第十卷第一期 中華民國一〇九年 三月

ISSN 2223-9413

戰略與評估

論文

Defense Strategy & Assessment Journal

Vol.10, No.1,
March 2020

財團法人國防安全研究院 出版

戰略與評估

第十卷第一期 中華民國一〇九年 三月

Defense Strategy and Assessment Journal

Vol.10, No.1, March 2020

出　　版：財團法人國防安全研究院
發 行 人：霍守業
主　　編：歐錫富
執行主編：李哲全
編輯委員：王高成、李瓊莉、李俊毅、李哲全、沈明室、林成蔚、林文程、馬振坤、劉復國、歐錫富
（依姓氏筆劃排列）
助理編輯：陳鴻鈞
校　　對：陳彥廷、陳蒿堯、舒孝煌、鍾志東
出版企劃：胡國荃
電　　話：(02)2331-2360 轉 314
傳　　真：(02)2331-2361
電子信箱：dsaj@indsr.org.tw
院　　址：10048 臺北市中正區博愛路 172 號
ISSN：2223-9413

戰略與評估

第十卷第一期

目錄

論文

作者簡介

王綉雯	日本京都大學法學博士，現任國防安全研究院博士後研究。主要研究領域為：制度變遷、產業創新、中國經濟、美中貿易戰、國防科技。
洪瑞閔	比利時法語魯汶大學政治學博士，現任國防安全研究院博士後研究。主要研究領域為：歐洲國防產業、國防戰略資源供應、歐洲聯盟、整合理論、認同研究。
蔡榮峰	澳洲國家大學外交碩士/戰略研究碩士，現任國防安全研究院政策分析員。主要研究領域為：澳洲與歐洲國防產業、南太平洋區域研究、太空產業。
Miguel Alberto Gomez	Miguel Alberto Gomez is a senior researcher at the Center for Security Studies. His area of research is centered around Cybersecurity. Specifically, he is interested in the strategic use of cyberspace as an instrument of national power as well the emergence of norms surrounding the use of this domain.
Christopher Whyte	Christopher Whyte is an assistant professor of Virginia Commonwealth University. His research interests include a range of international security topics related to the use of information technology in war and peace, political communication and cybersecurity doctrine/policy.

日本造艦計畫、造艦產業發展及經濟效益之評估

王綉雯

博士後研究

國防安全研究院國防資源與產業研究所

摘　要

本文主要探究日本造艦計畫和造艦產業之發展，並對其在日本全國層級和地方層級所產生之經濟效益進行評估。基於威脅認知和防衛戰略之轉變，日本造艦計畫自 2012 年底第二次安倍政權以來有大幅增長。然而，受限於憲法第九條與防衛預算不得超過 GDP1%等限制，造艦計畫朝向船體大型化和高性能化發展，目前聚焦於多功能護衛艦之建造。日本造艦產業和政府之間有很深的歷史淵源，並形成造船業者各有專精艦種建造技術之造艦體制和特殊的採購方式。近年來日本政府直接介入進行改革，導入公開競標和合作造艦方式，以期維持日本造艦技術和產業基礎。造艦產業除了各造船大廠之外，主要由地方海事聚落之中小企業所構成，對日本全國和地方均產生經濟效益。本文依據日本總務省和長崎縣政府網站上的經濟外溢效果試算工具，以及造船業勞工人數之變化，估算出造艦計畫帶來的經濟效益和就業機會，以供我國借鏡。

關鍵詞：造艦計畫、造艦產業、海事聚落、外溢效果

Japan's Warship Building Plans, Industries and the Economic Impact Assessment

Shiowwen Wang

Postdoctoral Fellow

Division of National Defense Resources and Industries

Institute for National Defense and Security Research

Abstract

This paper explores the evolution of Japan's warship building plans and industries, and offers an assessment of its economic impacts on local and national levels. Due to the change of national security thinking and the threat recognition, Japan's warship building plan has expanded since the second Abe cabinet in 2012. Restricted by Article 9 of the Japanese Constitution, and limits on the defense budget to not exceed 1% of GDP, the aim of Japan's warship building plan is towards obtaining larger and more high performance warships. Now it is focused on multi-mission frigates. There is a remarkably close connection between the shipbuilding industry and the government in Japan because the warship building industry was the first military-industrial complex in the early 1900s. Consequently, it has led to the current warship building system in which every manufacturer has as specialty and the unique style of governmental acquisition and procurement. One characteristic of Japan's warship building industry is that it is comprised of a lot of small and medium enterprises in local marine clusters. Therefore, warship building plans will create spillover effects both on local and national levels. Finally, using simple tools to calculate the spillover effects through Input-Output Table and the change of employment in the shipbuilding industry, we estimate the spillover effect and employment potential of Japan's warship building plans.

Keywords: *warship building plan, defense industry, marine cluster, spillover effect*

壹、前言

日本 2019 年新《防衛計畫大綱》中提出自衛隊新編制，並大幅增加海上自衛隊（以下簡稱為海自）之艦艇數量和配備。在原本 4 個護衛艦隊群之外，加上 2 個由新型護衛艦（Future Frigate for Multi-Mission, FFM 或稱 30DX）或掃雷艦組成的機動艦隊群，構成新的水面艦艇部隊。新編的護衛隊群，每隊以一艘直升機護衛艦（Helicopter Destroyer, DDH）與兩艘神盾級護衛艦（Guided Missile Weapon Destroyer, DDG）為中心，並另增巡防艦部隊。預計在 2019-2024 年內將新增 23 艘、總噸數達 6.6 萬噸的軍艦，包括：護衛艦 10 艘、潛艦 5 艘、巡防艦 4 艘和其他艦艇 4 艘。

日本艦艇數量近年來大量增加，主要是為了因應海自角色和任務之擴大。海自目前的任務，除了警戒監視中國在東海和南海之活動外，還必須對應離島爭議之武力紛爭、防範與周邊國家在海洋資源開發上的爭議，以及回應北韓核子武器和飛彈攻擊。此外，海上自衛隊也須處理屬於未達戰爭形式的「灰色地帶」（gray zone）之非法威脅，如：恐怖主義、游擊隊、毒品和人口走私等，並參與聯合國等國際和平維持活動。

海自角色之擴大主要源於日本防衛戰略之轉換，並受日美安全保障合作機制主導，最後反映在《防衛計畫大綱》（以下簡稱為《大綱》）和《中期防衛力整備計畫》（以下簡稱為《中期防》）。換言之，日本防衛戰略之演變和美國之全球軍事布局息息相關，並受日本國家預算、國內政治經濟、國際政治經濟情勢之變化所影響。海自的整編、戰力部署和造艦計畫等也必須置於此脈絡之下來探討。

除了實際的軍事效益之外，造艦計畫對日本國內也有一定的經濟效益。日本有超過百年的造艦歷史和雄厚的重工業基礎，不但曾建造出世界第一艘航空母艦，二次大戰期間更擁有許多著名的戰鬥艦和重巡洋艦。另一方面，戰後海上自衛隊雖然在日本憲法「專守防衛」原則下無法擁有攻擊型武器，但是擁有精良的海軍裝備如航空母艦等，一直是海上自衛隊長期追求的目標。造艦計畫所產生之經濟效益，如：關鍵技術之研發、造船產業和海事聚落之發展、地方就業人口之增加等，雖不受傳統的戰略領域或軍事研究者重視，但是對日本國內經濟之外溢效果（spillover effect）卻不容忽視。

本論文嘗試從經濟效益分析之角度，對日本造艦計畫、造艦產業發

展及其經濟效益進行初步探討。

貳、海上自衛隊之編制和現況

日本海上自衛隊的實力向來排名世界前茅。帝國海軍實力在二次大戰前即已長期列入世界五強，戰後又以舊海軍軍官為中心組成海上自衛隊，將帝國海軍的人才、知識和傳統保留下來。戰後為了記取二戰時期偏重艦隊對決而忽視海上交通線安全以致敗戰之教訓，並遵守憲法「放棄戰爭」之規定，海自將戰略重點置於反潛作戰和確保海上交通線安全，兵力部署則以護衛艦、反潛戰機和潛艦三者為主。

一、編制

海上自衛隊之組織結構，主要分為三大部分，分別是：1.海上幕僚監部：輔佐防衛大臣，相當於海軍參謀本部；2.各機關：負責教育和補給，例如補給本部、海軍軍校；3.部隊：即自衛艦隊和各地方隊，自衛艦隊是有事之際的作戰主力，而地方隊則負責自衛艦隊之修理或燃料補給等後勤工作。關於部隊之編制，可簡述如下：

（一）自衛艦隊：

自衛艦隊由約 90 艘艦艇和 200 架飛機編成，主要分為「護衛艦隊」、「潛水艦隊」及「航空集團」三部分，負責日本領海防衛之水面、水下和空中三大領域。其下又另編有其他功能型部隊，如：掃雷隊群、情報業務隊群、海洋業務/對潛支援群、開發隊群、輸送部隊等其他部隊。

1.護衛艦隊：其編制分為「隊」、「群」（或稱為「隊群」）、「艦隊」三級。由兩隻以上艦艇組成「隊」；兩隊以上組成「隊群」；兩個隊群以上組成「艦隊」。護衛艦隊編有四個隊群，共 8 小隊，主要編隊形式是自 1980 年代建立的「八艦八機」，稱為「八八護衛群」，駐防地點則在橫須賀、佐世保、舞鶴和吳港。隨著日本自衛隊自 1990 年代起擴大國際參與，護衛艦隊也開始發展遠洋長航之能力。

2.潛水艦隊：有兩個隊群，負責有事之際阻止敵國艦隊通過日本海峽。日本潛水艦隊最初負責偵測蘇聯潛艦之活動，部署於日本北方之宗谷、津輕和對馬海峽；近年來，隨著中國潛艦頻繁經由宮古海峽或巴士海峽穿越第一島鏈，日本潛艦數量快速增加，部署地點也由日本的北方轉為西南方。

3.航空集團：有 7 個隊群，負責日本周邊海域之空中警戒和確保海上交通路線之安全。

（二）地方隊：

地方隊源自明治時代「鎮守府」制度，[1]日本全國沿岸設為五大地方警備區，分別是大湊、橫須賀、舞鶴、吳港及佐世保，各地分別設有一座海軍基地。地方隊在戰前即負責前線作戰艦隊之補給和士兵訓練，目前則在各地方總監指揮之下防守所管海域，亦即負責近海防禦。因此，地方隊所需之艦艇並不是護衛艦般的大型航艦，而是能夠快速對處敵情的小型艦艇。此外，地方隊所在的五大軍港，和當地以造船業和海運業為中心的海事聚落息息相關。造艦計畫不僅能維持造船大企業之技術和生計，對地方經濟和就業也有很大的貢獻。

二、作戰實力

海自的反潛作戰能力和掃雷能力相當優異，神盾級護衛艦之數量也僅次於美國，居世界第二。依據 2019 年之資料，做為海自主要兵力之護衛艦共 48 艘（總排水量 26.8 萬噸，以下同）、傳統動力型潛艦 19 艘（5.4 萬噸）、掃雷艦 24 艘（2.3 萬噸）、巡邏艦艇 6 艘（1,000 噸）、運輸艦 11 艘（2.8 萬噸）、補給艦 29 艘（12.7 萬噸），人員總數則有 42,289 人。[2]

護衛艦主要分為「一般護衛艦（DD）」和「直升機護衛艦（DDH）」兩種。前者如「村雨」（Murasame） 型或「高浪（Takanami）」型；後者則有「出雲（Izumo）」型或「日向（Hyuka）」型。雖然日本艦艇總數量不及韓國艦艇總數 200 艘之一半，且除了「出雲」號和「日向」號之外幾乎都是小型艦艇，但是日本護衛艦隊之實力在亞洲仍是數一數二。

其中，直升機護衛艦「日向」號於 2009 年服役，是日本海上自衛

[1] 鎮守府是明治時期治理海軍艦隊母港的機構，負責所轄軍區之防備、所屬艦艇之指揮、補給、出發準備，兵員招募、訓練，政策執行和監管等工作。

[2] 參見防衛省，《防衛白書》（令和元年版），《防衛省》，2019 年，https://www.mod.go.jp/j/publication/wp/wp2019/w2019_00.html。

隊作戰能力大幅提昇的重要指標。「日向」號結合大型補給艦和運輸艦之功能，使得自衛艦隊可在東亞和西太平洋海域獨力作戰。[3]其後，2015年服役的「出雲」號受到世人更大的注目。「出雲」號是日本戰後噸位最大（19,500 噸）的直升機護衛艦。除了配備全通甲板之外，最多可搭載 13 架反潛直升機，被視為可用於指揮護衛艦隊和進行反潛對策的小型航空母艦。同型第二艘護衛艦「加賀」（Kaga）號也已於 2017 年服役。由於「出雲」級護衛艦稍加改造即可搭載戰鬥機，日本政府已在 2019-2024 年《中期防》預定將其改造為可搭載最先進匿蹤戰機 F-35B 的「多功能護衛艦」。

日本的潛水艦隊則由 20 艘潛艦和 2 艘救難母艦構成，主要任務是監視周邊海域之動態，特別是石油能源輸入必經的東海和日本海。日本潛艦之性能可執世界牛耳，以 1998 年成為主力艦的「親潮（Oyasio）」級普通動力潛艦而言，其潛水深度和續行距離都優於其他國家同類型產品。其後，日本又推出搭載絕氣推進系統（AIP）的「蒼龍（Souryu）」級潛艦，潛行時間可長達兩週，遠遠超越其他非核子動力潛艦最長潛行三天之紀錄，且其收集敵艦聲音數據之能力及高度匿蹤性都較「親潮」級大幅提升。2018 年，日本海自第 11 艘「蒼龍」級潛艦「凰龍號」（Oryu）舉行下水典禮，這是全球第一艘使用鋰離子電池的潛艦，潛行時間比使用傳統鉛酸電池的潛艦更長。2019 年 11 月，海自第 12 艘潛艦、第二艘搭載鋰離子電池之「蒼龍」級潛艦「鬥龍號」（Touryu）也開始下水，顯見日本持續不斷精進其潛艦性能和建造能力。[4]

---

[3] 内山昭，〈日本·軍事大国論と対抗戦略〉，《大阪經大論集》，第 69 卷第 2 號，2018 年 7 月，頁 15。

[4] 陳昭羽，〈日本海上自衛隊應對中共海軍威脅之研究─以潛艦發展戰略為例〉，《海軍學術雙月刊》，第 53 卷第 6 期，2019 年 12 月，頁 72-76；高橋浩祐，〈リチウムイオン電池搭載の海上自衛隊の最新鋭潜水艦「とうりゅう」が進水。韓国も同種の潜水艦を開発中〉，《Yahoo Japan ニュース》，https://news.yahoo.co.jp/byline/takahashikosuke/20191107-00149842。

參、日本防衛戰略之轉換

一、美國全球戰略之調整

日本防衛戰略在 2001 年 911 事件之後，因美國全球戰略之調整而出現大轉換。911 事件使美國之威脅認知對象由「國家」轉為「恐怖組織」等非國家主體，並對美軍之組織、編成、裝備和戰力運用等進行大規模調整。為了事前防範大規模毀滅性武器或恐怖威脅，美國提出「先發威懾」（Forward Deterrence）和「離岸制衡」(Offshore Balancing)之概念，強調可發動先發制人之攻擊。為此，美國將戰略由向來依賴戰略核武的「報復性遏止」，轉換為以核戰力、飛彈防衛、國防基礎戰力三者為主幹的「阻絕性遏止」，被視為美國戰後以來最重要的戰略轉換。[5]

同時，美國雖面臨龐大的財政赤字壓力，卻意識到亞太地區將出現強大軍事競爭對手之可能性，希望透過與同盟國或友好國家之合作，建構美國所期待的區域平衡和區域秩序。特別是小布希（George Walker Bush）政權時期對美日合作和分工提出明確的規劃，使美日同盟關係逐漸由「亞太地區安全保障之礎石」朝「世界規模的戰略夥伴關係」發展。[6]2002 年，美國發布了新國防戰略，大幅削減陸上軍力並增加關島的兵力部署、整編亞太地區的美軍軍力，以牽制中國在西太平洋和印度洋之威脅。[7]美軍主力由第一島鏈之沖繩移往第二島鏈之關島，使日本必須在亞太地區承擔越來越多的防衛責任。

與此同步發展的，是日本的威脅認知對象之轉變。冷戰結束後，日本認為主要國家間發生大規模戰爭之可能性降低，但是涉及領土、主權或海洋經濟利益等既非平時也非戰時之「灰色地帶」衝突則有長期化傾向，特別是北韓的飛彈開發及中國對日本領海和領空之任意侵入等，極

---

5 池田十吾、下平拓哉，〈ブッシュ・ドクトリンと日本〉，《政治研究》，第 9 号，2018 年，頁 15-18。

6 參見 Richard L. Amitage and Joseph S. Nye, *The US-Japan Alliance: Getting Asia Right through 2020*, Center for Strategic and International Studies, February 2007, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/070216_asia2020.pdf.

7 參見 The White House, “The National Security Strategy of the United States of America,” September 17, 2002, http://nssarchive.us/national-security-strategy-2002.

有可能擦槍走火演變為重大事件。[8]北韓擁有長程彈道飛彈和大規模毀滅性核子武器，於 1998 年試射射程 2,500 公里的大浦洞一號飛彈，直接飛越日本領土上空，對日本構成立即的威脅。其後，北韓自 2006 年起又數度進行地下核子試爆，更增加日本的危機感。至於中國，中國船艦在 21 世紀初突破第一島鏈進行遠海訓練，其海警、民兵船和潛艦則頻繁在東海出沒，其後更在南海造人工島礁，使日本海上交通線之安全備受威脅。因此，日本防衛戰略之重點由原本阻止蘇聯軍隊從北海道登陸為主的「登陸防衛」，轉為防範北韓的「彈道飛彈防禦」，及抵禦中國攻佔日本離島、必要時須奪回周邊島嶼（特別是西南方島嶼）的「周邊海域防衛」。主要防衛能力之建構也由陸上自衛隊轉為以海自和空中自衛隊為主的機動作戰能力，以及其與美軍之聯合作戰能力。[9]

另一方面，911 事件之後，國際上的安全威脅逐漸多樣化，除了恐怖組織之外，包括大規模毀滅性武器之擴散和海盜等的跨國界威脅。日本自古以海洋立國，海上貿易佔其全部貿易之 99.6%，特別是其食物和石油等能源幾乎完全依賴進口。[10]海上交通路線和海運對日本之重要性，從二戰期間美軍對日戰略首在切斷日本海運路線即可窺知一斑。特別是從中東到日本之海運路線，是日本石油輸入的命脈，但是沿線卻存在許多國際恐怖組織或海盜集團，對日本的經濟活動和海洋利用構成莫大威脅。因此，日本政府在 911 事件之後特別注重海洋安全保障，2008 年制訂《海洋基本計畫》，提出為確保海洋安全之艦艇和飛機之整備、相關部門對不明船之共同對處作業和訓練等。同年，自衛艦隊體制和任務全面改編，由第 1 至第 4 護衛艦隊群負責廣範圍海域之作戰任務，第 5 至第 8 護衛艦隊群則以神盾艦為核心負責彈道飛彈之防衛。[11]特別是前述之直升機護衛艦「日向」號於 2009 年服役，成為日本海自作戰範圍擴大和能力大幅提昇之里程碑。

---

8 參見防衛省，〈平成 17 年度以降に係る防衛計画の大綱について〉，《防衛省》，2014 年 12 月 10 日，https://www.mod.go.jp/j/approach/agenda/guideline/2005/taikou.html。

9 參見山下万喜，〈日本の海洋安全保障への取り組み〉，《海幹校戦略研究》，第 2 巻第 2 号増刊，2013 年 3 月，頁 8-14。

10 同前註，頁 11。

11 海上自衛隊幹部学校作戦研究室，〈冷戦後の海上自衛隊の体制と活動の変遷〉，《海幹校戦略研究》，第 7 巻第 2 号，2018 年 1 月，頁 68-70。

第二次安倍政權於 2012 年底成立以後，新的防衛思維明確反映在日本安全保障機制之重大改革上。安倍內閣創設日本版的國家安全會議（National Security Council, NSC）、制訂日本國家安全保障戰略、增加防衛預算、建立《特定秘密保護法》制度、制訂「防衛裝備移轉三原則」、彈性活用政府開發援助（ODA）、修訂「日美防衛合作方針」，以及運用憲法解釋之形式推動「集團自衛權」之行使，其目的是使日本恢復「正常國家」之形貌，且更有能力承擔日美同盟在東亞區域的責任。其中，2013 年訂定的《國家安全保障戰略》，除了以東亞和西太平洋為主要範圍外，為了確保海上航路之安全，也將西亞、印度洋區域納入視野。這些自然都獲得美國政府外交與國防部門之支持。[12]

二、2004 年《防衛計畫大綱》[13]

日本防衛戰略從 2004 年《防衛計畫大綱》起開始出現轉變。首先，日本認為其威脅對象已由傳統的「國家」軍事侵略，轉以「非國家行為主體」之恐怖組織、大規模毀滅性武器和彈道飛彈攻擊等新型態威脅。其次，日本首度表明為了國際社會之和平與安定，將主動且積極地參與國際活動。亦即，「國際安全保障環境之改善」和「不使日本遭受直接威脅，若遭受則能排除並使被害最小化」成為日本安全保障政策的兩大目標。其實踐方式主要是強化日美安保體制、積極參與國際維和活動、確保中東至東亞之海上交通路線安全，以及推動與東南亞各國在反恐和海盜防制等課題上之合作。這是日本首次將海外任務由原先的附帶任務改為主要任務。第三，日本指出朝鮮半島和台灣海峽問題仍存在不確定性，並首度點名北韓和中國值得注意。北韓之核武開發、彈道飛彈和備有大量特殊部隊等軍事活動，成為區域安全保障之重大不安定要素。中國則因推進核子飛彈之戰力、海空軍力之近代化及海洋活動範圍擴大等動向，使日本必須嚴密注意。

---

[12] 北岡伸一，〈「積極的平和主義」に転換する日本の安全保障政策〉，《nippon.com》，2014 年 2 月 5 日，https://www.nippon.com/ja/currents/d00108；矢野義昭，〈安倍政権の安全保障戦略の評価〉，《Intelligence Report》，No.71，2014 年 8 月，頁 17-35，轉引自《日本安全保障戦略研究所（SSRC）》，http://www.ssri-j.com/SSRC/yano/yano-9-20140725.pdf；佐古丞，〈日米同盟と東アジアの安全保障〉，《法政論叢》，第 55 巻第 1 号，2019 年 4 月，頁 129-143。

[13] 同註 8。

為此，2004 年《防衛計畫大綱》雖然部分承續 1976 年以來的「基礎防衛力構想」，但是防衛力整備改以建立「多功能且彈性有效之防衛力」為目標，強調「立即反應性、機動性、靈活性、多目的性、以高度技術力和資訊能力為後盾」，並注重防衛力之綜合運用。在新型態威脅與多樣化事件之應處上，日本提出應建立對彈道飛彈攻擊、受游擊隊或特殊部隊攻擊、島嶼被侵略、周邊海空域之警戒監視、領空受侵犯或武裝工作船侵入、大規模災害之對應能力，並縮減原先冷戰型本土防衛之兵力配置。2007 年，日本更將原為內閣府外局的防衛廳升格為防衛省，開始朝「正常國家」邁進。

因此，海自在 1976 年第一次《防衛計畫大綱》以來以反潛艦艇部隊為主的 4 個機動運用之護衛隊群中，新增 4 艘可實際有效回應彈道飛彈攻擊或武裝工作船、實行國際和平協力活動的護衛艦，組成共 8 艘護衛艦之 4 個護衛艦群。在潛艦部隊方面，雖然維持原本的 16 艘潛艦，但如前已述，部署重心由日本北方的宗谷、津輕和對馬海峽，轉為東海和日本海之海上交通要衝，以防範北韓和中國並維護海上交通路線之安全。[14]

日本政府 2001-2005 年《中期防》之造艦計畫內容，則包括：直升機護衛艦（13,500 噸級）1 艘、大型神盾艦（7,700 噸級）2 艘、「蒼龍」級潛艦（2,900 噸級）1 艘；至 2006-2010 年《中期防》，除了直升機護衛艦（13,500 噸級）1 艘之外，更增加建造「蒼龍」級潛艦（2,900 噸級）4 艘，以及採購 AH-64D 戰鬥直升機 4 架等，以體現日本的新防衛戰略。[15]

三、2010 年《防衛計畫大綱》[16]

2010 年制訂《防衛計畫大綱》時，日本的安全保障目標在原本的「不使日本遭受直接威脅，若遭受則能排除並使被害最小化」和「亞太地區安全保障環境更加安定化和全球安全保障環境之改善」之外，又加

[14] 同註 11。
[15] 內山昭，前揭文，頁 14。
[16] 防衛省，〈平成 23 年度以降に係る防衛計画の大綱について〉，《防衛省》，2010 年 12 月 17 日，https://www.mod.go.jp/j/approach/agenda/guideline/2011/taikou.html。

上第三個目標：「對確保世界和平安定和人類安全保障做出貢獻」，顯示日本在國際安全保障上的角色將越來越重要。

由於日本政府認為日本本土遭受大規模登陸攻擊之可能性很低，防衛力部署重心明顯由北方轉為西南方，防衛構想則由冷戰時期重視「防衛力存在」的「基礎防衛力構想」，全面轉換為重視「防衛力運用」的「機動防衛力」，並更加強調「立即反應性、機動性、靈活性、持續性與多目的性，以高度技術力和資訊力為後盾」，來因應複雜多變之事態。防衛力的角色則分為「有效抑制與應處」、「亞太地區安全保障環境更進一層之安定化」及「全球安全保障環境之改善」三項。其中，在有效抑制與對處方面，日本特別強調平時對周邊各國軍事動向之掌握，保持日本在周邊海空域之情報偵察等優勢，以防範及迅速對應各種突發事變。此外，在離島受攻擊時，日本應該迅速派出可機動運用之部隊，與島上駐軍合力阻止與排除入侵。因此，在離島周邊應建立包含巡弋飛彈應處之防空能力，並確保周邊海空域之航空優勢及海上運輸路線之安全。

另一方面，由於日本擴大參與國際維和活動，使其機動運用之護衛艦隊群的任務近乎飽和。為此，2010 年《防衛計畫大綱》改變地方部隊固守一地之體制，使其可跨警備區活動，也可用於西南部離島之警戒監視或國際維和活動。此外，在原本每個護衛隊群由 8 艘護衛艦組成、共 4 個護衛隊群（32 艘）之外，又組織了每隊由 4 艘新型護衛艦組成、共 4 個護衛隊（16 艘）之地方護衛部隊。這使得海自的護衛艦總數達到 48 艘。在潛艦方面，除了原先部署在東海與日本海之海上交通要衝之外，為了強化日本周邊海空域之情報收集和警戒監視、擴大與長期化國際任務、確保日本之情報優勢，並考量作戰海域與基地之地緣關係等，將潛艦部隊由原本 2004 年《大綱》的 4 個隊擴大為 6 個隊，潛艦數量也由 16 艘增加為 22 艘。[17]這是日本 1976 年以來首次增加潛艦數量，主要目的顯然是防範中國軍事勢力的快速擴張。

[17] 同註 11，頁 72-73。

四、2014 年《防衛計畫大綱》[18]

2014 年《防衛計畫大綱》的重點在於「綜合機動防衛力」之構築，強調陸海空之聯合作戰能力，以因應不斷變化、日益複雜且可能持續和同時發生之各種事態。日本認為其周邊海域和亞太地區安全保障課題之解決，必須依賴國家之間加強合作，特別是在非傳統安全保障領域上。同時，因領土主權和海洋經濟權益所導致的「灰色地帶」事件有長期化傾向，未來可能轉變為更重大事件。日本在此清楚地點名北韓核武器之小型化和彈頭化、在朝鮮半島之挑釁行為等，已成為日本重大且急迫之威脅。同時，中國變本加厲的軍事擴張行動，包括：大幅增加國防預算、阻止他國軍事力接近周邊地區、在東海與南海等海空域之活動急速擴大、嘗試變更現狀、設定「東海防空識別區」妨礙公海上空之飛行自由，以及艦艇與飛機進出東海之常態化、擴大在亞太地區活動領域等，使日本視中國為地區和國際安全保障上的隱憂。[19]

防衛力之角色依然設定為「各種事態之實質抑制與應處」及「亞太地區安定化和全球安全保障環境之改善」。前者應重視之能力項目中，包含了警戒監視、運輸、離島受攻擊時之對處、受彈道飛彈攻擊時之應處等，並新加入太空與網路空間之對處能力。其中，在「離島受攻擊時之對處」上，明確指出為了維持海空優勢，應強化日本遭受飛機、艦艇或飛彈攻擊時之對應能力；同時，若離島受外敵侵略，應強化日本拒敵於海上之綜合防衛力，並建立可迅速登陸、奪回和確保主權之水陸兩棲作戰能力。

此外，為了提升海自對防衛周邊海域之管控、確保海上交通安全及參與國際維和活動等多樣化任務之對處能力，同時追求船體精實化，日本在護衛艦部隊中增加多功能新型護衛艦之數量，並繼續保持神盾級護衛艦、潛艦部隊和掃雷部隊等編制。新型護衛艦由 48 艘增加為 54 艘，而護衛隊數量也由 12 個隊增加為 14 個隊。新型護衛艦之功能，主要是以無人潛具等進行掃雷，以及運用拖曳聲納進行反潛作戰，其搭載裝備

---

[18] 防衛省，〈平成 26 年度以降に係る防衛計画の大綱について〉，《防衛省》，2013 年 12 月 17 日，https://www.mod.go.jp/j/approach/agenda/guideline/2014/pdf/20131217.pdf。

[19] 參見沓脱和人、今井和昌，〈「積極的平和主義」と「統合機動防衛力」への転換〉，《立法と調査》，第349號，2014年2月，頁72-88。

必須可拆卸。另一方面，搭載神盾系統的護衛艦則新增建造 2 艘，成為 8 艘神盾級護衛艦之體制，並將旋翼巡邏機由 72 架增加至 80 架。[20]特別值得注意之點是，為了因應中國侵略離島而進行登陸與奪島作戰，陸上自衛隊也新增了以美國海軍陸戰隊為範本的「水陸機動團」。

五、2018 年《防衛計畫大綱》[21]

2018 年《防衛計畫大綱》是日本 2013 年底制訂《國家安全保障戰略》之後《防衛計畫大綱》的首次調整，被視為是體現日本《國家安全保障戰略》之戰略文書。[22]此次防衛大綱之主幹為「多次元綜合防衛力」之構築，如：太空、網路、電磁等新興空間的防衛能力，同時也進一步強化既有領域之防衛能力。所謂「多次元綜合防衛力」實際上是依據 2014 年《防衛計畫大綱》「綜合機動防衛力」之方向和精神而更加深化，2018 年《防衛計畫大綱》將其分為「新領域」、「既有領域」及「持續性與強韌性」三大類，並詳細指明具體內容。

相應於此，海自體制也做了大幅調整。新編「水面艦艇部隊」由「護衛艦部隊」和「護衛艦、掃雷艦艇部隊」構成。「護衛艦部隊」共 4 個群、8 個隊，每個隊群以 1 艘直升機護衛艦（DDH）和 2 艘神盾級護衛艦（DDG）為中心；「護衛艦、掃雷艦艇部隊」則由新型護衛艦（FFM）與掃雷艦艇編成，共 2 個群、13 個隊。此外，為了強化周邊海域的平時警戒監視，另新編「巡邏艦部隊」。結果，護衛艦體制包含有彈道飛彈防禦能力的神盾級護衛艦 8 艘，以及新型態護衛艦（FFM），總數達到 54 艘。在潛艦部隊方面，則為了強化水底情報偵搜與警戒監視，繼續維持 22 艘體制。[23]

此外，為了強化尖閣群島（釣魚台）周邊領海之警備，日本海上保安廳在 2016 年建立由 2 艘 3,800 噸級直升機搭載巡邏艇和 10 艘 1,000 噸級巡邏艇組成的「尖閣領海警備專從體制」，並建造 6,500 噸級、可

---

[20] 同前註，頁 74-76。

[21] 防衛省，〈平成 31 年度以降に係る防衛計画の大綱について〉，《防衛省》，2018 年 12 月 18 日，https://www.mod.go.jp/j/approach/agenda/guideline//2019/pdf/20181218.pdf。

[22] 齋藤聡，〈新大綱と今後の海上自衛隊について〉，《海幹校戦略研究》，第 9 巻第 1 号，2019 年 7 月，頁 7。

[23] 同前註，頁 11-13。

搭載直升機的大型巡邏艇，以對應中國和北韓船隻在日本領海或經濟海域之活動。[24]

肆、造艦計畫與預算的演變

為了配合防衛戰略之轉換，日本的造艦計畫也做了相應的調整。造艦計畫之內容自 1980 年代後半起都公布於《中期防》內。1986 年以後各《中期防》主要艦艇建造之預計數量可列出如表 1。

表 1 日本歷次《中期防》造艦預計數量

年度	護衛艦	潛水艦	其他	總數
1986	9	5	21	35
1991	8	5	15	28
1996	7	5	18	30
2001	5	5	15	25
2005	5*	4	8	17
2011	1	1	#	#
2014	5	5	5	15
2019	（10）	（5）	（8）	23

資料來源：王綉雯整理自日本防衛省，https://www.mod.go.jp/。
說明：單位為艘；另有 3 艘護衛艦是為對應飛彈防禦系統而改造的護衛艦，未記入。
#2011《中期防》因政權輪替於 2013 年廢止，其後提出新的 2014《中期防》。

[24] 〈尖閣警備に最大級巡視船３隻目の新造方針 海保概算要求〉,《産経ニュース》, 2017 年 8 月 29 日，https://www.sankei.com/economy/news/170829/ecn1708290024-n1.html。

由上表可看出，日本各《中期防》造艦之預定總數，在 2001 年以前都超過 20 艘，但是 2005 年和 2014 年兩次《中期防》（共 10 年）之造艦數量逐漸減少，至 2019 年《中期防》才又增加至 23 艘。

至於實際完成之艦艇數量，以 1986-2015 年各《中期防》而言可顯示如圖 1。各《中期防》之實際造艦數量，在 2000 年以前都在 20 艘上下，其後逐漸減少，但大致維持每次《中期防》（5 年間）約 13-14 艘左右，平均每年新建造 2-3 艘。如前所述，由於艦艇建造之趨勢朝向「集中化」、「大型化」及「高性能化」發展，使得 2011 年《中期防》之護衛艦建造數量（3 艘），約只為 1986 年《中期防》建造數量（9 艘）的三分之一。

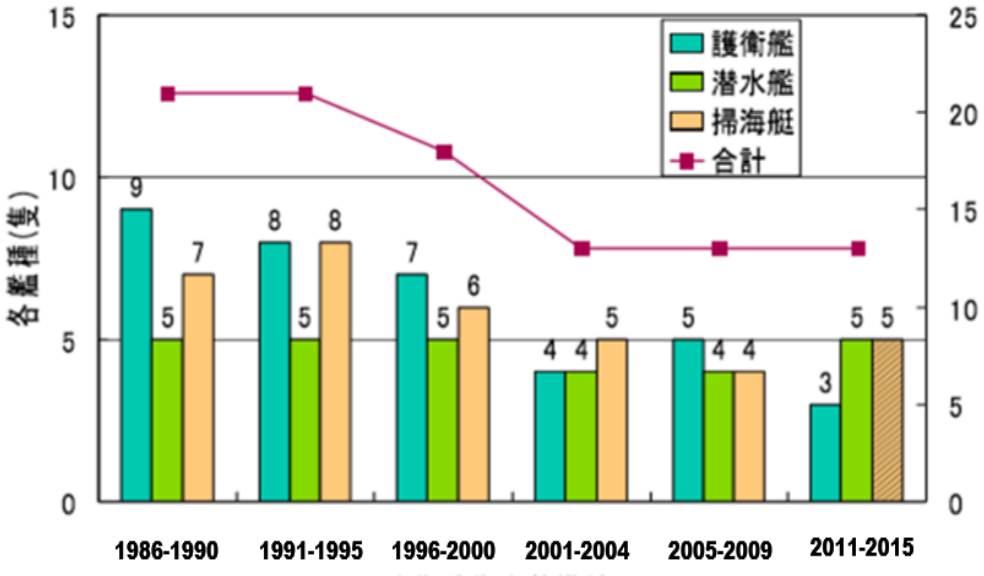


圖 1 日本各《中期防》時實際造艦數量之演變

資料來源：防衛省經理裝備局艦船武器課，〈艦船の生産・技術基盤の現状について〉，《防衛省》，2011 年 3 月，頁 3，https://www.mod.go.jp/j/approach/agenda/meeting/seisan/sonota/pdf/04/001.pdf.

日本造艦計畫當然受防衛預算之變化所影響。以 2006-2015 年這 10 年間的防衛預算來看，2009-2012 年非自民黨政權時期，防衛預算一路下滑，2012 年底第二次安倍政權成立之後，防衛預算才自 2014 年度開始大幅增加（圖 2）。

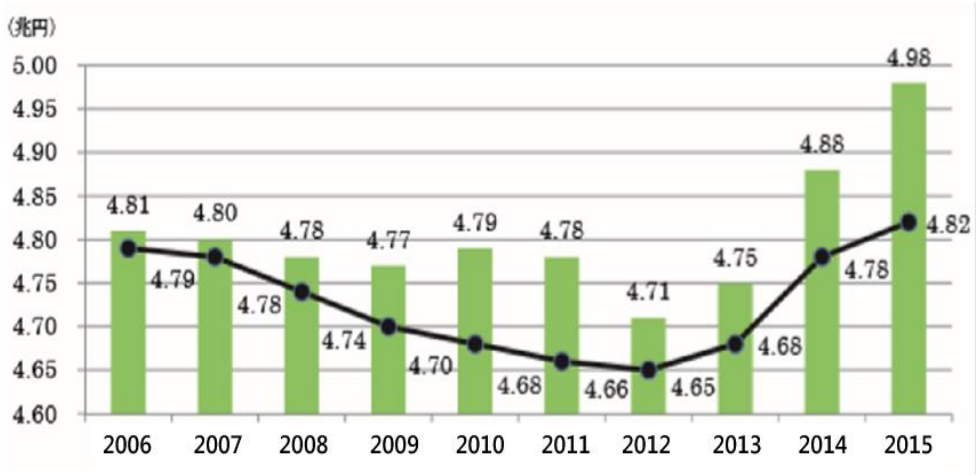


圖 2 日本防衛費 2006-2015 年之演變

資料來源：橫山絢子，〈平成 27 年度防衛関係費の概要〉，《立法と調査》，第 362 號，2015 年 3 月，頁 72。

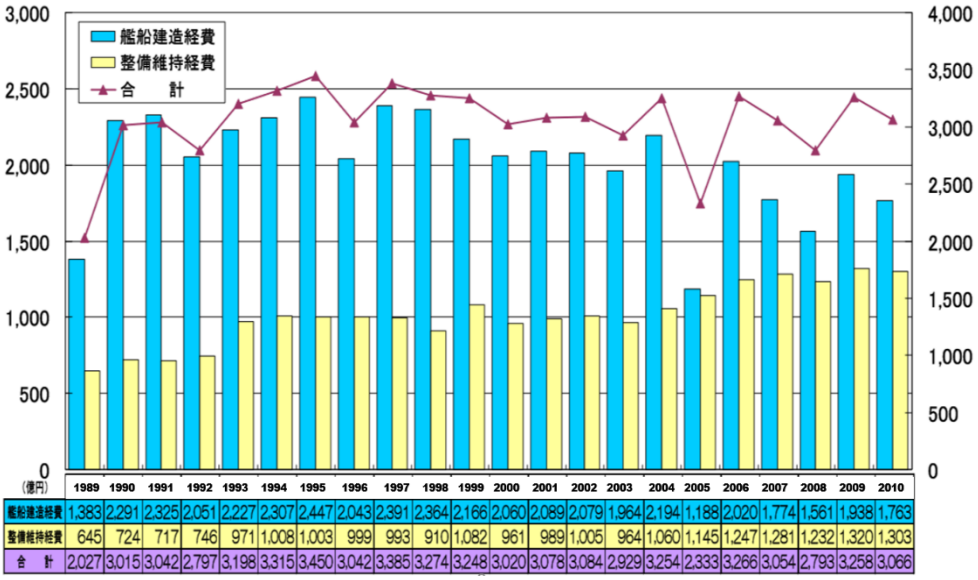
至於造艦預算在防衛費中所佔的比例，以 2011 年至 2016 年而言，大約維持在 5%左右。[25]而在 2003 年至 2012 年度這 10 年間，除了 2005 年度外，大約保持每年 1,800 億日圓左右（參見圖 3）。主要原因除了日本政府財政緊縮之外，和民主黨政權對造艦計畫並不積極也有關，特別是 2009 年民主黨政權成立之後縮減軍事裝備採購數量，加上 2011 年發生東北 311 大地震需要救災重建，防衛預算在 2012 年度降至 10 年內最低。2012 年底自民黨重新執政之後，2013 年度起防衛預算才開始增加，但仍在 GDP1%之限制下，增加幅度不大。另一方面，基於防衛戰略重視西南離島防禦和機動防衛力、武器輸出之規制緩和、[26]中國海軍實力快速增加等因素，日本造艦政策在預算有限之下，不得不朝向「船體大型化」、「裝備高性能化」方向發展，單一艦艇的建造成本大幅增加，造艦目標遂集中在少數類型（特別是多功能護衛艦）上。

所謂「多功能護衛艦」，日本政府指是為執行大規模災害等多樣化

[25] 內山昭，前揭註，頁 24。

[26] 由 1967 年制訂之「武器輸出三原則」轉換為「防衛裝備移轉三原則」。至於日本輸出「蒼龍」級潛艦至澳洲之失敗案例分析，詳見郭育仁，〈從澳洲潛艦個案看日本國防工業改革之挑戰〉，《全球政治評論》，第 55 期，2016 年，頁 85-105。

任務之多功能護衛艦。但是，實質上是針對中國海軍在太平洋和南海積極活動，預計改造「出雲」級直升機護衛艦，使其能夠搭載 F-35B 戰機，以與中國抗衡。雖然日本政府一再聲稱將「出雲」級護衛艦改造為多功能護衛艦，但是其他國家卻都認為這將成為日本戰後首艘的輕型航空母艦。



(億円)	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
艦船建造経費	1,383	2,291	2,325	2,051	2,227	2,307	2,447	2,043	2,391	2,364	2,166	2,060	2,089	2,079	1,964	2,194	1,188	2,020	1,774	1,561	1,938	1,763
整備維持経費	645	724	717	746	971	1,008	1,003	999	993	910	1,082	961	989	1,005	964	1,060	1,145	1,247	1,281	1,232	1,320	1,303
合　計	2,027	3,015	3,042	2,797	3,198	3,315	3,450	3,042	3,385	3,274	3,248	3,020	3,078	3,084	2,929	3,254	2,333	3,266	3,054	2,793	3,258	3,066

圖 3 日本 1989-2010 年度艦艇造修與裝備維修預算之演變

資料來源：日本防衛省，https://www.mod.go.jp/。

2019 年《中期防》之一大特色，是日本造艦數量開始增加。原本每年新造護衛艦 1 艘，至 2019 年《中期防》增為每年新造護衛艦 2 艘、每艘預算 476 億圓，5 年共計新增 10 艘；潛水艦則預定每年新造 1 艘、每艘預算 647 億日圓，共新增 5 艘。其他艦艇之建造單價，如：掃雷艦每艘 162 億日圓、音響測定艦每艘 221 億日圓、海洋觀測艦每艘 203 億日圓等，都所費不貲。再加上現有艦艇之維修、延用和改造，例如：將「出雲號」改裝為輕型航空母艦及油槽船之整備等，未來 5 年之造艦預算每年至少都在 2,000 億日圓以上。[27]相較於 2003 年至 2012 年度平均

[27] 防衛省，〈中期防衛力整備計画（平成 31 年度～平成 35 年度）について〉，《防衛

每年 1,800 億日圓，顯見增加不少。

此外，為了有效掌控近海有領土爭議之離島如釣魚台島，強化周邊海域之防衛能力，日本政府在 2017 年也編列 2,100 億日圓預算給海上保安廳（以下簡稱海保），用以建造可搭載直升機的新式巡邏艦。這筆預算是海保以往造艦預算的 2 倍，主要目的是用於釣魚台附近海域巡邏和監控調查北韓飛彈試射。[28]同時，安倍內閣也積極提供除役的海保巡邏艦給東南亞國家，如：菲律賓、越南等，除了增加海保巡邏艦之汰舊換新外，也可增加日本的國際貢獻和區域安全保障之能量。

伍、造艦產業能力與海事聚落

現代軍艦主要分為「載台」和「酬載」兩大部分。「載台」包括船體、結構、推進系統、航海系統、電力系統、管路系統等；「酬載」則包括偵感系統、武器系統、指揮管制通信情報與電腦系統、戰鬥系統等。因此，軍用造船主要分為造艦、造機、造兵（指武器系統）、電子系統之建造。日本造艦能力與美國旗鼓相當，造兵等能力則受戰後憲法限制無法發展，但是仍具有一定的產製「潛能」。目前除了神盾戰鬥系統仍須依賴美國之外，排水量 6,000 噸、作戰能力約等同於英、德等國海軍主戰兵力的秋月級驅逐艦，全艦含戰鬥系統在內，日本都已具有完全自主的建造能力。

其次，在日美安保體制下，日本軍艦必須裝配美國海軍武器系統，並循美國對外軍售（Foreign Military Sales, FMS）方式獲得。特別是日本水面艦必須採用的美式先進武器系統，如：神盾系統、協同交戰能力（Cooperative Engagement Capability, CEC）、多功能拖曳陣列聲納系統（Multi-Function Towed Array, MFTA）與彈道飛彈攔截能力等，均屬極

省》，2018 年 12 月 18 日，https://www.mod.go.jp/j/yosan/2019/yosan.pdf.；內野洋次郎，〈新防衛大綱・新中期防と平成 31 年度防衛関係費について〉，《財務省》，2019 年 4 月，https://www.mof.go.jp/public_relations/finance/201904/201904f.html。

[28]〈尖閣警備に最大級巡視船３隻目の新造方針 海保概算要求〉，《産経ニュース》，2017 年 8 月 29 日，https://www.sankei.com/economy/news/170829/ecn1708290024-n1.html；〈日本編列史上最大的海巡預算〉，《中時電子報》，2016 年 12 月 13 日，https://www.chinatimes.com/realtimenews/20161213003860-260417?chdtv。

為高價的軍品。美國對外軍售使日本國內防衛產業無法受益，只能聚焦在由造船業工業基礎所支持的造艦上。因此，對日本造船大企業而言，相對於處處受美國掣肘的護衛艦，產製完全不須外求的潛艦，才是日本造艦能力可完全自主的重要品項。

日本造艦產業主要有以下幾項特徵：

一、能力優異的造船重工集團

造艦能力是以堅實的造船產業為基礎，優異的造船工業在電子、造機等產業配合下，才能夠發展出牢靠的造艦工業。日本新船完工量戰後以來一直位居世界第一，直到 2002 年被韓國、2009 年被中國超越，才退居世界第三。近來隨著國際造船市場大幅萎縮和中韓兩國低價競爭，日本造船業面臨嚴峻挑戰，全球市佔率也大幅減少。另一方面，造船業是技術、資本、勞力三者集中型之產業，相關產業還包括：鋼材加工與組合、配管、電裝、塗裝、引擎、機械等。造艦計畫除了使造船業直接受益之外，還會帶動相關電子、引擎、電池、高級製鋼、材料等產業，經濟效益非常龐大。

造船業可說是日本最早集軍、產、官合一的「軍產複合體」。20 世紀初，藉由日本政府提供補助金和提高進口稅、帝國海軍提供海外技術研修機會、購入外國潛艦進行逆向工程等措施，造船大企業如三菱和川崎等發展出先進的軍用造船工業規模，成為日本重工業之核心，也成為日本發動太平洋戰爭之物質基礎。其後的統制經濟體制，更加深日本政府與帝國海軍對民間造船業的介入，除了設置由 13 家造船大廠組成的「造船聯合會」（即今日的「日本造船工業會」），以及全國 5 大地區由中小造船企業組成的各地區「造船協議會」之外，帝國海軍還依據船種，建立起每個造船廠專精特定艦種的造艦體制，並將驅逐艦、魚雷艇、掃雷艇等由中小型造船廠建造。至 1941 年，為了降低造艦成本和進行生產統制，帝國海軍建立了「同型艦艇在同一造船廠連續建造」的生產模式。[29]這樣的造艦傳統在戰後直升機護衛艦（DDH）和神盾級護衛艦

[29] 堅田義明，《日本海軍とアメリカ》，（東京：日本評論社，2011 年），頁 9-17、95-98。

（DDH）之建造時仍持續保持下來。[30]

戰後日本雖然在美軍佔領下進行財閥解體，但是在日本政府大力扶持之下，轉而建立以民營企業為主的軍事工業。其型態是以數家造船重工大企業為首，其下則有眾多供給零件的中小企業。護衛艦主要由三菱重工、日本海事聯合（JMU）、三井 E&S 等各造船大企業負責；潛水艇則由三菱重工神戶廠和川崎重工神戶廠負責。至於掃雷艇、機雷艦、補給艦等其他水面艦艇，則由其他規模更小的造船企業負責。日本艦艇主要分為護衛艦、潛艦、掃雷艇三類，[31]無論哪一類，其生產結構都以眾多供給零件的中小企業為基礎。護衛艦建造體系約有 2,500 家、潛艦約 1,400 家、掃雷艇則約 1,000 家。[32]此種生產體制之最大特點是技術種類齊全且研發與生產能力強，其中許多中小企業更是擁有日本獨一無二的建造技術。

二、造艦能力遠超過採購需求

戰後日本造船能力長期位居世界第一，但是在軍用船舶的研發和建造及艦隊總規模上受到極大的限制。以日立、住友和三菱等 11 家大型造船公司一年造船能力為 1,800 萬噸而言，若比照二戰時期造船數量有 21%為軍艦之比例，海上自衛隊的艦艇數量將遠超過現狀，但是目前只有 2%的產能用於造艦。由於日本軍艦市場之需求不大，軍艦出口又有許多顧慮和限制，日本政府只能以一年更新一艘主戰兵力、一艘潛艦之方式來保持採購。但是，相較於造船大廠之商業需求，日本政府造艦計畫之採購數量可能只是杯水車薪，因此各造艦大廠開始希望能由日本政府主導護衛艦或潛水艦售予海外。[33]

---

[30] 秦尉二郎，〈艦船の就役期間について〉，2014 年 9 月，頁 19-20，《公益財團法人防衛基盤整備協會》，https://ssl.bsk-z.or.jp/kakusyu/pdf/28-2-1boueisyutoku.pdf。

[31] 其他還有巡邏艦、補助艦等，2019《中期防》更增加新型態護衛艦(FFM，或稱為 30DX)。

[32] 防衛省海上幕僚監部，〈海上自衛隊の艦艇における防衛生産・技術基盤に必要な要件〉，《防衛省》，2011 年 3 月 29 日，https://reurl.cc/nzm4mX。

[33] 寺井伸太郎，〈苦境の造船、護衛艦や潜水艦に輸出待望論〉，《日経ビジネス》，2017 年 4 月 12 日，https://business.nikkei.com/atcl/report/15/110879/041100660；日本經濟團體連合會，〈防衛産業政策の実行に向けた提言〉，《日本經濟團體連合會》，2015

然而，日本政府造艦計畫之主要目的，並不是增加造船大廠之營收，而是維持日本全國造艦產業之基礎和能量。如前所述，由於軍艦具備載台和酬載兩大部分，造艦比民間造船需要更專業的技術和人才，一旦因缺乏訂單而造成技術斷層和人才流失，短期內難以恢復。因此，在國際商船市場供給過剩且受中韓兩國夾攻之下，日本政府造艦訂單不但可使造船大廠不必和國際對手競爭、單價相對穩定，還可長期維持造船大廠與相關中小企業一定的工作量。[34]

再者，對造船大廠而言，造艦並不是其經營重心所在，還常被用來調節手中工事進度，因此，無論軍艦排水量之大小，從建造到服役之時間幾乎都是 5 年。[35]但是，建造新型艦艇之首艘艦可帶來同型艦後續建造和維修之訂單。造船大企業一旦獲得新型艦艇首艘艦之訂單，幾乎保證將負責未來同型艦的建造及維修。因此，各造船大廠莫不極力爭取政府造艦之採購訂單。

三、政府直接介入

為了平衡各大財團之利益和維持日本造艦潛力，日本政府直接介入造艦計畫之執行。其所採取的主要政策有「採購公開競標」和「推動聯合建造」。

（一）採購公開競標

至 1998 年為止，日本政府的造艦採購都是依據防衛廳長官之指示來決定採購對象，稱為「長官指示方式」。[36]政府在決定下訂之際，對於希望得到訂單之造船廠商的技術能力、價格等須加以精算，並將艦艇採

年，http://www.keidanren.or.jp/policy/2015/080_honbun.html。

[34] 宗吉道之，〈日本造船業の現状と艦艇調達基盤の維持〉，《防衛取得研究》，第 1 卷第 2 期，2007 年 10 月，頁 9-11；宗吉道之，〈日本造船業の現状と艦艇調達基盤の維持（その２）〉，《防衛取得研究》，第 2 卷第 2 期，2008 年 11 月，頁 1-2。

[35] 同註 28。

[36] 防衛省，〈防衛生産・技術基盤戦略〉，《防衛省》，2014 年 6 月，頁 10，https://www.mod.go.jp/atla/soubiseisaku/soubiseisakuseisan/2606honbun.pdf#search='%E6%BD%9C%E6%B0%B4%E8%89%A6%E5%8F%96%E5%BE%97+%E9%95%B7%E5%AE%98%E6%8C%87%E7%A4%BA。

購基礎之維持、基礎造船廠之確保等因素也納入考量。[37]但是，為了達到國際重視的公共採購之公正性和供給來源之多樣化，造艦採購自 1999 年起改採「公開競標方式」。新年度一開始就針對預定建造之艦艇公開招標，要求競標廠商提供資料，由艦艇技術審查會舉行公聽會，決定其有得標之資格。這種方式使各造船業者必須相互競爭，再加上防衛預算在 2002 至 2012 年間大幅削減，以及日本軍品出口限制等因素，使得 100 家以上的軍需產業廠商退出生產體制或倒閉，導致造艦產業體制大幅重整。

為何造艦採購不適合公開競爭？主要因為艦艇建造過程之特殊性。以新型艦之建造計畫而言，造艦預算提出之前 4-5 年，日本政府即須針對新型艦應具備的性能等進行構想研究和確定研究並做出初估。在新型艦首艘艦建造預算成立之年度，防衛省技術本部必須提出該艦之基本計畫和基本設計。此時，防衛省通常只提供所需性能最低限度的基本事項，其他部分則由造船廠在艦艇設計和技術方面提供短期的人力支援。在長官指示方式下，此短期人力支援契約簽訂之時，可說就內定了新型艦建造廠商。對造船廠商而言，其設計人員和技術人員預先參與新型艦之建造籌畫，可儘早掌握新型艦裝備系統之構想、技術需求，以及技術達成之可能性等，之後可全心全力和防衛省合作，完成該艦之建造。[38]因此，日本政府未來可能必須在「公開競標」和「造艦特殊性」之間加以調整。

（二）推動聯合建造

為了維持整體造艦能力、傳承經驗與開發新技術，以及避免單一大廠獨佔技術，日本政府戰後透過不同類型艦艇的輪流建造，保持主要艦船之建造船廠，並使其具備更先進類型艦艇的建造經驗。例如：一般護衛艦（DD）從 1950 年代起即導入由不同造船大企業輪流建造的方式。至 1990 年代，4,550 噸級「村雨」級反潛驅逐艦之建造更成為顯例。其中 9 艘由五家不同的造船廠承建，川崎重工則提供一些子系統，幾乎讓日本造船工業全部動員。近年來，日本政府更導入聯合建造模式。例如：

---

[37] 秦尉二郎，〈造船界の動向等について—日欧の比較—〉，《防衛取得研究》，第 7 卷第 4 期，2014 年 3 月，頁 7-8

[38] 秦尉二郎，〈艦船の建造技術力について—護衛艦一番艦の建造における設計力〉，《防衛取得研究》，第 6 卷第 3 號，2012 年 12 月，頁 8。

2018 年採購 3,900 噸級新型小型護衛艦時，日本政府要求得標的三菱重工必須以對手三井 E&S 為下包廠商，讓不同的造船大廠合作造艦，以維持日本造艦技術和人才。至於潛艦則分別由三菱重工和川崎重工的造船廠建造，雖然兩廠都具備一年一艘的建造能力，但日本政府還是選擇讓兩家企業各以二年一艘的頻率交替建造，以維持兩個潛艦建造團隊之能量。

日本政府努力維持造艦團隊和提升先進技術，且常年維持著和自身軍備規模不相符的造艦水準，其目的應是著眼於未來能在最短期間恢復海洋強國地位。目前日本的國防預算僅占 GDP 的 1%，如果未來日本如願成為「正常國家」，其造艦潛力將會大量釋放。日本目前可實現全面國產化的最大型戰艦為排水量 5,000 噸級以上的秋月級和朝日級反潛驅逐艦，如果造艦不再受到種種限制，至少有五家造船大廠有能力可立即開始建造該噸級軍艦，日本極有可能依靠此級別的軍艦而迅速擴軍。

然而，日本造艦計畫也有其弱點。和民間造船相似，造艦也容易產生不斷追加預算之情形。以大型直升機護衛艦「出雲號」為例，其下訂時之金額約 784 億日圓，但 JMU 官方網站記載建造成本為 1,139 億日圓，防衛省資料更記載為 1,208 億日圓。除了部分武器系統因向外國採購而受匯率影響之外，造艦預算後續不斷追加之特性恐值得特別注意。又如三菱重工在 2011 年接受歐洲大型客船建造訂單時，每艘建造本預估 500 億日圓，其後不斷追加成本，至最後完工時已高達 2,000 億日圓。此事造成三菱重工嚴重虧損，不得不於 2017 年改革長崎造船廠並大幅裁員。[39]換言之，如果不做好生產成本管理，造艦計畫之預算很可能不斷追加。

另一方面，日本造船／造艦主要以地方中小企業組成的產業聚落之形式進行。依據國土交通省 2016 年度資料，日本造船業年營業額約 2.3 兆日圓、員工人數約 8 萬人。造船相關工業年營業額約 9,700 億日圓，員工人數約 4.7 萬人。造船業者約 90%、船舶用相關產業約 80%，都是

[39] 三菱重工，〈客船事業評価委員会報告〉，《三菱重工》，2016 年 10 月 18 日，頁 7-14，https://www.mhi.com/jp/finance/library/others/pdf/161018_01.pdf。大幅裁員之結果，長崎造船廠工人數在 2018 年減為 1315 人。參見三菱重工，〈有價證券書〉（2018 年度），《三菱重工》，https://www.mhi.com/jp/finance/library/financial/2018.html。

資本額不到 3 億日圓的中小企業，且其建造量之 90%是在地方圈建造、零件國內採購率更佔 80%以上。[40]換言之，造艦計畫之訂單除了增加造船大集團之營收外，其經濟外溢效果更可活化地方產業。日本海事聚落之結構可參見圖 4。

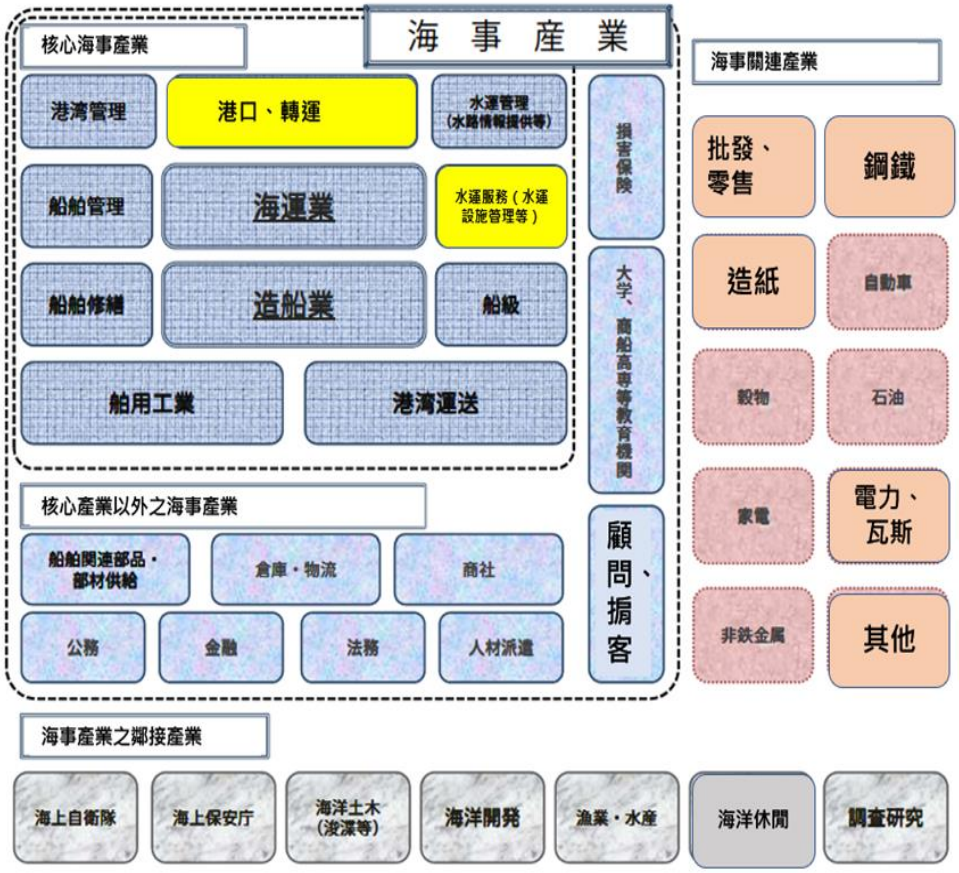


圖 4 日本海事聚落相關產業圖

資料來源：上野繪里子，〈産業連関表と海事クラスター概念〉，《日本海事新聞》，2015 年 12 月，頁 3，http://www.jpmac.or.jp/img/research/pdf/A201510.pdf。

[40] 國土交通省，〈船舶産業分野に係る経営力向上に関する方針〉，《國土交通省告示》（第 865 號），2016 年 7 月 1 日，http://www.mlit.go.jp/common/001136830.pdf。

陸、經濟效益

以地方產業聚落方式進行的造船方式，為地方和日本全國帶來多大的經濟效益？以下以三菱重工長崎造船廠和日本全國為例說明其經濟效益。

一、以三菱重工長崎造船廠為例

長崎是日本歷史悠久的造船重鎮，也是日本與中國、西洋交流之窗口。日本政府於 1855 年在長崎設立海軍傳習所，1857 年為了艦船修理又設立了長崎鎔鐵所（長崎製鐵所），成為日本學習近代造船技術之場域。長崎製鐵所即是三菱重工長崎造船廠之前身，是三菱重工最早也是最主要之造船廠，其造船能力和業績相當可觀。在艦艇建造方面，三菱重工長崎造船廠主要負責建造潛艦和驅逐艦，戰後以來已建造過多種多樣的艦艇，包括：「朝霧號」、「金剛號」、「高波號」等。

三菱重工長崎造船廠之員工數，在 2004 年有 6,299 人。其下包企業共 291 家，以位於長崎市者居多（198 家）。主要業種是製罐板金業（25 家），且多是年營業額 1-10 億日圓之中小企業（172 家），均為創立 50 年-100 年之老企業（125 家）。[41]

造船對長崎當地的經濟效益，依據長崎經濟研究所試算結果，若以 2011 年三菱重工長崎造船廠獲得排水量 12.5 萬噸大型商船 2 艘之訂單來估算，約可產生每年 381 億日圓、全部工期共 1,524 億日圓的經濟外溢效果。

另若依長崎縣政府網站提供的當地經濟外溢效果簡易計算工具來試算，[42]艦艇建造若投入 1,000 億日圓，乘以近年消費轉換率，合計其

---

41 参見株式会社帝国データバンク，〈特別企画：長崎県内における三菱重工の下請先実態調査〉，《帝国データバンク》，2016 年 10 月 18 日，https://www.tdb.co.jp/report/watching/press/s161002_85.html。

42 日本中央政府和許多地方政府的官方網站上，都有運用產業關連表來計算經濟外溢效果的簡易工具。只要在所需類別內輸入「需求金額」，如：訂單金額或造艦金額等，即可自動計算出其相關數據。長崎縣政府網站：〈経済波及効果分析ツール〉，https://www.pref.nagasaki.jp/bunrui/kenseijoho/toukeijoho/renkan/26io/381263.html。

直接效果、第一次間接外溢效果、第二次間接外溢效果，得出該筆投入在長崎當地將可誘發約 622 億日圓的直接生產、281 億日圓的粗附加價值、162 億日圓的勞工所得，並且增加 3,883 人的就業和 3,361 人的雇用。

二、 以日本全國為例

至於造艦對日本全國之經濟效益，依據總務省網站「產業關連表」計算工具來試算，若每年投入 2,000 億日圓，即可產生 5,142 億日圓的經濟外溢效果，約為 2. 57 倍。[43]此外，依據日本海事中心之研究，以國土交通省「2011 年度運輸部門產業連表」為基礎來試算，造船業每投入 1 兆日圓之需求，將誘發 2.5 兆日圓的生產，[44]最終產生近 3 倍的經濟外溢效果。

至於就業機會，如前已述，日本造船業勞工人數約 8 萬人左右。其中，在造船廠內工作之勞工之中，職員加上設計者（白領）約有 15,000 人，工廠內工作者（藍領）約 2 萬人；下包廠商員工則約有 45,000 人。若再加上船舶相關工業所雇用之勞工，全部造船相關勞工總數約在 13 萬人左右。[45]

勞動生產力最簡單之計算方法，是「總產值（總噸數）／投入勞工總人數」。日本造船業員工每人建造量，1989 年是每人 68 噸，2014 年是每人 170 噸 。以 2017 年而論，日本全國新造船總竣工量為 1,307 萬噸，而造船業員工人數為 81,437 人，每人年間生產力約為 160 噸。

另依據 2005 年和 2014 年兩次《中期防》與該當期間日本造船業之相關資料，兩次《中期防》造船業勞工人數之變化可列如表 2。

---

[43] 參見日本總務省網站，〈経済波及効果を計算してみましょう（平成 27 年（2015 年）産業連関表（統合大分類（37 部門））〉，《總務省》http://www.soumu.go.jp/toukei_toukatsu/data/io/hakyu.htm 及 http://www.soumu.go.jp/toukei_toukatsu/data/io/system.htm。

[44] 上野繪里子，〈産業連関表と海事クラスター概念〉，《日本海事新聞》，2015 年 12 月，頁 4-5，http://www.jpmac.or.jp/img/research/pdf/A201510.pdf。

[45] 國土交通省，〈造船市場の現状〉，《國土交通省》，平成 29（2017）年 12 月，https://www.mlit.go.jp/common/001215818.pdf.

表 2 日本 2005 年與 2014 年《中期防》期間造船業勞工人數之變化

期間	造艦計畫總計		新造船完工量／年（萬噸）		造船勞工人數		
	艦數	噸數（萬）	始	終	始	終	增加數
2005 年《中期防》	20	5.9	1752*	2022	77581	85045	+7464
2014 年《中期防》	15	5.2	1342	1307#	78561	81437#	+2876

資料來源：國土交通省，〈造船市場の現状〉，《國土交通省》，平成 29（2017）年 12 月，https://www.mlit.go.jp/common/001215818.pdf。
說明：*.此為 2007 年數據，無 2005 與 2006 年資料；#此為 2017 年資料。

由上表可看出，造艦計畫、年度新造船完工量、勞工人數之變化呈現正相關，證明造艦計畫確實能增加就業。特別是 2014 年《中期防》期間（2014-2018 年），日本正面臨造船業界嚴重不景氣，每年新造船完工數都只能維持在 1,300 萬噸左右，但雇用人數卻能小幅增加，可能就是造艦計畫的雇用效益。

更進一步試算，每萬噸新造船完工量約需勞工 27.6 人。以 2005 年《中期防》為例，（85045-77581）÷（2022-1752）=27. 6。另以上表兩次《中期防》來看，造艦計畫總噸數減少 0.7 噸（5.9-5.2）之同時，造船勞工人數減少 4,588 人（7464-2876）。如果其他條件不變，2019《中期防》預計建造總噸數 6.6 萬噸，正好比 2014《中期防》的 5.9 噸增加 0.7 萬噸，據此推估將可增加約 4,500 人左右的直接勞工（造船廠內勞工）就業機會。

至於間接工作機會，以「造船場外之勞工／造船廠內之勞工」之比例來估算，近年來最低倍數為 2013 年之 42258/23468 = 1.8 倍，因此預估增加的 5,000 人直接員工，至少將間接增加 9,000 人左右的新工作機會。

柒、結論

綜合以上針對日本防衛戰略之轉換、造艦預算和計畫之演變、造艦產業、以及海事聚落和經濟效益之探討，可得出結論如下。

第一，日本造艦計畫之擴大與其安全保障角色之轉變有關。鑑於美國全球戰略之轉換和日本周邊鄰國軍事活動之強化，特別是北韓的核武開發和飛彈試射，以及中國近年迅速擴張海權與增強海軍實力，日本為了維護其領土安全、經濟利益和從中東到東亞之海上交通路線安全，必須維持其海空方面之優勢。此外，隨著日本在國際安全保障方面之角色和任務之擴大，日本也需要能夠遠洋運輸、補給和保護商船安全之船艦。無論是近海防衛或遠洋航行，日本都需要建造質量均佳和高性能的大型船艦與潛艦，並搭載先進的武器系統，這是日本造艦計畫不斷擴大之主要原因。

第二，日本造艦計畫的另一個主要目的，在於維持其國內造船業之造艦或造船能量。造艦訂單雖不能為造船大企業增加鉅額的營收，卻能延續其建造能力與促進研究發展。特別是如上所述，日本造艦之產業結構中，大企業之下還有眾多相關的中小企業，政府的造艦訂單可在最低限度內保持其造艦技術基礎。因此，日本政府通常以輪流方式進行採購。例如：護衛艦向來每年採購 1 艘，至 2019《中期防》，為了強化海洋防衛能力，前所未見地改為每年採購 2 艘。又如潛水艦之採購，也是在僅有的兩家廠商——三菱重工和川崎重工之間輪流採購。

第三，日本各造船大廠都有其專精的造艦領域。由於新型艦首艘之建造，特別是需要尖端技術的主要艦種，幾乎就可以保證後續建造和維修之訂單，各造船大廠莫不積極爭取。此外，鑑於造艦之特殊性，造艦計畫必須採取公私合作夥伴方式進行。日本政府造艦採購之方式無論是長官指示或公開競標，都必須讓民間廠商儘早從基本設計階段就開始參與。但是，近年來由於世界造船產業嚴重不景氣，日本政府已開始要求廠商之間合作造艦。例如：2018 年採購 3,900 噸級新型小型護衛艦時，日本政府已開始要求得標的三菱重工，必須以對手三井 E&S 為下包廠商，讓不同的造船大廠合作造艦，以維持日本造艦之技術和人才。

第四，依據上述歷史數據和試算結果，日本造艦計畫能為地方產業聚落與全國帶來可觀的經濟效益和就業機會。日本造艦計畫每投入 2,000 億日圓，即可在日本全國產生 5,142 億日圓的經濟外溢效果，約為 2. 57 倍。若依據最新公布的 2019 年《中期防》來推算，應可為日本增加 4,500-5,000 個直接就業機會，並可增加約 9,000 個左右的間接工作機會。

參考書目

一、專書

堅田義明，《日本海軍とアメリカ》，（東京：日本評論社，2011 年）。

二、期刊論文

郭育仁，〈從澳洲潛艦個案看日本國防工業改革之挑戰〉，《全球政治評論》，第 55 期，2016 年，頁 85-105。

陳昭羽，〈日本海上自衛隊應對中共海軍威脅之研究─以潛艦發展戰略為例〉，《海軍學術雙月刊》，第 53 卷第 6 期，2019 年 12 月，頁 70-86。

上野繪里子，〈産業連関表と海事クラスター概念〉，《日本海事新聞》，2015 年 12 月，http://www.jpmac.or.jp/img/research/pdf/A201510.pdf。

山下万喜，〈日本の海洋安全保障への取り組み〉，《海幹校戦略研究》，第 2 巻第 2 号増刊，2013 年 3 月，頁 8-14。

内山昭，〈日本·軍事大国論と対抗戦略〉，《大阪經大論集》，第 69 卷第 2 號，2018 年 7 月，頁 7-30。

矢野義昭，〈安倍政権の安全保障戦略の評価〉，《Intelligence Report》，No.71，2014 年 8 月，頁 17-35，轉引自《日本安全保障戦略研究所（SSRC）》，http://www.ssri-j.com/SSRC/yano/yano-9-20140725.pdf。

池田十吾、下平拓哉，〈ブッシュ・ドクトリンと日本〉，《政治研究》，第 9 号，2018 年，頁 11-23。

佐古丞，〈日米同盟と東アジアの安全保障〉，《法政論叢》，第 55 卷第 1 号，2019 年 4 月，頁 129-143。

宗吉道之，〈日本造船業の現状と艦艇調達基盤の維持（その２）〉，《防衛取得研究》，第 2 卷第 2 期，2008 年 11 月，頁 1-2。

宗吉道之，〈日本造船業の現状と艦艇調達基盤の維持〉，《防衛取得研究》，第 1 卷第 2 期，2007 年 10 月，頁 9-11。

沓脱和人、今井和昌，〈「積極的平和主義」と「統合機動防衛力」への転換〉，《立法と調査》，第 349 號，2014 年 2 月，頁 72-88。

海上自衛隊幹部学校作戦研究室，〈冷戦後の海上自衛隊の体制と活動

の変遷〉,《海幹校戦略研究》,第7巻第2号,2018年1月,頁60-78。

秦尉二郎,〈造船界の動向等について―日欧の比較―〉,《防衛取得研究》,第 7 卷第 4 期,2014 年 3 月,頁 1-18。

秦尉二郎,〈艦艇の建造技術力について〉,《防衛取得研究》,第 6 卷第 3 期,2012 年 12 月,頁 1-10。

横山絢子,〈平成 27 年度防衛関係費の概要〉,《立法と調査》,第 362 號,2015 年 3 月,頁 72-79。

齋藤聡,〈新大綱と今後の海上自衛隊について〉,《海幹校戦略研究》,第 9 卷第 1 号,2019 年 7 月,頁 7-17。

三、官方資料

The White House, “The National Security Strategy of the United States of America,” September 17, 2002, http://nssarchive.us/national-security-strategy-2002/.

内野洋次郎,〈新防衛大綱・新中期防と平成31年度防衛関係費について〉,《財務省》,2019年4月,https://www.mof.go.jp/public_relations/finance/201904/201904f.html。

防衛省,〈中期防衛力整備計画(平成 31 年度～平成 35 年度)について〉,《防衛省》,2018 年 12 月 18 日,https://www.mod.go.jp/j/approach/agenda/guideline//2019/pdf/chuki_seibi31-35.pdf。

防衛省,〈平成 17 年度以降に係る防衛計画の大綱について〉,《防衛省》,2014 年 12 月 10 日,https://www.mod.go.jp/j/approach/agenda/guideline/2005/taikou.html。

防衛省,〈平成 23 年度以降に係る防衛計画の大綱について〉,《防衛省》,2010 年 12 月 17 日,https://www.mod.go.jp/j/approach/agenda/guideline/2011/taikou.html。

防衛省,〈平成 26 年度以降に係る防衛計画の大綱について〉,《防衛省》,2013 年 12 月 17 日,https://www.mod.go.jp/j/approach/agenda/guideline/2014/pdf/20131217.pdf。

防衛省,〈平成31年度以降に係る防衛計画の大綱について〉,《防衛省

》，2018 年 12 月 18 日 ， https://www.mod.go.jp/j/approach/agenda/guideline//2019/pdf/20181218.pdf。

防衛省，〈防衛生産・技術基盤戦略〉，《防衛省》，2014 年 6 月，https://www.mod.go.jp/atla/soubiseisaku/soubiseisakuseisan/2606honbun.pdf#search='%E6%BD%9C%E6%B0%B4%E8%89%A6%E5%8F%96%E5%BE%97+%E9%95%B7%E5%AE%98%E6%8C%87%E7%A4%BA。

防衛省，《防衛白書》（令和元年版），《防衛省》，2019 年，https://www.mod.go.jp/j/publication/wp/wp2019/w2019_00.html。

防衛省海上幕僚監部，〈海上自衛隊の艦艇における防衛生産・技術基盤に必要な要件〉，《防衛省》，2011 年 3 月 29 日，https://reurl.cc/nzmA0n。

防衛省經理裝備局艦船武器課，〈艦船の生産・技術基盤の現状について〉，《防衛省》，2011 年 3 月，https://www.mod.go.jp/j/approach/agenda/meeting/seisan/sonota/pdf/04/001.pdf。

長崎縣政府，〈経済波及効果分析ツール〉，《長崎縣政府》，https://www.pref.nagasaki.jp/bunrui/kenseijoho/toukeijoho/renkan/26io/381263.html。

國土交通省，〈船舶産業分野に係る経営力向上に関する方針〉，《國土交通省告示》（第 865 號），2016 年 7 月 1 日，http://www.mlit.go.jp/common/001136830.pdf。

國土交通省，〈造船市場の現状〉，《國土交通省》，平成 29（2017）年 12 月，https://www.mlit.go.jp/common/001215818.pdf。

總務省，〈経済波及効果を計算してみましょう（平成 27 年（2015 年）産業連関表（統合大分類（37 部門））〉，《總務省》，http://www.soumu.go.jp/toukei_toukatsu/data/io/hakyu.html。

總務省，〈経済波及効果を計算してみましょう（平成 27 年（2015 年）産業連関表（統合大分類（37 部門））〉，《總務省》，http://www.soumu.go.jp/toukei_toukatsu/data/io/system.htm。

四、網際網路資料

Amitage, Richard L. and Joseph S. Nye, *The US-Japan Alliance: Getting*

Asia Right through 2020, Center for Strategic and International Studies, February 2007, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/070216_asia2020.pdf.

〈尖閣警備に最大級巡視船３隻目の新造方針 海保概算要求〉,《産経ニュース》,2017 年 8 月 29 日，https://www.sankei.com/economy/news/170829/ecn1708290024-n1.htm。

〈日本編列史上最大的海巡預算〉《中時電子報》,2016 年 12 月 13 日，https://www.chinatimes.com/realtimenews/20161213003860-260417?chdtv。

三菱重工,《有價證券報告書》(2005-2018 年度),《三菱重工》，https://www.mhi.com/jp/finance/library/financial。

三菱重工,《客船事業評価委員会報告》,《三菱重工》,2016 年 10 月 18 日，https://www.mhi.com/jp/finance/library/others/pdf/161018_01.pdf。

日本經濟團體連合會,〈防衛産業政策の実行に向けた提言〉,《日本經濟團體連合會》,2015 年,http://www.keidanren.or.jp/policy/2015/080_honbun.html。

日本防衛省，https://www.mod.go.jp/。

北岡伸一,〈「積極的平和主義」に転換する日本の安全保障政策〉,《nippon.com》,2014 年 2 月 5 日，https://www.nippon.com/ja/currents/d00108。

寺井伸太郎,〈苦境の造船、護衛艦や潜水艦に輸出待望論〉,《日経ビジネス》電子版，2017 年 4 月 12 日，https://business.nikkei.com/atcl/report/15/110879/041100660。

株式会社帝国データバンク,〈特別企画：長崎県内における三菱重工の下請先実態調査〉,《帝国データバンク》,2016 年 10 月 18 日，https://www.tdb.co.jp/report/watching/press/s161002_85.html。

高橋浩祐,〈リチウムイオン電池搭載の海上自衛隊の最新鋭潜水艦「とうりゅう」が進水。韓国も同種の潜水艦を開発中〉,《Yahoo Japan ニュース》,2019 年 11 月 7 日，https://news.yahoo.co.jp/byline/takahashikosuke/20191107-00149842。

秦尉二郎，〈艦船の就役期間について〉，《公益財團法人防衛基盤整備協會》，2014 年 9 月，https://ssl.bsk-z.or.jp/kakusyu/pdf/28-2-1boueisyutoku.pdf。

法國造艦產業的安全與經濟效益

洪瑞閔

博士後研究

國防安全研究院國防資源與產業研究所

摘　要

本文目標在於分析法國造艦產業所帶來的影響。法國在公佈《安全檢討》與《軍事計畫法》之後，「戰略自主」與「歐洲雄心」成為法國國防戰略的主軸，法國政府開始大幅增加包括軍事裝備在內的國防預算。本文發現造艦產業主要為法國帶來兩個層面的影響。在安全層面上，造艦產業強化了法國在政治、作戰與產業層次的「戰略自主」。在經濟層面上，無論是從單一企業的營運、單一艦種的建造、區域產業聚落的形塑與國家產業的發展出發，法國造艦產業均有相當深遠與正面的影響。因此，造艦產業的永續發展對法國來說至關重要。此外，台灣所推動的國防自主政策也能夠在當中得到諸多啟發。

關鍵詞：法國海軍、造艦產業、戰略自主

The Security and Economic Impacts of French Defense Shipbuilding Industry

Jui-Min Hung

Postdoctoral Fellow

Division of National Defense Resources and Industries

Institute for National Defense and Security Research

Abstract

The purpose of this article is to analyze the influence of the defense shipbuilding industry to France. After the publication of *The Strategic Review of Defense and National Security 2017* (*Revue Stratégique de Défense et de Sécurité Nationale*) and *The Military Programming Act 2019-2025* (*La Loi de Programmation Militaire*), the "strategic autonomy" and the "European ambition" became core concepts of France's military strategy. The French government started to increase the defense budget including the expenditure for arms purchases. This article reveals a fact that in the security area, the defense shipbuilding industry reinforces France's strategic autonomy from the political, operational and industrial aspect. The French defense shipbuilding industry has far-reaching impact in the economic domain if one looks at the enterprise operation of major manufacturers, the construction of a particular type of vessel, the establishment of local industries and the development of national industry. It is therefore essential for France to maintain sustainable development of its defense shipbuilding industry. Taiwan, with its national defense self-reliance policy, can also learn lessons from France's experience.

Keywords: *French Navy, Defense Shipbuilding Industry, Strategic autonomy*

壹、前言

法國的國防產業由包括賽峰集團（Safran）、達雷斯集團（Thales）、海軍集團（Naval Group）、奈克斯特（Nexter）、達梭（Dassault）等 500 多家大小國內製造商所組成，這些廠商分布在法國各地的國防產業科技園區（Base industrielle et technologique de défense, BITD）當中。法國國防部長帕莉（Florence Parly）在《2019 年法國軍備出口報告》（Rapport au Parlement sur les exportations d'armement de la France）中指出，今日法國國防產業從業者占了全國工業就業人口的 13%，其中包括約 20 萬的直接就業與 40 萬的間接就業人口，對於法國的國家發展有著重要的影響力。本文嘗試以法國海軍的造艦產業為例，分析其對法國所帶來的影響，考量到法國國防的特殊性，除了傳統的海軍船艦外，法國海軍的核子嚇阻力量也將是本研究討論的範圍。本文將先由法國國防戰略出發，分析法國海軍目前的傳統與嚇阻力量的造艦政策與計畫，最後則探討法國造艦產業所帶來的安全與經濟效益以及其對台灣國防自主政策的啟發。

貳、法國國防戰略指導下的造艦發展

一、《安全檢討》與《軍事計畫法》

2017 年 10 月 13 日法國國防部應總統馬克宏（Emmanuel Macron）所請而發布的法國國防白皮書《2017 年國防戰略與國家安全檢討》（Revue Stratégique de Défense et de Sécurité Nationale，以下簡稱《安全檢討》），指出雖然法國所身處的全球戰略環境與過去相比並未有太大改變，然而既存政治經濟地緣等各項威脅卻有加速與加劇的情形出現。此外，《安全檢討》也列舉出法國現今所面臨到的新形態戰爭與衝突，當中包括了美俄中大國競爭的重返、生化武器的擴散。

在這樣的背景下，《安全檢討》最後主張以「戰略自主」（autonomie stratégique）與「歐洲雄心」（ambition européenne）作為法國國防戰略的兩大主軸。[1]「戰略自主」延續了過去 10 年的戰略基調，包含維持核

[1] Ministère des Armées, "Revue Stratégique de Défense et de Sécurité Nationale," December 2017, pp.52-86.

子嚇阻與高度作戰自主性，使法國能夠面對不同類型與不同區域的威脅與衝突，因此需要有一個相應的全方位外交政策，工業與科技實力以及堅強的作戰能力。「歐洲雄心」則強調考量到當今歐洲面臨到許多共同的威脅與挑戰，歐洲國家應該要共同追求國防戰略的自主性，因此法國將持續投入以歐盟為基礎的雙邊和多邊合作機制，期望能夠使歐洲國防能夠在質量上有顯著提升。

緊接著在 2018 年 11 月 2 日獲得通過的新一期法國國防計畫——《2019-2025 軍事計畫法》(La Loi de Programmation Militaire 2019-2025，以下簡稱《軍事計畫法》) 當中，可觀察到對《安全檢討》主軸的呼應。首先，國防總預算開始大幅度提升。如表 1 所示，法國在未來 6 年的國防支出將以約 5%的比率逐年遞增，法國的國防預算自 2019 年起以每年 17 億歐元的增幅逐步增加，至 2023 年時能夠一舉增加 30 億歐元，達到 440 億的國防年度總預算，國防預算占國民生產毛額（Gross National Product, GDP）的比例希望能夠從 2017 年 1.71%增加至 2023 年的 1.91%，最終在 2025 年達成 2%的目標。因此，相較於先前逐年削減的趨勢，法國國防預算達到冷戰結束 30 年以來的最高水準。[2]

表 1 法國軍備預算佔整體年度國防預算比例

	2019	2020	2021	2022	2023	2024	2025	總計
國防預算	35.9	37.6	39.3	41.0	44.0	-	-	197.8
軍備預算	19.5	20.8	22.3	23.7	26.1	28.8	31.5	172.8
佔比	54.3%	55.3%	56.7%	57.8%	59.3%	-	-	-

資料來源：Ministère des Armées, “La loi de programmation militaire 2019/2025 – Rapport annexé,” 2018, p. 60.
說明：單位為十億歐元，%。

[2] 相較於 2012-2017 年法國國防預算皆維持在 1.4%-1.5%的 GDP 比例。

隨著國防總預算的增加，軍備預算也隨之提升，所占比例逐年增加至將近六成。2019 至 2025 年間法國預計將投入超過 1,700 億歐元預算於軍備開發、建造與更新。法國政府認為當潛在敵人擁有越來越精良武器的同時，法國海軍不只需要彌補既有能力的不足，也需要發展新科技，因此具備雄厚財政實力以取得更多新式裝備有其必要性，以下就《軍事計畫法》中的法國海軍造艦計畫分為傳統力量與嚇阻力量的部分作一說明。

二、傳統力量的發展

法國海軍艦隊傳統部分的主要力量包括 64 艘各式戰艦，包括 1 艘航空母艦、17 艘巡防艦、3 艘兩棲突擊艦、6 艘警戒護衛艦、4 艘多任務艦、15 艘掃雷艦等。除此之外，還有 3 艘補給艦、42 艘各式附屬船艦、33 艘小型船艦、8 艘教學船艦。法國海軍艦船主要部署在本土，另有少部份則負責保護海外領地之任務，目前法國海軍的主要造艦計畫可分述如下：

（一）阿基坦級多用途巡防艦（Frégate multi-missions, FREMM *Classe Aquitaine*）

由法國海軍集團與義大利船廠芬坎蒂尼（Fincantieri）合作開發的阿基坦級多用途巡防艦是法國海軍的骨幹，其用來取代包括土維爾級（*Classe Tourville*）、卡薩爾級（*Classe Classe Cassard*）、喬治萊格級（*Classe Georges Leygues*）在內的舊型船艦。整個計畫共投入 70 億歐元，[3]將會建造 8 艘，其中 6 艘將以反潛作戰為主，另外 2 艘則強化防空能力。目前法國海軍已經取得了 5 艘反潛型阿基坦級，預計將在 2022 年全數交艦。

（二）中型通用巡防艦（Frégates de taille intermédiaire, FTI）

投入 38 億歐元的中型通用巡防艦造艦計畫不但將逐步取代拉法葉級（*Classe La Fayette*）巡防艦成為法國水面艦隊主力艦，其體積大小

[3] Matthieu Maury, “Les frégates FREMM sur de bons rails chez DCNS,” *L’Usine Nouvelle*, October 9, 2009, https://www.usinenouvelle.com/article/les-fregates-fremm-sur-de-bons-rails-chez-dcns.N118921.

也能夠滿足出口的需求。第一艘中型通用巡防艦預計將在 2023 年交付給法國海軍，2025 年時取得第二艘，最終在 2030 年 5 艘全數服役。[4]

（三）昂特卡斯托級多任務艦(Bâtiment Multi-Mission, B2M *Classe d'Entrecasteaux*）

昂特卡斯托級多任務艦主要用以確保法國海外領地的相關利益，其中包括專屬經濟區（Exclusive Economic Zone）的保護、警戒與補給支援等任務。昂特卡斯托級由法國船廠 Kership 承建，[5]目前已經有 4 艘服役，分別派駐在新喀里多尼亞（Nouvelle-Calédonie）、大溪地（Tahiti）與留尼旺（Réunion）、馬丁尼克（Martinique）等島嶼。

（四）羅亞爾級支援艦（Bâtiments de soutien et d'assistance métropolitains, BSAM *Classe Loire*）

同樣由 Kership 負責的羅亞爾級支援艦建造計畫，目標除了在於逐步汰除各類老舊支援艦艇外，尚肩負確保海軍三項重要任務進行之使命：1.力量支持，包括船隻牽引、水面艦與潛艦護航、軍事演練；2.海洋保護，包括海上護衛、船隻援救、打擊海上汙染；3.區域支援，包括海上工程支援、海洋調查協助、運輸與補給。羅亞爾級支援艦建造計畫始於 2010 年，法國海軍目前已取得 4 艘。

（五）新式後勤補給艦（Flotte logistique, FLOTLOG）

後勤艦隊計畫目標在於建造 4 艘新式後勤補給艦，用以取代既有的油料補給艦，以確保法國海空作戰群在遠離本土的海外作戰，其後勤補給能夠無虞、符合相關國際規範並提升作戰的自主性。與阿基坦級多用途巡防艦相同，新式後勤補給艦的計畫由法國海軍集團與義大利芬坎蒂尼共同承建，內容包括：1.相關艦艇的設計、研究與發展。2.建造 4 艘可載運固液態物資（油料、彈藥與食物）的新式後勤補給艦。3.相關支援系統的開發。後勤艦隊計畫將投入 17 億歐元，前兩艘船艦預計在 2025

[4] "La nouvelle frégate de la marine française est enfin dévoilée," *Captial*, October 18, 2016, https://www.capital.fr/entreprises-marches/la-nouvelle-fregate-de-la-marine-francaise-est-enfin-devoilee-1176347.

[5] Kership 由海軍集團與專精中型船艦建造的 Pirou 公司共同出資成立，分別持有 45%與 55%的股份。

年交艦，目標則是在 2030 年時建成 4 艘。[6]

綜合來說，法國海軍傳統部分的造艦計畫呼應了《安全檢討》兩大主軸「戰略自主」與「歐洲雄心」。一方面新一代核動力攻擊潛艦、新式後勤補給艦的開發製造，顯示出法國希望能夠持續強化其長期獨立在外作戰的能力，另一方面，與義大利合作開發的阿基坦級多用途巡防艦、新式後勤補給艦兩大計畫，顯現法國不僅希望「戰略自主」，也想在歐盟層次有所作為，同時藉由造艦案的夥伴關係使歐洲在國防戰略上更加獨立。軍備預算的增加使法國軍隊部在財政資源運用上相當充裕，這又直接反映在交艦的時間表上；大多數計畫中的船艦均能夠在 2025 年以前完成（見表 2）。

表 2 法國海軍傳統部分的主要造艦計畫與交艦數量時間表

船級	2020 年初數量	2020-25 交艦數量	2030 建軍總數
阿基坦級 FREMM	5	8	8
中型通用巡防艦 FTI	0	2	5
昂特卡斯托級 B2M	4	0	4
羅亞爾級 BSAM	4	0	4
新式後勤補給艦 FLOTLOG	0	2	4

資料來源：Ministére des Armées, *op.cit.*, 2018, pp.41-43.
說明：單位，艘。

三、嚇阻力量的發展

法國對於嚇阻力量的發展肇始於 1950 年代，主要動機來自三個方面。首先，在美國、蘇聯與英國相繼取得核子打擊力量後，作為世界強權之一的法國認為身為聯合國安理會的五強之一也應該要擁有。再者，在歷經 1962 年蘇伊士運河危機（Suez Crisis）危機之後，巴黎深刻的體

[6] "France officially orders four FLOTLOG replenishment ships under €1.7 b contract," *Navaltoday.com*, January 31, 2019, https://navaltoday.com/2019/01/31/france-officially-orders-four-flotlog-replenishment-ships-under-e1-7-b-contract.

認到華盛頓並不是個可靠的盟友，上述原因促使法國積極投入核子武器的開發以作為其嚇阻力量的基礎。第三，在法國傳統的國防戰略思考中，他們將核子嚇阻力量視為一種避免全面戰爭爆發的一種政治性工具。[7]

在二次世界大戰的英雄與法國第五共和（Fifth Republic）的首任總統戴高樂（Charles de Gaulle）的大力推動下，法國先是在 1945 年成立「原子能和替代能源委員會」（Commissariat à l'énergie atomique et aux énergies alternatives, CEA）開始進行原子能的研究，在 1960 年成功試爆第一枚核子武器後，法國成為世界第 4 個擁有核子武器的國家，戴高樂更以此為後盾在 1967 年選擇退出「北大西洋公約組織」（North Atlantic Treaty Organization, NATO）的作戰指揮機制，尋求法國在國際舞台上的獨立自主。然而，一直要到 1980 年代法國才擁有成熟的核子嚇阻力量，其中包括核動力攻擊潛艦（Sous-marins nucléaires d'attaque, SNA）、核動力彈道飛彈潛艦（Sous-marin nucléaire lanceur d'engins, SNLE）與潛射彈道飛彈所構成的海洋核武嚇阻能力（composante océanique）以及由颶風戰鬥機（Rafale）與中程空對地核打擊飛彈（Air-Sol Moyenne Portée）所構成空中核武嚇阻能力（composante aéroportée）。

儘管近年來由於恐怖主義等新型態威脅的崛起使得核子武器的嚇阻性受到質疑，但巴黎當局並未因此停止嚇阻力量的建構。目前法國海軍艦隊嚇阻部分由 6 艘紅寶石級（Classe Rubis）核動力攻擊潛艦、4 艘配有 M-51 潛射彈道飛彈的第二代彈道飛彈核潛艦凱旋級（*Classe Le Triomphant*）所組成。如同表 3 所示，《軍事計畫法》中規劃興建敘佛倫級（*Classe Suffren*）核動力攻擊潛艦作為法國戰略海洋部隊（la force océanique stratégique, FOST）的一部分，用來取代即將逐步退役的紅寶石級核動力攻擊潛艦以確保在作戰時的可信度。敘佛倫級核動力攻擊潛艦由法國海軍集團負責整體建造，法國核能公司阿海琺（Areva TA）負責核子反應爐，第一艘已於 2007 年開始建造並在 2019 年 7 月交艦，法國海軍預計在 2025 年取得 4 艘敘佛倫級核動力攻擊潛艦，目標在 2030 年能夠配備 6 艘該型潛艦。

---

[7] Pascal Drouhaud, "La dissuasion nucléaire de la France et l'environnement international," *Guerres mondiales et conflits contemporains*, No. 223, March 2006, p.139.

此外，第三代彈道飛彈核潛艦（Sous-marin nucléaire lanceur d'engins de troisième generation, SNLE 3G）的開發正在進行中，預計在 2023 年開始建造，2030 年首艘能夠投入運作，此型潛艦預估壽命長達 50 年，可確保法國的海洋核子嚇阻力量至 2080 年。[8]同時 M51 潛射彈道飛彈的升級計畫 M51.3，希望能夠在 2025 年投入運作。整體而言，《軍事計畫法》預計在裝備購置預算方面於 2019 年至 2023 年間投入 250 億歐元進行研發與製造以確保法國核子嚇阻力量的常駐。[9]

表 3 法國海軍嚇阻部分的主要造艦計畫與交艦數量時間表

船級	2019 年初數量	2019-25 交艦數量	2030 建軍總數
敘佛倫級 *Suffren*	0	4	6
第三代彈道飛彈核潛艦 SNLE 3G	0	0	1

資料來源：作者整理自 Ministére des Armées, *La loi de programmation militaire 2019/2025 – Rapport annexé* 與法國國防部網站 https://www.defense.gouv.fr.
說明：單位，艘。

總而言之，從法國海軍的造艦計畫內容可以看出，其目標在於回應《安全檢討》的需求，以警覺性、共同作戰能力、穩定性、持久力、回應能力以及卓越能力等六項指標做為指導原則。[10]藉由新式船艦的建造達成現任法國海軍參謀長普拉澤（Christophe Prazuck）所稱之「尖端海軍」（une marine en pointe）。[11]

---

[8] Olivier Mélennec,"Économie de la mer. SNLE 3G : la mise en chantier prévue pour 2023," *Ouest France*, October 26, 2018, https://www.ouest-france.fr/economie/economie-de-la-mer/economie-de-la-mer-snle-3g-la-mise-en-chantier-prevue-pour-2023-6038236.

[9] Ministère des Armées, "La loi de programmation militaire 2019/2025 – Rapport annexé," July 2018, p.62.

[10] Bernard Rogel, "Enjeux et défis stratégiques de la Marine nationale," *Revue Défense Nationale*, No. 789, April 2016, pp.14-16.

[11] Christophe Prazuck, "STRATÉGIE : Le plan Mercator de la Marine nationale," *Association de soutien à l'armée française*, December 17, 2018, https://www.asafrance.fr/item/le-plan-mercator-de-la-marine-nationale.html.

參、造艦產業的安全效益

毫無疑問的，法國造艦產業蓬勃發展所帶來最重要的安全效益，正是在《安全檢討》與《軍事計畫法》當中不斷重申的「戰略自主」，以下將分別從「戰略自主」的概念發展以及造艦產業所能帶來的政治、作戰與產業等層面的「戰略自主」一一分析之。

一、「戰略自主」的概念發展

「戰略自主」首次出現於 1994 年 6 月的法國國防白皮書當中，其被視為是法國國防戰略思考的核心，包括幾項關鍵能力的掌握，如戰場資訊的蒐集、整體情勢的掌握以及戰略機動性維持。[12]在《安全檢討》中，「戰略自主」依舊是法國國防政策的主要目標之一，其所代表的是在不穩定與不確定的國際體系中，國家單獨行動與進行決策以捍衛自身利益的能力。法國的「戰略自主」具有兩大特色。首先，「戰略自主」是依情況而定的，不但取決於主事者想要進行何種戰爭，也隨著戰爭的場域與型態而有所不同。例如，在歐洲進行的反恐戰爭與在非洲所進行的維和任務所需要考慮的條件會有所不同，而國家間進行的領土戰爭也必定會和網路作戰所要考量的因素有所差異。因此，絕對的「戰略自主」並不存在，在沒有清楚的脈絡描述之狀況下，探討「戰略自主」是沒有意義的。此外，「戰略自主」是相對的，我們可以將「戰略自主」區分成很多細部項目，例如，一個國家可以擁有進行一個危機處理的軍事行動的自主性，但是這種自主性是有限制的，它可能在許多方面（情報、行動、補給等等）仍然需要依賴它國程度不一的協助。

二、政治層面的「戰略自主」

藉由海軍傳統與嚇阻力量的建設將強化政治自主，其代表的不僅只是做一國想做的事，還能夠依照一國所設定的規則來行事，換言之，海軍船艦的建設將使得法國得以自由地制訂戰略計畫、行動的目標與活動的內容，確保國防領域的決策制定與執行能力並不會被其他的強權所阻撓。完整的海軍建設也能夠確保法國的關鍵利益免於外國勢力的威脅與侵害，並且對其在「北大西洋公約組織」（North Atlantic Treaty

[12] Ministère de la Défense, “Livre Blanc sur la Défense,” June 1994, pp.52-53.

Organization, NATO）與「歐洲聯盟」（European Union, EU）的盟邦安全做出貢獻。

三、作戰層面的「戰略自主」

藉由海軍傳統與嚇阻力量的建設能夠促進「作戰自主」，其代表的是在一段時間內自主地進行軍事行動的能力，擁有專屬的海軍傳統與嚇阻力量就能夠具備計劃與執行作戰任務的能力，也能夠確保後勤補給上的安全。法國海軍所具備的航空母艦、核動力攻擊潛艦與核動力彈道飛彈潛艦等即能夠帶來此種作戰效益，這些船艦均可以長期在海外作戰而不需依賴它國的協助，能夠完成巴黎當局所指派的各種作戰任務。

四、產業層面的「戰略自主」

依靠海軍傳統與嚇阻力量的建設可以支持產業自主，其代表的是關鍵技術的掌握，對於國家來說，這些關鍵技術使其具備生產執行軍事行動所需裝備之能力，法國可以不必花費高昂成本透過國外取得，因此就得以免除與他國合作的可能爭端，更毋須擔心需要得到他國允許方能獲得的窘境，從設計到出口能夠完全地憑藉一己之力完成。對於造艦產業來說，關鍵技術使它們得以在全球市場上競爭，造就一個專門的產業鏈誕生，其中包括設計、生產、操作、應用、維護、修正與出口等等面向，擁有完整的造艦產業體系就能夠帶動國家收入與製造就業機會。

肆、造艦產業的經濟效益

近年來，法國在武器出口上有著日益亮麗的表現，根據斯德哥爾摩國際和平研究所（Stockholm International Peace Research Institute, SIPRI）的資料顯示，法國的武器出口在 2015 至 2019 年間佔全球武器出口的 7.2%，與 2010 至 2014 年間相較大幅成長了 72%，包括埃及、卡達與印度都是其主要的出口對象，僅次於美國與俄羅斯居世界第三位。[13]因此，軍備生產的經濟效益成為法國政府目前在推動國防產業發展時相當強

[13] "USA and France dramatically increase major arms exports; Saudi Arabia is largest arms importer, says SIPRI," *SIPRI,* March 9, 2020, https://www.sipri.org/media/press-release/2020/usa-and-france-dramatically-increase-major-arms-exports-saudi-arabia-largest-arms-importer-says.

調的部分，在造艦產業部分，如表 4 所示，軍艦出口在 2019 年為法國帶來 3.98 億美元的收入，與 2018 年相較有著飛躍式的成長。

表 4 法國 2018 至 2019 年軍備出口情況

	2018	2019	Total
戰機	904	1880	2785
防空系統	115	60	175
裝甲車	71	65	136
大砲	52	12	64
發動機	70	152	222
飛彈	344	598	943
海軍武器	10	20	30
其他	10	10	20
衛星	50	0	50
感測器	125	172	297
船艦	21	398	419
總計	1773	3368	5141

資料來源：斯德哥爾摩國際和平研究所。
說明：單位為百萬美元。

除了出口所帶來的外匯收入，法國造艦產業與經濟發展之間的緊密性相當明顯，以下將就單一企業、單一艦種的建造、區域產業聚落的形塑、國家產業的發展等四個層面說明之。首先將探討法國海軍最主要承包商法國海軍集團的經濟貢獻，第二將討論法國海軍主要造艦計畫所帶來的效益。第三則將聚焦在布列塔尼大區（Bretagne）與羅里昂市（Lorient）以分析造艦產業對這些地區所帶來的社會與經濟效益。最後則論述整個「海洋嚇阻產業」（La Filière Industrielle Composante Océanique de la Dissuasion）對法國整體經濟之影響，也就是核動力攻擊潛艦、核動力彈道飛彈潛艦與潛射彈道飛彈的設計、建造與維護帶來的效益。

一、單一企業的營運：法國海軍集團的貢獻

1631 年創立擁有悠久歷史的法國海軍集團一直是法國公務船造船產業的主要承包商，負責絕大多數的海軍建造計畫。[14]2007 年法國海軍集團與法國航太國防集團達雷茲（Thales Group）的聯合是法國造船產業的關鍵性時刻，在法國政府的主導之下，雙方進行資本的整合，由達雷茲集團購入法國海軍集團 25%的股份。同時還有著部門的整合，法國海軍集團買下達雷茲集團分公司達雷茲船舶（Thales Naval）的除了裝配部門以外的大部分部門，彼此之間也共同成立許多合資公司以參與各項計畫。[15]法國政府採取這些動作除了是為了要籌備當時第二艘航空母艦的興建，更反映出將國防產業加以結合以做為歐洲國防產業整合基石的企圖心。

法國海軍集團在重組過後便成為法國國防產業海軍部門的領導者與法國海軍水面艦與潛艦建造計畫唯一的主導者。法國海軍集團帶來了大量的就業機會，在法國本土雇用了 13,612 名員工，佔法國造船產業從業人數的 32.4%。[16]在海外市場，亮麗的出口表現是法國海軍集團為法國經濟所帶來的另一貢獻，單就 2019 年上半年而言，法國海軍集團就已在國際上贏得超過 32 億歐元的合約（見表 5）。因此，法國海軍集團的存在除了確保約其 13,000 名勞工的就業機會以外，對於自 2003 年以來便長期處於貿易逆差狀態的法國來說，法國海軍集團所得到的外銷訂單不可不謂一個亮眼且重要的國家收入來源。

---

[14] 海軍建造與武器局（Direction des constructions et armes navales, DCAN）、海軍建造局（Direction des constructions navales, DCNS）是海軍集團的前身，在 2017 年時改為現稱。

[15] 如參與第二艘航母建造的 MOPA2，負責 FREMM 出口的 Armaris。

[16] Naval Group, *Rapport financier 2018*（Paris : LABRADOR, 2019）, p.68.

表 5 法國海軍集團 2019 年 1 月至 7 月外銷成果一覽表

時間	國家	金額	內容
2 月	澳洲	3.61 億歐元	12 艘「短鰭梭魚級」（*Shortfin Barracuda class*）潛艦的設計部分
3 月	比利時/荷蘭	1.8 億歐元	12 艘獵雷艦
3 月	阿拉伯聯合大公國	7.5 億歐元	2 艘「追風級」（*Gowind*）護衛艦
7 月	羅馬尼亞	12 億歐元	4 艘「追風級」護衛艦與 2 艘 22 型（type 22）巡防艦的升級

資料來源：作者整理自 Franz-Stefan Gady, "Australia, France Sign $35.5 Billion Submarine Contract," *The Diplomat*, February 11, 2019, https://thediplomat.com/2019/02/australia-france-sign-35-5-billion-submarine-contract; Anne Bauer, "Naval Group s'impose en mer du Nord dans la guerre des mines," *Les Echos*, March 15, 2019, https://www.lesechos.fr/industrie-services/air-defense/naval-group-simpose-en-mer-du-nord-dans-la-guerre-des-mines-1001024; Michel Cabirol, "Emirats Arabes Unis : et un nouveau contrat important à l'export pour Naval Group," *La Tribune*, June 7, 2019, https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/emirats-arabes-unis-et-un-nouveau-contrat-important-a-l-export-pour-naval-group-812087.html; Michel Cabirol, "Si, si Naval Group déclaré vainqueur... en Roumanie," *La Tribune*, July 2, 2019, https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/si-si-naval-group-declare-vainqueur-en-roumanie-822378.html.

二、單一艦種的建造

法國海軍主要造艦計畫所能夠帶來的經濟效益可呈現如表 6，分述如下：

（一）敘佛倫級核動力攻擊潛艦

整個敘佛倫級核動力攻擊潛艦從設計、建造到維護將投入79億歐元。每一艘潛艦包含800萬人力工時，將會為法國海軍集團與一百多個承包商分別帶來2,000與500個直間接工作機會，[17]涉及諾曼第（Normandie

[17] Vincent Lamigeon, "Dans l'antre du nouveau sous-marin nucléaire français Barracuda," *Challenges*, December 5, 2018, https://www.challenges.fr/entreprise/defense/dans-l-

）、羅亞爾河（Pays de la Loire）、普羅旺斯-阿爾卑斯-蔚藍海岸（Provence-Alpes-Côte d'Azur）、新阿基坦（Nouvelle-Aquitaine）、布列塔尼（Bretagne）與法蘭西島（Île-de-France）等六個大區。[18]

（二）阿基坦級多用途巡防艦

從 2006 年到 2022 年，整個多用途巡防艦建造計畫將投入 70 億歐元。整個計畫包含 5 千萬人力工時，[19]平均每艘阿基坦級代表約 417 萬人力工時，將會為法國海軍集團與其承包商帶來 2400 個工作機會，涉及諾曼第、布列塔尼與法蘭西島等三個大區以及布雷斯特（Brest）、瑟堡（Cherbourg）與羅里昂等城市，[20]這些地區超過一半以上的在地承包商都會受益，包含船舶維修與保養企業 Timolor、氣動與液壓技術商 ADES Technologies、與船舶技術公司 Navtis 等等。[21]

（三）中型通用巡防艦

中型通用巡防計畫艦計畫將投入 38 億歐元。[22]整個計畫包總共含 400 萬人力工時，其中設計與建造階段各自需要 40 萬與 200 萬人力工時。[23]在 2015 年到 2025 年間將會為法國海軍集團有關部門帶來工作機會，主要涉及布列塔尼的洛里昂與南特（Nantes）等地區。[24]

---

antre-du-nouveau-sous-marin-nucleaire-barracuda_629916.

18 "L'impact économique du programme Barracuda," *Ministère des Armée de la France*, August 6, 2010, https://www.defense.gouv.fr/english/marine/dossiers/barracuda/l-impact-economique-du-programme-barracuda.

19 Matthieu Maury, op. cit.

20 "Le CEMM au lancement de la construction de la FREMM Provence," *Ministère des Armée de la France*, December 16, 2010, https://www.defense.gouv.fr/english/marine/a-la-une/le-cemm-au-lancement-de-la-construction-de-la-fremm-provence.

21 "FREMM: le plus grand programme naval militaire européen," *DCNS*, 2010, https://www.naval-group.com/wp-content/uploads/2010/10/DCNS_DP_FR.pdf.

22 "DCNS Lorient fabriquera cinq frégates intermédiaires," *Le Télégramme*, April 21, 2017, https://www.letelegramme.fr/morbihan/lorient/defense-dcns-lorient-fabriquera-cinq-fregates-intermediaires-21-04-2017-11484424.php.

23 "Programme de frégates de taille intermédiaire: DCNS se félicite de l'annonce de la notification du marché par le Ministère de la Défense," *Naval Group*, April 21, 2017, https://www.naval-group.com/wp-content/uploads/2017/04/cp-notification-fti_def-1.pdf.

24 "Construction navale. DCNS est en ordre de marche," *Ouest France*, June 6, 2015, https://www.ouest-france.fr/economie/economie-de-la-mer/construction-navale-dcns-est-en-ordre-de-marche-4473741.

（四）羅亞爾級支援艦

羅亞爾級支援艦建造計畫將投入 1 億 6 千萬歐元，共計 100 萬人力工時，因此單一支援艦的造價為 4 千萬元與 25 萬個人力工時的需求，將會為法國海軍集團與其承包商分別帶來 150 個與 300 個工作機會，分布於布列塔尼大區的孔卡爾諾（Concarneau）與拉內斯泰爾（Lanester）等地。[25]

表 6 法國主要造艦計畫成本效益分析表

	排水量/噸	預算	單位造價	人力工時	創造職缺
敘佛倫級 *Suffren*	浮航 4,650 潛航 5,300	79 億歐元	13.3 億歐元	800 萬小時	420
阿基坦級 FREMM	6,000	70 億歐元	8.5 億歐元	417 萬小時	300
中型通用巡防艦 FTI	4,250	38 億歐元	7.6 億歐元	240 萬小時	-
羅亞爾級 BSAM	2,960	1.6 億歐元	4 千萬歐元	25 萬小時	112

資料來源：作者整理自 Ministére des Armées, La loi de programmation militaire 2019/2025 – Rapport annexé 與法國國防部網站 https://www.defense.gouv.fr.

[25] Catherine Magueur, “Piriou. Un nouveau contrat de 160 millions d’euros,” *Le Télégramme*, September 4, 2015, https://www.letelegramme.fr/economie/piriou-un-nouveau-contrat-de-160-millions-d-euros-04-09-2015-10760841.php.

三、區域產業聚落的形塑：布列塔尼大區與羅里昂市

（一）布列塔尼大區

布列塔尼的國防相關產業不只是該區經濟上的重要支柱，其同時也是法國國防產業的重要發展地帶。在 2013 年，布列塔尼大區所帶來的國防相關收入為 32 億 8,300 萬歐元，占全國總收入的 8.4%，居法國第 4 位。[26]布列塔尼國防產業總產值的 82%，皆來自國防造船，其中船舶修復與保養占 35%，船舶建造占 30%，航海周邊設備製造則占 17%。[27]法國海軍集團在布列塔尼大區的布列斯特市與羅里昂市均設有造船廠區，共雇傭了 16%的法國海軍集團法國本土部門的員工。[28]布列斯特船廠是法國海軍集團在該區的最大廠區，主要負責包括戴高樂航空母艦的建造與軍艦的維修，羅里昂則為其第二大廠區。

（二）羅里昂市

法國海軍集團在羅里昂的廠區主要負責的是巡防艦與小型船艦的建造，也是阿基坦級多用途巡防艦計畫與中型通用巡防艦計畫的負責建造廠區，我們可以從社會與經濟面向來分析兩大造艦計畫所帶來的影響。

在社會面向上，羅里昂船廠為當地船舶產學體系的完善上貢獻甚多。在產業方面，藉由前述長期的造艦計畫吸引承包商參與進駐，得以逐步建立穩定的合作關係，法國海軍集團也能夠因此確保地方造艦能力的永續維持。同時，法國海軍集團也透過合資收購 Kership 造船廠，進一步的提升了羅里昂廠的造船能力。在教育方面，法國海軍集團羅里昂船廠是法國海事學校（Campus Naval France）在 2007 年成立時的重要促成者，同時也是羅里昂當地自中學以上各級海事相關學校的重要夥伴，提供造船、海洋環境與海洋再生能源等相關課程的協助，學生們在畢業之後也得以直接就近到羅里昂船廠或其他承包商內部工作。因此，法國海軍集團在羅里昂的投入，不只大幅度降低了生產成本，也強化並維持了該地的造船能力。

---

[26] Ministère des Armée de la France, “La défense dans les régions, ” June 2016, p.12.
[27] *Ibid*, p.17.
[28] Naval Group, *Rapport financier 2017*（Paris : LABRADOR, 2018）, p.95.

在經濟面向上。一方面，在就業的部分，羅里昂船廠的運作支撐了9,107份工作職位，包括在羅里昂船廠內部的1,876個直接工作職位、外部供應鏈的2,962個間接工作職位與日常運作相關事務所產生的4,269個衍生性工作職位。換言之，在羅里昂船廠每創造1個工作機會，等於為全法國就業市場增加4.9個工作機會，其中39%的工作職位都集中在布列塔尼。另一方面，在經濟收入的部分，羅里昂船廠的活動為全法國帶來了6.63億歐元的收入，其中羅里昂所處的布列塔尼大區與莫爾比昂省（Morbihan）各自獲得當中的2.72億與2.36億歐元。[29]此外，在羅里昂船廠每產生1歐元的產值，則可以對法國經濟帶來3.3歐元的附加價值。[30]

四、國家產業的發展：海洋嚇阻產業的案例

（一）海洋嚇阻產業的發展與現況

法國的海洋嚇阻產業主要有三大本土廠商參與其建造，首先法國海軍集團主要承擔總體設計與組裝，該集團參與了潛艦壽期的每一個階段，目前負責的任務有——第一代艦的解體與拆裝、現役 4 艘第二代艦的維護與 M51 彈道飛彈的裝設以及第三代艦的開發。此外阿海琺主要承辦法國海軍船艦的核子反應爐建設，其中包括反應爐的設計、研發、製造、維護與拆除。阿利安集團（Ariane Group），主要負責彈道飛彈的武器系統，也就是 M51 彈道飛彈與其發射器的開發設計與拆除。

在歷經了數十年的發展後，海洋嚇阻產業已經使主要建造廠商對其產生相當程度的依賴，法國海軍集團的 6 個廠區、阿海琺的 3 個廠區以及阿利安集團的 6 個廠區所雇用的員工，當中共 15,835 人皆從事與海洋嚇阻產業的相關工作，占此三大企業員工總數的 71%（表 7）。

[29] 根據法國的地理行政區劃分，羅里昂市屬於莫爾比昂省的一部分，而莫爾比昂省則是布列塔尼大區的一部分。

[30] Naval Group, *op. cit.*, 2018, p.95.

表 7 海洋嚇阻產業相關廠區雇用人數與主要業務

廠區	員工數	主要業務
法國海軍集團所屬廠區		
瑟堡	2,250	核動力彈道飛彈潛艦的設計、建造、整合、試驗與拆除
布列斯特	2,760	檢修與更新
南特	1,300	能源驅動系統的設計、製造與測試
土倫（Toulon）	3,210	武器戰鬥系統
呂埃爾（Ruelle）	830	重要次系統（魚雷發射管、飛彈發射管等）的設計與製造與火藥
聖特羅佩（Saint-Tropez）	240	魚雷設計、製造與測試
小計	10,590	
占全體員工比例（%）	79%	
阿海琺所屬廠區		
薩克萊（Saclay）	120	計劃管理、技術支援
卡達哈許（Cadarache）	700	核子反應爐、燃料生產、實際安裝與模擬課程
艾克斯-普羅旺斯（Aix-en-Provence）	500	國防核子工程
小計	1,320	
占全體員工比例（%）	92%	
阿利安集團所屬廠區		
雅萊地區聖梅達爾（Saint-Médard-en-Jalles）	716	計劃管理、研究、飛彈系統配件製造、產品裝載、推進器組裝等
勒艾朗（Le Haillan）	1,346	火藥、研究、M51 飛彈噴口組裝
伊薩克（Issac）	1,364	飛彈組裝
勒布歇（Le Bouchet）	188	研發
土魯斯（Toulouse）	93	推進器相關原料生產
布列斯特	218	飛彈組裝、基地演練、維護
小計	3,925	
占全體員工比例（%）	54%	
總計	15,835	
平均占全體員工比例（%）	71%	

資料來源：Hélène Masson and Stéphane Delory, *Impact économique de la filière industrielle « Composante océanique de la Dissuasion » Volet 2*（Paris: la Fondation pour la Recherche Stratégique, 2017）, p.45.

若將三大主要企業與其中下游承包商納入計算，法國海洋嚇阻產業的各項活動在造艦活動停止的「未更新時期」（Hors Renouvellement），可以在全國產生 12,700 個工作機會，其中 9,900 個為直接工作機會，2,800 個為間接工作機會，而啟動造艦的「更新時期」（Renouvellement）則可以產生 17,300 個工作機會，包括 13,000 個直接工作機會與 4,300 間接工作機會（表 8）。

表 8 海洋嚇阻產業活動所產生的工作機會

	2011-15 年度平均（未更新時期）	其餘 20 年年度平均（更新時期）
直接工作機會	9,900	13,000
間接工作機會	2,800	4,300
總計	12,700	17,300

資料來源：Assemblée Nationale, “Rapport d’information sur les enjeux industriels et technologiques du renouvellement des deux composantes de la dissuasion,” December 2016, p.22

（二）產業聚落及對地方收入之貢獻

海洋嚇阻產業的三大主要廠商、供應商與承包商的活動已經對地方發展有著不可忽視的貢獻。在法國本土的96個省（département）當中，與海洋嚇阻產業經濟活動有關的為90個，而該產業經濟活動整體的70%，都集中在關聯度最高的12個省分，[31]主要分布在法國海軍集團、

[31] 依序為濱海阿爾卑斯省（Alpes-Maritimes）9%、上賽納省（Hauts-de-Seine）8.4%、瓦爾省（Var）8%、伊夫林省（Yvelines）7%、巴黎（Paris）6.4%、菲尼斯泰爾省（Finistère）5.6%、埃松省（Essonne）5%、芒什省（Manche）4.9%、羅亞爾-大西洋省（Loire-Atlantique）4.5%、隆河河口省（Bouches-du-Rhône）4.4%、吉倫特省（Gironde）4.1%、上加龍省（Haute-Garonne）2.5%。

阿海珐與阿利安集團廠區所在地的周遭地區，不但對當地的經濟挹注良多，也可以從此種集中趨勢觀察到以主要廠商廠區所在地為核心，形成一個以海洋嚇阻產業的生產聚落。

（三）技術發展所產生之外溢效應

技術發展的外溢效應主要可分為三種類型。首先是從嚇阻到傳統武器的外溢效應。海洋嚇阻產業所開發出的技術對於其他傳統武器項目的發展有相當正面的影響。例如紅寶石級與敘佛倫級等核動力潛艦的研發經驗使傳統動力潛艦如奧古斯塔級（*Classe Augosta*）與鮋魚級（*Classe Scorpène*）的開發過程獲益良多。此外，在開發凱旋級彈道飛彈潛艦的過程中所獲得的船體焊接技術、靜音技術、戰鬥系統的程式、推進系統與通信系統等等，皆能被廣泛應用在敘佛倫級核動力攻擊潛艦上。同時敘佛倫級潛艦所應用的核子反應爐也是在既有核動力彈道飛彈潛艦與戴高樂航空母艦的基礎上加以改良而成。

第二則為從自用到出口的外溢效應。從國防自主的原始發展理念出發，自用的需求開始帶來了出口的可能性，法國核動力彈道飛彈潛艦多年的開發與自製經驗，不但增加其在國際潛艦市場上的能見度與可信度，也提升了法國海軍集團的國際名聲。該集團良好的科學與技術形象，使缺乏必要技術但希望提升國防能力的國家，紛紛向法國購買武器，如智利、馬來西亞、印度、巴西與澳洲都是十分成功的案例，這些軍售案不但為法國帶來可觀的外匯收入，同時這些收入又回過頭來使國內的海洋嚇阻產業進一步壯大，為開發出更新的技術奠定良好的財政基礎。

第三則為從軍用到民用的外溢效應。在海洋嚇阻產業中所投入的研發成本，無論是核動力彈道飛彈潛艦或是核動力攻擊潛艦的開發計畫均涉及相當多項的技術，其中的許多技術隨後又可進一步在民用領域上發揚光大，當中比較具代表性的例子如下所示（表 9）。

表 9 海洋嚇阻產業技術轉移民用情況一覽

軍用技術	民用領域
潛艦聲納與雷達	醫學超音波檢查
潛艦與飛彈的慣性導航設備	大地測量、海洋探測、工程測量
核動力彈道飛彈潛艦、核反應爐與彈道飛彈的開發與建造程序	系統工程能力
核子反應爐	核電廠安全性、核子工程技術

資料來源： Hélène Masson and Stéphane Delory, *op. cit.*, pp.48-50.

此外，法國彈道飛彈開發計畫與歐洲航太計畫彼此間也存有相互啟發的關係。法國核動力彈道飛彈潛艦所使用的 M51 彈道飛彈與歐洲太空總署（European Space Agency）的阿利安 6 號（Ariane 6）運載火箭均出自於相同的設計開發團隊——阿利安集團（Ariane Group）。

從整體的角度來看，此種關係也有助於工業資源的有效利用與分配，考量到彈道飛彈計畫的高度敏感性，在計畫受到外力干擾而中斷或是暫時沒有需求之時，相關技術依舊可依賴太空運載火箭的開發而繼續維持。因此，海洋嚇阻產業外溢到其他民用領域的技術，不但為此些領域帶來革新，同時也成為這些敏感技術的保存與開發場所，不因為政治等外力的干擾而中斷。

伍、政策的啟示與討論

在《中華民國106年國防報告書》與《中華民國108年國防報告書》中，國防自主已是台灣國防政策的重心之一。[32]毫無疑問地，當談及法

[32] 參見國防部國防報告書編纂委員會著，《中華民國 106 年國防報告書》，（台北：中華民國國防部，2017 年）；中華民國 108 年國防報告書編纂委員會，《中華民國 108

國發展經驗對台灣國防自主政策啟示時，法台兩國在造艦產業的發展狀況上存有相當程度的落差，法國是今日數一數二的海上強權國家，從一般的巡邏艦到技術高度複雜的核動力潛艦與航空母艦，法國造艦產業皆有完整的自製能力，台灣造艦產業儘管過去也曾自製成功級巡防艦、錦江級巡邏艦與磐石號油彈補給艦等水面艦隻，但主力戰艦與潛艦的建造能力依舊不足而有賴國外技術的援助，因此若直接將法國發展套用在台灣恐有揠苗助長之疑慮。然而，在今日台灣強調國防自主，海軍推動國艦國造之際，法國經驗仍可從以下三點提供進一步思考：

一、強調資金投入的穩定

由法國的經驗可知，欲提振一國的軍事力量，則穩定的資金挹注是一切發展的基礎，國防領域所應用的高科技研發成本較高，更要承擔研發失敗的風險，因此需要大量資金以確保其永續發展。我國近年來的國防預算已有不小成長，然而除了透過增加技術研發與軍備建造的預算以外，也可透過其他方式為相關研發與投資增加更多財源，無論是專門基金的創設或是額外稅收的補貼均是可以考慮的方式。

二、重視外溢效應的發散

作為國防大國，法國軍備在全球市場上一直有著亮麗表現，在 2018 年法國的軍備出口總額來到 91.18 億歐元，相較 2017 年成長了 31%。[33] 如此的銷售佳績維持了法國國防產業生產線的基本運作與擴張，帶來更多的國內就業機會，同時產量提升也使得單位製造成本降低。

然而，艱困國際處境使得台灣無法像法國那般藉由拓展外銷帶來上述好處，因此外溢效應的強化便是重中之重。將國造項目的高階軍用技術釋出轉為商用，使該項技術的經濟效益最大化。亦或邀請民間企業參與軍備建造計畫，以此為手段進行技術升級，進一步提高企業的國際競爭力。但更為關鍵的是，政府應該有一個明確的長期軍備建造計畫使得國內廠商得以依循與預作規畫，方能使增加國內企業的信心，增加投入大量資本進行研發的意願。

年國防報告書》，（台北：中華民國國防部，2019 年）。

[33] Ministère des Armées, “Exportations d’armement : le rapport au Parlement 2019,” June 2019.

三、強化社會大眾的溝通

作為一個民主國家，政府的相關決策均需接受國會的監督，耗資不斐的軍備國造項目更有賴社會大眾的支持，除了國家安全的動機以外，經濟好處應作為軍備國造計畫的論述主軸，從法國的案例分析可知，軍艦建造所帶來的經濟效應相當深遠，無論是經濟加乘效益、就業機會的創造與外溢效應的發散都是值得主事者在與人民溝通時進一步強調的論點，藉由簡單明瞭的數字陳述，將有助於大多不熟悉國防與軍事事務的普通百姓理解軍備國造計畫的意義與好處，有著多數人民支持，政府對於相關政策的推動將更加得心應手。

陸、結論

本研究的目的在於探究法國造艦產業的安全與經濟效益，試圖確認造艦產業對法國安全與經濟的影響，最新的國防白皮書《安全檢討》揭示法國將以「戰略自主」與「歐洲雄心」作為核心目標，《軍事計畫法》所提出的預算規劃回應了《安全檢討》的基調，軍備預算大幅度的上升並應用在法國海軍傳統與嚇阻力量的相關船艦建構上。

本文認為法國造艦產業的蓬勃發展至少為法國帶來兩大層面的影響，在安全層面上，海軍船艦的建設無疑地促進了法國「戰略自主」目標的達成，對於政治、作戰與產業等面向的「戰略自主」均能有所貢獻。在經濟層面上，造艦產業更是有深遠的影響，無論是從單一的企業、船艦的建造、區域產業聚落的建立或是國家產業的發展等角度來分析，造艦產業對於法國經濟有著相當正面的影響。

因此，本研究確認了法國造艦產業對法國的重要性，對於巴黎來說，此項產業的永續發展是重要的，無論是在安全與經濟層面，法國造艦產業都已經扮演著舉足輕重的角色，這也是為何法國總統馬克宏自 2017 年上任以來，迥異於前幾任政府大舉在國防事務領域投入資源的重要原因之一。此外，台灣的國防自主政策也可從法國發展經驗得到諸多啟發，其中包括強調資金投入的穩定、重視外溢效應的發散與強化社會大眾的溝通等等。

參考書目

一、專書

中華民國 108 年國防報告書編纂委員會，《中華民國 108 年國防報告書》，（台北：中華民國國防部，2019 年）。

國防部國防報告書編纂委員會著，《中華民國 106 年國防報告書》，（台北：中華民國國防部，2017 年）。

Masson, Hélène and Stéphane Delory, *Impact économique de la filière industrielle « Composante océanique de la Dissuasion » Volet 2*（Paris: la Fondation pour la Recherche Stratégique, 2017）.

Naval Group, *Rapport financier 2017*(Paris : LABRADOR, 2018).

Naval Group, *Rapport financier 2018*(Paris : LABRADOR, 2019).

二、學術性期刊論文

Drouhaud, Pascal, “La dissuasion nucléaire de la France et l’environnement international,” *Guerres mondiales et conflits contemporains*, No. 223, March 2006, p.139.

Rogel, Bernard, “Enjeux et défis stratégiques de la Marine nationale,” *Revue Défense Nationale,* No. 789, April 2016, pp.14-16.

三、官方文件

Assemblée Nationale, “Rapport d’information sur les enjeux industriels et technologiques du renouvellement des deux composantes de la dissuasion,” December 2016.

Ministère de la Défense, “Livre Blanc sur la Défense,” June 1994.

Ministère des Armée de la France, “La défense dans les régions, ” June 2016.

Ministère des Armées, “Exportations d’armement : le rapport au Parlement 2019,” June 2019.

Ministère des Armées, “La loi de programmation militaire 2019/2025 – Rapport annexé,” July 2018.

Ministère des Armées, “Revue Stratégique de Défense et de Sécurité Nationale,” December 2017.

四、網際網路資料

法國國防部網站，https://www.defense.gouv.fr.

“Construction navale. DCNS est en ordre de marche,” *Ouest France*, June 6, 2015, https://www.ouest-france.fr/economie/economie-de-la-mer/construction-navale-dcns-est-en-ordre-de-marche-4473741.

“DCNS Lorient fabriquera cinq frégates intermédiaires,” *Le Télégramme*, April 21, 2017, https://www.letelegramme.fr/morbihan/lorient/defense-dcns-lorient-fabriquera-cinq-fregates-intermediaires-21-04-2017-11484424.php.

“France officially orders four FLOTLOG replenishment ships under €1.7 b contract,” *Navaltoday.com*, January 31, 2019, https://navaltoday.com/2019/01/31/france-officially-orders-four-flotlog-replenishment-ships-under-e1-7-b-contract.

“FREMM : le plus grand programme naval militaire européen,” *DCNS*, 2010, https://www.naval-group.com/wp-content/uploads/2010/10/DCNS_DP_FR.pdf.

“L’impact économique du programme Barracuda,” *Ministère des Armée de la France*, August 6, 2010, https://www.defense.gouv.fr/english/marine/dossiers/barracuda/l-impact-economique-du-programme-barracuda.

“La nouvelle frégate de la marine française est enfin dévoilée,” *Captial*, October 18, 2016, https://www.capital.fr/entreprises-marches/la-nouvelle-fregate-de-la-marine-francaise-est-enfi

n-devoilee-1176347.

“Le CEMM au lancement de la construction de la FREMM Provence,” Ministère des Armée de la France, December 16, 2010, https:// www.defense.gouv.fr/english/marine/a-la-une/le-cemm-au-lancement-de-la-construction-de-la-fremm-provence.

“Programme de frégates de taille intermédiaire : DCNS se félicite de l’annonce de la notification du marché par le Ministère de la Défense,” *Naval Group*, April 21, 2017, https://www.naval-group.com/wp-content/uploads/2017/04/cp-notification-fti_def-1.pdf.

“USA and France dramatically increase major arms exports; Saudi Arabia is largest arms importer, says SIPRI,” *SIPRI*, March 9, 2020, https://www.sipri.org/media/press-release/2020/usa-and-france-dramatically-increase-major-arms-exports-saudi-arabia-largest-arms-importer-says.

Bauer, Anne, “Naval Group s’impose en mer du Nord dans la guerre des mines,” *Les Echos*, March 15, 2019, https://www.lesechos.fr/industrie-services/air-defense/naval-group-simpose-en-mer-du-nord-dans-la-guerre-des-mines-1001024.

Cabirol, Michel, “Emirats Arabes Unis : et un nouveau contrat important à l’export pour Naval Group,” *La Tribune*, June 7, 2019, https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/emirats-arabes-unis-et-un-nouveau-contrat-important-a-l-export-pour-naval-group-812087.html.

Cabirol, Michel, “Si, si Naval Group déclaré vainqueur... en Roumanie,” *La Tribune*, July 2, 2019, https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/si-si-naval-group-declare-vainqueur-en-roumanie-822378.html.

Gady, Franz-Stefan, “Australia, France Sign $35.5 Billion Submarine Contract,” *The Diplomat*, February 11, 2019, https://thediplomat.com/2019/02/australia-france-sign-35-5-

billion-submarine-contract.

Lamigeon, Vincent, “Dans l’antre du nouveau sous-marin nucléaire français Barracuda,” *Challenges*, December 5, 2018, https://www.challenges.fr/entreprise/defense/dans-l-antre-du-nouveau-sous-marin-nucleaire-barracuda_629916.

Magueur, Catherine, “Piriou. Un nouveau contrat de 160 millions d’euros,” *Le Télégramme*, September 4, 2015, https://www.letelegramme.fr/economie/piriou-un-nouveau-contrat-de-160-millions-d-euros-04-09-2015-10760841.php.

Maury, Matthieu, “Les frégates FREMM sur de bons rails chez DCNS,” *L’Usine Nouvelle*, October 9, 2009, https://www.usinenouvelle.com/article/les-fregates-fremm-sur-de-bons-rails-chez-dcns.N118921.

Mélennec, Olivier, “Économie de la mer. SNLE 3G : la mise en chantier prévue pour 2023,” *Ouest France*, October 26, 2018, https://www.ouest-france.fr/economie/economie-de-la-mer/economie-de-la-mer-snle-3g-la-mise-en-chantier-prevue-pour-2023-6038236.

Prazuck, Christophe, “STRATÉGIE : Le plan Mercator de la Marine nationale,” *Association de soutien à l’armée française*, December 17, 2018, https://www.asafrance.fr/item/le-plan-mercator-de-la-marine-nationale.html.

.

澳洲國防造艦計畫與其經濟效益

蔡榮峰

政策分析員

國防安全研究院國防資源與產業研究所

摘　要

澳洲《2016 國防白皮書》公布的國防造艦計畫，達到該國二戰以來的最大規模，包括潛艦、主要水面艦、海軍小型艦艇共 57 艘。澳洲政府希望藉著下一代船艦的汰換期，打造可長可久的國防造艦生態圈。坎培拉從人才供給與市場需求兩方面著手，企圖降低造船業景氣波動對國防工業能力的負面影響；透過較為平均分散的國防造艦策略，扶植南澳與西澳兩大聚落，讓國防造艦經濟帶動就業成長。澳洲造船政策的規劃經驗為中型國家的海軍帶來了寶貴的啟示。

關鍵詞：澳洲、國艦國造、潛艦、國防經濟

Australia's Naval Shipbuilding Plan and Its Economic Benefits

Oddis Jung-Feng Tsai

Policy Analyst

Division of National Defense Resources and Industries

Institute for National Defense and Security Research

Abstract

Australia's largest naval shipbuilding plan since WWII revealed in the 2016 Defence White Paper consisted of 57 vessels, including submarines, surface warships and smaller patrol boats. The Australian government sought to build sustainable industries in naval shipbuilding through the replacement of next-generation production. To reduce the negative impact on defence industrial capabilities brought by business cycles, Canberra intended to balance the supply and demand in both skilled labour and shipbuilding needs. By avoiding the disproportionate distribution of shipbuilding demands, Canberra intended to boost two industry clusters in South Australia and Western Australia simultaneously, and the thriving shipbuilding economies then benefited the local employment. There were certain virtues in the way Australia formed its naval shipbuilding plan, which deserves the attention of navies from other middle powers.

Keywords: *Australia, indigenous shipbuilding, submarine, defence economics*

壹、前言

澳洲位於南太平洋一隅，雖遠離地緣衝突熱點，其經濟高度仰賴通往北半球之國際海運。全國85%人口在離海不超過50公里之廣袤沿海地區，雖然擁有綿延海岸線卻因地廣人稀難以防守國境，特殊國情為其國防安全帶來挑戰。基於二戰達爾文港遭日軍轟炸的慘痛教訓及冷戰經驗，澳洲自1951年簽訂《美澳紐防禦條約》（*Australia, New Zealand, United States Security Treaty*, *ANZUS Treaty*）至今，皆以有限軍事能力對美軍同盟關係做出貢獻，以期未來再度遭逢亞洲強權南下侵擾時，能夠仰賴美軍透過海路馳援。因此澳洲戰略目標本質上以不違反美軍印太區域戰略部署的利益為前提，否則將難以落實，而此類本質又進而影響其建軍思維，反映了「中型國家」（middle power）追求「有限國防自主」的特色。該如何將敵對勢力及時遏止於本土大陸周遭海域、避免通往美國與亞洲的海上交通線遭到截斷，成為澳洲海權發展的重心所在。

除了安全因素之外，澳洲政府希望藉著下一代船艦的汰換期，打造可長可久的國防造艦生態圈，以利進入全球供應鏈，包括次要系統、零組件、保修服務以及載台輸出。澳洲2018年公布的《國防出口策略》（*Defence Export Strategy*），即表明欲在10年內躋身全球十大國防產業出口國。該份報告提及將編列38億澳幣預算來推動對美國、加拿大、英國、紐西蘭、印太地區及中東地區之國防出口，其中包括潛艦、水面艦、小型艦艇。另外，每年對本土國防產業之中小企業補助410萬澳幣、撥款320萬澳幣成立「澳洲國防工業出口辦公室」（The Australian Defence Export Office）以提高國際競爭力。[1]

本文爬梳官方出版報告書及相關委託研究報告，聚焦分析其造艦計畫之政策擬定與經濟效果，從國防經濟角度檢視澳洲相關國防產業最新

[1] 作為對外單一窗口，其組成橫跨各政府機構，包括澳洲貿易投資委員會（Austrade）、國防產業能力建構中心（Centre for Defence Industry Capability）、國防部（Department of Defence）、內政部（Department of Home Affairs）、產業創新暨科學部（Department of Industry, Innovation and Science）、澳洲外交暨貿易部（Department of Foreign Affairs and Trade）、澳洲出口信貸機構（Export Finance and Insurance Corporation, EFIC），見 Department of Defence of Australian Government, “Defence Export Strategy,” 2018, p.77, https://www.defence.gov.au/Export/Strategy.

的發展策略，主要分三個部分：「澳洲海軍造艦政策」檢視澳洲皇家海軍（Royal Australian Navy，以下簡稱澳洲海軍）現有艦隊組成以及新一代水面艦、潛艦的汰換規劃；「澳洲國防造艦產業」闡述澳洲現有國防造艦產業聚落發展、主要參與廠商以及各自在造艦計畫當中所扮演的角色；「國防造艦經濟效應與就業機會」則分析主要計畫可能帶來的經濟效益以及澳洲海軍對於造艦經濟的計算方式。

貳、澳洲海軍造艦計畫

根據澳洲《2016國防白皮書》（*2016 Defence White Paper*）的戰略利益排序，該國防衛重心依次可分為：一、本土大陸及其北面島弧（包括印尼群島、巴布亞紐幾內亞、東帝汶及索羅門群島）；二、鄰近地區（東協海島地區與南太平洋地區）；三、印太區域以及全球秩序。未來20年，各國先進潛艦半數以上會出沒於印太地區，而中國潛艦更在2018年就已達到76艘，規模可能長期維持在70艘以上只增不減。為因應2035年的印太戰略情勢，特別是太平洋的美中船艦比、北韓核武、東協國家潛艦擴散等議題，未來20年澳洲海軍在人力有限的情況下，其建軍方向具有「鄰近地區內技術最先進」、「盟國協同作戰能力」兩大特點。[2]為了確保海軍軍力能夠符合戰略與作戰構想，《2016國防白皮書》擬訂了二戰以來最大規模的造艦計畫，數量達到57艘之譜。然而在任何民主國家，政府投入龐大的國防預算，都需要仰賴全民達成共識，因此政策規劃的目標除了滿足戰力需求以外，還必須將產業發展與經濟效益納入考量，才能真正藉由扶植國防造艦產業，來保有長期永續的國防自主能力。[3]

澳洲國防部《2016整合投資計畫》（*2016 Integrated Investment Program*）內容顯示，至2026年為止，陸海空建軍預算總額為1,950億澳幣，其中用於提升海軍海上作戰及反潛能力之預算占總額25%。[4]澳洲

---

[2] 根據最新官方統計數據，澳洲國防軍（Australian Defence Force）總兵力共約 5 萬 8,000 人，其中海軍員額 14,206 人。Department of Defence of Australian Government, "Annual Report 2018-19," September, 2019, p.234, https://www.defence.gov.au/AnnualReports/ 18-19.

[3] 澳洲官方文件中多半稱「國防自主能力」為「主權能力」（sovereign capacity）。

[4] Department of Defence of Australian Government, "2016 Integrated Investment

國防部2017年公布的《海軍造艦計畫》（*Naval Shipbuilding Plan*），其造艦總預算達到約900億澳幣。[5]

澳洲這一波國防造艦三大主要計畫分別為「未來潛艦計畫」（Future Submarine Program）、「未來巡防艦計畫」（Future Frigate Program）、「小型海軍艦艇更替計畫」（Minor Naval Vessel Continuous Build Program）。基礎建設部分則斥資約 13 億澳幣於南澳的奧斯本（Osborne）與西澳的韓德森（Henderson）進行國防造艦基礎建設現代化工程，並以 3,500 萬澳幣預算重新規劃西部艦隊基地（HMAS Stirling），預計 2020 年完工。人才培養的部分，則定於 2019 至 2021 年間投入 6,200 萬澳幣在南澳建立「海軍造船專科學校」（Naval Shipbuilding College），以期穩定人才供給。[6]以下就三大主要造艦計畫的規劃內容分述之。

一、未來潛艦計畫

計畫代號 SEA1000 的「未來潛艦計畫」為澳洲國防史上規模最大的造船案，達 500 億澳幣，約合新台幣 1 兆 1,500 億元。澳洲政府考量了價格、規劃與執行能力、服役壽期的後續服務、技術轉移及本土國防工業參與程度等因素後，最終「創造多少就業機會」成為決策關鍵，載台設計最終由現在的法國海軍集團澳洲分公司（Naval Group Australia，以下簡稱海軍集團）得標，擊敗德國 TKMS 船廠與日本三菱-川崎聯合團隊。[7]澳法雙方於 2019 年 2 月 11 日完成《戰略夥伴協議》（Strategic Partnering Agreement, SPA）簽訂，建造 12 艘 4,500 噸「進擊級」（Attack class）大型遠洋柴電潛艦，[8]首艘於 2032 年間下水，接著每兩年下水一

Program," 2016, pp.22-24, https://www.defence.gov.au/WhitePaper/Docs/2016-Defence-Integrated-Investment-Program.pdf.

5 Department of Defence of Australian Government, "Naval Shipbuilding Plan," 2017, p.11, https://www.defence.gov.au/navalshipbuilding/Plan.

6 Department of Defence of Australian Government, "2018 Defence Industrial Capacity Plan," 2018, p.66, https://www.defence.gov.au/SPI/Industry/CapabilityPlan/Docs/DefenceIndustrialCapabilityPlan-web.pdf.

7 得標當時該公司名稱為 DCNS，2017 年 6 月 28 日才改名為 Naval Group，為避免混淆，本文統一使用該集團新名稱。

8 Naval Group, "Naval Group Signs the Strategic Partnering Agreement," February 11, 2019, https://naval-group.com.au/2019/02/11/naval-group-signs-the-strategic-partnering-agreement.

艘，現階段規劃使用年限至 2070 年。「進擊級」將逐步替代現有的 6 艘柯林斯級（Collins class），將艦隊規模擴張一倍。

「進擊級」又名「短鰭梭魚級」（Shortfin Barracudas class），衍生自法國核動力潛艦「梭魚級」，採用先進的泵噴推進系統（Pump-Jet Propulsion），其匿蹤效果優於德日方案的傳統螺旋槳推進器。[9]

澳洲海軍潛艦作戰涵蓋範圍廣大，跨越多緯度複雜海底作戰環境，欲滿足該國特殊國防需求勢必得「量身打造」世界獨有的澳洲規格，然而這也代表未來澳洲海軍必須獨自承擔所有成本與風險。

表 1 進擊級飛彈潛艦諸元

排水量/噸	浮航 4,500
尺寸	全長 97 公尺，艦寬 8.8 公尺
動力系統	柴油發電機、泵噴推進器、鉛酸蓄電池[10]
最高航速	潛航 20 節（37km/h-23mph）
續航力	1800 浬/10 節-浮航（19km/h-12mph）
續行天數	80 天
載員	60 人
作戰系統	AN/BYG-1 （Raytheon）
武器系統	Mark 48 型魚雷（MOD 7）、垂直發射器

資料來源：蔡榮峰整理自 Stephen Kuper, “Sub scuttlebutt: SEA 1000 in deep water, or is it?” *Defence Connect*, October 8, 2018, https://www.defenceconnect.com.au/maritime-antisub/2978-sub-scuttlebut-sea-1000-in-deep-water-or-is-it.

[9] 澳洲海洋資源與安全國際研究中心（Australian National Centre for Ocean Resources and Security）研究員、前澳洲海軍軍官貝特曼（Sam Bateman）的說法，見 Pierre Tran, “How a French firm beat out Japanese companies in Australia’s submarine tender,” *Defense News*, November 21, 2017, https://www.defensenews.com/global/europe/2017/11/21/how-a-french-firm-beat-out-japanese-companies-in-australias-submarine-tender.

[10] 海軍集團於 2018 年 10 月宣布成功研製出潛艦用高功率鋰電池系統（LIBRT），未來選用何種電池仍有變更的可能性。

二、未來巡防艦計畫

代號 SEA5000 的「未來巡防艦計畫」由英國航太系統 BAE 澳洲分公司（BAE Systems Australia，以下簡稱 BAE）承建，預算總額 350 億澳幣，將造 9 艘獵人級（Hunter Class）飛彈巡防艦，主要任務為反潛、防空、水面作戰、偵防、救災，陸續下水後將取代現役的 8 艘紐澳軍團級（Anzac class）直升機巡防艦。

2023 年陸續下水的 9 艘獵人級巡防艦，以及 2020 年成軍的 3 艘荷巴特級（Hobart class）驅逐艦，未來皆搭配神盾系統，能夠與美軍勃克級驅逐艦進行資訊鏈結協同作戰，形成澳洲新一代水面艦主力。維持 12 艘神盾艦規模，將使澳洲有能力在至少兩個地理區域作戰。以 1 艘荷巴特級與 3 艘獵人級為一組，當兩組編隊值勤時，還有一組可進行 3~6 個月的中繼維修（Intermediate Maintenance Activity, IMA）。

澳洲選擇 BAE 的 Type26 型巡防艦，除了考量英國脫歐之後的經濟互惠之外，也與英國皇家海軍確定採購 8 艘同款巡防艦之決定不無關聯。這代表未來在印太地區，最多將出現 17 艘同款巡防艦，提高澳英兩國海軍聯合作戰能力。此外獵人級與荷巴特級共 12 艘主力戰艦未來皆搭載神盾系統，增加了美國、日本與澳洲三邊的作戰互通性（Inter-operability）。

表 2 獵人級飛彈巡防艦諸元

排水量/噸	8,800（滿載）
尺寸	全長 149.9 公尺，艦寬 20.8 公尺
動力系統	複合柴油電力或燃氣渦輪機(Combined Diesel-Electric or Gas Turbine, CODLOG)
最高航速	27 節
續航力	7,000 浬
武器系統	• Eurotrop（Whitehead Alenia, Naval Group, Thales 合資）MU90 魚雷 • BAE Mk45（Mod 4） 5 英吋艦砲 • Raytheon RIM-162 進化型海麻雀飛彈（RIM-162 Evolved SeaSparrow Missile, ESSM） • Raytheon 標二飛彈（SM-2） • 反艦飛彈 • Lockheed Martin MK41 垂直發射系統 • 2 x 30 釐米 短距火砲 • 2 x 20 釐米 近迫武器系統 • BAE Nulka 離艦懸浮式主動電子干擾誘餌（Off-board Active Expendable Decoy, AED）
載員	180 人，容納上限 208 人
艦載機	1 架 MH-60R 海鷹直升機

資料來源：蔡榮峰整理自 Royal Australian Navy, "Hunter Class FFG," http://www.navy.gov.au/fleet/ships-boats-craft/future/ffg.

三、小型海軍艦艇更替計畫

小型海軍艦艇更替計畫，目前主要包括代號 SEA1180 的「近海巡邏艇計畫」(Offshore Patrol Vessel Program)，以及代號 SEA3036 的「太平洋巡邏艇更替計畫」(Pacific Patrol Boat Replacement Project)。

「近海巡邏艇計畫」由德國 Lürssen 公司與澳洲 Civmec 合資成立的 Australian Maritime Shipbuilding & Export Group（AMSEG）承建，預算總額為 35 億澳幣，將造 12 艘阿拉芙拉級（Arafura class）近海巡

邏艇，負責海疆巡邏、獵雷任務、水文探測。該計畫將澳洲國防工業輸出東協海島國家之商機納入考量，澳洲政府希望未來以單一型號巡邏艇，取代既有的 2 艘岬級（Cape class），13 艘阿米代爾級（Armidale class），以「單型多造」的方式鼓勵國防出口。AMSEG 也表明未來有意向以南太與東南亞國家輸出以阿拉芙拉級為原型之巡邏艇，且有兩個東協國家傳出有意購買改良版。[11]

「太平洋巡邏艇更替計畫」則由澳洲本土船廠 Austal 承建，將於 2018 至 2023 年斥資 3 億澳幣，共造 21 艘衛士級（Guardian class）巡邏艇，初建 19 艘給原有「防衛合作計畫」（Defence Cooperation Project）參與的 12 國，[12]2023 年以後再建 2 艘給區域新生國家東帝汶。此案為澳洲「太平洋海事安全計畫」（Pacific Maritime Security Program）的一部分，坎培拉將其視為兌現南太區域安全合作既有承諾之延續。[13]「太平洋巡邏艇更替計畫」延續過去「一魚兩吃」的軍事外交方針，以國防預算穩定國內造船產業能量，同時發揮整合南太國家海防之實質效果。坎培拉也將該計畫，視為鞏固 2018 年南太區域安全協議《波耶宣言》（*Boe Declaration*）的具體政策之一。

---

[11] Andrew Tillett, “Shipbuilding capacity expanding as regional clients beckon,” *Australian Financial Review*, October 3, 2018, https://www.afr.com/policy/foreign-affairs/shipbuilding-capacity-expanding-as-regional-clients-beckon-20180927-h15x9u.

[12] 根據 1982 年聯合國海洋法公約（*United Nations Convention on the Law of Sea*, UNCLOS）第三次會議上取得之國際共識，將各國專屬經濟海域（Exclusive Economic Zone, EEZ）定為 200 浬。當時南太國家急需應對此一變化，澳洲於是順水推舟，提出「防衛合作計畫」，藉此穩定區域局勢，並擴大影響力。該計畫的重要項目之一，就是由 Tenix 公司（2008 年被貝宜澳洲分公司合併）建造 22 艘巡邏艇，於 1987 至 1997 年間分送給參與計畫的 12 個南太島國：巴布亞紐幾內亞、斐濟、密克羅尼西亞、萬那杜、東加、庫克群島、薩摩亞、索羅門群島、吉里巴斯、馬紹爾群島、帛琉、吐瓦魯；名單上末 3 個國家，現為我國太平洋友邦。

[13] 「太平洋海事安全計畫」（Pacific Maritime Security Program）總預算 20 億澳幣，執行期間為 30 年，內容除了巡邏艇援助以外，還有如空中偵察合作等一系列以澳洲為首的區域安全合作項目。Department of Defence of Australian Government, “Annual Report 2017-18 Pacific Maritime Security Program,” 2018, http://www.defence.gov.au/annualreports/17-18/Features/Maritime.asp.

表 3 阿拉芙拉級近海巡邏艇諸元

排水量/噸	1,640
尺寸	全長 80 公尺，艦寬 13 公尺
吃水	4 公尺
動力系統	2 具 4,250 瓩柴油引擎
最高航速	20 節
續航力	4,000 浬
快艇（Sea Boat）	2 艘 8.5 公尺快艇（側面）、1 艘 10.5 公尺快艇（艇尾）
武器系統	• 40 釐米火砲 • 2 具 M2 重機槍 （50 Calibre Machine Gun）
載員	40 人，容納上限 60 人

資料來源：蔡榮峰整理自 Royal Australian Navy, “Arafura Class OPV,” http://www.navy.gov.au/fleet/ships-boats-craft/future/opv.

表 4 衛士級太平洋巡邏艇諸元

排水量/噸	約 160*
尺寸	全長 39.5 公尺，艦寬 8 公尺
吃水	76 公分
動力系統	2 具 4,250 瓩柴油引擎
最高航速	20 節
動力系統	Caterpillar 3516C 船用柴油引擎
續航力	3,000 浬（12 節）
載員	23 人

資料來源：蔡榮峰整理自 Austal, “Pacific Patrol Boat (Guardian Class),” https://www.austal.com/ships/pacific-patrol-boat-guardian-class.
*官方未公布，不過前一代太平洋巡邏艇排水量為 162 噸。

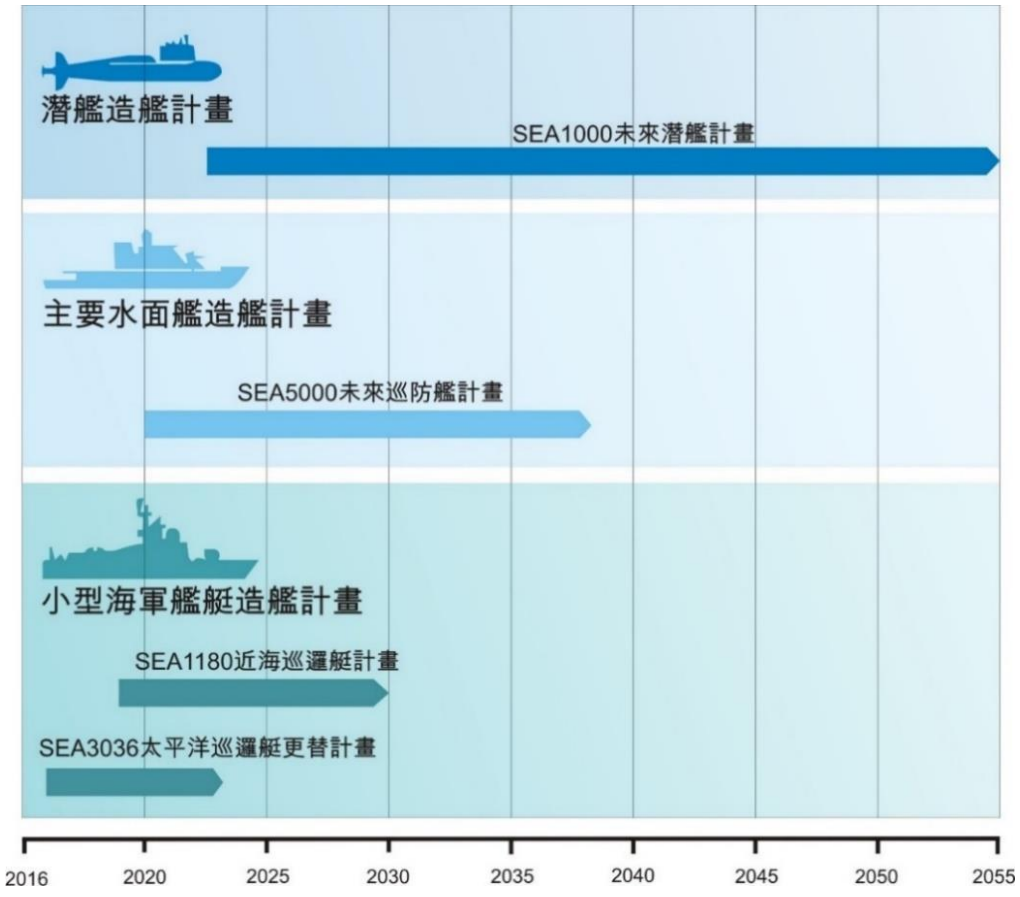


圖 1 澳洲主要國防造艦計畫時程表

資料來源：蔡榮峰重製，資料來自 Department of Defence of Australian Government, "Naval Shipbuilding Plan," 2017, p.24, https://www.defence.gov.au/navalshipbuilding/Plan.
說明：本圖未納入規劃細節尚不明朗的獵雷艦與調查船更替計畫。

表 5 澳洲海軍艦艇一覽表

船級	艦種	排水量/噸	數量	艦名	下一代船艦
坎培拉級 Canberra class	直升機船塢登陸艦 LHD	27,000	2	HMAS Canberra HMAS Adelaide	
荷巴特級 Hobart class	飛彈驅逐艦 DDG	7,000	3	HMAS Hobart HMAS Brisbane HMS Sydney	
阿德雷德級 Adelaide class	飛彈巡防艦 FFG	4,100	2	HMAS Melbourne （2019年10月26日除役） HMAS Newcastle （2019年6月30日除役）	9 艘 獵人級 飛彈巡防艦 Hunter class FFG
紐澳軍團級 Anzac class	直升機巡防艦 FFH	3,600	8	HMAS Anzac HMAS Arunta HMAS Ballarat HMAS Parramatta HMAS Perth HMAS Stuart HMAS Toowoomba HMAS Warramunga	
海灣級 Bay class	船塢登陸艦 LSD	16,190	1	HMAS Choules	
胡恩級 Huon class	海岸獵雷艦 MHC	732	4	HMAS Choules HMAS Gascoyne HMAS Huon HMAS Yarra	
杜倫斯級 Durance class	綜合補給艦 AOR	滿載46,755	1	HMAS Sirius	2 艘 運補級 綜合補給艦 Supply class AOR
成功級 Success class	油料補給艦 AO	滿載18,000	1	HMAS Success	

船級	艦種	排水量/噸	數量	艦名	下一代船艦
阿米代爾級 Armidale class	巡邏艇 PB	300	13	HMAS Albany HMAS Ararat HMAS Armidale HMAS Bathurst HMAS Broome HMAS Childers HMAS Glenelg HMAS Larrakia HMAS Launceston HMAS Maitland HMAS Maryborough HMAS Pirie HMAS Wollongong	12 艘 阿拉芙拉級 近海巡邏艇 Arafura class OPV
岬級 Cape class	巡邏艇 PB		2	ADV Cape Fourcroy ADV Cape Inscription	
柯林斯級 Collins class	飛彈潛艦 SSG	浮航 3,100 潛航 3,407	6	HMAS Collins HMAS Dechaineux HMAS Farncomb HMAS Rankin HMAS Sheean HMAS Waller	12 艘 進擊級 飛彈潛艦 Attack class SSG
陸文級 Leeuwin class	測量艦 AGS	2,205	2	HMAS Leeuwin HMAS Melville	
帕魯瑪級 Paluma class	海岸測量艦 AGSC	325	4	HMAS Benalla HMAS Mermaid HMAS Paluma HMAS Shepparton	
	航海訓練船		1	STS Young Endeavour	

資料來源：蔡榮峰整理自公開資訊。

*採外購模式，向西班牙 Navantia 採購，故不列入本文討論範圍。

參、澳洲國防造艦產業

澳洲造船業總產值約 42 億澳幣，相關就業人口約 15,000 人。澳洲造船業主要分為民用造船（civil marine manufacturing）以及國防造艦（naval shipbuilding）兩大部分，其中後者占了總產值約 2/3，從業人員約 10,000 人左右。國防造艦聚落主要位於以南澳州阿德雷德(Adelaide)、西澳州柏斯（Perth），而提供船舶維修服務之廠商，除了分布於前述兩地，還包括北嶺地達爾文（Darwin）、昆士蘭州的凱恩斯（Cairns）、維多利亞州威廉斯鎮（Williamstown）、新南威爾斯州新堡（Newcastle）及雪梨（Sydney）。此外，在官方釋出的最新統計當中，與造艦息息相關的造船基礎建設與港口管理業總產值為 7.19 億澳幣，從業人口 3,766 人。船舶五金業總產值則為 13.5 億澳幣，從業人口 2,803 人。[14]

過去澳洲政府對於國防造艦產業的穩定投資不足，且需求波動幅度過大，因為人才流失、工資短期上漲、仰賴外國新技術等種種原因，以致於造艦成本比美國多出 30 - 40%。[15]澳洲若想降低成本，供需雙方都需要改革既往模式。政府規劃造艦案須避免因生產要素不足與超額需求所帶來的弊病，並從戰略性公共財的角度去看待整體產業生態系：（一）需要持續投入預算充實人才庫，並且導入人力資源規劃概念，以平衡長期的造艦人力供需；（二）需要以政府力量來興建公共造艦基礎設施，降低進入門檻，才能擴大中小企業參與、提高就業外溢效果；（三）需要從政策來協助船廠進行技術升級，才能一步一步降低對外國技術之依賴。就已經發布的各項政策報告內容來看，這些也是澳洲希望努力的方向；總預算規模達 900 億澳幣的澳洲國防部《海軍造艦計畫》，投資項目涵蓋軍艦建造、基礎建設、人才培養等三大面向。從該計畫 2017 年發布以來，澳洲國防部不斷以各種報告向國會與外界凸顯龐大預算背後所代表的永續意涵，強調透過國外廠商主導設計、部分技術移轉、澳洲在地建造、提高國產設備比例的循環模式，來強化澳洲國防自主能力。

---

[14] Australian Institute of Marine Science (AIMS), “The AIMS Index of Marine Industry 2018,” December 2018, pp.25-26, https://www.aims.gov.au/aims-index-of-marine- industry.

[15] John Brikler et al., “Australia’s Naval Shipbuilding Enterprise-Preparing for the 21st Century,” *RAND*, 2015, https://www.rand.org/pubs/research_reports/RR1093.html.

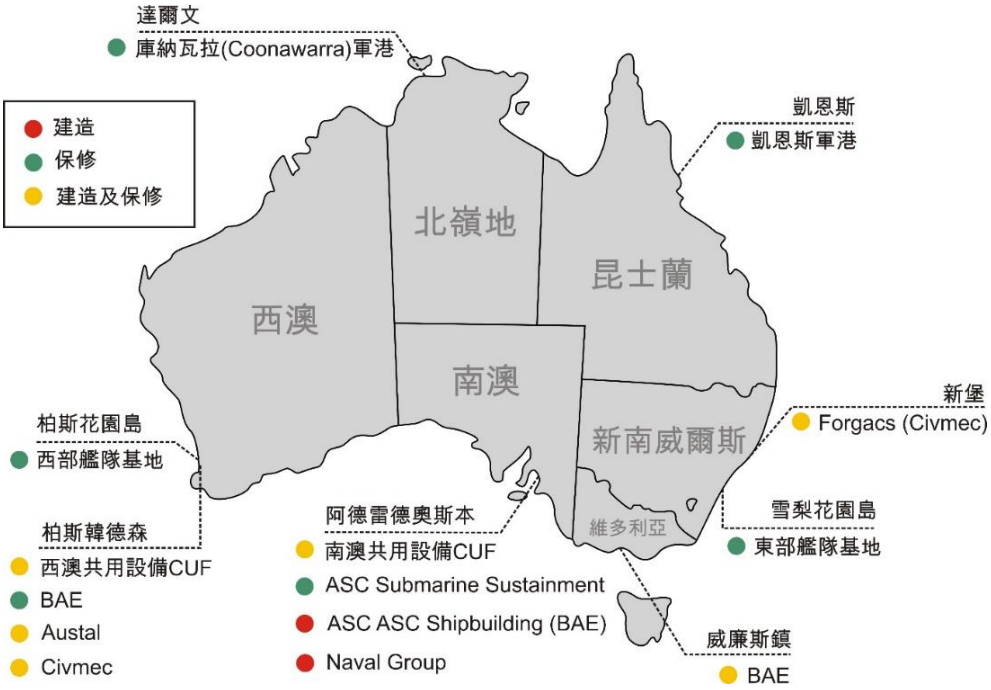


圖 2 澳洲國防造艦產業聚落

資料來源：蔡榮峰整理自公開資訊。

一、主要船廠概況

目前澳洲具有公務船舶建造能力的5家船廠為澳洲本土企業ASC、Austal、Civmec、英國BAE的澳洲分公司、法國海軍集團。而海軍船艦保修主要由8家船廠承包；除上述船廠外，尚包括兩家澳洲企業Defence Maritime Systems Group與Naval Ship Management，[16]以及法國達雷茲澳洲分公司（Thales Australia）。

總部位於西澳的Austal為全球最大鋁構船廠，也是唯一能參與美國海軍造船的外國廠商。[17]而總部位於南澳的國營船廠ASC為全國最大船

[16] 由澳洲本土的兩家企業 Babcock 與 UGL 合資成立。
[17] Andrew Tillett, “Can Australia really be a Top 10 defence exporter?” *The Australian*

廠，地位有如我國的台灣國際造船公司（台船）。2014年澳洲公務船造船業相關從業人員共有7,950人，其中ASC就占了一半左右，可見該公司規模之大。[18]來自法國的海軍集團則是藉著未來潛艦案，成為繼ASC之後，澳洲第二家有能力製造潛艦的船廠。[19]

然而，外界多半認為ASC於柯林斯級潛艦與荷巴特級驅逐艦的建造效率與效果並不理想，遂使澳洲官方欲改變其國艦國造與潛艦國造之模式，向「外國設計、本地製造」模式調整，不過定義國造之門檻仍以60%在澳製造為基準。澳洲官方體認到建造潛艦與水面艦之專業需求區別過大，為了增進效益，已於2016年10月11日宣布將ASC拆解成3個事業體：專責潛艦的「ASC潛艦後勤公司」（ASC Submarine Sustainment）、負責水面艦的「ASC造船公司」（ASC Shipbuilding）、負責相關基礎建設的「ASC海軍基礎設施公司」（ASC Naval Infrastructure）。[20]後兩者引入民間資本與管理，其中「ASC造船公司」現併入BAE，不僅負責建造頭兩艘阿拉芙拉級近海巡邏艇，也參與未來巡防艦計畫。

二、國防造艦產業聚落

澳洲國防造艦產業聚落集中兩地：南澳阿德雷德的奧斯本以及西澳柏斯的韓德森。前者為潛艦與大型水面艦建造地點，後者以小型艦艇建造、潛艦與水面艦保修為主。從主要造艦計畫得標廠商與區域發展的布

Financial Review, January 29, 2018, https://www.afr.com/politics/can-australia-really-be-a-top-10-defence-exporter-20180129-h0prwv.

[18] John Brikler et al., "Australia's Naval Shipbuilding Enterprise-Preparing for the 21st Century," *RAND*, 2015, xxiii, https://www.rand.org/pubs/research_reports/RR1093.html.

[19] 該公司興建中的潛艦廠房，位於南澳阿德雷德 Osborne North 廠區，由 KBR 以及 Aurecon 兩家本土企業參與設計，Laing O'Rourke Australia 建築公司（英商）負責興建，2018 年 12 月正式動工。見 Stephen Kuper, "Major milestones as Future Sub program gathers pace," *Defence Connect*, December 13, 2018, https://www.defenceconnect.com.au/maritime-antisub/3300-major-milestones-as-future-sub-program-gathers-pace 以及 Department of Defence of Australian Government, "Future Submarine construction yard on track," July 31, 2018, https://www.minister.defence.gov.au/minister/christopher-pyne/media-releases/future-submarine-construction-yard-track.

[20] Michael Coggan, "Federal government announces Adelaide-based shipbuilder ASC to be split into three companies," *ABC News*, October 11, 2016, https://www.abc.net.au/news/2016-10-11/shipbuilder-asc-adelaide-to-be-split-into-three-companies/7921894.

局來看，澳洲政府試圖透過分配建造數量來減少聚落競爭成本，以期有效分配國防預算來降低其國內造船業景氣波動之影響（表 6）。

南澳的奧斯本海軍廠區（The Osborne Naval Shipyard）占地約 60 公頃，分為三個部分：生產水面艦的「奧斯本南廠區」（Osborne South）、生產潛艦的「奧斯本北廠區」（Osborne North）、以及包括共用設備（Common User Facility, CUF）在內的「澳洲科技港園區」（Techport Australia）。[21]值得一提的是，澳洲政府將造船基礎建設視為造船案的一環，2018 年已投入 5.35 億澳幣於「奧斯本南廠區」升級工程。[22]

西澳的「韓德森海洋產業區」（Henderson Maritime Precinct）位於該州的「澳洲海洋複合工業區」（Australian Marine Complex）內，占地 35 公頃，約 150 多家廠商聚集在此，國防造艦與商業造船活動皆有之。韓德森海洋產業區南邊的共用設備 CUF，則由西澳的州政府與聯邦政府合資興建。[23]該場址現有浮塢最大噸數 12,000 噸。未來澳洲政府規劃進一步提升至 28,000 噸，足以供坎培拉級直升機船塢登陸艦進行保修作業。[24]

---

[21] 共用設備 CUF 是南澳的州政府為擴大國防造艦聚落，獨資興建之公共財，可供租用，以此降低在地船廠造艦成本。該州政府也成立新單位「澳洲海軍基礎建設局」（Australian Naval Infrastructure, ANI）來協助管理造艦業資產與硬體設施、協調計畫發展以及提供商轉服務。2017 年澳洲聯邦政府以 2.3 億澳幣將南澳 CUF 收歸國有，以便擴大規模。Australian Defence Business Review (ADBR), “Commonwealth acquires shipbuilding facility from SA government,” May 14, 2017, https://adbr.com.au/commonwealth-acquires-shipbuilding-facility-from-sa-government.

[22] Department of Defence of Australian Government, “Future Submarine construction yard on track,” July 31, 2018, https://www.minister.defence.gov.au/minister/christopher-pyne/media-releases/future-submarine-construction-yard-track.

[23] Australian Marine Complex, “Common User Facility,” 2019, https://www.australianmarinecomplex.com.au/common-user-facility.

[24] Department of Defence of Australian Government, “Naval Shipbuilding Plan,” 2017, p.53, https://www.defence.gov.au/navalshipbuilding/Plan.

表 6 澳洲海軍主要國防造艦計畫

造艦計畫代號船級	建造期間	預算/澳幣	載台設計	戰系整合	船體建造聚落	
					西澳韓德森 Henderson	南澳奧斯本 Osborne
SEA1000 未來潛艦計畫 Future Submarine Project ***進擊級 Attack class***	2023-2054	500 億	Naval Group Australia 法商	Lockheed Martin Australia 美商	0	12 艘 Naval Group Australia 法商
SEA5000 未來巡防艦計畫 Future Frigate Program ***獵人級 Hunter class***	2020-2038	350 億	BAE System Australia 英商	Lockheed Martin Australia 美商 /Saab Australia 瑞典商	0	9 艘 ASC Shipbuilding 現 BAE 分公司
SEA1180 近海巡邏艇計畫 Offshore Patrol Vessel Program ***阿拉芙拉級 Arafura class***	南澳 2018-2019 西澳 2020-2030	36 億	AMSEG 德澳合資[25]	Saab Australia 瑞典商	10 艘 Civmec 澳商	2 艘 ASC Shipbuilding 現 BAE 分公司
SEA3036 太平洋巡邏艇更替計畫 Pacific Patrol Boat Replacement Project ***衛士級 Guardian class***	2017-2023	3 億			21 艘 Austal 澳商	0

資料來源：蔡榮峰整理自公開資訊，修改自作者初始版本，見蔡榮峰，〈澳洲「未來潛艦計畫」爭議評析〉，《國防安全週報》，第 28 期，2018 年 12 月 28 日，頁 32-36。

說明：由於圖表涵蓋多間國際廠商，為避免名稱紊亂，本表以原文標示。

[25] 由德國 Lürssen 與澳洲 Civmec 合資成立。

肆、國防造艦經濟與就業機會

澳洲政府將承包軍艦製造的船廠分成三類：載台系統設計（Platform System Designer）、戰系整合工程（Combat System-Systems Engineer）、船體建造（Shipbuilder），不過大致上可分為載台與戰系兩種供應鏈。以水面艦為例，載台與戰系分占總成本的比例大約是 6：4。就載台供應鏈來看，80%的人力將集中在船體結構建造與艤裝兩個項目。

若從船體本身的造船過程來看，則可以分成兩階段：緊扣船艦作戰目標、由大而小的「定義與解構」階段與由下而上組建整艘船並投入實用的「組裝測試」階段。

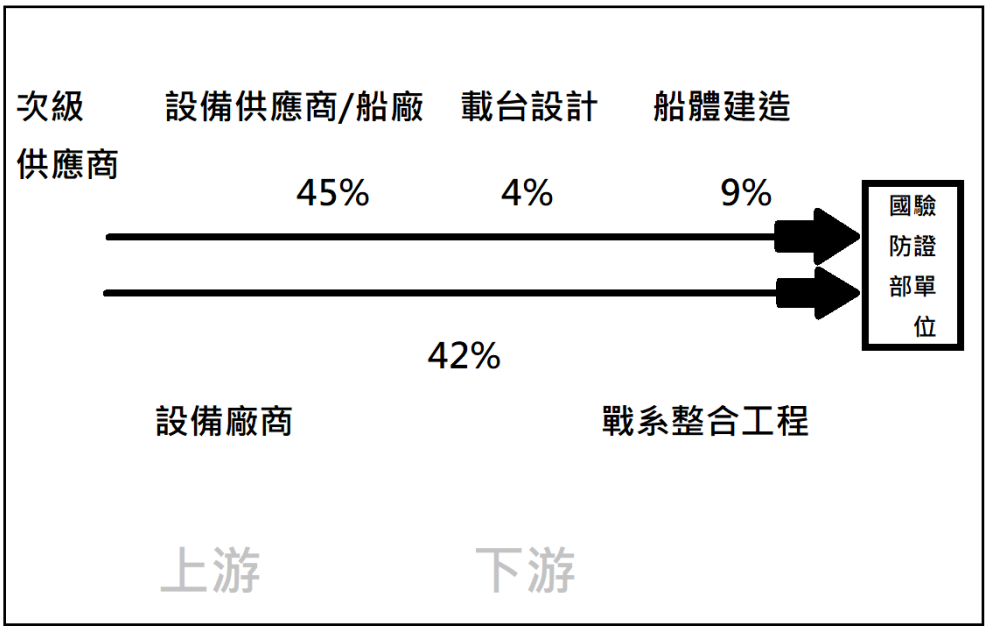


圖 3 澳洲水面艦供應鏈成本分布

資料來源：蔡榮峰重製，整理自 Stefan Markowski, Peter Hall and Robert Wylie, "Australian Naval Procurement Cycles: Lessons for Other Small Countries," Conference Paper of the 5th Annual Acquisition Research Symposium of the Naval Postgraduate School, April 23, 2008, p.376, https://apps.dtic.mil/dtic/tr/fulltext/u2/a493940.pdf.
說明：第一條為載台供應鏈，第二條為戰系供應鏈。

表 7 水面艦船載台供應鏈之人力需求比例

需求職務類別	比例
計畫管理	**10%**
機電工程	**5%**
船體結構	**35%**
艤　　裝	**45%**
支　　援	**5%**

資料來源：蔡榮峰重製，資料整理自 John Brikler et al., “Australia’s Naval Shipbuilding Enterprise-Preparing for the 21st Century,” *RAND*, 2015, p.56.

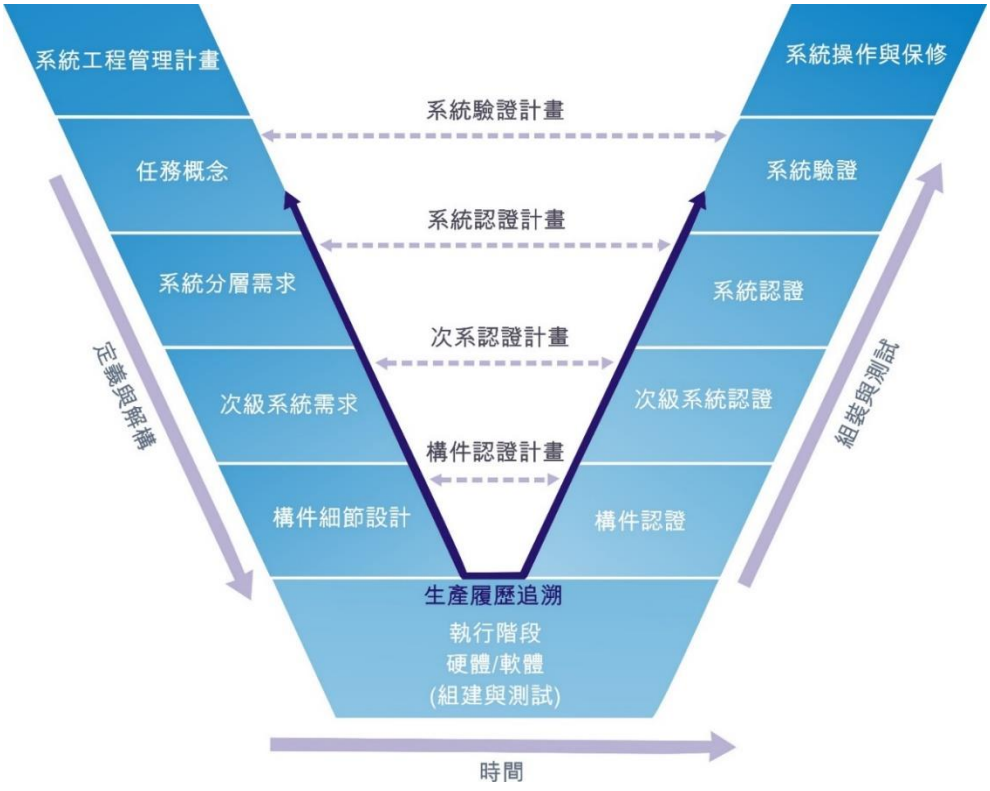


圖 4 造艦流程示意圖

資料來源：蔡榮峰重製，整理自Department of Defence of Australian Government, “Future Submarine Industry Skills Plan,” 2013, p.12, https://www.defence.gov.au/casg/Multimedia/Future_submarines_industry_skilling_plan.pdf.

一、國防造艦人力需求

澳洲目前就下一代潛艦、水面艦及小型艦艇等造艦計畫共造 57 艘船，其中 54 艘在澳建造，[26]投入預算總額達到約 900 億澳幣，這還是只占軍艦全壽期總預算的 30%，剩餘的 70%皆為潛在保修成本。這也意味著本土廠商在造船階段所學習掌握的技術比例越高、後續保修階段能由本土廠商承辦的越多，國防預算所能產生的總體經濟效益也就越高。根據澳洲過往造船經驗，一艘水面艦造經費的 70%，將流向其本土供應鏈當中的中小型企業。[27]

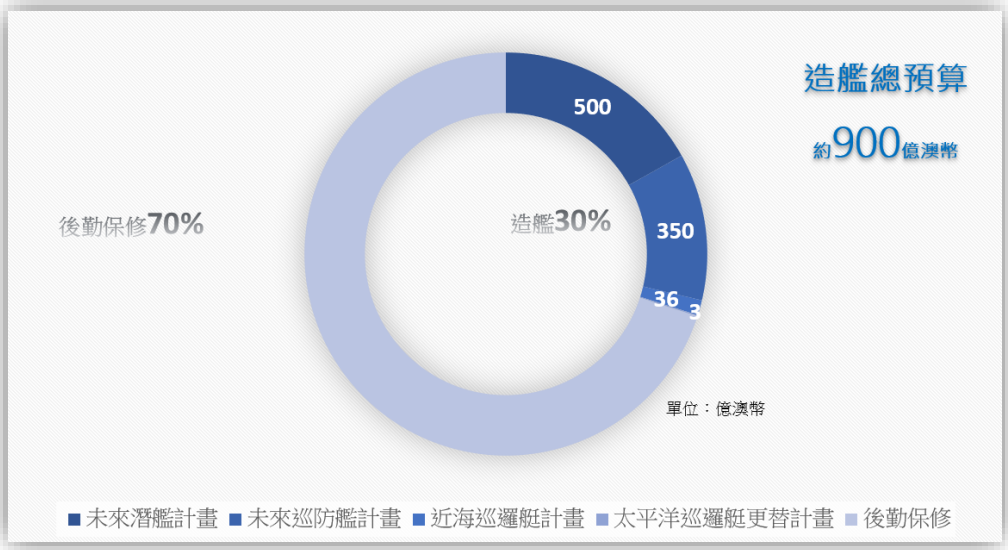


圖 5 澳洲主要國防造艦計畫預算結構

資料來源：蔡榮峰重製，資料整理自 Department of Defence of Australian Government, "Naval Shipbuilding Plan," 2017, p.80, https://www.defence.gov.au/navalshipbuilding/Plan.

---

[26] 含規劃細節尚未公布的獵雷艦與調查船更替計畫以及建軍完成的 3 艘荷巴特級。

[27] 公司雇員 25 人以下為小型，25-200 人為中型。Stefan Markowski et al., "Australian Naval Procurement Cycles Lessons for Other Small Countries," 5th Annual Acquisition Research Symposium of the Naval Postgraduate School, April 23, 2008, p.372, https://apps.dtic.mil/dtic/tr/fulltext/u2/a493940.pdf.

造艦工程、後期保修、造船基礎建設升級工程以及人才培養等項目的人力需求，將於 2026 年前創造 5,200 個與造船工程有關的直接就業機會，並為供應鏈帶來超過 10,000 個間接工作機會，新增總就業機會將超過 15,000 個。[28]其中至少約 8,000 個新的人力需求將集中在國防造艦最大聚落南澳，其次為西澳、新南威爾斯與昆士蘭。[29]造艦計畫預料將為南澳 GDP 帶來至少 3.4%的增長幅度，相當於該州礦業總產值，十分可觀。[30]然而，澳洲海陸空國防工業直接就業人口約 25,000 人，其中與造船相關產業約 10,000 人，該如何填補未來 30 年內所需超過 5,000 人的技術人力缺口，將是能否同時推動諸多大型造船案之關鍵。

2016 年出版的《澳洲國防產業政策聲明》（*Defence Industry Policy Statement*）明確指出，澳洲國防資金之投入應以建立國防自主能力為目標。以澳洲海軍角度來看，造艦計畫必須具備以下三種要件：第一，讓本土廠商有能力建造船艦載台、配裝電戰系統並擁有設備知識產權；第二，國際技術持續轉移，讓本土廠商維持下一代船艦之建造、保修、升級能量；第三，皆須本土廠商參與，以穩定技術人才庫。[31]

澳洲過去建造柯林斯級潛艦與紐澳軍團級巡防艦時，得標船廠招募人力的來源往往與海軍技術人員高度重疊，公私部門競相攬才反而導致海軍人才流失或過早退役，造成挖東牆補西牆的資源錯置情況。

若能配合造艦計畫提前培養所需人才、引入先進管理技術提高生產力，將能大大改善此一情況。因此「海軍造船專科學校」於 2018 年

---

[28] 澳洲自由黨籍眾議員麥克當勞（Hon Ian Macdonald）以及休姆（Jane Hume）認為所有造艦計畫所創造的工作機會最終將達到 25,000 個。The Senate of Parliament of Australia, “Future of Australia’s Naval Shipbuilding Industry – Final Report,” Economics Reference Committee, June 2018, p.145, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Navalshipbuilding45th/Report.

[29] Department of Defence of Australian Government, “Naval Shipbuilding Plan,” 2017, p.18.

[30] Jeremy Thorpe et al., “What we know about the economic benefits of naval shipbuilding for South Australia,” *PWC*, 2017, pp.5-6, https://www.pwc.com.au/publications/pdf/defence-briefing-note-oct17.pdf.

[31] The Senate of Parliament of Australia, “Future of Australia’s Naval Shipbuilding Industry – Final Report,” Economics Reference Committee, June 2018, p.101, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Navalshipbuilding45th/Report.

10 月，正式於南澳首府阿德雷德建立。該校第一階段目標將於 2020 至 2023 年間先培養一批初階技術人員，2023 至 2033 年的第二階注重增加高階技術與特殊需求技能人才比例。不同於前面兩階段以滿足現階段造船案為導向，2033 年後的第三階段焦點將轉向培養永續人才庫。[32]

除了育才專職機構之外，以轉換人力，藉由擴大造船業來改善南澳汽車工業衰退所帶來的結構性失業，也是澳洲政府思考的策略之一。汽車工業的工程、行政、業務人員也都有機會成為造船產業的一部份。因景氣循環失業或退休的造船業資深技術人員應該評估能否重新雇用，來擔任監工、中階主管、技術顧問。礦業、石油與天然氣業的工程人員所持有的專業技術與造船業重疊性相當高，具有轉換跑道的潛力，例如水下焊接鑽油平台的技工經輔導，或可轉職參與潛艦船體焊接工程。

以下就「未來潛艦計畫」與「未來巡防艦計畫」兩案為例，進一步說明澳洲政府對於造艦經濟效益的計算方式。

二、「未來潛艦」與「未來巡防艦」的國防造艦經濟

在澳洲國防造艦的最大聚落所在地南澳，整個州過去曾因為豐田汽車（Toyota）與福特汽車（Ford）等國際汽車大廠相繼關閉工廠，導致 6,500 個工作消失。當地 2015 年失業率一度高達 8.2%，居澳洲之冠。因此，「未來潛艦計畫」是澳洲政府安撫南澳民眾的代表性政策。[33]潛艦國造對於當地經濟來說，有如一劑強心針。可以說，雖然外界對於澳洲「潛艦國造」的首次嘗試多有批評，不過對於南澳民眾說，即使如此，建造柯林斯級潛艦的 16 年間仍為當地帶來了 60 億澳幣的經濟規模。而當年的學習經驗為潛艦國造奠定基礎，讓澳洲政府能在此基礎之上修正政策與執行計畫的擬定方式，過去經驗不足所帶來的風險已可望大幅降低。

一艘大型柴電潛艦約由50萬個組件組成，[34]為期30年的「未來潛艦

---

[32] Department of Defence of Australian Government, “Naval Shipbuilding Plan,” 2017, p.64, 111.

[33] Department of Defence of Australian Government, “Building Submarines in Australia-Aspects of Economic Impact,” May 2015, p.2, https://www.defence.gov.au/FOI/Docs/Disclosures/145_1516_Documents2.pdf.

[34] Stefan Markowski et al., “Australian Naval Procurement Cycles Lessons for Other Small Countries,” 5th Annual Acquisition Research Symposium of the Naval Postgraduate

計畫」，建造12艘進擊級潛艦的人力需求預估能為澳洲本土帶來1,100個直接工作機會，而相關的供應鏈進一步還能提供1,700個工作機會。[35]除了載台設計、戰系整合、船體建造主要承包商之外，全澳洲有資格參與未來潛艦計畫之中小型本土企業達169間。[36]由於投資金額龐大，澳洲國會對於該案是否能促進本國就業市場十分關注，例如澳洲參議院即要求，「未來潛艦計畫」在法國創造的工作職缺上限不得超過50個，藉此確保經濟擴散效果集中於本土。對此法國海軍集團回應在澳雇用人數已從2017年1月的87人上升到2018年6月的130人。[37]

建造軍艦相關系統的先進技術，也會隨著外國廠商與澳洲國防產業的合作，產生擴散效益，例如2018年10月16日，法國沙法倫電子與防衛澳洲分公司（Safran Electronics & Defense Australasia, SEDA）傳出與澳洲先進導航（Advanced Navigation）已簽署合作備忘錄，在共同研製進擊級飛彈潛艦導航系統的前提下，發展海陸通用的慣性導航系統。[38]

School, April 23, 2008, p.372, https://apps.dtic.mil/dtic/tr/fulltext/u2/a493940.pdf.

35 Department of Defence of Australian Government, “Naval Shipbuilding Plan,” 2017, p.26.

36 Naval Group, “Naval Group Signs the Strategic Partnering Agreement,” February 11, 2019, http://naval-group.com.au/2019/02/11/naval-group-signs-the-strategic-partnering-agreement.

37 The Senate of Parliament of Australia, “Future of Australia’s Naval Shipbuilding Industry – Final Report,” Economics Reference Committee, June 2018, p.128, 149, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Navalshipbuilding45th/Report.

38 Stephen Kuper, “Safran signs new partnership with Aussie companies to enhance transfer of sub tech,” *Defence Connect*, October 16, 2018, https://www.defenceconnect.com.au/maritime-antisub/3015-safran-signs-new-partnership-with-aussie-companies-to-enhance-transfer-of-sub-tech.

表 8 潛艦建造技術人力需求分類表

技術種類		技術服務與產品（列舉）
製圖人員	電機	電機系統、電機系統分析與設計、電力控制
	機械	機械系統、系統分析與設計
	管線空調	管線設計、空調系統、排水系統、液壓系統
	結構配置	結構工程、結構配置、系統設計
工程人員	特徵分析	聲學、尾跡、熱力學、電磁學等特徵分析
	戰鬥系統	戰系設計與整合、航行導航系統
	電機	引擎與發電機設計、配電、控制、流量分析、零組件設計與安全分析
	流體	液壓系統、冷卻系統、流體分析、計算流體力學分析、浸水與損管分析
	機械	機械零組件製造、機械設計、機械系統、武器處理系統、輪機系統、輔助系統
檢驗人員	橫向整合	一般與火藥安全、隱蔽性測試、抗衝擊測試、環境測試

資料來源：蔡榮峰重製，資料整理自 Department of Defence of Australian Government, "Future Submarine Industry Skills Plan," 2013, p.53, https://www.defence.gov.au/casg/Multimedia/Future_submarines_industry_skilling_plan.pdf.

估算造船人力需求所衍生的就業機會，澳洲官方採用的方法為工時換算。以獵人級飛彈巡防艦為例，一艘巡防艦約由 17 萬個部件組成，[39] 首艘需時 550 萬人工小時，若以學習曲線比例 95%來算，第二艘只需要 500 萬人工小時，後續各艘船艦耗時以此類推，而最後 6 艘出廠頻率（drumbeat）可達到 1 年 1 艘。[40]因此「未來巡防艦計畫」所帶來的經濟效應，若以人力需求高峰期的 2028 年來看，單年度預估創造的工作

[39] Stefan Markowski et al., "Australian Naval Procurement Cycles Lessons for Other Small Countries," 5th Annual Acquisition Research Symposium of the Naval Postgraduate School, April 23, 2008, p.372, https://apps.dtic.mil/dtic/tr/fulltext/u2/a493940.pdf.

[40] John Brikler et al., "Australia's Naval Shipbuilding Enterprise-Preparing for the 21st Century," p.53.

達 6,310 個，其中光是船體設計得標廠商 BAE 就占了約 2,360 個。這意味著「未來巡防艦計畫」當中，澳洲廠商參與較多的船體建造部分，預算投入將能產生槓桿效應，為整體就業機會帶來加乘效果。該計畫創造的工作機會乘數約為 2.7 倍；也就是說該計畫每產生 1 個工作機會，就為澳洲整體就業市場增加 2.7 個工作機會。

表 9 澳洲水面艦建造工時

船級	排水量/噸	單艘人工小時/萬小時	期間/季
獵人級飛彈巡防艦 Hunter class FFG	8,800	首艘　550	26
		第二艘　500	24
阿拉芙拉級近海巡邏艇 Arafura class OPV	1,640	70	12
衛士級太平洋巡邏艇 Guardian class PB	約 160[41]	1.4	5
荷巴特級飛彈驅逐艦 Hobart class DDG	7,000	552.4	22

資料來源：蔡榮峰重製，資料整理自 John Brikler et al., “Australia’s Naval Shipbuilding Enterprise-Preparing for the 21st Century,” *RAND*, 2015, p.175.

就經濟產值來看，獵人級飛彈巡防艦的船體設計與建造部分，到了 2028 年度將有機會為澳洲 GDP 直接貢獻約 4.2 億澳幣，上游供應鏈則為 2.33 億澳幣，後續消費需求的擴散效應達 9.8 億澳幣，GDP 乘數為 2.3；也就是說，此計畫在該年度每投入 1 塊澳幣國防預算，就會產生

[41] 官方未公布，不過前一代太平洋巡邏艇排水量為 162 噸。

2.3 塊澳幣的經濟產值。若拉長 30 年來看（2018-2048 年），其 GDP 乘數為將為 2.4 倍，GDP 增額達到 170.2 億澳幣，包括直接貢獻 70.6 億澳幣，上游供應鏈 43.7 億澳幣，後續消費需求的擴散效應 55.9 億。[42]全澳洲有資格參與未來巡防艦計畫之本土企業至少達到 500 間，[43]預期該造船案將為澳洲產業界帶來可觀的經濟產值。

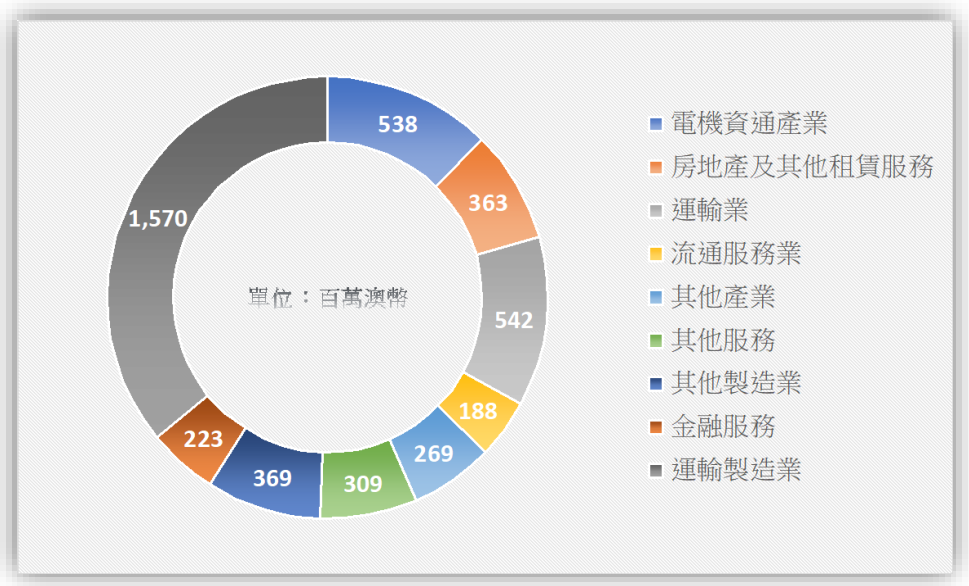


圖 6 2018-2048 年獵人級飛彈巡防艦船體供應鏈產值預估

資料來源：蔡榮峰重製，資料整理自 BIS Oxford Economics, “The Economic Contribution of BAE Systems in Australia,” November 2018, p.25, https://www.baesystems.com/en-aus/download-en-aus/20181127151654/1434623092503.pdf。

[42] BIS Oxford Economics, “The Economic Contribution of BAE Systems in Australia,” November 2018, pp.22-24, https://www.baesystems.com/en-aus/download-en-aus/20181127151654/1434623092503.pdf.

[43] Andrew Greene, “Hunter class frigates will be built by BAE in Australia — but what can the warships do and why do we need them?” *ABC News*, June 29, 2018, https://www.abc.net.au/news/2018-06-29/hunter-frigate-build-bae-what-you-need-to-know/9923912.

伍、結論

澳洲國防部近年陸續公布《2016 國防白皮書》、《2016 整合投資計畫》、《2016 國防產業政策聲明》等三份文件擬定戰略走向，希望為其海軍建立可長可久的國防工業能力以及產業生態系。澳洲海軍則依其戰略國防目標，規劃出未來 30 年的建軍方向。坎培拉規劃以「國外廠商主導設計、部分技術移轉、澳洲在地建造、提高國產設備比例」的模式，在國防自主與建造效用之間取得平衡，除了滿足建軍作戰需求之外，也藉著政府預算的投入帶動國防產業升級，讓澳洲相關企業能逐漸往國際供應鏈的上游移動。澳洲有意在 10 年內躋身全球前十大國防產業出口國。

澳洲國防造艦策略近年來則明顯出現兩條發展路線：以大型船艦吸收外國技術，以落實自製率之提升，同時以小型艦艇布局全球市場並作為區域外交之利器。對澳洲整體社會來說，發展國艦國造更重要的意義在於，藉由資格審定、程序標準化來擴大全國產業界的參與，讓中小企業雨露均霑。逐步健全國防產業鏈之餘，也間接強化軍民關係、培養全民國防的意識。

澳洲在國防造艦產業的發展策略上，以維持同等級的國防廠商至少兩家以上的方式來維持其競爭力。值得一提的是，在船艦的計畫中，澳洲聯邦政府也將廠商區位因素、國家區域發展平衡納入整體考量，刻意透過「大船南澳造、小船西澳造」的發展策略，減少國內產業聚落的競爭成本，並依照這個目標，在新一輪的國艦國造預算當中為兩大聚落規劃各自的基礎建設升級預算。尤其南澳「海軍造船專科學校」之設立即一代表性指標，象徵澳洲產官學界合作培養未來發展性之決心。澳洲從人才供給與市場需求兩方面著手，企圖降低造船業景氣波動對國防工業能力的負面影響。

儘管澳洲公眾對於過去同樣標榜「國艦國造」的柯林斯級潛艦與荷巴特級飛彈巡防艦建軍過程多有批評，但也看得出來澳洲國防部在新一輪的建軍案當中，產業布局與人才培育被納入規劃，並強調永續性的重要，希望藉此帶動整體的產業升級並擴大國防預算所能帶來的經濟效應。可以說，總人口與台灣差不多的澳洲，其經驗為我國帶來了寶貴的啟示。

參考書目

一、研究機構報告

蔡榮峰，〈澳洲「未來潛艦計畫」爭議評析〉，《國防安全週報》，第 28 期，2018 年 12 月 28 日，頁 32-36。

BIS Oxford Economics, "The Economic Contribution of BAE Systems in Australia," November 2018, https://www.baesystems.com/en-aus/download-en-aus/20181127151654/1434623092503.pdf.

Colton, Greg, "Stronger Together: Safeguarding Australia's Security Interests through Closer Pacific Ties," Lowy Institute, April 2018.

Hellyer, Marcus, "Special Report-Thinking through Submarine Transition," *ASPI*, October 2018, https://www.aspi.org.au/report/thinking-through-submarine-transition.

Brikler, John, et al., "Australia's Naval Shipbuilding Enterprise-Preparing for the 21st Century," *RAND*, 2015, https://www.rand.org/pubs/research_reports/RR1093.html.

Thorpe, Jeremy, et al., "What we know about the economic benefits of naval shipbuilding for South Australia," *PWC*, 2017, https://www.pwc.com.au/publications/pdf/defence-briefing-note-oct17.pdf.

二、研討會論文

Markowski, Stefan, Peter Hall and Robert Wylie, "Australian Naval Procurement Cycles: Lessons for Other Small Countries," Conference Paper of the 5th Annual Acquisition Research Symposium of the Naval Postgraduate School, April 23, 2008, https://apps.dtic.mil/dtic/tr/fulltext/u2/a493940.pdf.

三、官方文件

Australian National Audit Office (ANAO), "Air Warfare Destroyer Program," 2014, https://www.anao.gov.au/work/performance-audit/air-warfare-destroyer-program.

Australian National Audit Office (ANAO), "Future Submarine—Competitive Evaluation Process," 2017, https://www.anao.gov.au/work/performance-audit/future-submarine-competitive-evaluation-process.

Australian Institute of Marine Science (AIMS), "The AIMS Index of Marine

Industry 2018," December 2018, https://www.aims.gov.au/aims-index-of-marine-industry.

Department of Defence of Australian Government, "Future Submarine Industry Skills Plan," 2013, https://www.defence.gov.au/casg/Multimedia/Future_submarines_industry_skilling_plan.pdf.

Department of Defence of Australian Government, "Building Submarines in Australia-Aspects of Economic Impact," May 2015, https://www.defence.gov.au/FOI/Docs/Disclosures/145_1516_Documents2.pdf.

Department of Defence of Australian Government, "2016 Defence White Paper," 2016, https://www.defence.gov.au/WhitePaper.

Department of Defence of Australian Government, "2016 Integrated Investment Program," 2016, https://www.defence.gov.au/WhitePaper/Docs/2016-Defence-Integrated-Investment-Program.pdf.

Department of Defence of Australian Government, "2016 Defence Industry Policy Statement," 2016, https://www.defence.gov.au/WhitePaper/Docs/2016-Defence-Industry-Policy-Statement.pdf.

Department of Defence of Australian Government, "Naval Shipbuilding Plan," 2017, https://www.defence.gov.au/navalshipbuilding/Plan.

Department of Defence of Australian Government, "Annual Report 2017-18," 2018, http://www.defence.gov.au/annualreports/17-18/Features/Maritime.asp.

Department of Defence of Australian Government, "Annual Report 2018-19," September 2019, https://www.defence.gov.au/AnnualReports/18-19.

Department of Defence of Australian Government, "Defence Export Strategy," 2018, https://www.defence.gov.au/Export/Strategy.

Department of Defence of Australian Government, "2018 Defence Industrial Capacity Plan," 2018, https://www.defence.gov.au/SPI/Industry/CapabilityPlan/Docs/DefenceIndustrialCapabilityPlan-web.pdf.

The Senate of Parliament of Australia, "Future of Australia's Naval Shipbuilding Industry – Final Report," Economics Reference Committee, June 2018, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Navalshipbuilding45th/Report.

四、網際網路資料

Austal, “Pacific Patrol Boat (Guardian Class),” https://www.austal.com/ships/pacific-patrol-boat-guardian-class.

Australian Defence Business Review (ADBR), “Commonwealth acquires shipbuilding facility from SA government,” May 14, 2017, https://adbr.com.au/commonwealth-acquires-shipbuilding-facility-from-sa-government.

Australian Defence Business Review (ADBR), “ANZAC Midlife Capability Assurance Program,” December 17, 2018, https://asiapacificdefencereporter.com/anzac-midlife-capability-assurance-program.

Australian Marine Complex, “Common User Facility,” 2019, https://www.australianmarinecomplex.com.au/common-user-facility.

Coggan, Michael, “Federal government announces Adelaide-based shipbuilder ASC to be split into three companies,” *ABC News*, October 11, 2016, https://www.abc.net.au/news/2016-10-11/shipbuilder-asc-adelaide-to-be-split-into-three-companies/7921894.

Department of Defence of Australian Government, “Future Submarine construction yard on track,” July 31, 2018, https://www.minister.defence.gov.au/minister/christopher-pyne/media-releases/future-submarine-construction-yard-track.

Greene, Andrew, “BAE Systems beats Spanish and Italian designs for $35 billion warship building program,” *ABC News,* June 29, 2018, https://www.abc.net.au/news/2018-06-29/bae-systems-selected-for-warship-building-program/9922666.

Greene, Andrew, “Hunter class frigates will be built by BAE in Australia — but what can the warships do and why do we need them?” *ABC News*, June 29, 2018, https://www.abc.net.au/news/2018-06-29/hunter-frigate-build-bae-what-you-need-to-know/9923912.

Kuper, Stephen, “Sub scuttlebutt: SEA 1000 in deep water, or is it?” *Defence Connect*, October 8, 2018, https://www.defenceconnect.com.au/maritime-antisub/2978-sub-scuttlebut-sea-1000-in-deep-water-or-is-it.

Kuper, Stephen, “Safran signs new partnership with Aussie companies to enhance transfer of sub tech,” *Defence Connect*, October 16, 2018, https://www.defenceconnect.com.au/maritime-antisub/3015-safran-sign

s-new-partnership-with-aussie-companies-to-enhance-transfer-of-sub-tech.

Kuper, Stephen, "Major milestones as Future Sub program gathers pace," *Defence Connect*, December 13, 2018, https://www.defenceconnect.com.au/maritime-antisub/3300-major-milestones-as-future-sub-program-gathers-pace.

McHugh, Gary, "New shipyard tower to increase productivity," *Navy Daily*, January 9, 2019, http://news.navy.gov.au/en/Jan2019/Fleet/5017.

Naval Group, "Naval Group Signs the Strategic Partnering Agreement," February 11, 2019, http://naval-group.com.au/2019/02/11/naval-group-signs-the-strategic-partnering-agreement.

Royal Australian Navy, "Hunter Class FFG," http://www.navy.gov.au/fleet/ships-boats-craft/future/ffg.

Royal Australian Navy, "Arafura Class OPV," http://www.navy.gov.au/fleet/ships-boats-craft/future/opv.

Tillett, Andrew, "Can Australia really be a Top 10 defence exporter?" *The Australian Financial Review*, January 29, 2018, https://www.afr.com/news/politics/can-australia-really-be-a-top-10-defence-exporter-20180129-h0prwv.

Tillett, Andrew, "Shipbuilding capacity expanding as regional clients beckon," *Australian Financial Review*, October 3, 2018, https://www.afr.com/policy/foreign-affairs/shipbuilding-capacity-expanding-as-regional-clients-beckon-20180927-h15x9u.

Tran, Pierre, "How a French firm beat out Japanese companies in Australia's submarine tender," *Defense News*, November 21, 2017, https://www.defensenews.com/global/europe/2017/11/21/how-a-french-firm-beat-out-japanese-companies-in-australias-submarine-tender.

Cyber Wargaming: Grappling with Uncertainty in a Complex Domain

Miguel Alberto Gomez

Senior Researcher

Center for Security Studies

ETH Zurich

Christopher Whyte

Assistant Professor

L. Douglas Wilder School of Government and Public Affairs

Virginia Commonwealth University

Abstract

Cybersecurity literature depends heavily on observational studies to discern state-behavior during periods of conflict. Frequently, underlying motivations that govern the exercise of cyber power are inductively perceived through the lens of the existing strategic environment. While this approach continues to contribute to the advancement of this burgeoning area of study, it is fundamentally constrained by the secretive nature of interstate cyber operations. Moreover, observational studies that analyze state-level actions offer limited insight regarding the individual and group-level mechanisms from which these emerge. The need to move towards these levels of analysis is made even more salient by the uncertainty that permeates this domain that provokes a host of cognitive biases that influence strategic preferences. Consequently, this article offers readers an overview as to the benefits of wargaming as a tool to improve our understanding of crisis decision-making within the cyber domain.

Keywords: *Cybersecurity, Wargame, Experiment, Decision Making*

網路兵推：複雜領域中的不確定性

Miguel Alberto Gomez

資深研究員

蘇黎世聯邦理工學院安全研究中心

Christopher Whyte

助理教授

維吉尼亞聯邦大學 L. Douglas Wilder School 政府與公共事務學院

摘　要

網路安全文獻在很大程度上依賴於觀察研究來識別衝突期間的國家行為。通常，通過現有戰略環境的視角來歸納地認知控制網路力量行使的潛在動機。雖然這種方法繼續為這一新興研究領域的發展做出貢獻，但從根本上，其受到國際網路運營秘密性的限制。此外，分析國家級行動的觀察性研究，對產生這些機制的個人和團體級機制的瞭解有限。滲透到這個領域的不確定性，使這些不同分析層次的需求更加突出，該不確定性引發了許多影響戰略偏好的認知偏見。因此，本文為讀者提供了關於兵棋推演作為一種工具的概述，該工具可以增進我們對網路領域危機決策的理解。

關鍵詞：網路安全、兵棋、實驗、決策

I. Introduction

The past decade has seen the increased usage of cyber capabilities by states to further foreign policy interests. Via the exploitation of the instruments and characteristics of strategic engagement of this human-made domain, belligerent state actors have successfully stolen large volumes of intellectual property, interfered with the operation of critical infrastructure facilities, and influenced the internal political processes of more than two dozen countries. With organizational and technological capabilities advancing year-on-year and with no apparent pause in the exercise of power, the recent characterization of interactions within this space as necessarily persistent appears apt.[1] However, despite most incidents occurring well-below the threshold of armed conflict, the absence of escalation is far from guaranteed.[2] Recent events such as the kinetic response by Israel to Hamas cyber operations, while not a perfect example, highlights the potential for a militarized retaliatory strike. Moreover, with most state-to-state interactions in cyberspace framed in the context of existing rivalry dynamics, the threat of escalation remains a reality should the appropriate conditions come to the fore.[3]

Some would argue that continued interactions between states online should eventually lead to the normalization of "acceptable" and even agreed-upon cyber conflict behavior.[4] Even were that the case,

---

1 Brandon Valeriano and Ryan C. Maness, "The dynamics of cyber conflict between rival antagonists, 2001-11," *Journal of Peace Research*, Vol. 51, No. 3, May 2014, pp.347-360.

2 The lack of escalation may be rooted in the limited effects of these operations.

3 Brandon Valeriano and Ryan C. Maness, *Cyber war versus cyber realities : cyber conflict in the international system* (New York: Oxford University Press, 2015); Erik Gartzke and Jon R. Lindsay, "Thermonuclear cyberwar," *Journal of Cybersecurity*, Vol. 3, No.1, March 2017, pp.37-48.

4 Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace," *Lawfare*, November 9,

misperception among decision-makers and publics continues to exist as a match that could light the tinderbox of prospective escalation. Misperception may emerge from sudden shifts in strategy between rival states, and the ease of access with which certain actors may obtain offensive capabilities[5] may provoke a shift in the status quo that an opposing party may interpret as a move towards aggression. This situation is further complicated by the inherent uncertainty surrounding the domain that weighs heavily on our inherent cognitive limitations and our dependence on motivated reasoning.[6] Moreover, while the available evidence illustrates the limits of cyber operations relative to their conventional counterparts, biased thinking may result in an inappropriate reaction from those affected by these activities.

Although the complete mitigation of bias is unlikely to occur, acknowledging its presence serves to temper the worst of its effects. At the level of the individuals, this requires one to be aware of what triggers the emergence of this phenomenon and how best to minimize its occurrence. From an organizational perspective, this implies an understanding of both organizational structure and culture that can either decreases or enhances biased thinking. While these lessons may be learned from past failures, adopting this reactive approach is unsuitable given the pace of engagement

---

2018, https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward- constructing-norms-cyberspace.

5 Primarily through illicit markets online. Though this approach does constrain the extent of damage possible. Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security*, Vol. 41, No. 3, January 2017, pp.72-109.

6 Jacquelyn Schneider, 2017; Miguel Alberto Gomez, "Sound the alarm! Updating beliefs and degradative cyber operations," *European Journal of International Security*, Vol. 4, No. 2, June 2019, pp.190-208; Miguel Alberto Gomez and Eula Bianca Villar, "Fear, Uncertainty, and Dread: Cognitive Heuristics and Cyber Threats," *Politics and Governance*, Vol. 6, No. 2, June 2018, pp.61-72.

in cyberspace. Consequently, simulations in the form of wargames provide policy elites and critical organizations the opportunity to observe the effects of biased reasoning and to develop the necessary measures to contain its effects in a controlled environment.

To this end, this article offers readers an overview as to the benefits of cyber wargaming as a tool to improve crisis decision-making. The article progresses by first establishing uncertainty as a crucial characteristic within cyberspace that, in turn, prompts the use of biased reasoning. It then progresses to discussing how wargaming serves as an ideal instrument through which to demonstrate our dependence on these biases and its effects on decision-making. From this point, the article presents readers with the beneficial outcomes of three cyber wargames; the first being a series of annual wargames conducted at the Naval War College, this is followed by a largescale cross-population wargame, and the final simulation being that facilitated by the authors of this article. The article then moves on to provide general guidelines on how readers may develop their cyber conflict wargames and concludes with providing a discussion on the future of wargames in the context of interstate cyber dispute

II. Uncertainty in Cyberspace

A. Technological Uncertainty

Uncertainty is a fundamental characteristic of interstate interactions. Whether it be a question of intent, capabilities, or meaning, the presence of uncertainty constraints our ability to meet the stringent requirements of rational choice.[7] For cyberspace, uncertainty is a function of both the

[7] James D. Fearon, "Rationalist Explanations for War," *International Organization*, Vol. 49, No. 3, Summer 1995, pp.379-414; Dominic Johnson and Dominic Tierney, "The Rubicon theory of war: how the path to conflict reaches the point of no return," *International Security*, Vol. 36 No.1, Summer 2011, pp.7-40; Daniel Kahneman, "A

unique characteristics of this space as well as the strategic environment through which cyberspace is fast becoming an adjunctive instrument of statecraft.[8] Consequently, uncertainty at both these levels facilitates the emergence of biased reasoning from those that respond to cyber incidents.

It is fair to say that cyberspace is the only genuinely human-made operational space. While land, sea, air, and space are, to an extent, malleable, only in cyberspace do we have almost complete control of the laws that govern action and consequences. Although consensus regarding the exact nature of cyberspace continues to elude us, we can characterize this space as consisting of three unique yet interdependent levels: physical, syntactic, and semantic.[9]

The physical level is best described as consisting of the hardware that allows for the transmission and processing of data as either electrical signals, pulses of light, or waves within the electromagnetic spectrum. This level encompasses the physical hardware that allows computation to take place. Above this is the syntactic level that is governed by unique protocols that enable computers to process the transmitted signals. Artifacts such as operating systems and applications exist at this layer. These protocols allow for interoperability across different manufacturers. Finally, the semantic represents the human-readable information itself that can be presented within a standalone environment (e.g., a PDF document on your computer)

---

perspective on judgment and choice - Mapping bounded rationality," *American Psychologist*, Vol. 58, No. 9, September 2003, pp.697-720.

8 Benjamin Dean and Rose McDermott, "A Research Agenda to Improve Decision Making in Cyber Security Policy," *Penn State Journal of Law & International Affairs*, Vol. 5, No. 1, April 2017, pp.29-71; Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (London: Hurst & Company, 2017); Brandon Valeriano, Benjamin Jensen and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018).

9 Martin C. Libicki, *Cyberdeterrence and cyberwar* (Santa Monica, CA.: Rand Corporation, 2009).

or in a networked space (e.g., posts on Facebook).

To demonstrate the functionality of these levels, imagine how an e-mail is sent. A sender first decides on a specific message to transmit and then types this into an e-mail client (Semantic). The e-mail client then formats this message per the transmission protocol (Syntactic). Once formatted, the computer then transforms this information into electromagnetic signals to be sent across a network such as the Internet to the recipient (Physical). Once received, the recipient's computer then reconstructs these signals into the appropriate format as required by the protocol (Syntactic), which the e-mail client then presents to its user in a human-readable form (Semantic).

Despite the seeming simplicity of the above process, uncertainty emerges through several mechanisms. Foremost among these is the overall complexity of cyberspace given the linkages between individual computers and networks operating within this space. This interconnectedness increases overall complexity that limits our ability to predict points of failure and its corresponding consequences.[10] Moreover, this sense of unknowability is further aggravated by the concern – merited or otherwise – of the possibility of cascading effects between the three levels.[11] For instance, a disruption in the Physical level will undoubtedly affect our ability to transmit signals between two points that eventually affect both the Syntactic and Semantic levels as well. Similarly, the manipulation of the protocols governing the Syntactic level can result in incorrect information being presented at the Semantic level.

---

[10] Charles Perrow, *Normal accidents: living with high-risk technologies Princeton paperbacks* (Princeton, NJ.: Princeton University Press, 1984).

[11] Ilai Saltzman, "Cyber posturing and the offense-defense balance," *Contemporary Security Policy*, Vol. 34, No. 1, March 2013, pp.40-63; Myriam Dunn Cavelty, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse," *International Studies Review*, Vol. 15, No. 1, January 2013, pp.105-122.

Further complicating this situation is the persistent lack of expertise concerning this domain. Hansen and Nissenbaum[12] argue further that this lack of domain expertise contributes to the hyper-securitization of cyberspace, further contributing to notions of "cyber doom" as a result of malicious behavior aimed at critical infrastructure. This exaggeration of effects is apparent in a study by Jarvis, Macdonald, and Whiting[13] that demonstrate the persistence of headlines over the past decade that frame cybersecurity incidents through these apocalyptic analogies.

While the use of analogies is a common cognitive short-cut that allows aids in the comprehension of a complex phenomenon in uncertain situations, bias ensues when it fails to depict reality accurately. The use of analogies during periods of political crisis is relatively common, references to Munich or Pearl Harbor tend to surface in response to autocratic leaders or periods of surprise. However, the context between the original events and their intended parallels are rarely mirror images of one another. As a result, the lessons from those cases may not be wholly suitable for the present.[14]

In the context of cyberspace, events akin to 9/11 or Pearl Harbor have yet, if ever, to occur.[15] The exercise of cyber power resulting in first-order

---

[12] Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly*, Vol. 53, No. 4, December 2009, pp.1155-1175.

[13] Lee Jarvis, Stuart Macdonald, and Andrew Whiting, "Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat," *European Journal of International Security*, Vol. 2, No. 1, February 2017, pp.64-87.

[14] Robert Axelrod, "A Repertory of Cyber Analogies," in Emily O. Goldman and John Arquilla, eds, *Cyber Analogies* (Monterey, CA: Dept. of Defense Information Operations Center for Research, 2014); Yuen Foong Khong, *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965* (Princeton, NJ.: Princeton University Press, 1992).

[15] Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *The New York Times*, October 11, 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

effects that result in the loss of life.[16] Furthermore, the idea of a sustained assault on an adversary's cyber infrastructure that would force a regime and its populace to yield is unlikely given the immense resource requirements and the availability of conventional alternatives.[17] However, despite the available evidence, political elites continue to promote the idea of an apocalyptical attack against critical cyber infrastructure that, in turn, result in increasingly aggressive strategies being developed.[18]

B. Strategic Uncertainty

Apart from technical considerations, uncertainty is also associated with the strategic environment in which cyber power is exercise. Although early advocates promoted the idea of the domain's a-strategic nature, empirical evidence highlights the strategic context in which interstate interactions within this space takes place.[19] Maness and Valerianio note that cybersecurity incidents often occur between established rivals within a given region.[20] Rarely do we observe cybersecurity incidents occurring without a preexisting strategic cause, whether this be political, economic, or military. Furthermore, both authors argue that exchanges between these rivals are also characterized by stability resulting from past interactions with one another. While this suggests a degree of understanding between adversaries, uncertainty can still emerge through capability acquisition,

---

[16] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, Vol. 35, No. 1, February 2012, pp.5-32.

[17] Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies*, Vol. 26, No. 3, May 2017, pp.452-481.

[18] The 2018 United States strategy best represents this shift towards increased aggression and engagement. USA. "National Cyber Security Strategy of the United States of America," 2018.

[19] Colin S. Gray, *Making Strategic Sense of Cyber Power: Why The Sky is Not Falling* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2013).

[20] Op. cit, pp.347-360.

perceived intent, and motivated reasoning.[21]

An enduring myth surrounding the exercise of cyber power is the notion of the low cost of entry into this space.[22] While it is easy to trace the roots of this belief to the ready availability of capabilities, it should be noted that the utility gained from its usage is directly proportional to the resources spent on its development.[23] Phrased another way, while tools to take down websites or botnets to conduct Distributed Denial-of-Service attacks are easily accessed, the ability to inflict lasting damage requires additional investment.

On the surface, this suggests that truly damaging attacks are limited to a handful of actors with the appropriate material and organizational resources to mount an effective attack. However, a shift from the status quo due to the appearance of new capabilities may trigger a security dilemma between rivals despite the actual effects.[24] This is particularly true if the targets are increasingly dependent on cyberspace. Cognitive phenomenon such as the endowment effect and negativity bias can prompt an overreaction on the part of the targets regardless of the actual damage suffered.[25] This situation could encourage the slighted party to develop capabilities to operate in cyberspace – further destabilizing the precarious balance.

---

[21] Buchanan, Op. cit.

[22] Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security*, Vol. 41, No. 3, January 2017, pp.72-109; Op. cit., pp.452-481; Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, Vol. 22, No. 3, July 2013, pp.365-404.

[23] Adam Liff, "Cyberwar: a new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war," *Journal of Strategic Studie*s, Vol. 35, No. 3, June 2012, pp.401-428. Ibid.

[24] Buchanan, Op. cit.

[25] Dominic Johnson and Dominic Tierney, "Bad World: The Negativity Bias in International Politics," *International Security*, Vol. 43, No. 3, February 2019, pp.96-140.

Apart from the acquisition of capabilities, the exercise of such also raises questions of intent. The use of conventional weapons is commonly associated with destructive intent. Malicious code, however, serves to establish a foothold in a privileged system to either exfiltrate privileged information or cause damage at a later date. This characteristic of dual-usage opens up the possibility for misperception on the part of the target that is further aggravated by the system affected.[26] A compromise of the national tax system may be of limited consequence while gaining access to a state's Nuclear Command, Control, and Communications (NC3) would have genuine consequences.

This ambiguity of intent is further worsened by the emergence of motivated reasoning that individuals may use to explain events in the absence of complete information while still maintain pre-existing beliefs.[27] Since interactions in cyberspace are strategic in nature, past experience may serve to frame actions in the present. If an adversary demonstrated belligerence in the past, an enemy image[28] might exist to inform judgments in the present.[29] Moreover, since individuals tend to maintain beliefs rather than expend precious cognitive resources to re-evaluate them, it seems likely that a target may perceive this incident as an attempt by an adversary to further its interests at the cost of the target. In conjunction with limited

---

[26] Op. cit., pp.37-48; Buchanan, Op. cit.

[27] Ziva Kunda, "The case for motivated reasoning," *Psychological Bulletin*, Vol. 108, No. 3, December 1990, pp.480-498; Robert Jervis, *Perception and misperception in international politics*. New edition. ed. (Princeton, NJ.: Princeton University Press, 1976); Robert Jervis, "Understanding beliefs and threat inflation," in Trevor A. Thrall and Jane K. Creamer, eds., *American Foreign Policy and the Politics of Fear: Threat Inflation since 9/11,* (Abingdon-on-Thames, UK: Routledge, 2009), pp. 16-39.

[28] Preconceived notion of how a potential adversary behaves based on past cases.

[29] Ole R. Holsti, "The Belief System and National Images: A Case Study," *The Journal of Conflict Resolution*, Vol. 6, No. 3, September 1962, pp.244-252; Ole R. Holsti, "Cognitive Dynamics and Images of the Enemy," *Journal of International Affairs*, Vol. 21, No. 1, 1967, pp.16-39.

familiarity with cyberspace and the use of analogies, the destabilization of the status quo is perceived to be more likely as a result of this biased reasoning.

C. Real-World Cases

While it would be easy to dismiss the logic previously laid out, several real-world cases demonstrate biased reasoning stemming from some of the mechanisms established previously. Incidents such as Solar Sunrise, the Estonia DDoS, and the Pyeongchang Olympics highlight the emergence of biased reasoning.

Over three weeks in February 1998, the United States Department of Defense suffered a series of attacks against its unclassified computer networks. These incidents utilized several known operating system vulnerabilities that allowed for the exfiltration of data. The sources of the attacks appeared wide-spread and were thought to have originated from countries such as Israel, the United Arab Emirates, France, etc. These attacks occurred when the United States was preparing possible military action against Iraq due to weapons inspection issues. As such, it was initially assumed that the source of these incidents was the Iraqi regime, given the timing and surrounding strategic context. Later analysis revealed, however, that teenagers in the United States and Israel were responsible.[30]

Similarly, the massive Distributed Denial-of-Service attack against Estonia in 2007 appears to highlight biased reasoning on the part of political elites when attributing the incident to the Russian Federation. Stemming from the decision to move a World War II Memorial, Estonia experienced a series of attacks that disrupted government and financial systems. Based on

---

[30] Richard Power, "The Solar Sunrise Case: Mak, Stimpy, and Analyzer Give the DoD a Run for Its Money," *informit*, October 30, 2000, http://www.informit.com/articles/article.aspx?p=19603&seqNum=4.

reports leaked through the whistleblower website WikiLeaks, it appears that Estonian officials cited both the benefits gained by Russia and their previous actions as justifications for this incident. Furthermore, despite later forensic analysis, the Estonia leadership appeared reluctant to change their belief even with the presence of disconformity evidence.[31]

Finally, the opening ceremonies for the 2018 Pyeongchang Olympics were disrupted by a cyber attack. Early assessments appeared to have attributed the incident to North Korea, given the underlying strategic context. This, however, was later found to have been a false flag operation.[32]

While authors such as Harknett and Fischerkeller argue that persistent engagement would result in a better understanding between adversaries,[33] this possible socialization alone cannot address our concern with biased reasoning. Knowing how adversaries behave does not remove the inherent uncertainty associated with the nature of the domain. Moreover, further socialization cannot wholly address shifts in behavior or the questions of intent with the appearance of malicious code. Consequently, learning from the past is a necessary but not sufficient means of addressing biased

---

[31] Peter Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic," *The Washington Post*, Last Modified May 17, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html; USGOV. 2007a. "Estonia's Bronze Soldier: It's Deja Vu All Over Again," WikiLeaks, Last Modified 16.02.2007, accessed 13.06. https://wikileaks.org/plusd/cables/07TALLINN106_a.html; USGOV. 2007b. "Estonia's Cyber Attacks: World's First Virtual Attack Against Nation State," WikiLeaks, Last Modified 04.06.2007, accessed 13.06. https://wikileaks.org/plusd/cables/07TALLINN366_a.html.

[32] Paul Rascagneres and Martin Lee, "Who Wasn't Responsible for Olympic Destroyer?" Talos Intelligence, February 26, 2018, https://blog.talosintelligence.com/2018/02/who-wasnt-responsible-for-olympic.html.

[33] Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace," *Lawfare*, November 9, 2018, https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace.

reasoning in this increasingly conflict-prone space.

III. Surfacing Bias Through Wargaming

Simulations such as wargames are frequently utilized as a pedagogic or evaluative instrument. The former as a means of demonstrating a particular concept while the latter serves to assess the efficacy of a given plan. However, this instrument can also be called up as a means to investigate, demonstrate, and address the shortcomings of dynamic decision-processes that emerge in high-stress environments.

A. Suspension of Disbelief

Despite its fictitious origins, wargames provide participants with an environment in which equivalent real-world decision-making processes are surfaced for evaluation. A key enabler being the narrative format that wargames typically adopt. As noted by Perla and McGrady,[34] the suspension of disbelief that is fundamental to the success of these simulations depend on the differences between the "automatic" and "systematic" cognitive processes at work. The former is typically associated with adaptive processes that serve to provide an immediate assessment of a given situation with minimal cognitive resources. At the same time, the latter is typified by more deliberative reasoning that, in turn, requires considerable cognitive effort.[35] Procedurally, the former precedes the latter when we process information.

Consequently, the suspension of disbelief required to allow participants to behave as they would in the real-world hinges on the ability to suppress these systematic processes. Neurological research suggests that the

---

[34] Peter P. Perla and ED McGrady, "Why wargaming works," *Naval War College Review*, Vol. 64, No.3, Summer 2011, pp.111-130.

[35] Daniel Kahneman, *Thinking, fast and slow.* 1st ed. (New York: Farrar, Straus and Giroux, 2011).

activation of these systematic processes is tied to the extent to which real-action is required in response to the information provided. That is to say, when presented with a narrative such as that contained in a wargame scenario; its success rests on our ability to respond in the real-world. Without such, automatic processes enable us to engage in the narrative without questioning its authenticity.[36]

As an example of these processes, students were presented with two accounts concerning the career of the first president of the United States, George Washington. The first contains a factual account of how Washington become the first president. The second employs dramaturgical techniques to introduce a degree of uncertainty as to whether or not he would be elected into office. Those exposed to the latter took longer to answer whether or not he was indeed elected as the first president. The author believes that even though these participants were well aware of who the first president was, the ambiguity in the construction of the narrative made the students believe otherwise (albeit briefly) before the engagement of "systematic" processes.[37]

This phenomenon enables designers to frame an environment in which participants are convinced to behave in a manner that parallels the real-world. This, in turn, allows us to observe decision-making processes that would otherwise be inaccessible due to administrative requirements (i.e., security clearance requirements) or probabilistic constraints (i.e., rare events).

---

[36] Norman N. Holland, "Spider-Man? Sure! The neuroscience of suspending disbelief," *Interdisciplinary Science Reviews*, Vol. 33, No. 4, December 2008, pp.312-320.
[37] Richard Gerrig, *Experiencing Narrative Worlds* (New York: Routledge, 2018).（Ebook）

B. Minimizing Risks, Encouraging Actions

The ability to shape reality and the extent to which these are believed to be fact enables participants to act accordingly without fear of consequences. This is not to say that consequences are omitted outright; instead, designers can shape these consequences in a manner that best suits their needs. For instance, in studying whether or not cybersecurity incidents prompt decision-makers to gravitate towards information that would provide immediate closure as a function of their role; designers may limit consequences on a participant's continued position of a given role (e.g., being voted out of office due to his or her failure to act).[38] In effect, this is akin to the application of specific treatments within an experimental design.

Assuming that the narrative is effective in suspending disbelief, designers can introduce features such as specific consequences or the availability of information that would elicit the processes described in the previous section. In turn, this could trigger biased judgments that would typically occur in the real-world without the corresponding real-world effects discouraging.

This is the crux of this article's argument. The ability to convince wargame participants that the environment they are operating in is similar to that in the real-world allows parallel actions and decisions to be enacted. This being a constructed space, designers introduce features that trigger specific cognitive or affective responses that result in the emergence of bias. These and their effects are observed throughout the gameplay and are then communicated to the participants as part of the debriefing activity. It is at this point that participants, with perhaps the assistance of the game designers, can design processes that would mitigate the worst effects of

[38] Arie W. Kruglanski and Donna M. Webster, "Motivated closing of the mind: "Seizing" and "freezing"," *Psychological Review*, Vol.103, No.2, April 1996, pp.263.

based judgments under real-world conditions.

C. Pitfalls of Wargaming

While the previous subsections appear to frame wargames as a panacea for addressing biased decision-making, these are not without their limitations. Designers could fail by either under/overestimating certain conditions in the fictitious narratives or may provide an over-simplified scenario due to complexity issues or a lack of knowledge.

It is not unheard of for designers to misrepresent the likelihood of threats and the severity of consequences. High-profile simulations have fallen into this trap resulting in the emergence of inappropriate policies.[39] For cybersecurity, the potential for this is very much a reality given the opaque nature of events. Events such as the annual Cyber 9/12 Challenge depict conditions that, while engaging for participants, may not necessarily be representative of real-world conditions.[40] While such a representation may still result in the emergence of specific biases, these would not necessarily be identical to those observed under real-world conditions.

Relatedly, designers can also fall into the trap of oversimplifying the narratives presented in the course of wargames. Oversimplification, however, may not always be unintentional. If the objective is to understand the specifics of a given process, the omission of certain aspects could provide additional analytic clarity that better serves the intent of the designers. Unfortunately, oversimplification may also emerge from a lack of understanding concerning real-world processes and may or may not be addressable. In any event, simplification may prevent specific processes

---

[39] Tara O'toole, Mair Michael, and Thomas V. Inglesby, "Shining light on "Dark Winter"," *Clinical Infectious Diseases*, Vol. 34, No. 7, April 2002, pp.972-983.

[40] This is not a failure on the part of the designers but to provide an engaging and thought-provoking scenario on the part of the participants who are mostly students.

from being observed when these omitted variables are crucial for their emergence. For instance, assuming the absence of small-decision groups and assigning individuals as the sole decision-maker would not allow group dynamics to unfold that contribute to the effects of specific biases.

Ultimately, designers should be cognizant of the limitations inherent in their scenarios. The opaque nature of cybersecurity is unlikely to yield a perfect representation of the threat, and the complex nature of this environment can make a faithful reproduction within a simulated space prohibitively expensive. Nevertheless, by keeping these in mind, designers can account for the extent to which these wargames simulate reality, and the overall utility offered to participants.

IV. Notable Cyber Wargames & Key Observations

The appearance of wargaming as a crucial instrument has come to the fore given limited access to elite decision-making artifacts during periods of conflict. More importantly, the growing popularity of wargaming allows researchers to evaluate better the extent to which uncertainty and biased reasoning interact, resulting in sub-optimal judgments on the part of military and political elites. In recent years, interest has formed around the study of the psychological aspects of cybersecurity.[41] Although experimental designs demonstrate the importance of this micro-level approach and the potential for sub-optimal judgments, these observations are drawn from non-elite samples that may differ from individuals exposed to real-world

[41] Miguel Alberto Gomez, "Sound the alarm! Updating beliefs and degradative cyber operations," *European Journal of International Security*, Vol. 4, No. 2, June 2019, pp.190-208; Michael L. Gross, Daphna Canetti, and Dana R. Vashdi, "Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes," *Journal of Cybersecurity*, Vol. 3, No.1, March 2017, pp.49-58; Miguel Alberto Gomez, "Past behavior and future judgements: seizing and freezing in response to cyber operations," *Journal of Cybersecurity*, Vol. 5, No.1, September 2019, pp.1-19.

incidents.[42] The rise of wargaming, as such, offers a means through which these experimentally derived observations are either validated or refuted. While larger events such as the annual Locked Shields (CCDCOE 2019) exercise by NATO are typical of these activities,[43] little has been said regarding specific patterns of behavior exhibited by participants.[44] Taking into consideration the objectives of this article, it briefly recounts the research conducted by Schneider, Jensen and Valeriano, and Gomez and Whyte.[45] The three are comparable in the sense that these articles focus on elite decision-making vis-à-vis the escalatory risks associated with cyber operations.

Serving as an entrepreneur with respect to cybersecurity wargaming, Schneider discusses the data obtained from the wargames conducted at the United States Naval War College from 2011 to 2016.[46] These activities took the form of table-top exercises wherein elite participants[47] were presented scenarios involving disputes with near-peer or asymmetric adversaries that occurs within one of the conventional domains (i.e., land or sea). These individuals (blue team) interacted with the adversary (red team) that is role-played by another set of elites. Consequently, these wargames take the form of an open-play type exercise.[48]

Before proceeding further, it is essential to note the critical difference

---

[42] Alex Mintz, Steven B. Redd, and Arnold Vedlitz, "Can We Generalize from Student Experiments to the Real World in Political Science, Military Affairs, and International Relations?" *The Journal of Conflict Resolution*, Vol. 50, No. 5, October 2006, pp.757-776.

[43] CCDCOE, "Locked Shields 2019," CCDCOE, https://ccdcoe.org/exercises/locked-shields.

[44] Although reports have emerged from these events, scientific analysis is limited, if at all present.

[45] Jacquelyn Schneider, 2017; Benjamin Jensen and Brandon Valeriano, "The Cyber Character of Crisis Escala," presented at the International Studies Association Annual Convention (Toronto, March 27, 2019); Miguel Alberto Gomez and Christopher Whyte, 2019.

[46] Ibid.

[47] Military and government officials.

[48] No pre-structured/pre-planned response based on the participants' actions.

between her study and the other two as it frames the generalizability of the findings. First, the wargames Schneider analyzes is not an exclusively cyber-on-cyber exercise. Instead, cyber operations are treated as one of the policy options available to participants. This is crucial as the findings cannot be said to apply directly to situations where interactions remain exclusively within cyberspace. On the other hand, it does realistically depict the cross-domain nature of interstate interactions in the modern interstate system.[49] Second, these wargames were not designed as experiments such that specific behavioral outcomes cannot be ruled out as the effects of confounding variables. This limitation, however, is offset by the fact that the scenarios and participants remain relatively consistent across this period and limit the impact of confounders.

That being said, Schneider makes several noteworthy observations regarding behavior during periods of crisis. Foremost among these is the belief in the escalatory nature of cyber operations that limited both cyber exploitation and information operations. When these were considered, the emphasis was placed on the need to ensure reversibility and non-attribution. Moreover, it was observed that analogies were drawn between cyber operations and nuclear capabilities but none between these and conventional weapons. These observations, at least at the time of the wargames, are significant for conceptual and pragmatic reasons. Conceptually, the conflation between cyber and nuclear speaks to the continued prevalence of the "Cyber Doom" scenario in which cyber operations are believed to have significant escalatory potential such that the mere discovery of these (even if solely for espionage) could signal an intent to escalate.[50] Pragmatically,

---

[49] Ryan C. Maness and Brandon Valeriano, "The Impact of Cyber Conflict on International Interactions," *Armed Forces & Society*, Vol. 42, No. 2, April 2016, pp.301-323.

[50] Erik Gartzke and Jon R. Lindsay, "Thermonuclear cyberwar," *Journal of Cybersecurity*, Vol. 3, No.1, March 2017, pp.37-48; Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (London: Hurst & Company, 2017).

these findings demonstrate alignment with existing strategic considerations at the time. Before the 2018 version of the Department of Defense Cyber Strategy, restraint was reflected in past strategic documents.[51] Although the wargame cannot definitively confirm it, this perceived escalatory potential of cyber operations may have influenced the framing of strategic thought and documents at the time.

Inversely, the wargames also highlighted a cross-over point in which cyber operations were perceived to be less escalatory. Except for a single case, cyber operations are thought to be less escalatory only once conventional operations were initiated. This observation is relevant given that most real-world cyber operations aimed at the United States, and others occur well before armed conflict is initiated. These results highlight the importance of emotions in the formulation of judgments that later inform policy decisions. Schneider notes that anxiety, rather than fear, may account for the absence of escalatory tendencies on the part of the participants.[52] Unlike fear that provokes a hardening of one's position, anxiety may manifest as risk-averse behavior, much like that observed in the series of wargames noted in the study.[53] Furthermore, while the article is unable to surface the role of emotions definitively, these findings find support in published research on the importance of emotions in response to incidents in cyberspace.[54]

---

[51] Jacquelyn Schneider, "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy," *Lawfare*, May 10, 2019, https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy.

[52] Schneider, op. cit.

[53] Paul J. Whalen, "Fear, Vigilance, and Ambiguity: Initial Neuroimaging Studies of the Human Amygdala," *Current Directions in Psychological Science,* Vol. 7, No. 6, December 1998, pp.177-188.

[54] Michael L. Gross, Daphna Canetti, and Dana R. Vashdi, "Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes," *Journal of Cybersecurity*, Vol. 3, No.1, March 2017, pp.49-58.

Following up on their findings, Jensen and Valeriano (2016) are conducting a series of wargames in the context of an experimental study. Whereas cyber operations were not the primary policy response of interest in the wargames evaluated by Schneider, Jensen, and Valeriano are instead interested in how the expression of power within this human-made domain either encourages or mitigates escalatory risks among parties involved.

For these authors, the wargames involve peer rivals currently embroiled in a territorial dispute with each other. The authors then manipulate the underlying conditions along two dimensions. First, a recent issue necessitating a response (does or does not) involve an offensive cyber operation by one of the parties. Second, those reacting to this incident (do or do not) have a cyber operation as one of several possible response options. This design allows the authors to isolate the effects of both factors on decision-making and the propensity for bias. To maximize the generalizability of their findings, the authors recruited participants from the government, academia, and industry.

Although the study is yet to be completed, the initial findings are proving to be significant. Cyber operations do not appear to increase the risk of escalation in a militarized dispute. Matching Schneider's earlier findings, the exercise of cyber power once conventional means have been employed does not appear to be provocative. In line with this, participants with the option to respond via cyber means are less escalatory than those without. Phrased differently, lacking the ability to respond in kind, targets of cyber operations opt to escalate into the physical domain in order to demonstrate resolve.

The policy implications of these findings are crucial. If cyber operations do not affect the strategic calculus between rivals engaged in a militarized dispute, then escalation should not be of significant concern. A similar pattern was observed in a recent article by Kostyuk and Zhukov that explored the escalation associated with cross-domain engagements in the

ongoing dispute between Ukraine and Russia.[55] On the other hand, it is essential to note that operations to date have limited physical effects. Should this change, the escalatory calculus may respond in kind.

Furthermore, this finding does not speak much about the dangers of collateral damage beyond the intended target, possibly inviting a response from an unintended target. Schematic reasoning that may emerge due to the continued use of cyber operations owing to its "limited effects" may lead to a less deliberate justification of its use in the future. The recent introduction of the United States' persistent engagement model harkens to this issue. Although the United States may view sustained cyber operations as a necessity with limited escalatory risk, its justification for this strategy may simply be a product of mirror imaging bias rather than deliberative reasoning.

While the design offered by Jensen and Valeriano is a step in the right direction, it does suffer from the limitation that intra-group dynamics do not appear to have been taken into consideration. Although the scenario is tackled as a group, the authors do not provide insight into the dynamics resulting in the final decision. This is an essential limitation as groups can either mitigate or enhance individual-level biases.

Finally, research conducted by Gomez and Whyte tackles the question of escalation from the point of view, distance, and temporality.[56] As with Jensen and Valeriano, their research tackles the issue through an experimental design. An initial large-N survey experiment is conducted on

---

[55] Nadiya Kostyuk and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *The Journal of Conflict Resolution*, Vol. 63, No.2, February 2019, pp.317-347.

[56] Miguel Alberto Gomez and Christopher Whyte, 2019; Distance refers to the proximity of an actor to the effects of an operation while temporality is the urgency associated with responding to the said event.

(non-elite) individuals from Five Eyes member states.[57] Because of the nature of the participants, a follow-on wargame matching the initial survey experiment was conducted with the Institute for National Defense and Security Research (INDSR) in Taiwan to strengthen the generalizability of the findings. It should also be mentioned that unlike the experimental design adopted by Jensen and Valeriano, this wargame attempts to establish the effect of organizational structures have on decision-making. Instead of having a group decide as a single individual, participants assume specific roles and are given privileged information as determined by their role.[58] While not explicitly instructed to do so, participants are free to withhold information from the rest of the group – thus increasing uncertainty commonly observed in these incidents.

A key differentiator between this and that of the former two is the exclusivity of cyberspace in the scenario. Wherein Schneider and Jensen and Valeriano framed their first scenario as disputes occurring within the conventional domains, the issue prompting the use of cyber operations is that of cyber operations targeting the media and critical infrastructure. This design choice has both inherent weaknesses and strengths. On the one hand, this reduces the wargame's overall realism. As issues beyond the domain often initiate most interstate interactions in cyberspace, it is possible that more informed participants are unable to suspend their disbelief and thus fail to commit fully to the scenario. On the other hand, this allows the authors to isolate the decision-making processes that may give rise to bias in cases where disputes are grounded solely on malicious behavior in cyberspace.

A key finding of this wargame is the dependence on pre-existing

[57] Participants are limited to those of the Five Eyes to control for variation owing to culture of threat perception vis-à-vis cyberspace.
[58] Policy Expert, Military Expert, and Cybersecurity Expert.

beliefs in formulating decisions in response to cyber operations. Theoretically, these findings align with current social and cognitive psychology literature. When faced with uncertainty, individuals fall back on readily available concepts and frame their judgments within the bounds of these structures.[59] While these cognitive mechanisms allow for an efficient assessment of the situation, overreliance is likely to result in biased judgments. In one case, a team decided to yield to the demands of an adversary due to the value/importance they have on preserving human life. However, as valid and noteworthy as this may be, the influence exerted by this belief limited their ability to realize the negative signal this may send to potential adversaries in the form of perceived weakness. Apart from this, the results also highlight the importance of information, as seen in the intra-group dynamics and the justification of their actions. Less knowledgeable individuals actively sought out information from more knowledgeable members of their team. Barring that, assumptions were made based on their understanding of past incidents and their expertise.

The importance of pre-existing belief and domain expertise expressed by the participants reflects earlier findings by both authors. Whyte (2016) notes that the failure of the coercive operation by North Korea against the United States is linked to the former's underlying beliefs (i.e., liberal-democratic values) and its influence on the decision to resist North Korean demands.[60] Similarly, both belief systems and domain expertise weigh heavily in a series of experiments that investigate the attribution of cyber operations. Enemy images, in particular, provoke schematic thinking through which decision-makers preempt available evidence and form narratives (whether or not these conform to reality) that serve to explain an

[59] Deborah Welch Larson, "The Role of Belief Systems and Schemas in Foreign Policy Decision-Making," *Political Psychology*, Vol. 15, No.1, March 1994, pp.17-33.
[60] Christopher Whyte, "Ending cyber coercion: Computer network attack, exploitation and the case of North Korea," *Comparative Strategy*, Vol. 35, No. 2, March 2016, pp.93-102.

adversary's current and future actions.[61]

The above findings reflect significant policy implications. An overreliance on beliefs constraints the search for information and potentially discounts the negative consequences of specific actions. The search for information and a reliance on experts may, in turn, may disproportionately increase the influence of an individual or sub-organization in the decision-making process. Consequently, this may result in policies driven primarily by parochial interests rather than the overall well-being of the organization or state.

Although the above wargames vary in terms of design, the observations derived from these contribute significantly to our understanding of decision-making in this domain. More importantly, the intersections of the above findings with those derived from observational and experimental research point to the importance of wargaming in broadening our understanding of actors within cyberspace. These highlight the genuine possibility of bias stemming from the uncertainty associated with events in cyberspace. With the utility offered by cyber wargames established, the remainder of this article provides a general guideline on how best to design these activities of research or training purposes.

V. Designing Cyber Wargames

It is crucial to note that despite its history and frequent use, no clear guidelines exist on how best to design wargames. More so for those tailored for the domain of state-level cybersecurity. While this article does not aspire to establish clear rules as to how best to engage in this endeavor, it proffers vital considerations that should go into the conceptualization, development,

---

[61] Miguel Alberto Gomez, "Past behavior and future judgements: seizing and freezing in response to cyber operations," *Journal of Cybersecurity*, Vol. 5, No.1, September 2019, pp.1-19.

and execution of cybersecurity wargames. Readers should be aware that cybersecurity wargames conducted at the strategic rather than operational level, which are the focus of this article, are not fundamentally different from those that involve the conventional domains of air, land, and sea. The introduction of uncertainty to simulate real-world conditions is achieved either explicitly through the manipulation of the underlying organizational and/or strategic relationships amongst the participants and implicitly by the very nature of the simulated cyber environment.[62] Consequently, the extent to which biased and sub-optimal decisions are surfaced depends on the preceding manipulation. The careful manipulation of these attributes allows game designers to better approximate real-world conditions that elicit useful observations.

A. Overall Objective

What purpose does the wargame serve? Mundane as this question may be, it serves as the cornerstone for any planned wargame – cyber or otherwise. Wargames serve to either test the feasibility of existing plans, the readiness, and capabilities of specific groups or to identify specific decision-making behavior and shortcomings. Although wargames would share common features, their specific function dictates the structure, flow, and ultimate utility of these activities.

For instance, those designed to test pre-existing plans contribute significantly to understanding whether or not an organization currently possesses the capabilities to face certain eventualities but is unlikely to demonstrate improvisational capabilities. Similarly, those structured to compare the performance of different groups are unsuitable if the designer

---

[62] Myriam Dunn Cavelty, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse," *International Studies Review*, Vol. 15, No. 1, January 2013, pp.105-122.

intends to observe cooperative behavior between these groups.

Consequently, the objectives of these activities must be established before further steps being taken. This does not only increase the value of the activity but may assist in reducing unnecessary administrative overheads and resource expenditures.

B. Level of Play

One crucial point to acknowledge when designing cyber wargames is the level at which the wargame takes place. In the context of cybersecurity, this can occur either at the operational or strategic level. Wargames at an operational level are technical and serve to evaluate the ability of operational teams to react to an individual or related technical incidents independent of the overall strategic context. In contrast, strategic games involve the exclusive or adjunctive use of cyberspace in a broader strategic environment. Games of this type require cybersecurity incidents to be evaluated not only on a technical but on political, economic, and/or military aspects as well. The decision to engage in either of the above types requires special considerations in terms of resources and expected findings.

Operational-level cyber wargames, to be as realistic as possible, require the use of a dedicated network(s) through which participants may engage in offensive and defensive acts. This requires significant material resources and technical expertise to design, deploy, and evaluate. From an analytical perspective, these events are useful in evaluating the extent to which operational elements of an organization is effective in dealing with an individual or related security incidents.[63] However, higher-level decision-makers are usually not involved, and, as such, the observations

[63] These types of events are fairly common in the Information Security field in which individuals and/or groups are evaluated on their skill level or adherence to specific standards such as the NIST Cyber Security Framework.

gained are limited.

Strategic-level cyber wargames, in contrast, can be limited to a table-top exercise or extended to include an operational aspect as well given available resources. Unlike the above, these games also involve vital decision-makers that are responsible for high-level policies (e.g., foreign policy experts). Involving them in the process allows the designers to better replicate real-world incidents in which operational-level individuals provide strategic decision-makers with information necessary to make policy decisions. However, care must be taken in providing a balance between realism and analytical reality.

Although both operational and strategic-level wargames are useful in understanding organizational behavior, the choice between the two depends on the overall objectives of the game designer. Moreover, the decision also influences other considerations discussed in the succeeding subsections.

C. Participant Identification

Once the wargame objective is established, the makeup of its participants should also be considered. Fundamentally, the identity of game participants is a function of both the game objectives and access granted to designers. Keeping these in mind is crucial as it contributes directly to the practicability of the game itself as well as the generalizability of the data gathered throughout gameplay.

Participants in a wargame can either be elite or non-elites. Elites, in this case, refers to individuals with specific real-world roles that correspond directly to some aspect of the game. For instance, a military officer may play the role of the chairman of the Joint Chief of Staff in a game that attempts to simulate the upper levels of the United States Government. In contrast, non-elites are individuals who better represent the general public as a whole. The use of students serves to exemplify this case. As a question of practicality, the decision to favor one group over another in the conduct of a

wargame is a matter of access. Beyond this, however, participant background also has crucial theoretical implications that could have a serious bearing on how these individuals interact with the activity and the informative value offered by their observed actions.[64]

The decision to select elites or non-elites is influenced by the task assigned to them and the level of expertise required. Tasks not requiring specialized knowledge or expertise, such as the formation of judgment and initial perceptions, renders the distinction between experts and non-experts moot. By their nature, these tasks tap into cognitive and psychological processes that are either common to most individuals or are easily induced through experimental manipulation.[65] At worst, the decision to employ non-elites may result in less pronounced effects compared to that of elites.[66] The difference, however, can be accounted for during evaluation by citing real-world equivalents or other related cases. In contrast, structured tasks may require familiarity with real-world processes or situations inaccessible to non-elites. This distinction suggests a clear difference between how the former would behave in a wargame compared to that of the latter.

---

[64] Emilie M. Hafner-Burton, Alex D. Hughes, and David G. Victor, "The Cognitive Revolution and the Political Psychology of Elite Decision Making," *Perspectives on Politics*, Vol. 11, No.2, June 2013, pp.368-386; Alex Mintz, Steven B. Redd, and Arnold Vedlitz, "Can We Generalize from Student Experiments to the Real World in Political Science, Military Affairs, and International Relations?" *The Journal of Conflict Resolution*, Vol. 50, No. 5, October 2006, pp.757-776.

[65] Daniel Kahneman, Paul Slovic, and Amos Tversky, *Judgment under uncertainty: heuristics and biases* (New York: Cambridge University Press, 1982); Paul Slovic, Melissa L. Finucane, Ellen Peters, and Donald G. MacGregor, "The Affect Heuristic," *European Journal of Operational Research*, Vol. 177, No. 3, March 2007, pp.1333-1352.

[66] Richard R. Lau and David P. Redlawsk, "Advantages and Disadvantages of Cognitive Heuristics in Political Decision Making," *American Journal of Political Science*, Vol. 45, No.5, October 2001, pp.951-971; Joshua D. Kertzer and Kathleen M. McGraw, "Folk Realism: Testing the Microfoundations of Realism in Ordinary Citizens," *International Studies Quarterly*, Vol. 56, No.2, June 2012, pp.245-258; Elizabeth N. Saunders, "No Substitute for Experience: Presidents, Advisers, and Information in Group Decision Making," *International Organization,* Vol. 71, No. S1, April 2017, pp.219-247.

D. Group versus Individual Gameplay

Apart from individual participant backgrounds, in-game interactions (or the lack thereof) require consideration relative to the modeled real-world processes. While decision-making can be easily left to the individual, most state-level actions are the result of group dynamics. Even in the most autocratic of regimes, decisions may still be the result of small group dynamics. Although game designers may opt to delegate this process to an individual for either administrative (e.g., time) or design (e.g., complexity) constraints, this risks the failure to capture particular dynamics that only appear within a group setting.

For instance, cognitive biases are either aggravated or mitigated through interpersonal interactions. Groupthink could surface, thus allowing the propagation of biased and sub-optimal thinking. Inversely polythink could emerge, thus resulting in a less biased decision on the part of the group.[67] In either case, limiting game-play to individuals comes at the cost of allowing these processes that frequently occur in the real-world to unfold. This does reduce not only the overall realism of the exercise but also limits its overall generalizability.

This is not to say, however, that all wargames and related simulations should be done as a group. Instead, we argue that gameplay should take into consideration aspects of the environment being replicated. Furthermore, concerning this article's focus on complexity resulting in biased decision-making, developing an environment wherein these mechanisms manifest themselves is crucial if the objective of the designers is to understand decision-making processes better.

E. Level of Engagement

[67] Alez Mintz and Carly Wayne, "The Polythink Syndrome and Elite Group Decision-Making," *Political Psychology*, Vol. 37, No. S1, February 2016, pp.3-21.

Wargames can either be designed to progress based on a pre-determined ruleset or to flow more naturally through free-play (e.g., Red Team versus Blue Team).[68] While one is not necessarily better than the other, selection would depend primarily on the underlying objectives of the game. With the increasing use of games as a pseudo-experimental method, this decision cannot be made lightly.

Although allowing the game to develop through a series of pre-determined rules, possibly leading players towards the win condition is experimentally preferable, this denies players the freedom of action that would be common in a real-world setting. In contrast, free-play increases the overall realism offered by the wargame but limits the analytical power available to the designers. This is especially salient in the case of a pseudo-experimental design where granting players the freedom to act limits the ability to imposed controls and treatments.

Ultimately, one cannot say that one approach is better than the other. Design considerations and objectives should drive the decision of whether or not to grant players the freedom of action within the simulated environment. Furthermore, should designers opt to adopt an experimental approach, the game design ought not to be compromised in order to force aspects of a preferred method into a construct not wholly suited to it.

With respect specifically to understanding decision-making behavior within an uncertain environment, providing participants with the freedom of action contributes significantly to increasing the level of realism. As in the real-world where interpreting adversarial behavior is a daunting task, free-play is the best solution to mimic this salient characteristic. This, in turn, should prompt participants to resort to the equivalent cognitive mechanisms

---

[68] Peter P. Perla and ED McGrady, "Why wargaming works," *Naval War College Review*, Vol. 64, No. 3, Summer 2011, pp.111-130.

to reduce the degree of uncertainty and thus result in behavior comparable to that in the real world.

F. Cyber-Specific or Cyber-Adjunctive Environment

While being the only aspect directly associated with running a wargame about the cyber domain, the extent to which cyberspace is manifested in the game should be taken into consideration. Tempting as it may be to present a wargame that focuses exclusively on interactions within this domain, most real-world cases are cross-domain in nature. As noted by a growing number of authors, cyberspace is an adjunctive instrument of foreign policy is serves as one of the expressions of national power.[69] With that being said, the extent to which cyber capabilities feature in wargames is a direct reflection of the activity's realism that, in turn, interacts with other aspects of game design such as participant backgrounds. Elites that have experience with real-world cases may find wargames that unfold solely in cyberspace or involve exclusively cyber events unrealistic. Consequently, their actions during the activity may not align with how they would respond under normal circumstances.

This is not to say, however, that there is no merit to running wargames that unfold solely within the cyber domain. Designers are more than welcome to do so as long they bear in mind that decision-making behavior may reflect differently depending on the extent to which participants are exposed to this uncertain environment and their ability to address this uncertainty.

---

[69] Benjamin Jensen, Ryan C. Maness, and Brandon Valeriano, "Cyber Victory: The Efficacy of Cyber Coercion," presented at the Annual International Studies Association Meeting (Atlanta, Georgia, March 17, 2016); Jon R. Lindsay and Erik Gartzke, "Cross-domain deterrence as a practical problem and a theoretical concept," Erik Gartzke and Jon R. Lindsay, eds., Cross-Domain Deterrence: Strategy in an Era of Complexity, (La Jolla, CA: Manuscript, 2016).

VI. Conclusions

Wargames are an under-utilized and under-realized instrument with which both scholars and defense planners might better understand the operational-level pathologies of operation in the fifth domain. The recent turn in cyber conflict studies towards the use of experiments has successfully illustrated the degree to which focus on dynamics at the levels of analysis traditionally found in international relations (IR) scholarship falls short of producing knowledge that can inform policy. Likewise, the increasing tendency to characterize cyber conflict neither as warfighting nor as isolated incidents uncoupled from the broader strategic context of adversary campaigns of contestation supports the notion that one-off findings in research must be corroborated and replicated in diverse methodological applications. Simulations, both simple and complex, are ideally positioned to help researchers answer these imperatives.

Perhaps the most particular point in support of increased use of wargames both in research and in operations planning and training is the utility of the simulation for calibrating what some have called “nano-second” manifestations of policy. In interpreting strategy documentation, operators, investigators, and policymakers alike must build procedures conducive to the effective exercise of cyber conflict response actions. Given that such procedures must effectively highlight and incentivize appropriate reactive options in relatively short time frames, additional efforts must continuously be made to ensure congruence with high-level strategy and doctrine.

With the 2018 promulgation of American cyber policy as now built around the concept of persistent engagement, this reconciliation imperative is stronger than ever. Where the purpose of constant interaction via both preemptive and reactive “defending forward” activities is intended to force the development of mutual understandings of conflict parameters with adversaries, there is a distinct need to simulate and test assumptions about how foreign powers might interpret the actions of the U.S. and her close

partners on a repeating basis. After all, the artificiality of the domain and how cyber engagements take on meaning from real-world corollaries of digital conflict means that defense planners should be unwilling to assume that such interpretations will remain constant over time.

Bibliography

Axelrod, Robert, "A Repertory of Cyber Analogies," in Emily O. Goldman and John Arquilla, eds, *Cyber Analogies* (Monterey, CA: Dept. of Defense Information Operations Center for Research, 2014).

Borghard, Erica D. and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies*, Vol. 26, No. 3, May 2017, pp.452-481.

Buchanan, Ben, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (London: Hurst & Company, 2017).

Bumiller, Elisabeth and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *The New York Times*, October 11, 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

CCDCOE, "Locked Shields 2019," CCDCOE, https://ccdcoe.org/exercises/locked-shields/.

Dean, Benjamin and Rose McDermott, "A Research Agenda to Improve Decision Making in Cyber Security Policy," *Penn State Journal of Law & International Affairs*, Vol. 5, No. 1, April 2017, pp.29-71.

Dunn Cavelty, Myriam, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse," *International Studies Review*, Vol. 15, No. 1, January 2013, pp.105-122.

Fearon, James D., "Rationalist Explanations for War," *International Organization*, Vol. 49, No. 3, Summer 1995, pp.379-414.

Finn, Peter, "Cyber Assaults on Estonia Typify a New Battle Tactic, " *The Washington Post*, Last Modified May 17, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html.

Fischerkeller, Michael P. and Richard J. Harknett, "Persistent Engagement

and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace," *Lawfare*, November 9, 2018, https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace.

Gartzke, Erik and Jon R. Lindsay, "Thermonuclear cyberwar," *Journal of Cybersecurity*, Vol. 3, No. 1, March 2017, pp.37-48.

Gerrig, Richard, *Experiencing Narrative Worlds* (New York: Routledge, 2018).（Ebook）

Gomez, Miguel Alberto, "Past behavior and future judgements: seizing and freezing in response to cyber operations," *Journal of Cybersecurity*, Vol. 5, No.1, September 2019, pp.1-19.

Gomez, Miguel Alberto, "Sound the alarm! Updating beliefs and degradative cyber operations," *European Journal of International Security*, Vol. 4, No. 2, June 2019, pp.190-208.

Gomez, Miguel Alberto and Eula Bianca Villar, "Fear, Uncertainty, and Dread: Cognitive Heuristics and Cyber Threats," *Politics and Governance*, Vol. 6, No. 2, June 2018, pp.61-72.

Gomez, Miguel Alberto and Christopher Whyte, 2019.

Gray, Colin S., *Making Strategic Sense of Cyber Power: Why The Sky is Not Falling* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2013).

Gross, Michael L., Daphna Canetti, and Dana R. Vashdi, "Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes," *Journal of Cybersecurity*, Vol. 3, No. 1, March 2017, pp.49-58.

Hafner-Burton, Emilie M., Alex D. Hughes, and David G. Victor, "The Cognitive Revolution and the Political Psychology of Elite Decision Making," *Perspectives on Politics*, Vol. 11, No. 2, June 2013, pp.368-386.

Hansen, Lene, and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly*, Vol. 53, No. 4, December 2009, pp.1155-1175.

Holland, Norman N., "Spider-Man? Sure! The neuroscience of suspending disbelief," *Interdisciplinary Science Reviews*, Vol. 33, No. 4, December 2008, pp.312-320.

Holsti, Ole R., "The Belief System and National Images: A Case Study," *The Journal of Conflict Resolution*, Vol. 6, No. 3, September 1962, pp.244-252.

Holsti, Ole R., "Cognitive Dynamics and Images of the Enemy," *Journal of International Affairs*, Vol. 21, No. 1, 1967, pp.16-39.

Jarvis, Lee, Stuart Macdonald, and Andrew Whiting, "Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat," *European Journal of International Security*, Vol. 2, No. 1, February 2017, pp.64-87.

Jensen, Benjamin, Ryan C. Maness, and Brandon Valeriano, "Cyber Victory: The Efficacy of Cyber Coercion," presented at the Annual International Studies Association Meeting (Atlanta, Georgia, March 17, 2016).

Jensen, Benjamin and Brandon Valeriano, "The Cyber Character of Crisis Escala," presented at the International Studies Association Annual Convention (Toronto, March 27, 2019).

Jervis, Robert, *Perception and misperception in international politics*. New edition. ed. (Princeton, NJ.: Princeton University Press, 1976).

Jervis, Robert, "Understanding beliefs and threat inflation," in Trevor A. Thrall and Jane K. Creamer, eds. *American Foreign Policy and the Politics of Fear: Threat Inflation since 9/11,* (Abingdon-on-Thames, UK: Routledge, 2009).

Johnson, Dominic and Dominic Tierney, "The Rubicon theory of war: how

the path to conflict reaches the point of no return," *International Security*, Vol. 36, No. 1, Summer 2011, pp.7-40.

Johnson, Dominic and Dominic Tierney, "Bad World: The Negativity Bias in International Politics," *International Security*, Vol. 43, No. 3, February 2019, pp.96-140.

Kahneman, Daniel, "A perspective on judgment and choice - Mapping bounded rationality," *American Psychologist*, Vol. 58, No. 9, September 2003, pp.697-720.

Kahneman, Daniel, *Thinking, fast and slow.* 1st ed. (New York: Farrar, Straus and Giroux, 2011).

Kahneman, Daniel, Paul Slovic, and Amos Tversky, *Judgment under uncertainty: heuristics and biases* (New York : Cambridge University Press, 1982).

Kertzer, Joshua D. and Kathleen M. McGraw, "Folk Realism: Testing the Microfoundations of Realism in Ordinary Citizens," *International Studies Quarterly*, Vol. 56, No. 2, June 2012, pp.245-258.

Khong, Yuen Foong, *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965* (Princeton, NJ.: Princeton University Press, 1992).

Kostyuk, Nadiya and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *The Journal of Conflict Resolution*, Vol. 63, No. 2, February 2019, pp.317-347.

Kruglanski, Arie W. and Donna M. Webster, "Motivated closing of the mind: "Seizing" and "freezing"," *Psychological Review*, Vol. 103, No. 2, April 1996, pp.263-283.

Kunda, Ziva, "The case for motivated reasoning," *Psychological Bulletin*, Vol. 108, No. 3, December 1990, pp.480-498.

Larson, Deborah Welch, "The Role of Belief Systems and Schemas in Foreign Policy Decision-Making," *Political Psychology*, Vol. 15, No.1, March 1994, pp.17-33.

Lau, Richard, R. and David P. Redlawsk, "Advantages and Disadvantages of Cognitive Heuristics in Political Decision Making," *American Journal of Political Science*, Vol. 45, No. 4, October 2001, pp.951-971.

Libicki, Martin C., *Cyberdeterrence and cyberwar* (Santa Monica, CA.: Rand Corporation, 2009).

Liff, Adam, "Cyberwar: a new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war," *Journal of Strategic Studies*, Vol. 35, No. 3, June 2012, pp.401-428.

Lindsay, Jon R., "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, Vol. 22, No. 3, July 2013, pp.365-404.

Lindsay, Jon R. and Erik Gartzke, "Cross-domain deterrence as a practical problem and a theoretical concept," Erik Gartzke and Jon R. Lindsay, eds, Cross-Domain Deterrence: Strategy in an Era of Complexity, (La Jolla, CA: Manuscript, 2016).

Maness, Ryan C. and Brandon Valeriano, "The Impact of Cyber Conflict on International Interactions," *Armed Forces & Society*, Vol. 42, No. 2, April 2016, pp.301-323.

Mintz, Alex, Steven B. Redd, and Arnold Vedlitz, "Can We Generalize from Student Experiments to the Real World in Political Science, Military Affairs, and International Relations?" *The Journal of Conflict Resolution*, Vol. 50, No. 5, October 2006, pp.757-776.

Mintz, Alez, and Carly Wayne, "The Polythink Syndrome and Elite Group Decision-Making," *Political Psychology*, Vol. 37, No. S1, February 2016, pp.3-21.

O'toole, Tara, Mair Michael, and Thomas V. Inglesby, "Shining light on "Dark Winter"," *Clinical Infectious Diseases*, Vol. 34, No. 7, April 2002, pp.972-983.

Perla, Peter P. and ED McGrady, "Why wargaming works," *Naval War College Review*, Vol. 64, No. 3, Summer 2011, pp.111-130.

Perrow, Charles, *Normal accidents: living with high-risk technologies Princeton paperbacks* (Princeton, NJ.: Princeton University Press, 1984).

Power, Richard, "The Solar Sunrise Case: Mak, Stimpy, and Analyzer Give the DoD a Run for Its Money," *informit*, October 30, 2000, http://www.informit.com/articles/article.aspx?p=19603&seqNum=4.

Rascagneres, Paul and Martin Lee, "Who Wasn't Responsible for Olympic Destroyer?" Talos Intelligence, February 26, 2018, https://blog.talosintelligence.com/2018/02/who-wasnt-responsible-for-olympic.html.

Rid, Thomas, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, Vol. 35, No. 1, February 2012, pp.5-32.

Saltzman, Ilai, "Cyber posturing and the offense-defense balance," *Contemporary Security Policy*, Vol. 34, No. 1, March 2013, pp.40-63.

Saunders, Elizabeth N., "No Substitute for Experience: Presidents, Advisers, and Information in Group Decision Making," *International Organization,* Vol. 71, No. S1, April 2017, pp.219-247.

Schneider, Jacquelyn, 2017.

Schneider, Jacquelyn, "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy," *Lawfare*, May 10, 2019, https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy.

Slayton, Rebecca, "What Is the Cyber Offense-Defense Balance?

Conceptions, Causes, and Assessment," *International Security*, Vol. 41, No. 3, January 2017, pp.72-109.

Slovic, Paul, Melissa L. Finucane, Ellen Peters, and Donald G. MacGregor, "The Affect Heuristic," *European Journal of Operational Research*, Vol. 177, No. 3, March 2007, pp.1333-1352.

USA. "National Cyber Security Strategy of the United States of America," 2018.

USGOV. 2007a. "Estonia's Bronze Soldier: It's Deja Vu All Over Again," WikiLeaks, Last Modified 16.02.2007, accessed 13.06. https://wikileaks.org/plusd/cables/07TALLINN106_a.html.

USGOV. 2007b. "Estonia's Cyber Attacks: World's First Virtual Attack Against Nation State," WikiLeaks, Last Modified 04.06.2007, accessed 13.06. https://wikileaks.org/plusd/cables/07TALLINN366_a.html.

Valeriano, Brandon, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018).

Valeriano, Brandon and Ryan C. Maness, "The dynamics of cyber conflict between rival antagonists, 2001-11," *Journal of Peace Research*, Vol. 51, No. 3, May 2014, pp.347-360.

Valeriano, Brandon and Ryan C. Maness, *Cyber war versus cyber realities : cyber conflict in the international system* (New York: Oxford University Press, 2015).

Whalen, Paul J., "Fear, Vigilance, and Ambiguity: Initial Neuroimaging Studies of the Human Amygdala," *Current Directions in Psychological Science,* Vol. 7, No. 6, December 1998, pp.177-188.

Whyte, Christopher, "Ending cyber coercion: Computer network attack, exploitation and the case of North Korea," *Comparative Strategy*, Vol. 35, No. 2, March 2016, pp.93-102.

撰稿規則

一、 分節標題：文章之大小標題，
中文請以「壹、一、(一)、1.、(1)、a.、(a)」為序。
英文請以「I. A. (A) 1. (1) a. (a) 」為序。

二、 引語：原文直接引入文句者，於其前後附加引號；若引言過長，可前後縮排二字元獨立起段，不加引號。若為節錄整段文章，則每段起始空二字。

三、 簡稱或縮寫：引用之簡稱或縮寫，可依約定俗成之用法；惟於第一次出現時必須使用全稱，並以括號註明欲使用之簡稱（寫）。

四、 譯名：使用外來語之中文譯名，請盡量用通行之翻譯，並請於第一次出現時以括號附加原文全稱。

五、 標點符號：中文標點符號一律以「全形」輸入。引用中文書籍、期刊、雜誌、報紙、網站等名稱，請以《》標記；文章名稱以〈〉標記；外文書籍、期刊、雜誌、報紙、網站等名稱請用斜體字，索引文章名稱加“”標記。

六、 數字表示：

（一）年月日、卷期等數字及頁碼一律以中華民國年份（本國資料）或西元年份（中共資料）及阿拉伯數字表示。

（二）屆、次、項等採用國字表示，如：第一屆、第三次、五項決議。

（三）整的數字採用阿拉伯數字，如：50 人；但百位以上整數之數字「可以」國字表示者，以國字表示，如：二億三千萬。

（四）不完整之餘數、約數以國字表示，如：七十餘件、約三千人。

七、附圖、附表：

（一）編號採用阿拉伯數字，寫法如：圖 1、圖 2、表 1、表 2，圖 1-1、圖 1-2 等類推。

（二）表之標題在該表上方（置中），圖之標題在該圖之下方。

（三）圖表的資料來源與說明，請置於圖表的下方（置左）。

註釋體例

一、 所有引註均須詳註來源。如係轉引非原始資料來源，須予註明，不得逕行錄引。

二、 簡、繁體字中文書籍，使用相同註釋體例。

三、 所有注釋置於正文頁腳。

四、 時間表示：中文註腳內日期，以民國○年○月○日或西元○年○月○日表示；英文以 month day, year 表示。

五、 出版地的寫法

（一） 出版地若在美國，要分別列出城市名及州名，州名採縮寫且不加縮寫號。

（二） 若非美國，則寫出城市名和國名。

（三） 出版地若為下列主要城市，則不必寫出州名或國名，包括：

臺灣／臺北 (Taipei)；

美國／巴爾的摩 (Baltimore)、波士頓 (Boston)、芝加哥 (Chicago)、洛杉磯 (Los Angeles)、

紐約 (New York)、費城 (Philadelphia)、舊金山 (San Francisco)；

英國／倫敦 (London)；

法國／巴黎 (Paris)；

德國／柏林 (Berlin)、法蘭克福 (Frankfurt)、

慕尼黑(Munich)；

荷蘭／阿姆斯特丹 (Amsterdam)；

義大利／米蘭 (Milan)、羅馬 (Rome)；

奧地利／維也納 (Vienna)；

瑞士／日內瓦 (Geneva)；

瑞典／斯德哥爾摩 (Stockholm)；

俄羅斯／莫斯科 (Moscow)；

中國／香港 (Hong Kong)、上海 (Shanghai)、

北京 (Beijing)；

日本／東京 (Tokyo)；
韓國／首爾 (Seoul)；
以色列／耶路撒冷 (Jerusalem)。

六、 專書

（一）中文書籍：作者姓名，《書名》（出版地：出版者，年），頁 x-x。（初版無需註明版別）

（二）英文書籍：Author's full name, *Complete title of the book* （Place of publication: Publisher, Year）, p. x or pp. x-x.

（三）如引用全書時，可註明該書起迄頁數或省略頁數。

範例

陳鴻瑜，《南海諸島之發現、開發與國際衝突》，（臺北：國立編譯館，1997 年），頁 3。

Kenneth N. Waltz, *Man, the State, and War: A Theoretical Analysis* (New York: Columbia University Press, 1959), p. 2.

七、 專書譯著

（一）中文：Author(s)' full name 著，譯者姓名譯，《書名》（書名原文）（出版地：出版者，出版年），頁 x 或頁 x-x。（初版無需註明版別）

（二）英文：Author(s)' full name, *Complete Title of the Book,* trans. Translator(s)' full Name（Place of publication: Publisher, year of publication）, Volume number (if any), p. x or pp. x-x.

範例

布里辛斯基（Zbigniew Brzezinski）著，林添貴譯，《大棋盤-全球戰略大思考》（台北：立緒出版社，1999 年），頁 67。

Jhumpa Lahiri, *In Other Words*, trans. Ann Goldstein (New York: Alfred A. Knopf, 2016), p. 146.

八、 期刊譯著

（一）中文：Author's full name 著，譯者姓名譯，《篇名》（篇名原文），《刊物名稱》，第 x 卷第 x 期，年月，頁 x 或頁 x-x。

（二）英文：Author’s full name, “*Title of the Article,”* trans. Translator(s)’ full Name, *Title of the Journal*, Vol. x, No. x, Month Year, p. x or pp. x-x.

範例

Kelvin Fong 著，王玉麟譯，《亞太區域潛艦概況》〈Submarines in the Asia-Pacific〉，《國防譯粹》，第 33 卷第 7 期，2006 年，頁 89-95。

九、 專書論文或書籍專章

（一）中文：作者姓名，〈篇名〉，編者（群）姓名，《書名》（出版地：出版者，出版年），頁 x 或頁 x-x。（初版無需註明版別）

（二）英文：Author’s full name, “Chapter Title,” in Editor/Editors’ full Name(s), ed(s)., *Complete Title of the Book*, (Place of publication: Publisher, Year of publication）, p. x or pp. x-x.

範例

林正義、歐錫富，〈宏觀 2009 亞太和平觀察〉，林正義、歐錫富編，《2009 亞太和平觀察》（台北：中央研究院亞太區域研究專題中心，2011 年），頁 3。

Kaocheng Wang, “Bilateralism or Multilateralism? Assessment of Taiwan Status and Relations with South Pacific,” in Ming-Hsien Wong, ed., *Managing regional security agenda*, (New Taipei City: Tamkang University Press, 2013）, p. 29.

十、 學術性期刊論文

（請依個別刊物實際出刊項目，完整臚列）

（一）中文：作者姓名，〈篇名〉，《刊物名稱》（出版地），第 x 卷 x 期，年月，頁 x 或頁 x-x。（臺灣出版之期刊無需註明出版地，但若與其他地區出版期刊名稱相同者，仍需註明出版地，以利識別）

（二）英文：Author’s full name, “Title of the article,” *Name of Periodical*, Vol. x, No. x, Month Year, p.x or pp. x-x.

範例

汪毓瑋，〈美近公布「威脅評估報告」之評析〉，《展望與探索》，第 4 卷第 4 期，2005 年 4 月，頁 92-97。

Randall L. Schweller, "Bandwagoning for Profit: Bring the Revisionist State Back in," *International Security*, Vol. 19, No. 1, June 1994, pp. 72-107.

十一、學位論文

（一）中文：作者姓名，《學位論文名稱》，學校院或系所博士或碩士論文（畢業年份），頁 x 或頁 x-x。

（二）英文：Author's full name, "Complete Title of Dissertation/ Thesis," （Ph.D. Dissertation/Master' s Thesis, Name of the Department, Name of the Degree-granting University, year of graduation）, p.x or pp. x-x.

範例

馬振坤，《從克勞塞維茲戰爭理論剖析中共三次對外戰爭》，國立臺灣大學政治學研究所所博士（2002），頁 1。

Stacia L. Stinnett, "*The Spratly Island Dispute: An Analysis,*" (Master's Thesis, Florida Atlantic University, 2000), p.1

十二、研討會論文

（一）中文：作者姓名，〈篇名〉，發表於○○○○研討會（地點：主辦單位，舉辦年月日），頁 x 或頁 x-x。

（二）外文：Author's full name, "Paper Title," presented for Complete Title of the Conference (Place of conference: Conference organizer, Date of conference in month day, year), p. x or pp. x-x.

範例

許文堂，〈南沙與西沙-他者的觀點〉，發表於「七 0 年代東亞風雲-台灣與琉球、釣魚台、南海諸島的歸屬問題」學術研討會（臺北：台灣教授學會，2013 年 10 月 27 日），頁 1。

Wen-cheng Lin, “Cross-strait Confidence Building Measures,” presented for Comparing Different Approaches to Conflict Prevention and Management: Korean Peninsula and the Taiwan Strait Conference (Stockholm: Central Asia-Caucasus Institute Silk Road Studies Program, December 16-17, 2005), p. 1.

十三、官方文件

（請依個別刊物實際出刊項目，完整臚列）

（一）中文：官署機構，〈文件名稱〉（行政命令類）或《文件名稱》（法律類），卷期（案號），日期，頁 x 或頁 x-x。

（二）外文：Author’s Full Name, “Title of the Article,” Date, Section or Page Numbers.

範例

中華民國總統府，〈總統令〉，《總統府公報》，第 7426 號，中華民國 108 年 5 月 22 日，頁 3。

White House, “National Security Strategy of the United States of America,” December 18, 2017, p. 1.

十四、報刊、非學術性雜誌

（若為社論、短評、通訊稿或作者匿名，則可不列作者欄）

（一）中文報紙：作者姓名，〈篇名〉，《報紙名稱》（出版地），年月日，版 x。（一般性新聞報導可省略作者和篇名，臺灣出版之報紙無須註明出版地。）

（二）中文雜誌：作者姓名，〈篇名〉，《雜誌名稱》（出版地），年月日，頁 x 或頁 x-x。（無須註明第卷第 x 期。臺灣出版雜誌無須註明出版地）

（三）英文報紙：Author’s full name, “Title of the Article,” *Title of the Newspaper*, Date, Section or Page Numbers.

（四）英文雜誌：Author’s full name, “Title of the Article,” *Title of the Magazine*, Date, Page x or pp.x-x.

範例

張晏彰，〈臺美夥伴關係 印太安定力量〉，《青年日報》，2019 年 6 月 19 日，版 3。

陳文樹，〈澎湖空軍基地的設立和演進〉，《中華民國的空軍》，2019 年 6 月 12 日，頁 21。

Jason Pan, “Defense think tank inaugurated,” *Taipei Times*, May 2, 2018, p. 3.

Office of Defense Studies, “Commentary: 2012 Pentagon Report on Mainland China’s Military Development,” *Defense Security Brief*, July 2012, p. 9.

十五、網際網路資料

（一）請依照個別線上網站實際資訊，詳細臚列。

（二）引用網路版報紙的一般報導，無須註明版次，但須附上網址，其餘體例不變。

（三）引用電子報紙雜誌評論文章，或電子學術期刊論文，在頁碼後面註明網址，其餘體例不變，無頁碼者得省略之。

（四）直接引用機構網站的內容，請註明文章標題、機構名稱，日期與網址。

（五）中文：

1. 專書：作者姓名，《書名》（出版地：出版者，出版年），《網站名稱》，網址。
2. 論文：作者姓名，〈篇名〉，《刊物名稱》，第 x 卷第 x 期，年月，頁 x 或頁 x-x，《網站名稱》，網址。
3. 官方文件：官署機構，〈文件名稱〉（行政命令類）或《文件 名稱》（法律類），卷期（案號），日期，頁 x 或頁 x-x，《網站名稱》，網址。
4. 報導：作者姓名，〈篇名〉，《媒體名稱》，日期，網址。

範例

王業立編，《臺灣民主之反思與前瞻》（臺北市：臺灣民主基金會，2016 年），《台灣民主基金會》，http://www.tfd.org.tw/export/sites/tfd/files/download/book20160830.pdf。

舒孝煌，〈美陸戰隊 F-35B 前進遠征與輕型航艦部署〉，《國防情勢月報》，143 期，2019 年 5 月，頁 36，《國防安全研究院》，

https://indsr.org.tw/Download/%E5%9C%8B%E9%98%B2%E6%83%85%E5%8B%A2%E6%9C%88%E5%A0%B1-143.pdf。
中華民國國防部，《106 年國防報告書》，2017 年 12 月，頁 1，《中華民國國防部》，https://www.mnd.gov.tw/NewUpload/歷年國防報告書網頁專區/歷年國防報告書專區.files/國防報告書-106/國防報告書-106-中文.pdf。
游凱翔，〈國防安全研究院掛牌 唯一國家級國防智庫〉，《中央社》，2018 年 5 月 1 日，https://www.cna.com.tw/news/aipl/201805010122.aspx。

（六）外文：

1. 專書：Author(s)' full name, *Complete title of the book* (Place of publication: Publisher, Year）, p. x or pp. x-x, URL.
2. 論文：Author(s)' full name, "Title of the article," *Name of the Periodical*, Vol. x, No. x, Date, p.x or pp.x-x, URL.
3. 官方文件：Author's Full Name, "Title of the Article," Date, Section or Page Numbers, URL.
4. 報導：Author's full name, "Title of the article," *Name of the Media*, Month Day, Year, URL.

範例

Robert D. Blackwill, *Trump's Foreign Policies Are Better Than They Seem* (New York: Council on Foreign Relations Press, 2019), p. 1, Council on Foreign Relations, https://cfrd8-files.cfr.org/sites/default/files/report_pdf/CSR%2084_Blackwill_Trump_0.pdf.

Ralph A. Cossa, "Regional Overview: CVID, WMD, and Elections Galore," *Comparative Connections: A Quarterly E-Journal on East Asian Bilateral Relations*, Vol. 6, No. 1, April 2004, p.1, Pacific Forum, http://cc.pacforum.org/2004/04/cvid-wmd-elections-galore.

White House, "National Security Strategy of the United States

of America," December 18, 2017, p. 1, White House, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

Colin Clark, "Mattis' Defense Strategy Raises China To Top Threat: Allies Feature Prominently," *BreakingDefense*, January 18, 2018, https://breakingdefense.com/2018/01/mattis-military-strategy-raises-china-to-top-threat-allies-feature-prominently.

十六、第二次引註之格式

首次引註須註明完整之資料來源（如前述各案例），第二次以後之引註可採以下任一格式：

（一）作者姓名，《書刊名稱》或〈篇名〉，或特別註明之「簡稱」，頁 x-x。

（二）如全文中僅引該作者單一作品，可簡略為——作者，前引書（或前引文），頁 x 或頁 x-x。

（三）某一註解再次被引述，簡略為——同註 x，頁 x 或 x-x。

（四）英文資料第二次引註原則相同：op. cit., p.x or pp.x-x（前引書，頁 x 或頁 x-x。）

（五）Ibid. p.x or pp.x-x.（同前註，頁 x 或頁 x-x。）

十七、文末之參考文獻

（一）參考文獻原則上與第一次引述的註釋體例格式相同，惟書籍、研討會論文及博碩士論文無須註明頁數。

（二）所有文獻依前述註釋類別排列，並依中文、英文、其他語文先後排序。

（三）中文著作依作者姓氏筆畫排序，英文著作依作者姓氏字母排序。

（四）將書籍專章列為參考書目時，依專章作者排序。

（五）翻譯作品依翻譯語文類別，中文譯作按譯者姓氏筆畫排序，英文譯作按原作者姓氏字母排列。

（六）同一作者有多篇著作被引用時，按出版時間先後排序。

（七）每一書目均採第一行凸排 2 字元。

出版源由

衡諸 21 世紀國防事務發展趨勢，為整合國防政策之專業研究能量，拓展國際交流合作，以提升整體國防思維，建構符合國家發展、最適資源配置之政策建議，國防部參酌各先進國家國防智庫運作與發展經驗，捐助設立「財團法人國防安全研究院」，並發行本刊。本院設立宗旨：

一、增進國防安全研究與分析。

二、提供專業政策資訊與諮詢。

三、拓展國防事務交流與合作。

四、促進國際戰略溝通與對話。

本刊係國防安全研究院所發行之綜合性政策學術期刊，旨在提供國防安全研究專家與學者之專業諮詢與討論平台，提升我國國防安全研究能量。

稿約

一、《戰略與評估》以探討國防事務、區域安全情勢及戰略研究等議題為宗旨，每年三、九月出刊。本刊歡迎學有專精之學者、專家踴躍投稿。

二、論文請依一般學術論文規格撰寫，使用註解，說明來源，並以另紙書明中英文題目、姓名，兩百字以內之中英文摘要及四個關鍵詞。文長以一至二萬字為宜。來稿請附電子檔。來稿請一併示知服務單位、職稱、主要學經歷、研究專長、聯絡地址和電話。

三、本刊採隨到隨審方式，無截稿日期之限制。來稿均須經本刊正式審稿程序，本刊對來稿有編輯與刪改權。

四、請作者自留原稿影本或電子檔，來稿未刊登者，本刊恕不退件。來稿一經刊載，除贈送作者本刊外，另依本刊規定致奉稿酬。

五、本刊恕不刊登翻譯著作。

六、凡本刊刊登之論文，版權歸本刊所有；本刊所載文章為作者個人之意見，僅供學術研究發展之參考，不代表本單位及任何機關政策或立場。

七、來稿如有違反著作權法，作者負完全之法律責任，另本刊不接受作者申訴。

八、稿件請以掛號郵寄「10048 臺北市中正區博愛路 172 號『戰略與評估』編輯部」或電子郵件寄至 dsaj@indsr.org.tw。

財團法人國防安全研究院

Institute for National Defense and Security Research

I N D S R

ISSN 2223941-3