# 第二章 資訊科技與安全

*一般認爲在資訊時代，網際網路可以減輕窮困、強化個人、改革商務以及擴展民主—只要政府不干涉的話。但是，再想想，如果沒有謹慎的規範，資訊科技可能會摧毀低收入社群、消滅個人隱私，而高壓政權也會利用網際網路來增加政府對人民的權力。*

By Andrew L. Shapiro[1]

## 壹、「資訊科技」—雙面刃的力量

資訊及資訊科技其本身的性質，基本上是中立而沒有特殊的價值取向來引導其往好的方向或是壞的方向，而是經由人們所賦予才有所謂的價值傾向產生。[2]網際網路雖有助於減緩全球貧窮、促進商業革命化、以及散播民主的曙光到世界遠方的角落；但是如果缺乏謹慎的規範，也可能侵犯到個人隱私。資訊科技的進步，也使得全球的人民有機會去參與整個公共的對話，但由於網路是屬於無主性質的，因此在沒有人掌控之下，網際網路扮演了某種角色的開放及公共效用。[3]但我們也必須清楚的了解到，資訊科技在促進民主的同時也有可能利用過濾資訊的方式而抑制民主。

「資訊科技」是全球化的重要媒介，此乃是因爲科技的創新與全球化相輔相成，透過科技整合(像是利用網際網路、全球金融體系及商業往來的擴展)而產生

[1] Andrew L. Shapiro, "The Internet," *Foreign Policy*, ll5 (Summe, l999), p. 14.
[2] James N. Rosenau, , J. P. Singh (eds.), *Information technologies and global politics: the changing scope of power and governance*. (Albany, N.Y.: State University of New York Press, 2002), p. 275.
[3] Andrew L. Shapiro, "The Internet," *Foreign Policy*, ll5 (Summer, l999), pp. l4-22.

互賴關係，[4]而且根據經濟學人(The Economist)所描述的全球化根基，即在於成本大幅降低的電信設施、拜微晶片、人造衛星、光纖及網際網路的發明，上述這些資訊科技雖能夠把整個世界編織的更爲緊密，[5]但卻也使得國家相對的更爲不安全，因爲這些同樣容易成爲恐怖份子運用來攻擊的工具。「資訊科技」的開放性質，使得任何人只要擁有簡單的上網設備，就可以上網取得其所需之訊息；而隨著網際網路和其他資訊基礎建設變得更加複雜龐大且相互依賴的同時，未經許可入侵電腦系統及網路的情形卻越發常見與嚴重。在網際網路的使用背後，或許正潛伏存在一個未知且成在成型中的威脅，對於組織中連接公開網路的系統而言，安全化工作之意義也是日益重大。

「水能載舟，亦能覆舟」，就其中一方面來說，「資訊科技」在國家經濟建設、國家防衛和社會發展中的作用日益增強，位居關鍵性因素；但另一方面，「資訊科技」往往容易被國內外的敵對勢力使用而危及到國家安全，使得國家利益遭受損害，甚至恐怖主義可以藉由「資訊科技」加以散播，而使得恐怖活動變得更加駭人聽聞。所以當私人所擁有的資產時被納入範疇更廣的國家安全事務之中考量時，資訊科技尤其是網際網路部分，所構成的挑戰尤其顯得棘手。[6]經由網際網路的連結，來自世界各地的駭客得以入侵、密碼偷取、或是發動阻斷服務攻擊(Denial of Service, DoS)[7]等網路攻擊事件。由於其特性使然，網際網路在現今及未來都可能是種不穩定、不成熟與不安全的科技，很容易受到利用與濫用。[8]由此可見，即使「資訊科技」本身的發展並不是出於人爲的惡意，但仍會產生有一

---

[4] 翁明賢著，**全球化時代的國家安全** (臺北縣新店市：創世文化出版：聯豐書報社總經銷，2003)，頁 5-6、177。

[5] 佛萊曼(Friedman, Thomas L.)著，蔡繼光譯，**了解全球化：凌志汽車與橄欖樹** (臺北：聯經，2000 年)，頁 7-9。

[6] Arnaud de Borchgrave, 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)

[7] 「阻斷服務(Dos)攻擊」，是一種以「破壞」爲目的之攻擊方式，這種攻擊使得電腦主機或網路系統無法提供服務，大部分Dos攻擊目標爲網路頻寬或電腦主機的連線資源，網路系統因而充斥著攻擊流量或要求連線服務的流量。可參考馬淑貞著，「以網路流量資料探勘協助進行阻斷服務攻擊偵測與防禦之研究」，國立中山大學資訊管理學系在職專班，碩士論文，2005 年。

[8] Arnaud de Borchgrave, 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. 1.

定程度的負面影響存在。[9]

## 貳、「資訊科技」安全的定義

「資訊科技」安全的歷史淵源，相較於和政治安全、軍事安全、經濟安全等國家安全之相關概念而言，顯而是一個較爲嶄新的概念。國家首度將「資訊科技能力」納入國家安全的想法，則首見於 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。[10]在現今全球化的過程之中，世界各國也紛紛注意到發展資訊科技的重要性，更把其當作是捍衛國家利益、提高綜合國力、以及參與全球化競爭的重要手段。

「資訊科技」安全所所涵蓋的面將比「網際網路」安全的範圍更爲廣泛，其本體論知識將同時包含:「密碼學、電腦系統安全、網路與通訊安全」等議題。「資訊科技」安全，狹義的理解主要是指資訊科技領域的安全，包括單一系統安全的管理與維護；以及電腦與電腦相互之間，因爲資訊交換所產生的網路通訊及系統安全的管理與維護。[11]這個定義是將「資訊科技」做爲一個特定的系統，以該系統自身的安全狀態來決定資訊科技安全的內涵。

而廣義的「資訊科技」安全則主要指的是綜合性的資訊安全，包括經濟、政治、科技、軍事、思想文化、社會穩定等各個領域的安全。[12]這個定義指明了「資訊科技」是國家安全的重要組成部分，「資訊科技」直接影響著政治安全、軍事安全、經濟安全、和文化安全等國家安全的其他要素；同時也說明「資訊科技」安全的水平取決於本國的資訊科技實力及潛力，這是國家安全的基礎。

---

[9] 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 220。
[10] Thomas E. Copeland (ed.), *The information revolution and national security*. (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2000), p.119.
[11] 胡毓忠著，「企業網路安全新方向：資訊安全的因應與突破」，2003 年發表於「鐵衛神補—網路安全之運用」研討會。
[12] 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 17。

「資訊科技」安全的保障，根本上而言即是一個資訊安全技術與管理以及發展能力水平之問題[13]，以及對於影響國家利益及國家安全的控管。爲了保障國家安全，各國政府無不投入大量資金加速國家的資訊基礎建設(National Information Infrastructure, NII)。像是 1998 年 5 月美國總統柯林頓發佈第 63 號總統決策令(Presidential Decision Directive 63, PDD-63)，要求動員一切力量保護美國「關鍵性電腦基礎設施」(Critical Cyber-based Infrastructures)，以使美國資訊系統免遭攻擊，確保國家的資訊安全。[14]美國在遭受到 911 恐怖攻擊之後，小布希更頒佈「確保安全網路空間的國家戰略」(The National Strategy to Secure Cyberspace)以維護國家安全，均代表了「資訊科技」安全的保障受到日益重視。

## 參、「資訊科技」安全的重要性

「資訊科技」對於國家安全上有著重大的意義存在。[15]一個國家如果能夠擁有光纖網路或是衛星通訊器材，就可以做爲外交及國防方面的政策工具。光纖設備有助於增強指揮與控制能力，因此即使在冷戰結束之後美國政府仍盡力阻止業者將相關技術售予俄國。[16]由此可見，「資訊科技」安全不但是國家安全的重要組成部分，也是國家安全的技術基礎。全球化的發展則是進一步突顯了「資訊科技」的重要性，其已成爲決定國家安全總體態勢的決定性指標。[17]

學者Dorothy E. Denning在其書”*Information Warfare and Security*”中提到：「有心人士只要利用資訊科技技術搭配使用鍵盤和滑鼠，就可以進入電腦大肆破壞，造成無預警的動力中斷；或是使得食物供給出問題；甚至是引起股票市

[13] 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 20。
[14] 見U.S. The White House, *Defending America's Cyberspace: National Plan for Information Systems Protection*, Version 1.0, An Invitation to a Dialogue, (Washington D. C.: The White House, 2000)
[15] 有關資訊科技在國家安全中的戰略地位的探討，詳見第四章。
[16] 高德斯坦(Goldstein, Joshua S.)著，歐信宏、胡祖慶譯，**國際關係** (臺北市：雙葉書廊，2004 年)，頁 421。
[17] 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 220。

場經濟的崩塌。」雖然到目前爲止這些災害仍未發生，但我們能必須對於資訊科技的安全關注，因爲即使青少年都可以輕易的透過電腦對美國國防部所掌控的系統進行惡作劇。[18]

1995 年美國中央情報局(Central Intelligence Agency, CIA)和國防部發表的一份共同聲明中提到：「資訊系統以及網際網路的安全，是這十年以來甚至是下一個世紀所面臨的最主要安全挑戰。」[19]而根據美國首先成立的「電腦緊急事件反應小組協調中心」(Computer Emergency Response Team Coordination Centre, CERT/CC)[20]公布的數字顯示，安全事件(Incidents)以及弱點(Vulnerabilities)自從 1998 年以來就一直呈現穩定增加狀態，到了 1999 年時更是急遽性地大幅增長。

2001 年該中心接到的電腦安全事件報告(Incidents reported)[21]有 52,658 件，比起前年 2000 年(21,756 件)成長一倍多；2002 年發生的安全事件爲 82,094 件，是 2000 年的 4 倍；而 2003 年安全事件(137,529 件)更成長爲 2000 年時的 6 倍。根據CERT/CC的統計資訊，自從 1988 年成立以來，共接獲 319,992 件安全事件的回報件數，其呈現逐年上升的趨勢。詳細統計數字如表 2-1：

[18] Dorothy E. Denning, *Information Warfare and Security*. (New York: ACM Press, 1999), Preface.
[19] Rosenau, James N., J. P. Singh (eds.), *Information technologies and global politics: the changing scope of power and governance*. (Albany, N.Y.: State University of New York Press, 2002), p. 115.
[20] CERT/CC，是一個由聯邦政府提供資金的機構，位於匹茲堡的卡內基梅隆大學(Carnegie Mellon University )內。創立於 1988 年，是現有最早成立的安全應變小組。它的主要職能是對軟體中的安全漏洞提供咨詢，對病毒和蠕蟲的爆發提供警報，向電腦用戶提供保護電腦系統安全的技巧以及在處理電腦安全事故的行動中進行協調。根據 CERT 的定義，任何屬於電腦安全有關的事件，包括大規模的病毒爆發，或者其他的小問題，都屬於電腦安全事故。可參考：艾倫 (Allen, Julia H.) 著，孫宇安譯，**CERT網路與系統安全實務** (臺北市：臺灣培生教育，2002)
[21] 事件(Incident)，是描述一個或多個有關連性的攻擊事件之資料集合。多個攻擊事件之間的關連性也許跟攻擊者、攻擊方式、目的、地點或是時間有關。

表 2-1 電腦安全事故及弱點統計數量表

- 安全事件報告(**Incidents reported**)

**1988-1999**

| 年(Year) | 1988 | 1989 | 1990 | 1991 | 1992 | 1993 | 1994 | 1995 | 1996 | 1997 | 1998 | 1999 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Incidents | 6 | 132 | 252 | 406 | 773 | 1,334 | 2,340 | 2,412 | 2,573 | 2,134 | 3,734 | 9,859 |

**2000-2003**

| 年(Year) | 2000 | 2001 | 2002 | 2003 |
|---|---|---|---|---|
| Incidents | 21,756 | 52,658 | 82,094 | 137,529 |

安全事故總計 **(1988-2003)**: **319,992**

- **弱點數量報告(Vulnerabilities reported)**

**1995-2006**

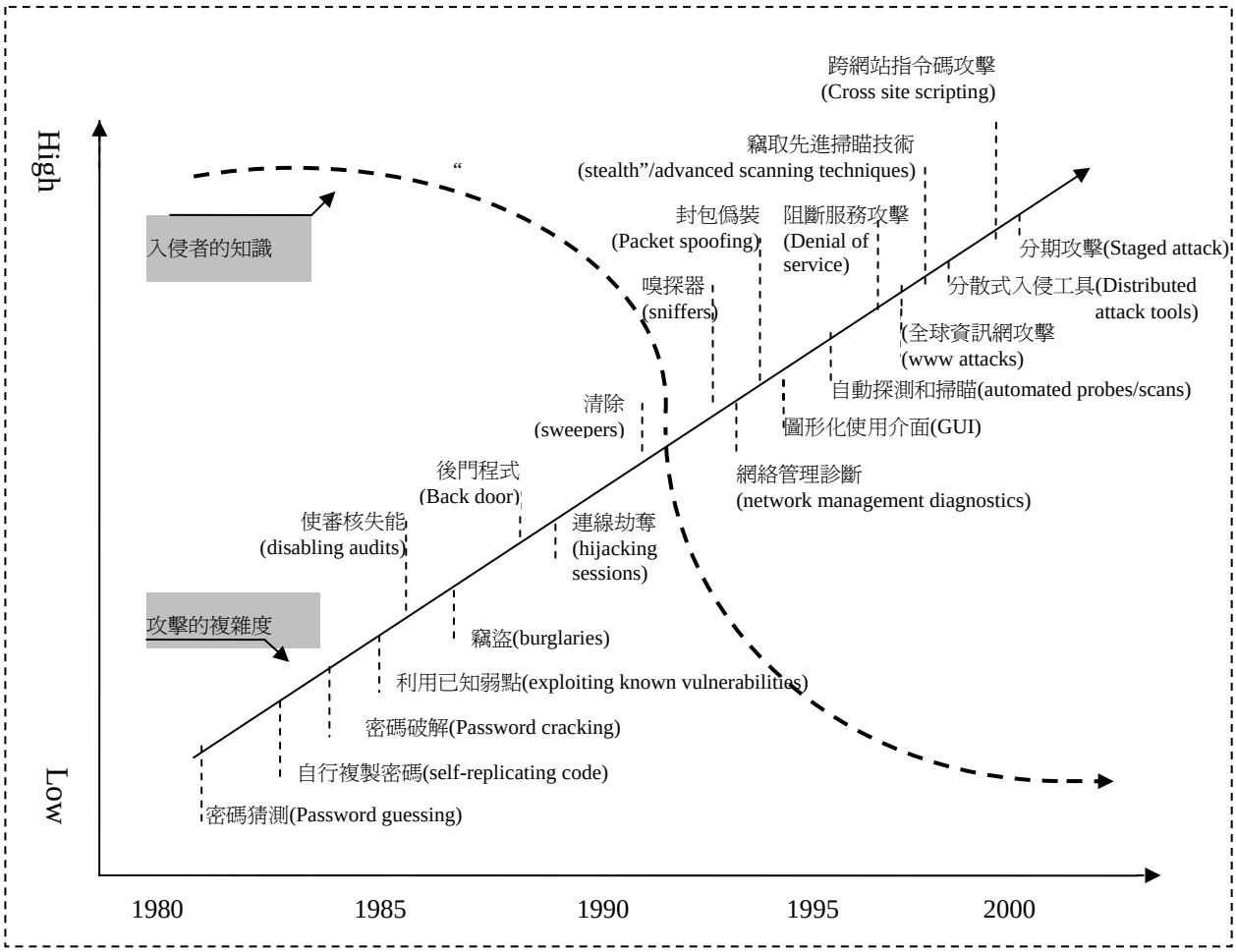
| Year | 1995 | 1996 | 1997 | 1998 | 1999 | 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | Q1,2006 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Vulnerabilities | 171 | 345 | 311 | 262 | 417 | 1,090 | 2,437 | 4,129 | 3,784 | 3,780 | 5,990 | 1,597 |

弱點統計報告總計 (1995-Q1,2006): **24,313**

資料來源：CERT/CC網站 http://www.cert.org/stats/cert_stats.html

CERT/CC 公布的數字顯示，2005 年該中心接到的電腦安全事故報告中指出發現弱點數爲 5,990 個，是 2000 年發現弱點數 1,090 的將近 6 倍，由此我們可得知，弱點數量與安全事件是成正比的。安全事故報告數目的增加，代表著廣泛應用的軟體所受到的攻擊數量增加。現今資訊科技時代下人們的安全意識雖逐漸增強，也越來越多人開始注意網際網路的安全問題。但是相較於入侵危害資訊科技安全所需要的技術知識而言，則是逐漸降低當中(也就是「Less knowledge Required to Attack」)，在這裡可參考圖 2-1。

**圖 2-1 攻擊的複雜程度 v.s 入侵者具備的知識技術**




資料來源：艾倫(Allen, Julia H.)著，孫宇安譯，**CERT 網路與系統安全實務** (臺北市：臺灣培生教育，2002)

如圖 2-2 所描述的，在 1980 年代入侵者都是一些具有高階技術，或是有能力自己創造出入侵系統方法的電腦專家級人物。但是到了 2000 年，由於用來攻擊網路的工具及程式較以往容易取得，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。且當有經驗的入侵者經由更多更精密的攻擊方式以證明自己能力時，相對地也給予新手入侵者只要利用比較少的知識複製並利用這些方法，就可以展開對於資訊科技安全的攻擊。[22]

[22] 艾倫(Allen, Julia H.)著，孫宇安譯，**CERT網路與系統安全實務** (臺北市：臺灣培生教育，2002)，頁 1-3.

此外根據Computer Security Institute在 2004 年所進行的電腦系統與安全調查報告中指出，在 456 家受訪企業中，有 53%的企業表示組織內的電腦系統曾發生未經授權使用的情形(1999-2004 年的平均值爲 61%)，且其中 269 家企業回報因網路安全所造成的金錢損失高達 1 億 4 千多萬美元。[23]上述的統計資料意味著現今的網際網路環境之中，資訊科技安全面臨著許多重大的考驗，攻擊方法所造成的危害及影響範圍正在逐漸增加當中。因此我們必須針對資訊科技的背景作一初步瞭解，並對於資訊科技所要維護的具體安全目標有更進一步的認識，以透過現有機制去加以維護資訊科技的安全。

## 第一節 資訊科技的演變

現今世界上發生的新科技革命，以資訊和網路科技爲代表，正以龐大力量推進社會生產力發展並改變了人類社會面貌。首先，微電子和軟體科技的快速發展，導致晶片、電腦的效能和價格相較之下的比值，持續以幾何速度增加，讓數位化資訊得以被大規模、高效率的方式加以收集、儲存和處理。再者，受到三項科技的推動—微電子、軟體和雷射，電信網路技術得以從模擬走向數位，從低速晉升高速，更從單一媒體形式進步至多媒體。特別值得一提的是，網際網路和IP通訊協定技術的應用，造成電信網路技術另一次的躍進，讓新世代的公共網路系統慢慢浮現。第三，電腦、電信和媒體科技正在經歷彼此交錯應用和整合的過程，將資訊和網路科技的發展，推向另一個嶄新的時代。[24]使得無論是國家或者是非國家的行爲者都深受影響。

---

[23] L. A. Gordon, M. P. Loeb, W. Lucyshyn,, R. Richardson, *2004 CSI/FBI Computer Crime and Security Survey* (Computer Security Institute, June, 2004) <http://www.gocsi.com/press/20040609.jhtml.>

[24] 龍安志(Laurence J. Brahm)編著，劉世平譯，**中國的世紀** (臺北市：商周出版：城邦文化發行，2002 年)，頁 411-412。

資訊傳播科技是世界改變的引擎(engine)，而知識爲推動革命的燃料(fuel)，兩者的相互作用造就了資訊時代。[25]拜先進技術所帶來的理念、資訊及圖像之所賜，人類訊息傳達方式與以往截然不同，「網際網路」(Internet)所帶來的未來數位化[26]通訊模式，使得資訊的傳達幾乎不需耗費任何成本，距離遠近也無關緊要，在任何地方都可以立即取得。[27]

但是「資訊科技」的革命，並非只是侷限於更低廉的通信或是更快速的電腦，「資訊科技」的革命是從各種角度影響全球的經濟與政治，包括在資訊蒐集、分析、傳播等方面。當前「資訊科技」革命時代基本科技趨勢，可以用三句話來概括表達：「即能力增加、成本降低及連結性增加」。[28]二十世紀以來，資訊科技的提升已讓人無法輕忽其所產生變化的效果。

未來的人們將生活在資訊密集的國際社會之中，國際關係也因此產生巨大變化。科技進步不僅大幅改變行爲者之間的力量對比，通訊科技的進步與電腦化使得人們在政治、經濟與文化的生活觸角延伸到世界的每個角落，資訊科技革命已經成爲「全球化」的主要動力，[29]而這些都是過去所做不到的。

自國際體系出現以來到一百五十年前，大多數時候利用快馬及船舶傳遞手寫信息是最迅捷的聯絡方式，而目前的資訊已經可以經由各種媒介傳遞，[30]若是要瞭解資訊革命的起源，時間更可追溯至第二次世界大戰期間，1946 年當時英國解碼人員發明了第一部電腦—「巨像」(Colossus)。如今電腦的運算速度及容量

---

[25] Alvin Toffler, “The Accelerative Thrust,” *Future Shock* (London: Pan Books, 1970), pp. 25-31.

[26] 所謂的數位化，就是把聲音、圖像、數字或文字轉成 0 與 1 的形式，透過電子通信系統傳輸到另一端，再由彼端接收器解碼，重新組合，恢復成接近原有的狀態。可參考佛萊曼(Friedman, Thomas L.)著，蔡繼光譯，**了解全球化：凌志汽車與橄欖樹** (臺北：聯經，2000 年)，頁 66-68。

[27] France Cairncross, *The death of distance : how the communication revolution will change our lives*. (Boston, Mass.: Harvard Business School Press, 1997), p. 89.

[28] 薄科維茨(Bruce D. Berkowitz)、戈德曼(Goodman, Allan E.)著，王振坤、高一中譯，**最佳的事實：資訊時代的情報** (臺北市：國防部史政編譯局，2001 年)，頁 16。

[29] 高德斯坦(Joshua S. Goldstein)著，歐信宏、胡祖慶譯，**國際關係** (臺北市：雙葉書廊，2004 年)，頁 14。

[30] 高德斯坦(Joshua S. Goldstein)著，歐信宏、胡祖慶譯，**國際關係** (臺北市：雙葉書廊，2004 年)，頁 418。

的大量增加而成本卻大幅的降低，已非昔日「巨象」可堪比擬，電腦已經成爲推動資訊科技革命的主要力量，並成國家資訊發展的重要基石。

資訊科技的演變階段大致歷經以下三個階段：[31]

- **第一階段**爲 1837-1963 年之電報與無線電。當時大型公司(通信獨佔公司)掌控了如何建構資訊來源的權力。各種系統體積龐大，而且是中央系統的型態。
- **第二階段**始於 1964 時 IBM360 商用電腦成功研發，大型公司(如銀行與汽車製造商)因需要特製通信系統與特定服務，相關供應商即可發揮影響力。這個階段於 1990 結束。
- **第三階段**始於 1991 年，由於網際網路民營化，故可稱爲「分散」(distributed)年代。政府與企業掌控的科技因經濟界與其他領域分別研製而降低了成本，這個重大改變還有許多人未掌握。而非政府組織、組織犯罪、以及恐怖分子具備優異能力，能將各種訊息發送至全球，挑戰政府的權威，因此處於新的世界政治環境之中，許多老舊的規範似乎不再適用。

資訊科技革命所帶來的成就及其結果，雖是不平均的發展但仍維持在持續進行之中，其核心特質之一即是不斷地創新與變遷。[32]而到了二十世紀末的資訊革命其最重要的課題即是電腦傳播，尤其是以「網際網路」最爲顯著，不但將人類帶入網際網路世界，也成爲維持國家運作之資訊建設中最重要的關鍵。

「網際網路」此一系統的最初設計目的在於提供科學家分享彼此非機密性研究資訊，且不認爲這些科學家們會對網路進行破壞。時至今日，這套網際網路系統已經連結上數百萬的其他電腦網路，以協助國家運作大部分的重要服務，連貫國家重要基礎建設之運作。網際網路既是這些功能的神經系統，也是其控制系統之所在。「網路空間」乃是由數以億計相互連節之電腦、伺服器、路由器、轉接

[31] James N. Rosenau, J. P. Singh (eds.), *Information technologies and global politics: the changing scope of power and governance*. (Albany, N.Y.: State University of New York Press, 2002), pp. 53-54.
[32] 陶尼(John Downey)著，江淑琳譯，**科技新城鎮** (臺北縣永和市：韋伯文化，2003)，頁 87。

器，以及光纖電纜所共同組成，[33]根據估計，網際網路流量每三年增加 1000 倍，每十年將增加 100 萬倍以上。現今半數美國家庭均已具備上網能力，也就是自從 1998 年以來，上網人口數已增加了 60%，光是在美國國防部內就擁有將近一萬個電腦系統，其中 2000 個電腦系統具備重要的任務功能，而電腦總數則達 150 萬部。[34]也就是這些組件使得國家重要基礎建設得以發揮正常運作功能。因此，網際空間能否充分且安全的運作，對國家經濟及安全至關重要。

「網際網路」的主要定義是指：透過「傳輸控制協定／網際協定」(Transmission Control/Internet Protocol, TCP/IP)而連結在一起的所有電腦。在網際網路上由某部電腦傳送至另一部電腦的資料，是被分割成許多小型的資訊封包(packet)，內含網址資訊及完整訊息的一部份。這些封包在網際網路間獨立流動，並在接收端的電腦加以組合。這些資料封包能在複雜的網路間傳送，並以可讀取的格式到達目標，其主要靠的是兩個網路傳輸協定。這兩項傳輸協定分別是：[35]

- **「傳輸控制協定」**(Transmission Control Protocol, TCP)：該傳輸協定將資料分解成訊息包，並確保其可在接收端正確地被重新組合。
- **「網際網路傳輸協定」**(Internet Protocol, IP)：此一協定導引或排定訊息包括在網際網路中的流向。以上這兩個協定通常合併稱爲「傳輸控制協定／網際網路傳輸協定」(TCP/IP)。

「傳輸控制協定／網際協定」起源於一九六０年代，美國國防部及學術界有感於無法及時交換電腦主機之間資料，因此成立一個專案計畫及組織來推動電腦之間資料傳送的技術發展，稱爲「Laboratory's DARAPA[36] contract」與

[33] U.S. The White House, *The National Strategy to Secure Cyberspace*. (Washington D. C.: The White House , 2003), Introduction.
[34] Arnaud de Borchgrave, 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)
[35] U.S. The White House, *The National Strategy to Secure Cyberspace*. (Washington D. C.: The White House , 2003), pp. 29-30.
[36] 「防衛先進研究計畫署」(Defensive Advanced Research Project Agency, DAPRA)

「ARPA/IPTO[37]」。[38] 隨後在一九六九年時由美國的加州大學的一群科學家們，建成了連接史丹佛等四個大學實驗室的第一個世界上採用分組交換技術的計算機網路：先進研究計畫署網路(ARPANET) [39]，便成爲成千電腦網路之全球傳播的基礎。

隨後到了一九七八年，TCP/IP被建議爲電腦交換的良好模式；一九八三年TCP/IP成爲「先進研究計畫署」(ARPANET)上唯一的通訊規範，[40]所有與「先進研究計畫署」(ARPANET)相連結的網路都完全以新式的TCP/IP取代舊式的網路控制協定。從此時開始，互相連接的網路集合群與使用TCP/IP協定以提供大眾使用的網路便被稱爲「網際網路」。

然而，在一九八０年代，「先進研究計畫署」做爲持久性或骨幹性網路的角色地位，已經逐漸被「國家科學基金會」(National Science Foundation)所設立的「超級計算中心網路」(network of supercomputing centers，NSFNET)所取代。[41]發展至今，由「ARPANET」擴展而成的網際網路(Internet)已成爲全世界最大的電腦網路系統，數以萬計次的網路連結上網際網路，[42]其迅速發展以及其不同於以往媒體的特性，使得電腦應用及技術的發展無遠弗屆，爲整個世界及國家帶來革命性的影響。

網際網路的全面性開放及商業利益的行爲，使得人類日常生活已經和資訊科技及網際網路脫離不了關係，[43]「網際網路」已經成爲個人、組織與國家基礎設

---

[37] Advance Research Projects Agency of the Department of Defense(DoD) Information Processing Techniques.

[38] 多奇(Martin Dodge)著，江淑琳譯，**網際空間的圖像** (臺北縣永和市：韋伯文化國際，2005)，頁 3。

[39] 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 23。

[40] 多奇(Martin Dodge)著，江淑琳譯，**網際空間的圖像** (臺北縣永和市：韋伯文化國際，2005)，頁 3。

[41] 史列芬(James Slevin)著，王樂成譯，**網際網路與社會** (臺北市：弘智文化，2002 年)，頁 31-32。

[42] 多奇(Martin Dodge)著，江淑琳譯，**網際空間的圖像** (臺北縣永和市：韋伯文化國際，2005)，頁 3。

[43] 胡毓忠教授，「企業網路安全新方向：資訊安全的因應與突破」，2003 年發表於「鐵衛神補—網路安全之運用」研討會。

施所殷切依賴的系統，此一現象完全不受國界的限制。網際網路已經成爲一種「骨幹中的骨幹」(backbone of backbones)，一種複雜且缺乏明顯範圍的網路系統。[44]

網路的發展隨著個人電腦的普及化和數位技術的突破也不斷得在成長當中，電腦中央處理器運算速度根據「摩爾定律」(Moore's Law )[45]：「IC上可容納的電晶體數目，約每隔 18 個月便會增加一倍，性能也將提升一倍」；網路上網連結的頻率也是不斷倍增。從電腦文書信件處理、到電子化政府甚至是飛彈衛星導航系統，無不仰賴電腦網路系統，資訊科技串連所形成的世界性網絡儼然而生，進而達到「網路地球村」的境界。[46]

從最早的農業革命、工業革命到現今的資訊科技革命以來，資訊科技的不斷進步爲人類帶來的不只是便利性，更消除國與國之間的壁壘，而形成了所謂的「平坦世界」(The World is Flat)出現。抹平世界的力量，隨著大量I BM個人電腦(PC)的崛起以及賦予PC生命的視窗作業系統，使得橫向溝通大幅改善。網景(Netscape)瀏覽器的出現、資訊服務(像是Google革命)助長了個人資料蒐集，增強了個人的力量，個人只要透過無線技術，就可以在任何時間任何地點獲得數字信息。微軟科技長孟迪(Craig J. Mundie)認爲：「連接全球電話網路系統的PC、傳真、視窗系統、撥號數據機的日益普及，自八０年代末、九０年代以來，形成了全球資訊革命肇使的基本平台。」[47]個人拜通訊技術之賜或許將可以與國家處在分庭

---

[44] 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)

[45] 「摩爾定律」，是由英特爾(Intel)名譽董事長摩爾經過長期觀察發現得之。摩爾定律是指一個尺寸相同的晶片上，所容納的電晶體數量，因製程技術的提升，每十八個月會加倍，但售價相同；晶片的容量是以電晶體（Transistor）的數量多寡來計算，電晶體愈多則晶片執行運算的速度愈快，當然，所需要的生產技術愈高明。可參考薄科維茨(Bruce D. Berkowitz)、戈德曼(Goodman, Allan E.)著，王振坤、高一中譯，**最佳的事實：資訊時代的情報** (臺北市：國防部史政編譯局，2001 年)，頁 17。

[46] 彭慧鸞，「資訊時代國際關係理論與實務之研究」，**問題與研究**，第 39 卷第 5 期(民國 89 年 5 月)，頁 1-3。

[47] 佛萊曼(Thomas L.Friedman)著，楊振富、潘勛譯，**世界是平的** (臺北市：雅言文化，2005)，頁 46-51。

抗禮的地位。[48]

藍德(RAND)基金會受委託替美國國家情報委員會(National Intelligence Council)所做的技術預測調查報告認爲在 2015 年之前，生物科技、奈米科技、材料科技與資訊科技對於世界的趨勢會有重大的影響。「資訊科技」的繼續發展趨勢將使現有學科融合形成新學科，並且藉由材料與奈米科技的突破持續獲得幫助，資訊科技已經徹底改革我們的生活[49]，其對於國民經濟和世界經濟的發展有相當大的推進作用，其進步的幅度也正以前所未見之推進力量影響著國際關係。

## 第二節 資訊科技的管理及安全規範

隨著資訊流動的加速，網際網路的連結變的更加複雜，國家結構上的壓力也相對應的增加。[50]當個人電腦取代簡易型終端機(dumb terminals)在桌上的地位，再加上越來越多的個人電腦連接上了網際網路時，電腦的安全問題也就相對增加。光是運用硬體的解決辦法，像是安裝「防火牆」(Firewalls)[51]或是建立「自動稽核日誌」(automating audit logs)都總是無法安全避免遭受到破壞。[52]

在此衍生出兩個中要議題：首先，非國防用途的非機密性系統，儼然已經成爲國家安全中的重要一環；接著，資訊基礎建設的弱點產生，使得遭受網路攻擊的可能性增加。於是若要針對資訊科技的安全維護進行管理，筆者認爲必須從這

[48] 有關國家權力內涵及本質的轉變的討論，請見本文第三章第二節。
[49] Global Trends 2015: A Dialogue About the Future With Non-government Experts (http://www.cia.gov/cia/reports/globaltrends2015/index.html)
[50] James N. Rosenau, J. P. Singh (eds.), *Information technologies and global politics: the changing scope of power and governance*. (Albany, N.Y.: State University of New York Press, 2002), p. 134.
[51] 防火牆常被安置在區域網路連上骨幹網路的門口路由器(Router)之後，用來保護私人網路內的機密資料，以防止駭客破壞(主要防護功能有存取隔離、封包過濾及加值服務等)。參考自：國家實驗研究院科技政策研究與資訊中心編，**資通安全分析專論彙編：94 年度** (臺北市：國研院科技政策中心，民國 94 年)，頁 77。
[52] Thomas R. Peltier, *Information Security Risk Analysis*, (Boca Raton, Fla.: Auerbach, 2001), p. 246.

兩方面進行著手。

## 壹、資訊科技安全的具體目標

「資訊科技」安全維護機制的發展與執行，是每個國家及使用者的責任，所要達成的目標在於發展安全穩固的機制，使資訊科技能夠支援國家當前與未來的需求，這項工作將包含網際網路賴以運作的各種協定，確保導引資料流通的路由器之安全，並執行有效管理作爲。[53]

針對網路犯罪的行爲具有隱匿性、智慧性、普遍性、多樣性與偵察困難等特色[54]，總的來說，「資訊科技」安全的具體主要目標即是要維護：(1)資訊的隱密性(2)資訊的完整性(3)資訊來源的可認證性(4)資訊發送者的不可抵賴性[55]。並且能夠做到準備和預防(Prepare and Prevent)、偵察和反應(Detect and Respond)，以及建立牢固的基礎設施(Build Strong Foundation) [56]。以確保關鍵基礎設施所受到的任何中斷或是控制都對國家利益造成的損害最小。

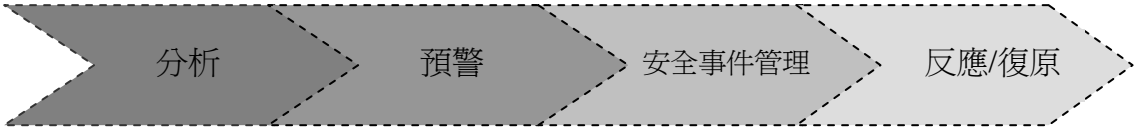
美國所制訂的「確保安全網路空間的國家戰略」內容旨在提高網路安全層次，並補救既有網路弱點。其中更律定出五個國家層級的優先事項，包含：[57]

- 優先事項一：國家網路空間安全反應系統。
- 優先事項二：國家網路空間安全威脅與弱點降低計畫。
- 優先事項三：國家網路空間安全覺知與訓練計畫

[53] U.S. The White House, *The National Strategy to Secure Cyberspace.* (Washington D. C.: The White House , 2003), p. 29.
[54] 行政院研究發展考核委員會編，**網路使用犯罪問題及預防措施之研究** (臺北市：行政院研考會，民國 89 年)，頁 9-12。
[55] 胡毓忠教授，「企業網路安全新方向：資訊安全的因應與突破」，2003 年發表於「鐵衛神補—網路安全之運用」研討會。
[56] 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 440。
[57] U.S. The White House, *The National Strategy to Secure Cyberspace.* (Washington D. C.: The White House , 2003), pp. 2-4.

- 優先事項四：確保政府網路空間的安全
- 優先事項五：國家安全與國際網路空間安全合作

美國對於網路空間的安全反應系統維護，則認為必須做到以下幾點目標組成要素：[58]




- **分析**：提供有關網路攻擊與弱點評估之戰術與戰略層次評估。
- **預警**：a.鼓勵私人企業發展能力以分享健全網路空間的整體觀。b.擴大「網路預警暨資訊網絡」以支援「國土安全部」在網路空間危機管理上的協調者角色。
- **安全事件管理**：國家網路安全事件的管理，在必要的情況下也必須結合其他國際團體的力量。
- **反應/復原**：a.建立可用以協調國家層級之政府/民間的緊急應變計畫程序。b.在聯邦網路系統中運用網路安全持續運作計畫。

## 貳、維護資訊科技安全的現有機制

本論文所提相關資訊安全的維護機制，並不針對較低層級的弱點防制，像防火牆(firewall)、防毒軟體(Anti Virus Software)、入侵偵測系統(Intrusion Detection System)、內容過濾器(Content Filter)、網路流量即時分析等等，都只是針對提供網路存取安全、資料加密、系統安全不同等級的所進行的防護措施，而本文是針對維護國家「資訊科技」安全所做出的資訊立法，以進行網路監管和資訊科技安

[58] U.S. The White House, *The National Strategy to Secure Cyberspace*. (Washington D. C.: The White House , 2003), pp. 21-24.

全的重要制度保障，並以國家資訊安全的基本立法和資訊安全管理兩個層面進行探討，分別提出可供參考和採納的具體立法建議。

有關資訊安全管理方面，在國際上有以下幾個著名的緊急反應組織，皆是國際上公認的專業網絡安全保障機構。

- **電腦緊急事件反應小組暨協調中心**(Computer Emergency Response Team /Coordination Center, CERT/CC)

CERT/CC是一個由美國聯邦政府提供資金的電腦危機的處理機構，，其起源是 1988 年在卡內基梅隆大學(Carnegie-Mellon)大學內製造出來的摩里斯病毒(the Morris Worm)襲擊網際網路事件。國防部先進研究計畫局(DARPA)立即回應，「電腦緊急事件應變小組」(Computer Emergency Response Team, CERT)應運而生[59]。它的主要職能是對軟件中的安全漏洞提供諮詢，對病毒和蠕蟲的爆發提供警報，向計算機用戶提供保證計算機系統安全的技巧以及在處理計算機安全事故的行動中進行協調。後來各國政府也相繼成立自己的CERT組織(在我國則是稱爲TW-CERT。

CERT/CC的功用不只是在控管國際上的安全事件，並且還負責與其他各國的CERT在國際上的合作。像是在亞洲地區，就有由 17 個成員(分屬 13 個經濟體)的CERTs所組成每年定期召開的網路反應協調會議(Internet response coordination conference)[60]。而「亞太地區電腦網路安全事件處理會議」(Asia Pacific Security Incident Response Coordination Conference，APSIRC)，是亞太地區各國電腦網路危機處理共同體(CERT/CSIRT community)之間的關鍵會議，由亞太地區電腦緊急反應小組(APCERT)發起，並由日本電腦網路危機處理中心(JPCERT/CC)擔任主辦國。

[59] Thomas E. Copeland (ed.), *The information revolution and national security*. (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2000), p. 107.
[60] Cameron Ortis, Paul Evans, "The Internet and Asia-Pacific security: old conflicts and new behavior," *The Pacific Review*, Vol. 16, No. 4, (December, 2003), p. 554.

- **事件反應及安全團隊論壇**(Forum of Incident Response and Security Teams，FIRST)

FIRST成立於 1990 年，是第一個最早被認可成爲安全事件反應的全球領導者。其整合了來自政府及團體不同的電腦安全事件反應團隊，負責與資訊界、政府與民間企業的相關組織與專家協調，目的在培養對於安全事件預防的合作協調，及對於安全事件做出快速反應，並且促進成員間資訊的共用。到目前爲止，FIRST擁有超過 170 個成員，散佈於美洲、亞洲、歐洲及大洋洲。[61]現在已經逐漸演變成爲以國家或地區爲單位成員的民間組織，旨在加強國家或者地區之間的網路安全交流。

FIRST 的主要目標是爲參與的組織提供一個相互協作的論壇，促進當前資訊的共享，綜合解決共同關注的問題，並以技能和經驗共同促進一個更加安全、更加可靠的全球電子環境。

- **亞太地區電腦緊急反應小組**（Asia Pacific Computer Emergency Response Team, APCERT)

APCERT是於 2002 年由澳大利亞、中國、日本、韓國等國家的電腦緊急事件反應小組(CERT)所發起成立的，是目前亞太地區最有影響力的緊急反應聯合組織，負責與CERT以及CSIRTs(Computer Security Incident Response Teams)的合作，以確保亞太地區的網路安全。目前，該組織已經吸引了亞太地區 13 個經濟體的 15 個反應組織作爲正式成員。[62]

- **歐洲計算機網路研究教育協**會（Trans-European Research and Education Networking Association, TERENA)

[61] 資料來源參考自FIRST網站(http://www.first.org/)

[62] 資料來源參考自APCERT網站(http://www.apcert.org/index.html)。另可參考Cameron Ortis, Paul Evans, “The Internet and Asia-Pacific security: old conflicts and new behavior,” *The Pacific Review*, Vol. 16, No. 4 (December, 2003), pp. 549-572.

TERENA成立於 1994 年，旨在推廣和參與爲教育和研究而進行的高級國際資訊和電信設施建設。該組織採取一切必要措施，以促使這些設施建立在開放的標準和最先進的技術之上。TERENA開展一系列的技術活動，提供討論平臺，以鼓勵爲歐洲研究團體建立高質量的電腦網路。[63]

有關國家資訊科技安全的基本立法部分，以下則是針對最具代表性的美國以及我國爲例。

- **以美國的資訊科技立法爲例**

美國是最早提出、也是最重視建構「資訊科技」安全體系的國家。從 1984 年的「關於通信和自動化資訊系統安全的國家政策」(NSDD-145)，到 1996 年柯林頓政府開始努力設法解決網際恐怖主義的問題，在 1998 年美國總統柯林頓發佈的第 63 號總統決策令(PDD-63)中將此行動正式化，要求動員一切力量重新建構美國「關鍵性基礎設施」，以使美國資訊系統免遭攻擊，確保國家資訊安全。[64]

2000 年 1 月，根據之前PDD-63 的要求，美國政府制訂了「資訊系統保護國家計畫」，該計畫是美國 21 世紀資訊安全總體戰略的行動指南。因其綜合性、全面性、現實性而成爲美國資訊安全保障工作中具有里程碑意義的文件。[65]

2001 年太空司令部(SPA-CECOM)發表「網際網路戰略」，正式承認網際空間爲第四戰爭領域。2001 年 9 月美國同時發生多起恐怖事件，一般設施、基礎亦成爲攻擊對象，對全體國民生計有很大的影響。針對社會基礎建設的網際攻擊，其受害者無法計數。2001 年 10 月，布希總統發表「資訊時代重要基礎建設的保護」(13231 號總統行政命令)。

美國有鑑於資訊攻擊已成爲資訊安全的重要威脅，針對電腦遭受攻擊的事件

---

[63] 資料來源參考自TERENA網站(http://www.terena.nl/)

[64] 見U.S. The White House, *Defending America's Cyberspace: National Plan for Information Systems Protection*, Version 1.0, An Invitation to a Dialogue, (Washington D. C.: The White House, 2000)

[65] 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 439-440。

不斷發生，參議院在 2002 年 1 月提出法案，以編列經費補助的方式，保護政府的電腦免於被攻擊。這是第一個提供大筆經費補助，有關研究與執行政府電腦安全標準的參議院法案。該法案在未來的五年內，提供 35,000 萬美元給從事研究與對抗電腦駭客、病毒的國家標準技術局(National Institute of Standards and Technology, NIST)。其中網路反恐怖主義戰備法(The Cyberterrorism Preparedness Act)要求設立一個非營利的組織，來執行政府機關內部的電腦安全標準。[66]

2002 年 11 月 25 日簽署設立「國土安全部」(Department of Homeland Security, DHS)，更發表了「國土防衛構想」做爲根據，防備包含網際恐怖主義在內的新一波攻擊。[67]這些政策和命令都對如何維持關鍵基礎設施和資訊系統的安全提出了具體的要求。

- **以我國的資訊科技立法爲例**

以我國爲例，台灣電腦網路危機處理暨協調中心(TW-CERT/CC) [68]自八十七年九月正式成立以來，爲了防止電腦網路安全危機的發生，即積極協助台灣地區電腦網路安全相關事件、成爲全台灣處理網路安全方面事件的對外窗口，並肩負任起與世界各國 CERT 組織溝通的任務。

GSN-CERT/CC 是 Government Service Network - Computer Emergency Response Team / Coordination Center 的縮寫，意即「政府網際服務網-電腦網路危機處理／協調中心」。GSN-CERT/CC提供了以下的服務：電腦緊急事故處理建議、定期對外公佈電腦安全相關資訊、推廣教育訓練及提供課程訓練、加強使用者對電腦安全認識，並與協助各單位成立自己的電腦緊急事故處理小組，俾協助

[66] 科技法律要聞，美國參眾議院提案加強電腦安全，財團法人資策會法律中心網站，第一期，民國 91 年 3 月 18 日，<http://stlc.iii.org.tw/epaper/1/content.htm#2>
[67] 岸田明著，林雯譯，**學資訊安全的第 1 本書** (臺北縣汐止市：博碩文化，2003)，頁 68。
[68] 台灣電腦危機處理暨協調中心，其網址http://www.cert.org.tw/index.php

各單位組織改善系統安全。[69]

我國政府早在民國 76 年 4 月 20 日，由行政院令頒「行政院所屬機關電腦設備暨資訊機密維護準則」，來規範電腦設備安全、資訊機密維護、以及資訊作業管制等安全工作。但因缺乏對「網路安全」的管理與作法，乃於 1999 年廢止該準則，另頒「行政院所屬各機關資訊安全管理要點」，進一步強化資訊安全管理，確保資料、系統、設備及網路安全有關的政策。2000 年總統核定行政院 2718 次院會通過「建立我國通訊基礎建設安全機制」計畫，分別由政策、管理、技術三方面來推動資訊安全保護工作。並於行政院下設立「國家資通安全會報」，內設有「國家資通安全應變中心」，負責建立資通安全事前預警機制，彙總各組資通安全會報、分析及協調適當單位提供技術支援等相關事宜。加上台灣電腦網路危機處理中心的設立，以及政府憑證管理中心GCA的成立(1998 年 2 月)，我國在資通安全的保護傘上，應以具備一定程度的認知與能力，可謂國家關鍵基礎建設中的資通基礎建設提供合理的保障。[70]

[69] 國家實驗研究院科技政策研究與資訊中心編，**資通安全分析專論彙編：94 年度** (臺北市：國研院科技政策中心，民國 94 年)，頁 114。

[70] 財團法人國家政策研究基金會
(http://www.npf.org.tw/PUBLICATION/TE/092/TE-R-092-002.htm)

# 小　結

單靠政府無法確保網路空間安全，僅管人們對資訊科技安全重要性的警覺日益增加，各國政府也紛紛採取各項措施改善能力，但是資訊科技，特別是經由網際網路，所造成的風險仍是每個國家將來在國家安全管理上的隱憂。

涉及到技術以外的領域，需要跨行業合作，進一步的擴展和完善應急合作體系。國際合作的好處，除了能及早預警，以及資料、技術、資訊的共享，更能阻止來自其他國家的攻擊，或有助於追查出攻擊的來源。

到目前爲止，有更多的國際合作組織成立，像是FIRST、APCERT、EGC(European Government CERT)[71]等等，彼此間正積極制訂多邊體系與制度以因應資訊科技，並針對網際網路、電子商務等研擬相關制度。[72]國際間各國也紛紛夠過國際會議或國際合作的方式來解決網路犯罪問題，因此，唯有透過國際合作，並建構更多新的合作管道，像是納入非政府組織參與相關活動以及分享權力，方可有效因應資訊科技安全所遭受到的挑戰，畢竟像資訊科技這種全球化下衍生的國際性問題，還是需要國際間合作與協調以解決此方面的脆弱性問題。

[71] EGC是由英國、法國、德國、芬蘭、瑞典、荷蘭所組成。
[72] Thomas E. Copeland (ed.), *The information revolution and national security*. (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2000), p. 54-55.