

第一章 導論

第一節 研究動機

美國未來學者艾文·托弗勒(Alvin Toffler)在其所著「新戰爭論」¹中首創「第三波戰爭」的論點，即第一波戰爭係以農業為主的科技革命，第二波戰爭係以工業為主的科技革命，第三波則係以資訊為主的科技革命，也就是由機械化戰爭轉向資訊化戰爭的轉變，這種轉變是由於「資訊科技」的運用。而學者丹尼爾·貝爾(Daniel Bell)則是認為，人類近代史上有三波工業革命：第一波是約兩百年前蒸汽動力與工廠式機械生產；第二波是約一百年前電力學與化學的進步；而第三波則是電腦與長途電信通訊的發明，亦即「資訊科技」的應用與傳播。²

所以資訊革命(Information Revolution)儼然已經被視為是繼工業革命之後，全球所面臨最重要的轉型。目前的資訊革命乃是以電腦、通訊與軟體等各方面的快速革新做為基礎，然後導致接收與傳輸資訊的成本大為降低。³資訊科技的進步，使得全球最先進的國家紛紛從工業社會進步至資訊社會；而網際網路(Internet)的發展，則是進一步建構了網路社會與形成「網際網路空間」(Cyperspace)，對個人、團體、國家、與全球都產生了巨大的影響。

「資訊科技」範圍包括甚廣，所謂的「資訊科技」(Information Technology, IT)一詞，應當是指「資訊通訊科技」(Information and Communication Technologies, ICTs)的簡稱，而這正是資訊社會所賴以建立的基礎。這種技術被使用來做為資料的收集、操作、歸類、儲存及擷取，也包含電腦、電信系統、廣播媒體以及多

¹ 杜佛勒(Toffler, Alvin)著，傅凌譯，**新戰爭論** (台北：時報文化，1994年)

² Daniel Bell, "The World and the United States in 2013," *Daedalus*, Vol.116, No.3 (Summer, 1987), pp. 1-21.

³ 奈伊(Nye, Joseph S., Jr.)著，蔡東杰譯，**美國霸權的矛盾與未來** (臺北市：左岸文化，2002年)，頁 112。

媒體的整合。⁴於是隨著傳播、運輸及軍事科技的進步，全面性提升了整個世界的交流程度與相互連結的緊密度。

「資訊科技」的革命並非侷限於更低廉的通信或是更快速的電腦而已，「資訊科技」的革命是從各種角度影響全球的經濟與政治，包括資訊蒐集、分析、傳播等各方面。當前「資訊科技」革命的時代，其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。⁵在此筆者認為，二十世紀以來「資訊科技」的提升，已經讓人無法輕忽其所產生變化的效果。正如同自由主義學者所認為的，這種科技的新進展將會引領我們走向新舊國際關係的分水嶺，舊有的權力政治關係及行為模式將隨著傳播與運輸科技的發展，而形成一種全新的國際關係。⁶

然而，「資訊科技」革命所帶來的影響亦有其負面之處，資訊國家與非資訊國家間落差日益擴大，會產生所謂的「數位落差」(digital divide)問題。⁷再加上資訊時代的人民與政府，日益仰賴高速度及高品質的資訊科技來從事日常事務，各種的資訊科技成爲人們之間互動的基礎，但是這卻造成了資訊社會高度依賴資訊科技之後，所產生的脆弱性(vulnerability)問題。⁸甚至「資訊科技」有時會被有心份子用來蓄意破壞民間或是政府的網路系統，而對於國家安全造成危害。

「國家安全」就字面上意義來看，意指國防和人民的安全。國家安全所討論的範圍也不限於軍事問題，更包含了外交政策、國防和科技發展等層面。⁹「資

⁴ 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. 2.

⁵ 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。

⁶ 休茲(Hughes, Barry B.)著，歐信宏、陳尙懋譯，**最新國際政治新論** (臺北縣永和市：韋伯文化，2002年)，頁558。

⁷ 「數位落差」的真正內涵可解讀爲由於資訊通信科技的資源分配不均，以及其所造成對於資訊通信科技的運用之不平等，導致國與國之間、族群與族群、甚至個人與個人間產生「擁有(Have)」與「未擁有(Have-Not)」的差別。數位落差的產生可視爲因資訊通信科技的發展與普及化所造成之一種現象。

⁸ 彭慧鸞，「數位時代的國家安全與全球治理」，**問題與研究**，第43卷第6期(民國93年11、12月)，頁29。

⁹ 林碧炤著，**國際政治與外交政策** (臺北市：五南，1997年)，頁154-158。

訊科技」的進步不僅使得國際關係以及「權力」概念的內涵本質有了改變，提升了非國家行為者的角色；同時也增加了柔性國力在外交政策中的重要性；¹⁰更影響了國家所重視的傳統國家安全概念及範圍。

資訊科技的進步也產生了許多的國際問題，像是虛擬外交、資訊戰爭、網路恐怖活動、高科技轉移等等，因此「資訊科技」與國家安全之間的關連性便成為了新的研究課題。¹¹此外，隨著全球化的發展，「資訊科技」安全在國家安全中的地位日益重要，資訊科技已然成為 21 世紀國家綜合戰力的表徵，掌握資訊優勢為目的的資訊戰，亦必然成為國與國對抗的焦點，「資訊科技」所引發的資訊戰將是未來國家安全的重要威脅之一。

不同於以往在舊世代之中，是由核子支配優勢作為聯盟領導的關鍵；而在現今的資訊世代中，資訊支配的優勢則是扮演了重要關鍵角色。¹²在資訊時代中，核子嚇阻、邊界巡邏與海外駐軍儘管還是可以維持區域性的權力平衡，但在提供國家安全方面卻顯然還是不足夠的。所以當美國在全球資訊時代制訂其外交政策時，我們自己也必須更瞭解「資訊科技」在創造新的溝通途徑、以及賦予個人與非國家行為者權力，甚至是提升柔性國力角色方面的重要性，¹³以因應新時代下國家安全所面臨的威脅和挑戰。

第二節 研究目的

在探討「資訊科技」對於國家安全之重要性時，我們必須先對「資訊科技」

¹⁰ 奈伊(Nye, Joseph S., Jr)著，蔡東杰譯，*美國霸權的矛盾與未來*（臺北市：左岸文化，2002年），頁 113。另可參閱Richard Rosecrance, "The Rise of the Virtual State," *Foreign Affairs*, Vol. 75, No. 4 (July/August, 1996), pp. 45-61.

¹¹ 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 13-14。

¹² Nye, Joseph S., Jr., William A. Owens, "America's Information Edge," *Foreign Affairs*, Vol. 75, No. 2 (March/April, 1996), pp. 27-29.

¹³ 奈伊(Nye, Joseph S., Jr)著，蔡東杰譯，*美國霸權的矛盾與未來*（臺北市：左岸文化，2002年），頁 131-136。

的進步所造成國際關係及權力的本質所改變的部分，先作一個背景的瞭解。在此筆者認為其所造成的改變主要有以下兩項：第一，「資訊科技」的進步，將使得柔性國力的問題日益突出，因而影響國家權力的行使；第二，由於資訊時代的來臨不但為政府與私人部門在國家安全事務上創造了新的角色，也讓個人、小規模團體與跨國的非國家行為者有強化本身力量的機會。¹⁴個人也可運用網際網路等資訊科技影響國家安全，所以非國家行為者在資訊科技時代所能發揮的影響權力也比以往增加許多。這兩項因素都影響了傳統國家安全的概念和範圍。¹⁵

另外，針對「資訊科技」攸關國家安全關鍵性地位的探討，乃是因為現代科學技術不但是國家安全的助推器，高科技的競爭也成為各國綜合國力競爭的焦點，更是維護國家主權和經濟安全的命脈所在。但是水能載舟亦能覆舟，「資訊科技」就形同雙面刃一樣，國家在享受資訊時代所帶來的便利性及速度的同時，「資訊科技」也對於國家安全產生了一些新的威脅和挑戰(例如網際網路的駭客、病毒以及資訊戰等等)，若處理不慎同樣也會嚴重危害到國家安全，所造成的影響確是不容小覷。

所以本研究的主要目的在於：

- (一) 就背景理論層面上來看：目的是要研究「資訊科技」嵌入國際關係領域內可能引發爭議之不同思考的探討；以及其對於國家權力的本質及內涵所造成之影響，進而探討國家安全概念範圍的轉變。
- (二) 從實務層面上來看：則是研究「資訊科技」的進步對國家安全造成的新威脅和挑戰。研究焦點著重在「資訊科技」所造成的網際網路之威脅，及引發之資訊戰爭部分作探討。研究並結合「資訊科技」對國家安全造

¹⁴ 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. 4.

¹⁵ 以安全因素來說，「傳統安全觀」認為，軍事是維持國家安全的最重要手段，安全主體是以國家為中心；而「非傳統國家安全觀」，則不以軍事為影響和決定國家安全的唯一要素，並出現大量非國家行為主體，對國家安全產生威脅的主體呈現多元化趨勢。

成影響的個案作分析，綜合整理提出合理可行的「資訊科技」安全政策，以維護國家安全。

以上這些都是本論文所主要討論的問題，並期望能為「資訊科技」與國家安全之間，提出一個正面的合作面向。

第三節 文獻探討

與本論文探討主題有關的文獻，大致可歸類成下列幾項：

壹、第一類著作是探討資訊科技之發展與應用。此類文獻的研究重點在於討論資訊科技的演進，以及其所產生的效益及安全損害部分；並介紹資訊科技的安全目標及目前現有安全機制為何。

相較傳統的暴力犯罪研究而言，「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。研究資訊科技安全的學者普遍認為，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或國防安全系統進行滲透或破壞。因此，犯罪行為已不再受傳統地理範圍所限制，而更可在虛擬空間中進行。

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」，而這也是認為政府無法管理網路的一個主要理由。¹⁶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。

¹⁶ Andrew L. Shapiro, "The Internet," *Foreign Policy*, 115 (Summer, 1999), pp. 17-19.

「資訊科技」更促成了新的戰爭型態出現。因此，為維護國家安全，也必須適時的調整國家戰略。有關「資訊戰爭」的著作部分，「資訊戰爭」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。¹⁷

有關資訊科技安全的相關研究此部分可參考：Louise I. Shelley、Eliot A. Coben、Martin C. Libicki、Andrew L. Shapiro、Dorothy E. Denning、Timothy L. Thomas、James Adams、Alvin and Heidi Toffler、Arnaud de Borchgrave、Shih, Timothy K.等學著的相關著作。¹⁸

貳、其次，第二部分是討論有關國家安全方面的文獻。研究方向是從「資訊科技」對於國際關係以及國家權力本質所造成的影響，進而詮釋國家安全觀念的轉變。主要針對「資訊科技」如何提升國家柔性權力並促其發揮作用，及如何提供非國家行為者強化本身力量之機會，進而瞭解這些轉變如何促成國家傳統安全觀念的改變。

有關資訊對於國際體系的影響，學者Morton Kaplan在1957年出版的國際政治體系和過程(*System and Process in International Politics*)一書中，從五個分析面向對每種體系進行分析，其中一個面向提到資訊(information)變數：說明體系內資訊的傳達及交流程度，資訊是影響任何一種政治或社會體系運動過程的重要因

¹⁷ Thomas, Timothy L., "Deterring information warfare: A new strategic challenge," *Parameters* 26 (Winter 1996-1997): 83.

¹⁸ Louise I. Shelley, "Crime and Corruption in the Digital Age," *Journal of International Affairs*, vol.51 no.2 (Spring 1998): 605-620. Eliot A. Coben, "A Revolution in Warfare," *Foreign Affairs*, vol.72 no.2 (March/April 1996):37-54. Martin C. Libicki, "Information War, Information Peace," *Journal of International Affairs*, vol.51 no.2 (Spring 1998): 411-428. Andrew L. Shapiro, "The Internet," *Foreign Policy*, 115 (Summer 1999): 14-27. Dorothy E. Denning, "Information Warfare and Security," (New York: ACM PRESS, 1999) Timothy L. Thomas, "Deterring information warfare: A new strategic challenge," *Parameters* 26 (Winter 1996-1997): 81-90. James Adams, "Virtual Defense," *Foreign Affairs*, vol.80 no.3 (May/June 2001): 98-112. Shih, Timothy K., "*Intelligent virtual world : technologies and applications in distributed virtual environment .*" (N.J. : World Scientific, 2004) 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) 杜佛勒(Toffler, Alvin)著，傅凌譯，**新戰爭論** (臺北市：時報文化，1994年)

素。¹⁹而資訊時代的柔性國力來自國家對於資訊力量的掌握，有關「資訊科技」方便「軟權力」運作的概念，是將資訊科技與傳統的物資力量，例如油產、部隊、軍事配備與農產品與以區隔開來。波灣戰爭與科索沃的戰爭之中，證明了今日的軍事科技力量取決於先進的資訊科技，例如飛彈的瞄準、短波傳播傳佈消息、電子資訊干擾等等，更證明了「資訊科技」可與現代安全戰略結合。²⁰資訊時代所帶來的變革，不只是在軍事事務上，而且也改革了「軟權力」所運用的工具及其適用機會和有利環境，更使得柔性國力問題日益突出。

有關資訊促成軟權力之運用的相關探討可從Robert O. Keohane、Joseph S. Nye, Jr.、William A. Owens等著作中得到進一步的瞭解。²¹

Robert O. Keohane與Joseph S. Nye, Jr.就提到如何即時、正確而有效的掌握資訊，是取得競爭優勢的重要關鍵。只有在正確、即時、透明化資訊製造過程下，資訊本身才具備可信度，也才能具備「軟權力」的條件。²²

在資訊革命所促成的全球化過程底下，不僅在主權部分有所失去，更造成權力與非政府組織或是與個人的向下分享，Joseph S. Nye, Jr.提出了「資訊權力」(informational power)的概念。²³在他看來，資訊革命透過促進非集中化和民主，正在改變政府以及其主權之性質，使得非政府角色的作用得以增強，而外交政策

¹⁹ Kaplan A. Morton, "System and Process in International Politics," (New York: R. E. Krieger Pub. Co., 1957)

²⁰ Thomas E. Copeland (ed.), *The information revolution and national security*. (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2000), p. 13.

²¹ Joseph S. Nye, Jr., *Soft power: the means to success in world politics*. (New York: Public Affairs, 2004) Robert O. Keohane and Joseph S. Nye, Jr., "Power and interdependence in the Information Age," *Foreign Affairs*, Vol. 77, No. 5 (September/October, 1998), pp. 81-94. Joseph S. Nye, Jr., and William A. Owens, "America's Information Edge," *Foreign Affairs*, Vol.75, No.2 (March/April, 1996), pp. 20-36. Joseph S. Nye, Jr., "Redefining the National Interest," *Foreign Affairs*, Vol.78 No.4 (July/August, 1999), pp. 24-25.

²² 「軟權力」(Soft Power)，根據美國前助理國防部長Joseph S. Nye, Jr.在"*Bound to lead: The changing nature of American Power*"一書中，把「軟權力」定義為在國際事務中透過吸引而不是脅迫以達到目的的能力。而在他的另一篇文章"*Redefining the National Interest*"中，認為「軟權力」是透過文化和意識型態以打動人心的能力。文中並指出“硬權力和軟權力固然同樣重要，但是在資訊時代，「軟權力」正變的比以前更為突出。”另可參考Robert O. Keohane and Joseph S. Nye, Jr., "Power and interdependence in the Information Age," *Foreign Affairs*, Vol.77, No.5 (September/October, 1998), pp. 81-94.

²³ Joseph S. Nye, Jr., *Bound to Lead: The Changing Nature of American Power*. (New York BasicBooks, 1990), p. 34.

中「軟權力」的重要性亦獲得增加。此部分的著作可參考Jessica T. Mathews、Richard Rosecrance等人的著作。²⁴

資訊科技對於國家安全概念範圍影響的部分，Paul Kennedy在其「霸權興衰史」書中曾強調：「在過去 500 年國際對抗的歷史說明了，只具有軍事的『安全』是絕對不夠的。」²⁵資訊時代所造成衝突的型態及方式已有轉變，而將資訊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，該文件將資訊列為第四種國力。²⁶除此之外，國家利益的改變也會使得國家安全的範圍有所變動，像是柯林頓政府時代政府官員威廉·培里(William Perry)和阿許頓·卡特(Ashton Carter)曾提出一項評估美國安全風險的報告，以助於重新確認國家政策的優先性。其中將威脅分為ABC三個等級，而奈依認為C級事件在全球資訊時代中具有主導媒體的能力，比起A級事件來講會引起更多公眾注意。²⁷

而對於「資訊科技」與國家安全戰略探討的重要資料可參考 1999 年 12 月由美國陸軍戰院戰略研究所(U.S. Army College Strategic Studies Institute)與匹茲堡大學李奇威國際安全研究中心(University of Pittsburgh Matthew B. Ridgway Center for International Security Studies)所共同主辦會議之討論，會中探討了關於資訊革命對全球之意涵以及國家資訊安全戰略之需求的研究，諸位專家學者針對有關資訊時代國家安全本質改變情形發表了許多論述。²⁸

有關國家安全觀念的探討另可參閱學者Peter J. Katzenstein、Robert Mandel、Barry Buzan、Ole Waever、Jaap De Wilde或是國內學者林碧炤教授、翁明賢教授、

²⁴ Jessica T. Mathews, "Power Shift." *Foreign Affairs*, Vol.76, No.1 (January/February, 1997), pp. 50-66. Richard Rosecrance, "The Rise of the Virtual State", *Foreign Affairs*, Vol. 75, No. 4 (July/August, 1996), pp. 45-61.

²⁵ 甘迺迪(Kennedy, Paul)著，張春柏譯，**霸權興衰史：1500 至 2000 年的經濟變遷與軍事衝突**（臺北市：五南，1995 年），頁 708。

²⁶ Thomas E. Copeland (ed.), *The information revolution and national security*. (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2000), p. 119.

²⁷ 奈伊(Nye, Joseph S., Jr)著，蔡東杰譯，**美國霸權的矛盾與未來**（臺北市：左岸文化，2002 年），頁 282-284。

²⁸ Thomas E. Copeland (ed.), *The information revolution and national security*. (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2000),

彭慧鸞教授及汪毓瑋教授等人的著作。²⁹

綜觀上述各類文獻，可以發現大部分的著作比較缺乏整體性的討論與分析。換言之，以「資訊科技」影響國際關係為重點的文章，多是著墨於「資訊科技」對於國家安全可能危害的重要性，但是探討資訊科技對整個國際關係及國家安全改變的本因，則著墨略顯不足；而以討論國家安全觀念轉變為中心的著作，在探討國家關係及國家權力本質轉換的同時，則往往忽略了資訊科技此一影響當代世界各個層面甚鉅的因素，也甚少針對資訊科技進行深入的研究。

因此之故，對於介紹資訊科技的發展運用以及闡述其安全特質，且同時針對資訊科技對國際安全所造成之影響，在整個背景方面作一完整且有系統的研究分析此類的文獻，在國外十分罕見，而國內更是付之闕如。因此，本論文的研究議題與研究成果在學術上自有一定的價值與貢獻。

第四節 研究方法

本研究論文，是以文獻分析法作為基本運用方法，廣泛蒐集國內外學者專家對於「資訊科技」與國家安全之討論等相關書籍、定期刊物及學術論文進行研究，整理歸納出「資訊科技」對於國家安全所造成的影響和衝擊；再配合個案研究，探討「資訊科技」在國家安全中扮演的角色。最後並根據研究結果，提出結論與建議，以作為相關決策者的參考，期望國家安全能與「資訊科技」產生正向之合

²⁹ Peter J. Katzenstein(ed.), *The Culture of National Security: Norms and Identity in World Politics*. New York: Columbia University Press., 1996. Robert Mandel, *The changing face of national security: a conceptual analysis*. Conn. : Greenwood Press, 1994. Barry Buzan, Ole Waever, Jaap De Wilde eds. *Security: A New Frame Work for Analysis*. Lynne Rienner Publishers Inc. 1997. 林碧炤, *國際政治與外交政策* (台北:五南, 1997年) 翁明賢著, *全球化時代的國家安全* (台北:創世, 2002年) 彭慧鸞,「數位時代的國家安全與全球治理」, *問題與研究*, 第43卷第6期(民國93年11、12月), 頁29-52。

作。

第五節 研究範圍與限制

「資訊科技」範圍包括甚廣，所謂「資訊科技」(Information Technology, IT)一詞，應當是「資訊通訊科技」(Information and Communication Technologies, ICTs)的簡稱。舉凡透過媒體，如廣播、電視、衛星到網際網路等管道，從事信息的製造(production)、傳輸(distribution)和取得(consumption)等等，都是屬於「資訊科技」的範疇。³⁰但由於「資訊科技」領域中的技術層面牽涉甚廣，於是筆者將本論文所稱的「資訊科技」研究範圍限制於：資訊傳輸及軍事科技方面。其中資訊傳輸的部分，則是著重目前對人類溝通模式產生最大衝擊的網際網路部分；而軍事科技的部分，則是探討未來所謂的資訊戰爭方面。

在研究限制方面，由於「資訊科技」安全是一個複合的概念，且伴隨著全球化的發展，「資訊科技」的改革仍在不斷地革新和進步之中，所以需研究的範圍屬於動態研究，必須根據當代最新發展才能做出更多的評估。而且其中牽涉到有關軍事的資訊科技部分，由於技術層面太過專業非筆者能力之所及，故仍有遺漏和缺憾的地方，還望後進研究此相關題目者能更深入探討。

³⁰ 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 3。

第六節 論文架構

本論文共分為五章，論文架構可參閱附圖 1-1。各章節主要內容分述如下：

第一章為「導論」，主要介紹本論文的研究動機與目的、相關文獻探討、研究範圍與限制、研究方法與論文架構。

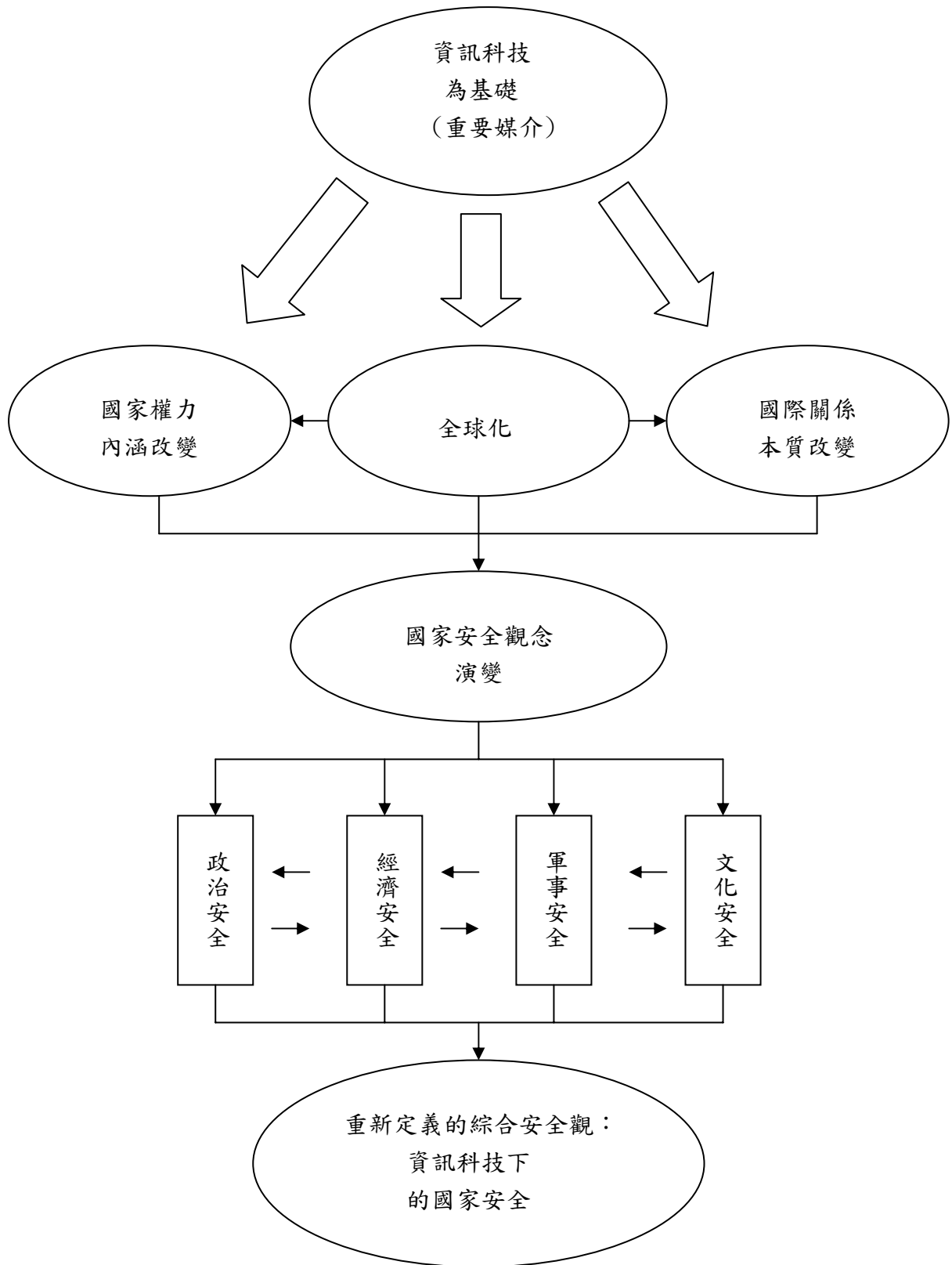
第二章「資訊科技與安全」，首先將「資訊科技」的演變作一簡單背景瞭解，探討「資訊科技」安全的定義，瞭解其所能發揮之安全的效用，及其安全管理及目前現有維護機制之重要性為何。

第三章「資訊科技趨勢下之新國家安全思維」，主要分析「資訊科技」所帶來的國際關係的改變，以及國家權力的內涵及本質的轉變。研究「資訊科技」如何形塑「軟權力」的行使，以及如何影響非國家行為者的角色，來探討國家安全觀念的轉變。

第四章「資訊科技與國家安全之衝擊」，則是探討「資訊科技」如何影響國家安全，產生何種新的威脅和挑戰，再配合資訊科技對國家安全造成影響的個案作分析，並研擬出國家安全與「資訊科技」正面合作的面向方案。

第五章為「總結與展望」，將本論文的研究主題作一統整回顧，結合各章節的討論結果，將「資訊科技」對於國家安全的衝擊，以及國家安全採取的因應之道加以彙整歸納而成，提出研究心得與展望。

圖 1-1 研究概念架構圖



資料來源：作者自製