著平、戰時結合的理念，推動下列主要政策：

(一) 國防資訊基礎建設：配合國家資訊基礎建設（NII）各項推動方案，全力推動國防資訊基礎建設，主要任務爲建置「國軍資訊傳輸主幹」等相關網路，以提供軍事戰情、指管、人事、後勤、財務等系統資訊傳遞與交換，並運用各網路與各地區構連交換資訊。目前正持續依任務需要，賡續擴增網路交換中心及擴充骨幹網路頻寬，並運用民間固網公司的數據網路，建置軍事備援系統，以提升軍事網路的運作效益

及戰場存活率。

(二) 建立優勢資訊作戰戰力：國軍資訊作戰係以確保「國防通信、資訊系統及網路安全」爲目的，依「防護爲先、快反先制」的指導，採「主動監偵、積極防護」諸般手段，建立「早期預警、應變制變」的通資安全防護能力，期確保通資優勢。爲使國軍具備因應電腦病毒戰的反制能量，已經成立資訊作戰專業部隊，持續配合通資安全關鍵技術等研發專案，建立國軍病毒監控與防治技術研製能量。

(三) 有效整合通資網路：爲因應未來作戰任務需求，新一代軍事通資裝備系統的構建將持續推動，期整體規劃與整合電信資源，並加強通資系統作業環境與平臺整合，以整合軍種與聯戰網路爲目標，建立作業相容、程序一致的三軍聯合作戰通信系統。

(四) 整合指管通資情監偵系統：爲發揮三軍新一代兵力統合戰力，賡續建置一體性指管通資情監偵系統（C4ISR），構連三軍指管系統與武器平臺，俾同步交換即時情資，提升戰場透明度，消弭戰場迷霧，構建「看得到、聽得到、能指揮」的即時指管決策系統，爲我國建立資訊優勢，發揮資訊作戰能力的關鍵目標。

(五) 強化電子戰作業能量：針對未來戰爭型態與聯合作戰需求，全力推動電子戰戰備整備，包含攻守兼備的電子戰力與頻譜資源管理能力，並須確保通信紀律與資訊安全防護，以提升國軍資訊整體作戰戰力。

4.5 我國的資訊戰準備

鑑於資訊戰的範圍包括「資訊運用」與「資訊防禦與反制」等，國軍近年來經過多方面的努力，在近年漢光演習的驗證中，已獲得具體成效；然而後續如何整合國防資訊基礎建設，建立三軍通用的自動化數據傳輸鏈路，以及未來應如何擴大運用民間資源、凝聚共識，並由各單位依任務特性，以「三軍聯合作戰」的觀點，就通信、資訊及電子戰的戰備整備、教育訓練、通訊/資訊人力資源管理及後勤補給保障等方面持續改良精進，是爲現今國防通資政策重要課題。國防部爲有效整合現有國家與社會資源，建立更精實的國防通訊/資訊/電腦系統，滿足各軍種及三軍聯合作戰需求，有效提升國軍整體戰力，正全面性積極推展各項具體作爲，其執行重點如下[18]：

- 有效整合通信網路：
  傳輸平台之建設是爭取「資訊優勢」之關鍵要素；國防部指管通情及資訊傳輸系統之整合，係以建立三軍通用戰術聯戰網路爲目標，結合國軍有線/無線電通訊系統及民間通訊資源，形成軍民共用多重節點、複式網路的通聯手段，以充分有效運用整體國家資源，建構多備援系統，提升通資戰力，有效支援作戰。
- 強化電子戰作業能量：
  針對未來戰爭型態、電磁戰場環境、敵情威脅及軍種作戰需求，國防部正全力推動國軍電子戰戰備整備工作。依照國軍未來電子戰作戰構想及任務特性，進一步強化電子戰對抗能力，除頒行「國軍電子戰作戰構想及專業單位（部隊）規劃」，指導三軍電戰部隊定期演訓外，並責成中科院研製先進電戰裝備，以加速推動國軍電子戰戰力整備，建立一個局部優勢跨越陸、海、空域的整體電戰防護網，以發揮部隊

[18] 本小節所提各點主要參考資料是國防部六月十九日記者會通信電子資訊局資料而整理。

整體戰力。

- 建立優勢資訊戰力：
  資訊戰防禦首重「安全」。國軍基於當前戰略構想，且考量資訊安全應以網路防護爲優先，目前資訊戰的重點乃在網路安全防護，且以全方位思考與創意運用爲原則，發展安全防護機制與系統裝備，朝向構建自動化、系統化以及資訊化之安全防護系統目標邁進。由被動性的防護進而建立主動性的監控偵察能量及反制作爲，同時結合產、官、學、研各界能量，構建國防自主能量，俾確保國軍在資訊戰場的優勢，以維護台海均勢，保持和平。另因應未來中共資訊戰的威脅，國防部已指導由「通信資訊指揮部」及三軍總部積極進行各項資訊戰相關作爲之規劃作業，以利在未來的資訊戰領域中，能發揮克敵致勝預期的效果。
- 落實國軍頻譜管理：
  爲落實「國家電信自由化」政策，國防部完成「國軍頻譜資料庫自動化管理系統」之建置，以有效管理軍用頻率，確保通信紀律及通資安全，提升國軍無線電頻率使用效率。
- 籌建聯戰指管鏈路：
  數據資料鏈路爲未來戰場掌握情資、有效遂行指揮管制、發揮火力之首要工具，國軍秉持一貫強化戰備理念，並考量聯合作戰需求與指導，正依據現況賡續整合三軍通資現有能量，並充分運用民間科技，整體規劃並建置出一套完整的國軍指、管、通、情、資訊系統及三軍共通的自動化數據傳輸鏈路，俾以整合、提升新一代兵力、武器系統之有效戰力。
- 嚴密管控通訊/資訊安全：
  爲配合政府資通安全政策及因應近年國軍資訊網路蓬勃發展，國防部已積極規劃建置國軍資訊戰防護及通資訊緊急應變、制變作業能量，目前正逐步發展各軍種積極資訊防護及主動網路監控偵察能力，以確保三軍部隊通資安全，維持部隊完整指通力、機動力、打擊力，鞏固部隊安全。

伍、資訊反恐的分析與作爲

2006 年 7 月 11 日在印度的孟買又發生了一起火車爆炸攻擊事件[19]，並且造成至少兩百人死亡，面對這突如其來的爆炸，各國領導人紛紛進行譴責，也激起了各界對於反對恐怖主義的決心。就IT觀點而言，反恐的作爲應由發現恐怖主義資訊開始，再提出安全防護對策。以下分別論述之。

5.1 發現恐怖主義資訊

由於恐怖主義的匿蹤性，發現恐怖主義資訊這成爲首要任務。恐怖主義相關資訊包括恐怖份子的行蹤跡、恐怖份子的組織及人際網絡、恐怖份子的經濟來源、恐怖活動之計畫、恐怖主義之文宣等。發覺恐怖主義資訊的方法有：

(1) 利用特殊蒐尋引擎：例如 e-Detective[Chen 2000]即可用來在網路上蒐尋恐怖犯罪資

[19] http://www.epochtimes.com/b5/6/7/13/n1384224.htm，存取日期 2006/12/09。

訊。

(2) 利用網路分析方法：如 CopLink 系統[Chen et al. 2003]可以用來自動連結犯罪者與犯罪者、犯罪行爲與犯罪行爲、犯罪者與犯罪行爲之間的關係。我國刑事局刑案知識庫亦備有此類蒐尋工具。

(3) 利用網路監聽技術：利用傳統的電話監聽技術，掌控可疑電話之通聯，惟須得到檢察官之許可[江舜明 2005]。此外，由於電話、資訊網路及電話之整合(Computer-Telephony Integration)，監聽之範圍必須擴大於網路電話(Voice over IP)及未來無線寬頻網路，其技術多樣，可參考[Milanovic et al. 2003]。

(4) 蒐尋傳統平面媒體之資訊：雖然犯罪已逐漸 e 化，但部份不法者反而會利用傳統報紙等平面媒體，作爲他們的聯絡及發佈消息之管道。

5.2 資訊之安全防護

現在恐怖份子攻擊的方式有很多種，有的是利用資訊技術入侵政府或是企業竊取機密，或是散佈假消息、有的是以劫機或劫船的方式來獲取目的、也有的是利用散播病毒如炭疽熱、還有的是直接以炸彈攻擊的方式或是以自殺式攻擊讓人措手不及。但其中影響最大的應該算是資訊作戰，因爲資訊產品不斷的推陳出新，手機普及率越來越高，網路的使用更是無遠弗屆，因此若是恐怖份子所採用的攻擊方式是屬於資訊戰，可以說是最方便取用，而影響的範圍也會是最廣的。

因此，在於反恐的具體作爲上，除了防護人身的安全之外，資訊戰的安全防護也是相當重要的一環，以下也提出了幾點看法：

(1) 反制恐怖主義散播的訊息，避免將恐怖主義的思想傳送到人們心中，使其組織逐漸龐大，避免人們盲目地追從；或有效的防止恐怖份子散佈不實謠言。

(2) 建置更安全的資訊防衛系統，避免駭客入侵國家政府部門，破壞人民生活秩序與竊取國家機密文件。

(3) 建立精確及完整的身份辨識系統，在各個重要地點如機場、地鐵或公車上，利用臉型、虹膜或是指紋來辨識身份，以確保在公共場合的個人安全，這也有助於犯罪率的降低或破案率的提升。

(4) 阻斷或干擾恐怖組織或個人間溝通管道。

(5) 以媒體資訊戰譴責恐怖主義，發動全民的力量共同來抵禦恐怖行動，讓恐怖主義無所遁形。

(6) 完整進行恐怖主義情蒐作爲，才能再意外發生前預先制止。

由於網路化的影響，使得財政、通訊、軍事等各個系統皆透過網路緊密相連，使得反恐作戰又更加複雜。全球化是種趨勢也不斷的進行中，它帶給多數人方便與利益，也使得國與國之間的界線不再如此分明，而各國的防恐標準都不盡相同，無形間也帶給了恐怖主義者機會。

5.3 反恐資訊戰之未來發展

世局變化，瞬息萬變，尤其是恐怖主義的發展，更令人難以捉摸。立足此刻，展望

未來，我們應特別注意以下幾個動向：

(1) 由於生化武器攻擊的應用，產生了所謂生物恐怖主義(Bioterrorism)，因此我們也應注意感染性疾病資訊(Bioterrorism & Disease Informatics)之研究。[Berndt et al. 2004]提供了這方面的分析技術。

(2) 資料探勘(Data Mining)是發覺恐怖資訊的利器，必須持續研究。由於恐怖主義的國際性特質，多語言資料檢與探勘技術尤其應加強[Last et al. 2006]。

(3) 發展詐欺偵測(Deception Detection)技術：欺騙、僞裝是恐怖份子掩蔽身份的手段，也是他們入侵資訊系統的方法。身份確認是資訊安全的第一步，惟有良好的防僞措施，方能阻止不法份子進入政府/企業資訊系統。

(4) 加強基礎設施防護(Infrastructure Protection)及災變回復能力(Disaster Recovery)：由於恐怖攻擊的事實存在，系統應將資訊分享與協同作業(Collaboration)概念融入於設計中。另外，也應作好復原的應變措施[Shao 2004]。

陸、結論

未來的戰爭模式將趨向於多元化，速度和即時的資訊將掌握整體的勝敗關鍵，「資訊戰」也是在這種趨勢下發展出來的新型態戰爭模式，而情報的收集及防護上，可藉由密碼及浮水印等加密技術獲得保護；而恐怖份子的資訊，可藉由身分辨識系統的提昇及普遍應用，讓各國加強安全防護設備，使得恐怖主義無所遁形。也由於近來恐怖事件接連發生於各國重大城鎮，使得恐怖主義逐年受到各界的重視，也突顯出反恐行動是一刻也不容停緩。

在維護國家資訊安全的戰術思維與行動上，政府與國防軍事部門都必須瞭解，資訊作戰的核心力量爲人才與技術能力，並需建構安全的「資訊系統網路平台」，俾確保政府、軍事與民間重要產業等，所使用的資通基礎建設，都能免於敵人的破壞，俾從整體資訊安全環境中，發揮各類組織正常運作的效益。

總之，現代高科技與高資訊化下的作戰，無論攻與防，資訊作戰都已成爲決定戰場勝負關鍵因素。憑藉資電優勢來控制戰場與奪取勝利，在現代化戰爭型態中已是不爭的事實。國軍面對中共的嚴重威脅，已戮力發展各項資訊作戰系統與戰術戰法，旨在爭取資訊優勢。惟其他有關對於非軍事的政治、經濟、心理、社會、文化等層面的發展，政府更要迫不容緩，加緊整合發展，如此方能因應新時代資訊作戰型態的特性，確保國家的安定與發展。

參考文獻

[王湘穗、喬良 2004] 王湘穗、喬良，*超限戰*，左岸文化，2004。

[江舜明 2005] 江舜明，論監聽處所限制與手段之正當性，月旦法學，127 民 94.12 頁 149-164。

[陳志誠 2005] 陳志誠，資訊戰及其對國家社會安全之影響，*資通安全分析專論彙編*，國家實驗研究院科技政策與資訊中心，Dec., 2005，第 133-155 頁。

[陳志誠等 2006] 陳志誠、曾章瑞、彭彥倫，資訊戰在反恐怖主義之具體作爲，*資通安全分析專論彙編*，國家實驗研究院科技政策與資訊中心，June, 2005。

[凱文 2002] 凱文(譯)，*驚爆資訊戰－911 事件對資訊科技的影響*，培生教育出版，2002。原著: E. Yourdon, *Byte War*: The Impact of September 11 on Information Technology, Pearson Education, Inc. 2002.

[彭錦珍 2004] 彭錦珍，資訊時代中共國防現代化之研究－解放軍資訊戰發展及其對台海安全之衝擊，復興崗學報，2004，82 期，頁 187-218。

[曾章瑞等 2006] 曾章瑞、陳志誠、張榮鋒，認識資訊戰、資訊作戰及政府應有軍政作爲，*資通安全分析專論彙編*，國家實驗研究院科技政策與資訊中心，Dec.,2006。

[曹邦全 2002] 曹邦全，中共信息戰之研究，國立中山大學大陸研究所碩士論文，2002。

[國防報告書 2006] 中華民國國防部，2006 國防報告書，2006 年。

[國家安全報告 2006] 中華民國國家安全會議，2006 國家安全報告。

[Berndt et al. 2004] D. J. Berndt, S. Bhat, J. W. Fisher, A. R. Hevner, and J. Studnicki, Data Analytics for Bioterrorism Surveillance, Second Symposium on Intelligence and Security Informatics, Tucson, June 2004, pp. 17-27.

[Chen 2000] P. S. Chen, An Automatic System for Collecting Crime Information on the Internet, *Journal of Information, Law and Technology*, 2000, Issue 3.

[Chen et al. 2003] H. Chen, D. Zeng, H. Atabaksh, W. Wyzga, and J. Schroeder, COPLINK: Managing law enforcement data and knowledge, Communications of the ACM, Vol. 46(1), 2003, pp.28-34.

[Dearstyne 2005] B. W. Dearstyne, Fighting Terrorism, Making War: Critical Insights in the Management of Information and Intelligence, *Government Information Quarterly*, Vol. 22, 2005, pp.170-186.

[Demchak 2003]C. C. Demchak, "Atrium"──A Knowledge Modelfor Modern Security Forces in the Information and Terrorism Age, Intelligence and Security Informatics, LNCS 2665, Springer, 2003, pp. 223-231.

[Jones 2005] A. Jones, Information Warfare －what has been happening?, *Computer Fraud & Security*, Nov. 2005, pp.4-7.

[Last et al. 2006] M. Last, A. Markov, and A. Kandel, Multi-lingual Detection of Terrorist Content on the Web, Intelligence and Security Informatics, LNCS 3917, Springer, 2006, pp. 16-30.

[Medd & Goldstein 1997] R. Medd & F. Goldstein, "International Terrorism on the Eve of a New Millennium", in *Studies in Conflict and Terrorism*, Taylor & Francis, 1997.

[Merritt et al. 2004] S. M. Merritt, A. Stix, and J. E. Sullivan, Security Informatics: A Paradigm Shift, Second Symposium on Intelligence and Security Informatics, Tucson, June 2004, pp. 516-517.

[Milanovic et al. 2003] A. Milanovic, S. Srbljic, I. Raznjevic, D. Sladden, D. Skrobo, I. Matosevic, Methods for Lawful Interception in IP Telephony Networks Based on H.323, IEEE Computer as a Tool, Vol. 1, pp. 198-202, Sep. 2003.

[Shao 2004] B. B. M. Shao, Optimal Redundancy Allocation for Disaster Recovery Planning in the Network Economy, Second Symposium on Intelligence and Security Informatics, Tucson, June 2004, pp. 484-491.