理事長開講：一場被允許的破壞 ～ 海底基礎設施與韌性航運的重構♠

A Permitted Disruption: Subsea Infrastructure and the Reconstruction of a Resilient Maritime Order

陳彥宏*

前言：在看不見的海上，秩序悄然轉向

我們正處於一個物理海洋與數位海洋深度交織的時代，而這種交織並非單純的技術疊加，而是一種結構性的轉變。過去，海洋之所以重要，在於它承載了貨物與能源的流動；航道、港口與船舶構成了一個可以被觀測、被規範、也相對可控的體系。然而，在今日的全球化架構中，真正維繫運作的，早已不只是海面之上的航行，而是深埋海床、無聲傳輸的海底電纜網絡。當流動的本質從物資轉向數據，海洋的風險也隨之發生了轉變，從可見的事故，轉為難以察覺、難以歸因的干擾。

在這樣的轉變之中，一種新的脆弱性逐漸浮現。它並不以明確的敵對形式出現，也不依賴傳統意義上的武力展示，而是嵌入於日常海事行為之中，隱身於合法操作的外觀之下。當一個行為可以在操作上被解釋為合理，在法律上被視為過失，在證據上無法指向意圖時，它便能同時穿越技術監控與制度判準，成為一種既存在、卻難以被定義的風險。在這樣的條件下，破壞不再必須呈現為異常，而可以被輕鬆的歸類為意外事件，以一種被接受的形式進入既有秩序之中。這種現象所動搖的，不只是安全機制，而是整體治理邏輯本身。

長期以來，海事體系建立在事故可被識別、責任可被歸因、風險可被管理的基本假設之上；然而，當行為與意圖之間出現結構性的落差，當風險存在於法律所允許的範圍之內，這些假設便開始失去支撐力。於是，我們所面對的，不再只是個別事件的處理問題，而是一種，當民用航運工具被系統性地戰略化與武器化之後，既有以事故管理與航行安全為核心的制度，是否仍具備維持秩序的能力？抑或，它已在不自覺之中，轉化為一種允許風險生成與擴散的結構？

♠ 本文之構思與撰寫，承蒙理律法律事務所合夥人黃欣欣律師於法律分析與制度詮釋方面多所指導，對相關論述之深化助益良多，謹此致上誠摯謝意。

* 陳彥宏 Solomon CHEN，英國威爾斯大學海洋事務與國際運輸學博士，台灣海事安全與保安研究會理事長，新台灣國策智庫諮詢委員，國家運輸安全調查委員會諮詢委員，海洋委員會海巡艦隊分署海損評議審查會委員，海事仲裁人。曾任教於臺灣海洋大學、澳大利亞海事學院國家港埠與航運中心、高雄海洋科技大學。曾客座於上海交通大學凱原法學院國際海事研究中心、廈門大學南海研究、澳大利亞海運學院。EMAIL: solomonyhchen@gmail.com。

本研究正是從這樣的裂隙出發，試圖在物理與數位交會的界面上，重新理解海洋風險的生成機制，並分析當灰色地帶行動成為常態時，全球航運體系與海洋治理將如何被迫調整。這不是一篇僅止於技術或案例的分析，而是一種對秩序轉變的觀察，特別是在當流動仍在持續，但其安全條件已然改變時，我們是否仍能辨識風險的所在，並在其跨越邊界之前，做出有效的回應。

在這片看不見的海上，潮汐或許仍在規律更替，但支撐它的力量，已悄然轉向。

一、數位時代的風險轉向

當全球化從貨物流動轉為數據流動，海洋的意義也隨之改寫，它的表層是航道，深處是神經。我們所依賴的不再只是船舶的航行安全，而是資訊在毫秒之間的無聲通行。當兩個海洋在同一空間重疊，風險便不再是單一事故，而是跨系統的脆弱共振；這是一場隱形的耦合，將海床的微小顫動，轉化為文明的生存危機。

1.1 研究背景：從物流全球化到數據全球化

自二十世紀中葉以來，全球化(globalisation)的核心長期建立於物資流(flow of goods)之上，以貨櫃航運為基礎的實體物流體系，不僅促成跨國生產鏈的形成，也塑造了現代國際分工與貿易秩序。在此一階段，海洋的戰略意義主要體現在航道控制、港口建設與船隊規模，其風險亦多屬可觀測的物理性威脅，例如天候、碰撞、擱淺、失火爆炸、進水沉沒或武裝衝突。

然而，進入二十一世紀後，隨著數位經濟的快速發展，全球化的動力結構發生根本性轉變。國際數據資訊(International Data Corporation, IDC)及多項經濟研究顯示，跨境數據流(cross-border data flows)的成長速度已顯著超越實體貿易。資本的移動，不再依賴貨輪運輸的黃金或現金，而是透過光纖網絡，在毫秒之間以電子訊號的形式完成。

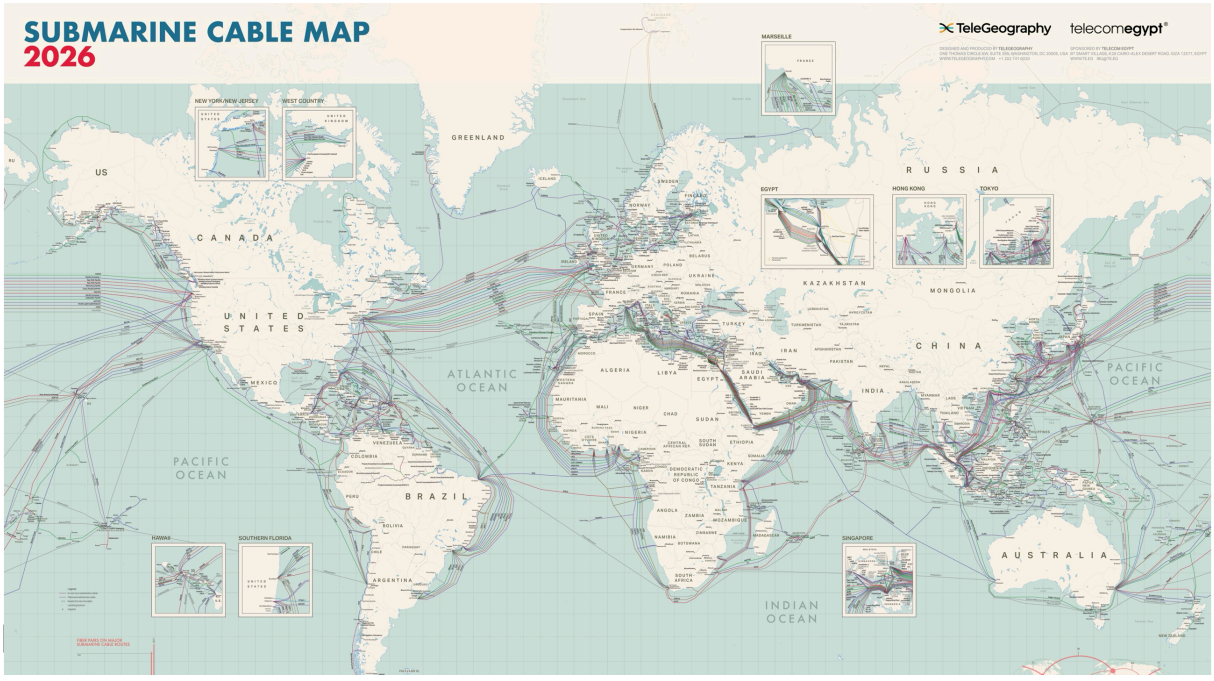
此一轉變標誌著全球經濟已由原子(atoms)的移動，轉向位元(bits)的流動。全球運作所依賴的流動性，亦隨之由可見的海洋航路(shipping lanes)，下沉至不可見的海床之下，形成一個高度密集且持續運作的數據傳輸網絡。

在此數據全球化的架構下，海底電纜已成為支撐全球運作的關鍵基礎設施。儘管低軌衛星通訊(如 SpaceX 的 Starlink)近年快速發展，但目前全球約 95%至 99%的洲際數據傳輸，仍依賴鋪設於海床之下、直徑僅約數公分的光纖電纜完成。海底電纜的功能，早已超越傳統通訊意義，而成為當代國家主權與全球金融體系的數位神經系統。

首先，在金融層面，全球資金流動高度依賴低延遲(latency)的即時數據傳輸。跨國銀行結算、外匯市場交易與高頻交易系統，皆仰賴穩定的海纜連線。一旦電纜中斷，其影響將不僅止於通訊延遲，而可能導致區域性金融市場失序，甚至引發連鎖性的流動性風險。

其次，在主權層面，海底電纜的登陸點(landing stations)與路徑選擇，已成為國家控制資訊流的重要節點。正如十九世紀列強競逐加煤站與海峽控制權，當代國際政治的競爭，正逐步轉向對數位咽喉點(digital chokepoints)的掌握。數據路徑的配置，不僅涉及經濟效率，更牽涉國家安全、情報控制與聯盟體系的構建。

本研究觀察，全球最繁忙的物流航道，與最關鍵的海底電纜網絡，在地理空間上呈現高度重疊。舉例而言，馬六甲海峽、紅海、波羅的海以及台灣海峽，不僅是全球貨輪運輸的樞紐，同時也是數據傳輸的關鍵節點。



這種物理層面的重疊，形成了一種結構性的系統耦合(structural coupling)，其一方面，航運體系仍在物理海洋中運作；另一方面，其導航、調度與安全管理，卻高度依賴數位海洋中的數據流支撐。

在此耦合架構下，風險不再侷限於單一系統。原本屬於物流操作範疇的工具，例如船錨或漁具，在特定條件下，可能對海底電纜造成損害；而電纜的中斷，則可能反過來影響航運體系的運作，例如港口調度失靈、航線資訊延遲或金融結算受阻。更關鍵的是，當數據全球化程度持續深化，這種跨系統風險將呈現非線性放大。一個看似

局部且低強度的物理干擾，可能透過數據網絡迅速擴散，最終影響全球供應鏈的運作效率與穩定性。

因此，當代海事安全所面臨的挑戰，已不再僅是如何保護船舶免於傳統威脅，而是如何在一個高度耦合的海洋系統中，防範那些隱蔽且難以歸因的干擾行為，避免其演變為跨領域的系統性風險。

1.2 問題意識：海事工具的戰略轉化

在數個世紀的航海史中，船錨(anchor)始終被視為船舶安全體系中的核心裝置，其功能在於提供碇泊穩定、抵抗風流影響，並在緊急情況下避免船舶失控。從操作實務到制度設計，錨具長期被定位為一種防禦性工具(defensive instrument)，象徵人類對不可預測海洋環境的控制與秩序維繫。

然而，當前海底電纜頻繁受損的現象，揭示出一個重要且深層的轉變，特別是，錨具的物理特性，其重量、剛性結構與強大抓地力， 在特定條件下，已被重新詮釋為一種具備破壞潛力的動能干擾機制(kinetic disruption mechanism)。此一轉變並非來自技術創新，而是源於對既有航運行為的功能性再利用(functional re-purposing)。

在航運實務中，例如因應潮流變化、等待靠泊或進行緊急制動的拋錨與拖錨，本屬常見操作，然而，當此類行為發生於海底電纜密集區域，且其操作方式，如低速長時間拖行、異常錨鏈釋放，偏離正常作業模式時，錨具便可能從被動的穩定工具，轉化為主動的物理破壞手段。更關鍵的是，此類轉化具有高度隱蔽性，極不容易被發覺。

在繁忙水域中，船舶拋錨屬於合法且正常的操作，而海底環境本身的不可視性，使外部觀察者難以判斷該行為究竟屬於操作失誤(navigational negligence)，抑或具備特定目的的干擾行動。此種可被解釋為正常操作的破壞行為，一種操作上合法，戰略上破壞的行為 (Operationally legitimate but strategically destructive behavior)，正是構成錨具武器化(anchor weaponisation)的核心特徵。

海底基礎設施的破壞，已構成當代灰色地帶行動(grey-zone operations)的典型案例。此類行動並不追求立即且明確的破壞效果，而是透過低強度、持續性且難以歸因的干擾，逐步侵蝕既有秩序與對手能力。這樣的灰色地帶行動之所以具有高度戰略價值，在於其能同時產生三種模糊化紅利(ambiguity advantages)：

1 界線模糊(Threshold Ambiguity)：此類行動發生於和平與戰爭之間的模糊區域，利用商用船舶或民用平台作為載體，使受害國難以將其界定為傳統軍事攻擊，從而無法正當啟動集體防衛或軍事回應機制。

2 法律模糊(Legal Displacement)：透過將破壞行為包裝為海事事故或操作疏失，原本可能屬於國際安全議題的事件，被轉化為民事責任或保險理賠問題，進而規避國際法與制裁機制的直接適用。

3 意圖模糊(Attribution Ambiguity)：即使物理損害已被確認，行為者仍可否認其主觀意圖，使行為(act)與意圖(intent)之間產生斷裂，進一步提高追責難度。

在上述模糊性架構下，錨具的武器化提供了一種極具效率的合理否認性(plausible deniability)工具。相較於傳統軍事手段，如飛彈攻擊或水下爆破，利用商用船舶進行拖錨行動，不僅成本極低，且可維持高度的行為正常性(operational normalcy)，使其在國際輿論與法律評價中易被歸類為意外事件 (an incident framed as an accident, deliberately framed as an accident)。

此一策略性模糊，直接導致受害國面臨嚴峻的防禦困境。一方面，若對可疑船舶採取強制措施，如攔截或軍事護航，可能被指控違反航行自由原則；另一方面，若反應不足，則關鍵數位基礎設施將持續暴露於低強度但高頻率的干擾之中。

因此，本研究提出的問題是：

1. 當民用航運工具被系統性地戰略化與武器化後，既有以事故管理與航行安全為基礎的海事治理邏輯，是否仍足以保護支撐全球化運作的數位基礎設施？

2. 當破壞可以被解釋為事故，當敵意可以被包裝為常態操作，當風險存在於法律所允許的行為之內，則治理本身是否已成為脆弱性的來源，而非其解方？

3. 當行為在操作上合法、在證據上無害、在意圖上不可證時，海事治理是否仍能區分事故與攻擊？抑或僅能在破壞發生之後，為其提供一個可被接受的解釋框架？

綜上所述，錨具的武器化並非單一技術或個別事件的問題，而是一種反映結構性轉變的現象。在物理海洋與數位海洋高度耦合的條件下，原本屬於日常操作的航運行為，已具備被轉化為戰略工具的可能性。這種轉化意味著，海上安全的分析框架，必

須從傳統的風險防範(risk prevention)轉向對模糊威脅(ambiguous threats)的持續辨識與管理。而這一轉變，正是當代全球航運體系在高不確定環境中所面臨的根本挑戰。

1.3 理論框架：海洋系統的雙層耦合

傳統上，海事安全與網路安全被視為兩個彼此獨立的領域。前者聚焦於船舶運作、航道控制與物理威脅，後者則關注資訊系統、數據傳輸與網路防護。然而，隨著全球航運體系的數位化程度持續深化，這種區分已逐漸失去解釋力。當代海洋不再僅是承載貨物流動的物理空間，同時也是支撐全球數據流動的關鍵載體。正是在這一背景下，海事系統與數位系統之間產生了高度的結構耦合。

為了描述此一轉變，本研究提出「海事 - 數位耦合風險」(Maritime-Digital Coupling Risk)模型，主張當代海洋系統應被理解為一種由物理層與邏輯層所構成的雙層架構。在此架構中，風險不再侷限於單一層級，而是透過兩者之間的耦合界面持續傳導與放大，最終形成跨系統的連鎖效應。

1 物理層：指的是傳統意義上的海事運作空間，包括航道、船舶以及各類操作工具，例如錨具與漁具。此一層級的運作邏輯，建立在航行自由與空間進出權之上，其規範基礎主要來自於《聯合國海洋法公約》(UNCLOS)所確立的制度框架。由於物理層具備明確的地理定位與可觀測性，其風險通常以具體且可辨識的形式呈現，例如碰撞、擱淺或拖錨損害。

2 邏輯層：指的是構成當代航運體系的隱性基礎設施，其核心在於數據的傳輸與處理。海底光纖電纜、雲端服務、港口作業系統以及金融清算機制，共同構成一個高度依賴即時資訊流的運作網絡。此一層級的特徵，在於其不可見性與時間敏感性，其系統的穩定性往往不為使用者所察覺，但一旦中斷，其影響將迅速擴散至多個領域。

關鍵在於，這兩個層級並非各自獨立運作，而是透過海底電纜與相關基礎設施形成緊密的耦合關係。當船舶於電纜密集區域進行拖錨操作時，一個原本屬於物理層的行為，即可能直接轉化為邏輯層的系統中斷。反之，當數據傳輸受阻時，其影響亦會反饋至物理層，例如港口調度失靈、航運延誤甚至供應鏈中斷。此種雙向作用，使得單一事件得以在不同系統之間傳導，並形成持續放大的風險循環。

在此耦合架構下，海事風險呈現出新的特徵。首先，風險具有跨域傳導性，一個局部的物理干擾，可能迅速擴散為跨區域的數據中斷與經濟影響。其次，影響具有非

線性特質，小規模事件亦可能因節點集中而產生不成比例的後果。最後，風險呈現出可見性不對稱的特徵，即行為本身可被觀察，但其對整體系統的影響卻難以即時評估。

基於上述分析，海事 - 數位耦合風險模型的理論意涵，在於將海事安全從傳統的點狀事故管理(Point-source Incident Management, Isolated Event Management)提升為對系統性脆弱性(Systemic Vulnerability, Structural Fragility)的整體理解。在此視角下，任何發生於關鍵電纜路徑的異常行為，即使尚未造成明確損害，也應被視為潛在的系統風險。更重要的是，這一模型亦揭示了灰色地帶行動的運作邏輯，也就是行為者正是利用物理層的低可疑性操作，精準打擊邏輯層的高依賴性節點，從而在不引發直接衝突的情況下，產生跨系統的戰略效果。

因此，當代海事安全的核心挑戰，已不再僅是避免事故的發生，而是如何在高度耦合的系統中辨識並管理那些模糊且跨域的風險。這一轉變，不僅重新定義了風險本身，也為後續分析灰色地帶行動與航運體系重構，提供了必要的理論基礎。

1.4 研究目的與方法

在前述理論架構的基礎上，本研究的目的，在於建立一套能夠有效辨識與解釋灰色地帶海事行動的分析工具。具體而言，本文提出灰色地帶海事風險識別模型(Grey-Zone Maritime Risk Identification Model)，試圖將傳統上被視為偶發事故的海事事件，重新置於結構性與戰略性的分析框架之中。此一模型的出發點在於觀察到，現行海事監控機制，例如以自動識別系統(AIS)為核心的航跡追蹤，主要設計目的在於避免碰撞、監控非法捕撈或維持航行秩序，對於低強度、具隱蔽性的基礎設施干擾行為，缺乏足夠的辨識能力。

因此，本研究將風險識別的焦點，由單一事件的結果轉向行為模式的異常性。透過整合船舶航跡資料、海底基礎設施分布以及地緣政治環境，本模型嘗試辨識那些在統計上偏離正常操作邏輯的行為，例如船舶在特定電纜交會區域的不自然減速、關閉自動識別系統的時機與持續時間，以及船舶所有權結構的高度不透明性。這些看似零散的訊號，若置於適當的分析脈絡中，將不再只是個別異常，而可能構成具有一致邏輯的潛在風險模式。

在方法設計上，為避免單一視角所造成的解釋侷限，本研究採取多維度分析架構，將灰色地帶海事風險拆解為操作層、制度層與戰略層三個相互交織的分析層級。此一分層並非僅為分類工具，而是構成一種由下而上的解釋邏輯。

在操作層面，分析聚焦於具體海事行為的執行方式與技術細節，包括船舶操縱模式，如精準拖錨、錨鏈釋放與張力控制，以及自動化系統，如 AIS 與 ECDIS，可能遭受的操弄。在此層級中，研究的重點不在於判斷行為的合法性，而在於還原破壞如何發生，並辨識正常操作與策略性行為之間的細微差異。

然而，僅憑操作層的觀察，難以充分解釋這些行為為何能夠持續存在。因此，制度層的分析進一步檢視現行海事治理架構的限制，特別是 UNCLOS 所建立的管轄權分配、船旗國制度以及責任歸屬機制。在灰色地帶行動的情境下，法律規範往往以可證明的行為為依據，而實際操作卻刻意利用意圖不可證明(Evidentiary Impossibility of Intent, Plausible Deniability of Intent)的空間進行。此種行為與意圖之間的落差，使得原本應由國際法處理的問題，被轉化為民事責任或保險理賠爭議，進一步削弱制度的威嚇效果。

在戰略層面，本研究則將上述操作行為與制度條件，置於更廣泛的地緣政治脈絡中加以理解。具體而言，灰色地帶行動並非隨機發生，而是一種高度策略化的行為，其目的在於透過低成本、低可見度的方式，對對手的關鍵基礎設施施加持續壓力。此類行動之所以具有吸引力，在於其同時具備成本低廉與風險可控的特性，使行動者能在不觸發全面衝突的情況下，逐步侵蝕對手的系統韌性。於此脈絡下，海底電纜的干擾，不僅是技術或法律問題，更是資訊封鎖、數位主權競爭與航運秩序重構的一部分。

在研究方法上，本文結合關鍵案例分析與情境建模兩種途徑。一方面，透過對波羅的海、台灣海峽及紅海等區域近期事件的深入分析，比對不同事件中行為模式、操作特徵與政策回應之間的差異與共通性，以建立實證基礎。另一方面，透過情境建模，模擬在不同風險條件下，海底基礎設施受干擾可能對航運體系與數位供應鏈產生的連鎖影響，從而評估系統韌性的極限與潛在脆弱點。

綜合而言，本研究在於將原本分散於海事操作、法律制度與地緣政治之間的分析視角，整合為一個具有層次性與動態性的研究框架。透過此一框架，灰色地帶行動不再被視為難以界定的例外現象，而是可以被系統性辨識、分析與預測的風險類型。這不僅為後續章節的案例分析提供方法基礎，也為未來海事安全政策與國際治理機制的調整，提供了一個可操作的分析起點。

二、灰色地帶的武器轉化

真正危險的，不是武器的出現，而是工具可以被當成武器。當破壞可以被解釋為操作，當行動可以被包裝為例行程序，攻擊便隱身於秩序之中，利用意圖不可證明性

作為掩體。在這樣的海洋裡，最有效的打擊不在於力量，而在於那種令人窒息的合理推諉。

2.1 可否認性的設計

在探討灰色地帶行動與航運工具的武器化之前，必須先釐清一個關鍵但經常被忽略的事實，也就是要先釐清，全球海上物流網絡與數位通訊基礎設施，並非彼此獨立運作的系統，而是在空間上呈現高度重疊的結構。儘管航運路徑與海底電纜鋪設在功能需求上存在差異，前者著重於航行安全與物流效率，後者則優先考量地質穩定性與施工成本，但兩者最終卻呈現高度的空間重疊。此一現象並非源於功能一致，而是源於共同的結構性約束，包括有限的地理通道、沿海經濟活動的高度集中，以及維修與可及性需求。既有研究與產業數據，如國際電纜保護委員會(International Cable Protection Committee, ICPC)與世界海底電纜地圖(Submarine Cable Map, TeleGeography)均顯示(如下)，多數海底電纜路徑與全球主要航運走廊呈現顯著重合，並導致船錨與漁業活動成為海纜損壞的主要來源。

此種結構性共址 (structural co-location)，正是海事 - 數位耦合風險的根本來源。在這些被極度壓縮的戰略狹縫中，海洋的物理空間已不再是緩衝，而是一處處精確對準文明神經的預置戰場。正是在此結構性共址條件下，原本中性的航運行為，開始具備了潛在的破壞能力。

灰色地帶行動之所以能在高度監控與制度化的海洋環境中持續運作，其關鍵並不在於技術的複雜性，而在於行為本身的設計方式。與傳統軍事行動強調力量投射不同，此類行動的核心在於將敵對意圖完全嵌入於日常海事活動之中，使其在外觀上維持高度的正常性與合理性。換言之，破壞並非以異常事件的形式出現，而是以可被接受的例外(acceptable deviation)存在於航運體系的日常波動之中。

在繁忙的海洋貿易環境裡，船舶因機械故障、天候惡化或避碰需要而改變航速與航向，乃至進行緊急錨泊(emergency anchoring)，均屬常見現象。這些行為在船藝(Seamanship)與《國際海上避碰規則》(COLREGs)的操作邏輯下，不僅被允許，甚至在特定情境中被視為必要的安全措施。然而，當這些行為被精確地安排於海底電纜密集區域，並與特定的航跡模式結合，例如異常的減速、延長的停留時間或不尋常的錨鏈拖行距離時，一種看似偶然的操作，便可能轉化為具有明確效果的基礎設施干擾或破壞行為。

此種現象可被理解為一種設計過的偶然性(engineered contingency)一種偽裝出來的應急操作，就如《聖經》哥林多後書 11:14 所說的「這也不足為怪，因為連撒但也裝作

光明的天使」一樣，行動者並不直接製造顯著的異常，而是利用航運操作本身所固有的不確定性，將破壞行為嵌入於一個高度複雜且充滿雜訊的運作環境之中。在這種操作雜訊場(operational noise field)下，單一事件往往難以脫離其背景被獨立識別，從而使破壞行為得以隱匿於統計上可接受的變異範圍之內。

在此基礎上，不可歸因性(non-attributability)成為灰色地帶行動最具決定性的戰略優勢之一。與傳統戰爭中明確可追溯的攻擊來源不同，海底基礎設施的破壞往往缺乏直接證據鏈，使得責任歸屬高度依賴間接推論。即使透過衛星影像、AIS 航跡或航運資料分析，能夠辨識出高度可疑的船舶行為，在法律層面上，仍難以證明該行為係基於蓄意(Intention, Premeditated)而非過失(Negligence, Inadvertence)。特別是在深海環境中，關鍵證據，如錨具與電纜接觸的微觀痕跡，往往難以保存或重建，使舉證過程面臨結構性限制。

這種舉證困境不僅增加法律追責的難度，也直接削弱戰略回應的可能性。當受害國無法將事件明確歸因於特定行為者或國家時，其可採取的措施往往被限制於技術修復與風險緩解，而難以升級為具有嚇阻效果的外交或軍事回應。結果，行動者得以在極低政治成本下，對對手關鍵基礎設施進行持續性的低強度消耗(low-intensity attrition)，形成一種難以察覺但長期累積的戰略壓力。

更進一步而言，這種可否認性(Plausible Deniability)的設計，並非僅依賴操作層的隱蔽性，亦受到現行國際法體系的結構性支撐。在多數情況下，相關事件被歸類為海事事故，其處理機制落入民事責任與保險理賠的範疇。若受害國對可疑船舶採取強制攔截或扣押措施，則可能被視為違反航行自由原則，或構成對航運的不當干預。於是，法律體系本身反而形成一種防護罩，使行動者得以在規則之內運作，卻產生規則之外的效果。

在這樣的結構條件下，錨具的武器化不再只是技術層面的問題，而是一種結合操作合理性、證據模糊性與法律保護機制的複合性設計。船錨不僅是鋼鐵構成的物理裝置，更成為一種嵌入制度與戰略邏輯中的工具，使原本對稱的國際海事秩序，逐步轉化為一個有利於灰色地帶行動者的非對稱競爭環境。因此，當前海事安全所面臨的挑戰，已不再只是如何辨識單一異常事件，而是如何在充滿正常行為的表象之中，識別那些被刻意設計的偏離模式。

2.2 拖錨機制分析

相較於前一節所揭示的可否認性設計(Plausible Deniability)，拖錨(Dredging Anchor)之所以能在灰色地帶行動中發揮穩定效果，關鍵在於其同時具備可精準控制的物理執

行能力與可被合理化的環境敘事空間。換言之，拖錨並非單純的失控狀態，而是在特定條件下被轉化為一種可調節、可導引的水下深耕(subsurface ploughing)戰術，這個戰術，它不追求瞬間破壞，而是透過持續接觸與橫向刮削，在海床上沿既定路徑施加動能干擾，對海底電纜造成切斷或結構性損傷。

在物理執行層面，拖錨的核心並非在於是否拖行？而是如何讓拖行維持在可控的臨界狀態。於實務操作中，船舶會將航速壓制在一個既不完全停滯、亦不明顯航進的區間，使錨具持續與海床接觸並保持張力。此種低速航行狀態，一方面能增加錨爪嵌入海床的穩定性，另一方面亦可在外觀上呈現為逆風、逆流或機械受限下的一種艱難前進的操作。透過對主機推力、舵角與錨鏈釋放長度(scope)的細緻調整，操作者得以控制拖行方向與接觸角度，使錨具沿著預期路徑產生持續刮削。當海床條件，如砂質或泥質底，有利於嵌入時，這種受控拖行將顯著提高對埋設電纜的干擾效率。

與此同時，現代導航與定位技術，使拖錨行為具備了超越傳統經驗判斷的位置導向能力。在一般商用差分定位(DGPS)與航行資料的輔助下，操作者即便在不公開外部訊號的情況下，仍可精確掌握自身位置與航跡變化。當此一能力與海底電纜分布資訊相結合時，拖錨便不再是隨機發生的副作用，而成為一種對關鍵耦合節點的定向干擾。其技術門檻並不高，但在操作層面上卻具備足以影響跨區域數據連通性的精準效果。

然而，若僅從物理角度理解拖錨，其戰術價值仍不完整。此類行動之所以能長期運作，關鍵在於能將上述操作嵌入一套高度可信的環境敘事之中，使其外觀與事故模式保持一致。惡劣氣候與複雜海況，正是最常被利用的掩護條件。在強風、湧浪或急流作用下，船舶航跡出現偏移、減速或短暫停滯，本屬合理現象；同樣地，為了避碰或維持安全距離而採取非典型航線，亦符合航行安全原則。在這樣的背景下，即使拖錨距離異常延長，其行為仍可被解釋為對環境條件的被動回應，而非主動干擾。

此外，複雜的海底地形與高密度航運活動，進一步加強了這種掩護效果。在海床起伏明顯或多條電纜交錯的區域，拖錨所留下的物理痕跡難以在事後被清楚辨識；同時，頻繁往來的船舶也會在航跡資料中形成大量重疊訊號，降低單一事件的可辨識度。於是，物理層的干擾行為與環境條件共同作用，形成一種可被合理化的結果，使事故敘事在統計上顯得可信。

在此基礎上，導航誤差亦被納入戰術的一部分。於事後說明中，行為者可將拖錨歸因於海圖標示誤差、定位系統偏移或電子海圖(ECDIS)資料異常。這些說法並非全然虛構，而是建立在真實存在的不確定性之上。正因為航海本身即包含測量誤差與環境干擾，任何位置偏差都具備一定的合理性空間。當此類不確定性被策略性地利用時，便在法理上構成一個模糊區域，使過失與蓄意之間的界線難以清晰劃分。

綜合而言，拖錨機制在灰色地帶行動中的運作，呈現出一種關鍵特徵，拖錨機制是以可控的物理操作，生成不可確定的解釋結果：

1 其技術執行可達到相當程度的精準控制；

2 其外在表徵卻始終維持在事故敘事可接受的範圍之內；

3 這種可控的不確定性(controlled uncertainty)不僅使拖錨成為有效的干擾手段，也使其在制度與法律層面上難以被明確界定。

從更宏觀的角度來看，拖錨機制的戰術價值，並不僅在於其對單一電纜的破壞能力，而在於它揭示了一種新的行動邏輯，拖錨機制在當物理操作、環境條件與制度解釋三者能被同時整合時，即便是最基本的航海工具，也可以轉化為具有跨系統影響的戰略手段。

2.3 武器化光譜

為了在事故(accident)與攻擊(attack)之間建立更具辨識力的分析框架，本研究提出武器化光譜(weaponisation spectrum)模型，將海事行為依其意圖透明度(intent transparency)與戰略影響力(strategic impact)進行定位。此一光譜並非靜態分類工具，而是一種動態判讀機制，用以理解行為如何沿著由低到高的轉化路徑，逐步從單純的操作偏差(operational deviation)，演變為具備戰略目的的干擾行動(strategic disruption)。光譜可以簡單分類為下列這四個層級：

第一層級 L1 意外事故(Accidental Incidents)：純粹的操作失誤

在光譜的起點，屬於典型的意外事故(accidental incidents)。此類事件通常源於機械故障(mechanical failure)、極端氣候(extreme weather)或人為操作失誤(human error)，其行為本身不具備敵對意圖(hostile intent)。在操作特徵上，船舶航跡往往呈現高度隨機性(random drift pattern)，且事故發生後，船方多依循海事慣例進行通報(distress reporting)與現場處置。此一層級的風險，仍屬傳統海事安全(maritime safety)範疇，主要透過保險機制(marine insurance)與民事責任(civil liability)加以解決。

第二層級 L2 高風險操作(High-Risk Maneuvers)：過失與試探的邊界

當行為開始偏離上述模式時，光譜進入第二層級，即高風險操作(high-risk maneuvers)。在此情境中，船舶可能在已知為海底電纜密集區(subsea cable corridor)或

限制錨泊區(anchoring restricted zone)的情況下，仍進行錨泊(anchoring)或低速漂移(slow drifting)。此類行為在形式上仍可被解釋為操作決策的一部分，但其風險承擔顯著提高，並將潛在損害外部化至關鍵基礎設施(critical infrastructure)。更重要的是，在灰色地帶行動(grey-zone operations)的脈絡下，此類行為往往被用作戰術試探(tactical probing)，透過反覆出現在敏感區域，測試沿岸國家在監控(surveillance)、識別(identification)與執法(enforcement)上的反應能力與門檻。

第三層級 L3　蓄意破壞(Targeted Sabotage)：精準的物理打擊

當行為進一步呈現明確的目標導向(target orientation)時，便進入第三層級，即蓄意破壞(targeted sabotage)。在此階段，拖錨行為(anchor dredging)不再是風險的副產品，而是被用作一種具備方向性與目的性的干擾手段。其操作特徵通常包括與電纜走向呈交叉或平行的異常航跡(linear track anomaly)、在關鍵節點(critical nodes)附近的長時間停留(prolonged loitering)，以及完成行動後的迅速離場(rapid exit)。儘管這些特徵單獨存在時未必具有決定性證據價值，但其組合所呈現的模式，已顯著降低純屬意外的解釋可能性。在此層級中，行動者多為具特定目的的商業或準商業實體，其目標在於造成局部通訊中斷(localized disruption)或短期經濟擾動(economic disturbance)，同時維持一定程度的可否認性(plausible deniability)。

第四層級 L4　國家指導行動(State-Directed Operations)：混合戰爭的極致

位於光譜頂端的，則是國家指導行動(state-directed operations)。此類行動不僅在目標選擇上更具系統性，其執行亦往往與更廣泛的情報體系(intelligence apparatus)與戰略規劃(strategic planning)相結合。在此情境下，拖錨或其他物理干擾手段，通常與網路攻擊(cyber operations)、資訊操弄(information operations)及心理戰(psychological operations)形成協同效應(operational synchronisation)，構成所謂的混合戰爭(hybrid warfare)。其行動模式亦可能呈現多點分布(multi-node disruption)或時間序列設計(temporal sequencing)，以放大對關鍵基礎設施的系統性壓力，並削弱受害國的整體韌性(system resilience)。

值得強調的是，這四個層級之間並不存在明確且固定的分界，而是形成一條連續且可操作的戰略空間。灰色地帶行動的本質，正是在於將自身行為維持於高風險操作(L2)與蓄意破壞(L3)之間的門檻以下區域(below-threshold zone)，使其既能產生實質影響，又不致觸發明確的法律或軍事回應。此種門檻操作(threshold manipulation)策略，使武器化光譜不僅描述了風險的層級，也揭示了行動者在制度與認知邊界中的運作方式。

因此，武器化光譜的理論意義，在於提供一個連結操作層(operational layer)與戰略層(strategic layer)的分析橋樑。透過此一框架，即使面對表面上相似的海事事件，分析者仍可根據其行為模式(behavioral pattern)、空間分布(spatial distribution)與時間序列(temporal sequence)，判斷其在光譜中的位置，進而推論其潛在意圖與風險程度。

2.4 影子船隊的運作邏輯

在武器化光譜的高端區段，灰色地帶行動之所以能長期維持低可見度與高效能，關鍵並不僅在於單一技術或個別船舶，而在於一整套可供調度的運作載體。所謂影子船隊的運作邏輯(Shadow Fleet Dynamics)，正是這樣一種結構性存在，影子船隊並非固定編制的艦隊，而是一組在法律身份、所有權結構與營運紀錄上刻意維持模糊的船舶集合。其戰略價值，在於能夠把操作層的行為與制度層的責任追溯分離，從而讓灰色地帶行動在制度邊界之內持續運作。

影子船隊的生存空間，首先建立於權宜船旗制度(Flags of Convenience, FOC)的制度特性之上。依循 UNCLOS 的基本架構，船舶的主要管轄權歸屬於船旗國(flag state)。在此制度下，船東得以在與實際營運地無直接關聯的國家完成登記，藉此降低成本並提升營運彈性。然而，在實務操作中，FOC 制度亦使所有權鏈條(ownership chain)呈現高度分散的狀態。透過多層離岸公司(offshore entities)與空殼公司(shell companies)的轉包甚或再轉包安排，最終受益人(ultimate beneficial owner, UBO)往往被隱藏於複雜的法律結構之後。此種制度性隱身(institutional opacity)意味著，一旦發生海底電纜損壞或可疑行為，即使船舶本身被識別，追溯至真正決策者的過程仍可能因跨法域與公司結構而中斷。

與此同時，影子船隊亦常運作於一種近似監管真空(regulatory vacuum)的環境之中。這些船舶可能未受主要保賠體系的完整覆蓋，例如未納入國際船東互保協會(International Group of P&I Clubs)的標準保障範圍，或僅維持最低限度的合規狀態。當事故或損害發生時，傳統依賴保險理賠與船旗國責任的追償機制，便難以有效運作。結果是，法律責任與經濟成本被系統性地外部化，使行動者能在低風險承擔的情況下，利用商用船舶執行具有潛在戰略效果的任務。

在此制度基礎之上，影子船隊的第二項關鍵特徵，在於其作為雙重用途平台(dual-use platform)的轉化能力。這些船舶在外觀與功能上仍維持一般商用運輸的形式，但在特定條件下，其航行行為與技術配置可同時承擔資訊蒐集(intelligence collection)與物理干擾(physical disruption)的角色。舉例而言，船舶於電纜密集區域的反覆航行，不僅可能對海底設施構成潛在風險，亦可被用於蒐集航運流量、監測節點活動，或驗證既有

海圖與定位資料的精確性。當此類行為與前述的拖錨操作結合時，船舶即由單純的物流載具，轉化為具備觀測與干擾功能的複合節點。

更進一步而言，影子船隊的運作往往呈現出網絡化與分散式的特徵(distributed operations)。在特定敏感海域中，可能出現多艘船舶以不同旗國與所有權結構交替出現，其航跡與操作行為彼此重疊，形成一種航跡雜訊(traffic noise)的效果。對監控方而言，這種群體性的異常活動會顯著提高辨識難度，固然，單一船舶的行為可被解釋為偶發事件，但當多艘船舶同時呈現類似模式時，其整體效果卻可能構成對關鍵基礎設施的持續壓力。這種群體偽裝(collective masking)機制，使海上交通由原本可預測的秩序狀態，轉變為充滿戰略不確定性的動態環境。

從風險治理的角度觀之，影子船隊的存在揭示了一項結構性問題，意即當國際海事秩序建立於透明度(Transparency)與責任鏈(Chain of Responsibility)之上時，任何能夠系統性削弱這兩項要素的機制，都將對整體安全架構產生放大效應。影子船隊並非單純的違規船舶集合，而是一種能夠將航運、法律制度與戰略目的連結起來的運作模式。當其與可否認性設計與拖錨機制相結合時，便形成一套完整的灰色地帶行動體系，使低強度干擾得以在長期、分散且難以歸因的條件下持續發生。

2.5 航跡與數據操控

在灰色地帶行動的整體設計中，對被看見的方式進行控制，與對海床的物理干擾同樣關鍵。自動識別系統(Automatic Identification System, AIS)原本是為避碰(collision avoidance)與海上交通管理(VTS)所設的安全工具，但在監控高度依賴其資料的情境下，AIS 同時成為可被操弄的資訊入口。行動者不必讓自己完全消失，只需在關鍵時段改變或中斷可觀測性，即可在資料層面重寫行為的敘事(data narrative reconstruction)，從而為前述拖錨與影子船隊的運作提供掩護。

數位匿蹤：AIS Dark Activity (訊號隱沒)

所謂 AIS 訊號隱沒(AIS dark activity)，是最基礎且成本最低的數位匿蹤手段。船舶在接近電纜密集區或關鍵耦合節點(critical interface nodes)之前，選擇關閉或間歇發送 AIS 訊號，於公開監控系統中形成一段時間的黑暗期(dark gap)。在這段期間內發生的低速拖行、臨時錨泊或異常停留，將缺乏直接的航跡證據支持。由於國際規範允許在特定安全情境下暫時關閉或限制訊號，單次隱沒本身難以構成違規；更關鍵的是，當影子船隊在特定咽喉點(chokepoints)反覆進行此類切換，便會將訊號遺失常態化(normalisation of loss)，其外觀上可被解釋為設備老化、天候干擾或衛星接收品質不佳，

但結果是，執法與監控單位在判斷何時為刻意隱藏時的門檻被顯著抬高，從而在制度上形成持續性的監控斷層(surveillance gap)。

數位偽裝：AIS Spoofing (訊號欺騙)

相較之下，AIS 訊號欺騙(AIS spoofing)則是一種更進階的數位偽裝策略。其核心不在於消失，而在於創造一條看似合理、實則錯置的航行軌跡。透過發送偏移的地理座標(geospatial offset)、不一致的航行狀態(navigational status)，或重播既有訊號(replay)，船舶可以在資料上維持連續航行，而實際上卻在敏感區域執行低速拖行或停留。典型效果包括地理偏移(positional displacement)， 即實際在 A 區域作業，AIS 卻顯示於數海里外的 B 區域 ，以及身份重疊(identity collision)或 MMSI 複用(MMSI cloning)，在監控畫面上形成多個相似或重疊的目標，削弱對單一船舶的追蹤連續性。這種資料層的合理化錯誤，使事後回溯時難以將損壞點與特定船舶建立穩固關聯。

關鍵在於，AIS 隱沒與 AIS 欺騙往往與物理操作形成時間上的協同。常見模式是，船舶在進入敏感區前維持正常訊號以建立合規基線(baseline compliance)；進入關鍵區段後短暫隱沒或進行座標偏移；完成拖錨或停留後再恢復正常廣播。對外部觀察者而言，整體航跡仍呈現可接受的連續性，而真正關鍵的操作則被嵌入於一段難以直接觀測或被錯置的時間窗內。這種時間分割(temporal segmentation)與空間錯置(spatial misalignment)的結合，正是數據操控在灰色地帶行動中的技術精髓。

數據操控導致的歸因困境(The Attribution Gap)

上述做法直接導向一個更深層的問題，即歸因落差(attribution gap)。在海事調查與司法程序中，AIS 航跡長期被視為重建事件因果關係的重要證據(evidentiary record)。然而，一旦資料源頭本身被系統性操弄，證據鏈便出現數位污染(data contamination)。即使受害方掌握了其他來源的觀測，例如合成孔徑雷達(synthetic aperture radar, SAR)影像、光學衛星資料或現場巡查紀錄，若無法與 AIS 軌跡形成一致的時空對應(spatio-temporal alignment)，在法律上仍難以完成嚴謹的因果論證(causation)。於是，證據不再是不存在，而是彼此不相容，使案件長期停留在高度懷疑但難以定論的狀態。

進一步而言，為彌補 AIS 所造成的監控斷層，防禦方必須引入更高成本的感測與執法手段，例如持續調用 SAR 衛星、整合多源資料(multi-source fusion)，或進行海上攔截與臨檢。這種由數據操控所引發的調查成本外溢(cost externalisation)具有明顯的非對稱性，一種行動者以低成本改寫或中斷資料，而受害方則需以高成本重建真實的非對稱成本與作為。當此種成本差長期存在時，便形成一種穩定的戰略紅利(strategic advantage)，使灰色地帶行動得以在不升高衝突門檻的情況下持續運作。

從整體架構來看，AIS 操控並非孤立技術，而是與拖錨機制、影子船隊與可否認性設計共同構成一個跨層級的干擾體系。航跡不再只是航行的紀錄(record of movement)，而是可以被設計、分割與重寫的資訊產品(engineered data artifact)。當物理層的行為、環境層的掩護與數據層的操控相互耦合時，海事安全所面臨的挑戰，便從「如何觀測」船舶轉變為「如何驗證觀測」本身。這一轉變，正是理解灰色地帶行動運作邏輯的關鍵。

三、戰略咽喉的斷裂風險

全球網絡看似分散，實則集中；看似冗餘，實則共命。地理的緊湊本是為了效率的極致，卻在動盪時代演變為無法逃脫的戰略負債。當效率將路徑壓縮至極限，脆弱性便在同一處被放大，使這些關鍵咽喉點，從數位文明的加速器轉化為隨時可能被單一錨具觸發多點斷裂的系統性地雷。

3.1 海底電纜的網絡拓撲結構

在前兩章釐清技術機制與行動載體之後，分析的重心需回到結構本身。也就是說，即便不考慮拖錨、影子船隊或 AIS 操控，海底電纜系統是否已內含可被利用的脆弱性？答案在其網絡拓撲(network topology)之中。為追求效率與成本最適化，全球電纜體系呈現出高度集中化的樞紐軸輻網路(hub-and-spoke)特徵，而這種結構正是灰色地帶行動得以產生超比例效果的基礎條件。

首先，核心節點(core nodes)的集中，構成整體網絡的關鍵瓶頸。全球跨區域數據流最終匯入少數岸端登陸站(cable landing stations)與互連樞紐(interconnection hubs)，這些節點同時依賴港口設施、電力供應與陸地骨幹網(terrestrial backbone)的接入能力。由於選址與建設成本高昂，替代節點的冗餘(redundancy)往往有限，導致網絡在節點層面呈現高集中、低替代的結構特性。一旦登陸站周邊海域遭受持續騷擾、封鎖或反覆干擾，即使未直接破壞設施本體，也可能透過運維受阻(maintenance disruption)與流量再路由(traffic re-routing)造成區域性通訊品質劣化，進而放大為跨區域的服務中斷。

其次，路徑(routes)的集中化同樣顯著。受制於海底地形(bathymetry)、地質風險(如海溝、火山帶)與鋪設成本，多條跨洋電纜在接近陸地或穿越狹窄水域時，往往沿著相似甚至重疊的走廊(cable corridors)平行鋪設，形成路徑輻輳(route convergence)。在這些寬度有限的通道內，數十條電纜可能共享數海里的空間，將原本應分散的風險壓縮至單一地理區域。其直接後果，是典型的單點故障放大(single-point-of-failure

amplification)，也就是一次針對該走廊的精準干擾，即可能同時影響多條獨立系統，並在短時間內切斷主要對外通訊路徑。

更具結構性意涵的，全球最繁忙的商用航道，往往亦是電纜主幹線路的首選路徑，因其代表最短距離、最低成本與最佳維修可及性。結果是在馬六甲海峽、紅海走廊、蘇伊士通道與台灣海峽等區域，物理層的海運航道(shipping lanes)與邏輯層的數據管線(data routes)幾乎完全重合。這種數位 - 航運共用通道(digital-maritime shared corridors)的空間重疊現象，使日常航運行為，如操船、避碰、臨時錨泊或漁撈活動，得以直接作用於數位基礎設施，將原本屬於航行安全的事件，轉化為潛在的系統性風險。

在這些共用通道中，高密度交通意味著大量船舶在有限空間內進行動態調整，單一異常航跡更容易被淹沒於整體流量之中；同時，執法與監控資源在面對海量目標時，對個別行為的識別門檻被動抬高。這樣的擁擠效應(congestion effect)與監控飽和(surveillance saturation)進一步放大了脆弱性。此種大隱於市(masking by density)的環境，使灰色地帶行動能在統計上維持低可疑度，而在效果上卻集中於關鍵節點與路徑。

從戰略角度觀之，在節點 - 路徑高度集中且與航運通道重疊的條件下，行動者無需進行全面性破壞，只需在少數戰略咽喉點(strategic chokepoints)上實施精準干擾，即可誘發跨系統的連鎖效應(cascading effects)。此一結構性不對稱，對防禦方形成分散防護對抗點狀干擾(distributed defense vs point disruption)的長期壓力，並揭示了當前海事與數位體系的共同盲點，這種拓撲結構也為行動者提供了顯著的攻擊槓桿(attack leverage)。

因此，海底電纜的網絡拓撲不僅是工程配置問題，更是決定風險分布與衝擊幅度的戰略變數。當效率導向的設計導致節點與路徑的高度集中，而這些關鍵區域又與航運活動深度重疊時，全球系統便在無形中暴露於少數可被精準利用的脆弱點之下。理解此一結構，是後續區域案例分析與韌性重構策略的前提，也說明了為何全球航運秩序必須由效率優先(efficiency-first)轉向韌性優先(resilience-first)的根本原因。

3.2 系統性脆弱性

在具備冗餘(redundancy)設計的前提下，海底電纜網絡理應能以替代路徑(alternate routes)維持基本連通。然而，灰色地帶行動所揭示的問題在於當干擾從單點擴展為多點、且集中於同一拓撲走廊時，系統不再線性退化，而會出現級聯式失效(cascading failure)。此一轉變，正是系統性脆弱性的核心。

首先，多點同時失效(multi-point failure)會在極短時間內耗盡原本設計用於緩衝的冗餘能力。由於多條電纜在狹窄走廊內平行鋪設，一旦行動者在同一海域對多條主幹

線(trunk routes)實施同步或近同步的干擾，備援路徑將迅速被迫承接突增流量。當替代容量(spare capacity)不足時，網絡即由降級運作(degraded operation)滑入部分中斷(partial outage)，甚至形成區域性的數位黑洞(digital blackout)。更關鍵的是，骨幹網絡(backbone network)在承壓後會出現壓力級聯(load cascading)，使得流量外溢至次級節點(secondary nodes)，引發擁塞(congestion)、封包丟失(packet loss)與路由震盪(route flapping)，進而將局部干擾擴散為跨區域問題。

其次，重新路由延遲(rerouting latency)構成這種失效的時間成本。當主要電纜中斷後，流量需改走非最優路徑(non-optimal paths)，例如跨洋繞道(inter-ocean detours)或增加中繼節點(additional hops)。在技術上，邊界閘道協定(Border Gateway Protocol, BGP)的路由收斂(convergence)本就需要時間，而跨多個自治系統(autonomous systems)的協調，會放大這一延遲。即使路由最終穩定，較長的物理距離與更多節點亦會推高往返時延(round-trip time, RTT)，並降低有效吞吐(throughput)。

對於高度依賴低延遲的應用，這種變化具有實質經濟影響。在金融領域，高頻交易(high-frequency trading, HFT)與即時清算系統(如 SWIFT、Fedwire)對毫秒級延遲極為敏感；哪怕數十毫秒的增加，亦可能改變撮合順序與價格發現機制，造成流動性下降與波動放大，甚至在極端條件下觸發閃崩(flash crash)。在航運與物流領域，港口作業系統(terminal operating systems, TOS)與供應鏈協同平台(logistics platforms)依賴穩定連通以進行排程與調度；一旦資料同步出現延遲或不一致(data inconsistency)，即可能引發船舶壅塞(vessel congestion)、碼頭周轉率下降與內陸運輸失序，最終反映為運價波動與交期不確定性的上升。

再次，系統性脆弱性還體現在數位後遺症(digital aftereffects)上，即修復與恢復過程本身的限制。海纜不同於衛星鏈路，其修復依賴專業電纜維修船(cable repair vessels)進行定位、打撈與熔接(splicing)。此類船舶在全球屬於戰略性稀缺資源(strategically scarce assets)，且受合約排程、氣象條件與作業安全限制所制約。在衝突頻仍或准入受限的海域，維修時程(repair latency)往往被進一步拉長，使中斷從短期事件轉化為中期壓力。更重要的是，即便物理連通恢復，長期的不穩定與安全疑慮會改變資本與數據的地理配置(geographic reallocation)，其雲端與資料中心可能轉移至更穩定的節點，金融與航運活動亦隨之重組，對區域樞紐(如東京、上海、香港、台灣、新加坡)的競爭力造成結構性影響。

綜合而言，系統性脆弱性揭示了一個關鍵事實，在高度耦合的海事 - 數位體系中，風險的影響力不再取決於單一破壞的強度，而取決於其對時間、容量與連續性的擾動能力。當多點失效與重新路由延遲相互作用時，小規模、低強度的干擾即可觸發跨系

統的連鎖效應，形成遠超其物理規模的影響。這一認識，為後續區域案例的解讀與韌性重構策略的設計，提供了必要的分析基礎。

3.3 區域案例深度分析

3.3.1 波羅的海(Baltic Sea)：Yi Peng 3 事件中的多國取證僵局

波羅的海案例的關鍵意義，在於它展示了灰色地帶行動如何在一個高度監控(high-surveillance environment)與制度成熟的海域中，仍能成功製造取證斷層(evidentiary gap)。這並非因為監控不足，而是因為行動本身被設計於法律與技術邊界之內。

從 2022 年起，波羅的海，共有 10 條 電纜被割斷，其中有 7 條集中在 2024 年 11 月至 2025 年 1 月之間。在 2024 年底，連接瑞典、立陶宛、芬蘭與德國的多條海底電纜接連中斷。中國籍散裝船伊鵬 3 號(Yi Peng 3)因其航跡異常(anomalous vessel behavior)而成為核心觀察對象。伊鵬 3 號在關鍵電纜區域上方出現低速漂移(low-speed loitering)，並呈現與既定航道不一致的運動模式。此類行為在技術上高度符合前述 L3/L4 層級之拖錨操作特徵(targeted anchor dredging)。

然而，真正的問題並不在於是否存在破壞行為，而在於是否能證明其為蓄意。儘管北約(NATO)成員國迅速部署海空監控力量，但該船在公海或專屬經濟區(EEZ)範圍內，

依法仍享有航行自由(freedom of navigation)與船旗國專屬管轄權(exclusive flag state jurisdiction)。在缺乏直接證據(direct evidence)與明確敵對行為(hostile intent)的情況下，沿岸國難以採取強制登檢(boarding)或扣押(detention)措施。

此案例揭示了一個結構性矛盾，意即當行動同時具備物理可行性(physical plausibility)與法律不可證性(legal non-attributability)時，國際法體系將失去其介入能力。換言之，波羅的海並非單純的事故現場，而是一個典型的法律失效空間(legal incapacity zone)，其本質正是灰色地帶行動的理想操作場域。

3.3.2 台海與印太海域：非對稱作戰下的「準封鎖」(Quarantine)

相較於波羅的海所呈現的取證僵局，台海案例進一步揭示了灰色地帶行動如何在反覆發生、逐步累積的過程中，轉化為一種具體且可感知的戰略壓力機制(persistent strategic pressure mechanism)。

台灣海峽同時具備兩項高度敏感特徵：其一為全球最繁忙的航運通道之一，其二為連接東北亞與東南亞的數據主幹路徑(data trunk corridor)。這種數位 - 航運共用通道(digital-maritime shared corridor)的高度重疊，使得任何海事行為，都可能同時作用於物流與資訊流兩個系統層面。

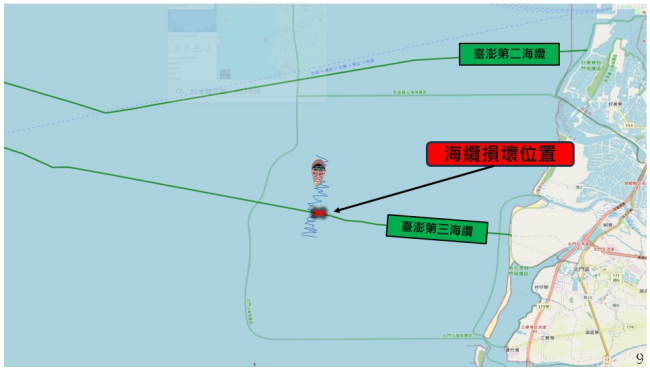
在此背景下，台灣外離島(特別是馬祖)海底電纜的多次中斷，呈現出與傳統事故截然不同的特徵，它並非單一高強度破壞，而是高頻率、低強度、可否認性極高的反覆干擾(high-frequency, low-intensity disruption)。涉事船隻類型多樣，包括抽砂船、漁船與不明貨輪，其共同特徵在於行為模式高度接近武器化光譜中的 L2 至 L3 區間。

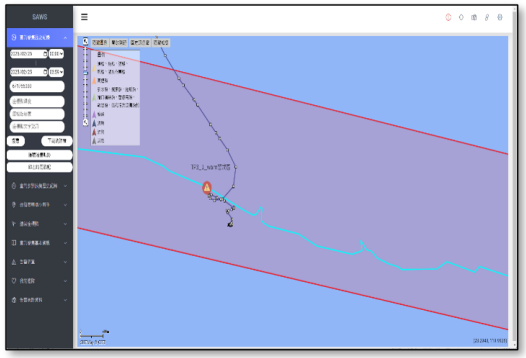
然而，台灣海峽案例最具突破性的發展，在於部分事件已進入司法層面的定性。例如「宏泰 58」案件中，法院認定該船在已知電纜位置且屬禁止錨泊區域的情況下，仍進行異常錨泊與航行操作，最終導致海底電纜損壞。判決指出，船長對於海纜存在具有可預見性(foreseeability)，其行為已超越單純過失(negligence)，構成對關鍵基礎設施的損害責任。此一判例的重要性在於，它將海底電纜破壞從海事事故(maritime incident)提升為關鍵基礎設施攻擊(critical infrastructure damage)的法律範疇。換言之，台灣在特定條件下，已能將灰色地帶行動的一部分轉化為可裁判的法律事件，這與波羅的海案例的高度懷疑但無法定罪形成鮮明對比。

在戰略層面上，不同於傳統海軍封鎖(naval blockade)，此種模式不依賴軍事力量的全面部署，而是透過持續干擾數位連通性，使目標區域逐步進入功能性孤立(functional isolation)狀態，構成準封鎖(quarantine)的操作邏輯。其核心不在於完全切斷通訊，而

在於削弱其穩定性(stability)與可預測性(predictability)。當這種干擾集中於外離島或邊緣節點時，即會形成數位孤島化(digital islanding)效應。其影響不僅限於民生通訊，更可能透過金融市場、資訊流通與社會心理產生放大效應。此外，這種低強度但持續的干擾，同時具備戰略測試(strategic probing)功能，使行動者能在不觸發軍事衝突門檻的情況下，評估目標體系的韌性與國際反應。

因此，台灣海峽案例的核心意義，在於揭示，海底電纜不再只是脆弱基礎設施，而是被納入非對稱作戰中的壓力施加界面(pressure interface)的一種新的作戰範式。在這一界面上，法律、技術與戰略三者交錯，使灰色地帶行動從難以證明的威脅，逐步轉化為可被感知、甚至可被裁判的現實。這也意味著，台灣海峽並非僅是潛在衝突區域，而是灰色地帶行動最前沿的實驗場(frontline laboratory)。





3.3.3 紅海走廊(Red Sea Corridor)：衝突外溢與漂移錨具的持續風險

若波羅的海代表法律困境，台灣海峽代表戰略運用，則紅海案例則揭示了衝突外溢所產生的非意圖性系統風險(conflict-induced systemic risk)的第三種類型。

在 2024 年紅海危機期間，多條連接歐亞的海底電纜，包括 Seacom、TGN、AAE-1 及 EIG 在內，至少 4 條重要的國際海纜中斷，影響了亞歐中東地區約 25%的數據流量。調查顯示，損壞並非直接來自水下攻擊，而是由遭到胡塞武裝飛彈擊的貝里斯籍商船(MV Rubymar)在沉沒與漂移約兩週的過程中，其錨具與船體殘骸在海床拖行所致。這一機制本質上屬於次生破壞(secondary damage)，但其影響卻不亞於蓄意行動。

紅海案例的關鍵在於，它引入了一種新的風險來源，意即沉沒資產(sunken assets)可以轉化為持續性威脅(persistent hazard)。在高衝突密度海域中，受損船舶、漂移錨具與未清除殘骸，將隨時間與海流持續移動，對海底電纜形成長期且不可預測的干擾。

這種風險具有三項特徵：

1　非可控性(non-controllability)：不再依賴行動者決策；

2　長尾效應(long-tail risk)：影響可持續數月甚至數年；

3　修復困難(repair constraint)：受限於安全環境與維修船進入限制。

當此類風險發生於如曼德海峽(Bab el-Mandeb)這類全球數據與航運雙重咽喉點時，其影響將迅速外溢至歐亞之間的數據傳輸與供應鏈體系。因此，紅海案例的真正意義在於指出，海底基礎設施的威脅，並不僅來自灰色地帶行動本身，也可能來自傳統衝突所釋放出的無主風險(ownerless risk)。

四、灰色地帶的法律裂縫

法律原本用來界定行為，但在灰色地帶中，它開始保護模糊，演變成一場法治的諷刺劇。最深的危機，不在於規則被違反，而在於程序正義仍被精確遵守，卻淪為侵略者的防彈衣，讓防禦方陷入招架無力的法律枷鎖。這是一種主權的癱瘓，使法律在最需要介入的時點，僅能淪為一場場無濟於事的事後悼念。

4.1 UNCLOS 的結構性局限：主權延伸與執法真空

1982 年制定的 UNCLOS 常被稱為海洋憲法(constitution for the oceans)，其制度核心在於以分區管轄(zonal jurisdiction)平衡沿岸國權利與全球航行自由。然而，這一架構建立於以可見、可歸因威脅為前提的安全觀，當代以海底電纜為核心的數位基礎設施與海事行為高度耦合，已使原有邏輯出現明顯的結構性錯位(structural mismatch)。問題不在於規範是否存在，而在於規範是否允許在風險尚未轉化為明確違法之前進行有效介入(pre-emptive intervention)。

在專屬經濟區(Exclusive Economic Zone, EEZ)內，這種錯位最為顯著。依據 UNCLOS 第 56 條與第 58 條，沿岸國對自然資源享有主權權利(sovereign rights)，而各國同時保有航行自由與鋪設海底電纜的自由(freedoms of navigation and laying of cables)。然而，海底電纜在法律分類上並非自然資源，而是跨國私有與公共性兼具的基礎設施(subsea infrastructure)。由此產生一個沿岸國對經濟利益具有保護權，但對支撐數位經濟運作的關鍵設施，卻缺乏對應的前置執法權限的關鍵悖論。

在操作層面，這一悖論具體表現為管轄灰區(jurisdictional grey zone)。外國船舶在 EEZ 內進行低速漂移(low-speed loitering)、異常錨泊(abnormal anchoring)或短時 AIS 隱沒

(AIS dark activity)，即便位於電纜走廊(cable corridors)上方，仍難被直接界定為違法行為。除非沿岸國能證明涉及污染(pollution)、非法捕撈(IUU fishing)或其他明確違規，否則其進行登船檢查(boarding)或強制攔截(interdiction)的法源基礎極為有限。於是形成一種典型困境 - 國家可以觀察到風險(observe risk)，卻難以在法律上及時阻止(legally intervene)。

與 EEZ 相鄰的領海(territorial sea)情境，則呈現另一種形式的制度張力。UNCLOS 對無害通過(innocent passage)採取寬鬆標準，只要船舶維持連續且迅速的通過(continuous and expeditious transit)，即原則上被視為合法。這一設計原本旨在保障國際航運，但在灰色地帶操作中，卻可能被轉化為法律護盾(legal shield)。行動者可在過境過程中嵌入短時的拖錨或異常操作，使其行為在時間與空間上維持於尚可解釋為無害的區間。對執法機關而言，關鍵難題不僅在於是否攔截，更在於何時判定行為已從無害跨越為有害(prejudicial to peace, good order or security)。在舉證標準未明確之前，任何過早介入均可能被解讀為對航行自由的過度干預(excessive interference)，從而反向產生法律與外交風險。

若將視角進一步延伸至公海(high seas)，制度上的執法真空(enforcement vacuum)更為突出。UNCLOS 確立船旗國專屬管轄(exclusive flag state jurisdiction)為基本原則，除海盜、奴隸販運或無國籍船舶等少數例外外，其他國家原則上無權對外籍船舶進行登檢。當海底電纜受損發生於公海或接近公海之海域時，調查與取證即高度依賴船旗國的配合意願與能力。結合前述權宜船旗(FOC)與複雜所有權鏈(ownership chain)，此一機制往往導致責任主體的不可見(opacity of beneficial ownership)與執法行動的不可行(operational infeasibility)。

綜合 EEZ、領海與公海三種空間，可以觀察到一個共同結論，UNCLOS 所建立的，是一套以事後責任(ex post liability)為核心的秩序，而非以風險預防(risk-based prevention)為導向的體系。在傳統海事環境中，這一模式足以運作；但在灰色地帶條件下，行動刻意維持於違法門檻以下(below-threshold operations)，使法律機制在最需要介入的時點反而失效。結果是，海洋空間中的關鍵區域逐漸演變為一種低度管制、高度競逐的戰略灰區(low-regulation, high-contestation maritime space)。

因此，UNCLOS 的結構性局限，不在於其規範內容過於薄弱，而在於其分類邏輯與當代威脅型態之間存在根本落差。當威脅以高風險但可否認(high-risk yet deniable)的形式出現時，現行體系既無法有效阻止，也難以在事後確立責任。這一點，正構成後續歸因困境(attribution problem)與船旗國責任失效(failure of flag state responsibility)的制度前提。

4.2 行為與意圖的落差

在灰色地帶條件下，法律體系所倚賴的證明邏輯，由客觀行為(actus reus)推導主觀要素(mens rea)，被系統性地削弱。

海事與多數國內法在侵權與責任認定上，首先處理的是發生了什麼？航跡是否偏離？是否存在拖錨痕跡？電纜是否斷裂與訊號中斷？然而，灰色地帶行動的關鍵，正是在於讓可觀測的物理行為與合法海事操作在數據特徵上高度重疊，從而切斷由行為推論意圖的證據鏈(chain of evidence)。

這種重疊使過失(negligence)成為最自然、也是最容易被接受的法律分類。當船舶在電纜走廊上方低速漂移或拖錨，第一時間的法理歸屬往往是航行判斷失誤、氣象因素或設備異常所致。要將同一組事實上升為惡意破壞(sabotage)或敵對行動(hostile act)，則必須證明行為人具備主觀意圖。問題在於，意圖本身不可視(non-observable)且高度依賴內部證據，如通訊紀錄、指令鏈或人員供述。在缺乏直接證據的情況下，辯方得以以海況判斷錯誤、操船需要、避碰機動或機械故障導致非自願拋錨等替代敘事進行合理化，形成同一事實、雙重解釋(dual-interpretability)的格局。

灰色地帶行動正是利用這一落差，將破壞效果鎖定於客觀層，而將主觀要素維持在不可證狀態。其結果是，行為在物理上已造成損害，但在法律上仍停留於未證明的事故(unproven incident)。這不僅是證據不足的問題，而是一種意圖不可證性(intent non-provability)的制度性利用，一種證據結構被刻意設計為不足的現象。

這種意圖不可證性在實務操作中，進一步演變為一種策略性的法律掩體(Tactical Legal Bunker)。破壞者並非透過違反法律來達成目標，而是透過精確地遵守法律程序來武裝其破壞行為。

在現行 UNCLOS 框架下，無害通過(Innocent Passage)與船旗國管轄(Flag State Jurisdiction)被視為國際海洋秩序中不可侵犯的程序正義。蓄意破壞者的核心邏輯在於，如果一個國家意圖切斷海底電纜，它無需動用具備明顯敵意的軍事資產(如潛艦或特種部隊)，而僅需指導一艘掛著民用旗幟、身分合法的商船，在經過關鍵戰略節點時，將破壞行為包裝成一場意外。

當該船隻在形式上完全符合報備程序、維持著商用航行的外觀，卻因機械故障或氣象因素在敏感海域發生非自願拋錨與拖行時，法律的正當程序反而成了防礙干預的障礙。對沿岸國而言，在此情境下發起強制攔截，不僅面臨極高的舉證壓力(必須證明其非意外)，更可能反遭指控為破壞航行自由或濫用管轄權(Creeping Jurisdiction)。這種法律的束縛(Legal Constraints)創造了一種極端的不對稱，破壞者利用法治社會對程序正

義的堅持，將法律轉化為其行動的防彈衣，使防禦方在面對明顯的物理風險時，因法律上的投鼠忌器而陷入招架無力的困境。

在責任與成本配置上，這一機制進一步放大了非對稱優勢。海事賠償體系對過失行為的處理，多以民事責任為主，代價通常限於金錢賠償，且可透過保險(如 P&I)分散。當戰略性破壞被包裝為民事侵權(civil tort)，其法律後果被有效地去安全化(de-securitized)，由國家安全層級降為商業糾紛層級。對具備國家背景或高風險容忍度的行動者而言，這意味著可以以極低的邊際成本(marginal cost)，反覆施加對關鍵基礎設施的干擾。

更重要的是，這種以民事掩蓋刑事(civil masking of criminal/hostile conduct)的策略，會侵蝕法律的震懾功能(deterrence)。震懾的前提，是對惡意行為能夠被識別並施以高強度制裁；但當行為者只需避免留下明確的主觀證據，即可在被攔截或調查後仍被歸類為航行失當(improper seamanship)並以罰款或賠償了結時，預期制裁(expected sanction)將大幅下降。長期而言，這將誘發更多低強度、高頻率的試探性行動，使風險在系統中常態化。

從證據法(law of evidence)的角度觀察，現行框架在舉證責任(burden of proof)上呈現結構性傾斜。受害方反而需證明對方具有惡意或至少重大過失，而非要求在敏感區域操作的船舶證明其行為之正當性。於是形成一種保護數位海洋的一方承擔高證明門檻，而可能造成風險的一方則享有推定無害(presumption of innocuousness)的不對稱現象。在海底電纜等關鍵基礎設施密集區，這種配置使前置防護(ex ante protection)難以啟動，執法只能在事後責任(ex post liability)層面運作。

因此，行動與意圖之間的差距(Act-Intent Gap)並非單純的鑑識困難，而是當代法律設計與灰色地帶威脅之間的核心落差。只要主觀要素仍是責任成立的關鍵，而行動者又能持續在可疑但不可證(suspicious yet unprovable)的區間內運作，海底基礎設施的保護便會反覆陷入「已受損 - 難定性 - 低制裁」的循環。

4.3 歸因困境：從證據黑盒到法理對抗

在灰色地帶行動的語境中，歸因(attribution problem)不再只是技術鑑識的終點，而是法律、科學與政治三者交會的臨界點。海底電纜事件之所以難以被有效定性，不在於缺乏損害事實，而在於損害難以被穩定地連結到特定行為者，並進一步上升為可承擔法律或國際責任的主體。這種困境在引入數位取證與科學感測後，不僅沒有迎刃而解，反而引發了更深層的法理衝突。

科學證據與法律證明標準的位階衝突

當前的國際海事法庭(如 International Tribunal for the Law of the Sea, ITLOS)或國際法院(International Court of Justice, ICJ)在處理海事糾紛時，證據體系仍高度向傳統觀測傾斜。然而，灰色地帶行動的核心在於數位隱身，這迫使歸因必須仰賴分散式聲學感測(DAS)、合成孔徑雷達(SAR)或遙感探測等高階技術。

在法律實務中，這引發了演算法黑箱(Algorithmic Black Box)與證據透明度的衝突。例如，當 DAS 系統透過光纖震動分析技術鎖定某艘船舶的螺旋槳特徵(Acoustic Fingerprint)時，辯方律師可主張該技術的識別邏輯屬於開發商的商業機密，法院無法進行獨立的交叉詰問或司法覆核。在法庭對抗中，辯方可透過提出替代解釋，如地震活動、大型海洋生物干擾或既有沉船殘骸產生的聲學反射，來削弱科學數據的唯一性。於是，科學鑑識雖能提升高度可能性，卻難以跨越刑事或重大損害賠償中排除合理懷疑(Beyond Reasonable Doubt)的嚴苛門檻。

數位取證與形式真實的矛盾

其次，即便高品質的科學證據得以取得，其在向法律證據轉換的過程中，仍面臨數位真實與形式紀錄的因果斷裂。自動識別系統(AIS)資料在法律上通常具備公信力，但其在灰色地帶行動中卻是可被操控的脆弱工具。

當水下聲學感測明確顯示某艘船舶在電纜故障點執行了拋錨動作，但官方 AIS 紀錄卻顯示該船位於數十海浬外，或處於訊號中斷(Dark Activity)狀態時，法庭將面臨嚴重的證據不一致。在缺乏船舶數據記錄器(VDR)實體採證的情況下，法庭往往陷入技術推論與法定紀錄的權衡困境。

由於國際法對推定責任的適用極為謹慎，行為者只要能製造出 1%的數位模糊空間，例如利用 AIS 欺騙製造虛假座標，就能利用疑點利益歸於被告(In dubio pro reo)的原則，使受害國在法律歸因上空有感測數據，卻無法達成法律上的因果鏈閉環。

法律程序中舉證責任的失衡

進一步而言，目前的程序法並未針對數位隱身建立相應的舉證責任倒置(Shift of Burden of Proof)機制。在傳統海事法中，船東只需提交其符合規範的航行日誌與 AIS 紀錄即視為履行初步義務。

在灰色地帶環境下，這種證據結構對受害方極不公平。即使受害國能提供衛星 SAR 影像或水下音訊作為強烈間接證據，若無法達成高度精確的時空重疊，法官仍難以做出具有強制力的歸屬裁定。這種歸因困境體現為三重斷裂的疊加：

1 深海環境對物理證據的快速侵蝕；

2 演算法推論與法律採證標準之間的落差；

3 數位偽裝對法定紀錄的信用抵銷。

不確定性作為戰略資產

綜合而言，這種結構性的歸因難度，使海底電纜破壞事件往往停留於高度可疑但無法確證(Highly Suspicious yet Legally Unproven)的狀態。在國際政治實務中，公開歸因是一項具備高度政治風險的行為。當證據鏈存在技術漏洞時，受害國若進行指控，可能反遭法律制裁或外交報復。

破壞者正是利用這一點，確保其操作位於證據模糊區內。這種不確定性本身即成為一種戰略資產(Uncertainty as a Strategic Asset)，它有效削弱了國際社會的集體反應能力。只要技術證據在法庭上的採信門檻持續高於破壞者的操作成本，灰色地帶行動便能長期在制度的縫隙中獲得豁免，進而反向強化了這種以錨為武器之行動的可行性。

進一步而言，科技監控面臨著歸因灰色化與意圖黑箱的雙重挑戰。當代的數位監控技術或許能拍到誰在現場(Who)，卻無法判定其行為是否為故意(Why)。破壞者透過 AIS 欺騙(AIS Spoofing)或訊號干擾，在監控畫面上製造出幽靈船或多重虛擬分身，這種數據層面的戰爭(Data-level Warfare)人為地製造了情報的模糊性。對於防禦方而言，即便感測器發出警報，但在法理證據未明、行為意圖尚可否認的情況下，執法者往往難以在第一時間做出具有法律正當性的武力決斷或強制驅離。這種數據上的干擾與法理上的投鼠忌器相互交織，使得防禦方陷入看見了風險，卻無法定義威脅的認知癱瘓。歸因的門檻被刻意抬高，不僅是為了事後逃避法律追責，更是為了在行動當下癱瘓防禦方的反應機制。

4.4 船旗國責任的崩潰：權宜船旗制度下的海上免責區

在 UNCLOS 所建構的海洋秩序中，船旗國專屬管轄(exclusive flag state jurisdiction)原本是維繫公海自由(freedom of the high seas)的核心機制。然而，在灰色地帶行動與海事 - 數位耦合風險的條件下，這一制度逐漸發生功能性異化，它不再只是保障航行自由的

法律安排，而在特定情境下，轉化為規避責任與隱匿行為的制度性屏障(institutional shield for evasion)。

首先，權宜船旗(FOC)制度所帶來的主權商業化(commodification of sovereignty)，構成這一問題的制度根源。FOC 允許船東在與其缺乏實質聯繫(absence of genuine link)的國家註冊船舶，例如巴拿馬、賴比瑞亞與馬紹爾群島等。此一制度在經濟上具有合理性，但其副作用在於將國家主權的一部分轉化為可交易的行政服務。形式上，船旗國仍對其船舶負有確保遵守國際法之義務；但在實務上，部分船旗國的監管能力(regulatory capacity)與執法意願(enforcement will)有限，甚至將低干預(non-intervention)作為吸引註冊的競爭優勢。結果是，管轄權雖存在，卻呈現空殼化(hollow jurisdiction)。

在此基礎上，責任鏈(chain of accountability)進一步發生斷裂。灰色地帶行動中常見的影子船舶(shadow vessels)，其所有權結構往往透過多層離岸空殼公司(offshore shell companies)進行分散，使最終受益人(ultimate beneficial owner, UBO)難以追溯。當此類船舶涉及海底電纜損壞時，受害國即使向船旗國提出調查請求，也可能面臨資訊不完整、行政延宕，甚至無法確認實際控制者的情況。於是出現一種責任在法律上存在，但在實務上無法定位(responsibility without traceability)的典型困境。

更關鍵的是，FOC 體系在灰色地帶條件下，促成了實質控制(effective control)與法律責任(legal responsibility)的雙重分離。幕後的國家或準國家行為者，可以透過第三國船旗運作，將自身從法律責任鏈中抽離。這意味著，受害國在法律程序中，往往必須面對一個形式上中立的船旗國，而非實際發動行動的主體。這種結構性轉移，使責任追究在國際法上變得複雜且高度不對稱。

同時，即便船旗國形式上願意配合，其實際執行能力亦可能不足。部分 FOC 國家缺乏完整的司法資源與跨境執法機制，難以對涉及高階組織或外國情報體系的船員進行有效調查與起訴。在公海或遠洋區域，這種能力落差將進一步放大，使某些海域在功能上接近低執法密度區(low-enforcement density zone)。在這些空間中，行動者得以在極低法律風險下執行高影響力行動。

從制度演化角度來看，船旗國專屬管轄權正經歷一種由權利保障(rights protection)向行為掩護(operational cover)的轉化。原本為防止強權隨意干預商船的法律安排，在灰色地帶行動中，被重新利用為一種移動的法律屏障(mobile legal shield)。只要船舶維持形式上的合法身份，其行為即受到國際法的預設保護，而外部干預則須承擔較高的法律與政治成本。

對防禦方而言，這種制度轉化造成嚴重的行動遲滯(operational hesitation)。即使監控系統已識別出高度可疑的行為模式，沿岸國與其他利害關係國仍須在及時介入與遵守國際法之間進行權衡。過早採取強制措施，可能被指控違反航行自由或干預第三國主權；過晚介入，則可能導致關鍵基礎設施受損。這種結構性兩難，使法律體系在實務上傾向保守，進一步放大灰色地帶行動的操作空間。

因此，所謂船旗國責任的崩潰，並非其法律地位的消失，而是其功能的弱化與轉向。當主權登記制度無法確保實質監管、責任鏈無法追溯、且執法能力存在明顯落差時，海洋空間中將逐漸形成一種準制度性的海上免責區(maritime zone of impunity)。在此區域內，行為者可以在合法外觀與責任缺席之間運作，將低強度行動轉化為高影響力的系統性風險。

這一現象進一步說明，在灰色地帶條件下，問題已不僅是個別違規或事故，而是整體國際海事法架構在面對非對稱威脅時的適應性不足。若船旗國責任無法重新與實質控制與執行能力相連結，則海底基礎設施的保護，將長期暴露於制度性缺口之中。

在界線模糊、法律模糊與意圖模糊的掩護下，現有的海洋治理架構在面對國家指導下的蓄意破壞時，往往缺乏有效的即時招架能力。即便擁有再先進的科技監控，如 DAS 或 AIS 追蹤，監控的本質僅在於觀測而非阻止。當物理破壞在數分鐘內即可完成，而法律定性卻需要數年時間時，無辜的受害方在制度上呈現出近乎單向的脆弱。目前的國際法規與行政措施，在實質功能上更接近於事後悼念(Post-incident Lamentation)而非事前防護(Proactive Defense)。這種體系的失效，迫使我們必須誠實地直面這樣一個殘酷的事實。

因此，正如本章所述，國際海事法體系最大的危機，不在於其被公然違反，而在於其被精確遵守的同時，仍然無法阻止破壞的發生。更深層的問題在於，法律不只是無法阻止風險，而是透過其分類與歸責邏輯，將原本應被視為敵對行為的破壞，轉化為可被吸收的事故類型。在此過程中，規範不再只是治理工具，而逐漸演變為一種風險分配與責任稀釋的制度性機制。

當法律條文本身被轉化為風險生產機制的一部分，且程序正義(Procedural Justice)成為戰略破壞(Strategic Sabotage)的助產士時，我們所處的並非一個法治海洋，而是一個法律化的叢林空間(Legalized Jungle)。這正是當前全球航運秩序面臨重構的最根本誘因。

4.5 法律追責的時間與空間落差

在灰色地帶條件下，法律體系面臨的不僅是權限與證據問題，更是節奏(tempo)與空間(space)兩個維度上的結構性錯位。海底電纜破壞屬於瞬時完成的物理事件，而跨國法律追責則依賴程序、證據與多方協作，其運作本質上是遞進且緩慢的。當即時破壞遇上滯後追責，制度的有效性便在起點上被削弱。

首先，在時間維度上，存在明顯的速率失配(temporal mismatch)。從錨具接觸光纖到數據傳輸中斷，往往僅需數秒至數分鐘；但從事件發生到完成證據保全、確認船舶身分、啟動跨國司法程序，通常需歷經數月甚至數年。這段落差不僅意味著回應延遲，更直接導致證據品質的衰減(evidentiary decay)。海底痕跡迅速消失，船舶操作數據被覆寫，關鍵物證(如受損錨具)可能被拋棄或替換，而涉案船舶亦可在短時間內完成轉籍(reflagging)、更名(renaming)或拆解(scrapping)，於是形成一種當法律行動真正啟動時，物理行為早已結束且難以重建的典型情境。

此外，執法效能面臨著嚴峻的物理時間落差(Physical Temporal Gap)。即便現有的DAS(分散式聲學感測)或衛星監測系統能在毫秒等級偵測到異常拋錨動作，但這種技術上的觀測並不等同於實際的阻止。

在實務佈署中，從監控中心識別風險、通報指揮鏈到派遣海巡艦艇或空中執法單位抵達現場，往往需要數十分鐘甚至數小時的物理航程；然而，破壞一條底棲海纜僅需數分鐘的拖行即可完成。這種監控即時性與執法滯後性的極端不對稱，使得科技手段在灰色地帶行動面前，往往淪為記錄損害的「行車紀錄器」，而非能夠中斷犯罪的防禦盾牌。這種時間上的防禦真空，正是行動者得以反覆實施低成本、高收益破壞的戰略窗口。

灰色地帶行動的目標，往往並非長期佔據，而是短時間內製造數位中斷、金融波動或決策干擾。即使若干年後透過仲裁或訴訟獲得有利判決，對於當時的市場動盪、指揮鏈干擾或社會心理衝擊，法律結果已無法提供等價補償。換言之，法律的時間尺度與戰略效果的時間尺度完全錯位。這種時間落差同時為行動者創造了可被利用的戰略紅利期(window of strategic gain)。

其次，一次拖錨行動可能橫跨多個法律空間，操作發生於甲國專屬經濟區(EEZ)，損害出現在乙國管轄海域，而船舶最終駛入公海或第三國港口。這種地理上的分散，使任何單一國家都難以完整行使執法權，必須依賴跨國合作與司法互助。然而，合作本身受制於政治關係、法律制度差異與程序要求，往往進展緩慢且充滿不確定性。因此，在空間維度上，灰色地帶行動明顯放大了法域的破碎化(jurisdictional fragmentation)。

更複雜的是，現代航運的法律結構本身即高度多層化。船舶可能掛有 A 國船旗，由 B 國船員操作，實際所有權屬於 C 國離岸公司，並在 D 國投保。當事件發生後，受害國需同時面對多個法律體系的證據規則(rules of evidence)、程序門檻(procedural thresholds)與管轄權主張(jurisdictional claims)。在這一過程中，任何一個環節的延誤或拒絕合作，均可能中斷整體追責流程。結果是，空間上的分散性轉化為程序上的阻滯性(procedural inertia)。

在時間與空間雙重落差的交互作用下，一種可被稱為法律疲勞(legal fatigue)的現象逐漸浮現。每一次跨國追責，都需要動員外交、司法、海事與技術鑑識等多重資源；當此類事件以低強度但高頻率的方式反覆發生時，受害國將面臨持續性的資源消耗。長期而言，這種高成本、低確定性的追責機制，可能導致執法意願下降，甚至在策略上選擇不追究(strategic non-pursuit)。

這種狀態對國際秩序具有深遠影響。當破壞成本趨近於可控甚至極低，而追責成本持續攀升且結果不確定時，制度將出現逆向激勵(perverse incentives)。行為者不僅不再畏懼法律制裁，反而可能將其視為可計算的風險成本；而守法一方則因高昂的程序負擔而逐步失去回應能力。於是，法律不僅無法抑制灰色地帶行動，反而在客觀上形成其運作的背景條件。

因此，法律追責的時間與空間落差，不僅是效率問題，更是制度適應性的核心挑戰。只要物理行動的節奏持續快於法律反應，且責任分散於多重法域之中，海底基礎設施的保護便難以從事後補救轉向事前預防。

4.6 法律正當性的結構性崩解：從規範秩序到風險生產機制

現行國際海事法律體系的正當性(legal legitimacy)，長期建立於一種近乎典範性的法理假設，其規則具有可預測性，行為者能在規範邊界內調整行動，而違規行為則可透過證據與責任歸屬機制加以矯正。然而，灰色地帶行動的興起顯示，這套以法律實證主義(legal positivism)為基礎的制度架構，正面臨一種法律並非被違反，而是被精確運用以實現破壞的更深層的危機。

法律之所以具有約束力，正如牛津大學法學教授 H. L. A. Hart 在《法律的概念》一書中的核心觀點，在於行為者對規則採取內在觀點，即將規則視為行動的理由而非外在限制(The internal point of view for Hart is the perspective of those who accept and use the rules of a legal system as standards for their behavior.)。然而，在灰色地帶行動的語境中，這種內在觀點被策略性地顛覆，其行動者並不拒絕規則，而是利用規則的語義空間與

證據門檻，使其行為在形式上符合合法性(legality)，卻在實質上達成敵對效果。於是，法律的遵守(compliance)，與秩序的維持(order preservation)，二者間出現結構性分離。

進一步而言，法律證據體系本身亦呈現出明顯的非對稱性。傳統法律依賴對行為(actus reus)的可觀測性，並假設意圖(mens rea)可透過證據推導。然而，在海事灰色地帶情境中，行為(如拖錨、減速、航跡偏移)高度可見，卻同時具備充分的合理解釋空間；相對地，戰略意圖則隱於不可觀測領域。這種結構導致舉證責任的極端傾斜，其防禦方需證明蓄意破壞，而行動者僅需維持合理否認(plausible deniability)。此種證據不對稱(evidentiary asymmetry)，正如法律現實主義(legal realism)所批判的，揭示了法律運作並非純粹的規範推理，而是深受權力、資訊與制度限制所塑造。

更為根本的問題，則體現在主權原則的功能反轉。政治理論家 Carl Schmitt 在《政治的神學》曾指出主權者乃能決定例外狀態者(The absolutist sovereign did possess the sovereign power to decide on the exception, and was thus capable of authorizing commissars to use dictatorial methods in his name.)。然而，在 UNCLOS 所構築的海洋秩序中，國家卻往往無法在灰色地帶情境中有效宣告或行使此種例外權力。船旗國管轄(flag state jurisdiction)與航行自由(freedom of navigation)原意在於防止權力濫用，但在實踐中卻轉化為對可疑行為的保護機制，使防禦方在法律上陷入無法行動的主權(paralyzed sovereignty)狀態。主權不再是秩序的最終保證，而成為責任逃逸的制度性通道。

在此背景下，哈佛大學法哲學家 Lon L. Fuller 所提出的法律的內在道德(Inner Morality of Law)亦受到挑戰。Fuller 認為，法律必須具備一致性、可理解性與可實現性，方能維持其正當性。然而，當法律規範在灰色地帶行動中無法有效區分合法行為與敵對操作時，其規範功能便逐漸空洞化。法律仍然存在，但其指引行為的能力已顯著削弱，從而導致一種形式存在、實質失效的規範狀態。

綜合而言，當前海事法律體系所面臨的，不僅是執行層面的不足，而是一種法律從風險抑制機制(risk mitigation mechanism)，轉化為風險生產結構(risk-generating structure)的結構性轉變。行動與意圖之間的差距(Act-Intent Gap)降低了行動成本，歸因困境(Attribution Gap)提高了追責成本，FOC 制度切斷責任鏈，而跨法域碎片化則延長了回應時間。這些因素共同構成一種系統性誘因，使灰色地帶行動在理性選擇框架下變得高度可行，甚至具備戰略優勢。

最終，法律正當性的危機並不在於其被違反，而在於其無法再提供有效的行為指引與風險約束。當遵守法律不再等同於維持秩序，當法律程序無法回應即時威脅，國家將不可避免地轉向單邊解釋與非正式機制。此時，國際海洋法秩序將逐漸從一套具實質約束力的規範體系，退化為一種僅具象徵意義的形式性框架。

在灰色地帶行動的邏輯下，國際海事法體系最大的危機，不在於其被破壞，而在於其被遵守的同時，仍然無法阻止破壞的發生。

4.7 戰略滯後與非對稱陷阱：事後救濟的失能機制

在灰色地帶行動的衝擊下，現行法律框架不僅面臨程序上的遲滯，更陷入了深層的戰略滯後(Strategic Lag)。這種滯後並非單純的行政效率問題，而是由損害的非對稱性與決策癱瘓所交織而成的結構性陷阱。

經濟損失的極端非對稱性：賠償與損害的質變

傳統海事法規將海底電纜損害視為一種民事侵權，其救濟核心在於事後賠償。然而，在海事 - 數位耦合的背景下，損害的性質已發生根本性的質變，導致賠償金額與實際戰略損失之間出現了極端的非對稱性。

依據現行《海事賠償責任限制公約》(LLMC)，船東的賠償責任上限通常與船舶噸位掛鉤。對於一艘數千噸的商船而言，其法律賠償額度可能僅限於數百萬美元；然而，若該船舶精確切斷了位於咽喉點的核心電纜，所引發的全球金融結算延遲、跨國通訊中斷乃至供應鏈休克，其社會經濟成本往往以十億美元為計。這種萬倍級的損害差距使事後索賠在戰略上顯得毫無意義。對國家級行動者而言，這類賠償僅被視為極低廉的操作規費，法律不僅無法起到震懾作用，反而因其賠償上限制度，客觀上成了破壞者規避重大損害責任的「避稅天堂」。

決策癱瘓：不確定性作為心理戰武器

比經濟損失更具破壞力的，是灰色地帶行動誘發的政治決策癱瘓(Decision Paralysis)。法律體系對證據確定性的嚴苛要求，在不確定的環境下，反而轉化為限制受害國反擊的枷鎖。

由於前述的歸因灰色化與意圖不可證性，受害國政府在面臨斷線危機時，往往陷入雙重恐懼，一方面擔心在證據不足的情況下發起外交反擊或國際控訴，會導致指控錯誤而引發國際法理上的反噬；另一方面則擔心強力干預會被視為過度反應而引發更大規模的衝突。行動者正是利用這種不確定性，在物理上切斷數據聯繫的同時，在心理上癱瘓了受害國的戰略回擊。這種法律上的投鼠忌器，使得受害國在危機發生的黃金時間內，無法做出具備威懾力的政治決斷。

法律從防禦者轉向旁觀者

綜上所述，現行的事後行政與法律措施，在面對國家指導的蓄意破壞時，已從秩序的維護者退化為災難的記錄者。法律體系未能體認到，當行為者精確地在界線、法律與意圖的模糊地帶運作時，任何無法即時介入的法規都只是無濟於事的事後悼念。無辜的一方若持續寄望於這套滯後的秩序，將在下一波海事灰色地帶衝突中，持續處於有監控卻無招架、有法規卻無正義的結構性劣勢之中。

五、航運體系的連鎖衝擊

一次斷裂，未必只是一條電纜的問題，而是整個系統的延遲與失序。我們正面臨幾百萬美元的民事賠償上限，對照的是數十億美元的國安崩潰極端的非對稱性損失。當戰略破壞被包裝為民事糾紛，法律的震懾功能便徹底瓦解，使局部衝擊能以萬倍級的槓桿，引發全球供應鏈的節奏休克。

5.1 連鎖風險傳導模型

本節所提出的連鎖風險傳導模型，並非單純的因果鏈描述，而是一個強調跨層級耦合(cross-layer coupling)與非線性放大(non-linear amplification)的分析框架。其核心意義在於，灰色地帶行動並不直接攻擊航運體系本身，而是選擇其最脆弱的數位支撐層(digital substrate)，透過間接路徑實現對實體物流的高強度干擾。

第一階段：物理損毀與即時斷裂(Physical Rupture)

在第一階段，物理損毀(physical rupture)發生於海事與數位系統的交會節點。當船舶透過精準拖錨切斷海底光纜時，事件本身在動能上極為有限，但其戰略效果卻取決於該電纜在網絡拓撲中的位置(topological centrality)。若破壞發生於高流量主幹路徑(high-capacity trunk routes)，則其後果不僅是區域性頻寬下降，而可能導致連線重路由(rerouting)失效或網絡擁塞。此時，風險仍停留於基礎設施層，但已具備向上傳導的條件。

第二階段：邏輯層失效與數據中斷(Logical Failure)

進入第二階段，風險開始轉化為邏輯層失效(logical failure)。與傳統通訊中斷不同，現代數位系統高度依賴低延遲(low latency)與即時同步(real-time synchronisation)。當光纖連線中斷或品質下降時，雲端服務、分散式資料庫(distributed databases)與港口操作系統(Terminal Operating System, TOS)將出現同步錯誤(synchronisation errors)或服務降級(service degradation)。船舶交通服務系統(Vessel Traffic Services, VTS)與海關清關平台亦

可能因資料延遲而失去即時性，導致決策資訊的時效性喪失。此階段的關鍵並非完全斷網，而是資訊可靠性(data reliability)與可預測性(predictability)的崩解。

第三階段：港口自動化停擺(Operational Paralysis)

第三階段則標誌著風險由數位層向操作層的反饋(feedback to operations)。現代智慧港口(smart ports)高度依賴自動化設備，如自動導引車(Automated Guided Vehicles, AGV)與遠端操控起重機(remote-controlled cranes)。這些系統需持續接收中央調度指令與即時數據更新，一旦連線延遲或中斷，操作安全性將無法保證。港口管理單位通常被迫降低自動化程度，轉入人工或半自動模式(manual or degraded mode)。然而，這種切換並非無縫，往往伴隨吞吐量急劇下降(throughput collapse)與作業節奏失序(operational desynchronisation)。船舶靠泊計畫(berthing schedule)失準，貨櫃定位錯誤(misallocation)增加，最終導致港口擁塞(port congestion)與錨地壅塞(anchorage buildup)。

第四階段：全球供應鏈休克(Systemic Shock)

當這些影響累積並跨越臨界點(critical threshold)後，系統進入第四階段，即全球供應鏈的結構性震盪(systemic shock)。在高度依賴及時生產(Just-in-Time, JIT)的供應鏈模式下，港口延誤將迅速向上游與下游擴散。製造業因原料延遲而停工，零售端因庫存不足而斷貨，物流成本因不確定性上升而增加。此時，航運市場開始反映風險，運價指數出現劇烈波動，保險市場則重新評估區域風險，將原本屬於戰爭險(war risk)的概念，擴展至涵蓋非傳統基礎設施風險(non-traditional infrastructure risk)的範疇。

值得進一步強調的是，此一傳導鏈具有時間壓縮效應(temporal compression)與空間擴散效應(spatial diffusion)的雙重特性。前者意味著從電纜損毀到港口失效的過程可能在數小時內完成，而後者則意味著其影響範圍可在數日內跨越洲際。這種以極小的物理投入，撬動極大的系統性結果的特性，使灰色地帶行動具備極高的戰略槓桿。

因此，「電纜損毀⇨數據中斷⇨港口停擺⇨供應鏈休克」不應被視為線性事件序列，而應理解為一種多層耦合系統中的動態失穩過程(dynamic systemic destabilisation)。它揭示了一個關鍵事實就是，在當代航運體系中，風險的本質已從「船舶與海況」轉向「數據與連線」。任何忽略此一轉變的安全設計，都將低估灰色地帶行動所帶來的實際衝擊。

5.2 操作層：航運路徑的重新定義

在灰色地帶風險持續升高的背景下，航運操作層正經歷一種結構性轉型，航道，不再只是地理與氣象條件的函數，而逐漸演變為由數位基礎設施風險所共同塑造的管制空間(risk-conditioned maritime space)。

「海纜保護區」擴大與航道物理縮減

首先，海底電纜保護區(Cable Protection Zones, CPZ)的擴張，標誌著航道從開放流動向風險分區(risk zoning)的轉變。原本僅具警示性質的海纜區域，正在逐步制度化為高監控密度與高行為約束的半封閉空間(semi-restricted maritime corridors)。在這些區域內，拋錨(anchoring)、低速漂移(loitering)乃至於不符合預測航跡的機動，都可能觸發監管關注甚至法律風險。其結果是，全球主要咽喉水域中的可自由操作空間(operational white space)被壓縮，航道在功能上變窄，而非在地理上改變。

這種壓縮帶來的第一層效應，是航道擁塞與安全距離的再配置(reconfiguration of safe separation)。當船舶被迫集中於較窄的可通行區域時，傳統依賴距離與時間餘裕(time and distance margin)的操船或避碰策略(COLREGs-based maneuvering)將受到壓縮。在高流量海域，船長可能同時面對兩種互相牴觸的要求，一方面船長需依操船需求與《國際海上避碰規則》(COLREGs)進行即時機動，另一方面又必須避免進入海纜敏感區域。於是，操船需求優先與基礎設施保護(infrastructure protection)之間出現操作張力，並可能在事後轉化為責任認定上的法律爭議。

航運成本的結構性上升

其次，航道重塑不可避免地導致航運成本的結構性上升(structural cost escalation)。當營運商為避免被歸類為高風險航跡(L2 profile)，而選擇採用經認證或低風險的替代航線時，航程延長(route elongation)與燃料消耗增加(bunker consumption increase)成為常態。更重要的是，這種成本不再僅屬於單一航次，而是反映為整體營運模型的改變。航運公司開始將數位風險暴露(digital risk exposure)納入航線規劃演算法，使最佳航線不再是最短距離，而是風險與成本之間的折衷解(risk-cost trade-off equilibrium)。

與此同時，合規成本(compliance cost)亦顯著上升。為避免被誤判為灰色地帶行動者，船東需投資於更高精度的導航與監控系統，例如強 AIS 訊號完整性(AIS integrity assurance)、航跡驗證(track validation)與數據紀錄保存(data logging)。這些措施在技術上提升透明度(transparency)，但在經濟上則增加營運負擔，特別是對中小型航商而言，可能形成進入門檻(barrier to entry)。

緊急拖帶服務(Emergency Towing Vessel, ETV)的戰略化轉型

在此背景下，緊急拖帶服務(Emergency Towing Vessel, ETV)的角色轉型，構成操作層最具戰略意義的變化之一。傳統上，ETV 屬於事後救助資產(post-incident salvage asset)，其任務是在船舶失控後防止擱淺或污染。然而，在錨具武器化(anchor weaponisation)的威脅下，ETV 正逐步被前移至風險鏈的前端，轉化為即時干預與預防性控制工具(pre-emptive intervention asset)。

具體而言，ETV 的部署邏輯從事件觸發(event-driven)轉為風險導向(risk-based deployment)。在高密度海纜區域，ETV 被常態化配置於關鍵節點，一旦監測系統發現船舶失去動力、異常減速或進入漂流狀態，即可在其拋錨之前介入拖帶(preventive towing)。這種能力實質上改變了灰色地帶行動的操作條件，使得原本低成本、低風險的拖錨行為，將面臨更高的被即時阻斷(real-time interdiction)機率。

因此，ETV 不再僅是技術性資產，而是具備戰略外溢效果的安全節點(strategic security node)。其拖力能力(bollard pull)、反應時間(response time)與部署密度，將直接影響一國對數位基礎設施的保護能力。進一步而言，這甚至可能催生新的制度安排，例如將 ETV 部署納入關鍵基礎設施保護(critical infrastructure protection, CIP)體系，或發展數位連通性保障服務(digital connectivity assurance service)等新型態公私協力模式。

航行規則的權衡困境

最後，在操作層面浮現出一個難以迴避的「船隻安全 vs.電纜安全」核心悖論，是船舶自保權(right of self-preservation)與數位基礎設施安全之間的衝突。在極端海況下，拋錨是避免擱淺或碰撞的最後手段，亦是航海實務與法律所承認的正當行為；然而，在海纜密集區域，這一行為可能被重新詮釋為高風險甚至敵對操作。這使船長在瞬時決策中，需同時衡量三種風險，包括：船舶本身的物理安全、對外部基礎設施的潛在損害，以及事後可能承擔的法律責任。

這種多重風險疊加，意味著航運操作已從傳統的航海技術問題(seamanship problem)轉變為一種「法律 - 技術 - 戰略」三位一體的決策問題(tri-layer decision problem)。在此情境下，未來航運體系的安全，不再僅依賴更好的船舶或更精準的導航，而取決於能否在動態風險環境中，建立一套能同時整合操作效率與系統韌性的運行邏輯。

5.3 商業層：保險與成本的範式轉移

若說前兩節所揭示的是物理層與操作層的重構，那麼在商業層面，灰色地帶行動所造成的衝擊，最直接的表現即是風險定價機制(Risk Pricing Mechanism)的改變。保險市場、再保險市場與供應鏈金融體系，原本建立在對風險可分類、可估算與可分攤的

假設之上；然而，當錨具武器化與海底電纜破壞行為同時具備事故外觀與戰略效果時，既有的保險分類與責任分配模式便開始失去穩定性，促使全球海事金融進入一個由戰略不確定性主導的新週期。

戰爭險(War Risk)範疇的模糊化與「數位 - 物理」溢價的常態化

首先，最顯著的變化體現在戰爭險範疇的模糊化與擴張。傳統上，戰爭險主要對應明確的武裝衝突、恐怖攻擊或水雷等高可辨識性風險；但在當前情境下，針對數位基礎設施的物理破壞，雖未必伴隨炮火或正式宣戰，卻足以產生與戰爭行為相當的系統性效果。

在實務中，這導致了《協會網路攻擊排除條款》(Institute Cyber Attack Exclusion Clause CL380)在應用上的範式轉移。過去，CL380 條款主要用於排除軟體層面的邏輯攻擊，但保險人現在被迫重新思考敵對行為(Hostile Act)的定義，並逐步將這類針對海底電纜或關鍵數據通道的物理干預，納入戰爭險或特殊附加險(Additional Premium Cover)的評估範圍。

這意味著，全球航線開始出現一種新的數位地緣保費(Digital-geostrategic Premium)，使得船舶航行的成本結構發生了本質性的翻轉，成本不再僅取決於海面上的風浪或海盜威脅，也取決於海床下方數位設施的戰略敏感度。當船舶進入高密度海纜區時，保險費率將不再與船舶噸位成正比，而是與其行為可能誘發的數位系統風險(Systemic Risk)掛鉤。

保險排除條款對「影子船隊」的絞殺機制與契約約束

其次，保險排除條款(Exclusion Clauses)的演變，正在對影子船隊(Shadow Fleet)形成一種比國際法更即時、更具經濟威懾力的市場性約束。由於灰色地帶行動高度依賴 AIS 操控、船旗不透明與所有權鏈條模糊，保險市場開始透過契約邏輯主動壓縮其生存空間。

最具代表性的實務趨勢，是倫敦保險市場協會(Lloyd's Market Association, LMA)與國際承保人協會(International Underwriting Association, IUA)聯合成立的聯合戰爭委員會(Joint War Committee, JWC)與各保賠協會(P&I Clubs)對 AIS 完整性義務的強化。契約中明確規定，若船舶在無正當理由(如避開海盜)下執行 AIS 黑暗行動(AIS Dark Activity)，將被視為實質性的風險顯著加重(Material Aggravation of Risk)。一旦船舶在此狀態下涉及海底電纜損害，保險人得引用 AIS 斷線即失效原則主張免責(Coverage Denial)。

此舉的實質意義在於，保險市場並不直接處理國際法上的船旗國責任崩潰問題，而是透過商業制裁(Commercial Sanction)，對低透明度船籍施加特殊保證條款(Special Warranties)。當影子船隻因不可保(Uninsurable)而無法獲得一線港口准入或貿易融資時，這種市場擠壓效應將迫使影子船隊在數位隱身與商業存續之間做出代價高昂的選擇。

賠償代差與責任限額的體系重構

然而，這樣的市場反應也引出了另一項更深層的法律問題，即海底電纜損害與次生經濟衝擊，已遠超過傳統海事責任限制(Limitation of Liability)所能吸收的範圍。

依現行《海事賠償責任限制公約》(LLMC)，船東的賠償額度多以船舶噸位計，這在處理傳統船舶碰撞時尚稱妥適。但在海事 - 數位耦合風險下，一條核心電纜在戰略節點被切斷，所引發的全球金融結算延遲與供應鏈休克，損失可能高達數十億美元。這種明顯的賠償代差(Compensation Gap)，使得法律上可求償的責任額度，與現實中產生的社會成本之間存在巨大落差。正因如此，航運保險的邏輯正從保護船舶實體(Protecting the Vessel)轉向保護航運環境中的數位資產(Protecting Digital Assets)。這將引發一場保險範式的革命，很顯然的，未來高風險海域的通行權，可能必須以購買額外的基礎設施第三方責任險為前提，從而將航運責任從單純的航行安全，提升至維護數位文明運作的高度。

供應鏈金融的風險重新定價與連鎖反應

最後，這種保險結構的轉變會進一步向供應鏈金融(Supply Chain Finance)傳導。銀行與貿易融資機構在評估信用狀(L/C)與貨運融資時，已開始將航線的數位安全評級(Digital Security Rating)納入隱含變數。

當金融機構察覺到某條航線穿越頻繁發生 L3 或 L4 等級事件的海域時，不僅保費會上升，融資成本亦會隨之波動。其結果是，數位基礎設施風險不僅重塑了保險市場，也從金融底層重新塑造了全球貿易與貨物流向。這意味著，市場正先於法律以價格、排除條款與信用條件作出回應，逐步成為界定灰色地帶行為邊界的重要治理力量。

5.4 戰略層：航運業的國安化轉向

從物流中介到主權韌性節點

首先，航運業從物流中介(logistics intermediary)轉向主權韌性節點(sovereign resilience node)，本質上是一種功能定位的重新編碼(functional re-coding)。在傳統全球

化架構中，航運公司之所以能維持中立，是因為其活動被視為純粹的經濟交換媒介；然而，在錨具武器化與海底電纜戰略化之後，航運行為開始直接影響國家資訊主權(digital sovereignty)與經濟穩定性(economic stability)。因此，航運企業不再只是承載貨物流動，而是嵌入於國家安全結構中的運作節點(embedded node within national security architecture)。這種轉變意味著，航線規劃、錨地選擇與操作決策，已從技術性選擇轉化為具有戰略外溢效果的行為。

在此基礎上，數據共享機制的擴張，使航運公司逐步承擔準情報角色(quasi-intelligence function)。AIS 數據、船舶感測器紀錄與現場觀測報告，實際上構成了一種分散式監測網絡(distributed sensing network)。與傳統由國家單一掌控的情報體系不同，這種網絡的優勢在於其廣泛覆蓋與即時性，但同時也帶來治理上的新問題，究竟企業所掌握的數據在何種條件下應共享？其準確性與法律地位應如何界定？一旦企業提供的數據被用於指控特定行為者，企業本身是否會被捲入地緣政治衝突？這些問題顯示，航運業的國安化不僅是功能擴張，更是責任與風險的同步外溢。

航運供應鏈的「陣營化」與「認證化」

進一步而言，航運供應鏈的陣營化(bloc formation)與認證化(certification)現象，標誌著全球航運市場從效率導向(efficiency-driven market)轉向信任導向(trust-mediated system)。在灰色地帶風險無法透過法律完全約束的情況下，市場開始自發建立信任溢價(trust premium)機制。所謂數位安全航道(digitally secured corridors)的出現，本質上是一種結合國家監控能力與企業合規性的混合治理模式(hybrid governance model)。這些航道並非單純的地理路徑，而是經過安全認證(security accreditation)、數據透明度(data transparency)與風險評級(risk rating)篩選後的制度化通道(institutionalized corridors)。

然而，這種機制同時帶來排他性(exclusivity)。低透明度船舶、影子船隊(shadow fleet)或與特定政治風險相關的船東，將逐步被排除於主流航運網絡之外。這不僅改變了競爭條件，也可能導致航運體系的結構性分裂(structural fragmentation)。換言之，全球航運市場正在從單一體系演化為多個相互競逐的安全陣營，其運作邏輯更接近於國際政治中的同盟體系，而非自由市場。

企業韌性與國家戰略的深度對齊

在企業治理層面，大型航運與港口集團開始聘用具備網路安全與地緣政治背景的專業人員進入決策層，將地緣政治合規列為年度風險評估的首要指標。這種將國安專業進入決策核心具有關鍵意義。這不僅是人事安排的改變，而是決策理性(decision rationality)的轉型。當董事會開始納入地緣政治風險(geopolitical risk)、網路安全

(cybersecurity)與數位基礎設施保護(critical infrastructure protection)等議題時，企業的戰略目標將不再僅限於利潤最大化(profit maximisation)，而是轉向風險最小化與存續能力(resilience and survivability)的優化。這使航運公司在某種程度上具備準國家行為者(quasi-state actor)的特徵，其決策將同時受到市場與安全邏輯的雙重約束。

此外，公私協作模式(Public-Private Partnership, PPP)的重構，進一步鞏固了這一轉向。傳統的 PPP 多集中於基礎設施建設或營運；但在當前情境下，其重心轉向即時安全協作(real-time security coordination)。國家透過衛星監控(satellite surveillance)、訊號情報(signals intelligence)與海上巡邏能力，提供風險識別與預警；企業則以航跡透明度(operational transparency)與即時回報作為交換。這種互補關係形成了一種新型安全共生結構(security symbiosis)，國家，依賴企業的分散式觀測能力；而企業，則依賴國家的強制力與資源保護其營運環境。

綜合而言，航運國安化並非單一政策或短期現象，而是全球海洋治理邏輯的深層轉型。當航運公司被重新定位為基礎設施保衛者(infrastructure guardian)時，其所承擔的不僅是營運責任，更是一種維繫數位文明運作的結構性角色。這一轉變的核心意義在於，全球航運秩序正從以自由流動為核心的開放體系，轉向以安全、信任與韌性為基礎的分層體系(layered and security-oriented order)。在此新秩序中，效率仍然重要，但已不再是唯一標準；能否在不確定與高風險環境中維持穩定運作，才成為決定航運企業與國家競爭力的關鍵。

六、航運治理的多層轉型

韌性不再只是承受風險，而是提前辨識風險、限制風險、轉化風險。我們必須從事後救濟轉向事前防護，拆解那些保護惡意的法律護盾。透過技術、法律與市場的深度耦合，建立一套有刺的韌性，讓監測延伸至海床，讓市場成為執法工具，使破壞者在切斷數據的同時，也切斷自己的生存命脈。

6.1 技術韌性：深海監測自動化

在前述分析中可以看出，海事 - 數位耦合風險並非源於單一脆弱點，而是來自不同層級之間的連鎖傳導。因此，本章所提出的韌性重構，並不建立於任何單一技術或制度的強化，而在於跨層級的整合能力。系統韌性的核心，不在於某一環節的防禦強度，而在於感測(sensing)、應變(response)與治理(governance)三者之間是否能形成同步且無縫的協同機制。

換言之，在高摩擦海洋環境下，韌性不再只是承受衝擊，而是能否在風險跨越物理與數位邊界之前，即時識別其徵兆、快速介入其演變，並透過制度性機制將局部事件限制於可控範圍之內。唯有在此種跨層整合架構下，灰色地帶行動所依賴的非對稱優勢才可能被有效削弱。

在海事 - 數位耦合風險已具系統性特徵的情況下，單一監測工具已無法應對灰色地帶行動所依賴的隱蔽性與可否認性。本研究因此主張建構一套由海床延伸至太空的海床到衛星(Seabed-to-Satellite)立體感知體系，其本質並非單一技術突破，而是一種跨域整合的感知與反應架構(integrated sensing-response architecture)。在此架構中，深海不再是不可視的盲區，而成為可持續觀測與即時干預的運作空間。

分散式聲學感測(Distributed Acoustic Sensing, DAS)

首先，分散式聲學感測(Distributed Acoustic Sensing, DAS)的戰略價值，在於其對可否認性(plausible deniability)的根本削弱。透過將雷射訊號注入既有光纖，並分析背向散射(backscatter)所反映的微小變化，DAS 能將原本被動的通訊電纜轉化為主動感測系統。其關鍵並不僅在於可偵測振動，而在於能夠建立行為特徵譜(behavioral signature spectrum)，使得拖錨、拋錨、船舶推進器運轉，乃至於不同噸位船隻的水動力特徵，都可被轉譯為可辨識的訊號模式。

在灰色地帶環境中，這意味著一項質變，行為者即便關閉 AIS (Automatic Identification System)或進行訊號欺騙(AIS spoofing)，仍無法規避來自物理層的持續觀測。換言之，DAS 並非單純提升監測能力，而是將防禦從依賴行為者自我揭露(self-reporting systems)轉向不可規避的物理感知(non-bypassable physical sensing)。

水下無人機(UUV)與常態化巡航

然而，感測本身並不足以形成完整防禦。水下無人載具(Unmanned Underwater Vehicles, UUV)與自主水下載具(Autonomous Underwater Vehicles, AUV)的引入，使系統具備從感知(sensing)到行動(actuation)的閉環能力。當 DAS 系統標記出異常點後，UUV 可在極短時間內抵達現場，執行高解析影像紀錄(high-resolution imaging)、結構檢測與環境取樣。這種能力的關鍵，在於其時間壓縮(temporal compression)效應，這使得可以在行為船舶尚未離開現場前，即完成證據採集。

這對灰色地帶行動構成根本性挑戰。其運作邏輯原本依賴時間差(time lag)與證據消散(evidence dissipation)；但當取證能力前移至事件發生當下，事後否認(post hoc

denial)的空間將大幅縮減。從這個角度看，UUV 並非單純的維修或巡檢工具，而是歸因能力(attribution capability)的物理載體。

AI 驅動的行為預測模型(Behavioral Analytics)

進一步而言，AI 驅動的行為分析(behavioral analytics)則構成整個體系的預測層(predictive layer)。透過整合歷史 AIS 軌跡、氣象數據、船舶性能參數與 DAS 訊號資料，機器學習模型可建立正常航行行為基準(baseline behavior)與異常偏離模式(anomalous deviation patterns)。當特定船舶在敏感區域出現不符合統計分佈的低速漂移、橫向位移或停滯行為時，系統可在尚未發生實質損害前觸發預警。

此一能力的戰略意義，在於將防禦從事件回應(incident response)推進至風險預判(risk anticipation)。結合緊急拖帶船(Emergency Towing Vessel, ETV)或海巡力量的部署，異常行為可在進入高風險狀態前即被干預，形成一種動態風險抑制機制(dynamic risk suppression mechanism)。

當 DAS、UUV 與 AI 分析進一步與衛星合成孔徑雷達(Synthetic Aperture Radar, SAR)、光學遙測與 AIS 數據融合(data fusion)時，一個多層次的海洋態勢感知(Maritime Domain Awareness, MDA)體系將逐步成形。此體系的核心不在於單一數據來源的準確性，而在於跨來源交叉驗證(cross-domain validation)的能力。AIS 可被關閉或偽造，但無法同時操控海床振動、衛星影像與水下觀測結果。

最終，技術韌性的真正意義，不僅在於防護能力的提升，而在於建立一種可見性即秩序(visibility as order)的治理邏輯。當海底活動從不可見轉為持續可觀測時，灰色地帶行動所依賴的模糊性與不確定性將被系統性壓縮。這種轉變不需要完全消除威脅，而是透過提高被偵測與被歸因的機率，改變行為者的成本 - 收益計算(cost-benefit calculus)。

因此，深海監測自動化不僅是技術升級，而是一種以技術作為秩序擔保(technology as guarantor of order)的治理轉型。當隱蔽不再是可行選項，灰色地帶行動的戰略優勢將逐步瓦解，而全球航運與數位體系的韌性，亦將在這種可觀測性之上獲得新的基礎。

6.2 操作韌性：動態防護與應變

在海事 - 數位耦合風險已具備即時傳導特性的情境下，操作韌性的核心不再是單點防護，而是建立一套能夠「即時感知、即時決策、即時調整」(sense-decide-act)的動態防護體系。

即時避讓與預警系統(Real-time Avoidance & Early Warning)

首先，即時避讓與預警系統(Real-time Avoidance & Early Warning)的本質，是將航運體系從被動接受風險轉化為主動管理風險。為化解 3.1 節所揭示的數位與航運共用通道(shared maritime-digital corridors)問題，必須建立一套結合地理圍欄(geofencing)、行為監測與即時通訊的協同系統。

在此架構下，核心電纜區域不再只是地圖上的靜態標示，而成為具備動態警戒能力的智慧區域(intelligent zones)。當船舶進入這些區域時，其航速、航向與操作行為將被持續分析；一旦出現異常減速、非必要漂移或疑似拋錨前動作，系統即可透過數位航行警告(NAVTEX)、Satellite AIS 或船橋整合系統(bridge integration systems)即時發送警報。這種警報不僅是提示，更因為它使船舶的操作進入被觀測狀態(observed state)，讓船舶更具有行為約束效果。

更具戰略意義的是雙向透明化預警(bidirectional transparency)。當 DAS (Distributed Acoustic Sensing)偵測到海床異常振動時，資訊不僅回傳至監管機構，也同步推送給周邊商船。這種分散式見證(distributed witnessing)機制，實質上將海上監控從單一執法體系擴展為多節點網絡，使影子船隊難以在低可見度環境中操作。當任何可疑行為都可能被多方觀測與記錄，其可否認性(plausible deniability)將被系統性侵蝕。

其次，針對 3.2 節所揭示的多點失效(multi-point failure)與數位孤島風險，操作韌性的關鍵在於建立非線性通訊備援(non-linear communication redundancy)。傳統備援多依賴海纜之間的重新路由(rerouting)，但在灰色地帶行動中，行為者往往針對平行電纜進行同步干擾，使此一機制失效。因此，必須引入跨媒介(cross-medium)的備援架構。

衛星與海纜的多路徑備援(Satellite-Cable Hybrid Redundancy)

低軌衛星(Low Earth Orbit, LEO)通訊在此扮演關鍵角色。透過預先建立海纜 - 衛星自動切換協議(cable-to-satellite failover protocol)，關鍵數據流(如港口調度、金融結算與政府指揮)可在海纜中斷時，於極短時間內轉移至衛星網絡。儘管衛星頻寬與延遲無法完全匹配光纖，但其價值不在於維持最佳效能，而在於確保最低可運作能力(minimum viable operation)的持續。

在此基礎上，戰略韌性容量(strategic resilience capacity)的概念亦逐漸浮現。要求電信與航運樞紐保留一定比例的非海纜通訊能力(例如 20%備援容量)，不僅是技術設計問題，更是政策與監管選擇。這種容量預留，實質上是將效率的一部分轉換為韌性，是從最佳化(optimisation)走向穩定化(stabilisation)的典型表現。

港口運作的「離線韌性」與自動化容錯

港口運作的韌性，決定了連鎖風險是否會從數位層擴散至實體供應鏈。為中斷 5.1 節所描述的系統性崩潰鏈，現代港口必須發展離線運作能力(offline operability)。

這意味著智慧港口的自動化系統需從高度集中式(centralized control)轉向分散式控制(distributed control architecture)。例如，自動導引車(AGV)與碼頭起重機應具備本地決策能力(local decision-making capability)，能在與外部網絡斷聯時，依據預先下載的作業邏輯維持基本操作。這種設計並非追求完全自治，而是確保在通訊中斷時不會出現全域停擺(total system halt)。

此外，定期進行數位全斷演習(digital blackout drills)亦成為操作韌性的必要組成。透過模擬海纜斷裂、衛星受限與數據延遲等複合情境，航運公司與港口管理單位可驗證備援系統的實際效能，並調整應變流程。這種演習的價值，在於將原本抽象的風險轉化為具體的操作經驗，降低在真實事件中出現決策遲滯(decision latency)的可能性。

修復與護航應變資源的戰略布局

最後，應變資源的戰略布局，將決定整體防護體系的回復速度(recovery velocity)。與 4.5 節所指出的法律追責滯後性相對應，操作層面必須強化即時修復與預防性部署能力。

1. 在修復端，建立海事預備役(maritime reserve)機制，可將具備深海作業能力的工程船與專業人員納入快速動員體系，並透過制度設計簡化其進入敏感海域的行政程序。這不僅縮短修復時間，也降低自理(autonomy)所造成的長期影響。

2. 在預防端，聯合巡邏(joint patrol)與前置部署的緊急拖帶船(Emergency Towing Vessel, ETV)，則構成一種可見防護(visible protection)機制。當高風險海域具備持續的巡邏與即時拖帶能力時，即便船舶因機械故障進入漂流狀態，也可在拋錨前被控制，避免其成為無意或刻意的破壞載體。

綜合而言，操作韌性的本質在於建立一種不中斷的調整能力(continuous adaptability)，當風險發生時，航運體系不需完全避免衝擊，而是能在衝擊中維持運作並迅速重組。這標誌著一項從傳統的穩定即安全(stability equals safety)，走向可調適即安全(adaptability equals security)的關鍵轉變。在灰色地帶行動成為常態的未來，唯有具備動態防護與即時應變能力的航運體系，方能在不確定中維持流動。

6.3 制度韌性：國際協作的新模式

在灰色地帶行動的條件下，單一國家的技術升級與執法強化，雖能局部提升防護能力，卻無法從根本上解決問題。原因在於，海底電纜風險本質上是一種跨主權(trans-sovereign)、跨產業(cross-sectoral)與跨層級(cross-layer)的威脅，其行為發生於某一海域，證據分散於多個國家與企業手中，影響卻可能沿著全球數位與航運網絡迅速擴散。正因如此，制度韌性的核心，不在於單一國家擁有多強的控制力，而在於國際協作是否能建立一套速度足夠快、資訊足夠通、責任足夠明確的新型治理架構。

建立「全球海事－數位情資共享平台」(Maritime-Digital Intelligence Hub)

首先，最迫切的制度創新，是建立一個真正跨國運作的全球海事 - 數位情資共享平台(Maritime-Digital Intelligence Hub)。如 4.3 節所指出，歸因困境之所以難解，並不只是因為深海取證困難，而是因為證據總是分散於不同主體，例如：AIS 軌跡資料掌握在航運與海事監管機構手中，衛星 SAR (Synthetic Aperture Radar)影像可能由國家安全或商業遙測公司持有，而 DAS (Distributed Acoustic Sensing)與電纜故障資料則多屬於電信業者或電纜聯盟。若這些資訊不能在同一平台上被即時整合，灰色地帶行動者便能持續利用資訊碎片化(information fragmentation)作為掩護。

因此，所謂情資共享平台，其核心不僅是資料匯集，而是建立一套可即時交叉驗證(real-time cross-validation)的制度。當某一海域出現異常聲學擾動、電纜延遲突升或通訊中斷時，平台應能在最短時間內整合鄰近海域的 AIS 記錄、衛星雷達影像與歷史航跡模式，進行數位回溯(digital backtracking)，藉此縮短歸因時間並降低證據流失風險。換言之，制度韌性的首要前提，不是更多數據，而是讓數據能以跨國界、跨部門的方式流動起來。

在此基礎上，預警白名單(trusted operator whitelist)與聯合觀察名單(joint watchlist)機制，則是將制度韌性進一步轉化為風險分級治理(risk-tiered governance)的關鍵工具。長期以來，國際航運體系建立在形式平等的原則上，即船舶只要符合基本法定要求，即可在全球市場中運作。然而，在灰色地帶風險持續升高的背景下，這種一體適用的中性規則，已難以反映不同船舶之間在透明度、合規程度與風險行為上的實質差異。

因此，未來更可行的做法，是透過跨國平台與保險、港口國管制(Port State Control, PSC)及安全機構協作，建立一套以透明度與可信度為基礎的分級制度。對信譽良好、數據透明、長期配合安全要求的航運公司與船舶，可賦予較高程度的信任與快速通行待遇；相對地，對頻繁更名(renaming)、轉籍(reflagging)、掛權宜船旗(Flags of Convenience, FOC)且存在 AIS 異常紀錄的船舶，則納入聯合觀察名單，進行更高強度的跨國監控。這實際上意味著，全球航運治理將從形式中立逐步轉向基於風險與透明度的差異化治理。

推動「海底電纜保護區」(CPZ)的國際法地位更新

其次，若要真正壓縮灰色地帶行動的操作空間，僅有情資共享仍嫌不足，還必須推動海底電纜保護區(Cable Protection Zones, CPZ)的國際法地位更新。目前多數 CPZ 主要來自各國國內法或行政規則，雖可在本國法域內發揮一定效果，但欠缺足夠的國際強制力。一旦船舶主張其行為僅屬正常航行、無害通過(innocent passage)或 EEZ 內的航行自由，沿海國的干預空間便立刻受限。這意味著，在現行體系下，CPZ 更像是被建議尊重的區域，而非真正具有制度牙齒(legal teeth)的安全區。

若從制度韌性的角度出發，下一步應是在 IMO 框架或透過 UNCLOS 的補充協議中，逐步提高 CPZ 的法律層級，使其不再只是國內行政管制區，而成為具備某種程度國際可承認性的敏感海域。這將牽動一項更根本的法律調整，即重新界定無害通過(innocent passage)在數位時代的內涵。當船舶在 CPZ 內無正當理由地拋錨、低速漂移、關閉 AIS 或從事異常操作時，其行為是否仍屬無害？若答案是否定的，則沿海國是否應獲得某種有限的預防性攔截權(preemptive interdiction)？這將是未來海洋法改革中最具爭議、但也最不可迴避的問題之一。

進一步而言，針對高風險海域，制度韌性還應體現為共同維修與護航協議(joint repair and escort mechanism)的建立。紅海案例已說明，海纜風險不只來自蓄意破壞，也來自衝突外溢下的沉船殘骸與漂移錨具；台灣海峽與印太情境則顯示，一旦地緣政治緊張升高，維修船能否安全進入現場、修復能否在短時間內完成，將直接決定一個區域是否進入長期性的數位孤島化(digital islanding)。在此情境下，單一國家的維修能力不足以應對高壓風險，必須透過多國聯合的護航、伴航與快速維修安排，為海底基礎設施建立某種類似亞丁灣反海盜合作模式的國際公共安全機制。

建立「跨國責任溯源」與「金融制裁」連動機制

此外，考量到 4.5 節所述法律追責的時間滯後性，制度韌性還必須延伸至跨國責任溯源(cross-border liability tracing)與金融制裁連動(sanctions linkage)機制。當法律程序需

要多年才能完成時，單靠傳統司法追責已難形成即時威懾。更有效率的做法，是將歸因結果迅速轉化為市場與金融後果。一旦某一船舶被多國平台與技術證據認定涉及 L3 或 L4 級破壞，其船舶本身、相關空殼公司(shell companies)與關聯船隊，應能被主要港口、保險機構與融資銀行同步列入限制名單。如此一來，法律責任仍可繼續追究，但在法律結果出現之前，行為者已先承受來自全球港口准入、保險承保與資金流動的實質壓力。

與此相配套的，則是建立一種國際性的海纜保險共同分擔機制(subsea cable insurance pool)或修復基金機制。當歸因已達高度可能性，但船旗國怠於作為或實際賠償遙遙無期時，應由該基金先行支付修復費用與部分經濟損失，再由國際組織、保險聯盟或多國機制代位追償。這種安排的重點不僅在於減少修復延遲，更在於避免受害方因高昂成本而被迫放棄追責，從而落入法律疲勞(legal fatigue)陷阱。

綜合而言，制度韌性的重構，並不是要否定海洋自由(freedom of the seas)的傳統原則，而是要將其從一種近乎無條件的放任自由，重新轉化為負責任的海洋連結(responsible maritime connectivity)。這意味著未來的海洋治理，不再只是保障任何船舶都能自由航行，而是要求這種自由必須建立於透明度(transparency)、可追責性(accountability)與共同風險承擔(shared risk responsibility)之上。唯有當國際協作的速度超過灰色地帶行動的破壞速度，當資訊整合的效率高於行為者製造模糊的能力，全球航運與數位秩序的韌性，才可能真正建立。

6.4 航運業策略建議：對策矩陣

此一分層對策矩陣(Layered Response Matrix)的核心邏輯，在於將風險依其時間維度與影響層級，區分為預防性準備(proactive)、即時反應(reactive)與戰略韌性(strategic)三個階段；並進一步依據航運體系中的三大關鍵角色，船東與營運商、港口管理機構以及政府監管部門，分配具體責任。透過這種設計，原本分散的安全行為被重新整合為一套具有內在邏輯的協同行動系統。

利益相關者	預防性準備(Proactive)	即時反應(Reactive)	戰略韌性(Strategic)
船東與營運商	建立數位航跡透明化(Trace Transparency)認證；部署防竄改 AIS 與錨具監測系統	接收異常警報後即時避讓並切換衛星備援通訊	納入 ESG 與國安揭露；加入安全航運聯盟
港口管理局	建立離線運作協議；部署 DAS 與登陸站監測整合	啟動降級運作模式並調整靠泊與引水優先序	投資數位－實體雙備援；與國安單位數據直連
政府監管部門	劃設動態海纜保護區(DCPZ)；建立跨國數據共享平台	派遣 ETV 預防性拖帶並啟動聯合歸因	推動國際法修正與黑名單/金融制裁機制

針對船東：從「合規」到「防禦性營運」

在傳統海事治理中，船東的責任多集中於遵循既有規範(compliance)。然而，在灰色地帶風險環境下，僅僅沒有違規已不足以保護自身。更關鍵的是能否證明自身行為不具敵對意圖，即建立一種可驗證防禦(verifiable defense)能力。

這意味著，船舶操作數據本身將從內部管理工具，轉變為法律與保險體系中的核心證據。例如，錨具操作的時間序列、張力變化與海床接觸紀錄，不再只是技術參數，而是未來界定過失與蓄意的關鍵依據。透過這種數據化透明機制，船東不僅降低被誤判為灰色地帶行為者的風險，也在制度層面重新界定自身的責任邊界。

此外，通訊備援的投資亦需被重新理解。低軌衛星(LEO)系統的導入，不僅是維持通訊的技術選擇，更是確保在數位斷裂情境下，船舶指揮鏈(command chain)與決策能力不致崩潰的關鍵條件。

針對港口：轉化為「數位安全前哨」

港口在整個風險傳導鏈中，扮演著從數位中斷轉化為實體衝擊的關鍵節點。因此，其角色必須從傳統的物流中樞，轉型為具備防護與緩衝能力的數位安全前哨(digital security outpost)。

這種轉型的核心，在於建立離線可運作性(offline operability)。當外部海纜中斷時，港口不應立即陷入全面停擺，而應具備在有限資訊條件下持續運作的能力。這要求其自動化系統具備本地決策邏輯與資料快取機制，使關鍵作業(如裝卸與場內調度)能在與外部網路斷聯的情況下維持基本功能。

更進一步，港口也應融入區域風險監控網絡。透過與海纜登陸站與國家安全單位的數據連結，港口可在船舶進出之前即識別潛在風險，並在必要時採取留置檢查或優先調度等措施，將風險隔離於節點之外。

針對政府：法律武器化與國際博弈

在整體對策矩陣中，政府的角色具有結構性意義。面對灰色地帶行動對既有國際法體系的侵蝕，政府已不僅是規則的執行者，更是規則的重塑者(rule rewriter)。

1. 在空間治理上，動態海纜保護區(Dynamic CPZ)的概念代表著一種新的管制邏輯。與其依賴靜態劃設，不如透過即時數據與風險評估，動態調整敏感區域

的範圍與管制強度，提升制度的靈活性與回應速度。

2. 在制度工具上，金融與保險機制將成為最具實效的約束手段。相較於軍事介入的高政治成本，透過保險拒保(denial of insurance)、港口禁入(port denial)與融資限制(financing restriction)所形成的市場壓力，更能有效將高風險船隻排除於關鍵航運網絡之外。這種經濟型威懾(economic deterrence)實際上構成了一種非軍事形式的封鎖機制。

綜合而言，本對策矩陣所揭示的，不僅是航運業應如何應對新型風險，更是一種治理邏輯的轉變。過去的全球航運體系建立在低摩擦(low-friction)與高效率的原則之上，但在灰色地帶行動常態化的背景下，這種模式已逐漸暴露其脆弱性。

未來的核心，不在於消除所有風險，而在於確保系統在風險中仍能運作並迅速調整。這意味著航運體系必須從自由流動(free flow)轉向可控流動(controlled resilience)，並將透明度、可驗證性與跨域協作，納入其基本運作邏輯之中。

當船東、港口與政府能在同一套風險框架下形成協同關係時，灰色地帶行動所依賴的模糊空間將被逐步壓縮，而全球航運與數位秩序的韌性，也將在這種新的治理架構中重新被建構。

6.5 IMO 的角色重塑

若說前述技術韌性、操作韌性與制度韌性，分別回應了如何看見風險、如何承受風險與如何協同風險，那麼本節所處理的問題則更進一步的探討，誰有權將這些分散的防護措施，上升為全球一致的強制規範。在現行多邊制度架構中，最具正當性與可操作性的機構，仍然是國際海事組織(IMO)。這不只是因為 IMO 長期主導國際航運安全、海洋環境保護與船舶合規制度，更因其本身就具備將技術性風險轉化為強制性國際義務的規範傳統。SOLAS、MARPOL、ISPS Code、Polar Code 乃至 Member State Audit Scheme 的制度演進，都說明 IMO 並非只能發出建議，而是能在條件成熟時，把新型風險納入全球強制框架。

正因如此，IMO 應啟動制定一部暫可稱為《海底基礎設施保護國際章程》(International Code for the Protection of Subsea Infrastructure, ICPSI)的新型規範文件，並將其定位為國際海事秩序中繼航行安全(safety)與海洋環境保護(environmental protection)之後的第三支柱。這樣的倡議，並不是要把 IMO 轉變為軍事安全機構，而是要承認一個二十一世紀的基本事實，海洋，已不再只是船舶與貨物流動的表面空間，而是同時承載數據、金融、通訊與國家韌性的立體基礎設施空間。在這種情況下，若國際規範

仍僅將海底電纜視為附屬設施，而不把它納入核心治理視野，現行制度便會持續落後於風險本身。

從規範路徑來看，ICPSI 最可行的方式不是另起爐灶，而是先由指南(guidelines)走向強制章程(mandatory code)。這條路徑較符合 IMO 的制度風格。事實上，IMO 目前已有若干相鄰制度可作為前導，例如針對 Places of Refuge 與 Maritime Assistance Services(MAS)的安排，本質上就是在處理高風險船舶、沿岸國干預與多方協調之間的平衡。這些既有制度雖非為灰色地帶行動設計，但它們提供了一個重要啟示，說明IMO已經具備處理船舶行為可能對公共利益造成重大外溢風險的規範經驗。未來若要推進ICPSI，完全可以從現有的風險通報、臨時干預、協同應變與資料交換邏輯出發，逐步擴展至海底基礎設施保護。

若從實質內容推想，ICPSI 至少應包含四個核心模組。

1 敏感海域操作規範(navigation rules for sensitive subsea corridors)：目前 SOLAS 已要求一定噸位以上國際航行船舶配備電子海圖顯示與資訊系統(ECDIS)，這為未來強制納入「海底基礎設施圖層(subsea infrastructure layer)」提供了技術基礎。若透過 SOLAS Chapter V 或相關性能標準修正，要求船舶在進入高風險海纜區時，必須由 ECDIS 即時顯示電纜敏感區、限制錨泊區與維修區資訊，將可把原本事後辯解的「不知道」大幅壓縮。

2 數位身份與 AIS 完整性合規(AIS integrity and digital identity compliance)：這點非常重要，而且具有現實可行性。IMO 現行制度並未建立一個專門針對 AIS 欺騙(AIS spoofing)、無故長時間斷訊(unjustified AIS dark activity)或數位身份異常的全球強制標籤機制。未來若要真正壓縮灰色地帶行動的操作空間，就應考慮比照 ISPS Code 的安全邏輯，建立某種高風險船舶數位合規分類(digital compliance classification)制度。這不一定要一開始就成為刑罰工具，但至少可以作為港口國監督(Port State Control, PSC)、保險承保與航道通行風險分級的依據。換言之，AIS 完整性不應再只是技術問題，而應成為國際航運信用的一部分。

3 船舶數據記錄與歸因能力強化(enhanced recordkeeping and attribution support)：現有 VDR 制度主要是為事故調查與航行重建而設，且 ECDIS 畫面已可納入 VDR 記錄。這為未來擴充記錄範圍提供了一個現成制度基礎。若 IMO 未來要求在特定敏感海域內，船舶需保留更完整的錨機操作紀錄、航向與推進器輸出資料，甚至與 ECDIS 圖層結合，則第 4 章所反覆出現的歸因困境與行為 - 意圖落差便可在某種程度上被壓縮。這一改革的價值不在於保證每次都能證明惡意，

而在於讓行為者更難完全隱身於技術模糊地帶之中。

4 建立全球海事數位安全協調中心(GMDSC)專門協調節點：就現實制度而言，較可行的寫法也許不是直接主張已存在的正式中心，而是倡議 IMO 與 ITU 共同建立一個常設或半常設的跨域協調機制。原因在於，海底電纜既是海事問題，也是電信與數位韌性問題。ITU 在 2025 與 2026 年已持續召開國際海底電纜韌性峰會，並推動國際顧問機制，這說明全球治理已開始承認此議題不能由單一部門處理。若 IMO 能與 ITU 形成制度化合作，建立共同事件回報、臨時調查支援、修復優先通道與跨國資料共享框架，那麼第 6.3 節所主張的國際合作將真正具備組織化載體。

此外，將 IMO Member State Audit Scheme(IMSAS)升級以處理權宜船旗與船旗國不作為問題。IMO 目前的 Member State Audit Scheme 自 2016 年起已屬強制性，且稽核內容本就包括成員國對適用 IMO 文書的立法、執行、監控與違規執法成效。未來若把是否有效監理本國船旗船在海底基礎設施敏感區的操作行為納入稽核重點，或將相關不作為視為執行缺失，那麼 IMO 就能間接對權宜船旗國施加更實質的制度壓力。這不必立即變成懲罰性機制，但足以透過白名單排名、港口國檢查強度與市場聲譽，逐步把船旗國責任從形式義務拉回功能義務。

當然，IMO 角色重塑也不會沒有阻力。這些阻力本質上反映了地緣政治大國對於海洋公共性與國家主權延伸之間權力平衡的深層擔憂。

1. 航行自由與管轄權擴張的拉鋸 - 預防性攔截權對傳統海洋秩序的挑戰：傳統海洋強權，特別是美、英等國，長期將航行自由視為海洋秩序基石，推動 ICPSI 可能被質疑為航行自由的倒退。反對者可能主張，若賦予沿岸國在海纜廊道內擁有預防性攔截或強制檢查的權力，將演變為一種變相的領海擴張(Creeping Jurisdiction)。大國擔心，這類條款可能被部分國家惡意利用，以保護基礎設施為名，行封鎖戰略水道之實，進而干擾海軍戰略部署或商船的正常通行。

2. 歸因技術的雙重用途爭議 - 數位海權霸權與水下軍事敏感性的權衡：在 ICPSI 框架下提出的數據共享與技術歸因機制，亦會面臨技術中立性的質疑。部分國家可能指控，由少數具備先進感測技術(如 DAS 或 UUV)的大國所主導的歸因系統，可能演變為一種數位海權霸權。他們擔心這些技術不僅監測船錨，更會被用於偵測潛艦動向或水下軍事布點。因此，如何在透明度與軍事敏感性之間取得平衡，將是 IMO 在談判中最大的政治雷區。

3. 主權避風港與船旗國利益的抵觸 - 權宜船旗(FOC)模式與強制透明化的對立：如 4.4 節所述，權宜船旗(FOC)國家通常依賴低度監管吸引船隻註冊，若 ICPSI 要求強制性的數位合規與責任溯源，將直接衝擊其商業模式。此外，一些將影子船隊視為戰略工具的大國，亦會透過外交影響力阻礙任何導致其船隻透明化的強制性代碼，主張這干涉了船旗國的專屬管轄原則。

4. 規範執行與市場機制的整合障礙 - 透過功能性導向尋求博弈夾縫中的共識：即使制定了章程，若無法與保險、港口、航運市場與數據共享機制連動，它仍可能停留於書面規範。面對這些大國博弈下的阻力，ICPSI 的推進應採取功能性導向，將監管範圍嚴格限制於與海纜安全直接相關的物理行為，而非對航行權的全面限制。透過界定清晰的技術門檻而非政治邊界，才有可能在博弈的夾縫中尋求國際共識。

總結來說，IMO 的角色重塑，不應被理解為機構權限的單純擴張，而是對海洋治理邏輯的一次必要更新。當海底電纜與其他海底關鍵設施已成為全球經濟、國家韌性與航運秩序的共同基礎時，IMO 若仍只把海洋視為船舶通行的表面空間，其規範能力將愈來愈難回應現實。相反地，若它能推動一部以透明度、可追責性、敏感海域操作義務與跨國協作為核心的《海底基礎設施保護強制章程》，那麼它不僅是在補上現有制度的缺口，更是在重新界定二十一世紀海洋治理的正當性基礎。

七、效率導向到安全流動

海洋不再是低摩擦的通道，而是高風險的交界；真正的挑戰，是文明如何不被自身偽善的規則所癱瘓。當流動需要被保護，效率便必須讓位於安全；當自由不再無條件，秩序便需要重新定義。這個時代，我們必須在法律化的叢林中覺醒，讓不確定性反向施加於破壞者，在崩解的秩序殘骸上，守護住數位文明最後一絲聯結的光芒。

7.1 核心發現：全球海洋進入「高摩擦環境」

本研究的首要發現，在於全球海洋空間的性質已發生根本性轉變，海洋正從一個以公共通行為基礎的低摩擦空間，轉化為一個由風險、監控與競爭所構成的高摩擦戰略場域。

這種轉變的核心，在於我們必須誠實面對現行國際海事體系的秩序悖論。正如第四章所述，法律條文雖然被精確遵守，卻無法阻止破壞的發生。當程序正義淪為破壞

者的戰略掩體，原本用於促進流動的透明機制(如 AIS、無害通過)，反而成為蓄意行為者隱匿意圖的漏洞。

這種數位摩擦(Digital Friction)的全面上升，意味著海洋的運作邏輯已不再是單純的物理航行。海洋已不再是一個透明的通道，而是一個布滿感測、監控與風險標記的可計算戰略空間。船舶的每一次航行、每一次錨泊，都必須在效率與合規的巨大張力中進行重新校準。

7.2 理論貢獻：建立「海事灰色地帶風險模型」

在理論層面，本研究不僅描述了一種新型威脅，更提出了一套可供分析與預測的整合模型。其核心，在於將原本分離的海事安全(maritime security)與數位安全(cyber/information security)納入同一分析框架。

首先，本研究提出「海事 - 數位耦合風險(Maritime-Digital Coupling Risk)」的概念，指出風險的本質不再是單一層級的破壞，而是跨層級的傳導與放大(cross-layer cascade)。物理層的微小動作(如拖錨)，可在瞬間轉化為邏輯層的系統性失效(如數據中斷、金融延遲、港口癱瘓)。

其次，本研究進一步建立風險判讀的簡化模型：

$$R = P \times V \times I$$

其中

- P (Physical Proximity)：物理接近度 (船舶與電纜節點的空間關係)
- V (Digital Vulnerability)：數位脆弱性 (節點的重要性與冗餘程度)
- I (Strategic Intent)：戰略意圖 (可否認性條件下的行為動機)

這一模型的關鍵意義在於，風險不再僅由「能力」決定，而是由「位置 × 脆弱性 × 意圖」的交互作用所產生。一艘普通商船，在特定時間與地點，亦可能轉化為高戰略影響力的行為體。正如第三章與第四章的交叉分析所顯示，一艘普通商船在咽喉點的物理接近(P)，結合海底電纜的數位脆弱性(V)，在戰略意圖(I)的驅動下，能在瞬間轉化為跨層級的系統性失效。

更重要的是，本研究挑戰了一個長期被視為理所當然的假設，即經濟互賴會降低衝突。在數位時代，這一命題出現反轉。當多國共享同一條海纜路徑或數據節點時，

這種高度耦合反而形成了高價值脆弱點(high-value vulnerability)，使攻擊具有更高的報酬率。這種非對稱性，正是當代灰色地帶行動得以反覆操弄秩序的核心。

7.3 政策意涵：從「事後追責」轉向「事前威懾」

本研究最直接的政策結論，在於現行法律體系那種以事後追責為核心的邏輯已經徹底過時。

傳統國際法建立在「行為發生⇨證據蒐集⇨責任歸屬⇨補償或制裁」的時間序列上。然而，在灰色地帶環境中，這一序列完全失效。攻擊的關鍵價值在於當下效果，而非長期責任。當法律機制啟動時，戰略目標早已達成。

在面對損失非對稱性，即數百萬美元的民事賠償與數十億美元的系統性崩潰之巨大落差時，任何依賴事後訴訟的規約都顯得蒼白無力，僅能被視為一種戰略上的事後悼念。由於物理時間落差與歸因灰色化的限制，監控系統往往只能觀測災難，而無法阻擋破壞。因此，未來治理的核心不應是強化追責能力，而是建立即時威懾能力(real-time deterrence)，必須將威懾的起點從法庭移至操作現場與市場終端：

1 技術執法化(Technological Enforcement)：既然意圖不可證，我們就必須以行為特徵作為干預依據。透過數據融合與即時監控，將海底基礎設施的保護從事後紀錄轉向事前介入。

2 市場與金融的韌性鏈條：如第五章所述，當法律無法即時定罪時，市場必須先行。透過保險費率的精算、融資條件的約束以及港口准入的篩選，建立一套「法律 - 技術 - 市場」三位一體的威懾體系。讓那些意圖模糊、隱匿身分的行為體，在物理上切斷數據的同時，在經濟上切斷自己的生存命脈。

7.4 未來展望：海底基礎設施作為地緣政治前線

展望未來，海底基礎設施將成為全球權力競爭最隱蔽、但最關鍵的戰場之一。我們必須誠實地面對，無辜的一方在舊有秩序下，確實面臨著難以招架的結構性劣勢。

1 主權的垂直化：主權的概念正在發生垂直化(verticalisation)。傳統國界是水平劃定的，但在數位時代，國家安全正不可避免地向海床延伸。海底電纜廊道與數據節點，將形成事實上的水下戰略邊疆。這雖然不是領土，但在安全維護上的位階將與領土等同。

2 航運產業的結構：航運產業的權力結構也將重塑。未來的海上強權，不再僅取決於船隊規模或運力，而取決於誰能掌握數據流的安全與可信度(security and integrity of maritime data flows)。航運公司將不再只是物流服務提供者，而是數位基礎設施的共同守護者，甚至成為國家安全體系的一部分。

3 秩序的韌性轉型：全球秩序將面臨一個不可迴避的選擇，是維持以效率最大化為核心的開放體系，還是轉向以韌性與安全為優先的受控流動(controlled mobility)，轉向成為一個有刺的韌性體系(Armed Resilience System / Deterrence-based Resilience)。這兩者並非完全對立，但在高風險環境下，效率必然讓位於安全。

4 誠實的防禦觀：承認海洋已成為一個法律化的叢林空間(Legalized Jungle)。在這種環境下，防衛不再僅僅取決於武力的展現，而取決於對數據流完整性的守護與對風險成本的精確定義。

在制度的殘骸上尋找海洋的未來

總結而言，本研究的終點，並非一個完美的解決方案，而是一次對當前全球秩序崩壞過程的沉痛側寫。我們必須誠實而殘酷地承認，在當前灰色地帶行動的邏輯下，國際海事法體系正經歷一場「優雅的潰敗」。這種危機最令人絕望之處，並不在於法律被粗暴地踐踏，而在於法律被精確、冷靜地遵守的同時，我們卻眼睜睜看著支撐現代文明的數位神經被一根根切斷。

這是一場法治的諷刺劇(The Paradox of Legal Formalism)。當破壞者披著無害通過的合法外衣，在眾目睽睽之下利用人類對程序正義的尊重，將原本保護弱者的法律轉化為行惡的防彈衣時，無辜的防禦方所面對的，不僅是物理設施的毀損，更是對公平、正義與國際誠信的徹底幻滅。監控鏡頭與感測器雖然捕捉到了破壞者的航跡，卻無法捕捉其隱匿於主權屏障後的惡意。這種「看見了風險，卻在法律與時空面前招架無力」的集體窒息感，正是二十一世紀數位海洋最誠實的寫照。

如果我們繼續寄望於這套已然戰略滯後的舊秩序，那麼所有的事後追責都將淪為一場場無濟於事的事後悼念。唯有當我們徹底拋棄對舊有安全感的依賴，轉而將法律、技術與市場力量進行近乎冷酷的深度耦合，我們才可能在廢墟中重建韌性。我們必須學會將不確定性這把利刃，反向施加於那些玩弄規則的人身上；我們必須讓破壞者明白，當他們試圖切斷全球數據的流動時，他們也同時在切斷自己與現代金融、商業與文明體系的連結。

這不僅僅是一場關於海底電纜的防禦戰，更是一場關於文明如何不被偽善的規則所癱瘓(How civilisation survives the trap of its own legalism.)的保衛戰。在動盪的二十一世紀，全球通訊與航運的安全底座，絕不會自動修復。唯有建立在這種對現實的深刻覺醒與悲劇危機感之上，我們才可能在法律化的叢林中，守護住最後一絲屬於全人類的互聯光芒。

後記：在潮汐轉向之際，聽見深海的崩裂聲

我們習慣於島嶼表層的明亮與安穩。在霓虹與訊息的流動之中，在日復一日的討論、選擇與對立之中，時間被切割為一段段短暫而可掌握的現在。我們關注眼前的競逐，沉浸於制度內部的變動，彷彿這片環繞四周的海洋，仍只是那道熟悉、溫和、可以依賴的邊界。

然而，真正的變化，從來不發生在可見之處。在那片沒有聲音、沒有光線的深海之下，支撐整個文明運作的結構，正經歷一種緩慢卻不可逆的位移。當連結開始出現裂縫，當訊號在無聲之中被切斷，世界並不會立即崩塌，而是以一種更隱晦的方式，逐漸失去其穩定的節奏。這正是當代最深的危機，這不是崩潰的瞬間，而是崩潰尚未被察覺之前的寧靜。

對於一座島嶼而言，海洋從來不只是風景。它是邊界，也是通道；是屏障，也是命脈。當全球的流動建立在看不見的網絡之上，當這些網絡的安全開始動搖，島嶼的處境便不再只是地理位置的問題，而是對風險感知與回應能力的考驗。如果我們只凝視土地之上的變動，而忽略海洋之下的擾動，那麼我們所理解的現實，終究只是被截斷的一部分。

這種斷裂，並非偶然。當破壞可以被解釋為事故，當行動可以被包裝為操作，當一切都被歸類為「意外事件」，風險便得以在秩序之內生成，而不再需要對抗秩序本身。於是，威脅不再來自邊界之外的明確對抗，而是滲入於規則允許的空間之中。真正的危險，不是我們看見了敵意，而是我們逐漸失去了辨識敵意的能力。在這樣的時刻，問題不再只是安全，而是清醒。

哲學告訴我們，真正的盲點並非無知，而是選擇不去看見，就如沙特(Jean-Paul Sartre)在自欺(Bad Faith/Mauvaise foi)所闡述的「自欺的人是知道真相卻又選擇不去看見真相的人。」也應了柏拉圖(Plato)在地穴寓言(Allegory of the Cave)中指出的「最令人感到憐憫的盲目，莫過於靈魂對真實事物的視而不見」的核心哲學。人最大的危機，並非外在的毀壞，而是內在對真實的遺忘。當一個島嶼，沉浸於內部的對立與消耗，當短暫的安穩取代了長遠的警覺，那麼即使風險已然逼近，人們仍可能在表面的秩序中，錯過了轉向的時刻。這並不是一種指責，而是一種提問。

在這片海開始改變之際，我們是否願意重新理解它的意義？在那些尚未被命名的擾動之中，我們是否願意承認，它們已經與我們的命運產生連結？當秩序不再自動運作，當安全不再理所當然，我們是否仍能在複雜與不確定之中，做出面向未來的選擇？

或許真正需要被守護的，不只是海底的電纜，而是我們對連結的珍惜，對現實的誠實，以及在關鍵時刻不選擇不去看見、不選擇逃避的勇氣。

海洋從未改變它的本質。改變的，是我們看待它的方式。在潮汐轉向之際，深海並不發聲。但裂縫早已存在。而我們，是否願意聽見。