第九卷第一期 中華民國一〇七 / 一〇八年 冬季 ISSN 2223-9413

戰略與評估

Defense Strategy & Assessment Journal

論文

黃恩浩
中國崛起與中日釣魚台爭端

黃宗鼎
中華民國南沙主權論述的再檢視

Brooke A. Smith-Windsor
From 'Armed Attack' to 'Cyber Attack':
The Evolution of Collective Self-Defense in NATO

Hyeong-Wook Boo
Kyung-Roak Kang
An Assessment of North Korean Cyber Threats and the Republic of Korea's Policy Responses: An Update

Vol.9 No.1
Winter 2018/2019

財團法人國防安全研究院 出版

戰略與評估

第九卷第一期 中華民國一〇七／一〇八年 冬季

Defense Strategy and Assessment Journal

Vol.9 No.1 WINTER 2018/2019

出　　版：財團法人國防安全研究院
發 行 人：馮世寬
主　　編：李瓊莉
編 輯 委 員：王高成、李瓊莉、李俊毅、沈明室、林正義、林文程
馬振坤、劉復國、歐錫富（依姓氏筆劃排列）
執 行 編 輯：舒孝煌
助 理 編 輯：蔡榮峰
校　　對：林愷萍、許智翔
出 版 企 劃：胡國荃
電　　話：(02)2331-2360 轉 732
傳　　真：(02)2331-2361
電 子 信 箱：stellar.shu@indsr.org.tw
院　　址：10048 臺北市中正區博愛路 172 號
I S S N：2223-9413

戰略與評估

第九卷第一期

目錄

論文

中國崛起與中日釣魚台爭端	黃恩浩	1
中華民國南沙主權論述的再檢視	黃宗鼎	35
From ‘Armed Attack’ to ‘Cyber Attack’: The Evolution of Collective Self-Defense in NATO	Brooke A. Smith-Windsor	59
An Assessment of North Korean Cyber Threats and the Republic of Korea’s Policy Responses: An Update	Hyeong-Wook Boo Kyung-Roak Kang	79

作者簡介

黃恩浩	澳洲墨爾本大學政治學博士。現任國防安全研究院國防戰略與政策研究所助理研究員。曾任澳洲墨爾本大學社會暨政治科學院榮譽研究員、國立政治大學國際關係研究中心博士後研究員、東海大學社會科學院博士後研究員。研究領域為戰略文化、海權研究、中共海軍與海洋戰略、澳洲國防與外交。
黃宗鼎	國立暨南國際大學博士。現任國防安全研究院中共政軍研究所助理研究員。曾任兼任助理教授、天下雜誌、東森雲論專欄作者、越南翰林院訪問學者。研究領域為中國東南亞關係、中國政治、越南研究、南海問題。
Brooke Smith-Windsor	Senior Research Fellow at RAND Europe, former Director of Strategic Guidance at the Canadian Department of National Defense. Dr. Smith-Windsor served in NATO for ten years as Canada's Senior National Representative and Deputy Head of Research at the NATO Defense College.
Hyeong-Wook Boo	A Virginia Tech Ph.D. in Public Affairs, Research Fellow at the Center for Security and Strategy, Korea Institute for Defense Analyses (KIDA), former Chief of Defense Strategy Research Division for KIDA. Dr. Boo was the Deputy Secretary of Peace and Arms Control to the South Korean President.
Kyung-Roak Kang	A London School of Economics and Political Science (LSE) M.SC. in Political Science and Political Economy, Research Assistant at the Center for Security and Strategy, KIDA.

中國崛起與中日釣魚台爭端

黃恩浩

國防安全研究院國防戰略與政策研究所　助理研究員

摘　　要

自從中國大陸與日本於 2012 年爆發釣魚台群島主權爭端以來，造成雙方關係緊張與衝突危機升級，此狀況直到近期才似乎有逐漸緩和之趨勢。儘管「中」日關係之間經濟互賴迄今依舊緊密，但是雙方在東海區域釣魚台主權歸屬議題上的爭議卻難以消弭。事實上，這「中」日在 2012 年對釣魚台主權的衝突事件，可以被視為是在中國崛起的現象中，「中」日雙方不斷提升對彼此威脅認知所形成的對抗案例。當時雙方面對釣魚台問題時都藉由堅持領土主權主張、擴大軍事武力展示、拉攏戰略同盟，以及提升國際影響力等方式來表達各自對釣魚台主權的訴求。為了能夠清楚了解，究竟這「中」日之間釣魚台衝突的本質為何？本文乃試圖在中國崛起的脈絡中，從「中」日雙方的釣魚台政策與國際作為，探討「中」日釣魚台衝突所造成政策困境的核心關鍵，並分析「中」日是否能夠超越彼此對領土與歷史主觀詮釋，並共同尋求區域安全合作的可能性。

關鍵詞：「中」日衝突、政策困境、威脅認知、釣魚台問題、安全戰略

The Rise of China and the Sino-Japan Diaoyutai Islands Conflicts

Paul An-Hao Huang

Assistant Research Fellow
Division of National Defense Strategy and Policy Research,
Institute for National Defense and Security Research

Abstract

Since the outbreak of the Sino-Japanese sovereignty disputes of the Diaoyutai (Senkaku) Islands in 2012, tension between China and Japan has increased and the probability of a conflict crisis has also escalated. This tense situation has only recently appeared to have gradually eased. Although economic interdependence between China and Japan is still tight, the controversy over the sovereignty of Diaoyutai in the East China Sea region remains difficult to resolve. In fact, this Sino-Japanese conflict over Diaoyutai in 2012 can be seen via the context of the rise of China, as a case of political-military confrontation between China and Japan, and the perception of threats between the two sides has been continually amplified. When the two sides faced the problem of Diaoyutai, they constantly expressed their claim on the terrirorial sovereignty of Diaoyutai, expanding the display of military forces, rallying strategic alliances, and enhancing international influence. In order to clearly understand the nature of the Diaoyutai conflicts between China and Japan, this paper attempts to explore the core of the policy dilemma created by the conflicts between the two

sides, and to analyze whether China and Japan can transcend each other's subjective interpretation of territory and history, and possibly jointly seek regional security cooperation on the Diaoyutai issue in the context of the rise of China.

Keywords: *Diaoyutai (Senkaku) islands, Sino-Japanese disputes, security strategy, strategic realignment, threat perception*

壹、前言

中國大陸與日本在 2018 年 6 月 8 日啟動延宕已久的「海空聯絡機制」，但這機制究竟能否解決雙方當前東海區域的釣魚台爭端？這是個值得觀察的問題。自 2012 年以來，「中」日爭奪釣魚台主權已經造成雙方武裝衝突危機升高，中共當時藉由民族主義手段，不斷煽動仇日情節與反日示威抗議活動來吸引國際社會注意，回應日本將釣魚台群島收歸國有化之舉。北京當時更發佈《釣魚台是中國固有領土》白皮書並指責日本竊佔該群島。[1]日方則解釋，此舉是為了防止東京都知事對釣魚台群島的掌控，並且發表《關於尖閣諸島的基本見解》聲明釣魚台是日本固有國土。[2]當時北京認為，將釣魚台收歸國有化是日本刻意之舉動，因此強烈以民族主義為立足點來處理釣魚台主權爭議。日本政府認為釣魚台為日本領土是無庸置疑地，於 2012 年以後更展現強力決心要維持對釣魚台的實質控制。對此，中共則宣布在東海區域建立防空識別區將釣魚台包含在內，並且持續派遣艦艇與飛機在東海釣魚台周邊進行例行巡邏，導致「中」日雙方衝突逐漸惡化。

學者菅沼雲龍認為，「中」日釣魚台衝突是到了 1970 年代初期才逐漸浮現出來的，因為聯合國亞洲與遠東經濟委員會下設的「近海地區礦產資源勘查聯合協調委員會」[3]於 1968 年在東海區域附近發現石油與天然氣資源之後，中共與台灣才開始積極對釣魚台聲稱擁有主權。釣魚台在二戰後原本是由美國所控制，依據 1971 年的《美日琉球及大東協

* 筆者除了感謝審查委員的指導，亦感謝國防安全研究院王尊彥博士與林彥宏博士提供寶貴建議與日文協助。

1 中華人民共和國國務院新聞辦公室，《釣魚台是中國固有領土》白皮書，2012 年 9 月 25 日，http://www.scio.gov.cn/tt/Document/1222670/1222670.htm。

2 日本外務省，《關於尖閣諸島的基本見解》，2012 年 11 月， https://www.mofa.go.jp/region/asia-paci/china/pdfs/r-relations_cn.pdf。

3 Unryu Suganuma, *Sovereign Rights and Territorial Space in Sino-Japanese Relations: Irredentism and the Diaoyu/Senkaku Islands* (Honolulu: Association for Asian Studies and University of Hawaii Press, 2000), p. 271；「近海地區礦產資源勘查聯合協調委員會」的正式英文名稱為 “Committee for Coordination of Joint Prospecting for Mineral Resources in Asian Offshore Areas”。

定》，美國於 1972 年轉交釣魚台給日本。[4]雖然當時中共主張，釣魚台原本就屬於中國大陸領土，是日本在甲午戰爭後趁機將之竊取。[5]日方則堅持釣魚台群島並不存有爭議，這群島原是屬「無主地」（*terra nullius*），[6]日本是基於「先占原則」所獲取的。因為「中」日在 1972 年 9 月 29 日發表《建交聯合公報》後，雙方互動焦點是促進雙邊關係正常化，當時中共國務院總理周恩來與日本首相田中角榮都有默契想擱置這釣魚台議題，所以雙方當時在東海的漁業行為也都相當克制。[7]

當談到釣魚台主權爭議涉及能源資源爭奪問題時，文獻上的論點主要有兩派看法。首先，重視經濟自由主義的樂觀派主張，這「中」日領土衝突危機的升高並不會阻礙雙邊經貿合作與發展，而經貿合作亦會限制這無限上綱的衝突。[8]然而，強調現實主義的悲觀派則認為，「中」日會將這領土危機與國內政治做一個連結，最後導致一個民族主義對抗的局面。學者 Reinhard Drifte 曾指出，由於受到改革開放的影響，導致中國大陸國內社會多元化快速發展，各種以民族主義為號召的社會團體與鷹派軍事集團因此可以更積極的聲稱釣魚台主權，這使得專責處理中國問題的日本外務省於 1990 年代末期逐漸喪失對於中國大陸政策的全面掌握。[9]學者 Phil Deans 認為，在當時在中國大陸、台灣與日本各自的國內政治衝突中，各方已經藉由釣魚台衝突議題，開始醞釀並型塑各自

[4] UN Treaty Collections, "Agreement between Japan and the United States of America Concerning the Ryukyu Islands and the Daito Islands," https://treaties.un.org/doc/publication/unts/volume%20841/volume-841-i-12037-english.pdf.

[5] 林泉忠，〈釣魚台列嶼爭議一百二十年〉，《明報月刊》，2015 年 3 月號，https://www.mofa.gov.tw/Upload/RelFile/642/152410/釣魚臺列嶼爭議的形成過程.pdf。

[6] Shigeyoshi Ozaki, "Territorial Issues on the East China Sea: A Japanese Position," *Journal of East Asia & International Law*, Vol. 3, No. 1, 2010, pp. 151-174.

[7] Unryu Suganuma, *Sovereign Rights and Territorial Space in Sino-Japanese Relations: Irredentism and the Diaoyu/Senkaku Islands* (Honolulu: Association for Asian Studies and University of Hawaii Press, 2000), p.136.

[8] Min Gyo Koo, "The Senkaku/Diaoyu Dispute and Sino-Japanese Political-Economic Relations: Cold Political and Hot Economics?" *The Pacific Review*, Vol. 22, No. 2, 2009, pp. 205-232.

[9] Reinhard Drifte, "Japanese-Chinese Territorial Disputes in the East China Sea between Military Confrontation and Economic Cooperation," Asia Research Centre Working Paper (2008). Asia Research Centre, London School of Economics and Political Science, http://eprints.lse.ac.uk/20881/1/Japanese-Chinese_territorial_disputes_in_the_East_China_Sea_(LSERO).pdf.

的民族主義意識型態以轉移國內衝突的焦點。[10]釣魚台衝突的複雜性就北京當局而言，學者潘仲琦認為主要是受到於領土衝突與國內政治的影響，因「中」日領土爭端跟國際權力鬥爭及民族主義的連結很深，釣魚台議題因此成為「中」日關係發展中的關鍵問題。[11]

究竟「中」日間領土衝突議題為何會在短時間之內變成一個雙方高度爭論的焦點？目前這個問題尚鮮少被拿出來討論。回顧相關文獻可以了解到，「中」日雙方在歷史的論述上都堅持各自的歷史解釋，加上從日本首相參拜靖國神社至日本教科書修改二次大戰史實等事件，這些種種導致雙邊都面臨外交僵局的壓力。目前「中」日雙方對於釣魚台爭端危機儘管已趨向保持沈默，但實際上仍無和緩的跡象。一般認為導致這「中」日衝突危機的主要因素有四點：一、中共崛起造成區域權力平衡的變化；二、日本面對中共擴張的政治經濟壓力；三、釣魚台群島的地緣位置；四、美國在釣魚台爭議中的角色。[12]目前中國解放軍海軍已具備將武力投射至第一島鏈以外的能力。面對中共擴張，美國因此直接給予日本關於領土衝突的安全承諾，但卻無助於解決釣魚台爭端。筆者認為，因在釣魚台衝突中，「中」日面對彼此的威脅壓力與雙方的政策困境，乃是加劇釣魚台爭議的重要因素。

貳、中共崛起對「中」日關係的影響

中共在快速的經濟成長下，直接帶動了其政治軍事影響力的提升。在中共崛起之過程中，受影響最多的就是亞洲區域國家，對日本的影響更是深刻。雖然中國大陸經濟發展順勢帶動著日本的經濟成長，例如許多中國大陸旅客和留學生在日本大量消費，刺激日本經濟，但是中共軍事政治力量的增強卻相對地減低了日本對亞洲的影響力。基於日本長期遭受經濟不景氣的困境，中共崛起對日本而言，是一個經濟上的機會，

[10] Phil Deans, "Contending Nationalisms and the Diaoyutai/Senkaku Dispute," *Security Dialogue*, Vol. 31, No. 1, 2000, pp. 119-131.

[11] Zhongqi Pan, "Sino-Japanese Dispute over the Diaoyu/Senkaku Islands: The Pending Controversy from the Chinese Perspective," *Journal of Chinese Political Science*, Vol. 12, No. 1, 2007, pp. 71-92.

[12] Paul J. Smith, "The Senkaku/Diaoyu Island Controversy: A Crisis Postponed," *Naval War College* Review, Vol.66, No.2, 2013, pp. 27-44.

但同時也是一個政治軍事上的挑戰。究竟要如何接受機會並且避免挑戰，日本在嘗試制訂一個「政經分離」的中共政策時遇到瓶頸。反之，因為中國經濟和技術高度依賴日本，所以中共在制訂日本政策時，究竟要如何維持與日本關係，同時又能夠擱置雙方在歷史與領土上之爭議，這狀況也造成中共對日政策的困境。

就釣魚台爭議而言，中共在進行改革開放之初，對釣魚台問題的基本態度是傾向「大事化小」，這亦是當時周恩來與田中角榮於建交談判中就「釣魚島問題放一放，留待以後解決」達成重要諒解和共識；[13]而鄧小平在 1978 年底訪問東京也曾提及「釣魚台主權問題可在日後慢慢解決。」[14]中央研究院林泉忠副研究員認為，當時中共領導人對釣魚台的處理方式影響了日本在釣魚台不駐軍、不進行島上開發、不開採海底資源之作為。[15]隨著中共崛起與擴張，「中」日雙方當時對釣魚台的外交默契與行為克制於 1990 年代後就逐漸鬆動，在雙方面對彼此威脅的壓力下，雙邊外交關係與政策也遭遇兩難，因而導致今日雙方釣魚台爭議的公開化與常態化。

一、「中」日彼此威脅認知與釣魚台問題

國家對威脅的主觀認知是形塑國家行為與國際互動的重要關鍵，瞭解這威脅認知是如何在國家之間被建構出來的，這因此是瞭解「中」日釣魚台爭議與衝突時的一個重要課題。基本上，「中」日之間的競爭與衝突不會因著釣魚台問題解決而終止，因為雙方之間的矛盾一直交雜著客觀環境與主觀認知等要素。倘若雙方都能夠改變對即存威脅的主觀認知，這才有可能讓彼此關係走向和平發展，否則釣魚台問題將會一直是「中」日之間的發生摩擦與爆發衝突的引爆點。

根據學者 Tuomas Forsberg 的觀點，領土爭端並非只是表現在具體的權力政治衝突，更是呈現在國際法領域的爭議。聯合國憲章對領土原

[13]日本外務省，〈有關尖閣諸島的問與答〉之第十四問，http://www.hk.emb-japan.go.jp/chi/territory/senkaku/question-and-answer.html。

[14] 中國社會科學院近代史研究所，「歷年保釣事件記載」，《中國社會科學網》，2008 年 6 月 16 日，http://jds.cass.cn/ztyj/tgas/201605/t20160506_3326567.shtml。

[15] 林泉忠，〈釣魚台列嶼爭議一百二十年〉，同前註。

則有明文規範，領土衝突將逐漸被視為法律規範領域。在二戰結束後，國際領土爭奪案件已逐漸減少，假使領土主張若非依據無主地原則，以民族自決原則處理領土主權議題將必須訴諸法律途徑。所以當國家之間對具爭議領土的法律地位主觀認知不同時爭端就會發生，爭議國之間對於領土主權爭議其實並不容易達成一個具有規範性的共識，使得擱置爭議的妥協默契成為解決爭端之暫時方法。

換言之，任何國家對於領土相關的主張與行動，都會直接挑戰到周邊國家的領土主張與其法定領土主權的地位，因而產生威脅認知，在彼此都克制以武力解決領土問題的情況下，就會導致政策上的困境。當然，領土衝突亦可以被視為是一種情緒上的主觀互證之結果，因為領土不僅涉及到國家戰略利益或經濟利益，同時也涉及到主權、民族主義與國家認同的領域。目前東北亞地區大部分國際間領土爭端幾乎都源自於，二次戰後國際制度規範對領土與歷史認知的不一致性的結果，而「中」日之間的釣魚台爭議就是如此。

二、釣魚台爭議下的「中」日外交困境

中共崛起伴隨軍事力量的提升，難免會給其他國家窮兵黷武的印象，甚至造成 1990 年代以來「中國威脅論」在日本及其他亞洲國家甚囂塵上。雖然中共強調「大國崛起」是和平的，但是如同歷史上的強權崛起一般，中共強權之路難免也會與其他周遭國家發生一些爭端與衝突。在今日美國主導的印太秩序之下，中共似乎不太可能像過去普魯士須發動普丹、普奧及普法戰爭，以及日本帝國需發動甲午和日俄戰爭般，以戰爭做為大國崛起的步驟。[16]然而與鄰近國家的利害衝突，卻是中國大陸自 1980 年代開始崛起以來迄今難以避免的宿命，這也導致東亞地區國家對於中共崛起與壯大現象產生安全困境。[17]

---

[16] 蘇俊斌，〈諸國崛起後的日本對中政策〉，《台灣國際研究季刊》，第 8 卷第 2 期（2012 年夏季號），頁 18-19。

[17] 安全困境是國際關係理論中用以解釋國際緊張、對立乃至造成衝突的一個重要概念。理論上，國際之間安全困境的情境是發生於，當國家行為者雙方在安全問題上彼此資訊不透明，以及互相不信任的情況下，對他國可能的行為做出最壞的評估，因此不斷透過增添軍備、建立預防措施與強化軍事活動來維護國家利益與安全，殊

從 1990 年代中期起，日本開始重新檢視這一個崛起中但不十分友善的強鄰。畢竟對許多日本人而言，中共對日本的強硬態度，不過是內部的政治鬥爭工具，卻強把日本當標的。在外交領域上，為了對應中共的強大，日本對東海區域安全與釣魚台主權問題則逐漸轉向強硬。在經貿上，「中」日兩國的互補性，也因為中國大陸經濟快速成長，雙方逐漸成為競爭態勢，尤其是對資源的爭奪更為明顯，例如在釣魚台附近的海底石油與天然氣。中共的崛起使得中日雙方對彼此更不具有好感，[18]但是在又得在經貿上相互依賴之情況下，兩國外交發展就陷入了政策制訂的兩難。在這種政策制定環境下，「中」日因此得制定既競爭又合作的政策，目前「中」日對釣魚台的處理方式就是如此，雙方在政策上都主張對該列島有主權，但是在行動上卻又克制住不讓對峙情況提升至軍事武裝衝突。

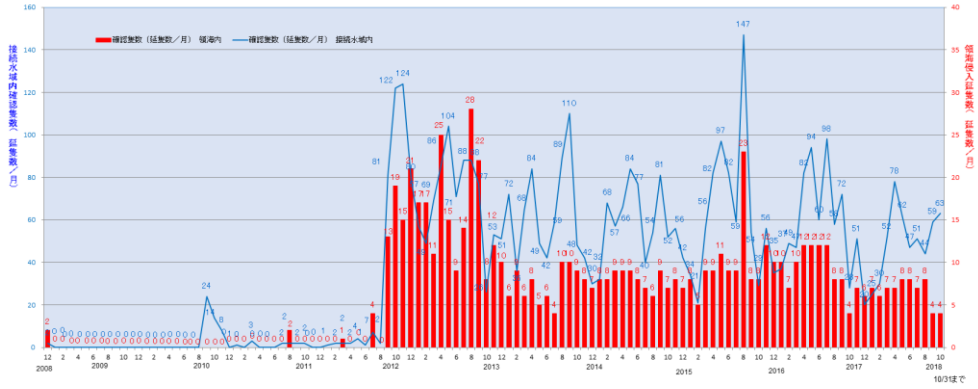
儘管在「中」日在 1970 年代達成擱置釣魚台爭議的默契，但是而隨中共崛起導致這雙邊默契逐漸被打破。北京的外交方向從鄧小平的「韜光養晦」走向習近平的「有所作爲」，對釣魚台主權爭議亦從被動「擱置」逐漸轉到主動「聲索」，這因此構成目前釣魚台困境的重要背景。例如：2004 年中國大陸出現首波民間保釣運動，中國保釣人士首次登島。2008 年 12 月 8 日，中共海監 46 號與海監 51 號首次進入釣魚台 12 浬。在 2010 年「『中』日釣魚台撞船事件」發生之後，中共漁政船開始在釣魚台海域頻繁巡戈，試圖以行動來片面改變該海域現狀。[19]日本政府於 2012 年 9 月 11 日宣佈對釣魚台「國有化」之後，中共海警船

不知自己在他國的眼裡，卻變成最大的威脅，使他國的安全感被大幅降低的情況下，亦爭相擴充軍備和增加軍事活動，這反而使自己處於更不安全的弔詭狀態。參考：Robert Jervis, “Cooperation under the Security Dilemma,” *World Politics*, Vol. 30, No.2, January 1978, pp. 167–170; John H. Herz, “Idealist Internationalism and the Security Dilemma,” *World Politics*, Vol. 2, No. 2, January 1950, pp. 157-180.

[18] 根據 BBC 在 2010 年 4 月所公布的調查（BBC World Service Poll, 2010），約只有 18%的日本人對中國持有正面的印象，但是卻有 38%的日本人持負面印象。相對地中國則有 29%的人民對日本持正面印象，卻有 47%不具好感，http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/160410bbcwspoll.pdf.

[19] 路西，「日中島嶼之爭，安倍稱不許以實力改現狀」《BBC 中文網》，2013 年 7 月 12 日，https://www.bbc.com/zhongwen/trad/world/2013/07/130712_japan_abe_sea；亦可參考：畠山京子，「中日爭奪亞洲區域領導地位之靜默對抗」，《歐亞研究》，第二期（2018 年 1 月），頁 105-112。

與公務船在釣魚台海域的「維權」行動更是趨於例行化與頻繁化（請參考圖 1），[20]在 2017 年以後，中共每月三次派出公務船且每次維持四艘，在日本主張的釣魚台領海內每次航行兩小時之狀況很多，日本將此稱為「3、4、2 模式」。[21]在 2013 年，中共更片面設置「東海防空識別區」直接與日本防空識別區重疊並涵蓋釣魚台，造成該區域緊張情勢升高（請參考圖 2）。



圖一、中共公務船進入釣魚台海域之統計

資料來源：日本海上保安廳，「尖閣諸島周辺海域における中國公船等の動向と我が國の対処」。 http://www.kaiho.mlit.go.jp/mission/senkaku/senkaku.html

[20] 日本海上保安廳，「尖閣諸島周辺海域における中国公船等の動向と我が国の対処」，http://www.kaiho.mlit.go.jp/mission/senkaku/senkaku.html。

[21] 「國有化」5 年後的東海與中日，《日經中文網》，2017 年 9 月 12 日，https://zh.cn.nikkei.com/politicsaeconomy/politicsasociety/26955-2017-09-12-04-51-10.html。

圖二、中日防空識別區重疊區域示意圖

資料來源：藍孝威，「大陸東海防空識別區含釣魚台」，《中時電子報》，2013 年 11 月 24 日。https://www.chinatimes.com/newspapers/20131124000713-260108

面對中共擴張的壓力，日本於 2010 年對釣魚台議題正式提出「尖閣諸島不存在領土問題」與「『中』日不存在擱置領土問題的共識」之主張，傾向強化對「南西諸島」之防衛，形成直接與北京較勁的新局面。當日本政府將釣魚台「國有化」後，引發中國社會的激烈反應與最大規模的反日遊行，雙方關係跌到 1972 年「關係正常化」以來的最低點，東海局勢也隨之緊繃。此時，「中」日釣魚台衝突似乎已經達到白熱化的地步，雙方對彼此的威脅感也達到前所未有的極端。

儘管美國並非本文所要探討的重點，但在論述中共與日本之間的釣魚台衝突時，美國在東亞區域的安全角色就顯得重要且值得一提。當美國在國際體系內有能力牽制中共擴張時，任何美國在東亞所涉及的區域或雙邊事務，都將對中共與日本造成一定程度的影響。對中共而言，美國在區域上牽制中共擴張的作為，將會弱化中共在區域上的主權聲索、對抗或挑釁行為。例如：《日美安全保障條約》明白規定美國對日本負

有防衛義務，這無疑對中共就是一種無形的嚇阻。[22]就日方而言，由於美日在區域與雙邊事務上交往是具有安全利益的，假使美國不願意或是沒有能力在東亞區域制衡中共的擴張與威脅，日本不僅將可能在區域中自立強化國防能力，也將尋求區域其他支持者並深化與周邊國家的關係。具體來說，假使「中」日之間的衝突不存在美國因素，那麼雙方在釣魚台困境中的衝突將可能是更為直接。

一般而言，全球與區域的安全連結是國防戰略中所不可忽視的要素，對國際共同安全利益的考量有可能會限制「中」日武裝衝突。然而，領土衝突對主權國家而言卻是核心利益，所以領土無法成為「中」日談判的工具。因此當兩國關係發展存有領土爭議的，武力展示或使用就會成為解決這爭議的必要途徑，尤其是當這具爭議的領土還包含有經濟與安全利益時。假使支持維持釣魚台現狀的日本以行動捍衛該領土現狀，中國將會視日本行為是種挑釁，並且會使雙邊對抗局勢更難緩和。反之，假使中國試圖以軍事手段控制這爭議的領土，日本就會認為其安全受到威脅，並且會以增強防衛力量的方式來因應中國的挑戰。

參、中日關係正常化以來的釣魚台爭議

中日關係自1972年正常化以來，中日釣魚台問題就隨著中國崛起而逐漸從雙邊民間保釣運動擴散至官方衝突。在中共加速軍事現代化而造成日本強化威脅感的過程中，釣魚台問題可以說是「中」日敵對關係的導火線，而這雙邊敵對關係更是與國內政治、國家認同和民族主義等因素緊密糾纏在一起所導致。在1970年代鄧小平推行改革開放之初，中共國力相對比較弱勢，所以北京當局對日本表現較為友善的態度。然而，到了1980年代末期江澤民上台後，中共綜合國力發展與影響力開始擴張，挑戰區域安全，造成「中」日關係中的釣魚台困境逐漸浮現，迄今更發展成具有可能引發衝突危機之局勢。以下就從1970年代「中」日關係正

[22] 美日安保條約第五條規定，對於日本施政之下的領域出現的「武力攻擊、共同危險」，日美需共同應對。參考：〈日美安全保障條約第 5 條是什麼？〉，《日本經濟新聞》，2017 年 2 月 4 日，https://zh.cn.nikkei.com/politicsaeconomy/politicsasociety/23552-2017-02-04-11-08-41.html。

常化以來迄今，探討「中」日間一系列釣魚台爭議的發展。

一、1970-1980年代被擱置的「中」日釣魚台議題

「中」日兩國1972年建交之初，中共剛歷經了大躍進及文革的混亂時期，整個社會還是處於均貧的狀況；相對地日本卻已經過了1950至1960年代的高度經濟成長，並成為當時世界上的第二經濟大國，在雙方經濟互補的情況下，「中」日兩國進入了前所未有的外交蜜月期。中共自1970年代中葉開始經歷改革開放，雖然「中」日雙方間尚存著無可抹滅的二戰記憶與領土爭端，但當時雙方政府都願意展示對彼此的友好態度。日方當時不僅協助提供大量「政府開發援助」（Official Development Assistance）協助中共經濟發展，也藉此方式表達對中國大陸社會的關切。[23]重要的是，日本希望以此經濟援助方式推促中共走向國際社會。北京當時也歡迎日本提供的協助與貿易機會，並視此為獲得國際資金與先進技術促進國家經濟發展的重要途徑。[24]在「中」日政府建立外交關係後，雙邊在經濟互補的前提下維持友好關係，而鄧小平也將日本視為中國大陸經濟發展的模範，因為進行經濟改革與推動現代化被當時中國列為國家發展的第一優先順位，所以處理釣魚台爭議也就顯得沒有那麼重要。

在1982年，日本文部省修改歷史教科書，其中內容試圖淡化日本侵略亞洲行為，引發了中共與其他亞洲國家不滿，但是此爭議在當時並沒有升級到嚴重的衝突情境。北京當時沒有要求日本對此事件做深入調查與道歉，部分原因除了中國大陸經濟發展戰略的優先考量之外；另外部分原因是，由於日本當時的內閣官房長官宮澤喜一提出「鄰近國家條款」，[25]他不僅承認錯誤，而且把照顧鄰近亞洲國家關係作為審定教科

[23] 日本安倍首相於 2018 年 10 月 26 日訪問中國期間，宣布終止對中國近四十年以來的開發援助，但承諾會持續強化與中國合作。Steven Lee Myers and Motoko Rich, "Shinzo Abe Says Japan Is China's 'Partner,' and No Longer Its Aid Donor," *The New York Times*, 26 October 2018. https://www.nytimes.com/2018/10/26/world/asia/shinzo-abe-china-japan.html?_ga=2.68125393.1744460237.1541647946-68342518.1527481371.

[24] Tsukasa Takamine, *Japan's Development Aid to China: The Long-Running Foreign Policy of Engagement* (London: Routledge, 2006), pp. 136-157.

[25] 王大軍，「日本教科書審定制度」，《人民網》，2001 年 4 月 4 日，http://www.people.

書的基礎之一。基於以上背景，時任日本首相中曾根康弘在1985年8月15日參拜靖國神社，即使引起北京的譴責，但中共並未將這不滿情緒轉變成政治衝突。

在1972年美國總統尼克森與中共總理周恩來會面，美中關係終於破冰，北京那時已經瞭解到區域局勢必將隨著中國大陸的改革開放而有變化。因為「中」日友好關係的基礎並非是建立在深入相互瞭解與歷史共識之基礎上，所以北京當時也意識到，隨著美「中」關係正常化的轉變，日本面對中共的危機感，將有可能使日本再次走向軍事強權。這種權力關係與威脅認知的轉變，讓中共在1980年代埋下日後對日本的不信任感。更甚者，北京亦在新教育體系與國內媒體報導中，種下以民族主義為基礎的反日情緒。[26]學者鈴木章悟認為，在北京刻意的煽動下，日本因此就成為在中國大陸民族主義下對抗的目標，[27]這也為「中」日之間的關係添增了敵對的因素。

二、1990年代逐漸浮現的「中」日釣魚台爭議

在1990年代中期，基於國際與國內方面的劇烈變化，使得「中」日當時衝突的焦點主要是集中在歷史詮釋與安全建構方面，以下就國際與國內方面說明之。

（一）在國際方面：因為前蘇聯的解體，中共與日美安全合作的企圖不復存在。於1995年台海飛彈危機發生，中共在台灣海峽附近發射飛彈，依其說法是試圖「遏止台獨勢力」，造成了區域對中國軍事威脅產生恐懼。為了因應區域威脅，像是中共軍事擴張與北韓核武危機等，日本與美國因此開始升級區域安全機制，例如，1996年的《美日新安保宣言》及1997年《美日防衛合作新指針》。這安全機制擴大了美日關於維持亞太和平穩定與日本「周邊有事」的防禦範圍，在2000年後日本部署了愛國者3型（PAC-3）飛彈，也和美國合作開發陸基神盾系統，搭配

com.cn/BIG5/guoji/20010404/432568.html。

[26] Yinan He, “History, Chinese Nationalism and the emerging Sino-Japanese Conflict,” *Journal of Contemporary China*, Vol. 16, No. 50, 2007, pp. 1-24.

[27] Shogo Suzuki, “The Important of ‘Othering’ in China’s National Identity: Sino-Japanese Relations as a Stage of *Identity* Conflicts,” *The Pacific Review*, Vol. 20, No. 1, 2007, pp. 23-47.

標準三型（Standard Missile 3，SM3）海基反彈道飛彈系統。[28]然而，這日本方面的安全升級卻激起了中共對日本的反感。

（二）在國內方面：「中」日敵對關係的浮現亦是由雙方領導人擴大威脅認知所導致。一方面，隨著中國大陸快速的工業化與經濟成長，日本乃對此感到有相當的壓力，因為中國大陸經濟力的快速提升，相對就弱化了日本原本可以制衡中共的經濟實力量。此外，日本新世代都瞭解到二戰已經是過去的遙遠歷史，對於持守和解與補償的心態很不以為然，他們在意的焦點是當代中國大陸與日本發生的衝突事件。[29]日本激進修正主義領導人亦試圖藉著強化中共崛起的意象，為日本尋求軍事正常化的理由。[30]另一方面，中共採取新市場取向的經濟政策進行大幅度的經濟與社會改革，這改革使得中共在國家機器與社會結構兩層面能夠獲得一個平衡的發展，因此中共也不可能無視於社會大眾的輿論。[31]在2001至2005年間，北京對於日本首相參拜靖國神社之舉開始表達強力抗議，將其描述為日本軍國主義復甦的象徵，並且不斷宣傳日本侵略亞洲的歷史，目的不外乎就是想要藉此方式來獲得國內社會支持。儘管「中」日經貿關係自1972年以來就不斷成長，但雙方卻越來越著重以激進方式表達彼此敵對的歷史立場，導致雙方不時陷入外交上的僵局。

在1990與2000年間，中共的經濟與軍事擴張，對區域安全已構成挑戰。在中共快速崛起的背景下，「中」日對彼此的威脅感不斷地被放大，雙方對釣魚台議題的爭議也就越來越明顯，但此期間雙方的爭議卻只有限縮在非官方的表達範圍，例如：當時由右翼激進團體或是資源探勘行動所引起的民間對釣魚台的爭論。這段期間，中共官方只有以口頭聲稱根據1992年的《領海及毗連區法》擁有釣魚台合法主權，並且強調會積極開發東海區域資源。日本方面，右翼團體日本青年社則在1990與1996

[28] Tomonori Sasaki, “China Eyes the Japanese Military: China’s Threat Perception of Japan since the 1980s’,” *The China Quarterly*, No. 203, 2010, pp. 560-580.

[29] Ryosei Kokubun, “Changing Japanese Strategic Thinking toward China,” in Gilbert Rozmsn, Kazuhiko Togo and Joseph P. Ferguson eds., *Japanese Strategic Thought toward Asia* (London: Palgrave Macmillan, 2007), pp. 153-156.

[30] Richard J. *Samuels*, *Securing Japan: Tokyo’s Grand Strategy and the Future of East Asia* (Ithaca: Cornell University, 2007), pp. 120-127.

[31] James Reilly, “Remember History, not Hatred: Collective Remembrance of China’s War of Resistance to Japan,” Modern *Asian Studies*, Vol. 45, No. 2 (2011), pp. 463-490.

年企圖在具爭論的釣魚台重修燈塔，並藉此宣示日本的釣魚台主權。儘管雙方民間如此緊張對峙，但雙方政府卻都克制住而沒有將這緊張局勢擴大到外交層面。

現實上，當時北京面對民間的釣魚台爭議時，並不把日本政府與日本右翼團體混為一談，因為中共不想失去日本在中國大陸實際的經濟投資與優惠貸款，因這些都遠比跟日本爭奪釣魚台主權還重要。[32]在2008年6月18日，前中共國家主席胡錦濤訪日時已經與前日本首相福田康夫達成暫時擱置領土爭議並要聯合開發東海油氣的共識，包括：（一）雙方同意在東海地區擇一區塊共同開發；（二）中國大陸同意日本按照中共法律參與春曉油氣田合作開發案；（三）盡快完成相關換文與國內程序。[33]但是這嘗試以經濟途徑解決領土爭議的效果卻是相當有限的，因為中共一直在雙方東海中間線附近推進新天然氣田開採的相關設施建設，在日本認定中共已違反東海聯合開採行動之後，「中」日東海聯合開發計畫就終止了。雖然雙方在未來重啟聯合開發似乎也不太可能，但是這計畫的終止在當時卻沒有激發雙方政治鬥爭，只因為雙方當時的經濟利益仍大於領土爭議。

三、2010年以來逐步升級的「中」日釣魚台危機

在2010年之前，「中」日面對釣魚台主權爭議時，彼此都還能保持一定程度的自我克制。在日本自民黨上台後，當時首相鳩山由紀夫的中共政策主張，日本應主動與中共改善關係，尋求與中共發展戰略關係並且積極與北京進行交流。然而其任期不到10個月，所以「中」日之間可能發展的戰略合作關係規劃乃隨鳩山由紀夫下台而停滯。[34]而當時首相鳩山由紀夫下台的原因主要是在2009年並沒有處理好美國海軍陸戰隊普天間基地（US Marine Futenma Air Base）的遷移議題。[35]

---

[32] Erica S. Downs and Phillip C. Saunders, “Legitimacy and the Limits of Nationalism: China and the Diaoyu Islands,” *International Security*, Vol. 23, No. 3, 1999, pp. 114-146.

[33] 林正義、陳鴻鈞，「兩個『中國』在東海的油氣勘探與美日的角色」，《遠景基金會季刊》，第 15 卷第 4 期（2014 年 10 月），頁 37-38。

[34] 石原忠浩，「『政治主導』的對外政策？—日本民主黨執政下的日『中』關係」，《展望與探索》，第 10 卷第 7 期（2012 年 7 月），頁 49-56。

[35] 美國國防部在 2010 年 2 月 1 日公布《四年期國防總檢討》（QDR）。 該報告基於台

（一）東海撞船事件激發「中」日釣魚台衝突

日本民主黨的菅直人在2010年6月上台後，並沒有持續前首相鳩山由紀夫的中共政策。於2010年9月7日，發生日本海上保安廳11管區巡視船與那國號（PL63）和水城號（PS11）在釣魚台海域兩度衝撞中共漁船閩晉漁5179號，並將該中共籍船長詹其雄扣押。[36]此事件使得中方指控這是日本侵略中共釣魚台主權之行為所致，為了要求日方立即釋放中共漁船與人員，北京政府當時以直接和間接的方式施壓日本，包括：片面取消「中」日部長級會議、不合外交禮儀地召見日本大使、終止向日本出口稀土，和未經授權逮捕4名進入軍事區域的日本公民等，藉此對日本政府表達強烈抗議。[37]直到2010年11月的亞太經合會中，胡錦濤與菅直人舉行會談後，才讓這事件才有所緩和，儘管雙方在釣魚島主權問題上都依然堅持立場互不相讓，各自宣稱對釣魚島擁有主權。這此東海事件可說是在2010年以來，「中」日雙方首次將此領土爭議升級至政府之間直接的衝突危機。

面對中共的強大壓力，日本當時菅直人內閣卻因內部缺乏協調，決策上優柔寡斷，而無法立即因應中共強勢態度。反而日本媒體與新聞報導卻不斷提供民間關於中共政府與社會反日情節與抗議事件，試圖藉此在日本社會中型塑中共威脅的公共輿論，指責北京放任反日示威是不負責任的行為等。[38]在多方考量下，日本政府最終決定釋放中共漁船與船員，據當時《讀賣新聞》統計，只有少數日本人民支持政府的決定，多數認為不適當。經此事件後，日本公共輿論已經形成對中共威脅的反感態度，此認知更給日本政府必須發展正常化國防的重要理由。

「中」日領土衝突危機於2010年被激發之後並沒有降溫的趨勢，雙

海與朝鮮半島有事之想定，再度確認美軍陸戰隊所屬戰鬥部隊仍有持續駐防沖繩之必要性。普天間基地替代設施之所以難覓，在於美方對於陸戰隊整體機能之要求。由於陸戰隊是在緊急事態發生時，必須分秒必爭地緊急馳赴前線，因此，美國要求替代設施興建地點，必須在直昇機 20 分鐘航程可抵達 200 海浬內範圍，否則將讓駐沖繩陸戰隊失去作為快速反應之戰略嚇阻功能。

36 黃菁菁，「釣魚島衝突，日拘留陸船長 10 天」，《中國時報》，2010 年 9 月 11 日。

37 王尊彥，「尖閣／釣魚台争議を中心とした第二次安倍政権下の日中関係」，《問題と研究》，第 42 巻第 4 号（2013 年 12 月 30 日），頁 112-115。

38 同前註，頁 116-118。

方都藉此態勢強化對彼此的威脅觀，也將威脅認知也都寫進各自公開的官方文件中。例如：在日本防衛省在2011年發佈的《日本防衛》就寫到，中共將可能擴張軍事建設，與擴大海軍在東海、南海以及太平洋區域的活動。[39]該白皮書亦提及，美國已經關注到中共軍事日益壯大是對美國安全同盟的威脅，日本也注意到其領海在未來將可能會被中共海軍所入侵。[40]北京對日本描述的反應則表達強烈不滿，認為日本沒有立場指控中共是入侵者。中共在2012年9月發佈《釣魚台是中國固有領土》白皮書更強硬聲稱，日本竊取釣魚台且美日對釣魚台私相授受，強力反對日本對這些島嶼主張主權，中共將堅決捍衛釣魚台等。[41]

（二）日本將釣魚台收歸國有化導致「中」日嚴重海上對峙

日本野田政府於2012年9月11日決定「購買」三個釣魚台島嶼，企圖將釣魚台收歸國有，此舉引發了「中」日官方間大規模激烈的爭論。因為當時任東京都知事的石原慎太郎提出聲明，要與擁有釣魚台島嶼的日本島主談判收購，更指責當時日本政府面對中共時的懦弱外交，以及對北京的卑躬屈節作為，並要求海上保安廳與海上自衛隊應該強力驅逐中國船隻。對此，日本民主黨政府乃決定趕在石原慎太郎收購釣魚台島嶼之前先將釣魚台國有化，並單方認為這不會導致與「中」方的任何衝突，因為依據日本國內法，這些島嶼原本就是日本所掌控，購買這些島嶼僅涉及所有權轉移而已。[42]

針對日本將釣魚台國有化之舉動，中共認為這是日方有計畫地對釣魚台進行事實控制的關鍵步驟。於是北京在同年9月14日成立「中國共產黨中央海洋權益維持工作指導小組」，由習近平擔任組長，分別從經濟、外交與法律等方面對抗日本的國有化舉措。[43]再者，北京譴責日本

[39] Ministry of Defense of Japan, *Defense of Japan 2011*, p.84. http://www.mod.go.jp/e/publ/w_paper/2011.html.
[40] *Ibid*., p. 28.
[41] 中國國務院新聞辦公室，《釣魚島是中國的固有領土》，2012 年 9 月 25 日，http://www.scio.gov.cn/zxbd/tt/Document/1222670/1222670.htm。
[42] 楊明珠，「日內閣會議確認釣魚台國有化」，《大紀元》，2012 年 9 月 10 日，http://www.epochtimes.com/b5/12/9/10/n3679216.htm。
[43] 董佩琪，「習近平領軍設指導小組捍海權」，《旺報》，2013 年 2 月 5 日，https://tw.news.yahoo.com/習近平領軍-設指導小組捍海權-213000898.html。

行為之強烈措辭，在經由中共官方媒體有計畫的傳播後，導致有超過中國大陸50個城市發生反日示威事件並杯葛日本商品，此時官方媒體顯然是中國煽動民族主義與愛國主義的工具。[44]在日本收歸釣魚台之後，不僅中國的民間私人船隻，連軍方的岸防艦艇、海軍驅逐艦與軍機等都靠近該爭議群島以表示抗議。在2013年1月後，中共海軍在東海海域數次將射控雷達鎖定日本自衛隊船艦或艦載直升機。在2017年5月18日，中國更首次派出小型無人機進入釣魚台海域，[45]這些挑釁導致「中」日關係日益緊繃。

日方認為，這中共官方與民間共同對釣魚台國有化反應的擴大，將會危及到日本安全與經濟利益。究竟當時中國國內進行政權轉移是否對這事件有影響這很難說明，在2012年11月習近平確定成為中共領導人之後，日本就假設中國大陸社會對日本的抗議與杯葛，將會刺激中共領導人對日本採取強硬政策。同年12月，自民黨的安倍首相再次執政後，日方公開表達要強化在東海區域巡邏與防禦能力之決心。在2013年，日本十年以來首次增加國防預算，並升級無人機、飛機與戰機等軍事武器系統。[46]日本自衛隊也藉由展示自二戰結束以來最大的「出雲號」驅逐艦（JS Izumo, DDH-183），並參與相關的海上軍事演習等行動以展現武力，試圖藉此牽制中共的威脅。

分析中共在東海的行為時，中共內政局勢與民族主義這兩要素就顯得至關重要。在2013年，薄熙來事件的發生明顯呈現出中國共產黨內部的權力鬥爭現象，為了防止黨的醜聞造成民心背離，當時習近平乃提出「中國夢」的論調，想藉此重新強化社會對中共和國家的凝聚力。[47]在

[44] Ian Johnson and Thom Shanker, "Beijing Mixes Messages over Anti-Japan Protest," *The New York Times*, September 16, 2012. http://www.nytimes.com/2012/09/17/world/asia/anti-japanese-protests-over-disputed-islands-continue-in-china.html?partner=rss&emc=rss&smid=tw-nytimes&_r=0.

[45] Reuters Staff, "Japan scrambles jets over China drone flight near disputed islets," *Reuters*, May 18, 2017. https://www.reuters.com/article/us-japan-china-drone-idUSKCN18E1Q9.

[46] Toshiya Takahashi, "Japan's 2013 defense white paper stirs tensions with China," *East Asia Forum*, July 31, 2013, http://www.eastasiaforum.org/2013/07/31/japans-2013-defence-white-paper-stirs-tensions-with-china/#more-36915.

[47] Zheng Wang, "The Chinese Dream: Concept and Context," *Journal of Chinese Political Science*, Vol. 19, No. 1, 2014, pp. 1-13.

這背景之下，釣魚台爭端乃成為北京當局藉以強化中國人民對黨國向心力的一個可操作之議題。加上，安倍首相再次執政後，其參拜靖國神社之舉更深化了中共對日本的觀感，使得「中」日在釣魚台主權歸屬議題上的對峙更加嚴重。

肆、「中」日雙方處理釣魚台主權的外交作為

當釣魚台爭端達到高峰時，「中」日都傾向將此爭議訴諸國際社會以求獲支持，使得雙方對彼此的威脅認知得以擴散到國際上。在2012年的聯合國大會中，中共代表就提出一份官方的釣魚台列嶼海洋基線聲明，強烈控訴日本在1895年甲午戰爭時竊取這些群島，並指責軍國主義日本於1937至1945年武裝侵略中國大陸。許多中共學者與外交官員也對著當時國際媒體譴責日本行為，指控日本以假和平主張來掩蓋偷竊中國大陸釣魚台領土的事實，並且將日本與戰後德國相比，形容其為是一個執迷不悟的國家。[48]

對於中共向國際社會指控日本偷竊釣魚台，日本外交官對聯合國與國際媒體也做出強烈回應認為，北京聲稱其主權涵蓋釣魚台群島是完全沒有立場的。安倍政府為了處理與中共的領土爭議，因此在2013年設立了領土整合溝通顧問小組，主要是處理針對與中共領土議題之溝通行動。這小組也建議日本應該重建一個相對應於中共處理領土議題的官方辦公室，同時也要利用私部門資源來主張日本的釣魚台立場。[49]安倍政府在策略上傾向將「中」日釣魚台衝突與在南海衝突兩議題做一連結，企圖凸顯中共在東海與南海聲索主權的非法行為是對區域安全的挑戰，並藉此鞏固日本對於釣魚台的合法立場。

「中」日在國際層面的衝突，不僅是基於對領土主權歸屬的分歧，

[48] Agencies, "Chinese Ambassador Urges Japan to Learn from Germany over Wartime History," *Global* Times, January 15, 2014. http://english.jschina.com.cn/20322/201402/t1400612.shtml.

[49] Office of Policy Planning and Coordination on Territory and Sovereignty of Japan, *Recommendations of the Advisory Panel on Communications Concerning Territorial Integrity*. https://www.cas.go.jp/jp/ryodo_eg/torikumi/ryodoshitsu/ryodoshitsu-adp-03.html.

更是源於二戰的歷史記憶。有鑒於此，中共的部分論述是，當今日本持有釣魚台與二戰時日本帝國主義與殖民主義入侵與擴張息息相關，因此日本聲稱擁有釣魚台是不合法的主張。於2013年11月，北京當局乃藉擁有釣魚台主權在東海區域設置了防空識別區，這識別區涵蓋了部分日本控制的區域。日本認為中共設置的防空識別區直接挑戰到了道德上的立場。在二戰後，因為基於日本國憲法第9條規範的三大主軸：「放棄戰爭」、「不保持戰力」以及「否定交戰權」，[50]日本堅守成為一個和平與守法的國家，並在恢復國家聲譽方面積極做出努力，日本在戰後大力發展經濟的同時，其不僅不涉入任何國外軍事戰役，而且還提供發展中國家各種經濟與技術援助。

日本官方主張其對釣魚台事實與合法的控制是在二戰結束後，安倍強調日本一直是一個國際制度與規範的支持者，強力反對中共單方面設置防空識別區之行為。於2013年12月26日，安倍參拜靖國神社引起了中共與其他亞洲國家的反彈，也再次刺激到了中日之間敏感的領土爭議神經。於2014年，中共時任駐英國大使劉曉明在英國《每日電訊報》（*The Daily Telegraph*）撰文，指責安倍無視亞洲鄰國感情公然參拜靖國神社，並將日本形容成哈利波特系列電影中的佛地魔，時任日本駐英國大使林景一也以同樣的比喻形容中共，同時也嚴厲提出聲明，假使中共不信任日本而做出無根據的控訴，雙方的協調管道則將會關閉。[51]這種「中」日雙邊官方之間的相互指責與指控，在「中」日關係中是史無前例的。由於「中」日對彼此的威脅認知都交雜著相左的歷史經驗與敵對的民族主義，雙方相互之間的猜忌與不信任狀況更使得釣魚台衝突議題更趨於複雜。

「中」日為了避免在東海的海空域發生不可預期的衝突，早在十幾年前雙方就有意簽訂海空聯絡機制。2007年安倍首次擔任日本首相時，與時任中共國務院總理溫家寶達成共識，雙方國防部門從2008年4月起

[50] 張茂森，「日相促修憲法『放棄戰爭』條款，《自由時報》，2016 年 11 月 2 日，http://news.ltn.com.tw/news/focus/paper/100220。

[51] Agencies, “Latest China-Japan Spat: Who’s Voldemort?” *The New York Times*, January 9, 2014. http://sinosphere.blogs.nytimes.com/2014/01/09/latest-china-japan-spat-whos-voldemort/?_r=0.

組成共同作業小組展開協商，但因兩國關係於2012年因釣魚台而生變，雙邊協商也受到影響。為了處理東海危機管控問題，中日終於在2018年5月9日達成共識，在「擱置對立」的前提下，於6月8日開始啟用「海空聯絡機制」，該機制並不設置熱線也不標明釣魚台周邊海空域範圍，試圖以「模糊」方式處理釣魚台爭議可能引起的武裝衝突與外交對抗。

具體言之，釣魚台仍是「中」日難以解決的爭端，目前中共機艦在釣魚台海域的活動並未減少，所以該機制也只能制度性的處理非關釣魚台的偶發性衝突。[52]雖然這是戰後70多年來「中」日軍事部門簽署的第一份軍事防衛合作協議，初步代表雙方對於避免衝突危機升高已有共識。值得注意的是，中共總理李克強於2018年5月21日訪日，這是自2012年「中」日關係惡化以來中共總理首次訪日；而日本首相安倍亦在三連任自民黨黨魁後於2018年10月25日訪「中」。李克強稱「中」日關係已經「雨過天晴」，[53]安倍也稱雙方關係已經「回歸正軌」，[54]但是中共公務船與海警船照樣在釣魚台附近海域定期巡邏，[55]日本也只能低調向中共提出抗議。這海空聯絡機制是否能發揮「信心建立措施」實質功能，或僅是象徵意義，目前仍是未知數。

伍、釣魚台爭端引起的區域安全戰略

自釣魚台衝突逐漸白熱化以來，「中」日都藉機擴張軍事實力與區域影響力來建構彼此的國際安全環境，亞太區域權力結構也因此面臨重

---

52 毛峰，「李克強會晤安倍敲定中日海空聯絡機制」，《亞州週刊》，第 32 卷 19 期，2018 年 5 月 20 日，https://www.yzzk.com/cfm/blogger3.cfm?id=1525922220571&author=毛峰。

53 「中國總理李克強訪問日本：中日關係期待破冰」，《BBC 中文》，2018 年 5 月 9 日，https://www.bbc.com/zhongwen/trad/world-44036906。

54 楊明珠，「安倍將訪中，日本財經界逾 500 人隨行」，《中央通訊社》，2018 年 10 月 24 日，https://www.cna.com.tw/news/firstnews/201810240370.aspx。

55 於 2018 年 7 月 1 日，中國已經將海警部隊轉隸武警部隊並且受中央軍委統一指揮，中國海警未來在東海區域的海洋維權與海上執法行動將會更加具有效率。參考：〈全國人民代表大會常務委員會「關於中國海警局行使海上維權執法職權的決定」〉，《新華社》，2018 年 6 月 23 日，http://military.people.com.cn/BIG5/n1/2018/0623/c1011-30078248.html。

組的問題，這局勢發展使得釣魚台問題似乎已經不再是「中」日衝突的唯一因素，在雙方衝突的背景下，其實更隱藏著區域對中共民族主義的興起，以及對中共威脅論的憂心與恐懼。基於雙方威脅感的逐漸擴大，導致「中」日釣魚台爭端之危機感外溢到國際層面，且雙方早在2010年後就開始採取特定的戰略，除了在亞太區域重申領土主權外，各自在國際上也積極擴張政治與經濟影響力。[56]

在2012年的雙方釣魚台爭端達到最高點後，更加速了軍事衝突危機的升高。日本開始強化與美國的傳統戰略安全伙伴關係，積極參與美國主導或周邊與海洋安全的軍事演習。雖然當時美國對釣魚台衝突的立場相當模糊，日本政府仍然持續在亞太區域支持美國歐巴馬政府的亞洲「再平衡戰略」政策，參與介入制衡中共的擴張行為。為了制衡中共的威脅，日本不僅著手於強化其軍事能力，並試圖與亞太國家建立安全合作關係。日本安倍首相更在外交上強調東海與南海在海洋安全的相互依賴性，呼籲東南亞國家要正視且共同維護海洋「自由航行權」。

到了美國川普政府執政之後，日本全力支持美國「印太戰略」，[57]期待以同盟的力量來制衡中共對區域安全的挑戰。於2013年習近平上台後，中共積極推行「一帶一路」倡議與「亞洲基礎設施投資銀行」（簡稱亞投行），試圖以經濟外交的「魅力攻勢」（charm offensive）來同時處理內部產能過剩，並弱化民主國家聯盟的成型等問題。再者，北京亦積極強化東海演習的頻繁度和擴大演習範圍，藉以形成對日本的威懾。

一、日本推動安全合作機制圍堵中共擴張

於2013年，安倍在捷克《報業聯盟》（*Project Syndicate*）發表言論，

---

[56] Christopher J. Hughes, "Japan's Response to China's Rise: Regional Engagement, Global Containment, Dangers of Collision," *International Affairs*, Vol. 58, No. 4, 2009, pp. 837-856.

[57] 於 2017 年底，從美國國務卿提勒森（Rex Tillerson），在華府戰略與國際問題研究中心（CSIS）演說中提出建立「自由且開放的印太區域」的想法和其訪問印度的作為中，可以明白瞭解到，其主要目的是擬構建川普上任以來的「印太聯盟」，並以「印太」（Indo-Pacific）取代「亞太」（Asia-Pacific）的戰略思維，為美國川普政府的新亞洲政策作一定義。

提出要建構一個由日本、美國、澳洲和印度形成一個「亞洲民主安全鑽石」網絡，來包圍中共在海洋方向的擴張行為。[58]安倍在文中指出，儘管中共不時在東海海域進行軍事演習，打算將釣魚台主權「中國化」，但日本絕不會向中共屈服。安倍亦指出，類似情況也發生在南海，使該海域愈來愈像中共的「北京湖」，就像鄂霍次克海變成前蘇聯的內海一樣，南海也可能成為中共內海，南海的深度足以成為中共核潛艦的基地，不久後中共海軍的航空母艦也將頻繁出入該海域。面對中共海洋威脅，安倍強調日本除與印度、澳洲與美國夏威夷連結，從印度洋到西太平洋形成保護廣大海洋權益的「鑽石網」外，也應與英國、馬來西亞、新加坡、紐西蘭和大溪地的法國太平洋海軍合作。[59]

在參考五國防禦協定（Five Power Defense Arrangements, FPDA）之概念上，安倍計畫要推廣建立一個多邊海洋安全制度化的亞洲，不僅要將美國與東南亞國家連結起來，也將邀請英國與法國參與。此外，日本前防衛大臣森本敏卸任後重返學者身分後，對中共的分析更為尖銳。森本指出，中共雖在釣魚台問題上顯得沒有章法，但中共是認真想「奪取」釣魚台，而且也可能發動慣有的「三戰」策略（心理戰、輿論戰及法律戰）以達成目的。[60]在此情況下，日本不能挑釁，但也不能接受挑釁，而且一定要避免軍事衝突，因此獲得美國及區域各國的支持非常重要。

除了戰略想定外，安倍也積極到東協國家進行外交訪問，以尋求能獲得這些區域國家對日本維持海洋規範與自由航行原則的支持。為了說服東協國家，在戰略上，安倍將中共在東海與南海的衝突視為一體，強調中共海洋勢力擴張與海軍部署是全面性的，東南亞國家將無法置身事外。對此，日本不僅將會積極與東協國家強化海洋安全合作，也會積極參與馬來西亞與菲律賓的海軍聯合演習。在海上安全能力改進計畫下，

58 盧素梅，「日制衡陸：六角鑽石安全網已成型」，《中時電子報》，2015 年 06 月 08 日，http://www.chinatimes.com/newspapers/20150608000760-260301。

59 Shinzo Abe, “Asia’s Democratic Security Diamond,” *Project Syndicate*, December 27, 2012, https://www.project-syndicate.org/commentary/a-strategic-alliance-for-japan-and-india-by-shinzo-abe?barrier=true.

60 朱顯龍，「中國『三戰』內涵與戰略建構」，《全球政治評論》，第 23 期（2008 年），頁 29-50。

日本提供官方發展協助給菲律賓岸防部隊。[61]

在2017年底，時任美國國務卿提勒森（Rex Tillerson）提出「印太戰略」的構想，這主張幾乎與日本安倍積極倡導的「民主鑽石聯盟」概念吻合。提勒森用「印太」取代「亞太」一詞，代表美國地緣戰略思維的轉變，顯然是想把印度當作美國新亞洲戰略的重要支點國家。在提勒森的印太地緣戰略思維中，印度是西部支點，日本是東部支點，澳洲是南部支點，美國自然是連結這些戰略支點的領導國家。提勒森認為，只要四國能聯合起來，就有能力牽制中共的擴張方向。然而，這因應中共擴張的印太戰略還正在發展中，日本在這戰略中要如何協力對抗中共的挑戰還需要持續關注。

二、中共對民主國家聯盟的因應作為

對於日本自2012年以來在釣魚台議題上所做出的種種行為，都讓中共直接強烈感受到來自日本威脅。[62]中共對此日方行為不僅要求美國對釣魚台問題要保持中立且勿介入，也同時向韓國與俄國傳達訊息，提醒不要忘記曾經與日本有過領土衝突的歷史記憶。儘管韓國是美國的盟邦，照理應該支持日本，但是韓國卻與中共相同，有著受日本入侵的歷史記憶，加上韓日間存有獨島（或稱竹島）的爭議，中共與韓國於2013年8月同意在歷史議題上共同對抗日本。雖然俄國在釣魚台議題上保持中立，但是在俄日對北方四島仍存爭議，這因此為「中」俄海上合作提供了一個立足點。於2015年5月，「中」俄韓三國在2015年慶祝二戰結束70周年與日本戰敗紀念日時，在歷史議題上更是保持立場一致。雖然「中」俄韓共同參與慶祝二戰結束活動之意涵在於連結日本侵略亞洲的歷史回憶，這雖然不影響日本對釣魚台的控制，這卻強化了「中」日對彼此的負面觀感。[63]

---

[61] Japan Marine United Cooperation, “Maritime Safety Capability Improvement Project,” June 4, 2015. https://www.marubeni.com/news/2015/release/20150604E.pdf.

[62] Jia Xiudong, “Encircling China just Japan’s Wishful Thinking,” *People’s Daily Online*, 17 January 2013, http://china.org.cn/opinion/2013-01/17/content_27715063.htm.

[63] Antoni Slodkowski, “Japan’s Abe backs Putin with visit, in contrast to China, Korea ties,” *Reuters*, February 6, 2014, http://www.reuters.com/article/us-japan-russia-sochi-summit-idUSBREA1603M20140207.

北京到目前為止在區域上還沒有結盟政策，不用像華府那樣需要承擔安全聯盟的責任。在中共受到美國及其盟國圍堵的情況下，與具有戰略重要性的國家進行經濟、外交、軍事等多方位合作仍是需要的，但是這不代表北京會與他國建立正式同盟關係。對於中共這樣一個世界上人口最多，經濟規模世界第二，需要的是發展自身政治、經濟與軍事實力，而不需要去跟其他國家建立同盟來找安全感。出於抗衡美國「亞太再平衡」與「印太戰略」等一系列考慮，中共則積極推動陸海並進的「一帶一路」倡議，一方面在戰略空間上可以實現向西面拓展，另一方面也能滿足中共快速增長的能源進口需求和急迫的海上航道安全。中共刻意在帶路倡議中強調建立區域多邊關係，在全球事務上拉攏俄國，並在政治與經濟等諸多方面試圖打造一個「去美國化」的地區及全球秩序。

面對日本積極拉攏美澳印成立四國聯盟，北京除了以推廣帶路倡議的手段來弱化該聯盟的形成之外，也積極在東海與南海區域舉行軍演，不僅演習規模逐漸擴大，對美日的針對性也愈來愈很明顯。為了回應未被美國邀請參與2018年「環太平洋軍演」，中共因此擴大在沿岸地區的例行演習範圍，例如：於2018年7月16日，中共舉行的「東海海域實際使用武器訓練」實彈軍演，其規模與範圍比近年的東海演習還要廣，此次演習是以持續時間長、區域範圍大和參與兵力眾多著稱，針對釣魚台的意味相當濃厚。[64]此外，為了與美國主導的環太軍演互別苗頭，中共也計畫與東協10國在8月展開聯合海上軍演，以拓展雙方的軍事交流和安全合作。[65]北京近年在東海軍演目的不外乎就是要展示「反介入與區域拒止」的能力，這種「項莊舞劍」式的軍演，向日本傳達捍衛釣魚台的意味明顯，這亦可說是中共對釣魚台爭議採取「鬥而不破」的軍事手段。

三、日本與台灣雙邊關係的強化

面對「中」日間釣魚台爭議，日本與台灣方面互動亦值得一窺究竟。

---

64 呂欣憓，「共軍東海演習武嚇台灣是虛，針對美日安保為實」，《中央通訊社》，2018年7月19日，www.cna.com.tw/news/firstnews/201807190207-1.aspx。

65 莊蕙嘉，「首次電腦兵推後，陸與東協 10 月海上實兵演練」，《聯合新聞網》，2018年8月4日，https://udn.com/news/story/11314/3289758。

雖然台灣也聲稱對釣魚台擁有主權，論調也與中共部分一致，日本為了避免台灣與中共在釣魚台議題上合作，所以決定拉攏台灣。在2013年4月，日本不管當時沖繩漁民的極力反對，決定給予台灣在釣魚台海域附近漁權。於同年4月10日台日雙方在台北賓館簽署「台日漁業協議」，長達十七年的台日重疊專屬經濟海域漁業問題乃獲得妥善安排，台日漁業談判終於達成具體成果。[66]對此，北京當局認為日本違反了在1978年簽訂「『中』日和平友好條約」中的「一個中國」原則，所以對日本當局表達不滿。[67]

該次台日漁業談判之所以有重大進展，筆者認為主要原因有三：第一、美國不希望台日釣魚台之爭影響其重返亞洲的戰略，故急於促成此事。第二、日本外交主軸明顯是要圍堵中共擴張。但近年來，日本與俄國因北方四島爭議而不愉快，與韓國因獨島問題鬧僵，與兩岸因釣魚台問題也關係惡化。安倍政府急於突破此一困局，故決定先拉攏台灣。第三、時任總統馬英九到彭佳嶼宣示釣魚台主權時，一直沒有清楚聲明不與中共聯手，使得日本忐忑不安，覺得若不略施小惠，台灣將會成第二個釣魚台難題。在上述因素壓力之下，日方因此願意迅速與台灣簽訂延宕許久的漁業協議。

---

[66] 台日從 1985 年開始進行漁業談判，談了 17 年沒有結果，2013 年 4 月 10 日的漁業會談是第 17 次的漁業談判，雙方在釣魚台海域漁權爭議上作出讓步，此項協定是一項重大的突破，雙方不再堅持原本各自堅持的台灣「暫定執法線」及日本「中間線」，改採經緯度為基準：（一）台日雙方暫時擱置釣魚台主權爭議，不談該島 12 浬領海海域，只談別區的漁權。（二）台灣漁船過去遭日方驅趕，未來可以進入北緯 27 度以南、日本先島諸島以北之間的海域，漁業作業權益獲得保障，日方不致干擾。也就是說，此項「台日漁業協定」將台灣漁民的海域作業範圍推廣到原來的「暫定執法線」以外，台灣漁民的作業海域增加了 4,530 平方公里或 1,400 平方海里，叫做「協議適用海域」，台日漁民均可自由作業，不受對方公務船的干擾。參考：中華民國外交部亞東太平洋司，「台日漁業協議」，2014 年 4 月 29 日，http://www.mofa.gov.tw/cp.aspx?n=90BEE1D6497E4C58。

[67] Ko Shu-Ling, “Details of New Japan-Taiwan Fisheries Pact Are Explained: Both Sides Win Gains From Row Over Senkakus,” *The Japan Times*, April 23, 2013. http://www.japantimes.co.jp/news/2013/04/23/national/details-of-new-japan-taiwan-fisheries-pact-are-explained/.

陸、結論

「中」日釣魚台主權爭端之背景可說是，一個在崛起中且試圖改變安全現狀的中共，與試圖維持安全現狀的日本，雙方之間因對彼此威脅的恐懼所導致的衝突現象。「中」日釣魚台爭端所以演變的越來越複雜，乃因為目前這領土爭端已經不再是僅僅侷限於「中」日雙邊關係，而且已經牽扯並擴散到周邊國家和區域安全穩定問題，像是美國、俄國、台灣、韓國，與其他東南亞國家。自從美國歐巴馬政府確定重返亞洲之後，日本對於領土爭端問題就開始朝國際多邊主義的方向尋求解決方式，並試圖以這多邊主義來遏止中共單方改變區域安全現狀。目前日本也積極要與美國、澳洲與印度建構一個民主鑽石合作機制，以期能在美國川普政府「印太戰略」的安全考量方面牽制中共的「一帶一路」戰略。

自野田政府把釣魚台收歸國有之後，「中」日在釣魚台周邊海空領域的摩擦，目前已經趨於常態化。對於中共海警或公務船艦與飛機持續巡航釣魚台附近之作為，日方迄今也無計可施，中共事實上已經打破了日本單方控制釣魚台的局面，雙方也都無法預料今後的情勢走向。只要任何一方輕啟戰端，都會有損區域安全與穩定。如同日本軍事專家文谷數重在2017年7月的日本《軍事研究》月刊曾發表一篇文章客觀提及，平息尖閣諸島（釣魚台）爭議的最佳方法就是「維持現狀」，因為「中」日雙方都無法透過軍事武力佔領該群島來解決問題。[68]

此外，「中」日目前在工業技術和經濟領域上的發展仍是有所差距，所以雙方互補作用仍未完全消除。在經貿合作仍是「中」日間優先戰略的前提上，縱使兩國在釣魚台議題上仍然維持不妥協的態度，但這也不過是在應付國內壓力，所以雙方都不至於把釣魚台爭端發展到無法收拾的地步而影響到雙方經貿利益，這因此使得雙方釣魚台衝突得以逐步走向停損點，而這也似乎符合了經濟自由主義學者的觀點。對於釣魚台議題究竟是要衝突還是合作，「中」日對此都陷入了政策上的兩難，所以雙方都試圖將該議題模糊化來處理之。

[68] 文谷数重，「尖閣諸島になんら価値は存在せず」，《軍事研究》 2017 年 7 月号，http://gunken.jp/blog/archives/2017/05/10_0000.php。

總而言之，「中」日若是發生嚴重釣魚台衝突，雙方都未必能占到便宜，目前的狀況也不太可能發生戰爭，最多就是貿易、文化交流中斷以及人民上街抗議。[69]當下也只有在雙邊都有默契願意維持釣魚台現狀，並且在政治上建立互信，才有可能跳脫這釣魚台困境的制約。釣魚台議題發展至今，目前中共所採取各種釣魚台行動背後的主要動力，已經不再是東海石油、天然氣和豐富漁產等天然資源的獲取，而是民族主義、國家尊嚴、海洋戰略，以及企圖重新取回東亞中心地位的霸權渴望。而釣魚台爭端正是此渴望的縮影，因此讓其仍具潛在引爆戰爭的危險性。

[69] 在中日因為釣魚台發生糾紛時，中國就擬以限制稀土輸出來制衡日本，因為工業大國日本的絕大部份稀土是來自中國，可是後來世界貿易組織居然判定中國的限制稀土輸出是違反「內外無差別」的國際原則，等於是對中國的外交手段一個嚴重打擊。

參考書目

一、官方聲明及文書

〈全國人民代表大會常務委員會『關於中國海警局行使海上維權執法職權的決定』〉，《新華社》，2018 年 6 月 23 日，http://military.people.com.cn/BIG5/n1/2018/0623/c1011-30078248.html。

中國國務院，〈釣魚島是中國的固有領土〉，2012 年 9 月 25 日，http://www.scio.gov.cn/zxbd/tt/Document/1222670/1222670.htm。

中華民國外交部，《台日漁業協議》，2014 年 4 月 29 日，http://www.mofa.gov.tw/cp.aspx?n=90BEE1D6497E4C58。

日本外務省，《關於尖閣諸島的基本見解》，2012 年 11 月，https://www.mofa.go.jp/region/asia-paci/china/pdfs/r-relations_cn.pdf。

日本外務省，「有關尖閣諸島的問與答」之第十四問，https://www.hk.emb-japan.go.jp/chi/territory/senkaku/question-and-answer.html#q14。

日本海上保安廳，「尖閣諸島周辺海域における中国公船等の動向と我が国の対処」，http://www.kaiho.mlit.go.jp/mission/senkaku/senkaku.html。

Abe, Shinzo, “Asia’s Democratic Security Diamond,” *Project Syndicate*, December 27, 2012, https://www.project-syndicate.org/commentary/a-strategic-alliance-for-japan-and-india-by-shinzo-abe?barrier=true.

Japan Marine United Cooperation, “Maritime Safety Capability Improvement Project,” June 4, 2015, https://www.marubeni.com/news/2015/release/20150604E.pdf.

Ministry of Defense of Japan, *Defense of Japan 2011*, http://www.mod.go.jp/e/publ/w_paper/2011.html.

Office of Policy Planning and Coordination on Territory and Sovereignty of Japan, *Recommendations of the Advisory Panel on Communications Concerning Territorial Integrity* https://www.cas.go.jp/jp/ryodo_eg/torikumi/ryodoshitsu/ryodoshitsu-adp-03.html.

UN Treaty Collections, “Agreement between Japan and the United States of America Concerning the Ryukyu Islands and the Daito Islands,” https://treaties.un.org/doc/publication/unts/volume%20841/volume-841-i-12037-english.pdf.

二、期刊論文

Deans, Phil, “Contending Nationalisms and the Diaoyutai/Senkaku Dispute,” *Security Dialogue*, Vol. 31, No. 1, 2000, pp. 119-131.

Downs, Erica S. and Saunders, Phillip C., "Legitimacy and the Limits of Nationalism: China and the Diaoyu Islands," *International Security*, Vol. 23, No. 3, 1999, pp.114-146.

Drifte, Reinhard, "Japanese-Chinese Territorial Disputes in the East China Sea between Military Confrontation and Economic Cooperation," Asia Research Centre Working Paper (2008), *Asia Research Centre of London School of Economics and Political Science*, http://eprints.lse.ac.uk/20881/1/Japanese-Chinese_territorial_disputes_in_the_East_China_Sea_(LSERO).pdf.

He, Yinan, "History, Chinese Nationalism and the emerging Sino-Japanese Conflict," *Journal of Contemporary China*, Vol. 16, No. 50, 2007, pp. 1-24.

Hughes, Christopher J., "Japan's Response to China's Rise: Regional Engagement, Global Containment, Dangers of Collision," *International Affairs*, Vol. 58, No. 4, 2009, pp. 837-856.

Herz, John H., "Idealist Internationalism and the Security Dilemma," *World Politics*, Vol. 2, No. 2, January 1950, pp. 157-180.

Jervis, Robert, "Cooperation under the Security Dilemma," *World Politics*, Vol. 30, No. 2, January 1978, pp. 167–214.

Koo, Min Gyo, "The Senkaku/Diaoyu Dispute and Sino-Japanese Political-Economic Relations: Cold Political and Hot Economics?" *The Pacific Review*, Vol. 22, No. 2, 2009, pp. 205-232.

Ozaki, Shigeyoshi, "Territorial Issues on the East China Sea: A Japanese Position," *Journal of East Asia & International Law*, Vol. 3, No. 1, 2010, pp. 151-174.

Pan, Zhongqi, "Sino-Japanese Dispute over the Diaoyu/Senkaku Islands: The Pending Controversy from the Chinese Perspective," *Journal of Chinese Political Science*, Vol. 12, No. 1, 2007, pp, 71-92.

Reilly, James, "Remember History, not Hatred: Collective Remembrance of China's War of Resistance to Japan," *Modern Asian Studies*, Vol. 45, No. 2, 2011, pp. 463-490.

Sasaki, Tomonori, "China Eyes the Japanese Military: China's Threat Perception of Japan since the 1980s'," *The China Quarterly*, No. 203, 2010, pp. 560-580.

Smith, Paul J., "The Senkaku/Diaoyu Island Controversy: A Crisis Postponed," *Naval War College Review*, Vol. 66, No. 2, 2013, pp. 31-48.

Suzuki, Shogo, "The Importance of 'Othering' in China's National Identity: Sino-Japanese Relations as a Stage of Identity Conflicts," *The Pacific Review*, Vol. 20, No. 1, 2007, pp. 23-47.

Takahashi, Toshiya, “Japan’s 2013 defense white paper stirs tensions with China,” *East Asia Forum*, July 31, 2013, http://www.eastasiaforum.org/2013/07/31/japans-2013-defence-white-paper-stirs-tensions-with-china/#more-36915.

Wang, Zheng, “The Chinese Dream: Concept and Context,” *Journal of Chinese Political Science*, Vol. 19, No. 1, 2014, pp. 1-13.

文谷數重，「尖閣諸島になんら価値は存在せず」，《軍事研究》，7 月號（2017 年），http://gunken.jp/blog/archives/2017/05/10_0000.php。

王尊彥，「尖閣／釣魚台争議を中心とした第二次安倍政権下の日中関係」，《問題と研究》，第 42 卷第 4 號（2013 年 12 月 30 日），頁 107-144。

石原忠浩，「『政治主導』的對外政策？─日本民主黨執政下的日『中』關係」，《展望與探索》，第 10 卷第 7 期（2012 年 7 月），頁 42-58。

朱顯龍，「中國『三戰』內涵與戰略建構」，《全球政治評論》，第 23 期（2008 年），頁 29-50。

林泉忠，「釣魚台列嶼爭議一百二十年」，《明報月刊》， 3 月號（2015 年），https://www.mofa.gov.tw/Upload/RelFile/642/152410/釣魚臺列嶼爭議的形成過程.pdf。

林正義、陳鴻鈞，「兩個『中國』在東海的油氣勘探與美日的角色」，《遠景基金會季刊》，第 15 卷第 4 期（2014 年 10 月），頁 1-59。

畠山京子，「中日爭奪亞洲區域領導地位之靜默對抗」，《歐亞研究》，第 2 期（2018 年 1 月），頁 105-112。

蘇俊斌，「諸國崛起後的日本對中政策」，《台灣國際研究季刊》，第 8 卷第 2 期（2012 年夏季號），頁 18-19。

三、專書及專書篇章

Kokubun, Ryosei, “Changing Japanese Strategic Thinking toward China,” in Rozmsn, Gilbert, Togo, Kazuhiko, and Ferguson, Joseph P., ed(s)., *Japanese Strategic Thought toward Asia* (London: Palgrave Macmillan, 2007), pp. 137-158.

Samuels, Richard J., *Securing Japan: Tokyo’s Grand Strategy and the Future of East Asia* (Ithaca: Cornell University, 2007), pp. 120-127.

Suganuma, Unryu, *Sovereign Rights and Territorial Space in Sino-Japanese Relations: Irredentism and the Diaoyu/Senkaku Islands* (Honolulu: Association for Asian Studiesand University of Hawaii Press, 2000).

Takamine, Tsukasa, *Japan’s Development Aid to China: The Long-Running Foreign Policy of Engagement* (London: Routledge, 2006).

四、新聞資料

"Beijing Mixes Messages over Anti-Japan Protest," *The New York Times*, September 16, 2012, http://www.nytimes.com/2012/09/17/world/asia/anti-japanese-protests-over-disputed-islands-continue-in-china.html?partner=rss&emc=rss&smid=tw-nytimes&_r=0

"Chinese Ambassador Urges Japan to Learn from Germany over Wartime History," *Global Times*, January 15, 2014, http://english.jschina.com.cn/20322/201402/t1400612.shtml

"Details of New Japan-Taiwan Fisheries Pact Are Explained: Both Sides Win Gains From Row Over Senkakus," *The Japan Times,* April 23, 2013, http://www.japantimes.co.jp/news/2013/04/23/national/details-of-new-japan-taiwan-fisheries-pact-are-explained/

"Encircling China just Japan's Wishful Thinking," *People's Daily Online*, January 17, 2013, http://china.org.cn/opinion/2013-01/17/content_27715063.htm

"Japan's Abe backs Putin with visit, in contrast to China, Korea ties," *Reuters*, February 6, 2014, http://www.reuters.com/article/us-japan-russia-sochi-summit-idUSBREA160320140207

"Japan scrambles jets over China drone flight near disputed islets," *Reuters*, May 18, 2017, https://www.reuters.com/article/us-japan-china-drone-idUSKCN18E1Q9

"Latest China-Japan Spat: Who's Voldemort?" *The New York Times*, January 9, 2014, http://sinosphere.blogs.nytimes.com/2014/01/09/latest-china-japan-spat-whos-voldemort/?_r=0

"Shinzo Abe Says Japan Is China's 'Partner,' and No Longer Its Aid Donor," *The New York Times*, October 26, 2018, https://www.nytimes.com/2018/10/26/world/asia/shinzo- abe -china-japan.html?ga=2.68125393.1744460237.1541647946-68342518.1527481371

〈中國總理李克強訪問日本：中日關係期待破冰〉，《BBC 中文網》，2018 年 5 月 9 日，https://www.bbc.com/zhongwen/trad/world-44036906。

〈日本教科書審定制度〉，《人民網》，2001 年 4 月 4 日，http://www.people.com.cn/BIG5/guoji/20010404/432568.html。

〈日相促修憲法『放棄戰爭』條款〉，《自由時報》，2016 年 11 月 2 日，http://news.ltn.com.tw/news/focus/paper/100220。

〈日內閣會議確認釣魚台國有化〉，《大紀元》，2012 年 9 月 10 日，http://www.epochtimes.com/b5/12/9/10/n3679216.htm。

〈日中島嶼之爭，安倍稱不許以實力改現狀〉，《BBC 中文網》，2013 年 7 月 12 日，https://www.bbc.com/zhongwen/trad/world/2013/07/130712_japan_abe_sea。

〈日美安全保障條約第 5 條是什麼？〉，《日本經濟新聞》，2017 年 2 月 4 日，https://zh.cn.nikkei.com/politicsaeconomy/politicsasociety/23552-2017-02-04-11-08-41.html。

〈日制衡陸：六角鑽石安全網已成型〉，《中時電子報》，2015 年 06 月 08 日，http://www.chinatimes.com/newspapers/20150608000760-260301。

〈共軍東海演習武嚇台灣是虛，針對美日安保為實〉，《中央通訊社》，2018 年 7 月 19 日， www.cna.com.tw/news/firstnews/201807190207-1.aspx。

〈安倍將訪中，日本財經界逾 500 人隨行〉，《中央通訊社》，2018 年 10 月 24 日，https://www.cna.com.tw/news/firstnews/201810240370.aspx。

〈李克強會晤安倍敲定中日海空聯絡機制〉，《亞州週刊》，第 32 卷 19 期，2018 年 5 月 20 日，https://www.yzzk.com/cfm/blogger3.cfm?id=1525922220571&author=毛峰。

〈首次電腦兵推後，陸與東協 10 月海上實兵演練〉，《聯合新聞網》，2018 年 8 月 4 日， https://udn.com/news/story/11314/3289758。

〈釣魚島衝突，日拘留陸船長 10 天〉，《中國時報》，2010 年 9 月 11 日。

〈『國有化』5 年後的東海與中日〉，《日經中文網》，2017 年 9 月 12 日，https://zh.cn.nikkei.com/politicsaeconomy/politicsasociety/26955-2017-09-12-04-51-10.html。

〈習近平領軍設指導小組捍海權〉，《旺報》，2013 年 2 月 5 日，https://tw.news.yahoo.com/習近平領軍-設指導小組捍海權-213000898.html。

〈歷年保釣事件記載〉，《中國社會科學網》，2008 年 6 月 16 日，http://jds.cass.cn/ztyj/tgas/201605/t20160506_3326567.shtml

中華民國南沙主權論述的再檢視

黃宗鼎

國防安全研究中共政軍研究所 助理研究員

摘　要

長期以來，有關南沙之主權衝突常流於政治論述或文本之爭，其一定程度反映了爭端國在聲索主權之初，動輒「先射箭、後畫靶」，即言「先提主張、後覓事證」之通病。本文透過檢視「南沙群島」之「名」，釐清了中華民國於該群島主權論述之「實」，進而揭示我國於「南沙群島」聲索之利基。

本研究發現，在「南沙群島」中扣除「團沙」部分，其他絕大多數之海域島嶼地區，乃係二戰後中華民國政府自日領之「新南群島」接收而來；加以「南沙群島」之名，乃至於可被視為「U 形線」（九段線）之母的「八段線」，一直要到 1946 年 9 月內政部提出「南海諸島位置略圖」才正式出現，可知中華民國於「南沙群島」之有力或有利聲索，蓋以二戰結束伊始為起點。

關鍵詞：南沙群島、南海、新南群島、斯普拉利島群、團沙

A Re-examination of the Arguments of the Republic of China's Sovereignty Claim on the Nansha Islands

Chung-Ting Huang

Assistant Research Fellow,
Division of Chinese Politics and Military Affairs,
Institute for National Defense and Security Research

Abstract

The purpose of this article is to distinguish between the facts and arguments associated with the Republic of China's (ROC) sovereignty claim on the Nansha Islands. The author finds that most of the territories of the Nansha Islands were in fact the same territories of Shinnan Gunto controlled by the Japanese government before the end of the World War II (WWII). The territories of Shinnan Gunto were transferred to the ROC from the Japanese government by the end of the WWII. The name of "Nansha Islands", as well as the "Eight-Dash line," which can be regarded as the origin of the "Nine-Dash line," only officially appeared for the first time when the ROC Ministry of the Interior released a "Map of the Islands in the South China Sea" in September 1946. This article thus argues that the ROC official, public sovereignty claim on the Nansha Islands started after the end of WWII.

Keywords：*Nansha Islands, South China Sea, Shinna Gunto, Spratly Islands, twan-sha*

壹、前言

2013 年 1 月 22 日，菲律賓就「中」菲有關南海海洋管轄權的爭端提起強制仲裁。菲國藉由《聯合國海洋法公約》（以下簡稱《公約》）提出新說，盼能破解中共南海「九段線」之主張:首先，由於《公約》對有權產生領海或專屬經濟區之地物有明確規定，包括要求天然地物須符合漲潮時在水面以上，或得維持人類居住或經濟生活等條件，故不利於在南沙僅擁有 5 個低潮高地與 3 個岩塊的中共。其次，菲國盼其專屬經濟區之主張能獲得仲裁庭肯認，進而使中共於此範圍內無法提出任何「歷史權利」。[1]

所謂「歷史權利」，意指國家並非係以一般國際法規則來取得對特定土地或海洋區之權利，而這些權利係國家在歷史發展過程中所取得。[2]中共蓋以「九段線」主張其於南海之「歷史權利」，惟 2016 年 7 月 12 日公布的南海仲裁《判斷》，已明白否定了「歷史權利」說及「九段線」論述。仲裁庭認定，沒有證據顯示中共曾在《公約》存在以前，對南海水域的生物及非生物性資源建立專屬使用的「歷史權利」；無論如何，任何基於「九段線」主張的「歷史權利」，也會因為《公約》專屬經濟區制度的創設、中共加入《公約》，以及《公約》生效，而歸於消滅。[3]

就中華民國外交部現行之《南海主權說帖》來看，南沙群島同西沙群島、中沙群島、東沙群島及各群島周遭海域，無論就歷史、地理及國際法而言，均屬中華民國固有領土及海域。然而，在南海仲裁《判斷》否定「九段線」效力，並解構「歷史權利」做為南海主權論述基礎的同

[1] 海頓（Hayton, Bill），《南海 ： 21 世紀的亞洲火藥庫與中國稱霸的第一步?》（臺北市：麥田出版，2015），頁 170-172、175；”SC justice says China's claim ‘a gigant ic historical fraud’,” GMA News June 9, 2014, http://www.gmanetwork.com/news/st ory/364910/news/nation/sc-justice-says-china-s-claim-a-gigantic-historical-fraud Access ed on 2015/7/7。

[2] *Encyclopedia of Public International Law, Instalment 7: History of International Law — Foundations and Principles of International Law — Sources of International Law — Law of Treaties* (Amsterdam: North Holland Publishing Cie., 1984), p.120.

[3] The South China Sea Arbitration Award of 12 July 2016, para 262; 631.

時，也使得我國於「南沙群島」之聲索權利遭到一定程度之挑戰。

長期以來，有關南沙之主權衝突常流於政治論述或文本之爭，其一定程度反映了爭端國在聲索主權之初，動輒「先射箭、後畫靶」，即言「先提主張、後覓事證」之通病。爭端國在尋覓事證，強化論據之際，仍可能在確立聲索內涵，仍可能要修正主張，俾縮小事證與主張間的差異。無論是中華民國政府、越南政府，還是菲律賓政府，在建構各自對「南沙群島」／「長沙群島」／「卡拉揚群島」主權論述的伊始，舉凡標的物之命名、標的物所涉之範疇，乃至於領有標的物之理由（中/越主張固有領土說，菲國主張鄰近性與「發現」說），既為舉證之所在，亦是爭端之所在。

就在諸如 Spratly Islands、Spratly and other islands、「新南群島」、「團沙群島」、「南沙群島」、Spratly or Storm Island、Spratly Group of Islands、Spratly `group、Spratly Island Group、Kalayaan Islands（卡拉揚群島）、Spratly archipelago 、Kalayaan Island Group（卡拉揚島群），以及 Truong Sa（長沙）等互有牽涉之稱謂陸續登場之間，主權論述愈成各說各話之勢。

筆者係從「歷史研究途徑」作論，並以中華民國外交部檔案作為分析文本。本文擬梳理「南沙群島」相關之「名」，藉以檢視中華民國於該群島主權論述之「實」，進而揭示我國於「南沙群島」聲索之利基。

貳、成為「南沙群島」以前：「新南群島」與「斯普拉利島群」之間的關聯

1928 年，「中央政治會議」廣州分會命中山大學農林科教授沈鵬飛一行赴西沙群島進行調查。沈氏返回後撰寫之「調查西沙群島報告書」中兩處明白指出，西沙為中國最南之領土。換言之，在 1928 年時，中國官方並不將「斯普拉利島群」（Spratly Islands）視為其領土。不過到了 1946 年時，廣東省官方卻又在給外交部的電文中指出，志書謂「團

沙群島」為中國最南海界。[4]（附圖一）

鑒此，相關問題隨之產生：究竟「南沙群島」係在何種情況下取代「團沙群島」而成為中國之最南海界？倘若「南沙群島」與「團沙群島」範疇有別，中國政府又是如何將「南沙群島」納入版圖?欲探究該等疑問，吾人勢須釐清「南沙群島」之前身——「新南群島」，與「斯普拉利島群」、「團沙群島」之關聯。

在 16 世紀歐洲航海家認識南沙所涉地區之前，在該區活動的漁民大抵是中國人、馬來人及安南人。而最早對南沙地區聲索主權之國家實可謂英國。據英國外交檔案所示，英國海軍於 1864 年調查了該區的兩個島嶼，名之曰 *Spratly*（Spratley）及 *Amboina*，前者係以英籍捕鯨船長 Richard Spratly 來命名。1877 年，英軍復於該等島嶼升旗，嗣以「斯普拉利島群」（Spratlys）稱呼該區諸島。[5]

20 世紀後，法人又成主要之歐洲訪客。1930 年 4 月，法艦訪查了「斯普拉利島群」。1933 年 4 月，再於部分島嶼豎立法旗。同年 7 月 25

[4] 按許文堂教授所言:「此某種程度說明廣州官方與知識界尚且不存在今日所謂南沙群島為中國最南領土之認知。即令知道南沙島，也只是今日所謂之中沙群島，因為直到 1947 年才將南沙群島改稱為中沙群島。」許文堂，〈南沙與西沙---他者的觀點〉，「七○年代東亞風雲—臺灣與琉球、釣魚台、南海諸島的歸屬問題」學術研討會（臺北：台大社會科學院國際會議廳，2013 年 10 月 27 日），頁 17、21；〈美 35 字第 13916 號（1946/10/31）〉，中央研究院近代史研究所檔案館藏，《外交部檔案》，館藏號：019.3/0012，「南沙群島」；Marwyn S, Samuels, *Contest for the South China Sea*, New York : Methuen, 1982, p.68. 又按圖一 （1930 年代中華民國堤沙淺洲群島，Tizard Bank and Reefs）所示，「堤沙淺洲」音近「團沙」而兩者英文同為 Tizard，故應為同地異名。又按〈島礁資料庫 —— 近代歷史上我國政府為南海諸島命名的情況〉一文所示，1935 年 1 月出版的《水陸地圖審查委員會會刊》第一期，首次將南海諸島分成四部分：東沙島（今東沙群島）、西沙群島、南沙群島（今中沙群島）和團沙群島（今之南沙群島），http://www.nansha.org.cn/islandsdatabase/4/South_China_Sea_Islands_Names.html。

[5] 1956 年，英外交部以 1951 年英海軍發現太平島（Itu Aba）上已有許多中文印記，以及英方超過 20 年不曾行使主權於「斯普拉利島群」等事由，而自認難以主張對該群島擁有主權。Sovereignty of Off-Shore Islands of China, 1956, FO371/1209371, *Foreign Office Files: China, 1949-1976*. Electronic Databases, Academia Sinica; Spratly and Other Islands（Shinnan Gunto）, May 29, 1944, Reel 15, *Confidential U.S. State Department Special Files. Southeast Asia, 1944-1958* [microform] / [edited by Gregory Murphy], Bethesda, MD.: University Publications of America, 1989.

日，法人正式宣告兼併包括 Spratly、d'Amboine 在內等九小島暨相關沙坍（參見附圖 2）。對於法方舉措，日政府旋即提出嚴重抗議，以其人員早在 1921 年便為開採磷礦，而佔領該群島，且在 1929、1933 至 1938 年間，持續派遣海洋研究船於當地活動。據日本報紙宣傳謂，1922 年時，農學博士福島在臺灣與馬來半島間之無人島曾載鳥糞二千噸歸日，並將之定名曰「新南群島」。迨 1939 年 2 月 27 日，巴黎乃建議將法日爭端送交海牙常設法院予以仲裁。日本於 3 月 31 日加以拒絕，同時宣告正式將該區兼併為「新南群島」，而法國在 4 月 5 日拒絕承認該項兼併。[6]

究竟法佔小島與「新南群島」有何交集？據相關地圖所示，法佔範圍係在北緯 11 度 29 分至 7 度 52 分，東經 114 度 25 分至 111 度 55 分；至於「新南群島」之範圍，則環繞於北緯 12 度東經 117 度、北緯 9 度 30 分東經 117 度、北緯 8 度東經 116 度、北緯 7 度東經 114 度、北緯 7 度東經 111 度 30 分、北緯 9 度東經 111 度 30 分，北緯 12 度東經 114 度之間（參見附圖 4）。按美方估計，法佔島嶼牽涉之海域僅日人所置「新南群島」所跨海域之三分之一，但法佔海域囊括了絕大多數之島嶼（參見附圖 3）。值得注意的是，在 1933 年法國公告其兼併行動之同日，中國政府雖即時透過駐巴黎公使向法方提出抗議，惟就當時美國駐南京大使館來看，中國對於「斯普拉利島群」的主權主張可謂薄弱，因為「中國官方教課書所述及中國水域之南界，係延伸至西沙群島下方，乃至於本爭議地區的北方。」[7]足見 1928 年「調查西沙群島報告書」有關西沙

[6]〈美 35 字第 13916 號（1946/10/31）〉，中央研究院近代史研究所檔案館藏，《外交部檔案》，館藏號：019.3/0012，「南沙群島」；Catley, Bob and Keliat, Makmur, Spratlys: *The Dispute in the South China Sea* (Aldershot and Brookfield: Ashgate, 1997), p.25; Sovereignty of off-shore Islands of China, 1956, FO371/1209371, *Foreign Office Files: China,* 1949-*1976*. Electronic Databases, Academia Sinica; Spratly and Other Islands (Shinnan Gunto), May 29, 1944, Reel 15, *Confidential U.S. State Department Special Files. Southeast Asia, 1944-1958* [microform] / [edited by Gregory Murphy], Bethesda, MD. : University Publications of America, 1989; To SEA from PI, Jan. 31, 1947, Reel 16, *Confidential U.S. State Department special files. Southeast Asia, 1944-1958* [microform] / [edited by Gregory Murphy], Bethesda, MD.: University Publications of America, 1989.

[7] 1939 年 5 月 17 日，美國務卿向日大使表示美國政府不認為日本所兼併的既有東方又有東南方走向的島嶼，可以視為一個島群，亦不認為日本該項措施可被視為具有國際效力之行為。〈美 35 字第 13916 號（1946/10/31）〉，中央研究院近代史研究所檔案館藏，《外交部檔案》，館藏號：019.3/0012，「南沙群島」； Bob Catley and

群島為中國最南海界之說殆非孤證。

至少在日本投降之前兩年，美國國務院即已針對「新南群島」（Shinnan Gunto）之歸屬問題展開討論。就該等資料所示，「新南群島」實等同於「斯普拉利島群」，即使以經緯度所圈範疇來看，「斯普拉利島群」與「新南群島」亦相重合。美國國務院主要透過下列文件來闡述「新南群島」之聲索問題，其分別為 1943 年 5 月 25 日提出之 T-324、1944 年 5 月 29 日提出之 H-68a，以及 1944 年 12 月 19 日提出之 CAC-301 等三份文件。這些文件除了以「斯普拉利島群」（Spratlys）來指涉「新南群島」，亦使用了「斯普拉利與其他島嶼」（Spratly and other islands）（圖三）來作為「新南群島」的同義詞。

美方據以認為，在日本因《開羅宣言》而再難保有「新南群島」的情況下，由於法國是第一個正式對「斯普拉利島群」部分島嶼進行兼併之國家，加以被認為具有持續性之佔領，故較其他國家更能提出有力的主權主張。至於中國，美方指出該區距離中國本土過於遙遠，其立論基礎仍然只能建立在中國船隻或人民多年來以捕魚或貿易為目的而前往該區等事實之上。不過該評論亦稱，一旦中國在未來成為強權，擁有大量海軍或被國際安全機制賦予一定之區域責任時，將會較有主張主權之優勢。此外，1944 年時菲政府雖未對「新南群島」提出任何正式之主權主張，但部分菲人領袖基於鄰近（propinquity）原則而對該群島感到興趣。儘管菲律賓在美國國務院之討論中被美方視為得在日後領有「新南群島」的一個可能對象，但此純係基於日本威脅之考量，該等文件皆強調「新南群島」確定不在 1898 年 12 月 10 日《美西條約》所規範的菲國疆界之內；再就船運量過小及缺乏屬島管理經驗等面向

Makmur Keliat, *Spratlys: The Dispute in the South China Sea* (Aldershot and Brookfield: Ashgate, 1997), p.25; Sovereignty of off-shore Islands of China, 1956, FO371/1209371, *Foreign Office Files: China, 1949-1976*. Electronic Databases, Academia Sinica; Spratly and Other Islands (Shinnan Gunto), May 29, 1944, Reel 15, *Confidential U.S. State Department special files. Southeast Asia, 1944-1958* [microform] / [edited by Gregory Murphy], Bethesda, MD. : University Publications of America, 1989; To SEA from PI, January 31, 1947, Reel 16, *Confidential U.S. State Department special files. Southeast Asia, 1944-1958* [microform] / [edited by Gregory Murphy], Bethesda, MD.: University Publications of America, 1989。

而言，美方認為菲國更難主張該區權利。[8]

綜言之，「斯普拉利島群」與「新南群島」就位置來說並無二致；另就戰後「新南群島」可能之歸屬而言，美方顯認法國之聲索能力較強。

參、納版成為「南沙群島」:「新南群島」與「團沙群島」之間的關聯

以「新南群島」戰後之接收問題而言，蓋涉及英、法、美、菲等盟國。按 1971 年外交部〈南沙群島說帖〉之認知，中華民國政府於 1946 年 11 月間係以臺灣「高雄州」之一部接收「新南群島」，惟又有資料指出該地之日軍似已於 1946 年 8 月向「東南亞戰區」之英軍投降，[9]或有言美軍艦艇早在 1945 年 11 月便已登陸太平島（Itu Aba）。[10]

除了接收代表及接收時間，接收內涵亦成問題。中國在接收「新南群島」前夕（至少是在 1946 年 9 月以前）仍不清楚該群島與「團沙群島」、「南沙島」（即日後之「中沙群島」）之關係，[11]即令行政院在 1946 年 7 月初已核議將「團沙」、「南沙」與海南島、東沙、西沙等群島置諸擬成立之「海南行政長官公署」治下。[12]

---

[8] Kimie Hara, *Cold War Frontiers in the Asia-Pacific : Divided Territories in the San Francisco System*, London ; New York : Routledge, 2007, pp.146-147; Spratly and Other Islands (Shinnan Gunto), May 29, 1944, Reel 15, *Confidential U.S. State Department Special Files. Southeast Asia, 1944-1958* [microform] / [edited by Gregory Murphy], Bethesda, MD.: University Publications of America, 1989.

[9] 許文堂，〈南沙與西沙---他者的觀點〉，頁 23；〈南沙群島專案小組第一次會議紀錄〉，中央研究院近代史研究所檔案館藏，《外交部檔案》，檔號：019.3/89016，「南沙群島中菲卷」。

[10] 《海軍巡弋南沙海疆經過》，（臺北市：臺灣學生書局，1975 ），頁 14。

[11] 1946 年 7 月 20 日，中國駐菲總領事段茂瀾電報南京外交部，稱其奉查新南群島是否係南沙群島一事，雖經探詢美海軍司令等單位，均毫無所悉。24 日，《中央日報》報導馬尼剌 23 日聯合社有關菲與我作團沙島主權爭議之電訊，外交部美洲司長程希孟在該份新聞之簡報上旁注了「似係西沙群島」一語。〈駐馬尼剌段茂瀾第 22 號電（1946/7/20）〉；〈民國 35 年 7 月 24 日中央日報簡報〉，中央研究院近代史研究所檔案館藏，《外交部檔案》，館藏號：019.3/0012，「南沙群島」。

[12] 〈內政部致行政院秘書處函稿（1946/7/9）〉，國家檔案局藏，《內政部檔案》，檔號：A301000000A/0035/E41502/1，「進駐西南沙群島案」。

1946 年 7 月 25 日，外交部據外電報導有關中菲兩國爭領「新南群島」或「團沙群島」（Tizard Bank）之消息，乃產生「該二群島是否同地別稱?」「我方已否接收迄未獲悉」等疑問，繼電請駐菲總領事館調查無果之餘，復函電廣東省政府、臺灣行政長官公署，以及駐河內總領事館密查據報。[13]8 月 4-5 日，又以《字林西報》稱中菲所爭議之島係 *Spratley*，再電前述單位詢問該島是否有別於「新南群島」或「團沙群島」，而究係指何島？[14]

1946 年 8 月 12 日，駐馬尼剌（拉）總領館電外交部表示，關於「新南群島」是否即「團沙群島」，經向美、菲多方查詢，均無所知，但 *Spratly* 似非菲方所訴求者。[15]13 日，外交部收到海軍總司令部之回覆，指出「團沙群島」（Tizard Bank）似為「新南群島」之一部，*Spratley* 為英美海圖用名，又稱「風暴島」（Storm Island），即日圖所稱之「西鳥島」。[16]24 日，外交部再收到駐臺灣行政長官公署復電，該電指出，「新南群島」在商務印書館出版之地圖載為「團沙群島」，乃我「西沙群島」之一部，據外交部比對，「團沙群島」內含之島礁與海總電文所示相同者，僅為三角島（Thi Thu I.）、中小島（Loaita I. or South I.）、長島（Itu Aba I.）、西鳥島（Spratry I.）。[17]（詳見表一、新南（南沙）群島意指表）

1946 年 9 月初，外交部顯已決定採納前述臺灣行政長官公署就「新南群島」範圍提供之界說，即視「新南群島」、「團沙群島」乃同地而兩名，盼據以加緊完成接收。該月 11 日，行政院訓令外交部會商內政、國防兩部妥為應付，並協助廣東省政府進行接收「東沙、西沙、南沙、

---

[13]〈外交部稿（1946/7/25）〉，中央研究院近代史研究所檔案館藏，《外交部檔案》，館藏號：019.3/0012，「南沙群島」。

[14] 〈外交部稿（1946/7/31）〉;〈美 35 字第 04840 號（1946/8/5）〉，中央研究院近代史研究所檔案館藏，《外交部檔案》，館藏號：019.3/0012，「南沙群島」。

[15]〈外交部收電第 5473 號（1946/8/12）〉，中央研究院近代史研究所檔案館藏，《外交部檔案》，館藏號：019.3/0012，「南沙群島」。

[16] 〈海京發字 9258（1946/8）〉，中央研究院近代史研究所檔案館藏，《外交部檔案》，館藏號：019.3/0012，「南沙群島」。

[17] 關於新南群島原屬西沙群島一部之說，外交部簽注意見認為所謂西沙係為南沙之誤。〈未篠署民(一)字第 16909 號(1946/8/17)〉;〈總收文字第 9614 號(1946/8/24)〉，中央研究院近代史研究所檔案館藏，《外交部檔案》，館藏號：019.3/0012，「南沙群島」。

團沙等群島」。[18]13 日，相關部會召開「團沙群島專案會議」，決議由國防部協助廣東省從速接收「團沙群島」，並強調目前不必向各國提出群島之主權問題，有關資料送外交部以備交涉。但此時當局對於「團沙群島」之認知仍屬有限，是故決議中對於「團沙群島」之地理位置與接收之地理範圍，乃有另由內政部擬定之模糊表示。[19]1946 年 9 月 25 日，內政、外交與國防三部奉政院令召開「協助接收南海諸島案會議」，內政部乃提出「南海諸島位置略圖」（參見附圖 5）及「南海諸島譯名表」，會中並對譯名表加以修正。前述略圖可謂南海最早之「八段線」圖，此外，據該等圖表所示，內政部係將「新南群島」更名為「南沙群島」，並偏向將早先海總對「新南群島」所調查之結果，作為官方正式之立場，即言以「團沙群島」為「南沙群島」之一部，惟該「團沙群島」（Twan-Sha Chiin-Tao）之概念與海總所稱之「團沙群島」（Tizard Bank）顯有不同。

據 10 月 9 日內政部呈院之〈南沙群島概況〉所示，「團沙島」為南海四群島下「南沙群島」之中最大一群之島礁，內含雙子島（North Danger）、帝都島（Thi Thu）、賴他島（Loaita I.）、長島（Itu Aba）、北小島（Sand Cay）、南小島（ Nam Yit I. ）、斯普拉利島（Spratly I.）、安波那島（Amboyna Cay）。（惟海總所謂之「團沙群島」不含帝都島（Thi Thu）、賴他島（Loaita I.）等島嶼）[20]10 月 31 日，廣東省方面之調查方電至外交部，該電亦呼應了臺灣行政長官公署之論點，其指出：綜合日書《南支那五省之現勢》及陳清展所著《海南島與太平洋》之內容研判，認為「新南群島」與「團沙群島」實係同地兩名。[21]（詳見表一、新南（南沙）群島意指表）惟此時當局似不擬將「團沙群島」與「新南群島」

[18] 〈節京陸字第 10858 號（1946/9）〉，中央研究院近代史研究所檔案館藏，《外交部檔案》，館藏號：019.3/0012，「南沙群島」。

[19]〈關於團沙群島（即新南群島）案會議記錄（1946/9/13）〉；〈美 35 字第 07834 號（1946/9/20）〉；〈致酉虞署民字第 30598 號（1946/10）〉，中央研究院近代史研究所檔案館藏，《外交部檔案》，館藏號：019.3/0012，「南沙群島」。

[20] 〈為奉令籌商協助接收南海諸島一案抄附呈說原文等件並請查照由（1946/10/9）〉；〈奉院令協助接收南海諸島案會商紀錄（1946/9/25）〉；〈沈默之報告（1946/9/25）〉；〈南海諸島名稱一覽表〉；〈南海諸島位置略圖〉，中央研究院近代史研究所檔案館藏，《外交部檔案》，館藏號：019.3/0012，「南沙群島」。

[21] 〈美 35 字第 13916 號（1946/10/31）〉，中央研究院近代史研究所檔案館藏，《外交部檔案》，館藏號：019.3/0012，「南沙群島」。

視為相同一物。內政部之所以定義如是，或許是因為「團沙群島」（Tizard Bank）有其為英美所認定之既定範圍，難以觀照「新南群島」全境，而另行制訂「南沙群島」，猶可避免劃地自限。

然就外交部而言，即令到了《舊金山對日和約》簽署前夕，仍有將「團沙群島」、「南沙群島」混用之現象。1951 年，外交部葉公超部長與駐美顧維鈞大使曾論及「團沙群島」應否列入對日和約事，其間公文既有所謂「團沙群島」改名為「南沙群島」之表示，亦有將「南沙（團沙）群島」等同於「新南群島」之認知。[22]

綜觀上述名實之辨可知，「團沙」或附屬或等於「新南群島」，而「南沙群島」之範圍又大過於「新南群島」（前者位處北緯 3 至 12 度東經 109 度至 118 度之間，後者位處北緯 7 至 12 度東經 111/112 至 117 度。表一、新南（南沙）群島意指表）。

職是之故，在「南沙群島」中，扣除「團沙」部分，其他絕大多數之海域島嶼地區，係二戰後中華民國政府自日領之「新南群島」接收而來；加以「南沙群島」之名，乃至於可被視為「U 形線」（九段線）之母的「八段線」，一直要到 1946 年 9 月內政部提出「南海諸島位置略圖」才正式出現，可知中華民國於「南沙群島」之有力／有利聲索，蓋以二戰結束伊始為起點。

[22] 〈團沙群島〉；〈外（40）東一字第 02640 號（1951/4/19）〉；〈外（40）東一字第 02639 號（1951/4/19）〉，中央研究院近代史研究所檔案館藏，《外交部檔案》，館藏號：012.6/0040，「對日和約」。

表一、新南（南沙）群島意指表

呈報機關	資料來源	位置	緯度	與團沙群島之關係
海軍總司令部	美國海軍	新南群島在南沙群島（Macclesfield Bank[按:原為南沙島，1947 年改為中沙群島]）、菲律賓、婆羅洲、交趾半島之中間。	北緯 7 至 12 度東經 112 至 117 度	團沙群島（主要島嶼為長島（Itu Aba Is.）、Sand Cay、Petley Reef、Eladad Reef、南小島（Namyit Is.）、Gaven Reefs）在新南群島內西北之區塊，與中小島（Loaita Bank）、三角/千津島（Thi Tu Island & Reefs）及北險礁（North Danger）成為新南群島之主要島嶼。
臺灣省行政長官公署	日本臺灣總督府	新南群島在西沙群島、菲律賓婆羅洲及交趾半島之間。	北緯 7 至 12 度東經 111 至 117 度	即團沙群島。含北二子（North-East Cay）、南二子（South-West Cay）、西青島（West York I.）、三角島（Thi Thu I.）、中小島（Loaita I. or South I.）、龜甲島（Flot I.）、南洋島、長島（Itu Aba I.）、北小島、南小島（Nam Yit I.）、飛鳥島（Sin Coure I.）、西鳥島（Spratry I.）、丸島（Amboyna Cay）。
廣東省政府	中、日史籍	新南群島位於南中國海中，安南與菲律賓 Palawan 間。	北緯 7 至 12 度東經 111 至 117 度	新南群島與團沙群島實係同地兩名。原團沙群島之名於 1922 年後為日人所改。團沙位於北緯 10 度東經 110 至 111 度之間，大小島嶼 96 個，主要島嶼 9 個，包含斯巴特列島（Spratley I. ）、安波拿島（Amboyna Cay）、伊杜亞巴島（Itee Apu）、洛愛太島（Loaita I.）、替都島（Thi Tu I.）、北危島（North Danger）、納伊島（Nan Yet）、西約島（West York），即 1933 年法佔之九小島。
內政部	自擬	南沙群島為我國南海四群島（東沙島、西沙群島、中沙群島、南沙群島）之最南一群。	北緯 3 至 12 度東經 109 度至 118 度之間	團沙島為南沙群島之中最大一群之島礁，內含雙子島（North Danger）、帝都島（Thi Thu）、賴他島（Loaita I.）、長島（Itu Aba）、北小島（Sand Cay）、南小島（ Nam Yit I. ）、斯普拉利島（Spratly I.）、安波那島（Amboyna Cay）。

（表一由作者製作。〈美 35 字第 13916 號（1946/10/31）〉；〈為奉令籌商協助接收南海諸島一案抄附呈說原文等件並請查照由（1946/10/9）〉；〈關於團沙群島（即新南群島）案會議記錄（1946/9/13）〉；〈海京發字 9258（1946/8）〉；〈未篠署民（一）字第 16909 號（1946/8/17）〉；〈總收文字第 9614 號（1946/8/24）〉，中央研究院近代史研究所檔案館藏，《外交部檔案》，館藏號：019.3/0012，「南沙群島」；〈關於團沙群島（即新南群島）案會議記錄（1946 年 9 月 13 日）〉，中央研究院近代史研究所檔案館藏，《外交部檔案》，檔號：019.3/0001，「中菲南沙群島案取出之複本」；〈菲律賓製造南沙群島事件簡析〉，中央研究院近代史研究所檔案館藏，《外交部檔案》，檔號：019.3/89016，「南沙群島中菲卷」。）

肆、結論

長期以來，有關南沙之主權衝突常流於政治論述或文本之爭，其一定程度反映了爭端國在聲索主權之初，動輒「先射箭、後畫靶」，即言「先提主張、後覓事證」之通病。爭端國在尋覓事證，強化論據之際，仍可能在確立聲索內涵，仍可能要修正主張，俾縮小事證與主張間的差異。

無論是中華民國政府、越南政府，還是菲律賓政府，在建構各自對「南沙群島」／「長沙群島」／「卡拉揚群島」主權論述之初，舉凡標的物之命名、標的物所涉之範疇，乃至於領有標的物之理由，既為舉證之所在，亦是爭端之所在。

本文係從「歷史研究途徑」作論，並以中華民國外交部檔案作為分析文本。筆者透過檢視「南沙群島」之「名」，藉以釐清中華民國於該群島主權論述之「實」，進而揭示我國於「南沙群島」聲索之利基。

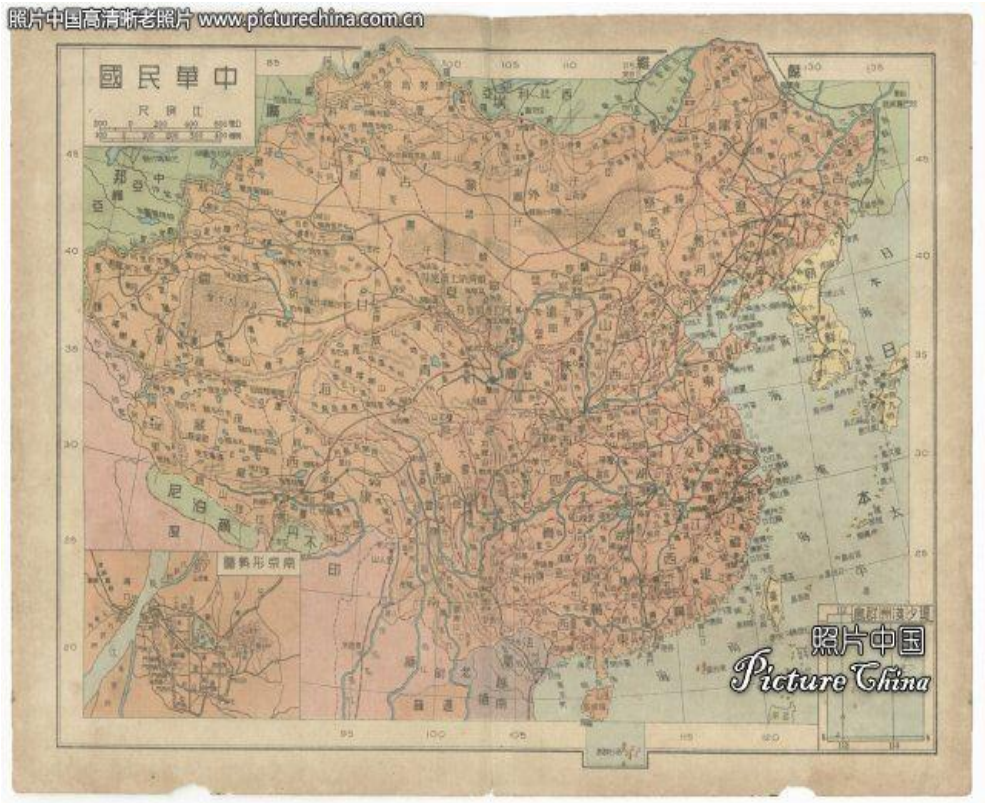
本文首在梳理 1946 年以前「南沙群島」前身「新南群島」與「斯普拉利島群」之間的關聯，從而確認「斯普拉利島群」與「新南群島」就位置來說並無二致；另就戰後「新南群島」可能之歸屬而言，美方顯認法國之聲索能力較強。

其次筆者梳理了「南沙群島」納版及定名之過程，據以界定「新南群島」與「團沙群島」之間的關聯。經研究，可知「團沙」或附屬或等於「新南群島」，而「南沙群島」之範圍又大過於「新南群島」。

職是之故，在「南沙群島」中，扣除「團沙」部分，其他絕大多數

之海域島嶼地區，純係二戰後中華民國政府自日領之「新南群島」接收而來；加以「南沙群島」之名，乃至於可被視為「U 形線」（九段線）之母的「八段線」，一直要到 1946 年 9 月內政部提出「南海諸島位置略圖」才正式出現，可知中華民國於「南沙群島」之有力／有利聲索，蓋以二戰結束伊始為起點。

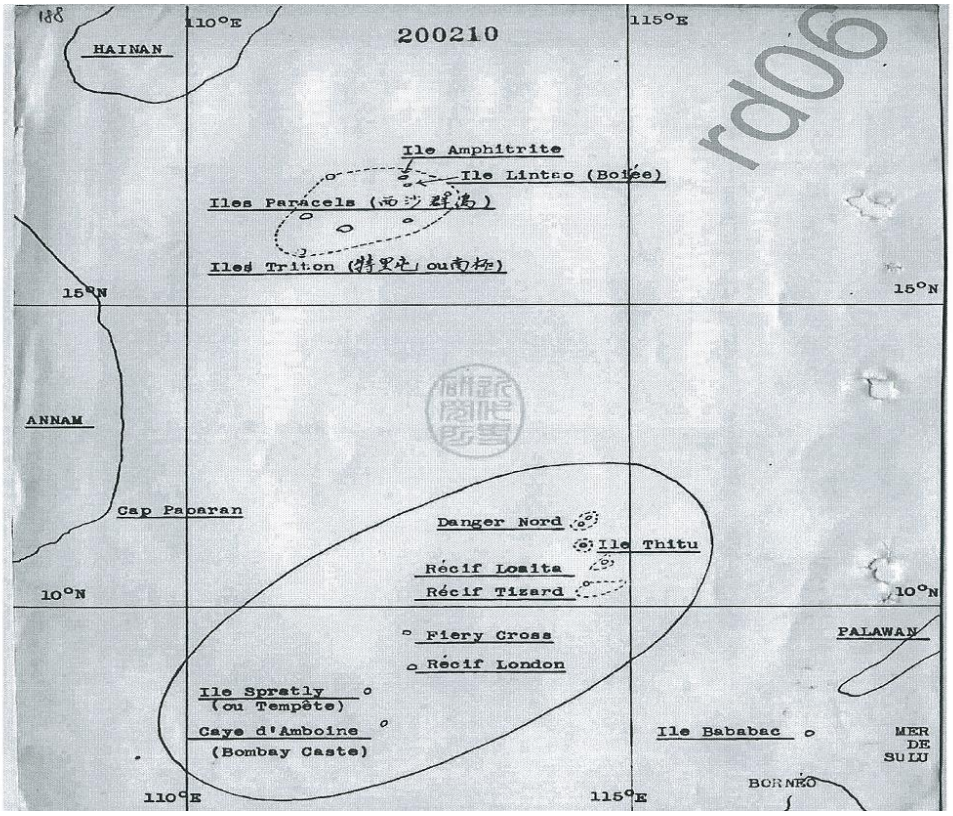
附圖



附圖一、1930 年代中華民國堤沙淺洲群島

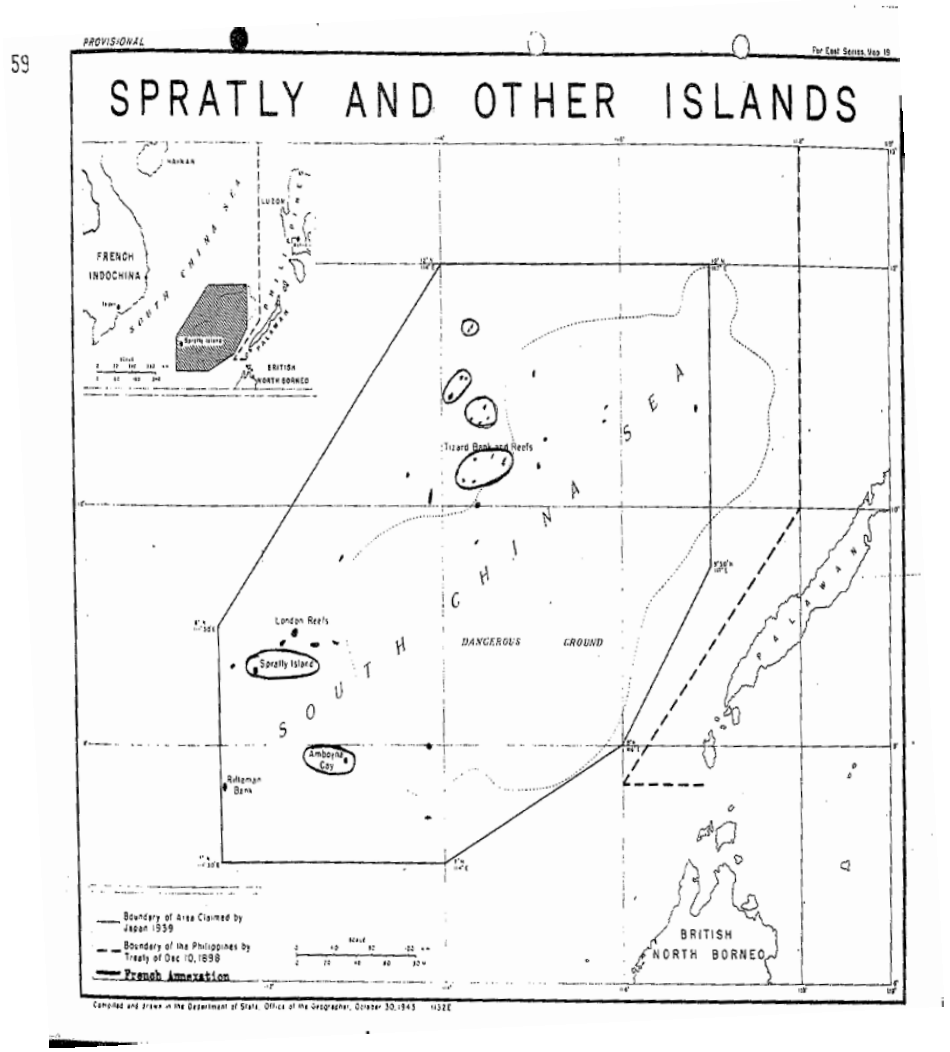
（地圖右下小框，Tizard Bank and Reefs）

資料來源：http://www.picturechina.com.cn/BBs/viewthread.php?tid=155160



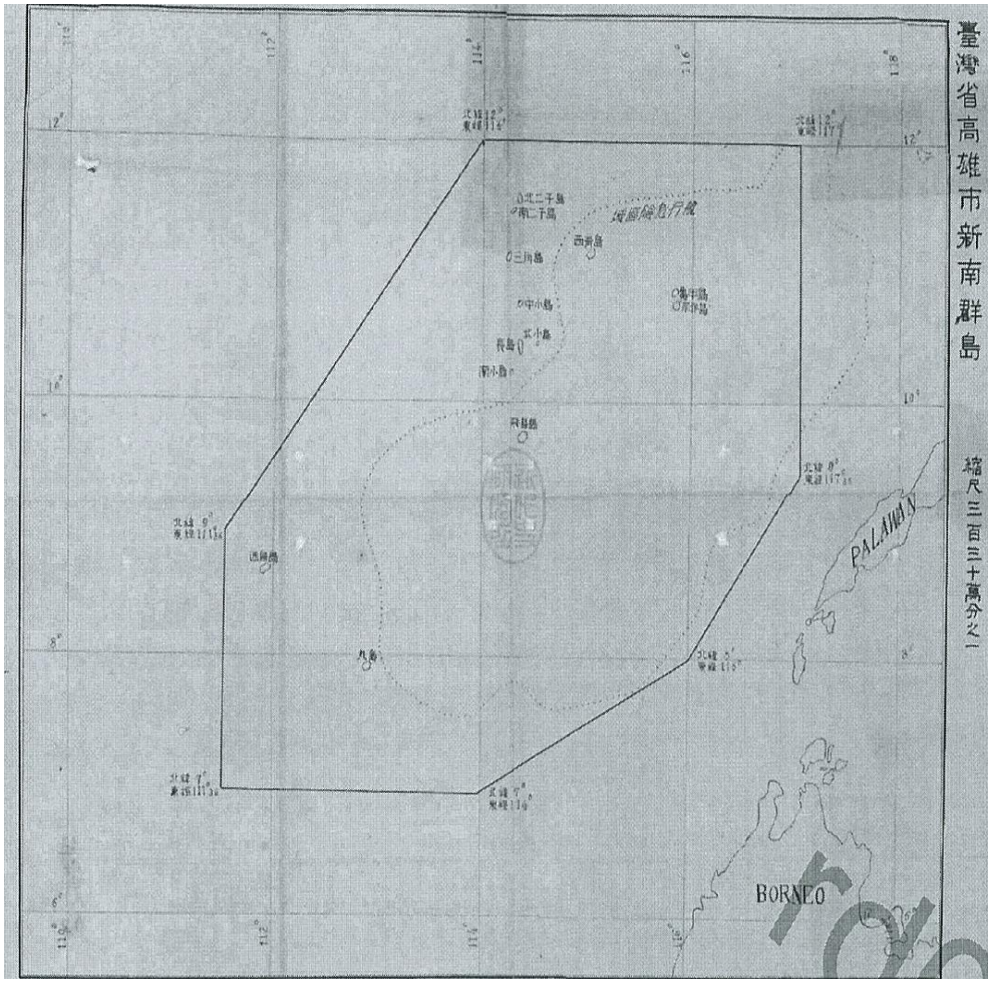
附圖 2、1933 年法國所佔島嶼

資料來源：中央研究院近代史研究所檔案館藏，《外交部檔案》，檔號：019.3/0001，「南沙群島」。



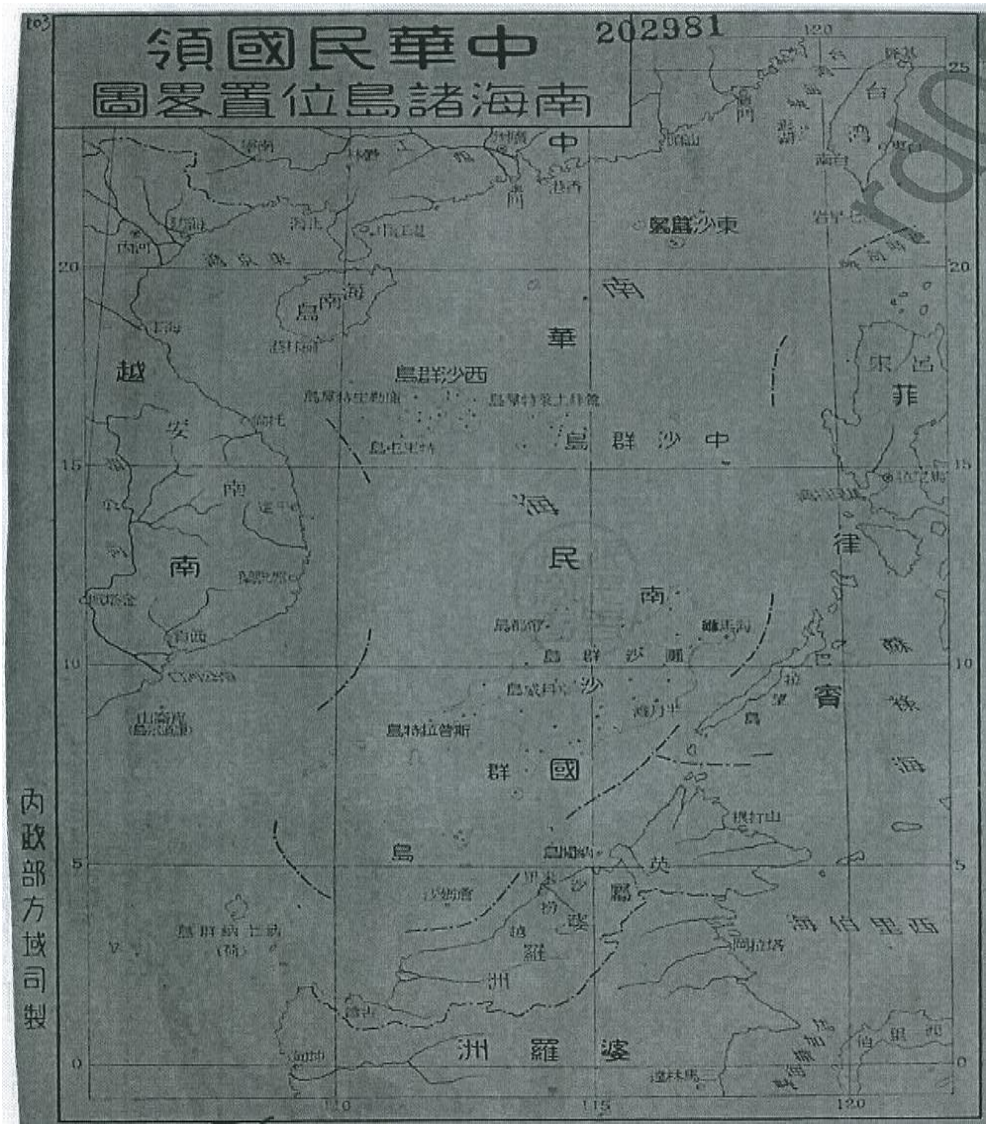
附圖 3、Spratly and other islands

資料來源：Spratly and Other Islands（Shinnan Gunto）, May 29, 1944, Reel 15, Confidential U.S. State Department special files. Southeast Asia, 1944-1958 [microform] / [edited by Gregory Murphy], Bethesda, MD.: University Publications of America, 1989.



附圖 4、臺灣省高雄市新南群島

資料來源：中央研究院近代史研究所檔案館藏，《外交部檔案》，館藏號：019.3/0012，「南沙群島」



附圖 5、南海諸島位置略圖（1946.9）

資料來源：中央研究院近代史研究所檔案館藏，《外交部檔案》，館藏號：019.3/0012，「南沙群島」

參考書目

一、檔案

Confidential U.S. State Department special files. Southeast Asia, 1944-1958, [microform] / [edited by Gregory Murphy], Bethesda, MD.: University Publications of America, 1989.

中央研究院近代史研究所檔案館藏，《外交部檔案》

館藏號：012.6/0038，「對日和約」。
館藏號：012.6/0040，「對日和約」。
檔號：019.3/0001，「中菲南沙群島案取出之複本」。
檔號：019.3/0001，「南沙群島」。
館藏號：019.3/0004，「南沙群島」。
館藏號：019.3/0005，「南沙群島」。
館藏號：019.3/0006，「南沙群島」。
館藏號：019.3/0012，「南沙群島」。
分類號：019.3，案次號：89001，「西南沙群島說帖、圖表資料」。
分類號：019.3，案次號：89002，「西南沙群島說帖、圖表資料」。
分類號：019.3，案次號：89016，「南沙群島中菲卷」。
分類號：019.3，案次號：89017，「南沙群島中菲卷」。

總統府檔案：

檔號：21002/0001，「中日和平條約」。
檔號：3310903/0005/001，「中菲越交涉南沙西沙群島主權問題」。
檔號：3310602/0033/001，「中菲（菲律賓）外交關係文件」。

國防部國軍史政檔案影像借調閱系統：

《總統府檔案》

檔號：00042932，「撤回西沙南沙島戍守」。

《海軍總部檔案》

檔號：00003044，「東南沙群島防務案」。

《部本部檔案》

檔號：00000082，「南沙群島資源開採案」。
檔號：00000084，「南沙群島資源開採案」。
檔號：00003165，「南沙群島國際糾紛案」。

國史館檔案：

《蔣中正總統文物》

入藏登錄號：002000001928A，「一般資料-呈表彙集（一一二）」。

《蔣經國總統文物》，

入藏登錄號：005000000783A，「外交-駐外單位之外交部收電（十六）」。
入藏登錄號：005000000843A，「軍事-增強南沙守備區防務情形等」。

《行政院檔案》

入藏登錄號：020000012043A，「院會資料」。

《國民政府》，

入藏登錄號：001000004852A，「渤海灣海峽及南海島灣名稱」。

檔案管理局藏：

《內政部檔案》

檔號：A301000000A/0035/E41502/1，「進駐西南沙群島案」。

《國防部史政編譯局檔案》

館藏號：34/002.6/4010.2/2/045，「台灣光復案專輯」。

二、專書

Borders of the Philippines: Malaysia-Philippines Border, Territorial Disputes of the Philippines, Spratly Island, Sabah, North Borneo, North Borneo, dispute, territories claimed by the Philippines, Scarborough Shoal, Macclesfield Bank, Itu Aba Island, Island of Palmas (Tennessee: Books LLC, 2010).

Catley, Bob and Keliat, Makmur, *Spratlys: The Dispute in the South China Sea* (Aldershot and Brookfield: Ashgate, 1997).

Crawford, James, *State Responsibility: The General Part* (Cambridge: University Printing House, 2013).

Encyclopedia of Public International Law, Instalment 7: History of International Law — Foundations and Principles of International Law — Sources of International Law — Law of Treaties (Amsterdam: North Holland Publishing Cie., 1984).

Hara, Kimie, *Cold War Frontiers in the Asia-Pacific: Divided Territories in the San Francisco System* (London, New York: Routledge, 2007).

Marsot, Alain G., *The Chinese Community in Vietnam under the French* (San Francisco: Em Text, 1993).

Pablo-Baviera, Aileen San ed., *The South China Sea Disputes: Philippine Perspectives*

(Quezon City: Philippine-China Development Resource Center and the Philippine Association for Chinese Studies, 1992).

Samuels, Marwyn S., *Contest for the South China Sea* (New York: Methuen, 1982).

Spratly Islands: Spratly Islands, policies, activities and history of the Philippines in Spratly Islands, Kalayaan, Palawan, Itu Aba Island, Thitu Island, Southwest Cay, Tomas Cloma, Mischief Reef, West York Island, Republic of Morac-Songhrati-Meads, Loaita Island (Tennessee: Books LLC, 2010).

《中華民國對日和約》(台北：中國國民黨中央委員會黨史委員會發行，1995)。

《海軍巡弋南沙海疆經過》(台北：臺灣學生書局，1975)。

王正華編註，《蔣中正總統檔案：事略稿（68)》(臺北縣：國史館，2003)。

中國陸軍總司令部編，《中國戰區中國陸軍總司令部處理日本投降文件彙編》(上卷)，1945。

中國國民黨中央委員會黨史會編，《中華民國重要史料初編：對日抗戰時期 第三編 戰時外交（三)》。

中國國民黨黨史委員會編，《光復台灣之籌劃與受降接收》(台北：國民黨黨史會出版，1990)。

海頓（Hayton, Bill)，《南海：21 世紀的亞洲火藥庫與中國稱霸的第一步?》(臺北：麥田出版，2015)。

三、會議論文

Beckman, Robert C., "The South China Sea Dispute: An International Lawyer's View," 2011, http://cil.nus.edu.sg/wp/wp-content/uploads/2009/09/Beckman-Paper-on-SCS-Dispute-ISEAS-ASC-18-Feb-2011-final.pdf.

Carpio, Antonio T., "Historical Facts, Historical Lies, and Historical Rights in the West Philippine Sea," http://www.imoa.ph/imoawebexhibit/The%20Historical%20Facts%20in%20the%20WPSLOW.pdf.

許文堂，〈南沙與西沙---他者的觀點〉，發表於「七〇年代東亞風雲—臺灣與琉球、釣魚台、南海諸島的歸屬問題」學術研討會（臺北：台大社會科學院國際會議廳，2013 年 10 月 27 日)。

四、期刊論文

Aguda, Henry Rhoel R. and Arellano-Aguda, Jesusa Loreto A., "The Philippine Claim Over the Spratly Group of Islands: An Application of Article 76 of the UNCLOS," *Law Journal*, 83 Phil. L.J. 573, 2009, pp.573-608.

黃宗鼎，〈越南共和國之華人政策（1955-1964)〉，《國史館學術集刊》，第 11 期，(台

北：國史館，2007），頁 189-249。

黃宗鼎，〈「分裂國家」的「大局外交」：以中華民國對越之西、南沙交涉為例（1955-1975）〉，《國史館館刊》，第 43 期，（台北：國史館，2015 年 3 月），頁 141-197。

五、學位論文

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

黃宗鼎，〈冷戰體制下中華民國對越南共和國之外交政策（1955-1975）〉，國立暨南國際大學東南亞研究所博士論文（2014）。

六、網路資料

Current Law Journal Content, http://lawlib.wlu.edu/CLJC/index.aspx

Division for Ocean Affairs and the Law of the Sea, "Chronological lists of ratifications of, accessions and successions to the Convention and the related Agreements", Office of Legal Affairs, United Nations, http://www.un.org/Depts/los/reference_files/chronological_lists_of_ratifications.htm.

University of Wisconsin-Madison Libraries and University of Illinois at Chicago Libraries, "Foreign Relations of the United States", University of Wisconsin Digital Collections Center, http://uwdc.library.wisc.edu/collections/FRUS.

GMA News Online, http://www.gmanetwork.com/news/.

Harry S. Truman Library and Museum, http://www.trumanlibrary.org/.

Bureau of Oceans and International Environmental and Scientific Affairs, "Limits in the Seas," U.S. Department of State, http://www.state.gov/e/oes/ocns/opa/c16065.htm.

NewspaperArchive.com, http://newspaperarchive.com/.

ChanRobles & Associates Law Firm, "PHILIPPINE LAWS, STATUTES and CODES", ChanRobles Virtual Library, http://www.chanrobles.com/otherlaws.htm.

Philippine Star, http://www.philstar.com/.

Taiwan Documents Project, http://www.taiwandocuments.org/index.htm.

中華人民共和國外交部，http://www.fmprc.gov.cn/mfa_chn/.

台灣大百科全書，http://taiwanpedia.culture.tw/web/content?ID=3834.

行政院海岸巡防署，〈歷史背景〉，行政院海岸巡防署，http://www.cga.gov.tw/GipOpen/wSite/ct?xItem=10574&ctNode=1306&mp=999.

南沙群島在線，http://www.nansha.org.cn/.

照片中國，http://www.picturechina.com.cn/BBs/index.php.

永井和，〈映像で見る占領期の日本〉，永井和のホームページ，http://nagaikazu.la.coocan.jp/GHQFILM/DOCUMENTS/index.html.

From 'Armed Attack' to 'Cyber Attack': The Evolution of Collective Self-Defense in NATO

Brooke A. Smith-Windsor

Senior Research Fellow,
RAND Europe

Abstract

In 2014, the world's most powerful political-military alliance in history, the North Atlantic Treaty Organization (NATO), decided to officially associate cyber attacks with its collective self-defense mandate. The development marked a significant milestone in the evolution of the 70 year-old defense alliance with widespread implications for its future military capabilities, doctrine, and partnerships with like-minded states. This paper explains how this landmark decision came about and considers NATO's continued "cyber adaptation" in the perspective of the September 2018 US National Cyber Strategy.

Key Words: *NATO, cyber defense, collective defense, hybrid threat, European Union*

From Armed Attack to Cyber Attack

從「武裝攻擊」到「網路攻擊」
北大西洋公約組織集體自衛的演變

Brooke A. Smith-Windsor

蘭德歐洲智庫 資深研究員

摘　　要

在 2014 年，世界上有史以來最強大的政治與軍事同盟，北大西洋公約組織（北約），正式決定將網路攻擊納入共同防禦之範疇。此發展可謂該防衛同盟 70 年來演進的重大里程碑，廣泛涉及了未來的軍事能力、準則，以及理念相同國家之間的夥伴關係。本文闡釋了此標誌性決議之形成過程，並從 2018 年 9 月美國《國家網路戰略》的案例來思索北約該如何「深化網路防禦」。

關鍵詞：北約、網路防禦、集體防禦、混和威脅、歐盟

Introduction

Founded in 1949, the North Atlantic Treaty Organization (NATO) routinely has been described as the most successful collective defense alliance in history. Today, its 29 (soon 30)[1] member states represent over half of the world's economic and military might collectively pooled to defend the territory and shared liberal democratic values of Europe and North America. NATO's success is a function of its proven ability to adapt to an ever-changing security environment. The Alliance consistently has demonstrated the flexibility to address new threats to transatlantic security whether in terms of actors or capabilities. The shift from preoccupation with a Soviet invasion to concern with global terrorism since 911 is one such adaptation. Its refocus on inter-state warfare and the defense of Europe against a resurgent Russia since 2014 is another. To these can be added recent efforts to bolster defenses against ballistic missiles in view of their proliferation. What is more is NATO's response to threats posed in the cyber domain. As the Alliance's Secretary General, Jens Stoltenberg, remarked in May 2018, "From the moment a rock was first used as a hammer, society has been driven by technology. Today's great leap forward is not physical, but it is digital … But there is a dark side to this technology. In recent years we have seen many large-scale cyber-attacks."[2]

Cyber attacks represent a particularly daunting challenge because they were not envisioned in collective defense terms when the United Nations (UN) Charter was founded in 1945 (Article 51) or when NATO was created four years later. As NATO's founding treaty's collective defense provision (Article 5) states:

> *The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of*

[1] In July 2018, NATO invited the former Yugoslav Republic of Macedonia to begin accession talks.

[2] Jens Stoltenberg, "Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defense Pledge Conference." Cyber Defense Pledge Conference, May 15, 2018, Paris. Speech. *NATO*, May 15, 2018. https://www.nato.int/cps/en/natohq/opinions_154462.htm.

> *individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.*[3]

Nevertheless, at their Wales summit of September 2014, NATO and its member states took the historic step of associating cyber with Article 5. "Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence."[4] This acknowledgment was no small feat considering that all decisions in NATO require consensus. How the Alliance arrived at this point and the policy implications that followed it is the subject of this paper. It begins with a summary of the principal historic events in Europe that helped galvanize NATO's thinking about cyber threats. This is followed by consideration of some of the conceptual foundations that supported official decision-making within the Alliance. The next part examines the components of NATO's formal "cyber adaptation" over the last decade. The paper concludes with observed challenges facing NATO's continued adaptation in the cyber realm.

Real-world Milestones

The 20th century American political journalist, Norman Cousins, observed that "history is a vast early warning system." The words ring no less true when it comes to cyber in more recent times. For NATO, four real-world crises in the European theater were the harbinger of the dark side of the digital age.

---

[3] "The North Atlantic Treaty," *NATO*, 1949, https://www.nato.int/cps/ua/natohq/official_texts_17120.htm.

[4] "Wales Summit Declaration," *NATO*, 2014, https://www.nato.int/cps/ic/natohq/official_texts_112964.htm.

Kosovo

In 1999, NATO embarked on a 78-day aerial bombardment of the Federal Republic of Yugoslavia to halt mass atrocity crimes in Kosovo. Operation Allied Force succeeded. However, the experience also brought to light in unprecedented terms the vulnerabilities of NATO information systems and networks to cyber assaults during a military campaign. A notable occurrence was the temporary disruption of the NATO public affairs website by pro-Serbian hackers.[5] Not surprisingly, at their first wide-ranging summit since the Kosovo operation, NATO and its member states affirmed the need to "Strengthen our capabilities to defend against cyber attacks."[6]

Estonia

If Kosovo for the first time highlighted the risks to NATO's own information technology (IT) infrastructure, an event taking place eight years later would firmly elevate the Alliance's awareness about the dangers of cyber attacks from the tactical-operational level to the strategic one: where an entire society could be adversely affected. In 2007, three years since becoming a NATO member state, Estonia suffered a distributed denial of service attack (DDoS) on both the public and private (economic) sector networks. While in this instance, the attacks did not result in casualties and physical destruction, their comprehensive nature and the suspicion of state (Russian) sponsorship had not been seen before. NATO's subsequent Strategic Concept (2010) acknowledged the new reality: "Cyber attacks are becoming more frequent, more organised and costlier in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure …"[7]

---

[5] Christine Hegenbart, "Semantic Matters: NATO, Cyberspace and Future Threats." *NATO Defense College Research Paper*, No. 103, 2014, p.3.

[6] "Prague Summit Declaration," *NATO*, 2002, https://www.nato.int/cps/en/natohq/official_texts_19552.htm.

[7] "Strategic Concept – Active Engagement, Modern Defence," *NATO*, 2010, https://www.nato.int/strategic-*concept*/pdf/Strat_Concept_web_en.pdf.

Georgia and Ukraine

Conflict in Georgia and Ukraine in 2008 and 2014 respectively saw the first European case of the coordination of state-sponsored cyber attacks as part of a military campaign with societal-wide disruption. When Russian forces moved into the breakaway republics of Abkhazia and South Ossetia, Georgia's internal communications were effectively shut down. Six years later, a similar yet reportedly 32 times larger DDOS attack, targeted Ukraine as pro-Russian forces seized control of Crimea and fomented separatism in eastern Ukraine.[8] Although Georgia and Ukraine are NATO partners, not members, the lessons from the experience were not lost on the Alliance. As the NATO website acknowledges to this day, "the conflict between Russia and Georgia demonstrated that cyber attacks have the potential to become a major component of conventional warfare,"[9] it also is no coincidence that the association of cyber with Article 5 cited earlier came within months of Russia's illegal annexation of Crimea from Ukraine. Cyber defenses to guard against a similar fate for a NATO member state are now as important as conventional and nuclear ones.

Conceptual Foundations

In tandem with the real-world experiences of cyber attacks in Europe—and informed by them— analysts on both sides of the Atlantic began in earnest to debate the political, legal and military underpinnings of collective defense in the cyber realm. The best-known example is the so-called Tallinn Manual facilitated by the NATO-accredited Cooperative Cyber Defense Center of Excellence, initiated in 2009, first published in 2013 and now in its second edition.[10] It is beyond the scope of this paper to delve into every aspect of the (ongoing) debate. However, highlighting a

[8] Robert Windrem, "Timeline: Ten Years of Russian Cyber Attacks on Other Nation s." *NBC News*, December 18, 2016, https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111.

[9] "Cyber Defense." *NATO*, July 16, 2018. https://www.nato.int/cps/en/natohq/topics_78170.htm.

[10] Information on the Tallinn Manual's development is available at: https://ccdcoe.org/tallinn-manual.html.

few elements sheds light on the conversation that has helped shape official policy-making in NATO.

Typology of Cyber Threats

A 2013 study published by the NATO Defense College Research Division offered a succinct catalogue of cyber threats ranging from: (i) hacktivism and cyber vandalism; (ii) cyber crime; (iii) cyber espionage; (iv) cyber sabotage; (v) cyber terrorism; (vi) cyber war.[11] The categorization avowedly was important to determining the extent of NATO's involvement in the cyber domain. Beyond the routine protection of NATO's own networks through the Computer Incident Response Capability for instance, the first two contingencies were situated as primarily the subject of civil law enforcement within individual nations. Only the latter four categories were considered to have significant national security implications. And the ones viewed as exhibiting the greatest potential for the infliction of a significant degree of harm on NATO and its member states were cyber sabotage, cyber terrorism and cyber war. In such a scenario Article 4 of the NATO's founding treaty conceivably could be involved—high level consultations if the territorial integrity, political independence or security of any of the member states is threatened—but also possibly Article 5. In the context of NATO's collective defense, the Tallinn Manual's definition of a cyber attack was considered informative: "'a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.' The definition is shaped by the result: if a cyber operation is followed by significant destructive consequences, it qualifies both as a cyber attack and as use of force."[12] During the same period, others also argued that cyber attacks that threaten human beings' integrity and cause significant disruption and destruction, within or outside cyberspace, would qualify as the use of force under the UN Charter.[13] In sum, a recurring theme was that when it comes to collective self defense, the severity of negative

[11] Hegenbart, pp.6-10.
[12] Ibid., pp.8-9.
[13] Iulian F. Popa, "NATO's Cyber Security and Defense: Before and After 2014 Wales Summit." *Annals of the "Constantin Brancusi" University of Targu Jiu, Letterand Social Sciences Series*, No. 3, 2014, p.127.

consequences for a society resulting from a cyber attack matters.

The Attribution Challenge

Even if real and considerable harm were to be inflicted on a NATO member through cyber sabotage, terrorism or warfare thus warranting a collective response, analysts have long recognized that cyberspace presents a challenge when it comes to attribution. Whether it be an online terrorist cell, a state's intelligence service or a country's use of "cyber proxies" to do its bidding, a plethora of actors with the conceivable intent and means to disrupt and destroy are active in cyberspace. Moreover, in this domain none need be geographically proximate to the targeted area and encryption shields identities. Yet, without reasonably assured identification of the perpetrators of an attack, determination of the proportionate response including potential retaliation becomes exceedingly difficult. This predicament is perhaps best summed up in a phrase coined by NATO's Secretary General that "Nowhere is the 'Fog of War' thicker than in cyberspace."[14] To break through the cyber fog, writing in 2015, two analysts suggested a multi-layer approach to the question of culpability. As summarized a year later in the paper entitled, "Cyber Operations and Gray Zones: Challenges for NATO," the model is about understanding: (i) how the attack was perpetrated in technical terms (tactical level); (ii) what non-technical factors—determined through signals intelligence and human intelligence for example—combined with the former to realize the attack (operational level); and finally, who masterminded the attack and why (strategic level).[15] Combined, such factors can serve to propel decision-makers closer to the "proof beyond reasonable doubt" threshold when it comes to apportioning responsibility for the large scale disruption and destruction of societies enacted through cyberspace.

Deterrence

As with nuclear and conventional war, states of course wish to prevent cyber attacks before they happen. Here, the question of deterrence comes

[14] Stoltenberg.
[15] Oliver Fitton, "Cyber Operations and Gray Zones: Challenges for NATO," *Connections*, Vol. 15, No. 2, 2016, pp.114-115.

into play. In cyberspace, an element of self restraint on the part of actors operating within it is "built in." Sometimes this is referred to as "deterrence through interdependence." In other words, some attackers will be wary of going too far to degrade or destroy the IT infrastructure on which they also rely. [16] However, analysts steadily recognized that this type of self-regulation was an unreliable defense. More and more sophisticated attacks as in Estonia, Georgia and Ukraine revealed how widespread disruption to targeted populations and economies could be achieved by a state sponsor without adversely affecting its own. Pro-active deterrence measures, therefore, also would be required. Not surprisingly, advocacy for a retaliatory cyber defense capability on the part of NATO and its member states multiplied. It would have to be credible—able to impose costs on an adversary greater than the gains to be achieved from an attack. And it would have to be deliberately ambiguous—to instill in an adversary uncertainty as to the threshold for NATO retaliation.[17]

Comprehensive Approach

Following the 911 terrorist attacks on the US and NATO's intervention in the place of their origin, Afghanistan, the Alliance realized early-on that it could not act in isolation. Counter-terrorism and stabilization missions required a whole-of-government, inter-agency effort with states working alongside non-state actors each according to its respective mandates and strengths. As a political-military actor, NATO had a role to play but so did others who might at times be in the lead. To recall the common refrain, "Lessons learned from NATO operations show that addressing crisis situations calls for a comprehensive approach combining political, civilian and military instruments. Building on its unique capabilities and operational experience, including expertise in civilian-military interaction, NATO can contribute to the efforts of the international community for maintaining peace, security and stability, in full coordination with other actors. Military means, although essential, are not enough on their own to meet the many

[16] Jamie Shea, "NATO Dealing with Emerging Security Challenges?" *Georgetown Journal of International Affairs*, Vol. 14, No. 2, 2013, p.194.
[17] Fitton, p.117.

complex challenges to our security."[18] Informed by this experience, it was not difficult for analysts to purse similar logic in conceptualizing the Alliance's approach to cyber defense. A 2009 commentary entitled "NATO in Cyberspace" is indicative: "As NATO commanders have learned, defending cyber-based assets is a duty which requires constant, twenty-four hour communication and coordination, mainly with non-military organizations which control more than ninety percent of global cyber infrastructure."[19] For NATO, this would mean moving beyond traditional linkages with foreign and defense ministries, and strengthening ties with interior ministries, intelligence and police services, and national security councils. It also would mean working with the same in partner countries. And to an extent not contemplated in Afghanistan, a comprehensive approach to cyber defense would mean interacting with industry and the private sector as the principal developers and users of information technologies.[20]

NATO's Cyber Adaptation

In 2013, one year prior to NATO associating cyber with collective self defense, its Deputy Assistant Secretary General for Emerging Security Challenges, Jamie Shea, outlined what he saw as the three essential components of the way forward for the Alliance and cyber.[21] Using that blueprint as a guide, this final part explains what has formally transpired in each area over the last decade: *(i) Mandate; (ii) Policy; (iii) Institutionalization and capability development.* Combined, these developments explain how NATO has consensually adapted in official terms to meet the cyber challenge.

---

[18] "A 'comprehensive approach' to crises." *NATO*, June 26, 2018, https://www.nato.int/cps/su/natohq/topics_51633.htm.
[19] Rex Hughes, "NATO in Cyberspace: Digital Defenses." *The World Today*, Vol. 65, No. 4, 2009, p.20.
[20] Shea, p.196.
[21] Ibid., pp.197-198.

Mandate

Delineating a mandate for NATO in cyberspace has necessarily been grounded in its founding treaty. While, as mentioned previously, cyber is not mentioned in the North Atlantic Treaty given the period of its compilation, this fact has not prevented the member states from adapting their interpretation of its principles to fit the digital age. Principally, Articles 3 (capabilities), 4 (consultation) and 5 (collective defense) have been formally implicated drawing on the lessons of the real-world experiences and advice cited earlier. Reference to a selection of official texts is illustrative.

Where Articles 3 and 4 are concerned, the 2010 Strategic Concept is noteworthy. Article 3 of the North Atlantic Treaty commits NATO members to "separately and jointly, by means of continuous and effective self-help and mutual aid, [to] maintain and develop their individual and collective capacity to resist armed attack."[22] The Strategic Concept carried forward the spirit of this article into the cyber domain with a collective member state commitment to "develop further our ability to prevent, detect, defend against and recover from cyber attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations."[23] Building on this earlier interpretation, six years later, the Cyber Defense Pledge (discussed further below) would specifically associate Article 3 with cyber defense capability development.[24] Where Article 4 is concerned, the advocacy for high-level consultations in the event of a member state feeling threatened by a cyber attack has been mentioned. As early as 2010, its translation into official policy may be observed in the Strategic Concept's assertion that "Any security issue of interest to any Ally can be brought to the NATO table."[25]

While the Strategic Concept spoke of deterring and defending against

[22] The North Atlantic Treaty.
[23] Strategic Concept – Active Engagement, Modern Defence.
[24] "Cyber Defense Pledge", *NATO,* July 8, 2016, https://www.nato.int/cps/en/natohq/official_texts_133177.htm.
[25] Strategic Concept – Active Engagement, Modern Defence.

"emerging security challenges" in the perspective of Article 5, as highlighted at the outset of this paper, it was not until 2014 at the NATO Wales summit when cyber was formally associated with the article. Cyber was further linked to Article 5 at the NATO Brussels summit of July 2018 in the context of so-called hybrid warfare: "We face hybrid challenges, including disinformation campaigns and malicious cyber activities … While the primary responsibility for responding to hybrid threats rests with the targeted nation, NATO is ready, upon [North Atlantic] Council decision, to assist an Ally at any stage of a hybrid campaign. In cases of hybrid warfare, the Council could decide to invoke Article 5 of the Washington Treaty, as in the case of armed attack."[26]

Similar to the 2018 NATO Brussels Summit Declaration, the earlier Wales declaration affirmed the applicability to cyberspace (and, therefore, NATO activities therein) of the UN Charter (presumably Article 51 in particular) as well as international and humanitarian law. Reflective of the policy advice heard years before about deterrence, the 2014 pronouncement also was deliberately ambiguous about the threshold for retaliation whether against cyber sabotage, terrorism or war: "A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis."[27] As suggested above, however, the magnitude of harm inflicted would likely be a key factor. Using history as a guide, the direction of the attack also would likely figure in the deliberations. In reflecting on the criteria used to invoke Article 5 in response to 911, Edgar Buckley, Assistant Secretary General for Defence Planning and Operations from 1999 to 2003, recalled that alongside the scale of an attack, "External direction was important because it was clear that the Allies did not regard attacks by internal terrorist organisations—such as in Belfast or Oklahoma City—as falling under the Treaty."[28] For reasons discussed previously, determining the external direction of a cyber attack might prove more difficult than unearthing a

[26] "Brussels Summit Declaration," *NATO*, 2018, https://www.nato.int/cps/en/natohq/official_texts_156624.htm.

[27] *Wales Summit Declaration*. The North Atlantic Council is NATO's highest decision-making body.

[28] Edgar Buckley, "Invoking Article 5." *NATO Review*, No. 2, 2006. https://www.nato.int/docu/review/2006/Invokation-Article-5/Invoking_Article_5/EN/index.htm.

plot to hijack airliners hatched in Afghanistan, but confirming foreign culpability would still be significant. At least one model for helping to do so has been presented.

In recent years, the strategic ambiguity that has deliberately surrounded a NATO response to a cyber attack also has included the possibility of action short of collective defense. As NATO's Secretary General explains, "The level of cyber-attack that would provoke a response must remain purposefully vague. As will the nature of our response. But it could include diplomatic and economic sanctions, cyber-responses, or even conventional forces … We need a full spectrum response. So we can respond to serious cyber-attacks even if they don't cross the Article 5 threshold."[29] Since the 1990s, NATO's mandate has evolved to comprise crisis management alongside collective defense (and cooperative security) as a core task; so the Secretary General's remarks may be viewed in this context.

Finally, it is worth noting that 2016 was another watershed year for NATO's mandate in cyberspace. Cyberspace was for the first time officially identified as a domain of Alliance operations joining the traditional ones of land, sea and air.[30]

Policy

With a defensive mandate in cyberspace established, policies to realize it in practice have continued apace. Published in 2014, the third iteration of a NATO Cyber Defense Policy identified the protection of NATO's own communications and IT systems as the chief priority, but also instituted several governance and educational measures to enable individual member states to draw on NATO support in response to cyber attacks and to build national capacity. The policy also integrated cyber defense into operational and civil-emergency planning. Reflective of previously referenced calls for a comprehensive approach, the policy went on to advocate for cooperation

[29] Stoltenberg.
[30] "*Warsaw Summit Communiqué*," *NATO*, 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

with partner countries and relevant international organizations.[31] Two years later, the Cyber Defense Pledge further compelled each member state to step up the "cyber hygiene" and defense of national infrastructures as well as static and deployable networks including those on which NATO relies. Improved information sharing and collaboration among Allies likewise was pledged.[32] Other policy milestones have included a concerted effort to engage industry. At the behest of Estonia, the Netherlands and United Kingdom, the NATO Industry Cyber Partnership was launched in 2014. Among its objectives is to improve sharing of best practices and expertise on preparedness and recovery including technology trends and malware information. In May 2018, for example, the Alliance signed bilateral agreements with industry leaders CY4GATE, Thales and Vodafone. The agreements are designed to facilitate rapid early bilateral exchange of non-classified technical information related to cyber threats and vulnerabilities to be integrated into NATO's 24/7 detection and prevention system.[33] The comprehensive approach to cyber defense, moreover, has not ended with industry. In July 2016, the European Union and NATO also signed a bilateral Joint Declaration. Cybersecurity was one of seven areas highlighted for concerted collaboration. The EU's External Action Service recently emphasized the (ongoing) exchange that has ensued on cyber concepts and doctrine, training and education, and threat indicators.[34]

Institutionalization and capability development

When Jamie Shea wrote about the essential components of NATO's cyber defense portfolio, "creating a firm bureaucratic foothold in the NATO organization" was one of them.[35] The point was that policy statements do not create defense capabilities by inertia. Dedicated organizations and processes do. Thus, it should come as no surprise that NATO's "cyber

---

[31] "Cyber Defense," *NATO*, July 16, 2018, https://www.nato.int/cps/en/natohq/topics_78170.htm.

[32] Cyber Defense Pledge.

[33] "New NATO-industry cyber partnerships signed at NITEC18." *NCI Agency*, May 23, 2018, https://www.ncia.nato.int/NewsRoom/Pages/180523-IPAs_signature_NITEC.aspx.

[34] "EU-NATO Cooperation – Factsheet." *EEAS*, July 10, 2018. https://eeas.europa.eu/headquarters/headquarters-Homepage/28286/eu-nato-cooperation-factsheet_en

[35] Shea, p.197.

bureaucracy" steadily has expanded. The following constitute some of the key organs.

The Cyber Defense Committee provides high-level political oversight of NATO cyber defense initiatives. Working-level support is provided to it by the NATO Cyber Defense Management Board. Technical advice resides in the NATO Consultation, Control and Command Board. The NATO Communications and Information Agency supports NATO operations and connects as well as defends NATO networks. The Agency is a core function of its NATO Computer Incident Response Capability Technical Center of 200 experts. Recognizing the importance of nurturing the next generation of such experts, the Agency is also establishing a 20 million-euro NATO Communications and Information Academy to be opened in 2019.[36] Furthermore, at the 2018 NATO Brussels summit, the creation of a dedicated Cyberspace Operations Center was a central plank of the first expansion of the NATO Command Structure in several years.[37] It is intended to provide situational awareness and coordination of NATO operational activity within cyberspace. The same Brussels meeting also announced the establishment of NATO Counter-Hybrid Support Teams, adding to the Alliance's cyber-defense portfolio that already includes the precursor NATO Cyber Rapid Reaction Teams. These teams are designed to provide tailored, targeted assistance to individual member states upon their request. It also is worth recalling that alongside the constitution of these official cyber organs within the NATO bureaucracy, new processes have been added. Significantly, since 2012, cyber defense has been integrated into the NATO Defense Planning Process through which the Alliance and national capability targets are harmonized. Successive Cyber Defense Policy statements have, in turn, been accompanied by a Cyber Defense Action Plan to guide their implementation.[38]

Finally, outside the formal Alliance structures, the previously mentioned NATO-accredited Cooperative Cyber Defense Center of

[36] "NATO breaks ground on IT academy." *NCI Agency*, May 23, 2017. https://www.ncia.nato.int/NewsRoom/Pages/170523-NCI-Academy_groundbreaking_ceremony.aspx

[37] Brussels Summit Declaration.

[38] "Cyber Defense," *NATO*, July 16, 2018. https://www.nato.int/cps/en/natohq/topics_78170.htm.

Excellence (CCDCOE) also has been a longstanding hub of interdisciplinary research, training and education on cyber issues. In addition to the development of the unofficial Tallinn Manual, this contribution has included the annual conduct of the world's largest live-fire exercise Locked Shields on the so-called NATO Cyber Range. In February 2017, a contract to update the Range was granted. As the winning bidder, Guardtime, affirmed at the time, "For NATO we will provide a state of the art flexible, operationally relevant and representative environment design that enables integrated simulation and training and collaboration for a wide variety of blue and red team cyber mission exercise areas …"[39] What is more, since 2017, the work of the CCDCOE has been complemented by the establishment of the NATO-EU sponsored European Center for Countering Hybrid Threats based in Helsinki, Finland (a NATO partner nation). As its mandate states: "Due to increased opportunities for hybrid influencing during the present information age, the hybrid challenge will grow. The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) is to serve as a hub of expertise supporting the participating countries' individual and collective efforts to enhance their civil-military capabilities, resilience, and preparedness to counter hybrid threats with a special focus on European security." [40]

Future Challenges

Preceding pages have illustrated NATO's considerable effort to adapt to meeting cyber threats. Yet, a mantra of defense policy planners is that "transformation is a journey, not a destination." NATO's cyber adaptation is no different. So what challenges lie ahead? This paper concludes by briefly discussing one notable policy development: the advent of the new US National Cyber Strategy.

---

[39] Meelis Vill, "Guardtime Awarded Contract for Next-Generation NATO Cyber Range." *Guardtime*, February 1, 2017. https://guardtime.com/blog/guardtime-awarded-contract-for-nato-cyber-range.

[40] Information on the Hybrid COE is available at: https://www.hybridcoe.fi/.

US National Cyber Strategy

In September 2018, the US Administration published the National Cyber Strategy[41]—the first in fifteen years. In the Trump era of "America First," allies as well as adversaries will be obliged to take note. NATO is no exception. While, as mentioned previously, consensus is a core operating principle of the Alliance, US leadership matters to agenda-setting. Its pre-eminence in defense spending is why the United States is understandably referred to as the "indispensable Ally" in NATO circles. Washington will expect NATO and its Canadian and European members to take note of this latest US policy pronouncement and reflect on the implications for the Alliance. Reference to the US National Cyber Strategy of the United States of America released last year should leave no doubt in this regard. It affirmed the US commitment to Article 5 and referred to NATO as one of America's great strategic advantages over competitors, but went on to frankly state that "The NATO alliance will become stronger when all members assume greater responsibility for and pay their fair share to protect our mutual interests, sovereignty, and values."[42] So what are some of the possible repercussions for NATO's cyber deterrence and defense?

The American strategy for one profile increased concern about the growing cyber-related threats to space assets and supporting infrastructure related to: "positioning, navigation, and timing (PNT); intelligence, surveillance, and reconnaissance (ISR); satellite communication and weather monitoring."[43] It goes without saying that each is critical to military operations, including NATO-led ones. While for a country like the US that has long recognized outer-space as an operating domain, redoubling efforts to link it to the cyber one may seem logical. The US also avowedly wants to work with industry and international partners to improve

---

41 *National Cyber Strategy of the United States of America.* United States of America, 2018. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

42 "National Security Strategy of the United States of America," *The White House*, December 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

43 "National Cyber Strategy of the United States of America," *The White House*, September 2018, p.10, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

"space cybersecurity" including the cyber resilience of existing and future space systems. However, for the Alliance that does not yet recognize space as an operating domain alongside cyber, land, sea and air, following the American lead may prove somewhat more challenging. Nevertheless, there are signs that things may evolve in space as rapidly as they have for NATO in the hybrid sphere. In another landmark decision taken at their 2018 NATO Brussels summit, the member states declared: "Recognising that space is a highly dynamic and rapidly evolving area, which is essential to a coherent Alliance deterrence and defence posture, we have agreed to develop an overarching NATO Space Policy."[44]

The Brussels summit was also notable for its commitment to reinvigorate NATO's maritime deterrence and defence posture including maritime warfighting skills to protect critical sea lines of communications. While on this occasion the Alliance did not specifically mention cyberspace in a maritime context, it may soon be urged by the US to do so. The National Cyber Strategy singles out the criticality of maritime transport to the US and global community and, consequently, the need to "accelerate the next-generation cyber-resilient maritime infrastructure."[45] Should calls for an updated Alliance Maritime Strategy be heeded, maritime cybersecurity (which the 2011 version does not mention) surely will receive attention.

Lastly, in September 2018 the US also launched the International Cyber Deterrence Initiative. The aim is to build an international coalition of like-minded states to address malicious cyber behavior including better information and intelligence sharing, reinforcing attribution claims, coordinated public statements of support for responses, as well as the joint imposition of consequences for disruptive and destructive behavior in the so-called "technical ecosystem."[46] Whether in a space or maritime context or elsewhere, NATO's future mandate, policy and capability development in the cyber and related domains will most certainly be influenced by this latest American endeavor.

---

[44] Brussels Summit Declaration.
[45] "National Cyber Strategy of the United States of America," *The White House*, September 2018, pp.9-10.
[46] Ibid., p.21.

Bibliography

"A 'comprehensive approach' to crises," *NATO*, June 26, 2018, https://www.nato.int/cps/su/natohq/topics_51633.htm

"Brussels Summit Declaration," *NATO*, 2018, https://www.nato.int/cps/en/natohq/official_texts_156624.htm

Buckley, Edgar, "Invoking Article 5," *NATO Review*, No. 2, 2006, https://www.nato.int/docu/review/2006/Invokation-Article-5/Invoking_Article_5/EN/index.htm.

"Cyber Defense Pledge", *NATO*, July 8, 2016, https://www.nato.int/cps/en/natohq/official_texts_133177.htm.

"Cyber Defense," *NATO*, July 16, 2018, https://www.nato.int/cps/en/natohq/topics_78170.htm.

"EU-NATO Cooperation – Factsheet," *EEAS*, July 10, 2018, https://eeas.europa.eu/headquarters/headquarters-Homepage/28286/eu-nato-cooperation-factsheet_en.

Fitton, Oliver, "Cyber Operations and Gray Zones: Challenges for NATO," *Connections*, Vol. 15, No. 2, 2016.

Hegenbart, Christine, "Semantic Matters: NATO, Cyberspace and Future Threats," *NATO Defense College Research Paper*, No. 103, 2014.

Hughes, Rex, "NATO in Cyberspace: Digital Defenses," *The World Today*, Vol. 65, No. 4, 2009.

Meelis, Vill, "Guardtime Awarded Contract for Next-Generation NATO Cyber Range," *Guardtime*, February 1, 2017, https://guardtime.com/blog/guardtime-awarded-contract-for-nato-cyber-range.

"National Cyber Strategy of the United States of America," United States of America, 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

"National Security Strategy of the United States of America," United States of America, 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

"NATO breaks ground on IT academy," *NCI Agency*, May 23, 2017, https://www.ncia.nato.int/NewsRoom/Pages/170523-NCI-Academy_groundbreaking_ceremony.aspx.

"New NATO-industry cyber partnerships signed at NITEC18," *NCI Agency*, May 23, 2018, https://www.ncia.nato.int/NewsRoom/Pages/ 180523-IPAs_signature_NITEC.aspx.

Popa, Iulian F., "NATO's Cybersecurity and Defense: Before and After 2014 Wales Summit," *Annals of the "Constantin Brancusi" University of Targu Jiu, Letter*

and Social Sciences Series, No. 3, 2014.

"Prague Summit Declaration", *NATO*, 2002, https://www.nato.int/cps/en/natohq/official_texts_19552.htm.

Shea, Jamie, "NATO Dealing with Emerging Security Challenges?" *Georgetown Journal of International Affairs*, Vol. 14, No. 2, 2013.

Stoltenberg, Jens, "Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defense Pledge Conference," *NATO*, May 15, 2018, https://www.nato.int/cps/en/natohq/opinions_154462.htm.

"Strategic Concept – Active Engagement, Modern Defence", *NATO*, 2010, https://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf.

"The North Atlantic Treaty", *NATO*, 1949, https://www.nato.int/cps/ua/natohq/official_texts_17120.htm.

"Wales Summit Declaration", *NATO*, 2014, https://www.nato.int/cps/ic/natohq/official_texts_112964.htm.

"Warsaw Summit Communiqué", *NATO*, 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

Windrem, Robert, "Timeline: Ten Years of Russian Cyber Attacks on Other Nations," *NBC News*, December 18, 2016, https://www.nbcnews. com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111.

An Assessment of North Korean Cyber Threats and the Republic of Korea's Policy Responses: An Update

Hyeong-Wook Boo

Research Fellow

Center for Security and Strategy, Korea Institute for Defense Analyses (KIDA)

Kyung-Roak Kang

Research Assistant

Center for Security and Strategy, KIDA

Abstract

Recent cyber threats from North Korea and its transformations since 2009 are introduced and analyzed in this present study. There is a clear difference in North Korea's recent behavior in cyberspace, compared to prior years. Currently refraining from continuing any saber-rattling cyber attacks against South Korea and the world, North Korea's recent cyber operation cases are regarded as primarily motivated by financial objectives. This crucial development is relevant to the rapidly transforming geopolitical situation of the Korean Peninsula, and represents a strategic overturn of Kim Jung Un's national strategy. This, in turn, will cause cyberwar logic in the Peninsula to eventually lose its existential rationales in the future. Thus, it is necessary to develop a multidimensional approach towards existing North Korean cyber threats, in both domestic and international policy. Such efforts should include renewing domestic cyber-response systems, securing international cooperation to restrict the mobility of North Korean hackers, and even lifting international sanctions to some extent, in order to provide incentives to discourage North Korea's cyber activities in the pursuit of financial resources.

Keywords*: cybersecurity, North Korean, cyber capabilities, geopolitical situation, international sanctions*

An Assessment of North Korean Cyber Threats

北韓網路威脅評估與大韓民國政策回應：最新觀察

Hyeong-Wook Boo

韓國國防研究院安保戰略研究中心 研究員

Kyung-Roak Kang

韓國國防研究院安保戰略研究中心 研究助理

本文闡述並分析北韓近期網路威脅與 2009 年以來之演變。近年來北韓的網路行為模式與過去存在明顯差異。目前北韓透過網路攻擊對韓國與世界發動文攻武嚇的行為有所節制，其近來網路行動目的多半被認為已轉為金融目標導向。這個關鍵發展與韓半島上快速轉變的地緣政治局勢息息相關，同時也反映了金正恩的戰略轉變。此轉變將使得大規模網路戰爭在韓半島最終失去存在的理由。為了應對新型北韓網路威脅，（韓國）勢必要發展貫穿國內外政策在內的全方位網路政策，包括更新國內網路應變系統、透過國際合作抑制北韓駭客的機動能力，甚至將其納入制裁標準以嚇阻北韓透過網路行動來攫取金融資源。

關鍵詞：網路安全，北韓，網路能力，地緣政治，國際制裁

Introduction

As of December 2018, we are witnessing a renewed strategic environment on the Korean Peninsula, which is unprecedented for those accustomed to the decade-long confrontations between the two Koreas. The South and North Korean leaders met three times in the course of six months, and the world is looking forward to seeing the second US-DPRK summit in a month or two. People around the world are waiting for the remarkable news of North Korea's submission of a denuclearization roadmap to the international community. Suddenly, the advent of permanent peace on the Korean Peninsula seems inevitable.

However, many skeptics still believe that North Korea's announcement of denuclearization is just a show or another deception tactic. According to an official from the United States Department of Defense (DoD), North Korea has made more than five nuclear warheads in 2018, despite the progress of peace talks.[1] Thus, we need to maintain dual perspectives and take a cautious approach in handling the current situation of the Peninsula. This attitude is necessary because concrete results that will ensure peace are not yet in our grasp, despite the burgeoning prospect of peace in the Peninsula. This supports us to support the rationale of delving into North Korean cyber threats assessment without making this case a political issue.

In 2018, however, we have not heard of cyber activities that might have had a huge impact on the military and other means of security. North Korean cyber threats became an important issue last September when the US Department of Justice prosecuted the North Korean hacker, Jin-Hyok Park, for launching several cyber attacks.[2] The FBI field officer's criminal complaint submitted to the US District Court does not deal with his activities in 2018. It concerns Park's activities in the years of 2017, 2016 and 2014.[3]

---

[1] Kube, Courtney and Andrea Mitchell, "North Korea is Still Producing Ballistic Missiles after Summit," *NBC NEWS,* August 1, 2018. https://www.nbcnews.com/news/north-korea/north-korea-still-producing-ballistic-missiles -after-summit-n896331.

[2] The U.S authority has tracked the North Korean hackers' activities with clues detected when the hackers used the G-mail. While the investigation of other hackers that colluded with Mr. Park is still going on, the Interpol reveals the plan for issuing the 'Red Notice (to seek the location/arrest of a person wanted by a judicial jurisdiction)', if asked by the U.S.

[3] Shields, Nathan, "Criminal Complaint (U.S. vs. Park, Jin Hyok)," *US. District Court for*

Meanwhile, cyber threats posed by North Korea became an issue when cyber money began drawing attentions starting last year. Some newspapers printed several articles implicating North Korean hackers for exchanging encrypted cyber money.[4] Those arguments were not validated by authorities, but experts in the cybersecurity field are keeping an eye on the situation. It also has been suggested that some parts of the government may be working on this as well.[5]

In any case, it can be argued that North Korean hackers have been relatively quiet in 2018. While it is possible that the world simply has not uncovered North Korea's hacking activities, North Korea does not seem eager to disrupt the peace-oriented mood on the Peninsula with any hacking attempts. As many commentators have stated, Kim Jung Un wants to obtain a reputation from the world that he is sincere in his participation in the peace talks and that he is trustworthy. From another perspective, analysts have postulated that North Korea may be focusing more on the financial side of its cyber operations than the military and security related side. This speculation reflects a highly plausible scenario because North Korea needs new financial sources to maintain both its economy, and Kim Jung Un's luxurious lifestyle. The regime continues to talk with South Korea, the United States and others, hoping that the economic sanctions will be lifted. However, this presents a struggle, as the international community does not want to lift the sanctions over North Korea until North Korea's denuclearization presents visible progress. Whatever the case may be, we need to carefully look at North Korea's cyber capabilities and assume that it poses a very serious threats until North Korea clarifies its intention to terminate cyber attacks. Thus, for now, we must ensure that the dual stances toward North Korea and North Korean cyber issues be maintained for a while. Under these considerations, in this article, North Korea's activities in cyberspace and its characteristics will be

---

the Central District of California, June 8 ,2018. https://www.justice.gov/opa/press-release/file/1092091/download.

[4] Min-seo Kim, "More Than 7,000 Cyber Warriors in North Korea, Earning 1 Trillion Won Annually," *Segye Ilbo*, November 23, 2017. http://www.segye.com/newsView/20171123005037.

[5] Seon-mok Lee, "US reveals that, North Korea will continue to focus on cyber activities, to secure Funds for the WMD Development," *Chosen Ilbo,* September 10, 2018. http://news.chosun.com/site/data/html_dir/2018/09/10/ 2018091000625.html.

reviewed. In the following section, recent cases of North Korean cyber threats and their major differences from the past will be analyzed in a comparative perspective. Then, South Korea's policy responses including recent developments and limitations will be briefly reviewed. Lastly, policy implications and suggestions will be proposed.

Cases of North Korean Cyber Attacks[6]

In this section, the author of this article argues that the focus of North Korean cyber operations is moving toward profit seeking, contrary to the past motivation of saber rattling cyber attacks. The premise is that North Korea and its cyber strategy is rapidly changing. In 2018, as mentioned above, the North Korean cyber strategy has proved to be less militaristic than before-even though this strategy is still dangerous and poses preponderance of threats to free and safe transactions in cyberspace. While some evaluate that North Korea has reset its national strategy, there is a general consensus that North Korea wants to be seen as a normal country and to claim membership in the international community. This is why Kim Jung Un changed his strategic stance earlier this year. It also seems that the strategic turnover has been reflected in North Korea's behavior in cyberspace. Reviewing the short history of North Korea's cyber provocations will reveal the validity of the argument. To begin, cases of the 2000s will be discussed.

The social discourse regarding cybersecurity has a relatively short history in South Korea. The 7.7 DDoS attacks in 2009 marked a watershed moment in raising the general public's awareness regarding cyber threats posed by North Korea. Compounding traditional security threats with non-traditional threats was a remarkable feature of the 7.7 DDoS attacks. North Korea coordinated cyber-attacks with the second nuclear test on May 2009 and missile launches on the July 4, 2009 and others, with the primary intention of shattering South Korean minds. Similar cyber attacks having occurred after the 7.7 DDoS attacks include the DDoS attack on July 7, 2010. North Korea sank the Cheon-an corvette in March 2010 and scheduled a

[6] Please see Boo, Hyeong-wook, "An Assessment of North Korean Cyber Threats." *The Journal of East Asian Affairs*, Vol. 31, No. 1, 2017, pp.97-117.

cyber-attack after a major military provocation. On April 12, 2011, North Korea caused the paralysis of the Nonghyup Internet banking system. In that month, South Korea and the United States carried out their annual combined military exercises which North Korea had always condemned. On March 20, 2013, about one month after the third nuclear test, North Korea launched the Master Boot Record (MBR) wiper attacks which shut down 32,000 computers of banks and media agencies.[7] North Korea also increased cyber attacks after the fourth nuclear test on January 4, 2016. As many commentators argued, North Korea had deliberately chosen the date of the cyber attack because it wanted to sound an alarm in South Korea. In other words, North Korea seemed to cause psychological damage to the South Korean society by using its cyber capabilities.

In 2014 and 2016, there were many cyber attack cases that were considered serious incidents in military perspectives. It seemed North Korea was trying to prove that it could cause real, physical damage in wartime through cyber attacks. In 2014, there were hacking attempts on Seoul Metro, the city's subway system. North Korea intended to compromise the mass transportation management system which would result in widespread chaos. It also sent an ominous sign to the general public of South Korea, which forecast a transportation disaster to be triggered by a cyber attack. In December 2014, there were cyber-attack attempts against the information system of the South Korean nuclear power plant corporation, Korea Hydro & Nuclear Power (KHNP). North Korea even hacked South Korea's Ministry of National Defense (MND) in 2016. North Korean hackers infiltrated the MND intranet using a malware-implanted USB stick and eventually stole South Korea's War Plan 5027 material. This was an extremely shocking incident because the MND Intranet, which operated separately from the Internet, had seemed highly secure and safe from hacking attempts. There was also a hacking attempt on defense-related corporations in 2016. The hackers stole the maintenance manuals of F-16's, photos of South Korean drone parts, and other sensitive documents. Authorities estimated that 42,600 documents were

[7] Kwang-hyung Cho, "Malicious Code Penetration Aginst Network of KBS, North Korea's Deed." *New Daily,* March 20, 2013. http://www.newdaily.co.kr/site/data/html/2013/03/20/2013032000061.html.

stolen. This was a new phenomenon that once again conveyed an impression of North Korean hackers as being more military-oriented in the purposes of their attack.

Meanwhile, there were different types of North Korean cyber behavior that seemed to have financial motive. These kinds of behavior can be observed from 2015. In 2015, North Korean hackers had penetrated the Vietnamese and Philippino banks. They had created bank accounts that were used as money-laundering accounts for the Bangladesh Bank penetration later in 2016. In February 2016, North Korean hackers infiltrated the Bangladesh Bank and stole USD 81 million. According to a FBI field officer, "Approximately 81 million dollars was routed to accounts in the Philippines, and 20 million dollars was routed to an account in Sri Lanka. But the 20 million dollars sent to Sri Lanka was stopped by the recipient bank." The money sent to the Philippinn bank was laundered in various ways, and this became the largest successful cyber theft from a financial institution.

In Korean history, 2017 will likely be remembered as one of the most dangerous years from the perspective of North Korean military provocations, while being marked as a turning point in North Korean cyber strategies. Kim Jung Un rushed to finish nuclear weapons and intercontinental ballistic missiles (ICBM) developments. On average, there had been a North Korean military provocation once every two weeks. However, in cyberspace, there had not been saber-rattling cyber attacks in 2017, targeting transportation networks, nuclear power plants and Internet banking systems. However, North Korean hackers did launch the Wannacry ransomware attacks and tried to hack crypto-currency markets. Arguably, the primary motivations of those cyber operations were monetary.

When the Wannacry ransomware attacks occurred, the *New York Times* conducted an interview and wrote the following; "Boo Hyeong-wook said the scale of the attack was large enough that it was likely to have been supported on a national level. He also said it would be a logical extension of growing boldness of North Korean hackers to exploit their abilities to raise much-needed funds for the government, which has been starved of cash by

international sanction."[8] A recent FBI complaint submitted to US District Court confirmed that the Wannacry ransomware attack was orchestrated by North Korean hackers, also known as Lazarus. The complaint designated Park, Jin Hyok as a member of Chosun Expo, which is a North Korean company operating in Dalian, China.[9] Chosun Expo is affiliated with the North Korean hacking organization, Lab 110 and is suspected to have launched many cyber attacks across the world, with the intention of obtaining cash for the government at that time. According to Dune Lawrence of *Bloomberg Businessweek*, three Wannacry bitcoin wallets had received 277 payments by May 17, 2017, at a value equivalent to USD 82,000.[10]

North Korean hacker groups, especially Lazarus, have broken into crypto-currency exchanges all over the world. This is a recent development in North Korean cyber operations. Most of these recent North Korean cyber operations concerning crypto-currency are under investigation and the details have yet to come to light. Some of the penetrations known to the public occurred in 2017 and 2018. For example, in June 2017, the Coinrail and Bithumb exchanges were compromised owing to hacking and estimated losses were equivalent to USD 50 million.[11] In September 2017, North Korean hackers seemingly affiliated with the 121 Bureau under the General Bureau of Reconnaissance broke into Coinis, a South Korean crypto-currency exchange and stole crypto-currencies equivalent to about 1.5 million dollars. In December 2017, Youbit, another South Korean crypto-currency exchange was compromised by alleged North Korean hackers, resulting in a loss of crypto-currency worth more than USD 14 million. In January 2018, authorities found malware that had the command

---

[8] Sang-Hun Choe et al, "Focus Turns to North Korea Sleeper Cells as Possible Culprits in cyber attack," *The New York Times,* May 16, 2017. https://www.nytimes.com/2017/05/16/world/asia/north-korea-cyber-sleeper- cells-ransomware.html.

[9] David Sanger and Katie Banner, "U.S. Accuses North Korea of Plot to Hurt Economy as Spy is Charged in Sony Hack," *The New York Times*, September 6, 2018. https://www.nytimes.com/2018/09/06/us/politics/north- korea-sony- -wannacry-indictment.html

[10] Dune Lawrence, "North Korea's Bitcoin Play: Cut off from the hack world economy by sanctions, Pyongyang is looking for ways to get its hands on cryptocurrency," *Bloomberg Businessweek*, December 15, 2017. https://www.bloomberg.com/news/articles/2017-12-14/north-korea-s-bitcoin-play.

[11] *"*North Korea Cyber Activity,*" Recorded Future Insikt Group*, June 14, 2017. https://go.recordedfuture.com/hubfs/reports/north-korea-activity.pdf.

lines to mine Monero, a crypto-currency, and transferred funds to a Kim Il-sung University bank account. In March 2018, Lazarus launched spear-phishing[12] attacks across the world by using Falcon coin accounts which are similar to the Falcon coin of the Turkish crypto-currency exchange. Research presented by McAfee, an international security firm based in California, has revealed that Lazarus reused the code used in previous hackings when attacking Falcon accounts.[13] In August 2018, Lazarus penetrated the Cosmos Bank in India, compromised the alarm system and stole USD 13 million. They created a fake debit card and successfully made ATM deals through which they can transfer money to other places.

Policy Response to North Korean Cyber Threats: A Brief Overview

In review of North Korean cyber activities since 2009, security experts have consistently suggested that the primary feature of North Korean cyber attacks are characterized as an implementation of asymmetric strategy. This strategy provides less-developed countries with scarce resources the opportunity to damage information and communications technology (ICT) environments of developed counterparts at low costs.[14] As South Korea may be at particular risk due to developed ICT, the high frequency of cyberspace usage and immature awareness of cybersecurity among South Koreans, a few attacks on core infrastructure may cause catastrophic confusion in the society.[15] As a world-renowned information technology (IT) giant, these

[12] Spear phishing sends malicious e-mail to a specific person, which infects the computer and takes information when the attachment file is opened.

[13] Jay Rosenburg and Christiaan Beek, "Examining Code Reuse Reveals Undiscovered Links Among North Korea's Malware Families." McAfee, August 9, 2018. https://securingtomorrow.mcafee.com/mcafee-labs/examining-code-reuse-reveals-undiscovered-links-among-north-koreas-malware-families/.

[14] Jong-In Lim et al., "North Korea's Cyber War Capability and South Korea's National Counterstrategy," *The* Quarterly *Journal of Defense Policy Studies,* Vol. 29, No. 4, 2013, p.32. (in Korean)

[15] Hyeong-wook Boo, "Issues of Cyber Security and Policy Directions: Discussions for the Establishment of Defense Ministry's Cyber Policy," *Journal of National Defense Studies*, Vol. 56, No. 2, 2013, p.106. (in Korean)

reasons are precisely why South Korea has been targeted by major North Korean cyber attacks for more than a decade. Moreover, South Korea's increasing network dependency has exposed some system vulnerabilities, despite enhanced societal cybersecurity measures. Networks are compromised due to their own vulnerabilities, compounded by North Korea's improved cyber capabilities. These two factors are not only interconnected, but also expected to trigger devastating societal effects once a cyber attack occurs.

Faced with the abovementioned cases, the South Korean government has developed a variety of policy efforts in the cybersecurity area. The establishment of Cyber Command in 2010 was an important initial measure by the Ministry of National Defense. In order to foster experts in cybersecurity, the government also sponsored the introduction of cybersecurity programs at universities and various public competition events. In 2011, the government announced a Cybersecurity Master Plan, which was significant as it marked the first plan to serve as a foundation for future national cyber -security strategies. The plan, aiming for a thorough defense of national cyberspace from cyber threats, emphasized the specific roles of each ministry, along with their cooperation.

Following these developments, the National Cyber Threat Joint Response Team was established within the National Cyber Safety Center to promote information sharing and multi-level cooperation. Their underlying principles were to achieve early detection of cyber attacks while establishing an essential response system. Importantly, the Plan also included efforts to enhance citizens' cybersecurity awareness throughout society. It proposed to enact "The Information Security Day," a statutory anniversary on the second Wednesday of every July, to raise awareness of cybersecurity and information protection. The plan also promoted private-sector campaigns to protect personal information from zombie personal computers (PC) and strengthening education in information security in primary and secondary schools. However, it has been suggested that palpable effects of these countermeasures in the early 2010's seem to be negligible, likely due to the constant development of cyber threats over time.

These efforts led to the National Cybersecurity Strengthening Plan in

2015, which was proposed following the hacking of the Korea Hydro & Nuclear Power (KHNP) in December 2014.[16] First, the government planned to establish and expand the role of government organizations dedicated to cybersecurity, enabling improvement of security capabilities in central administrative agencies. The Presidential Secretary for Cybersecurity was established, and in May 2015, a meeting was held with the Office of National Security. The aim of this meeting was to gather the National Intelligence Service (NIS), military, police, and senior officials from various government ministries to discuss cyber-attack countermeasures. The government also announced a plan to expand its professional manpower, strengthening its capacity to cope with cybersecurity affairs. At the same time, the government has also been actively sponsoring relevant industries, such as anti-hacking and security technology companies, to maintain major information and communication networks. Lastly, the government revealed a plan to cooperate closely with the international community regarding hacking cyber incidents.

The most recent example, according to the *White Paper for National Information Protection* published in May 2018, is the Office of National Security's designation as the sole control tower of cybersecurity. This is a part of a "five-year plan for state affairs," announced immediately after the Moon Jae-in administration assumed office in 2017.[17] The National Assembly Advisory Planning Committee, which drafted the proposal, announced that the proposal is a part of an "enhancement of the cybersecurity control tower," balancing the organizational capabilities in cybersecurity areas that was once concentrated in the NIS.[18] This settles the controversy over which organization should play the leading role in cybersecurity affairs, while also partially resolving security experts' concern that the NIS was previously overgrown with an information monopoly. Such prevention of organizational inefficiency in cyber countermeasures is consistent with plans specified in the

[16] Sea Min, "Strengthening National Cyber Security Significantly," *Boan News*, March 18, 2015. https://www.boannews.com/media/view.asp?idx=45697&kind=2.

[17] Jae-woon Lee, "The Government's New Cyber Security 'Center' is The National Security Office." *E-Daily,* May 21, 2018. http://www.edaily.co.kr/news/read?newsId=02660086619211216&mediaCodeNo=257&Out LnkChk=Y.

[18] *Ibid.*

Defense Reform 2.0, released on July 2018; this is an expansive initiative to restructure and modernize South Korea's defense capacity.[19] The cybersecurity section of the initiative specified a plan to establish a cyber response team, ensuring an increasingly responsive cyber defense operation. It has been reported that the organization will concentrate on 'cyber operations' after completely abolishing the function of "cyber psychological-operations," the central topic of recent political controversy.

South Korea's responses to North Korean cyber activities have been gradually evolving. However, despite the various efforts undertaken, several experts consistently identify loopholes within the response system, still fragmented and highly complicated, that impact the provision of effective responses in the face of rapidly evolving cyber threats. This problem is aggravated by the fact that the Blue House recently abolished the position of Presidential Secretary for Cybersecurity, which was established in 2015 as part of an organizational restructuring.[20] Moreover, the additional bill responding to North Korean cyber attacks has been pending in the National Assembly for a long time, making active and responsive countermeasures infeasible. It is of little surprise that successive government-wide meetings to discuss countermeasures against cyber threats have ended fruitlessly. This may be due to several reasons, including a lack of adequate legislation and legal basis, as well as the absence of coordination between related organizations. Experts state these problems repeat due to insufficient system management regarding cyber threats.[21] For example, the role of the control tower for cybersecurity has still not been clearly defined, and the division of roles by government agencies remains vague.[22] Another problem is sparse

[19] Sung-young Jang, "How Will 'Defense Reform 2.0 Change South Korea's Defense? A Closer Look at Moon Jae-in's Ambitious Defense Modernization Plan,'" *The Diplomat*, August 27, 2018. https://thediplomat.com/2018/08/how-will-defense-reform-2-0-change-south-koreas-defense/.

[20] Young-dong Son, "Stop Acting! The United States Gives a Red Card to the North Korean cyber attacks." *Choong-Ang Daily*. September 14, 2018. https://news.joins.com/article/22970263.

[21] Hyeong-wook Boo, "An Assessment of North Korean Cyber Threats," *The Journal of East Asian Affairs*, Vol. 31, No. 1, 2017, p.110.

[22] A specific implementation schedule of the plan specified in "A five-year plan for state affairs" and the details of the responsibility sharing among related government organizations still remains unclear.

debate regarding how to share the costs between the public and the private sectors for cybersecurity projects, which is a significant responsibility. No viable plan for how the government should build and develop a flexible regulatory system for cybersecurity has been suggested. The outcome of such shortcomings, combined with the absence of endeavors to forge social consensus on cybersecurity issues, has resulted in reactive measures only, focusing on minimizing damage following an attack taken, rather than any preemptive measures.

Given the above-mentioned situations, responses to cyber threats in South Korea can be evaluated as insufficiently discussed, with limited strategic consideration. Compared to the intensity of North Korea's cyber threats, the South Korean government and the public's interests in cybersecurity are limited. According to the recently published article of Lee et al.,[23] the current national cybersecurity system demonstrates difficulties in preventive detection of cyber attacks from North Korea, which conducts simultaneous attacks on various parts of society. Inconsistent political support for sustainable budget allocation for cybersecurity affairs and nascent efforts to develop international cooperation are other important factors that impede further development. Due to this array of obstacles, vulnerability is still pervasive within the South Korean response system against North Korean cyber threats. In 2013, experts evaluated the cybersecurity system, which was current at the time, by sharing Delphi results representing South Korea's cyber preparedness. The results stated their level of goal sharing, organizational process and culture for cooperation were below average.[24] More recent policy development of cybersecurity does not support much improvement at the time of this article's writing, However, most importantly, the response system needed to be adequately updated to reflect the swift transformation of North Korean cyber activities; this will be discussed in the following section.

---

[23] Yong-joon Lee et al., "The Countermeasure Strategy Based on Big Data against Nor th Korean Cyber Attacks," *The Korean Journal of Defense Analysis*, Vol. 30, No. 3, 2018, p. 445.

[24] Hyeong-wook Boo et al., "A Study on Future Directions of Defense Cyber Policy," *KIDA report,* 2013 (in Korean).

Changing Trends and Policy Implications

There is a qualitative change in North Korea's cyberspace behavior in recent years. A review of the recent behavior of North Korean hackers in cyberspace reveals North Korea is abstaining from launching saber-rattling cyber attacks against South Korea and the world. With recent strategic changes in both the Peninsula and North Korean cyber operations especially in 2017 and 2018, it seems North Korea does not want to be viewed as plotting a future cyber warfare. Cyberwar logic does not match with Kim Jung Un's strategic overturn and does not have solid grounds considering North Korea's behavior in 2018. This situation, in turn, will eventually render cyberwar logic in the Peninsula obsolete in the future, which is an important and radical development.

Interpreting North Korea's intentions requires a review of their radically changed national strategy. Professor Hwang Il-do of the Korean National Diplomatic Academy argued North Korea established a two-year plan for the completion of nuclear weapons and ICBM in 2015.[25] He estimated that North Korea secured ICBM technologies and a RD-250 engine from Ukraine in 2015, and with these technologies, Kim Jung Un became confident that North Korea would eventually obtain the ICBM in less than two years. The reason for establishing this two-year plan, according to Professor Hwang, is due to the presidential election in December 2017 (it was for the impeachment of the former president Park in May 2017).[26] Thus, the North Korean leader thought he could make a deal with the newly elected president regarding his nuclear warheads and ICBMs. North Korea also wanted to aggrandize their nuclear capacities, making the Trump administration interested in dealing with North Korea. In so doing, however, North Korea had to prepare for possible reinforcement international sanctions given their needs to test missile engines and nuclear explosions for the completion of nuclear-tipped ICBMs by the end of 2017.

Evading international sanctions is not an easy task and we percive that North Korea viewed cyber activities as a means of obtaining financial

[25] Il-do Hwang, "North Korea's 'Guam Enemy Shooting' Threat: Intention and Calculation." *Institute of Foreign Affairs and National Security FOCUS*, 2017 (in Korean).
[26] *Ibid.*

resources. It should be noted that, compared to other financial sources such as laborer dispatching, US-dollar forgery, and drug trafficking, cyber operations are not a reliable source of finances. However, the cyber bureau of North Korea and Kim Jung Un's policy orientation can be clearly considered "all-in" for the completion of nuclear weapons and ICBMs. Thus, the cyber bureau should assume any kind of role for the policy. Since they have obtained technologies from Ukraine, locating sources of money to help in furthering Kim's policy became a essential choice. Through this method, they could claim their raison d'etre in the North Korean regime. We think that this candidate scenario has been guiding North Korea's policy transformations in cyber operations.[27]

Though North Korea would not be expected to pose meaningful military threats via cyber, this does not necessarily indicate that North Korea is a reliable and trustworthy player in cyberspace. Following this, evaluation of the danger of North Korea's cyber threats should be provided. North Korea still uses its cyber capabilities in siphoning money from various sources and, by doing this, poses a marked threat in cyberspace. As reviewed earlier, recent cyber activities of North Korean hackers include compromising Internet banking systems, crypto-currency exchanges, e-mail service providers, and other financial systems. If these activities continue in the future, they may bring about a devastating impact on world financial systems and the virtual economy. In some respects, this may be as dangerous as a cyberwar, from a military point of view. The difficulty of cybersecurity is that defenders are much more vulnerable than attackers. Attackers have freedom of choice. Their behavior cannot be detected on time due to attribution issues. Several months of hard work would be needed in confirming who the attackers were and how they completed their mission. Further, North Korea would seek to take advantage of the attacker's merits to the greatest extent.

After the third Inter-Korean Summit, the prospect of complete denuclearization and the establishment of permanent peace in the Korean Peninsula seems more probable than ever. This shift in prospect provides

[27] Anonymous research from LogRhythm Labs posits North Korean Cyber activity for financial resources will continue to escalate in 2018; they speculate the public impact of this will rise as well.

significant incentives for the Kim Jung Un regime to behave properly. Thus, South Korea, and the world, do not need to worry about cyberwar-like provocations in the near future. However, the ability of North Korean hackers to compromise financial systems and other money-making cyber business systems remains a worry. North Korea needs financial resources and the authorities might overlook their cyber warriors' illicit operations. Because of the precise restraints made by international sanctions, North Korea's illicit operations in cyberspace will continue despite peace talks and denuclearization negotiations.

Along with updating domestic policy responses and countermeasures management, two additional efforts can be suggested. First, international sanctions may need to be lifted in accordance with the progress of North Korea's efforts in denuclearization. This should provide breathing room for the North Korean economy, which might alter the incentive calculations of the regime's cyber operations. That is, if Kim Jung Un considers compliance with international norms will bring more profits than illicit cyber operations, there remains no reason to continue cyber hacking for financial resources. Second, interested parties should put joint pressure on North Korea to not employ additional illicit cyber operations. For example, international communities should ask the candidate countries where North Korean hackers freely travel and launch cyber attacks using that countries' cyber infrastructure, to follow regulating measures. These countries include China, South Asian countries, and countries in the Middle East and Africa. China, especially, should take this seriously; cities such as Dandong, Shenyang, Beijing and Shanghai are frequently visited by North Korean hackers and presumably have hosted North Korean cyber operation base camps.

Conclusion

This article analyzes the recent cyber threats of North Korea and discussed its break with past performance. North Korea recently discarded saber-rattling cyber attacks against South Korea and adopted cyber activities mainly driven by financial objectives. These transformations are relevant to the radically changing strategic topology in the Korean Peninsula. Thus, a

new approach is needed for North Korea and its cyber threats. Considering this, South Korea and the international community may need a flexible strategy to tame North Korean cyber threats. For now, lifting some of the international sanctions and reinforcing self-regulations and responsibilities of interested states in cyberspace would be the corresponding way of action to North Korea's strategic change. Meanwhile, President Moon of South Korea ascertained it is not yet known how the results of North Korea's denuclearization will unfold, as he expected a number of turmoil and challenges in the process. In some potential scenarios, the denuclearization process may take longer than initially expected. Thus, South Korea and the international community should continue to monitor possible illicit behavior of North Korean hackers, since, as President Moon stated, it is not yet known how long the process of denuclearization may take. Therefore, a cautious and reserved approach toward North Korea's cyber threats should continue to be taken by both the domestic South Korean and international policy communities.

Bibliography

Boo, Hyeong-wook, "Issues of Cybersecurity and Policy Directions: Discussions for the Establishment of Defense Ministry's Cyber Policy," *Journal of National Defense Studies*, Vol. 56, No. 2, 2013, pp.97-122. (in Korean)

Boo, Hyeong-wook et al., "A Study on Future Directions of Defense Cyber Policy," *KIDA Report,* 2013. (in Korean)

Boo, Hyeong-wook, and Choi, Suon., "Crisis Pattern Change and Its Implication for National Crisis Management System," *Journal of Defense Policy Studies*, Vol. 30, No. 1, 2014, pp.123-152. (in Korean)

Boo, Hyeong-wook, "An Assessment of North Korean Cyber Threats," *The Journal of East Asian Affairs*, Vol. 31, No. 1, 2017, pp.97-117.

Chanlett-Avery, Emma et al., "North Korean Cyber Capabilities: In Brief," *Congressional Research Service Report*, August 3, 2017, https://fas.org/sgp/crs/row/R44912.pdf.

Cho, Kwang-hyung, "Malicious Code Penetration Aginst Network of KBS, North Korea's Deed," *New Daily,* March 20, 2013, http://www.newdaily.co.kr/site/data/html/2013/03/20/ 2013032000061.html.

Choe, Sang-Hun et al., "Focus Turns to North Korea Sleeper Cells as Possible Culprits in cyber attack," *The New York Times,* May 16, 2017, https://www.nytimes.com/2017/05/16/world/asia/north-korea-cyber-sleeper-cells-ransomware.html.

Comfort, L. K, "Rethinking Security: Organizational Fragility in Extreme Events," *Public Administration Review*, Vol. 62, No. 1, 2002, pp.98-107.

Han, Hee, "Cyber Threat by North Korea: Capability and Intention,", presented at the 6th RINSA-KAS Joint International Conference (2016).

Hwang, Il-do, "North Korea's 'Guam Enemy Shooting' Threat: Intention and Calculation," *Institute of Foreign Affairs and National Security FOCUS,* 2017. (in Korean)

Jang, Sung-young, "How Will 'Defense Reform 2.0 Change South Korea's Defense? A Closer Look at Moon Jae-in's Ambitious Defense Modernization Plan," *The Diplomat*, August 27, 2018, https://thediplomat.com/2018/08/how-will-defense-reform-2-0-change-south-koreas-defense/.

Kim, Min-ho, "An Assessment of North Korean Cyber War Threats," *KIDA Presentation*, 2016. (in Korean)

Kim, Min-seo, "More Than 7,000 Cyber Worriers in North Korea, Earning 1 Trillion Won Annually," *Segye Ilbo*, November 23, 2017, http://www.segye.com/newsView/20171123005037.

Kube, Courtney and Mitchell, Andrea, "North Korea is Still Producing Ballistic Missiles after Summit," *NBC NEWS*, August 1, 2018, https://www.nbcnews.com/news/ north-korea /north-korea-still-producing-ballistic-missiles-after-summit-n896331.

Lawrence, Dune, "North Korea's Bitcoin Play: Cut off from the hack world economy by sanctions, Pyongyang is looking for ways to get its hands on cryptocurrency," *Bloomberg Businessweek*, December 15, 2017, https://www.bloomberg.com/news/ articles/2017-12-14/north-korea-s-bitcoin-play.

Libicki, Martin, C., *Cyberdeterrence and Cyberwar* (Santa Monica, California: RAND, 2009).

Lim, Jong-In, et al., "North Korea's Cyber War Capability and South Korea's National Counterstrategy," *The Quarterly Journal of Defense Policy Studies,* Vol. 29, No. 4, 2013, pp.10-45. (in Korean)

Lee, Seon-mok, "US reveals that, North Korea will continue to focus on cyber activities, to secure Funds for the WMD Development," *Chosen Ilbo,* September 10, 2018, http://news.chosun.com/site/data/html_dir/2018/09/10/2018091000625.html.

Lee, Jae-woon, "The Government's New Cybersecurity 'Center' is The National Security Office," *E- Daily,* May 21, 2018, http://www.edaily.co.kr/news/read? newsId=026600 8661921 1216&mediaCodeNo=257&OutLnkChk=Y.

Lee, Yong-joon et al., "The Countermeasure Strategy Based on Big Data against North Korean Cyber Attacks," *The Korean Journal of Defense Analysis*, Vol. 30, No. 3, 2018, pp.437-454.

Mahnken, G, Thomas, "Cyberwar and Cyber Warfare," in Lord M., Kristin and Sharp, Travis ed(s)., *America's Cyber Future: Security and Prosperity in the Information Age,* Vol. 2 (Washington, DC: Center for a New American Security, 2011).

Min, Sea, "Strengthening National Cybersecurity Significantly," *Boan News*, March 18, 2015, https://www.boannews.com/media/view.asp?idx=45697&kind=2.

"North Korea Cyber Activity," *Recorded Future Insikt Group*, June 14, 2017, https:// go.recordedfuture.com/hubfs/reports/north-korea-activity.pdf.

Rosenburg, Jay and Beek, Christiaan, "Examining Code Reuse Reveals Undiscovered Links Among North Korea's Malware Families," *McAfee*, August 9, 2018, https:// securingtomorrow.mcafee.com/mcafee-labs/examining-code-reuse-reveals-undiscover ed-links-among-north-koreas-malware-families/.

Sanger, David and Banner, Katie, "U.S. Accuses North Korea of Plot to Hurt Economy as Spy is Charged in Sony Hack," *The New York Times*, September 6, 2018, https:// www.nytimes.com/2018/09/06/us/politics/north-korea-sony--wannacryndictment.html.

Shields, Nathan, “Criminal Complaint (U.S. vs. Park, Jin Hyok),” *U.S. District Court for the Central District of California,* June 8, 2018, https://www.justice.gov/opa/press-release/file/1092091/download.

Son, Young-dong, “Stop Acting! The United States Gives a Red Card to the North Korean cyber attacks,” *Choong-Ang Daily*, September 14, 2018, https://news.joins.com/article/22970263.

撰稿規則

一、 分節標題：文章之大小標題以「壹、一、(一)、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。如引註係轉引自其他書籍或論文，則須另予註明，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，以民國〇年〇月〇日或西元〇年〇月〇日表示；英文依序以 month, day, year 表示。

五、 專書

（一）中文書籍：作者姓名，《書名》（出版地：出版者，年月），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。

六、 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.

七、 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：（略）

八、 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.

九、 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.

十、 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.

十一、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.

十二、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.

十三、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.

十四、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〉，《網站名稱》，網址。

（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. 報導：Author’s full name, “Title of the article” , *Name of the Newspaper*, Date Month Day, Year, URL.

十五、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。）

十六、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）所有文獻依據中文、英文、其他語文先後排列。

（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。

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「國防安全研究院」，並發行本刊。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，為整合國防安全研究能量，以提供專家與學者專業諮詢與討論平台為宗旨。

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、六、九、十二月出刊。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，本刊編著並對來稿有刪改權。

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 stellar.shu@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