RDEC-MIS-089-014

中共發展「信息戰」對我國建立資訊安全制度影響之研究

行政院研究發展考核委員會編印

中華民國九十一年四月

RDEC-MIS-089-014

中共發展「信息戰」及對我國建立資訊安全制度影響之研究

受委託單位：財團法人國家政策研究基金會

研究主持人：李英明

研　究　員：溫洽溢

研究助理　：魏澤民

研究助理　：陳美娜

行政院研究發展考核委員會編印

中華民國九十一年四月

目　次

圖次

表次

提 要

關鍵詞：資訊戰、信息戰、電子化/網路化政府、資訊安全、安全稽核

一、研究緣起

八０年代初，美國社會預測學家艾文.托夫勒(Alvin Toffler)所著的**《第三波》**（The Third Wave）一書問世。這本書著重從人們眼前看到的生活變革的事實入手，分析了人類社會文明正由工業社會走向資訊社會（Information society）並提出了資訊社會完全不同於工業社會的生產方式、工作方式和生活方式。這本書的出版，引起人類對資訊時代的重視，有人開始研究資訊時代的戰爭。一九九０年十一月，托夫勒的另一本研究資訊社會的書－**《權力的轉移》**（Powershift）出版。在這本書中，首次提出資訊（信息）戰（Information warfare）的觀念，但這不是從軍事意義上講的，而是從市場意義講的。一九九三年，托夫勒的**《新戰爭論》**（War and anti-War）一書出版，開始將眼光由社會移轉至軍事領域，一時之間有關資訊（信息）戰的研究蔚為風潮。

在一九九０年波灣戰爭中，中共看到美軍在遙遠的華府運籌帷幄，藉著高科技的電子設備竟能指揮調動自如，不但掌握了戰場的資訊，又能反制伊拉克使用電子設備，徹底掌握戰場而打一場絕對勝利的高科技戰爭。而這場高科技武器主宰的戰爭型態所呈現的戰場盛況，正是以美為首所倡導的「軍事軍務革命」（Revolution in Military Affairs,RMA），其中「資訊戰」（中共稱為信息戰），正是這場軍事革命的主要特質之一。根據了解中共認為發展信息戰可以獲得最佳作戰效益，癱瘓敵方金融、交通、電力、電信及軍事核心機制。因此中共面對以美國為首的這場革命，亦積極學習推動，企圖趕上這一場軍事革命潮流。

本研究計畫將從不同面向對廣義的資訊(信息)戰試圖賦予嚴謹的定義與描述，再據此研析中共發展高科技「信息戰」的發展現況，從而探討中共發展信息戰對我國目前推動電子化政府產生哪些層面的影響？尤其是我國在建構電子化政府的同時，面對中共發展高科技信息戰的威脅，將會對我國建立安全稽核制度產生哪些方面的衝擊？這些問題都是本計畫亟欲解決的。因此本研究計畫希望透過對中共發展高科技信息戰進行研究，從而對照我國在建構電子化政府同時，在建立資訊安全稽核制度上尋求提出政策因應上的建議。

二、研究方法及過程

本研究計畫基本上是認為在世紀之交來臨之前，資訊（信息）時代正邁著震撼寰宇的步伐向我們走來。以波灣戰爭為標誌，一種新的戰爭型態-資訊（信息）戰正在形成和發展。由於資訊（Information）具有全球化，非線性效應、光速傳播、多方共享、用之不竭等特性，因此若能操縱和控制戰爭中的物質和能量，則必能大大提高作戰效能，並減少其他戰鬥力要素的投入。因此，資訊既是力量倍增器，又是重要戰略資源。

所以本研究計劃將從文獻研究著手，藉由對相關研究參考文獻的研析總結出資訊（信息）的特質，再依此特質有系統地透過實證資料的整彙，瞭解當前中共發展高科技「信息戰」的形式與可能發展趨勢。亦即從廣義的資訊時代下的戰爭型態進行分析，從而描繪出中共發展「信息戰」的現況，並於瞭解其現況後，深入探究中共發展高科技「信息戰」對我國在建構電子化政府上關於建立安全稽核制度所造成衝擊，進而提出政策因應之建議。

三、重要發現

中共在研究資訊（信息）戰進程上，雖然起步比台灣早，且在戰術戰法上已有相當成果，但在資訊科技上的基礎實力與技術仍處於初級研發階段，主要原因之一是中國大陸的資訊產業係以代工生產為主，實無研發能量可言；相反地，在我國國內民間長期累積的資訊科技能量（尤其是電腦病毒攻防技術）則是相當可觀的。連美國國防部在其最近的「台海安全情勢報告」[1]中都特別指出國內在這一方面居全球領先地位。不過，若從發展的層面來說，中共在資訊戰的發展上，是以國家層級來推動，並且還包括「戰略、戰術、戰鬥與戰技」等不同層次，不但顯現其結合戰略研究與科技研發的努力與決心，更充分表明了中共在未來以資訊科技主導的戰爭中採用非傳統與「不對稱作戰」方式之企圖；反觀我國，雖大力推動資訊發展，但相對地卻對資訊相關設備之依賴日益加深，而我國又因社會變遷，人民危安意識淡薄，使得現階段我國資訊戰的發展僅止於軍事層面，而關係民生甚鉅之各種金融、電信、電力與交通運輸及當前政府所推動的電子化/網路化政府等計畫中各種資訊系統已成為中共之最佳攻擊目標而不自覺，儼然成為國家安全之嚴重隱憂。

我國目前正朝建構電子化/網路化政府的目標前進，並同時面對中共以資訊戰 --電腦病毒「軟殺」和實體破壞「硬殺」方式企圖癱瘓我

---

[1] （一九九九）二月，美國國防部向國會提出台海安全情勢報告，在報告中指出，中共領導人迄今拒絕公開表示放棄對台動武，並揚言一旦台灣宣布獨立，或有外國勢力介入與統一有關之事務，將激起中共武力犯台。另外，中共也重申如果台灣擁有核武，則將提前對台動武。詳見楊志恆，＜從「兩岸軍力平衡」報告看台灣國防安全＞，http://www.kmtdpr.org.tw/4/49-5.htm

國政府運作。我國因應「軟殺」之道，應是將指揮管制系統採實體隔離措施，減少病毒入侵機會；因應「硬殺」之道，則應首重長程預警能力，其次是系統採分散式設計，以避免因破壞而喪失政府運作能力。

四、主要建議事項

(一)、立即可行性建議

1. 訂定專法規範網路行為（主辦機關：法務部；協辦機關：行政院研考會、交通部、行政院新聞局）：隨著網路快速發展，各種利用網路所進行的破壞與犯罪問題也逐漸出現。為解決網路對社會所帶來的衝擊，國內主管機關可以考慮甚至進一步對網路脫序問題就相關法規進行研究、增修或廢止。

2. 建構資訊網路安全防護網（主辦機關：交通部；協辦機關：行政院研考會、國防部、法務部）：網際網路目前的發展，可以用美國大西部的拓荒期來形容，當我們使用網路愈頻繁，對網路的依賴愈深，就愈需要在這個西部蠻荒建立一些文明的準繩。目前政府機關的電子化／網路化正處於初級發展階段，系統主機內可能並無重要資料，不過，當系統處理的資料份量增加後，安全機制的防護若未能改善的話，私密資料遭盜竊刪改的潛在危機將不時面臨，且當被盜竊的資料成為機關內部的人事資料、機密檔案或重要報表時，其間所潛藏的危機就不是任何系統管理者可以承擔的，這樣的問題也正是電子化／網路化政府未來的隱憂。對此，建構一全面性的資訊網路安全防護網是必須進行的工作，而這一全面性的資訊網路安全防護網，基本上，應具備以下功能：

(1)、使用者付費：今天，有心人士可以肆無忌憚的用垃圾郵件發動攻擊，而且完全不必負擔任何費用，所以他們何樂而不為？不必付費的

資源，一定會被濫用而導致浪費。如果攻擊者必須為所發出的所有訊息付費，攻擊的規模就不可能太大。如果受害人也必須負擔攻擊者的成本，則要竊取他人的帳號就不會太容易。如果竊用他人帳號的竊賊眾多，則市場必定會出現防制的安全產品。

(2)、分級計價：藉著依服務等級計價收費，便可以兼顧網路的開放型與創意空間特性。為全民或團體提供類似聯邦快遞般的高價值服務，例如，如果你願意出示身分並付出一定的費用，則可以享受某種品質等級的服務；如果你不願出示身分且堅持免費，仍可享受基本的服務，但不保證垃圾郵件的騷擾，如此，網路最可貴的創意空間仍可保留。

(3)、來函身份顯示：對那些毫無限制的網路訊息，們有必要知道發信者的身份；否則要如何清算帳目與建立活動規範？沒有身份，就無法辨別伺服器上流通的資料封包到底是誰的。和在汽車上懸掛牌照一樣，我們送到網路上的資料封包上面也應該加蓋所有人的印記，這樣才能辨別封包所有人並執行傳遞的規則。付出較高等級費的服務，必須有相對的數位認證，以便取得優先使用網路資源的權利。

(4)、硬體的安全防護：個人電腦非常不安全，因為它設計時，安全根本就不在考慮之列。所幸，一些安全性較佳的網路通路設備已陸續問世。這些「個人通信器」內建防止破壞的身份辨識晶片，又有密碼或生物檢測設施，安全性遠較個人電腦為佳，很適合做為儲存數位鈔票的地方。

有了資訊安全防護網之後，仍須對資訊系統安全稽核管理，而這可透過下列各種方式來進行：

(1)加強訓練政府業務單位及主管。
(2)培育專責稽核單位。
(3)各機關擬定標準作業規範。
(4)任務編組，進行設定資訊安全及稽核相關法規之增修。

(5)定期舉辦研討會，提供資訊系統安全稽核技術與工具教育訓練。
(6)宣導 Data Owership 觀念，建立 Data Owner 權益受損通報管道。
(7)確實執行稽核，執行從嚴。

3. 制訂法令獎勵研發資訊安全科技（主辦機關：行政院國科會；協辦機關：行政院研考會、交通部、行政院新聞局）：藉引進國外技術、整合軍民專才，並結合市場機制獎勵研究密碼技術及相關資訊網路攻防科技。

4. 結合產官學研與推展委外政策（主辦機關：行政院研考會；協辦機關：交通部、國防部、法務部、行政院國科會、行政院新聞局、）：資訊科技屬軍民通用科技，國內民間與學術單位資訊科技潛力雄厚。是故應落實資訊業務委外服務, 有效整合民間業者, 公民營研究機構、政府機關等單位，透過諮詢顧問、委外合作方式，加強資訊戰綜合性理論研究，以落實資訊安全建設，以擴大政府資訊產能。

5. 確立政府部門及民間產業的角色扮演及法規制訂（主辦機關：行政院研考會；協辦機關：交通部、國防部、法務部、行政院國科會、行政院新聞局）：為維護國家的資訊安全, 資訊戰因應措施必涉及政府部會、立法部門及公民營產業。在民主社會中不同立場之角色扮演, 包含政府公權力尺度、立法寬嚴、產業運作機制及人民自由權益約束度等都需審慎考量。其折衷原則須能至少包含「最起碼不可或缺的資訊基礎架構」, 亦即是說, 平時能防範對國家社會的不當騷擾及破壞, 戰時則能確保起碼的政府、產業及民生運作機制，以及軍事任務之必要需求。此項角色扮演及法令規章的制訂，需要許多專業論辯方能完成，故宜儘早實施。

6. 逐步推廣資訊戰教育與基礎訓練及研究，成立研究所、訓練中心等專責機構（主辦機關：行政院國科會；協辦機關：交通部、國防部、教育部、法務部、行政院研考會）：除了積極汲取先進國家資訊科技，

發展我國資訊戰武器裝備之外，還應迅速結合民間、政府、研究機構共同成立資訊戰研究中心或研究所，共同發展資訊安全的能量，並積極推動資訊戰法、武器之研究模擬。最後應將結合的研究成果擴大應用於電子畫/網路化政府的工作項目上。

7. 成立各級政府資訊安全專責單位（主辦機關：行政院研考會；協辦機關：內政部、外交部、交通部、國防部、法務部、經濟部、財政部）：隨著所謂電子化政府的到來，政府資訊安全的問題也應該隨之得到重視，因此，建議各級政府能增設資訊安全相關部門，針對一般網路駭客(hacker)甚至來自於中共的資訊破壞，有一防堵的作用。

8. 建立可信賴度電腦產品驗證組織與標準（主辦機關：內政部；協辦機關：外交部、交通部、國防部、法務部、經濟部、財政部、行政院研考會）：可由交通部研議，與民間相關科技企業合作，以企業現有的技術及人力，配合並執行政府所訂定出來的電腦產品驗證標準。此一方面可以節省國家資源，另一方面，則可在短時間之內建立可行機制。

9.健全模擬演練機制（主辦機關：內政部；協辦機關：外交部、交通部、國防部、法務部、經濟部、財政部、行政院研考會）：由行政院統合成立跨部會資訊小組，在假設遭遇不明網路資訊破壞時的情況下，研擬一套演練機制，能在最短時間內圍堵破壞根源，並進一步予以反制。

（二）、中長期建議

1. 推動國家層級資訊戰指揮機制（主辦機關：國安會；協辦機關：內政部、外交部、交通部、國防部、法務部、經濟部、財政部、行政院研考會、行政院國科會）：資訊戰涵蓋範圍廣泛，舉凡政治、心理、經濟、科技和軍事各領域，均為中共運用資訊技術手段爭奪資訊優勢的

目標。職是之故，建立國家層級資訊戰指揮機制，宜由總統府與行政院共同主導，結合國家安全局與內政、外交、國防、財政、教育、法務、經濟、交通等部會，針對電力、電信、金融、交通等國家基礎建設之安全防護，共同研擬相關因應作為。

2. 建立國家多層、多頻、多型的模式資訊網絡架構（主辦機關：行政院研考會；協辦機關：國防部、行政院所屬各機關）：藉建置多層、多頻與多型複式網絡體系，提升資訊網路的存活度，以降低中共或網路駭客的攻擊效益。尤其更應建構一套「資訊戰模組」（Information Warfare Model）即所有政府單位與軍事的指揮、管制、通訊、資訊、情報系統，均應仔細推敲在資訊戰下是否能正常的發揮功能，並推演替代功能設備與替代方案。此外，建立資訊戰鬥部隊編裝，並修訂軍職專長也是迫切應進行之工作。

3. 製訂國家資訊安全管理、預警及危機處理機制。（主辦機關：行政院研考會；協辦機關：國防部、交通部、行政院新聞局、行政院國科會）：推動資訊安全管理，預警及危機處理機制是大家的共識，而這是一個需要長期投入的工作。建議可從專業證照的角度切入，進而加強資訊安全人才的培訓並建立一個專職機構，這個專職機構可稱為資訊安全防範小組，專司下列五項工作：

(1)各單位資訊安全政策的核定、監督與管理。

(2)各單位之資訊資產的保護與預警制度。

(3)各單位所應擔負資訊安全責任之分配，以及各單位的協調，致力將資訊安全觀念融入政府文化中。

(4)資訊系統遭破壞或入侵後危機處理機制之建立。

(5)以「軍民一體」理念，制訂「國家資訊安全管理及危機處理」相關法令，有效運用珍貴資訊資產。

4. 以全民國防理念推動全民資訊戰教育（主辦機關：國防部；協辦機關：教育部、法務部、行政院新聞局、行政院研考會）：非軍事資訊

戰防不勝防，其反制之道，在於政府、產業、媒體、官員與民眾等，都要具備資訊戰相關知識，並能了解中共資訊戰的手段與影響，俾能降低中共資訊戰奇襲效應，並於必要時配合政府發揮反制效果。

5. 鼓吹國際訂定反資訊恐怖行動公約，以遏止中共資訊戰威脅。（主辦機關：外交部；協辦機關：國防部、教育部、行政院新聞局）：藉國際輿論與專家學者聯合造勢，將資訊戰非軍事運用視為國際恐怖主義行為，期以國際公約遏阻中共資訊戰對我國之奇襲行動。

6. 藉與先進國家資訊互動及技術交流提升我國資訊安全的實力（主辦機關：國防部；協辦機關：交通部、外交部、教育部、行政院國科會、行政院研考會）：例如我國可運用「台灣關係法」，使美國將資訊安全與危機處理納入其對我國安全維護的承諾範圍，或者定期指派學有專精的學者專家赴國外進修、參訪、座談進行技術交流。以利我國資訊安全技術之獲得建立我國資訊研發優勢。

7. 全方位評估中共資訊戰對我國政治、軍事、經濟、社會之影響。（主辦機關：國安會；協辦機關：國家安全局、法務部、國防部、外交部）：編制預算並責由專業小組研究包含政治、經濟、社會心理、外交及軍事等層面，全方位評估中共各種資訊戰威脅與影響。此項研究涉及層面廣泛，推動時機愈早愈好。

第一章　緒論

第一節　研究動機與目的

八０年代初, 美國社會預測學家艾文.托夫勒(Alvin Toffler)所著的《第三波》（The Third Wave）一書問世。這本書著重從人們眼前看到的生活變革的事實入手，分析了人類社會文明正由工業社會走向資訊社會（Information Society）並提出了資訊社會完全不同於工業社會的生產方式、工作方式和生活方式。本書的出版，引起人類對資訊時代的重視，有人開始研究資訊時代的戰爭。一九九０年十一月，托夫勒的另一本研究資訊社會的書－《權力的轉移》（Powershift）出版。在這本書中，首次提出資訊（信息）戰（Information Warfare）的觀念，但這不是從軍事意義上講的，而是從市場意義講的。一九九三年，托夫勒的《新戰爭論》(War and Anti-War：Survival at the Dawn of the 21st Century)一書出版，開始將眼光由社會移轉至軍事領域，一時之間有關資訊（信息）戰的研究蔚為風潮。

在一九九０年波灣戰爭中，中共看到美軍在遙遠的華府運籌帷幄，藉著高科技的電子設備竟能指揮調動自如，不但掌握了戰場的資訊，又能反制伊拉克使用電子設備，徹底掌握戰場而打一場絕對勝利的高科技戰爭。而這場高科技武器主宰的戰爭型態所呈現的戰場盛況，正是以美為首所倡導的「軍事軍務革命」（Revolution in Military Affairs, **RMA**），其中「資訊戰」（中共稱為信息戰）（Information War），正是這場軍事革命的主要特質之一。根據了解中共認為發展信息戰可以獲得最佳作戰效益，癱瘓敵方金融、交通、電力、電信及軍事核心機制。因此中共面對以美國為首的這場革命, 亦積極學習推動, 企圖趕上這一場軍事革命潮流。

本研究計畫將從不同面向對廣義的資訊（信息）戰試圖賦予嚴謹

的定義與描述，再據此研析中共發展高科技「信息戰」的發展現況，從而探討中共發展信息戰對我國目前推動電子化/網路化政府產生哪些層面的影響？尤其是我國在建構電子化/網路化政府的同時，面對中共發展高科技「信息戰」的威脅，將會對我國建立資訊安全稽核制度產生哪些方面的衝擊？這些問題都是本計畫亟欲解決的。因此本研究計畫希望透過對中共發展高科技「信息戰」進行研究，從而對照我國在建構電子化/網路化政府同時，在建立資訊安全稽核制度上尋求提出政策因應上的建議。

第二節　研究主題背景

回顧歷史，十九世紀的科技發展促進了二十世紀工業經濟的突飛猛進。而二十世紀以來電子資訊技術的迅猛發展，孕育了二十一世紀的知識經濟和資訊化戰爭。自九０年代以來，世界經濟向全球化、知識化轉移，一個國家知識經濟的規模和質量，將決定他們的國際競爭實力和地位。因此，當我們正步入資訊年代的同時，資訊革命所造成影響範圍更是全面性的。就軍事層面而言，工業時代的戰爭是以裝甲機械化為主的軍隊之作戰，是以資源為基礎的戰爭，即以拼鋼鐵、拼能源，進行陣地戰，消耗戰的戰爭，而資訊時代的戰爭則是一種基於資訊、知識的一種複雜的戰爭，這可以說是以資訊為基礎的戰爭，亦可以說是資訊（信息）戰。這種以資訊為基礎的戰爭，即在作戰過程的每一環節都是在以資訊指導下進行，亦即當代戰爭只要交戰一方已進入資訊社會，充分運用資訊技術於作戰之中，就屬於資訊戰爭。因此，一九九０年的波灣戰爭可說是歷史上的第一次資訊戰爭。

針對目前兩岸統一問題，中共最希望透過政治談判，不用武力而獲取一個完整的台灣，但如果中共一旦決心以武力犯台，所花費龐大軍費，加上美國為維護其在太平洋地區的國家利益，勢必不會坐視不理，因此中共積極研發其「信息戰」能力，就是為其將來武力犯台做

準備。因此，順著探討資訊（信息）戰，不能將中共此一變數抽離的邏輯，從事對中共發展高科技「信息戰」及對我國建立資訊安全影響之研究，進而謀求我國在建構電子化/網路化政府同時，因應中共發展「信息戰」的威脅，提供政策上的因應建議，是必然要加速推動的工作。

本計劃名稱為中共發展高科技「信息戰」及對我國建立安全稽核制度影響之研究，由於此一研究範圍涉及相當廣泛，因此宜以科技整合的方式進行持續性的研究。然而，在中長期整合性研究之落實尚待相當時日推動情況下，為爭取時效，則應從相關的個別型研究計劃著手，為中長期整合性研究進行部分奠基的工作。本研究計劃之提出即基於此一考量，避免研究範圍過大而失當，企圖尋求在較短時間，獲致中共發展高科技「信息戰」的初步認識。進一步研析中共對於未來戰爭型態看法有何差異？以及中共如何發展信息戰？對我國在建構電子化/網路化政府上關於建立資訊安全稽核制度產生何種形式衝擊？進而提出政策因應上的建議。

第三節　研究方法與步驟

本研究計劃基本上是認為在世紀之交來臨之前，資訊（信息）時代正邁著震撼寰宇的步伐向我們走來。以波灣戰爭為標誌，一種新的戰爭型態-資訊（信息）戰正在形成和發展。由於資訊（Information）具有全球化，非線性效應、光速傳播、多方共享、用之不竭等特性，因此若能操縱和控制戰爭中的物質和能量，則必能大大提高作戰效能，並減少其他戰鬥力要素的投入。準此，資訊既是力量倍增器，又是重要戰略資源。

所以本研究計劃將從文獻研究著手，藉由對相關研究參考文獻的研析總結出資訊（信息）的特質，再依此特質有系統地透過實證資料

的整彙，瞭解當前中共發展高科技「信息戰」的形式與可能發展趨勢。亦即從總體層面的資訊時代下的戰爭型態進行分析，從而描繪出中共發展高科技「信息戰」的現況，並於瞭解其現況後，深入探究中共發展高科技「信息戰」對我國在建構電子化/網路化政府安全稽核制度所造成的衝擊，進而提出政策因應之建議。

基本上，本研究主要是採用文獻探討方式進行。由幾位參與研究計畫的同仁和研究助理分頭蒐集相關資料。國內關於資訊戰的相關研究雖尚處於初級階段，雖已有一定程度的研究成果；不過相較於大陸方面而言，台灣的相關研究則是起步較晚。職是之故，本研究僅就美國及大陸方面一些期刊、報導及我國一些專論、期刊、報導和網路上所公佈的一些訊息進行研究。總體而言，本研究之進行可以分為下列諸階段：

第一階段：就現有文獻資料之蒐集與檢閱。
第二階段：撰寫研究報告，並提出初步檢討。
第三階段：提送初步研究報告，請研考會審議。
第四階段：依據研考會審議意見進行研究報告修正。
第五階段：提送修正後完整研究報告並進行結案。

第四節　預期目標

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，在未來的戰爭裡，電腦與通訊網路，已是戰場中指揮、管理、通訊、資訊，情報的命脈。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，是當前我政府在建立資訊安全稽核制度上的一項重要課題。

本研究預期可達成下列目標：

1. 釐清當前中共發展「信息戰」的形式、特點、方法、手段及對我國資訊安全系統的衝擊。
2. 評估當前我國建立電子化/網路化政府中資訊安全制度的運作障礙。這些障礙將會對政府施政造成哪些不適當的後果。
3. 從總體層面評估我國在建立資訊安全稽核制度上面對中共發動「信息戰」，我國的因應之道。

第二章　電子化/網路化政府的機遇與挑戰

第一節　電子化/網路化政府背景：網路經濟世紀來臨

全球網際網路（**World-Wide Web**）自一九九五年發展至今不過短短數年已發展到近擁有五千萬名使用者，而它的前輩－收音機花了卅八年，電視機花了十三年才爭取到五千萬名聽眾，它的成長速度顯然是十分驚人的，另一個消息是到二千零一年，在全球網際網路上交易金額將超過二千億美元，這個數字雖僅占全球經濟總值 1%[1]，但已經是像我國如此貿易大國外貿總額二倍[2]，但這一切也只不過數年光景而已，有誰會想到枯坐在個人電腦前竟會創造出六兆台幣商機。

而此種不可思議的網上「虛擬交易」又是憑藉何種條件成功？甚至成為未來經濟主流？它有下列五個要素：

(一)、市場(Market)

數千萬名網際網路使用者早已超出人們對電腦玩家刻板印象中**「30 歲以下，好色的小伙子」**，且和主流人口形象更加吻合。許多新加入全球網際網路的使用者，其中成長最快的族群，這些族群即使在個人電腦盛行時期也似乎注定和 PC 無緣，因為他們在電腦面前顯得不知所措，但網際網路的力量驅使他們成為「使用者」。

(二)、時機(Timing)

「Y2K」危機的降臨，使得 1998-99 年新款個人電腦需求量大增，許多用戶為徹底解決問題，便替換掉大量過時設備，然而新款式的個人電腦，除了沒有 Y2K 問題外，更重要是它們都具有「上網」功能，

[1] Chunck Martin 著，林以舜譯，**e 時代的七大趨勢**（台北：美商麥格羅.希爾台灣分公司，2000 年），頁 27。

許多想要儘快解決危機的使用者便在此時搭上網際網路列車。

(三)、行為(Behavior)

當在職場上普遍採用網際網路時，便訓練出一大群慣於使用「線上下單」的顧客，在公司他們用網路替老板交易，下了班他們就會習慣用網路消費，因為兩者之間差異極小，不像買賣股票和到超市購物那樣截然不同。

(四)、價值(Value)

對廠商而言，網際網路最大好處在他們可以知道「市場」在那裡，因為消費者會自動「上門」購物，使得倉儲和物流費用大幅減少，更重要的是節省一大筆傳統通路費用，[3]例如設置一個數百坪賣場的費用遠高於建立一個拍賣網站。

(五)、空間化(Space)

而網際網路價值就在於它是一個「電子空間」（electric space）而非「場所」（location），也就是說在網路出現之前消費者必須親赴商店、賣場等「場所」，親自挑選、購物才可以交易，但在網路經濟使用者只需安坐家中，透過個人電腦向設有網站的廠商瀏覽商品，而後下訂單，連同取貨和付款在內一切的動作都在個人電腦上完成，此種「交易制度」可說是人類歷史上最具革命性變化，「電子空間」的出現使得人們透過網際網路，地理距離變得失去意義，因為在 1/8 秒內使用者便可進行交易（扣除掉頻寬因素），[4]從台北到彼岸的美國亦復如此，也就是說地理上的「距離」已消失，取而代之是「頻寬」，也就是電子空間中輸送「位元」的能力，傳遞資訊的速度，而這一切都只是在電

---

[2] 台灣每年出口總額約為 1000 億美元，資料來源 www.wto.org.

[3] Chunck Martin 著，林以舜譯，**e 時代的七大趨勢**，頁 28-29。

[4] Kevm Kelly 著，趙學信譯，**NET & TEN**（台北：大塊文化，1997 年 7 月），頁 165-170。

子世界中發生、運作，使用者不需親臨任何場所。[5]如此一來太平洋小島上的使用者可以不受時空限制選購巴黎時尚精品；從東京買賣華爾街上億美元股票，比訂購披薩還容易，只要他們都「上了網」，如此便利的交易制度自然風行於全世界。

而網際網路的出現又對人類政治、社會、經濟產生下列效應：

(一)、開放的企業與政府

如前所述在網際網路中，地理上的「距離」已失去意義，透過網際網路廠商與企業和千里之外的客戶（使用者）產生極為密切的關係，顧客將不再經由經銷商反應，而是直接和廠商互動，**E-mail**（電子郵件）很容易把全球顧客的意見告訴廠商，企業此時將不可能再以一兩條「客服專線」應付，他們必須為地球彼端的客戶在網際網路上提供服務，甚至讓他們參與決策制定。

在美國著名的 1-800 Flower 花店網站，在旺季時十萬名使用者在沒有任何一名店員、經銷商的協助下選購，約有 20%的人會訂購花束，對客戶而言 1-800 Flower 是完全開放，他們可以直接和 1-800 Flower 溝通，確認訂單和追蹤貨品，甚至線上交談，在只有電話線路的年代，越洋電話費用將十分驚人，而 1-800 Flower 也將因為對客戶開放資訊和直接服務，獲得「真正」市場訊息。[6]

在網際網路最發達的美國，政府也隨網路經濟型態而調整，相對

[5] 在網際網路中，資料以光速傳遞（30 萬公里／秒），繞地球一圈(約 4 萬公里)只需 1/8 秒，因而理論上來說，傳遞資料只需 1/8 秒，現實上受限於網路設備頻寬，而現今最快的寬頻網路傳輸速度亦可達 1Mb/Sec，為電話撥接速度 200 倍，預計新一代網際網路通訊協定可達 420Mb/Sec，為現今電話撥接傳輸速度的 8 萬倍，前者有能力在 2~3 秒內傳送上約 100 頁文件（1 頁以 20Kb 計算），後者更僅需千分之一秒。邱裕榮，「固網開放：台灣電信市場面臨變天」，**工商時報**，2000 年 3 月 21 日，第 12 版；Kevin Kelly 著，趙學信譯，**NET & TEN,** 頁 166~167。

[6] 根據筆者以 E-mail 美國最大圖書網站 **Amazon** 提出訴願之經驗，Amazon 多半可以在 8~12 小時內給予滿意回覆，而國內網站多半需要 2~3 天。

於「開放企業」是「隨時待命的政府」，在美國麻州，居民可以像線上購物般繳交罰單，在密蘇里州，州政府開放失蹤孩童資料，提供網際網路使用者瀏覽，而維吉尼亞州，民眾可以在線上查詢到自己退稅資料，不過網路對政府最大衝擊是組織重整，以加州為例，各州紛紛設立「資訊長」的職位和相關單位，加州的「資訊長」約有 20 億美金預算和 8000 名人力，傾全力將政府大部份業務以「電子形式」完成，[7]也就是說以往侷限於公務機關般的場所(location)，將逐漸被網際網路的「空間」(space)取代。

(二)、資料資訊化

因應企業和政府開放，是資料資訊化，成千上萬的文件、數字將被轉換為磁碟可讀寫的資訊放在主機、伺服器上供駭客竊取或守法公民使用，不過對企業和政府而言不僅是如此，當他們的資料、文件都被「磁碟化」後，「科層組織」這個鐵律就很快要被瓦解，以往大型組織內部的運作原則是一份命令、文件要在一層又一層單位中作「公文旅行」，已經耗去許多光陰，因為它是「紙上作業」。

但「資訊化」後，透過內部網路傳遞資訊，組織的領導人可以輕易向全部成員發送指示（**以 E-mail 型式**），當然也只需要 1/8 秒，而各單位回覆領導者的型式亦同，如此一來原先疊床架屋單位和組織型態便由原來「金字塔」型式趨向扁平式，而各平行單位也可輕易利用網路交換訊息、溝通業務或舉行視訊會議（Visual Conference），視訊會議可讓纜線另一端所有使用者，坐在個人電腦前一起開會，各單位主管可免於奔波之苦。[8]

---

[7] Chumck Martm 著，林以舜譯，**ｅ時代七大趨勢**，頁 124-147。

[8] 視訊會議是利用網際網路傳輸影像與聲音, 使用者只需坐在設有攝影機和螢幕的電腦前，便可看到聽到纜線另一端的使用者，與會者無須遠渡重洋即可有如臨現場效果，總統當選人陳水扁於今年 4 月中旬即利用視訊會議隔海與美國國會議員「面對面」密談。「年省 100 萬的的開會方式－視訊會議」，**網路通訊雜誌**，第 81 期，民國 87 年 4 月)，頁 45-69；林銘義，「陳水扁保證:改善兩岸關係維持台海和平與美國會重量級議員越洋對話」，**中國時報** ，民國 88 年 4 月 14 日，1 版。

網際網路帶給人類當然不僅僅是好處，它也帶了一些問題，因其便利性所導致負面效應：

(一)、開放的企業、政府網站——不設防的要塞

在網際網路發明之前，人們必須親臨「場所」例如去商店才可購物，赴機關才可洽公，雖然這對消費者和公民而言有些不便，但對企業和政府而言卻十分有保障，因為在超市搶劫的風險極大，更不要說攻擊政府機關，一旦企業和政府都網路化後,「空間」取代了「場所」，他們所要面對的問題卻比以前嚴重千百倍，因為有可能威脅企業與政府是距離只有 1/8 秒的敵人和成千上萬的入侵者（invader），而他們拜科技所賜不必親臨現場，全在纜線另一端用垂手可得的入侵程式用以攻擊網站，他們又被稱做駭客（hacker）或毀客（cracker）。[9]

也就是說在「第二波」年代的持槍歹徒已不復見，[10]纜線另一端的使用者可能是老是少，甚至有可能是「菜藍族」或未成年人，只要利用入侵程式敲打鍵盤便可對網站造成不一傷害。試問為何企業和政府上了網便如此脆弱？因為網際網路設計原理－TCP/IP[11]原本就是為開放網站而設計，根本料想不到會有那麼多入侵者利用它的便利性來犯罪。

---

[9] 依據美國電子安全對入侵者的分類，駭客(hacker)屬於非惡意性入侵者，入侵對方主機目的多半只為了求樂趣，因而破壞程度較輕，然而毀客(cracker)多半懷有惡意，入侵目的複雜而危險，有恐怖主義成分在，其破壞程度正如恐怖主義行動，對主機傷害多半十分嚴重。詳見馬榮安,「駭客的種類」，**網路生活雜誌** ，第 47 期，頁 18-20。

[10] Alvin Toffler 著，黃明堅譯，第三波（台北：經濟日報出版社，民國 70 年），頁 145。

[11] **TCP/IP** 協定，是連結所有上網電腦及區域網路共同程式，它使得任一區域網路間均可輕易傳遞訊息，使得連結速度極快，因為它的原理是將欲傳遞資訊放在全球共同網路上，再去尋找目的地，等於是將傳遞資訊放在所有連結網路電腦中，M. Strebe 等著，卓正民等譯，**NT 安全實務評論**(台北：儒林圖書公司，1999 年 2 月)頁 3-9~3-15。

再者在「場所」的時代中，企業和政府都會有武裝警衛看守，嘗試侵犯這些地方的下場可能會送命，但在「空間」的年代中，拜 TCP/IP 協定所賜，只要使用者知道網址（IP）便可大搖大擺進入，若網站未裝設防火牆（firewall），那就如入無人之境，可恣意妄為，而受害者多半要等到事態嚴重才會察覺。

(二)、資料資訊化—便於竊取。

當成千上萬的數字、文字都化為位元後，對企業和政府而言固然減少許多成本，無論是資料儲存、調閱都極為便利，對使用者而言當然也分享到這些好處，但倘若使用者成了駭客時，網站便成活靶。

在「場所」的年代中，到銀行式提款機提款需要數點鈔票，向政府機關洽公，需由公務人員辦理紙上業務，但「電子空間」時代降臨後，電子錢包（electric wallet）[12]便取代現鈔，持槍搶匪的行為將不復出現，駭客們有能力將大筆資金由金融機構的網站轉到自己戶頭，1995 年花旗銀行就被俄國駭客竊取上億美金，[13]此種風險遠比搶劫銀行低。

在「場所」的年代中，鮮少人會去攻擊政府機關，除了少數不怕死的恐怖份子外，但在網際網路年代中，成千上萬的公文、機密都被儲存在電腦主機中，拜科技所賜一片光碟可儲存上 2~3 萬頁資料，對政府單位而言傳遞、調閱都極為便利，不過這些主機當然也是「開放」的，拜 TCP/IP 協定帶來的便利，注定這些機密將不再被鎖入櫃中，纜線另一端的使用者利用程式竊取、破壞政府機密的速度將十分驚人。如前所述一萬頁的機密不過 1/2 片 CD-ROM 大小（約 200~300MB），而傳遞資料的速度與距離無關，只和「頻寬」有關，

[12] 電子錢包是網路交易付款的應用程式，使用者由銀行帳戶或信用卡匯入在網路上建立的虛擬帳戶，再以此帳戶在網上消費。Bryan Pfaffenberger 原著：張寶源譯，**Microsoft 官方資料－Internet Explorer 4 中文手冊**（台北：碁峰資訊，1998 年 2 月），頁 8-1~8-9。

[13] 鄭哲政，「俄羅斯駭客入侵銀行「搬」錢」，**聯合報**，1999 年 3 月 5 日，第 3 版。

萬里之遙的使用者若以寬頻上網（速度約 1 MB／Sec），下載一萬頁政府機密的時間只需 300 秒，甚至比用手搬運它們時間還短。1994 年美國國防部內部有關北韓核武危機的機密，就被一名英國 16 歲青少年加以公佈於世，此種入侵事件據美國國防部估計每天高達 7000 次。[14]

第二節　我國電子化/網路化政府政策與理念

在網路經濟世紀來臨年代，政府必須跟隨整體經濟腳步，如同企業，政府業務也必須隨之「電子化」、「網路化」。時任行政院蕭院長上任後即著手政府角色調整，以改善政府經營與服務方式，其中推動「電子化/網路化政府」是施政主軸。[15]行政院資訊通信發展推動小組（以下簡稱行政院 NICI 小組）則作為規劃推動「電子化政府」專責單位。NICI 小組訂定我國電子化/網路化政府政策乃是基於下列長遠規劃；

1、 企業化政府理念

如前所述，本世紀末網路經濟一大特性即為廠商極為快速反應能力，俾使其能迅速獲知消費者喜惡而做出調整，而本世紀末政府政重點是「向企業學習」，[16]如何建立政府與民眾良好溝通管道與提升政府反應能力，便成為迫切課題，如何使得固守在辦公桌前的公務員變成為「電子公僕」，能「隨時」、「隨地」為民眾服務，是我政府在網路世紀來臨。

2.提升政府行政效率與施政品質

當大部分數字、資料被「資訊化」後，「公文旅行」的時間只下

---

[14] 路透社，「三年前英國少年普萊斯用家中電腦破解 200 道安全措施，登入五角大廈彈道飛彈資料」，**聯合報**，民國 86 年 3 月 23 日，10 版。

[15] 行政院國家資訊發展推動小組編，**邁向二十世紀的電子化政府**（台北，行政院國家資訊發展推動小組編印，民國 87 年），頁 1-7。

[16] 江岷欽、劉坤億著，**企業型政府**，(台北：智勝文化，1998 年)頁 41-59。

1/8 秒，借由行政作業高度資訊化、網路化，一紙公文也不再要逐層批閱，因而以往疊床架屋的行政體系便顯得不合時宜，朝向網路式、交錯式組織發展是大勢所趨，[17]此種趨勢所帶來當然不僅僅是組織改造，而是對內行政效率和對外施政能力飛躍性進步，在電子空間中對外交換資訊所需時間極短，行政人員可以很快獲知訊息而做出決定，以往給人印象不佳「官僚」形象將被瓦解。而我國在「電子化政府」之政策又可分為下列項目：

1、 建構政府網際網路服務網**(Government Service Network ,GSN)**

推動電子化/網路化政府最基礎建設便為網路工程，一般民間企業、個人上網多半經由網路撥接公司**（ISP)**，但在安全性上有所顧慮，政府網際網路使用特性不同於民間，因而建構專用網路工程便為首要任務，我政府於 86 年 7 月起便建構完成各機關間的網際網路，除了在安全性上較能獲得保障外，也同時省下由私營撥接所帶來通訊成本。

2、「課股有信箱，訊息瞬間近」

「課股」做為我國各級公務機關基層單位，當然做為推動網際網路業務基礎，本計劃目標在各級機關內部提供：

（1)、政府整體性電子郵遞系統。

（2)、提供電子目錄查詢維護服務，希望藉由此項網際網路軟硬體建設，使得政府內各級單位能率先應用電子郵遞系統處理公務，而後提供民眾服務。

3、便民資料庫：

（1)、法規資料庫：

在網際網路上放置「全國性電子法規資料庫」，供公、民機關與一般民眾即時性、快速法規服務。

（2)、信用資料庫：

---

[17] *W. E. Halal" From hierarchy to Enterprise: internal market are the new fund ration of management"*

Academy of Management Execute (*1994) Vol.3, No.4, and p70.*

將目前由金融機構內部終端機連接的信用資料，將可供個人至網際網路檢索。

(3)、戶政人口資料庫：

預計將全國現有戶政資料資訊化，便於公務機關間傳遞和供民眾服務。

(4)、電子公路監理：

在網際網路上提供所有紙上公路監理資料，包括車籍、違規記錄及交通法規，未來在第一階段將可提供網上繳納罰款，第二階段將提供換補照、駕照、地址變更等網路服務。

4、便民行政應用

(1)、電子稅務：

八十六年推行線上報稅是我電子化政府之先河, 是首次採用全套網路行政服務的手續，也是相應安全稽核制度 GCA 首次應用，每年將可節省民眾大量報稅時間。[18]

(2)、國民識別卡（IC 卡）

八十六年行院研考會便推動「國民 IC 卡」, 將一般民眾最常利用各種證件、卡片（身份證、健保卡、金融卡和信用卡）合併於一 IC 卡中, 冀望能藉由簡化國民識別和金　交易方式，加速資訊化政府發展，在八十七年公布建議書後, 在與民間議約過程中, 因安全性顧慮而停頓, 但政府仍將改由預算方式推動身份證和健保卡兩卡合一推行。[19]

5、資訊安全政策與規範

電子化／網路化政府帶來的正面效益將如同網路商機般無可限量，但所伴隨而來的負面效應也十分驚人，如前所述全球網際網路所採用的 TCP/IP 協定，造成機密形同置於桌上供人索取，而電子商務的風險和其便利性亦成正比，因而一套完善資訊安全政策與規範，是

[18]行政院國家資訊發展推動小組編，**邁向二十世紀的電子化政府**，頁 37-70。

[19] 巫靜宜、呂麗琴、李鴻璋,「國民卡策略規劃與其運作安全及法源規則」，**中華**

發展網際網路先決要件，目前我政府推動下列資訊安全政策：

（1)、訂定政府各機關安全管理規範

以各機關內部現有資訊人員為管理單位, 由各機關副主管或高級主管督導，並將內部人員加以資訊安全訓練。[20]

(2)、建立憑證機構

憑證（**Certificate Authority, CA**）是網際網路拓展應用範圍最主要關鍵，在 CA 能有效保障任一筆交易安全性受到保障前題下，網路經濟和電子化政府才有意義可言，若非如此，全球互聯網只是一個提供犯罪的天堂。 **CA** 是一種安全密碼，當使用者使用政府電子服務和網路消費時，必須使用個人所有 **CA** 來代替紙上作業時代的簽章，因而又稱為金鑰（key），是保障政府和個人機密在網上不受窺伺的。[21]我國 **CA** 由行政院研考會於民國八十六年委託中華電信規劃並建立電子化政府共同 **CA** 又稱 **GCA**（Government Certificate Authority），配合首次線上報稅試行, 做為我建立資訊安全試金石。**GCA** 運作過程如（圖 2-1）[22]

民國資訊學會通訊，第二卷第一期，民國 88 年 3 月，，頁 7。

[20] 行政院研究發展考核委員會編，**行政院及所屬機關資訊安全管理規範**（台北：行政院研究發展考核委員會編印，民國 88 年 11 月），頁 3-26。

[21] 樊國楨，「虛擬社會資訊安全機制初探——從密碼模組領域認證體系談起」，**資訊安全通訊**，第五卷第二期，民國 88 年 3 月，頁 7-16。

[22] 賴溪松，「中華民國資訊安全之活動與發展」，**資訊安全通訊**，第五卷第二期，民國 88 年 3 月，頁 28-29。

圖 2-1.我國 GCA 申請過程圖

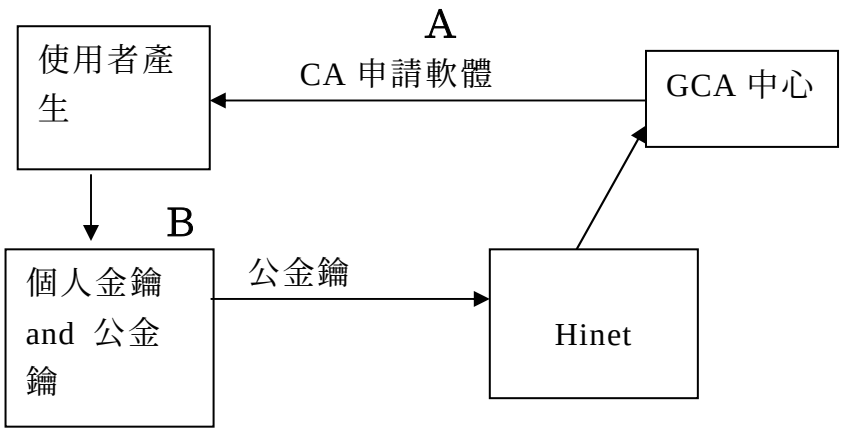
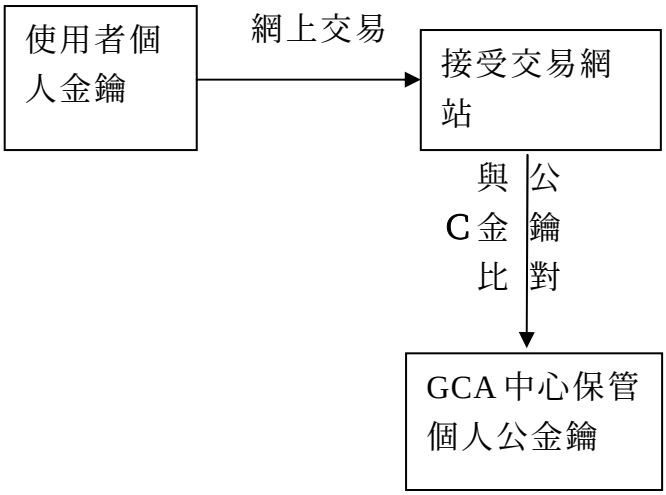


圖 2-2 我國.GCA 認証過程圖



A.網路使用者在線上向政府憑證管理中心伺服器下載 CA 申請軟體。

B.軟體會自動產生公、私金鑰(Public and Private Key)各一，也就是兩份網路憑證，公金鑰連同個人資訊透過 Hinet（中華電信）送回政府憑證管理中心伺服器備存。(圖 2-1)

C.此後使用者利用電子化政府各項服務，必須使用個人私金鑰和政府保存公金鑰比對方可使用。(如圖 2-2)[23]

[23] 吳明義,「線上報稅餘波盪漾」，**網路通訊**，82 期，1998 年 4 月，頁 36-37。

(3)、建立網路安全國家標準

行政院研考會民國八十八年八月有鑑於疑似中國大陸駭客攻擊我政府網站，便積極擬定全國性統一資訊安全標準，此安全規範是 CA 普遍化、制式化之關鍵，唯有建立規格安全共同規範，方可建立統一、安全防衛體系。[24]

(4)、民間網路安全活動

資策會在八十八年七月大陸駭客入侵我政府網站後，即成立「網路安全防護服務組」，為民間企業提供網路安全資訊和服務。另一個性質相似的組織是「台灣電腦網路危機處理中心」（**TW-CERT**），提供即時性線上救援和遠端線上掃描，其性質較接近一般網路安全業務。[25]

第三節　我國電子化/網路化政府的挑戰

電子化/網路化政府透過網際網路所帶來便民效益是前所未有的，因為電子化/網路化政府是在「空間」中運作，是在纜線中「隨時隨地」為民眾服務，可說沒有時空限制，電子化/網路化政府好處是由於網際網路兩大優勢帶來一開放性與資料資訊化，開放性使得民眾隨地都可透過網路 24 小時享受政府網站的服務，因為伺服器是沒有下班時間，而資料資訊化使得使用者瀏覽或下載成千上萬份資料也不需太長時間，在電子空間中，只要使用者頻寬足夠，竊取一萬頁資料也只需 1 秒鐘以內。[26]但猶如雙面刃的道理，網際網路兩大特質注定使它成為 21 世紀最佳犯罪工具。

1、 開放性－隨時隨地成千上萬入侵者

---

[24] 林志成，「駭客止步，我擬建立網路安全國家標準」，**中國時報**，1999 年 8 月 27 日，9 版。

[25] 陳京城，「駭客猖獗資策會布網防護」，**經濟日報**，1999 年 8 月 31 日 ，10 版。

[26] 1 萬頁文件約合 200~300MB，以下世代網際網路通訊協定傳輸速度 420MB/sec 計算，下載只需 1/2~2/3 秒。

電子化/網路化政府的目標是冀望二千三百萬國民都能享受網上政府服務，但網際網路對全球開放的特性，使得使用者絕不侷限於我國守法國民，境外的使用者雖沒有上網報稅的必要，但他們對中華民國成千上萬線上報稅民眾私人資料可能極感興趣，即使有 GCA 這個阻礙，有利可圖的犯罪行為仍將源源不絕發生，且其數量極可能遠超過人們所能想像。最受駭客「歡迎」的美國國防部，每日試圖入侵者多達 7000 人次, 而我政府於去年 7-8 月間亦遭中國大陸駭客入侵上數千次。[27]

2、 資料資訊化—形成洩密管道

當政府各項公文、資料都數位化後，存入上萬頁的文件的意義是300 秒就會被竊取一空，如此便利的「管道」，除了供民眾利用外，有心人士會想盡辦法進入主機中，破壞或竊取機密，敵方不必像情報員干冒風險，在千里之遙即可從事間諜活動，此種誘因對我敵對國家來說實在太大，解決掉一個防火牆的代價絕對比打下一架戰機便宜。網際網路發展過程中暴露出如此嚴重洩密的弱點，檢視我國電子化政府及其安全措施便顯得極為迫切，筆者認為現今資訊安全管理有下列缺失：

（1)、政府內部網路安全未設專責單位管理

電子化/網路化政府是推動「政府再造」關鍵所在，政府投入大量人力、物力推動，因而成果豐碩，但網際網路的特性猶如「雙面刃」，在得不到安全保障前提下，網路將成為我安全上一大漏洞所在。現階段負責我政府內部網路安全是分散在各機關非專職資訊人員，這群散兵游勇，在未經統整和訓練下，卻要面對來自對岸成千上萬入侵者，往往根本沒有反應時間，多半是事後才發現網站遭攻擊，而駭客早已張揚而去，導致攻擊事件層出不窮。[28]

---

[27] 羅曉荷,「本月上旬對岸駭客七千餘次來襲」, **聯合報** , 1999 年 8 月 17 日，8 版。

[28] 1999 年 7 月上旬，因「兩國論」因素，對岸駭客大舉入侵我政府網站，包括經濟部、國大在內多個政府網站被駭客成功破壞，至今仍未知入侵者身分。曹逸雯,「經部網站疑遭駭客入侵工商登記網路查詢系統無法運作」, 胡慧文, **中央日報**,

（2)、未設立網路安全預警系統。

網路入侵的速度在使用網路下，較彈道飛彈攻擊快上四百倍，[29]因而在未設立網路預警安全警報系統下，我政府網路像是一個又一個待宰活靶，根本沒有能力在第一時間反應而採取補救措施，[30]避免損失擴大。而根本問題如前所述，政府內部亦無專職人員、單位負責此一業務，更遑論購置預警設備。

美國政府部門一向是駭客熱門網站，國防部網站更是入侵者最愛，因而美國國防部為強化網路防衛，首要目標便是建立預警系統，1999 年 10 月便展開一場網路模擬攻防戰，代號「天狼星」的預習，五角大廈統合了國安局、中情局、聯調局、軍方專家、設備，成功追到假想敵入侵位置。[31]而民間企業為求自保，美國金融機構率先建立內部預警系統，在 2000 年 2 月初雅虎（Yahoo)、**CNN** 和 **Amazon** 等大型網站受攻擊前，此系統便已進入「備戰狀態」。[32]

3、 政府憑證制度評價

基本上 GCA 做為我政府資訊安全制度先河，卻有下列缺失：

（1)、整體委外經營合理、合法性

1999 年 8 月 24 日，6 版；夏念慈,「國民大會網站 遭駭客「廢」了攻擊程式入侵軟硬體都嚴重受損」，**中國時報**，1999 年 8 月 12 日，3 版。

[29] 中共最精良的 M 族飛彈從發射至命中目標約需 30 分鐘(1800 秒)，我方預警時間約有 5 分鐘(300 秒)，然而網路攻擊行動如前所述在使用寬頻網路下，竊取上百頁資料只需數秒鐘，破壞網站所需時間更短。蔡明聰,「共軍 M 族飛彈對台澎防衛作戰之影響及我因應之道」，**陸軍學術月刊** ，第 397 期，頁 8~12。

[30] 1999 年 7 月，國民大會網站在遭大陸駭客入侵後的 12 小時後才發覺，經濟部網站在遭破壞後的 10 餘小時後才恢復運作。詳見劉添財,「國大網站二度遭入侵，暫時關閉」，**中國時報**，1999 年 8 月 13 日，第 2 版。

[31] 路透社,「美建立網路防衛網具成效」，**中國時報**，1999 年 11 月 1 日，13 版。

[32] 白德華,「駭客攻擊知名網站金融機構獲預警」，**工商時報**，民國 89 年 2 月 14 日，10 版。

GCA 是我電子化/網路化政府發展之成敗決定性因素，在各先進國家發展 GCA 過程中多半由政府全程主導，故人力物力較為充沛，但我國 GCA 由民間企業（中華電信）委外設計，並參與經營，以線上報稅為例，公金鑰必須經由民間網路才可遞送至政府憑證中心，其風險性便大大提升，個人機密在便民化政府措施下，都成為駭客窺伺目標，中華電信是否有能力負擔起整個 GCA 安全重責大任成為一大疑問，[33]再者在中華電信民營化後，是否可經營此種公用事業，這便牽扯到違憲的問題。[34]

(2)、未建立網路安全稽核制度和攻擊預警系統

要從線上報稅普及化到各項電子化政府服務，網路安全稽核制度是首要問題，首先必須有專責單位，人員定期考核、監督各機關網路軟硬體是否合乎相關國家安全標準。目前我政府的狀況並不樂觀，各機關多半有架設防火牆和其他相關設備，但現在的狀況各單位多半各行其是狀態，易遭各個擊破。

此外我政府現階段幾乎缺乏防禦駭客攻擊的基本能力－網路攻擊預警系統，以去年七至八月間我政府網站遭對岸駭客入侵為例，由於缺乏網路攻擊預警系統緣故，導致接連多個政府單位網站遭到程度不一破壞，相關單位遭攻擊後所需反應時間長達十餘小時，[35]更遑論追查入侵者身分。若當時我方擁有類似美國國安局的網路預警電腦，在遭攻擊第一時間內即可通知各政府單位網站戒備和追查入侵者來源，[36]在擁有網路攻擊預警系統前提下，才有可能談所謂「網路安全」。

---

[33] 吳宗成，「淺談密碼模組驗證制度與資訊安全系統委外」，**資訊安全通訊**，第五卷第一期，民國 87 年 12 月，頁 101-102。

[34] 巫靜宜等，「國民卡策略規劃與其運作安全及法源規則」，頁 19。

[35] 指發現入侵者並恢復網站原貌和正常運作所需時間，2000 年 2 月間美國各大網站遭入侵後均在第一時間內發現，並在 2 小時內修復完畢。

[36] Chris Taylor Behind, “The hackers are Attack”, **Time** (Feb 21 2000), pp35~45.

第三章　資訊(信息)戰之理論與實際

第一節　資訊戰之總體意涵

資訊競爭和人類的衝突一樣古老久遠，每個國家、公司和個人都設法要增加並保護自己所儲存的資訊，同時也致力於限制與突破對方的資訊。基本上從七〇年代以來，人類在蒐集、儲存、分析和傳送資訊的技術方法上都有長足的進步，因此，資訊技術改變了原有社會的產業結構和經濟結構，改變了人們勞動方式和生活方式，也改變了社會生產的組織和管理體制，使社會進入資訊時代。

八〇年代初，美國社會預測學家托夫勒（Alvin Toffler）所著的**《第三波》**（The Third Wave）一書問世。這本書著重從人們眼前看到的生活變革的事實入手，分析了人類社會文明正由工業社會走向資訊社會，並提出了資訊社會完全不同於工業社會的生產方式、工作方式和生活方式。[1]此書的出版，引起學界相當大的重視，認為資訊時代的來臨，人類所面臨的將是一種不同以往的新型態社會，而這本書的出版，也引起其它不同領域的學者專家進行辯論。

一九八九年，美國軍方開始研究資訊時代的戰爭，並提出「計算機病毒戰」的概念，一時之間，有關資訊時代的戰爭引起學界極大的反響。一九九〇年十一月，托夫勒的另一本研究資訊社會書籍——**《權力變移》**（Power shifts）出版，在這本書中，提出了資訊戰（Information Warfare）的概念，但這並不是從軍事意義講的，而是從市場意義講的。[2]一九九三年，托夫勒的**《新戰爭論》**（War and anti-War）一書出版，人們逐漸把眼光把資訊對人類的影響由社會領

---

[1] *Alvin Toffler,* ***The Third Wave*** *(New York: Morrow, 1980), pp.3-9.*

[2] *Alvin Toffler,* ***Power shifts Knowledge, Wealth and Violence at 21st century*** *(Published by Bantam Books, 1990), pp.58-72.*

域轉向軍事領域。[3]與此同時，學界關於資訊戰的研究風潮日漲。

就資訊戰研究興起之原因，可以遠溯自史瓦陶（Winn Schartau）的著作，即**《資訊作戰：混亂的電子高速公路》**一書，該書描寫善用電子詭計的正反兩方人馬以先進的資訊科技，進行鬥法的故事。這個故事很自然地引起大家對資訊戰的注意力，並激發廣泛討論的火花。其討論範圍包括如何善用資訊科技，應採取何種措施以防制資訊科技之濫用及資訊科技的擴散將個人道德、社會規範、國家法令產生怎樣的衝擊。在正反雙方意見人士之中，持正面看法的保守人士則認為資訊戰具有軍事革命的象徵性意涵，其影響力之深遠有如十九世紀工業革命對當時戰爭型態的改變一樣；持反面看法的保守人士則認為資訊戰只是個響徹雲霄的口號，與其花費大筆經費還不如將這筆預算用來改良現有的作戰方式。[4]

正是由於資訊戰的概念是由社會領域向軍事領域進行轉折，其影響層面又相當地廣泛，因此，資訊戰這個概念的意涵也是相當地廣泛。從軍事層面來面，資訊戰的定義就有好幾個版本。第一個版本係於一九九五年由主管指、管、通、情與電腦業務的美國國防部次長沛吉（Emmet Paige）所提出，沛吉將資訊戰定義為：「為獲得國家軍事戰略所需之資訊優勢，藉由各種手段以癱瘓對方的資訊系統與情報作業能力之外，更應妥善採取防禦與反制措施以鞏固其情報作業能力與資訊系統之安全。」第二個版本係由美國空軍現行採用定義，即「美軍應發揮情資功能，採行任何以壓制、削弱、破壞或摧毀敵人情資系統

---

[3] *Alvin Toffler,* ***War and ant-war: Survival at the dawn of the 21st century*** *(Boston: Little, Brown, c1993), pp.25-26-27*。托夫勒認為人類的戰爭方式依其所處的時代文化背景可區分為農業、工業與資訊戰爭。農業時代的典型作戰方式係用手製武器來掠奪城市內的多餘糧食及財富；工業時代的作戰方式則是消耗戰，交戰雙方均側重以機器量產出來的機動性軍備；資訊時代的作戰方式則完全仰賴資訊科技所發展的通訊裝備及即時處理情資的資訊系統。

[4] *Daniel E. Magi, "Information age of information Warfare", available at massaged@ comm.hg.af.mil.*

及其功能之措施，以防範美軍遭到敵人反噬之破壞攻擊行動。」第三個版本係美國陸軍所下之定義，並經「參謀首長聯席會議」與各軍種認可，即「美軍在確保其情資來源、情資作業流程及資訊系統安全的同時，應採取各種手段以摧毀對方的情資來源、情資作業流程及資訊系統，以獲取資訊優勢。」[5]

從上述三種有關資訊戰的定義，我們可以看出，對資訊戰的定義，大致上都是從國家的觀點來強調資訊的重要性，而忽略了資訊對與國家安全無關之個人及組織亦會造成傷害。雖然美國陸軍所下的定義版本，適用於個人、組織團體及軍隊，但其揭櫫的「資訊優勢」包含那些層面卻又未說明，仍是此定義美中不足之處。

有鑑於資訊戰的定義，眾說紛紜且無權威性的解釋，美國國防部進一步於一九九八年十月在「聯戰準則 3-13 資訊作戰」中重新闡述美國資訊戰的作為。最初，聯戰準則編撰委員會選定「資訊戰聯戰準則」（Joint Doctrine for Information Warfare），但是在最後完稿時，題目改為「資訊作戰聯戰準則」（Joint Doctrine for Information Operations）。這項變更主要目的是要釐清資訊作戰與資訊戰的關係。依據「資訊作戰聯戰準則」的說明，資訊作戰與資訊戰的差異如下：[6]

＊資訊作戰（Information Operations）：不分平、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（Information Warfare）：在危機或衝突期間，針對特殊的敵人，為達成特定目標，所遂行的資訊作戰。

由上述的定義可以清楚看出資訊作戰包含之意涵已更為寬涵，亦即是說資訊無遠弗屆的特性，已使戰場中「前線」（the front）的定

---

[5] 國防部史政編譯局主編，**資訊作戰譯文彙編**（台北：國防部史政編譯局，1997 年），頁 250-251。
[6] See *Joint Pub 3-13, "Information Operations", **Dodd US**, December 1998.*

義日趨模糊化，在未來的戰爭中，處處可能是戰場。因此，當人們發現可將外界事物的一切簡化成數位中的「0 與 1」組合，並根據電子方法以資料的方式傳送、接收時，這亦代表著資訊已經密切與人類生活結合起來。資訊時代的特點，就是資訊已經在人類基本生活之中扮演著愈來愈重要的角色，因此當人們越來越依賴資訊的正常運轉，破壞或操縱資訊傳遞就成為這個極端依賴資訊時代所新產生出來的戰爭手段。在過去以往的戰爭手段都是以摧毀「原子」為目標，無論是手腳、棍棒、刀矛、槍炮或是核武，無非是能力的擴展，但目標還是「原子」的，然而在資訊時代，則是完全可以以「位元」（byte）為直接目標，通過破壞或操縱「位元」的手段可以是「原子」的——如電磁脈衝炸彈(Electric magnetic pulse bombs, EMP）等，也可以是「位元」的——如電腦病毒（computer viruses)。後一種手段當然更具有資訊時代的特點，而且它可能使戰爭的型態，以及人類社會生活的許多方面都大為改觀。[7]

一九九六年，美國蘭德(RAND)公司出版《戰略信息戰》(Strategy Information Warfare）一書，描述資訊戰乃是一種動態發展的產物，資訊戰一詞現正加速地運用於更廣泛的資訊時代「作戰」觀念。這種新興的作戰觀念直接關聯到一種情況，即現行發展迅速的網路全球化趨勢，可能會顛覆過去傳統作戰的方式，亦即是說，資訊戰已經衝破以往固有的邊界觀念。因此，針對此一新興作戰領域，蘭德公司將之稱之為「戰略資訊戰」。[8]

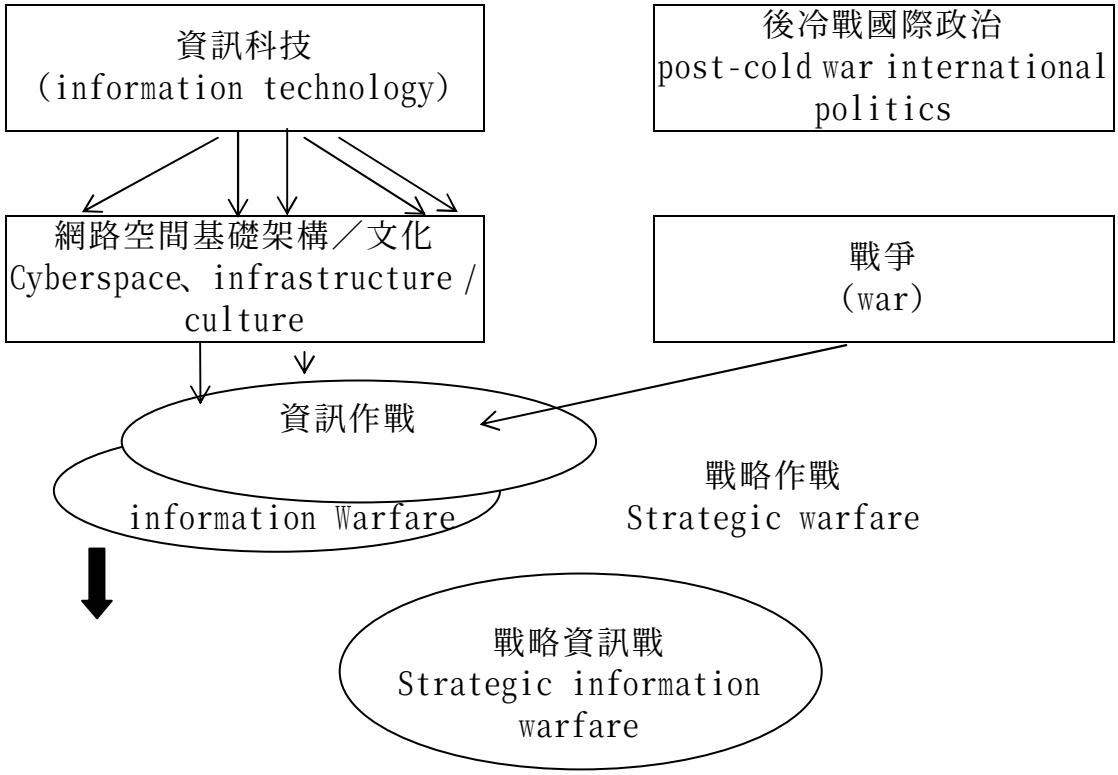
所謂戰略資訊戰，在本質上乃是動態發展中的資訊戰與後冷戰時期「戰略作戰」兩種觀念之結合（見圖 2-1)。這亦即說，資訊科技的發展，帶動網路空間基礎架構與文化，電腦網路之興起與其特性，已經將資訊戰推向新境界。而後冷戰時期，面對資訊科技的發展，新的

---

[7] 王小東，**信息時代的世界地圖**（北京：中國人民大學出版社，1997 年），頁 90-91。
[8] *Roger C. Colander, Andrew S. Riddle. Peter A. Welcomed.* ***Strategic information Workface: a new face of war*** *(CA; Rand Company: 1996) P1.*

戰略威脅與新的戰略弱點也同時浮現（如電腦網路威脅與弱點）。準此，將以網路空間基礎架構加上後冷時代戰略形式特點，就是戰略資訊戰。

圖 3-1　戰略資訊戰示意圖



資料來源：Roger C. Molander、Andrew Riddile、Peter A. Wilson eds., Strategic information Warfare: a new face of war (RAND, 1996), p.2.

每一個國家，基本上，都擁有若干實質的資訊基礎資源，包括複雜的管理系統和網路設施，用以管制電力、資金流通、空中交通、油料以及資訊有關物品。就概念上來說，若潛在的敵人企圖運用資訊戰技術去破壞上述系統，資訊戰就必然是一種戰略資訊戰。換言之，講得通俗一點，戰略資訊戰就是通過破壞或操縱電腦網絡上的資訊流通

的辦法，對敵人的電話網、油氣管道、電力網、交通管制系統、國家資金轉移系統、各種銀行轉移系統和衛生保健系統等實施破壞，以達到戰略目的。

總的來說，美國蘭德公司出版的戰略資訊戰一書告訴我們，隨著資訊科技的不斷發展，以資訊為核心的新型態戰爭已儼然成形，誰擁有資訊主導權與制資訊權，將是資訊時代的大贏家。總結來說，戰略資訊戰，具有下列特點：

（一）、低進入成本（Low entry cost）

戰略信息戰的一個最具本質性的特徵就是低進入成本。這亦即是說戰略信息戰並不像傳統武器科技需要大量經費或由國家來主導。在資訊技術不斷更新發展的時代，能夠擁有專業資訊系統知識與處理重要網路連接的能力，才是戰略資訊戰的必要條件。[9]

（二）、傳統邊界的模糊（Blurred traditional boundaries）

由於有各式各樣的敵人、武器和策略，因此，實在很難分辨出外在或內在的資訊戰威脅和行為之來源。職是之故，在資訊社會中，公用和私用網路互聯，軍用和民用網路互聯，各國之間的網路都已聯為一體，各類網路用戶數量極大，你很難搞清楚攻擊是來自國內還是國外，也很難搞清楚某次攻擊究竟應算是犯罪活動，還是戰爭。準此，以傳統方式來區分（公家與私人利益、戰爭與犯罪的行為）以及地理分界線（如國與國之間的疆界），基本上，都會因為資訊網路的相互連結而錯綜複雜。[10]

（三）、認知處理（Perception Management）之擴大

資訊技術的日新月異，可能會大為增強欺敵作為與資料竄改作為

[9] Roger C.,Colander, Andrew S. Riddle. Eds., OP. cit., pp.17-18.
[10] Ibid, PP.19-21.

之能力，從而促使政府對安全相關方案尋求政治支持之工作甚感困難。尤其在資訊戰領域上，存在著高度不明確和不確定性的情況下，政府為因應可能的資訊戰攻擊，所採取的任何管制行動，都已使政府認知處理角色擴大。[11]

（四）、戰略情報（Strategic intelligence）的挑戰

傳統式情報蒐集與分析方法，在因應戰略資訊戰情報挑戰上之用途可能極為有限。在資訊戰時代，你可能不知道你的敵人是誰、意圖是什麼、能力有多大。由於資訊戰的低進入成本與邊界模糊不清，情報機關在提供當前和未來的威脅的及時和可信的情報方面將面臨極大困難。傳統的戰略情報蒐集是把注意力集中於若干特定的國家，但現在，種種非國家實體，如非政府組織、國際犯罪集團等，也有可能構成威脅，因此順應戰略資訊戰的發展，也應該將上述非國家實體列入戰略情報蒐集的對象之中。[12]

（五）、戰術警報與攻擊評估（Tactical Warning and attack assessment）面臨挑戰

由於戰略信息戰的防衛及進攻術極為精密與多樣化，因此，結果是你可能不知道你已經受到攻擊、誰在攻擊、怎樣攻擊。現在的通訊網絡、數據管理系統和系統控制都極為複雜，有些事故可能是由於操作、偶然故障或自身系統設計錯誤引起的，因此，如何將這些與敵人的資訊戰破壞相區別是個極其困難的任務。另外，完全有可能系統是在長達數年的「戰場準備」過程中被滲透或損害的一敵人可以在你的軟體或硬體中設置「邏輯炸彈」（Logic Bomb），[13]平時完全正常，到關鍵時刻用一個特殊指令啟動，便會破壞你整個系統。職是之故，我們可以清楚知道，在目前仍無適切的戰術預警系統，可以分辨戰略資

[11] Ibid, PP22-23.
[12] Ibid, PP.24-26.
[13] 邏輯炸彈（Logic Bomb），基本上是一種精密病毒程式，在植入一段時間後會毀掉電腦或整個網路的程式與資料。

訊戰攻擊行為和其它網路空間活動行為，這頗值得我們警惕。[14]

（六）、建立和持續聯合作業之困難（Building and Sustaining coalitions）

依靠聯合作業，可能會增大所有合作伙伴之安全體系，易於招致戰略資訊作戰攻擊，而給予敵人一種相當大的戰略優勢。例如，已開發國家依靠行動通訊網絡，很可能使那些國家的電話通信高度地易於招致損害。在資訊變革之初期階段，其它領域（例如能源、金融、交通）也可能是脆弱之處，敵人可能會採取攻擊行為以破壞多國參與之聯合作業。[15]

（七）、本土易招致攻擊（Vulnerability of the homeland）

誠如前述，資訊技術已使地理空間概念趨於模糊，戰場也已無前、後方之分。電腦網路系統可連線到的地方，都是潛在的戰場。現行的發展趨勢已顯示出，在資訊時代的國家，將日益仰賴複雜的網路管制系統，而這些系統亦將成為被攻擊的主要目標。[16]

總體而言，在上述對資訊戰這個總體概念的初步釐清之後，我們可以發現，資訊戰所涵蓋的範圍是相當廣泛的。誠如國防分析家黎比奇（Martin Libicki）所言，資訊戰此一名詞已經是「一種全包式的詮釋」。[17]這亦即是說，資訊戰不應只是將之定位在軍事層面，隨著資訊科技的發展，如果資訊戰要發揮概念上的作用，它就必須抓住以往一些名詞未涵蓋的層面。在理論上，資訊科技網路作業係立基於各作業點之間的相互連線，這些作業點可能是電腦位置、工作站或小型網路本身。因此，該網路強度主要係取決於其相互連線之程度，而不是取決於其個別作業點。就軍事方面來說，軍事網路本質（亦即相互連

[14] Ibid, PP.26-27.
[15] Ibid, PP.28-29.
[16] Ibid, PP.30-31.
[17] *Richard J. Harknett, Information Warfare and Defense (Parameters, US Army War*

線之概念）顯然就是關鍵目標。準此，若我們進一步將概念性網路連線結構來區分資訊戰之意涵就可得出，資訊戰乃是專注於「軍事連線網路」和「社會連線網路」形式的戰爭。

人們所嚮往的電腦網路時代, 是一個時間、距離幾乎為零的社會, 而自從電報、電話發明後，人類在文字通信和語言通信兩方面就開始嘗到縮小資訊時間差和空間差的甜頭。但是, 眼下必須正視的事實是, 隨著計算機、衛星通訊、光纖通信以及資訊影響絡處理技術的迅猛發展，資訊的產生、交換、傳遞、控制和利用也都發生著深刻變化，資訊資源不但成為繼物質資源和人力資源之後的另一種戰略資源，而且具有取之不盡、用之不竭的特性。為此，繼美國率先推出「資訊高速公路」計劃之後，許多國家也相繼提出「資訊高速公路」設想，並把此舉作為廿一世紀經濟騰飛的希望所在。但資訊科技是廣泛滲透各種領域的總體綜合技術，既可民用，也可軍用，因此，當四通八達，縱橫交錯的網際網路的興起，使軍用與民用資訊系統聯為一體，軍用資源開始融入社會網路系統，同樣，民用資訊資源也不斷與軍用系統滲透、交叉, 並與之重疊, 共享資訊, 形成軍民兼容的一體化網絡系統, 同「機」共濟時，[18]可以試想，若這些網絡遭到攻擊，其結果可想而知。上述軍民網絡聯為一體的特點已使現代戰爭與社會運行機制之間的關係更加緊密，戰爭的勝負影響社會的穩定性，社會的不穩定性也影響到戰爭的勝負。職是之故，在資訊時代來臨之際，所謂的資訊戰可能是由金融系統網絡混亂而引發，也可能是軍事、政治、經濟互為一體的連鎖反應，分不清是軍事較量或是政治論戰或是經濟紛爭了。

第二節　資訊戰的後設理論基礎

College, 1996), PP16-20

[18] 這裡所說的一體化網絡系統是指例如士兵所領軍餉的銀行網絡系統，也可能是其它所有人薪金的銀行系統，而我們所用的電力、水力、通訊系統其實也都來自同一網絡，並無嚴格區分軍用或民用。

今天，人類社會正處在時代大變革時期。從世界範圍來看，雖然不少發展中國家還處於農業經濟、農業社會向工業經濟、工業社會轉軌時期，但從世界經濟發展速度來看，以資訊和知識為基礎的知識經濟正在迅速發展，工業經濟向知識經濟的轉變已經成為不可逆轉的趨勢。人類社會型態正處在從工業社會向資訊社會的變革之中，資訊時代和資訊社會正迎面而來。一個創造知識財富的新型社會經濟型態和文明時代已經展現在我們面前。

科學技術的迅猛發展，社會時代的巨大變革，也正促使軍事領域發生一場全新的革命，眾多國家也都加入了這場新軍事變革的激烈角逐。雖在這場競爭中走在前面，誰就將贏得戰略主動。因此，在全新的資訊時代和資訊社會，我們所面臨的戰爭也將是全新的戰爭型態戰——資訊戰爭。這種新的戰爭型態固然與舊的戰爭型態有千絲萬縷的聯繫，但新的戰爭型態更有其特殊的、反映新新時代的特徵，以下本節力圖在把握資訊戰爭所處的時代特徵的理論基礎上，進行分析。

一、資訊戰爭的技術基礎——資訊技術及其變革

眾所皆知，當今時代的變革和社會的發展，是以科學技術革命為核心的新技術革命直接作用的結果。資訊科學與資訊技術的迅速發展，不僅全面推動著政治、經濟、科技、文化等持續的快速發展，而且從根本上改變社會的生產方式和生活方式。與此同時，資訊科學技術也將從根本上改變傳統武器裝備的性質，改變傳統戰爭的作戰方式，繼而成為資訊戰爭的形成和發展的關鍵技術基礎。

資訊作為一種資源，它的普遍性、共享性、增值性、可處理性和多效用性，使其對於人類具有特別重要的意義，無論是認識世界還是改造世界，都始終依賴於資訊並貫穿著對資訊的認識和利用。[19]因此，

[19] 李繼宗主編，**現代科學技術概論**（上海：復旦大學出版社，1994 年），頁 15-18。

簡單地說，所謂資訊技術，就是認識資訊、利用資訊、與資訊打交道的技術。它包括資訊的產生、獲取、變換、傳遞、存貯、處理、顯示、識別、提取、控制和使用的技術。作為一種綜合性的科學技術體系，資訊技術涉及到許多學科和技術分支。其主要包括：[20]

（一）　資訊獲取技術。又稱資訊採集技術或傳感技術，包括各種資訊檢測、變換和顯示等技術。

（二）　資訊傳遞技術。又稱通信技術，包括資訊的處理、傳遞和提取等技術。

（三）　資訊處理技術。主要是指計算機技術。包括資訊的存貯、分析和控制等技術。

隨著資訊的獲取技術、傳遞技術、處理技術不斷地發展。資訊技術是直接擴展人類資訊功能的技術。它是當代新技術革命的主導技術，代表了新技術革命的主流和方向。以資訊技術革命為核心的新技術革命改變了過去以物質和能量二者為中心的傳統自然科學觀念，讓位於以資訊、能量和物質三者為中心的現代科學觀念；傳統意義上的力量的科學，讓位於智慧和力量相結合的科學；以解放人類體力勞動為目標的傳統科學。因此，資訊科學技術的興起，就從根本上改變了整個科學技術的結構、內容和方向，改變了科學技術發展的景觀和科學思維的方式。人類普遍認識到，除人們所熟悉的物理性空間外，還有資訊空間的存在。人類在認識上的突破和由此而來的以資訊技術革命為核心的新技術革命的發生，促進了時代的變革，改變了人類社會的生產和生活方式。在軍事領域則變革了武器、變革了戰爭。人們所熟悉的物理性空間的戰爭，將演變為從物理空間到資訊空間的戰爭；演變為知識和力量相結合的戰爭；以物質和能量力量為基礎的機械化

[20] 鍾義信著，**信息的科學**（北京：光明出版社，1998 年），頁 60-63。

戰爭，將演變為以資訊為基礎的資訊戰爭。[21]

二、資訊戰的社會基礎——社會資訊化

隨著資訊技術不斷的變革、發展，資訊技術在社會各個領域中已被廣泛應用，資訊社會也已儼然成形。基本上，資訊化相對於工業化而言，是一個技術與現代社會相互作用的結果。這亦即是說，資訊化已超越工業化，成為國民經濟和社會結構框架的重心。當然社會資訊化進程是一個不平衡的發展過程（因為每個國家發展程度不一）。但從世界發達國家資訊化進程來看，資訊化有三個階段，即產業資訊化、經濟資訊化和社會資訊化，它們又相互作用和相互影響。不過這裡必須指出的是，資訊化的一個基本前提是社會對資訊、知識、科學技術的強烈需求。隨著社會資訊化的投入發展與資訊作為戰略資源的地位和作用越來越突出，這種需求意識就表現得更加強烈，資訊和知識日益成為生產力、競爭力和經濟發展的關鍵因素。[22]

隨著資訊化發展的延伸，建立一個能夠滿足社會日益增長的資訊需求，即既能高速傳輸資訊又能對所傳輸的資訊進行加工處理的資訊網路，就成為社會發展的必然趨勢。社會的資訊網路化也就成為現代社會資訊化的一個突出標誌。資訊網路的建立和使用早在六〇年代就已經開始，歷經數十年發展，其數量、規模、功能、普及率和上網人數，都是其初建時所始料未及的。[23]目前，這種能極大地擴展人類生存與發展空間的資訊網路，正處於更迅猛的發展時期，即處於網際網路（Internet）向建設資訊高速公路發展時期。而世界上多數國家也都承認，僅管各國經濟基礎、科技水平和社會發展水平存在明顯差異，但在資訊技術已發展到電腦網路化的新時代，建設本國的資訊高速公路並將其聯結成全球資訊高速公路是歷史發展潮流之所向。面對網路

[21] 周碧松等著，**信息戰爭**（北京：解放軍出版社，1998 年），頁 18-19。
[22] 熊光樹、鄔焜著，**信息與社會發展**（四川：西南財經大學出版社，1998 年），頁 169-173。
[23] *Neil Barrett, **The State of the Cybernation** (London: Kogan Page, 1996), PP.17-23.*

全球化的發展趨勢，雖然各國在管理經濟和社會生活的過程中將遇到一系列新的難題，國際關係也將受到嚴峻的挑戰，但是網路全球化的發展，相信有利用於強國經濟、科技和教育合作，推動文化交流，為各國提高綜合國力提供難得的機遇，這是一個挑戰與機遇並存的發展和變革時代。[24]

總的來說，以資訊技術革命為核心的新技術革新的發展和社會資訊化進程，為我們帶來的不僅是上面所說的變化而已，更重要的是關於知識和資訊網路為基礎的智能工具以及與之相關的生產方式的出現。知識是財富，科學是第一生產力，國家間的競爭是科學技術的競爭，這些概念反映在未來戰爭問題上則是知識力量間的競爭和較量。資訊社會生產工具、產業結構、生產方式的特徵，雖然不能完全對應地反映在資訊戰爭中，但其主要特徵如生產工具的資訊智能特徵、生產式綜合化、智能化、集約化、精細化特徵，產業和產品結構的知識特徵、生產和經營管理直接面向對象的特徵，以及對資訊的快速、準確、全面、高效的追求，都將體現在未來的資訊戰爭中。

資訊社會是網路化社會。網際網路的共享性和開放性，奠定了其在資訊社會中的基礎地位和基本價值。不過，它也是一柄「雙刃劍」，若被惡意地利用，用來製造動亂，將也會動搖社會根基。因此，可以這麼說，資訊戰爭也就是建立在上述這樣一個社會基礎之上的新型戰爭。

三、資訊戰爭的軍事基礎——軍事資訊化

在資訊技術革命的推動下，社會資訊化已成為當代社會發展中一股不可逆轉的潮流。在社會資訊化的同時，軍事資訊化也就成為軍事發展的必然。因為軍事領域是整個社會的一個重要組成部分，而軍事資訊化實際上就是在軍事領域廣泛地採用先進的資訊技術和裝備，有

[24] 鞠慶麒，**世紀工程：信息高速公路**（北京：經濟科學出版社，1996 年），頁 18-25。

效地開發和利用與國家安全和國家利益相關的資訊資源，從而全面提高軍事管理、教育、訓練、創新的效率和戰鬥力的過程。軍事資訊化的基礎與社會資訊化的基礎一樣都是資訊技術，所不同的是軍事資訊化依賴於軍事資訊技術（即用於軍事目的的資訊技術）。[25]在軍事資訊化進程中，軍事資訊技術起著十分關鍵的基礎作用，並集中體現在軍事技術結構和功能的變化之中，尤其是表現在軍事資訊系統裝備結構和功能的興革之中。

自六〇年代以來，以資訊技術為核心的迅猛發展及其在軍事領域的廣泛應用，不僅為提高武器裝備性能開闢了一條新的發展道路，更重要的是導致了軍事技術領域發生一場新的軍事技術革命，從而開創了武器裝備發展的一個嶄新時代。軍事資訊技術發展的一個直接結果，就是武器系統大量採用微電子技術及網路通訊技術為基礎的資訊技術，從而導致武器系的電子化、資訊化和網路化，大大地提高了武器裝備的戰鬥性能和現代化水平。此外，軍事資訊技術在推動武器裝備電子化、資訊化和網路化的同時，這導致一種新型武器系統——軍事資訊系統的出現，而且使其成為整個武器裝備體系的核心。[26]

總體而言，軍事資訊系統是一個以軍事資訊技術為核心的武器裝備體系，包括六大組成部分：（一）可獨立運行的自動化指揮系統和電子資訊對抗系統；（二）與平台一體化的資訊與制系統，如艦載、機載、車載、星載資訊系統；（三）與武器一體化的資訊與控制系統，如精確制導系統、武器火控系統等；（四）軍事人員使用的資訊與控制系統；（五）軍事教育訓練系統與控制系統；（六）其它軍事資訊系體系。以上各種系統進一步構成了完整軍事資訊系體系。不僅如此，軍事資訊技術還導致了大量情報作戰、電子作戰、網際空間作戰武器的出現和

[25] 這裡所指軍事資訊技術，包括軍用微電子技術、軍用傳感器技術、軍用通訊技術和軍用電腦網路技術等領域。周碧松等著，**信息戰爭**（北京：解放軍出版社，1998 年），頁 44-46。
[26] 王凱，**數字化部隊**（北京：解放軍出版社，1998 年），頁 7-16。

使用，使資訊技術在整個武器裝體系中的比重進一步提高。[27]

總的來說，軍事資訊技術的發展，直接導致了以精確制導武器為代表的資訊化彈藥、以電腦為主的資訊化、以 C4I 系統[28]為代表的軍事資訊與控制系統以及以電子戰武器為代表的資訊（網路）作戰武器等一大批高科技武器裝備的產生，大大地提高了整個武器裝備體系中資訊技術的含量和整體作戰效能，推動軍事資訊化的進程，使戰爭機器的運轉越來越依賴資訊和資訊資源。不過，若從另一個角度，從人類社會生產和生活方式的資訊化（即社會資訊化）到軍事資訊化，一個重要的共同特徵或共同基礎，就是現今資訊網路的普及。正是由於資訊網路特殊重要性，才使其成為資訊戰爭中交戰雙方爭奪的重心，但與此同時，也正是由於資訊網路的普及與易受攻擊的脆弱性，又將使其成為資訊戰爭中交戰雙方攻擊的首要重要重點。[29]

第三節　資訊戰之作戰形式變化及其影響

人類戰爭的實踐證明，軍事技術的每一次進步，戰爭的空間就或多或少地擴展一步。人類戰爭從叢林到平原、從平原到海洋、從天空再到太空，幾千年來，凡是人類能夠到達的空間，戰爭都會自覺或不自覺地延伸到那裡。而當人類進入資訊時代後，資訊科技正以其有的滲透性、普及性和衝擊性，進入社會政治、經濟和軍事領域之中，所引起的變革是前所未見的。就軍事層面來說，資訊時代的戰爭不僅遍

---

[27] 周碧松等著，**前揭書**，頁 48。

[28] C4I 系統是指保證指揮官和指揮機關對部隊人員和武器實施指揮與控制的「人——機」系統。其主要是由 C3I——「指揮」（command）、「控制」（control）、「通信」（communications）、「情報」（Intelligence）系統延伸而來，相較 C3I 系統，C4I 系統更強調計算機（computers）作用以及突出計算機網絡（computer Net）的作用。其它詳見王凱，**數字化部隊**（北京：解放軍出版社，1998 年），頁 23-26。

[29] Gerard P Brohm 著，蔣永芳譯，「掌握資訊優勢的利器」，**國防譯粹**，第 26 卷第 1 期，民國 88 年 1 月，頁 5-9。

及陸、海、空、天，而且還進入一個嶄新的領域——電子網路空間。[30]

從第一節我們對資訊戰總體概念的分析中，我們可以進一步區分資訊戰有廣義和狹義二種說法。廣義的資訊戰，指的是資訊已占有主導地位，運用資訊化裝備或由資訊化部隊進一切戰爭行動或非戰爭行動。它不僅包括軍事領域，還包括政治、經濟、文化等領域，一包括物質領域，還包括精神領域。而狹義的資訊戰僅僅只包括軍事資訊系統的對抗。[31]然而，事實上，若從未來資訊戰可能作用的實際範圍上考察，資訊戰決不會只限在軍事領域內較量，它滲透到社會生活的方面，使戰爭的概念及範圍空前的擴大，因為：

第一，資訊科技的發展，軍民兼容日趨緊密，對民用資訊的破壞也可以造成軍資訊的破壞。資訊科技迅猛發展使軍用、民用的界線日趨模糊，軍事資訊技術在為民用服務的過程中也不斷增強了對民用技術的依賴性，更多的新技術將從民間開發出來。這一方面提高資訊資源的利用效率，促進了經濟發展，另一方面也為敵方的攻擊行動提供了新的突破口。[32]

第二，資訊戰人員多樣化。在資訊時代，不僅軍人掌握著資訊技術，就連普通百姓也可以是資訊戰的參與者，他可以藉助網際網路（Internet）上的無限通道，攻擊敵方的金融、電力、政府、交通等系統。另外，像企業、宗教團體、恐怖組織、販毒集團等由於擁有資訊技術和便利條件都能夠實施資訊攻擊。[33]

第三，攻擊目標多樣化。在資訊時代，軍事、政治、經濟、社會、文化等密相關連，任何一個領域遭受損害，都可使其它領域受到強烈的

---

[30] 滕建群,「信息時代呼喚新的國防觀」, **中國國防報**, 1997 年 6 月 6 日, 第 8 版。
[31] 張韋杰、蘇劍飛,「信息戰應確立幾個觀念」, **現代軍事月刊**, 1999 年 2 月, 頁 29。
[32] **前揭文**, 頁 29。
[33] **前揭文**, 頁 30。

衝擊。因此，為達成戰爭目的而使用旁敲側擊手段將經常出現，如運用金融資訊手段造成敵方股市狂跌、貨幣貶值、經濟崩潰，使之失去維持戰爭的基礎。再如，利用資訊傳播廣泛及傳播速度快的特點，組織一些誤導性資訊來影響敵國民心，從內部進行分化。[34]

第四，攻擊手段的多樣化。單就軍事領域的資訊戰就有指管戰、情報戰、電子戰、心理戰、駭客戰、經資戰及網路戰等。[35]如果再加上其它領域的攻擊方法，資訊戰的手段可謂五花八門，種類繁多。[36]

由上述可知，未來資訊戰不單單出現在戰場上，而將會遍佈整個社會。在資訊時代，先進的網路系統將軍隊乃至整個社會聯結在一起，軍隊社會各個部分的組合運轉，都要靠微電腦處理器；這使得軍事裝備和民用設施聯繫緊密，相互兼容。在這樣一個網路時代世界裡，每個微處理器都是一種潛在的武器，各台電腦都有可能成為一個有效的作戰單元。任何社會團體或個人，只要掌握電腦通訊技術，擁有一台電腦和上網的電話線，就可以攻擊裝有微處理器的系統和網路相聯的裝備，利用網路來發動資訊戰。

國家間的戰爭，攻擊的首要目標是聯結國家政治、經濟、軍事設施和整個社會的電腦網路系統，利用新奇的資訊科技，多渠道、多形式地對敵方軍事與民用電腦網絡和通信系統進行快速、隱蔽的摧毀性破壞，包括破壞和癱瘓敵方軍事，金融、電信、行政、電力系統和電腦網絡，並且運用心理戰和戰略欺騙手段，動搖軍心、民心和政府信念，達到遏制敵對國家發動戰爭或使其失去戰爭能力。目前資訊戰正

---

[34] **前揭文**，頁 30。

[35] 根據美國國防大學的馬丁．李必克博士（Dr. Martin Libicki）的看法，資訊戰共有七種作戰形式。每一種作戰形式的目標、方法也都不一樣。其餘詳見國防部史政編譯局主編，**資訊作戰譯文彙輯**（台北：國防部史政編譯局，民國 86 年），頁 255-256。

[36] 張韋杰，前揭文，頁 30。

在向民間化發展，資訊戰既可以是正規軍人，也可以是十幾歲的青少年。資訊戰的非殺傷性武器裝備，主要是在民間開發和生產的，而不再為軍隊所獨有；作戰不僅僅在傳統武力戰場，而且還分佈於整個社會。[37]

由於資訊戰所衍生而來作戰形式的變化，資訊戰的攻擊形式也有所改變。這裡所說的資訊戰攻擊形式的變化，泛指綜合運用電子、網路、心理、火力等多種手段，針對敵方資訊系統的要害和薄弱環節，靈活採取相應戰法，積極干擾或破壞資訊，加以獲取、傳遞、處理和利用，最大限度地削弱敵方資訊優勢和指揮控制能力。它是軟殺和硬殺、物理攻擊與心理攻擊等多種手段的綜合運用。[38]換言之，隨著資訊戰理論的發展和資訊化武器裝備的大量使用，將使傳統的以機械化大兵團攻防作戰為主的樣式成為歷史；靈活多變的、以「軟殺」為主的資訊戰和機械化與資訊化相結合的「軟硬兼施」的作戰樣式將得到廣泛運用。[39]

伴隨著網際網路發展的全球化趨勢，以計算機技術為核心的資訊科技的迅猛發展，網際網路已開始向地球的各個角落輻射，其觸角也伸向了社會的各個領域。根據有關資料介紹，當今網際網路的發展已廣泛運用於醫療、交通、金融、貿易、軍事等各個領域，上網人口仍在以每月遞增 10%~15%的速度擴大，預計二〇〇五年全球上網人口將達到十億人。顯而易見，網際網路的興起已成為全球注視的焦點，而世界各國正在加緊建設的國家、地區乃至全球資訊基礎設施，最終將建成使各國乃至個人都能互聯互通的全球資訊網絡，完全超越過去傳

---

[37] 沈偉光,「遏制信息戰——知識軍事的時代使命」, **解放軍報**, 1999 年 2 月 2 月, 第 6 版。

[38] 孫強銀,「信息攻擊手段面面觀」, **現代軍事月刊**, 2000 年 3 月, 頁 30。

[39] 張鋒, **潮頭：全維信息化戰爭**（北京：中國青年出版社, 1995 年）, 頁 251。或見林中斌, **核霸**（台北：學生書局, 民國 87 年）, 頁 7-8。根據林中斌的說法, 軟殺傷的武器有四大類, 即電子干擾武器、電腦病毒、定向能武器或光束武器（directed energy weapons）及電磁脈衝炸彈（electromagnetic pulse bombs）。

統地理空間概念，形成一種新的「網路空間」(Cyber space)。[40]

在社會經濟領域普遍資訊化和網路化的同時，以計算機為核心的資訊科技也被大量採用，各種資訊系統聯上網路，形成龐大的資訊網絡系統。因此，一旦資訊網絡遭到攻擊甚至被摧毀，其影響範圍絕不單單只限於某一個領域，而是全面性的。準此，資訊網絡在未來作戰中, 則具有十分重要的地位和作用。正是因為資訊網絡的極端重要性, 決定了資訊網絡成為資訊戰的重點攻擊對象，而資訊網絡上的無限通道也顯示其自身的脆弱性，並也決定了資訊網絡必將成為資訊戰中最容易受到打擊的對象。[41]職是之故，一種全新的以計算機系統（電腦系統）和網路為主要對象的資訊網絡攻擊，已隨之出現並不斷發展。目前，這種對資訊網絡攻擊，已隨之出現並不斷發展。目前，這種對資訊網絡的攻擊已不再僅僅侷限於火力摧毀和電子干擾等傳統手段，而將逐步演變成資訊戰中一種全新的作戰樣式——網路空間作戰。

一般來說，網路空間作戰是以計算機（電腦）和計算機（電腦）網路作為主要目標，以先進資訊科技為基本手段，在整個網路空間上所進行的各類資訊攻防作戰的總稱。網路空間作戰在近年來已初步顯露，進入九〇年代以後，隨,者網際網路應用的日益普及，一些意外事件和越來越多的針對計算機（電腦）網絡的犯罪活動不斷出現。這種意外事件和犯罪活動所造成的嚴重危害已經使人們看到，即使無意中對公共計算機網絡的破壞，也可以輕易地使一個計算機（電腦）網絡發展較普及的國家難以招架，產生非常嚴重的後果。[42]例如，在一九九一年，美國一位農民在掩埋死牛時，意外挖斷一條光纜，結果導致美國聯邦航空管理局所屬三十個主要空中交通控制中心有四個關閉達五個多小時。一九九四年，美國最大電信公司，美國電話電報公司地區交換中心系統的一個軟體出現一個小小的故障，結果導致其長途電

---

[40] 魏特罕（Margaret Wertheim）著，**空間地圖：從但丁的空間到網路的空間**（台北：台灣商務印書館，1999 年），頁 177-181。
[41] 孫偉平、陳先彬，「計算機戰」，**現代軍事月刊**，1997 年 7 月，頁 26-29。
[42] **前揭文**，頁 27。

話網絡中斷九小時。同時，軍事資訊網絡也未能逃脫這類無意或有意的攻擊。波灣戰爭期間，美國國防部計算機網絡曾遭到破壞，一百多名專家經過四十八小時努力才使它恢復正常。一九九〇年代末期，美國軍方的報告亦指出，敵人不用直接進入美國，就能對美國計算機網絡系統進行攻擊，據美國國會總審計署披露，每年企圖滲透到美國軍用計算機網絡的行為達二十五萬起，而且 65%獲得了成功。這些事件也許是無意造成的，但從中足以看出蓄意破壞將會引起嚴重後果。據倫敦資訊安全會議公佈，預計二〇〇〇年，全球計算機網絡犯罪損失將達到二〇〇〇億美元。美國矽谷一名技術權威還指出，網路空間作戰足以使一個國家經濟陷入停頓，其作用不亞於核爆炸後產生的強大電磁脈衝。[43]

正因為網路空間作戰將產生如此巨大效力，以美國為首的發達國家紛紛採取各種有效措施，為未來實施網路空間作戰作準備，希望未來能利用電腦鍵盤與滑鼠在網路空間與敵人展開全面的資訊對抗，以資訊科技手段操縱敵人的媒體；通過網際網路進攻破壞敵人的金融和交通等經濟系統等等。

總的來說，網路空間作戰是在特定的時代背景和技術條件下出現的一種全新作戰樣式。與它作戰樣式相比，它具有以下特點：
第一、是作戰力量的廣泛性。由於只要掌握了資訊系統的專門知識並能有效地「闖入」重要的計算機（電腦）網絡，就可以實施網路空間作戰。因此，網路空間作戰將不再是軍人獨占的舞台，而是國家甚至非政府組織乃至個人都能實施的普遍行動。在網路空間作戰中，資訊科技的軍民通用性和計算機（電腦）網絡的互聯性，使得作戰力量非常廣泛化，不管是國家、地區、組織、集團還是個人，不管是軍人還是平民，只要備一定的計算機知識，掌握一定的網路攻擊手段，都有

[43] 周碧松，**前揭書**，頁 150。

可能介入其中。[44]

第二、是作戰手段的知識性。與傳統作戰不同，網路空間作戰人員並不是操縱槍、砲、飛機、艦船等傳統武器裝備，而是通過操縱電腦鍵盤和滑鼠，利用其豐富的計算機技術知識，尤其是入侵計算機網絡和傳播計算機病毒等方面的技能來實施作戰。[45]

第三、是作戰空間的廣闊性。網路空間作戰是在資訊網絡空間中實施的作戰。這種資訊網絡空間與有形的物理空間不同，它不受地域的任何制約，只要是網路能夠到達的地方，都是網路空間作戰可及的範圍。換言之，國家之間的地理分界線在這裡將失去作用，因為很難確定網路攻擊是來自國內還是國外，甚至根本就不知道誰在實施襲擊，有時還很難分清從犯罪到戰爭這些不同層次的反國家行為。[46]

第四、是作戰時間的連續性。網路空間作戰幾乎不受任何外界自然條件的干擾，沒有天候因素的制約，沒有地理環境的影響，沒有白天和黑夜的區別，其作戰時間具有連續性，而且網路空間的作戰的起始時間一般很難判斷，它並不以是否「交火」作為作戰開始的區分標誌，加上一般性網路犯罪和發動網路空間作戰之間也沒有明顯的界限。[47]因此，網路空間作戰的出現將真正淡化戰前、戰時、與戰後等時間觀念。[48]

第五、是作戰過程的突變化。網路空間作戰不同於傳統作戰，它並不完全是雙方物質、力量、智力的綜合競賽，而是一定意義上的知識力

---

[44] 李宗健，「網絡戰特點及手段」，**解放軍報**，1997 年 7 月 22 日，第 5 版。
[45] 張鋒，**前揭書**，頁 205-206。
[46] 前揭書，頁 203-204。
[47] 沈偉光，「信息邊界」一個必須關注的戰略話題，**中國國防報**，1997 年 4 月 15 日，第 6 版。
[48] 徐華保，「世紀之交的戰場走向」，**中國國防報**，1997 年 9 月 5 日，第 6 版。

競賽。其攻擊效果不受時間和距離的影響，而且有光速傳輸、瞬時到達的特性。當一方成功地對另一方網絡系統實施攻擊後，就會對其社會、政治、經濟、科技、文化、軍事系統造成極大的破壞，使整個作戰態勢發生急劇的變化，但整個網路空間作戰過程卻往往會在很短的時間內完成，也許是幾十分鐘、幾分鐘甚至幾秒鐘。[49]

從上述的網路空間作戰特點的論述中，我們可以進一步得到一些啟示，由於計算機網絡（電腦）系統的脆弱性，加上網絡攻擊的高度隱蔽性，使進攻者在網路空間作戰處於一種絕對的優勢地位，任何系統都可能受到攻擊。網路空間作戰的低投入和高效益的特點，使得開發資訊網路攻擊技術，不像研製和生產硬殺傷武器那樣需要巨大的人力、物力和財力支持，只要具備資訊系統的專業技能和少量資金就能進行。因此，網路空間攻擊能取得常規軍事行動無法達到的效果，能成為小國或弱國對付大國或強國的一種十分有效的手段，但同樣也是強國追求「不戰而屈人之兵」的強有力手段。

[49] 王健華,「簡析網絡戰」，**中國國防報**，1998 年 11 月 27 日，第 3 版。

第四章　中共資訊（信息）戰戰略及其逐行工具

當資訊戰（Information Warfare）或網路戰（Cyber-War）在本世紀末成為世界軍事研究顯學時，早在八０年代中期，尚不知軍事軍務革命（Revolution Militancy Affairs，簡稱 RMA）[1]為何物時，在北京某一角落，一位業餘研究者—沈偉光，[2]揭露了它的劃時代意義，因而沈偉光可以說是中共研究資訊戰爭第一人，更是該領域之世界先行者。因而我們可以從而了解到中共在所謂「資訊／信息戰」[3]研究領域上，非但不處於落後地位，更有持世界牛耳趨勢，和硬體的軍事現代化相比，共軍在戰爭理論上的突破更值得國人關切。

第一節　中共資訊（信息）戰戰略與其理論發展

一、信息戰之先驅——沈偉光的對稱論(Symmetric Information Warfare Theories)[4]

如前所述，中共「信息戰」理論提出始於八〇年代中期，沈偉光，這位非資訊專業領域中級軍官，卻比未來學研究大師托佛勒（A.Toffler）更早關切此一命題，沈偉光早在一九八七年的《解放軍

---

[1] 軍事軍務革命(**Revolution Militancy Affairs, RMA)**，到波灣戰爭後方成為世界軍事研究主流，資訊戰屬於 RMA 一環，而中共在這方面的發展最受到注意。Ginsberg, Daniel, "Transformational change and the future of the Chinese military", **SAIS Review** (: Winter/Spring 1998), pp153-174.

[2] 沈偉光雖有軍職，但本人未受過任何相關訓練，其理論自創成份較多。

[3] 「資訊」和「信息」均從英文的 Information 而來的，兩詞本義相同。

[4] 沈本人未將信息戰分類為「對稱」(Symmetric)、「不對稱」(asymmetric)，然而沈主張發展以通訊系統(即為美軍的 C4I)為中心的作戰體系，和 90 年代中期共軍理論界強調發展網路戰爭和破壞 C4I 為主的「不對稱信息戰」大異其趣，筆者將沈的信息戰理論定義為「對稱」信息戰論。

報》就提出此一概念，而美軍到九〇年代中期才將焦點轉移至此。[5]在九〇年代初的波灣戰爭，美軍各種「智慧武器」如隱形轟炸機、巡弋飛彈的威力，才使得艾文托佛勒受到刺激，著手撰寫**<<新戰爭論>>**，[6]將自己的第三波社會論轉移到軍事研究領域，不過他的腳步還是比沈偉光晚了三年，早在美軍全面攻擊伊拉克前的一九九０年三月，沈出版了世界第一本有系統介紹資訊戰爭專書—**《信息戰》**，依照沈的定義，沈將未來戰爭的焦點放在情報上，所謂情報也就是指「資訊」而言，以往戰爭中由人腦下達命令、傳達資訊，沈認為未來戰爭趨勢是將人腦和電腦經由網路串連起來，共同完成作戰指揮，才是抓住了未來戰爭「制高點」。[7]

沈偉光的見解在當時未受重視，然而當美軍利用C4I系統(Command Control Communication Computer-Intelligence Systems)，以數十枚衛星、預警機和上萬台電腦所構築出來的資訊作戰指揮體系，在波灣戰場上神乎奇技的表現，讓全世界都大吃一驚，而還處在「人民戰爭」年代的共軍也切身反省到自身在科技上落後的程度，[8]沈偉光的理論成果，令解放軍為之一振，好像在自家後院挖到寶藏般。

然而自一九九五年起全球軍事理論掀起資訊戰和信息戰熱潮，沈偉光亦發表了中國大陸第一篇有系統文章**＜信息戰研究導論＞**，[9]沈認為信息戰不光只是在戰術上運用電腦傳送情報、指揮作戰，作為「火力戰」配角，而是將其提升到「軟打擊」程度，也就是在雙方都高度依賴資訊系統前提下，以打擊對方 C4I 中樞為主要目標的戰爭，它給戰爭帶來下列震撼性變化：

---

[5] 林中斌，**核霸：透視跨世紀中共戰略武力**（台北：學生書局，1999 年），頁 13。
[6] 原名**"War and Anti-War; Sunnyvale at the Dawn of the 21st Century" ,**中文版,Alvin Toffler 原著，傅凌譯，**新戰爭論**（台北：時報文化，1994 年）。
[7] 本書在 90 年 2 月波灣戰前，由浙江大學出版社出版，詳見沈偉光，**新戰爭論**，（杭州，浙江大學出版社，1990 年 3 月）。
[8] 徐華保，「世紀之交的戰場走向」，**中國國防報**，1997 年 9 月 5 日，第 6 版。
[9] 沈偉光，「信息戰研究導論」，**解放軍報**，1995 年 11 月 7 日。

(一)、軍隊行動自由取決於信息戰。
(二)、作戰目標的選擇以打亂對方決策程序為主。
(三)、火力運用從打覆蓋面轉為「點穴」。

沈的論點不外乎歸結美軍在波灣戰爭獲勝經驗，反映出「第三波部隊」過度依賴資訊弱點，而科技相對落後的共軍，應將力量放在「資訊化部隊」和「智囊團」建設。

九０年代後半開始共軍年輕將領也對此理論深感興趣，不過被稱之為「點穴戰爭」，所謂「點穴」也就是指「敵方之電子系統弱環節和要害部位，點其要穴，癱其全身，尋求最佳作戰效益」，也就是說共軍希望藉由此一手段，先摧毀 C4I，使其作戰指揮系統失靈，致使敵先進武器無法動彈，而共軍便可乘虛而入[10]，而非投注力量建立類似美軍的 C4I 系統，因為許多共軍將領認為中國大陸無能力組建一支「第三波部隊」，因為付出財力將十分驚人。世紀末的一九九九年，共軍內部對此又有了理論上突破，《**超限戰**》一書，可以說是中共對信息戰理論加以重新詮釋。

二、信息戰再詮釋——「超限戰」的不對稱論（Asymmetric Information Warfare Theories）

(一)、「信息戰」再認識：

本書認為諸如巡弋飛彈等智慧武器只不過將第二波武器加裝信導向裝置雷達，算不上是 100%資訊武器，使用電腦程式破壞對方 C4I 系統，才是真正「信息戰」戰爭。

（二)、在何地作戰？

作者認為從陸權、海權到空權，都不脫離地球的自然空間，然而

[10] 林中斌，**核霸**，頁 4。

在資訊戰爭時代一大突破是戰場走向非自然空間、電子空間，[11]在未來的資訊戰爭中，陸、海、空防禦都失去意義，因為「網路空間」根本毫無限制，只要有電腦存在的場所都是戰場。

（三）、誰在作戰？

入侵看似神聖不可侵犯的美國國防部的歹徒，居然只是一名十六歲高中生，他成為駭客目的只是遊戲，參與這場「遊戲」的駭客，光是「光顧」五角大廈，每天約有 7000 件。大部份的駭客只存惡作劇心態，像上述這位十六歲英國少年，但阿拉伯恐怖份子的打算不會那麼單純，對五角大廈的興趣決不比對美駐坦桑尼亞大使館少，因而信息戰爭中，入侵者的身分可說級為複雜而危險。

（四）、用什麼手段作戰？

作者認為未來戰爭趨勢是「非戰爭軍事行動」，也就是在不見軍隊、武器出場情形下，以電腦入侵敵方政府機關、金融機構和媒體網路，竊取機密、破壞經濟秩序、散布虛假消息，進而擾亂整個社會秩序，而這些手段都是非武力、非軍事甚至是非殺傷方法，它們超越以往暴力戰爭界限，因而稱做「超限戰」。[12]

三、中共新世代信息戰爭理論背景——「不對稱戰爭論」(對稱和不對稱信息戰的理論與實際見表 4-1)

新一代共軍將領，熱衷「不對稱信息戰」重要原因是——「武器代差」，波灣戰爭中的 F-117 隱形轟炸機、阿帕契攻擊直昇機等美軍「硬殺」裝備，共軍內部估計最少落後美軍十五至二十年以上，且這個差距不因共軍現代化而有所減少，而且共軍到達到這個水平起碼要花上

[11] 電子空間如前章所定義，無地理上距離可言，排除掉網路頻寬因素，彼此間距離只有 1/8 秒，在寬頻網路或下世代固定網路下即可接近此一水平。

[12] 喬良、王湘穗著，**超限戰——對全球化時代戰爭與戰法的想定**（北京：解放軍文藝出版社，1999 年 2 月），頁 34-55。

千億美元，因而沈偉光在九〇年代初期所定義「信息戰」理論，似乎是個遙不可及夢想，因而喬、王等人在內的共軍專家，以孫子兵法「以弱戰強，以虛避實」名言，發展所謂「軟殺」武器，[13]也就是以網路入侵等方式破壞敵 C4I 系統、網際網路為主，而先避開與敵人精良「硬殺」裝備交鋒，待其耳目癱瘓再展開正規戰役。

「不對稱戰爭」理論要義套孫子兵法一句銘言就是「以上駟制下駟」，共軍了解到自身三軍武器現代化程度遠遠落其假想敵美、日乃至於中華民國之後，然而這些國家卻又依賴資訊化、科技化，因而這個「脆弱環節」便成為共軍「電子珍珠港」（An Electronic Pearl Harbor）侵襲極佳目標。[14]

林中斌認為中共發展不對稱戰爭除了技術上顧慮，尚有政治上考量：

（一）、不願重創台灣經濟

中共若以火力武器硬殺武器即便可順利占領台灣，但一切基礎建設均毀於戰火，到時中共不但得不到經濟利益，還會負擔沈重重建經費而得不償失，而「信息戰」、「點穴戰」[15]只破壞電子設備無此顧慮。

（二）、殺戮不足以恐其心。

「最好不死人，儘量不死人，要死死軍人。」這是一九九０年代末期共軍研究攻台方式的考慮，但台灣地狹人稠，死傷人數必然十分驚人，將超過二二八事件，而不管在滿清、日本統治下血腥鎮壓措施，台灣依然有三十二次革命爆發，而二二八事件帶給國民黨更是半世紀

---

[13] 信息戰軟殺武器如駭客使用個人電腦（PC）、寬頻數據機（Fixed Network Modem）等「裝備」，價值不超過 3000 美元，最精密的電磁脈衝炸彈也不會超過數百萬美元，而一架美軍 F-15 造價超過 5000 萬美元，且訓練飛行是成本尚不計算在內。其他詳閱喬良、王湘穗著，**前揭書**，頁 11-17。

[14] 喬良、王湘穗著，**超限戰——對全球化時代戰爭與戰法的想定**，頁 18-27；Edward Topeka and William Triplet II, **Red Dragon Rising -Communist- China's Military Threat to Camera**, (Washington: Regency Publisher, 1999), PP121-184.

[15]點穴戰即為「點」敵 C4I 系統，為不對稱戰爭另一種說法。

困擾，因而中共不願再步上國民黨後塵。

（三）、政治勢力干預

正規方式攻台必然動用海空軍封鎖海峽，以飛彈攻擊、轟炸，耗時費日必然引起國際干預和制裁，而點穴戰、不對稱戰爭必可速戰速決，減少對他國衝擊，減低干預意願。[16]

[16] 林中斌，**核霸**，頁 18-20。

	「對稱」	「不對稱」
時　　間	1980 年後半至 1990 年初	1990 年代後半
代表性人物	沈偉光	喬良、王湘穗
目　　標	以傳統軍事目標為主	所有上網主機
戰術特徵	以 C4I 系統為中心的傳統戰爭	網路游擊戰
作戰場域	場所(距地球表面 180KM~ －1KM)	電子空間
攻擊速度	以 M 族飛彈需 20 分	1/8 秒~1 秒
攻擊效果	不定	極大[17]
防禦能力	與資訊化程度、科技能力成正比	與資訊化程度、能力比反比
預警時間	5~15min	極短[18]
造成政治影響	極大	小
裝　　備	建構Ｃ４Ｉ系統為主	廉價個人電腦 ＥＭＰ
耗費經費	USD$100billoin	USD$3000

10million

10million

表 4-1．中共「對稱」和「不對稱」信息戰理論與實際比較[19]

[17] 若遭攻擊方資訊化程度高而又毫無準備，經濟、社會、國防體系將一夕崩潰，Edward Topeka and William Triplet II, **Red Dragon Rising-Communist-China's Military Threat to Camera,** pp121~184.

[18] 遭入侵後若無法在第一時間內反應，所有主機將在很短時間內被駭客大量破壞，2000 年 2 月初美國多個大型網站遭入侵事件，4 月中旬查明嫌犯為一 15 歲加拿大青少年，竟在 4 個小時內單槍匹馬破壞 1000 多個網站，「癱瘓 CNN 網站 15 歲「黑手黨小子」被逮」，**中時電子報，2000 年 4 月 20 日，** http://www.chinatimes.com.tw

第二節　中共發展「信息戰」實際作為

戰略理論（Strategy theories）要成為政策（policy），必須經過相當時間蘊釀期，但中共發展信息戰似乎有迫不及待心態，在一九九八年此一熱潮興起後，成為中共整軍備戰重心所在，而中共在發展信息戰有下列幾方面建設：

.

1、組織整建

(1)、成立解放軍信息工程大學

中共軍委主席江澤民於一九九九年七月，下令組建了「解放軍信息工程大學」，合併了信息工程學院、電子技術學院和測繪學院，[20]其用意不言可喻，顯然有意將此學院做為「網軍」培訓搖籃，這是全世界第一所資訊戰專業軍事學校，稱它做「駭客大學」亦不為過。

(2)、成立政府網路安全中心

「網路戰」是「信息戰」戰略中較易實行戰術，這從駭客「地不分東南西北」、「人不分男女老幼」的特性可得知，因而中共本身也易成為「網路戰」目標，台灣「愛國」駭客對大陸多個機關改網頁的惡作劇，致使中共警覺自身網路安全之脆弱，隨即在一九九九年八月成立「網路安全中心」，以管制不良信息和保護信息安全，[21]但其成效猶令人存疑，因為大陸和台灣一樣，未設有美國國安局（NSA）的網路監控預警電腦，一旦網站遭入侵，無法一時間內反應，在缺乏預警系統情形下，大量網站將在極短時間內逐個被破壞或殲滅。

---

[19] 本表為作者自製。

[20]紅燕，「軍隊組建四所新院校」，**大公報**（香港），1999 年 7 月 3 日，第 3 版。

[21]大公報專電，「網絡安全中心成立，管制不良信息入侵」，**大公報**（香港），1999 年 8 月 11 日，第 2 版。

2、 軍隊演訓與建軍備戰

共軍作為中共發展「信息戰」主力，自然投注最多人力、物力軍隊建設、演訓，有下述作為：

（1)、建立 C4I 系統——建構「對稱」信息戰能力

C4I 系統是美軍八〇年代的產物，它係結合情報搜集、作戰指揮、訊息控制於一體，是信息戰基本建設，即使沈偉光等人早對此重要性有所體認，但 C4I 系統絕對是一個「大錢坑」，美軍最少用了 40 顆衛星才有波灣戰爭輝煌戰績，但中共似乎也甘願跳入此一「錢坑」。中共「九五計劃」的太空項目，準備效法美軍建立 C4I 系統，以數千億人民幣和 10 年時間，發射數十顆偵察和通訊衛星、建立 200 個地面通訊站、舖設 10 萬公里光纖通訊網、購十餘架 A-50 空中預警機，企圖達到和美軍相當的 C4I 能力，作為踏入信息戰基石，[22]此作為和「不對稱作戰」邏輯恰恰相反，「照搬照抄」成分更重。

（2)、購置超級電腦

一九九六年一月，中共以「學術用途」向美採購六台超級電腦（super-computer)，但此種每秒運算可達數兆次的設備，除了可用於民間科學用途外，也是發展核武不可一缺的裝備（用以模擬試爆)，更危險是它的運算能力是一般個人電腦千倍，應用在「網路戰」上是牛刀小試，這些超電腦絕對有能力在極短時間內癱瘓、破壞整個中、小型國家網路。[23]

(3)、「網軍」模擬對抗

---

[22] 廖宏祥、張國城，「共軍對資訊戰硬體建設的準備」，**中共對信息戰之研發與影響研討會**（台北：台灣綜合研究戰略與國際研究所，2000 年 2 月)，頁 2-13~2-19。「中共太空指管通情系統的建設」，**全球防衛雜誌**，157 期，1997 年 9 月，，頁 50~65。

[23] 依美國眾議員寇克斯（Cox）的中共軍情報告，認為這些電腦極有可能用來破壞美國或其他國家網路。See House Representation Chrisuphor Cox, **Report of the Select Committee on v-s Natural Security and Military / Commercial concerts with PRC** (統稱 Cox Report),www.house.gov/coxreport/,ch-3.

這裡指的「網軍」不是先進國家所慣用的「電子兵棋」，而是網路軍隊（cyber force），共軍企圖將常見駭客入侵行為應用在軍事行動，一九九六年共軍「瀋陽軍區」便舉辦一場「網軍」模擬對抗，進攻方的網軍便成功瓦解敵方司令部通訊、指揮系統，[24]此種「電子空間對抗」，已成為時下共軍最熱門項目，因為就戰術層面而言，網路入侵（cyber invasion）絕對是「不對稱」，因為此種駭客式軍事行動不需要先進科技，只針對網際網路 TCP/IP 協定開放性弱點，便可瓦解敵軍指揮系統。[25]

(4)、「863 計劃」

「863 計劃」是中共最早進行 RMA 的軍事科學研究計劃，它的發展項目有太空、激光（雷射）、生物科技、信息戰系統、能源、新材料，本計劃初發展目是有鑑於 80 年代中期美國推動星戰計劃（SDI），而中共亦欲「迎頭趕上」，在九〇年代「信息戰」和「不對稱戰爭」理論興起後，「863 計劃」中的「定向能武器」和「電磁脈衝」(Electric magnetic pulse)項目便成為炙手可熱項目。定向能武器包括微波武器（high powered microwave weapons）用以電子干擾、打擊隱形飛機；電磁脈衝項目中最具威力是「電磁脈衝炸彈」（Electric magnetic pulse bombs ,EMP），[26]此種小型特殊中子炸彈，能放出巨量電磁波，破壞半徑數百公里內一切電子設備。

3、 中共「不對稱」信息戰遂行戰術

如前所述，廣義信息戰理論包含建構 C4I 系統的「對稱」信息戰，與發展入侵敵 C4I 系統、網際網路的「不對稱」信息戰，而本文對信息戰戰術定義便是應用此種「不對稱武器」以破壞對方通訊系統和干擾社會秩序，而中共理論界認為信息戰有下列戰術：

---

[24] 沈偉光，**新戰爭論**（北京：人民出版社，1997 年 6 月），頁 167-198。
[25] 林中斌，**核霸**，頁 10-12。
[26] 汪志道，「電磁脈衝炸彈=EMP-bomb」，**尖端科技**(台北)，180 期(1999 年 8 月)，頁 62~65。

（1)、網路戰（Cyber warfare）或計算機戰（Computer warfare）

網路遭入侵、破壞是全球各地使用者的最痛, 然而共軍熱中此道, 稱為「計算機戰」, 因為諸如美、日、台等先進國家舉凡食、衣、住、行乃至於國防安全離不開資訊化設備與網際網路, [27]而網路戰有下列戰法：

Ａ、電腦「病毒」攻擊

所謂電腦「病毒」, 也就是一種人為破壞性程式, 它的型態有：

(a)、「定時炸彈」型

此種病毒會潛伏在對方網路, 等到特定時間才會突然起破壞作用, 例如中共可對某國的網路植入此種病毒, 該病毒會在共軍入侵前一刻才對敵國 C4I 系統發動攻擊, 癱瘓對方作戰指揮體系, 以配合正規作戰 , 不過此種攻擊型態還是有可能被發現而加以防止。

(b)超載型式複製型

此種病毒侵入後會巨量自我複製, 致使主機超載而無法工作, 美國多個大型網站於二０００年二月初皆受到此種病毒攻擊而停頓, 而此種網路攻擊型態雖然是破壞性最小, 但也是最難以防禦的, 因為網路主機永遠不可能拒絕接受外來資料, 此種手段可以輕易突破最高段防禦措施, 暫時癱瘓對方主機。 [28]

(c)、間諜型

此種病毒進入對方主機後, 會按程式設計並竊取特定文件, 而自動轉發至特定地點, 同樣的手法亦可用來攻擊金融機構主機, 將竊取主機內的資料(帳戶), 大規模的入侵將造成被入侵國經濟混亂。

---

[27] 汪志道, **前揭文**, 頁 65。

[28] Chris Taylor Behind, “The hackers are Attack”, **Times** (Asian Edition), Feb 21 2000, pp35-36.

(f)、邏輯炸彈型(Logic bomb)

邏輯炸彈型態類似「定時炸彈」，同樣藉由潛伏在對方主機中等待突擊，只不過邏輯炸彈攻擊能力更強，可以在發作時完全控制對方主機而為所欲為，例如中共可以潛伏此一病毒於某國戰管系統中，邏輯炸彈型可以在發作時控制戰管系統，令戰管系統下達錯誤指令，造成對方誤擊發生敵機／艦等混亂事件；邏輯炸彈型亦可潛伏在敵國民用交通管制系統如航空管制或捷運控管電腦中，誤導飛機或電聯車路線，令其發生大量重大交通意外，造成被入侵國社會秩序完全失控。

Ｂ、電腦滲透

滲透和入侵一向是駭客最愛，因為多半可神不知鬼不覺竊取資料、控制對方主機活動，包括：

(a)、應用密碼破解技術，突破防火牆和電子安全措施，而後可自由竊取機密信息。

(b)、硬體滲透，預先在電腦設備上裝置接收晶片，待被入侵主機運作，機密便會自動洩密。

(c)、控制對方主機網路，此種滲透難度較高，不過一旦控制對方電腦設備，形同將網路指揮下的武器、措施拱手送人。[29]

Ｃ、目標

網路戰所要打擊目標可分為軍事與非軍事目標。而軍事目標有：

(a)、C4I 系統指揮下軍種及偵察預警設備

軍事目標中以控制 C4I 中樞為首要目標，因而一旦 C4I 落入敵方駭客手中或遭癱瘓，三軍形同喪失指揮系統和耳目，中共「不對稱信息戰」理論便以入侵敵國 C4I 系統為主要軍事目標。[30]非軍事目標有：

---

[29] 孫偉平，「計算機戰」，**現代軍事**（北京）（1997 年 7 月號），轉載自**共軍「信息戰」研究專輯**(台北：國防部史政編譯局編印，民國 86 年)頁 322-328。

[30] **前揭書**，頁 329。

（a)、政府網站—竊取個人和政府機密

如前所述，中共軍事理論界認為以電腦病毒或滲透的方式竊取敵國國防機密，而非軍事目標的政府機構同樣有價值，因為在所謂全面推行「電子化政府」後，大部分的政府資料將會資訊化，入侵者便有機會從網路上竊取，這些政府機密諸如首長個人資料、民眾稅務資料、戶政資料、犯罪資料和軍民兩用科技等，在若遭中共自網路上竊取，後果將十分嚴重，因為如前所述在今日網際網路傳輸能力已經可以在 5 分鐘內下載 1 萬頁資料，到下一世代的網際網路通訊協定，這個時間將只剩下不到 1 秒鐘。因而「電子化政府」若沒有相關配套措施，頃刻間鉅量個人和政府機密將輕易成為中共情治單位桌邊材料。

(b)、破壞交通運輸控制系統（SCADAS）引發人為災害和社會秩序動亂

如前所述邏輯炸彈最佳攻擊目標之即為交通運輸控制系統（SCADAS)，在現代化國家大眾交通運輸工具如飛機、火車和捷運系統多半極度倚賴電腦系統操作，交通運輸系統可說是整個現代化國家經濟社會命脈，一但此系統出問題後果將十分嚴重，[31]在遭到邏輯炸彈攻擊後，電腦將被邏輯炸彈接管，而造成大量陸空交通意外，類似大園空難的人為交通意外將間連不斷發生，造成被入侵國交通完全停擺和社會秩序大亂。

(c)、入侵金融機構——引發經濟動亂

中共稱此種戰術為「金融戰」，東南亞金融危機給了中共軍事理論界一個很好示範，那就是像索羅斯這種國際炒家，光以炒作外匯方式亦可以顛覆一個中型國家的經濟，而索羅斯炒作方式乃是由網際網路自千里以外進行，喬良等人認為駭客亦可以入侵國際金融交易網路，入侵之後在一瞬間鉅量「買賣」敵對國家貨幣，令其經濟一夕間「泡沫化」，[32]然而事實上根本沒有「買賣」可言，只是駭客在網路中灌輸

[31]**前揭書**，頁 329。
[32] 喬良、王湘穗著，**超限戰——對全球化時代戰爭與戰法的想定**，頁 50~51。

不實數字而已。

(2)、信息心理戰（Information psychological warfare）

信息心理戰是由網路戰衍生而來，因為心理戰目標經由入侵敵方政府、傳媒主機來遂行其目的——信息威懾和信息欺騙，中共軍事研究專家認為未來世界傳媒發展趨勢將整合成「網路化」，電視、廣播、報紙等信息將皆由網際網路輸送，因為徹底控制網路將可擁有整個傳媒世界，因而信息戰戰略目標就不可不放在掌控日趨一體化的傳媒，藉此手段威嚇、擾亂敵國社會，使已方能「不戰而屈人之兵」，而心理戰又可分為兩種手段：

A、信息威懾

信息威懾的戰術是中共以網路入侵手段全面性控制敵方政府、傳媒網路，令其散布各種失敗消息，例如軍隊全面失敗或政府投降，而遭威懾國家軍隊、人民因傳媒控制無辨別真假，紛紛喪失鬥志或投降，而共軍趁此良機再乘虛而入。

B、信息欺騙

信息欺騙之手段乃是由共軍向敵國網路、傳媒散佈各種不實信息和謠言，由於遭入侵國傳媒、網路高度發達，致使不實信息也迅速為大眾所知，致使政府決策遭到阻斷，而社會大眾也惶惶不可終日，[33]例如 1998-1999 年我國股市多次因香港傳媒散佈中共軍演不實消息，在極短時間內致使台北股市多次重挫，[34]我方亦無計可施。

(3)、電磁脈衝炸彈（EMP）——電子性全面性破壞

此種戰術為信息戰中最具破壞力，因為其攻擊目標不限於電腦式

[33] 國防部史政編譯局編，樓海強，「威懾理論與理論威懾」，**共軍「信息戰」研究專輯**，頁 254-256。。

[34] 尤惠玲，「傳中共演習 國內股、匯市重挫」，**工商時報**，87 年 4 月 14 日，第 2 版。

網路，破壞半徑內一切電子裝備，精密如雷達、電腦，到最簡單的電子手錶，都會在其電磁波威力下完全被毀壞，可以說是一種「電子原子彈」(electric atomic- bomb)，但卻又對人體、一般建築物和設備不構成威脅。此種無選擇性電子性攻擊，將使得遭攻擊方軍隊裝備回到原始時代，除了喪失 C4I 系統外，一切電子偵察、火控設備皆成廢鐵，再精良「第三波部隊」也只有二次大戰水平。

對政府和民間而言損失恐怕更驚人，當政府大部機密、文件皆「資訊化」後，主機和硬碟卻葬送於 EMP 手中，整個政府將形同停擺。當民間金融機構交易「電子化」後，EMP 摧毀一切數據，千萬民眾的身家將隨強力電磁波一起消失。[35]此種廉價而又威力強大的「電子原子彈」，據美方情報顯示共軍已掌握相當技術。

第三節　中共信息戰能力評估及限制

本節中共信息戰能力評估重點在「不對稱能力」，因而 C4I 系統能力，不在本文討論中。

一、　中共信息戰能力評估

（一）、網路戰能力的迷思

由表 4-2 一九九六年美軍對中共資訊系統科技（Information Warfare Technology）評估中，中共只在資訊安全（Information Security）和訊息處理（Signal Processing）上粗具能力，而資訊戰科技幾乎無法與美日相比，連日本和台灣在許多面向都表現比中共好，這份九六年軍事科技報告似乎告諭世人，中共是一個”電子科技落後大國”。

[35] 國防部史政編譯局編，孫偉平等，「計算機戰」，**共軍「信息戰」研究專輯**，頁 324。

但網路戰是等同於有組織性駭客入侵，分佈在全球的駭客們多半只使用價值不超過３０００美金個人電腦（PC）和寬頻數據機，這些「武器」絕稱不上是高科技電子裝備，但荷蘭青少年用它幾乎控制駐沙美軍飛彈系統，[36]英國學生用它入侵美、韓核武研究機構[37]，更明顯例子是，一九九四年美軍內部「網軍」演習中，一名海軍軍官也用它令大西洋艦隊停擺。[38]這些「裝備」任何一個北京市民都可以在北京大學附近中關村電子街買到，遑論財力雄厚的解放軍。

美軍這份報告重點多放在 C4I 和電子偵察、火控分析上，而「不對稱戰爭」特性正是避開此種優勢，以網路 TCP/IP 協定脆弱性加以打擊，因而美軍也過份高估日、台資訊安全能力，日、台政府網站在 99 年成為大陸駭客成功惡作劇目標，而專責單位卻在事後才成立，兩國政府可以說是搞得狼狽不堪。

因而評估網路戰能力，決策者的意願（Will）、戰術運用（Strategy）、攻擊被攻擊國資訊化程度（Information）之反比(1/I)乘以網路預警能力(Alert)之和

＝W*S*(１／Ｉ)*A　是較為適切的定義（見表 4-3）

1、 意願（Will）

如表 4-3 所示，中共相較於自由世界的美、日各國，敢於冒犯網際網路空間神聖性，這可以從「不對稱戰爭」和「超限戰」理論在大陸被重視程度了解，因而中共發動網路戰意願對十分強烈，不像其他國家對此有所顧忌。

2、戰術運用（Strategy）

---

[36] 胡憶平，「入侵五角大廈「高手」年僅十七歲，荷蘭跨國組織差一點癱瘓美軍飛彈系統」，**中國時報**，1998 年 5 月 9 日，3 版。

[37] **前揭報**，第 3 版

[38] 馮良、徐立生，「未來作戰，無網不勝」，**解放軍報**，1998 年 7 月 7 日，第 6 版。

共軍戰史中，靈活運用「非正規戰術」，配合正規進攻，獲勝的成果十分豐碩，因而進入網路世紀後，「高科技條件下人民戰爭」口號也出爐，共軍專家正研究動員民間大量個人電腦從事駭客行動，破壞敵國 C4I 或網路，為正規作戰舖路，[39]此種合理化電腦犯罪行為，大概也只有以提倡「人民戰爭」為榮的共軍敢於運用，因而我們可以說，中共網路戰戰術運用可以說到了無所不用其極地步，先進國家未見有類似主張。

3、資訊化程度（Informational level），網路防禦力（１／Ｉ）

如 4-2 所示，中共整體資訊化程度甚低，遠遠落後於美、日、台之後，這猶如雙面刃道理，越依賴電腦、網路運作政治、經濟體系國家，等於是受網路攻擊機會更大，受創也將更嚴重，也就是說資訊化程度（Ｉ）和其防禦能力恰恰成反比(１／Ｉ)，因而資訊化程度愈高是越不利於發動資訊戰爭。中共緩慢的資訊化，對外網路呈現半封閉狀態，反使其在網路戰防禦上具有優勢，因為當先進國家要攻擊中共時，大概才會發現這個國家上網人口不到 3%，不知從何攻起。[40]

4、網路攻擊預警能力(Cyber-attack alert capability)

如我們在第三章所述，全世界目前只有美國政府部門和民間金融機構有網路攻擊預警能力，可在第一時間內偵測網路入侵者，並作出立即性防禦措施，台灣有所謂網路「八號分機」，但到目前為止未曾逮過任何一位境外入侵者，連調查局的網站都被攻破，[41]多個政府網站在遭境外駭客入侵後的 8~10 小時後方能恢復運作，這個時間足以下載九十六萬頁資料和破壞兩千個網站，而海峽兩岸像是一對難兄難弟，中共網路預警能力恐怕比台灣更差。

---

[39] 王新、張光軍，「把信息戰植根於人民戰爭沃土中」，**中國國防報**，1998 年 7 月 3 日，第 3 版。

[40] See Stephen Lawson ,Survey: China Internet use soaring ,**CNN.COM** http://www.cnn.com/2000/TECH/computing/01/25/china.net.use.idg/index.html

[41] 馬淑華，「調查局網站昨清晨遭篡改並被貼上五星旗 挑釁意味濃」，**中央日**

國家 / 指標	中國大陸	日本	美國	台灣
電子干擾能力 (Electronic Attack)	1	2	4	N-A
電子反制能力 (Electronic Protection)	0	2	4	N-A
高性能電腦 (High Performance Computers)	1	4	4	3
軟體研發能力 (Software)	1	3	4	2
資訊交換 (Info Exchange)	2	4	4	3
資訊安全 (Info Security)	2	4	4	3
資訊管理 (Info Sys Management)	2	4	4	3

表 4-2.美國軍事關鍵技術評估(MCTL)－資訊戰部分(Information Warfare Technology & Information Technologies[42]

報，:1999 年 8 月 16 日， 第 8 版。

[42] 轉載自: 廖宏祥、張國城，「共軍對資訊戰硬體建設的準備」，**中共對信息戰之研發與影響研討會論文集，**頁 2~9。其餘詳見 *U.S.DoD,Militarily Critical Technologies List,PartI&II,Office of theUnder Secretary of Defense for Acquistion and Technology,Jane 1996.*

國家 指標	中國大陸	台灣	美國[43]
意願(Will)	4	1	2
戰術(Strategic)	3	2	4
防禦能力=**資訊化程度反比(1/I)**	(1/1) [44]	(1/2)	(1/4)
預警能力(Alert)	1	1	3
總估：網路戰能力	12	1	6

表 4-3 各國網路戰能力評估.=(W＊S＊1/I＊A)

資料來源：U.S.DoD,Militarily Critical Technologies List,PartI&II,Office of theUnder Secretary of Defense for Acquistion and Technology,Jane 1996.

表 4-2 與 4-3 指標(Index)說明

0=不具(No Capability)

1=有限(Limited)

---

[43] 美國為網路戰爭研究先趨並在內部多次舉行演訓，故網路戰攻擊能力絕對在中共之上，但因美國資訊化程度極高，防禦面太廣，對網路戰防禦心有餘而力不足。Roger. C. Molander, *Andrew S. Riddle. Peter A. Welcomed,* **Strategic Information Warfare** (CA: RAND Company 1996), xi~xxi.；James Adams 著，**下一次世界大戰**，（台北：新新聞文化，1999 年），頁 175~250。

[44] 如前所述共軍極力建構類似美軍的 C4I，但至今成果有限，且政府與企業「網路化」比例不高，資訊化程度遠遠落後美、台，反使其網路戰防禦較易。

2=粗具(Some)
3=過半(Majority)
4=完全(All)
N-A：沒有評估

第四章　中共資訊（信息）戰戰略及其遂行工具

第五章　高科技資訊戰對我國資訊安全管理之影響

電腦與傳播科技大師尼洛龐帝（Nicholas Negroponet）在其**《數位生存》**（Being Digital）一書中指出，從原子潮流演變到位元潮流已是勢不可擋，不可逆轉。在網路通訊、多媒體技術日趨成熟的今天，我們也確實可以看到如文件資料、音樂、影片等傳統上必須藉助原子型態（紙張、錄音帶、影碟等）送文的物件，正漸漸地轉變成位元的型態，經由高效率的網路，傳送到大眾的眼前。[1]隨著網路普及與資訊設備型態持續提高而價格卻不斷下滑，已使許多的電子文件可以藉由電腦與網路系統進行，網際網路急遽成長已改變人類許多行為，但也衍生了許多管理上的問題。當人與資料互動的時候，如何在捕捉、分配、儲存及管理資訊流程中，提供適當的防護措施來確保資訊系統時竄改、竊取、遲滯、冒名傳送、否認已傳送、非法侵入等問題，而建置一個可以信賴的資訊系統作業的安全環境，以奠定資訊社會的基石，已是眾所矚目的焦點。

在網際網路發展之初，由於電腦設備價格昂貴，人們藉由網路的架設來共享這些昂貴的設備，從早期僅供學術單位、國防專用實驗計畫，發展至今隨著網路技術日漸成熟，相關電腦設備及網路使用成本降低，網路的使用越來越普及，網路架設的目的，逐漸從網路資源的共享轉為資料的共享，使用者更能便利的在網路上存取資料。我國為了因應網路全球化的發展趨勢，面對二十一世紀全球網路經濟競爭的新時代，亦積極推動國家資訊通信基礎建設，以提升國家競爭力，而「電子化政府／網路化政府」就是我國為了提升國家競爭力的一個重要環節。[2]

---

[1] *Nicholas Negroponte, **Being Digital** (New York: A. A. Knopf, c1995), pp.2-7.*

[2] 所謂的「電子化／網路化政府」，就是透過資訊與通信科技，將政府機關、民眾與資訊連在一起，建立互動系統，讓政府資訊與服務更加方便，隨時隨地可得；「電子化／網路化政府」是政府建立一與各界網網相接的資訊網路，把政府的公務處

隨著我國政府機關自民國五〇年代開始運用電腦設備處理行政業務以來，因為資訊科技不斷創新、發展，過去政府在處理行政業務上，從專屬主機、封閉網路、開放式分散處理系統，進入到現今已可大量運用個人電腦進行國際間網際網路之多媒體資訊交流應用，資訊之取得運用可謂極其方便而快速。然而隨著系統的的愈開放、電腦系統網網相連後，網路系統的安全考量，已大大超越了傳統大型主機的安全需求，不僅要保護網路資源的安全，更要考慮政府訊息在網路上傳遞的安全性。各種敏感的訊息在廣域、區域的網路間流通著，如何使訊息能快速正確的在網路上傳遞，同時又需要確保其機密性、避免被未授權者瀏覽。此外，還需確認訊息來源的正確性等，都是我們在建構「電子化／網路化政府」時所要考量的安全因素。

第一節　資訊系統安全與資訊系統安全稽核

「資訊系統安全」乃指一切保護資訊系統資源，包括：硬體、軟體、資料庫，以防止遭受變更、破壞未授權使用資訊系統資源之控制措施。其範圍不僅包括技術層面，尚包括組織管理面。以下擬將資訊系統安全區分下列五個方面來說明：[3]

（一）、安全管理（Security Management）

資訊系統安全問題根據過去研究指出，其主要問題是組織全面性問題而非資訊單位之問題，是管理問題而非技術問題，因此資訊系統安全首重安全管理。安全管理包括：資訊系統安全政策及策略之擬定、

理及服務作業，從現在的人工作業及電腦作業轉為數位化及網路化作業，以便利各界在任何時間、任何地點都可經由網路查詢政府各種資訊，並且在網路上直接申辦。簡言之，「電子化／網路化政府」就是化身在網路上來替民眾服務政府。因此，電子化／網路化政府的建構，不僅可提高政府效能，更能減少不必要資源浪費，亦能進一步創造國家競爭優勢。

[3] 吳琮璠，「國外政府機構資訊系統安全稽核制度」，**存款保險資訊季刊**，第 10 卷第 2 期，頁 21-22。

安全管理行政事宜、標準與作業之擬訂、資訊系統安全權責之歸屬，風險分析、資訊系統安全訓練等。

（二）、實體安全

乃指包括電腦相關實體資源，如：電腦機房、個人及各辦公室各種電腦相關設施、機房環境之控制措施。

（三）系統軟體安全

系統軟體基本上包括支援電腦及通訊作業支援、開發系統之環境及安全軟體等，系統軟體安全乃指包括系統軟體之安裝、修改、使用及存取資訊系統資源之管理與偵測等安全控管措施。資訊系統於開發時即應將一些系統安全功能安置在系統內，並於日常運作過程中持續維護改善。

（四）網路安全

基本上包括網路管理、上網之控制、撥接網路資源之安全控管等。

（五）應用系統安全

基本上包括系統開發、購置及系統變更之管理及控制、應用系統線上交易之控制。

當行政組織的業務廣泛運用資訊系統時，資訊系統是否安全，會影響行政組織業務執行的效率與效能。而資訊系統安全稽核的主要目的，乃在於確保資訊系統是否能安全有效的運用。因此，我們可廣義地對資訊系統安全稽核定義為「資訊系統安全稽核」乃指一套有系統之程序、蒐集受查人對資訊系統安全的主張或聲明之相關證據，並評估其與規定標準或準則相符的程度，並將稽核結果報告予相關人士。

根據美國內部稽核協會在一九九一年，針對企業內部稽核單位所作的調查結果發現（見表 5-1）：

（一）、在 247 個受訪者中有 61%指出使用電腦最高風險的區域乃在未經授權接近、修改資料或系統。在 61%的受訪者中，有 46%覺得這項風險在未來會降低，28%認為風險不會改變，甚至有 26%覺得未來這項風險還會上升。

（二）、有 73%受訪者認為免除這項風險的最有效控制方式是增強資訊系統安全與管制，其次有 7%認為是政策、標準、程序上的改變，亦有 6%認為是職權分工。

（三）、調查發現有 54%的組織已增強了資訊系統安全與接近控制，其中更有 46%組織對資訊系統接近全面性的管制。

（四）、有內部稽核單位不論規模大小都計畫在往後三年內增加對資訊系統安全的稽核管圍。下表顯示在小型稽核單位（一至十名稽核人員）、中型（十一至六十名稽核人員）、大型（六十名以上的稽核人員）內部稽核單位中，預計與實際的稽核範圍。

	過去二年實際稽核的範圍				未來三年實際稽核的範圍			
稽核類別	全體樣本	小型 (1-10 人)	中型 (11-60 人)	大型 (260 人)	全體樣本	小型 (1-10 人)	中型 (11-60 人)	大型 (260 人)
實體安全	88%	79%	90%	91%	96%	96%	94%	97%
資訊 (邏輯) 安全	91%	83%	93%	97%	97%	97%	96%	100%

表 5-1　預計與實際的稽核範圍

從以上調查資料顯示出一項重要訊息，即是資訊系統安全乃是稽核的一項重點，且其稽核範圍有逐年增加的趨勢。在我國政府機構努

力推動「電子化／網路化政府」的同時，是否也應慎重考慮在電子化／網路化過程中，如何確各機關建立適當之資訊全稽核制度以確保資訊系統之有效實施，保障國民之權益。[4]一般而言，由於電腦與網際網路的普及，利用電腦儲存資訊並以網際網路高速傳送資訊已是現代人最經濟與最便捷處理資訊的方式。以電子方式儲存在計算機（電腦）內部（如 ROM 及 RAM）或外加記憶體（如磁片、磁帶、光碟等）的資訊稱之為靜態資訊。而利用網際網路傳輸之資訊則稱之為動態資訊。不論是靜態資訊或動態資訊，這些電子化資訊均具有容易被偽造、複雜、加入、刪除及攔截的特性，為了避免這些資訊被非法存取、偽造及竊取，如何建構資訊系統安全稽核體系成為當前我國發展電子化／網路化政府中最重要的課題之一。

一九九八年八月，國內曾發生兩起與資訊安全有關的犯罪案例。第一件是某學校在其招生作業中，發生網路管理者竄改應試者的考試成績，讓考試分數較低的應試者，亦可跨越錄取門檻而上榜。第二件是國內某電信公司在招考技佐、技工過程裡，亦發生類似的情形，有人竄改電腦中所記載的考試分數，讓整個招考過程失去公平性。[5]一九九九年八月，兩岸更因「兩國論」效應，引爆網路大戰，兩岸網路駭客（hacker）皆鎖定對方政府及公營機構網站，造成網站運作停擺。[6]而今年二月，一些國際知名大型電子商務網站如 Yahoo、Amazon、E-Trade 與 e-Bay 等皆被網路駭客攻擊，以雅虎（Yahoo）為例，其搜尋引擎與入門網站因此停頓了將近三小時，並無法提供服務給其客戶。[7]雖然雅虎的電腦系統沒有完全被突破，只是網路上不肖人員有計畫地將大量的儲封包送到其網站干擾伺服器，導致該系統無法處理這

[4] 吳琮璠，**前揭文**，頁 23。
[5] 朱瑞秋，「談 NT 的稽核功能與資訊安全」，**旗標資訊月刊**，1998 年 10 月第 57 期，頁 239。
[6] 詳見羅添成，「中國電子戰，侵台 60 餘次」，**自由時報**，1999 年 9 月 15 日第 3 版；羅如蘭，「中共發動資訊戰」，1999 年 8 月 17 日，第 14 版。
[7] 詳見**聯合報**，2000 年 2 月 16 日第 5 版。

些巨量的需求而停止運作。從上述所列舉的實例當中，可以清楚看出，隨著網路全球化的發展不斷地深化，網際網路已是電腦入侵者活動與孳生的溫床，一天之內有成千上萬個電腦駭客活動其間是常有的事。據估計全球網路被電腦駭客入侵而被發現者只有四分之一，相對地，有四分之三未被發現。網際網路上的無限通道，提供許多有心人士可以不費吹灰之力從一系統轉換到另一系統。現代竊賊用電腦網路比用槍能竊取更多更貴重的東西，而恐怖分子也可能以鍵盤取代炸彈。[8]

整體而言，隨著資訊科技的革新使得電腦的處理速度和資訊儲存量大增，電腦的售價相對地大幅降低，功能也愈來愈強。這種資訊科技的突破與創新，使得利用電腦來處理人類經濟活動的資訊社會已然成形。而各國政府面對電腦通訊網路的發展趨勢，亦積極推動國家資訊通信基礎建設，並建構電子化／網路化政府，以提昇政府行政效率。而各大型企業，如航空公司飛機訂位、氣象預測、銀行資金往來、產業生產活動及產品交易等，也無不使用網際網路。由於個人電腦的普及化加上政府大力發展網際網路，舉凡政治、經濟、社會及其他活動也都愈來愈依賴網際網路，在在顯示網際網路未來將成為人類生活中不可或缺的工具。然而，就在網際網路的使用不斷深入人類社會各個領域之際，伴隨著社會大眾的電腦知識及操作技巧的日漸增強，因為電腦本身不具有道德判斷力，於是在處理資料之過程，即有其先天之缺陷存在，加上人為因素的介入，濫用益形普遍，致使一種新的犯罪型態也就產生了——網路犯罪。雖然我國網路犯罪危害之程度不如歐美先進國家嚴重，但就以網際網路在我國發展的趨勢與速度來說，若不及時預防，先作未雨綢繆之準備，將來勢難倖免。屆時對國家、社會所造成之危害，必較今日之傳統犯罪更為嚴重。[9]

基本上，網路化犯罪的發展速度是令人恐懼的。重大的安全破壞

[8] 李麒麟，「駭客攻防」，**資訊安全通訊**，第 5 卷第 3 期，1999 年 6 月，頁 86。
[9] **前揭文**，頁 87。

事故、駭客活動、軟體病毒製作都在以爆炸般的速度在發展。一般來說，恐怖主義最常見的行動方式是「不是激烈衝突」，這亦即是說通過靈活機動的小部隊，對薄弱部分發動攻擊以吸引國家政府和大眾儘可能多的關注，實際上是製造恐怖。但在資訊時代，網路恐怖主義也正在興起，網路恐怖主義者驚喜地發現在網路化空間比在現實空間更能為他們提供行動時不留任何痕跡的可能。一個毫不猶豫地在公共場所使用塑膠炸彈的恐怖主義分子顯然不會對在電腦系統內放置病毒有任何顧慮。類似這樣的攻擊行為，可以從幾英哩外的地方發起，也可以從另一個國家，甚至是從另一個大陸發起。[10]

一般而言，恐怖主義分子最可能攻擊的目標有三個：一是國家政府機關；二是對恐怖主義分子造成威嚇或被恐怖主義分子認為有妨礙作用的公司或某個企業；三是某個特定的社會團體或種族團體。[11]而網路恐怖主義對國家政府機關的電腦系統最主要的行動是發動駭客攻擊和設置病毒。這種攻擊行為實際上只是恐怖主義在網路化時代表現方式一種變更。在我國邁向網路化時代的同時，資訊安全對政府乃至於企業甚至是個人生活的成功至關重要，切斷一個人與資訊的聯繫就如同將他扣押或綁架一樣。能切斷某個人、某個團體或某個更廣泛的社會與外部通信聯繫的恐怖分子，就能夠散佈恐懼和驚慌。隨著人類社會步入網路化時代，網際網路產生了一個潘朵拉盒子般的效果。這些自由發展的技術已對國家、企業以及個人安全造成了威嚇。如果人們不能在這些技術控制人類之前對其加以控制，就必須為其所制，恐怖主義與網路化的結合就是一個明證。

我國近年來大力推動國家資訊通信基礎建設（NII）且之獲得相當大的成績，但相對地隨著國家資訊通信基礎建設的深化，台灣的經濟和社會愈來愈依賴資訊系統；資訊系統透過網路將資訊串連起來，因

[10] 郝瑞庭、賴輝亮主編，**信息霍亂——世紀末的冷面殺手**（北京：世界知識出版社，1999 年），頁 290。

此，資訊系統安全管理已儼然成為一個極重要的課題。就以台灣目前在網路建設上的程度而言，國家資訊基礎建設的防護已成為國家安全的問題，因為[12]：

（一）、台灣已逐漸成為國家資訊通信基礎建設完整性的國家，而這樣一個依賴國家資訊通信基礎建設的國家很容易遭受攻擊而陷入危險。這亦即是說，經由資訊戰的大規模破壞威脅已經被視為核戰大規模破壞威脅的潛在繼承者。換言之，若以兩岸情勢的發展來說，大陸當局如欲武力威嚇台灣統一，其動武方式也不見得需要透過傳統軍事力量，可以透過資訊戰方式破壞我國的國家資訊通信基礎建設，造成我國之癱瘓。

（二）、由於資訊戰是較不血腥但具有潛在更廣大效果的恐怖活動。一旦兩岸情勢緊張，大陸當局便可利用訓練有素的駭客以一具電話或電子郵件連線就足以通達眾多不同電腦。駭客能從一個節點跳到另一個節點，直到發現並利用一個重要的弱點為止。由於被偵測到的風險極底，而且遭反擊的風險更低，一次網路空間上的資訊戰的攻擊行動可能是很低廉而相當不具風險的。

（三）、由於海外科技商品、技術陸續傳回國內，同時使用現成科技商品已成為常規，因此，台灣的國家資訊基礎建設的一些科技產品（如電腦硬體、軟體）皆以外國規格為主。準此，一個未設防的國家資訊基礎建設將縱容敵人埋葬傳統的軍事作戰。

有鑑於資訊系統安全對於國家資訊通信基礎建設的重要性與日俱增，因此，隨著人類對資訊科技的依賴，所以各政府在努力推動國家資訊通信基礎建設的同時，也注意到必須防止攻擊國家資訊通信基礎

---

[11] **前揭書**，頁 290。

[12] *Martin C. Libicki,* ***Defending Cyberspace and Other Metaphors*** *(NDU Press, 1997), PP p.9-p11.*

建設的「資訊戰」的方式來保護自己資訊系統安全。美國可算是最早注意資訊系統安全問題的國家，一九九六年七月美國總克林頓簽署一份「國家關鍵基礎建設」的行政命令（Executive 0rder 13010），其部份內容如下：[13]

由於資訊設施的能力不足或被破壞可能使得美國的國防或經濟安全遭受損害，因而它們的作用至關重要。這類設施包括電子通信、電力系統、石油、天然氣的儲存、運輸、金融、交通、供水系統、緊急事故服務（醫藥、警察、消防和救護）和政府的連續性。對這些過程的威嚇可分成兩大類：一類是對有形財產的物質性威嚇，另一類是基於電子、無線電、計算機，對控制重要基礎設施的資訊和通信等關鍵機構的威嚇。

為了要克服易受攻擊的弱點並創建有效的資訊安全基礎，當前世界各國在努力推動國家資訊通信基礎建設的同時，也已經注意到資訊系統安全管理問題。不過由於一般人對資訊安全的認識大部份停留在模糊、不完備、不正確的觀念上，因此，許多電腦系統的運行缺乏足夠的安全防衛。其實防衛是尋求一個二度空間（見表 5-2）上的一點，其中一個向度是方便存取程度，從完全封閉至完全開放，一個系統若只能靠將壞人全部擋在系統之外才能安全，將使好人很難做他們工作。第二個向度是花在複雜程度的資源，一個複雜的系統能將壞人擋在系統外，而不會給合法的用戶帶來極大不方便。[14]

---

[13] *See Donn B. Parker,* ***Fighting Computer Crime*** *(John Wiley & Sons, 1999), pp.12-14.*

[14] *Martin C. Libicki, op. Cit, pp.18-22.*

安全選擇	安全削弱	安全支出
緊縮存取	用戶被阻擋在外或被迫改變工作習慣	用戶得費點力進入，但駭客們不行
放鬆存取	系統很容易受攻擊	用戶很容易進入，但大部份駭客行

表 5-2　安全選擇

從明顯的方法開始，一個位於安全地點，不接受任何外界輸入的電腦系統是無法侵入的。假使內部人士和原版軟體靠得住的話，資訊系統是很安全的。這樣的封閉資訊系統當然只有有限的價值，但對某些系統而言，更自由存取的利益卻不能和即使是最小安全缺失所可能造成的損失相比。換言之，若資訊系統內部缺乏一套安全稽核機制，將更容易造成嚴重的損失。根據調查顯示，在所有嚴重駭客入侵事例中，大約 70%至 85%牽涉到內部人士。準此，不僅是資訊系統安全需求性增大，連同建立一套資訊系統安全稽核制度也同等重要，因為多數資訊系統安全問題來自不當心的用戶差勁的系統安全管理稽核制度或錯誤偏佈的軟體。用戶經常選用容易猜的通行語而且還讓它們曝光，安全管理很差的系統包括那些讓用戶自行選擇通行語（明顯易猜）、使用預設的通行語或後門，未能安裝安全補強程式，或給用戶存取全部系統資源的權限來讀取或寫入檔案，而這些其實都是安全稽核制度所應禁止的項目。[15]

第二節　電子化／網路化政府之資訊安全理念、管理策略及其措施

為了提高國家競爭力，增進民眾的福祉，我國政府近年來積極推動全方位施政。在政治建設上，實施全民直接，並落實地方自治法制化，以精進民主政治之發展；在經濟建設上，加速推動十二項建設計

[15] *Ibid. pp.22-23.*

畫，以提昇國家整體競爭力，同時結合全民力量積極將台灣建設為亞太營運中心，俾能在區域性的競爭發展中取得優勢；在社會與文化建設上，政府努力推動文化與社會建設，以充實民眾生活內涵，提升全民生活品質。另為充分支援各項政經、社會及文化建設之推展，政府積極推動國家資訊通信基礎建設，並訂定「三年三百萬人上網」的目標（目標已於去年達到），全力推廣網際網路的普及使用；政府部門亦依據這項目標，全力推展「電子化／網路化政府」，以提高政府競爭力及服務品質。[16]而事實上政府在擬定電子化／網路化政府的實施計畫時，亦已經體認整個資訊安全管理工作的重要性。

基本上，電子化／網路化政府的資訊安全是以以下的基本理念來規劃及推動的[17]：

（一）、利用資訊與保護資訊同等重要。電子化政府一方面要充分利用資訊化及網路所帶來的效益及便利，一方面也要投入適當的資源來維護及保護政府資訊安全。

（二）、事前的預防重於事後的補救。電子化政府各項系統的發展及設計，都應該在系統發展的生命周期初期階段，即要依據資訊及系統的重要性，考量不同安全等級的安全措施。

（三）、資訊安全必須從全方位的觀念永續推動。電子化政府之資訊安全措施，除了要適度地採行各種資訊安全措施外，也要從管理及教育方面，從全方位的觀點推動。同時也要建立「資訊安全，人人有責」的觀念，把電子化政府的資訊安全工作，賦予在每一位機關的員工，而不僅是資訊單位的責任。

---

[16] 行政院資訊發展推動小組編，**邁向二十一世紀的電子化政府**（台北：行政院研考會，民國 87 年），頁 2。

[17] 何全德，「如何建立電子化政府資訊安全機制」，**資訊與電腦**，1999 年 10 月，頁 50-51。

（四）、資訊安全是相對的觀念，而非絕對的觀念。在此思維下，必須以各機關都有可能發生資訊安全事件作為前提，預先規畫各種防護措施。

（五）、資訊安全是一種看得見的服務品質。為了提供民眾安全及可信賴的網路應用環境，政府必須投入適當的資源來保護電子化政府的安全。

依據上述電子化／網路化政府之資訊安全的基本理念，政府進一步參酌一九九二年經濟合作暨發展組織（Organization of Economic Cooperation and Development; OECD）訂頒的資訊安全指導原則，採取三個 E 的管理策略來建立整體的資訊安全管理機制。各項管理措施茲修例分述如下[18]：

１、第一個 E：資訊安全技術（Engineering）

為了保護汽車駕駛人的生命安全，汽車製造商研發了安全氣囊反防鎖死煞車系統等各種主動式及被動式的防護措施；同樣的，為了保護資訊安全，也應該從資訊技術工程的觀點，針對系統上的弱點及安全漏洞，適當地利用防火牆、數位簽章、加密、IC 卡、SSO(Single Sign-On)、生物科技、系統安全漏洞掃描及入侵偵測等各種安全工具或技術，建構安全防護體系。

利用資訊安全技術建置資訊安全防護措施，是保護資訊安全的第一道防線。使用資訊安全技術，不一定保護絕對的安全；但是，沒有使用資訊安全技術，保護絕對不安全。至於應該選用哪一種安全技術或工具？要投入多少資源建構防護系統？則必須視要保護的資訊或系統的價值，分析可能的威脅、安全的漏洞或弱點，進行風險分析，再採行適當的安全對策。此外，從這次數起疑似大陸駭客入侵政府網站

[18] 轉引自何全德，**前揭文**，頁 50-53。

的事件分析，主要是利用已知的系統安全漏洞或不良設定，趁虛而行。所幸，很多技術上的致命傷及安全漏洞是可以彌補的；目前，台灣電腦危機處理中心（TW-CERT）及國外類似的組織，都會定期詳列最新發現的安全漏洞及修復的辦法。只要定期研讀參考這些安全報告，及早針對可能的系統弱點採取補救行動，就能減少被入侵的機會。

為了強化各機關資訊系統及網路存取的安全管理，行政院將要求各機關開放外界連線作業之資訊系統，必須視資料及系統之重要性及價值，採用資料加密、身分鑑別、電子簽章、防火牆及安全漏洞偵測等不同安全等級之技術或措施，防止資料及系統被侵入、破壞、竄改、刪除及未經授權之存取。例如，行政院研究發展考核委員會已經配合公文電子交換作業，決定採行數位簽章及電子信封的技術，並應用具有密碼處理能力的 IC 卡，存取機關的簽章私鑰及電子憑證，以強化系統存取的安全控制。

２、第二個 E：強制執行（Enforcement）

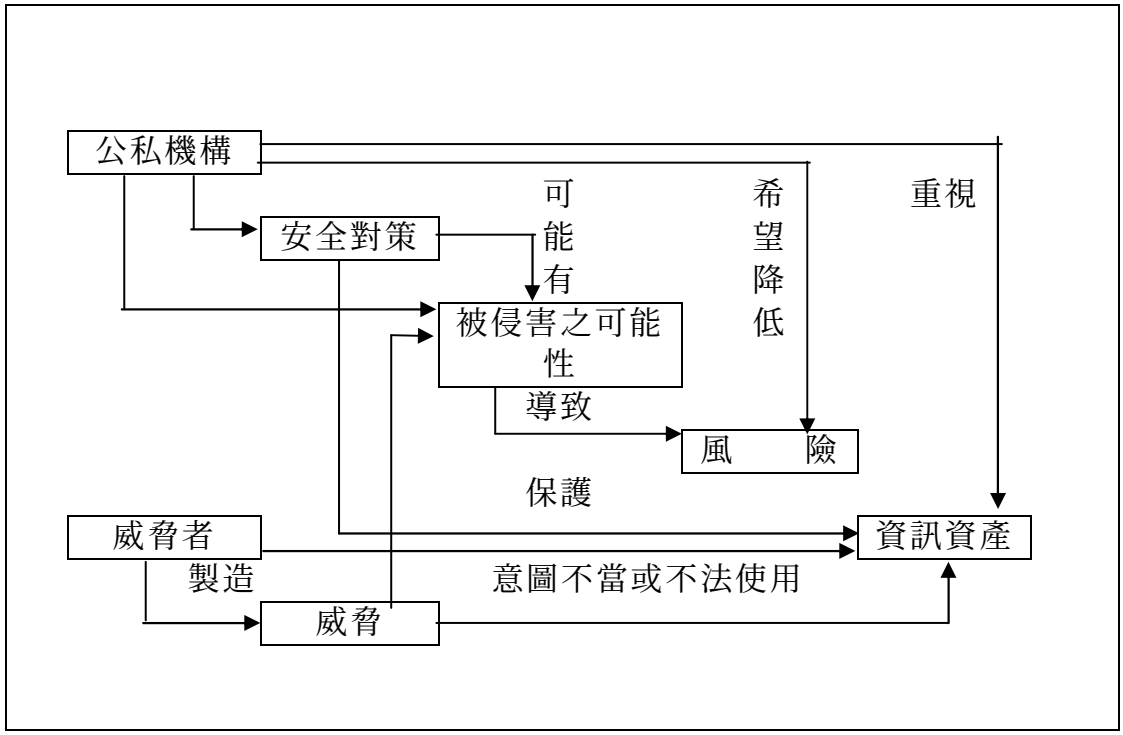
資訊安全是一項持續性的管理過程，而不是一項短期的計畫，資訊安全可說是一項「沒完沒了」的管理工作，隨著政府資訊化和網路化的依賴程度日深，以及資訊科技的日新月異，政府的資訊安全管理工作也必須與時俱進，從「全方位」的觀點，以「永續經營」的理念，持續地加強。並且要投入必要的資源強力執行，同時也要建立執行成效的監督及稽核制度，以確保電子化政府的資訊安全。

為推動政府各機關強化資訊安全管理，建立安全及可信賴之電子化政府，確保資料、系統、設備及網路安全，保障民眾權益，行政院研究發展考核委員會經參酌歐美等主要國家政府部門的資訊安全管理實務作業，並特別參考英國政府推動的資訊安全管理規範（BS 7799, Code of Practice for Information security Management），研訂「行政院及所屬各機關資訊安全管理規範」，並於八十八年十一月訂頒。就我國而言，可由國防部主導跨部會「網路安全組」推動。

根據資訊安全管理規範，各政府機關必須從下列重點逐步建立整體性的資訊安全管理機制（如圖 5-1、5-2）：

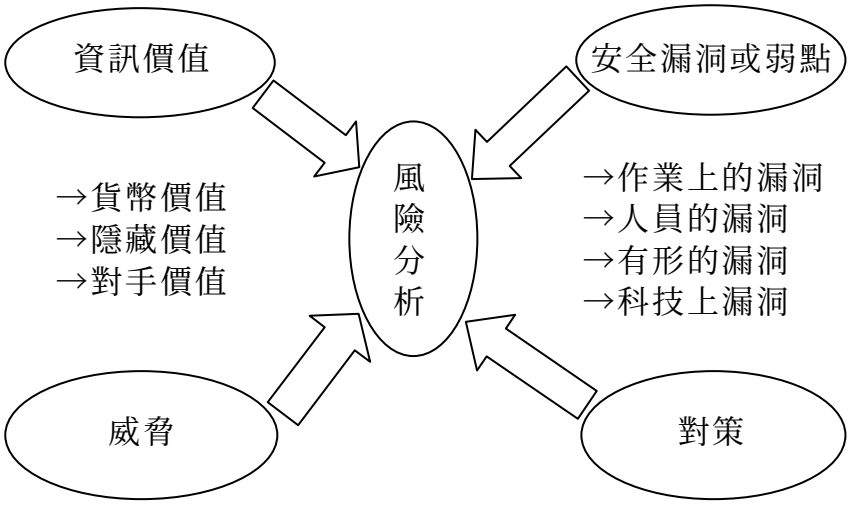
(1)、資訊安全政策制定及評估。
(2)、資訊安全組織及權責。
(3)、人員安全管理及教育訓練。
(4)、電腦系統安全管理。
(5)、網路安全管理。
(6)、系統存取控制。
(7)、系統發展及維護之安全管理。
(8)、資訊資產安全管理。
(9)、實體及環境安全管理。
(10)、業務永續運作計畫之規劃及管理。

圖 5-1　資訊安全對策分析示意圖



資料來源：何全德,「如何建立電子化政府資訊安全機制」,**資訊與電腦**, 第 231 期, 1999 年 10 月, 頁 50。

圖 5-2　資訊安全風險評估示意圖



資料來源：何全德，「如何建立電子化政府資訊安全機制」，**資訊與電腦**，第 231 期，1999 年 10 月，頁 50。

以網路安全管理為例，資訊安全管理規範特別規定：

1.各機關利用公眾網路傳送資訊或進行交易處理，必須評估可能之安全風險，確定資料傳輸具完整性、機密性、身分鑑別及不可否認性等安全需求，並針對資料傳輸、撥接線路、網路線路與設備、接外連接介面及路由器等事項，研擬妥適的安全控管措施。

2.規定各機關開放外界連線作業之資訊系統，應視資料及系統之重要性及價值，採用資料加密、身分鑑別、電子簽章、防火牆及安全漏洞偵測等不同安全等級之技術或措施，防止資料及系統被侵入、破壞、竄改、刪除及未經授權之存取。

3.各機關與外界網路連接之網點，必須以防火牆及其他必要安全設施，控管外界與機關內部網路之資料傳輸與資料存取。

4.各機關開放外界連線作業之資訊系統，必要時應以代理伺服器等方

式提供外界存取資料，避免外界直接進入資訊系統或資料庫存取資料。

5.各機關利用網際網路及全球資訊網公布及流通資訊，應實施資料安全等級評估，機密性、敏感性及未經當事人同意之個人隱私資料及文件，不得上網公布。

6.各機關應訂定電子郵件使用規定，機密性資料及文件，不得以電子郵件或其他電子方式傳送：機密性資料以外之敏感性資料及文件，如有電子傳送之需要，各機關應視需要以適當的加密或電子簽章等安全技術處理。

雖然，資訊安全管理規範對電子化／網路化政府之資訊系統安全維護提供一完整性規劃措施，但實際上仍須配合資訊系統安全稽核機制之建立，方能得到妥善的管理效益。基本上，所謂資訊系統安全稽核的主要目的，乃在於確保資訊系統是否能安全有效地運作。資訊系統安全稽核是指一套有系統蒐集受查對封象對資訊系統安全的主張或聲明之相關證據，並評估其與規定標準或準則相符的程度，且將稽核結果報告予相關人員的管理活動。

政府機關在推動電腦化的過程中，為確保資訊品質及資料的完整性與真確性，多少都已經建置了相關之控管措施。然而，資訊安全管理工作是否能夠落實執行，必須建立獨立的電腦稽核機制，由客觀的電腦稽核人員，依據政府及相關主管機關訂定的資訊安全管理政策及規定，持續評估機關推動資訊安全的實施績效，以確保資訊安全管理機制之落實執行。

目前，在國內除了少數財稅單位及國營事業，已經建立獨立及專責的稽核單位之外，大部分機關都還沒有建立電腦稽核制度。為了推動政府部門建立電腦稽核制度，行政院研究發展考核委員會會正協調中華民國電腦稽核協會，將電腦稽核的相關準則及實作經驗引進到政

府部門，以協助各機關建立電腦稽核制度。在實務作業上，政府電腦稽核工作將區分內部稽核及外部稽核兩種方式，由稽核人員定期對機關組織之安全管理、網路安全、實體安全、系統軟體安全、應用系統安全及資訊安全進行查核。

不過，世上沒有完美無暇的安全。總體而言，政府在推動電子化／網路化政府的同時，雖有資訊安全管理規範與資訊系統安全稽核機制的配套措施，但仍須建立起資訊安全事件的緊急處理機制，以發揮事前預防、偵測、事中監督及事後有效處理的功能。參考國外的經驗，政府應推動下列各項措施[19]：

1. 結合產、政、學、研等有關資訊科技、犯罪、社會學、心理學等各方面的專家，籌建電子化政府資訊安全事件警急處理機制，以發揮類似「網路 119」的功能。
2. 要求各機關從業務永續經營的觀點，評估各種人為及天然災害對機關正常業務運作之影響，訂定緊急應變及回復作業程序和相關人員之權責，並定期演練與調整更新計畫。
3. 要求各機關應建立資訊安全事件緊急處理機制，在發生資訊安全事件時，應依規定之處理程序，立即向權責主管單位或人員通報，採取反應措施，並聯繫檢警調單位協助偵查。

4.「前事不忘後事之師」，為避免各機關犯同樣的錯誤，研考會將結合建立資訊安全網站，提供各機關有關資訊安全弱點等各種資訊。

（三）第三個 E：教育及宣導（Education）

從各種統計資料及實務經驗顯示，人為疏失、員工缺乏安全警覺、不了解問題的嚴重性，是所有組織所面臨的最大安全漏洞。任何系統最薄弱的一環是人，在各種資訊安全對策中，投資報酬率最高的反制

[19] 何全德，**前揭文**，頁 52。

對策是對員工進行安全警覺訓練。唯有透過不斷的資訊安全教育及訓練，建立資訊安全的組織文化，才能使電子化政府的資訊安全管理工作落實到機關組織的運作中。

為了提升政府機關工作同仁的資訊安全警覺，行政院研考會已經擬定及實施「資訊安全及電腦稽核種子人才訓練計畫」。這項計畫共有五個系列，將針對各機關負責資訊業務處理的一般業務人員、政風人員、電腦稽核人員、資訊安全管理人員及網路安全管理人員，進行有計畫的培訓。以提升政府機關資訊安全管理的專業能力。

第三節　資訊戰對電子化／網路化政府的資訊安全之影響

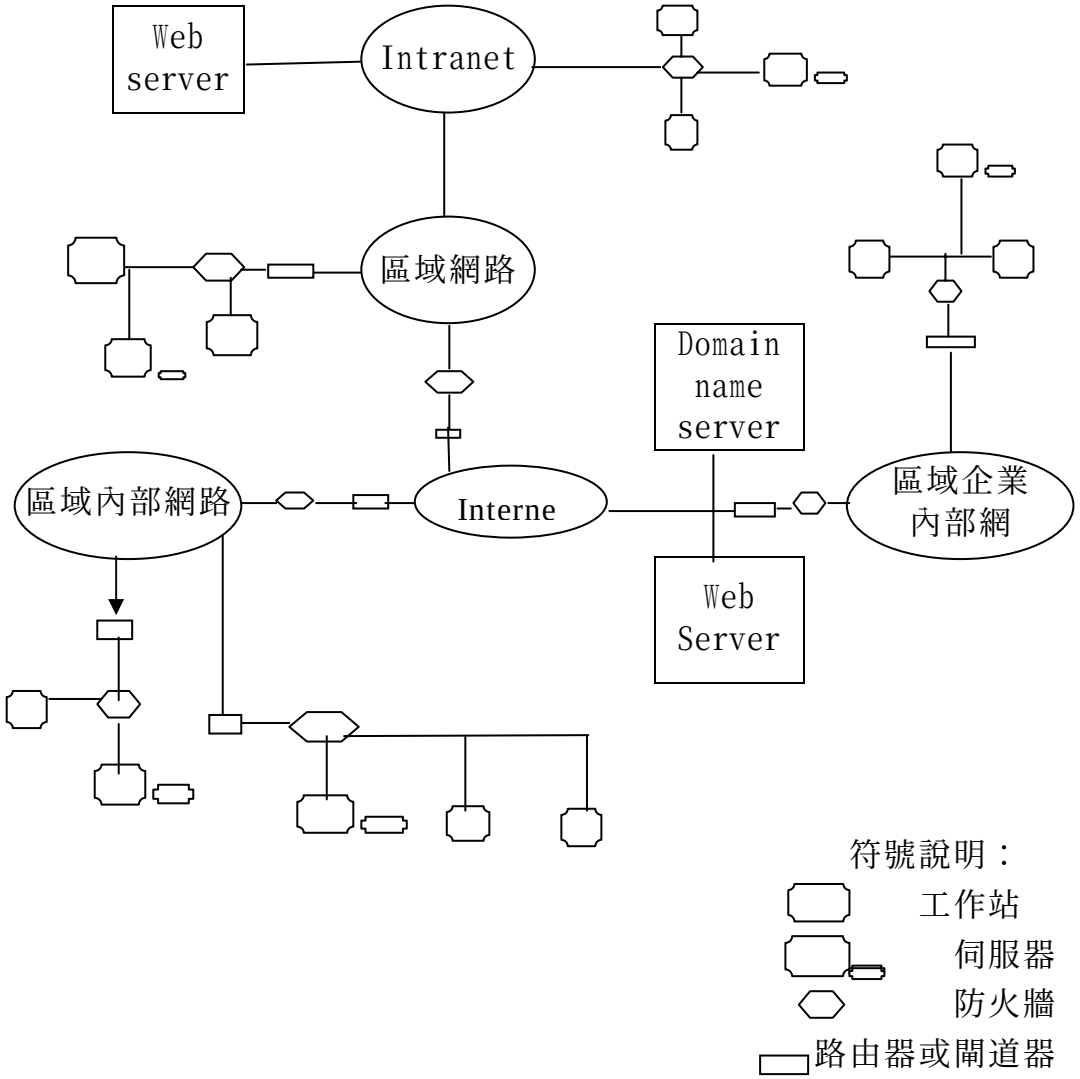
綜合上述二節之分析，我們可以清楚知道電子化／網路化政府的建構，首重於資訊系統的安全管理。因此，要做好電子化／網路化政府之網路系統的安全管理，首先得先了解電子化／網路化政府整體的架構，系統架設了那些硬體，使用何種作業系統、使用了哪些協定、安裝了哪些應用軟體、哪些人會使用這些系統，授權了哪些權限使用者。管理者需了解這些資訊後，進而分析系統的弱點何在，哪些人有可能會攻擊此系統、他們的目的是什麼、要攻擊哪些地方，有了這些資訊就可以幫助管理者訂定安全需求，採取必要的安全策略。

高科技資訊戰對電子化／網路化政府資訊安全所產生的最大威脅，即是由電腦網路系統作為其主要侵入點。而所謂的電腦網路又包含硬體、軟體及通訊機制。圖 5-3 簡單說明電腦網路系統的架構及其可能入侵點。其中路由器（Router）主要是銜接兩個或多個網路，其接收訊息封包，並根據繞路表（routing table）將訊息轉送往目的地；

閘道器（Gateway）連結了使用不同協定的網路；防火牆（Firewall）用於過濾可疑訊息；這些網路中的節點關係到訊息能否正確的送傳目的地，藉由這些硬體的控制，可確保系統正確的運作，訊息也得以在網路上傳送。此外，大部份的使用者對於網路的存取都是經由應用層的協定，這些協定包含了支援電子郵件的 SMTP（Simple Mail Transfer Protocol）、支援檔案傳輸的 FTP（File Transfer Protocol），及支援全球資訊網路（WWW）的 HTTP 等，這幾個協定雖帶給網路有更廣泛便捷的應用，但這幾個節點亦是最容易遭惡意侵入破壞的地方[20]。常見入侵並危及網路安全的方式包含了：利用電子郵件、利用 telnet 登入、試圖得到具有高存取權限的帳號、刪除或移動檔案等。近來，許多針對網路或個別主機上可疑活動的偵測方法被廣泛的討論，利用這些技術可自動找出可疑的活動．並事先加以防範。

圖 5-3　電腦網路架構圖及其可能入侵點

[20] J. Kimmins, “Network Security management and administration; Concepts and issues”, **Network Operations and Management Symposium, 1992, NOMS Computer Networks, 1996, Proceedings 21st IEEE Conference** on, pp.116-125, 1996.



在了解網路系統的整體架構後，管理者須對整個系統作一個風險評估，及其可能面臨的潛在威脅。首先我們需站在攻擊者的角度思考，哪些地方是攻擊者可以入侵的，要如何入侵。什麼樣的資訊是我們想要竊取及竄改的，攻擊者是外部或內部合法的使用者，是蓄意或無意間所進行的破壞，這都是我們必須加以考量的。例如：入侵者可以竊取合法使用者的登入資料，進行登入；經授權的合法使用者，利用其

存取權限洩漏機密資料。甚至蓄意的破壞網路；儲存在主機上的商業機密資料及業務資料等敏感訊息如何加以保護；系統如何防止病毒的入侵等。這些可能危及系統安全的缺失，大部分是意外所引起的，也常常是在正常的操作行為下無意間所發生的，攻擊者身分常常是對系統有相當了解的離職員工或蓄意的破壞者及間諜等，這些資訊都可以幫助我們研擬系統所需要的安全對策。以下歸納出幾個電子化/網路化政府的資訊系統可能面臨的安全威脅（security threats）[21]：

1.非法的侵入。
2.授權使用者蓄意的破壞及洩密。
3.攔截或修改網路上傳送的訊息。
4.惡意的軟體、電腦病毒的入侵。

有鑑於上述所歸納出可能對我電子化／網路化政府之資訊系統所面臨之安全威脅，筆者認為上述四種之可能性威脅，只要使資訊系統作到機密性（confidentiality)、完整性（integrity)、可驗證性（authentication)、不可否認性（non-repudiation)、存取控制（access control)、稽核（audit）等功能，配合封包過濾機制（packet-filtering mechanisms)、加密機制（encipherement mechanisms)、數位簽章機制（digital signature mechanisms)、資料完整性機制（data integrity mechanism)、使用者身分驗證機制（human user identification / authentication mechanism)、存取控制機制（access control / mechanisms)、金匙管理機制（key management mechanisms)、繞路控制機制（routing control mechanisms)、稽核機制（auditing mechanisms）等機制，自然可以作到基本上的安全管理要求[22]。

---

[21] *B. C. Soh, T. S. Sillon and P. County, "Quantitative risk assessment of Computer Virus attacks on computer networks",* ***Computer Networks and ISDN System****, Vol.27, pp.1447-1456, 1995.*

[22] 林詠章、黃明祥,「網路系統安全之技術」, **資訊安全通訊**, 第 5 卷第 3 期, 1996

不過，若從資訊戰的總體意涵來看，由於兩岸關係的歷史包袱，許多研究兩岸軍事學者，多認為資訊戰乃是大陸當局對付台灣之最佳戰爭手段之一，因為其容易達成「損失小、效率高、速戰速決」之功效，而且資訊戰包含政治、經濟、心理、軍事等綜合戰略目的。因此，兩岸處於政治、經濟、社會心理、外交、地理及軍事等處境特殊，使得影響國家整體運作安全的資訊及資訊基礎建設存在相當程度的脆弱性，因而構成國家資訊戰的罩門（Achilles' Heel)。僅就下述實例就可看出我國國家安全與資訊基礎建設的脆弱性[23]：

（一)、中共針對性敵意凸顯我國重要資訊結構的脆弱面：

民國 84 年 8 月至 85 年 3 月間，中共對我發動針對性飛彈試射及各類文攻武嚇行動，及民國 89 年中共對我總統大選所發表種種強硬措詞的談話，皆造成的社會間歇性不安、外匯流失與股市波動現象，顯示出我國「政治、經濟及社會心理資訊基礎建設」的脆弱性。

（二)、重大意外事件凸顯經濟資訊結構的脆弱面：

民國 88 年「729 大停電」，造成民生不便、金融交易停滯、國家經濟損失及社會短暫恐慌等現象，禍首只是電塔倒塌造成的「輸配電網路故障」，顯示我國「經濟資訊基礎建設」的脆弱性。

（三)、重大災害凸顯國家危機處理潛力與資訊結構要害：

民國 88 年「921 大地震」，因資訊傳播工具及通信系統能力不足，以致初期救災重點難以正確掌握，形成政府應變及統一指揮的困境；災變期間的斷電、斷水與限電、限水，相當程度的影響交通、工業生產、金融交易與經濟市場。當然，政府領導全民同心共度震災的努力，

年 6 月，頁 12-15。

[23] 曾章瑞，「中共研究信息戰對我國之影響及因應之道」，**中共對信息戰之研發與影響研討會論文集**（台北：台灣綜合研究院戰略與國資研所，2000 年 2 月），頁 4-6。

使政治及社會秩序穩定；惟根據中華經濟研究所分析，當期經濟景氣仍受相當影響。國軍的救災表現贏得國內外的高度肯定，不過，在經歷類似戰場管理的救災過程中，卻也充分檢驗了國軍掌握戰場資訊透明度及整合「指管通情」資訊系統效能的精進空間。這次天災的顯示是：「政治與社會心理資訊基礎建設」是可以教育及經營的，不過，整體上的「經濟及軍事資訊基礎建設」則仍有相當脆弱性。

（四）、國家資訊安全有備無患的必要性：

面對全球共同的 Y2K 資訊危機，我國股市停市、金融歇業、航班減飛、核電管理體系如臨大敵及軍事單位升高戰備，在政府萬全整備及預應措施下，各種政經心軍資訊危機都沒發生，結果發人深省。

上述案例正印證美國資訊戰研究學者 Michael Wilson 在 1996 年就提出 Infrastructure Warfare 的理念，他將信息戰明確的詮釋為包含資訊與基礎結構的「雙資」作戰（Information and Infrastructure Warfare－I2W）。從這種信息戰的本質，我們當可更加體會，無論平、戰時，對於有關國家政治、經濟、社會心理及軍事等資訊及資訊基礎建設，一旦遭受敵人計畫性的破壞或不當處理，即可能發生政府運作機制癱瘓、交通與社會秩序紊亂、產業受挫、金融交易停滯、民生供調失常及軍事指揮管制通信失利等國家安全危機。因此，基於資訊及其系統結構與國家安全休戚與共的關係，我們豈能不掌握中共研究信息戰現況興對我的威脅及影響，並思考對策？

就本文第四章所述，中共當局在波灣戰後質量建軍的重點，包含制導武器的精準攻擊及信息戰力的建置。為了反制外力干預，並期保有台灣經濟成就，完成「祖國統一」，中共可能的犯台模式據判為以「損小、效高、快打、速決」為戰略指導，並實施以信息技術為主的局部戰爭。因此，我們可深切理解中共積極研究信息戰的企圖。根據美國

國防部評估，與中共比較，我國目前仍保有資訊優勢。[24]故中共為確保犯台有利態勢，必以其集權之便，傾國力超越我資訊優勢，以利犯台最佳準備。

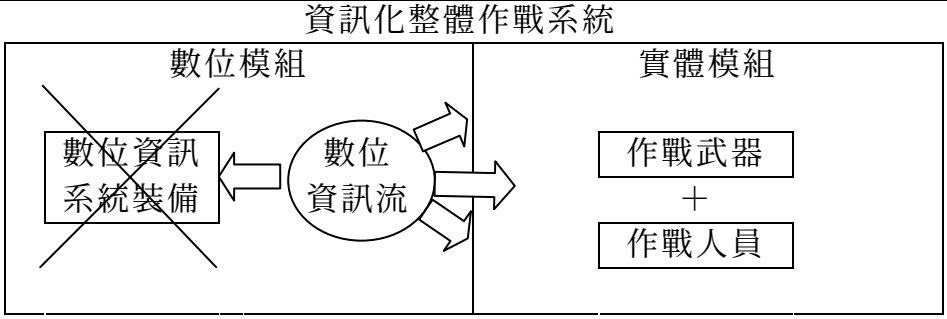
中共當局研究資訊戰（信息戰），以國家戰略從資訊技術、相關基礎建設、戰術戰法以及戰略思維等方面同步著手，並以支持打贏「高技術條件下的局部戰爭」為著眼。台海局部戰爭既為此類典型模式，中共追求資訊優勢自然迫不及待，並可供為其資訊與質量建軍之試驗戰場。

中共當局資訊戰建設，在戰略上，以 863 計畫，採取「有限目標」、「突出重點」的方針，選取包括「信息技術」等領域，發展重點高科技，建立優勢的高技術條件，並為資訊戰科技奠定基礎。戰術上，研究各類點穴戰術戰法，結合三軍情蒐與太空監偵系統的聯線，建立戰區戰場透明化指揮管制能力，除已具備電腦網路攻防技術外，並已構想組建「網軍」新兵種。其他發展概況，如自力研製「電腦病毒」、「邏輯炸彈」及核爆電磁脈衝等武器，及研究「以破壞數位模組癱瘓實體模組」的資訊戰槓桿戰略（示意如圖 5-4）

[24] 詳見大陸新聞中心編譯，「台灣海峽的安全情勢——美國國防部提報國會評估報告」，聯合報，1999 年 2 月 27 日，第 4、13 版。

圖 5-4　中共當局資訊戰思維：槓桿戰術之運用

信息槓桿戰略	1.以破壞「數位模組」使「實體模組」失能。 2.以「四兩」癱瘓「數位模組」，取代以「千斤」摧毀「實體模組」。 3.以「間接、無形、虛擬」奇襲資訊裝備的「數位模組，達成使「實體模組」系統，例如作戰系統以及政府機制、經濟、社會機能等運作癱瘓的效果。



資料來源：轉引自曾章瑞，「中共研究信息戰對我國之影響及因應之道」，中共對信息戰之研發與影響研討會論文集（台北：台灣綜合研究院戰略與國資研所，2000年2月），頁4-6。

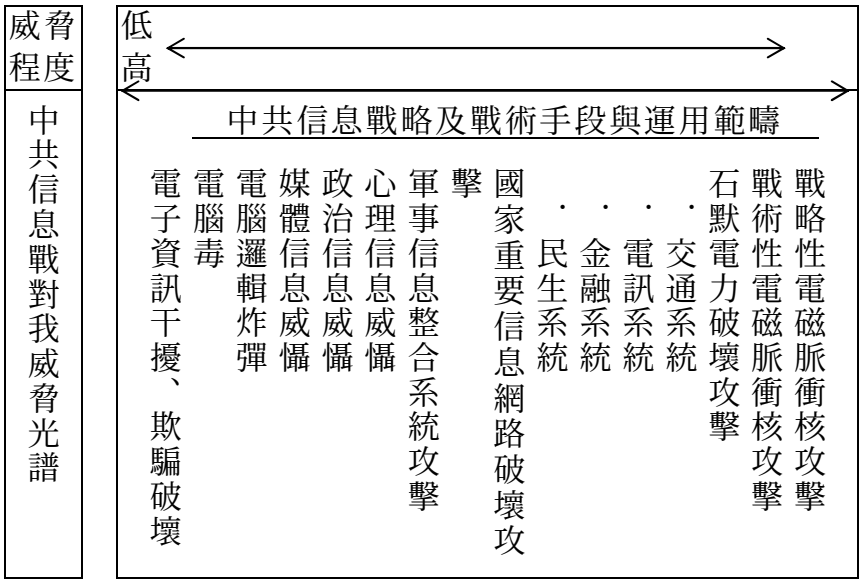
上述中共資訊（信息）戰的發展，包含了「戰略、戰術、戰鬥、戰技」各層次；此外，中共為藉信息戰支持高技術作戰，也不斷研究新軍事思想，以期納入「不對稱作戰」、「不接觸作戰」及「超限戰」等戰爭思維，配合高技術特性實施配套作戰。

《超限戰》基本上是中共依游擊戰思維，藉城市游擊戰、恐佈主義及電腦病毒等「超限」思維，追求超越傳統戰爭模式，打破一切限制與手段、結合非軍事手段，從各層次領域及對象來打敗軍事優勢大國。超限戰法也包含以資訊手段執行的電子、網路及媒體戰等，以資訊點穴戰術結合超限理論的組合運用，預判可以對攻擊對象形成相當程度的威懾。[25]

[25] 喬良、王湘戰，**超限戰——對全球化時代戰爭與戰法的想定**（北京：解放軍文藝出版社，1999年），頁153。

綜合研析，中共多年來研究發展資訊（信息）戰已有相當成果，也已確立以「不對稱作戰」及超限運用的戰略思維，來運用「點穴」的信息戰術戰法，達到破壞、操縱或干擾其他國家運作機制及中樞指揮系統，瓦解其國防安全之目的。針對中共信息戰研發的戰略戰術與可能的超限運用，中共對我的信息戰威脅光譜可分類如圖 5-5。

圖 5-5　影響我國家安全的中共「信息戰」威脅光譜



資料來源：轉引自曾章瑞，「中共研究信息戰對我國之影響及因應之道」，**中共對信息戰之研發與影響研討會論文集**（台北：台灣綜合研究院戰略與國際研究所，2000 年 2 月），頁 4-7。

綜上所述，當前我國在建構電子化／網路化政府的同時，其實應該及早因應資訊戰對我建立資訊安全系統所可能帶來之衝擊與影響。早期由於資訊系統不見殺傷力的軟性特質以及技術不普及，過去鮮少重視資訊系統之安全，以致於資訊本身事務系統要素都存在相當脆弱性，因此，當我國在邁向資訊化社會，而國家政府運作機制、經濟發展、社會民主及軍事運作等，逐漸升高對資訊系統的倚賴程度後，資訊系統的脆弱性，亦就如影隨形的轉嫁到資訊化的國家社會機制之中。職是之故，當資訊科技的迅猛發展並為國家帶來資訊化社會與資

訊化武力時，也相對帶來資訊戰爭型態，而使國家整體安全的脆弱性同步提高，此種脆弱性每下愈況的主因，導源於我國整體運作機制對資訊化倚賴的成長速度，遠超出於人們對不斷增高的脆弱性所能理解的速度。

準此，本節最後擬對我國重要運作體系在資訊安全現況進行觀察，謹提出供國人思考我國對承受高科技資訊戰（尤其是大陸當局信息戰）的脆弱性。

（一）、國防部門：

經過多年推廣軍事革命與推動資訊教育的努力，加上軍事安全的實際需要，我國防體系對資訊戰的研究，已由理念進展到實務推動。無論是整體規劃、網路建設、通資安全規範，專屬資網防護、攻防技術研發、資訊教育普及、軍民專業整合等，都已積極推動。加上軍事單位的特別衛護，國防部門在通資整體安全機制，目前確是國內最具完整認知，最重視、也最具資訊戰能力的政府單位。

（二）、一般政府部門：

一般政府部門的資訊安全通常位及於單位機房門禁、重要資訊攫取的安全管制及網路防火牆等；至於跨部門系統架構、系統與資料庫及聯網結構等的安全機制則多欠完善。此外，攸關全國通資安全的事權統一運作與稽核機制、通資安全法規、密鑰認證，國家密碼模組標準與技術管制、國家整體通資安全法令、資訊危機處理機制及公務人員的通資安全教育需求等，都缺乏認知與實際作為。加上缺乏「資訊戰」敵情意識與特別防衛措施，故承受信息戰的脆弱性相對升高。去年，當兩岸情勢較緊張之際，曾經發生的陸委會系統被侵入置放病毒，國民大會系統被入侵受損，執政黨以及政府新聞局駐位單位網頁被不當篡改等都是警訊。

（三）、金融體系：

為維護客戶權益及提高市場競爭力，企業體系對資網科技的運用及倚賴度都很高，其安全機制也非常嚴密。為囿於國內技術不足，以及國家通資安全法規與稽核機制的不全，企業體系的資安措施，或能防堵一般資訊犯罪行為，對經濟金融資訊攻擊的破壞恐怖行動，包含破壞信用機制、擾亂金融秩序及製造客戶恐慌等，恐怕都會一籌莫展。就金融體系與社會秩序穩定間所存在的高敏感度而言，我國金融資訊體系的高脆弱性，不僅存在於廣佈社會各地的接觸口，金融從業人員缺乏資訊戰的警覺與資安素養等，都是國家級金融資訊安全的隱憂。

（四）、重要公民營產業：

公民營產業是我國經濟的命脈，而經濟則是國家安全的主要戰略重心（Center of Gravity）。我國經濟屬海島外貿型，公民營產業包含通信、電力、航空、交通、電子、資訊、金融衍生品等，所賴以生存及發展的理作機制，幾乎部是資訊與資訊基礎建設。從 729 停電及 921 地震對國內經濟的衝擊，就可充份證明國家經濟資訊的高度脆弱性。此項脆弱特性既屬國家戰略重心，產業界又難完全自行解決，由政府建立相關通資安全機制及危機管理措施，的確是迫不及待。

（五）、資訊傳播媒體網路體系：

社會民心是我國家安全第二個戰略重心。逐步國際化與開放的的台灣社會，各類媒體發展迅速，傳媒管道多重，上網人口也已逼近 500 萬，故敵人以資訊傳媒進行心理資訊戰可謂易如反掌。以去年七月九日「特殊的國與國關係」論迄去年十二月止，中共循各種媒體管道對台文攻武嚇的訊息計三十一次，我國防部及時採取澄清導正的作為也高達十九次。目前，國內無線與有線傳媒林立，資訊網路普及，在寬頻網路快速發展，國際媒體聯網趨勢與個人網站及電子郵媒盛行之際，敵人發動資訊傳播戰，影響社會心理安定的行動將更趨多元。因此，相對上，媒體傳播、接受及通路等資訊安全的脆弱性將可預期。如何有效防制、反制或是快速有效澄清不當資訊傳媒的整合機制，應

是國家資訊安全要務。

（六）、海島地理環境的資訊脆弱特性：

基於海島地理環境、外貿型經濟發展、外交情蒐困境及主要軍事裝備外購等特色，我國對外通聯與資訊傳遞的暢通是國家安全的關鍵。敵人若對我採取資訊封鎖戰略，將可收一石多鳥——同時達到政經心軍多重信息戰效益。此種海島型地理加上高資訊倚賴的混合特性，使對外通信與資訊傳遞的海底電統、衛星及無線通信等成為我國資訊戰的罩門。根據報載，近來金馬地區海底纜線多次遭到不明原因之破壞，該是重要警訊。

上述我國特殊國情加上資訊化社會環境與政府機制現況，在面對中共資訊（信息）戰威脅之際，的確凸顯出許多脆弱性，國人宜慎思因應對策並展開行動，以維護國家安全。

第六章　結論與建議

第一節　研究發現

人類的戰爭行為與社會型態的轉變有著密不可分的關係，從傳統農業社會，進步到工業社會，再到目前的資訊社會，各國莫不以創新的手法，來改變傳統戰爭的進行方式。資訊戰的低進入成本、傳統迅界的模糊化、本土易遭受攻擊等特性，已使資訊科技對戰爭型態帶來革命性的影響，卻也對相當倚賴資訊的先進國家造成極大的壓力。我國自從推動「國家資訊通信基礎建設」（ＮＩＩ）以來，資訊科技的迅猛發展，已使我國名列世界「資訊大國」之一。然而伴隨我國對資訊的依賴日益增加，相對地，遭受資訊攻擊比例也隨之增加。相信「七二九大停電」與「九二一大地震」對台灣社會所造成的影響，大家應還記憶猶新；未來我們是否有能力因應資訊時代戰爭型態的變化，從而在我國建構電子化／網路化工程的同時，也能有一套完整的資訊安全體系，以因應資訊戰的衝擊，成為我國在邁向資訊社會的一個重要立基點。

基本上，中共對於資訊（信息）戰的研究，是以波斯灣戰爭為標誌，認為一種新戰爭型態－資訊戰正在形成和發展。由於資訊具有全球到達、非線性效應、光速傳輸、多方共享、用之不竭等特性，能操縱和控制戰爭中的物質和能量，從而大大提高作戰效能，並減少其他戰鬥要素的投入。因此，對於中共而言，資訊既是力量倍增器，又是重要的戰略資源。透過波斯灣戰爭的歷史經驗，中共清楚地看到，在未來戰爭中，資訊攻擊將左右戰爭的型態和前途，善於控制與利用資訊者往往與勝利同在。中共在研究資訊（信息）戰進程上，雖然起步比台灣早，且在戰術戰法上已有相當成果，但在資訊科技上的基礎實力與技術仍處於初級研發階段，主要原因之一是中國大陸的資訊產業係以代工生產為主，實無研發能量可言；相反地，在我國國內民間長

期累積的資訊科技能量（尤其是電腦病毒攻防技術）則是相當可觀的。連美國國防部在其最近的「台海安全情勢報告」中都特別指出國內在這一方面居全球領先地位。不過，若從發展的層面來說，中共在資訊戰的發展上，是以國家層級來推動，並且還包括「戰略、戰術、戰鬥與戰技」等不同層次，不但顯現其結合戰略研究與科技研發的努力與決心，更充分表明了中共在未來以資訊科技主導的戰爭中採用非傳統與「不對稱作戰」方式之企圖；反觀，我國雖大力推動資訊發展，但相對地卻對資訊相關設備之依賴日益加深，而我國又因社會變遷，人民危機意識淡薄，使得現階段我國資訊戰的發展僅止於軍事層面，而關係民生甚鉅之各種金融、電信、電力與交通運輸及當前政府所推動的電子化網路化政府等資訊系統已成為中共之最佳攻擊目標而不自覺，儼然成為國家安全之嚴重隱憂。

中國大陸網際網路的發展，在近幾年發展相當迅速，早期，曾因網際網路是個全方位開放的「無國界、無主管、無警察」世界，既不能設紅綠燈，也不能設路障，促使外界相信這是「和平演變」中共的重要管道。不過隨著中共近年來透過法令、國安部、公安部及保密局的介入，「限制連接」已成為大陸上網人士的夢魘，再度阻斷大陸上網人士汲取國外資訊的機會。[1]中共為了進一步遏止西方國家、國際組織和海外民運人士不斷利用網際網路向大陸傳播各種資訊，委託深圳大學為此特別研發一套「國際惡意郵件過濾系統」，進行截取攻擊中共制度和國家領導人的電子郵件。據了解初期使用在短短不到二個月時間，就截獲近千餘封惡意政擊中共制度與國家領導人的電子郵件。[2]不過此系統是否真如預期可以完全過濾、清除國外「惡意中傷的資訊」，相信答案是否定的。前一陣子，兩岸因為「兩國論」所引爆網路大戰，即是一明顯例子，任憑大陸或是台灣網站如何努力的進行過濾，仍敵不過有心駭客（hacker）的入侵，台灣與大陸的駭客更因其信仰意識

[1] 詳見「大陸網際網路限制多」，**中國時報**，民國 87 年 6 月 7 日，第 14 版。
[2] 詳見「深圳大學研發國際惡意郵件過濾系統」，**聯合報**，民國 87 年 6 月 7 日，第 13 版。

形態差異，不僅修改對方網站首頁，更大膽互相批判對方的主張。[3]

總體而言，中共研發資訊（信息）戰起步較我國早，且其為共產專制國家，可傾全國之力推動資訊戰發展，在現階段其無論是科技、預算、人力投入、政策指導與執行等方面，均較我國突出。不過，由於資訊戰涵蓋層面寬廣，且資訊科技發展一日千里，因此，我們也不能僅以目前之發展與成就來論成敗，更何況我國資訊產業體質健全，在研發與生產方面仍具有相當潛力，且美國國防部的「台海安全情勢報告」中，美方仍認定我國在基本因應能力上仍可占有優勢。是故，如何以實際行動全面推動資訊戰發展是我國在邁向資訊社會之首要工作。

第二節　研究建議

當前，由於兩岸關係仍處於高度不確定的時期，而未來五年更是兩岸資訊戰力競爭之關鍵時刻。根據資料顯示，中共已成立所謂「第四軍種」之網路部隊專責資訊戰攻防作為，亦已籌設「信息戰模擬中心」利用高科技模擬技術與設備，營造資訊戰及模擬戰場環境，用以進行對抗演練。[4]而在技術研發上，中共亦計劃未來開發以癱瘓指管系統為目標之料鍊，網路連線傳輸型「病毒」程式集對應之傳輸裝置，或研製無核輻射污染的戰術性電磁脈衝武器，以增進其從事資訊作戰之潛力。準此，本文最後擬就總體國家安全層次，提出立即可行性建議與長期建議以作為本研究的政策因應建議：

一、立即可行性建議

---

[3] 詳見**中國時報**，民國 87 年 6 月 9 日，第 14 版。

[4] 根據,**<<中共解放軍報>>和<<中國國防報的報導>>**, 中共於九八年已成立網路部隊, 並編有程序班、操作班、保障班和培訓中心等。所訓練出來的「網路民兵」, 基本上都已通過計算機等級考試, 百分之六十獲得技術職稱。在資訊安全防護和網路攻防戰術方面, 取得了一些初步成果。詳見 http://news.kimo.com.tw/2000/04/26/international/ctnews/30/630.htm/.

1. 訂定專法規範網路行為（主辦機關：法務部；協辦機關：行政院研考會、交通部、行政院新聞局）：隨著網路快速發展，各種利用網路所進行的破壞與犯罪問題也逐漸出現。為解決網路對社會所帶來的衝擊，國內主管機關可以考慮甚至進一步對網路脫序問題就相關法律進行研究、規範或修正。

2. 建構資訊網路安全防護網（主辦機關：行政院研考會、交通部；協辦機關：國防部、法務部）：網際網路目前的發展，可以用美國大西部的拓荒期來形容，當我們使用網路愈頻繁，對網路的依賴愈深，就愈需要在這個西部蠻荒建立一些文明的準繩。目前政府機關的電子化／網路化正處於初級發展階段，系統主機內當無一些重要資料，不過，當系統處理的資料份量增加後，安全機制的防護若未能改善的話，私密資料遭盜竊刪改的潛在危機將不時面臨，且當被盜竊的資料變成機關內部的人事資料、機密檔案或重要報表時，其間所潛藏的危機就不是任何系統管理者可以承擔的，這樣的問題也正是電子化／網路化政府未來的隱憂。對此，建構一全面性的資訊網路安全防護網是必須進行的工作，而這一全面性的資訊網路安全防護網，基本上，應具備以下功能：

(1)、使用者付費：建立使用者付費的基本原則。不必付費的資源，一定會被濫用而導致浪費。如果攻擊者必須為所發出的所有訊息付費，攻擊的規模就不可能太大。如果受害人也必須負擔攻擊者的成本，則要竊取他人的帳號就不會太容易。如果竊用他人帳號的竊賊眾多，則市場必定會出現防制的安全產品。

(2)、分級計價：藉著依服務等級計價收費，便可以兼顧網路的開放型與創意空間特性。為全民或團體提供類似聯邦快遞般的高價值服務，例如，如果你願意出示身分並付出一定的費用，則可以享受某種品質等級的服務；如果你不願出示身分且堅持免費，仍可享受基本的服務，

但不保證垃圾郵件的騷擾，如此，網路最可貴的創意空間仍可保留。

(3)、來函身分顯示：對那些毫無限制的網路訊息，們有必要知道發信者的身份；否則要如何清算帳目與建立活動規範？沒有身份，就無法辨別伺服器上流通的資料封包到底是誰的。和在汽車上懸掛牌照一樣，我們送到網路上的資料封包上面也應該加蓋所有人的印記，這樣才能辨別封包所有人並執行傳遞的規則。付出較高等級費的服務，必須有相對的數位認證，以便取得優先使用網路資源的權利。

(4)、硬體的安全防護：個人電腦非常不安全，因為它設計時，安全根本就不在考慮之列。所幸，一些安全性較佳的網路通路設備已陸續問世。這些「個人通信器」內建防止破壞的身份辨識晶片，又有密碼或生物檢測設施，安全性遠較個人電腦為佳，很適合做為儲存數位鈔票的地方。

有資訊安全防護網之後，仍須對資訊系統安全稽核管理與執行，而這可透過下列各種方式來進行：
(1)加強訓練政府業務單位及主管。
(2)培育專責稽核單位。
(3)各機關擬定標準作業規範。
(4)任務編組，進行設定資訊安全及稽核相關法規之增修。
(5)定期舉辦研討會，教育訓練資訊系安全稽核技術與工具。
(6)宣導 Data Ownership 觀念，建立 Data Owner 權益受損通報管道。
(7)確實執行稽核，執行從嚴。

3. 制訂法令獎勵研發資訊安全科技（主辦機關：行政院國科會；協辦機關：行政院研考會、交通部、行政院新聞局）：藉引進國外技術、整合軍民專才，並結合市場機制獎勵研究密碼技術及相關資訊網路攻防科技。

4. 結合產官學研與推展委外政策（主辦機關：行政院研考會；協辦機關：交通部、行政院國科會、行政院新聞局、國防部、法務部）：資訊科技屬軍民通用科技，國內民間與學術單位資訊科技潛力雄厚。是故應落實資訊業務委外服務，有效整合民間業者，公民營研究機構、政府機關等單位，透過諮詢顧問、委外合作方式，加強資訊戰綜合性理論研究，以落實資訊安全建設，以擴大政府資訊產能。

5. 確立政府部門及民間產業的角色扮演及法規制訂（主辦機關：行政院研考會；協辦機關：交通部、行政院國科會、行政院新聞局、國防部、法務部）：為維護國家的資訊安全，資訊戰因應措施必涉及政府部會、立法部門及公民營產業。在民主社會中不同立場之角色扮演，包含政府公權力尺度、立法寬嚴、產業運作機制及人民自由權益約束度等都需審慎考量。其折衷原則須能至少包含「最起碼不可或缺的資訊基礎架構」，亦即是說，平時能防範對國家社會的不當騷擾及破壞，戰時則能確保起碼的政府、產業及民生運作機制，以及軍事任務之必要需求。此項角色扮演及法令規章的制訂，需要許多專業論辯方能完成，故宜儘早實施。

6. 逐步推廣資訊戰教育與基礎訓練及研究，成立研究所、訓練中心等專責機構（主辦機關：行政院國科會；協辦機關：交通部、國防部、教育部、行政院研考會、法務部）：除了積極汲取先進國家資訊科技，發展我國資訊戰武器裝備之外，還應迅速結合民間、政府、研究機構共同成立資訊戰研究中心或研究所，共同發展資訊安全的能量，並積極推動資訊戰法、武器之研究模擬。最後應將結合的研究成果擴大應用於電子畫/網路化政府的工作項目上。

7. 成立各級政府資訊安全專責單位（主辦機關：行政院研考會；協辦機關：內政部、外交部、交通部、國防部、法務部、經濟部、財政部）：隨著所謂電子化政府的到來，政府資訊安全的問題也應該隨之得

到重視，因此，建議各級政府能增設資訊安全相關部門，針對一般網路駭客(hacker)甚至來自於中共的資訊破壞，有一防堵的作用。

8．建立可信賴度電腦產品驗證組織與標準（主辦機關：內政部；協辦機關：外交部、交通部、國防部、法務部、經濟部、財政部、行政院研考會）：可由交通部研議，與民間相關科技企業合作，以企業現有的技術及人力，配合並執行政府所訂定出來的電腦產品驗證標準。此一方面可以節省國家資源，另一方面，則可在短時間之內建立可行機制。

9.健全模擬演練機制（主辦機關：內政部；協辦機關：外交部、交通部、國防部、法務部、經濟部、財政部、行政院研考會）：由行政院統合成立跨部會資訊小組，在假設遭遇不明網路資訊破壞時的情況下，研擬一套演練機制，能在最短時間內圍堵破壞根源，並進一步予以反制。

二、中長期建議

1．推動國家層級資訊戰指揮機制（主辦機關：國安會；協辦機關：內政部、外交部、交通部、國防部、法務部、經濟部、財政部、行政院研考會、行政院國科會）：資訊戰涵蓋範圍廣泛，舉凡政治、心理、經濟、科技和軍事各領域，均為中共運用資訊技術手段爭奪資訊優勢的目標。職是之故，建立國家層層級資訊戰指揮機制，宜由總統府與行政院共同主導，結合國家安全局與內政、外交、國防、經濟、財政、教育、法務、交通等部會，針對電力、電信、金融、交通等國家基礎建設之安全防護，共同研擬相關因應作為。

2．建立國家多層、多頻、多型的模式資訊網絡架構（主辦機關：行政院研考會、國防部；協辦機關：各機關）：藉建置多層、多頻與多型複式網絡體系，提升資訊網路的存活度，以降低中共或網路駭客

的攻擊效益。尤其更應建構一套「資訊戰模組」（Information Warfare Model）即所有政府單位與軍事的指、管、通、資、情系統，均應仔細推敲在資訊戰下是否能正常的發揮功能，並推演替代功能設備與替代方案。此外，建立資訊戰鬥部隊編裝，並修訂軍職專長也是迫切應進行之工作。

3. 製訂國家資訊安全管理、預警及危機處理機制。（主辦機關：行政院研考會；協辦機關：國防部、交通部、行政院新聞局、行政院國科會）：推動資訊安全管理，預警及危機處理機制是大家的共識，而這是一個需要長期投入的工作。建議可從專業證照的角度切入，進而加強資訊安全人才的培訓並建立一個專職機構，這個專職機構可稱為資訊安全防範小組，專司下列五項工作：

(1)組織內資訊安全政策的核定、監督與管理。
(2)各單位之資訊資產的保護與預警制度。
(3)各單位所應擔負資訊安全責任之分配，以及各單位的協調，致力將資訊安全觀念融入政府文化中。
(4)資訊系統遭破壞或入侵後危機處理機制之建立。
(5)以「軍民一體」理念，制訂「國家資訊安全管理及危機處理運用」相關法令，有效運用珍貴資訊資產。

4. 以全民國防理念推動全民資訊戰教育（主辦機關：國防部；協辦機關：教育部、行政院新聞局、行政院研考會、法務部）：非軍事資訊戰防不勝防，其反制之道，在於政府、產業、媒體、官員與民眾等，都要具備資訊戰相關知識，並能了解中共資訊戰的手段與影響，俾能降低中共資訊戰奇襲效應，並於必要時配合政府發揮反制效果。

5. 鼓吹國際訂定反資訊恐怖行動公約，以遏止中共資訊戰威脅。（主辦機關：外交部；協辦機關：行政院新聞局、國防部、教育部）：藉國際輿論與專家學者聯合造勢，將資訊戰非軍事運用視為國際恐怖

主義行為，期以國際公約遏阻中共資訊戰對我國之奇襲行動。

6. 藉與先進國家資訊互動及技術交流提升我國資訊安全的實力（主辦機關：教育部；協辦機關：國防部、交通部、外交部、行政院國科會、行政院研考會）：例如我國可運用「台灣關係法」，使美國將資訊安全與危機處理納入其對我國安全維護的承諾範圍，或者定期指派學有專精的學者專家赴國外進修、參訪、座談進行技術交流。以利我國資訊安全技術獲得建立我國資訊研發優勢。

7. 全方位評估中共資訊戰對我國政、軍、經、社會之影響。（主辦機關：國安會；協辦機關：國家安全局、法務部、國防部、外交部）：編制預算並責由專業小組研究包含政治、經濟、社會心理、外交及軍事等層面，全方位評估中共各種資訊戰威脅與影響。此項研究涉及層面廣泛，推動時機愈早愈好。

附錄一

中共發展「信息戰」對我國建立資訊安全制度影響之研究

學者專家座談會紀錄

一、開會時間：八十九年八月十日（星期四）上午九時三十分
二、開會地點：行政院研考會七樓簡報室
三、主席：紀副主任委員國鐘
四、出（列）席人員：　　紀錄人：顧偉川
(一)學者專家（依姓氏筆劃順序排列）：
王教授孟平（警察大學）
林總經理真真（財金資訊公司）；陳協理則黎、張淑貞小姐代
林執行長逢慶（資策會）；鄭資深顧問祥勝代
林局長勤經（國防部通資局）；柴組長惠珍代
徐主任恩普（行政院 NII 小組）
許副總經理奎壁（中華電信公司）；郭處長國燦代
陳主任立祥（教育部電算中心）
陳教授年興（中山大學資管系）；請假
陳總經理振楠（關貿網路公司）
陳處長熙揚（立法院資訊處）
曾董事長憲雄（台灣網路資訊中心）
萬主任鎮歐（行政院主計處電子中心）；請假
謝教授清俊（中研院資訊科學研究所）
鍾教授堅（清華大學原子科學系）；請假
簡局長仁德（交通部電信總局）；蘇總工程師宗弘代

(二)研究小組成員

李教授英明（政治大學東亞所）

黃研究助理健群

(三)本會列席人員

盧處長鄂生

孫科長百佑

闕助理設計師秀英

五、主席致詞：略

六、研究小組報告：略

七、發言要點（依發言順序）：

（一）謝教授清俊：

1、 本研究主題可能涉及國家機密，資料獲取不易，因此建議將資料範圍說明清楚。

2、 廣義的「資訊戰」可細分為文化戰、經濟戰及武裝戰，建議界定本研究的範圍或由不同層面探討不同作法。另「模擬戰」、「虛擬戰」、「資訊戰」之深層意涵亦各不相同，建議有所區隔。

3、 戰爭有進攻、有防衛，建議在危機處理方面亦可從兩個層面探討。

4、 安全可以分為技術面及管理面，往往管理面又較技術面來的重要，因此建請就管理面的建議作法多所著墨。

（二）柴組長惠珍：

1、 「資訊戰」可視為陳總統「境外決戰」意涵之部分體現，國防部對此亦積極研究辦理中。

2、 從「資訊戰」的觀點來看，國家之領土及主權可能有重新探討的必要。

3、 本研究係從中共「資訊戰」之觀點切入，因此對有意、無意的駭客或病毒入侵較少探討，而前述方式亦可能成為中共侵犯之手段，宜多加以探討。

4、 報告中提到與國際規範不同之作法，此舉是否妥適，請再酌。

5、 行政院資推小組第三十九次委員會達成建立「網路安全組」之決議，由國防部會同行政院研考會共同召集，此項資料建議納入，以宣示政、府加強資訊安全防護之具體作法。

6、 第 119 頁,「藉與先進國家資訊互動及技術交流提升我國資訊安全的實力」之建議，因涉及學術及技術部分，似不宜由國防部主辦，以發揮更大效益。

7、 研究結論部分，建請考量增加「成立各級政、府機關資訊安全專責單位」、「建立可信賴度電腦產品驗證組織與標準」及「健全模擬演練機制」等項。

（三）徐主任恩普：

1、 我國網際網路的發展及應用基本上是超越中共的，因此在談論「資訊戰」的同時，宜對我國之優勢亦有所描述及說明。

2、 「資訊戰」可說是全面性戰爭，因此在觀念上有必要作全面性的推動。但與「國家安全」結合時，其軍方與行政機關及民間之分野宜有所說明，或就某些重要資訊系統之安全管理提出建議，並建請留意本研究之建議宜考量網際網路基本精神及其多元化之特性。

3、 網際網路是全球性的應用，而在 G8 會議時亦達成協助資訊發展落後國家平衡落差之共識，因此在討論中共試圖運用網際網路發動「資訊戰」之同時，其對全球之影響亦可探討，或可考量我國如何運用國際力量以收保護之效。

（四）陳主任立祥：

1、 第 114 至 115 頁，建請刪除在網際網路實務運作方面不

易達到之建議。

2、 本報告似較偏重實體網際網路方面的探討，建議就網際網路系統面及應用面亦能有所著墨。

（五）陳總經理振楠：

1、 戰爭有分戰略、戰術、戰技等方面,「資訊戰」自不例外，建議於報告中說明本研究之範圍或分別說明。

2、 第 14 至 17 頁，係描述「戰略資訊戰」，可否以此與中共「資訊戰」進行差異分析。

3、 建請討論「資訊戰」與安全稽核之關聯性，以及於主動性或被動性之防禦或攻擊時，不同之作法。

4、 第 91 頁，論及英國 BS7799 資訊安全管理規範。就我國而言，應由那一機關主導規劃、建立及推動，似可建議；並能否依 BS7799 建構一套完整案例及風險管理之作法以供各界參考。

（六）曾董事長憲雄：

1、 依網際網路的特性而言，政府的管理宜降到最低。本研究立論很好，但在實務建議上請再作考量。

2、 資訊空間、資訊主權的概念很好，但建議就其如何界定，以及政府、民間應如何分別掌控有所說明。

3、 「資訊戰」的範圍相當龐雜，建議由電子商務(E-Commerec)切入，再行延伸。

4、 我國各種網站的安全管理如能落實，將可作為「資訊戰」防護的後盾，因此建請增列建立站主(Web Master)或主機管理者(Host Master)證照制度或標準作業程序、建立被信任節點(Trusted-Node)制度、以及建立機關資訊訊安全專責單位或人員之建議。

（七）陳處長熙揚：

1、 研究資料如能進一步蒐集較為機密之資料則更佳。
2、 建請增列我國「資訊戰」主導單位及發展優先順序之建議，並就我國密碼工作應發展之方向有所著墨。
3、 報告中各章節內容重複之處請整理，而名詞統一、加入英文關鍵字及錯漏字部分，亦請增列或修正。

（八）陳協理則黎：
1、 中共之作戰及管理思維與我國不同，我們在討論「中共資訊戰」之同時：且有不同之思考方式。
2、 本報告應具國家級資訊安全之引言性質，國防部似可據此繼續深入研究。而報告中宜建議以國家安全為考量主體之資訊安全主導機關。
3、 本研究之範圍請再界定清楚。

（九）鄭資深顧問祥勝：
1、 「資訊戰」的背後有龐大的技術資源，本研究似宜有所留意，如增列中共發表於技術性刊物之資料、兩岸資訊資產之比較、及中共對「資訊戰」之防禦等。
2、 第 62 至 63 頁，部分資訊宜再加檢視。
3、 建請增列我國為因應「資訊戰」所需人力及物力之預估。
4、 各級政府機關資訊人力本已缺乏, 且由於對資訊作業「整體委外」未能通盤瞭解，以至於實務上是否能斟酌人力專責資訊安全，亟待考量；因此於建議事項中，宜增列由相關機關對資訊安全人力問題謀求解決之建議。

（十）蘇總工程司宗弘：
1、 以本研究名稱而言，其建議事項似宜集中於如何建立或增強我國資訊安全稽核制度上。
2、 本報告之閱讀者未必是專業人員，因此建請用語儘量通俗化。

3、 建議事項宜考慮實務運作之可行性。

（十一）郭處長國燦：

1、 第 113 頁，有關訂定專法規範網路行為之建議很好，但需要行政、立法機構之積極配合。

2、 我國民間資訊實力確實受到國際肯定，然於必要時，政府要如何整合民間力量共同參與宜可再加討論。

（十二）王教授孟平：

1、 本研究傳統與現代研究方法與技術兼容並蓄，且具新視野、新觀念、新展望之新時代創見。

2、 研究結論建請增列：

(1) 鼓吹國際訂定反資訊恐怖行動公約以喝阻中共「資訊戰」的威脅；

(2) 制定國家資訊安全管理預警及危機處理機制；

(3) 制定法令獎勵產業界研發資訊安全科技。

（十三）本會意見：

1、 本案研究方式僅為文獻研析及分析歸納，實務面著墨較少，宜就研究發現，訪談具實務經驗之各界人士，以印證文獻分析之結果並補充不足之處。

2、 建議事項內容宜再歸納，另「信息戰」之攻防與民間電子商務活動關聯密切，應如何喚起各界注意或推動分工，宜可建言。

3、 網際網路係為自由開放環境，為加強網路安全防護，如何結合民間力量，宜進一步討論。

4、 報告章節結構請考慮均衡性，酌予調整。

5、 修正本封面編號為「086-014」，並刪除研究人員資料。

6、 修正本書脊以「本會全名」、「研究全名」、「計畫編號(僅有號碼)」之方式排列。

7、 目次中之「圖表目次」請分列，並以黑體字打印。

8、 本報告中相關作圖請整理美化。

八、研究小組說明：

(一) 謝謝各位學者專家的寶貴意見，研究小組會再調整報告，希望可以呈現更好的研究成果。

(二) 在章節上會再調整。

(三) 本研究係以審慎自由的態度來進行，並試圖提出鞏固我國資訊空間之作法，其意圖係屬維護而無意保守。

九、主席結論：各位學者專家所提意見請研究小組作為修正報告的參考。

十、散會(中午十一時五十分)

附錄二

學者專家座談會意見答覆說明

發言人	意見與相關建議	答覆說明
謝教授清俊	1. 本研究主題可能涉及國家機秘密，資料獲取不易，因此建議將資料範圍說明清楚。	因本研究主題是針對中共發展「信息戰」對我國資訊安全制度的影響，故研究資訊主要是以近期中國大陸出版之一般相關期刊、雜誌、書籍，涉及機密之研究資料，因取得不易或基於安全理由，並未在此報告中。
	2. 廣義的「資訊戰」可細分為文化戰、經濟戰及武裝戰，建議界定本研究的範圍或由不同層面探討不同作法。另「模擬戰」、「虛擬戰」、「資訊戰」之深層意涵各不相 同，建議有所區隔。	已修改於報告書第 2 頁。
	3. 戰爭有進攻、有防衛，建議在危機處理方面亦可從兩個層面探討。	此建議可作為後續研究主題，唯本研究主在針對我國防制、反制資訊戰危機的處理及因應，故較不探討主動進擊部分。
	4. 安全可以分為技術面及管理面，往往管理面又較技術面來的重要，因此建請就管理面的建議作法多所著墨。	已增列報告書第 101 頁，立即可行內容第 7、8、9 三點。

柴組長惠珍	1. 本研究係從中共「資訊戰」之觀點切入，因此對有意、無意的駭客或病毒入侵較少探討，而前述方式亦可能成為中共侵犯之手段，宜多加探討。	已增補內容於報告書中第 89-90 頁。
	2. 報告中提到與國際規範不同之作法, 此舉是否妥適，請再酌。	資訊安全管理與資訊自由化界限爭議甚大, 國際間亦有爭論, 研究小組建議採較積極的作法, 讓資訊安全問題成為國際性議題。
	3. 行政院資推小組第三十九次委員會達成建立「網路安全組」之決議，由國防部會同行政院研考會共同召集，此項資料建議納入，以宣示政府加強資訊安全防護之具體作法。	已補充於報告書第 98 頁。
	4. 第 103 頁,「藉與先進國家資訊互動及技術交流提升我國資訊安全的實力」之建議，因涉及學術及技術部分，似不宜由國防部主辦，以發揮更大效益。	經討論之後, 研究小組採納此建議, 將此結論建議主辦單位以教育部為主, 以期發揮更大效益。
	5. 研究結論部分，建請考量增加「成立各級政府資訊安全專責單位」、「建立可信賴度電腦產品驗證組織與標準」及「健全模擬演練機制」等項。	已補充於報告書第 101 頁。

徐主任恩普	1. 我國網際網路的發展及應用基本上是超越中共的，因此在談論「資訊戰」的同時，宜對我國之優勢亦有所描述及說明。	已於報告書第六章結論與建議，增設研究發現與建議。並做補強說明。
	2. 「資訊戰」可說是全面性戰爭，因此在觀念上有必要作全面性的推動。但與「國家安全」結合時，其軍方與行政機關及民間之分野宜有所說明，或就某些重要資訊系統之安全管理提出建議，並建請留意本研究之建議宜考量網際網路基本精神及其多元化之特性。	已做修改與潤飾。
	3. 網際網路是全球性的應用，而在 G8 會議時亦達成協助資訊發展落後國家平衡落差之共識，因此，在討論中共試圖運用網際網路發動「資訊戰」之同時，其對全球之影響亦可探討，或可考量我國如何運用國際力量以收保護之效。	已修改於報告書第六章第二節研究建議中第一一九頁。
陳主任立祥	1. 第 114 頁至 115 頁，建請刪除在網際網路實務運作方面不易達成之建議。	已修正於報告書第一一四、一一五頁。
	2. 本報告似較偏重實體網路方面的探討，建議就網際網路系統面及應用面亦能有所著墨。	此建議甚好，惟研究小組認為較不符合本研究主題，應作於後續研究。

陳總經理振楠	1. 戰爭有分戰略、戰術、戰技等方面，「資訊戰」自不例外，建議於報告中說明本研究之範圍或分別說明。	已增加說明於報告書中第二頁。
	2. 第 14 至 17 頁，係描述「戰略資訊戰」，可否以此與中共「資訊戰」進行差異分析。	已作修正補充於報告書中第三十一至三十七頁。
	3. 建請討論「資訊戰」與安全稽核之關聯性，以及於主動性或被動性之防禦或攻擊時，不同之作法。	已作修正補充於報告書中第四十五至五十三頁。
	4. 第 91 頁，論及英國 BS7799 資訊安全管理規範。就我國而言，應由那一機關主導規劃、建立及推動，似可建議；並能否依 BS7799 建構一套完整案例及風險管理之作法以供各界參考。	已作增補說明於修正報告書中第九十一頁。
曾董事長憲雄	1. 依網際網路的特性而言，政府的管理宜降到最低。本研究立論很好，但在實務建議上請 再作考量。	本研究建議方面是希望提供政府部門一個政策參考的方向，尤在進入資訊化、全球化的新世紀，政府部門應更具前瞻性。
	2. 資訊空間、資訊主權的概念很好，但建議就其如何界定，以及政府、民間應如何分別掌控有所說明。	已修正於報告書中第六章。
	3.「資訊戰」的範圍相當龐雜，建議由電子商務 (E-Commerce)切入，再行延伸。	此建議非常的好，研究小組可作為後續研究。
	4. 我國各種網站的安全管理如能落實，將可作為「資訊戰」防護的後盾，因此建請增列建立站主(Web Master)或主機管理者(Host Master)證照制度或標準作業程序、建立被信任節點(Trusted-Node)制度、以及建立機關資訊訊安全專責單位或人員之建議。	此建議極有價值。惟研究小組認為網路管制不論在技術上亦或法令上，目前都有實行上的困難，甚至西方先進國家在面對網路侵害事件時，也常有無法可管或刑責不一的問題。

陳處長熙揚	1. 研究資料如能進一步蒐集較為機密之資料則更佳。 2. 建請增列我國「資訊戰」主導單位及發展優先順序之建議，並就我國密碼工作應發展之方向有所著墨。	此建議立意甚好，但研究小組限於物力人力，此應作為後續研究為佳。
	3. 報告中各章節內容重複之處請整理，而名詞統一、加入英文關鍵字及錯漏字部分，亦請增列或修正。	已作修正於報告書中。
陳協理則黎	1. 中共之作戰及管理思維與我國不同，我們再討論「中共資訊戰」之同時，宜有不同之思考方式。 2. 本報告應具國家級資訊安全之引言性質，國防部似可據此繼續深入研究。而報告中宜建議以國家安全為考量主體之資訊安全主導機關。	此建議非常的好，研究小組可作為後續研究。
	3. 本研究範圍請再界定清楚。	已作說明於第四頁。

鄭資深顧問祥勝	1.「資訊戰」的背後有龐大的技術資源，本研究似宜有所留意, 如增列中共發表於技術性刊物之資料、兩岸資訊資產之比較、及中共對「資訊戰」之防禦。 2. 第 62 至 63 頁，部分資訊宜再加檢視。	已修正於報告書中第六十二、六十三頁。
	3. 建請增列我國為因應「資訊戰」所需人力及物力之預估。	研究小組認為此有其必要，此項建議可在後續研究中繼續研究。
	4. 各級政府機關資訊人力本已缺乏, 且由於對資訊作業「整體委外」未能通盤瞭解，以至於實務上是否能斟酌人力專責資訊安全，亟待考量；因此於建議事項中，宜增列由相關機關對資訊安全人力問題謀求解決之建議。	已修正於第六章中立即可行建議第四點。
蘇總工程司宗弘	1. 以本研究名稱而言, 其建議事項似宜集中於如何建立或增強我國資訊安全稽核制度上。	本研究名稱已作修正，著重在我國因應中共發展「信息戰」建立資訊安全制度。
	2. 讀者未必是專業人員, 因此建請用語儘量通俗化。 3. 建議事項宜考慮實務運作之可行性。	因本研究較具專業性，故難免有專業用語，但在字句上已儘量作修正。

郭處長國燦	1. 第 113 頁，有關訂定專法規範網路行為之建議很好，但需要行政、立法機構之積極配合。 2. 我國民間資訊實力確實受到國際肯定，然於必要時，政府要如何整合民間力量共同參與宜可再加討論。	已增補於第六章結論中長期建議。
王教授孟平	1. 本研究傳統與現代研究方法與技術兼容並蓄，且具新視野、新觀念、新展望之新時代創見。 2. 研究結論建請增列： (1) 鼓吹國際訂定反資訊恐怖行動公約以喝阻中共「資訊戰」的威脅； (2) 制定國家資訊安全管理預警及危機處理機制； (3) 制定法令獎勵產業界研發資訊安全科技。	研究小組認同王教授的建議，已增補內容於修正報告書中一百二十頁。
行政院研考會研展處意見	1. 本案之研究方式僅為文獻研析及分析歸納，實務面著墨較少，宜就研究發現，訪談具實務經驗之各界人士，以印證文獻分析之結果並補充不足之處。	本研究限於研究時程，故只能以文獻研究作分析歸納，然而研究資料雖較少，但都具有一定代表性，未周延之處盼在後續研究中可以作更多補充。

	3. 建議事項內容宜再歸納，另「信息戰」之攻防與民間電子商務活動關聯密切，應如何喚起各界注意或推動分工，宜可建言。 4. 網際網路係為自由開放環境，為加強網路安全防護，如何結合民間力量，宜進一步討論。	已修正並增補於報告書中第六章。
	5. 報告章節結構請考慮均衡性，酌予調整。	經研究小組討論，同意貴會意見，在章節上已作修正。
	6. 修正本封面編號為「086-001」，並刪除研究人員資料。	已依照貴會意見修正於報告書修正本封面。
	7. 修正本書脊以「本會全名」、「研究全名」、「計畫編號(僅有號碼)」之方式排列。	已依照貴會意見修正。
	8. 目次中之「圖表目次」請分列，並以黑體字打印。 9. 本報告中相關作圖請整理美化。	已依照貴會意見修正。

參 考 書 目

中文部分

中文專書

1. 王小東，信息時代的世界地圖（北京：中國人民大學出版社，1997年）。
2. 王凱，數字化部隊（北京：解放軍出版社，1998 年）。
3. 台灣綜合研究戰略與國際研究所編，中共對信息戰之研發與影響研討會（台北：台灣綜合研究戰略與國際研究所，2000 年 2 月）。
4. 江岷欽、劉坤億著，企業型政府，(台北：智勝文化，1998 年)。
5. 行政院研究發展考核委員會編，行政院及所屬機關資訊安全管理規範（台北：行政院研究發展考核委員會編印，民國 88 年）。
6. 行政院國家資訊發展推動小組編，邁向二十世紀的電子化政府（台北：行政院國家資訊發展推動小組編印，民國 87 年）。
7. 李繼宗主編，現代科學技術概論（上海：復旦大學出版社，1994年）。
8. 沈偉光，新戰爭論，（杭州：浙江大學出版社，1990 年）。
9. 周碧松等著，信息戰爭（北京：解放軍出版社，1998 年）。
10. 林中斌，核霸（台北：學生書局，民國 87 年）。
11. 林以舜譯，Chunck Martin 著，ｅ時代的七大趨勢（台北：美商麥格羅.希爾台灣分公司，2000 年）。
12. 卓正民等譯，M. Strebe 等著，NT 安全實務評論(台北，儒林圖書公司，1999 年)。
13. 郝瑞庭、賴輝亮主編，信息霍亂——世紀末的冷面殺手（北京：世界知識出版社，1999 年）。
14. 國防部史政編譯局主編，資訊作戰譯文彙編（台北：國防部史政編譯局，1997 年）。

15. 國防部史政編譯局主編，資訊作戰譯文彙輯 I（台北：國防部史政編譯局，1996 年）。
16. 國防部史政編譯局編，共軍「信息戰」研究專輯(台北，國防部史政編譯局編印，86 年)。
17. 張鋒，潮頭：全維信息化戰爭（北京：中國青年出版社，1995 年）。
18. 張寶源譯，Bryan Pfaffenberger 原著 ，Microsoft 官方資料－Internet Explorer 4 中文手冊（台北：碁峰資訊，1998 年 2 月）。
19. 喬良、王湘穗著，超限戰——對全球化時代戰爭與戰法的想定（北京：解放軍文藝出版社，1999 年）。
20. 熊光樹、鄔焜著，信息與社會發展（四川：西南財經大學出版社，1998 年）。
21. 趙學信譯，Kevm Kelly 著，NET & TEN（台北：大塊文化，1997 年 7 月）。
22. 鍾義信著，信息的科學（北京：光明出版社，1998 年）。
23. 鞠慶麒，世紀工程：信息高速公路（北京：經濟科學出版社，1996 年）。
24. 魏特罕（Margaret Wertheim）著，空間地圖：從但丁的空間到網路的空間（台北：台灣商務印書館，1999 年）。

中文期刊

1. 朱瑞秋，「談 NT 的稽核功能與資訊安全」，旗標資訊月刊，1998 年 10 月第 57 期，頁 239-247。
2. 何全德，「如何建立電子化政府資訊安全機制」，資訊與電腦，1999 年 10 月，頁 50-56。
3. 吳宗成，「淺談密碼模組驗證制度與資訊安全系統委外」，資訊安全通訊，第五卷第一期，民國 87 年 12 月，頁 101-112。
4. 吳明義，「線上報稅餘波盪漾」，網路通訊，82 期，1998 年 4 月，頁 36-43。

5. 吳琮璠,「國外政府機構資訊系統安全稽核制度」，存款保險資訊季刊，第 10 卷第 2 期，頁 21-27。
6. 巫靜宜、呂麗琴、李鴻璋,「國民卡策略規劃與其運作安全及法源規則」，中華民國資訊學會通訊，第二卷第一期，民國 88 年 3 月，頁 7-15。
7. 李麒麟,「駭客攻防」，資訊安全通訊，第 5 卷第 3 期，1999 年 6 月，頁 84-89。
8. 汪志道,「電磁脈波炸彈=EMP-bomb」，尖端科技，180 期，1999 年 8 月，頁 62~72。
9. 林詠章、黃明祥,「網路系統安全之技術」，資訊安全通訊，第 5 卷第 3 期，1996 年 6 月，頁 11-19。
10. 孫偉平、陳先彬,「計算機戰」，現代軍事月刊，1997 年 7 月，頁 26-32。
11. 孫強銀,「信息攻擊手段面面觀」，現代軍事月刊，2000 年 3 月，頁 30-33。
12. 馬榮安,「駭客的種類」，網路生活雜誌 ，第 47 期，頁 18-22。
13. 張韋杰、蘇劍飛,「信息戰應確立幾個觀念」，現代軍事月刊，1999 年 2 月，頁 27-30。
14. 樊國楨,「虛擬社會資訊安全機制初探——從密碼模組領域認證體系談起」, 資訊安全通訊, 第五卷第二期, 民國 88 年 3 月, 頁 7-20。
15. 蔣永芳譯,「掌握資訊優勢的利器」，國防譯粹，第 26 卷第 1 期，民國 88 年 1 月，頁 5-10。
16. 蔡明聰,「共軍 M 族飛彈對台澎防衛作戰之影響及我因應之道」，陸軍學術月刊 397 期，1998 年 5 月，頁 8~15。
17. 賴溪松,「中華民國資訊安全之活動與發展」，資訊安全通訊，第五卷第二期，民國 88 年 3 月，頁 28-36。

中文報紙

1. 大公報專電,「網絡安全中心成立，管制不良信息入侵」，大公報（香港），1999 年 8 月 11 日，第 2 版。
2. 大陸新聞中心編譯,「台灣海峽的安全情勢——美國國防部提報國會評估報告」，聯合報，1999 年 2 月 27 日，第 4、13 版。
3. 王健華,「簡析網絡戰」，中國國防報，1998 年 11 月 27 日，第 3 版。
4. 王新、張光軍,「把信息戰植根於人民戰爭沃土中」，中國國防報，1998 年 7 月 3 日，第 3 版。
5. 白德華,「駭客攻擊知名網站金融機構獲預警」，工商時報，2000 年 2 月 14 日，第 10 版。
6. 李宗健,「網絡戰特點及手段」，解放軍報，1997 年 7 月 22 日，第 5 版。
7. 沈偉光,「信息戰研究導論」，解放軍報，1995 年 11 月 7 日，第 7 版。
8. 沈偉光,「信息邊界」一個必須關注的戰略話題，中國國防報，1997 年 4 月 15 日，第 6 版。
9. 林志成,「駭客止步，我擬建立網路安全國家標準」，中國時報，1999 年 8 月 27 日，第 9 版。
10. 林銘義,「陳水扁保證:改善兩岸關係維持台海和平與美國會重量級議員越洋對話」，中國時報 ，89 年 4 月 14 日 ，第 1 版。
11. 11 邱裕榮,「固網開放：台灣電信市場面臨變天」，工商時報，2000 年 3 月 21 日，第 12 版
12. 紅燕,「軍隊組建四所新院校」，大公報（香港），1999 年 7 月 3 日，第 3 版。
13. 胡慧文,「國民大會網站 遭駭客「廢」了攻擊程式入侵 軟硬體都嚴重受損」，中央日報，1999 年 8 月 24 日，第 6 版。
14. 胡憶平,「入侵五角大廈「高手」年僅十七歲，荷蘭跨國組織差一點癱瘓美軍飛彈系統」，中國時報，1998 年 5 月 9 日，第 3 版。
15. 夏念慈,「國民大會網站 遭駭客「廢」了攻擊程式入侵 軟硬體都嚴重受損」，中國時報，1999 年 8 月 12 日，第 3 版。

16. 徐華保,「世紀之交的戰場走向」, 中國國防報, 1997 年 9 月 5 日, 第 6 版。
17. 曹逸雯,「經部網站疑遭駭客入侵工商登記網路查詢系統無法運作」, 中央日報, 1999 年 8 月 24 日, 第 6 版
18. 陳京城,「駭客猖獗資策會布網防護」, 經濟日報, 1999 年 8 月 31 日 , 10 第版。
19. 馮良、徐立生,「未來作戰, 無網不勝」, 解放軍報, 1998 年 7 月 7 日, 第 6 版。
20. 路透社,「三年前英國少年普萊斯用家中電腦破解 200 道安全措施, 登入五角大廈彈道飛彈資料」, 聯合報, 1997 年 3 月 23 日, 第 10 版。
21. 滕建群,「信息時代呼喚新的國防觀」, 中國國防報, 1997 年 6 月 6 日, 第 8 版。
22. 鄭哲政,「俄羅斯駭客入侵銀行「搬」錢」, 聯合報, 1999 年 3 月 5 日, 第 3 版。
23. 羅如蘭,「中共發動資訊戰」, 1999 年 8 月 17 日, 第 14 版。
24. 羅添成,「中國電子戰, 侵台 60 餘次」, 自由時報, 1999 年 9 月 15 日第 3 版。
25. 羅曉荷,「本月上旬對岸駭客七千餘次來襲」, 聯合報 , 1999 年 8 月 17 日, 第 8 版。

英文部分

BOOKS

1. *Barrett Neil, The State of the Cybernation (London: Kogan Page, 1996).*
2. *Colander Roger C., Riddle Andrew S., Welcomed Peter A., Strategic*

information Workface: a new face of war (RAM), 1996.

3. *Daniel, Ginsberg Transformational change and the future of the Chinese military, SAIS Review (: Winter/Spring 1998).*
4. *Harknett Richard J., Information Warfare and Deferrence (Parameters, US Army War College, 1996).*
5. *Hill Michael W.,The impact of information on Society(London ; New Providence, N.J. : Bowker Saur, c1999).*
6. *Jones.Steven G.Cybersociety:The culture and politics of cyberspace and the internet(Sage Publications.Inc.1995).*
7. *Jordan Tim.,Cyberpower(London ; New York : Routledge, 1999).*
8. *Kimmins J.,「Network Security management and administration; Concepts and issues」, Network Operations and Management Symposium, 1992, NOMS Computer Networks, 1996, Proceedings 21st IEEE Conference on, 1996.*
9. *Libicki Martin C., Defending Cyberspace and Other Metaphors (NDU Press, 1997).*
10. *Negroponte Nicholas, Being Digital (New York: A. A. Knopf, c1995).*
11. *Parker Donn B., Fighting Computer Crime (John Wiley & Sons, 1999).*
12. *Topeka Edward and Triplett William II, Red Drag Rising-Commun-Chira's Military Threat to Camera, (Washington, Regency Publisher, 1999).*
13. *Alvin Toffler, The Third Wave (New York: Morrow, 1980).*
14. *Alvin Toffler , Powershifts Knowledge, Wealth and Violence at 21st century (Published by Bantam Books, 1990).*
15. *Alvin Toffler, war and anti-war: Survival at the dawn of the 21st century (Boston: Little, Brown, c1993).*

二、*Periodical*

參考書目

1. *1.B. Sillon C. Soh, T. S. and County P., 「Quantitative risk assessment of Computer Virus attacks on computer networks」 Computer Networks and ISDN System, Vol.27, pp.1447-1458, 1995.*
2. *Chris Taylor Behind, The hackers are Attack, Time, (Feb 21), pp35~52*
3. *Halal.W. E., 「From hlerachy to Enterprise: internal market are the new fund ration of management」, Academy of Management Execute (1994) Vol.3, No.4, p70.*
4. *Joint Pub 3-13, 「Information Operations」, Dodd US, December 1998.*