# 第四章 資訊科技對國家安全之衝擊

由於資本、人民、資訊、科技、理念等全球流動之增加，所產生的「全球化」現象已經成爲具有國際主導及影響力量。全球化可以是一個正面之力量，例如全球科技與資訊的擴散，可以增加較小國家、團體與個人的破壞力量來勇於對抗強權。但是也有可能惡化地區之發展與造成區域緊張，進而增加衝突的能力與可能性。因此在鼓勵與鞏固全球化的正面意義的同時，也要避免不當的破壞力量，這將是各國政府所要面對的持續挑戰。[1]

比起研究傳統的暴力犯罪形式而言，「資訊科技」所引起的跨國性安全問題，更值得投注更多的注意力。現代化的技術抵銷掉地緣距離上所產生之效果，也增加了手段的多樣性以及破壞的範圍，更增加了有能力發動攻擊的行爲者數量，[2]成爲非國家行爲者的主要力量來源。研究資訊科技安全的學者普遍認爲，資訊科技的進步使得安全問題變的難以掌握，意圖破壞國家安全的有心份子只要透過遠端的鍵盤及滑鼠，再搭配駭客或是病毒程式，就可以對國家賴以維生的金融系統或是國防安全進行滲透或破壞，犯罪將不再受地理範圍所限制。

在網際網路中的使用者可以隱藏自己的真實身份，「在網際網路中，沒有人知道你是誰」，而這也是認爲政府無法管理網路的一個主要理由。[3]當高技術以及電子通訊和網路空間的來臨時，所面臨到的問題是：國家沒有邊界可防守；也難以管理一個存在於電腦網路中的位址。除此之外，「資訊科技」與戰爭的相結合也促成了新的戰爭型態出現。因此爲維護國家安全，必須瞭解資訊科技，尤其是網際網路爲國家安全所帶來之影響和衝擊，以適時的調整出因應之國家安全戰略及合作之擬議。

---

[1] 汪毓瑋，**新安全威脅下之國家情報工作研究** (台北：遠景基金會，2003 年)，頁 46。
[2] Zbigniew Brzezinski, *The choice : global domination or global leadership*, (New York: Basic Books, 2004, p. 11.
[3] Andrew L. Shapiro, "The Internet," *Foreign Policy*, Issue. ll5 (Summer, l999), p. 17-19.

## 第一節 資訊科技在國家安全中的戰略地位

資訊科技改變了世界，以資訊爲主的戰略，需透過國家資訊目標與方法，以達成國家安全政策之目標，像是支援國家事務，包括在政治、經濟與軍事、科技、文化與資訊各方面；以及平時、危機與戰時危機處理、國與國之間互動等事項。[4]網際網路的發展在推動人類社會進步的同時，也帶來了安全維護上的問題。其開放性廣泛接觸的基本特點，使得網際網路成爲個人、組織與國家基礎設施所殷切依賴的系統。這個現象雖爲資訊資源的共享創造了有利條件，但也爲敵對國家的資訊入侵提供了不受國界限制的「不設防邊境」。

每一次傳播和交通工具的革新都對時空維度以及國家的政治過程和軍事戰略產生重要影響，這種影響表現爲國家實力的損益程度以及安全的範籌、格局以及戰略思維上。[5]在資訊時代，國家安全的疆界已從物理疆界擴展到虛擬疆界，這種疆界不是以傳統的地緣、領土、領空、領海來劃分，而是以帶有政治影響力的資訊輻射空間來劃分。邊界線的變化，也在一定程度下體現了國家軍事安全概念演變的歷史軌跡。隨著戰場上飛機的使用，國家間的戰爭及軍事安全，也從原本的陸地或海上這一、二維平面的進行，拓展到了三維。爾後，人造衛星的發射，更使得軍事鬥爭觸角伸向了外層空間，新的立體戰場已初步出現，戰爭空間呈現出四維狀態，國家軍事安全也日益四維化。[6]

當人們還沒對這種新的第四維邊界—太空邊界進行充分認識跟用時，先進的計算機、通訊和網路技術的發展運用，加上網路戰的出現，不僅使人類社會進入一個新的時代—資訊時代，也直接導致了資訊時代的新邊界—第五維邊界，也就是資訊邊界或是網路邊界的產生。國家安全的戰略概念和內涵也俗之產生新的變

[4] Thomas E. Copeland (ed.), *The Information Revolution and National Security*, (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2000), p. 117.
[5] 張新華，**信息安全：威脅與戰略** (上海：上海人民出版社，2003 年)，頁 46。
[6] 馬維野，**全球化時代的國家安全** (武漢：湖北教育出版社，2003 年)，頁 117-118。

化。[7]安全戰略(Security Strategy)是安全主體實現其目標的方法與策略。國家要維護自己的安全，就要有適當的安全戰略。一個國家的安全戰略應包括對國際安全形勢的基本認識，對國際安全環境的總體判斷，以及對實現國家安全利益的戰略性安排。於是以下便就資訊時代爲國家安全的戰略環境帶來之影響作一論述。

## 壹、資訊科技趨勢下之宏觀戰略環境

資訊時代的國家安全應該是綜合性的安全概念，包括政治、經濟、軍事、科技與資訊等各方面的安全。政治資訊的安全關係到政府的穩定、命運與前途；經濟資訊的安全關係到國家經濟的正常運作;軍事資訊的安全關係到國家軍事力量的可靠程度；科技資訊的安全關係到國家的發展潛力；文化資訊的安全關係到國家文化藝術的發展和民族觀的繼承。由此可見，資訊科技爲國家安全戰略之重要基石，若無法得到保障，國家就會政治不穩、經濟紊亂、軍事低落、文化迷失、科技落後，進而影響國家在國際上的地位與形象。[8]

Robert Walters和David Blake認爲，先進的科技是國家達到軍事、政治以及經濟目標的必要條件，也是國家實現外交政策的重要工具。[9]資訊科技在國家安全中的重要戰略地位，也決定了資訊科技安全與國家安全其他方面的關係。

### 一、資訊科技安全與政治安全

在本論文的第三章中曾經提到，科技的創新與應用提升的國家的柔性國力，亦間接增加國家在國際政治上的影響力。掌握先進資訊科技的國家，能夠透過尖端的通訊設備將其文化、意識型態或價值觀傳播至世界其他角落，使他國逐漸習慣並融入其價值觀，因而提升該國在國際事務上的主導地位與政治力量。

---

[7] 馬維野，**全球化時代的國家安全** (武漢：湖北教育出版社，2003 年)，頁 118。國家實驗研究院科技政策研究與資訊中心編，**94 年度資通安全分析專論彙編** (臺北市：國研院科技政策中心，民 94)，頁 102。

[8] 羅承烈著，「資訊科技與國家安全」，**空軍學術月刊**，第 541 期(2001 年 12 月)，頁 76。

[9] Robert S. Walters; David H. Blake, *The politics of Global Economic Relations* (Englewood Cliffs: Prentice Hall, 1992), p. 165.

然而資訊科技的迅速發展，加上網際網絡的日益擴大，使得各國對於資訊擴散的控制能力明顯減弱，對國家主權也搆成一大挑戰。主權的行使範圍也不斷弱化。資訊科技還可以製造虛假政治資訊，以用來操縱他國政治左右該國政治輿論優勢，破壞該國的政治穩定。[10]另外無庸置疑是，網路影響政治的情況將蔚爲趨勢，中共內部網路發展爲例子，網路的普及以及網民的「言論自由」，正逐步升高對中共長期以來的「封閉型政治體制」的衝擊，即使官方透過「網軍」的強勢管制，似乎也無法改變這樣的趨勢。

根據大陸的互聯網中心統計，大陸網路用戶數量已超過一億以上，而且還在快速成長之中，網路已經成爲年輕一代的重要溝通媒介，「QQ網」動輒百萬人上網，網路的快速發展以及無遠弗屆的特質，基本打破了中共官方對媒體封鎖的藩籬。其實，就民間的觀點來看，大陸正要走入的或許是「網路影響政治」的時代，而不是「網路服務政治」的時代。[11]資訊科技正利用它的特性來影響政治方面的安全。

## 二、資訊科技安全與軍事安全

軍事安全的目標是以武力保衛國家利益，面遭敵對國家的威脅和侵犯。冷戰前，維護軍事安全的主要手段是軍備競賽和戰爭；而現在高科技的發明和應用所引起的軍事事務革命，已經將過去以能量爲基礎的機器戰轉爲以微電子技術和電子計算機技術爲基礎的資訊戰。[12]交戰一方利用程式則有可能使對方的指揮系統、通訊系統和武器系統癱瘓，無法投入戰鬥，達到不戰而屈人之兵的目的。[13]

不論是以科技知識或武器裝備的劃分來分析戰爭型態，它都說明了「資訊科技」對於軍事安全的影響。1991 年的波灣戰爭，即是美軍以資訊科技爲基礎的

---

[10] 羅承烈著，「資訊科技與國家安全」，**空軍學術月刊**，第 541 期(2001 年 12 月)，頁 76-77。
[11] 「中共闢國網，盼邁向網路政治」、「網路影響政治 才是趨勢」，**中國時報**，民國 95 年 1 月 9 日，A13 版。
[12] 馬維野編，**全球化時代的國家安全** (武漢：湖北教育出版社，2003 年 10 月)，頁 231。
[13] 馬維野編，**全球化時代的國家安全** (武漢：湖北教育出版社，2003 年 10 月)，頁 231。

戰爭，因而成爲世界戰史型態上的重要里程碑，終將成爲未來戰爭的趨勢。[14]

另外，值的注意的一點是，國家對於科技創新的投資，尤其是軍事科技的研究與發展，將帶動軍事力量的提升。科技創新及其所產生的經濟效益有助於軍事力量的發展，以在軍事力量上佔有競爭優勢。[15]

## 三、資訊科技安全與經濟安全

與國家經濟安全的相關因素很多，其中最重要的就是資訊科技的進步和安全。但是網路世界中的經濟一體化，卻也使得國家經濟活動受到攻擊的脆弱度大爲增加，透過電腦網路資訊攻擊，或是切斷(癱瘓)被封鎖國與外部所有的經濟資訊聯繫，將使得國家經濟活動陷於癱瘓。[16]故經濟安全離不開資訊科技安全的保障，繁榮的經濟也需要隨科技增加的力量來加以保護。

## 四、資訊科技安全與文化安全

資訊網路無疆界的大量流動，所形成跨疆界的虛擬社區，將衝擊該國人民在文化上，以致於族群及國家之認同。[17]當前，資訊科技發達的國家往往也是世界主流文化的代表，西方發達國家爲實現其全球戰略目標，便利用現代科學技術之大眾資訊傳播來強化並發揮軟權力的作用，將西方所謂的自由、民主、人權價值觀進行文化侵略，將使得受到文化侵略的發展中國家的國家安全造成不利影響。[18]

隨著資訊革命以及全球化的普遍推進，全球大戰略正發生某種程度的變化，傳統上國家安全考慮的是政治、軍事、經濟及文化安全，而現今國家安全中的「資訊戰略」此一新的領域正在浮現。將資訊能力納入國家安全的想法，則是首見於

---

[14] 張祥山著，「非傳統不對趁安全威脅初探」，**展望與探索**，第 4 卷第 4 期(民國 93 年 4 月)，頁 38。

[15] Karen Rasler; William R. Thompson, "Technological Innovation, Capability Positional Shifts, and Systemic War," *Journal of Conflict Resolution*, Vol. 35, No. 3 (September, 1991), pp. 424-439.

[16] 羅承烈著，「資訊科技與國家安全」，**空軍學術月刊**，第 541 期(2001 年 12 月)，頁 77。

[17] 羅承烈著，「資訊科技與國家安全」，**空軍學術月刊**，第 541 期(2001 年 12 月)，頁 77。

[18] 馬維野編，**全球化時代的國家安全** (武漢：湖北教育出版社，2003 年 10 月)，頁 232。

1981 年雷根政府之「國家安全戰略」文件，該文件將資訊列爲第四種國力。[19] 資訊科技的安全問題成爲國家安全的核心領域。在此新世界之中，要成功維護國家安全的關鍵，即在於對資訊科技能力和資源進行有效之戰略性管理。[20]

## 第二節 資訊科技所造成的非傳統安全威脅

有別於傳統安全以國家爲中心、軍事是維持國家安全最重要手段的觀念，資訊科技對國家安全所造成的影響，乃是其對國家安全產生威脅的主體是呈現多元化，資訊科技所引起的跨國性安全問題單靠軍事力量也不足以應付，因而值得我們對於這樣的非傳統安全威脅投注更多的注意力。像是敵對國家、恐怖主義者、擴散者、毒品走私者及組織犯罪者，將會利用新且快速的資訊環境及其他科技，以進行非法活動，且影響全球之安定與穩定。資訊、科技等方面的擴散，將會繼續對人們的生活方式、思考、工作、組織及作戰產生深遠影響。[21]科技的全球化、不同科技成就的相容整合及不可預料浮現中科技的運用，已使得預測未來科技發展更加困難。[22]

網際網路之所以特別容易受到商業或是個人使用，甚至是恐怖主義者使用上的青睞。正是因爲具有以下幾點特性：首先，是網際網路可以被匿名性地使用；第二，網際網路是全球的，可以即時傳播且便宜；第三，網際網路受到的規範很少，因爲其做爲一個開放、分散的相互操作網絡發展，僅受到少數最小限度的約

[19] Thomas E. Copeland ed., *The Information Revolution and National Security*, (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2000), p. 119.
[20] 張新華，**信息安全：威脅與戰略** (上海：上海人民出版社，2003 年)，頁 53。
[21] Thomas E. Copeland ed., *The Information Revolution and National Security*, (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2000), p. 3.
[22] 汪毓瑋，**新安全威脅下之國家情報工作研究** (台北：遠景基金會，2003 年)，頁 50-51。

束。[23]網路攻擊不像某些比較傳統型態的攻擊，或是本土防衛所應該注意的生化作戰那樣，網路攻擊本身不太可能造成一國的瓦解。然而，像是美國的軍事通信有 95%是透過民間的電信與電腦系統而進行的，故美國對資訊系統的依賴已經成爲一種戰略上的弱點。雖然網路攻擊所直接造成的破壞效果尚不及傳統型態的攻擊來的嚴重，但網路攻擊可能對於國家目標與國家安全利益造成重大的不良影響。[24]

## 成形中的新威脅

日益增多的網絡安全事件，爲各國軍事資訊系統的安全保密帶來了巨大威脅。初步統計，現在世界上已有 2000 多萬人具有網絡攻擊的潛力，「駭客」運用的軟件工具已達 1000 多種。資訊科技已經對國家整體安全形成了巨大影響。[25]在此種新環境之中，可能會出現好幾種威脅；每一種威脅都對國家安全的危害程度各不相同。此等威脅的類型有以下幾種：[26]

### 一、破壞通信流、經濟運作、公共資訊宣傳、電力網與政治談判、供水系統及國家基礎設施的其他組成要素等之等之威脅

此方面的破壞效果純粹在經濟領域，因此私人部門對之特別感到憂慮。若於戰時軍隊的通信若遭到破壞，將可能造成人命的損失或使攻擊任務因而中止。由於製造破壞性病毒及展開「阻斷服務」攻擊所需的工具可取得性及性能都不斷提升，故此類威脅變成事實的可能性很高。過去發生過許多類似性質的攻擊事件，其在美國所造成的經濟損失都是以數十億美金計算。

---

[23] Ashley S Deeks, Barbara Berman, Susan W Brenner, James A Lewis. “Combating terrorist uses of the internet,” American Society of International Law. *Proceedings of the Annual Meeting*. Washington: 2005. p. 104-105.

[24] Arnaud de Borchgrave (ed.), *Cyber threats and information security :meeting the 21st century challenge* (Washington, D.C.: CSIS Press, 2001), p. 7.

[25]「漫談信息時代的國家安全」，解放軍報網路版，<http://army.news.tom.com/Archive/10000/2002/7/24-36197.html> (2002 年 07 月 24 日)

[26] Arnaud de Borchgrave et al., *Cyber threats and information security: meeting the 21st century challenge* (Washington, D.C.: CSIS Press, 2001), pp. 8-10.

## 二、敏感資訊、專利資訊或機密資訊遭到利用的威脅

資訊的竊取、詐騙及網路犯罪，會對個人層級(像是身份竊取)；或是制度層級(像是線上信用卡詐欺或竊取大量信用卡號碼)；甚至是國家安全層級(例如有計畫地刺探機密性或雖非機密性但十分敏感的政府系統)帶來極嚴重的後果。爲

舉凡盜用身份及對政府系統進行有計畫的刺探行爲等等，此種型態的攻擊大部分屬於零星性質，其動機不外乎是爲了求取個人的經濟利益或意圖揭露某些系統安全性不足的事實。最糟糕的事，要發現此等型態的入侵行爲極受其危害的系統，均是十分地困難。和上述前一項的破壞性威脅一樣，發生此一威脅的可能性也是相當高。

## 三、基於政治、經濟、軍事或製造動亂的目的而操控資訊之威脅

使用網際網路用來做爲操縱資訊的強有力手段是相當具有潛力的。雖然許多操縱資訊的事例中，許多只是想藉機發表言論罷了，而這類的行動所造成的影響也比較容易被修復。但是有些尚未被察覺的事例將變的更加危險：像是操縱金融資料、軍事資訊或有關操縱基礎設施的功能性資料(如洩洪時間)等等，此等型態的攻擊所需要的手段，比起進行破壞行動所需手段更爲複雜。基於政治、經濟、軍事或製造動亂的目的敵人只要擁有少量資源及相當精密的科技，即可輕易遂行此種攻擊。

## 四、摧毀資訊、或摧毀支撐資訊的重要基礎設施組成要素之威脅

摧毀資訊或支持資訊的基礎設施此一威脅會嚴重危害到經濟安全與國家安全。因爲就像對資訊的破壞一樣，同樣只需使用相當簡單的駭客技術即可遂行此種攻擊行動。有關電腦病毒的事例不勝枚舉，像是「我愛你病毒」(The Love Bug virus)不僅會塞爆電子信箱及竊取密碼，更會導致硬碟檔案被銷毀。

但由於目前重要國家資產的周遭通常都具備有較爲嚴密的防護措施，故摧毀

重要資訊基礎設施的可能性仍然比較低。然而此種可能性確實是存在的，我們不可掉以輕心。

處理資訊時代的威脅已經漸漸成爲國家本土防衛以及戰略考量的中心議題。我們很難去加以區分民族國家與非國家行爲者之間所發動攻擊的差別。也很難去界定確認，甚至是想要迴避或是逮捕犯罪者都顯得相當困難。除非能夠充分瞭解上述這些成形中的新威脅間的差異，並改善提升國家的能力，俾能對此等攻擊即發動者的性質做出正確、迅速之評估，乃是我們當前所需面對的主要問題。以下便針對威脅形成類型分成兩大重點進行討論。分別是網際網路所造成的的新威脅部分(包括病毒、駭客及網路恐怖主義部分)；以及資訊結合戰爭所產生之戰略資訊戰的問題。

## 壹、網際網路的新威脅-病毒、駭客、網路恐怖主義

網際網路的普及，使得個人或組織對於網路的依賴性大增，而這種現象也是不受國界所限制的。網際網路的變遷與進步也加速了滲透到人民日常生活的速度。但即使資訊科技與其相關的網際網路技術已經成爲當代世界主流和重要的必須品，其對於國家甚至是全人類社會的危害和負面影響也是層出不窮的。舉凡駭客入侵與病毒攻擊事件，對於越是依賴科技的先進國家所造成的損失也越加嚴重。網際網路犯罪活動對國際社會安全和穩定產生以下威脅：[27]

### 一、網路的發展為病毒的傳播創造了條件：

2000 年 5 月 4 日，一種來自菲律賓名爲「我愛你」(I Love You)的電腦病毒透過電子郵件傳播，經過兩天時間就已侵襲全球 4,500 萬台電腦，造成了高達上

[27] 魏澤民，林志昶著，「資訊時代的國際關係圖像：以Internet爲例」，**展望與探索**，第 2 卷第 2 期(民國 93 年 2 月)，頁 25-27。

百億美元的損失。[28]在網際網路普及前，電腦病毒的傳播途徑主要是透過軟碟，然後現在電子郵件、下載資源、甚至是有些網頁等等都成爲傳播病毒的便利途徑，令人防不勝防。

## 二、網路成為駭客(Hacker)天堂

隨著網際網路應用的日益普及，使得駭客技術更加平民化。在本文第二章中便提到，數年前有能力進行駭客入侵動作的人都是具有高階技術的專業人才，而今用來攻擊網路的工具及程式比起以往來說更加容易取得，這使使得任何人都可以輕易地利用已知的入侵方法來攻擊網路。有些駭客是爲了炫耀自己的電腦才能或是以正義仲裁者自居，有的則是爲了竊取政治、軍事、商業機密等。[29]運作範圍則是包括：運用駭客技術對付目標網站，試圖中斷其正常操作但不造成嚴重傷害。相關案例包括網頁駭客、電腦入侵、電腦病毒、蠕蟲及自動電子郵件炸彈等。[30]

有些駭客受政府和社會團體所網羅，專門針對敵對國家進行攻擊。未來敵對國家只要使用網路掃瞄工具或密碼破解軟體侵入國防、交通、電力及金融等電腦網路或滲入爲嚴密監控的全球網路，便可不必進入對方國土領域，默默進行遠端下達指令的工作，相對造成電腦主機擁有者的恐慌。[31]像是中共有計畫的在網路上成立「網軍」(Net Army)的意圖，以進行刺探我國政府網站的防護機制，藉機植入木馬程式(Trojan Horse)[32]以破壞往暫獲竊取資料。[33]正因如此，隨著時空環境

---

[28] Stuart Biegal, *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace* (Cambridge, Mass.: MIT Press, 2001), p. 227.

[29] 魏澤民，林志昶著，「資訊時代的國際關係圖像：以Internet爲例」，**展望與探索**，第 2 卷第 2 期(民國 93 年 2 月)，頁 26。

[30] John Arquilla and David Ronfeldt eds.，楊永生譯，**網路及網路戰** (台北：國防部史政編譯局，民國 92 年)，頁 303-304。

[31] 高大宇、王旭正著，**資訊安全** (北縣汐止市：博碩文化，2003 年)，頁 184。

[32] 主要是指隱藏未授權程式碼並執行使用者不想或不知道功能的程式。參考：高大宇、王旭正著，**資訊安全** (北縣汐止市：博碩文化，2003 年)，頁 217。

[33] 魏澤民，林志昶著，「資訊時代的國際關係圖像：以Internet爲例」，**展望與探索**，第 2 卷第 2 期(民國 93 年 2 月)，頁 26。 「中共發動網軍 侵入政府電腦操演資訊戰」，**大紀元報**，2003 年 9 月 3 日。<http://www.epochtimes.com/b5/3/9/3/n369583.htm> 「中共網軍入侵？國防部『老虎

因素的演變，網路駭客的時代意義也有所變革。

## 三、網路恐怖主義

根據學者Stuart Biegel在其書「超越我們的控制？」(*Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace)*中，對網路恐怖主義做出以下定義：指的是「存在於網路環境下的一股極強烈力量，導致意想不到或是反常的結果，其目的是爲了脅迫、強制或是製造無政府的恐怖氣氛、失序或是混亂。」[34]

資訊時代不僅對恐怖份子選擇目標與武器有所影響，同時亦對其行動方式和組織架構產生影響。在網際網路問世之前，透過有線電視新聞網(CNN)所傳送美軍人員在索馬利亞被拖行的畫面得已被圖像呈現散播開來，而今恐怖份子受益於資訊科技的力量，得以運用電腦、軟體、電傳通訊設施及網際網路等資訊技術在心理上製造威脅並予以強化，[35]甚至用來進行資訊募集及宣傳工具，或是用來研究弱點以及選擇進攻目標。[36]

全球電腦網路的普及，使得像是奧薩瑪・賓拉登(Osama bin Laden)、恐怖組織「卡達」(al-Qaeda)及好戰回教組織哈瑪斯(Hamas)，就利用網際網路做爲行動資訊分享與聯繫的工具。[37]哈瑪斯認爲由於反恐組織的情報單位無法精確追蹤網際網路上的所有資訊流與內容，因此利用聊天室或電子郵件甚至是加密軟體等，能夠有效相互聯繫散居分屬美國或是加薩走廊、約旦河西岸及黎巴嫩各地的組織

---

部隊』迎敵」，**東森新聞報**，2006 年 5 月 15 日。 <http://tw.news.yahoo.com/060515/195/35397.html>

[34] Stuart Biegal, *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace* (Cambridge, Mass.: MIT Press, 2001), p. 232.

[35] Thomas E. Copeland ed., *The Information Revolution and National Security*, (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2000), p. 86.

[36] Ashley S Deeks, Barbara Berman, Susan W Brenner, James A Lewis. "Combating terrorist uses of the internet," American Society of International Law. *Proceedings of the Annual Meeting*. Washington: 2005. p. 103-109.

[37] Arnaud de Borchgrave (ed.), *Cyber threats and information security :meeting the 21st century challenge* (Washington, D.C.: CSIS Press, 2001), preface x.

成員，以保護協調行動的重要通信內容。[38]這種新的、具有彈性的網路更容易以極爲加密的方式進行聯絡，且這種組織也不需要設立一個具有脆弱性的中央總部。[39]

對於以上這些攻擊所需要做出的防禦，對國家而言不啻是一項棘手的挑戰。國家必須建立更佳的系統，以及戰術的預警與攻擊，以及更多性能更好的偵測系統，在加上遭受到攻擊之後的回應措施需要合作與協調，方可對付網際網路所伴隨之新威脅。

## 貳、資訊與戰爭結合的新挑戰-戰略資訊戰(Strategic information warfare)

由於資訊時代來臨，加上電腦與網路的普遍與便利的特性，徹底改變了未來戰爭的面貌與作戰型態，資訊科技移轉到戰場上軍事的攻防即是資訊戰，[40]且以其爲核心的軍事技術革命已大幅增強蒐集、處理和傳送的實戰能力。[41]一場以資訊科技爲核心的新軍事革命在全球範圍中蓬勃發展，「新戰爭」型態應運而生。[42]其作戰範圍涵蓋政治、經濟、心理等國家資訊基礎建設，以及戰略、戰術的軍事資訊基礎建設，凡對此等基礎進行攻擊或防護作爲者，均爲資訊戰之範疇。[43]

相較於傳統的戰爭而言，它是一個全新的作戰型態與思維，此名詞是在 90 年代初期的波灣戰爭之後才被納入軍事作戰研討概念之中。資訊戰容易給人留下

---

[38] John Arquilla and David Ronfeldt eds.，楊永生譯，**網路及網路戰** (台北：國防部史政編譯局，民國 92 年)，頁 35-44。
[39] Arnaud de Borchgrave (ed.), *Cyber threats and information security :meeting the 21st century challenge* (Washington, D.C.: CSIS Press, 2001), preface x.
[40] 國家實驗研究院科技政策研究與資訊中心編，**94 年度資通安全分析專論彙編** (臺北市：國研院科技政策中心，民 94)：頁 95。
[41] 國家實驗研究院科技政策研究與資訊中心編，**94 年度資通安全分析專論彙編** (臺北市：國研院科技政策中心，民 94)：頁 95。
[42] 中國現代國際關係研究所編，**信息革命與國際關係** (北京：時事出版社，2002 年)，頁 7。
[43] 曾章瑞著，**新世紀國家安全與國防思維** (台北：空中大學，2005 年)，頁 252。

涵蓋範圍廣泛、不易確認範疇的印象，目前先進國家並也未有完全一致的定義。[44]但是卻也都意識到這個概念不可避免是朝向動態的發展形式。[45]

學者Timothy L. Thomas認爲，「資訊戰」(information warfare)乃指的「是一國保護自身的資訊系統，免於遭受他國的入侵與破壞，並且在國家的軍事戰略上，能夠有應用資訊的優勢。在保護本國的資訊系統同時，也能夠有影響他國資訊與資訊系統的能力。」[46]另位學者Dorothy E. Denning則是資訊戰區分爲攻勢以及守勢兩種不同運作模式，把資訊戰看成是一種「得-失」(win-lose)的概念而區分爲：[47]

一、**攻勢資訊戰** (offensive information warfare)，意圖在於當目標面對防衛能力受到減損時，而能夠增加目標在反擊方面的能力，並且針對敵人最脆弱之處予以攻擊。[48]範圍包括攻擊敵人的資訊設施，發動電子戰(像是干擾)、心理戰、網路戰以及欺敵等等。[49]

二、**守勢資訊戰**(defensive information warfare)，則是試圖底抵銷可能受到減損的重要性，去保護資訊資產免於遭受到攻擊，跟資訊安全有密切相關。範圍包括作業安全、反制心戰、電子防護、資訊能力的確保、以及欺敵反制措施等等。[50]

1996 年美國蘭德(RAND)公司出版的「戰略資訊戰」(Strategy Information Warfare)一書，則是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

---

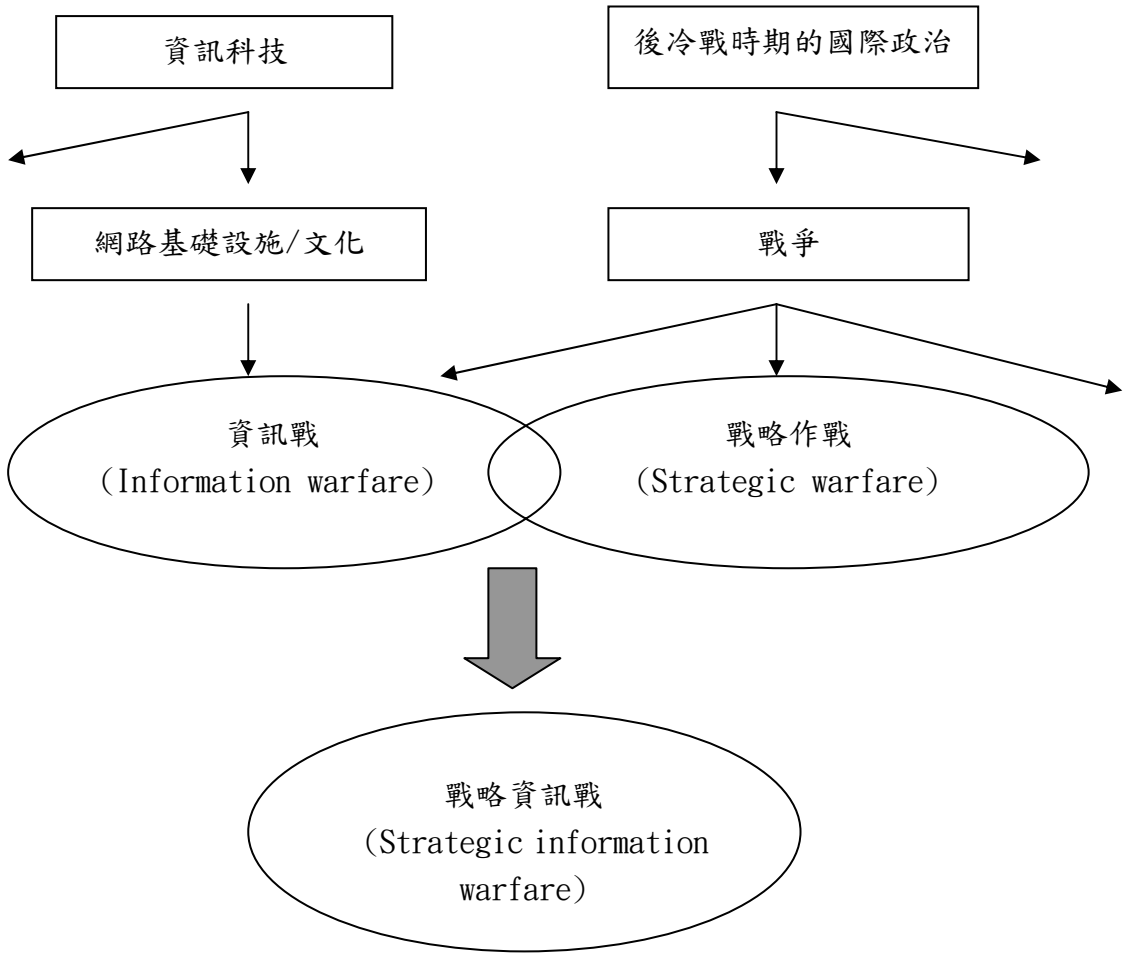
[44] 林哲正，中共資訊戰戰略思維，**國防雜誌**，第 20 卷第 4 期，民國 94 年 4 月，頁 98-106。
[45] Roger C. Molander, Andrew S. Riddile (eds.), *Strategic information warfare : a new face of war* (CA: Rand Company: 1996), p. 1.
[46] Thomas, Timothy L., "Deterring information warfare: A new strategic challenge," *Parameters* 26 (Winter 1996-1997): 83.
[47] Dorothy E. Denning, *Information Warfare and Security*, (New York: ACM Press, 1999), p. 10-12.
[48] Thomas E. Copeland (ed.), *The Information Revolution and National Security*, (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2000), p. 130.
[49] Thomas E. Copeland (ed.), *The Information Revolution and National Security*, (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2000), p. 59.
[50] Thomas E. Copeland (ed.), *The Information Revolution and National Security*, (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2000), p. 59.

地運用於更廣泛的資訊時代「作戰」觀念。國家運用網路空間去影響戰略的軍事運作以及對國家資訊基礎設施造成損害，這種新興的作戰觀念直接關連到一種情況，即發展迅速的網路全球化趨勢，將顛覆過去傳統作戰的方式，亦即是說，資訊戰突破以往固有的邊界概念。因此，蘭德公司將這種逐漸浮現的衝突領域稱做爲「戰略資訊戰」[51]

所謂「戰略資訊戰」，在本質上乃是資訊戰與後冷戰時期「戰略作戰」兩種觀念之結合，由於後冷戰時期，面對資訊科技的發展，新的戰略威脅與新的戰略弱點正在浮現(像是電腦網路威脅與弱點)。因此，將以網路空間基礎架構加上後冷戰時代戰略形式特點，即爲「戰略資訊戰」。[52](見圖 4-1)

[51] Roger C. Molander, Andrew S. Riddile (eds.), *Strategic information warfare : a new face of war* (CA: Rand Company: 1996), p. 1
[52] Roger C. Molander, Andrew S. Riddile (eds.), *Strategic information warfare : a new face of war* (CA: Rand Company: 1996), p. 1-2.

**圖 4-1 戰略資訊戰示意圖**




資料來源：Roger C. Molander, Andrew S. Riddile eds., Strategic information warfare : a new face of war (CA: Rand Company: 1996), p. 2.

## 以中共資訊結合戰爭之發展為例

中共集中力量發展資訊技術及其衍生的資訊戰硬殺(Hard-Kill)武器，亦將成爲對抗其他強權的重要武力。其正在研究資訊戰結合戰略作戰的攻擊性運用，以對抗外國的經濟、後勤和指管通電與情報系統($C^4I$)[53]，特別是極力建構一個可以

[53] 指的是指揮(Command)、控制(control)、通訊(communications)、電腦(computer)及情報(intelligence)。

攻擊其他國家電腦的能力(包括軍、民用電腦)，[54]以及將資料操縱、資訊利用及「超限戰」(unrestricted warfare)[55]等觀念納入其新的軍事計畫中。[56]

基本上，集中力量投入資訊科技的創新，以利發展電磁權之武器裝備，僅是中共在進行「不對稱作戰」的重要考量之一。[57]所以對於新一代的國家與軍事安全作爲而言，面對的重要方向與課題便是如何進行研究發展資訊科技與戰略之相結合，以建立國家安全機制與戰場上的通資電優勢。[58]

資訊時代的戰爭和以往的傳統戰爭時代不同，資訊時代可能面對的是不確定的敵人與充滿摩擦的戰場，一些流氓國家會試圖以資訊戰爭做爲手段，結合可獲得的電腦工具來針對連結對方經濟和軍事的重要節點(nodes)發動攻擊。[59]因此，要能夠充分瞭解資訊時代的特性乃爲決勝的關鍵，但是軍事力量的保有與發展也是不可忽略的事。[60]資訊科技也永遠是用來防範和打擊恐怖主義的最好方法。[61]廿一世紀資訊科技將成爲國家綜合戰力的象徵，國與國間的經濟利益主要展現於對資訊的優勢與建設，而掌握資訊優勢爲目的戰略資訊戰亦必然爲國家對抗的焦點，也爲平時及戰時的經濟運作、社會互動與軍事作戰的本質帶來重大改變。

---

[54] 國家實驗研究院科技政策研究與資訊中心編，**94 年度資通安全分析專論彙編** (臺北市：國研院科技政策中心，民 94)，頁 71。

[55] 見喬良與王湘穗合著，**超限戰** (北京：解放軍文藝出版社，1999 年 2 月)。書中指出資訊科技已擴展了戰爭概念，並根本改變了戰爭的本質跟手段。

[56] Borchgrave, Arnaud de, Frank J. Cilluffo, Sharon L. Cardash, Michele M. Ledgerwood , Cyber threats and information security: meeting the 21st century challenge. (Washington, D.C.: CSIS Press, 2001), p. 5.

[57] 國家實驗研究院科技政策研究與資訊中心編，**94 年度資通安全分析專論彙編** (臺北市：國研院科技政策中心，民 94)，頁 71。

[58] 國家實驗研究院科技政策研究與資訊中心編，**94 年度資通安全分析專論彙編** (臺北市：國研院科技政策中心，民 94)，頁 96。

[59] David C. Gompert, "National Security in the Information Age," *Naval War College Review*, Vol. 51, No. 4 (Autumn, 1998), p. 32.

[60] 翁明賢著，**全球化時代的國家安全** (台北縣：創世文化，2003 年)，頁 197。

[61] Joseph S. Nye, Jr. "America's Information Edge." *Foreign Affairs*, Vol. 75, No. 2 (March/April, 1996), p. 32.

## 第三節 資訊科技影響國家安全之個案研究

美國前國家安全顧問布里辛斯基(Zbigniew Brzezinski)在其書「美國的抉擇」(The Choice: Global Domination or Global Leadership)中提到，未來國際情勢中衝突所產生的暴力手段，除了舊式傳統的殺傷性武器外，更包括新式由網路所進行的癱瘓性攻擊，可能是由國家、恐怖組織或是反政府人士發動，以用來攻擊先進社會中的基礎運作設施，讓對方陷入混亂。[62]在運用資訊科技攻擊的案例底下，需要有一項明確的規範來要求國家對情勢做出適當反應，一旦缺乏規範將無法避免遭到報復。[63]以下便針對資訊科技影響國家安全的個案進行探討：

### 壹、「月光迷宮」事件(MOONLIGHT MAYHEM)[64]

1998 年 3 月，國防部偵測一連串嚴重電腦攻擊美國政府與私人部門，但是這項刺探作業已經持續了一年以上才被美方發現，於是美國著手針對此進行調查，並將其調查工作取名代號爲「Moonlight Maze」。此一攻擊事由駭客群們利用精密工具侵入數百台美國國家航空太空總署(NASA)、五角大廈、及其他政府機構的電腦網絡。數位侵入者竊取數以千計的檔案，包括技術研究、電腦加密技術和大量非機密性，但具敏感性的資料攸關五角大廈的戰爭計畫系統。

自從「Moonlight Maze」首度被發現以來，美國情報圈開始致力於最大的數位情報的投資，但是此等攻擊行動到 2000 年仍一直持續進行。美方經過三年以上的努力卻只有很少的線索，攻擊顯示來自七個分佈於俄羅斯境內各不同地點的

---

[62] Zbigniew Brzezinski, *The choice : global domination or global leadership*, (New York: Basic Books, 2004, p. 12-13.

[63] Libicki, Martin C, *Defending cyberspace, and other metaphors* (Honolulu, Hawaii: University Press of the Pacific, 2002), p. 53.

[64] Arnaud de Borchgrave (ed.)., *Cyber threats and information security: meeting the 21st century challenge* (Washington, D.C.: CSIS Press, 2001), pp. 8-9. Adams James., "Virtual Defense," *Foreign Affairs*, Vol. 80, No. 3 (May/June, 2001), pp. 98-112.

網址，但是不清楚是否由國家所資助，莫斯科方面也否認其與此等攻擊事件有任何關係，也不願對於防制攻擊做出合作。

整起事件中，駭客透過建立「後門」(back doors)以滲透進入系統竊取資料，儘管經過調查，美國政府仍無法得知誰是攻擊的幕後推手。「Moonlight Maze」攻擊讓美國嘗試到失去資訊戰場將會嚴重危害到國家能力。此等攻擊雖不具破壞性，但其所構成的整體效應卻具有危險性，因爲一旦飛彈防禦受到數位攻擊其軟體或是基礎設施，將無法發揮其原有的價值功效，對國家安全所造成之影響不容小覷。

## 貳、聯想電腦事件（Lenovo PC）

去年(2004 年)中國聯想集團以 17 億 5000 萬美元買下IBM個人電腦部門，但是美國國務院在今年向聯想集團採購的 1 萬 6000 電腦卻遭受到眾議員的反對，爲回應眾議員擔心採購聯想電腦可能引發「木馬屠城」效應。[65]美國眾議院撥款委員會主席伍爾夫(Frank Wolf)指出，此一決定將對國家安全產生嚴重後果，也將危害美國對保密資訊基礎建設的投資。因此，在重重壓力之下國務院只好同意放棄採購這九百台聯想電腦並將其連線到華府及全球外館機密網路的構想。而僅將這些電腦用於非機密性質的工作，以確保國家資訊安全。[66]這個事件也凸顯美、中不管是在政治、經貿或科技等安全領域問題彼此糾纏之深。經濟上雖相互依賴，但是卻也伴隨著相互的不信任。[67]

其實中美之間一直存在這類性質的問題發生，去年(94 年)年底，專研美國網路安全的「系統管理稽核網路安全協會」(Sans Institute)主席帕勒(Alan Paller)在一場研討會上發表論文指稱，美國政府與企業的電腦正遭到駭客有系統、組織性

[65] 白德華，「反聯想 美國國務院向議員低頭」，**中國時報**，民國 95 年 5 月 24 日，A13 版。
[66] 張沛元，「美國務院拒聯想電腦碰機密」，**自由時報**，民國 95 年 5 月 20 日，A7 版。
[67] Steve Lohr, "State Dept. Yields on PC's From China," *New York Times*, May 23, 2006, p. 4.

大規模入侵並竊取機密資料，而透過追蹤攻擊者路徑來源發現，發現極可能來自中共解放軍，但大陸方面則是極力否認。帕勒研究這些攻擊行動後發現，該批駭客不但能神不之鬼不覺自由進出電腦網路系統、且未留下任何蛛絲馬跡，並能在短短三十分鐘內撰寫程式，建立一道供駭客入侵時所使用的「後門」。由於這些駭客行動具有組織、系統性且紀律嚴明，帕勒認爲「除了軍方組織外，目前沒有其他組織能夠作得到。」而整起事件更稍早前，美國國防部承認五角大廈網站遭一個名爲「Titan Rain」的駭客組織攻擊，帕勒表示，由於五角大廈的網路安全管理較爲嚴密，駭客不易取得機密等級文件，但敏感性較小的情報資料極可能已遭竊取。[68]

有上述案例可見得，國家往往會對其關鍵性的基礎設施都會建立起重重保護關卡，但相信隨著資訊科技的不斷進步，對於國家安全的威脅及破壞性將是有增無減，未來難保國家將無法避免面臨關卡失守的窘況發生。關鍵問題就在於：「在網際網路中，沒有人知道你是誰」(On the Internet, No one Knows You're A Dog.)[69]；「網際網路的廣大力量就在於你的指尖」(The immense power of the internet is at your fingertips)。[70]

總結以上資訊科技影響國家安全的案例討論裡頭，我們可以發現，對於資訊科技對於國家安全所可能造成之危害，我們或許可以很容易假設一些可能發生的劇本模式，像是金融市場因爲駭客的侵入竄改交易資料而導致國家經濟崩解；或甚至是恐怖份子利用駭客技術影響飛航系統或更改航線造成飛機發生事故。但儘管如此，我們還是很難去評估這些假設劇本在真實世界中發生的可能性。因爲有太多的因素必須被考量到，包括資訊科技的脆弱性或是它們被運用的方式，甚至

[68] 林克倫，「美指共軍駭客竊密」，**中國時報**，民國 94 年 12 月 14 日，A14 版。
[69] Andrew L. Shapiro, "The Internet," *Foreign Policy*, ll5 (Summer, l999), pp. 17-19.
[70] John J. Stanton, , "Terror in Cyberspace," *The American Behavioral Scientist*, Vol. 45, No. 6 (February, 2002), pp. 1017.

是有能力發動攻擊的人們存在什麼樣的動機及機會去執行。[71]

雖然到目前為止，有關使用駭客入侵工具和技術造成像是生命損失等重大傷害的網路恐怖主義，是否會對國家政策方面造成影響的結論極少，因為一直沒有符合這些標準的事件報告。也依然沒有任何研究說明，何以網頁的竄改會被視為未來可能發生利用電子交易竊取財富；或是關閉水電供應等事情會發生。[72]許多的例子不過只能反映出，一旦網路恐怖主義的威脅與一般駭客入侵威脅結合後，將對有關國家和國際層級的網際防禦之政策決定造成影響。[73]「我愛你」病毒或「梅莉莎」(Melissa)病毒在繁殖 100 倍之後即可能迅速提升為國家安全的危機。[74]甚至在最極端的狀況下，潛在的敵人或敵對勢力將可能對網路系統發動大規模奇襲，藉由此類「電子珍珠港事件」(Electronic Pearl Harbor)的網路突襲，同時散播不實訊息，以快速造成大規模的紊亂，瓦解社會秩序，以為其後續的行動或軍事攻擊創造有利條件。[75]

乍看之下，雖然資訊科技確切影響國家安全的案例不多，但是在此有個疑問，就是國家若對資訊攻擊的案例做出強烈的反應或是事件報告是明確之舉的嗎？因為這麼做可能意味著這類的攻擊行動已經擊中國家的神經命脈，且傷重到無法對危機做出減低利益遭受到損害的行動。所以反過來看，資訊攻擊的問題只會發生在那些疏於維護系統安全的國家，國家不可以因為這樣的事件發生就太過改變改變其外交或軍事態勢，否則將會讓潛在敵人反而因此受到更多鼓舞，因為他們可以藉此影響而獲得到任何政治上的收穫。[76]

---

[71] Dorothy E. Denning, *Information Warfare and Security*, (New York: ACM Press, 1999), p. 19.
[72] Thomas E. Copeland ed., *The Information Revolution and National Security*, (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2000), p. 98.
[73] John Arquilla and David Ronfeldt eds.，楊永生譯，**網路及網路戰**（台北：國防部史政編譯局，民國 92 年)，頁 356。
[74] Arnaud de Borchgrave (ed.)., *Cyber threats and information security: meeting the 21st century challenge* (Washington, D.C.: CSIS Press, 2001), Executive Summary XIX.
[75] 國家安全會議，**2006 年國家安全報告**，(台灣：中華民國總統府，2006 年 5 月 20 日)，頁 76。
[76] Libicki, Martin C, *Defending cyberspace, and other metaphors* (Honolulu, Hawaii: University Press of the Pacific, 2002), p. 54.

舉例來說，網際網路最大搜尋家Google去年夏天所推出的Google Earth時，強調以高解析度人造衛星圖像做爲教學和辨識方向的有效工具，但是卻引起多個國家的安全顧慮。因爲Google Earth對許多國家的重要軍事設施和政治建築提供詳細圖像，擔心嚴重危害到國家安全。但是美國政府和民間專家則是基本上認爲，單單把Google Earth視爲安全威脅無疑是庸人自擾，因爲它所提供的人造衛星圖像並非自有，而也是來自一般人都可去購買到的圖像公司。[77]因此對於資訊科技究竟影響國家安全的承認與否，或許根據各國各自的考量而會出現不同的評估狀況產生。

再以 2001 年 911 恐怖攻擊事件爲例，儘管美國軍力獨霸全球，但在錯失資訊情報之下，而導致華府經濟與軍事命脈遭受重創，此例也說明未來戰爭的可能情況：也就是疏漏了資訊防衛，軍事大國也不見得穩居上風；相對地，若能攻擊對方資訊要穴[78]，居於弱勢的一方乃可運用不對稱優勢扭轉劣勢。由此可知在資訊社會裡面，擁有能攻能守的資訊戰力，不但是大國的重要權力，更是小國最佳的防衛策略，因爲以小博大是可能的。[79]

總結以上，也就是資訊科技與國家安全之間問題的重重複雜性，所以在處理上必須更爲小心謹慎，即使「電子珍珠港事件」雖尚未真實呈現在現今世界，但不可不防其在未來可能形成之威脅。

## 第四節 資訊科技協助國家安全之可能擬議

早在資訊社會形成之前，資訊的流動以及科技就扮演著維持國家安全及穩

[77] 尹德翰，「Google Earth『圖』增困擾？」，**中國時報**，民國 94 年 12 月 22 日，A14 版。
[78] 所謂的要穴，是指敵人的資訊系統、指揮中樞及力量重心。
[79] 國家實驗研究院科技政策研究與資訊中心編，**94 年度資通安全分析專論彙編** (臺北市：國研院科技政策中心，民 94)：頁 138。

定的重要角色。[80]今日的大國在民主與經濟上的整合，將會因爲資訊革命之故，而使得維和作用持續增強下去。對資訊科技的需求與資訊科技的效果，將會激發強國融入核心集團，使得強國間的多極關係將以合作、共同利害關係、與相容性目標爲其特性。[81]全球日益增加的資訊通路以及相互分享，將鼓勵各國共同坐下來面對那些可能來自具敵意之網際網路使用者威脅。一個密佈全球的網路體系亦能使不懷好意的網路行爲者，能透過幾千哩外的電腦系統從事不法勾當，因而危害到國家安全。網際網路可以以光速姿態跨越國界，因此要判斷網際網路的來源並不容易。爲提升國家安全，必須建立一套國際合作體系，以提升資源分享、降低網路弱點、並嚇阻不懷好意的網路行爲者。[82]

## 壹、資訊維和之作為

資訊科技終究是一個可抵銷浮現威脅之力量，且是避免以及解決衝突的最有效益手段。資訊科技透過更開放式的系統將更能促進和平，像是 1979 年埃及與以色列之間的西奈協定(Sinai agreement)，就是利用感應系統來監測兩邊可能的潛在攻擊，進而達成維持和平之作用。[83]

「資訊維和」不是運用資訊科技來支援傳統軍事維和或人道援助之軍事行動；而是發展與使用傳統心理作戰，是置焦點於操縱認知與施以戰略欺騙，或是做爲影響媒體或準軍事行動之秘密媒介。「資訊維和」主動運用資訊與資訊科技以搜整對於特定目標之情資，而達成政策目標。有三個要素：(1)情報，以提供有用可行動之資訊；(2)資訊科技，以提供工具，使接受者可以進入國際資訊且

[80] Lynne Rudasill and Jessica Moyer, "Cyber-security, cyber-attack, and the development of governmental response: the librarian's view," *New Library World*, 105, (July/August, 2004), p. 248.
[81] Zalmay M. Khalilzad, John P. White，王振坤、高一中譯，**戰爭中資訊角色的變化(上)** (台北：國防部史政編譯局，民國 90 年)，頁 56-57。
[82] U.S. Government, *The National Strategy to Secure Cyberspace* (Washington D.C., Feb, 2003), p. 4.
[83] Martin C. Libicki, "Information War, Information Peace," *Journal of International Affairs*, Vol. 51, No.2 (Spring, 1998), p. 423.

有能力與其他人溝通；(3)電子國土防衛，以遏阻資訊戰之攻擊。[84]因此，「資訊維和」在發揮情報最大效用之前提下，需要有全國性之資訊戰略及國家資訊架構之精緻發展，才能充分整合全國性資訊結構。[85]

有鑑於全球安全的本質受到資訊科技影響之所及，犯罪型態更容易跨國間擴散，再加上敵對國家之意圖等要素影響，因此需要將國家性的安全政策，諸如政治、軍事、執法、情報單位等作一整合，並建立起全球性之資訊架構相互分享，努力進行協同一致作爲，才得已充分發展資訊科技維和之作爲。

## 貳、資訊科技與國家安全之合作方案

爲了防範網際網路上的惡意作爲，不論是來自犯罪個人、國家行爲者或恐部分子，都是必須加以防範的對象。而爲了因應每一次的攻擊，也都必須做好支援國家重要國防及情報系統必須具有的高度安全性，同時與他國政府充分密切合作也是相當必要的，以進一步確保全球經濟及全球市場之運作，可透過以下幾點作爲：[86]

### 一、加強有關網路安全之反情報工作

建立一套「安全反應系統」(security response system)，以尋求發展對於網路事件辨識及反應的更多合作關係。[87]在此層級中，政府與企業也被要求分享資訊以提供攻擊的預警。調查局與情報單位也必須擁有堅強之反情報能力，以反制一切針對國家團體所進行的網路情蒐活動，此一作爲必須包含對敵人利用網路作爲間諜手段之相關能力與企圖，進行更深入的了解。[88]

---

[84] 汪毓瑋，**新安全威脅下之國家情報工作研究** (台北：遠景基金會，2003 年)，頁 399。
[85] 汪毓瑋，**新安全威脅下之國家情報工作研究** (台北：遠景基金會，2003 年)，頁 399。
[86] U.S. Government, *The National Strategy to Secure Cyberspace* (Washington D. C., Feb, 2003), p. 49-52.
[87] Lynne Rudasill and Jessica Moyer, "Cyber-security, cyber-attack, and the development of governmental response: the librarian's view," *New Library World*, 105, (July/August, 2004), p. 252.
[88] U.S. Government, *The National Strategy to Secure Cyberspace* (Washington D.C., Feb, 2003), p. 50.

## 二、提升找出網路攻擊源頭與預防的能力

提高法律執行的力量來防止或從事攻擊。情報單位、國防部及執法部門必須改進國家快速找出威脅性攻擊來源之能力，俾採取適時而有效之反應。依據「國家安全戰略」，此類作爲尚包括發展各種能力，以預防重要系統或基礎建設遭到攻擊。[89]這部分的策略也包括使用數位控制系統以及資訊探測系統，以及運用心的技術減低軟體部分的脆弱性。[90]

## 三、安全機構加強協調如何因應網路攻擊

國家必須就資訊科技安全的維護增強安全意識的訓練計畫，就像歐盟實施的「e-Europe」計畫所提出對於電腦安全的一種全面性公眾意識。除此之外，也必須加強執法、國家安全及國防機構等與網路攻擊及間諜活動相關單位之協調，確保適時將犯罪活動資訊通報各單位，[91]以增加現存訓練計畫的效率。

## 四、透過國際合作發展安全網路並建立預防機制

大多數的網路攻擊皆是由海外的系統發動或傳送，穿越數個國界，因此需要國際性的調查合作來加以遏阻。支援重要經濟與安全作業之全球網路系統，必須具備安全性及可靠度，因此需透過國際共同合作，在國際上培養預警通訊協定和網路發展，[92]以提高各界之知覺、推廣安全標準，發展更安全的網際網絡來共同維護網路安全之目標。

---

[89] U.S. Government, *The National Strategy to Secure Cyberspace* (Washington D.C., Feb, 2003), p. 50.
[90] Lynne Rudasill and Jessica Moyer, "Cyber-security, cyber-attack, and the development of governmental response: the librarian's view," *New Library World*, 105, (July/August, 2004), p. 252.
[91] U.S. Government, *The National Strategy to Secure Cyberspace* (Washington D.C., Feb, 2003), p. 50.
[92] Lynne Rudasill and Jessica Moyer, "Cyber-security, cyber-attack, and the development of governmental response: the librarian's view," *New Library World*, 105, (July/August, 2004), p. 252.

國家除了扮演好資訊戰的防衛角色，更必須扮演好確保資訊安全以負擔起國家安全之、經濟安全公眾安全、以及法律及秩序等重責大任。[93]資訊科技可以說既是一項迫切的危機，更也是一個重要轉機。如何運用資訊科技進步的成效，發揮自由主義所提倡的功能整合及國際合作之精神，相信定能爲資訊科技及國家安全合作研擬出最佳合作方案。

[93] Dorothy E. Denning, *Information Warfare and Security*, (New York: ACM Press, 1999), p. 397.

## 小結

資訊科技既可以是經濟或是技術的關鍵，更可以是軍事力量的關鍵。資訊系統的脆弱性使得有心破壞份子得以有機可乘，且資訊結合戰爭作戰之運用問題也都必需格外受到國家安全的重視。部分原因固然是因爲資訊科技會影響到國家關鍵基礎設施，但並非因爲它所造成的災難性攻擊不可避免，而是我們必須對於不確定的未來有所防備。[94]

雖到目前爲止，純粹藉由網際網路癱瘓一個國家以致於國家安全受到嚴重損害的例子，尚未發生在這個世界上，但並不代表國家對此一威脅就可以加以忽視。現今世上強國像是美國，均針對資訊科技以及關鍵性基礎設施做出相關保護及防治措施，我國日前所公布的國家安全報告書中，亦針對資訊科技安全的維護設有專章討論。可見得資訊科技的進步使得國家在對其依賴性大增之後，所產生的副作用，也就是脆弱度問題，是目前世界各國都紛紛關注的新安全威脅，也正是一種非傳統性的安全問題。

傳統安全重視政治及軍事的力量，尤其是軍事上的力量包括傳統殺傷型武器、飛彈導彈等各項物理性質的武器；時至今日資訊科技雖能透過網際網路無遠弗屆的穿透影響力發揮更多破壞國家安全之作用，但並不就因此意味著其可以完全取代傳統的軍事力量。資訊科技之所以愈發重要，就在於它與軍事科技的相結合而發揮出更大屈服之功效。

就目前世界上所發生的案例而言，光靠資訊科技等網路駭客、病毒並不足以徹底毀滅另一個國家或是造成國家安全的嚴重損害，透過資訊科技或許可以比起以往更容易竊取對方資訊或是侵入其系統，但國家往往對其關鍵性的基礎設施都會建立起重重保護關卡，所以真正要危害到國家安全的重大案例目前尚未呈現，

[94] Dorothy E. Denning, *Information Warfare and Security*, (New York: ACM Press, 1999), p. 19.

但相信隨著資訊科技的不斷進步，對於國家安全的威脅及破壞性將是有增無減。

因此本章節便是針對資訊科技在國家安全中的重要戰略性之地位，以及其所產生之非傳統國家安全之威脅，像是透過網路駭客、病毒，甚至是應用在軍事事務革新上的資訊戰等新觀念，在研擬出國家與資訊科技之間合作的可能擬議，相信是對於未來資訊科技與國家安全之間調和的一項最佳模擬方案。