國防大學政治作戰學院政治學系政治研究碩士班

碩士論文

美軍「第三次抵銷戰略」與美中網路資訊作戰之研究

－兼論對兩岸軍事對峙之影響

A Study of U.S. “The Third Offset Strategy” and U.S.-China Cyber Information Warfare--Also on the Impact of Military Confrontation on Both Sides of the Taiwan Strait

研究生：高清華 撰

指導教授：莫大華 博士

中華民國一○七年五月

國防大學政治作戰學院政治學系碩士學位論文

口試委員會審定書

美軍「第三次抵銷戰略」與美中網路資訊作戰之研究－兼論對兩岸軍事對峙之影響

A Study of U.S. "The Third Offset Strategy" and U.S.-China Cyber Information Warfare--Also on the Impact of Military Confrontation on Both Sides of the Taiwan Strait

本論文係高清華君（學號 1070720103）在國防大學政治作戰學院政治學系完成之碩士學位論文，於民國 107 年 5 月 14 日承下列考試委員審查通過及口試及格，特此證明。

指導教授 莫大華

委員 張中勇

委員 [illegible]

學系主任 莫大華

中華民國 107 年 5 月 14 日

國防大學

National Defense University

國防大學政治系碩士生論文文責自負聲明書

本人瞭解並保證所撰寫之論文完全遵守著作權法及學術倫理規範，指導教授已善盡告知、審查、監督之義務。論文倘有抄襲、捏造、改作、妨礙他人著作權，或其他一切有違著作權及學術倫理規範之情事，以及衍生相關民、刑事責任者，概由本人負責，與指導教授、論文口試委員及政治學系所有師長無關。

論文題目：美軍「第三次抵銷戰略」與美中網路資訊作戰之研究－兼論對兩岸軍事對峙之影響

研究生：高清華（簽章）

學號：1070720103

指導教授：莫大華

我已閱讀下方說明，並同時繳交原創性檢測報告。：

☑論文原創性檢測報告

☑學位論文口試作業規定第肆(六)條

經遭檢舉論文抄襲，且調查屬實者，雖已授予學位，專案報請國防部予以撤銷，並註銷其已發給之結業證書與學位證書。

中華民國 107年 5 月 14 日

國防大學

National Defense University

謝辭

時光荏苒，轉眼間一年九個月的研究生生涯準備結束，雖有所不捨，但這是人生一個里程碑的達成，也告訴著我該準備往人生下個階段前進。研究所這段時光是段奇幻旅程，猶記考試前在部隊經常忙到三更半夜，打開書本經常是凌晨一點之後的事，放榜時，看到自己的名字後方寫著正取 19，只有驚訝兩字形容，雖不知當時閱卷老師姓名，但仍心存感激，是他給予我這個機會，領略學海的浩瀚與無窮。

首先要感謝的是我的父母，總是給予我支持與鼓勵，無論是在低潮或是難過時，總是成為我溫暖的避風港，在得知我錄取碩士班後，也高興的為我喝采。

第二位要感謝的是臺灣建構主義大師莫大華老師（這樣會不會太浮誇），有幸能夠成為老師的指導學生，無論是在學術上的發展或是人生道理的經驗分享，使人如沐春風，獲益良多。

接下來感謝我的先生鄭宗瑋，容忍我暴躁的脾氣，始終當個好好先生，謝謝你用心陪伴與關愛，也期盼我們能夠繼續迎接人生的下個階段。

最後要感謝李亞明老師、劉興祥老師、陳建源老師、蔡侑成學長、周琮凱學長、黃君則、連翰梧、戴彥平以及王馨儀，沒有你們這一年九個月的陪伴，研究生生活必會遜色不少。這段時光裡，台北四處有我們足跡，小陶鍋、越南料理、北部美味餐館、各大夜市、成功攀登玉山等等，都是值得回憶的紀念，也感謝你們，給予我學業以及生活上的協助與幫忙。

紙短情長，要感謝的人太多，相遇相識是得來不易的緣分，期盼我們都能充滿力量，繼續面對接下來的挑戰。

高清華　謹誌於復興崗

2018.5.24

國防大學 National Defense University

國防大學

National Defense University

中文摘要

1950 年代美國為抵銷蘇聯具壓倒性優勢傳統武力和核武，提出「新視野戰略」（New Look）；1970 年代由國防部長布朗(Harold Brown)提出的抵銷戰略(Offset Strategy)，以可攜帶多核彈頭的精準導引武器對抗蘇聯核武數量以及規模龐大的傳統武力優勢。以前兩次成功經驗為基礎，美軍 2014 年所提出國防創新倡議，目的是因應中共快速軍事現代化以及反介入與區域拒止能力增強的威脅。

美軍的作戰概念與時俱進，從空地作戰（Air Land Battle）、空海作戰(Air Sea Battle)、全球公域介入與機動之聯合構想(Joint Concept for Access and Maneuver in the Global Commons, JAM-GC)，越發強調聯合作戰之重要，而聯合作戰首重各軍種資訊溝通交流無礙，因此網路資訊安全重要性不言可喻。

臺灣自民國 38 年國民政府播遷來台後，與中共持續軍事對峙已近七十載，我國與美國也維持良好的軍事合作關係。隨著中共在世界上政治、經濟影響力的增加，使中共投入軍事預算持續增長，以致兩岸軍力逐漸失衡，受限於我國防經費之獲得有限，因此必須在有限的經費與資源下，思考我國發展不對稱軍事思想與作為。

因此，本文透過美軍三次抵銷戰略之歷史脈絡，探討美中競合關係下之網路資訊作戰，兼論我國因應兩岸軍力失衡，發展不對稱作戰之思維，希冀在網路資訊作戰領域取得我國的相對優勢。

國防大學
National Defense University

關鍵字：國防創新倡議、第三次抵銷戰略、網路資訊作戰、不對稱作戰

國防大學

National Defense University

Abstract

In the 1950s, the United States proposed a “New Look” strategy to offset the Soviet Union's overwhelming superiority with traditional force and nuclear weapons. In the 1970s, the offset strategy proposed by Harold Brown could be carried. The precision of the multi-nuclear warheads guided the weapons against the Soviet nuclear weapons and the large-scale advantages of traditional force. Based on the previous two successful experiences, the US military’s proposed defense innovation initiative in 2014 was designed to respond to the China rapid military modernization and the threat of anti-access and regional rejection.

The combat concept of the US military keeps pace with the times, from Joint Concept for Access and Maneuver in the Global Commons to Air Land Battle, Air Sea Battle, and Global Commons. It is increasingly important to stress the importance of joint operations and the importance of information security in the Internet is imperceptible.

After Taiwan’s republication of the Nationalist Government in the 38th year of the Republic of China came to Taiwan, there was almost 70 years of continuous military confrontation with the Chinese Communist Party. Taiwan and the United States also maintained a good military cooperation relationship. With the increase of the political and economic influence of the China in the world, China investment in military budgets has continued to grow. As a result, the cross-strait military forces have gradually become unbalanced and are limited by the limited availability of China’s defense funds. Therefore, we must consider China with limited funds and resources. Develop asymmetric military thoughts and actions.

Therefore, through the historical context of the US three-offset strategy, this paper explores the cyber information warfare under the US-China competitive relationship, and discusses the thinking of China to develop asymmetric operations in response to the imbalance of military power across the Taiwan Straits, and Hope to gain Taiwan's comparative advantage in the field of cyber information and operations

National Defense University

Keywords：Defense Innovation Initiative, The Third Offset Strategy, Cyber Information Operations, Asymmetric Operations

國防大學

National Defense University

目錄

目錄.....I

圖目錄.....III

表目錄.....IV

第一章 緒論.....1

第一節 研究動機與目的.....1

第二節 研究途徑與研究方法.....3

第三節 研究範圍與限制.....5

第四節 文獻回顧.....6

第五節 研究架構與章節安排.....16

第二章 美軍三次抵銷戰略的戰略目標與分析.....19

第一節 美軍第一次抵銷戰略之緣起與意涵.....19

第二節 美軍第二次抵銷戰略之緣起與意涵.....26

第三節 美軍第三次抵銷戰略之緣起與意涵.....31

第四節 小結.....38

第三章 美中網路資訊作戰之發展與運用.....43

第一節 網路資訊作戰之本質與特色.....43

第二節 美軍網路資訊作戰之發展與運用.....49

第三節 中共網路資訊作戰之發展與運用.....56

第四節 小結.....62

第四章 美軍第三次抵銷戰略對兩岸軍事對峙之影響.....65

第一節 美中競合下的兩岸關係.....66

第二節 我國資訊產業發展現況.....71

第三節 我國因應之國防與軍事戰略.....74

國防大學 National Defense University

第四節 小結 77
第五章 結論 79
第一節 研究發現 79
第二節 未來研究建議 80
參考文獻 83

國防大學
National Defense University

圖目錄

圖 1- 1　研究架構圖 16

國防大學
National Defense University

表目錄

表 2- 1　美國三次抵銷戰略比較分析表 42

表 2- 2　網路資訊攻擊技術型態分類 49

國防大學
National Defense University

第一章 緒論

第一節　研究動機與目的

一、研究動機

現今美國所面臨的競爭對手不如過去冷戰時期的單純。在冷戰期間，美國所要打擊的目標相當明確，就是蘇聯及其扶植的共產政權，美軍三次抵銷戰略都是在戰爭結束初期、國力相對下降，有大國挑戰的背景下，尋求技術的創新來維持美國的軍事優勢。美國過去在 1950 年代艾森豪總統的所提出的「新視野戰略」（New Look）設法發展先進核子武器戰力，以抵銷蘇聯具壓倒性優勢傳統武力和初期核子戰力，以及 1970 年代由國防部長布朗(Harold Brown)提出的抵銷戰略(Offset Strategy)，以精準導引武器對抗蘇聯核子火力在數量和科技均勢上的新進展，還有部署在東歐和全球其他地區數量持續佔優勢的傳統兵力，過去兩次的抵銷戰略均成功融合了創新技術和新的運營理念，時代的變遷以及潛在對手的改變，亦直接影響了戰略的目標與手段。

美軍三次的抵銷戰略均帶有戰略預置性，但相較於前兩次的抵銷戰略，第三次抵銷戰略則更加突顯其超前的戰略預置性，過去兩次戰略的提出，美、蘇的軍力對比中，美國並不佔優勢，甚至略居下風，但本次的抵銷戰略則是在美國軍力明顯優於對手的背景下提出，更加突顯出美國面對長期的競爭下，必須確保其領先及絕對優勢的地位。過去兩次的抵銷戰略，實質為尋求核技術以及資訊技術的優勢，第三次抵銷戰略面臨的則是尋求改變未來戰局的顛覆性技術，而為了有效執行的相關科研經費，美國國防部在 2017 財年編列 718 億美元作為研究經費，目的在維持美國對中共和俄羅斯等競爭對手的軍事優勢，2017 財年的預算相較於 2016 財年的研究開發預算增加了 6900 萬美元，約提升了 4 個百分點，並規劃投入 180 億美元在其「未來國防計畫」（Future Years Defense Program）中，作為研究及發展第三次抵銷戰略的先進科技及作戰概念。[1]

---

[1] Franz-Stefan Gady, “New Us Defense Budget: $18 Billion for Third Offset Strategy,the Pentagon Wants to Spend More Money to Offset Anti-Area/Access-Denial (A2/AD) Technologies.,”*The Diplomat*,

現今美國所面臨的潛在對手，因先進科技的擴散，導致區域強權甚至是弱國、「非國家行為者」都能夠取得並發展高科技的武器裝備及軍事科技，而具備反介入與區域拒止能力；再者，雖然各盟國均有提供軍事基地，但因考量各自的利益而不願長期提供美國使用，以及美國可用的資源受限與部隊安全等考量因素，將使美國在全球的軍事佈署充滿許多不確定性，最後，太空科技及網路空間在未來的作戰中將日益重要，但隨著其他競爭對手在相同領域的發展，美國已將無法獨佔太空及網路空間的優勢，也將在未來面臨嚴峻的考驗及挑戰。

基上所述，筆者研究此議題的動機可分為以下幾點：

（一）面對多面向的威脅，美軍所提出的第三次抵銷戰略將如何做出因應，值得吾人探討。

（二）高科技的軍事裝備，需要在安全的網路資訊空間中方能發揮其效能，而美中未來在網路資訊空間中的發展與競爭，亦是本文持續關注的重點。

（三）從「反介入與區域拒止」（Anti Access and Area Denial, A2/AD）的概念[2]到「空海一體戰」(Air Sea Battle)再轉變為「全球公域介入及機動聯合構想」(JAM-GC)，美軍軍事戰略的核心要素隨著外部威脅的改變有所不同，面對美軍的改變與進步，中國將如何應處，其中牽涉的兩岸關係，臺灣所扮演之角色值得吾人持續關注。

二、研究目的

在過去至少十餘年的時間裡，中國投入了相當多的財力和人力來建設其國防軍事力量，尤其是中國海軍和空軍，已逐漸可以向西太平洋投送數量可觀且可以維持的軍力，並最終有能力向更廣闊的開放海域投送軍力。中共快速的軍事現代化帶來的威脅，就是美軍提出第三次抵銷戰略之主要原因，科技發展一日千里，網路資訊作戰勢必是雙方角力戰場，承上所述，本文的研究目的在於：

一、　了解美軍因應外部複雜威脅，第三次抵銷戰略未來之發展與影響。

Feb. 10, 2016 At https://thediplomat.com/2016/02/new-us-defense-budget-18-billion-for-third-offset-strategy/.(Accessed 2017/10/16)

2 Roger Cliff, Mark Burles, Michael S. Chase, Derek Eaton, Kevin L. Pollpeter, *Entering the Dragon's Lair: Chinese Antiaccess Strategies and Their Implications For the United States* (Santa Monica, CA, RAND Corporation, 2007)p.27.

二、　分析第三次抵銷戰略對美中軍事科技與網路資訊作戰之發展。

三、　探討美中科技競爭關係對兩岸軍事對峙的影響。

第二節 研究途徑與研究方法

一、研究途徑

所謂研究途徑，乃指研究者對於研究對象的研究，是以何種層次為出發點、著眼點、入手處，去進行觀察、歸納、分類與分析，由於切入點的不同，便各有相呼應的一組概念，作為分析的架構。[3]

本文將採用「歷史研究途徑」(Historical Approach) ，「歷史」一詞有著數重意義，首先，它指過去的事件，即實際發生之事，其次，歷史一詞意味著事件的紀錄或敘述，最後，歷史意味著一門學科，一個研究領域，他已經發展出一套方法和概念，通過這些方法和概念，歷史學家收集過去事件的證據，評價這種證據，並就題目進行有意義的討論，[4]對於過去已經發生的現象，有系統地加以描述與分析，並解釋涉及過去已發生事件的當代政治現象。它強調解釋與理解，而非僅限於陳述法則而已，[5]透過蒐集美國與國際上各國之官方網站、智庫及新聞報導等相關資料，多面向的了解美國抵銷戰略之歷史脈絡，以及第三次抵銷戰略中資訊作戰之運用及發展，藉以分析此戰略對國際政治經濟局勢產生之衝擊與影響。

二、研究方法

研究方法是期望透過建立一個組織架構，並且綜整、蒐集各方研究之經驗與資料，將其歸納成一套具邏輯性的概念。[6]是蒐集與處理資料的技術。[7]因此依據研究性質與蒐集資料之不同，本文主要以「文獻資料分析法」(Documentary Analysis)進行研究。

---

[3] 朱浤源，《撰寫博碩士論文實戰手冊》（新北市：正中書局，2006 年 12 月 25 日），頁 182。

[4] 趙干城、鮑世奮，《史學方法論》（台北：五南圖書出版公司，1999 年 10 月初版），頁 2。

[5] David Marsh、Gerry Stoker 著，陳義彥譯，《政治學方法論與途徑》（台北市：韋伯文化事業出版社，2009 年），頁 61。

[6] 呂秋文，《如何撰寫學術論文》（新北市：臺灣商務印書館，2007 年 2 月 1 日），頁 25。

[7] 易君博，《政治理論與研究方法》 (台北市：三民書局，2003 年)，頁 97-98。

文獻資料分析法約有下述幾項特點：

（一）它所研究的事件是過去而非目前發生：

文獻資料分析可超越過去時空的限制，在歷年累積的資料中，找尋有關的研究材料。

（二）文獻資料分析可超越個人的經驗與視野：

對於每個文獻資料分析的個人來說，不僅能廣泛涉及前人在各領域的調查成果，以超越自己調查研究的侷限性，而且也是對以前每個人調查研究侷限的超越。

（三）文獻資料分析可超越調查互動中的不良影響：

社會行為科學工作者在從事研究工作時，經常會遭遇到某些特殊問題，既無法用實驗來加以驗證，又不能以社會調查來尋求解答，期解決的唯一方式，便是從分析既有的資料中得到答案。

（四）可提供解決問題的有效方案：

在撰寫研究報告時，必須對該一社會問題提供詳實可靠的背景資料，這些資料的最大來源自然是現成的既有文獻。這樣做一方面研究者可以檢視其研究結果是否可以應用於現實社會中，一方面關心該一問題的社會大眾也比較容易接受他的看法。[8]

本文主要透過蒐集相關專門書籍、學術期刊、報刊、正式的學術論文及官方資料，引用原始檔、官方資料等相關檔案，以一手資料為主、二手資料為輔進行研究，以求符合事實並貼近研究，有所貢獻，探討自 1950 年代第一次抵銷戰略(又稱新視野戰略)、1970 年代第二次抵銷戰略至 2014 年美國國防部所提出的「國防創新倡議」(Defense Innovation Initiative)之脈絡研究，分析當時戰略形成的國內、外背景，與其中所改變之內容，以及後續是否達成預期目標，作為我國因應軍事創新發展趨勢，應變政策制定之參考。

[8] 葉至誠、葉立誠，《研究方法與論文寫作》 (臺北市：商鼎文化，1999 年)，頁 136-140。

第三節 研究範圍與限制

一、研究範圍

本論文以美國自 1950 年代起提出新視野戰略、1970 年代的第二次抵銷戰略至 2014 年 11 月 5 日美國國防部長黑格提出「國防創新倡議」描繪出美軍第三次抵銷戰略之構想，其成因背景及歷史脈絡，以及第三次抵銷戰略中，資訊作戰之運用及發展為研究重點，進而探討在第三次抵銷戰略提出之後，對於美國以及東亞區域安全之影響。

在研究範圍部分，新視野戰略一詞首見於美國艾森豪總統執政期間，於 1953 年 10 月 30 日批准的 NSC 162/2 文件當中，它反映了艾森豪總統對平衡美蘇冷戰軍事承諾與國家財政資源的關切。[9]該政策強調依靠戰略核武來阻止來自以蘇聯爲首的共產集團，對抗其所擁有的常規武器和核武器的潛在威脅，1970 年代，美國前國防部長布朗提出了第二次抵銷戰略，原因為前蘇聯所發展的核武已和美國達到「相互保證毀滅」（Mutual Assured Destruction）的階段，無法繼續保持其對蘇聯的核優勢，而新戰略強調了「情報，監視和偵察」(intelligence, surveillance, and reconnaissance,ISR)平臺，改進了精準導引武器(precision-guided weapons)，隱形技術(stealth technology)和太空軍事通信和導航(space-based military communications and navigation)，藉以阻止蘇聯入侵北約的可能性。[10]2014 年 11 月 15 日，美國國防部長黑格為了擴大美國與其潛在競爭對手之軍事優勢，所提出的國防創新倡議及第三次抵銷戰略，亦將影響美、中在軍事科技上的競逐，總言之，本文研究範圍如下：

（一）自 1953 年「新視野戰略」提出後至 2014 年「第三次抵銷戰略」之歷史脈絡。

（二）因應中共軍事科技擴展所發展之「全球公域介入及機動聯合構想」(Joint

---

[9] James S. Lay,Jr., "A Report to the National Security Council," *Federation of American Scientists*, Oct. 30, 1953.At https://fas.org/irp/offdocs/nsc-hst/nsc-162-2.pdf (Accessed 2017/10/21)

[10] Rebecca Grant, "The Second Offset," Jul. 2016.At http://www.airforcemag.com/MagazineArchive/Documents/2016/July%202016/0716secondoffset.pdf（Accessed 2017/10/16）

Concept for Access and Maneuver in the Global Commons A New Joint Operational Concept)。

（三）第三次抵銷戰略對美、中、臺關係之影響。

（四）美、中在網路資訊空間的發展與運作。

本論文資料主要來源是美國官方及其媒體所公開之文件、智庫與學者發表之報告與心得，亦包含美國學界發表之研究專書或期刊論文，而第三方評析資料則主要將中共官方公佈之文件與數據資料以及學界公開發表之期刊、論文納入參考資料範圍內，此外，網際網路上擷取之各國相關電子新聞傳媒資訊亦會納入本研究資料之搜索。

二、研究限制

本次研究的限制在於第三次抵銷戰略其相關議題仍正在進行，故相關資料仍在更新，且第三次抵銷戰略目前僅是美國提出之軍事創新概念，尚未有實際運用及數據，僅能以其智庫及學界提出之資料內容進行分析。

在美國所面對「潛在對手」的界定上，雖中共、俄羅斯、伊朗、北韓等均是美國遭遇的外部挑戰之一，本文聚焦於中共快速擴張之軍力，以及美中台三邊關係之影響，故本文在討論美國對手一詞上，均以中共為主。

目前資料收集至 2018 年 4 月，因此對於該研究議題，有其侷限，而在美國總統川普上臺後，「第三次抵銷戰略」此一名詞討論熱度已逐漸減少。但筆者認為，軍事科技的改革以及取得資訊空間的優勢是未來戰爭之趨勢，即便因為政黨輪替，導致政策名詞有所不同，但實際運作之方向與內容亦差距不遠。在文獻蒐集的部分，以官方網站，公開資料為主，有部分涉及軍隊機密之資料，無法取得，將以能夠取得的公開資料進行分析，在外文文獻翻譯部分，會盡力接近其原意，不致相差太遠。

第四節 文獻回顧

文獻回顧的功能是向讀者說明研究是如何依據其他研究成果為基礎而進行的且與他人研究之間有何區別、解決了文獻中尚存的問題等等，或是以那些理論基礎或研究途徑上進行的，也就是討論多年來整個領域內所有相關的研究成果。通常也能讓讀者簡單地接觸到相關領域且重要的研究。文獻回顧必須要具有綜合、分析、

還要能夠進一步批判現有文獻的功能，並指出目前文獻的優缺點、有何不足之處，並由這些不足來發展出研究者自身研究的理論方向與命題。

本研究論文運用「國家圖書館全國博碩士論文」「臺灣期刊論文索引系統」及「Airiti Library 華藝線上圖書館」等國內期刊論文網站，亦透過美國政府機關網站(例如：美國白宮、國務院、國防部等)等國際知名政策智庫，蒐整現今有關於抵銷戰略的研究，加以統整並建立其參考價值。

以下為相關文獻之研究探討，臚列於後，請參考下文：

一、第一次抵銷戰略

Richard M. Leighton 指出，在面對前蘇聯之軍事擴張與共產主義的勢力，杜魯門總統大幅增加國防預算，1953 年韓戰結束，美國為振興國內經濟發展，準備執行減稅方案，若仍維持高額的國防經費支出，將使得國內財政嚴重赤字，艾森豪總統在執政的前三年（1953-1956 年）中，強調政府將不斷努力地降低國防費用，平衡韓戰後國內經濟所面臨的挑戰，艾森豪總統認為，穩定健全的國內經濟，是國家政策依賴之基礎，本文件旨在分析經濟與戰略之間的關係，在當時歷史背景下研擬「新視野」戰略，並開始重視空戰與戰略性核武的作用。[11]

David Holloway 指出，1950 年代，核嚇阻是美蘇冷戰的產物，也是造成緊張局勢的因素，而核武的發展也有助於冷戰「更冷」。1960 年代中期，美蘇雙方制定了一系列公約來規範彼此管理核武，以避免造成大規模死亡和毀滅的局面。作者認為大規模的核戰是不可能被接受的，這亦是有權利使用核武的美蘇領導人之間的常識，這種共識構成了冷戰的基本前提，塑造了未來幾年的核嚇阻政治，美蘇雙方領導人願意發動核嚇阻，但這與實際行動之間有很大的區別。[12]

Samuel F. Wells,Jr.認為，大規模報復的中心思想在於當前蘇聯欲侵略及危害美國國家安全時，美軍可運用其在核武力量的優勢，在特定時間地點，給予前蘇聯本

---

[11] Richard M. Leighton, "*Strategy, Money, and the New Look, 1953-1956 , Volume III,*" (Washington D.C.: Historical Office of the Secretary of Defense,2001), pp. 65-68.

[12] David Holloway, "Nuclear Weapons and the Escalation of the Cold War, 1945-1962," in Odd Arne Westad and Melvin Leffler, eds., *The Cambridge History of the Cold War*, Vol. 1 (Stanford, CA:Cambridge University Press, September,2010), pp. 387-392.

土大規模之核武反擊，進而對其產生無法承受之傷害，藉以達到前蘇聯不敢輕易發動軍事侵略的嚇阻效果。[13]

二、第二次抵銷戰略

Rebecca Grant 於 2016 年清楚地描述了由美國國防部長布朗所主導的第二次抵銷戰略，前蘇聯的戰車、戰機、火炮等傳統武器裝備數量對美國佔有極大優勢，1950 年代美國發展核打擊能力，足以威懾前蘇聯。但隨著前蘇聯在核武上的發展，美國已失去核武的優勢。在「大規模報復」軍事戰略的優勢地位喪失，傳統武器裝備的弱點等原因上，美國希望藉由創新思維，尋求解決之道，便將軍事科技的研發重點置於「精準導引彈藥」的研發，增進戰鬥車輛的機動力與火力、提高部隊通信能力以及研發新型武器投射載臺，使美軍逐漸具備精準打擊的能力，而為了延續第二次抵銷戰略的發展，即便執政黨有所輪替，仍持續投入金錢、時間，以達到政策的延續，[14]藉由本文獻可了解當時第二次抵銷戰略之背景及其當時武器裝備之發展。

三、第三次抵銷戰略

（一）中文文獻

劉一鳴及石海明從技術層面剖析了第三次抵銷戰略的內涵以及其邏輯思維，但在結論部分僅以中國大陸立場審慎看待美軍此戰略之發展，加速中國大陸國內的技術創新發展，並未提出具體可因應之構想。美軍第三次抵銷戰略中，其所欲「抵銷」的潛在對手為中共，目的在從各層面對中共的崛起進行遏制。第三次抵銷戰略仍然將過多資源投入在技術方面，但未來的對手能夠迅速縮短與美國的技術差距，真正需要被改善的是美國古板、僵化的國防採購系統。若僅追求技術上的進步，最終美國將會失去其軍事霸權，現階段美國面臨的國際環境更加複雜多元，過去兩次抵銷戰略的時代背景，所處的是一個威脅分明的兩極世界。目前及未來，所面臨的是不確定且多極的環境，再者，抵銷戰略也並非單一的國家戰略或是國防戰略，而

---

[13] Samuel F. Wells, “The Origins of Massive Retaliation,” *Political Science Quarterly*, Vol. 96, No. 1,1981,pp. 31-52.

[14] Rebecca Grant, “The Second Offset,” Jul. 2016.At http://www.airforcemag.com/MagazineArchive/Documents/2016/July%202016/0716secondoffset.pdf（Accessed 2017/10/16）

僅是國防部政策的構想、框架，不僅需要國防部配合，更需要國會的支持、各軍種的配合、工商業界的合作，甚至是外交政策的因應，如何進行跨部門的整合，是相當嚴峻的考驗。[15]

郭瑞鵬除闡述新視野戰略至第三次抵銷戰略之時代背景外，亦提出了美國在推動第三次抵銷戰略中將會面臨的困境，[16]明確指出第三次抵銷戰略在推動上可能遇到的問題，但結論亦無提出具體建議，而美軍未來將提出的解決方法，亦值得吾人持續觀察。

（二）外文文獻

美國戰略與國際研究中心（Center for Strategic and International Studies ,CSIS）於2017年三月發布了一篇《評估第三次抵銷戰略》(Assessing the Third Offset Strategy)的報告，第三次抵銷戰略重點發展的五個技術領域：自主學習系統、人機協同決策、機器輔助人員作戰、先進有人-無人編隊作戰、網路賦能自主武器，[17]該報告匯集了美國國防部高級官員、戰略專家、國防企業高階管理人等各方專家對第三次抵銷戰略相關問題的討論與分析，有助於吾人更深入認識美第三次抵銷戰略未來的發展與走向。

James R. McGrath在「美國聯合部隊季刊」指出，在美軍提出的第三次抵銷戰略中，先進的資訊作戰力扮演相當重要的角色，在作戰環境（尤其是資訊環境）的改變下，美國敵人藉由對資訊空間，特別是在操作資訊和認知面向的創新運用，逐漸削弱美國所擁有的優勢。先進資訊作戰實彈(兵)、虛擬暨建構式模式模擬系統或許不是第三次抵銷戰略唯一被重視的領域，但若不能夠認清其重要性，將會造成重大的錯誤。這些資訊作戰模式模擬能力，應當是任何未來先進、半自主全球效用系統的基礎和重心。因此，先進資訊作戰模式模擬絕對是不可或缺的能力，可讓聯合部隊充分獲得持久不對稱優勢，達到第三次抵銷戰略成功之目標，[18]本文作者清楚的臚列現代資訊作戰當中重要的領域及工具，對於本論文研究有莫大助益。

---

[15] 劉一鳴、石海明，〈技術致勝：美軍第三次抵銷戰略評析〉，《指揮與控制學報》，第 2 卷第 2 期，2016 年 6 月，頁 167-171。

[16] 郭瑞鵬，〈第三次「抵銷戰略」的困境〉，《軍事文摘》，第 13 期，2016 年 7 月，頁 6-9。

[17] Jesse Ellman, Lisa Samp, and Gabriel Coll, *Assessing the Third Offset Strategy*, (Washington DC: CSIS, 2017).

[18] James R. McGrath, "Twenty-First Century Information Warfare and the Third Offset Strategy," *Joint Forces Quarterly* , No. 82, 2016 pp.16-23.

Timothy A. Walton在提出針對戰略、想定、評估程序，就投資優先項目和兵力規劃的建議，美國面臨許多需要克服的挑戰，第一，先進的反介入與區域拒止系統，將可能擴散到目前已部署這些系統以外的更多國家；第二，反介入與區域拒止作戰網路(感測器、指揮、管制和通信，以及武器)將趨成熟，並且朝精密、區域與全球覆蓋範圍改進；第三，中共將可能持續發展更適合全球兵力投射的戰力、態勢及部隊，其進步幅度將遠超過目前區域霸權的估計，而囿於時間和資源受限，每一個改革都充滿了挑戰和困難，[19]而此戰略後續的發展，則有賴吾人持續觀察。

Peter Dombrowski指出歐巴馬總統執政時代，當時的政策為「重返亞洲」，在2017年1月川普就任後，主要政策以「美國優先」。雖然如此，中共所推動的一帶一路、亞投行等等的經濟策略，都使美國無法忽視其經濟增長與軍事科技的發展強盛，亞太成為世界經濟成長的中心，人民幣的在金融市場的影響，以及中共的軍事現代化，及其外交與安全政策上一連串的積極作為帶來的潛在威脅，[20]本篇主要將美國在亞太地區所發展的軍事聯盟與中共對美的威脅實施連結，一切都考驗著美國國防部長如何在其盟軍與中共的威脅當中，找出最適當的解決方法，而文章中另一重點則提及了網路戰的趨勢與重要性，在未來的生活之中，萬物都要使用網路，如車聯網、智慧城市、智慧家庭、工業4.0等應用，未來的戰場將是在網際網路之中，只有比對手更快研發出「絕對優勢」的科技，方能在戰場中，取得先發制人的機會。

美國前國防部長黑格(Chuck Hagel)在2014年11月15日發布了「國防創新倡議」，文件中寫到，美國欲在二十一世紀以創新的方法保持美軍領先的軍事能力，並改善整個部門業務運作的模式，因為現階段美國在作戰方面的優勢正逐漸消失，而潛在的對手不僅致力發展軍事現代化的建設與發展，也獲得長足的進步與軍事能力，這對於美軍的軍力是相當明確而且持續增強的挑戰，而此狀況亦將會持續下去。與此同時，面臨美國國內財政的壓力，國防預算的裁減，將會限制美國發展創新、敏捷的國防戰略，因此美國國防部必須動員全軍單位，在有限的資源之下尋求創新的方

[19] Timothy A. Walton, "Securing the Third Offset Strategy," *Joint Force Quarterly*, no. 82, 2016, pp.6-15.
[20] Peter J. Dombrowski, "America's Third Offset Strategy: New Military Technologies and Implications for the Asia Pacific," *S. Rajaratnam School of International Studies*, June 2015. At http://www.rsis.edu.sg/wp-content/uploads/2015/06/PR150608_Americas-Third-Offset-Strategy.pdf (Accessed 2017/9/26)

法，以維持甚至擴大美軍的軍事優勢。[21]黑格所發布的這份文件大略的寫出美國所面臨的威脅與困難，亦提出了第三次抵銷戰略的概念，將欲改革或研發的領域提出，本文獻的重要性在於首次提出第三次抵銷戰略之概念，但僅是描繪大略，較詳細的部分仍是有賴其智庫或其他釋出的官方文獻。

Michael E. Hutchens等人介紹了「全球公域介入及機動聯合構想」(Joint Concept for Access and Maneuver in the Global Commons: A New Joint Operational Concept, JAM-GC)的發想，是為了取代「空海一體戰」（Air-Sea Battle），此構想聚焦於擊潰敵人的計畫與企圖，本身是屬於戰爭的作戰層次，也是遂行戰略的手段，對「全球公域」的定義，作者解釋為「不屬於任一國之空、海、太空及網路空間區域」，陸地領域則不屬於全球公域，因為所有適合居住的陸地均為各國或國家實體擁有。第二次世界大戰以來，美國的兵力投射不受任何限制與挑戰，這種來去自如的情況，也使得確保作戰介入的思維、計畫作為與作戰再也不是首要目的。但時至今日，美國的潛在敵人致力於獲得強大、先進的科技與軍事能力，以反制美國及盟邦兵力投射，不斷侵蝕美國傳統軍事優勢，這些能力不僅是飛機、潛艦、水雷與飛彈等傳統武器，更包括太空與網路空間等領域的新興能力，其中用於反制美國兵力投射，以及挑戰介入及機動之武器與手段，可總稱為反介入與區域拒止能力。[22]作者提出為肆應作戰問題之種種挑戰，未來聯合部隊必須能分散配置、迅速恢復、靈活調整，以及在充分規模下與足夠期程內執行任務，此文獻價值在於揭櫫有關美軍第三次抵銷戰略在戰術部分之內容構想，此一構想為各軍事部門及各軍種提供一套統一的合作架構，使聯合部隊能夠持續保持在全球投射美國兵力的能力。

國防大學
National Defense University

[21] Chuck Hagel, "The Defense Innovation Initiative," *DoD, Washington* Nov. 15,2014.At http://www.defenseinnovationmarketplace.mil/resources/DefenseInnovationInitiative.pdf (Accessed 2016/09/30)

[22] Michael E. Hutchens et al., "Joint Concept for Access and Maneuver in the Global Commons A New Joint Operational Concept," *Joint Force Quarterly*, Jan. 2017.At http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-84/jfq-84_134-139_Hutchens-et-al.pdf?ver=2017-01-27-091816-550 (Accessed 2017/9/20)

四、資訊作戰

有學者對資訊的概念解釋如下：資訊是我們適應於外部世界，並使這種適應為外部世界所感知的過程中，與外部世界進行交換的內容的名稱，能夠用來消除不確定性的東西，並通過文字、數據和各種信號來傳遞、處理和表現客觀事物特性的知識流；資訊比情報的概念寬泛，是指消息、數據、情報、知識，是生靈萬物相互賴以生存和進化的訊息，是人類感受到的客觀存在和差異，資訊的特性有四，一是要依附於各種形式的載體（運載工具），二是資訊具有價值和共享性；三是資訊具備可處理性；四是資訊具有時效性。[23]

資訊戰的基礎是資訊，其涉及的基本理論相當深刻廣泛。1996年美國陸軍部頒布的《FM100－6 資訊行動》(Field Manual－6 Information Operation)條令稱，資訊戰是在「軍事資訊環境中，在確保己方部隊可自由地採集、處理資訊並根據所獲得資訊採取行動的情況下，在各種條件下實施的勝敵一等的、不間斷的軍事行動」。美國國防大學校長塞爾姜中將認為：「資訊戰是以奪取決定性軍事優勢為目的、以實施資訊管理和使用為中心而進行武裝鬥爭的手段」。美國空軍大學政治學教授喬治斯坦認為：「資訊戰是利用資訊達成國家目標的行動……。也可以把資訊戰視爲部分地通過全球聯網的資訊與資訊手段進行的國家間衝突」；俄國軍事理論家卡莫夫則認為：「資訊戰可定義為，在準備和實施軍事行動的過程中，為奪取和保持對敵資訊優勢，按統一的意圖和計劃而採取的一整套資訊保障、資訊對抗和資訊防護措施」。[24]布蘭克拉克則認為，資訊戰是一項整合功能，基本上是包括資訊及資訊系統之特定力量的整合，而資訊戰的目的在於運用資訊及資訊系統去影響所望目標決策者及聽眾的作為，相對的，資訊戰亦防護友軍決策者及聽眾免於敵人資訊或資訊系統的不當影響。[25]Leigh Armistead認為，資訊戰包含六項組成要件：電腦網路攻擊、欺敵行動、摧毀行動、電子戰、作戰安全、心理作戰，且大部分與實際戰

---

[23] 嚴怡民，〈今日天涯若比鄰:著名科學家談信息科學〉(廣西師範大學出版社，1999 年)，頁 10-11。

[24] 王保存、劉玉建，〈外軍信息戰研究概覽〉，(北京：軍事科學出版社, 1999)，頁 18。

[25] Blane Clark、Dennis M. Murphy 著，國防大學譯印，〈資訊戰入門〉(桃園：國防大學，2010 年 12 月)，頁 9-10。

鬥期間的作戰遂行有關。[26]

吳奇英將「資訊戰」的定義總結為：它是一種利用資訊及資訊系統，採取摧毀、破壞、阻絕、干撓、誤導、說服和箝制等方式，迫使敵方的資訊和資訊系統無法發揮作用；同時保護自己免受上述攻擊，並藉絕對資訊優勢，掌握「制資訊權」，以澈底動搖、弱化敵人的信心與鬥志，從而達成國家目標的行動。[27]

美國的四大國力是政治、經濟、軍事、資訊，資訊指的就是資訊力，而心理作戰則是資訊力的核心能力之一，大抵而言，心理作戰的定義是指對付敵人、其指揮官，以及其官兵政治意志的行動，也包括對準任何有能力向敵人或友軍表示同情或支持第三方的告知或影響作業。基本上，美國心理作戰在美國對外行為中，不論外交或軍事，都具有舉足輕重的地位，無論在作戰計畫的形塑階段，或是嚇阻的階段都尤其重要。過去，心理作戰總是不離「宣傳」一詞的定義框架，但現今已經能夠接受美軍心戰部隊此一國家資產運用於國內（領土內）災害救援時之信息散布的功能，而非僅限於傳統影響公眾心理或行為的負面刻板印象。換言之，美軍心理作戰之影響力未曾稍減，更是持續運用於各項軍事行為之中，[28]

William R. Gery等人認為，在網路科技蓬勃發展的時代，許多裝置間更加的相互依賴，以發揮其功能，如運動手環、手機、個人電腦、工作電腦、居家監視系統、汽車、網路電視、印表機、掃描器及地圖，進而建立出「物聯網」的機制，而「互聯」的概念並不僅有物聯網而已，還包括改變網際網路的資訊，以及資訊如何影響我們的日常決策。[29]本文以俄羅斯持續發動資訊作戰入侵克里米亞的成功案例，指出美國當前的軍事組織，已無法因應快速變遷的資訊時代，進而呼籲美國政府應成立以資訊作戰為重點部門，鼓勵在資訊空間裡發揮創新思維、具備高度的適應力與靈活度。作者在文章中明確指出發展資訊作戰之必要性，並提出建議。

Martin C. Libicki 提到，網路攻擊與傳統的武力攻擊不同，不應該受限於過去

---

[26] Leigh Armistead 著，國防部譯印，〈資訊作戰〉（台北市：國防部史政編譯室，2012 年 5 月），頁 68-69。

[27] 吳奇英，〈資訊時代政治作戰中心理戰的運用與發展-以美伊戰爭及兩岸資訊心理戰為例〉《復興崗學報》，第 85 期，2005 年，頁 80-81。

[28] 曾維國，〈廿一世紀美國心戰部隊的發展研究〉，收錄於洪陸訓、莫大華編，《廿一世紀歐美主要國家心戰部隊的發展》（台北：國防大學政治作戰學院，2011 年），頁 1。

[29] William R. Gery, SeYoung Lee, and Jacob Ninas, "Information Warfare in an Information Age," *Joint Force Quarterly*, No.85, April 2017,pp.22-29.

作戰方式的標準作業程序，網路攻擊的首要目的在於動搖敵軍心智、打擊敵軍自信，所以網路攻擊的特色與程序將會對未來的作戰型態帶來全新的樣貌。作者認為，欲管制網路攻擊的效果就必須要控制網路戰士，在實體世界中，無論是指揮或管制，皆受益於日漸普及的監視及通訊網路的擴散，戰爭的實體成效可以一絲不苟的被歸檔及分析。但是在網路的空間中，任何地方都能敲擊鍵盤，在無法明確假定一次攻擊對某類目標所代表意義為何時，更別提可以預判網路攻擊的可能成效。在這樣的情況下，標準作業程序就成為一個糟糕的基準。作者認為網路戰爭的指揮者必須被賦予權力，讓他們能夠迅速、適當的處理危機，進而卻選擇是否該遵循標準作業程序，或是跳脫這樣的思考框架。[30]

Edward C. Cardon 等人認為，資訊產業的快速發展，使戰爭的範圍拓展到網路社群及雲端空間，資訊的特殊在於有其時效性，其威脅來源則可能來自具備高度能力與豐沛資源的國家層級人員、恐怖主義與犯罪之組織及個人，以及激進駭客。與傳統戰爭相比，美國目前並不具有壟斷網路空間作戰的手段，美軍必須評估其優勢與弱點，貼合實際環境，承認創新的解決方案可能同時來自內部與外部，網路空間反覆無常的本質與快速演變的技術與實務，需要靈活和適應性強的網路空間實力，如同在實戰經驗中所示範的，網路所造成的影響，將作戰機動和任務指揮與網路空間能力相結合。作者在結論中提到，隨著作戰模式的轉變，未來陸上的優勢將轉變至網路作戰的能量，而為確保美軍的優勢地位，領導幹部應優先考量創新與專業建議，並提供其資源或發展條件，以達到目的，[31]但在文章中提出理論與實務上的衝突，並點出當中問題，實際生活中，組織文化所形成既定的生態，往往影響創新思維的發展，

Daniel P. Taylor認為，美國海軍的戰力已擴及網路，這象徵著其技術的里程碑，網路攻擊在海軍戰略中所扮演的角色日益吃重，但目前在運用網路攻擊時，美國海軍仍是略顯生澀，那是因為它屬於一種嶄新而且未經測試的戰術，且該能力的未來發展方向上不十分明確，而這並非只是戰術上的問題，其中也包括了組織文化，許

---

[30] Martin C. Libicki, "Planning a Cyberwar,"*Proceedings Magazine*,Oct 2016,At https://www.usni.org/magazines/proceedings/2016-10/planning-cyberwar (Accessed 2017/9/20)

[31] Edward C. Cardon, David P. McHenry, and Christopher Cline 著，趙炳強譯，〈網際空間作戰中創新重要性(The Relevance of Culture: Recognizing the Importance of Innovation in Cyberspace Operations) 〉，《國防譯粹》，第 44 卷第 3 期，2017 年 3 月，頁 22-28。

多已經習慣傳統戰鬥方式的幹部，可能會對嘗試某些嶄新且未經測試的攻擊敵防衛措施抱持懷疑的態度，[32]從本篇文章中能夠了解到，網路攻擊的戰術已持續在發展，但組織僵化往往是一個企業乃至於部隊環境進步的阻礙，即使網路的重要性顯而易見，但最終的走向，卻仍是取決於領導者的決策，而這對我國軍隊來說，情況似乎有些類似。

Bindiya Carmeline Thomas提到，網路空間弱點評估/獵殺武器系統所提供的網路安全能力，可以深入評估諸如電腦、基礎設施、應用程式、數據及網路作戰等方面的資訊系統資產。[33]

Daniel Stefanus認為美國海軍無可避免的遭遇到無法完全運用電磁頻譜的狀況，水面部隊必須研擬創新與決定性的戰術，方能克敵致勝。更重要的，是適應通信拒止的環境，這仰賴的則是各層級指揮官的訓練及溝通關係，再由全軍官兵引領戰術的發展，並加強回饋與知識共享，最後，為未來裝備引進新觀念，了解並掌控黑暗作戰是必要的規範轉變，如此將確保美國海軍於全球戰場空間的持續優勢。[34]

以下幾點是在文獻探討中歸納出的心得，第一、部分文獻帶有強烈個人主觀意識，認為資訊作戰發展未獲得國家重視，如Daniel P. Taylor在Force Multiplier：Navy Looks to Develop Cyber Capabilities as Part of Its Air Warfare Domain所述。第二、網路空間重要性常被提及，但深入性不足。第三、對於美、中網路部隊發展研究的文獻較缺乏。以上都是在本次論文研究中將盡力補足的方向。

國防大學
National Defense University

---

[32] Daniel P. Taylor 著，劉慶順譯，〈戰力加乘因子：網路能力（Force Multiplier：Navy Looks to Develop Cyber Capabilities as Part of Its Air Warfare Domain）〉，《國防譯粹》，第 44 卷第 3 期，2017 年 3 月，頁 30-33。

[33] Bindiya Thomas 著，黃文啟譯，〈網路反恐新概念：網路應變能力（Resilience－the Solution to Cyber Terrorism?）〉，《國防譯粹》，第 44 卷第 3 期，2017 年 3 月，頁 34-39。

[34] Daniel Stefanus,"Embracing the Dark Battle：Electronic Warfare, Distributed Lethality, and the Future of Naval Warfighting," *Proceedings Magazine*,April 2017.At https://www.usni.org/magazines/proceedings/2017-04/embracing-dark-battle (Accessed 2017/08/20)

第五節 研究架構與章節安排

本研究為探討美國歷史上三次的「抵銷戰略之形成因素，受當時國內外政治經濟環境趨勢的影響，所規劃出的國家發展與外交戰略。闡述抵銷戰略之緣起，並分析在美國實施第三次抵銷戰略後，對兩岸可能造成的政治與軍事方面之影響，且觀察中共對於美國第三次抵銷戰略之因應，作為我國未來在因應中共政治、經濟與軍事的強勢拓展下，制定政策之參考。由此，期能達到所設定之研究目的。

一、研究架構

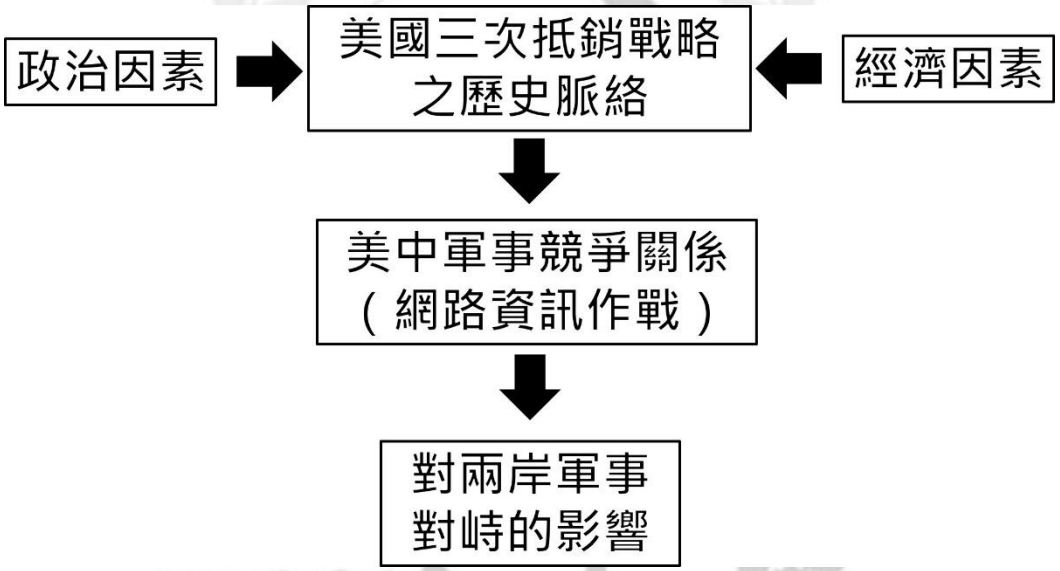

圖 1- 1　研究架構圖

資料來源：筆者自繪

國防大學 National Defense University

二、章節安排

本論文共區分五章十九節，第一章為緒論，第二、三、四章為本文，第五章為結論。以下筆者僅就各章節安排作說明：

第一章為緒論，本章共計五節，主要針對主要對研究動機與目的、研究方法、研究範圍與限制、文獻探討、章節安排與研究架構作說明。

第二章為美國三次抵銷戰略的戰略目標與比較分析，本章內容將闡述美軍自

1950 年代為抵抗前蘇聯之及其共產勢力所提出之新視野戰略、1970 年代為應對前蘇聯所發展之核武所提出的第二次抵銷戰略，以及為持續美國的軍事優勢，於 2014 年所提出的第三次抵銷戰略之概念，分析其成因背景，以及後續之影響。本章內容包括四節：第一節—美軍第一次抵銷戰略之緣起與意涵；第二節—美軍第二次抵銷戰略之緣起與意涵；第三節—美軍第三次抵銷戰略之緣起與意涵；第四節—小結。

第三章為美、中網路資訊作戰之發展，本章將闡述資訊作戰應用於科技上之演進，以及於軍隊中所扮演之角色與影響，藉以給予我國未來資訊作戰之啟發與建議。本章內容如下：第一節—網路資訊作戰之本質與特色；第二節—美軍網路資訊作戰之發展與運用；第三節—中共網路資訊作戰之發展與運用；第四節—小結。

第四章為美軍第三次抵銷戰略對兩岸軍事對峙之影響，本章著重於中共之看法及回應，分析第三次抵銷戰略對美、中、臺關係所造成之影響。本章內容包括四節：第一節—美中競合下的兩岸關係；第二節—我國資訊產業發展現況；第三節—我國因應之國防與軍事戰略；第四節—小結。

第五章為結論，研究發現的部分，將會綜整前述各章節的研究與分析，依本論文之研究內容，分析說明美國如何對國家本身之政治、經濟與外交政策實施戰略調整，藉以延續美國在世界領先之地位，以及對我國通資電部隊發展之啟發與建議；另本論文之研究為正在進行式，因此也會針對後續值得深入探討與研究之部分提出相關建議，作為往後持續深入研究的基礎。

本文章節大綱安排如下：

第一章　緒論

第一節　研究動機與目的

第二節　研究途徑與研究方法

第三節　研究範圍與限制

第四節　文獻回顧

第五節　研究架構與章節安排

第二章　美軍三次抵銷戰略的戰略目標與比較分析

第一節　美軍第一次抵銷戰略之緣起與意涵

第二節　美軍第二次抵銷戰略之緣起與意涵

第三節　美軍第三次抵銷戰略之緣起與意涵

國防大學 National Defense University

第四節　小結
第三章　美中網路資訊作戰之發展與運用
第一節　網路資訊作戰之本質與特色
第二節　美軍網路資訊作戰之發展與運用
第三節　中共網路資訊作戰之發展與運用
第四節　小結
第四章　美軍第三次抵銷戰略對兩岸軍事對峙之影響
第一節　美中競合下的兩岸關係
第二節　我國資訊產業發展現況
第三節　我國因應之國防與軍事戰略
第四節　小結
第五章　結論
第一節　研究發現
第二節　未來研究建議

國防大學
National Defense University

第二章　美軍三次抵銷戰略的戰略目標與比較分析

在第二次世界大戰結束後，以歐洲為中心的國際關係體系進入了美蘇競爭與對抗的兩極體系，歐洲的大國中，英、法在戰爭中遭到重創，原有的殖民地走向獨立，國家實力和影響力一落千丈；德國和義大利在第二次世界大戰中徹底失敗，德國被戰勝國分區佔領，以歐洲為中心的國際關係已然結束。美國在戰爭中得到飛速的發展，蘇聯也通過戰爭的考驗，成為了政治軍事大國。在戰後的國際關係和國際政治中，美國和蘇聯在履行戰時協議、處理國際問題上產生了意見分歧與衝突，再加上社會制度、意識形態和國家利益的差異，美國和蘇聯形成了處於對立的兩極。軍事安全為美蘇首要關注議題，兩個超級大國為了爭奪軍事戰略優勢，展開了毫無止境的軍備競賽，不斷擴大軍事活動的範圍，形成了「安全困境」。美蘇兩國都認為軍事安全高於一切，雙方都欲佔據優勢的軍事力量和核嚇阻能力，兩國都將對方為了自身安全採取的增加軍備措施視為對自己的威脅，將對方的行為視為圍堵與挑釁，如此你來我往，軍備競賽越演越烈。

冷戰結束後，蘇聯解體成為「獨立國協」(Commonwealth of Independent States)，仍由俄羅斯領導，但已不復以往蘇聯具備的實力。反之，中國大陸經濟改革開放後，國力逐漸增強，美國為因應競爭強國國力的大幅提升，遂採取抵銷戰略因應，以維持美軍的戰力優勢，並遏制戰爭爆發。

面對不同對手的在政治、經濟以及軍事上的挑戰，美軍傾力擘劃足以扭轉戰局的戰略，以維護其霸權地位。因此，本章將說明美軍三次抵銷戰略所發生之歷史背景與戰略構想，並加以分析。

第一節　美軍第一次抵銷戰略之緣起與意涵

雅爾達和波茨坦會議確立了戰後國際體系，規定了大國應該遵守的遊戲規則，特別是美、蘇兩大國，也形成美蘇勢力範圍的重新劃分。蘇聯依據雅爾達協議鞏固了沙俄在東歐與東亞的傳統勢力範圍，美國也掌控了日本和西歐，然而對於雅爾達協議沒有規範的南歐與中東地區，及新興的原子武器管制上，美蘇的歧異也逐漸擴大。雅爾達體系的建立，是大國外交、強權政治、實力政策和美蘇妥協的結果，勢力範圍的區分為戰後的美蘇對立與對抗埋下了禍根。蘇聯謀求國家的安全，視東歐為自己的勢力範圍，希望在此擁有充分的行動自由，不容美國等

西方國家干涉。在建立和鞏固勢力範圍與確保國家安全時，採取了一切可能的措施，美國一心要建立世界霸權，不許蘇聯對其利益與權威提出挑戰，並保護資本主義的中心－歐洲。而蘇聯則要按照自己的意志改造東歐，兩相衝突下，歐洲便成為戰後美蘇對立的主要地區。

一、時空背景

1945 年 9 月，日本簽屬投降書，第二次世界大戰正式宣告結束，蘇聯作為二次世界大戰的主力，軍事力量和國際影響都空前增強，蘇聯更徹底消除資本主義所帶來的威脅感。在資本主義大國中，德國、義大利、日本戰敗，處於被佔領狀態；英、法雖然勝利，國力明顯衰弱；美國雖然強大，卻遠在太平洋一端。史達林認為，當下國家戰略目標應當擴大並維護社會主義陣營，在與美國的爭奪中取得優勢，即使國內經濟困難，飢荒遍野，仍將增加國防實力置於首位。戰爭結束五個月後，史達林在莫斯科發表重要演說，頌揚蘇維埃制度，將二戰勝利結果片面歸於蘇維埃社會制度，更大肆批判資本主義對世界經濟帶來衝突與危機，[35]將資本主義與戰爭劃上等號，此演說一發表，便在西方造成了強烈反彈，加劇了雙方的不信任。1946 年 2 月，時任美國駐蘇聯大使館喬治・肯南（George Kennan）發表了著名的八千字長電報，內容涵括了蘇聯對世界的看法，分析了蘇聯外交政策，亦提出了美國對蘇聯政策的設想，這篇電文也反映了美國國內主張對蘇聯採取強硬態度的立場，也成為了美國制定對蘇政策的邏輯依據。[36]同年三月，正值美蘇關係未來發展的關鍵時刻，英國首相邱吉爾發表演說，並呼籲美國肩負起領導世界的責任，建立英美兩國特殊關係，更稱世界被「鐵幕」(Iron Curtain)分裂為兩個對抗的部分。[37]邱吉爾的演說公開道出英國的想法與立場，也表達美國圍堵蘇聯與共產主義的需要，為美國圍堵戰略的制定與實施做了準備。

---

[35] 米洛凡・吉拉斯，《同斯大林的談話》(北京：世界知識出版社，1989 年)，頁 122。

[36] George Kennan, "The Charge in the Soviet Union (Kennan) to the Secretary of State ," *George Washington University,* Feb. 22, 1946.At https://nsarchive2.gwu.edu//coldwar/documents/episode-1/kennan.htm (Accessed 2017/3/23)

[37] Winston Churchill, " Iron Curtain," *USA.gov,* Mar. 5, 1946.At https://www.cia.gov/library/readingroom/docs/1946-03-05.pdf (Accessed 2017/3/23)

另一方面，第二次世界大戰勝利後，由蘇聯所主導的共產主義勢力在全球蔓延，蘇聯支援東歐各國的社會主義革命，但實質上則將其收為從屬國，又推動中國、北韓以及越南等亞洲國家的革命，也幫助非洲各國獨立。西元 1945 年到 1949 年間，東歐和亞洲各地共產政權快速建立，共產主義的赤化與野心，無疑對國家安全造成極大威脅，使得以美國為首的自由民主國家產生強烈及迫切的危機意識。

1947 年 3 月 12 日，杜魯門總統發表國情咨文，要求對希臘與土耳其提出經濟與軍事援助，主張：「自由人民正在抵抗少數武裝份子或外來勢力征服之意圖，美國政策必須支持他們。」[38]杜魯門總統認為，共產主義對於國際和平與美國國家安全造成巨大威脅，依據杜魯門主義所提出的報告與法案，美國提供希臘政府六億四千八百萬美元的援助，而其中軍事物資占五億兩千九百萬美元，以防止當地落入共產黨手中；並實施「馬歇爾計畫」，四年之間投下一百三十億美元對歐洲進行援助，除了使歐洲經濟得以復興外，更促成西歐的整合，也奠定「歐洲聯盟」（European Union）的基礎。[39]美國亦透過與世界超過 50 多個國家相互締結軍事條約，以建立具全球性的軍事安全組織架構，與許多友邦及非共產國家簽訂一連串之公約組織，諸如：北約組織（North Atlantic Treaty Organization, NATO）、東南亞條約組織（Southeast Asia Treaty Organization, SEATO）、中部條約組織（Central Treaty Organization, CENTO）、美澳紐安全條約組織（Australia, New Zealand, United States Security Treaty, ANZUS）、美洲國家組織（Organization of American States, OAS），故在圍堵上產生了相當效用。同時利用美中、美韓、美日、美非及美西等雙邊條約之簽訂，逐步在亞洲、歐洲、非洲與美洲建立完整的防禦體系，以有效圍堵共產勢力在歐亞地區的侵略與擴張。

杜魯門以圍堵政策取代了前總統羅斯福的大國合作與集體安全，孤立主義正式結束，利用民眾對共產主義的恐懼心理，說服民眾接受冷戰外交政策，並以反對共產主義為由，廣泛介入與干涉別國內政，積極推行霸權主義和強權政治。冷

---

[38] Harry S. Truman," Special Message to the Congress on Greece and Turkey: The Truman Doctrine," *The American Presidency Project*, Mar. 12, 1947.At http://www.presidency.ucsb.edu/ws/?pid=12846 (Accessed 2017/3/23)

[39] Harry Bay, *The Marshall Plan and Its Meaning*（New York :Connell University Press,1955）,p.398.

戰逐漸變成一種國際體系，美國通過援助和保衛自由把世界一分為二，杜魯門主義明確、公開的提出反對共產主義是美國國際戰略的中心環節，美國參議員James William Fulbright 為此寫到：「杜魯門主義中的反共主義遠遠超過其他因素，一直是二戰之後美國外交的主要思想。」[40]1950 年代至 1960 年代初，國際關係處於冷戰的高潮，美國的杜魯門、艾森豪、甘迺迪三任總統則持續推行圍堵政策。

二、軍事戰略

冷戰期間，美國推動西德的重新武裝和北約的擴大，北約的成員國由原來的十二個增加到十五個，更扶植日本簽訂美日安保條約，結成戰略聯盟，並與菲律賓、泰國、韓國、台灣簽訂共同防禦條約，組成軍事同盟。美國還通過美澳紐安全條約和東南亞條約，在亞太地區構築對抗共產勢力的防禦屏障，包圍蘇聯及中國；蘇聯組織東歐國家，建立了華沙條約組織，歐洲形成北約與華沙兩個軍事政治集團的對抗，德國首都柏林一分為二，以柏林圍牆區隔，美蘇坦克在兩側對峙，而冷戰也從歐洲逐步擴展亞洲、中東和拉丁美洲，殖民帝國的瓦解和民族獨立與革命運動的蓬勃發展，成為美蘇所爭奪第三世界地緣政治真空的主要內容。美蘇在冷戰期間展開了激烈的軍備競賽，軍事科技的進步與發展，加劇了全球權力的轉換和力量對比的變化，許多新技術已經或即將用於戰爭，傳統武器表現出巨大的殺傷力和破壞力，特別是原子武器的出現和使用，對國際關係的發展具有重大且深遠的影響。原子武器是一種毀滅性的武器，是影響國際體系穩定和發展的重要因素，各方為防止遭到對手突然的攻擊以及確保國家安全而拼命擴充軍備，蘇聯為打破美國的「核壟斷」，則是加速擴充蘇聯的核力量，美國則是千方百計保持對核武的壟斷或主導地位，[41]1949 年 8 月，蘇聯成功試爆第一顆名為「南瓜」的原子彈，隨著本次的試爆成功，美國核壟斷不復存在，亦表示美國所擁有核嚇阻的軍事優勢面臨挑戰。

在軍事方面，美國在 1950 年 4 月初提出編號 NSC68 的報告文件中指出，因為美國軍力不足而無法有效圍堵前蘇聯共產勢力的擴張，並預判蘇聯在 1954 年

[40] James William Fulbright 著，伍協力譯，《跛足巨人-美國對外政策及其國內影響》（北京：上海人民出版社，1976 年），頁 24。

[41] 劉金質，《冷戰史上》（北京：世界知識出版社，2003 年），頁 7。

將擁有約 200 枚的核彈頭。因此，為有效因應未來可能爆發的區域衝突或全面戰爭，政府必須大幅增加國防預算，建立與加強西方戰略同盟，擴充軍備建設，全面圍堵蘇聯和共產主義，建構足以抵抗與嚇阻前蘇聯軍事侵略的大規模常規武力的軍事力量。[42]在韓戰爆發前夕，美國全軍規模低於一百五十萬人，而在共產主義逐漸崛起後，美國為對抗共產勢力，一年內，美軍部隊便擴增至三百三十萬人。1953 年，美軍部隊更達到了巔峰的三百六十萬人，在韓戰末，越戰初期，美軍武力未曾低於兩百五十萬人，平均人數約在二百八十萬人左右。[43]但當時正在競選總統的艾森豪將軍則持相反意見，認為杜魯門的政策將會過度耗費美國的國力，並且指出前蘇聯的戰略目標，是美國和其盟友將部隊和金錢投注於東亞的邊緣衝突，[44]迫使美國進行軍備競賽進而導致破產。當時美國為振興國內戰後經濟發展，準備執行減稅方案，若聯邦政府的稅收大量減少，又將經費大量挹注至國防發展，將會造成收支失衡，導致財政赤字快速惡化。[45]因此，艾森豪總統在 1953 年初執政後，便召集幕僚組成專案委員會，重新檢視國防政策，並根據兩項基本原則執行「新視野」的戰略規劃：一是建立足以嚇阻共產主義勢力侵略的軍事力量，二是在不能危害國家經濟體系與發展為前提下，有效維繫足以嚇阻共產勢力侵略的軍事能力。[46]國家的經濟穩定與軍事能力密不可分，若是國家經濟發展走向衰竭，那麼亦無能力維持穩定的軍事力量，美國國家戰院積極尋找出異於杜魯門總統政策之替代方案，於西元 1953 年 6 月成立「日晷專案」（Project Solarium）[47]，該專案研究發現，與前蘇聯相比，美軍傳統部隊數目大幅低於蘇聯，但美軍在核武的數量上仍維持相對的優勢地位，具體而言，與其耗費大量國防經費發建立傳統軍力來對抗前蘇聯的威脅，不如加強軍事科技的發展，並運用

國防大學 National Defense University

[42] Paul H. Nitze, "NSC 68: United States Objectives and Programs for National Security," in Ernest R. May, ed., *American Cold War Strategy: Interpreting NSC* 68 (Boston: Bedfort Books, 1993), pp.23-80.
[43] Herman S. Wolk,"The New Look,"*Air Force Magazine*, Aug. 2003.At http://www.airforcemag.com/MagazineArchive/Documents/2003/August%202003/0803look.pdf (Accessed 2017/10/24)
[44] Peter Grier, "The First Offset," *Air Force Magazine,* Jun. 2016.p.57.
[45] Richard M. Leighton, *History of the Office of the Secretary of Defense. Volume 3: Strategy, Money, and the New Look 1953-1956,* (Washington：DC Office of the Secretary of Defense, 2001). pp. 65-68.
[46] United States Department of Defense, *Semiannual Report of the Secretary of Defense and the Semiannual Reports of the Secretary of the Army, Secretary of the Navy, Secretary of the Air Force, January 1 to June 30, 1953* (Washington D.C.: Government Printing Office, 1953), p. 3.
[47] John Lewis Gaddis, *Strategies of Containment: A Critical Appraisal of American National Security Policy During the Cold War* (New York: Oxford University Press, Jun. 23, 2005), pp. 145-147.

戰略性及戰術性核武，除可達到嚇阻的效果，對國防經費的需求也較低，同時也可以確保與健全美國經濟的長足發展。基此，美軍強調軍事科技的發展以抵銷對武裝人員數量的需求，並制定所謂「大規模報復」軍事戰略的概念，建立「先發制人核打擊」的能力，而此概念也成為「新視野」戰略規劃中重要的基礎。[48]

美國國務卿杜勒斯（John Foster Dulles）於 1954 年 1 月發表了一篇著名的演說，內容強調為了對付共產主義敵人的「強大的陸上力量」，美國將以其擁有之龐大核武庫做為「大規模報復」戰略之依靠，作為美國與其盟國最大限度威懾的工具。[49]1952 年底，美國國內核彈頭數量達 841 枚，蘇聯僅有 50 枚，此外，美國國內的可儲備量增長了兩倍，美軍以每年數百枚的速度增加，蘇聯則是不到 100 枚，[50]美國也成功測試了新的熱熔核裝置，使新型的核彈破壞力更加強大。當時，美軍核運送能力遠超過蘇聯，美國空軍使用遠程噴氣動力轟炸機，如 B-47 戰鬥機，B-52 戰鬥機也於 1955 年開始服役，相比之下，蘇聯的轟炸機相對落後，且蘇聯在美國附近沒有任何空軍基地，而美國則由在歐亞的盟國提供位於蘇聯邊界的基地。[51]

在「新視野」戰略預算執行方面，根據戰略和預算評估中心報告指出，自 1954 年至 1957 年，美國空軍約佔國防部預算的百分之四十七，而海軍約佔百分之二十九，陸軍佔百分之二十二，陸軍預算削減幅度最大，減少約百分之四十，1953 年，美國在國防預算上的支出在艾森豪總統執政時期達到了頂峰，當時約佔美國國內生產總額百分之十四，之後分段逐漸下跌，直到 1956 年降低至 425 億美元，約佔國內生產總額的百分之九點七。[52]

艾森豪總統認為韓戰之所以爆發，以及美國在遠東地區的圍堵政策執行成效

國防大學 National Defense University

[48] 李建昇, 〈美軍抵消戰略之發展歷程〉,《國防雜誌》, 第 31 卷第 3 期，2016 年 9 月，頁 52-53。

[49] John Forest Dulles, *The Evolution of Foreign Policy*, (New York：Department of State Bulletin,1954), pp. 107-110.

[50] Hans M. Kristensen and Robert S. Norris, "Global Nuclear Weapons Inventories, 1945-2013," *Bulletin of the Atomic Scientists*, Vol. 69, No. 5, November 18, 2013, p. 78.

[51] Peter Grier, "The First Offset," *Air Force Magazine*, Jun. 2016.At http://www.airforcemag.com/MagazineArchive/Magazine%20Documents/2016/June%202016/0616offset.pdf （Accessed 2017/10/24）

[52] Peter Grier, "The First Offset," *Air Force Magazine*, Jun. 2016.At http://www.airforcemag.com/MagazineArchive/Magazine%20Documents/2016/June%202016/0616offset.pdf （Accessed 2017/10/24）

不彰，原因為當時的杜魯門政府未對前蘇聯等共產國家清楚表達倘若發生戰爭，美軍將不惜代價運用核武的決心。[53]「大規模報復」的中心思想就是當前蘇聯實施軍事侵略而危害美國安全時，美軍可利用其核武的優勢，在欲達到的時間及地點，對前蘇聯本土實施大規模的核武反擊，對其造成無法承受之損害，藉以達到前蘇聯不敢輕易發動軍事侵略的嚇阻效果。[54]在「大規模報復」的架構下，美軍軍事投資重點置於四個領域方面，第一是大規模擴大空中加油與戰略轟炸的能力；第二是強化美軍「整體防空及飛彈防禦」網路與能力，包括「長程預警」及「彈道預警」雷達系統等；第三為加強發展陸基及潛射型之各型「洲際彈道飛彈」(Inter-Continental Ballistic Missile, ICBM)，使美軍具備直接對前蘇聯本土實施核打擊能力；最後則是強化洲際彈道飛彈基地的防護，以及分散戰略轟炸機基地的部署等防禦作為。[55]

「新視野」戰略規劃的主軸就是在可負擔的國防預算條件下，充分利用與發揮美國優於前蘇聯的先進核武技術，中、長程戰略轟炸機，以及長程彈道飛彈等軍事科技與武器，以達到有效嚇阻前蘇聯軍事侵略的企圖。[56]同時為因應前蘇聯成功發射衛星至太空，便積極投入實施先進國防科技的研發與武器裝備的研製，也在 1958 年 2 月成立「高等計畫研究署」(Advanced Research Projects Agency,ARPA)，除快速追上前蘇聯的太空科技外，同時也加速擴大與前蘇聯在軍事科技上的差距。[57]

雖然「新視野」戰略在 1950 年代對蘇聯的共產勢力赤化威脅造成有效的嚇阻效果，但也導致 1960 年代末期美、蘇兩國軍備競賽的白熱化，[58]「新視野」戰略在美國國內遭受許多輿論批評與反對聲浪，但「新視野」戰略是否成功，從今天美國國防部的角度來看，所給出的答案是肯定的，雖以原子彈作為要脅蘇聯的武器，但在當時來講，的確提供了非常好的嚇阻效果，核武為美國傳統武力提供

---

[53] 周湘華，《遺忘的危機：第一次台海危機的真相》(台北市：秀威資訊，2008 年)，頁 190。
[54] Samuel F. Wells, "The Origins of Massive Retaliation," *Political Science Quarterly*, Vol. 96, No. 1 ,Spring, 1981, pp. 31-52.
[55] 同註 48，頁 53。
[56] 同上註。
[57] Richard Van Atta, "Fifty Years of Innovation and Discovery," in *DARPA: 50 Years of Bridging the Gap* (Arlington, Virginia: Defense Advanced Research Projects Agency, July 18, 2008), pp. 23-29.
[58] 同上註，頁 54。

了相當具有成本效益的支援。[59]

第二節　美軍第二次抵銷戰略之緣起與意涵

強大的軍事力量是冷戰的物質基礎，而激烈的軍備競賽和軍備控制談判是冷戰極為重要的內涵，1950 年代至 1960 年代是軍備競賽最為激烈與緊張的年代，主要表現在國際軍費開支大幅增長、擁有核武國家數目增加、軍事技術與武器不斷進步更新、以及核嚇阻戰略的確立。[60]

一、時空背景

1960 年 1 月，蘇聯成立戰略火箭軍、防空飛彈部隊、核子潛艇，並定位為「國防威力的基礎」，[61]主要為裝載各式核彈頭的洲際飛彈、中程飛彈，他認為即使戰爭從傳統軍力開始，最後必定以核子武器結束，並認為使用核武將可在最短的時間內結束戰爭。遂開始與美國展開激烈的核武軍備競賽，加速發展核融合武器和導彈、戰略轟炸機和核子潛艇。蘇聯儘管技術落後於美國，且國內工業基礎較不足，但是利用社會主義計劃經濟的優勢，集中國家的人力、物力、和財力，使得核武得到快速發展。在外交上則實施「核訛詐」，揚言以飛彈攻擊英、法，更威脅德國其領土為蘇聯核力量最集中的打擊目標。[62]1962 年，所發生的古巴飛彈危機，則是美蘇冷戰對峙的高潮，美蘇兩國對抗趨向白熱化，在核武層面的軍備競賽則更加的惡化。

1960 年代中期，因耗費龐大國防預算的軍備競賽導致兩國開始疲乏，再加上美國經濟成長開始趨於緩和，以及蘇聯國力崛起，時任美國總統尼克森及國務卿季辛吉為了考量現實環境後，制定一系列緩和冷戰的政策，宣告以談判代替對抗，以緩和代替冷戰的策略。古巴飛彈危機之後，蘇聯加速發展國內核武，至 1969 年美蘇開始第一階段限制戰略武器談判時，美國的核武優勢變成了美蘇戰略均勢，而此一時期，英國、法國、中國等國先後發展出核武，美國霸權地位的動搖，連帶影響了美國制定外交政策的信心及能力。1970 年代開始，尼克森總統與

---

[59] Robert Martinage, *Toward a New Offset Strategy* (Washington, DC :Center for Strategic and Budgetary Assessments, 2014).pp.71-73

[60] 同註 41，頁 542。

[61] "Strategic Missile Troops," *Federation of American Scientists*, Oct. 6, 2000.At https://fas.org/nuke/guide/russia/agency/rvsn.htm （Accessed 2018/03/26）

[62] 同上註，頁 551-553。

時任國家安全顧問的季辛吉在其外交事務及政策之經驗與追求全球和平的目標下，開啟了與共產國家談判的時代，並願意與蘇聯和解。[63]

而在緩和策略之下，美國於 1973 年與蘇聯中央總書記勃列日涅夫達成了《第一階段限制戰略武器協議》（SALT I Treaty）和《反彈道飛彈條約》（Anti-Ballistic Missile Treaty）。蘇聯自第一階段限武協議簽訂後，乃更積極發展核武能力，直至第一階段協議所允許的最高限額，蘇聯受到「第一限武協議中攻擊性武器協定」的限制，戰略投擲工具數目成長較為緩慢，但是個別戰略武器的能力，卻因汰舊換新，而有驚人的增加，由於蘇聯在改進準確性、更大的投擲重量，及多彈頭飛彈上的綜合努力，使得蘇聯戰略飛彈的毀滅能力，自 1974 年至 1978 年大幅增加，[64]在第二限武協議簽定前（1979 年 6 月），美蘇戰略核武的能力差異在於，美國核武的長處為準確性較高，彈頭數量較多，而蘇聯的長處為核彈威力較強，飛彈發射器較多，蘇聯的飛彈發射器一直維持著優勢，而且在 1970 年代末，其多彈頭飛彈之數目更已接近美國。[65]

在美國力量相對下降的同時，蘇聯的經濟和軍事實力都有了長足的發展，如尼克森總統所說：「從 1950 年到 1966 年，美國在戰略武器方面具有全面性的優勢；從 1967 年到 1969 年，美國仍維持重大優勢；但在今日，蘇聯所擁有的核子武器，不論其威力或精密性均已逐漸接近美國。」[66]戰略均勢的形成，使得美蘇兩國美國達到「相互保證毀滅」的「恐怖均衡」狀態中，當時美國甫結束越戰，美國國內面臨高通貨膨脹以及經濟發展低迷等議題。1977 年卡特總統執政後，由國防部長哈羅德·布朗(Harold Brown)及國防部次長威廉·佩里（William Perry）共同實施「第二次抵銷戰略」的戰略規劃，希望藉由創新的思維及過去「新視野」戰略的成功經驗，使美國能夠在軍力上得到領先。

卡特總統對於美蘇軍備管制上的基本政策，乃是繼續進行自尼克森至福特政府以來的限制戰略武器談判工作，並期望盡速達成第二階段的限武協議，卡特總統認為，就美蘇現有的飛彈彈頭數目而言，雙方的核武數量大幅增加，但兩國關

---

63 王萬里，《美蘇關係研究－冷戰・和解・對抗》（台北市：黎明文化事業公司，1986 年），頁 101。

64 Samuel B. Payne, Jr., The Soviet Union and SALT(Massachusetts: The MIT Press,1980),pp.86.

65 同註 63，頁 186-187。

66 同註 63，頁 68-69。

係卻仍處於不安全的情況，相反的，武器競賽只有增加雙方衝突的危險。[67]因此在卡特政府的施政優先次序上，除了建立一個較好、更合作的國際經濟體制，及促進人權的重視外，維持和平與減少武器競賽也成為主要目標之一。[68]1979 年 6 月，美蘇雙方在維也納的高峰會議中正式簽署「美蘇戰略攻擊性武器管制條約」(Treaty Between the United States of America and the Union of Soviet Socialist Republics of the Limitation of Strategic Offensive Arms)簡稱為第二階段限武協議(SALT II)，此為自 1982 年 1 月 1 日至 1985 年 12 月 30 日，為期三年的議定書，規範內容包括特殊武器項目的管制，如：巡弋飛彈、機動洲際彈道飛彈，以及洲際彈道飛彈「質」的改進等設限問題。[69]卡特總統自維也納返國後，曾就第二階段協議加以說明：「核子時代的世界大戰，就是全球自殺，必須加以預防。美國務求保持雄厚的軍力、強大的盟國及堅定的決心以維持和平。限武條約不是結束美蘇競賽，也不是終止軍備的發展，而是使今後的競賽與發展有明確的規則及查證的範圍。這樣比較安全，且可以預測。」[70]但此條約引起美國參議院的激烈辯論，因而延緩批准，同年 12 月 25 日，蘇聯入侵阿富汗，引起美蘇關係的嚴重緊張，此限武條約乃擱置而未受批准

二、軍事戰略

1978 年初，時任國防部次長佩里在「參議院軍事委員會」(Senate Armed Services Committee)的聽證會上說明，發展「精準導引武器系統」能使作戰更加有效率，更可大幅增進美軍的威懾能力，而不需要與蘇聯在傳統軍事裝備上進行軍事競賽，使美軍在戰場上具備對敵軍高價值目標精準打擊的能力，並且摧毀欲擊中的所有目標。[71]另外，國防部長布朗也在 1981 年 1 月時對國會的報告中指出，「科技」可以成為戰力的倍增器，是有助於抵銷敵人數量優勢的重要手段。[72]

國防大學 National Defense University

---

[67] Jimmy Carter, "Peace, Arms Control, World Economic Progress, Human Rights: Basic Priorities of U.S Foreign Policy," *The Department of State Bulletin,* Vol.76,No.1972,1977,p.329.

[68] Ibid.,p.330.

[69] 同註 63，頁 188-189。

[70] "Carter's Speech to Congress Asking Approval of Treaty," *The New York Times,* June 19,1979.At https://www.nytimes.com/1979/06/19/archives/carters-speech-to-congress-asking-approval-of-treaty-returned-two.html （Accessed 2017/10/24）

[71] Michael G. Vickers and Robert C. Martinage, *The Revolution in War* (Washington, DC : Center for Strategic and Budgetary Assessments, 2004).p.8-9

[72] Harold Brown, "*Department of Defense Annual Report Fiscal Year 1981,*" (Washington, DC : Department of Defense, 1981).pp. iii-x.

第二次抵銷戰略將軍事科技的發展置於四個重要面向，首先發展新的情報、監視、偵查與作戰管理系統；其次部署先進的精準打擊武器；再者將匿蹤科技應用於飛行器；第四則是太空科技的應用，如情監偵、通信及精準定位。[73]

三、作戰概念

(一)空地作戰(Air Land Battle)

美軍研發重點為可以達到事半功倍的軍事科技技術，以及相關武器裝備的研發，目標在於有效提升武器攻擊的精準度、增進戰鬥車輛的機動力及火力、提高部隊通信能力，以及研發新型武器投射載臺，如巡弋飛彈載臺及遙控載具(Remotely Piloted Vehicle, RPV)等方面領域的研究，[74]使美軍建立有效整合先進情監偵、目標獲得與指揮管制等網絡，增進快速打擊與精準打擊能力，以有效抵銷蘇聯的優勢，[75]由於蘇聯全力發展軍事科技，在傳統軍力上與美國相比則占有明顯的優勢，在重要武器裝備的生產速度及數量上大多也優於美國，故其軍力規模便逐漸擴大，美軍則規劃出「先制」(Initiative)、「縱深」(Depth)、「迅捷」(Agility)及「同步」(Synchronization)等特性的非線性作戰概念：空地作戰(Air Land Battle)。[76]美軍的研究分析指出，雖美軍處於數量上的劣勢地位，但蘇聯軍隊仍有諸多弱點，如「戰術戰法的運用過於僵化而沒有彈性」、「可預期性多梯隊作戰（戰鬥）梯隊的投入」，以及「軍事科技較為落後」等問題，[77]而美軍針對這些研究結果，逐漸發展具「縱深整體、同步作戰」特性的「空地作戰」的戰術思想。

1975 年，國防高等研究計畫局（Defense Advanced Research Projects Agency, DARPA）制定了一個詳細、長期的研究發展計劃，將重點放在如何有效提升武器投射的精準度、加強戰鬥車輛的機動性及火力、提高部隊通信能力，以及研發新型武器投射載台，如巡弋飛彈及遙控載具。1978 年，國防高等研究計畫署強調「看

國防大學 National Defense University

---

[73] Richard H. Van Atta et al., *Transformation and Transition: Darpa's Role in Fostering and Emerging Revolution in Military Affairs, Volume 1, Overall Assessment* (Alexandria, VA: Institute for Defense Analysis, 2003). pp. 38-42.

[74] Robert Martinage, *Toward a New Offset Strategy: Exploiting Us Long-Term Advantages to Restore Us Global Power Projection Capability* (Washington, DC : Center for Strategic and Budgetary Assessments, 2014).p.34.

[75] Robert R. Tomes, *US Defence Strategy from Vietnam to Operation Iraqi Freedom: Military Innovation and the New American War of War, 1973-2003* (New York：Routledge, 2006). pp. 58-62.

[76] 同註 48，頁 58。

[77] Douglas W. Skinner, *Airland Battle Doctrine* (Alexanderia, VA: Amphibious Warfare Research Department, 1988).pp.6-9.

得遠」、「打得遠」，整合了科技研發以及戰術運用，其中主要作為包含：機載合成孔徑雷達(Synthetic Aperture Radar,SAR）平台配合地面移動目標指示(Ground Moving Target Indication,GMTI)能力，如 E-8 聯合目標偵查與攻擊雷達系統可在安全距離下（約 300 公里）同時進入敵人陣地，對敵人進行偵查；BLU-108 傳感器引信武器(sensor fuzed weapon,SFW)能夠在大範圍辨識並摧毀數量眾多的裝甲車；陸軍戰術導彈系統(Army Tactical Missile System,ATACMS)能夠擁有道路移動、長距離且非常精準的陸上導彈系統，國防高等研究計畫署之後也相繼研發了「機載空中預警管制系統」(Airborne Warning and Control System,AWACS)、聯合戰術情報分發系統(Joint Tactical Information Distribution System, JTIDS)的戰術數位資訊鏈路、具匿蹤能力的 F-117A 夜鷹戰鬥攻擊機等武器裝備，同時也研發出一系列精準導引彈藥(Precision-Guided Munitions, PGMs)、無人飛行載具(Unmanned Aerial Vehicle, UAV)及全球定位系統(Global Positioning System, GPS)等現代化武器裝備，[78]1970 年代這些尚在研發中的能力還未被大量部署，直到 1980 年代後期才被系統性的運用，也是後人所知的「空地作戰」的作戰概念，在歐洲方面，北約組織盟軍也採用美軍「空地作戰」的概念，設計出所謂的「後續部隊攻擊」(Follow-on Force Attack)的作戰構想，其著眼點是在戰鬥展開後不久，快速發現華沙組織第二梯隊及後續梯隊的作戰部隊，以精準打擊方式，有效殲滅之。[79]

這些技術與經驗的累積，成為 1980 年代美國發展「聯合監視和目標攻擊雷達系統」（Joint Surveillance and Target Attack Radar System, JSTARS）的基礎。[80]在執行抵銷戰略期間，美軍在作戰準則、戰術思想、武器裝備與作戰模式上均有突破，並藉「空地作戰」戰術運用的規劃與設計，伴隨著軍事科技發展進程，結合先進武器裝備的研發，使美軍開始展開長期的「軍事事務革命」(Revolution in Military Affairs, RMA)的軍事現代化進程，即使在 1991 年的沙漠風暴行動中面對

[78] Richard Van Atta and Michael J. Lippitz," Transformation and Transition: DARPA's Role in Fostering an Emerging Revolution in Military Affairs Volume 1 – Overall Assessment," *Federation of American Scientists*, Apr. 2003.At https://fas.org/irp/agency/dod/idarma.pdf (Accessed 2017/11/25) pp. 8-25.

[79] Michael J. Diver, "NATO'S Follow-on Forces Attack Concept (FOFA): Past. Present and Future," *Defense Technical Information Center*, July 1, 1990,At http://www.dtic.mil/dtic/tr/fulltext/u2/a224090.pdf (Accessed 2017/11/25) pp. 6-9.

[80] "JSTARS," *Defense Advanced Research Project Agency.* At https://www.darpa.mil/about-us/timeline/joint-stars (Accessed 2017/11/25)

兵力超過 50 萬的伊拉克部隊，最後仍獲得勝利，資訊科技的發展使作戰事半功倍，美國的勝利被廣泛認為是改變戰爭型態的證據。[81]

第三節 美軍第三次抵銷戰略之緣起與意涵

因應中共軍事現代化的發展，以及「反介入與區域拒止」(Anti-access/Area denial,A2/AD)的軍事威脅，美軍在 2014 年年底提出國防創新倡議，目的在於在透過技術創新發展，藉發展新的軍事戰略為因應，運用不對稱作戰方式抵銷對手在軍力上的優勢。在第三次抵銷戰略當中，美軍除了傳統軍力、核嚇阻、飛彈防禦外，也將網路資訊作戰空間及人工智慧等領域亦是發展重點，我們也可從中窺見未來戰爭型態可能發生的改變。

一、時空背景

中共的快速軍事現代化與美軍願景中的美國霸權是相牴觸的，[82]共軍現代化引發了美國的危機意識，美國太平洋艦隊司令威拉德（Robert F. Willard）上將曾多次提出，中共的軍事發展「看似特意挑戰美國在亞太地區的行動自由，或是侵犯或威嚇包括美國盟邦與夥伴國家在內的周邊鄰邦。」[83]美國國務院國際安全顧問委員會（International Security Advisory Board）一份報告結論指出，共軍「試圖大力提升軍事能力與能力所及範圍」，最終特定目標是「鎖死美軍」，作法則是嚇阻美軍軍事行動，瓦解美國盟邦對於美軍的信賴，[84]由於中共崛起為強權的態勢已相當明顯，美國戰略也就越來越聚焦於亞太地區，進而證實了美國的擔憂。美國政府 2006 年版「四年期國防總檢討」表達了美國海軍駐防亞太的兵力高於駐防歐洲的意圖，美國過去著重在伊拉克和阿富汗兩個戰場的戰略比重已下降。2011 年版《國家軍事戰略》（National Military Strategy）中，「亞太地區」和「網路戰」成為美軍關注的新戰略重點，而中共的軍事現代化，則是亞太地區最為核

---

[81] Robert Martinage, *Toward A New Offset Strategy: Exploiting U.S. Long Term Advantages to Restore U.S. Global Power Projection Capability* (Washington D.C.: Center for Strategy and Budgetary Assessments, 2014), pp. 15-16.

[82] Denny Roy 著，周茂林譯，《崛起－中共與區域安全》（台北市：國防部史政編譯室，2015 年 11 月），頁 79。

[83] 同上註，頁 85。

[84] International Security Advisory Board report to the U.S. Department of State, "China's Strategic Modernisation, report from the ISAB Task Force," *Federation of American Scientists,*Sep. 2008, https://fas.org/nuke/guide/china/ISAB2008.pdf. （Accessed 2017/10/24）

心的部分。[85]美軍高度重視亞洲，部分原因固然是北韓的行為引起區域緊張，但實為美、中兩國在亞洲的競逐，布里辛斯基(Zbigniew Brzezinski)曾指出「美國必須防止歐亞大陸再出現可以挑戰美國霸權的準霸權產生。」[86]

中共海軍採購現代化的遠洋戰艦，是共軍挑戰美國的先鋒，美國海軍之所以被稱之為全球最頂尖，是因其兵力投射能力可深及全世界各角落，且以實踐全球自由航行的原則。中共採購遠洋艦，是反映出中共在不信任美國的基礎上，試圖建構起與美國相匹敵之戰力，有些觀察家深信。採購遠洋戰艦可能是中共企圖最終取代美國海洋角色的預兆，而且更強大的中共海軍也能加強對美國實施「反介入與區域拒止」的能力。[87]

美國國防部出版《聯合作戰介入概念》(Joint Operational Access Concept,JOAC)中對「反介入與區域拒止」做出界定，將「反介入」界定為「通常在遠距離實施，旨在防止敵對力量進入作戰區域的行動和能力」，而「區域拒止」則界定為「通常在短距離實施，旨在限制敵對力量在作戰區域內的行動自由，而非阻止其進入區域的行動和能力」，隨著中共快速發展其「反介入與區域拒止」能力，亦代表美國過去恣意於海外投射軍事力量的能力開始受到威脅。與此同時，中共、北韓、伊朗等國在網路空間取得了高度的進步和技術，並利用駭客、後門程式、病毒等對他國進行勒索與攻擊，此舉更危及美國過去數十年來所擁有的指揮、控制、通信、計算機、情報、監控、偵察的優勢。[88]

二、軍事戰略

2014 年 8 月 5 日，美國國防部常務副部長羅伯特·沃克在美國國防大學演講時，首次在公開場合提出了「抵銷戰略」的概念，指出這是美國保持長久軍事優勢的重要途徑，9 月 3 日，時任美國國防部長查克·黑格在「國防創新日」(Defense Innovation Day)的發言中再次提到「抵銷戰略」，10 月 27 日，美國戰略與預算評估中心（Center for Strategic and Budgetary Assessments, CSBA）則推出名

---

[85] Michael Wines, "U.S. and China Try to Agree on Military Strategy," *The New York Times* ,July 14,2011.At http://www.nytimes.com/2011/07/15/world/asia/15beijing.html (Accessed 2017/9/20)
[86] Zbigniew Brzezinski 著，林添貴譯，《大棋盤》（臺北：立緒文化，1996 年），頁 15。
[87] Sam J. Tangerdi 著，吳志丹譯，《反介入/區域拒止戰-即將到來的美中之戰和其他戰爭，2015 年》（香港：全球防務出版公司），頁 93。
[88] 同上註，頁 19-20。

為《邁向新抵銷戰略：利用美國長期優勢恢復美國全球力量投送能力》（Toward A New Offset Strategy Exploiting U.S. Long-Term Advantages to Restore U.S. Globle Power Projection Capability）的研究文件，就美國實施新的「抵銷戰略」提出了詳細的構想，2014 年底，美國國防部發佈一紙「國防創新倡議」，文件中寫道，美軍現在所擁有的軍事優勢正逐漸消失，而美軍必須尋找創新的方式來保持優勢以及在某些領域有所突破與擴張，除此之外，面臨國防預算的刪減與財政壓力，已對美軍達成保衛國家安全任務形成壓力，因此，美國國防部必須整合各部門，在有限的條件與資源下，尋求創新的思維與方法，藉以維持甚至是擴大美軍所擁有的優勢。[89]

第三次抵銷戰略目的在於在透過技術創新發展，運用不對稱作戰方式抵銷對手優勢，並增加對手軍事力量發展成本，特別是全面反制對手「反介入與區域拒止」的能力，以確保美國在大國軍事競爭中佔據絕對優勢地位，[90]美國必須維持美軍的全球力量投送能力以威懾潛在對手，並保護美國的盟國，即使面對「反介入與區域拒止」的威脅，也無需擔憂自身的安全。美國智庫公布的研究報告中指出，中共及伊朗的軍事發展實力被美國視為波斯灣地區及西太平洋區域中嚴重的威脅與挑戰。[91]「反介入與區域拒止」能力主要體現在下列四項科技之上：（一）中、長程戰術飛彈與巡弋飛彈；（二）海、空軍遠程打擊能力；（三）相當能量的網路攻擊能力；（四）先進的衛星及反衛星武器的能力。[92]基於上述，美軍將未來的軍事投資與軍事科技研發重點聚焦在武器裝備、核嚇阻、飛彈防禦、網路、太空等領域的軍事現代化，其中武器裝備包括第五代戰機、無人飛行系統、具長程打擊能力的遠程精準武器、先進情監偵系統、長程空中作戰系統、海軍各種水面

國防大學
National Defense University

[89] United States Secretary of Defense, “The Defense Innovation Initiatives,” Nov. 15, 2014, At http://www.defenseinnovationmarketplace.mil/resources/DefenseInnovationInitiative.pdf （Accessed 2017/10/24）

[90] 李大光，〈美國推出保持軍事優勢的「第三次抵消戰略」〉，《國防科技工業》，2016 年 7 月，頁 61。

[91] Robert Martinage, *Toward A New Offset Strategy: Exploiting U.S. Long Term Advantages to Restore U.S. Global Power Projection Capability* (Washington D.C.: Center for Strategy and Budgetary Assessments, 2014), pp. 6-7.

[92] 李建昇，〈反介入／區域拒止（A2/AD）威脅與美軍空海整理戰（AirSea Battle）發展概念〉，《國防雜誌》，第 27 卷第 5 期，2012 年 9 月，頁 61。

及水下作戰系統，以及超大規模作戰整合系統等高科技裝備。[93]

美國參議院於 2017 年 9 月 18 日通過了 2018 年度國防預算案，與 2017 年度相比增加百分之十二，整體國防預算達 6,920 億美元。依照國防預算計畫，美軍計劃在 2018 財年添置 70 架 F-35 型閃電戰鬥機、7 架 P-8A 型海神式海上巡邏機以及 2 艘維吉尼亞級核動力攻擊潛艦，其它優先項目包括核打擊力量的維護、網路作戰與升級防禦能力和研發超高音速武器項目。[94]

有學者則認為美軍第三次抵銷戰略成功的關鍵在於軍隊組織思維的創新，技術並非造就成功的關鍵，而戰略優勢與創新技術的結合，才是決定第三次抵銷戰略是否能夠獲得成功的關鍵因素。[95]

三、作戰概念

(一)空海作戰（Air Sea Battle）

第二次世界大戰以來，美國成為世界上領導民主國家與反對共產主義的大國，在軍事力量的投資上，無論是匿蹤技術或是空中平台還是水下系統，都享有絕對領先的優勢。時至今日，美國依然維持領先，但是與對手軍力差距卻快速的縮小，美國軍事主導的時代正在以加快的速度逝去，其中最明顯的部分體現在美國軍力投送的能力上，中共、俄羅斯、伊朗等國所發展之「反介入與區域拒止」能力迫使美國做出重要的戰略抉擇：默許一個新的世界秩序，在這個秩序中，美國無法自由投射其軍力，抑或是選擇能夠有效協助在受威脅的盟國，防止他們遭到侵略或脅迫。[96]「空海作戰」是為應對「反介入與區域拒止」的戰略，其中「反介入」戰略旨在阻止美軍進入某一戰區，而「區域拒止」戰略旨在透過直接控制某個區域而限制美軍行動自由，[97]

國防大學 National Defense University

---

93 United States Department of Defense, “Quadrennial Defense Review 2014,” Mar. 4, 2014, At http://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf （Accessed 2017/10/24）pp. 12-22.

94 U.S. Department of Defense, ” DoD Releases Fiscal Year 2018 Budget Proposal”, May 23, 2017.At https://www.defense.gov/News/News-Releases/News-Release-View/Article/1190216/dod-releases-fiscal-year-2018-budget-proposal/ (Accessed 2017/12/21)

95 Chuck Wald、Joe Mariani, ” The Key to Military Innovation,” Feb. 27,2017.At https://www.usnews.com/opinion/world-report/articles/2017-02-27/key-to-defense-departments-third-offense-is-use-of-military-technology (Accessed 2017/12/21)

96 Andrew F. Krepinevich, *Why AirSea Battle?* (Washington, DC: Center for Strategic and Budgetary Assessments, 2010), pp.7-8.

97 Andrew Krepinevich, Barry Watts & Robert Work, *Meeting the Anti-Access and Area-Denial Challenge*(Washington, DC: Center for Strategic and Budgetary Assessment,2003), p.5.

2010 年 5 月，美國智庫戰略與預算評估中心對外發布了兩份研究報告，闡述了「空海作戰」概念的背景與內涵，美軍「空海作戰」構想，充分借鑒了冷戰期間其「空地作戰」理論提出與演變的歷史經驗。[98]美軍在空海作戰概念中對潛在對手運用反介入與區域拒止能力進行了作戰預想如下：

（1）認為對手在無預警情況下會突然發動軍事行動，美軍要在短時間內準備好作戰力量，按照例行的一體化作戰展開部署。

（2）美軍前沿部隊在戰事初始就處於反介入與區域拒止的打擊環境中，需在快節奏的作戰環境中進行快速有效的回應。

（3）認為對手將攻擊美軍及其盟國支撐作戰的領域，除了攻擊美軍艦船、太空設備、網路外，還包括美軍基地。

（4）認為對手將在全作戰區域中展開對抗（太空、網路、空中、海上以及陸地）。網路以及太空作戰能力對於美軍至關重要，同時相關設施易受到電子網路攻擊以及電子干擾。

（5）認為對手無法完全控制某個作戰領域，五大作戰空間互相影響，美軍試圖在所有的作戰領域都能獲得行動自由，但其可能無法同時控制所有的作戰區或對每個作戰領域都有同等的控制力。[99]

從空海作戰構想公開以來，美軍已經全面加強了其在關島和日、韓等各基地設備和設施的建設強度，以鞏固與強化這些基地的作戰能力，並且在西太平洋地區尋求更多的備用基地，以進一步增加美軍和盟軍在戰時的疏散配置能力。[100]由於美軍須使用衛星雷達作戰，並在安全的軍事基地和不受干擾的網路空間發起攻擊，一旦中共軍隊攻擊這些基地和網路空間，將使美軍喪失真實和虛擬領域（包括太空、網路空間和電磁頻譜）的前沿防護，無法進入作戰地區，最終喪失戰略

國防大學 National Defense University

http://csbaonline.org/uploads/documents/2003.05.20-Anti-Access-Area-Denial-A2-AD.pdf（Accessed 2017/12/25）。

98 雷紅偉、桑士川，〈美軍「海空作戰」—西太平洋上的未來聯合作戰〉，《中共解放軍報，軍事論壇》。參見 https://wenku.baidu.com/view/5b871e30561252d380eb6ecc.html （瀏覽日期：2017 年 12 月 25 日）。

99 任雅廣，〈空海一體戰的演變〉，《航空電子技術》，第 47 卷第 2 期，2016 年 6 月，頁 2。

100 Mark A. Gunzinger, *Sustaining America's Strategic Advantage in Long-Range Strike*（Washington, DC: Center for Strategic and Budgetary Assessments, 2010). p.15.

和戰役主動權。[101]根據「空海作戰辦公室」(Air-Sea Battle Office)在 2013 年 5 月公布「空海作戰：因應反介入與區域拒止挑戰的軍種合作」(Air-Sea Battle: Service Collaboration to Address Anti-Access and Area Denial Challenges)的報告中可以了解美軍當前擘畫「空海作戰」的基本概念，就是建立所謂「NIA/D3」的作戰構想。NIA/ D3 意指發展具高度「網狀化」(Networked)及「整合性」(Integrated)的聯合作戰部隊，使其具備「縱深打擊」(Attack-in-deep)的作戰能力，以達到「襲擾」(Disrupt)、「殲滅」(Destroy)與「摧毀」(Defeat)敵軍的作戰目的。[102]

2014 年，美軍各軍參謀長均認為將空海作戰從原有的軍種協定，轉化為一種充分整合之聯合構想，是強化聯合作戰並能應對當前及未來競逐的環境，[103]2015 年 1 月前參謀長聯席會議主席鄧普西(Martin Dempsey)上將聽取各軍種參謀長的建議，為更強調有效整合陸、海、空三軍部隊聯合作戰戰力，而非僅是海、空軍而已，因此將「空海作戰」易名為「全球公域介入與機動之聯合構想」(Joint Concept for Access and Maneuver in the Global Commons, JAM-GC)，並將原「空海作戰辦公室」的銜稱改為「JAM-GC 辦公室」，但其具體內涵仍脫離不了原「空海作戰」的作戰構想。[104]

(二)全球公域介入與機動之聯合構想

全球公域介入與機動聯合構想的發想，是為了取代空海作戰的不均衡戰力，該構想聚焦於擊潰敵人的計畫與企圖，本身是屬於戰爭的作戰層次，也是遂行戰略的手段。2016 年 10 月 19 日，參謀首長聯席會議副主席空軍上將賽爾瓦（Paul Selva），簽署了全球公域介入與機動之聯合構想，正式宣告該構想已核准為一種支持「2030 年聯戰最高指導構想」(Capstone Concept for Joint Operations 2030)的聯戰構想，更重要的，是全球公域介入與機動之聯合構想將指導聯合部隊作戰，使美國能在全球公域中確保介入與機動能力、投射兵力，以及擊敗試圖拒止美軍

---

[101] 宋吉峰，〈美軍全新作戰二部曲－海空整體作戰〉，《國防雜誌》，第 27 卷第 2 期，2012 年 3 月，頁 50。

[102] Air-Sea Battle Office, United States Department of Defense, *Air-Sea Battle: Service Collaboration to Address Anti-Access and Area Denial Challenges* (Washington, DC: Department of Defense, 2013), p. 5.

[103] Michael E. Hutchens, "Joint Concept for Access and Maneuver in the Global Commons A New Joint Operational Concept,"*Joint Force Quarterly*, No. 84 ,1st Quarter, 2017, pp.135-136.

[104] Paul McLeary,"New US Concept Melds Air, Sea and Land," *Defense News*, Jan. 24, 2015, At http://www.defensenews.com/story/defense/policy-budget/warfare/2015/01/24/air-sea-battle-china-army-navy/22229023/ (Accessed 2017/12/27）

及盟軍行動自由之敵人，[105]此構想置重點於獲得並維持戰時介入能力，在軍事威脅日趨精密、擴散的年代中，在全球公域中保持行動自由，而此處所指的「全球公域」的定義，在美軍「聯戰進軍構想」(Joint Operational Access Concept)中，是「不屬於任一國之空、海、太空及網路空間區域」，陸地不屬於全球公域，因為所有適合居住的陸地均為各國或國家實體所擁有。」[106]

全球公域介入與機動之聯合構想保留並強化了空海作戰經證實後的精華部份，並找出經驗教訓加以融入，形成一種更有效、更具適應性之聯合構想，基於多年的全面性兵推與實驗，全球公域介入與機動之聯合構想對空海作戰的理念進行改良與調整，空海作戰構想是專為反制逐漸浮現的反介入與區域拒止威脅而設計，並針對敵人之反介入與區域拒止能力，採取干擾、破壞、擊潰的手段。全球公域介入與機動之聯合構想則是置重點於擊潰敵人的計畫與企圖，而非僅是專注於去除敵人反介入與區域拒止之能力，而全球公域介入與機動之聯合構想這個新名詞，也反映出聯合部隊要在相互競逐的過程中制勝的諸多重要理念，其中最明顯的改變就是在面對反介入與區域拒止全面威脅而進行作戰時，需要整合五個作戰領域（陸、海、空、太空、網路）的一切戰力，而非其前身空海作戰所僅注重的空、海兩個領域。此一構想也會因時因地制宜，將盟國的戰力與能量囊括在內，因為介入全球公域乃是國際社群的共同利益，全球公域介入與機動聯合構想未來仍將有賴於美國對全球盟邦與夥伴的承諾，而他們對於成功克服威脅以介入全球公域。就這點而言十分重要，提升美國與盟國及夥伴之間的作業互通性，乃是此一新構想的要義。此外，「介入與機動」反映出作戰介入與行動自由之重要性，「全球公域」則是劃出不屬於任何國家的陸、海、空、太空與網路空間，全球公域介入與機動聯合構想認知到，「介入」全球公域，無論作為目標或作為一種將兵力投射至敵境的手段，對美國國家利益而言均十分重要。[107]

全球公域介入與機動之聯合構想為聯合部隊提出一種漸進式解決方案，其核心為強化跨軍種全領域整合與兵力組成，即便在反介入與區域拒止威脅日趨複雜

---

[105] Michael E. Hutchens, " Joint Concept for Access and Maneuver in the Global Commons A New Joint Operational Concept,"*Joint Force Quarterly*, no.84, 1st Quarter, 2017, pp.134-135.
[106] United States Department of Defense, Joint Operational Access Concept, Version 1.0 (Washington, DC: Department of Defense, 2012), p.1.
[107] Hutchens,op. cit. pp.136-137.

之際，仍能發展出一支繼續確保在全球公域行動自由之部隊，此一構想問題總結如後：聯合部隊須能介入各個全球公域，並於其間維持機動力、投射兵力，以及擊敗企圖透過運用反介入與區域拒止能力以阻撓行動自由之敵人。[108]

用於全球公域之戰術與軍事戰略必須有高度適應性，俾與敵各類科技之進展並駕齊驅，包括定位與定時、導引、推進、計算能力、感測、精確度等各方面，在兵力架構「更精實」以及先進威脅與武器科技不斷擴散與進步之際，反制一個具備數量優勢與幾近相等程度科技潛力的敵人，就是全球公域介入與機動聯合構想作戰問題的核心。[109]

全球公域介入與機動之聯合構想所預設的落實方式，乃是一支完成備戰與訓練，並且具備陸、海、空、太空、網路作業互通能力的部隊，還擁有克服、突破潛在敵人目前所構成日趨複雜的挑戰，該構想經落實後，將能維持聯合部隊能力，使兵力能在任何時間投射至任何需要協助反制侵略或敵對的全球公域，以保障美國及其盟邦的利益。[110]

第四節 小結

美軍在過去執行兩次抵銷戰略，就如同是軍事事務革命的發展過程，面對不同的戰略環境以及敵情威脅，研發先進的軍事科技，結合創新思維，摸索並發展出足以改變戰略環境的戰爭思想、作戰模式、軍隊組織、高科技武器裝備等。而美軍現在正在執行的第三次抵銷戰略則是以過去兩次經驗為啟發，藉著整合民間的技術與資源，希望美軍能夠再一次擴大在軍事科技上的優勢。

因此在分析與比較的過程中，則可歸納出三次抵銷戰略的共同點，而在新視野戰略及第二次抵銷戰略的成功經驗上，則可做為第三次抵銷戰略的參考。

一、為因應戰後情勢所制定的國家策略

美軍於 1950 年代執行新視野戰略時，當時韓戰結束不久；1970 年代執行第二次抵銷戰略時，長達十餘年的越戰也剛結束；而美軍當前的第三次抵銷戰略，則是在結束歷經十多年的全球反恐戰爭之後，同是為因應「戰後」的國家安全環

[108] Hutchens,op. cit.,p.137.
[109] Ibid.
[110] Ibid., p.139.

境所制定的國防戰略，而美軍在執行抵銷戰略時，都面臨一個共同的特點，那就是國內普遍民意及輿論反戰思潮高漲，要求政府施政重點放在經濟發展的議題上，因此美國政府必須減少國防經費的支出，以回應美國民意的訴求。美軍透過執行抵銷戰略的戰略規劃，強調國家安全所面臨的威脅，藉由新的戰略規劃與作戰構想，說服國會及民眾，美國仍須建構足以確保國家安全及克敵制勝的國防力量。美軍實施第一次抵銷戰略為了對抗蘇聯，而致力於發展核子武器，展開與蘇聯的軍備競賽；第二次抵銷戰略面臨蘇聯軍力的提升，以及美軍核壟斷優勢的喪失，美軍致力發展精準打擊武器，以更有效率的方式對抗對手；第三次抵銷戰略，美軍則運用不對稱作戰與技術創新反制對手反介入與區域拒止能力，除發展聯合軍種作戰的全球公域介入與機動之聯合構想外，亦在網路作戰空間及人工智慧領域投資與研發。使美軍在執行抵銷戰略期間，仍能維持穩定的國防預算，使美軍可以獲得所需的資源與經費，執行相關軍事科技的研發與先進新型武器裝備的部署。[111]

二、軍事科技與軍事戰略的相輔相成

美軍執行抵銷戰略規畫的目的是為了發揮軍事科技的優勢，結合創新的思維，有效運用國防資源，抵銷敵軍優勢。然而要從眾多的軍事科技中，尋求具有潛力的科技，並且集中資源及人才投入研究與發展實屬不易。美軍在前兩次的抵銷戰略能夠得到成功主因是透過明確軍事戰略的規劃，擘畫出清晰的作戰構想，而美軍為使該作戰構想的相關戰術作為能夠具體可行，進而研發出相對應的軍事科技與武器裝備，同時調整部隊的組織編裝，以具備可以執行戰略規劃內相關任務的能力，因此軍事科技的研發與軍事戰略構想的具體內涵是相輔相成的。[112]而美軍第三次抵銷戰略則透過各部門的整合與武器裝備的研發，有效因應以及反制反介入與區域拒止的威脅。

三、現代化武器裝備鉅額投資

發展先進軍事科技的武器裝備需要鉅額的預算相支應，而越是科技先進的武器裝備，其研發的成本也就越高。因此美軍執行的第三次抵銷戰略也就必須承擔

[111] 同註 48，頁 70。
[112] 同上註，頁 70-71。

高額的新軍事科技的研發成本與武器裝備的籌購經費，而除了研發和生產成本高之外，維持組織運作也需要耗費龐大費用，以海軍的一個航母戰鬥群的基本編制為例，除一艘航母外，另外也至少配置五艘水面戰鬥艦、一艘攻擊型潛艦、一個航空聯隊，以及維持數量大約 6,700 人的兵力規模，而運作這樣一個基本編制的航母戰鬥群，每日的作業維持費就需要 6,500 萬美元。[113]美軍以作戰概念引領裝備發展，以裝備發展推動作戰概念創新，在以創新的作戰概念構建創新的裝備發展思路，如此循環，而這也是美軍軍事現代化快速的特色。

四、平衡各軍種的建軍需求

美軍在兩次抵銷戰略的發展過程中，都相同面臨各軍種因為爭取國防資源而形成競爭的壓力與挑戰。在不同戰略各軍種的建軍規劃上，空軍較易獲得國防部決策者的重視因而得到國防資源的挹注，因此空軍所獲得的預算與兵力規模是逐年增加，而陸、海軍兩軍種的預算與兵力規模則是逐年遞減，[114]如美軍在第二次抵銷戰略期間，因美軍是以執行「空地作戰」為主軸的軍事戰略規劃，所以在國防資源的分配上形成重陸軍、再空軍，而輕海軍的趨勢，因此當美軍要專案發展空海作戰概念時，對陸軍便造成相當大的壓力。因政策的制定，必定會造成預算的排擠效應，美軍雖在 2015 年 1 月將「空海一體戰」易名為「全球公域介入與機動聯合構想」，以強調三軍聯合作戰的內涵。美國陸軍在 2016 年提出多域戰（Multi-Domain Battle ,MDB）概念，並將此概念列入美國新版陸軍訓練準則「FM 3-0 作戰行動」(FM 3-0 Operations)中，多域戰要求各軍種在陸、海、空、太空及資訊空間(包含網路作戰空間)跨領域整合，[115]陸軍則將作戰力量從傳統的陸地和空中，拓展到海、空、網路空間、電磁頻譜等其他作戰領域。[116]此概念提升了陸軍在聯合作戰中的地位，隨著多域戰概念為其他軍種採納，在與其他軍種

國防大學 National Defense University

---

113 Henry J. Hendrix, *At What Cost a Carrier?* (Washington DC: Center for a New American Security, Mar. 2013), pp. 5-6.

114 Ernest J. Yanarella, *The Missile Defense Controversy: Technology in Search of a Mission* (Lexington, Kentucky: University Press of Kentucky, 2002), pp. 22-27.

115 Department of the Army,"FM-3.0 Operations," *Federation of American Scientists*, Oct. 2017.At https://fas.org/irp/doddir/army/fm3-0.pdf (Accessed 2018/3/24)

116 David G. Perkins、James M. Holmes," Multidomain Battle Converging Concepts Toward a Joint Solution," *Joint Force Quarterly,* 1st Quarter 2018.At http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-88/jfq-88_54-57_Perkins-Holmes.pdf?ver=2018-01-09-102340-943 (Accessed 2018/3/24)

「融合」的過程中，也使陸軍的裝備得以升級，以及預算不被排擠。

國防大學
National Defense University

表 2- 1　美國三次抵銷戰略比較分析表

	1950-1960 年代	**1970-1980 年代**	**2014 年-當前**
執政政府	艾森豪政府	卡特政府	歐巴馬至川普政府
國家安全戰略構想	新視野 (New Look)	抵消戰略 (Offset strategy)	「國防創新倡議」 (The Defense Innovation Initiatives)
美國歷經重要戰爭	韓戰(1950-1953 年) 杜魯門政府時期	越戰(1961-1973 年) 歷經甘迺迪、詹森及尼克森政府時期	全球反恐戰爭 (2001 年迄今) 歷經小布希及歐巴馬政府
國家安全威脅環境	前蘇聯 (共產主義意識形態的擴張與赤化)	前蘇聯 (共產主義意識形態的擴張與赤化)	中共、非國家行為者(恐怖組織)、區域強權，如蘇俄、伊朗、北韓等國
國內輿情	反戰思潮高漲	反戰思潮高漲	厭倦長期海外作戰
內政議題	著重經濟改革與發展	面臨高通膨及經濟蕭條的問題	貿易保護主義
國防政策	國防預算逐年遞減 持續實施兵力精簡	國防預算逐年遞減 持續實施兵力精簡	國防預算 10 年來新高
敵軍態勢	前蘇聯在傳統軍力上佔有數量上的優勢	前蘇聯在傳統軍力上佔有數量上的優勢	日益成熟的反介入/區域拒止軍事能力威脅美國海外軍力投射
美國優勢	敵人尚未建立核武投射能力，核武科技發展尚不及美國，無法直接威脅美國本土安全	敵軍戰術戰法運用僵化 軍事科技較美國落後	軍事科技仍較美國落後
戰略規劃重點	發揮軍事科技優勢，結合創新思維，以有限及有效之國防資源運用，抵銷敵軍之優勢	發揮軍事科技優勢，結合創新思維，以有限及有效之國防資源運用，抵銷敵軍之優勢	發揮軍事科技優勢，結合創新思維，以有限及有效之國防資源運用，抵銷敵軍 A2/AD 之威脅
美國制定的 軍事戰略	大規模報復	空地作戰	反介入/區域拒止(A2/AD) 空海作戰(Air Sea Battle) 球公域介入與機動之聯合概念(JAM-GC)
重要軍事投資發展項目	核彈頭儲備、戰略轟炸機、洲際彈道飛彈、核武投射能力	精準彈藥、先進情監偵系統、預警雷達系統、精準打擊能力	無人機載臺、網路、太空、雷射武器、人工智慧

資料來源：李建昇，〈美軍抵銷戰略之發展歷程〉，《國防雜誌》，2016，第三十一卷第三期，頁 69。更新部分由筆者自行整理。

第三章　美中網路資訊作戰之發展

隨著資訊科技的進步，軍事現代化也出現新的發展，18 世紀中期起，伴隨工業化而來的第一次現代化，將人類從農業社會帶向工業社會；而工業化社會的軍事現代化，是將農業社會人力過渡到因應工業社會機械的型態；20 世紀後期開始，伴隨資訊化而來的第二次現代化，正在引領人類從工業社會邁向資訊社會，而此時期的新軍事現代化，則從因應工業社會機械戰型態轉型為因應資訊社會資訊戰型態。[117]

何謂「資訊」?資訊可依附於各種形式的載體（運載工具），且具有價值、共享性、可處理性以及時效性，資訊是通過文字、數據和各種信號來傳遞、處理和表現客觀事物特性的知識流；資訊比情報的概念寬泛，是指消息、數據、情報、知識，是生靈萬物相互賴以生存和進化的訊息，是人類感受到的客觀存在和差異。[118]

隨著資訊的發達及科技的進步，隨之改變戰爭的型態，「資電優勢」將主導戰爭初期的重要因素，在 1991 年的波灣戰爭及 2003 年伊拉克戰爭中，都可以看到美軍使用資訊戰的身影，就連 2007 年以色列對敘利亞以 F-15 戰機實施空中攻擊前，也用網路資訊戰方式將敘利亞的防空系統癱瘓。[119]當前的資訊技術已大幅改變冷戰時代以來的世界政治架構、軍事戰略、經濟與資訊活動，無論是攻擊性或是防禦性的資訊作戰，其成功關鍵均仰賴跨部門統合，以及國防、外交、經濟與政治等全方位的協調合作，方能夠發揮最大效用，然而資訊作戰的內容廣泛，考量研究範圍及內容，僅就網路資訊戰於未來戰爭中的角色作為研析及論述。

第一節　網路資訊作戰之本質與特色

要了解資訊作戰(Information Operations, IO)的本質與特色之前，我們必須先確認其定義，以及資訊作戰與資訊戰（Information Warfare, IW）的不同，在美軍

---

117 彭錦珍，〈現代化發展趨勢下的資訊社會與資訊戰〉，《復興崗學報》，第 86 期，2006 年，頁 31。

118 嚴怡民，〈今日天涯若比鄰:著名科學家談信息科學〉（廣西師範大學出版社, 1999 年)，頁 10-11。

119 樊高月、趙力昌，〈不流血的戰爭-網絡攻防經典之戰〉，（北京：解放軍出版社，2014 年 3 月），頁 77-90。

1998 年版的「聯戰準則 3-13 資訊作戰」(Joint Publication 3-13 Information Operations，以下簡稱 JP3-13)中，將資訊作戰定義為「為影響敵方資訊及資訊系統，同時保護己方資訊和資訊系統所採取的各種行動。」[120]而資訊戰定義為「當危機或衝突發生時，為了達到或促成對敵的特定目標，所進行的資訊作戰。」[121]有許多軍事理論家認為，資訊戰是資訊作戰失敗後所採用的作戰方法，但這兩個領域間還有其他細微的不同之處。[122]此定義把資訊戰侷限在自「衝突」或「危機」發生後所進行的作戰方法，而這些方法也包含在資訊作戰的各種手段之中；資訊作戰，本身應是不論在平時或戰時皆應持續進行的形塑環境的有效工具，所以當然資訊作戰包含了資訊戰，兩者所利用的手段十分雷同，只是資訊戰是當危機或衝突發生時，才須採取的資訊作戰，那又如何定義危機與衝突呢？現今作戰型態的不斷改變，在一場戰爭或衝突事件中決定何時為衝突點或危機點，是件十分困難的事情，且這兩突發事件點，也可能代表著不同事件，再者，衝突點及危機點又常不代表著同一事件，指揮決策者要如何決定發起資訊戰的時機？另一方面，資訊作戰早在承平時期就已經在進行了，資訊戰與資訊作戰，事實上僅是密度與廣度的不同，對於執行單位、手段及裝備等都無顯著的差異。因此，有學者認為，沒有必要再從資訊作戰中分出資訊戰。[123]

基此，所謂網路戰是指敵對雙方爭奪制資訊權，取得自身戰爭可利用的資訊和網路環境。通過電腦網路保護自身資訊和網路系統的安全，並擾亂、破壞與威脅對方的系統。與傳統戰爭相比，網路戰具有突然性、隱蔽性、不對稱性和代價低、參與性強等特點，網路戰屬於資訊戰的特殊形式，乃在網路空間進行一系列的襲擾、竄改、竊取、監視與破壞的作戰行動。[124]

在美軍 2006 年版「JP3-13」中，將資訊作戰定義為：「整合運用電子戰

---

120 Joint Chiefs of Staff, Joint Pub 3-13, *Joint Doctrine for Information Operations*(Washington, DC: Joint Chiefs of Staff, 1998),p.7.

121 Ibid.

122 里 阿米斯德(Leigh Armistead)著，余佳玲譯，《資訊作戰-以柔克剛的戰爭》(Information Operations : Warfare and the Hard Reality of Soft Power)(台北：國防部，2008 年 8 月)，頁 29。

123 郁瑞麟，〈資訊作戰定義探討與釋疑〉，《國防雜誌》，第 3 卷第 24 期，2009 年 6 月，頁 50-53。

124 李程禹，〈中共網路作戰之戰略邏輯分析：網路戰與網路中心戰的區隔與應用〉，《復興崗學報》，第 90 期，2007 年，頁 252。

(Electronic Warfare, EW)、網路戰(Computer Network Operations, CNO)、心理戰(Psychological Operations, PSYOP)、軍事欺敵(Military Deception)及作戰安全(Operations Security)等核心能力並配合特定的支援及相關能力，去影響、中斷、破壞或奪取敵方人、機指揮決策機制，同時保護己方。」[125]但在 2012 年版的 JP3-13 中，則修改了對資訊作戰的定義:「在軍事行動中，綜合運用資訊相關能力，與其他作戰方式共同作用、影響、擾亂、破壞或竄改敵人或潛在敵人的決策，同時保護己方。」[126]，其中首次提出了「資訊相關能力」(Information-Related Capabilities，IRCs)的概念以及作出新的闡述，[127] 而為了將資訊作戰貫穿於聯合作戰的各個階段，以及達成作戰目標，必須將資訊相關能力與其他作戰行動與手段綜合交互使用，為此，在 2012 年版本中，專門用一個章節來說明資訊作戰的組織與協調，並強調所有資訊相關能力的綜合運用，而在此章節中表達最重要的一個觀念是—達成資訊作戰目標的關鍵不在於擁有多少種能力，而在於這些能力的運用；在制定作戰計畫時，必須全面考量所有資訊相關能力並綜合使用。[128]

資訊作戰具有戰場透明化、整體協調化、行動同時化、打擊精確化、空間廣闊化的特徵，[129]現在由於網際網路的流行，資訊交換的速度與便利性增加，使得資訊的的互聯性及使用性變得更加活絡且不易掌握，以致於網路資訊戰成為各國積極研發與投入的領域。

網路資訊戰是以網路為平臺的戰爭，人們真正關注網路資訊戰始於 1988 年的莫里斯事件（Morris worm）。1988 年 11 月 2 日，美國康乃爾大學 23 歲研究生

---

125 Joint Chiefs of Staff,op.cit., p.9.

126 Ibid,p.7.

127 「資訊相關能力」定義為「對資訊環境的三個領域產生影響的工具、手段或活動」，而這些能力包括：戰略通聯(Strategic Communication)、聯合跨機構協調小組(Joint Interagency Coordination Group)、公共事務(Public Affairs)、軍民聯合行動(Civil Military Operations)、網路空間作戰(Cyberspace Operations)、資訊確保(Information Assurance)、太空作戰(Space Operations)、軍事資訊支援作戰(Military Information Support Operations)、情報(Intelligence)、軍事欺騙(Military Deception)、作戰安全(Operations Security)、特種技術行動(Special Technical Operations，STO)、聯合電磁頻譜作戰(Joint Electromagnetic Spectrum Operations，JEMSO)及關鍵領導交戰(Key Leader Engagement，KLE)等。

128 Joint Chiefs of Staff, Joint Pub 3-13, *Joint Doctrine for Information Operations* (Washington, DC: Joint Chiefs of Staff, 27 Nov, 2012), p.II-1-5.

129 簡華慶，〈網路資訊戰所扮演角色及因應策略之研究〉，《國防雜誌》，第 27 卷第 1 期，2012 年，頁 123。

莫里斯用病毒入侵美國國防部戰略 C4I 系統的電腦主控中心和各級指揮中心，約 8500 台軍用電腦受感染，直接經濟損失達上億美元。[130]而首次把網路攻擊手段引入到戰爭中並發揮作用的是 1991 年的波灣戰爭，美國情報員在伊拉克新購買的印表機中嵌入病毒晶片，致使伊拉克防空體系中的預警和 C3I 系統癱瘓，為美軍順利實施空襲創造了有利條件。[131]

美國是世界上第一個提出網路戰概念的國家，1993 年，美國蘭德公司的阿爾奎拉和倫費爾特第一次正式提出了網路戰的概念，於 1996 年發表了題為「網路戰的來臨」（The Advent Of Netwar）的研究，認為網路戰為干擾、破壞敵方網路資訊系統，並保證己方網路資訊系統的正常運作而採取的一系列網路攻防行動。[132]

在網路資訊技術高度成熟的今天，網路戰的涵義又有了新的擴展，從廣義上講，資訊技術的發展快速地拓展了網路戰的平臺和基礎，網路戰不再僅僅依附於傳統的戰爭而存在，已經拓展和波及所有與網路相關的事件和人員。目前全世界網路使用者已經超過 40 億人，人類完全進入網路時代的今天，廣義網路戰必然成為未來網路戰的主要形式，也越來越呈現出與傳統戰爭不同的特點。網路資訊戰雖有行動快速、不易防護、難以估算以及可否認的特性，但其受限於網路平台及作業系統，其受攻擊的一方須有基本建設，如實體網路、伺服器、電腦終端的硬體設備以及系統作業軟體和數位資料等項，倘若受攻擊的一方電腦未開機作業、網路無法連接、系統嚴密監控、資訊傳遞加密等項，則網路攻擊所獲得的預期成果有限。另外，利用資訊網路戰實施攻擊時，也並非全部有利於攻擊一方，其所獲得之資訊，也並非全部可使用，須進一步分析與研究，有時攻擊的一方也會擷取到無用甚至假的資訊。[133]網路能夠載舟，亦能覆舟，現在資訊隨手可得，藉由網路的散播與傳遞，更加速氾濫的地步，面對蜂擁而來的龐大情報資訊，在

---

[130] Thomas A. Longstaff, "Security of the Internet," *Software Engineering Institute*,1997.At https://resources.sei.cmu.edu/asset_files/SpecialReport/1996_003_001_496597.pdf (Accessed 2017/10/24)

[131] 淡志隆，〈伊拉克自由行動中資訊作戰與快速掌控之實踐〉，《國防雜誌》，第 20 卷第 3 期，2005 年 3 月，頁 75-78。

[132] John Arquilla、David Ronfeldt," The Advent Of Netwar,"1996,*The RAND corporation*.At https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR789/MR789.ch1.pdf (Accessed 2017/10/24).

[133] 同註 129，頁 125-128。

作戰期間對於情報資訊的分類、判讀、處理及分發就變得相當重要。

在軍事作戰中，當網路攻擊與實體部隊搭配運用時，區分「戰術性網路攻擊」及「戰略性網路攻擊」等兩種，前者主要伴隨於軍事行動中，操作手以具部隊形態之軍文職人員為主，利用網路攻擊行為將敵指管機制破壞及癱瘓，或是蒐集敵情報與作戰資訊，加以研析後分送相關參謀作業運用，以利指揮官下達決心，其行為較為直接。例如以色列 2007 年 9 月 6 日所執行的「果園作戰」(Operation Orchard)，利用電腦網路，將「特殊程式」植入敘利亞的防空雷達系統使其癱瘓，以色列派遣 F-15 及 F-16 戰機直接飛越敘利亞領空轟炸其核子設施，事後並沿原路返回，毫無遭受任何攻擊。[134]在戰略性攻擊方面，則範圍較為廣大，不侷限於軍事行動，舉凡竊取金融資料、破壞電力設施、擾亂交通運輸及竊取網路資訊等，造成全國動亂或損壞社會秩序皆屬之，但此種戰略性攻擊，並不像戰術性攻擊，有其時間較短或行為較明顯特色，有時攻擊的時間長達數月甚至數年之久，其操作人員除部隊外、舉凡由政府機構所號召的駭客、學生、專業及業餘人士等皆可參與，[135]例如 2003 年起的驟商、科學研究室等受到網路攻擊；而 2009 年 12 月的極光行動(Operation Aurora)，使得 Google、Adobe、Jupiner 等 20 多家公司受到攻擊損失，[136]這些都可能來自中國大陸的網路攻擊，然舉證的困難、無適用的國際公法及無相關的協定條約，使得此種行動一直現存，難以防範消彌。

網路作戰是一種輔助作戰的形態，在攻擊方面，利用程式漏洞、網站攻擊、惡意程式等取得敵人資訊或癱瘓網路，其目的為使我方取得正確情報，另一方面讓敵人無法使用網路實施資訊傳遞，增加人工作業，並讓攻擊的實體部隊作戰行動取得較優態勢，加快作戰節奏；在防禦方面，屬於被動式範疇，不但在重要指管及機敏網路要有層層的建置，且花費的金錢、時間與人力，遠大於使用攻擊方式，但不論網路的攻防程度為何，是無法主導戰場勝負或是獲致決定性之勝負，

---

134 David A. Fulghum, "Israel used electronic attack in air strike against Syrian mystery target," *ABC News Internet*, Oct. 8, 2007.At https://abcnews.go.com/Technology/story?id=3702807&page=1 (Accessed 2017/10/24)

135 同註 129，頁 130。

136 John Markoff、David Barboza, ,2 China Schools Said to Be Tied to Online Attacks," *The New York Times*, Mar. 26 2010. At http://www.nytimes.com/2010/02/19/technology/19china.html. (Accessed 2017/10/24)

因為要達到傳統戰爭所帶來立即的人員死傷及財務損壞，依目前的網路技術仍有相當距離，就如同三軍聯合作戰，海、空軍行動所帶來之優勢，若無陸軍對敵國的實體攻擊與占領，很難達到讓敵人屈服的目的。[137]

國防大學
National Defense University

[137] 同註 129，頁 130。

表 2- 2　網路資訊攻擊技術型態分類

項次	名稱	特性
1	竊取 (Eavesdropping)	網路通訊時，大部分採用文字格式，若未加密時，只要能夠存取網路上的路徑，就可以截取或讀取相關資訊。
2	數據修改 (Data Modification)	利用非法擷取的資訊，在雙方（寄件及收件者）都不知情況下，實施竄改並放回網路繼續傳遞。
3	身分欺騙 (Identity Spoofing)	利用程式去建立假的IP數據封包，讓看起來像組織網路內合法的有效位址，以利修改、改變路由或刪除資料。
4	密碼相關攻擊 (Password-Based Attacks)	大多數資訊系統對於資料存取權限，皆以使用者名稱及密碼作為存取的基本條件，一旦被成功登入後，可獲得相關資料，甚至進而取得電腦控制權。
5	阻斷式服務攻擊 (Denial-of-Service Attack)	利用大量密集的封包傳送，癱瘓被攻擊的網站，使合法的使用者無法獲得服務。
6	中間人攻擊 (Man-in-the-Middle Attack)	第三者利用雙方通信過程且不知情的情況下，在網路監控及擷取相關資訊，並加以運用。
7	密碼破解攻擊 (Compromised-Key Attack)	利用工具來破解加密的密鑰，獲得其程式碼或字元，進而解密或修該資料。
8	嗅探攻擊 (Sniffer Attack)	利用應用程式或工具可讀取、監控網路所傳遞的封包及資料，並開啟及讀取資訊，作為後續運用。
9	應用層攻擊 (Application-Layer Attack)	用來攻擊應用層伺服器中的應用層式層，使作業系統或應用程式故意造成錯誤，例如溢位攻擊，進而取得應用程式或網路的控制權。

資料來源：”Common Types of Network Attacks,” *The Microsoft*, July 18 2012.At http://technet.microsoft.com/en-us/library/cc959354.aspx

第二節　美軍網路資訊作戰之發展與運用

網路資訊作戰發展，現已成為各國軍事的重要環節，除了中共的網軍一直是令美國頭痛的假想敵外，俄國的網軍實力亦不容小覷。自 2015 年 9 月俄羅斯介入敘利亞局勢以來，俄羅斯整體資訊網路控管的實力再次得到了提升。[138]面對美國外部不斷的威脅，美國總統川普在 2017 年 8 月 18 日宣佈，決定將美軍網路司

[138] 張乃千，〈招兵買馬，擴軍後的俄羅斯「網軍」戰力幾何？〉，《中國軍網》，2017 年 4 月 5 日。參見 http://www.81.cn/gjzx/2017-04/05/content_7551055.htm (瀏覽日期：2018 年 1 月 31 日)

令部升級為最高級別的聯合作戰司令部，川普強調，網路司令部將進一步強化美國的網路安全，也將加強與盟邦的合作，對全球網路安全威脅做出快速反應，[139]在網路司令部層級提高後，便與原來的上級單位戰略司令部同級，成為美軍最高級別的聯合作戰司令部之一，美軍原先共有九個聯合作戰司令部（Unified Combatant Command），其中六個按戰區劃分，分別為北方、南方、中央、非洲、歐洲、太平洋；三個以職能劃分，分別為戰略司令部、特種作戰司令部、運輸司令部，而網路司令部將成為第四個按照職能劃分的聯合作戰司令部，也是美軍第十個聯合作戰司令部，而將網路司令部升級成為聯合作戰司令部層級，意味著網路空間正式與陸、海、空和太空並列成為美軍的第五維戰場，而網路司令部升級之後，也成為與美軍陸、海、空三個軍種一樣的一級司令部，雖然網路是一個虛擬空間，但實際有其運作，而將之視為美軍新增的一個軍種「網軍」也無不可。

美軍網路司令部（United States Cyber Command）成立於 2009 年，由歐巴馬總統授權國防部長蓋茨正式簽署備忘錄，宣布合併全球網路作戰聯合特遣部隊和網路戰聯合功能構成司令部，組建美軍網路司令部，成為隸屬戰略司令部的二級司令部，它的實體屬於美國國家安全局，第一任網路司令部司令由國家安全局局長基思·亞歷山大(Keith B. Alexander)中將兼任，此後美軍網路司令部一直與美國國家安全局設置於同一地點，國家安全局局長兼任網路司令部司令， 2010 年正式運作後，統管全軍網路安全和網路作戰指揮，隸屬於美軍戰略司令部。

與此同時，歐巴馬政府推出一系列戰略，推進美國和美軍的網路戰建設，2011 年 5 月 16 日，歐巴馬政府公布「網路空間國際戰略」（International Strategy for Cyberspace），宣布「網路攻擊就是戰爭」，表示如果網路攻擊威脅到美國國家安全，將不惜動用軍事力量進行報復。[140]2011 年 7 月 14 日，美國國防部發布首份《網路空間行動戰略》，新戰略包括「五大支柱」(Five Pillars)：第一，將網路空間列為與陸、海、空、太空並列的「行動領域」，國防部以此為基礎進行組

[139] Jim Garamone and Lisa Ferdinando, " DoD Initiates Process to Elevate U.S. Cyber Command to Unified Combatant Command," Aug. 18, 2017. At https://www.defense.gov/News/Article/Article/1283326/dod-initiates-process-to-elevate-us-cyber-command-to-unified-combatant-command/ (Accessed 2018/1/31)

[140] Barack Obama, " International Strategy for Cyberspace,"May 2011.At https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (Accessed 2017/2/1)

織、培訓和裝備，以應對網路空間存在的複雜挑戰和巨大機遇；第二，變被動防禦為主動防禦，從而更加有效地阻止、擊敗針對美軍網路系統的入侵和其他敵對行為；第三，加強國防部與國土安全部等其他政府部門及私人部門的合作，在保護軍事網路安全的同時，加強重要基礎設施的網路安全防護；第四，加強與美國的盟友及夥伴在網路空間領域的國際合作；第五，重視高科技人才隊伍建設並提升技術創新能力。[141]

美國目前所編組 133 支網路部隊分別由 13 支國家任務小隊、68 支網路保護小隊、27 支作戰任務小隊與 25 支支援小隊組成，國家任務小隊主要保護美國國內電網、核電站等重要基礎設施；網路保護小隊主要保護美國國防部的網路與系統；作戰任務小隊主要執行進攻任務；支援小隊為國家任務小隊與作戰任務小隊提供分析與規劃方面的支持，美國網路司令部的官員亦表示，其目標是 2018 年 9 月 30 日之前將人員規模提升至近 6200 名，且要求 133 支團隊盡皆擁有全面作戰能力，相關官員同時補充到，全面作戰能力意味著各網路任務部隊下屬團隊擁有充分而全面的作戰能力。[142]

美軍網路司令部轄下網路任務小隊各團隊的關注重點聚焦於國防部網路發展戰略中提出的三項核心使命：防衛國防部網路並確保其數據安全性；支持聯合軍事指揮官制定的各項作戰目標；在接收到指令後，保護美國的各項關鍵性基礎設施，具體來講，網路任務部隊下轄各團隊需要經由以下任務支持上述目標：國家任務小隊下轄各團隊負責追蹤敵對勢力活動、阻斷攻擊並以機動性方式發動攻擊，從而保護美國國家安全；作戰任務小隊下轄各團隊負責支持各位作戰指揮官，從而完成自身網路層面軍事行動；網路保護小隊轄下各團隊負責防衛國防部資訊網路、保護高優先級任務並幫助各網路部隊作好戰鬥準備；網路支持小隊轄下各團隊為國家使命與戰鬥使命部隊提供分析與規劃性支持。

在為聯合軍事指揮官所制定的作戰目標提供支持時，各現役網路任務小隊轄

---

[141] Department of Defense , " Department of Defense Strategy for Operating In Cyberspace," July 2011, At https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf (Accessed 2017/2/1)

[142] Defense of Department, " DoD's Network Defense Headquarters Achieves Full Operational Capability," *U.S. Cyber Command News Release*, Jan. 31, 2018.At https://www.defense.gov/News/Article/Article/1429130/ (Accessed 2018/2/21)

下團隊分別根據各聯合軍事總部網路（Joint Force Headquarters Cyber,JFHQ）為作戰指揮官提供支持：JFHQ-C MARFORCYBER 負責支持美國特種作戰司令部；JFHQ-C ARCYBER 負責支持美國中央司令部、美國非洲司令部與美國北部司令部；JFHQ-C FLTCYBER 負責支持美國太平洋司令部與美國南部司令部；JFHQ-C AFCYBER 負責支持美國歐洲司令部、美國戰略司令部以及美國軍事運輸司令部，各網路司令部團隊亦被分配至網路國家作戰部隊與國防部聯合軍事資訊網路總部—即網路司令部旗下的各分支總部。[143]

網路國家作戰部隊負責規劃、指導並協調網路空間之作戰行動，旨在阻止、破壞並在必要時攻擊對方網路層面力量，從而捍衛美國國家安全。其中「捍衛國家安全」所涵蓋的具體任務包括：根據總統或者國防部長的指示捍衛美國及其相關利益，防止網路攻擊對美國國家關鍵性基礎設施造成的重大後果，此類重大後果將造成生命、重大財產損失、給美國外交政策造成的嚴重後果以及嚴重經濟影響;著眼於最為強大的網路敵對威脅，包括民族國家網路敵對勢力、非民族國家敵對勢力乃至新興威脅。[144]

國防部聯合軍事資訊網路總部則負責提供網路資訊作戰與全球範圍內防禦性網路作戰行動提供命令與控制支持，用以協調國防部轄下各部隊的保護任務以及一切跨戰區軍事行動，其網路保護團隊則積極致力於加強國防部網路邊界的防禦工作。[145]

面對瞬息萬變的網路環境，美國陸軍制定出三階段訓練法最具特色，分別從單兵訓練、集體訓練到任務預演型訓練等依階段性的訓練以達成目標。在單兵訓練時，讓官兵掌握實施網路攻防作戰所需的核心知識、技術和能力，接下來實施集體訓練，亦稱分隊訓練，是指讓網路分隊沉浸在貼近實戰的環境中演練如何應對各類網路威脅，重在練習戰術、檢驗資質和磨練團隊，最後是任務預演型訓練，強化分隊行動能力並為執行既定任務做好準備，重點是提高網路分隊指揮官

---

[143] Defense of Department, " All Cyber Mission Force Teams Achieve Initial Operating Capability," *U.S. Cyber Command News Release*, Oct. 24, 2016.At https://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability/ (Accessed 2018/2/21)

[144] Ibid.

[145] Ibid.

對任務、威脅和風險的理解和認識。[146]

為確保網路部隊具備高實戰能力，美軍要求網路訓練應與實戰狀況接近，一是場景設計上要求從難從嚴，而網路空間防禦無法做到無懈可擊，因此訓練時應把真實的網路空間條件融入所有兵棋推演和演習中。為此，美軍在構建訓練環境時強調緊貼實戰狀況，依據現實威脅的發展變化定期對模擬威脅和訓練條件進行更新調整，例如，為演練進攻性網路行動，陸軍國家訓練中心對訓練設施進行了大幅升級改造，包括將無線網路接入模擬村莊、提供手提電腦和智能手機等，敵人可利用無線網路定位美軍士兵，友軍也可利用該網路探測和挫敗威脅，二是演練方式上強調紅藍對抗，假想敵訓練是美軍訓練文化的組成部分，網路假想敵通常被稱為「紅隊」，目前，美軍已經建成專業化的網路「紅軍」，無論是大型網路演習還是小型分隊訓練，都採取紅藍對抗的形式組織實施，[147]2017 年 7 月，美國空軍網路司令部組織了為期 4 週的「黑惡魔」演習，專門協調了一支專家級網路「紅軍」參演，有效檢驗了兩支網路防護分隊的作戰能力。[148]

美軍認為，團隊合作是維護網路安全的首要原則，為了增強網路空間聯合行動能力，美軍提出了聯合網路訓練標準，摸索軍種間聯合的網路訓練，完善軍民聯合網路演習，而聯合網路訓練也有顯著的成效，其一，規範網路任務部隊的聯合基礎訓練，美軍網路任務部隊直屬於美國網路司令部，但人員和裝備卻由各軍種提供，為了統一訓練內容和標準，美國網路司令部提出了《聯合網路空間訓練和認證標準》（Joint Cyberspace Training and Certification Standards,JCT&CS），內容包括網路通用核心技術、網路行動計劃員課程、聯合高階網路戰課程等，確保軍種網路分隊能夠合作，截至 2017 年底，美國陸軍和海軍的網路任務小隊已經全部完成訓練，陸續通過美軍司令部的完全作戰能力驗證。[149]

國防大學
National Defense University

---

146 陸航輝、費玉春，〈備戰第五空間，美軍網路部隊如何練兵〉，《中國軍網》，2018 年 1 月 18 日。參見 http://www.81.cn/wjsm/2018-01/18/content_7914213.htm (瀏覽日期：2018 年 2 月 24 日)

147 Michael Giles, " Red Cell Challenges Cyber Warriors in Multiforce Exercise," *Defense of Department,* Apr. 28, 2017.At https://www.defense.gov/News/Article/Article/1166093/red-cell-challenges-cyber-warriors-in-multiforce-exercise/ (Accessed 2018/2/21)

148 同註 146。

149 林小春，〈美陸軍海軍網路部隊提前具備完全作戰能力〉，《新華網》，2017 年 11 月 13 日。參見 http://big5.xinhuanet.com/gate/big5/us.xinhuanet.com/2017-11/03/c_1121901605.htm (瀏覽日期：2018 年 2 月 24 日)

其二，探索軍種間聯合網路訓練，網路空間行動與陸、海、空、太空領域作戰行動的戰術融合，是美軍聯合作戰增效的助推器，過去一年，隨著「多域戰」概念被正式寫入陸軍新版作戰條令，美國陸軍率先嘗試了軍種間聯合網路訓練。2017 年 10 月，陸軍首次在「網路閃電戰」（Cyber Blitz）演習中邀請空軍國民警衛隊的聯合終端攻擊控制員參演，負責協助旅戰鬥隊指揮官運用動能和非動能武器，演練如何運用聯合終端攻擊控制員打擊目標。[150]

其三，定期展開軍民聯合網路演習，美軍認為，要完成軍方肩負的三大網路使命，必須與其他聯邦政府機構、州和地方政府特別是民間企業進行合作，鑑於恐怖分子與網路空間結合等趨勢，除了上述國土安全部被賦予執行網路安全等工作外，也主導結合各民間企業、大學、州政府，來強化對於資訊交換與合作的管道，主動管理網路相關威脅，以及協調網路資訊共享，目的是能夠在複雜環境中，迅速處理網路安全問題，其中重要的合作夥伴即是私人企業、學術界、聯邦機構以及國內外重要組織機構，[151]甚至後來國土安全部每兩年舉行一次的網路風暴演習(Cyber Storm)，也是強調在政府與私人企業進行合作，提升對於網路安全威脅的因應能力。[152]

美軍在第三次抵銷戰略中，對於網路資訊作戰以及研發人工智慧領域投注相當多資源，希望美軍具備陸、海、空、太空、網路空間的聯合作戰能力，並透過人工智慧以及機器人科技發展軍事武器，藉以對抗中國與俄羅斯的威脅。與 5 年前相比，美國在人工智慧、大數據與雲端運算等三大領域的投資從 56 億美元增加至 74 億美元，隨著美軍軍事訓練、計劃的變動，將會持續挹注經費研發。[153]紐約時報曾報導，中國企業透過人工智慧，在商業領域取得高度發展。微軟工程師團隊於 2016 年時宣稱已創造出可與人類匹敵的語言理解軟體，但中國最大搜

國防大學 National Defense University

[150] Mark Pomerleau, " Cyber Blitz: Army's military hide-and-seek tests cyber, EW tools," *Fifth Domain Cyber*, Oct. 2, 2017.At https://www.fifthdomain.com/electronic-warfare/2017/10/02/cyber-blitz-armys-military-hide-and-seek-tests-cyber-ew-tools/ (Accessed 2018/2/21)

[151] "About us-US-CERT," Department of Homeland Security, Mar. 15, 2015.At https://www.us-cert.gov/about-us (Accessed2018/2/28)

[152] "Cyber Storm: Securing Cyber Space," Department of Homeland Security, At https://www.dhs.gov/cyber-storm (Accessed 2018/2/28)

[153] Christian Davenport, " Future wars may depend as much on algorithms as on ammunition, report says," *Washington Post*, Dec. 03, 2017.At https://www.bostonglobe.com/business/2017/12/03/future-wars-may-depend-much-algorithms-ammunition-report-says/pVT69lcgAGW6XFipB3nF3J/story.html (Accessed 2018/2/28)

尋引擎－百度卻在兩年前就已發展類似軟體，且能在中文上取得相等的準確性。而現在於百度擔任總裁暨營運長的陸奇，則預劃將百度塑造為全球人工智慧的領導者，也使中國在人工智慧的領域又更加進步。[154]美國白宮於 2016 年十月份發布一份關於人工智慧科技的報告，報告指出中國在人工智慧領域的學術研究產出已超越美國，[155]代表美國已意識到中國在人工智慧科技的進步。新美國安全中心（Center for a New American Security）所發布的報告指出，未來美中兩國在人工智慧領域方面的競爭可能會改變經濟和軍事力量的平衡，且中國在人工智慧領域可能會在五年內超過美國。[156]具有人工智慧的軍事機器人一直存在著道德問題，美軍必須思考將這些技術應用在軍事的可能性，但若把具有人工智慧的機器人系統和技術視作對人類生存的威脅，可能會讓美國失去軍事優勢，因為中共、蘇俄也都在摸索與發展此技術。機器人技術和人工智慧對於未來軍隊設計最重要的特徵，包含可以縮小各個單獨平台的實際規模和總成本、提升偵查敵對力量的能力、實現電路小型化優勢以及零件和次微觀材料（submicroscopic structure）大規模訂製的出現。隨著成本降低，軍方便可以將其餘的經費拿來升級和保養昂貴軍艦、飛機與戰車或是增強進攻、防禦平台等。在未來的戰爭中，機器人技術必須把陸、海、空軍與網路能力相結合，以打擊敵人的平行或複雜的序列目標；從指揮控制的角度來看，對行動和能力進行分配，以實現不同單位間的持續聯絡，一名作戰人員可能就要指揮整個跨領域的作戰群體(swarm)，利用網路連貫性打贏這場競爭；忽視機器人和人工智慧的承諾並不能避免戰爭的開打，若因為道德問題或是擔憂，便阻止機器人開發，將會對美軍的軍事發展有所侷限。[157]

---

[154] John Markoff and Matthew Rosenberg, " China's Intelligent Weaponry Gets Smarter," *The New York Times*, Feb. 3, 2017.At https://www.nytimes.com/2017/02/03/technology/artificial-intelligence-china-united-states.html?_ga=2.54449640.1176452203.1523270908-2006262106.1521270436 (Accessed 2018/2/28)

[155] Executive Office of the President National Science and Technology Council Committee on Technology, " Preparing for the Future of Artificial Intelligence," *White House*, Oct. 2016.At https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf (Accessed 2018/2/28)

[156] Zachary Cohen, " US risks losing artificial intelligence arms race to China and Russia," *Cable News Network*, Nov. 29, 2017.At https://edition.cnn.com/2017/11/29/politics/us-military-artificial-intelligence-russia-china/index.html (Accessed 2018/2/28)

[157] Jeff Becker, " How to Beat Russia and China on the Battlefield: Military Robots," *The National Interest*, Mar. 18, 2018.At http://nationalinterest.org/blog/the-buzz/how-beat-russia-china-the-battlefield-military-robots-24963 (Accessed 2018/04/08)

隨著資訊化的普及帶動了現代化，各種威脅來源越來越廣泛，美國非常重視如何防範於未然，當應對有關網路安全威脅時，處理問題之前即具備專業性與獨特性，而情報體系更必須在龐大的組織體系中，發揮其專業能力，同時提升傳遞訊息的效率與安全，才能將危害降到最低，進一步確保國家安全。

第三節　中共網路資訊作戰之發展與運用

資訊作戰的戰場是多維的空間，以資訊技術為基礎的高科技武器裝備的使用，使戰場空間不再侷限於陸、海、空，而是擴大到太空，還出現了虛擬的電磁空間和網路空間，連同虛擬的認知空間，形成了一個多維且立體的作戰空間。而資訊作戰的任務是為了奪取和保持資訊優勢，共軍除了使用「資電優勢」的概念外，也提出了「制資訊權」的概念，所謂制資訊權，就是在一定時空範圍內控制戰場資訊的主導權，[158]徐國興則認為，當獲得了一定時空範圍內的「絕對資電優勢」也就可以理解為獲得了一定時空範圍內的「制資訊權」。[159]

（一）共軍資訊作戰力量建設之具體目標

資訊作戰是影響軍隊整體戰力和能否有效發揮的關鍵，平時保護資訊安全、確保資訊系統的穩定運轉，在戰時保持網路對抗，主動、掌握制網路權等，因此，提高資訊偵測、傳輸、處理、攻擊和防禦的能力已成為中共亟欲解決的課題。

1.多元的資訊偵測能力：發展軍用偵查監測衛星、預警機、遠程警戒探測設備和水下警戒探測設備，加強對戰場資訊的控制與運用，以提升第一時間的反應和打擊能力，並加強開發以偵測器為代表的資訊獲取技術，實現戰場的探測與監控，再者是將資訊獲取技術列入國防重點之列，並作為發展和提高資訊作戰能力的重點。

2.多樣化的資訊傳輸能力：除提高資訊傳輸系統的適應能力，確保訊息傳輸

---

158 戚世權，《論制信息權》，（北京：軍事科學出版社，2001 年），頁 50。
159 徐國興，《我軍信息作戰力量建設研究》，（北京：軍事科學出版社，2013 年 3 月），頁 8。

便捷外，更要提高資訊傳輸系統的防護能力，確保資訊傳輸順暢，再者是確立新型的資訊傳輸模式，提高資訊傳輸系統的傳輸能力。

3.快速準確的資訊處理能力：若只有先進的資訊取得手段而沒有高效率的資訊處理能力，就無法將取得的資料轉化為可用情報或資訊。

4.多手段的資訊進攻能力。一是發展電子對抗能力，提高電子偵察、通信干擾、雷達干擾、光電干擾等全方位資訊攻擊能力，以破壞打擊敵指揮控制中心、通信樞紐、雷達站等要害目標為重點，採取電子干擾、電子欺騙等手段，與傳統火力打擊、精準火力打擊等手段相結合。二是提高網路攻擊能力。加快網路攻擊手段的研究與戰法應用，發展用於摧毀網路的「病毒」、「駭客」等，提高攻擊網路的節點、癱瘓系統的能力。三是增強心理戰攻擊能力。研究現代心理戰的方法與手段，開展必要的心理戰訓練。四是發揮群眾的力量，大力發展地方資訊作戰力量，藉以獲得勝利。

5.多層次的資訊防禦能力，一是增強重點目標防護能力，加強指揮中心、資訊中心、網路中心和通信樞紐的防護，增強反偵察、抗干擾、防摧毀的防護能力。二是提高系統機動生存能力，利用現代通信技術，改造戰場資訊網基礎設備。三是強化網路安全保密能力。對資訊網路系統採取防火牆、防病毒、防駭客等手段。四式採取先進的資訊安全防禦技術、工具、手段和產品，在硬體與軟體部份等復原達到有備無患的狀態，一旦防護手段和措施失效，要及時復原，使系統恢復正常。[160]

國防大學 National Defense University

（二）中共網路戰的戰略指導

中共的軍事科學院軍事戰略研究部於2013年所出版的《戰略學》一書中提到，中共在軍方和民間都有從事網路攻防的網路戰部隊，共有以下三種作戰單位：「軍事專業網路戰部隊」，該單位旨在進行防禦性和攻擊性的網路攻擊；「授

[160] 同註 159，頁 76-79。

權力量」，該單位是由軍隊授權，並有組織性的專門從事網路戰的地方力量，主要在安全部、公安部等相關政府部門內；「民間力量」，則是民間自發進行網路攻防的力量，經過動員與組織後，可用於網路作戰，網路戰專業性強，而網路戰爭對抗激烈，所以「軍事專業網路戰部隊」明顯是實施網路戰的核心力量，也是網路戰投入建設的重點，而這些單位達成下述目標：

1.維護國家重要資訊和網路安全

網路戰的目標，訂定網路戰的基本方向，而網路戰目標的確立，受國家性質，國家戰略目標，社會資訊化網路程度，資訊科技產業基礎，網路攻防能力以及對手情況等多種因素影響。在網路戰中，帶有明顯的破壞性，敵對性和排他性；資訊化，網路化程度越高，對網路依賴性越強的國家，網路戰的目標通常會相對較高; 資訊科技產業基礎好，特別是壟斷著電腦網路核心技術的國家，其網路攻防能力往往更強，追求的網路戰目標及標準也會更高。

2.妥處網路戰平戰時、攻防與威懾等關係

2.1平時與戰時

受網路自身特性的影響，任何資訊網路，都隨時面對和承受著種類繁多的網路偵察和網路攻擊，網路的防護系統，無時無刻都在與這些非法偵察和攻擊行為作戰，保護著資訊和網路系統安全。網路攻防對抗是日常性的，隨時都在進行網路戰，而戰時的網路攻防作戰，由於規模更大、更加激烈，後果更加嚴重。

2.2進攻與防禦

網路戰在整體上具有「易攻難守」的特點，如何取捨網路進攻與防禦之間的平衡，成為進行網路戰的關鍵問題。

2.3威懾與實戰

網路戰的模糊性，不確定性，以及大規模網路戰造成的難以承受的後果的確定性，可預見性，使網路威懾在一定程度上具有與核威懾類似的特徵，但基於網路戰的恐怖後果以及對能否避免遭受對方網路攻擊的不確定，任何一個國家都不

國防大學 National Defense University

敢輕易地發動網路戰，因此，對於網路問題，人們首先考慮的是如何避免爆發網路戰爭，而不是如何打贏網路戰爭，從這一角度看，未來網路大國之間有可能形成一種都有網路攻擊的手段和能力，但誰也不敢輕易挑起戰火的「平衡」威懾態勢。

3.建立精良的專業網路作戰力量

網路的普及性以及軍民共用的特點，決定了網路攻防戰力的多樣性，用於網路作戰的力量可分為「軍隊專業網路戰部隊」、「授權力量」和「民間力量」，網路戰之攻防，須具備高度專業，而真正有能力進行網路作戰的人並不多；網路戰也不同於傳統定義上的戰場對抗，作戰力量數量規模並非決定性因素，「精良」是對專業網路部隊的基本要求，即專業網路戰部隊數量要少、規模要精簡，專業化，能力強。

軍隊編制精良的專業網路戰部隊，應著重於兩點，一是依賴民間力量，網路的普及性，網路的普及性、基礎性，決定了網路菁英主要產自於民間，要善於發掘和利用民間網路之人才和資源，使軍隊專業網路戰部隊真正能夠與民間網路菁英合作，方能真正體現和反映國家網路戰能力和水平，如中共人民解放軍第61398部隊；二是研發、建設與運用相互合作，從技術角度看，網路戰攻防主要是對相應網路軟體的使用，而網路軟體使用的過程又往往十分簡單，所以，日常開發和研製網路攻防軟體武器，是最直接、最重要的網路戰基礎，也是網路戰的核心，網路軟體武器研發人員，同時也是典型的網路戰戰士，可見，在網路戰力的規劃中，要將研發、建設與運用一體籌劃，才能創造最大效益。[161]

中共人民解放軍61398部隊位於上海市浦東新區，長期受到西方國家情報部門及網路安全公司的關注，被報導為從事相關駭客活動的「中國網路戰的總部」

[161] 中共軍事科學院軍事戰略研究部編著，《戰略學》，（北京：軍事科學出版社，2013 年 12 月），頁 188-197。

[162]。2013年2月美國麥迪安網路安全公司（Mandiant Corporation）根據7年追蹤的記錄證據做出總結報告，指控中共解放軍是美國所發生一系列遭到駭客攻擊的幕後操縱者，並推測此團體極可能是61398部隊。[163]報告指稱，自2006年以來，61398部隊極可能盜取了美國百餘家公司機構的大量資訊，並試圖操控美國的關鍵基礎設施，而且研究發現，中共為解放軍設定了重要任務—在全球進行網路間諜活動和盜取資訊，麥迪安公司仍持續追蹤已知超過20個同樣來自中國的「先進持續性滲透攻擊」(Advanced Persistent Threat，APT)駭客集團，而61398部隊僅為其中之一，報告認為，61398部隊最有可能是策動駭客襲擊的後台。麥迪安報告描述的駭客活動結論，提及美國政府情報人員證實「美方已對61398部隊的行為做了多年的跟蹤和研究」，其內容以智慧財產權和美國基礎建設為對象。[164]

根據報告，該部隊技術嫻熟，有一套明確攻擊方法，駭客對象橫跨二十個工業行業、近百餘企業及主機，目標在於竊取大量寶貴智慧財產權資訊，在成功入侵後，獲取存取通道，該部隊會在數月、數年內定期存取受害者以持續竊取各種資訊。七年中被監測到針對近一百五十家公司組織的攻擊企圖，遭竊資料達數十萬GB，內容「包括技術藍圖、專有的製造工藝流程、測試結果、商業計劃、定價檔案、合作協議、電子郵件、聯繫人列表。」[165]美國智庫報告顯示，61398部隊隸屬「總參三部二局」。總參三部，全稱「中國人民解放軍總參謀部技術偵察部」，為正軍級單位，負責蒐集海外軍事情報的官方機構，與國家安全部、總參

---

[162] 〈英媒：61398 部隊—中國網戰中心〉，《BBC 中文網》，2013 年 2 月 20 日。參見 http://www.bbc.com/zhongwen/trad/china/2013/02/130220_press_61398_cyber.shtml (瀏覽日期:2018 年 2 月 25 日)

[163] Dan Mcwhorter, "Mandiant Exposes APT1 – One of China's Cyber Espionage Units & Releases 3,000 Indicators," *FireEye*, Feb. 19, 2013.At https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html (Accessed 2018/2/21)

[164] David E. Sanger, David Barboza and Nicole Perlroth, " Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," *The New York Times*, Feb. 18, 2013.At http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html (Accessed 2018/2/21)

[165] "APT1：Exposing One of China's Cyber Espionage Units," *Fire eye*, Feb. 19, 2013.At https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf (Accessed 2018/2/21)

謀部情報部等，共同構成中共情報網路；總部設在北京，於上海、青島、珠海、哈爾濱、成都等地駐有機構，負責「信號情報」，工作估計包括監聽電子通訊、分析衛星情報、破解密碼等，編制估計上萬人，[166]共軍的61486部隊則是第二個由西方媒體揭露，中共用以竊取國外商業和軍事機密為任務的軍事單位。[167]

2014年5月，美國司法部起訴中共五名解放軍61398部隊的軍官，因為這些人涉嫌從西屋電氣(Westinghouse Electric)、美國鋼鐵公司(U.S. Steel)、美國鋁業公司(Alcoa)等幾家規模最大的美國公司竊取商業機密。[168]2015年6月，美國聯邦人事管理局宣布，共有超過四百萬筆的前、現任聯邦雇員個人紀錄資料外洩案。聯邦官員聲稱，本案為美國政府歷史上最大的資料外洩案之一，資料外洩的內容包含有可資識別的個人訊息，例如社會安全號碼、姓名、出生年月日與居住地址等。[169]《華爾街日報》及《華盛頓郵報》則引述不具名的政府官員說法稱，本起資料外洩案疑是中國駭客所為，[170]上述兩例，均顯現出中共對他國政府、跨國企業進行網路破壞、攻擊，雖中共均予以否認，且在共軍編裝與官方公開訊息中亦無明確事證，但從上一段落中所探討之內容，我們可明確得知中共確實有軍方及民間之網路部隊。

---

166 Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao, " The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," *Project 2049 Institute*, Nov. 11, 2011.At http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf (Accessed 2018/2/21)

167 Nicole Perlroth, " 2nd China Army Unit Implicated in Online Spying," *The New York Times*, Jun. 9, 2014.At https://www.nytimes.com/2014/06/10/technology/private-report-further-details-chinese-cyberattacks.html (Accessed 2018/2/21)

168 Michael S. Schmidt, " 5 in China Army Face U.S. Charges of Cyberattacks," *The New York Times*, May 19, 2014.At https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html (Accessed 2018/2/21)

169 Kevin Liptak, Theodore Schleifer and Jim Sciutto, " China might be building vast database of federal worker info, experts say," *Cable News Network*, Jun. 6, 2015.At https://edition.cnn.com/2015/06/04/politics/federal-agency-hacked-personnel-management/ (Accessed 2018/2/21)

170 Devlin Barrett, Danny Yadron and Damian Paletta, " U.S. Suspects Hackers in China Breached About 4 Million People's Records, Officials Say, " *The Wall Street Journal*, Jun. 5, 2015.At https://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888 (Accessed 2018/2/21)；Sam Sanders, " Massive Data Breach Puts 4 Million Federal Employees' Records At Risk. " *National Public Radio*. Jun. 4 2015.At https://www.npr.org/sections/thetwo-way/2015/06/04/412086068/massive-data-breach-puts-4-million-federal-employees-records-at-risk (Accessed 2018/2/24)

在過去十年中，中共不斷增強經濟及軍事實力，亦投入相當多的心力及資源，應對其所觀察到美國的國家戰略及軍事轉型的內涵。美國蘭德公司曾於2006年發表「中共對美國軍事轉型的反應及對美國國防部的隱示」（Chinese Responses to US Military Transformation and Implications for the Department of Defense）中推論出，中共因應美國軍事轉型最可能的選項之一，即是進行網路作戰。[171]

依據蘭德公司的長久觀察，中共對美國軍事轉型的因應作為必須均衡於四個基本的國家安全目標： (一)政治上，確保中共的內部穩定與國家統一，掌握穩定的政權；(二)經濟上，持續高度經濟成長，保障人民的就業，提升收入水平，促進國際貿易以及投資，加速科技現代化；(三)兩岸間，期望達成最終統一；(四)國際上，增加中國影響力。這不僅包括中共軍力的擴張，還包含經濟、外交、政治與「軟實力」的增強。此四點是中共各時期領導者所努力的國家安全目標。[172]而此報告距今已十餘年，依然能夠用來解釋中共目前在軍事現代化所實踐的方向。

2015 年 5 月，中共發表首部軍事戰略白皮書，強調貫徹積極防禦戰略，內容提到武器裝備將持續朝著遠程精確化、智能化、隱形化、無人化趨勢發展，而太空和網路空間也是重點發展之領域，戰爭形態加速向資訊化戰爭演變，故建設資訊化軍隊，以打贏資訊化戰爭有其脈絡，而中共認為運用資訊系統，將各種作戰力量、作戰單元及要素整合成爲聯合作戰能力，方能克服在作戰中可能遇見的矛盾與問題，除了資訊科技的開發與利用外，更要加强建設偵察預警系統和指揮控制系統，發展中、長程精準打擊武器，藉以建立有效的聯合作戰機制。[173]

第四節　小結

美國第三次抵銷戰略中，在人工智慧、大數據與雲端運算等三大領域實施大

---

[171] James C. Mulvenon, et al., *Chinese Responses to US Military Transformation and Implications for the Department of Defense*(Santa Monica, CA.: RAND Corporation Press, 2006),pp.5-10.
[172] Ibid.,p.6.
[173] 中華人民共和國國防部,〈中國的軍事戰略〉,2016 年 5 月。參見 http://www.mod.gov.cn/affair/2015-05/26/content_4588132.htm (瀏覽日期：2018 年 3 月 6 日)

規模的投資與發展，輔以網路空間進行聯合作戰，而網路資訊作戰具備低成本、行動快速、不易防護、難以估算以及可否認的的特性，因此網路資訊作戰最能有效發揮不對稱作戰的思維。

網路安全威脅是美國國家安全、公共安全和經濟安全所面臨的最嚴重的挑戰之一，在網路資訊普及的現在，各國都能夠適用，因為網路空間是現代生活的一個重要特徵，全世界的個人與團體都利用網路空間並透過網路空間進行互動、社交以及工作，全球網路用戶數已經突破了四十億，全球有一半的人口都在使用網路[174]，隨著網路應用的範圍持續擴大，網路與日常生活更加的密不可分。

網路現已成為促進世界經濟、技術進步、言論自由或是社群媒體的代表，而各國的關鍵基礎設施，包括能源、銀行、金融、交通、通信、國防工業基礎的有效運作，都仰賴於易遭破壞及盜用的網路、控制系統和資訊技術，對軍隊來說，必須依賴一個能夠保護基本自由、隱私和資訊自由流動的安全可靠的網路空間，部隊的指揮控制、情報與後勤以及研發和部屬的武器裝備，都依賴國防部的資訊網路，一旦遭到滲透或是破壞，後果不堪設想。

網路的設計原本就是用於相互協同工作、快速擴展和提供技術創新，而網路使用者的匿名性和隱蔽性，也給了一些非國家行為體或是對手盜用、滲透和攻擊的機會。惡意的網路行為進入的門檻很低，這也意味著個人或小團體就能夠給國家安全或經濟安全造成顯著的影響，2016年，北韓企圖從紐約聯邦準備銀行（Federal Reserve Bank of New York）竊取十億美元，卻因一個拼字錯誤而破功。儘管如此，他們仍設法竊走大約八千一百萬美元。2013年3月20日，三間南韓電視臺和一間銀行的電腦終端機，疑似因為北韓對南韓網路發起攻擊行動，使用惡意軟體清除數據，南韓網路因此遭到癱瘓。北韓之後陸續對英國的電視公司、索尼影業進行釣魚郵件攻擊及恐嚇，對菲律賓及越南的銀行進行網路攻擊搶劫，對

[174] Simon Kemp, " Digital in 2018: World's Internet Users Pass the 4 Billion Mark," *We Are Social*, Jan. 30, 2018,At https://wearesocial.com/uk/blog/2018/01/global-digital-report-2018 (Accessed 2018/2/28)

於孤立又貧窮的北韓來說，網路攻擊是相當有利的工具，僅需耗費低成本，便能對一個國家的基礎設施或是私人公司造成極大損害，北韓可能每年從網路搶劫中獲利最多達十億美元，這相當於北韓年均出口總值的三分之一。[175]

現代資訊科技以網路為平台的攻防無時不在，簡言之，國家安全已經被網路空間重新定義。然而，資訊攻防的最大效果乃在於整合應用資訊及網路科技後的整體軍事力量提昇。資訊能力已成為霸權相互較勁的戰場，特別是應用於軍事力量上，更突顯現今軍事霸權的主要特徵：全面、彈性而迅速的整合及反應軍事力量，以嚇阻、制壓敵人並主導戰場。美軍的網路戰並非僅是駭客攻防，這是在1980年代的早期資訊戰發展時期，就已經確認的差異及重點，實值得我軍事資訊部門參考。[176]

國防大學
National Defense University

[175] David E. Sanger, David D. Kirkpatrick and Nicole Perlroth, " The World Once Laughed at North Korean Cyberpower. No More." *The New York Times*, Oct. 15, 2017,At https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html?_ga=2.90413021.699713574.1520478934-1514276013.1506038331 (Accessed 2018/02/28)

[176] 李承禹，〈中共網路作戰之戰略邏輯分析：網路戰與網路中心戰的區隔與應用〉，《復興崗學報》，90 期，2007 年，頁 254。

第四章　美軍第三次抵銷戰略對兩岸軍事對峙之影響

在權力平衡的基礎上，國家的外交政策以追求平衡為目標，亦即不平衡的權力關係會對國家招致危險。所以當權力平衡發生變化，而這項變化對敵國有利時，該國必然要執行新的政策，以恢復平衡。因此，國家在政策上的制訂將是以國家本身的利益為考量。而為了解美國與中共戰略互動對臺灣的安全影響，必須先探究美國的對華政策，而欲了解美國的對華政策，亦必須先探究美國在兩岸的國家利益所在。[177]在最高階層，國家利益構成合理戰略的支柱。雖然利益是一種高度概括性的抽象概念，然而唯一「主要」的國家安全利益即為生存；至於次要的利益，無論其為積極或是消極，區域或全球，就是只作為此種最基本動力的補充。[178]

中共在經濟以及軍事現代化的快速發展之下，美國的霸權地位岌岌可危，而為了在大國競爭的環境中繼續維持領先的優勢，美軍在 2014 年提出了第三次抵銷戰略，以創新科技為核心，運用不對稱作戰的手段抵銷敵方的優勢如先進軍事技術和武器的快速發展，藉以增加對手的發展成本。

美中勢力的消長，與兩岸關係有著密切關係，中共近年憑藉其經濟實力與軍事力量，在國際上不斷恫嚇及打壓我國。中共 2018 年國防預算為人民幣 1 兆 1,070 億元（約新臺幣 5 兆 1839 億元）。[179]與去年相比，增加 8.1%，與我國 107 年度國防預算 3,318 億元[180]相比，差距約 16 倍。面對兩岸軍力失衡以及懸殊的軍事差距，我國當以「不對稱作戰」應處，而最能展現我國國防軍事力量或不對稱作戰戰力當屬資訊作戰，我國資訊產業人才濟濟，藉發展通資電軍（第四軍）

國防大學 National Defense University

177 陳建民，《兩岸關係中的美國因素》(臺北:秀威資訊科技股份有限公司，2007 年 6 月)，頁 25-27。

178 John M. Collins 著，鈕先鍾譯，《大戰略》(臺北:黎明文化事業公司，1997 年 10 月 5 版)，頁 17-19。

179 張藝藐、呂欣彤，〈一圖解讀 2018 年我國國防預算開支〉，《中華人民共和國國防部》，2018 年 3 月 6 日。參見 http://www.mod.gov.cn/shouye/2018-03/06/content_4806088.htm (瀏覽日期：2018 年 3 月 12 日)

180 行政院主計總處，〈107 年度中央政府總預算案暨附屬單位預算及綜計表與流域綜合治理計畫第 3 期特別預算案〉，《中華民國行政院》，2017 年 8 月 17 日。參見 https://www.ey.gov.tw/DL.ashx?s=2D1F225C97272116D9F3992D3E03C191299FC6CB75ABF932EAB5B57EA8D46E4D&u=%2fUpload%2fRelFile%2f19%2f753361%2fadc8189c-4a01-4351-b746-1bb1cff63c92.pdf (瀏覽日期：2018 年 3 月 12 日)

維護我國家網路資訊安全，於網路戰場中與中共角力，期能避開敵人強點，集中我方相對優勢來對付敵人相對劣勢，以創新的軍事技術或是戰術戰法以小博大，方能與軍力佔優勢的一方相抗衡。[181]

第一節　美中競合下的兩岸關係

自美臺斷交，中美建交以來，美中臺三邊一直建立著微妙的三角運作架構，數十年來兩岸的互動關係，美國均扮演要角，而美中兩國在「一個中國」的共識之下，維持模糊而有彈性的解釋空間。美國學者雷什特（Martin L. Lasater）認為，當美國與中共雙方關係交惡時，美國較會支持臺灣，而當美國與中共較具合作關係時，美國對臺態度就較為謹慎，[182]顯然美中關係交惡時對臺較為有利；但即使美中關係趨於友好，美國對臺灣的態度會趨於保守，但也不至於犧牲臺灣太多的利益。

美國智庫蘭德公司 2015 年的「美中軍力對比」(The U.S.-China Military Scorecard)報告中以四個重要的關鍵年份劃分，分別為 1996 年、2003 年、2010 年和 2017 年，從整體能力來看，中共目前戰力雖不及美國，但是在兩岸關係與南海主權爭議的議題上，已經能與之抗衡，分類項目上，中國在威脅臺灣的空軍基地和反制水面船艦較有優勢；制空能力與太空攻防上，兩者伯仲之間；因此美軍只剩下反制兩棲作戰、網路作戰和攻擊中共空軍基地有其優勢，另外，中共的短程彈道飛彈數量已經增長到 1400 枚，已足以癱瘓我空軍基地 ；不過美軍的水下作戰能力，仍可以在短期摧毀至少百分之四十的解放軍兩棲登陸戰力，避免其登陸。至 2017 年，純就東亞軍事力量推演，美軍將難以在七天短期戰役中取得優勢，也意味著即使美軍立刻決定介入我國也必須獨自作戰七天以上。[183]

在中共逐漸成為亞洲的區域霸權之時，美中的權力平衡關係亦引起許多學者討論，權力平衡是維持國際安定的條件，而政策的制定者則可能以追求權力平衡為一項政策，國家所從事的外交、結盟甚至是戰爭即成為落實此項政策的手段。

---

[181] 謝游麟、葛惠敏，〈論戰爭型態之發展與因應〉，《國防雜誌》，第 30 卷第 1 期，2015 年 1 月，頁 88。

[182] Martin L. Lasater, *The Changing of the Guard: President Clinton and the Security of Taiwan,*(New York:Routledge,1995),p.166.

[183] Eric Heginbotham,ed., " The U.S.-China Military Scorecard-Forces, Geography, and the Evolving Balance of Power, 1996–2017," At https://www.rand.org/pubs/research_reports/RR392.html (Accessed 2018/3/12)

[184]以下將以美國的角度探討美臺關係的變化，並試圖從中找出我國未來因應的作法與出路。

（一）離岸平衡戰略

冷戰後美國成為世界霸權，2001 年的 911 恐怖攻擊事件，以及之後兩場對阿富汗與伊拉克的戰爭都使美國陷入泥淖，美國國內面臨預算和財政壓力，在國際上亦無人可與之匹敵，美國霸權的地位顯得沒有必要，反而連帶產生了若干反效果。學者們也開始質疑，是否需要改為採取較為緊縮的戰略，以較低的成本來獲得較高的安全。[185]

在冷戰後美國大戰略的理論爭辯中，克里斯多福·雷恩（Christopher Layne）提出了「離岸平衡」策略（Offshore Balancing），建議美國放棄冷戰期間的戰略優勢，接受其他地區大國的崛起，以避免與其他崛起中大國有正面衝突的機會。[186]

米爾斯海默借鑒了雷恩所提出的離岸平衡的思想，並根據攻勢現實主義理論而有所創新，提出了「離岸平衡手」（The Offshore Balancers）。具體來說，作為歐亞大陸的海外大國（英國或美國），在歐洲或東北亞遭遇到一個潛在的霸主時，他們傾向於將責任推給其他的大國，而非親自對抗這些威脅。但是不僅僅是離岸平衡手，大多數國家都一樣會選擇推卸責任而不是抗衡策略。[187]攻勢現實主義主張國家對於權力平衡相當敏感，會尋找機會來增加自身實力，或削弱對方實力。在現實狀況下，這代表著國家將會針對當下的權力分配所創造出來的機會與限制，來擬訂相應的外交策略，而受威脅的大國思考究竟是要推卸責任還是組織抗衡聯盟時，地緣政治的考量與權力分配則是他們做決策的關鍵因素。[188]

有學者總結認為，由於美國仍然關切海外的權力分配結構，所以離岸平衡戰略並非孤立主義戰略，而是一種最低限度(minimalist)戰略，希望能以較少的義務和資源來維持美國的利益。[189]

國防大學 National Defense University

---

[184] 同註 177，頁 12-13。
[185] Hal Brands, “Fools Rush Out? The Flawed Logic of Offshore Balancing,”*The Washington Quarterly*, Vol. 38, No. 2,2015, pp. 7-9.
[186] Christopher Layne,” Offshore balancing revisited,”*The Washington Quarterly,* Volume 25, 2002.At http://www.comw.org/qdr/fulltext/02wqlayne.pdf (Accessed 2018/3/13)
[187] John J. Mearsheimer, *The Tragedy of Great Power Politics*(New York:Norton,2001),p.266.
[188] Ibid.,p.333.
[189] Hal Brands, “Fools Rush Out? The Flawed Logic of Offshore Balancing,”*The Washington Quarterly*, Vol. 38, No. 2,2015, p.10.

因此對於像美國這樣的海外大國而言，若要採取離岸平衡戰略，便不應隨意介入歐亞大陸國家的紛爭，最好讓這些歐亞陸權國家相互競爭，削弱彼此的實力。只有在歐亞大陸出現大國崛起足以成為地區霸權，或甚至試圖對外投射軍事力量時，海外大國／離岸平衡者才需要以個別或聯合盟國的方式，予以制衡打擊，這樣才能維護本國的利益與霸權地位。如此一來，便會出現希望美國拋棄歐亞大陸周邊盟國的政策建議，「棄臺論」自然也是其中一種。[190]

（二）美國「棄臺論」之爭辯

學者們對於美國棄臺論的爭議，一方面來自於離岸平衡戰略的理論推導，海外大國要減少對於歐亞大陸國家的安全承諾及干涉，但棄臺論本身卻未必一定來自於離岸平衡戰略的支持者，另一方面也來自於對美國與中國未來互動關係的不同期待與預判。

棄臺論是美國學界及政治圈的一種理論，認為美國應該放棄對臺灣的軍事承諾，以換取美國在國際的利益或是迴避難以處理的難題，因而讓美國利益最大化的理論。格里澤（Charles Glaser）發表的一篇名為《中國崛起可能導向戰爭嗎？》（Will China's Rise Lead to War?）提到美國應與中共建立「建設性夥伴關係。美國應扮演「平衡者」（balancer）角色，協助亞洲國家解決紛爭，不可再以冷戰時期觀點，以為可以再在亞洲稱霸」。這種設計可以使美、中兩國從現實環境中取得利益及互利，而避免衝突。也因為如此「臺灣不再具有重要性」，所以棄臺就成為美國唯一選項。[191]

2011 年 11 月 10 日哈佛大學研究員保羅·肯恩（Paul V. Kane）認為依照當時的發展趨勢，中共實現兩岸統一包含使用最下策的以武力犯臺，而世界上已經沒有國家可以阻止，包含美國，所以美國應在仍有籌碼談判時放棄臺灣，藉以交換多方面的利益，以免有朝一日事情演變到美國得接受同樣的結局且一無所得。[192]

---

[190] 陳麒安，〈美國學界離岸制衡戰略與「棄臺論」的爭辯〉，《遠景基金會季刊》，第 17 卷 3 期，2016 年 7 月，頁 68。

[191] Charles Glaser, " Will China's Rise Lead to War?"*Foreign Affairs*, March/April 2011.At https://iscs.elliott.gwu.edu/sites/iscs.elliott.gwu.edu/files/downloads/Glaser--China-FA-March-April-2011%20%283%29.pdf (Accessed 2018/3/13)

[192] Paul V. Kane, " To Save Our Economy, Ditch Taiwan,"*The New York Times*, Nov. 10, 2011.At http://www.nytimes.com/2011/11/11/opinion/to-save-our-economy-ditch-taiwan.html?_r=0 (Accessed 2018/3/13)

卡托學會（Cato Institute）資深研究員特德·蓋倫·卡彭特（Ted Galen Carpenter）提出他的論點，臺灣在經過政黨輪替與雄三飛彈誤射事件後，中共與臺灣關係更加惡化，這顆「定時炸彈」隨時都有可能引爆，但美國並非旁觀者的角色，根據 1979 年的《臺灣關係法》，美國有義務保護臺灣，雖然並未明確界定，現在穩定期已經結束，美國必須重新思考對於臺灣的安全承諾，僅僅是一場嚴重的意外，又或者是「臺獨」者的行動，都可能引發危機，對美國帶來災難性的結果。[193]

米爾斯海默（John J. Mearsheimer）在 2014 年所發表的「跟臺灣說再見」(Say Goodbye to Taiwan) 指出，目前中共的力量雖落後美國很多，受制於全球的權力平衡，無力與美國開戰。但國際現勢是變動的，情勢將迅速對臺灣及美國不利。數十年後，中國實力將與美國相仿，在未來將受到比現在更少的限制，也許世界各國不願意見到這種現象，但恐怕難以避免。米爾斯海默認為中國看待兩岸議題存在兩個因素，一是民族主義，二是國家安全思維，而這二者的結果都導向兩岸統一。儘管難以預測中國的能力會擴大大何種程度，但中國至少有可能會強大到一次的突襲就讓臺灣難以招架，而且，隨著中國逐漸晉身超級大國，美國保護臺灣的承諾也可能日趨減弱。米爾斯海默在結論提到，臺灣應盡一切努力爭取時間，爭取對自己最有利的條件，以維持現狀。「但如果中國持續出色的成長，臺灣顯然註定成為中國的一部分」。[194]

另一方面，則有其他學者以臺灣戰略位置為切入點反駁了棄臺論的觀點。卡普蘭(Robert D. Kaplan)認為，由於臺灣戰略地位非常重要，若中國統一了臺灣，便有機會突破第一島鏈。一旦美國放棄臺灣，不但會失去地緣上的優勢，更會影響亞太盟國的信心，懷疑美國的安全承諾是否可靠，因而可能轉為扈從中國，使得中國大為擴張在亞洲的勢力範圍。[195]施密特(Gary Schmitt)則以美國在亞太地區

---

[193] Ted Galen Carpenter, " America Should Step Back from the Taiwan Time Bomb," *The National Interest,* July 6,2016.At http://nationalinterest.org/blog/the-skeptics/america-should-step-back-the-taiwan-time-bomb-16864 (Accessed 2018/3/13)

[194] John J. Mearsheimer, " Say Goodbye to Taiwan," *The National Interest,* March/April 2014.At http://nationalinterest.org/article/say-goodbye-taiwan-9931 (Accessed 2018/3/13)

[195] Robert D. Kaplan, "Geography of Chinese Power: How Far Can Beijing Reach on Land and at Sea," *Foreign Affairs,*2010.At http://archives.cerium.ca/IMG/pdf/Kaplan_How_far_can_Beijing_reach_on_land_and_at_sea.pdf (Accessed 2018/3/13)

盟國的立場切入，認為中國並不會滿足於美國在臺灣問題上的退讓。而由於臺灣所具有的地緣戰略重要性，若美國一旦放棄，亞太地區的盟國，如日本和南韓將會懷疑美國的防衛決心與能力。[196]施密特表示臺灣能夠和平政黨輪替，已是正常的民主國家，且臺灣是美國第九大貿易夥伴，加上位處東亞「第一島鏈」的重要戰略位置，可削弱中國海空軍進入太平洋威脅美國的能力，因此呼籲美國與臺灣建交，在軍事、經濟與外交上強化與臺灣的關係絕對符合美國利益。[197]羅伊（Denny Roy）指出臺灣與中共之間的危機將使美國陷入兩難之中。守護臺灣的成本確實提升了，但若美國放棄臺灣，未來付出的成本會更大，並危及到美國的亞太地區政策，導致「美國和平」（Pax Americana）的終結。[198]陳麒安則認為學者們所提出棄臺論的政策建議，固然一部分來自於離岸平衡戰略的理論推導，另一部分也含括了對於美國與中國未來互動關係的悲觀預判。正是這兩項因素的交互影響，引發了美國學界對於是否要拋棄臺灣的不同面向討論，更有人士針對美國與中國之間未來可能發生衝突而提出呼籲，希望美國能降低對於臺灣的安全承諾，以免因兩岸關係的惡化而被迫捲入衝突。[199]

前美國在臺協會理事主席卜睿哲（Richard Bush）認為，美國改變對臺承諾在下面兩種情況下可能會發生。首先是美國的整體戰略出現變化。美中關係穩定才符合美國利益，美國必須降低雙方歧異到可以掌握的程度。這種思維可能導致美國降低或結束對臺安全承諾，這也出現在所謂的棄臺論中，減少或取消對臺軍售是當中的一部分，不過美國對臺軍售，並非中共無法達成統一的原因。再者，美中軍力消長，東亞戰爭形勢變化，也會對美國對臺承諾有所影響。中共希望建構有效阻攔與打擊美軍兵力投射，包括美國援助臺灣在內的盟邦夥伴戰力，也就是美方所指的「反介入與區域拒止」（A2／AD），中共解放軍發展反艦彈道飛彈

國防大學 National Defense University

196 Gary Schmitt, "When Will the Realists Get Real?" *The Weekly Standard*, March 2, 2011, At http://www.weeklystandard.com/when-will-the-realists-getreal/article/552769 (Accessed 2018/3/13)

197 Gary Schmitt, "It's time to ditch the one China fiction and normalize relations with Taiwan" *The Washington Post*, May 18, 2016, At https://www.washingtonpost.com/opinions/its-time-to-ditch-the-one-china-fiction-and-normalize-relations-with-taiwan/2016/05/18/e0f9d3a6-1b7a-11e6-8c7b-6931e66333e7_story.html?utm_term=.42fbd982d8a1 (Accessed 2018/3/13)

198 Denny Roy, " Collision Course: The Looming U.S.-China Showdown Over Taiwan," *The National Interest*, Feb. 21, 2015.At http://nationalinterest.org/feature/collision-course-the-looming-us-china-showdown-over-taiwan-12293 (Accessed 2018/3/13)

199 陳麒安，〈美國學界離岸制衡戰略與棄臺論的爭辯〉，《遠景基金會季刊》，第 17 卷第 3 期，2016 年 7 月，頁 59。

將影響美國的航空母艦打擊群，美軍則以「空海整體戰」回應。在此戰爭概念下，美軍必須實現對中內陸的精準攻擊，而非沿海港口與基地，這種局勢會升高危險性，美國將因此降低對西太平洋盟友的承諾。[200]

美國是否會與中國開戰呢？美國蘭德智庫在 2016 年列出五個美國可能對中國開戰的事由，其中一個便是中共以武力統一臺灣，但是兩國開戰將付出的代價透過報告中的分析，都將會對美中兩國造成極大損傷，從軍事、經濟、政治、國際角度權衡後，報告最後指出中美之間的戰爭會對雙方帶來非常大的傷害，所以應當優先選擇極力避免發生戰爭，因此在衝突前的「嚇阻」格外重要，中國軍事實力的發展抵銷了美國的軍事優勢，而且因為科技發展更有利於傳統的反擊能力，將帶給雙方巨大的損失。[201]

從以上學者的探討可知，中共快速的軍事現代化對美國造成極大壓力，雖然目前中共仍望其項背，但數十年後中共影響若加大，限制也將減少，若美國對中共能夠保持軍力的相對優勢，便能夠減少美國棄臺聲浪，美國目前致力於軍事科技創新，以抵銷對手軍力優勢，加大雙方差距。而除了美、中兩國的外部因素外，我國更應思考因應的國防與軍事戰略，強化我不對稱作戰能量，尤其我國資訊產業能力強大，更可利用此優勢發展我國之「抵銷戰略」，在其他戰場達到「嚇阻」之效。

第二節　我國資訊產業發展現況

我國資訊科技(Information Technology，IT)產業發展至今將近四十年歷史，從 1970 年間政府主導半導體技術引進，以及早期推動個人電腦組裝和周邊零組件標準化，之後衍生出完整電子產業生態鏈，在產業高度群聚效應推動下，已在全球電子產業站穩關鍵性地位，並累積堅強代工生產研發與製造實力。[202]2008 年英國經濟學人智庫（Economist Intelligence Unit，EIU）針對全球資訊科技產業競爭力

---

[200] Richard C. Bush, " Taiwan's Security Policy," *The Brookings Institution,* Aug. 3, 2016.At https://www.brookings.edu/wp- content/uploads/2016/08/ceap_20160804_taiwan_security_policy.pdf (Accessed 2018/3/13)

[201] David C. Gompert et al., " War with China Thinking Through the Unthinkable,"At https://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1140/RAND_RR1140.pdf (Accessed 2018/3/15)

[202] 〈臺灣電子產業回顧與展望〉,《工業技術研究院》, 2014 年 12 月 22 日。參見 https://www.itri.org.tw/chi/Content/NewsLetter/Contents.aspx?SiteID=1&MmmID=5000&MSid=621302513530161363 (瀏覽日期:2018 年 3 月 12 日)

所進行的研究發現，我國資訊科技產業競爭力排名為全球第二，[203]隨著韓國企業以及中國科技業迅速的發展，再加上我國面臨因以代工為主，研發創新能力不足，導致產業競爭力的流失。2016 年蔡英文總統提出「打造一個以創新、就業、分配為核心價值，追求永續發展的新經濟模式」之政策方向，並推動五大創新研發計畫，希望我國達到科技產業具備創新、研發之能量，並成為全球網路、大數據、物聯網之產業群落，[204]並由資訊科技產業轉型為物聯網(Internet of Things，IoT)產業。所謂物聯網所指的是網際網路、傳統電信網等資訊承載體，讓所有能行使獨立功能的普通物體實現互聯互通的網路。[205]資訊科技產業經多年的普及化發展，通訊傳輸愈來愈快速，而數位化亦累積廣大的資訊，利用所搜集的資訊和技術配合成為科技創新之新趨勢。科技發展已成從追求單點最適化，朝「系統性思考」和「技術融合」之整體最適化方向發展。物聯網強調所有物品的聯網，而且這些物品/設備需具備感測、邏輯與運算能力，以便透過資通訊技術（ICT）技術之蒐集數據、監控、分析，再回饋機器或物品，促成設備/物品的深度學習。[206]根據瑞穗銀行的報告，物聯網之所以能實現，主要來自三大技術創新，即感測器技術、網路技術與運算處理技術之創新。[207]

在網路創新方面，我國資訊科技自 1990 年代以來迅速發展，通訊科技的創新促使網路的傳輸更加快速且成本大幅下降，而隨著網路的升級，傳輸速度的加快之外，通訊覆蓋的範圍也不斷擴張及增加，因此有助於相關應用軟硬體的開發，更利於網路的發展。物聯網藉著物品及設備聯網，可收集到大量即時性的資料，當數據累積夠龐大足以進行分析後，便可得到新的資料，企業透過大數據分析出的資訊了解客戶的需求，進而創造出新的價值。

依據我國國家發展委員會「106 年數位機會調查」顯示，我國一般民眾上網

國防大學 National Defense University

---

[203] "How technology sectors grow Benchmarking IT industry competitiveness 2008," Business Software Alliance,2008.At http://global.bsa.org/2008eiu/study/2008-eiu-study.pdf (瀏覽日期:2018 年 3 月 12 日)

[204] 蔡英文，〈就職演說〉，《中華民國總統府》，2016 年 5 月 20 日。參見 https://www.president.gov.tw/Page/251 (瀏覽日期：2018 年 2 月 28 日)

[205] 劉雲浩，《物聯網導論》（北京：科學出版社，2010 年 12 月 1 日），頁 4。

[206] 王文娟，〈物聯網概念及應用〉，《經濟前瞻》，第 168 期，2016 年 11 月 12 日，頁 29-30。

[207] 王文娟，〈物聯網概念及應用〉，《經濟前瞻》，第 168 期，2016 年 11 月 12 日，頁 32。

率為百分之 82.3，手機族行動上網率為百分之 87.4，[208]臺灣網路普及率高，顯示我國在資訊網路軟硬體設備等均已成熟，我國所推動的大數據分析、人工智慧技術以及雲端計算等政策，在網路設備穩定的基礎之下方能有效研發與執行。我國科技部所提出的「我國 AI 的科研戰略」，預計五年內投入 160 億元經費，並於今年投資於我國國內四所頂尖大學，期望開發適用於不同產業之人工智慧工具與平臺；國家發展委員會所推動的「亞洲•矽谷」計畫亦將人工智慧納入未來將推動的關鍵議題之一，促進人工智慧技術結合雲端平臺、大數據分析等技術發展，例如自動駕駛、交通、環境等相關創新應用，以強化產業科技技術發展能量。[209]

Google 於今年（2018）3 月宣布，將在臺灣招聘以及培訓人工智慧機器人領域的學生；微軟也宣布，選中臺灣做為人工智慧事業發展基地，並將投資約 3,400 萬美元在臺灣成立研發中心；臺灣 IBM 總經理高璐華在 3 月宣布，將擴張在臺灣的研發中心，重點也為人工智慧、區塊鍊和雲端運算，預期今年內增聘百人，目前也正在臺灣設立雲端研究實驗室。臺灣具備人才、政策等優勢，且雖然中國勞工成本較低，但美國企業對美中貿易戰、智慧財產權遭侵犯和資料中心安全問題仍存有疑慮，在加上臺灣較穩定的電力和基礎設施，都是吸引美國高科技公司來臺擴大投資的重要因素。[210]

我國擁有豐富、穩定且充沛的網路資源，在美軍第三次抵銷戰略當中，網路資訊作戰是美軍實現不對稱作戰能力的基礎與核心，憑藉我國的網路資訊技術，美軍與臺灣在網路空間可進行密切合作，無論是在網路資訊安全方面，甚至是我國 2017 年成立的通資電軍技術的協助與軍事戰略的交流。美臺兩國所簽屬之《臺灣關係法》使美國無法對臺進行攻擊性軍事武器之軍售，但美國仍可在網路

國防大學 National Defense University

[208] 國家發展委員會，〈國人上網率再創新高 八成七手機族行動上網〉，2017 年 12 月 29 日。參見 https://www.ndc.gov.tw/News_Content.aspx?n=114AAE178CD95D4C&sms=DF717169EA26F1A3&s=9FC6B0AC9D855239（瀏覽日期：2018 年 2 月 28 日）

[209] 國家發展委員會，〈亞洲·矽谷推動方案行動計畫〉，2017 年 4 月。參見 https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvMC85OTUwLzFjM2UwNThjLTQ2NjgtNDYzMC1iYzYzLTkxMGRmZGVhZTc3ZS5wZGY%3d&n=MTA2MDMxNuS6nua0ssK355%2b96LC35o6o5YuV5pa55qGI6KGM5YuV6KiI55WrZmluYWwo5qC45a6aKS5wZGY%3d&icon=..pdf (瀏覽日期:2018 年 4 月 10 日)

[210] 林奕榮，〈為何 Google、IBM、微軟都相中臺灣？有三個原因〉，《聯合新聞網》，2018 年 4 月 6 日。參見 https://udn.com/news/story/7240/3072239?from=udn-ch1_breaknews-1-0-news (瀏覽日期:2018 年 4 月 10 日)

資訊的軟、硬體上給予我國協助，進而在美軍所規劃之第一島鏈之上扮演適當角色。

第三節　我國因應之國防與軍事戰略

中共2018年國防預算為人民幣1兆1,070億元（約新臺幣5兆1839億元），[211]與去年相比，增加8.1%，與我國107年度國防預算3,318 億元相比，[212]差距約16倍。我國在國防安全上最大的威脅來自中共，但兩岸軍事力量的天秤卻正向中共逐漸傾斜，中共依「積極防禦」軍事戰略，將原規劃「2000 至 2010 年」、「2010 至 2020 年」、「2020至2050年」之軍事「三步走」發展戰略，調整為「2020年基本實現機械化、信息化建設」，「2035年基本實現國防和軍隊現代化」，「至本世紀中葉把人民軍隊全面建成世界一流軍隊」。[213]臺海地區則成為中共能夠削弱美國國家威望和盟軍對其信心的場合。面對失衡的軍力，我國無法再以傳統武器與兵力的數量進行軍備競賽，取而代之的是發展屬於我國的不對稱戰力，創造我國軍的相對優勢。

我國《106年國防報告書》強調：「國軍積極發展『創新與不對稱』戰力，戰時運用有利時間與空間，打擊敵軍作戰重心及關鍵弱點要害，藉以阻滯破壞或癱瘓敵作戰節奏與能力，以創造局部優勢，期能「以小搏大、以弱擊強」。國軍依「防衛固守，重層嚇阻」之軍事戰略，思考與強化「創新/ 不對稱」戰力，將以共軍預期外的裝備與戰術戰法，使對方難以預測或防範，武器系統發展將以「機動、隱匿、快速、價廉、量多、損小、效高」為方向，作為未來軍事投資重點，

國防大學 National Defense University

---

211 張藝菟、呂欣彤，〈一圖解讀 2018 年我國國防預算開支〉，2018 年 3 月 6 日。參見 http://www.mod.gov.cn/shouye/2018-03/06/content_4806088.htm (瀏覽日期:2018 年 3 月 12 日)

212 行政院主計總處，〈107 年度中央政府總預算案暨附屬單位預算及綜計表與流域綜合治理計畫第 3 期特別預算案〉，2017 年 8 月 17 日。參見 https://www.ey.gov.tw/DL.ashx?s=2D1F225C97272116D9F3992D3E03C191299FC6CB75ABF932EAB5B57EA8D46E4D&u=%2fUpload%2fRelFile%2f19%2f753361%2fadc8189c-4a01-4351-b746-1bb1cff63c92.pdf (瀏覽日期:2018 年 3 月 12 日)

213 國防部「國防報告書」編纂委員會編，《中華民國 106 年國防報告書》(臺北:國防部，2017 年 11 月)，頁 32。

檢討各項軍備獲得優序，打造重層防衛及嚇阻戰力，遏止中共武力犯臺。」[214]

而網路資訊作戰便有「機動、隱匿、快速、價廉、量多、損小、效高」之優點。我國為資訊科技產業大國，在國防產業上若能與民間技術人才交流配合，創造我國在網路資訊作戰之相對優勢，甚至是效法美國，發展屬於我國的「抵銷戰略」，透過創新的思維，與「能夠改變戰場」的優勢技術，必能將網路資訊作戰之效益發揮到最大。

「不對稱作戰」（Asymmetric operation）是一種思想，也是一種作戰方式，一種作戰概念，StevenMetz 將不對稱作戰範疇區分「低度」與「高度」不對稱作戰：「低度不對稱作戰」指面對優勢對手時，避免與之正面交鋒，而是仰賴各種「打了就跑」戰術、欺敵行為、疏散、偽裝，於各種複雜地形採取游擊戰或恐怖活動等；「高度不對稱作戰」則指面對劣勢敵軍或是必須盡量減少傷亡時，運用優勢科技、資訊、訓練、領導統御或計畫協調能力加以因應。[215]我國 106 年國防報告書則將「不對稱作戰」定義為「以不對稱手段、不對等力量與非傳統方式進行作戰，迴避敵人強點，並以適當的戰法、戰具攻擊敵人的弱點，從而改變戰爭的結果，使戰爭朝向有利己方的方向發展。」[216]

隨著戰略環境的改變、科技的進步以及軍事事務革命的深入，戰爭型態已朝多元化、全方位、不規則等面向發展，但在戰爭中贏得勝利的本質，始終是敵對雙方共同的目標。[217]為達成此目的，戰爭中的各種作戰方式、工具及手段不斷推陳出新，特別是從上個世紀末 90 年代起的波灣戰爭、科索沃戰爭，到本世紀初所發生的阿富汗戰爭及伊拉克戰爭中，就共同出現一種作戰方式：「不對稱作戰」，這種作戰方式產生驚人的決定性效果。因此，如何以「不對稱」思維融入戰爭準備或戰爭遂行中，似乎已成為中外戰爭理論和作戰思想共同的研究焦點與發展趨勢。[218]

國防大學 National Defense University

---

[214] 國防部「國防報告書」編纂委員會編，《中華民國 106 年國防報告書》(臺北:國防部，2017 年 11 月)，頁 74。

[215] StevenMetz 著，謝凱帝譯，《廿一世紀的武裝衝突：資訊革命與後現代戰爭》（臺北：國防部史政編譯室譯印，2000 年 9 月），頁 48-49。

[216] 國防部「國防報告書」編纂委員會編，《中華民國 106 年國防報告書》(臺北:國防部，2017 年 11 月)，頁 74。

[217] 同註 181，頁 55。

[218] 同註 181，頁 80。

再者，兩岸軍力失衡，且受限於我國防經費之獲得有限，因此必須在有限的經費與資源下，思考我國發展不對稱軍事思想與作為，而我國雖已開始推動國艦國造、國機國造等政策，但目前仍仰賴向美採購武器，由於在裝備上質與量的限制，致使我國軍事戰略須配合軍售獲得之武器種類與數量，導致我國在戰略構想、戰術作為、人員編裝、後勤補給及軍事準則等，都必須做出適當的修正，無法真正達到軍事戰略目標。依據當前兩岸軍事實力的分析，國軍應調整戰略思維，採「創新與不對稱」用兵方式，以避免捲進傳統式的消耗戰，耗竭國家資源；在因應作戰理念的改變方面，過去對「勝戰」的認知是在戰場上全面戰勝敵人，但研析臺海現況，「勝戰」的定義應由以往的「全面打贏敵人」，調整為「擊敵於海峽半渡，不讓其登島立足」。[219]因此，國軍應將兵力結構之規劃，聚焦於爭取此一關鍵時空下的不對稱戰力優勢，此舉更可避免落入「軍備競賽」的泥淖，而危害國家的競爭力。[220]

為了爭取武器發展的相對優勢，須跳脫以往擁有大量傳統飛機、船艦、戰甲砲車等觀念，更不宜在敵高科技能量所形成的戰力優勢方面與之「軍備競賽」，應將國防資源與科技能力集中在關鍵戰力的發展能量上，擁有這些技術能夠讓戰爭在最短的時間及最少的損耗下，獲致勝利。鑑於現今電腦網路、資訊系統普及，資訊安全已成為國家安全之一環，因此發展資訊站其相關戰法與能力，並建置足以攻擊及癱瘓中共軍事與民間之力量，實屬必要。特別是我國面對中共導彈威脅尚無有效對策時，我國富潛力的資訊產業或可在中共採取導彈攻擊之際，對其進行資訊戰，爭取制電磁權優勢，另藉網路破壞、駭客入侵、植入病毒等滲透攻擊方式，入侵共軍相關網路，癱瘓指管機能，使其無法發揮。[221]

另外軍方應結合民間科技能量，研發關鍵技術，建構有效之資訊武器。[222]我國國防部參謀本部資通電軍指揮部於 2017 年 6 月成軍，首任指揮官由陸軍少將馬英漢擔任，我國總統蔡英文表示，資通電軍將以網路攻防為核心，通訊安全為

[219] 國防部「國防報告書」編纂委員會編，《中華民國 100 年國防報告書》(臺北：國防部，2011 年 7 月)，頁 66-68。
[220] 同註 181，頁 56。
[221] 同上註，頁 59-60。
[222] 同上註，頁 60。

基礎，電磁發展為前瞻。[223]2017 年 12 月，我國資通電軍與交通大學聯合成立國防資電科技中心，未來將在人才培育、網路聯防、滲透測試、機器學習、國際合作等項目進行交流合作，充實我國資訊人才。[224]

事實上無論是美軍或是共軍，軍民網路演習已行之有年，透過結合各民間企業、大學、州政府，來強化對於資訊交換與合作的管道，美軍甚至由國土安全部每兩年舉行一次的網路風暴演習，旨在強調政府與私人企業進行合作，藉以提升對於網路安全威脅的因應能力，有鑑於此，我國政府更應該積極將民間資源引入國軍發展不對稱作戰的資訊戰能力。[225]

第四節　小結

1950 到 1960 年代，美國將臺灣視為圍堵共產主義的基地，藉以確保美國的利益，因此對美國來說，臺灣的戰略價值相當重要。而到了 1970 年代，美國將中共視為圍堵蘇聯的戰略夥伴，而更勝於把中共視為是在臺灣海峽與美國對峙的敵人。因不同的國際情勢，美國優先考量自身利益，從而改變美、中、臺的三角關係。

隨著中共軍事現代化發展快速，美中關係逐漸改變，美國願意承認中共在亞太地區和全球發展中的重要地位，進而積極發展為戰略夥伴的關係，以合作化解衝突。美中兩國的關係非敵亦非友，美國並不信任中共，因從長遠局勢看來，中共在未來將有機會無論在政治、軍事、經濟挑戰美國的霸權地位；當然中共也清楚了解，現今與未來美國在全球政經體系中都扮演著超強的角色，以中共目前的實力，著實無法挑戰美國。一來一往之間，兩國微妙的關係也就使得處在美中兩國間的小國，無論什麼風吹草動，都會感到心驚膽顫。

兩岸關係自 1949 年國民政府播遷來臺後大致底定處於分裂的軍事對峙的狀

---

[223] 〈資通電軍成軍 蔡總統：捍衛數位國土〉,《自由時報》, 2017 年 6 月 30 日。參見 http://news.ltn.com.tw/news/politics/paper/1114892 (瀏覽日期：2018 年 3 月 20 日)

[224] 徐養齡,〈國防部攜交大 培育資通電軍〉,《中時電子報》, 2017 年 12 月 16 日。參見 http://www.chinatimes.com/newspapers/20171216000506-260107 (瀏覽日期：2018 年 3 月 20 日)

[225] U.S. Department of Homeland Security, “Cyber Storm: Securing Cyber Space,” Department of Homeland Security, At https://www.dhs.gov/cyber-storm (Accessed2018/2/28)

態，到目前為止，除了 2008 年至 2016 年馬英九政府執政，兩岸經貿政策使兩岸關係較趨緩和外，都維持著中共在國際上持續打壓、恫嚇臺灣的狀況。由於臺灣特殊戰略位置，美國將臺灣視為與中共談判之籌碼，但在臺灣安全方面，依據《臺灣關係法》，美國對於是否出兵防衛臺灣的立場並不明確，而這種模糊性的安全承諾，主要在嚇阻中共可能的對臺軍事行動。[226]但同樣也為臺灣安全帶來隱憂。

美中兩國在政治、經濟、軍事層面上維持競爭又合作的狀態，而在兩岸不改變現況的前提下，我國應以不對稱作戰思維面對兩岸軍力與國力嚴重失衡的現實，若僅是挹注大量國防預算與中共進行「軍備競賽」，將可能使臺灣經濟陷入泥淖。而最能展現我國不對稱戰力則屬網路資訊作戰，我國擁有豐富網路資訊設備、研發能量以及相關產業人才，而透過網路資訊作戰，臺灣可參與美軍第三次抵銷戰略，如此將對我國在發展資通電軍以及不對稱作戰方面有所助益。2017 年 6 月我國資通電軍的成立已為未來的網路資訊作戰奠下基礎，未來渴望政府能將更多國防能量挹注至發展網路資訊作戰，希冀在網路資訊作戰領域取得我國的相對優勢。

國防大學
National Defense University

[226] 同註 177，頁 311。

第五章　結論

美國為了因應發展反介入與區域拒止及在網路資訊安全帶給美國威脅的國家，如中共、俄國、伊朗及北韓等，美軍啟動了第三次抵銷戰略，除發展新的軍事戰略外，也在人工智慧、大數據分析與雲端運算等三大領域實施大規模的投資與發展，而網路資訊作戰是其中的核心關鍵。在美中的競合關係之中，兩岸關係與美中兩國的權力消長密切相關，當美國對中共軍事實力差距愈大，美國便可在政治、軍事方面給予臺灣協助；當美中實力接近或是相當時，美國國內便會有棄台論聲浪的出現。現階段美國在軍事科技的發展仍優於中共，但中共憑藉其政治、經濟之發展與影響力，國防預算每年持續以兩位數成長，持續對美國造成巨大威脅，中共軍力的提升，加速兩岸的軍事失衡，我國惟有發展不對稱作戰，方能與之相抗衡。

第一節　研究發現

一、　科技創新是美軍軍事發展的長期趨勢。

2014 年美國國防部長黑格提出國防創新倡議，希望透過技術以及組織的創新，發展新的軍事戰略因應外部的威脅，並運用不對稱作戰方式抵銷對手在軍力上的優勢。因應不同政黨的輪替，政策的延續性是相當大的關鍵因素，特別是在政策剛開始執行時，若遇政權輪替，往往因理念不同而無法延續。但長期的趨勢將會是科技的創新與發展不對稱作戰，而無關乎由誰執政，政策即使易名，內涵仍然不會改變。在歐巴馬政府提出第三次抵銷戰略時，透過智庫的研究與分析，美軍欲應對潛在敵人的威脅，則必須透過發展新的作戰概念、科技創新、國防改革等，並主張在重點科技上投入相當的國防預算，各項計畫和系統之設計要能應處未來戰鬥環境之挑戰，尤其在面對阻撓美國軍力投射的反介入與區域拒止的挑戰。

再者，現今各國在經濟上的密切交流，導致國際局勢牽一髮而動全身，已不像過去冷戰時期發展軍備競賽，以傳統武器數量作為對抗籌碼如此單純，因此發展更有效以及更加精準的武器，打擊敵方的弱勢，發揮我方的優勢及強項的不對稱作戰，如何能夠出「敵」意表，是各國持續努力與發展之方向。

二、　第三次抵銷戰略的核心關鍵為網路資訊作戰。

無論是人工智慧、無人載具、遠程作戰武器及太空能力，美軍在第三次抵銷戰略均投入大量研發人力與資金，企圖發展能夠扭轉戰爭局勢的關鍵戰力，而這些高科技武器的共通點，則是依賴網路空間，方能在聯合作戰時相互連結，換言之，美軍必須透過網路空間方能有效指揮這些距離千里以外的武器。

進入網路攻擊及作戰的門檻很低，因此駭客將會利用美國對於電腦與網路的依賴進行攻擊，藉以瓦解其在聯合部隊的自動化系統，使指揮管制的機制失靈，若此情況真實發生，將會使美軍遭受極大傷害，因此網路資訊安全的重要不言可喻。我們可以推想，未來作戰空間將會從實體轉向虛擬，從陸海空領域轉向網路空間，因一切指揮管制都須藉由網路完成，第三次抵銷戰略所發展的軍事科技以及更加完善的聯合部隊作戰模式，將使美國面臨潛在敵人積極致重點於瓦解美國自動化系統網路的電子攻擊，在未來的戰爭中，成敗將都取決於網路戰。

三、　美國可協助臺灣在網路資訊作戰領域發展不對稱作戰。

在《臺灣關係法》框架下，美國僅能售予我國防禦性武器，若在軍售議題上觸碰敏感話題，中共便會對美國提出抗議，以及在國際對我國施壓。面對中共對美臺兩國政治、軍事上的監控，網路空間所擁有的隱密性，將可對美台在軍事的交流有所幫助。臺灣是美國在東亞戰略上的盟友，且臺灣也擁有豐富的資訊科技設備與人才，在 2017 年 6 月時，我國通資電軍成軍，並且與交通大學共同成立國防資電科技中心，無論是在軍事或是與民間交流方面，已能達到我國的國防自主，因此對於美國來說，協助我國網路資訊作戰之發展，不僅在軍事方面能夠得到交流，亦可對美國在亞太地區的戰略佈署有所助益。

國防大學 National Defense University

第二節　未來研究建議

二次世界大戰後，美蘇兩強形成冷戰對峙的局面，因此有了核武的發展以及精準武器的產生，如今，中共的快速軍事現代化威脅美國的霸權地位，因此美國提出第三次抵銷戰略，期許在創新科技的幫助下，能夠有效抵銷對手優勢，維持美國的地位，事實上，中共要在軍事、科技上領先美國，仍有一段漫長的道路需

要突破，中共因經濟的高速發展，連帶投入大量預算資金進入國防工業，美國也同樣如此，不願意原地踏步，因此才有越來越多創新的科技與作戰模式出現。對於臺灣來說，是值得我們借鏡的，進入資訊時代以來，人類的生活逐漸與網路連接，甚至在進入物聯網後，我們已與「智慧生活」無法脫離，即使我國與中共軍力日漸失衡，但在我國具有優勢的網路資訊領域投資發展，將可以使我國獲得最大的效益，因此提出以下建議：

一、加強通資電軍與各軍種以及民間技術交流

美軍認為，團隊合作是維護網路安全的首要原則，為了增強網路空間聯合行動能力，美軍提出了聯合網路訓練標準，摸索軍種間聯合的網路訓練，完善軍民聯合網路演習，網路資訊作戰與陸、海、空、太空領域作戰行動的戰術融合，使美軍聯合作戰事半功倍。隨著「多域戰」概念被正式寫入陸軍新版作戰條令，美國陸軍率先嘗試了軍種間聯合網路訓練，2017 年 10 月，陸軍首次在「網路閃電戰」（Cyber Blitz）演習中邀請空軍國民警衛隊的聯合終端攻擊控制員參演，負責協助旅戰鬥隊指揮官運用動能和非動能武器，演練如何運用聯合終端攻擊控制員打擊目標。另定期展開軍民聯合網路演習，美軍認為，必須與其他聯邦政府機構、州和地方政府特別是民間企業進行合作，鑑於恐怖分子與網路空間結合等趨勢，除了上述國土安全部被賦予執行網路安全等工作外，也主導結合各民間企業、大學、州政府，來強化對於資訊交換與合作的管道，主動管理網路相關威脅，以及協調網路資訊共享。

我國通資電軍於 2017 年 6 月成軍，目前與國立交通大學共同成立「國防資電科技中心」，從教育與國防領域著手，目標是為資通電軍培養出更多具備資安專業能力的人才，進而提升臺灣通資電軍的網路作戰能力，雖我國通資電軍較其他先進國家晚成軍，但依然可憑藉我國在網路資訊設備之優勢，並配合行政部門之擘劃，將通資電軍與陸海空軍有效結合，並與民間科技人才技術交流，方能「以小博大」達成我國軍事作戰任務。

國防大學 National Defense University

二、發展屬於我國的「抵銷戰略」

面對中共逐漸壯大，且兩岸軍力失衡的情況下，我國無法與之實施正面衝突與對抗，亦不可能舉全國之力投入軍備競賽，因此創新的科技與思維將是臺灣軍事戰略的出路，如前一章所言，臺灣擁有資訊產業發展所需的人才以及友善的政策，且因美國企業對美中貿易戰、智慧財產權遭侵犯和資料安全問題存有疑慮，再加上臺灣穩定的基礎電力設施等，都是各國企業願意來台投資與從事研發的原因。

對於美國來說，棄台論出現的原因，就在於美中最後是否一戰，而臺灣問題就是其中的關鍵之一，美臺在網路作戰領域密切的接觸與交流，將使兩國關係更加緊密，我國可在美軍第三次抵銷戰略中提供相關人才與技術，並藉此引進美國在網路資訊作戰之戰略與戰術，加大我國資電優勢，發展我國對中共之不對稱作戰。

國防大學
National Defense University

參考文獻

壹、中文文獻

(一)專書

卜睿哲、歐漢龍著，林宗憲譯，2010，《不一樣的戰爭》，台北市：博雅書屋。

卜睿哲著，林添貴譯，2013，《台灣的未來》，台北市：遠流出版社。

卜睿哲著，林添貴譯，2013，《未知的海峽－兩岸關係的未來》，台北市：遠流出版社。

丹尼·羅伊著，周茂林譯，2015，《崛起：中共與區域安全》，台北市：政務辦公室。

方江、胡威標主編，2010，《空海一體戰：AirSea battle》，南京：中國人民解放軍海軍指揮學院。

王保存、劉玉建，1999，《外軍信息戰研究概覽》，北京：軍事科學出版社。

王萬里，1986，《美蘇關係研究：冷戰.和解.對抗》，臺北市：黎明出版社。

左鳳榮，2001，《致命的錯誤：蘇聯對外戰略的演變與影響》，北京：世界知識出版社。

布熱津斯基著，中國國際問題研究所譯，2007，《大棋局：美國的首要地位及其地緣戰略》，上海：上海人民出版社。

弗雷德瑞克·馬泰爾著，林幼嵐譯，2016，《全球網路戰爭 :全球化 vs 在地化》，新北市：稻田出版社。

石海明，2015，《科學，冷戰與國家安全：美國外空政策變革背後的政治》，北京：解放軍出版社。

朱浤源，2006，主編《撰寫博碩士論文實戰手冊》，新北市：正中書局。

呂秋文，2007，《如何撰寫學術論文》，新北市：臺灣商務印書館。

國防大學 National Defense University

宋鎮照、蔡相偉，2016，《大國戰略:安倍晉三和歐巴馬政府的東南亞區域發展競合》，台南市：成大出版社。

李丹慧主編，2008，《冷戰國際史 研究 no.7》，北京：世界知識出版社。

周湘華，2008，《遺忘的危機-第一次臺海危機的真相》，臺北市：秀威資訊科技。

明居正，2013，《大美霸權的浮現：後冷戰時期大國政治的邏輯》，台北市：五南出版社。

易君博，2003，《政治理論與研究方法》，臺北市：三民書局。

東鳥，2015，《鍵盤狙擊手 :不見硝煙的網路戰爭, 殺傷力卻更為驚人!》，臺北市 :有意思出版社。

Blane Clark、Dennis M.Murphy 著，洪淑貞、王慰慈譯， 2010，《資訊戰入門》，桃園縣：國防大學。

洪陸訓、莫大華，2011，主編《廿一世紀歐美主要國家心戰部隊的發展》，臺北市：國防大學政治作戰學院。

約瑟夫˙奈伊著，蔡東杰譯，2002，《美國霸權的矛盾與未來》，新北市：左岸文化出版社。

徐國興，2013，《我軍信息作戰力量建設研究》，北京 : 軍事科學出版社。

格爾多夫著，國防部史政編譯局譯，1996，《巨變：論美蘇關係與冷戰結束》，臺北市：國防部史政編譯局。

馬業西等人著，1999，《網路戰 : 地球村時代的戰爭》，北京 : 國防大學。

Leigh Armistead 著，高一中譯， 2012，《資訊作戰》，臺北市: 國防部史政編譯室。

Leigh Armistead 著，國防部譯， 2008，《資訊作戰-以柔克剛的戰爭》，臺北市: 國防部史政編譯室。

Thomas A. Johnson 著，國防部譯， 2017，《網路安全：捍衛網路戰時代中的關鍵基礎設施》，臺北市：政務辦公室。

張露，2013，《全球化時代的地緣政治與中美關係》，北京：軍事科學出版社。

強納森·霍斯雷格著，黃文啟譯，2017，《中共崛起 ： 亞洲的和戰難局》，台北市：政務辦公室。

理查德·克拉克等著，呂晶華、成高仲譯，2011，《網絡戰 ： 國家安全的新威脅及應對之策》，北京 ： 軍事科學出版社。

理查德·克拉克著，劉曉雪等譯，2012，《網電空間戰 ： 美國總統安全顧問 ： 戰爭就在你身邊》，北京：國防工業出版社。

Vojtech Mastny 著，郭懋安譯， 2002，《斯大林時期的冷戰與蘇聯的安全觀》，桂林：廣西師範大學出版社。

陳建民，2007，《兩岸關係中的美國因素》，台北市：秀威資訊科技。

陳毓鈞，1997，《戰爭與和平－解析美國對華政策》，台北市：環宇出版社。

David Marsh、Gerry Stoker 著，陳義彥譯，2009，《政治學方法論與途徑》，臺北市：韋伯文化事業出版社。

小川和久著，陳漢業譯， 1984，《深海核子冷戰》，臺北市：國防部史政編譯局

湯瑪士·詹森著，黃文啟譯，2017，《網路安全 ： 捍衛網路戰時代中的關鍵基礎設施》，臺北市 ： 政務辦公室。

United States Department of Defense 著，黃文啟譯， 2010，《2010 美國四期國防總檢討》(2010 Quadrennial Defense Review Report) ，臺北市：國防部史政編譯室。

葉至誠、葉立誠，1999，《研究方法與論文寫作》，臺北市：商鼎文化。

詹姆斯·斯塔夫里斯等著、胡升新等譯，2010，《「空海一體戰」新概念一體化打擊力量》，台北市：國防部政辦室。

趙干城、鮑世奮，1988，《史學方法論》，臺北：五南圖書出版公司。

劉金質，2003，《冷戰史　上》，北京：世界知識出版社。

樊高月、趙力昌主編，2014，《不流血的戰爭：網絡攻防經典之戰》，北京：解放

國防大學 National Defense University

軍出版社。

中川右介著，蔡昭儀譯， 2016，《惡的出世學：希特勒、史達林、毛澤東的手腕與謀略》，新北市：大牌出版。

羅伯特·吉爾平著，楊宇光等譯，1997，《國際關係的政治經濟分析》， 臺北市：遠流出版社。

羅伯特·哈狄克著，童光復譯，2017，《海上交鋒：中共、美國與太平洋的未來》，臺北市：政務辦公室。

羅納德·歐羅克主編，2014，《中共軍事現代化：戰略研析選譯》，台北市：國防部政辦室。

嚴怡民，1999，《今日天涯若比鄰：著名科學家談信息科學》。桂林：廣西師範大學出版社。

(二)期刊論文

吳奇英，2005，〈資訊時代政治作戰中心理戰的運用與發展-以美伊戰爭及兩岸資訊心理戰為例〉，《復興崗學報》，第 85 期，頁 71-93。

宋吉峰，2015，〈無聲無息的戰爭：電磁頻譜作戰的未來發展〉，《海軍學術雙月刊》，第 51 卷第 1 期，頁 61-73。

李大光，2016，〈美國推出保持軍事優勢的「第三次抵消戰略」〉，《國防科技工業》，第 7 期，頁 61-62。

李建昇，2014，〈從歷次《四期國防總檢討》探討美國國防政策內涵〉，《國防雜誌》，第 29 卷第 6 期，頁 35-62。

李建昇，2016，〈美軍抵消戰略之發展歷程〉，《國防雜誌》，第 31 期第 3 卷，頁 47-80。

李健，2015，〈美軍新「抵消戰略」的不確定性分析〉，《軍事文摘》，第 12 期，頁 54-55。

肖可，2016，〈第三次「抵消戰略」背景下美國國防科技發展〉，《軍事文摘》，第

國防大學 National Defense University

11 期，頁 14-16。

岳松堂、童真，2016，〈美國第三次「抵消戰略」全面解析〉，《現代軍事》，第 10 期，頁 91-96。

林哲正，2004，〈中共資訊戰戰略思維〉，《國防雜誌》，第 20 卷第 4 期，頁 98-106。

林海清，2005，〈二十一世紀臺灣戰略環境下的國家安全與資訊戰〉，《空大行政學報》，第 16 期，頁 111-142。

高志榮，2017，〈共軍的「反介入」戰略發展美國因應作為研究〉，《空軍學術雙月刊》，第 657 期，頁 31-39。

張洋，2016，〈第三次「抵消戰略」中的技術引入與創新〉，《軍事文摘》，第 13 期，頁 14-16。

章昌文譯，Timothy A. Walton 著，2017，〈確保「第三次抵銷戰略」：下任美國防部長的優先要務(Securing the Third Offset Strategy: Priorities for the Next Secretary of Defense)〉，《國防譯粹》，第 44 卷第 1 期，頁 16-30。

莫大華，1998，〈中共「軍事事務革命」之分析—資訊戰爭的探討〉，《中國大陸研究》，第 41 卷第 11 期，頁 45-56。

郭瑞鵬，2016，〈第三次「抵銷戰略」的困境〉，《軍事文摘》，第 13 期，頁 6-9。

陳勁甫、林建宏，2013，〈美國四次《四期國防總檢討》規畫思維之研究〉，《遠景基金會季刊》，第 14 卷第 2 期，頁 145-146。

陳勁甫、邱榮守，2007，〈論析美國「四期國防總檢」的立法與要求影響〉，《問題與研究》，第 46 卷第 3 期，頁 6-23。

彭錦珍，2006，〈現代化發展趨勢下的資訊社會與資訊戰〉，《復興崗學報》，第 86 期，頁 31-56。

童光復譯，James R. Holmes 著，2012，〈反介入的世界： 美國不容迴避的挑戰(U.S. Confronts an Anti-access World) 〉，《國防譯粹》，第 39 卷第 9 期，頁

50。

童光復譯，Jonathan Tepperman 著，2016，〈人物專訪：美國防部長卡特〉，《國防譯粹》，第 43 卷第 1 期，頁 82-89。

黃文啟譯，Bindiya Thomas 著，2017，〈網路反恐新概念：網路應變能力（Resilience－the Solution to Cyber Terrorism?）〉，《國防譯粹》，第 44 卷第 3 期，頁 34-39。

楊順利，2005，〈從美國戰略性資訊戰概念論資訊作戰對國家之影響〉，《國防雜誌》，第 20 卷第 11 期，頁 116-126。

葉志偉，2017，〈美軍資訊作戰聯戰準則之演進〉，《海軍學術雙月刊》，第 51 卷第 2 期，頁 114-126。

虞衛東，2015，〈美國第三次「抵消戰略」:意圖與影響比較研究〉，《國際關係研究》，第 3 期，頁 77-87。

路易斯．西蒙著，王濤編譯，2016，〈美國第三次抵銷戰略與歐洲面臨的「反介入」挑戰〉，《現代軍事》，第 10 期，頁 97-107。

趙炳強譯，Edward C. Cardon, David P. McHenry, and Christopher Cline 著，2017，〈網際空間作戰中創新重要性(The Relevance of Culture: Recognizing the Importance of Innovation in Cyberspace Operations) 〉，《國防譯粹》，第 44 卷第 3 期，頁 22-28。

劉一鳴、石海明，2016，〈技術致勝：美軍第三次「抵消戰略」評析〉，《指揮與控制學報》，第 2 卷第 2 期，頁 167-171。

劉戟鋒、盧瀟、劉楊鈺，2017，〈戰術心理戰的技術支撐〉，《國防科技》，第 2 期，頁 66-70。

劉棟，2016，〈軍隊內部創新的關鍵是機制和人才〉，《防務視點》，第 9 期，頁 9-11。

劉慶順譯，Daniel P. Taylor 著，2017，〈戰力加乘因子：網路能力（Force

國防大學 National Defense University

Multiplier：Navy Looks to Develop Cyber Capabilities as Part of Its Air Warfare Domain）〉，《國防譯粹》，第 44 卷第 3 期，頁 30-33。

蔡國堂，2012，〈共軍資訊心理戰之研究〉，《國防雜誌》，第 27 卷第 2 期，頁 56-67。

盧文豪，2015，〈美國亞太「再平衡」戰略下澳洲軍事部署戰略意涵探討〉，《國防雜誌》，第 30 卷第 2 期，頁 7。

謝冰峰，2016，〈第三次「抵消戰略」下，美國國防採辦改革與發展〉，《軍事文摘》，第 7 期，頁 10-13。

謝奕旭，2001，〈從美國 QDR 論我國國防政策之制定〉，《復興崗學報》，第 76 期，頁 89-112。

簡華慶，2012，〈網路資訊戰所扮演角色及因應策略之研究〉，《國防雜誌》，第 27 卷第 1 期，頁 122-138。

(三)網路資料

胡文玲譯，2017，〈【寰宇韜略】美重建軍力 2018 國防預算玄機大（上）〉，《青日報》，http://www.ydn.com.tw/News/250841（瀏覽日期：2017 年 10 月 5 日）。

胡文玲譯，2017，〈【寰宇韜略】美重建軍力 2018 國防預算玄機大（下）〉，《青日報》，http://www.ydn.com.tw/News/250999（瀏覽日期：2017 年 10 月 5 日）。

苑桂萍、胡冬冬、張紹芳，2016，〈美國國防預算 2017-2021 財趨勢分析〉，《每日頭條》，https://kknews.cc/zh-tw/military/z5ll3a.html（瀏覽日期：2017 年 9 月 5 日）。

高石，2017，〈7000 億美元！美國會通過金額最高國防授權案〉，《新華網》，http://big5.xinhuanet.com/gate/big5/news.xinhuanet.com/world/2017-09/23/c_129710890.htm （瀏覽日期：2017 年 10 月 16 日）

張國威，2014，〈美啟第 3 次抵銷戰略 意在制中〉，《旺報》，http://www.chinatimes.com/newspapers/20141206000921-260309（瀏覽日期：

國防大學 National Defense University

2017 年 9 月 5 日）。

陳建瑜，2016，〈美推抵銷戰略保優勢 抗中俄崛起〉，《旺報》，http://www.chinatimes.com/newspapers/20161030000556-260301（瀏覽日期：2017 年 9 月 5 日）。

曾復生，2016，〈美國國防預算與軍事戰略最新情勢研析〉，《財團法人國家政策研究基金會國政研究報告》，http://www.npf.org.tw/printfriendly/15750（瀏覽日期：2017 年 9 月 5 日）。

貳、英文文獻

(一)專書

Congressional Budget Office. 1982. *Building A 600-Ship Navy: Costs, Timing, and Alternative Approaches*. Washington, D.C.: The Congress of the United States.

Congressional Budget Office.1997. *Assessing the NATO/Warsaw Pact Military Balance*, Washington D.C.: The Congress of the United States.

Office of the Secretary of Defense.2015. *Military and Security Developments Involving the People's Republic of China 2015*., Washington, D.C.：Department of Defense.

The White House. 2012. *Sustaining U.S. Global Leadership: Priorities For 21st Century Defense*. Washington, D.C.:Department of Defense.

Mearsheimer. John J. 2001, *The Tragedy of Great Power Politics*. New York: WW Norton & Company.

(二)研究報告

Arquilla, John& David Ronfeldt. 1997. *In Athena's Camp: Preparing for Conflict in the Information Age*. CA: RAND Corporation.

Bitzinger, Richard A. 2016. *Third Offset Strategy and Chinese A2/AD Capabilities*.

Washington, D.C: Center for a New American Security.

Delvaux, Steven L. 2017. *America's Perpetual "Offset".* Fort Leavenworth, Kansas Army University Press.

Dombrowski, Peter. 2015. *America's Third Offset Strategy: New Military -Technologies and Implications for the Asia Pacific.* Singapore: Rajaratnam School of International Studies Press.

Ellman, Jesse, Lisa Samp, and Gabriel Coll. 2017. *Assessing the Third Offset Strategy.* Washington D.C.: Center for Strategic and International Studies.

Fan, Gaoyue. 2017. *A Chinese Perspective on the US Third Offset Strategy and Possible Chinese Responses.* CA: Institute on Global Conflict and Cooperation University of California.

Fiott, Daniel. 2015. *Europe and the United States Third Offset Strategy*. Belgium: The Institute for European Studies.

Hoag, Malcolm W. 1969. *What New Look in Defense?* CA: RAND Corporation.

Holloway, David, 2010. *Nuclear Weapons and the Escalation of the Cold War, 1945-1962*, CA：Cambridge University Press.

Kashin, Vasily& Michael Raska. 2017. *Countering The U.S. Third Offset Strategy: Russian Perspectives, Response And Challenges*. Singapore:Rajaratnam School of International Studies Press.

Larson, Eric V., David T. Orletsky, and Kristin Leuschener. 2001. *Defense Planning in a Decade of Change: Lessons From the Base Force, Bottom-Up Review, and Quadrennial Review.*CA: RAND Corporation.

Leighton, Richard M. 2001. *History of the Office of the Secretary of Defense. Volume 3: Strategy, Money, and the New Look 1953-1956*, Washington, D.C.: Office of the Secretary of Defense.

國防大學 National Defense University

Louth, John, Christian Moelling. 2016. *Technological Innovation-The US Third Offset Strategy and the Future Transatlantic Defense*. Belgium: The Armament Industry European Research Group.

Melanson, Richard A., David Mayers. 1986. *Reevaluating Eisenhower: American Foreign Policy in the 1950s*, Illinois: University of Illinois Press.

Ochmanek, David. 2014. *The Role of Maritime and Air Power in DoD's Third Offset Strategy*. CA: RAND Corporation.

(三)期刊論文

Cronin, Patrick M. and Seongwon Lee. 2016. "The ROK–U.S. Alliance and the Third Offset Strategy, " *The International Journal of Korean Studies*, Vol. XX, No.1, pp.72-97.

Gery, William R., SeYoung Lee, and Jacob Ninas. 2017. "Information Warfare in an Information Age," *Joint Force Quarterly*, Vol. 85, No.2, pp.22-29.

Grant, Rebecca. 2016. "The Second Offset," *Air Force Magazine*. No.7,pp.32-36.

Grier, Peter. 2016. "The First Offset," *Air Force Magazine*.No.6, pp.56-60.

Hutchens, Michael E. et al. 2017. "Joint Concept for Access and Maneuver in the Global Commons:A New Joint Operational Concept, "*Joint Force Quarterly*. Vol. 84,No.1, pp.134-136.

Lincoln, Bonner E. III. 2014. "Cyber Power in 21st-Century Joint Warfare," *Joint Force Quarterly*. Vol. 74,No.3,pp.102-109.

McGrath, James R. 2016. "Twenty-First Century Information Warfare and the Third Offset Strategy," *Joint Forces Quarterly*. Vol. 82,No.3,pp.16-23.

Norwood, Paul, Benjamin Jensen. 2016. "Wargaming the Third Offset Strategy," *Joint Force Quarterly*. Vol. 83,No.4,pp.34-39.

Walton, Timothy A. 2016. "Securing the Third Offset Strategy," *Joint Force Quarterly*.

國防大學 National Defense University

Vol. 82,No.3, pp.6-15.

Watts, Stephen, J. Michael Polich and Derek Eaton. 2015. “Rapid Regeneration of Irregular Warfare Capacity,”*Joint Force Quarterly*. Vol. 78,No.3,pp.32-39.

Wells, Samuel F. 1981. “The Origins of Massive Retaliation,” *Political Science Quarter*ly, Vol.96, No.1.pp.31-52.

Wolk, Herman S. 2003. “The New Look,” *Air Force Magazine*, No.8.pp.80-83.

(四)網路資料

Bialos, Jeffrey P.& Stuart L. Koehl. 2016. “What America's Big New Defense Plan Gets Wrong,”At http://nationalinterest.org/feature/what-americas-big-new-defense-plan-gets-wrong-16421（Accessed 2017/09/16）

Byers, Andrew. 2016. “Origins of a Third Offset Strategy,” At https://sites.duke.edu/andrewbyers/files/2016/09/Website_Origins-of-a-Third-Offset-Strategy.pdf (Accessed 2017/09/19)

Carberry, Sean D. 2017. “What's the future of defense innovation under Trump?,”At https://fcw.com/articles/2017/04/06/defense-innovation-under-trump.aspx?m=1（Accessed 2017/09/16）

Carter, Ash. 2016. “Remarks on "The Path to an Innovative Future for Defense" (CSIS Third Offset Strategy Conference),”At https://www.defense.gov/News/Speeches/Speech-View/Article/990315/remarks-on-the-path-to-an-innovative-future-for-defense-csis-third-offset-strat/（Accessed 2017/09/16）

Cavanaugh, Matt. 2017. “False Faith: the Third Offset isn’t a Strategy and Won’t Win Our Next War,”At https://mwi.usma.edu/false-faith-third-offset-isnt-strategy-wont-win-next-war/（Accessed 2017/09/16）

Davies, Andrew. 2016. “US Military's Third Offset Strategy: A Silver Bullet or Simply a

Bad Idea?" At http://nationalinterest.org/blog/the-buzz/us-militarys-third-offset-strategy-silver-bullet-or-simply-17227 (Accessed 2017/09/19)

Department of Defense. 2012. "Sustaining U.S Global Leadership: Priorities For 21st Century Defense." At http://archive.defense.gov/news/Defense_Strategic_Guidance.pdf (Accessed 2017/9/20)

Department of Defense. 2016."Deputy Secretary: Third Offset Strategy Bolsters America's Military Deterrence,"At https://www.defense.gov/News/Article/Article/991434/deputy-secretary-third-offset-strategy-bolsters-americas-military-deterrence/（Accessed 2017/05/20）

Dombrowski, Peter J. 2015. "America's Third Offset Strategy: New Military Technologies and Implications for the Asia Pacific,"*Rajaratnam School of International Studies,*June.At http://www.rsis.edu.sg/wp-content/uploads/2015/06/PR150608_Americas-Third-Offset-Strategy.pdf (Accessed 2017/9/26)

Faith, Ryan& Vice News. 2014. "Introducing the Pentagon's New 'Third Offset Strategy': Welcoming Your New Robot Overlords, "At https://news.vice.com/article/introducing-the-pentagons-new-third-offset-strategy-welcoming-your-new-robot-overlords（Accessed 2017/09/16）

Freedberg, Sydney J. 2016. "Pentagon Can't Afford To Field 3rd Offset Tech Under BCA: Frank Kendall,"At https://breakingdefense.com/2016/10/pentagon-cant-afford-to-field-3rd-offset-tech-frank-kendall/（Accessed 2017/08/16）

Gady, Franz-Stefan. 2016. "New Us Defense Budget: $18 Billion for Third Offset Strategy, the Pentagon Wants to Spend More Money to Offset Anti-Area/Access-Denial (A2/AD) Technologies," The Diplomat, At

國防大學 National Defense University

https://thediplomat.com/2016/02/new-us-defense-budget-18-billion-for-third-offset-strategy/.(Accessed 2017/10/16)

Gady, Franz-Stefan.2016. “New US Defense Budget: $18 Billion for Third Offset Strategy,”At https://thediplomat.com/2016/02/new-us-defense-budget-18-billion-for-third-offset-strategy/（Accessed 2017/09/16）

Grant, Rebecca. 2016. “The Second Offset, ”At http://www.airforcemag.com/MagazineArchive/Documents/2016/July%202016/0716secondoffset.pdf（Accessed 2017/10/16）

Hicks, Kathleen&Andrew Hunter. 2017. “What Will Replace the Third Offset? Lessons from Past Innovation Strategies,”At http://www.defenseone.com/ideas/2017/03/what-will-replace-third-offset-lessons-past-innovation-strategies/136260/（Accessed 2017/09/16）

Horres, Edward J. 2016. “Towards a Fourth Offset Strategy,” At file:///C:/Users/Administrator/Downloads/SWJ_Towards%20a%20Fourth%20Offset%20Strategy%20%20(1).pdf. (Accessed 2017/10/19)

Hunter, Andrew. 2015.“Keeping the Technological Edge :Leveraging Outside Innovation to Sustain DoDs Technological Advantage,At https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/150626_tech_edge_presentation.pdf.Accessed 2017/9/20)

Ignatius, David. 2016. “High-Tech Arms Race May Complicate Trump's Plan for Russia,”At http://www.newsmax.com/DavidIgnatius/russia-trump-weapons-china/2016/12/02/id/761762/（Accessed 2017/09/16）

Jackson, Craig& Robert Templeman. 2016. “The Third Offset and a Fifth Domain? Balancing Game-Changing Innovation and Cyber Risk Mitigation, ”At

國防大學 National Defense University

https://arxiv.org/ftp/arxiv/papers/1610/1610.07982.pdf (Accessed 2017/09/19)

Jackson, Van. 2015. “The Pentagon's Third Offset Strategy: What US Allies and Partners Need to Know,” At https://thediplomat.com/2015/04/the-pentagons-third-offset-strategy-what-us-allies-and-partners-need-to-know/（Accessed 2017/09/16）

Johnson, Thedore R. 2016. “Will the Department of Defense Invest in People or Technology?,”At https://www.theatlantic.com/politics/archive/2016/11/trump-military-third-offset-strategy/508964/（Accessed 2017/09/16）

Keck, Zachary. 2014. “Wanted: An Enemy for America's Third Offset Strategy,” At http://nationalinterest.org/feature/wanted-enemy-americas-third-offset-strategy-11781（Accessed 2017/09/15）

Lange, Katie. 2016. “3rd Offset Strategy 101: What It Is, What the Tech Focuses Are, ”At http://www.dodlive.mil/2016/03/30/3rd-offset-strategy-101-what-it-is-what-the-tech-focuses-are/ (Accessed 2017/09/19)

Libicki, Martin C. 2016. “Planning a Cyberwar,” At https://www.usni.org/magazines/proceedings/2016-10/planning-cyberwar (Accessed 2017/9/20)

Pellerin, Cheryl. 2016. “DoD Strategic Capabilities Office is Near-Term Part of Third Offset, ”At https://www.defense.gov/News/Article/Article/995438/dod-strategic-capabilities-office-is-near-term-part-of-third-offset/（Accessed 2017/09/16）

Pellerin, Cheryl. 2016.“Work: Great-Power Competition Aims for Deterrence, Not War,”At https://www.defense.gov/News/Article/Article/708827/work-great-power-competition-aims-for-deterrence-not-war/（Accessed 2017/09/16）

Pellerin, Cheryl. 2017. “Mattis: Impact of Industry Innovation Will Continue to Grow at DoD,” At https://www.defense.gov/News/Article/Article/1276282/mattis-

國防大學 National Defense University

impact-of-industry-innovation-will-continue-to-grow-at-dod/ (Accessed 2017/10/19)

Pomerleau, Mark. 2017.“The fate of the third offset under President Trump,”At https://www.c4isrnet.com/it-networks/2017/01/18/the-fate-of-the-third-offset-under-president-trump/（Accessed 2017/10/2）

Pomerleau, Mark. 2017.“The fate of the third offset under President Trump,”At https://www.c4isrnet.com/it-networks/2017/01/18/the-fate-of-the-third-offset-under-president-trump/（Accessed 2017/09/16）

Popescu, Ionut C. 2017. “Strategic Uncertainty, the Third Offset, and US Grand Strategy, ”At http://ssi.armywarcollege.edu/pubs/Parameters/issues/Winter_2016-17/9_Popescu.pdf (Accessed 2017/09/19)

Quencez, Martin. 2016. “The Impossible Transatlantic Discussion on the U.S. Third Offset Strategy,”At http://brussels.gmfus.org/publications/impossible-transatlantic-discussion-us-third-offset-strategy（Accessed 2017/06/16）

Rand Corporation. 2016. “The U.S.-China Military Scorecard Forces, Geography, and the Evolving Balance of Power, 1996–2017”, At http://www.rand.org/pubs/research_reports/RR392.html

Stefanus, Daniel. 2017.“Embracing the Dark Battle：Electronic Warfare, Distributed Lethality, and the Future of Naval Warfighting,” .At https://www.usni.org/magazines/proceedings/2017-04/embracing-dark-battle (Accessed 2017/08/20)

Thomas, Will. 2017. “Trump Budget Cuts Defense S&T by 5.8% While Funding Third Offset Priorities,”At https://www.aip.org/fyi/2017/trump-budget-cuts-defense-st-58-while-funding-third-offset-priorities（Accessed 2017/09/16）

國防大學 National Defense University

Wald, Chuck&Joe Mariani. 2017. “The Key to Military Innovation,”At https://www.usnews.com/opinion/world-report/articles/2017-02-27/key-to-defense-departments-third-offense-is-use-of-military-technology（Accessed 2017/09/16）

Wines, Michael. 2011. “U.S. and China Try to Agree on Military Strategy,”At http://www.nytimes.com/2011/07/15/world/asia/15beijing.html (Accessed 2017/9/20)

Work, Bob. 2015. “The Third U.S. Offset Strategy and its Implications for Partners and Allies, ”At https://www.defense.gov/News/Speeches/Speech-View/Article/606641/（Accessed 2017/09/16）

國防大學
National Defense University