台灣戰略研究

Taiwan Strategic Studies

第二卷 第一期 Volume 2, Issue 1
2026 年 1 月

目 次
CONTENTS

TAIWAN Thinktank 台灣智庫 出版

郭建中發行人發刊詞

英國戰略研究學者勞倫斯．弗里德曼（Lawrence Freedman）於《戰略：一部歷史》一書中指出，戰略是一門「創造權力的藝術」（the art of creating power）。他進一步闡明，若缺乏可供評估與檢驗的戰略，無論是軍事行動、企業投資或政府施政，都將流於漫無目的的嘗試，亦難以獲得社會支持並持續推進。因此，戰略的核心不只是方向的宣示，而在於能否透過評估與檢驗，確保其具備可行性、正當性與持續推動的可能。

當前地緣政治競逐加劇、國際秩序持續動盪未歇，民主與威權體制的對峙早已不再停留於理念層次，而是具體反映在軍事與外交、安全、經濟、科技與社會治理等多重面向。台灣身處印太戰略核心，是國際政治現實中不可忽視的重要支點，如何在劇烈變動的國際環境中維持戰略定力，考驗的是整體社會的集體判斷能力。

《台灣戰略研究》自創刊以來，即以回應此一世代的課題為使命，嘗試從台灣自身的結構條件與現實處境出發，系統性思考國家總體戰略的可能路徑。台灣總體戰略環境，從來不是單一面向加以概括，而是外交安全、產業布局、科技發展、社會韌性與民主治理彼此交織，共同形塑高度動態且複雜的戰略總體。《台灣戰略研究》持續透過跨領域、長期且累積性的研究，回應全球結構性變遷所帶來的挑戰，逐步深化具前瞻性的國家戰略視野。

台灣智庫作為連結知識生產與公共議題關懷的政策研究平台，致力於促進學術研究與實務運作之間的對話。《台灣戰略研究》承繼此一精神，定位於學術論述與政策關懷間辯證思考，搭建得以反覆交流、持續深化的公共論述平台，為台灣社會提供更為穩健且厚實的戰略理解基礎。

在此誠摯邀請關心台灣未來發展的學者與實務工作者，持續以研究與論述參與國家方向的集體思考。期盼《台灣戰略研究》能在動盪的時代中，成為台灣累積戰

略知識、深化公共理性、回應時勢挑戰的重要平台，為國家長遠發展貢獻堅實的思想力量。

財團法人台灣智庫董事長

李漢銘總編輯發刊詞

當前國際政經秩序正經歷自冷戰後最深刻的重組，美中戰略競爭持續加劇，歐洲因俄烏戰爭而重新調整安全架構，印太地區則在結盟、科技與軍力競逐中快速變化。科技安全、供應鏈治理、網路空間規範與民主韌性已成各國戰略競爭的新戰場；國際法、地緣政治與科技治理三者交織，使全球安全議題呈現出前所未見的複雜性。台灣作為民主前線，深受地緣壓力與科技變局交互影響，更需要在這場全球秩序轉換中，建立具有自信且具前瞻性的戰略論述。

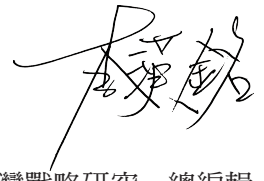
《台灣戰略研究》自創刊以來，即致力於提供一個結合學術深度與政策視野的跨域平台，使台灣的戰略分析能夠回應國際環境的快速動態。本期三篇文章，正是立基於此問題意識，從歐洲觀點、科技治理與國際法規範三個面向，展現了台灣在多重戰略壓力下所需具備的理解能力與應對視角。

周冠竹博士後研究員則以印尼與菲律賓為案例，剖析兩國如何在 5G 安全化與去安全化之間尋求科技與外交的平衡，凸顯新興科技已成中型國家制定避險策略的關鍵槓桿。林昕璇副教授以國際法視角探索網路敵意行為的灰色地帶，提醒台灣面對跨境網路威脅時，必須在法制、治理、歸責標準與國際合作上全盤布局，才能提升數位國安韌性。沈有忠教授從德國內政與歐洲戰略的變化切入，解析「紅綠燈聯盟」與「黑紅聯盟」在對中政策上的調整，反映歐洲在俄烏戰爭後重新定位中國角色的現實，亦呈現民主國家在安全、經濟與價值之間的權衡。

三篇研究不僅分別回應了台灣所面臨的不同風險面向，更共同呈現出一個清晰訊號：台灣所面對的安全挑戰已是跨域、複合且長期性的，其策略思考亦必須跨越單一領域的傳統框架。從歐洲政策轉向，到東南亞科技避險，再到網路法律戰的深化，台灣都需要在國際秩序快速變動時，培養足夠的理解能力與政策調適空間。

《台灣戰略研究》將持續作為連結國內外知識社群的平台，深化不同領域對台灣戰略處境的對話，使本刊不僅記錄當前的變局，也能為未來的政策規劃與國家戰

略提供思考。期盼本期內容能為讀者帶來新的視野與啟發，誠摯邀請各界學者與實務工作者持續關注、投稿與交流，以集體智慧厚實台灣的戰略能量。



「台灣戰略研究」總編輯
台灣智庫「戰略與安全研究中心」總召集人
國立臺灣科技大學產學創新學院講座教授

《台灣戰略研究》第二卷第一期
2026 年 1 月　1 頁～ 31 頁

Taiwan Strategic Studies, Vol.2 No.1
January 2026, pp.1-31
DOI: 10.30249/tss.202601_2(1).0001

5G 安全化與去安全化下的國家科技避險策略：印尼與菲律賓的比較

周冠竹 *

摘　要

在美中科技競爭與 5G 安全化趨勢下，次級國家如何在發展與安全間取得平衡，成為當代國際關係的重要課題。本文聚焦於印尼與菲律賓兩個東南亞次級國家，探討其面對中國 5G 科技擴張時所採取的科技避險策略。儘管兩國對中國的安全威脅認知差異甚大，前者傾向務實合作、後者則強化與美國安全連結，然在 5G 基礎建設上卻均未排除與中國廠商合作，呈現政策趨同現象。本文以「安全不確定性」與「國家科技能力」為分析軸，建立二乘二矩陣，將兩國分別歸類為「成本導向合作」與「多元化避險」類型。研究發現，科技能力與產業結構對國家避險空間產生關鍵約束，即便對中國安全疑慮升高，若缺乏替代技術與供應鏈資源，國家仍可能選擇務實合作以維持基礎建設推進。本文補充避險理論對科技政策情境的適用性，並指出避險行為不僅是外交回應，也反映政權正當性、制度能力與地緣政治壓力之間的綜合調適結果。

關鍵詞：5G 科技、美中競爭、避險、印尼、菲律賓

* 中央研究院政治學研究所博士後研究員。Email: kuanchuchou@as.edu.tw
收件：2025 年 6 月 3 日；一修：2025 年 7 月 3 日；二修：2025 年 7 月 21 日；通過：2025 年 7 月 21 日；接受：2025 年 12 月 15 日。

Technological Hedging under 5G Securitization and De-securitization: A Comparison of Indonesia and the Philippines

Kuan-Chu Chou**

Abstract

Amid intensifying U.S.-China technological competition and the securitization of 5G, how secondary states balance development goals with national security concerns has become a critical issue in international relations. This article examines Indonesia and the Philippines, two secondary states in Southeast Asia, to analyze their hedging strategies in response to China's 5G expansion. Despite significant differences in their threat perceptions toward China, both countries have adopted similar policies of maintaining technological openness, including cooperation with Chinese suppliers such as Huawei and ZTE. Using a two-dimensional framework based on "security uncertainty" and "technological capability," the study categorizes Indonesia as a case of cost-driven cooperation and the Philippines as one of diversified hedging. The findings suggest that structural constraints, particularly weak industrial capacity and limited technological alternatives, narrow the policy space for these states, making pragmatic engagement with China a rational choice even under geopolitical pressure. This study contributes to hedging theory by demonstrating its applicability in the domain of technology policy, showing that hedging is not only a foreign policy strategy but also a function of domestic legitimacy, institutional capacity, and the politics of technological interdependence.

Keywords: 5G Technology, Hedging, US-China Rivalry, Indonesia, Philippines

** Postdoctoral Researcher, Institute of Political Science, Academia Sinica. Email: kuanchuchou@as.edu.tw

壹、前言

2024 年 2 月，印尼最大電信商 Telkomsel 與華為簽署合作協議，推動第五代行動通訊技術（Fifth-Generation Mobile Communication Technology, 以下簡稱 5G）升級與節能科技發展。而早在 2022 年，華為早與菲律賓最大電信商 Globe 合作，在偏遠地區部署綠色節能基地臺。儘管兩國在 5G 政策上皆展現對中國科技企業的開放態度，並積極引入華為技術支援基礎建設，但在安全戰略認知上卻存在顯著差異。印尼對中國的安全疑慮相對溫和，僅在納土納群島（印尼語：Kabupaten Natuna）海域維護主權利益，但未將中國視為國家安全威脅；反觀菲律賓，面對日益頻繁的南海對峙與中國海警行動，已公開將中國視為區域安全挑戰，並強化與美國的軍事合作。然而，這種「政治認知分歧、技術政策收斂」的現象反映出東南亞國家的務實邏輯：即便面對區域安全壓力，科技部署仍以經濟可行性、技術可得性與基礎建設需求為核心考量，顯示國安與技術政策在實務上可能出現功能性脫鉤。

印尼與菲律賓的 5G 政策展現出，即便兩國面對中國的安全威脅感知有所不同，仍選擇採取相似的「避險」（hedging）策略，維持對中國科技的務實開放。馬來西亞學者郭清水（Cheng-Chwee Kuik）對東南亞國家避險行為的研究指出印尼與菲律賓皆屬「輕度避險」（light hedging）型國家：一方面接受中國的經濟與科技合作，另一方面在安全上維持一定程度的防範與多邊接觸（Kuik, 2008, 2021, 2024）。這種策略的核心目標是維護政策彈性與自主性，在中美競爭之間爭取最大空間。然而，當前避險策略正面臨兩項日益嚴峻的挑戰。首先，隨著美中對抗升高，雙方對第三國「選邊表態」的期待與施壓加劇，次級國家（secondary states）可操作的空間正在縮減。[1] 其次，5G、人工智慧（artificial intelligence，簡稱 AI）等新興科技模糊了「經濟合作」與「國家安全」的界線，使原本透過功能性切割來維持平衡的策略變得困難。印尼與菲律賓雖持續強調科技政策的「非政治化」，但實際上這種模糊地帶正

[1] 本文所稱「次級國家」係指國際體系中不具備改變體系結構能力，亦非主要強權之國家。儘管這類國家在區域層級可能擁有一定的經濟與軍事實力，但在面對美中科技競爭等結構性議題時，其影響力仍然有限，無法主導體系發展方向。本文選用「次級國家」而非「小國」，主因在於研究對象如印尼與菲律賓，雖具一定規模，惟在美中 5G 競爭背景下，仍屬於無法形塑競爭格局的從屬行為者，故更適合歸類為次級國家。

是未來風險與矛盾累積的關鍵所在。

本研究將採用比較個案研究法，深入分析印尼與菲律賓對中國 5G 科技的政策態度與戰略考量。儘管兩國在南海問題上的立場與對中國的安全認知明顯不同，菲律賓對中國具更高的防備與對抗傾向，而印尼則較為低調與務實。但在 5G 部署上卻展現高度相似的政策取向，皆未排除華為與中興等中國設備供應商，並強調開放市場與經濟合作的重要性。這種現象顯示，兩國的政策選擇在很大程度上受到國內經濟結構與工業能力的制約，特別是在資通訊設備、基礎建設融資與技術支援方面對中國仍有高度依賴。透過比較分析，本研究將回應郭清水「避險理論」的核心主張，說明即便安全威脅認知不同，國家仍可能因發展需求與制度能力的限制，採取相似的「輕度避險」策略。本研究將進一步檢視在美中科技競爭升高與國安邏輯滲入經濟領域的背景下，避險策略如何在實踐中產生張力與調整空間。[2]

貳、5G 安全化與避險策略

一、對中國 5G 安全化與去安全化

對中國 5G 科技安全化鑲嵌於美中競爭結構下，2018 年 9 月，美國白宮發布《國家網路戰略》（*National Cyber Strategy of the United States of America*），首次明確將 5G 通訊與資通訊基礎建設視為國家安全核心，並強調須確保 5G 供應鏈的安全性。同時，文件將中國視為主要戰略對手之一，批評其透過資通訊技術進行經濟間諜與影響力滲透，標誌著美國 5G 政策的安全化轉向與對中國科技實力的系統性防範（The White House, 2018）。這份文件不僅將 5G 視為下一代通訊基礎建設的核心，更標誌著美國將新興科技「安全化」（securitization），即視其為攸關國家安全的戰略領域，需由國家主導、管控與防衛。

「安全化」概念由 Ole Wæver 首次提出，即表示當政治菁英或政策制定者將某

[2] 美國企業在 5G 產業中主要聚焦於晶片設計與軟體標準（如高通、博通），並非基地臺與回傳網路等設備製造的主要供應者。印尼與菲律賓之所以缺乏與美國企業的直接電信合作，反映的是其在硬體供應鏈中的角色限制，並非政策上的刻意排除。美方對全球 5G 布局主要透過政策倡議與技術標準影響間接實現，本文聚焦設備合作，故未深入展開。

一議題定性為「安全問題」時，即透過語言將其移入安全領域，從而正當化動用軍事、法律以及排除程序等非常手段來應對該議題。Buzan 等人（1998）指出：

> 對執政者而言，安全意味著將某項議題自常規政治程序中提出，超越原有的政治遊戲規則，將其定義為例外狀態中的生存威脅，藉此形塑對政治的懷疑，甚至將其置於政治之外。（p. 23）

Buzan 與 Wæver 等人的論述指出，安全化的本質並非源於客觀威脅，而是透過執政者與觀眾（audience）之間的互動所建構出的社會過程。當執政者以語言行動（speech act）將某議題定性為「生存威脅」，即進行一種將議題從常規政治轉化為安全議題的政治操作。此過程能否成立，並非取決於該議題本身是否具備實質危險，而在於觀眾是否接受這一威脅框架（Buzan et al., 1998; Wæver, 1993）。

5G 具備高頻寬、低延遲與大規模連接等技術特性，使其成為智慧製造、遠距醫療與無人載具等關鍵應用的基礎建設，並與半導體製造、邊緣運算（edge computing）與系統整合等高科技產業高度耦合，構成未來數位工業體系的核心（European Telecommunications Standards Institute, n.d.）。正因其深度嵌入於現代經濟與社會運作的關鍵節點，5G 本身的技術特性賦予其高度戰略敏感性，也成為國家安全論述得以展開的物質基礎。美國自川普政府（Trump Administration）以來，正是利用這一特性推動 5G 的「安全化」敘事。例如美國司法部 2019 年公布的起訴書，華為與其美國子公司被控共謀竊取商業機密、7 項電信詐欺以及妨礙司法等 10 項罪名，其中涉及竊取 T-Mobile 測試設備設計與激勵員工蒐集競爭對手機密資訊。而美國智庫蘭德公司（RAND Corporation）則直接將中國 5G 設備與國家安全風險直接連接，指出華為不僅涉嫌竊取美國企業商業機密，更配合中國《國家情報法》強制配合情報任務（Gonzales et al., 2022）。除了對中國 5G 設備潛在資安風險的不信任外，美國政府與智庫進一步指出，中國在 5G 標準必要專利（Standard Essential Patent）與關鍵供應鏈環節上的優勢，正逐步轉化為對全球通訊標準制定的主導權，從而對美國在科技競爭中的結構性優勢構成威脅（Kahata, 2020; The White House, 2020; U.S. Department of State, 2019）。美國政府不僅透過調查與制裁華為等企業來

因應其可能的情報與技術滲透行為，也藉由政策工具遏止中國技術體系在全球擴張。與此同時，民間智庫如蘭德公司以及戰略與國際研究中心（Center for Strategic & International Studies）亦強調中國企業在專利布局、低價競爭與供應鏈整合上所形成的戰略性滲透能力，呼籲建立「可信賴 5G 生態系」（Gonzales et al., 2022; Lewis, 2018）。這些官方政策與民間研究的共識，構成一套有系統的「5G 安全化」敘事框架，將中國 5G 科技視為不僅是資安風險，更是制度性與地緣政治挑戰。

在此論述架構下，美國不僅封鎖華為進入本國市場，並發起「潔淨網路」（Clean Network）倡議、推動盟友排除中國設備，同時支持「開放無線接取網路」（Open Radian Access Network，以下簡稱 Open RAN）等替代性技術架構，試圖在安全可信的前提下重塑全球通訊技術供應鏈（Kim et al., 2023）。如同 Friis 與 Lysne（2021）所指出，5G 的物質特性與安全化話語之間形成互為前提的關係。正是這種技術與敘事的交織，使美國的政策得以在全球推動對中國科技企業的圍堵，並將供應鏈重組正當化為一項安全戰略，而非單純的經濟或技術選擇。Harwit（2024）澳洲與日本皆迅速接受並實踐美國所主張的 5G 安全化敘事，原因不僅在於兩國長期依賴美國的安全承諾，亦與雙邊對中關係的惡化密切相關。自 2016 年起，澳中與日中關係分別因間諜疑慮、政治干預、歷史爭議與區域安全議題趨於緊張，進一步強化對中國科技企業的不信任。此外，兩國均具備由本土或歐洲廠商替代華為設備的技術與產業條件，使其得以在不犧牲通訊品質與網路部署進度下，實施排除中國供應商的政策選項。

5G 的安全化反映出科技特性並非中立，而是受主觀認知與政治脈絡影響。美國基於資料主權與基礎建設風險，將中國 5G 設備視為國安威脅，推動技術標準的「安全化」敘事。然而，多數開發中國家因本身科技能力有限、仰賴中國資金與設備、並追求快速數位發展，對此持相反態度，傾向將中國 5G 視為可控資源而非風險，進而透過「去安全化」（de-securitization）敘事，將其重新包裝為成本效益與自主性的象徵。Heeks 等人（2024）則指出中國在全球南方的數位投資涵蓋從基礎設施到平臺應用的整體技術堆疊（technology stacks），逐步建構出區域性的科技生態系（ecosystem）。這使當地政府與企業在標準、資料與服務上形成對中國的依賴，產生路徑依賴效應，強化中國在區域影響力的籌碼。Arnold（2024）針對 42 個撒南非洲（sub-Saharan Africa）國家的研究指出，基於現實科技發展以及對中國資金

需求，撒南非洲國家傾向與中國建立資通訊科技領域合作關係。除此之外，由於傳統以來對西方國家「安全化」敘事的負面經驗，撒南非洲國家並不信任美國所主導的安全化敘事。van der Westhuizen（2024）則指出中國對全球南方國家在疫苗、醫療器材以及經濟發展等方面的援助外交對 5G 科技「去安全化」敘事有顯著成效。

總體而言，5G 安全化敘事並非純粹源於技術風險的客觀認定，而是深受國際權力結構與國家處境影響的政治建構。美國將 5G 納入國安議題，透過語言行動將中國科技描繪為「生存威脅」，並要求盟友排除中國設備。然各國對此敘事的接受與否，取決於其在美中競爭中的相對位置與利益考量。澳洲與日本因對美安全依賴與中關係惡化，接受並實施排中政策；而多數全球南方國家則基於發展需求、資金依賴與技術可近性，選擇去安全化，將中國 5G 視為合作機會。此一現象凸顯，安全化能否奏效，端賴敘事是否契合一國的國家利益與國際結構定位。

二、5G 安全化敘事下的避險策略

對次級國家而言，選擇中國 5G 科技並不意味著對中國安全威脅上扈從（bandwagoning），而是對於中國問題上的避險。有別於平衡（balancing）與扈從，避險是次級國家基於不確定下的風險管理策略。在中國經濟崛起以及美國對區域安全承諾下降的歷史背景下，東南亞次級國家在區域安全中面臨威脅來源不明確以及支援者不可靠等雙重風險。因此次級國家無法採取明確的平衡或扈從策略，只能透過多元、模糊、具備互補性的避險行動來保留政策空間與主動性（Jackson, 2014; Kuik, 2008, 2021）。而 Ciorciari（2019）認為避險是對潛在但不確定的威脅的回應策略，目的在於避免過早選邊站隊以保持政策彈性，同時爭取國家利益與預防損失。

避險研究指出，次級國家由於外交政策的首要目標是維持政權正當性與內部穩定。因此他們在面對外部風險時，會依據本國的民族政治、經濟結構、選舉壓力與政治敘事需求進行政策調整。避險因而成為一種內外風險交錯下的「雙重回應」策略，一方面避免捲入大國對抗，另一方面避免在國內被貼上「親中」或「選邊」的政治標籤（Kuik, 2008）。而 Ciorciari（2019）則認為避險策略若無法兼顧內部合法性，也可能反遭反對派質疑其搖擺不定或不具原則性，導致政治風險升高。換言之，避險不只是外交選項，更是一種維持政權穩定工具，其成效與風險取決於外部壓力

與國內正當性資源之間的平衡能力。簡而言之，對次級國家而言，避險是一種在外部威脅未明與支援者不可靠的雙重不確定性下，兼顧外交彈性與政權穩定的風險管理策略，其核心不在於選邊，而在於維持主動性與正當性空間。

誠然，避險作為一種中次級國家因應外部不確定性與內部正當性壓力的風險管理策略，其本質是一種回應型行為，而非具備改變國際體系結構的能力。當大國競爭加劇、國際秩序朝向對立與排他性邏輯發展時，次級國家原本依賴的模糊策略與多邊操作空間將遭到壓縮。此時，避險不再是一種穩定選項，而轉變為一種逐漸難以維繫的戰略奢侈品。Korolev（2019）從體系結構的角度補充與修正了郭清水的對東南亞國家避險策略選擇的預設。他指出，不確定性本身是一個體系條件的變量，取決於大國之間競爭的強度與清晰度。當大國競爭呈現模糊與混合互動時，次級國家具有操弄空間；但當競爭升高、對抗加劇，次級國家將面臨更強的壓力而被迫選邊，避險空間隨之壓縮。Korolev 對避險研究的修正將避險研究與新古典現實主義（neoclassical realism）理論進行連結，導入體系與單元間互動關係。Marston（2024）則指出，次級國家的避險策略是國內因素對國際體系變化的反應。具體而言，國內的戰略文化、歷史經驗、領導人感知與官僚結構等，會「過濾」外在壓力，如大國競爭與安全威脅，從而形塑國家的對外政策選擇。新古典現實主義對避險理論的修正，強調國內政治變數在塑造外交政策中的關鍵作用（Rathbun, 2008; Rose, 1998）。即便國際體系的結構條件發生變化，國家仍可能基於維繫自主性與鞏固統治正當性的內在需求，選擇採取避險策略，以在外部壓力與內部穩定之間取得平衡（Kuik & Lai, 2025）。

三、分析框架

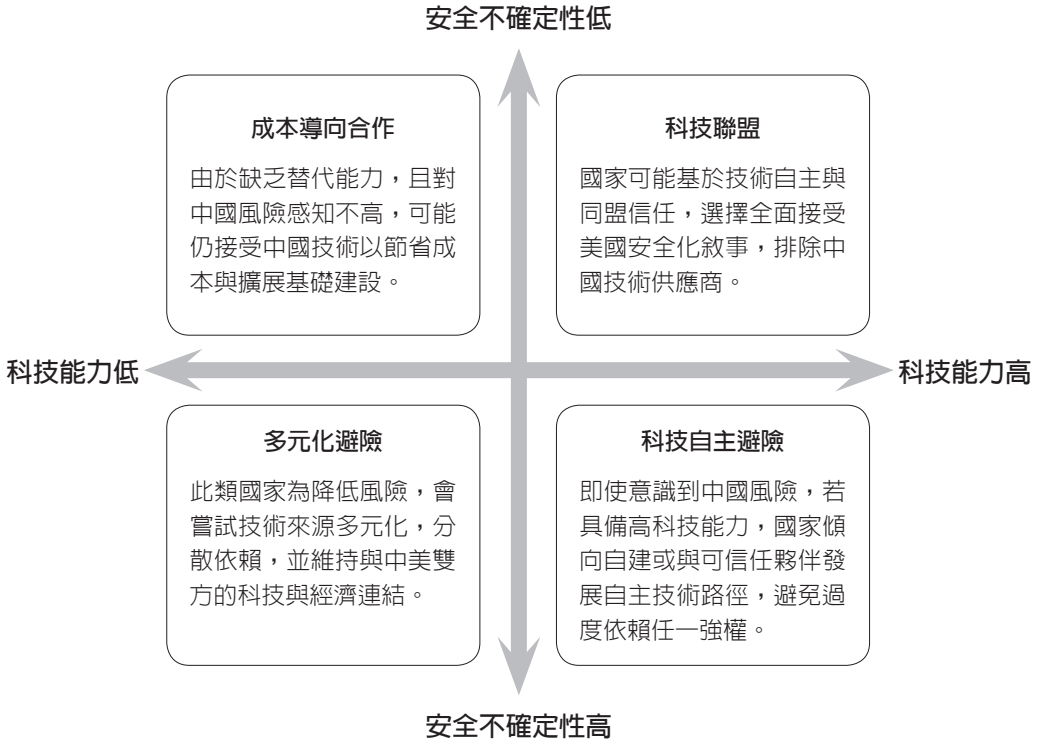
在美中戰略競爭的背景下，5G 科技已從單純的通訊技術演變為戰略性資產，並被雙方納入各自的安全化敘事。美國將中國 5G 科技視為潛在的國安威脅來源，並強調供應鏈與中國脫鉤（de-coupling）與去風險（de-risking）；中國則強調其科技供應的可靠性與自主性，將其納入數位絲路與「一帶一路」的延伸工具。對於次級國家而言，是否響應美國的 5G 安全化訴求，並不單純取決於意識形態或同盟關係，而是受到兩個關鍵變數的制約：其中一個變數是對安全的不確定性；其二是自身在高科技領域的能力與資源。

安全不確定性是美中競爭格局下體系結構轉變。隨著美中戰略競爭日益升溫，國際體系正從冷戰後的美國單極霸權，逐步邁向一種尚未穩定成形的雙極對抗格局。在此過渡時期，權力結構的重新分布與制度規則的模糊性相互交織，催生出前所未有的安全不確定性。這種不確定性不僅源自軍事實力的相對變化，更深層地體現在國際行為者對大國意圖、行為邏輯以及安全承諾可信度的模糊認知（Foulon, 2015; Lobell, 2009）。對多數次級國家而言，如何判斷美國的安全承諾是否堅實可靠，以及中國的崛起是否將轉化為具體的安全威脅，構成當前最具挑戰性的戰略判斷任務。不同區域國家的地緣位置與安全安排，影響其對安全風險的感知與回應空間。部分國家如日本與澳洲等美國條約盟邦，雖在地理上直接面臨中國擴張壓力，但因長期與美國建立穩固的軍事聯盟關係，面對區域安全壓力時具備較高的防衛穩定性與制度信任，因此安全不確定性較低。而地理距離較遠的拉美與非洲國家，則因距離中國軍事影響範圍較遠，對其擴張意圖的安全風險感知相對有限，安全不確定性較低。安全不確定性較低的結構下，次級國家較可能採取安全聯盟以平衡外部威脅，或扈從大國與獲取經濟利益。相較之下，東南亞與印度洋周邊國家處於美中勢力交會的前線，在承受雙重壓力與不確定風險的情況下，更傾向於採取避險策略以維持外交空間與戰略彈性（Kuik, 2008; Kuik & Lai, 2025）。

另一個影響 5G 避險策略的因素則為國家科技能力。科技能力是國家重要的權力稟賦之一，衡量國家將自然資源、人力資源轉化為產能與創新的能力（周冠竹，2024）。郭清水指出，避險策略是國家能力與統治合法性共同交織的結果，其中國家能力包涵調整外交與科技政策的治理能力，尤其是跨部會協調、科技理解與風險管理的能力（Kuik, 2024）。因此科技能力成為國家是否能進行靈活避險的關鍵因素。作者認為，在美中科技競爭構成的制度性壓力下，科技能力成為次級國家維繫主權與策略自主性的關鍵資產。科技能力越強，次級國家越能在數位基礎建設、技術標準以及國際標準制定（standard setting）中保有選擇空間；反之，科技能力薄弱國家，越依賴外部體系科技輸入，即使意識到潛在安全風險，也傾向採取「去安全化」的政策敘事與公共論述，以維繫發展所需的技術與資金來源。這種「去安全化」不代表完全信任外部技術，而是基於結構性資源不足與替代方案缺乏的務實選擇（Arnold, 2024; Heeks et al., 2024; van der Westhuizen, 2024）。

在此基礎上，作者將安全不確定性與科技能力進行比較，製作出 2x2 矩陣（圖1）。第一象限國家具備一定科技能力，能自主選擇基礎建設與技術標準。由於與美國維持穩定的安全聯盟與制度化合作，足以平衡中國崛起所帶來的安全風險，使其政策選擇更具自由度。此類國家傾向依據民主制度與資安原則，主動排除中國技術，並參與開放型科技聯盟。第二象限為成本導向合作，這類國家為低科技能力以及低對中安全風險。這類國家缺乏本土科技研發與製造能力，需依賴外國技術服務與基礎建設。同時，這些國家對中國崛起下的安全威脅感知較低，因此不排斥引進中國科技，將中國科技與服務視為低成本選項。第三象限國家面臨高度安全不確定性，卻缺乏足夠的科技能力，無法建立自主技術體系。由於缺乏研發資源與制度性安全保障，這類國家多採取務實的避險策略，透過引入多元化供應商分散風險，維

圖 1
次級國家選擇



資料來源：作者自行設計。

持與美中雙方的經濟與科技連結，以避免過度依賴任一強權體系。第四象限國家因缺乏與美國之間穩健的安全合作關係，對中國科技滲透具高度風險感知，但因具備一定程度的科技能力，傾向透過本土研發與可信賴夥伴合作，積極建立具可控性的數位基礎建設與技術體系。這些國家追求的不只是降低依賴，而是在戰略與制度上掌握科技自主性，以維護長期的國家安全與政策主動權。

綜合上述分析，美中科技競爭對次級國家構成的不僅是選邊壓力，更是制度性結構下的能力考驗。5G 科技作為戰略性資產，其選擇不再只是市場導向的技術決策，而是涉及國家安全、技術治理與外交布局的高度政治化抉擇。次級國家的策略選擇深受兩大因素影響：一為其對安全不確定性的感知，二為本身所具備的科技能力。本文所提出的矩陣模型顯示，科技能力與安全環境的交互作用，決定了國家是在成本導向合作、科技聯盟、多元化避險或科技自主避險之間做出抉擇。科技能力愈高、愈有可能在強權競爭中維持主權與策略彈性；反之，科技依賴程度愈高者，則愈傾向接受外部體系輸入，難以擺脫被動處境。在本文的後半段，作者將以印尼與菲律賓兩國作為個案，探討次級國家科技避險行為。最後在研究限制上，本文研究範疇聚焦於圖 1 所列之第二與第三象限類型，分別對應印尼與菲律賓兩國的政策實踐。第二象限「成本導向合作」與第三象限「多元化避險」在東南亞地區最具代表性，且具備充分資料來源，足以進行深入比較。至於第一與第四象限，雖具理論意義，亦有若干具代表性的國家個案，惟多數不屬於本文聚焦的東南亞區域，故未納入本篇分析範疇，將留待後續跨區域研究進一步探討。

參、印尼對中國 5G 政策

一、印尼－中國關係去安全化

在美中戰略競爭與區域格局動盪的背景下，中國與印尼之間的雙邊關係展現出「從安全化到去安全化」的明顯轉變。歷史上，印尼與中國的外交關係曾長期受到兩大結構性矛盾所制約：其一是關於印尼華人社群的國內族群衝突，其二是針對南海主權的地緣爭議。然而，進入 21 世紀後，雙方在應對這些敏感議題時，逐漸發展出一

種務實、風險可控的政策基調，透過刻意壓低衝突敏感度的「去安全化敘事」（de-securitization narrative），為雙邊在經濟、科技與地緣合作開啟新局（Sriyanto, 2018）。

印尼華人與土著之間的結構性矛盾可追溯至殖民時期。荷屬東印度政府以「分而治之」策略將華人集中於城市經濟職能，形成殖民經濟的中介族群，導致華人相對優勢與土著的邊緣化並存（Oostindie & Paasman, 1998）。華人社群的「中國連結」更在清末以降的民族主義與僑務運動中進一步被政治化，殖民政府與後來的印尼國家機器皆傾向將華人視為潛在的不忠代理人（Lasker, 1946; Liu, 2014; Vandenbosch, 1930）。冷戰時期，這一「安全化」敘事強化為對中國介入內政的疑懼，導致蘇哈托政府長期中斷與中共外交關係，並對華人施以文化與經濟上的制度性壓抑（Mozingo, 1961）。真正的轉折出現在 1998 年蘇哈托下臺與「黑色五月暴動」之後。中國政府在印尼社會動盪中採取克制立場，避免高調干預，並以「華裔印尼人」替代「華僑」的語言策略，象徵中國對印尼主權的尊重與對非干涉原則的堅持（Sukma, 2009; Zha, 2000）。這一外交節制不僅避免激化當地反華情緒，也為雙邊關係的重啟鋪平道路。自哈比比（Bacharuddin Jusuf Habibie）以降，印尼政府陸續解除對華人文化活動的禁令，瓦希德總統（Abdurrahman Wahid）與梅家瓦蒂總統（Megawati Sukarnoputri）更進一步將春節列入國定假日，象徵族群治理邁向去政治化，而中印關係亦隨之重返正軌（He, 2008）。

與此同時，在南海問題上，印尼對中國「九段線」主張始終持否定立場，堅持其對納土納群島海域的主權與專屬經濟區不容挑戰（Office of Assistant to Deputy Cabinet Secretary for State Documents & Translation, 2020）。然而，面對中國於南海的擴張行動，印尼政府並未公開激烈反制，而是選擇透過模糊性外交與合作框架進行管理。2024 年印尼總統普拉博沃（Prabowo Subianto）與中國簽署《海上合作諒解備忘錄》，即便內容未觸及法律約束力，仍引發外界對印尼在主權立場上是否出現模糊化的疑慮。印尼外交部隨後強調立場未變，惟在缺乏強硬反制機制下，仍呈現出「戰略模糊」與「低調抗議」並存的政策特徵。此一合作基礎最為明顯的體現在經貿與科技層面。自 2000 年起，中印雙方簽署多項合作協議，涵蓋衛生、海運、能源、稅收與智慧財產權等多元領域，展現雙邊關係從政治敏感轉向制度化合作的歷程（表 1）。自 2013 年起，中國成為印尼最大貿易夥伴，雙方形成資源－工業

產品互補的高度依賴結構。至 2023 年，印尼對中國出口總額達 707 億美元，自中國進口則為 627 億美元，享有 80 億美元的貿易順差（The Observatory of Economic Complexity, n.d.）。

表 1

印尼－中國雙邊協議

條約名稱	領域	簽署時間	條約生效時間
中華人民共和國衛生部和印度尼西亞共和國衛生部關於衛生合作的諒解備忘錄	科技	2000.02.23	2000.02.23
中華人民共和國衛生部和印度尼西亞共和國衛生部關於衛生合作的執行計劃	科技	2000.02.23	—
中華人民共和國政府和印度尼西亞共和國政府海運協定	經濟	2001.06.05	—
中華人民共和國政府和印度尼西亞共和國政府關於對所得避免雙重徵稅和防止偷漏稅的協定	稅收	2001.11.07	2003.08.25
中華人民共和國政府和印度尼西亞共和國政府關於合作打擊非法林產品貿易的諒解備忘錄	經濟	2002.12.18	2002.12.18
中華人民共和國政府和印度尼西亞共和國政府關於加強基礎設施建設和自然資源開發領域合作諒解備忘錄	經濟	2005.04.25	2005.04.25
中華人民共和國政府和印度尼西亞共和國政府關於擴大和深化雙邊經濟貿易合作的協定	經濟	2011.04.29	2011.04.29
中華人民共和國工業和資訊化部與印度尼西亞共和國工業部工業與技術合作諒解備忘錄	科技與智慧財產權	2011.04.29	2011.04.29
中華人民共和國政府和印度尼西亞共和國政府關於加強禁毒合作的諒解備忘錄	科技	2012.03.23	2012.04.23
中華人民共和國政府與印度尼西亞共和國政府關於探索與和平利用外層空間的合作協定	科技與智慧財產權	2013.10.02	—
中華人民共和國政府和印度尼西亞共和國政府高層經濟對話第一次會議紀要	經濟	2015.01.26	2015.01.26
《中華人民共和國政府和印度尼西亞共和國政府關於對所得避免雙重徵稅和防止偷漏稅的協定》議定書	稅收	2015.03.26	2016.03.16
《中華人民共和國政府和印度尼西亞共和國政府關於對所得避免雙重徵稅和防止偷漏稅的協定》諒解備忘錄	稅收	2015.03.26	—

資料來源：作者整理自中華人民共和國外交部（無日期）。

儘管上述發展展現出合作深化，但不可忽視的是，這樣的去安全化策略同樣來自於印尼自身科技與軍事能力的限制。印尼尚缺乏強化海上軍事威懾的能力，也無足夠技術資本建立完整的數位主權。即便印尼對中國在南海的軍事擴張與科技輸出具風險認知，卻因結構性能力限制，傾向將政治與主權議題「去安全化」處理，以避免升高衝突成本，進而維持發展合作與外交彈性。總結而言，中國與印尼關係的演變過程說明，開發中國家在面對強權崛起與地緣風險時，若缺乏對等的安全與科技能力，往往傾向透過去安全化敘事管理敏感議題，維持合作空間與主權彈性。這不僅是務實的外交選擇，也反映了在多極化國際秩序中，次級國家如何以有限資源在戰略風險與發展機會之間尋求平衡。

二、印尼 5G 發展狀況

2022 年，印尼政府正式將 5G 網路發展納入國家關鍵基礎建設規劃，視其為推動數位經濟與產業轉型的核心動能。然而，儘管政策層面展現高度重視，實際推進過程中仍面臨兩大結構性挑戰：首先是高昂的 5G 基礎建設成本，包含頻譜取得、基地臺部署與網路升級等均對電信業者形成沉重負擔；其二，印尼國內 5G 應用尚未普及，終端設備不足與消費者需求尚未成形，導致市場採用意願偏低，進一步抑制企業投資意願。這些因素交織，使印尼雖有政策企圖，卻在基礎設施擴展與商業模式落地上進展緩慢，形成「政策驅動－市場回應不足」的落差。

印尼在推動 5G 通訊網路建設的過程中，面臨基礎設施不足與行政管理碎片化的雙重挑戰。由於光纖網路建設進度緩慢，全國光纖滲透率僅約三成，再加上地方政府之間缺乏統一的許可制度與收費標準，導致電信公司在進行基地臺部署時成本高昂、效率低落。儘管近年來技術革新使得許多開發中國家能夠「跳躍式發展」，優先推動無線通訊網路，避免大規模鋪設有線設施的資本支出，但 5G 的技術特性本身卻對寬頻網路基礎設施提出了更高要求。特別是其強調的低延遲、高頻寬特性，使得基地臺間的通訊必須依賴穩定且高速的光纖回傳網路（backhaul）。因此，在缺乏完善光纖骨幹的情況下，即使建設 5G 基地臺，整體網路效能也無法發揮其應有的水準，使 5G 建設難以達到應有水準（Forge & Vu, 2020; Rahman et al., 2021; Sawad et al., 2023）。

直至 2025 年，印尼光纖網路普及率僅 30%，在面臨通訊網路基礎建設不足的情況下，印尼面臨 5G 通訊基礎建設建置緩慢問題，僅 2% 的普及率遠遠低於新加坡、馬來西亞與越南。為解決光纖網路建設不足與行政管理破碎化所導致的高昂 5G 建設成本，印尼政府正積極推動制度層面的整合，以提升治理效率並促進跨層級協調。

首先，政府聚焦於簡化並統一「通行權」（Right of Way, RoW）制度。由於各地在光纖布建過程中收費標準、程序許可與審查機制大不相同，導致企業布建光纖成本居高不下。為此，中央政府提出「一站式協議」（One-Stop Agreement）機制，並建議降低租金與行政門檻，同時訂定統一的服務水準協議，以減少不確定性並加快建設流程。其次，針對印尼全國超過 70 項互不相容的地方性法規，資訊與通信部（印尼語：Kementerian Komunikasi dan Digital, KOMINFO）主張由中央統籌建立統一指導原則，協助地方政府調整現行不合時宜或互相衝突的政策（Ministry of Communication and Information et al., 2023, p. 16）。這種中央－地方協作架構，將有助於營運商在多地同時推進布建作業。第三，印尼亦強調推動基礎建設共構制度。過去各業者為自建設施，常在同一路段架設多根電線桿與纜線，不僅成本高昂，也造成市容混亂與公共安全疑慮。為此，政府推動共構電線竿（Pole Sharing）、地下管道共構（Duct Sharing）等開放既有基礎建設，促進資源整合與投資效率。整體而言，印尼政府疊床架屋的管理制度以及基礎建設的重複投資使得 5G 建設面臨高昂行政成本，不利於大規模科技基礎建設投資（Ministry of Communication and Information et al., 2023, p. 31）。

在制度整合之外，印尼政府試圖引進新興技術解決光纖網路基礎建設不足問題。首先在技術層面，政府與產業界合作推廣數位快速光纖配線系統（digital quick optical distribution network, DQ-ODN）與預接式光纖（Pre-connected fiber）「即插即用」型的快速布建技術降低光纖網路建置門檻。傳統光纖布建仰賴專業熔接技術與高昂施工成本，難以大規模推廣；而預接式技術則無需專業人力，即可在短時間內完成布線，尤其適用於「光纖到戶」（fiber to the home, FTTH）與「光纖到房」（fiber to the room, FTTR）等家庭與企業場景。這種布建方式不僅能大幅縮短施工時間，也有助於降低整體成本，使營運商更具投資誘因（Ministry of Communication

and Information et al., 2023）。其次，印尼政府以蘇拉卡達市（Surakarta）作為 Giga City 示範點，[3] 與華為公司攜手打造 Solo Technopark 數位園區。該園區內部建置完整 FTTR 網路架構，並針對教育、智慧醫療與中小企業數位化進行應用場景測試。蘇拉卡達的實證經驗不僅作為當地發展的驅動力，也成為全國其他城市複製推廣的標竿。這類公私協力機制顯示，數位基礎建設若能結合技術支援與地方治理創新，將更具可行性與永續性。

最後，政府亦透過《印尼數位願景 2045》（*Indonesia Digital Vision 2045*, VID 2045）制定長期量化目標，作為全國推進數位城市的政策指引。根據規劃，至 2045 年，光纖家戶覆蓋率將達 98%，所有無線基地臺均將以光纖連接，固定寬頻下載速度目標提升至 5Gbps，並建成 200 座 Giga City。這些中長期目標展現出印尼政府推動數位基礎建設的堅定決心與政策主導力。面對基礎設施落後與行政協調困難等挑戰，政府透過示範城市、創新技術導入與制度改革，打造具備可擴展性與可複製性的建設模式。這些作為說明印尼並非僅止於應對現況瓶頸，而是積極塑造支撐數位經濟與智慧社會的長期戰略格局。

三、印尼科技避險政策

自中國於 2013 年提出「一帶一路」倡議以來，印尼即成為中國在東南亞地區最重要的合作夥伴之一。2014 年，印尼國營電信商 Telkomsel Indonesia 與中國華為海洋網絡（Huawei Marine）簽署合作協議，啟動第三路海底光纖電纜（3rd Route Submarine Cable）升級計畫，鋪設連接爪哇（Java）、蘇門答臘（Sumatra）與加里曼丹（Kalimantan）等主要島嶼的第三條國內骨幹海底光纖網路（Offshore Energy, 2014）。該項目不僅因應印尼數位化進程下對高速通訊的日益需求，也標誌著中國企業首次參與並主導印尼數位基礎建設工程，象徵印尼與中國基礎建設合作基礎。

除了骨幹光纖網路升級，印尼在 5G 回傳網路上也積極與外國參與合作，以提升國內數位基礎建設建置。回傳網路是 5G 網路中關鍵基礎建設，負責連接基地臺

[3] Giga City 是指具備「全光纖網路覆蓋」的城市，能提供十億位元（Gigabit）的高速通訊服務。該架構由 Giga Government、Giga Campus、Giga Society 以及 Giga Home 四大支柱組成，以響應《2045 印尼數位願景》（*2045 Digital Indonesia Vision*）目標（Asosiasi Penyelenggara Jaringan Telekomunikasi, 2023）。

與核心網路，支撐高速率與低延遲服務。光纖回傳具高頻寬與穩定性，適合城市與高需求場域；微波回傳則適用於偏鄉或臨時部署。在缺乏高速回傳網路建設情況下，5G 高速傳輸與低延遲的特性將效能難以發揮。然而與骨幹光纖網路由華為參與不同，Telkomsel 在回傳網路上採取多元化的合作方式，由中國、芬蘭、瑞典與澳洲等廠商參與（表 2）。

表 2
印尼電信的國際合作

廠商	國家	合作對象	合作內容
華為	中國	Telkomsel, XL Axiata	光纖回傳（fiber backhaul）與微波回傳（microwave backhaul）設備
中興通訊	中國	Telkomsel, XL Axiata	海事行動通訊設備
愛立信	瑞典	Telkomsel	E-Band 與 V-Band 等多頻段回傳設備與天線
Nokia	芬蘭	Telkomsel	企業私有網路
澳洲電信	澳洲	TelkomTelstra	企業私有網路

註：TelkomTelstra 為澳洲電信與 Telkomsel 成立之合資公司。
資料來源：作者整理自 Hetting（2018）、Huawei（2015）、Santoso（2025）。

印尼在推動全國 5G 網路發展的過程中，首先面臨的重大挑戰來自於其地理與行政條件。作為世界上島嶼最多的國家之一，且近半數人口居住於農村地區，印尼的光纖寬頻基礎建設在鋪設成本上極為高昂。此外，地方政府之間缺乏統一的基礎建設標準與共構政策，導致重複投資普遍，行政協調成本居高不下，使整體建設進度與效能受到嚴重制約。

在此背景下，中國華為提出一套涵蓋骨幹與接取層的完整解決方案，進一步鞏固其在印尼電信市場的主導地位。根據印尼通訊與資訊部與澳大利亞戰略政策研究所資料，華為目前在印尼擁有約 70% 的市占率，不僅主導城市間的光傳輸網路（Optical Transport Network, OTN）建設，更提供低成本且易於部署的光纖鋪設技術。其「數位快速光纖分布網路」為預接式、免熔接系統，無需高技術門檻的現場施工，即可完成光纖布建，顯著降低技術人力需求與鋪設成本（Ministry of Communication

and Information et al., 2023; Santoso, 2025）。與此同時，瑞典的愛立信（Ericsson）則是另一家參與印尼 5G 回傳網路建設的主要外商。不同於華為同時部署光纖與微波回傳系統，愛立信的策略則聚焦於與 Telkomsel 與 XL Axiata 兩大電信商合作，建置多頻段微波回傳網路與天線設備。對於尚未普及光纖骨幹的地區，微波回傳方案提供了一種相對靈活且成本較低的替代方案。儘管如此，由於華為在近年積極擴張，愛立信的市占率自 2016 年接近 50% 快速下滑至 2020 年的約 10%，直到 2023 年才略有回升（Santoso, 2025）。

不論是在威權統治時期，還是民主化之後，經濟成長始終是歷任印尼總統施政的核心目標。佐科威（Joko Widodo）執政期間，則更進一步將「以基礎建設帶動經濟成長」作為政策主軸，積極推動高速公路、鐵路、港口以及數位基礎設施等重大建設計畫，期望藉此促進區域連結、吸引投資並擴大國內市場（Antara News, 2024）。然而，印尼在基礎建設薄弱、工業製造能力有限與通訊技術人才不足等多重結構性限制下，政策選擇面臨現實掣肘。特別是面對地理破碎、島嶼分散與區域發展落差等挑戰，印尼政府與企業在推動 5G 等先進通訊建設時，往往須在成本、可行性與速度之間權衡，進而形塑出當前「技術混合、供應商多元、光纖與無線並行」的發展路徑。

印尼選擇華為作為 5G 與光纖基礎建設的主要合作夥伴，反映出其在成本控制、工業製造能力有限與基礎建設條件不足等現實約束下的務實選擇。儘管外界對中國企業的安全疑慮持續存在，印尼政府仍在關鍵數位基礎建設領域與華為保持合作，顯示其對技術可及性與建設效率的優先考量。然而，印尼同時也與瑞典愛立信維持合作關係，特別是在微波回傳網路與部分區域基地臺建置方面，展現出避免在戰略基礎設施上過度依賴單一國家的避險意圖。這種策略不僅體現在企業層級的選擇，也反映在其國際戰略姿態中：一方面與中國維持友好關係，另一方面透過與西方技術供應商的合作，保持在科技基礎建設上的靈活性與戰略平衡。印尼此種「雙重避險」（double hedging）的政策安排，有助於在國際競爭與地緣政治不確定性中維持自主空間。

肆、菲律賓對中國 5G 政策

一、菲律賓對中安全化敘事

與印尼對中國的顧慮主要來自國內族群問題不同，南海主權爭議是菲律賓對中國安全顧慮的核心。儘管菲律賓從未承認中國對南海九段線的主權聲索，但在 2012 年黃岩島事件前，雙方多維持克制。2002 年，中國與東協簽署《南海各方行為宣言》（*Declaration on the Conduct of Parties in the South China Sea*），雖無法律約束力，仍有效控管區域緊張。2005 年更與越南、菲律賓啟動《聯合海上地震調查協議》（*Joint Maritime Seismic Understanding*），惟未獲菲律賓國會支持，2008 年終止。2010 年後，中國海上實力迅速擴張，加劇東南亞憂慮。2012 年黃岩島對峙使中菲矛盾升高，至 2023 年雙方圍繞島礁與專屬經濟區頻頻衝突。在此背景下，菲律賓的避險策略深受總統個人信念與背景影響。不同總統依其政治合法性需求採取截然不同的對中路線，在合作、對抗與聯盟之間擺盪（Nguyen & Tok, 2025）。

2010 至 2016 年間，時任菲律賓總統艾奎諾三世（Benigno Simeon “Noynoy” Cojuangco Aquino III）推動多邊主義以抗衡中國，主張透過國際法與多邊機制維護主權，拒絕雙邊談判。他將政策轉向歸因於兩因素：其一是對前任總統艾若育的反貪腐承諾，後者推動的中菲合作案被指涉不透明與主權讓渡；其二是中國自 2010 年起將南海列為「核心利益」，並加速建軍，破壞區域權力平衡（De Castro, 2014）。外交上，艾奎諾強調與東協合作推動具法律約束力的《南海行為準則》，安全上則強化與美國軍事聯繫，簽署《強化防務合作協議》（Enhanced Defense Cooperation Agreement, EDCA），並擴大聯合軍演，提升嚇阻能力。

菲律賓對中採取強硬外交策略在 2016 年杜特蒂（Rodrigo “Rody” Roa Duterte）上臺後有所轉變。由於 2012 年中菲黃岩島（Scarborough Shoal）衝突時，杜特蒂執政達沃市（Davao City）為中國首要制裁區域。中國制裁壓力使杜特蒂認為艾奎諾對中強硬不利地方經濟。達沃市市長的個人經驗使杜特蒂選擇對中國擱置主權爭議、強調和平發展，試圖換取中國投資。不僅淡化南海仲裁案結果，更積與中國進行經貿合作。盼引進基礎建設資金支持“Build, Build, Build”計畫。然而中國承諾

多未落實，多項合作因預算與法規問題停擺；且 2019 年牛軛礁撞船事件等衝突激發反中情緒，使杜特蒂政策逐步回調，轉向有限平衡。儘管杜特蒂對美國持懷疑態度，甚至揚言終止《訪問部隊協議》（*The Visiting Forces Agreement*），但菲美軍事合作實質穩定。美方持續提供情報與軍事支援，特別在如馬拉維圍城等反恐行動中發揮關鍵作用（BBC, 2017）。此外，菲律賓軍方與美軍長期制度化合作，包括聯演、訓練與人員交流，使軍方堅持維繫與美國的戰略關係（De Castro, 2016, 2017, 2018）。

由於中國在南海的軍事擴張對菲律賓構成直接且持續的主權與安全威脅，菲律賓政府難以透過與中國的雙邊合作來有效降低衝突風險，轉而倚賴與域外國家，深化安全合作以進行戰略平衡。安全壓力使得中菲關係難以穩定制度化，雙邊協議的數量與合作深度遠不如中國與印尼間的合作模式，相較之下，菲律賓的避險空間受到結構性區域衝突限制，對中合作難以擴展至制度層次以降低安全化敘事（表 3）。

表 3
中國－菲律賓雙邊經貿條約

條約名稱	領域	簽署時間	生效時間
中華人民共和國商務部與菲律賓共和國貿工部投資署關於派遣中國投資諮詢專家的諒解備忘錄	投資貿易	2011.08.31	2011.08.31
中華人民共和國外交部與菲律賓共和國外交部關於加強合作的諒解備忘錄	政治	2011.08.31	2011.08.31
中華人民共和國政府與菲律賓共和國政府關於海關事務的互助協定	經濟	2010.04.23	2010.04.23
中華人民共和國衛生部與菲律賓共和國衛生部關於衛生合作的協議	衛生	2008.10.09	
中華人民共和國商務部與菲律賓共和國國家經濟發展署、貿易工業部關於建立經濟合作工作組的諒解備忘錄	經濟	2007.01.15	

資料來源：中華人民共和國外交部（無日期）。

總結而言，與印尼採取制度化與去安全化策略不同，菲律賓面臨的是更為直接且持續升高的安全威脅，核心在於南海主權爭議。自 2010 年以來，中國將南海視為核心利益並持續擴張海上實力，特別是在 2012 年黃岩島事件之後，中菲關係進

入高度對抗階段，頻繁衝突延續至 2020 年代。相較於印尼以維持自主與技術多元為核心的避險策略，菲律賓對中政策更具不穩定性與可變性，深受總統個人背景與政權合法性訴求影響。因此，與印尼相較，菲律賓所面對的中國威脅更加明確與迫切，其對中避險策略也更具政治波動性，反映出區域中次級國家在結構性壓力下所採取的多變回應模式。

二、菲律賓電信發展政策

與印尼採取由國家主導的 5G 發展模式不同，菲律賓政府在電信政策上明顯偏向市場導向，並未規劃由國家統籌的 5G 建設計畫。政府主要透過釋出頻譜、簡化行政程序，以及推動立法來創造有利的市場環境。其中最具代表性的制度改革，包括《開放資料傳輸法案》（*Open Access in Data Transmission Act*, S.B. No. 2146）與《行政命令第 32 號》（*Executive Order No. 32*）。前者致力於拆除資料傳輸產業的進入門檻、鼓勵設施共用與基礎建設開放；後者則簡化了電信設施興建的許可流程，授權各級政府協助加速部署，並支持共用電信塔政策（Macanan Palace, 2023; Senate of the Philippines, 2023）。在此架構下，主要電信業者如 Globe Telecom、Smart Communications 與 DITO Telecommunity，皆依據自身資源與策略，獨立推動 5G 基地臺與回傳網路建設。然而，缺乏中央統籌與統一技術規範的發展模式，也導致電信基礎建設管理破碎、重複投資嚴重。各業者傾向自行鋪設電線桿、地下管道與光纖路徑，導致同一路段可能存在多組桿件與線纜，造成資源浪費、城市景觀破壞與維修困難。雖然政府已意識到這些問題並嘗試透過立法與行政手段改善，但在缺乏強制性標準與執行機制的情況下，法令效果有限。若中央政府無法進一步統整規劃、落實監管與推動設施共用制度，菲律賓的 5G 與寬頻網路升級將持續受到基礎設施碎片化與制度效能不足的制約。

在菲律賓的 5G 基地臺部署過程中，成本效益始終是電信業者挑選供應商的首要考量。由於缺乏由政府主導的統一建設計畫，主要電信商如 Globe Telecom、Smart Communications（PLDT 子公司）以及 DITO Telecommunity 均採自籌資金、自行決策的方式推動 5G 網路發展。在設備採購方面，各業者普遍傾向選擇價格合理、建置效率高的方案，以最大化資本使用效益。Globe 與 Smart 自 4G 時代即大

幅採用華為基地臺設備，進入 5G 階段後延續既有供應鏈邏輯，華為因而成為其升級網路的首選夥伴。早在 2019 年，Globe 就宣布與華為簽署合作協議，預計投入 12 億美元建置 5G 設備與高速連線服務，並率先推出東南亞第一個商用 5G 寬頻服務（Morales, 2019）。在這種結構下，華為與中興通訊憑藉其具競爭力的價格與快速部署能力，在菲律賓市場占據領先地位。特別是 DITO Telecommunity，作為中資中國電信與本地企業 Udenna 合資成立的第三大業者，[4] 其 5G 網路幾乎全面採用華為與中興方案（Morales & Lema, 2020）。2023 年，DITO 推出一項強調低價與高效的 Home 5G 預付服務，入門套裝價格僅 1,990 披索，30 天內可享不限流量的 5G 連線，突顯其在成本控制與設備選擇上的策略優勢（DITO, 2025）。

然而，這種高度依賴中國供應商的策略也引發資安與政治風險的疑慮。美國國務卿蓬佩奧（Mike Pompeo）公開警告菲律賓政府，若持續使用華為的 5G 設備，可能對美菲軍事合作構成風險。他指出，華為的設備可能被中國政府用於間諜活動，並強調美國將重新評估與使用華為設備國家的情報共享與軍事部署安排。蓬佩奧發言強調美國對於盟友使用中國電信設備的安全疑慮。他提到，華為可能是中國情報機構的「特洛伊木馬」，使用其設備可能導致敏感資訊被竊取（Reardon, 2019）。為了在成本效益與政治風險之間取得平衡，部分電信業者採取「混合供應鏈策略」，即在基地臺建設階段使用華為或中興的設備，但在核心網路與回傳網路層則改採 Nokia、NEC 等非中國供應商。此外，菲律賓政府也開始探索 Open RAN 技術，以降低對單一供應商的依賴。2024 年，美國國際開發總署（United States Agency for International Development, USAID）與菲律賓大學迪里曼分校（University of Philippines Diliman）合作，在菲律賓建立了首個 Open RAN 實驗室，旨在促進本地電信業者對該技術的研究與應用（Gamba, 2024）。

總體而言，菲律賓在 5G 基地臺部署上雖展現出快速擴張的能力，但其背後也隱含著供應鏈依賴、資安監管與國際政治壓力交織的複雜現實。未來是否能逐步建構出技術多元、相容性高又具政治韌性的電信網路架構，將是菲律賓能否有效因應地緣科技競爭的重要指標。

---

[4] DITO Telecommunity 是由菲律賓 DITO 控股公司（DITO Holdings）以及中國電信所成立的合資公司，DITO 控股持有 60% 股份，中國電信持有 40%。

三、菲律賓科技避險政策

菲律賓的 5G 政策清楚展現出在「經濟利益」與「國家安全」之間的雙重避險策略。一方面，政府採取市場導向立場，未對中國廠商如華為與中興設限，使其憑藉價格優勢與快速部署能力，廣泛參與 5G 基地臺建設。特別是在缺乏政府補貼與整體規劃的情況下，中國供應商成為主要電信業者如 Globe、Smart 與 DITO 的首選，有助於降低資本支出、縮短建設時程，以及加速網路覆蓋。另一方面，面對來自美國對中國設備資安風險關切，菲律賓政府與業者則在回傳網路與核心設備層導入多元供應策略。2023 與 2025 年，菲律賓分別與以色列及日本簽署涵蓋資訊安全與通訊基礎設施的合作備忘錄，前者聚焦於個資保護與資安治理，後者則強調 5G 建設、網路韌性與可信供應鏈的推動（Ministry of Internal Affairs and Communications, Japan, 2023; The Privacy Protection Authority, 2025）。

在此背景下，菲律賓業者與政府逐步發展出「回傳與核心網路多元化」的策略，在接取層使用華為等中資設備的同時，於回傳與核心層導入 Nokia、NEC 等非中系供應商，以降低系統性依賴與潛在安全風險，形成一種務實的平衡架構。儘管菲律賓在 5G 基地臺建設上高度依賴中國廠商，特別是華為與中興，反映出對成本與部署效率的強烈重視，但在回傳網路的建設上，則呈現出明顯不同的策略樣態。具體而言，菲律賓的回傳網路建設展現出「技術分層、多供應商、地理分散」的特徵，體現出業者與政府在成本效益、技術可行性與政治風險之間所進行的綜合權衡。在技術層面，大城市與高密度地區傾向採用光纖回傳，以支撐高速、大容量的資料需求；而在地形複雜或偏遠島嶼地區，則依賴微波或衛星回傳作為替代方案。供應商選擇上，除了中資廠商外，也廣泛導入來自 Nokia、日本電器（NEC）、賽勒根（Ceragon）、吉萊特（Gilat）等多國設備商，降低對單一技術來源的依賴風險，亦回應來自美國與其他盟國對資安的擔憂。此外，不同區域由不同本地承包商負責系統整合與現地布建，反映出地理分散與地方治理制度對建設方式的影響（表 4）。

表 4

菲律賓回傳網路建設

廠商	國家	合作對象	合作內容
Nokia	芬蘭	Globe	升級 BNG 架構以強化光纖回傳網路
華為	中國	DITO	提供光纖回傳網路設備
中興通訊	中國	DITO	光纖回傳網絡
Ceragon	以色列	Smart	微波回傳網路
NEC	日本	Globe	提供微波 P2P 鏈路與備援方案
Gilat	以色列	Globe	偏鄉地區衛星與微波混合傳輸解決方案

資料來源：作者整理自 Athavale（2011）、Gilat Satellite Networks（2015）、INQUIRER.net（2025）、Morales（2019）、Telecom Review Asia（2025）。

Nokia 與菲律賓最大電信商 Globe Telecom 合作建設光纖回傳網路，目的是強化 Globe 在高用戶密度區域的寬頻容量與網路穩定性。Nokia 提供寬頻網路閘道器（Broadband Network Gateway, BNG）與光傳輸技術，協助 Globe 改善資料傳輸效率並支援未來 5G 與固定無線接入（Fixed Wireless Access, FWA）需求。在鄉村與偏遠地區，菲律賓電信業者廣泛採用微波傳輸（Microwave Backhaul）作為回傳網路方案，以因應地理障礙與鋪設光纖的高昂成本與施工困難。相較於城市地區常見的光纖骨幹，微波系統具備部署快速、初期投資較低、跨島連結彈性高等優勢，特別適合由七千多座島組成的國家建設網路基礎建設。

主要電信商如 Smart Communications 與 Globe Telecom 均在郊區與島嶼地區使用微波鏈路作為基地臺與核心網路之間的資料傳輸手段。其中，Smart 與以色列的 Ceragon Networks 合作升級其高容量微波網路，提供 5G 與 LTE 所需的高頻寬與低延遲連結；NEC 也為部分區域提供點對點（Point-to-Point, P2P）微波系統。儘管微波回傳在頻寬與穩定性上不如光纖，但在菲律賓這類基礎建設資源不均的地區，仍是目前最具經濟與可行性的替代方案，並且成為推動 5G 與固定無線接入服務普及的基礎支撐技術之一。NEC 與 Nokia 不僅在回傳網路建設方面具備成熟解決方案，更於 2020 年被美國國務院正式列為「潔淨網路」倡議中的可信供應商之一（U.S.

Department of State, 2021）。菲律賓電信業者採用 Nokia 作為核心與回傳設備供應商，除基於技術表現與建設效率考量外，也是對美國外交壓力的回應，進一步強化其科技避險策略的地緣政治導向。至於 Ceragon 雖未名列美國國務院「潔淨網路」名單，但其長期為美國國防部提供戰術網路與高安全性微波通信設備，為軍用等級的通訊供應商（Reuters, 2007）。此一背景賦予其高度可信性，使菲律賓在微波回傳設備選擇上，不僅考量成本與部署速度，更納入政治風險評估與盟邦安全敏感的結構性因素，展現出具戰略計算的科技避險行為。

伍、結論

儘管印尼與菲律賓在對中戰略上處理主權爭端的方式有所不同，前者傾向於去政治化與「管理衝突」，後者則採取明確的「外部平衡」與強化與美國的同盟連結。但在 5G 電信基礎建設的選擇上，兩國卻展現出高度的相似性。兩國皆大規模採用華為與中興的設備作為基地臺主體供應商，顯示在技術依賴與經濟誘因的推動下，即使對中國態度迥異，其實際策略選擇卻趨於一致。這種政策上的「趨同」反映出，在地緣政治不確定性與產業結構限制雙重條件下，東南亞中次級國家往往不得不採取務實與模糊的避險策略，以維持技術發展的可持續性與外交上的操作彈性。

從戰略態度來看，印尼傾向採取「管理衝突」的方式處理與中國的關係，展現出務實與非對抗性的傾向。相較之下，菲律賓則更傾向於「外部平衡」，尤其在南海議題上強化與美國的安全合作，以制衡中國的區域影響力。這種戰略取向不僅反映在外交與軍事層面，也滲透到其科技政策與供應鏈選擇之中。兩國在電子業供應鏈方面皆屬「薄弱」，尚未建立起完整的本地電子產業體系，對外部供應商高度依賴，使其在科技安全與經濟自主性上皆存在結構性限制。這種產業脆弱性使得他們在面對中美科技競爭時，選擇的空間相對受限，往往更易受到中國廠商提供的價格與融資優勢吸引（表 5）。

表 5
印尼與菲律賓 5G 比較

國家	印尼	菲律賓
對中國態度	管理衝突	外部平衡
電子業供應鏈	薄弱	薄弱
電信商所有權	國營電信為骨幹	民營
政策模式	國家主導	民間主導
電信商所有權	國營	民營
基地臺	華為、中興通訊	華為、中興通訊
回傳網路	華為作為骨幹，Nokia 無線方案	多元廠商

儘管兩國策略模式不同，但在實際電信設備的選擇上卻顯現出類似的結構性依賴。在基地臺供應方面，兩國皆大量使用華為與中興通訊的設備，顯示出中國廠商在東南亞電信基礎建設中的主導地位。這一趨勢即便在美國「潔淨網路」倡議後仍持續，突顯中國電信企業的價格競爭力與市場滲透力難以取代。然而，在回傳網路層級的設備選擇上，兩國呈現出差異化。印尼的網路骨幹主要由華為建構，並搭配 Nokia 的無線解決方案，顯示中國仍對印尼基礎建設有顯著影響力。相反地，菲律賓則在回傳網路層級在美國外交壓力下，展現出更多元的供應商選擇。菲律賓案例反映其民營部門在決策上較具彈性，也可能受到國際盟友對資安風險的關切影響，逐步採用非中系供應商以維持技術來源的多樣性與政治可控性。

儘管印尼與菲律賓在對中國風險的感知強度與外交取向上存在差異，兩國在 5G 設備選擇上卻同樣高度依賴中國供應商，顯示在低科技能力與基礎建設壓力下，次級國家難以完全脫離中國科技體系。然而，這種依賴並非單一邏輯所驅動，而是反映出不同的避險策略選擇。根據安全不確定性與科技能力的差異，印尼可歸為「成本導向合作」類型：由於其對中國風險認知較低，且與中國的制度化合作關係深厚，主要考量在於成本與部署效率，傾向接受中國技術以推進基礎建設。而菲律賓則屬於「多元化避險」類型：面對來自美中兩方的安全壓力，政府與業者在基地臺建設上雖仍依賴中資方案，卻在回傳與核心網路層導入可信供應商並與盟邦強化

資訊安全合作，藉此平衡政治風險與經濟利益，展現出更強的地緣政治敏感性與回應能力。

本文的貢獻在於補足現有避險研究的三項不足。首先，過去避險文獻多聚焦於外交戰略的「選擇強度」，以解釋國家如何在大國競爭中保持模糊與彈性（Ciorciari, 2019; Kuik, 2021, 2024），但忽略了產業結構與科技能力的差異如何形塑避險策略的可行性。本文透過印尼與菲律賓在 5G 建設上的比較指出，即便兩國對中戰略態度不同，其在電信設備選擇上仍高度依賴中國廠商，反映出結構性科技依賴對政策操作空間的深刻限制。其次，本文將避險視為一種科技政策與制度能力交錯下的實踐行為，說明不同制度模式如何透過不同的管制與合作機制來達成類似的避險結果。這使我們能超越傳統安全導向的避險分類，更具體理解科技領域中避險策略的具體執行路徑。第三，本文結合新興科技的模糊性與雙重用途特性，指出次級國家在面對技術擴散與規範缺位的「技術性不確定結構」中，其避險不僅是外交選擇，更是政權正當性、制度能力與風險管理的綜合政治抉擇。綜合來看，本文不僅驗證了避險理論在東南亞科技政策中的適用性，更補充其對產業結構與制度條件的敏感度，進而為理解中次級國家在全球科技競爭下的戰略行為提供更為細緻的解釋框架。

參考文獻

中華人民共和國外交部（無日期）。中華人民共和國 - 條約數據庫。http://treaty.mfa.gov.cn/Treaty/web/index.jsp [Ministry of Foreign Affairs People's Republic of China. (n.d.). *The treaty database of the People's Republic of China*.]

周冠竹（2024）。誰遙遙領先？權力轉移論與美中科技權力評估。問題與研究，**63**（3），29-77。https://doi.org/10.30390/ISC.202409_63(3).0002 [Chou, K. C. (2024). Leadership in technology: Analyzing the US-China dynamic in technological power. *Issues & Studies*, *63*(3), 29-77.]

Antara News. (2024, August 15). *Jokowi's legacy: Infrastructure gains amid regional challenges*. https://en.antaranews.com/news/322571/jokowis-legacy-infrastructure-gains-amid-regional-challenges

Arnold, S. (2024). Africa's roads to digital development: paving the way for Chinese structural power in the ICT sector? *Review of International Political Economy*, *31*(4), 1148-1172. https://doi.org/10.1080/09692290.2023.2297363

Asosiasi Penyelenggara Jaringan Telekomunikasi. (2023). *Indonesia Infrastructure Practise, Giga City Initiatives Towards the Digital Vision 2045*. https://apjatel.id/wp-content/uploads/2023/12/White_Paper_Apjatel_EN_2023.pdf

Athavale, D. (2011, September 21). Philippines' electric services distributor Meralco has chosen Tejas Networks high end optical transport (MSPP) solution. *The Times of India*. https://timesofindia.indiatimes.com/philippines-electric-services-distributor-meralco-has-chosen-tejas-networks-high-end-optical-transport-mspp-solution-/articleshow/10066136.cms

BBC. (2017, June 10). *Marawi siege: US special forces aiding Philippine army*. https://www.bbc.com/news/world-asia-40231605

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Ciorciari, J. D. (2019). The variable effectiveness of hedging strategies. *International Relations of the Asia-Pacific*, *19*(3), 523-555. https://doi.org/10.1093/irap/lcz007

De Castro, R. C. (2014). The Aquino administration's balancing policy against an emergent China: Its domestic and external dimensions. *Pacific Affairs*, *87*(1), 5-27. https://doi.org/10.5509/2014871005

De Castro, R. C. (2016). The Duterte administration's foreign policy: Unravelling the Aquino administration's balancing agenda on an emergent China. *Journal of Current Southeast Asian Affairs*, *35*(3), 139-159. https://doi.org/10.1177/186810341603500307

De Castro, R. C. (2017). The Duterte administration's appeasement policy on China and the crisis in the Philippine–US alliance. *Philippine Political Science Journal*, *38*(3), 159-181. https://doi.org/10.1080/01154451.2017.1412161

De Castro, R. C. (2018). Explaining the Duterte administration's appeasement policy on China: The power of fear. *Asian Affairs: An American Review*, *45*(3-4), 165-191. https://doi.org/10.1080/00927678.2019.1589664

DITO. (2025, February 25). *Enjoy the DITO high speed home 5G WiFi plans*. https://dito.ph/blog/enjoy-the-dito-high-speed-home-5g-wifi-plans-philippines

European Telecommunications Standards Institute. (n.d.). *5G*. Retrieved December 31, 2025, from https://www.etsi.org/technologies/mobile/5g

Forge, S., & Vu, K. (2020). Forming a 5G strategy for developing countries: A note for policy makers. *Telecommunications Policy*, *44*(7), Article 101975. https://doi.org/10.1016/j.telpol.2020.101975

Foulon, M. (2015). Neoclassical realism: Challengers and bridging identities. *International Studies Review*, *17*(4), 635-661. https://doi.org/10.1111/misr.12255

Friis, K., & Lysne, O. (2021). Huawei, 5G and security: Technological Limitations and political responses. *Development and Change*, *52*(5), 1174-1195. https://doi.org/10.1111/dech.12680

Gamba, B. (2024, September 12). *UPD, USAID ink MOU for Open RAN lab*. University of the Philippines Diliman. https://upd.edu.ph/upd-usaid-ink-mou-for-open-ran-lab/

Gilat Satellite Networks. (2015, February 2). *Delnet International Corp. Taps Gilat to provide cellular backhaul solution for SMART*. https://www.gilat.com/pressreleases/delnet-international-corp-taps-gilat-to-provide-cellular-backhaul-solution-for-smart/

Gonzales, D., Brackup, J., Pfeifer, S., & Bonds, T. M. (2022). *Securing 5G: A way forward in the U.S. and China security competition*. RAND Corporation.

Harwit, E. (2024). U.S.-China 5G competition, the economy-security nexus, and Asia. *Journal of Chinese Political Science*, *29*(3), 417-432. https://doi.org/10.1007/s11366-023-09879-7

He, K. (2008). Indonesia's foreign policy after Soeharto: International pressure, democratization, and policy change. *International Relations of the Asia-Pacific*, *8*(1), 47-72. https://doi.org/10.1093/irap/lcm021

Heeks, R., Ospina, A. V., Foster, C., Gao, P., Han, X., Jepson, N., Schindler, S., & Zhou, Q. (2024). China's digital expansion in the global south: Systematic literature review and future research agenda. *The Information Society*, *40*(2), 69-95. https://doi.org/10.1080/01972243.2024.2315875

Hetting, C. (2018, March 29). *Telstra's 'first taste of 5G' turns out to be.. Wait for it.. Wi-Fi!* WIFI Now. https://wifinowglobal.com/news-and-blog/telstras-first-taste-5g-turns-wait-wi-fi/

Huawei. (2015, October 12). *Huawei successfully hosts the 1st best experience mobile backhaul summit*. https://www.huawei.com/en/news/2015/10/huawei%20successfully%20hosts%20the%201st%20best%20experience%20mobile%20backhaul%20summit

INQUIRER.net. (2025, January 23). *Israel-PH tech relations reinforced by growing Israeli-owned BPO firm*. https://business.inquirer.net/502894/israel-ph-tech-relations-reinforced-by-growing-israeli-owned-bpo-firm

Jackson, V. (2014). Power, trust, and network complexity: three logics of hedging in Asian security. *International Relations of the Asia-Pacific*, *14*(3), 331-356. https://doi.org/10.1093/irap/lcu005

Kahata, A. (2020, November 24). *Managing U.S.-China technology competition and decoupling*. Center for Strategic & International Studies. https://www.csis.org/blogs/strategic-technologies-blog/managing-us-china-technology-competition-and-decoupling

Kim, M., Eom, D., & Lee, H. (2023). The geopolitics of next generation mobile communication standardization: The case of open RAN. *Telecommunications Policy*, *47*(10), Article 102625. https://doi.org/10.1016/j.telpol.2023.102625

Korolev, A. (2019). Shrinking room for hedging: System-unit dynamics and behavior of smaller powers. *International Relations of the Asia-Pacific*, *19*(3), 419-452. https://doi.org/10.1093/irap/lcz011

Kuik, C. C. (2008). The essence of hedging: Malaysia and Singapore's response to a rising China. *Contemporary Southeast Asia*, *30*(2), 159-185.

Kuik, C. C. (2021). Getting hedging right: A small-state perspective. *China International Strategy Review*, *3*(2), 300-315. https://doi.org/10.1007/s42533-021-00089-5

Kuik, C. C. (2024). Southeast Asian responses to U.S.-China tech competition: Hedging and economy-security tradeoffs. *Journal of Chinese Political Science*, *29*(3), 509-538. https://doi.org/10.1007/s11366-024-09882-6

Kuik, C. C., & Lai, Y. M. (2025). Deference and defiance in Malaysia's China policy: Determinants of a dualistic diplomacy. *International Journal of Asian Studies*, *22*(1), 5-24. https://doi.org/10.1017/S1479591423000104

Lasker, B. (1946). The role of the Chinese in the Netherlands Indies. *The Far Eastern Quarterly*, *5*(2), 162-171. https://doi.org/10.2307/2049741

Lewis, J. A. (2018). *How 5G will shape innovation and security: A primer*. Center for Strategic & International Studies.

Liu, O. (2014). Countering "Chinese Imperialism": Sinophobia and Border Protection in the Dutch East Indies. *Indonesia*, (97), 87-110. https://doi.org/10.5728/indonesia.97.0087

Lobell, S. E. (2009). Threat assessment, the state, and foreign policy: A neoclassical realist model. In S. E. Lobell, N. M. Ripsman, & J. W. Taliaferro (Eds.), *Neoclassical realism, the state, and foreign policy* (pp. 42-74). Cambridge University Press. https://doi.org/10.1017/CBO9780511811869.002

Macanan Palace. (2023). *Executive order no. 32: Streamlining the permitting process for the construction of*

telecommunications and internet infrastructure.

Marston, H. S. (2024). Navigating great power competition: A neoclassical realist view of hedging. *International Relations of the Asia-Pacific*, *24*(1), 29-63. https://doi.org/10.1093/irap/lcad001

Ministry of Communication and Information, Indonesian Telematics Society, & Telecommunication Network Providers Association. (2023). *Indonesia digital infrastructure best practice, giga city initiative towards the digital vision 2045*. https://apjatel.id/wp-content/uploads/2023/12/White_Paper_Apjatel_EN_2023.pdf

Ministry of Internal Affairs and Communications, Japan. (2023, February 9). *Signing of Memorandum of Cooperation in the ICT field between MIC and the Department of Information and Communications Technology of the Republic of the Philippines* https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pressrelease/2023/2/09_01.html

Morales, N. J. (2019, June 20). *Philippines' Globe Telecoms launches 5G service backed by Huawei equipment*. Reuters. https://www.reuters.com/article/technology/philippines-globe-telecoms-launches-5g-service-backed-by-huawei-equipment-idUSKCN1TL207/

Morales, N. J., & Lema, K. (2020, September 17). *China-backed telecom firm says won't spy on Philippines*. Reuters. https://www.reuters.com/article/technology/china-backed-telecom-firm-says-wont-spy-on-philippines-idUSKBN2681DV/

Mozingo, D. (1961). The Sino-Indonesian dual nationality treaty. *Asian Survey*, *1*(10), 25-31. https://doi.org/10.2307/3023470

Nguyen, P. L., & Tok, S. K. (2025). Domestic imperative of the Philippines' South China Sea policy: Personality-driven policymaking and constant shifts between China and the United States. *The Pacific Review*, *38*(1), 29-59. https://doi.org/10.1080/09512748.2024.2321268

Office of Assistant to Deputy Cabinet Secretary for State Documents & Translation. (2020, January 5). *On Natuna waters conflict, President Jokowi: We will prioritize peaceful diplomacy*. Sekretariat Kabinet Republik Indonesia. https://setkab.go.id/en/on-natuna-waters-conflict-president-jokowi-we-will-prioritize-peaceful-diplomacy/

Offshore Energy. (2014, March 27). *Huawei Marine upgrades PT Telkom 3rd route submarine cable*. https://www.offshore-energy.biz/huawei-marine-upgrades-pt-telkom-3rd-route-submarine-cable/

Oostindie, G., & Paasman, B. (1998). Dutch attitudes towards colonial empires, indigenous cultures, and slaves. *Eighteenth-Century Studies*, *31*(3), 349-355. https://doi.org/10.1353/ecs.1998.0021

Rahman, A., Arabi, S., & Rab, R. (2021). Feasibility and challenges of 5G network deployment in least developed countries (LDC). *Wireless Sensor Network*, *13*(1), 1-16. https://doi.org/10.4236/wsn.2021.131001

Rathbun, B. (2008). A rose by any other name: Neoclassical realism as the logical and necessary extension of structural realism. *Security Studies*, *17*(2), 294-321. https://doi.org/10.1080/09636410802098917

Reardon, M. (2019, March 1). *US warns Philippines against using Huawei 5G gear*. CNET. https://www.cnet.com/tech/mobile/pompeo-warns-philippines-against-using-huawei-5g-gear/

Reuters. (2007, January 10). *Israeli high-tech giant signs deal with US army*. Ynet News. https://www.ynetnews.com/articles/0,7340,L-3350805,00.html

Rose, G. (1998). Neoclassical realism and theories of foreign policy. *World Politics*, *51*(1), 144-172. https://

doi.org/10.1017/S0043887100007814

Santoso, J. R. (2025, April 29). *Indonesia is hooked on Huawei*. Australian Strategic Policy Institute. https://www.aspi.org.au/strategist-posts/indonesia-is-hooked-on-huawei/

Sawad, I., Nilavalan, R., & Al-Raweshidy, H. (2023). Backhaul in 5G systems for developing countries: A literature review. *IET Communications*, *17*(6), 659-669. https://doi.org/10.1049/cmu2.12578

Senate of the Philippines. (2023, May 9). *19th congress: Senate Bill no. 2146: Open access in data transmission act*. https://web.senate.gov.ph/lis/bill_res.aspx?congress=19&q=SBN-2146&utm_source=chatgpt.com

Sriyanto, N. (2018). Indonesia–China Relations: A political-security perspective. In L. C. Sinaga (Ed.), *Six decades of Indonesia-China relations: An Indonesian perspective* (pp. 65-77). Springer Singapore. https://doi.org/10.1007/978-981-10-8084-5_5

Sukma, R. (2009). Indonesia-China Relations: The politics of reengagement. In S. Tang, M. Li, & A. Acharya (Eds.), *Living with China: Regional states and China through crises and turning points* (pp. 89-106). Palgrave Macmillan. https://doi.org/10.1057/9780230622623_6

Telecom Review Asia. (2025, February 21). *NEC unveils near real-time RAN controller for smarter 5G networks*. https://www.telecomreviewasia.com/news/network-news/12533-nec-unveils-near-real-time-ran-controller-for-smarter-5g-networks/

The Observatory of Economic Complexity. (n.d.). *Indonesia (IDN) and China (CHN) trade*. Retrieved December 31, 2025, from https://oec.world/en/profile/bilateral-country/idn/partner/chn

The Privacy Protection Authority. (2025, April 24). *The Israeli Privacy Protection Authority expands its international collaborations: Signing of a mutual cooperation agreement (MOU) with the National Privacy Commission of the Philippines*. Gov.il. https://www.gov.il/en/pages/mou_25

The White House. (2018). *National cyber strategy of the United States of America*. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

The White House. (2020). *National strategy to secure 5G*. https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf

U.S. Department of State. (2019). *Huawei: Myth and fact*. U.S. https://2017-2021.state.gov/wp-content/uploads/2020/12/5G-Myth_Fact3-508.pdf

U.S. Department of State. (2021). *The clean network*. https://2017-2021.state.gov/the-clean-network/

van der Westhuizen, J. (2024). Huawei or the US Way? Why Brazil and South Africa did not securitize 5G. *Revista Brasileira de Política Internacional*, *67*(2), Article e016. https://doi.org/10.1590/0034-7329202400216

Vandenbosch, A. (1930). A problem in Java: The Chinese in the Dutch East Indies. *Pacific Affairs*, *3*(11), 1001-1017. https://doi.org/10.2307/2750073

Wæver, O. (1993). *Securitization and desecuritization*. Centre for Peace and Conflict Research.

Zha, D. (2000). China and the May 1998 riots of Indonesia: Exploring the issues. *The Pacific Review*, *13*(4), 557-575. https://doi.org/10.1080/095127400455323

《台灣戰略研究》第二卷第一期
2026 年 1 月　33 頁～ 58 頁

Taiwan Strategic Studies, Vol.2 No.1
January 2026, pp.33-58
DOI: 10.30249/tss.202601_2(1).0002

網路敵意行動之國際法評價與臺灣因應策略

林昕璇 *

摘　要

資通訊技術的迅即發展，帶動網路空間已成為國際政治、經濟與軍事互動的重要場域。各國間透過網路手段進行間諜活動、認知作戰、基礎設施攻擊等「網路敵意行為」（hostile cyber activities）日益頻繁，對國家安全與民主制度構成重大威脅。由於網路攻擊具備匿名性、超地緣性與模糊性，國際法對於此類行為的規範與評價尚處於發展階段，故而對行為歸責與法律界定帶來挑戰。臺灣作為高度依賴資訊基礎設施的民主社會，面臨來自國際網路敵意行為的多重威脅，亟需建立符合國際法與本土需求之因應策略。政府已推動《國家資通安全戰略 2025》，強調「資安即國安」理念，並建立國家資安戰情協同應變中心，以及強化國家資通安全會報，提升整體資安韌性。本文乃從當前國際法秩序的視野，檢視直接和間接規範網路攻擊之國際法體系的現狀與侷限，提出建立涵蓋政治、法律、外交與技術層次的分層回應機制，強化歸責標準、公私協作、數位外交與立法改革，提升臺灣資安韌性、應變能力、法制基礎與國際合作能量等若干制度整備之規範性建議。

關鍵詞：網路攻擊、網路戰、國際法規範、數位韌性、網路駭客主義

* 國立成功大學政治學系副教授，美國維吉尼亞大學法學博士（S.J.D.）。
收件：2025 年 6 月 13 日；一修：2025 年 7 月 29 日；通過：2025 年 8 月 4 日；接受：2025 年 12 月 15 日。

International Legal Implications for Hostile Activities in Cyberspace and Taiwan's Response Strategies

Hsin-Hsuan Lin**

Abstract

The rapid development of information and communication technologies has transformed cyberspace into a critical arena for international political, economic, and military interactions. Hostile cyber activities—such as espionage, cognitive warfare, and attacks on critical infrastructure—have become increasingly frequent among states, posing significant threats to national security and democratic institutions. The regulation and evaluation of such activities under international law remain in a developmental stage, primarily guided by principles of the United Nations Charter, including the prohibition of the use of force, state sovereignty, non-intervention, and countermeasures. However, the anonymity, transboundary nature, and ambiguity of cyberattacks pose challenges to attribution and legal classification. As a highly digitized democratic society, Taiwan faces multifaceted threats from hostile international cyber activities and urgently needs a response strategy that aligns with both international legal standards and domestic needs. The government has launched the "National Cybersecurity Strategy 2025," emphasizing the concept of "cybersecurity as national security," and established a joint cyber defense system and a situational awareness and emergency response center to enhance overall cyber resilience. From the perspective of the evolving international legal order, this paper proposes a multi-layered response mechanism encompassing political, legal, diplomatic, and technical dimensions. It offers normative recommendations for institutional preparedness in Taiwan, including strengthening attribution standards, fostering public-private collaboration, advancing digital diplomacy, and reforming legislation to enhance cybersecurity resilience, responsiveness, legal infrastructure, and international cooperation capacity.

Keywords: cyberattacks, cyber warfare, international legal norms, digital resilience, hacktivism

** Associate Professor, Department of Political Science, National Cheng Kung University; S.J.D., University of Virginia School of Law. Email: hl3bu@virginia.edu

壹、研究緣起

數位依賴（digital dependencies）所引發的國家安全挑戰，已在國家治理、企業營運與個人生活等層面日益顯著，且三者之交織互動也牽動國際戰略布局的敏感神經。析言之，資通訊技術肇致的風險具有高度系統性，伴隨著數位資料的集中化儲存固然有助於電子化基礎建設的整合匯流，於此同時，卻也將各國的資通基礎建設和國家基礎建設暴露於跨境網路敵意活動之風險之下，隨之伴生的資訊外洩規模日益猖獗、損失難以估計。美國人事管理局（U.S. Office of Personnel Management）之資安事件，導致逾 2,200 萬筆聯邦雇員個資遭駭，顯示國家級資安體系的結構性脆弱（Citron & Eichensehr, 2025, pp. 49-50）。2021 年 Colonial Pipeline 遭駭事件造成美國東岸主要輸油管線停擺數日，進而引發「恐慌性搶購」，適足彰顯關鍵基礎設施網路安全與能源安全之間的高度聯動性（Citron & Eichensehr, 2025, p. 50）。無獨有偶，網路敵意行為殃及之私部門亦有日益增加之勢，2017 年信用評等機構 Equifax 遭受的資料外洩事件，波及近 1.48 億名美國公民，進一步凸顯私部門在個資治理上的法遵與風險控管不足（Citron & Eichensehr, 2025, p. 50）。此外，對數位紀錄與網路系統的高度依賴，使企業面臨日益頻繁且具有高度毀滅性的勒索軟體攻擊。2017 年，WannaCry 病毒影響了全球至少 150 個國家的數十萬臺電腦，WannaCry 惡意軟體阻止微軟的 Windows 作業系統啟動，並加密受影響電腦上儲存的所有資料。前揭諸項憑恃網路之跨國性、難以追索性的侵害事件涉及網路攻擊具備匿名性與模糊性等特質，不僅對行為歸責與法律界定帶來挑戰，更攸關國家安全與公共利益之保障，催動各國政府莫不重行檢視與強化關鍵基礎設施的資安法制架構與應變機制（Sigholm, 2013）。

臺灣作為高度依賴資訊基礎設施的民主社會，面臨來自國際網路敵意行為的多重威脅，亟需建立符合國際法與本土需求之因應策略。本文旨在探討數位依賴日益加深下所引發的國家安全挑戰，首先就網路敵意行為與駭客行動主義分別涉及之模糊邊界與治理困境，提出網路敵意行為之概念混淆與適用侷限所涉跨境性與模糊性的法律挑戰。第三部分檢視現行國際法規範，涵蓋直接與間接針對網路攻擊之規範框架對於網路攻擊的適用性與侷限性，同時延伸至現行國際法中國家責任與盡職調

查（due diligence）適用於網路攻擊所肇致之適用難題與解釋取向。本文續而聚焦國家安全威脅與數位依賴日益加劇的國家地緣政治下，三種當前國際社群因應網路攻擊因應模式：「保持沉默不歸咎」、「歸咎但保留法律立場」、「歸咎並尋求多邊聯合認定」，進而探討不同模式背後隱藏之國際法秩序博弈與臺灣政策選擇的啟示。最後聚焦於臺灣現況，提出整合法制建構與國際合作之多層次應對策略，以建立具韌性的數位安全治理架構。

貳、網路敵意行為與駭客行動主義：模糊邊界與治理困境

一、網路敵意行為之概念混淆與適用侷限

根據史丹佛大學國際安全與合作中心高級研究專家 Herbert Lin 的定義，其將網路攻擊視為「使用刻意地行動和操作來改變、破壞、欺騙、降級或摧毀敵方電腦系統或網路或資訊」，並將其等同於攻擊性網路行動（Lin, 2010, p. 63）。惟誠如網路法專家 Oona Hathaway 精闢地指出當前各國在處理非國家網路活動時亟需回應三個核心問題：首先是缺乏對關鍵概念的明確定義，如「武力使用」和「武裝攻擊」。其主張儘管現代網路攻擊日益頻繁，並可能造成癱瘓電網、防空系統甚至損害核設施等嚴重損害結果，但在國際法下，占據絕大宗的此類攻擊仍未達「武裝攻擊」的標準，難以直接適用戰爭法。蓋戰爭法原為明確軍事衝突而設計，網路攻擊的手段和效果與傳統戰爭差異極大，致令「網路戰爭」一詞在規範行概念界定上爭議不斷（林昕璇，2023，頁 102-107；Hathaway et al., 2012, pp. 881-882）。

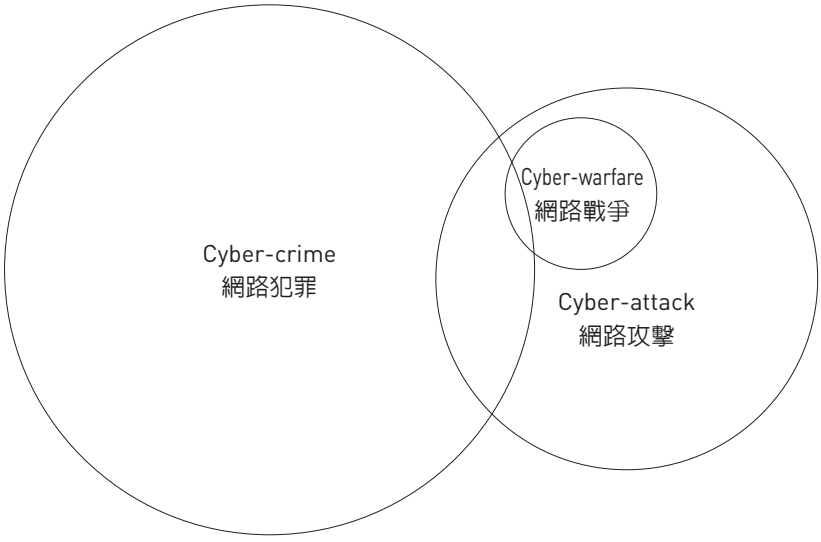
職此，區分網路攻擊的位階層級實有清楚釐清適用概念上的模糊性與混淆性的必要價值。進一步言，僅有構成「武裝攻擊」或發生於既有武裝衝突中的網路行動，方能納入戰爭法的適用範圍。其餘如間諜、滲透或政治破壞等，應由不干涉原則、國際刑法或國內法處理，而非一概視為戰爭行為。Oona Hathaway 等網路法專家更直言不諱地指出，當前必須擬定一部網路攻擊條約的首要任務，乃繫諸於建立一致性且可操作的定義，釐清「網路攻擊」（cyber-attack）、「網路犯罪」（cyber-crime）與「網路戰爭（cyber-warfare）」三者的界線。而前開三者定義不同之處，在於網

路攻擊僅指涉基於政治或國安目的蓄意削弱電腦網路功能的行為，網路犯罪則是非國家行為體或私部門組織違反刑法的電腦犯罪，而網路戰爭則需造成足以比擬武裝攻擊的人身或財產損害。這類定義不僅可作為各國立法基礎，也有助於建立跨國合作共識（Hathaway et al., 2012, p. 833），三者的關係可圖示如圖 1。

圖 1

網路犯罪、網路攻擊與網路戰的聯集關係圖

FIGURE 1: Relationship between cyber-actions



資料來源：作者重製自 "The law of cyber-attack," by O. A. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue, & J. Spiegel, 2012, *California Law Review*, 100(4), p. 833.

其次是歸因問題。Dennis Broeders、Els De Busser 和 Patryk Pawlak 指出，國際法並未提供具體規則說明何種證據足以歸因網路攻擊（Broeders et al., 2020, pp. 6-7）。特別是在國家與高級持續性威脅（advanced persistent threats, APTs）等代理組織之間建立證據聯繫更加困難，不啻彰顯國際法基本上忽略了此等模糊行為者作為國家力量延伸的現實（Katagiri, 2021, p. 3）。

不容忽視的是，現行國際法秩序未能充分維護網路空間和平的原因在於此等機制實無法有效規範非國家行為者（如個人駭客和科技公司）的行為。揆諸實際，

傳統國際法由政府官員制定，高度以國家為中心，與網路空間中非國家行為者占主導地位的現實不符。固然由北約合作網路防禦卓越中心邀集專家學者編纂的《適用於網路戰爭的塔林國際法手冊》（*Tallinn Manual on the International Law Applicable to Cyber Warfare, Tallinn Manual*, 以下簡稱塔林手冊）分別於 2013 年、2017 年輯錄出版成書，可謂國際法適用於網路空間討論的高峰，惟仍缺乏明確文獻和足夠的國際共識，凝聚據此確定各國真正接受這些規則作為管理網路行動的權威指南。

同時，國際法機構素來在懲罰非國家暴力行為方面普遍缺乏強制力的老病沉痾同樣也延伸至網路領域（Katagiri, 2021, p. 3）。在此等因國際社會現實導致的法律真空下，主要科技公司等私營部門則陸續填補此一領域的規範真空，利用其數位產品重塑規範，成為「規範企業家」（Katagiri, 2021, p. 3）。然而，該等企業干預這個場域的立法形成的結果亦導致各行為體之間缺乏協調，私部門利益與國家利益並不完全一致的弊端（Katagiri, 2021, p. 3）。此外，國際社會關於網路空間規範的討論高度不民主，主要由少數大國和積極的中等強國主導，而這些國家對應採用的規範存在重大分歧。國際法在應對這些挑戰時面臨嚴重缺乏的一致性、反覆性的國家實踐，可見一斑（Katagiri, 2021, p. 3）。

二、駭客行動主義者（hacktivists）之概念意涵

誠如上述，鑑諸網路空間中非國家行為者占主導地位的現實，實有必要就網路空間中的非國家行為者的組織型態與類型態樣予以系統性的分析（Sigholm, 2013）。職此，駭客行動主義者指涉利用網路進行政治或社會抗議，該等行為移離於時而合法，時而非法的灰色空間，並且背後多隱藏政治、軍事或商業目標。常見的行為包括：網頁篡改（defacement）、網路資源重導（redirects）、分散式阻斷服務攻擊（DDoS）、資訊竊取（data theft）等（Sigholm, 2013, p. 14）。往昔較為人所知、頗具代表性的駭客行動團體是「匿名者」（anonymous），他們發動過多起重大攻擊，如對山達基教會的戰爭、阿拉伯之春的支援行動等。這些行為主要是出於政治或社會立場，具有強烈的抗議性質。有學者將上述非國家行為體更系統化地賦予概念意涵與判斷基準（Sigholm, 2013, pp. 14-23），茲分述如下。

（一）駭客（hackers）

駭客乃指涉擁有高深技術知識的人，他們深入了解計算機硬體、軟體、操作系統及網路運作，並且能夠設計複雜的攻擊。根據動機和道德標準，駭客可分為三類（Sigholm, 2013, pp. 14-15）：

1. 黑帽駭客（black-hat hackers）：進行非法攻擊，通常以牟利為目的，無視法律後果。例如竊取信用卡信息或入侵企業系統。
2. 白帽駭客（white-hat hackers）：亦可稱為道德駭客，受雇於政府或企業，負責測試網路安全、修補漏洞，從而防止黑帽駭客的攻擊。
3. 灰帽駭客（grey-hat hackers）：介於黑帽與白帽之間，通常不以非法行為為主，但偶爾會進行一些未經授權的行為，如在未通報的情況下發現並修復漏洞。

（二）愛國駭客（patriot hackers）

愛國駭客的主要目的是協助本國政府，通過網路攻擊來支持或宣揚本國的政治利益，特別是在衝突或戰爭中。例如，中國的「紅客聯盟」曾發表愛國駭客宣言，並與其他駭客發動過「駭客戰爭」。俄羅斯的愛國駭客也在過去的數次戰爭中，發揮了重要作用，如在 2007 年愛沙尼亞 DDoS 攻擊、2008 年喬治亞網路戰等（Sigholm, 2013, pp. 16-17）。

（三）內部網路人員（cyber insiders）

內部網路人員是指擁有合法存取權限的人，他們因金錢、報復或個人動機背叛自己的公司或政府機構，進行資料竊取或內部攻擊。這些行為相對難以偵測，因為這些人擁有合法權限。例如，開發人員可能會在程式中植入後門，或者利用 USB 裝置竊取機密資料。最著名的案例是維基解密（WikiLeaks）事件（Sigholm, 2013, pp. 16-17）。

（四）網路恐怖分子（cyber terrorists）

網路恐怖分子利用網路技術發動攻擊，旨在達成政治或意識形態目標，並造成公眾恐慌。雖然專家對網路恐怖主義的威脅評價分歧，但如果網路攻擊成功，可能

對國家安全、經濟或公眾信任造成極大損害。網路恐怖攻擊的特點是具有高度隱蔽性與無國界的特徵（Sigholm, 2013, p. 18）。

（五）惡意軟體作者（malware authors）

惡意軟體作者專門開發用於惡意攻擊或犯罪活動的軟體，如病毒、木馬、勒索病毒等。他們的技術非常高超，並且擅長隱匿攻擊，避免被防毒軟體、間諜程式防護或垃圾郵件過濾技術發現（Sigholm, 2013, pp. 18-19）。

（六）網路詐騙者（cyber scammers）

網路詐騙者通過各種手段利用網路進行欺詐，目的是獲取受害者的金錢或敏感資訊。常見的詐騙手法包括：（1）隨機垃圾郵件詐騙：如假冒樂透獎金或高薪工作機會等。（2）網路釣魚（phishing）：發送假冒銀行或其他機構的電子郵件，誘騙受害者提供敏感資料。（3）標槍式網路釣魚（spear phishing）：更具針對性，利用社交工程技巧欺騙特定目標（Sigholm, 2013, p. 19）。

參、網路攻擊於國際法律體系之邊緣性及非拘束性

誠如前述，當前國際法上尚無一套全面性的國際法律架構能夠統一規範所有類型的網路攻擊，惟世界各地的多邊組織已開始透過零散的法律與政策措施，試圖遏制此一日益嚴重的安全威脅行動。本節簡要回顧由聯合國、北約、歐洲理事會、上海合作組織等機構發起的相關法律行動與制度。又此等國際規範體系基於系爭規約是否以網路攻擊行為直接規範客體，進而可分成「直接規範網路攻擊之國際法律體系」與「間接規範網路攻擊之國際法律體系」，茲解析如下。

一、直接規範網路攻擊之國際法律體系

（一）聯合國（United Nations）

聯合國在網路安全議題上的進展至今仍相對有限。儘管聯合國大會曾通過多項關於資訊安全的決議，惟核期性質多屬原則性聲明，未能落實化為具有強制規範

效力的具體遵循義務（Hathaway et al., 2012, pp. 860-861）。惟不容諱言的是聯合國大會允許所有會員國參與，係當前得以廣泛討論凝聚全球共識的超國界國際組織雖然其決議無法律拘束力，但具有象徵意義，可反映各國對網路安全政策的立場（Hathaway et al., 2012, pp. 860-861）。此外，大會亦可主導研究與設立專家小組，如 2004 年起運作的「政府專家小組」（Group of Governmental Experts, GGE），即已發表多份重要報告，扮演超國界組織引領未來制定規範前瞻視野的專家要角（Luzzatto, 2022, p. 266）。晚近值得注意的發展為 2015 年 GGE 發布之《關於從國際安全的角度看資訊和電信領域的發展政府專家組的報告》（*Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*），該份調查報告首度明確確認《聯合國憲章》適用於網路空間；要求國家不得蓄意損害他國關鍵基礎設施。國家應避免讓境內被用作發動惡意網路活動的平臺（Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015）。2021 年 GGE 報告《從國際安全角度促進網路空間負責任國家行為政府專家組的報告》（*Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*），重申 2015 年報告的原則與規範；強化對國際法適用的承認，尤其是《國際人道法》、《國際人權法》、《國家責任法》；呼籲各國建立國內政策協調機制與網路事件應變能力（Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 2021）。

（二）北約（North Atlantic Treaty Organization, NATO）

迄至 2007 年愛沙尼亞遭大規模網路攻擊後，北約方才開始重視網路安全威脅。似顯示其缺乏明確的網路防禦原則與整體戰略。2008 年布加勒斯特高峰會（2008 Bucharest NATO summit）後，北約設立合作網路防禦卓越中心（Cooperative Cyber Defense Centre of Excellence），負責整合成員國能力與制定長期戰略（Hathaway et al., 2012, pp. 861-862）。2008 年在北約網路防禦卓越中心的邀集下組成北約國際專家小組（International Group of Experts），該小組編纂的《塔林手冊》被稱為「第一

部網路戰爭規範法典」（孫國祥，2015，頁 167-168）。塔林手冊的編纂小組成員中不乏同時具備學術與軍事背景的專家，集結多位編輯委員、法律專家、同行評審人員，以及所有技術顧問、紀錄員與專案協調與管理人員，多來自北約或各國軍方。因此，自其發起機構、人員組成與編撰過程來看，《塔林手冊》成書背後所匯集兼具學術、政治與軍事等多重背景的專家學者雖不乏軍事強權國家試圖領軍成為網路攻擊法制之規範制定者的意圖，惟囿於國際地緣政治，與取得等同國際法之拘束力仍有一定程度的落差（孫國祥，2015，頁 167-168）。

《塔林手冊》嗣後於 2017 年推出《塔林手冊 2.0》版，仍堪稱人類迄今為止最具系統性地針對網路戰制定規則的重要嘗試。新一代專家沿用原始《塔林手冊》的格式，制定了補充性規則，並將其與原有規則合併，形成了這部《塔林手冊 2.0：適用於網路行動的國際法》。因此，《塔林手冊 2.0》取代了初版手冊的地位。首先須明確理解，《塔林手冊 2.0》並非法定文件，而是兩次由獨立專家群以個人身分進行之研究工作的成果（Schmitt, 2017, pp. 2-3）。該手冊不代表北約合作網路防禦卓越中心或北約本身之立場，亦不反映任何觀察員所代表之組織或國家的官方立場乃手冊中一再強調者（Schmitt, 2017, pp. 2-3）。此外，本手冊所呈現之法律內容係反映截至 2016 年 6 月兩屆國際專家小組採認時之國際法狀態。同時序言中亦明揭本手冊之問世，實非「最佳實務」指引，亦非國際法「漸進式發展」之產物，更不帶有任何政策性或政治性立場（Schmitt, 2017, pp. 2-5）。換言之，《塔林手冊 2.0》意圖客觀呈現現行有效之法律（lex lata），因此兩屆專家小組均刻意避免納入任何屬於擬制法（lex ferenda）之主張（Schmitt, 2017, pp. 2-5）。目前，直接處理網路行動的條約極為有限，即使已有者，其涵蓋範圍亦相當狹隘。同時，鑒於國家網路行動多屬機密，且關於「法之意見」（opinio juris）之公開表示亦屬稀少，因此現階段尚難明確界定是否已存在具體之網路習慣國際法。然而，此一法律上的空缺並不代表網路行動處於無規範的真空狀態。

（三）歐洲理事會（Council of Europe）

與其他國際組織相比，歐洲理事會在網路安全領域起步最早、規範也最具體，2001 年通過的《布達佩斯網路犯罪公約》（*Cyber-Crime Convention*）是全球首部針

對網路與電腦犯罪的國際條約，旨在透過立法與合作建立保護社會的共同刑事政策，《布達佩斯網路犯罪公約》制定之網路犯罪及相關行為包括：垃圾郵件、駭客攻擊、病毒散布、色情內容、身分盜用、資料竊取、資料操控、勒索軟體、分散式阻斷服務攻擊、企業電子郵件詐騙、電子郵件偽造、銀行詐欺、社群媒體濫用，以及智慧財產權侵害等。公約也涵蓋關於網路霸凌、網路騷擾、「復仇式色情」以及「假新聞」散播等事件的通報（Nguyen & Golman, 2021）。

圍繞網路攻擊的規範性指針需迄至 2019 年，歐盟（European Union, EU）理事會通過《2019/796 號規章：關於針對威脅歐盟或其成員國的網路攻擊所採取的限制性措施》（*Council Regulation [EU] 2019/796 of 17 May 2019 Concerning Restrictive Measures Against Cyber-Attacks Threatening the Union or its Member States*），針對威脅歐盟或其成員國的網路攻擊採取限制性措施。復根據系爭規章第 1 條第 3 款明確列舉「網路攻擊」涵蓋：（1）存取資訊系統；（2）干擾資訊系統；（3）干擾資料；或（4）攔截資料。制裁可針對不僅已完成的行為，也包括未遂的行動。欲成為制裁對象，網路攻擊必須符合兩項要件：（1）該攻擊具有重大影響；（2）該攻擊對歐盟或其成員國構成外部威脅（Council Regulation 2019/796, 2019）。

而判斷網路攻擊是否具有重大影響，系爭規章第 2 條訂有明文，亦即可考慮一系列指標：（1）攻擊造成的範圍、規模、影響或干擾的嚴重性；（2）受影響的自然人或法人、實體或機構的數量；（3）涉及的成員國數量；（4）造成的經濟損失金額；（5）行動人為自己或他人獲取的經濟利益；（6）被竊取的資料量或資料外洩的規模；（7）所存取的商業機密資料的性質（Council Regulation 2019/796, 2019）。

前開歐盟《2019/796 號規章》針對網路攻擊所設的制裁框架雖具體且具前瞻性，然其在實務執行層面仍面臨若干挑戰。首先，對「重大影響」的認定雖列有多項指標，但多為質性標準，如「嚴重性」、「規模」與「經濟利益」，易生解釋空間，恐導致成員國間標準不一，進而影響制裁的一致性與可信度。其次，規章設下「外部威脅」作為制裁必要條件，意即若攻擊源自歐盟內部，即便造成重大破壞，亦僅得由各國依其國內法處理，此對跨境網路犯罪實際威脅之應對明顯不足。再者，未遂行為雖納入制裁範圍，理應強化預防效果，然於證據蒐集與行為定性上仍具高難度，在技術上支持法律上歸責一節，仍存在重重阻礙。

（四）上海合作組織（Shanghai Cooperation Organization, SCO）

上海合作組織是由中國、俄羅斯、哈薩克、吉爾吉斯、塔吉克與烏茲別克等國於 2001 年創立之區域性政府間安全合作組織。2009 年於葉卡捷琳堡簽署《上海合作組織成員國保障國際信息安全政府間合作協定》，序言開宗明義明揭：「上海合作組織成員國政府（以下簡稱「各方」）注意到構成全球信息空間的信息通信新技術和新手段在發展和應用方面取得巨大進步；對在民用和軍事領域將這些技術和手段用於與維護國際穩定和安全相悖目的所引起的威脅表示擔憂；認為國際信息安全作為國際安全體系中的一個關鍵因素具有重大意義；深信各方在國際信息安全問題上進一步加深信任、加強協作是當務之急，符合各方利益……」（上海合作組織成員國保障國際信息安全政府間合作協定，2009）。值得強調者，前揭合作協定中提出釐清自身對網路攻擊的定義範疇，較值得注意者，系爭協定第 2 條定義網路技術為「用於傳播破壞國家政治、經濟和社會制度以及精神文化環境的信息」亦納入規範的射程範疇。[1] 此等擴張性理解與西方價值觀與權利觀產生相當大的歧異，蓋西方權利保障式的論述立基於儘可能減少並避免限制政治異議表達的網路活動上加諸過度規範。與此相對地，上海合作組織的規範模式提供了另一種關於網路攻擊的規範觀點，惟於此同時亦凸顯出一個不容否認的事實，亦即全球在定義「網路攻擊」本質與可接受範圍時的重大分歧。析言之中國與傳統西方陣營事實上於是否將「政治顛覆性言論」視為網路攻擊，仍存在深刻價值分歧（Hathaway et al., 2012, p. 865）。

二、間接規範網路攻擊的國際法律體系

除前開專門特定以網路攻擊對規範對象之公約或協議，國際法中尚且另外設置雖非專為規範網路攻擊而設，惟可能因其所涵蓋的「手段」與「工具」被間接適用於特定類型的攻擊行為，從而導致網路攻擊的途徑或工具手段上涉及如以電信資通

[1] 根據《上海合作組織成員國保障國際信息安全政府間合作協定》第 2 條所界定之國際信息安全領域的主要威脅涵蓋如下：（1）信息武器的研製和使用，信息戰的準備和實施；（2）信息恐怖主義；（3）信息犯罪；（4）利用在信息空間的領先地位損害他國的利益和安全；（5）傳播破壞他國政治、經濟和社會制度以及精神文化環境的信息；（6）對全球和各國信息基礎設施安全穩定運行的自然和（或）人為威脅。

訊技術、航空或海洋領域所規範的傳輸技術、設施或活動，這些「手段導向」或「途徑導向」的網路攻擊則會納入射程範疇。整體而言，此類制度提供了一套零散且有限的工具，僅適用少部分藉由特定媒介執行的網路攻擊，無法全面涵蓋所有網路威脅。茲析述如下。

（一）電信法

首先，國際電信法可能適用於涉及國際電纜或無線電頻率通訊的網路攻擊，由聯合國轄下的國際電信聯盟（International Telecommunication Union, ITU）負責制定與管理。該組織旨在「透過高效率的電信服務，維護世界和平並促進所有國家的經濟與社會發展」。ITU 制定的規範包括具條約效力的管理規則與無線電規則，以及不具拘束力的電信標準，主要作用是協調成員國間無線頻譜與通訊資源的分配與使用（Hathaway et al., 2012, pp. 867-868）。

揆諸實際，《國際電信聯盟憲章》（*Constitution of the International Telecommunication Union*）並未直接定義或規範「網路攻擊」，但憲章第 1 條開宗明義宣示憲章之本旨為促進全球通信安全、國際合作；復憲章第 45 條規定有害干擾（harmful interference）之禁止：「所有電臺，無論其用途為何，均應以不對其他成員國、已認可的運營機構，或依《無線電規則》規定運作並從事無線電業務的其他合法授權運營機構之無線電服務或通信造成有害干擾的方式設立與運作」（Constitution of the International Telecommunication Union, 1992）。條文為數甚少，且多是例示性、外交呼籲式的政策指針，難謂構成國際間對資安與跨國電信保護的法律基礎。

（二）航空法（aviation law）

當網路攻擊干擾非軍用航空系統時，可能誘發三項主要的國際航空法規之適用：亦即 1944 年《國際民用航空公約》（*Convention on International Civil Aviation*, 因簽署地點位於美國芝加哥，又稱為《芝加哥公約》）、1971 年《蒙特婁公約》（Montreal Convention），以及 1988 年《蒙特婁機場暴力行為制止議定書》（*Montreal Convention for the Suppression of Unlawful Acts Against Civil Aviation*）。揆諸前揭三公約之規範意旨，若攻擊造成航空管制中斷、乘客名單或禁飛名單被篡改，即可能違反上

述法律。事實上，各該公約各有規範重點，首先，《芝加哥公約》建立了國際民航組織（International Civil Aviation Organization, ICAO），要求成員國對「民用航空航行安全給予應有關注」，並禁止任何干擾民航飛行的行為。雖然公約 1984 年修正案禁止使用武器攻擊民航機，但在戰爭或緊急狀況下，成員國可暫時中止其部分義務，只需通知理事會。《蒙特婁公約》則進一步明定，任何人若「故意且非法地」使航空器無法飛行，或「危及其在飛行中的安全」，例如破壞導航設施或干擾其運作，皆構成犯罪。因此，若網路攻擊影響飛航操作或空管系統，即屬此犯罪範疇（Hathaway et al., 2012, pp. 869-870）。

復次，《蒙特婁議定書》則擴展法律保護至機場設施。第二條指出，若某人故意使用裝置、物質或武器對機場人員施暴，或破壞設施與航空器、干擾機場服務，若足以危及安全，亦構成犯罪。此包括透過網路干擾乘客資訊、禁飛名單或整體機場資訊系統的行為。承上所述，國際法層次的航空法規並非為網路戰而設，卻已涵蓋多數針對民用航空安全的數位攻擊，為應對此類威脅提供一系列間接但有效的國際規範框架與管制途徑（Hathaway et al., 2012, pp. 869-870）。

（三）海洋法（law of the sea）

近年臺灣海纜斷纜事件層出不窮，引發外界關注。台灣網路資訊中心董事長黃勝雄表示，99% 網路頻寬都依賴海纜，可謂臺灣的「數位生命線」，乘載全球超過 95% 的數據傳輸，舉凡日常的語音通話、看串流影片至金融匯兌交易，以及國際貿易、軍事資訊等，均大幅仰賴海纜進行傳輸，乃各國重要關鍵基礎設施（黃浩珉，2025；蘇思云，2025）。就此涉及海域之國際規範而言，1982 年《聯合國海洋法公約》（*United Nations Convention on the Law of the Sea*, UNCLOS）雖未專門針對網路攻擊設立規範，但其中若干條文，特別是第 19 條、第 109 條與第 113 條，在某些情況下可能間接適用於海上網路攻擊行為。

1. 根據公約第 19 條，外國船隻享有「無害通過」權，但不得對沿海國的和平、良好秩序或安全構成威脅。條文列舉數項「非無害行為」，其中包括（a）對沿海國主權或政治獨立的武力威脅、（c）為損害國防而蒐集情報、（d）涉及國防的宣傳行動，以及（k）干擾通訊系統或其他設施。第（k）款尤其

與網路攻擊密切相關，暗示若在通過時干擾對方的通訊設施，即可能構成違法（United Nations Convention on the Law of the Sea, 1994, Article 19）。

2. 第 109 條則規定，各國應合作制止來自公海的未授權廣播，定義為「從船舶或設施向大眾傳送音訊或電視節目，違反國際規範者，但不包括求救訊號」。因此，若網路攻擊透過海上船舶侵入並發送違法訊號，可能構成此規範之違反（United Nations Convention on the Law of the Sea, 1994, Article 109）。
3. 第 113 條要求各國制定法律懲罰蓄意破壞海底電纜的行為，包括透過網路攻擊導致的損害。若攻擊涉及跨國海底電纜系統，行為即可能構成應受追究的國際不法行為（United Nations Convention on the Law of the Sea, 1994, Article 113）。

整體而言，海洋法雖非專為網路攻擊設計，但部分條文已能提供有限的法律依據以應對海上發動的數位威脅（Hathaway et al., 2012, pp. 872-873）。

三、國際案例分析：三種網路攻擊因應模式

在面對國家主導的網路攻擊時，受害國常採取三種策略，選擇的博弈背後往往牽涉深層的地緣政治考量。其一為「沉默與不歸咎策略」，如伊朗在 2008 年震網事件、以及沙烏地阿拉伯與卡達於 2012 至 2017 年間遭遇 Shamoon 攻擊時所採行，出於避免直接挑戰強權、維持區域穩定或避免引發報復行動的政治現實，選擇不公開指責攻擊國。第二為「歸咎但法律立場保留策略」，即國家雖政治上點名攻擊來源國，但刻意不明言是否違反國際法，保留外交協商與未來對抗的彈性，常見於與大國有經濟或軍事依存關係的國家。第三為「歸咎與多邊聯合認定策略」，如美國與歐洲盟邦對中國 APT 駭客或俄羅斯選舉干預的回應，透過跨國合作建立指控的可信度，強化集體回應，顯示出地緣聯盟在網路安全領域的重要性。這三種模式反映國家在高度敏感且具戰略意義的網路空間中，如何在法律、政治與地緣結構間尋求平衡（Sander, 2019, pp. 365-368）。

（一）沉默與不歸咎策略

2008 年伊朗的震網事件是歷史上首次確認由國家主導的網路攻擊之一。儘管該攻擊導致離心機出現異常運作，伊朗當時並未立即察覺是網路攻擊所致，也未公

開將攻擊歸咎於其他國家（Sander, 2019, pp. 365-368）。類似情況同樣出現在 2012 至 2017 年間的 Shamoon 攻擊中，沙烏地阿拉伯與卡達的能源部門及媒體機構遭受嚴重破壞，然而兩國政府迄今未公開指責任何國家或組織。這種策略可能出於政治考量，避免衝突升高，但同時也可能使攻擊者得以持續行動，缺乏必要的威懾效果，尚且可稱之為沉默與不歸咎策略（silence as pertaining to the what attribution question）（Sander, 2019, p. 365）。

（二）歸咎但法律立場保留策略

第二種網路攻擊因應模式，學者稱之為歸咎但法律立場保留策略—— "publicly attributing cyber attacks to other States whilst remaining silent about whether international law is applicable to the situation"，其具體事例為 2014 年，美國 Sony 影業遭駭客入侵，事件不僅造成巨額財產損失，隨之觸發對國家資訊安全的高度警覺。美國政府迅速公開指控北韓為幕後主使，並對相關個人及機構祭出制裁。然而，美國並未就該攻擊是否違反國際法發表明確法律意見。這反映出美國傾向將此類行為視為「具敵意的行為」而非明確的「武力使用」，進而保留政策與法律空間（Sander, 2019, p. 366）。

（三）歸咎與多邊聯合認定策略

最後一種的策略乃歸咎與多邊認定策略—— "publicly attributing them to another State and confirming that the pattern of operations constituted a violation of international law"（Sander, 2019, p. 367）。2017 年 WannaCry 勒索病毒在全球造成大規模癱瘓，英國、美國及其他五眼聯盟國家（包含加拿大、澳洲、紐西蘭）相繼公開指控北韓為攻擊主謀。該事件是跨國聯合歸咎的典型案例，不僅展現出網路安全合作的重要性，也強化了攻擊來源國的政治壓力。值得注意的是，科技企業如微軟也加入歸咎行列，顯示出民間力量在網路安全領域扮演日益關鍵的角色（Sander, 2019, pp. 366-368）。

綜合以上所述，當前國際社群對網路敵意行為的回應暨究責模式歸納如表 1。

表 1
網路攻擊各國歸咎策略歸納表

因應模式	具體事例	發動主體	有無科技企業介入
沉默與不歸咎策略	2008 年伊朗震網事件、2012-2017 年 Shamoon 攻擊	伊朗、沙烏地阿拉伯、卡達	無
歸咎但法律立場保留策略	2014 年索尼影業遭駭事件	美國	無
歸咎與多邊聯合認定策略	2017 年 WannaCry 勒索病毒事件	英國、美國、加拿大、澳洲、紐西蘭	有

四、國家責任與盡職調查之適用與解釋

（一）國家責任歸因的適用侷限與解釋取向

綜上以言，鑒於當前網路攻擊日益盛行管制不易，基於網路環境及互聯網技術有其直接歸因上的技術困難性，聯合國國際法委員會（The International Law Commission, ILC）2001 年通過的《關於國家不法行為責任的條款草案》（*Draft Articles on the Responsibility of States for Internationally Wrongful Acts*, 以下簡稱《草案》）第 4 條至第 8 條明定國家行為的歸責原則。第 4 條確認，無論是行使立法、行政或司法等職能的任何國家機關，其行為均可歸責於國家；該等機關可包含具有此地位的個人或實體。第 5 條進一步擴張至非正式國家機關但依法受權行使政府權力的個人或實體，其在行使該等職權時所為行為亦可歸責於國家。第 6 條則處理跨國支配情形，即當一國機關受另一國控制並代表後者行使政府職能時，相關行為歸屬於支配國。第 7 條強調，即使行為者逾越職權或違背指示，只要其名義上仍為國家機關或授權者，行為仍視為國家行為。第 8 條則涵蓋非正式代理人，只要行為人實際受國家指揮、控制或指示，其行為亦可歸責於國家。整體而言，此部分規章明確釐清國家透過正式或非正式機構行為的歸責架構，實具有界定國際法上釐清國家責任的適用範圍之規範功能。

前揭《草案》規定可謂替國家機關的網路行動、他國機關的網路行動歸因與非國家行為體網路行動的責任確定揭示一可資參照的規範性指針。並且此歸因準則

也受到《塔林手冊 2.0》所部分承繼，舉例而言，《塔林手冊 2.0》第四章“Law of International Responsibility”一章中之規則 15 至 18 即直面網路行動歸責於國家的問題。根據前開規則，《塔林手冊 2.0》認為，地理因素在歸責問題上僅具有限的相關性。尤其當國家可能為了隱匿其行為，從其領土之外發動網路行動。例如，某國可指示（參見規則 17）位於他國的非國家行為者，將分布於多個國家的主機納入殭屍網路，並利用該殭屍網路攻擊受害國。此處的關鍵問題在於，該非國家行為者是否依據第一國的指示行事，而非其進行行動的地點。

如前揭手冊之規則 15 所述，網路行動發動之地，或殭屍電腦所在之國，僅因相關行為團體或殭屍電腦位於其境內，並不足以推定該國必然須對該行動負責。然而，若該領土國家未能對相關個人或網路基礎設施採取適當管控措施，則可能引發「應盡注意義務」問題。在此情況下，該發動網路行動之國家可能因自身未能採取必要補救措施而承擔國際責任，而非基於對該網路行動本身的歸責（朱玲玲，2019，頁 76），應予敘明。

（二）國家盡職調查義務之適用侷限

承上所述，於釐清網路行為與國家責任體系之關係後，需要續行處理的問題意識乃現行國際法體系是否足以規範跨國敵意行為？為何若干國家在既有國際法體系下仍選擇了歸咎但保留法律立場的譴責途徑？其具體成因實與網路敵意行動的本質與事實上對行為者進行歸屬判斷（factual attribution）上的困難使然。國際軍事法大儒 Michael N. Schmitt 即精闢地綜合國際法判決先例與《塔林手冊》對此一規範的詮釋後指出，部分國家對於將「應盡注意義務」（due diligence）原則適用於網路行為持保留態度，原因在於此舉將使其承擔相應的法律義務（Schmitt, 2015, pp. 71-72）。應盡注意義務源自「主權」原則。根據此原則，國家在其領土範圍內對各項事務與行為享有主權的同時，亦必然負有相應之法律責任（Schmitt, 2015, pp. 71-72）。

1941 年「煙塵事件仲裁案」（Trail Smelter Arbitration）中，國際仲裁法庭裁定，一國「於任何時候均有責任保護其他國家不受本國管轄範圍內個人所造成的損害行為」（Trail Smelter Arbitration, 1941）。嗣後於 1949 年，國際法院於其首案「科孚

海峽案」（Corfu Channel Case）中進一步指出：「每一國家皆有義務不得明知而容許其領土被用作從事侵害他國權利之行為」（Corfu Channel, 1949）。

然而，各界對於是否將此原則適用於網路空間持保留態度，亦屬情有可原，揆諸實際，某些國家的網路基礎設施經常被用來發動或協助對他國有害的網路行動，卻未涉及足以使該行為歸責於該國的任何國家行為（Schmitt, 2015, pp. 73-74）。再者，事實上對行為者進行歸屬判斷上的困難，會妨礙一國採取行動終止該等網路行動。此等顧慮在網路連結度高的國家尤其明顯，因為這些國家的惡意軟體感染率通常也最高。正因如此，這些國家的網路基礎設施極易受到惡意行為者的入侵，並被轉為殭屍網路（botnets），進而被用於對其他國家發動攻擊。換言之，這些國家恐將承擔最為沉重的「應盡注意義務」負擔（Schmitt, 2015, p. 74）。

肆、臺灣的網路攻擊風險與當前應對挑戰

臺灣因地緣政治敏感性長期處暴露於高度的資訊戰與網路攻擊風險之中。根據行政院發布之當前資安情勢分析，我國證券業遭 DDoS 攻擊、WannaCry 勒索病毒及遠東商銀 SWIFT 系統遭入侵事件，此外勒索軟體爆炸性成長、DDoS 攻擊遽增、組織型駭客猖獗，國內外資安威脅陡增（行政院資通安全處，2017）。目前，臺灣雖已建立《資通安全管理法》、設立國家資通安全研究院（National Institute of Cyber Security, NICS），政府已推動《國家資通安全戰略 2025》，強調「資安即國安」理念，並建立國家資安戰情協同應變中心，以及強化國家資通安全會報，提升整體資安韌性，惟仍面臨幾項來自制度面和執行面的多重挑戰，諸如歸責困難：臺灣缺乏足夠的技術與國際支援來進行攻擊來源溯源（attribution），導致難以對攻擊進行政治或法律回應，缺乏統一應對架構（目前資安事件的應變主要由各部會與民間單位個別處理）等。再者對於遭受的國家級攻擊是否屬於武力攻擊、是否適用國際法仍卻乏清楚立場，不啻加劇臺灣關鍵基礎設施遭受不預期威脅的突發性與脆弱性。根據本文前開分析，臺灣可從下列途徑強化網路攻擊應對策略。

一、建立分層回應模型

建立一套涵蓋政治、法律、外交與技術層次的「分層回應機制」，依據攻擊程度與來源可信度，分為低度、中度、高度危機應對模式。此一模式不僅需具備即時反應能力，更應融入「威脅中立性」、「內向聚焦」與「去政治化潛力」等韌性治理核心理念。

具體而言，在面對低度攻擊時，應以技術調查與快速修復為優先，並由國家資通安全研究院主導技術層面調查與系統恢復，同時持續監控相關威脅源頭是否擴大；由於此類攻擊未必能即時辨識來源，採取威脅中立（threat-neutral）手段，有助於提升整體資安結構對多樣威脅的普遍應對能力，例如資料備援、資訊同步與系統自動化回復。

當情勢升級為中度危機，則啟動政府跨部會協調與資訊發布機制，由國家資通安全研究院主導各部會資源調度與對外溝通。此階段強調「內向聚焦」（inward-focused），即此時與其對外歸責，毋寧應優先鞏固國內制度與資源整合，並聚焦於

圖 2
分層防禦機制示意圖

自我防禦能力的強化與社會秩序穩定。同時透過與民間企業、地方政府與公民社會的協作，強化各層級回應能量，提升整體國家韌性。

若攻擊明確可歸責於特定國家或組織，進入高度危機等級，則啟動外交與法律層面的反制機制。此時可由外交部發表聲明，提出國際訴求與尋求盟友支持，並由專業法律顧問團隊評估國際法之適用性與反制空間，例如援引《聯合國憲章》第51條自衛權原則，或參考《塔林手冊》提出國際法的回應策略與論述主張。

二、建立網路攻擊歸責標準與公開機制

建立網路攻擊歸責標準，例如攻擊工具特徵、指令與控制伺服器位置、語言指令特徵、攻擊歷史與目標一致性等。同時，建立公開歸責程序，在符合證據標準的情況下，由政府正式對外說明並發表政策立場，以建立國內外的信任。

本文分析三種主流網路攻擊歸責策略——「沉默與不歸咎」、「歸咎但保留法律立場」與「歸咎與多邊聯合認定」——之後，紆衡臺灣當前的國際地位、地緣政治處境、對外關係與資訊化戰爭所受威脅的型態，當前最適合臺灣採取的策略乃第二種：「歸咎但保留法律立場策略」。此一策略兼顧政治彈性、外交空間與國內外輿論管理，是在實力不對稱與國際承認受限下，相對穩健且具操作性的選項。

（一）政治與法律彈性兼具

首先，若直接採取「歸咎並訴諸國際法」的模式，網路攻擊歸責標準不明與國際法對於網路敵意行為意涵不清的基礎上，恐陷入更複雜的話語權競爭。相對而言，透過政治點名特定來源國，卻不立即啟動法律反制程序，可保留外交協商與未來回應的操作空間，同時對外表明立場、維護自身正當性與主權主張。

（二）因應地緣政治與軍事現實

考量臺灣長期面對的是來自中國的複合性灰色地帶作戰行為（如 APT 攻擊、假訊息滲透、供應鏈破壞等），直接採取「公開聯合歸責」可能引發對方更強烈的反制或侵擾行為，也可能致使第三方國家降低合作意願。因此，保留法律立場可作為一種戰略性模糊手段，減少地緣對抗的激化風險。在國內方面，透過有限度的公

開歸責，可回應社會對透明資訊的需求，強化民眾對政府的信任感；在國際方面，即使無法全面參與多邊安全合作機制，仍可藉由明確的政治語言與一致政策回應，建立臺灣在資安責任與規則遵守上的形象，促進理念相近國家的信任與合作意願。

（三）搭配公開歸責標準與程序建構，提升可信度

臺灣應通盤檢視現行既有法制，分別就電信資通訊技術、航空或海洋領域所規範的傳輸技術、設施或活動，這些「手段導向」或「途徑導向」的網路攻擊之法律意涵與違反後的制裁法律效果，形諸明文，建立一套制度化的歸責標準與公開機制，在對國際社群有限參或嗣後採多邊認定的情況下，也能以高度專業與透明的方式爭取國際輿論支持，彌補法律地位的弱勢。

三、明確國際法立場與解釋取向

總結上述討論，「歸咎但保留法律立場」策略提供了高度彈性與實務可行性，符合臺灣當前的國際角色與資安風險態勢。此策略既不會讓網路敵意行為無從究責，又不至於過度升高衝突風險，是臺灣在灰色地帶戰爭與認知作戰下穩健而務實的回應方式。搭配制度化歸責流程與跨部門協調機制，更能使此策略發揮最大效益。

其次，主管機關應針對網路攻擊是否構成「武力使用」或「武裝攻擊」提出法律見解，並釐清國際人道法、主權原則、禁干涉原則在網路領域的適用情境。同時，應修法擴大《資通安全管理法》適用範圍，涵蓋重要民間平臺（如社群媒體、雲端服務提供者）與跨境數據流通。而這類關鍵資訊基礎設施（critical information infrastructure, CII）所潛藏的弱點亦成為駭客或敵軍攻擊的目標。由於關鍵基礎設施具有相互依存的特性，部分關鍵基礎設施如果遭駭而失效，可能引發連鎖衝擊，造成系統性全面崩潰，不僅擾亂民眾生活秩序，也阻礙經濟發展，更可能危及國家安全。

在備受爭議的歸責議題上，若攻擊明確可歸責於特定國家或組織，則啟動外交與法律層面的反制機制，自不待言，而在非國家行為體涉嫌發動之攻擊之情境下，學者參考前揭國際法各項淵源與《塔林手冊》提出的判斷基準頗值參考，亦即當有害的網路活動可追溯至某政府的電腦時，除非該國能提出令人信服的解釋，證明該

電腦是被外部操控，否則該行動將被歸責於該國。而在當今網路行為也可能由非國家行為者（non-state actor）所發動之情境脈絡下，根據國際法，若非國家行為者的行動造成對他國的損害，僅在該行動可歸責於某一國家時，該國才須承擔國家責任（Couzigou, 2018, pp. 38-39）。

根據國際法，非國家行為者的網路行動可歸責於一國的情形，尤其包括下列三種情況：

第一，根據《國際不法行為國家責任草案》第 5 條關於行使政府權力要素的個人或實體之行為規定一節，系爭行動是由獲國家授權行使政府職權之個人或實體所為。例如，若國家授權某私人公司執行通常由政府行使的職權，並要求其執行網路行動，則該行為可歸責於該國（Couzigou, 2018, pp. 38-39）。

第二，當國家明確承認並採納某一網路行動為自身行為時，該行動亦視為該國之行為（Couzigou, 2018, pp. 38-39）。

第三種情況，也是最常見的一種，是行動實體係在一國的指示、指導或控制下執行行動。例如，當一國僱用某個人或某個組織來發動網路攻擊時在此情形中，該國對該行為的指導或控制程度必須是高度的，亦即，該國應對特定的網路行動具有實質上的指揮或控制。是否構成這種情形，應根據個案具體事實加以判斷（Couzigou, 2018, pp. 38-39）。[2]

伍、結論：以數位韌性為圭臬的中長程因應策略

資訊化戰爭已是各國莫不苦於應對之國家課題，隨著數位依賴的深化，臺灣所面對的網路安全挑戰日益嚴峻，卻無系統化、持續性的，以加強數位韌性為圭臬的中長程策略因應。其次，網路敵意行為跨越疆界、難以明確釐清歸責的特性，更突顯出現行國際法對於網路攻擊回應的制度性缺口。無論是國家行為者或非國家行為者，其交錯進行的網路行動，常在法律定義與實務操作上模糊不清，使得相關國際規範在適用上備受侷限。

[2] 參見國際法院 1986 年尼加拉瓜訴美國案（Nicaragua v. U.S.）乙案。Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States), 1986 I.C.J. 14.

本文爬梳目前的國際法體系，發現當前國際法上對於網路攻擊之相關準繩雖涵蓋聯合國框架下的資訊安全決議與北約主導的《塔林手冊》，但整體而言，前者多屬原則性宣示，欠缺法律強制力；後者雖為西方主導的初步法制建構嘗試，卻亦未具國際法律地位，尚無法形成普遍約束力。此顯示國際社會雖已意識到網路安全的重要性，但實質法治建構仍處於初步階段。

面對此一局勢，國際社會主要採取三種因應模式，包括「保持沉默不歸咎」、「歸咎但保留法律立場」以及「歸咎並尋求多邊聯合認定」。這些模式反映出各國在國際法秩序博弈中的策略選擇，也揭示出在國際共識尚未形成之前，國家多傾向保留法律彈性以維持自身利益。承襲此一脈絡，本文主張臺灣採取多層次策略應對此一挑戰。首先，需加強本土法律制度建構，明確界定網路攻擊與資安應對的法理基礎。另則須建立具備韌性的數位治理架構，不僅提升防禦能量，更應強化整體社會對資安風險的認知與韌性，加強社會對數位威脅的承受與復原能力及持續性，同時構築邁向兼顧本土需求與國際接軌的資安防禦韌性之國家安全戰略，俾利臺灣於變動不居的網路地緣政治中，確保自身安全與國際法治參與的能動性。

參考文獻

上海合作組織成員國保障國際信息安全政府間合作協定，2009 年 6 月 16 日，https://www.doj.gov.hk/en/external/pdf/lawdoc/127.pdf [Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization, June 16, 2009.]

朱玲玲（2019）。從《塔林手冊 2.0 版》看網絡攻擊中國家責任歸因的演繹與發展。當代法學，**2019**（1），70-78。[Zhu, L. L. (2019). Deduction and development of state responsibility attribution in cyber attacks from the perspective of Tallinn manual version 2.0. *Contemporary Law Review*, *2019*(1), 70-78.]

行政院資通安全處（2017）。當前資安情勢分析。行政院，11 月 2 日。https://www.ey.gov.tw/Page/448DE008087A1971/07afd354-6fb9-41dc-9091-929db6d8358a [Department of Cyber Security, Executive Yuan. (2017). *Dangqian zian qingshi fenxi*. Executive Yuan, November 2.]

林昕璇（2023）。淺談網路犯罪、網路戰與網路攻擊之分際線。載於丁綺萍（主編），數位韌性與科技倫理（102-107 頁）。財團法人台灣網路資訊中心。[Lin, H. H. (2023). Qiantan wanglu fanzui, wanglu zhan yu wanglu gongji zhi fenjixian. In Q. P. Ding (Ed.), *Shuwei renxing yu keji lunli* (pp. 102-107). Taiwan Network Information Center.]

孫國祥（2015）。《塔林手冊》的介紹與初步評析。全球政治評論，（51），167-173。[Sun, K. H. (2015). Introduction and assessment of the Tallin manual. *Review of Global Politics*, (51), 167-173.]

黃浩珉（2025）。海底電纜斷裂危機下，台灣維繫「數位生命線」的應變挑戰。報導者，2 月 13 日。https://www.twreporter.org/a/damaged-undersea-cables-raises-alarm-in-taiwan [Huang, H. M. (2025). *Haidi dianlan duanlie weiji xia, Taiwan weixi "shuwei shengming xian" de yingbian tiaozhan*. The Reporter, February 13.]

蘇思云（2025）。海纜安全危機 3 ／專家：海纜如台灣「數位生命線」99% 網路頻寬都靠它。中央社，1 月 10 日。https://www.cna.com.tw/news/aipl/202501100036.aspx [Su, S. Y. (2025). Hailan anquan weiji 3 / Zhuanjia: Hailan ru Taiwan "shuwei shengming xian" 99% wanglu pingkuan dou kao ta. Central News Agency, January 10.]

Broeders, D., De Busser, E., & Pawlak, P. (2020). *Three tales of attribution in cyberspace: Criminal law, international law and policy debates* [Policy brief]. The Hague Program for Cyber Norms. https://www.thehagueprogram.nl/wp-content/uploads/2020/04/Policy-Brief_Three-Tales-of-Attribution_Broeders-De-Busser-Pawlak.pdf

Constitution of the International Telecommunication Union, 1992.

Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 22 (Apr. 9).

Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, 2019 O.J. (L 129) 1.

Couzigou, I. (2018) Securing cyber space: The obligation of States to prevent harmful international cyber operations. *International Review of Law, Computers & Technology*, *32*(1), 37-57. https://doi.org/10.1080/13600869.2018.1417763

Citron, D. K., & Eichensehr, K. E. (2025). Resilience for a digital age. *University of Chicago Legal Forum*, *2024*, 45-74. https://chicagounbound.uchicago.edu/uclf/vol2024/iss1/2

Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. (2021). *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (Report No. A/76/135). United Nations. https://undocs.org/A/76/135

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. (2015). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (Report No. A/70/174). United Nations. https://undocs.org/A/70/174

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review*, *100*(4), 817-885.

Katagiri, N. (2021). Why international law and norms do little in preventing non-state cyber attacks. *Journal of Cybersecurity*, *7*(1), tyab009. https://doi.org/10.1093/cybsec/tyab009

Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14 (June 27).

Nguyen, C. L., & Golman, W. (2021). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'. *Computer Law & Security Review*, *40*, Article 105521. https://doi.org/10.1016/j.clsr.2020.105521

Lin, H. S. (2010). Offensive cyber operations and the use of force. *Journal of National Security Law & Policy*,

4(1), 63-86.

Luzzatto, C. A. (2022). Regulating cyber warfare through the United Nations. *The Cyber Defense Review*, *7*(4), 261-270.

Sander, B. (2019). The sound of silence: International law and the governance of peacetime cyber operations. In T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, & G. Visky (Eds.), *2019 11th International Conference on Cyber Conflict: Silent battle* (pp. 361-382). NATO CCD COE Publications.

Schmitt, M. N. (2015). In defense of due diligence in cyberspace. *Yale Law Journal Forum*, *125*, 68-81.

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations* (2nd ed.). Cambridge University Press. https://doi.org/10.1017/9781316822524

Sigholm, J. (2013). Non-state actors in cyberspace operations. *Journal of Military Studies*, *4*(1), 1-37. https://doi.org/10.1515/jms-2016-0184

Trail Smelter Arbitration (U.S. v. Can.), 3 R.I.A.A. 1911, 1963 (Arb. Trib. 1941).

United Nations Convention on the Law of the Sea, 1994.

《台灣戰略研究》第二卷第一期
2026 年 1 月　59 ～ 91 頁

Taiwan Strategic Studies, Vol.2 No.1
January 2026, pp.59-91
DOI: 10.30249/tss.202601_2(1).0003

德國對中國政策的轉型：「紅綠燈聯盟」的中國戰略報告與「黑紅聯盟」的對中政策分析

沈有忠 *

摘　要

德國 2021 年聯邦議會改選，社民黨成為第一大黨，Olaf Scholz 出任總理籌組中間偏左的「紅綠燈」聯合內閣，並意味著由前總理 Angela Merkel 所領導的中間偏右聯合內閣，正式結束長達 16 年的執政。德國的中國政策在選舉期間就已經是各黨激烈辯論的外交議題，選後出現政黨輪替，紅綠燈聯合內閣如何調整德國的中國政策，遂成為全球關注的焦點。然而，隨著新冠疫情全球爆發，加上俄國入侵烏克蘭，一方面延遲了德國對中國政策的調整，另一方面也成為影響新版中國政策的偶發因素。最終，新版的《中國戰略報告》，遲至 2023 年 7 月才正式對外公布，內容調整了德中的雙邊關係，依據不同議題將中國設定為伙伴、競爭者以及對手。德國後續在 2025 年再次進行聯邦眾議院改選，基民／基社盟重回第一大黨，並由 Friedrich Merz 著手與社民黨再次組成「大聯合內閣」。因應新內閣以及國際局勢的變化，德國是否會再次調整中國戰略值得關注。

關鍵詞：德國、中國戰略、紅綠燈聯合內閣、大聯合內閣、俄烏戰爭

* 東海大學政治學系教授，Email: yuchung@thu.edu.tw。
收件：2025 年 5 月 5 日；一修：2025 年 7 月 4 日；二修：2025 年 8 月 8 日；接受：2025 年 12 月 15 日。

The Transition of Germany's China Policy: Traffic Light Coalition's "Strategy on China" and the Grand Coalition's China Policy

Yu-Chung Shen**

Abstract

After Germany's 2021 Federal Election, the Social Democratic Party became the largest party. Olaf Scholz became the chancellor to form a center-left coalition cabinet so called "Traffic Light Coalition", which meant that the center-right coalition cabinet led by former Chancellor Angela Merkel officially ended 16 years of rule. Germany's China policy was already a diplomatic issue that was hotly debated by all parties during the election. After the election, there was a rotation of political parties, and how the traffic light coalition cabinet adjusted Germany's China policy became the focus of global attention. However, the global outbreak of the COVID-19 epidemic and Russia's invasion of Ukraine have delayed Germany's adjustment to its China policy on the one hand, and have also become incidental factors affecting the new China policy on the other. In the end, the new version of the *China Strategy Report* was not officially announced until July 2023. The new federal election was held in 2025. The CDU/CSU has regained the largest party again, and Friedrich Merz has formed a new "Grand Coalition". In response to the new cabinet and changes in the international situation, Germany's future 'China strategy' is worth paying attention to.

Keywords: Germany, strategy on China, traffic light coalition, grand coalition, Russia-Ukraine war

** Professor, Department of Political Science, Tunghai University. Email: yuchung@thu.edu.tw

壹、前言：德中關係的回顧

德國聯邦政府於 2023 年 7 月 13 日，由綠黨籍的外交部長 A. Baerbock 正式對外公布了新版的《中國戰略報告》（*Strategy on China of the Government of the Federal Republic of Germany*），意味著德中關係正式進入轉折。事實上，在《中國戰略報告》正式公布以前，外界對於德中雙邊關係出現變化就已經有所準備，一方面是執政的「紅綠燈聯合內閣」自 2021 年上臺，其中綠黨（Bündnis 90/Die Grünen）和自由民主黨（Freie Demokratische Partei, FDP）早在選前就已經將調整對中關係列為主要外交政見，並且被視為各政黨中，對中國立場趨於強硬的鷹派。因此，新政府上臺後，調整對中政策成為必然趨勢。另一方面，俄羅斯於 2022 年入侵烏克蘭，俄烏戰爭爆發。這場戰爭對德國與歐盟國家形成巨大的威脅，當歐盟國家與北美和全球其他自由民主國家同聲譴責與制裁俄羅斯之際，中國選擇中立，不僅未加入制裁行列，甚至不時表態維持親俄的立場，這使得德國內部對於中國是否能成為德國的「全球戰略伙伴」感到質疑。在俄烏戰爭的衝擊下，調整對中關係也成為勢之所趨。然而，在這份《中國戰略報告》公布一年後，2024 年紅綠燈聯合內閣宣布提前國會改選，選後由基民黨／基社盟（CDU/CSU）重回第一大黨，並於 2025 年由 Friedrich Merz 擔任總理，籌組「大聯合內閣」。當前新政府是否延續這份戰略報告？或是會再次調整對中政策？值得關注。

回顧德中關係的發展，1972 年建交以來，雙方從經貿的互動為基礎，逐漸開展出日益緊密於議題多元的伙伴關係。其間因為 1989 年六四天安門事件，雙邊關係幾乎陷入停擺，但 1993 年德國公布《亞洲政策綱要》（*The Federal Government's Concept on Asia*），這是德國在冷戰後第一份關於印太地區的官方政策綱要，內容將印度、日本與中國定位為德國在亞洲的重點交往國家。此後，德中關係開始迅速成長，1993 至 1998 期間，雙方部長級以上的官員面對面的會晤就高達 52 次。2005 年德國眾議院改選，隸屬基督教民主黨（Christlich Demokratische Union Deutschlands, CDU）的 A. Merkel 成為首位女性總理，領導中間偏右聯合內閣展開長達 16 年的執政。在這段時間，伴隨中國崛起的現實，中國成為區域甚至是全球大國。德中雙邊關係不僅全面深化，也呈現經濟外溢、合作議題由內而外的轉變，

建立「大國外交」的合作模式。德中兩國在 2011 年建立雙邊政府磋商機制之後，2013 年的「帶路倡議」、2014 年兩國簽訂戰略伙伴關係，兩國的政治與經濟關係就日益緊密（Ciesielska-Klikowska, 2023, p. 38）。

儘管兩國在經貿議題有著緊密的伙伴關係，但在政治制度與價值議題上，兩國始終存在分歧，尤其是人權、自由與民主。在中國處理新疆和香港問題上，對於人權價值的破壞，引起德國高度關注，兩國關係在制度與價值差異上始終存在歧見。這些問題在 1990 年代後期就曾經引發兩國外交危機。1996 年 6 月德國聯邦眾議院通過決議文，譴責中國迫害西藏人權，並支持西藏自治。中國則以德國干預中國內政，關閉德國諾曼基金會（Friedrich-Naumann-Stiftung）在北京的辦事處，並取消同年德國外長 Kinkel 訪問中國的計畫作為報復。諾曼基金會作為自民黨（FDP）的政黨智庫，後來從北京遷往香港，更在香港雨傘革命、北京公布港版國安法之後，該智庫以安全為由，再從香港遷往臺北迄今。整體而言，雙方在意識形態和政治制度雖然存在差異，但在 Merkel 擔任總理期間，沒有成為雙邊關係發展的阻礙，彼此合作議題更是從經貿外溢到政治、範圍從雙邊延伸到全球（沈有忠，2018，頁 208；Ulatowski, 2022, p. 390）。

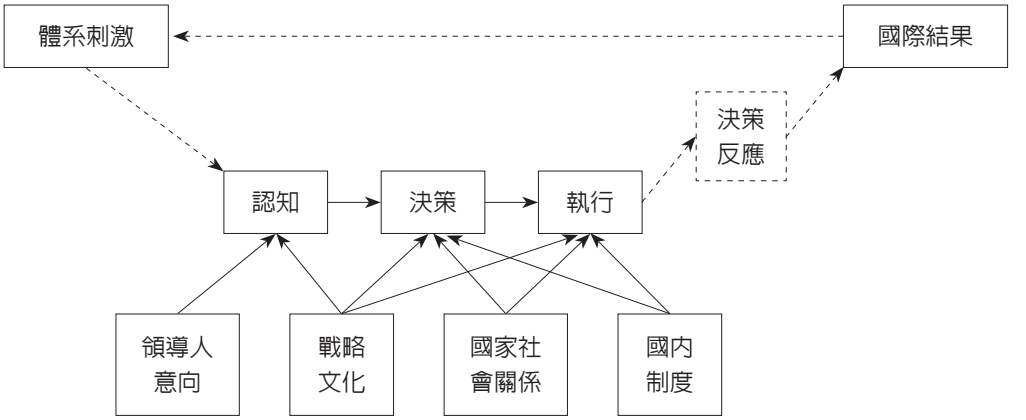
由前述可知，德中雙邊關係自 1993 年德國首次公布印太地區的政策綱要後不斷深化的發展，範圍由經貿外溢到政治以及區域安全。但伴隨中國持續的擴張性崛起，雙方在新疆、香港等人權議題以及自由價值上的分歧也越來越激烈。近年來到了 2021 年聯邦眾議院再次改選，紅綠燈聯合內閣上臺，而 2022 年爆發俄烏戰爭之後，雙邊關係正式出現巨大的轉折。簡單來說，當前德國對中政策的轉向，可以說是在價值分歧的結構性因素下，加上國內因素（政黨與選舉）與國際因素（俄烏戰爭）共同發揮影響，再加上決策者的認知所致。本文擬以新古典現實主義的分析架構，以結構性因素、國內以及國際的影響，加上決策者的認知，探討德國對中政策的轉向。主要以 2023 年公布的《中國戰略報告》進行內容分析，並就當前新政府黑紅聯盟的中國政策進行展望。

貳、新古典現實主義的分析架構

本文擬從國際局勢的變化，加上國內政黨政治的特性來探討德國 2023 年制訂中國戰略的過程和文本分析。在分析的途徑上，適用「新古典現實主義」（Neoclassical Realism）。客觀來說，研究外交政策的制訂，決策者的立場固然重要，但往往也會受到外部因素與國內因素共同影響甚至制約（Rose, 1998, p. 145）。在研究外交決策的理論中，新古典現實主義的分析途徑，就是主張應同時重視國內外的環境條件，以及決策者對外交事務的認知。Rose 在 1998 年首次提出新古典現實主義一詞，指出國家制訂外交政策，首先取決於國家在國際體系中的位置以及國家的權力認知。這是其之所以稱為「現實」的原因。但在評估其權力時，是間接且複雜的，尤其是決策者的主觀認知，這是其之所以為「新古典」的特性（Rose, 1998, p. 146）。新古典現實主義保留了現實主義對於國家利益與國際體系的重視，並加入了個別國家以及決策者對權力的主觀認知。有些學者或許質疑其是否能稱得上是國際關係的理論，但無庸置疑的，新古典現實主義是一個具有分析能力的研究途徑（Smith, 2018）。

國內學者鄭端耀（2005）評析新古典現實主義指出，該研究途徑強調國家外交政策行動同時受到國際體系和國內政治的影響，國內政治因素包括決策者認知、國內政治結構與國家利益（鄭端耀，2005，頁 128）。亦有學者指出，新古典現實主義在分析時仍舊承繼新現實主義對於體系與結構的假設與推論，再納入其他非體系（如國內政治因素）與非物質（如決策者的理念等）變項（廖舜右、蔡松伯，2013，頁 45）。基於前述的討論，以新古典現實主義來探究德國 2023 年制訂中國戰略的分析，要關注的面向即包括國際體系的變化、國內政治、決策者的認知等變數。在眾多變數中，Ripsman、Taliaferro、Lobell 等學者，將新古典現實主義的分析在自變數和依變數的部分都作了更細緻的推進。在依變數的部分，他們認所謂的外交決策，應該再細緻分為決策的認知、決策的制訂與決策後的執行三個階段，而自變數除了國際局勢對體系的刺激之外，也包括國內的領導者意向、國家的戰略文化、國家與社會關係、國內制度等變數。這些不同的變數分別在決策的三個階段中相互影響，最後決策後的執行產生反應，再回過頭影響國際局勢，整個過程會形成一組循環（Ripsman et al., 2016, p. 33）。分析架構如圖 1。

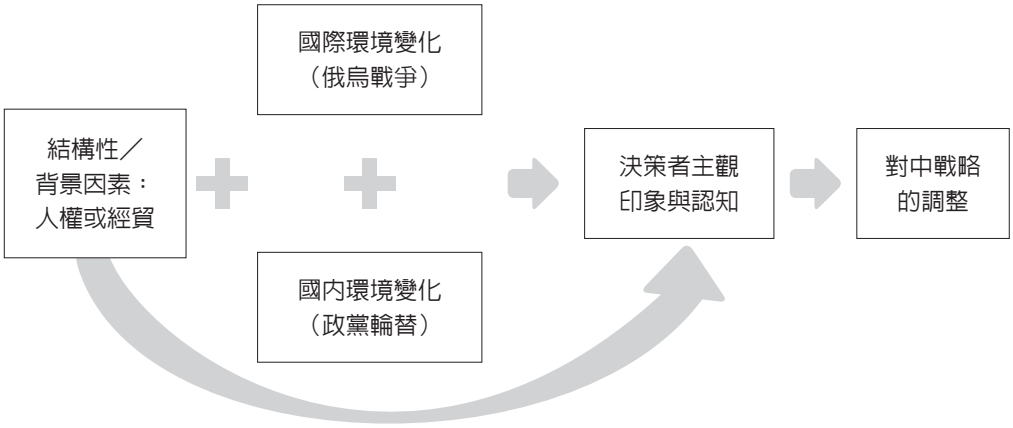
圖 1
新古典現實主義分析架構



資料來源：*Neoclassical Realist Theory of International Politics* (p. 34), by N. M. Ripsman, J. W. Taliaferro, and S. E. Lobell, 2016, Oxford University Press.

按圖 1 的分析架構，將整個外交決策的過程做了非常細部的分析，也增加了許多的變數。固然可以把外交決策的制訂脈絡和後續影響進行完整的分析，但兩難之處在於無法達到理論簡約化的效果。本文依據新古典現實主義的精神，將變數簡化為國際體系、國內政治、決策者因素，並且再加上一個背景條件，也就是決策制訂的「結構性因素」。本文認為，在制訂外交決策時，有其長時間累積的結構性基礎。在此結構性基礎之上，因為國際環境與國內政治的變化，影響了決策者從結構性因素中長期累積的認知，進而產生決策的調整與變化。在理論簡化的部分，作為一個研究紀要與初探，本文依據新古典現實主義的原型，將戰略文化、國家社會關係、國內制度等變數簡化為國內政治，並且依變數中的外交決策從認知、制訂到執行三個階段，都予以簡化為外交決策一個概念。分析架構如圖 2。

圖 2
新古典現實主義的分析架構

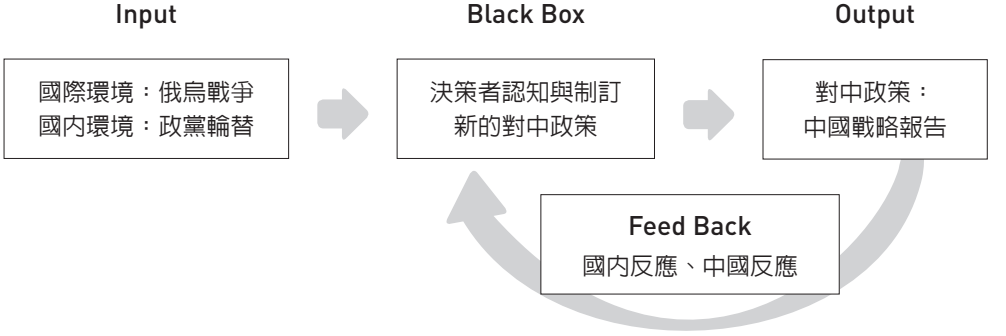


從圖 2 的架構中，以新古典現實主義的架構來看，結構性因素是背景因素，包括價值判斷與經貿利益。國際環境、國內的選舉，可以視為短期發生的自變項，決策者對於中國的認知則是中介變項，這個認知主觀上受到背景的結構性因素所框定，然後受到短期的國際環境與國內政治所影響。最後，本文所設定的依變項則是新政府對中國戰略的制訂。在這個分析框架下，本文認為，決策者對中政策的擬定，其感官認知的初始點是中國印象，一開始是來自於對中國的主觀想像出發，這樣的主觀想像是評定中國印象的標準。亦即，對於中國印象的投射，是來自於人權價值？歷史文化？經濟實力？意識形態？抑或其他。印象投射的結果，再受到國際環境與國內政治的影響，決定了制訂對中戰略的內容。例如，決策者對中國的想像，若是基於人權價值來建立中國印象，可能偏於負面；若是基於經濟實力，可能偏於正面。然後再受到國際政治與國內政治的影響，加深其中國認知，最終產出對中戰略的政策結果。

若以系統論（system theory）來看，這樣的分析架構也可以將國際環境變化當成輸入項（input），聯合內閣成為決策的黑盒子（black box），對中政策的產出則是輸出項（output）。只是就本案例來看，較欠缺反饋（feedback）的資料分析。本

文作為研究紀要，對於 2023 年所制訂的中國戰略，其後續的反饋與政策調整僅能以 2025 年德國新政府的論述為觀察對象略作分析。然而，2025 年上臺的 Merz 政府，是否會再度調整對中戰略尚無從得知，而市民社會或德國的企業對 2023 年中國政策的評價，也需要更多的資料來分析，應是後續值得研究的議題。系統論的分析架構如圖 3。

圖 3
以系統論分析 2023 年紅綠燈聯盟的中國戰略報告與黑紅聯盟的中國政策



依據圖 3 的系統論來看，影響體系的政策產出包括國際環境變化（俄烏戰爭）與選舉結果的政黨輪替（2021 年是紅綠燈聯合內閣；2025 年是黑紅聯合內閣）。而決策圈中的決策者認知和決策過程較為不透明，但就新古典現實主義的分析途徑而言，也是重要的中介變數。最後則是 2023 年《中國戰略報告》，以及黑紅聯盟對中政策的產出。在報告與政策方針公布後，必然引起國內社會（尤其產業）以及中國的反應，基於政策的穩定性，不會立刻調整或改變政府的對中政策，但有可能成為下一輪調整政策內容的變數。

參、對中政策的轉向：結構性因素與國內、國際政治環境的變化

德國在 2023 年 7 月正式公布《中國戰略報告》，究其內容而言，可以說是 21 世紀以來官方對中政策最大幅度的調整。以新古典現實主義來探究其轉變的過程，

整體來說是在結構性因素為基礎上，決策者基於國內與國際政治環境變化，建構其「中國認知」所導致的結果。所謂的結構性因素作為背景條件，主要有兩個可能的基礎：第一是中國經濟實力，帶給德國經濟成長的養分，因此必須與中國維持交往和經貿伙伴。相反的，背景的結構性因素也可能來自於中國持續性的經濟成長，並未帶來政治體制的開放與民主化，反而是透過經濟力量影響發展中國家，並成為西方民主國家的潛在威脅，因此必須改變對中國的經貿關係。這兩項結構性因素建立在經濟議題上，主要的原因在於眾多研究皆指出德國長期以來以經濟議題作為主導對中政策的依據。而德國與中國過於緊密的經貿關係，成為一個背景因素，是決策者的對中認知的起點。若是從經濟成長為目的，其對中國認知必然導向伙伴關係；從經濟安全與威脅來思考，對中國的認知將出現降低依賴的考量。而國際上的俄烏戰爭、選舉的政權輪替，新的決策者從經濟安全與威脅為認知基礎，出現了 2023 年調整中國戰略的結果。

在國際與國內政治的變數上，國際的政治環境變化，則是指美中全面競爭，以及俄烏戰爭的爆發。美國長期做為德國的盟友，美中從貿易戰升級為全面競爭，加上俄國入侵烏克蘭，中國不但未加入制裁，也未對和平與停戰做出積極貢獻，甚至與俄羅斯維持緊密的伙伴關係，使德國重新評估中國是否作為一個值得信賴的伙伴，也重新評估經濟上對中國過度依賴的風險。國內的政治環境變化，指的是 2021 年聯邦眾議院選舉出現政黨輪替，由 CDU/CSU 主導的中間偏右，相對保守也是主張持續與中國交往的梅克爾路線正式結束，取而代之的是社會民主黨（SPD）領導，加上綠黨與自民黨（FDP）的中間偏左紅綠燈聯合內閣。而綠黨與 FDP 的對中認知，則是從風險與經濟安全出發，與 CDU/CSU 有很大的差別。以下分別針對結構性因素以及國內外政治環境的變化進一步分析。

一、中國的擴張性崛起：經濟的伙伴或是威脅？

基於政權意識形態與制度本質上的差異，德國對於中國的人權與價值問題始終高度關注。早在 1970 年代，德國總理 Willy Brandt（SPD）提出「東進政策」（Ostpolitik），主張對東德加強接觸與交流，不僅改變兩德關係，在國際上也開啟德中雙邊關係的大門。此後，德國對於價值與制度迥異的中國，在人權與法治的議

題上，主張「透過接觸促成改變」（Wandel durch Annäherung）。到了 1993 年之後，兩國貿易大幅成長，在 Schröder 總理任內，甚至提出「透過貿易促成改變」（Wandel durch Handel）的主張，成為德國「遠東政策」（Fernostpolitik）的主軸（Kundnani & Parello-Plesner, 2012, p. 3）。換言之，從德國的角度來看，與中國接觸與強化貿易的往來，背後都希望能夠影響中國，促成中國意識形態與價值的轉變。也可以由此得知，德國與中國在價值與制度的上差異，從兩國交往開始就已經存在。

到了梅克爾執政時期，中國在印太地區持續的「擴張性成長」，尤其在新疆、香港對人權和法治造成的傷害日益惡化，引發德國各政黨一致的關注。國會內要求重新制訂對中政策的聲浪越來越大。在 2021 年聯邦眾議院選舉期間，自民黨和綠黨尤其展現出要求全面檢討對中政策的強硬態度，包括經貿，這和梅克爾主張接觸與交往的態度有很大的差異。選後，紅綠燈聯合內閣執政，基於中國認知的落差，主張重新檢討德國的對中政策，2023 年公布的《中國戰略報告》中，特別點出德國政府正在尋求重新進行德、中雙邊的「人權對話」與「法治對話」。同時，德國政府也依據 2023 年生效的《供應鏈盡職調查法》（Lieferkettensorgfaltspflichtengesetz, LkSG），要求德國企業評估中國投資帶來的人權風險，並制訂預防和補救措施。依據該法，德國得因應人權問題適當採取對中國的出口管制。凡此種種，皆可看出德國對中國人權與法治問題的關注，是影響兩國雙邊關係結構性的因素。兩國對人權、法治價值的分歧，不是偶然事件，是一種結構性的背景因素，而這項變數伴隨中國擴張性成長，成為印太地區不穩定的因素，尤其是香港、新疆人權法治問題的惡化。簡而言之，德國不同政黨對中國的認知和印象有不同的排序。梅克爾領導的保守黨，始終堅持經貿的往來，並認為透過伙伴關係可以促使中國改革開放，也帶給德國經濟成長的動能。而綠黨與 FDP 則是認為中國的經濟成長，不僅沒有帶來改革開放，更蛻變為擴張性成長的威脅，尤其在自身內部的人權惡化。也就是說，決策者的中國認知一開始就有差異，CDU/CSU 將中國視為伙伴，綠黨與 FDP 則視為威脅。這樣的認知差異終於在德國 2021 年選後的政黨輪替，綠黨和 FDP 加入聯合內閣，再加上國際上爆發的俄烏戰爭，加速了中國威脅的認知，使得德國在 2023 年制訂了新的對中政策，並且在梅克爾主政 16 年後出現了重大的轉向。Roderick Kefferpütz 在 2022 年初撰寫德國中國政策的分析，就指出德國社會在當時

存在三種對中政策的認知，一個是保守黨持續維持梅克爾長期「交往並改變」的接觸政策；一個是對中國採取較為嚴厲批判的聲音，以綠黨和 FDP 為代表；另一個則是和歐盟一致，對中國採取多種身分的定位，也就是視中國為伙伴、競爭者和制度性對手（Kefferpütz, 2022）。

二、國內因素：從中間偏右到選後的紅綠燈聯合內閣

從結構性因素可以看出德國內部對於中國政策一直以來就有不同的聲音，這是基於兩國制度上根本性的差異所致。再從德國的國內因素來看，當前德國外交與安全戰略，以及對中國政策出現轉變，可以從 2021 年選舉視為一個重要的分水嶺。2021 年第 20 屆的聯邦眾議院改選後，執政的聯合政府從 CDU/CSU 與 SPD 聯合執政的中間偏右大聯合內閣，向左轉為 SPD、綠黨、FDP 三黨聯合執政的「紅綠燈聯合內閣」，並由社民黨的 Olaf Scholz 出任總理，結束了長達 16 年的「梅克爾時代」。紅綠燈聯合內閣不僅是德國戰後第一次的三黨聯合執政，也出現對 Merkel 建立的外交與安全政策提出檢討的氣氛。

就新古典現實主義的觀點來看，此次聯邦眾議院的改選，結束了梅克爾的路線，聯合內閣的成員包括對中認知較為強硬、價值外交導向的綠黨與自民黨，自然是促成對中政策轉向的內部關鍵因素。亦即，在本文圖 1 的框架中，政黨輪替的結果，是由對中國認知偏向強硬、視為威脅，以及在結構性／背景因素上長期關注人權議題的綠黨和自民黨加入內閣，成為 2023《中國戰略報告》大幅檢討德國對中政策的國內因素。具體而言，紅綠燈聯合內閣在 2021 年籌組時，就已經達成調整對中國政策的協議，主要的內容包括：（一）將與中國的關係定性為「系統性競爭」，這裡的競爭關係，指的就是制度與價值差異。紅綠燈聯合內閣在調整對中關係上，希望「在與中國日益激烈的競爭中，制定公平的規則」。在人權和適用國際法的基礎上，會「盡可能」尋求與中國的對話。（二）人權被提及，特別是新疆地區少數民族的人權，那裡有數十萬人被關押在再教育營。（三）香港、臺灣問題和維護一個自由的印太地區成焦點。紅綠燈聯合內閣認為，民主的臺灣應該更緊密地融入國際組織，臺海兩岸衝突只能和平解決，香港應回歸「一國兩制」自治原則。新聯邦政府打算「顯著擴大」其在中國和印太地區的能力，並希望為「基於全球規

範和國際法的自由開放的印太地區」而努力。（四）預示紅綠聯合內閣「不再主要從經濟角度去看待與中華人民共和國的關係」。（五）在與中國的競爭中，德國也應該更多地參與歐盟的共同戰略。[1]

德國位在柏林的「國會研究中心」（Institute for Parliamentary Research, IParl），對德國主要政黨的中國立場進行分析，從政黨政治的角度來看，大致上來說，綠黨、自民黨一直被視為對中政策強硬的鷹派；社民黨相對溫和，尋找穩定與微幅的改變方式；而基督教民主黨與社會黨則是主張維持伙伴關係與持續對話；左翼黨基於社會主義的傳統，維持相對親中的路線；新興政黨另類選擇黨（AfD）主要訴求在於反難民、反整合的民粹路線，對中政策沒有太顯著的主張。[2] 因此，當 Merkel 領導的聯盟黨結束中間偏右的執政，改由社民黨、綠黨、自民黨籌組聯合內閣，對中政策往競爭的方向調整自然是可以預期的結果。

事實上，隨著中國崛起，對德國的經濟與安全形成不可忽視的力量，德國幾個主要政黨紛紛向選民表達了對中國的態度與立場，從中反映出不同政黨對中國認知的取向與價值觀，也提供我們觀察不同政黨主政時，可能採取的對中政策，也就新古典現實主義中強調決策者對外交政策認知的重要性。社會民主黨在 2020 年發布黨版的中國政策；基督教民主黨在 2023 年發布；自由民主黨也在 2023 年發布；綠黨儘管是德國國家戰略的推動者，但尚未發表明確的戰略文件，但在 2021 年選舉宣言中，廣泛提及中國高達 16 次。所有這些文件對中國的歷程和所面臨的中國挑戰都有類似的分析，但在強調未來道路選擇的方式上略有不同，綠黨在尋求合作機會方面更為悲觀，而社民黨似乎更為樂觀關於夥伴關係的議程（孫國祥，2023，頁 95）。這些主要政黨的表態，都顯示出德國亟欲重新定位中國的角色，而隨著對中國認知的評價差異，也影響了不同政黨主政下，將採取不同的對中政策。

三、國際因素：美中競爭與俄烏戰爭

從國際因素來看，國際政治的變化也是促成德國調整對中政策重要的外部因素，尤其是俄烏戰爭。基本上，由於德國和歐盟的外交政策維持高度一致，因此不

[1] 相關報導可以參見彭濤（2021）。
[2] 訪談資料。訪談對象為 IParl 中心主任 Danny Schindler，訪談時間 2023 年 7 月 6 日。

只德中關係，整個歐中關係在俄烏戰爭後都發生了變化。薛健吾認為，經貿為主軸的歐中關係難以在短期產生劇烈變化，但三個事件讓歐中關係轉往負面發展，分別是持續惡化的香港、新疆人權問題，COVID-19 疫情，第三個就是俄烏戰爭（薛健吾，2023，頁 29）。薛健吾進一步也以新古典現實主義解釋歐盟國家中，在地理上直接面對俄國威脅或是在地緣政治上將俄國定位為安全威脅的國家，對中國的威脅感更高，並且在俄烏戰爭後降低了與中國的和合作關係，這些國家中就包括德國（薛健吾，2023，頁 33）。也就是說，俄烏戰爭爆發後，中國第一時間沒有加入制裁的行列，後續也未對停戰與和平做出積極貢獻，沒有能展現大國應有的責任。不僅如此，中國與俄國的關係反而因為共同面對美國的壓力而日益緊密。基於國際政治的變化，德國對俄國不信任的氛圍，也轉變為對中國是否能成為可信任伙伴的疑慮。就本文以新古典現實主義的分析途徑來說，國際局勢的變化（俄烏戰爭）對德國產生新的國家安全觀，這個轉變包括德國對中國的外交關係定位，從戰略伙伴關係變成為制度性對手以及潛在的威脅來源，並且直接反應在 2023 年的《中國戰略報告》中。

德國學者 Sadeler 指出，當前的國際局勢下，與中國相關的議題都增加挑戰。現在人們日漸意識到，經濟利益也必須放在安全政策的範圍內看待；經濟和政治不能再分開看待和形塑；雙邊關係在許多領域皆缺乏互惠；中國正試圖破壞以法治為基礎的國際秩序，並利用這一秩序謀取自己的利益。而俄羅斯違反國際法對烏克蘭發動的侵略戰爭，或許最終喚醒了德國國內那些仍不願承認必須重新形塑與中國關係的人們，歐洲和德國都在密切關注中國對自身的定位。在聯邦議會「捍衛歐洲和平與自由：全面支持烏克蘭」之聯合提案當中，社民黨、基民盟／基社盟、90 聯盟／綠黨和自由民主黨等，都呼籲德國政府向中國傳達德國和歐盟的期望，放棄對戰爭的支持，積極支持停火，以及停止一些損害已實施的制裁的行動，甚至包括向俄羅斯提供武器都將導致經濟和個人制裁（夏瀾，2022，頁 16）。這段分析直接指出，過去德中關係是以經濟為主軸，現在必須以更宏觀的國家安全來看待，受到國際局勢的變化所影響，當經濟議題也成為國家安全的一部分時，德國對中政策就轉趨於保守。

依據慕尼黑安全會議 2023 年出版之《2023 年慕尼黑安全會議報告》（*Re:vision:*

Munich Security Report 2023），分析各國在 2022 年 11 月，也就是俄烏戰爭爆發後，分別就社會意向評估國家的安全風險來源。所調查的國家中，大多數西方民主國家都提高了對中國的風險評估。報告書中用「風險溫度計」進行評估，其中德國對中國的風險評估增加了 6 分，達到 63 分，是調查國家中分數第二高（僅次於日本），更是系列調查中，與前次相較風險溫度上升最多的國家（與前次相較提高 8 分）。相關資料請參見表 1。

表 1

各國對中國風險評估溫度計指數

國家	風險溫度指數	與前次評估相較
Japan	71	0
Germany	63	+8
USA	61	+1
Canada	60	+3
UK	59	+6
South Africa	54	-4
France	53	+1
India	51	-11
Italy	50	-1
Brazil	45	-9
Ukraine	19	X

資料來源：*Re:vision: Munich Security Report* 2023 (pp. 43-56), by T. Bunde, S. Eisentraut, N. Knapp, L. Schütte, J. Hammelehle, I. Kump, A. Mudie-Mantz, and J. Pauly, 2023, Stiftung Münchner Sicherheitskonferenz.

對於中國來說，俄烏戰爭也間接的影響了中國對美國以及對西方國家的關係。在 2020 年中共 20 大召開以前，全力維持國內外政治局勢的穩定，以完成 20 大通過習近平第三任期的政治議程，是習近平的首要目標。在當時的氣氛下，中共對俄烏戰爭盡量維持一種中立的狀態，就是希望不要成為西方國家接續制裁的對象。但事實上，在俄烏戰爭持續進行的情況下，中國並沒有減弱與俄羅斯的戰略夥伴關

係，外交立場備受歐美國家質疑。以北約對中國的反應為例，因應俄烏戰爭的發生，北約增強了共同防禦的機制，甚至尋求和澳洲、日本、南韓與紐西蘭建立全球夥伴關係，對中國形成壓力。2022 年 6 月，北約發布新版《戰略概念》（*Strategic Concept*），首度把中國列入對北約經濟、安全和價值的挑戰，並指出中國利用經濟、政治和軍事等工具，擴大全球影響力，也指出中國和俄羅斯之間不斷深化的戰略夥伴關係，以及相互加強破壞基於規則的國際秩序的企圖，與北約的價值觀和利益背道而馳。總體來說，德國的政治條件和民意氛圍，在 2021 年選後到俄烏戰爭的爆發，可以說是持續性的出現了一些變化。過往較於保守、不介入衝突、重視維持對俄關係的原則，慢慢的轉為積極介入、提高武裝。在對外威脅的評估部分，除了俄羅斯之外，對中國的評估，也成為主要的風險來源之一，成為德國聯邦政府重新制訂《中國戰略報告》的重要基礎。德國對中戰略調整的例子映證了新古典現實主義中，強調國家的外交政策必然受到國際局勢變化所影響的假定。

本紀要訪問了德國位於柏林最大的中國研究智庫 Mercator Institute for China Studies（以下簡稱 MERICS），訪談中該智庫研究員指出，俄烏戰爭的爆發迫使德國重新評估中國對德國的角色定位與影響。因為中國在戰爭中並未加入制裁行列，甚至連外交手段都沒有對俄國進行施壓。相反的，中國在許多國際場合或是提出的和平方案中，出現偏袒俄羅斯的情況。這讓德國感覺到，中國是否能成為可靠、信任的戰略伙伴出現重大疑慮。不僅如此，俄烏戰爭暴露出德國在能源進口過於依賴俄羅斯的風險，相同的，當前的德國在經濟上過於依賴中國，如果中國不值得信賴，甚至成為印太地區武力改變現狀的風險來源，未來一旦出現類似於俄羅斯的情況，將對德國帶來巨大打擊。[3] 因此，中國的戰略定位從「戰略伙伴」變成「競爭者」，加上經濟過於依賴的現實，對中國改採「去風險」的策略，也是俄烏戰爭帶給德國的雙重警示。

以新古典現實主義的分析途徑，綜合以上結構性因素、國內選舉結果以及國際上俄烏戰爭的影響來看，德國對中政策的轉變幾乎勢必然的結果。首先，德國不同政黨對中國的認知與評價在中國崛起後就出現分歧。有些側重於經濟的依賴而主

[3] 訪談資料。訪談對象為 MERICS 首席經濟分析師 Max J. Zenglein，訪談時間 2023 年 7 月 20 日。

張維持伙伴關係的連結；有些側重人權與自由的價值，強調制度性差異而偏向對中強硬的態度，這些是德中關係來自於背景的結構性因素。後續在國際上爆發俄烏戰爭，中國對戰爭的態度以及與俄羅斯深化合作，加深了各政黨對中國威脅的疑慮。而就國內的選舉來說，選後的紅綠燈聯合內閣，由認知上定位為對中鷹派的Baerbock（綠黨）出任外長，更加確立了對中戰略報告中，把中國朝向競爭者、對手的方向來調整。以行為者認知扮演關鍵中介變數來看，將中國以三重身分定位，也是凸顯出新內閣中總理 Scholz（SPD）與外長 Baerbock（綠黨）相互妥協的特性。整體而言，按本文以新古典現實主義的分析架構來看，德中關係的結構性因素本就存在價值上的差異、國際爆發俄烏戰爭突顯出中國威脅的疑慮、國內選舉由對中認知偏向強硬的政黨加入聯合內閣這些因素共同發揮影響，導致了對中戰略轉向的結果。

肆、《中國戰略報告》的公布與分析

2023 年 7 月 13 日，德國時間中午 12：00，由聯邦外交部長 Annalena Baerbock（綠黨），協同 Nils Schmid（SPD）、Nicolas Zippelius（CDU）等跨黨派國會議員，在智庫 MERICS 召開記者會，並正式發表了長達 64 頁的《中國戰略報告》。整份報告可以說非常謹慎的定位了中國的角色，也區分不同議題面向來界定德中關係。整體而言，德國公布的《中國戰略報告》，可以說延續了 6 月底歐盟對中戰略報告的特色，以「去風險」（de-risking）作為主軸，將對中關係以及中國的角色定位為伙伴、競爭以及系統性對手（partner, competitor and systemic rival）三種差異。在進入分析這份文件以前，可以先看看對中戰略提出以前，德國內部政黨立場，以及德中經濟關係的發展趨勢。

一、背景分析：聯合內閣下的務實與保守

事實上，早在 2021 年紅綠燈聯合內閣上臺時，就已經預告將會重新制訂對中政策，在地緣政治上，投入更多資源在印太地區也逐漸形成共識。對於中國的定位來說，把中國從 2014 年習近平訪問德國時，在聯合公報中的「全方位戰略夥伴關

係」，反轉成為「制度性的競爭對手」。另一方面，對國家安全的戰略思維調整，一方面降低對俄羅斯能源依賴，也思考經濟上如何重新平衡與中國過度依賴的關係。在疫情與俄烏戰爭兩個黑天鵝事件的影響下，加上三黨內部對細節的協調，以及等待歐盟整體對中戰略的制訂，這份《中國戰略報告》歷經多次辯論以及修正，一直到 2023 年 7 月才正式對外發布，距離聯合內閣上臺長達將近 2 年之久。

以新古典現實主義的分析途徑來看，決策者的認知是影響決策的中介變數，因此分析決策者的認知有其必要性。就政黨政治來看，在紅綠燈聯合內閣中，綠黨可以說是最積極主張對抗中國的政黨。選舉期間，綠黨的總理候選人 A. Baerbock（也是後來聯合政府中的外交部長）就曾公開表示，綠黨一旦參與組建新的政府，將對中國採取更強硬的貿易政策。Baerbock 後來成為德國的外交部長，對於聯邦政府制訂對中政策具有一定的影響力與話語權。稍晚在 2022 年 3 月，俄烏戰爭爆發後，Baerbock 當時也以聯邦政府外交部長的身份公開表示，聯合內閣在制訂新的德國國家安全戰略時，將會重新制訂對中政策。最後，在 2022 年 10 月曝光的戰略草案中，就直接點出：「德國外交部建議與歐盟同步，將中國描述為合作伙伴、競爭者和系統性對手，後二者尤其重要」。[4] 預告了聯合內閣的國家安全戰略中，將中國從戰略伙伴，轉變為競爭對手的變化。

德國當下的聯邦政府，是三個政黨組成的聯合內閣。在三黨共同執政下更加凸顯「務實、保守」的特性，所有對外政策的改變與制訂，都需要三個政黨的妥協，因此要有太大幅度的調整相當不容易，也反映出相對保守的結果。這也是本文前述反映出新古典現實主義中，行為者認知的重要性。依據與德國聯邦經濟合作與發展部（Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung），部長辦公室主任 Dr. Frank Meerkamp 的訪談指出，社民黨相較於綠黨與自民黨，因為是第一大黨，同時是總理所屬政黨，因此必須權衡經濟、安全、人權、外交、就業、能源……各項棘手議題，不能僅從單一部會的本位主義出發，因此顯得較為保守。尤其是經濟議題，要調整對中關係時，更需要謹慎，不僅要和其他聯合內閣的政黨達成一致，社民黨也希望與在野黨盡量取得共識，或降低反對聲浪。除了國會內的政

[4] 相關報導請參見德國之聲（2022）。

黨，就聯邦與地方來看，社民黨也希望在聯邦層級以及各邦政府都能有一致的共識。因此要調整對中的經貿關係、制訂新的中國戰略，對社民黨來說是一項非常巨大的工程。若是套用至 Ripsman、Taliaferro、Lobell 等學者對新古典現實主義為基礎，用更細緻的架構來分析，這段訪談中強調的聯邦制對聯邦政府制訂外交政策的影響，就是「國內政治制度」的特性。而決策者希望兼顧不同議題、也希望能得到聯合內閣甚至跨黨派的共識，則是反應出「領導者意向」以及「戰略文化」的特性。據此來看，以新古典現實主義來分析 Scholz 總理以及紅綠燈聯合內閣對中國政策制訂的謹慎，並且費時將近兩年才得以公布《中國戰略報告》，確有理論適用之處。

《中國戰略報告》的提出，對執政的社民黨來說，需要縱向（與各邦政府）與橫向（與各政黨）的協調，甚至還需要與歐盟與其他國家達成一致立場。再加上德中之間長期以來錯綜複雜，以及過於緊密的雙邊關係，也使得德國此刻公布的《中國戰略報告》，僅能以原則性點出方向。而其他各項具體政策和議題，都還需要跨部會、跨政黨來制訂具體的執行細節。

舉例來說，聯合內閣中對於是否在經濟上與中國脫鉤一直有不同的意見。聯合內閣中 FDP 的黨魁，聯邦財政部長 Christian Lindner 就表示，反對德國經濟與中國脫鉤，但對德國來說，其他市場必須變得更重要。這意味著短時間內德國不會立刻和中國變成完全競爭的關係，但會朝向降低對中國依賴的方向來調整。事實上，從經貿的角度來看，自 2016 年以來，中國一直是德國最大的貿易夥伴。幾乎占德國對外貿易總額的 10%，雙方在 2021 年的貿易額超過 2,450 億歐元，逆差約 400 億歐元（進口 1,420 億，出口 1,030 億）。再從兩國相互的經貿投資額比較，依據 2021 年的數據，德國對中國的投資總額，則是超過中國在德國的投資總額六倍之多（Müller, 2022）。再依據 2023 年的資料，中國第八年蟬聯德國最大貿易夥伴，德國對中國貿易逆差成長為 584 億歐元（進口約 1,557 億歐元；出口約 973 億歐元），是自 1950 年以來對中第二高的貿易逆差（第一高為前一年 2022 年的 861 億歐元逆差）。顯見德中兩國的貿易極為緊密，而且對德國而言是呈現逆差狀態。

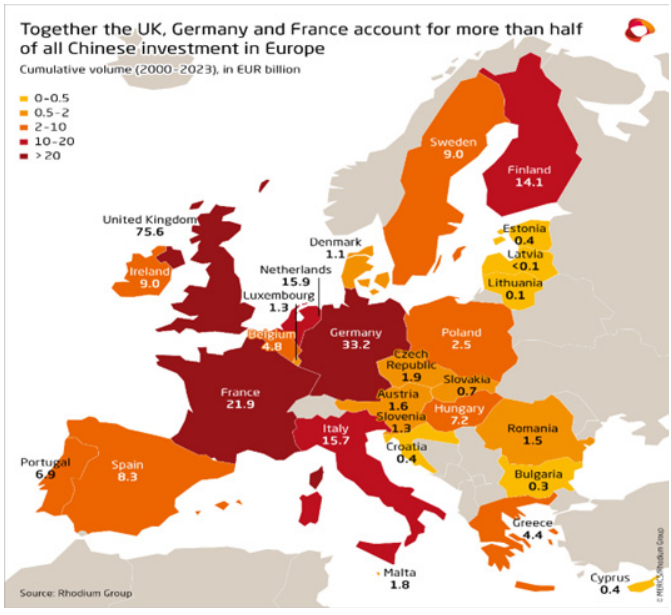
依據與 MERICS 研究員的訪談指出，德國經濟與中國連動緊密，尤其是汽車工業以及相關的機械與零件產業。由於德國是製造業為主的經濟結構，仰賴出口，要短時間調整出口結構並不容易。再受到俄烏戰爭影響，產業的脆弱面暴露，對中

國的風險評估即使增加，要調整與中國經濟往來的策略與結構，也非一蹴可幾。[5] 依據 MERICS 提供的文件資料與數據來看，觀察中國對歐洲國家的投資狀況，從 2000 年至 2023 年，中國在歐洲各國的投資中，以英國最高，累計達到 756 億歐元，德國第二，累計達到 332 億歐元。以歐盟國家來說，德國是唯一一個超過 300 億歐元的國家，這個資料也顯示了德中兩國經貿關係極為緊密的狀況。中國在歐洲國家投資狀況，請參見圖 4。

圖 4

中國對歐洲國家投資金額累計（*2000-2023* 年）。

單位：十億歐元



資料來源：*Dwindling Investments Become More Concentrated - Chinese FDI in Europe: 2023 Update*, by A. Kratz, M. J. Zenglein, A. Brown, G. Sebastian, and A. Meyer, 2024, Mercator Institute for China Studies (https://merics.org/en/report/dwindling-investments-become-more-concentrated-chinese-fdi-europe-2023-update).

總之，德國紅綠燈聯合內閣在 2023 年公布《中國戰略報告》，揭示了德國對中政策的轉型。然而，從新古典現實主義的角度來看，國內、國際環境的變化，僅能預示了德國的對中政策在此時機點必然出現變化。但變化的內容、幅度、與範圍

[5] 訪談資料。訪談對象為 MERICS 首席經濟分析師 Max J. Zenglein，訪談時間 2023 年 7 月 20 日。

甚至轉化為具體的政策，一方面受到既有德中關係的限制、二方面受到決策者意向與認知，以及整個執政團隊的共識建立，甚至包括聯邦制下的制度影響，這些都是影響這份中國略報告的變數。

二、新版中國戰略的目的

聯邦外長 Baerbock 在公布《中國戰略報告》的記者會上，用一連串數字描繪德國與中國之間充滿的矛盾。在中國的經濟成長方面，德國肯定中國在過去讓 8 億人口脫貧的成就，以及 8,700 萬度的太陽能裝置量，已經超越德國；在德中雙邊經貿之間，2,980 億歐元的雙邊經貿創下歷史新高；而中國限制出口的鎵，占全球 96%；69 艘軍艦，使中國成為全球軍艦數量最高的國家；100 萬港幣是中國對 8 名海外異議份子的懸賞。這一組數字肯定了中國的經濟成長、指出了德中的經貿依賴、中國的擴張性軍備、稀土出口對世界的影響力以及對香港人權與法治造成的破壞和威脅。德國認知到中國正在蛻變，經濟成長，但也成為區域穩定和人權法治的威脅。有鑑於此，德國必須調整對中政策，在《中國戰略報告》中指出，未來德國對中政策的制訂，方向上有五個目標：

1. 基本上指出德國聯邦政府對與中國關係的現狀和前景的看法；
2. 德國聯邦政府在與中國的複雜關係中，能有效地維護德國的價值觀和利益；
3. 提出德國聯邦政府與中國雙邊合作的方式，不能危及德國自由民主的生活方式、德國的主權、繁榮、與安全，以及與其他伙伴的關係；
4. 提供一個框架，使德國聯邦各部會能夠協調其中國政策；
5. 加強與德國、歐洲及其他利害相關者，在中國問題上協調的基礎。

這五項目的，綱領式的指出了德國對中政策的原則。字裡行間值得分析的有幾個地方：第一、對中政策要維持德國的「價值觀」和「利益」。就這點而言，已經看出中國對德國來說存在的矛盾。因為價值觀是衝突的，中國對人權、民主、法治的戕害，違背了德國的價值；但利益是掛勾的，中國在經濟實力甚至能源議題上的成就，是德國無法忽視的市場。單是這一點，已經足以說明德國將中國視為既是伙

伴也是對手的關係。價值觀與利益的矛盾，也說明了本文分析架構上，決策者對背景因素、結構性因素認知，將影響對中政策的制訂。顯然的，儘管紅綠燈聯合內閣包括了綠黨、自民黨等價值取向的政黨，但總理 Scholz 是社民黨，加上需要妥協，因此對背景因素的認知也就必須兼顧人權、民主的價值以及經貿利益的考量，充滿妥協。第二、德國對中政策對內要能整合，對外要能與地緣政治上（例如歐盟、北約等其他國家）相接軌。目的中指出的聯邦各部會的協調，以及與歐洲和其他利害相關者的協調，意在如此。就新古典現實主義的分析視角而言，德國的外交政策以及決策者的外交決策必然受到歐盟也受到國內政治制度的影響。第三、值得臺灣注意的一點，是措辭中提及德國和其他國家交往，避開了主權，而是使用了伙伴、利害關係的詞彙。這一點包括在對《中國戰略報告》中，後面多次提及的臺灣以及德臺關係有所關連。避免了政治上對主權國家的使用與承認，卻也包含進在德國在國際上有意深化的伙伴，後文就直接點出臺灣。

《中國戰略報告》的目的，價值的原則性取向大於具體的政策指導。在與 MERICS 以及德國媒體界訪談時，皆同意目前這一份《中國戰略報告》，是原則性揭示了德國未來對中國政策的「方向」，而欠缺具體的「內容」。主要原因就是在於德國認知到，與中國的關係既存在伙伴、合作的空間（尤其是經貿），也有價值上的衝突（人權、法治），而中國擴張性的成長，對地緣政治帶來的風險，更是影響德國的國家利益。[6] 在如此複雜的關係中，無法單一面向、單一議題的指出德中關係的發展趨勢，只能提出對中政策的基本原則，並且強調與歐盟和其他伙伴的一致性。

三、中國戰略的核心概念：去風險（de-risking）

過往，由於德國的經濟與中國市場過於緊密，因此常被形容為對中國過度依賴，在俄烏戰爭爆發後，這種過度的單一市場依賴，成為國家安全的風險。Noema 雜誌的主編、Berggruen 研究中心創辦人 Nathan Gardels 撰文指出，德國作為歐洲經濟的支柱，但在俄烏戰爭爆發前，德國的安全過渡依賴美國、能源依賴俄國、經濟則是依賴中國。俄烏戰爭的爆發將促使德國改變這三個依賴，儘管社民黨（SPD）

[6] 訪談資料。訪談對象為 MERICS 首席經濟分析師 Max J. Zenglein，訪談時間 2023 年 7 月 20 日。以及自由記者、撰稿員 Jens Kastner，訪談時間 2023 年 7 月 27 日。

的總理 Olaf Scholz、自民黨黨魁，身兼財長的 Christian Lindner 都表明，無意在經濟議題上與中國脫鉤，但也都同意，德國必須從烏克蘭戰爭中吸取教訓，必須避免片面依賴，尤其是中國（Gardels, 2023）。社民黨共同領導人 Lars Klingbeil 接受媒體 Zeit 訪問時也指出，由於德中雙方的經貿過於緊密，如果中國出兵臺灣，德國將與中國決裂，這將對德國造成重大的影響（Carrel, 2023）。從俄烏戰爭的教訓來看，德國現在必須開放其他市場，並積極尋找其他原材料貿易夥伴。「去風險」成為德國未來處理對俄、對中的政策原則。

去風險不表示脫鉤。以俄烏戰爭對德國能源供應的衝擊來看，德國在俄烏戰爭中尋求能源供應降低對俄羅斯的依賴，但不表示完全脫鉤。舉例而言，在戰爭期間，是否以限制原油進口進行對俄羅斯制裁，德國的立場和英、美相比顯得相對保守。在美國、英國相繼在 2023 年 3 月 8 日宣布禁止從俄羅斯進口原油以後，德國對此一制裁手段依舊保留。從官方反應來看，先是外交部長 Baerbock 之前就曾公開表示：「從現實考量，德國不會跟進英、美實施原油禁運的制裁」。接著也是綠黨籍的經濟兼能源部長 Habeck 也公開表示：「按照現實情況，德國短時間內無法完全禁止俄羅斯的能源進口。一旦全面禁運，恐怕會引發大規模的失業與貧窮問題，社會上出現暖氣停止供應或是交通工具無油可加的困境」（沈有忠，2022，頁 75）。

另一方面，因應德國提升能源自主與降低對俄羅斯的依賴，經濟部長 Habeck 也在 2022 年 3 月底陸續出訪挪威、卡達等國，商討再生能源以及分散天然氣進口等議題。綠黨不僅是德國能源轉型的推手，更是此次紅綠燈聯合內閣中，呼籲檢討德國外交政策最強硬的政黨。此次對於以能源禁運作為制裁手段的政策採取保留態度，勢必引發「理想與現實」相互矛盾的批評。也可以據此預期，俄烏戰爭將成為德國加速檢討能源政策，甚至可能在這一屆聯合政府就會有具體的改革內容。

以去風險、不脫鉤的原則處理德國對俄羅斯能源進口的議題，也成為德國處與中國經貿往來的原則。在 7 月 13 日公布的《中國戰略報告》中，特別強調德國呼籲企業對於中國市場保持警覺，提出了「去風險」的概念。報告指出，對於醫療技術、能源轉型所需要的稀土、甚至像是臺灣海峽對產業供應鍊，尤其是半導體的影響，都顯示中國對於市場穩定扮演不確定的風險因子。另外，像是企業前往

中國投資，面臨的是市場准入和投資機會的限制、被排除在公共政策之外的不平等競爭，例如公共補貼、監管歧視、強迫知識和技術轉讓，以及對知識產權的保護不足等。這些是市場競爭概念下，前往中國投資面臨到不公平競爭的風險。聯邦政府有責任提醒德國企業進行風險評估，也呼籲中國政府維護公平競爭的市場機制。

整體來說，聯邦政府無法透過法律限制企業前往中國投資或降低與中國的市場往來，但聯邦政府可以透過政策鼓勵企業在海外市場投資的多元化，這樣可以符合企業和國家的利益。再者，聯邦政府對於海外投資的保險，尤其是中國市場，已經開始降低政府的保障和補貼的比例，希望藉此讓企業赴中國投資時更加注意風險評估。中國對於德國這份《中國戰略報告》提出回應，指出去風險是一個「假議題」。如果德國把前往中國投資視為風險，將會降低許多企業在中國的機會。同時，中國也指出，中德之間只有伙伴，不存在對手的關係。2024 年 4 月，德國總理 Scholz 率團訪問北京，習近平高規格接待。中方學者認為，從中國的角度看，高規格接待也凸顯了中國政府重視德國的特殊作用。中國一貫主張保持中德關係行穩致遠對於應對時代挑戰意義重大，特別強調中德此次互動對世界的風向標意義，以及對於維護與穩定全球貿易、產業供應鏈的現實影響。習近平在北京釣魚臺國賓館會見 Scholz 時，高度評價中德合作的戰略意義，重申堅持中德關係的合作主基調和發展大方向，強調世界越是動蕩，雙方越要提升兩國關係的韌性和活力，指出中德互利合作不是「風險」，而是雙方關係穩定的保障、開創未來的機遇（伍慧萍，2024）。中國對此份報告沒有高調的反應，但以習近平會晤的規格與談話來看，顯然還在觀察德國如何將此份戰略報告轉化為政策與行動。

從歐盟的角度來看，在 2023 年 6 月 30 日歐盟理事會公布對中戰略報告，就率先提出去風險的概念。德國在中國總理李強訪問德國之後，也於 7 月 13 日公布德國的《中國戰略報告》，顯示出德國的中國政策鑲嵌在歐盟對中國的框架中。在這份戰略報告多次提到，德國不會在歐盟中單獨突出對中國關係的差異性，必須維持歐盟的一致，以及在歐盟對中的框架下來建立德中雙邊關係。因此，選擇在歐盟理事會公布的「去風險」概念下，即使李強訪問德國，德國也在同年 7 月 13 日一樣的把「去風險」放進《中國戰略報告》，而且成為未來對中政策的基調。

四、與臺灣的關係

最後，分析德國的《中國戰略報告》中，對於臺灣的定位以及未來德國對臺政策的趨勢。「臺灣」在德國公布的《中國戰略報告》中，一共出現 13 次，這已經是過往罕見的現象，顯見德國當前制訂對中國政策時，也關注到臺灣問題是無可迴避的部分。在《中國戰略報告》公布以前，臺德關係就已經不斷升溫。駐點期間與我國駐德國代表處謝志偉大使訪談時，謝大使提到，德國國會針對支持臺灣重回世衛組織，過往此案大約僅有大約 30 位議員願意連署與發言，去年在此案提出時，高達超過 130 位國會議員表達同意與支持，堪稱史上之最。另外，德國史無前例的派出六個政黨的跨黨派友臺小組到臺灣訪問，並與蔡英文總統見面。跨六黨派訪臺，規模之大，也是史無前例。不僅如此，德國也派出教育研究部長訪問臺灣，在駐點期間我國法務部長也到訪柏林，與德國聯邦政府司法部長正式、公開會晤，這些都是過去不曾見到的雙邊關係。從國會跨黨派的態度、雙邊部長級官員互訪，都可以看出臺德雙邊關係現在正處在高峰。

回到《中國戰略報告》中，13 次提及臺灣的部分，可以概括分為地理名詞以及政治實體。就地理名詞而言，「臺灣海峽」出現 3 次，皆指出德國已經關注到臺灣海峽的和平與穩定，是德國國家利益之所在，而中國對於臺灣海峽的穩定與和平而言，是一項風險來源。其他 10 次提及臺灣，就是把臺灣視為政治實體的概念下進行討論。包括德國闡述一個中國政策（提及 4 次）、中國對臺灣的假訊息威脅（提及 1 次）、將臺灣視為德國密切的合作伙伴，包括半導體、經濟、支持臺灣加入國際組織等議題（5 次）。以下分別分析其意涵。

首先，德國在「一中政策」中提及臺灣，指出德國並不尋求改變與北京外交關係，不會與臺灣建立官方的外交關係。但臺灣現況的改變，必須基於和平方式，以及雙邊共識這兩項條件。透過軍事升高對立，將傷及德國與歐盟的利益。這個部分的陳述，雖未提及德國所奉行的一中政策的具體內容，但對於現況改變提出兩項德國的主張：和平方式、兩岸共識。具體而言，德國對於一中政策以及臺海現狀的立場，相當符合臺灣對於兩岸關係的主張。

其次，在《中國戰略報告》中，提到德國雖然不會與臺灣建立官方的外交關

係，但不損及臺灣與德國在其他領域的合作與伙伴關係。例如半導體、經濟、科技以及市民社會的交流。值得一提的是，德國使用伙伴一詞形容與臺灣的關係，呼應了整份中國戰略提出的五項目的中，強調德國與中國雙邊的交往，不能危及德國的價值，以及與其他伙伴的交往。兩相對照之下，可以看出德國重視與臺灣的合作，並且認為應該從德中關係獨立出來，不能因為與中國的交往而損及臺德在經貿、科技、文教等方面的往來。作者在與我國駐德國代表處交流時，和謝志偉代表對於文件中細膩的用詞，間接但堅定的提到臺德關係的趨勢，可以視為一個重要的訊號。

第三，德國重視並支持臺灣在歐盟與德國的一個中國政策下加入國際組織。並呼籲聯合國以及附屬組織，重視臺灣社會的存在，並正視臺灣社會帶來的積極貢獻。這個主張放進《中國戰略報告》，凸顯德國支持臺灣加入國際組織的立場，這也是臺德關係、臺歐關係在過去迅速升溫所帶來的正面影響。整體而言，德國在《中國戰略報告》中多次提及臺灣，凸顯對臺海和平與穩定的重視，也凸顯德國目前主張，不會也不應該因為與中國的交往而傷害臺灣與德國在各項議題上的合作。

第四，基於前述德國在中國戰略中提到的對臺政策，也在德國對中「去風險」的概念下，臺灣非常值得提供德國與歐盟觀察中國、認識中國的觀點。德國在《中國戰略報告》的結論中提到，德國主張應該更加全面去認識中國，深化認識中國的專業知識。關於這點，過去中國在德國大量設立「孔子學院」，作為德國認識中國的媒介。然而，當孔子學院成為中國在德國的情報中心、進行認知作戰、宣傳中國立場而危及德國對民主、人權、法治的價值觀時，德國開始呼籲各大學重新檢視設立孔子學院的必要性，並大量關閉孔子學院。如今《中國戰略報告》在結論處提到，德國重視深化中國的專業知識，臺灣在孔子學院關閉的當下，可以適時成為德國認識中國的媒介，提供華語教學的人才、中國研究的相關合作、認識中國的視窗等。關於此項建議，不僅獲得我國駐德國代表處的認同，在與幾個智庫、部會辦公室主任、媒體、學者訪談中，多次建議讓臺灣成為德國研究中國的平臺和媒介，由臺灣補充在德國政府以及大企業、智庫中的華語教學，深化臺德雙方對中國研究的合作，都獲得非常正面的回應。

就民間的觀點來看，德國學界對於支持臺灣的民主韌性、維持臺海的穩定與和平也有一些具體的建議。例如：降低德國與歐盟對於中國的經濟依賴，但深化與臺

灣的經貿合作，尤其是關鍵技術、稀土進口、高科技產品、醫療等領域；其次，在基礎關鍵設施上（尤其是通訊），應該降低中國的風險和威脅；第三，在外交和國際空間上，適度的支持臺灣，確保臺灣有足夠的能力維持臺海現狀，也是符合德國與歐盟的利益（Demes & Krumbein, 2024, pp. 172-173）。整體來說，強化對臺關係，降低對中依賴，逐漸成為官方和民間的共識。

伍、黑紅聯盟的中國政策

德國的「紅綠燈聯合內閣」於 2024 年 11 月垮臺，聯邦眾議院於 2025 年 2 月提前進行選舉。最終選舉結果，CDU/CSU 再次成為國會第一大黨，由 F. Merz 出任總理，與 SPD 合組「黑紅聯合內閣」。此外，就政黨政治發展來看，此次改選呈現政黨體系極化且破碎化的趨勢，右翼民粹的「另類選擇黨」（AfD）一口氣成為第二大黨，政治影響力值得觀察。新政府的中國戰略該如何解讀與預判，成為當下重要的議題。作者在選舉前有機會與德國前執政黨（SPD）的國會議員 Michael Müller（德國聯邦眾議院外交委員會資深議員）與 Andreas Larem 訪談，針對德國在 2023 年提出新的「中國戰略」，是否成為下一個階段的對中政策綱領，兩位議員在選前指出，如果 CDU/CSU 重返執政，對中政策很有可能比紅綠燈聯合內閣更加強硬，尤其在經貿議題方面。[7] 如果新的聯合內閣沒有大幅調整中國戰略，甚至更加轉趨強硬，這份中國戰略將成為歷經兩次的主要政黨執政，也將意味德國這一版本的中國戰略將成為跨黨派的共識，就是德國下一個階段對中政策的綱領並具有定錨效果。

選後，德國多個智庫討論到黑紅聯盟新政府是否會再次調整對中戰略。其中「經濟與政治基金會」（Stiftung Wissenschaft und Politik, SWP）研究員 Nadine Godehardt 在改選前就德國當前的對中戰略進行較為全面的分析。分析報告中指出幾個重點：首先，德國並未在機構或制度層面出現應對中國政策的調整；其次，德國的對中政策長期以經濟議題主導，且欠缺較完整、長期性的規劃；第三，在對中

[7] 訪談資料。訪談對象為德國聯邦眾議員 Michael Müller（SPD，德國聯邦眾議院外交委員會資深議員）與聯邦眾議員 Andreas Larem（SPD），訪談時間為 2024 年 9 月 18 日。

的政治議題上，對外被動、對內保守；第四，三重身分的認定（伙伴、競爭與系統性對手）應該調整，說明以何者為主導；第五，建議進行中國政策的辯論，擬定長期規劃與目標（Godehardt, 2024）。這份報告寫在2024年選後，也具有對2023年《中國戰略報告》的檢討，以及對新政府中國政策建議的味道。

智庫 MERICS 的主任 Mikko Huotari 也提出了新政府對中戰略的分析與預判（Huotari, 2025）。首先，文中提到就兩國經貿關係而言，已經不再是單純的互補性，而是具有多方面的競爭關係，形成「中國衝擊 2.0」（China Shock 2.0）。另外，就安全議題而言，文中也提到中國在俄烏戰爭中加強了對莫斯科的支持，包括利用無人機運送武器。中國針對德國的間諜活動也成為日常生活中被低估的一部分，並且有惡化的趨勢。面對此一結構性的變化，德中關係也出現系統性、集團性的衝突，例如CRINK（中國、俄羅斯、伊朗、北韓）與威瑪三角（Weimar Triangle, 柏林、巴黎、華沙）。此外，MERICS 也在 2025 年 1 月舉辦了一場名為「未來聯邦政府的中國政策」（MERICS Forum: Die Chinapolitik der künftigen Bundesregierung）的論壇，[8] 與會學者包括 Benner 認為，新政府應該更為強硬與明確的執行對中政策，尤其是降低依賴，並且在與中國對峙的情況下領導歐洲的團結。Gottwald 則是指出，新政府需要立刻展現出必要的安全政策能力，以應對中國對德國在政治、商業和社會等不同方面的影響，尤其要應對中國支持俄羅斯侵略烏克蘭的議題。Jungblath 認為，德國應該在歐盟的平臺來實行對中政策，在歐盟層級達成共識，才能對中國釋放出清晰且一致的訊號。Matthes 從產業面指出，來自中國的不公平競爭，是對德國工業陷入困境的嚴重威脅。新一屆德國政府必須與歐盟合作，確保在中國對其產業非法補貼的情況下，為受到威脅的德國和歐洲提供公平的競爭環境。Maull 認為，新政府必須制定長期目標，在聯邦政府的範圍內，運用一切適當和必要的手段、工具，以貫徹實現這些目標。「去風險化」的概念過於籠統，也過於薄弱，無法充分體現

[8] 這場論壇由 MERICS 主辦，出席的學者包括 Thorsten Benner（Direktor des Global Public Policy Institute）、Jörn-Carsten Gottwald（Professor für Politik Ostasiens an der Ruhr-Universität Bochum）、Cora Francisca Jungbluth（Senior Expert China and Asia-Pacific, Bertelsmann Stiftung）、Jürgen Matthes（Leiter des Clusters Internationale Wirtschaftspolitik）、Hanns W. Maull（MERICS）、Wolfgang Niedermark（Mitglied der Hauptgeschäftsführung, BDI）。座談的主題是「未來聯邦政府的中國政策」"MERICS Forum: Die Chinapolitik der künftigen Bundesregierung"。相關資料可參閱 Mercator Institute for China Studies（2025）。

中國對德國和歐洲構成的安全威脅。Niedermark 建議新政府延續紅綠燈聯合內閣的中國政策，「去風險、不脫鉤」仍是主軸，並且強化歐盟的整合甚至建立跨大西洋的共識。

黑紅聯合內閣的執政協議中，正式承諾實施「去風險化」和加強「經濟安全」的策略，並明確將中國視為「系統性競爭對手」。依據媒體分析，新政府認為德國企業必須減少對中國依賴，並強調未來雙邊的貿易關係應強調更穩定、更安全的市場為基礎。值得注意的是，Merz 總理甚至提出警告，未來聯邦政府不會支持那些因「高風險」的中國投資而面臨損失的德國企業。綜合來看，在 Merz 領導下，德國雖然可能在經濟安全問題上採取更堅定的立場，並減少地緣政治風險帶來的傷害，但也將尋求與中國保持務實的接觸，尤其是在雙邊合作仍能帶來互利的領域。這種雙軌策略也是目前歐盟較廣泛的共識，也就是將中國多方定位，依不同議題視中國為合作夥伴、競爭對手或甚至威脅來源（Interesse, 2025）。

以新古典現實主義的架構來看，決策者的認知也是影響外交政策的重要變數。MERICS 研究員 Claudia Wessling 分析，黑紅聯合內閣的成員中，新任的外交部長 Johann Wadephul 以務實的政治家著稱。在對華政策上，他有望在經濟利益與戰略考量之間取得平衡。這位經驗豐富的議員私下推動了基民盟對華立場的轉變，使其立場更加批判中國。另一方面，他曾與其他基民盟／基社盟議員一起，並與中國全國人大代表和中共官員進行對話。他最近表示，自己的立場是保持與中國的接觸，同時對兩國的差異保持清醒的認知（Wessling, 2025）。長期駐德的資深記者廖林麗玲（2025）觀察 Merz 領導的新政府，也認為對中政策將趨於強硬。在新政府的聯合執政協議中提到「由於中國的作為，日益凸顯了制度性對立的元素。在這樣的背景下，我們將減少單方面依賴，並奉行去風險政策，以強化我們的韌性。面對中國，必要時，我們會展現堅定和實力」。而就人事背景而言，Merz 總理本人以及新任外長 Johann Wadephul，都被德媒歸類為「對中鷹派」，因此預判新政府對中國的態度將趨於強硬。

新任總理 Merz 在 5 月 6 日正式就職，5 月 14 日首次在聯邦眾議院發表了對中戰略的談話，指出對中國應採「戰略去風險」（strategic de-risking）的策略，一方面要求中國在結束俄烏戰爭中做出貢獻，二方面未來也將繼續減少對單方面的依

賴。所謂單方面依賴，一方面指的是經貿降低對中依賴，二方面也暗指安全的對美依賴。換言之，Merz 的對中戰略，將會是（一）維持溝通（要求中國協助終止俄烏戰爭）；（二）領導德國與歐洲強化國防；（三）降低經貿對中依賴等趨勢。

透過新古典現實主義的途徑，進一步對比 2023 年紅綠燈聯合內閣的《中國戰略報告》，以及 2025 年黑紅聯盟可能的中國政策來看，從 2023 年到 2025 年，德中的結構性因素不可能有劇烈變化，而外部因素中的俄烏戰爭、俄國威脅並沒有發生劇烈變化，內部政治結構導致決策者更換，而新的決策者 Merz 總理與外長 Wadephul 對此項議題的認知，遂成為解釋德國對中政策調整的關鍵變數。

陸、結論：展望中國戰略——務實、矛盾與定錨？

本文以新古典現實主義的分析途徑，透過對結構性因素、外部環境、內部環境、以及決策者認知的綜合分析，討論了德國對中政策在 2023 年正式官方報告中的戰略性調整，以及 2025 年黑紅聯盟對的對中政策之趨勢。就 2023 年對中戰略報告而言，這份文件延遲的發布反映了德國不同部會和其他利害關係者之間的內部分歧，該分歧可能會繼續影響德國對中國戰略的辯論。德國商界尤其強烈反對可能危及德中經濟關係的舉措，因為中國仍然是德國最大的貿易夥伴。儘管如此，如此文件的發布標誌著柏林的重要變化，並使德國政府與歐盟執委會更明確地結盟，歐盟執委會近年來對中國發出了更批評的聲音（孫國祥，2023，頁 94）。德國在 2023 年公布的對中戰略報告，是否意味著德國對中政策出現結構性與延續性的轉向，確實值得更多研究與分析的投入。

本次的研究紀要提出若干發現。首先，就背景來看，德中關係近年來出現轉變，是基於結構性因素加上國內與國際政治環境變化所致。所謂的結構性因素，指的是中國持續性的經濟成長，並未帶來政治體制的開放與民主化，反而是透過經濟力量影響發展中國家，並成為西方民主國家的潛在威脅。而國內的政治環境變化，指的是 2021 年聯邦眾議院選舉出現政黨輪替，由 CDU/CSU 主導的中間偏右，相對保守的梅克爾路線正式結束，取而代之的是 SPD 領導，加上綠黨與 FDP 的中間偏左紅綠燈聯合內閣。國際的政治環境變化，則是指美中全面競爭，以及俄烏戰爭

的爆發。美國長期做為德國的盟友，美中從貿易戰升級為全面競爭，加上俄國入侵烏克蘭，中國不但未加入制裁，也未對和平與停戰做出積極貢獻，甚至與俄羅斯維持緊密的伙伴關係，使德國重新評估中國是否作為一個值得信賴的伙伴，也重新評估經濟上對中國過度依賴的風險。俄烏戰爭是一個重要的催化，也促使德國將「去風險」設定為未來對中交往的原則。

第二、2023 年 7 月 13 日公布的《中國戰略報告》，是德國聯邦政府未來對中政策的官方文件，代表德國未來各項對中政策的基礎。該文件將德中關係重新定位為「伙伴、競爭、系統性對手」的多重關係，並以「去風險」作為德國對中政策的基調。其中，伙伴關係是延續過去德國與中國密切的經貿往來，並延伸至再生能源與科技領域的合作。但也調整為競爭和對手的關係，一方面在於降低對中國的依賴，並強調中國在地緣政治上的擴張，形成對臺灣海峽與印太地區不穩定的風險因子，也成為德國潛在的威脅來源。此外，德國對於中國在民主、人權、法治等價值議題，定位為「對手」，而與經貿、氣候、科技議題上定位為「伙伴」的矛盾。突顯出德國與中國關係正在重新調整，無法單一面向的定位雙邊關係，而是依據不同議題有不同的定位。在 2024 年，德國派遣兩艘軍艦穿越臺海，引起中國不滿的同時，德國對外的說法是將臺灣海峽定位為正常通道並且無害航行，並不挑戰中國對該水域的主張。這一例子也看到德國對中政策轉趨強硬的同時，卻也保留迴旋餘地，也凸顯了這份戰略報告略帶矛盾，卻又務實的作法。[9]

第三、德國的中國戰略，強調未來對中政策的制訂，需要多個行為者的共識，包括國會內的各政黨、聯邦政府與邦政府、德國與歐盟和其他伙伴。意味著德國的中國政策將是尋求共識，鑲嵌在歐盟以及與德國利益一致的國際社會中。德國不會單邊制訂單一的對中政策，也不會建立特殊而異於歐盟與國際社會下的對中關係。意味著德國對中政策將符合歐盟對中政策的一致性，並且不會出現特殊的德中關係。

第四、就德國與臺關係來說，既是德國對中政策的一環，也是臺德雙邊關係獨立開展的契機。德國罕見的將臺灣放入《中國戰略報告》，並多次提及，凸顯三個

[9] 德國 2023 年《中國戰略報告》，象徵德國印太戰略的轉變。這種轉趨強硬又不失迴旋空間的論述，可參見 Lai（2024）。

對臺政策的意涵：維持在臺海的和平與穩定、深化與臺灣非官方的實質合作、支持臺灣加入有意義的國際組織。此外，德國對中國展開重新的認識，是基於專業知識和民間交流，而臺灣可以提供德國重新認識中國的媒介與合作。例如深化雙邊共同合作展開中國研究、提供華語師資、強化雙邊高等教育與科技交流等。

中國戰略報告公布後一年，紅綠燈聯合內閣解散，國會提前改選，黑紅聯盟在 2025 年 5 月正式執政。從新古典現實主義的角度來看，改變的只有國內的政治環境以及決策者。新的決策者以更加務實的認知，加上對中鷹派的立場，在對中政策上採取了以競爭對手為主軸的立場，但也保持對話和合作的空間。整體而言，本研究紀要推估，在國際上的外部環境（俄烏戰爭、中國威脅）不變的情況下，德國對中政策只會在決策者因選舉替換而產生微調，短期內恐怕不會再出現本質上的變化。

值此國際秩序重組的關鍵時刻，全球民主國家面對中國擴張式崛起的壓力，紛紛調整對中戰略。在歐洲的地緣政治方面，基於德國在歐盟扮演重要角色，德國的對中戰略調整具有象徵與實質意義，值得後續深入研究。本文分析了德國紅綠燈聯合內閣在 2023 年制訂的對中戰略報告，從國際重大環境變化、國內政黨政治的變遷為背景，探究德國對中戰略轉趨強硬的意涵。德國新政府已於 2025 年上臺執政，短期來看，對中政策或許會調整細部的作法，但預判就結構面而言，仍將維持對中強硬的態度。

參考文獻

伍慧萍（2024）。中德關係正步入「新常態」。紫荊，5 月 4 日。https://bau.com.hk/article/2024-05/04/content_1235906890021543936.html [Wu, H. P. (2024). *China-Germany relations are entering a "new normal"*. Bauhinia Magazine, May 4.]

沈有忠（2018）。德國再起：透視德國百年憲政發展。新學林。[Shen, Y. C. (2018). *Germany's revival: A perspective on a century of constitutional development*. New Sharing Culture Enterprise.]

沈有忠（2022）。德國安全與能源政策在俄烏戰爭中之轉向。歐亞研究，（19），71-76。[Shen, Y. C. (2022). The major shift of Germany's policy in the Russia-Ukraine war. *Eurasian Studies Quarterly*, (19), 71-76.]

夏瀾（2022）。從「戰略夥伴關係」到多面向的歐洲策略途徑：德國對中政策的轉型。歐亞研究，（20），13-17。[Sadeler, C. (2022). From "strategic partnership" to a multifaceted European

approach: Germany's China policy in transition. *Eurasian Studies Quarterly*, (20), 13-17.]

孫國祥（2023）。德國之中國戰略文件解析。**新世紀智庫論壇**，（103-104），94-102。[Sun, G. X. (2023). An analysis of Germany's China strategy document. *Xin Shiji Zhiku Luntan*, (103-104), 94-102.]

彭濤（2021）。**新政府聯合協議出籠 德國對中更具對抗性**。獨家報導，12 月 2 日。https://www.scooptw.com/thinktank/world_affairs/65516/ 新政府聯合協議出籠 - 德國對中更具對抗性 / [Peng, T. (2021). *New coalition agreement unveiled: Germany adopts a more confrontational stance toward China*. Scoop Weekly Taiwan, December 2.]

廖林麗玲（2025）。德新總理上台 對中強硬。**自由時報**，5 月 20 日。https://talk.ltn.com.tw/article/breakingnews/5044487 [Liao Lin, L. L. (2025). Germany's new chancellor takes office, adopting a tough stance toward China. *The Liberty Times*, May 20.]

廖舜右、蔡松伯（2013）。新古典現實主義與外交政策分析的再連結。**問題與研究，52**（3），43-61。https://doi.org/10.30390/ISC.201309_52(3).0002 [Liao, S. Y., & Tsai, S. P. (2013). The re-linkage between neoclassical realism and foreign policy analysis. *Wenti Yu Yanjiu*, *52*(3), 43-61.]

德國之聲（2022）。**機密文件曝光：揭示德國未來對華戰略**，11 月 17 日。https://www.dw.com/zh/ 机密文件曝光揭示德国未来对华战略 /a-63784934# [Deutsche Welle. (2022). *Confidential documents exposed: Revealing Germany's future strategy toward China*, November 17.]

鄭端耀（2005）。國際關係新古典現實主義理論。**問題與研究，44**（1），115-140。https://doi.org/10.30390/ISC.200502_44(1).0005 [Cheng, T. Y. (2005). Analytical appraisal of neoclassical realism. *Wenti Yu Yanjiu*, *44*(1), 115-140.]

薛健吾（2023）。2022 年俄烏戰爭對歐中關係之影響。**歐亞研究**，（23），23-34。[Hsueh, C. W. A. (2023). The influence of the 2022 Russo-Ukrainian war on EU-China relations. *Eurasian Studies Quarterly*, (23), 23-34.]

Bunde, T., Eisentraut, S., Knapp, N., Schütte, L., Hammelehle, J., Kump, I., Mudie-Mantz, A., & Pauly, J. (2023). *Re:vision: Munich security report 2023*. Stiftung Münchner Sicherheitskonferenz. https://doi.org/10.47342/ZBJA9198

Carrel, P. (2023, January 11). *Germany's ties with China could change fundamentally - SPD leader*. Reuters. https://www.reuters.com/world/europe/germanys-ties-with-china-could-change-fundamentally-spd-leader-2023-01-11/

Ciesielska-Klikowska, J. (2023). Interest groups in shaping Germany's foreign policy towards China. *Przegląd Zachodni*, *2023*(3), 35-69. https://doi.org/10.60972/PZ.2023.3.35

Demes, D., & Krumbein, F. (2024). *Taiwan: Asiens erstaunliche Demokratie*. Bundeszentrale für politische Bildung.

Gardels, N. (2023, January 6). *Germany's Chinapolitik*. Noema. https://www.noemamag.com/germanys-chinapolitik/

Godehardt, N. (2024). *Die Logik deutscher Chinapolitik in der Zeitenwende*. Stiftung Wissenschaft und Politik, Deutsches Institut für Internationale Politik und Sicherheit. https://doi.org/10.18449/2024S20

Huotari, M. (2025, March 3). *A new German strategy toward China*. International Political Quarterly. https://ip-quarterly.com/en/new-german-strategy-toward-china

Interesse, G. (2025, May 26). *China-Germany economic relations 2025: What Merz's leadership means for trade*

and investment. China Briefing. https://www.china-briefing.com/news/china-germany-relations-2025-merz-leadership-trade-investment/

Kefferpütz, R. (2022, April 7). *Shifting politics: The future of Germany's China policy*. Institut Montaigne. https://www.institutmontaigne.org/en/expressions/shifting-politics-future-germanys-china-policy

Kratz, A., Zenglein, M. J., Brown, A., Sebastian, G., & Meyer, A. (2024, June 6). *Dwindling investments become more concentrated - Chinese FDI in Europe: 2023 update*. Mercator Institute for China Studies. https://merics.org/en/report/dwindling-investments-become-more-concentrated-chinese-fdi-europe-2023-update

Kundnani, H., & Parello-Plesner, J. (2012). *China and Germany: Why the emerging special relationship matters for Europe*. European Council on Foreign Relations.

Lai, Y. C. (2024). Germany's shifting Indo-Pacific strategy: From Indo-Pacific guidelines to the strategy on China. *Prospects & Perspectives*, (48). https://www.pf.org.tw/en/pfen/33-10892.html

Mercator Institute for China Studies. (2025, January 21). *MERICS Forum: Die Chinapolitik der künftigen Bundesregierung*. https://merics.org/de/kommentar/merics-forum-die-chinapolitik-der-kuenftigen-bundesregierung

Müller, W. (2022, October 31). *Deutschlands und Europas China-Politik: US-Bettvorleger oder Strategische Autonomie?* ISW. https://www.isw-muenchen.de/online-publikationen/texte-artikel/4881-80deutschlands-und-europas-china-politik-us-bettvorleger-oder-strategische-autonomie

Ripsman, N. M., Taliaferro, J. W., & Lobell, S. E. (2016). *Neoclassical realist theory of international politics*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199899234.001.0001

Rose, G. (1998). Neoclassical realism and theories of foreign policy. *World Politics*, *51*(1), 144-172.

Smith, N. R. (2018). Can neoclassical realism become a genuine theory of international relations? *The Journal of Politics*, *80*(2), 742-749. https://doi.org/10.1086/696882

Ulatowski, R. (2022). Germany in the Indo-Pacific region: Strengthening the liberal order and regional security. *International Affairs*, *98*(2), 383-402. https://doi.org/10.1093/ia/iiac008

Wessling, C. (2025, May 16). *Germany's China policy under Merz: A rocky road towards risk-aware pragmatism*. Mercator Institute for China Studies. https://merics.org/en/merics-briefs/chinas-overcapacity-and-eu-german-china-policy-under-merz-eu-china-trade

台灣戰略研究徵稿簡則

「台灣戰略研究」（Taiwan Strategic Studies）（以下簡稱本刊）為學術研究期刊，研究領域包括外交政策、國防安全、科技產業、國際關係、中國問題、資訊安全、金融穩定，以及其他戰略安全議題等。

本刊於 2025 年下半年創刊，初期採半年刊形式，未來將視發刊情況調整，歡迎各界人士針對戰略研究相關議題投稿。本刊以發表戰略研究相關中英文學術論文為主，不接受以譯代著或一稿兩投。

投稿論文請依「公共事務期刊協同格式」，以正體中文或英文撰寫，中文論文以一萬至兩萬字為原則，不超過兩萬五千字，英文論文以五千至一萬字為原則，不超過一萬兩千字。來稿並請附上中英文摘要、關鍵詞與參考文獻。

投稿論文採取隨到隨審制，編輯部於收件後將進行初審，通過初審的論文將交予兩至三位專家學者進行雙向匿名審查。編輯部保留對投稿論文格式與文字之修改及潤稿權。

投稿論文若經刊載，著作權即歸「財團法人台灣智庫」所有，未經同意請勿轉載。本刊將致贈原作者當期期刊三本，並酌贈稿酬。

來稿請以電子郵件寄至 frontier@dimes.org.tw（財團法人台灣智庫台灣戰略研究編輯部）。

台灣戰略研究（第二卷第一期）

發 行 人：郭建中

總 編 輯：李漢銘

編輯委員（依姓氏筆劃順序）：

呂曜志、沈明室、吳瑟致、洪文玲、張國城、陳宜欣、陳牧民、
黃智聰、劉玉皙、劉奇峯、劉孟俊、鄭政秉、魏百谷

執行編輯：劉奇峯

行政編輯：高家楨

助理編輯：吳宣頤

網站編輯：趙哲儒

出 版 者：財團法人台灣智庫

地址：台北市萬華區長沙街二段 96 號 4 樓

信箱：frontier@dimes.org.tw

創刊年月：2025 年 7 月

刊期頻率：半年刊（一月、七月出刊）

印 刷 者：秀威資訊科技有限股份公司

地址：台北市內湖區瑞光路 76 巷 65 號 1 樓

本刊由財團法人大肚山產業創新基金會、及其他社會賢達人士贊助出版，謹此致謝。