AIS 與 GPS 系統脆弱性對國際航運安全之影響及政策因應研究

A Study on the Impact of AIS and GPS System Vulnerabilities on International Maritime Navigation Safety and Policy Responses

蔡奇呈[1]、陳嘉陵[2]

摘要

隨著全球供應鏈與國際貿易高度依賴海上運輸，自動識別系統(AIS)與全球定位系統(GPS)已成為現代航運導航與海上交通管理之核心技術，對提升航行安全與海事態勢感知具有關鍵作用。然而，隨著導航系統高度數位化，訊號欺騙(spoofing)與訊號干擾(jamming)等威脅日益增加，可能造成定位錯誤、態勢誤判與航行決策偏差，進而影響國際航運安全。本研究探討 AIS 與 GPS 之技術特性與脆弱性，分析其對船舶導航安全、交通管理及搜救作業之影響，並透過文獻分析與政策比較，檢視國際海事組織(IMO)、國際航標協會(IALA)及各國主管機關之監管措施。研究結果指出，AIS 與 GPS 具高度依賴關係，單一系統異常可能引發多層次風險，未來應強化系統韌性、建立異常偵測機制及促進國際資訊共享，以提升整體海事安全治理能力。本研究建立 AIS–GPS 資料依賴架構分析模型，以說明導航系統間之耦合關係與風險傳遞機制。

關鍵詞：船舶自動識別系統(Automatic Identification System, AIS)、全球定位系統(Global Positioning System, GPS)、國際航運安全、系統脆弱性、政策因應

Abstract

With global supply chains and international trade increasingly dependent on maritime transportation, the Automatic Identification System (AIS) and the Global Positioning System (GPS) have become core technologies in modern maritime navigation and vessel traffic management, playing a critical role in enhancing navigational safety and maritime situational awareness. However, as navigation systems become highly digitalized, threats such as signal spoofing and jamming are increasing, potentially causing positioning errors, misjudgment of

[1] 蔡奇呈 Chi-Cheng Tsai，中央警察大學水上警察學系專任助理教授，E-mail：oceanjerry@gmail.com

[2] 陳嘉陵 Chia-Ling Chen，中央警察大學水上警察學系專任助理教授，E-mail：chiaclloyd@gmail.com

situational awareness, and biased navigational decision-making, thereby affecting international maritime safety.

This study investigates the technical characteristics and vulnerabilities of AIS and GPS, analyzes their impacts on ship navigation safety, traffic management, and search and rescue (SAR) operations, and examines regulatory measures adopted by the International Maritime Organization (IMO), the International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA), and national maritime authorities through literature analysis and policy comparison. The findings indicate that AIS and GPS are highly interdependent, and abnormalities in a single system may trigger multi-layered risks. Therefore, future efforts should focus on strengthening system resilience, establishing anomaly detection mechanisms, and promoting international information sharing to enhance overall maritime safety governance capacity. In addition, this study develops an AIS–GPS data dependency framework to illustrate the coupling relationships and risk propagation mechanisms among navigation systems.

Keywords: Automatic Identification System (AIS), Global Positioning System (GPS), international maritime safety, system vulnerabilities, policy responses.

壹、前言

國際航運長期以來被視為全球經濟運作的重要支柱。根據聯合國貿易與發展會議(United Nations Conference on Trade and Development, UNCTAD)之統計資料，全球約九成以上之貨物流通需仰賴海上運輸完成，顯示航運系統之安全與穩定對國際貿易與全球供應鏈具有關鍵影響(UNCTAD, 2024)。隨著全球航運活動日益頻繁及航線密度持續提升，如何有效提升船舶航行安全與海上交通管理效率，已成為國際海事治理的重要議題(Bueger, 2015)。

近年來，隨著資訊與通訊技術快速發展，航運領域逐漸邁向數位化與智慧化，自動識別系統(Automatic Identification System, AIS)與全球定位系統(Global Positioning System, GPS)已成為現代航海不可或缺之核心技術(Lee et al., 2019)。其中，AIS 系統透過船舶之間以及船舶與岸基站之間之自動化資訊交換，可傳輸船舶識別資訊、位置、航向、航速及航行狀態等動態與靜態資料，大幅提升海上態勢感知能力與航行透明度，並在防止碰撞、海上交通服務(Vessel Traffic Service, VTS)管理及搜救行動中扮演重要角色(IMO, 2004；USCG Navigation Center)。另一方面，GPS 作為全球導航衛星系統(Global Navigation Satellite System, GNSS)之核心組成，能提供高精度定位、導航與授時

(Positioning, Navigation and Timing, PNT)服務，並廣泛整合於電子海圖顯示與資訊系統(Electronic Chart Display and Information System, ECDIS)、自動舵及各類智慧導航設備之中，成為現代船舶航行決策的重要依據(Reselman, 2021)。

然而，隨著航運系統對數位導航技術依賴程度日益加深，AIS 與 GPS 系統本身所存在之技術脆弱性亦逐漸浮現。研究指出，AIS 系統在設計初期較偏重資訊共享與透明性，對於資安防護考量相對不足，因此容易受到資料偽造或訊號操控之影響(Wilhoit et al., 2016；Thomas & Chiego, 2022)。近年來，在地緣政治衝突及海事灰色地帶行動背景下，AIS spoofing 與 jamming 事件逐漸增加，例如波斯灣地區之導航訊號異常即被視為重要案例(Skuld, 2025；Kpler, 2024)。當 AIS 訊號遭受欺騙時，可能導致船舶位置或身份資訊被偽造，進而誤導周邊船舶及岸基監控系統，降低海上態勢判斷準確性(London Maritime Academy, 2025)。

此外，GPS 訊號亦可能遭受干擾或欺騙攻擊，導致定位資訊失真甚至完全失效，迫使船員回歸傳統導航方法，進而增加航行偏差、擱淺或碰撞風險(Rudnik et al., 2025；Balić et al., 2024)。由於 AIS 多數情況需依賴 GPS 提供定位資訊，兩者之間存在高度耦合關係，一旦導航訊號遭受攻擊，往往可能引發連鎖性安全問題，對整體海事安全體系造成影響(Farah et al., 2022；Androjna et al., 2021)。

基於上述背景，本研究旨在探討 AIS 與 GPS 系統之技術特性與系統脆弱性，分析其在國際航運安全架構中的功能角色及潛在風險影響，並進一步探討訊號欺騙與干擾威脅對船舶導航安全、海上交通管理及海事保安所帶來之挑戰。同時，本文亦將檢視國際海事組織(International Maritime Organization, IMO)、國際航標協會(International Association of Marine Aids to Navigation and Lighthouse Authorities, IALA)、國際電信聯盟(International Telecommunication Union, ITU)等國際機構所提出之政策、法規與技術標準，以了解目前國際社會在面對相關威脅時之治理策略與因應方向。本研究將基於技術分析與政策探討之結果，提出強化 AIS 與 GPS 系統韌性之建議，包括提升導航系統安全性、加強異常偵測能力，以及促進國際合作與資訊共享等面向，以期作為未來海事安全治理與政策制定之參考。

本研究採用文獻分析法與政策比較分析法，並依據系統化程序進行資料蒐集與分析。

在文獻蒐集方面，本研究主要使用 Scopus、Web of Science 及 Google Scholar 等資料庫，並輔以國際組織官方網站(IMO、IALA、ITU、USCG)之政策文件。檢索關鍵字包括「AIS spoofing」、「GNSS spoofing」、「GPS jamming」、「maritime cyber security」、

「navigation system vulnerability」等，時間範圍設定為 2015 至 2025 年，以確保涵蓋最新研究發展。

文獻篩選標準包括：(1)與 AIS 或 GNSS 安全相關之研究；(2)涉及 spoofing 或 jamming 技術分析；(3)具海事應用背景之研究；排除非同行評審文獻及與主題關聯性較低之研究。

在政策比較分析方面，本研究建立四項分析構面：

(1) 是否明確涉及 spoofing / jamming 威脅。

(2) 是否提出具體技術防護措施。

(3) 是否建立事件通報與資訊共享機制。

(4) 對航運業者之義務要求強度。

並據此對 IMO、IALA 與各國主管機關之政策進行系統化比較。本研究之分析流程可分為三個主要步驟：

(1) 文獻蒐集與篩選

(2) 多層級系統架構建構

(3) 政策比較與案例分析整合

以確保研究方法具系統性與可重現性。

本研究聚焦於以下核心研究問題：

(1) 現行國際與國家層級導航安全政策，在應對 AIS 與 GPS spoofing 與 jamming 威脅時，存在哪些具體制度與技術缺口？

(2) AIS–GPS–ECDIS–VTS 之多層級資料依賴結構，如何放大單一導航異常所造成之連鎖性風險？

(3) 現有導航系統安全防護機制，是否足以應對跨層級資訊耦合所帶來之系統性

脆弱性？

(4) 如何建構一套結合「技術依賴關係」與「政策治理」之整合分析框架，以評估海事導航風險？

本研究之主要貢獻如下：

(1) 建立 AIS–GPS–ECDIS–VTS 多層級資料依賴分析架構，系統性揭示導航資訊鏈之耦合關係與風險傳遞機制。

(2) 提出「跨層級連鎖風險(Cascading Risk)」分析觀點，說明技術異常如何擴散至操作與管理層。

(3) 建立國際導航安全政策比較框架，系統性評估 IMO、IALA 與各國主管機關之治理落差。

(4) 整合技術防護、異常偵測與政策治理，提出多維度導航安全強化策略。

本文後續章節將依序說明 AIS 與 GPS 系統技術架構與功能(第貳章)、系統脆弱性與連鎖風險機制(第參章)，以及國際政策比較與治理分析(第肆章)，最後提出結論與政策建議(第伍章)。

貳、AIS 與 GPS 技術規格及其在航運安全中的作用

2.1 自動識別系統(AIS)

自動識別系統(AIS)作為現代航海電子化之核心關鍵，利用特高頻(Very High Frequency, VHF)無線電頻道作為傳輸媒介，實現了全球船舶資訊的高速互聯與自動化廣播。根據國際標準，AIS 固定發送包含船舶靜態資訊(如船名、編號)、動態資訊(如即時經緯度、航向、航速)以及航次相關數據，使船舶與岸基監控中心能夠掌握精確的海上交通態勢。由於該系統具備跨國界、跨設備的互操作性，不同噸位與國籍之船舶皆能在同一開放式通信架構下進行資料交換。這種高度的資訊對稱性不僅有助於港口流量管制(VTS)，更在船舶避碰、搜救作業(Search and Rescue, SAR)中發揮了決定性的作用，有效降低了海上碰撞風險並提升了整體航行之安全性(USCG Navigation Center)。

為了說明 AIS 與 GPS 系統在船舶導航中的資料耦合關係與訊號依賴性，本研究首先建立其整體概念架構，如圖 1 所示。該架構顯示 AIS 系統高度依賴 GNSS/GPS 所提供之定位資訊，而 GNSS 層之訊號異常可能透過 AIS 傳播至上層航行態勢感知系統。

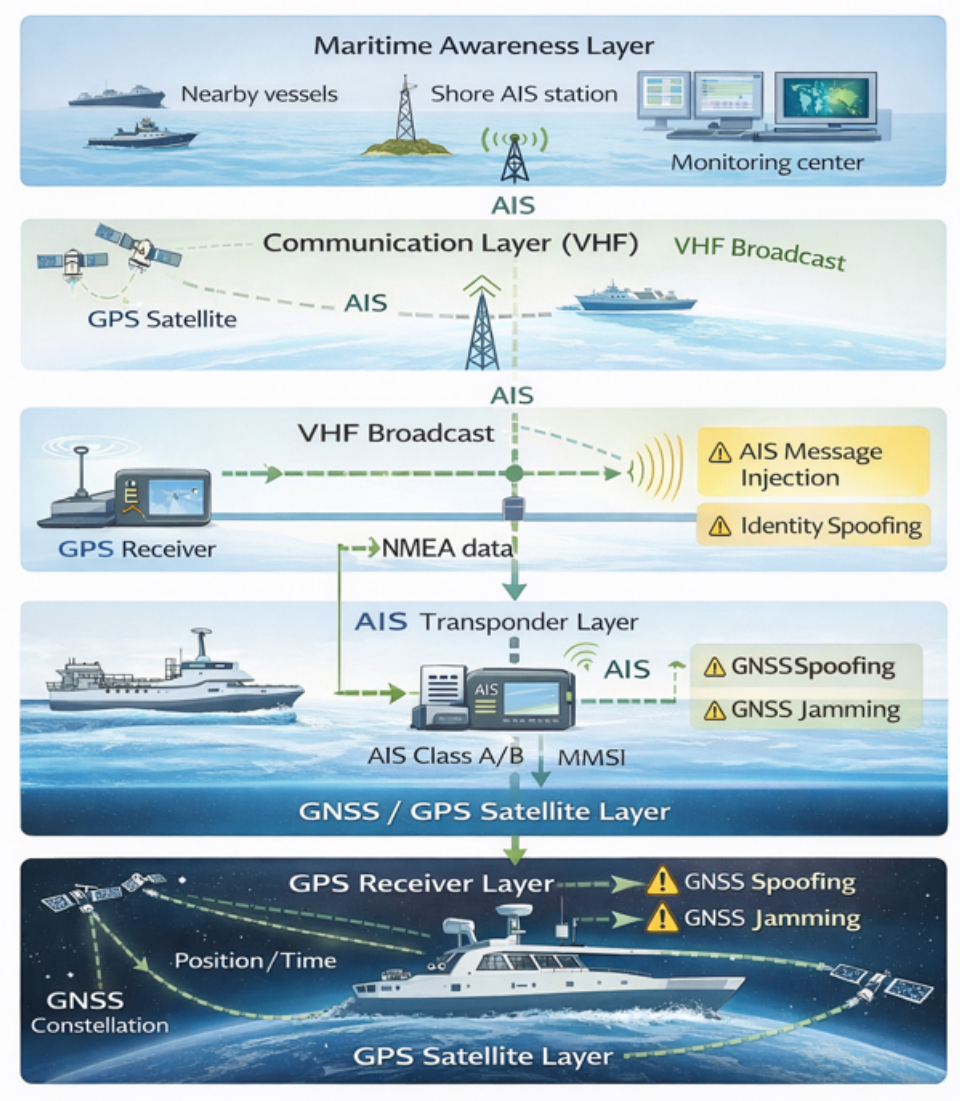

圖 1　海事航行中 AIS 與 GPS 系統之概念性耦合架構(本研究整理)

如圖 1 所示，AIS 系統在航行資訊傳輸過程中高度依賴 GPS 所提供之定位與授時資料，船舶位置資訊經由 GPS 接收器輸入後，再透過 AIS 應答器轉換為標準化廣播訊息。此種資料耦合架構使 AIS 與 GNSS 系統形成緊密的依賴關係，當 GNSS 層出現訊號異常或干擾時，其影響可能向上傳遞至 AIS 通訊與海上態勢感知層，進而影響整體航行安全。

研究指出，AIS 所提供之持續性動態資訊，已成為海事交通管理、碰撞預防與航跡分析的重要基礎資料來源，並廣泛應用於船舶行為分析與異常偵測研究(Pallotta et al., 2013；Mazzarella et al., 2015)。此外，AIS 資料亦被用於航運排放監測、船舶交通模式分

析與環境治理等領域，顯示其應用範圍已超越傳統導航用途(Jalkanen et al., 2014；Robards et al., 2016)。依據國際標準，AIS 訊息可依用途與優先級區分為多種類型，其主要內容如下：

(1) 位置報告(Messages 1、2、3、18、19、27)：此類訊息屬於高優先級資訊(優先級 1)，主要提供船舶即時位置、航向、航速及航行狀態等動態資料。A 類 AIS 設備通常採用 SOTDMA(Self-Organized Time Division Multiple Access)、RATDMA(Random Access TDMA)及 ITDMA(Incremental TDMA)等多址存取方式，以確保在高密度航行環境中仍能有效傳輸資料，其中 Message 27 主要應用於超視距通訊場景。

(2) 岸台報告(Message 4)：此訊息用於傳送岸基站位置、UTC 時間、日期及時隙資訊，優先級同樣為 1，並透過 FATDMA(Fixed Access TDMA)與 RATDMA 機制維持系統同步與時序管理。

(3) 靜態與航次相關資料(Messages 5、24)：此類訊息主要傳輸船舶靜態資訊，如船名、呼號、船舶尺寸及類型，以及航次相關資料，例如目的港、預計抵達時間與吃水深度等，優先級為 4，提供船舶識別與航行計畫資訊。

(4) 二進制資料訊息(Messages 6、8、25、26)：主要用於定址或廣播方式傳輸特定應用資料，可支援單時隙或多時隙資料交換，常應用於特殊服務或延伸應用需求。

(5) 安全相關訊息(Messages 12、14)：此類訊息用於廣播或定址安全警示資訊，對於海上安全通報具有重要功能，其中 Message 13 為安全訊息確認用途。

(6) 航標報告(Message 21)：主要用於傳送航標(Aids to Navigation, AtoN)之位置與狀態資訊，有助於航道安全維護與導航輔助。

透過上述標準化訊息架構，AIS 能有效實現船舶間與岸台之資訊共享，並提升碰撞預防與搜救效率。然而，AIS 亦存在訊號可信度不足之問題，相關研究指出其容易遭受資料偽造與訊號操控，進而影響態勢判斷與海事安全(Wilhoit et al., 2016；Skuld, 2025)。然而，此類開放式與標準化之訊息架構，在提升互操作性的同時，也可能成為訊號偽造(spoofing)攻擊之潛在基礎。

2.2 全球定位系統(GPS)

全球定位系統(GPS)為目前最廣泛應用之衛星導航系統之一，其透過多顆中軌道衛星持續發射訊號，由地面接收器進行解碼與定位解算，以獲得高精度之三維位置與時間資訊(Reselman, 2021)。GPS 所提供之定位、導航與授時 (Positioning, Navigation and Timing, PNT) 能力，已成為現代航海導航之核心基礎。

在海事應用中，GPS 接收器通常依據美國國家海洋電子協會(National Marine Electronics Association, NMEA)所制定之標準格式輸出導航資料。其中，NMEA 0183 為目前航海設備間廣泛採用之通訊標準，並作為多種船舶設備之核心資料來源(USCG Navigation Center)。此類標準化資料格式能促進多設備整合，但同時亦形成單點依賴風險，當訊號遭受干擾時可能影響整體導航系統之可靠性(Spanghero & Papadimitratos, 2024)。

近期學術研究與實務案例均指出，全球導航衛星系統欺騙(GNSS Spoofing)技術已取得突破性進展。現有的攻擊手段已證明能於靜態錨泊或動態航行環境中，成功模擬具備高度邏輯一致性的偽造訊號，進而誘導船載接收器產出錯誤的定位結果，顯示此類非傳統安全威脅對全球航運韌性的挑戰正與日俱增(Balić et al., 2024；Mistrapau et al., 2025)。更深層的風險在於，現代船舶高度仰賴多設備整合與資料融合(Data Fusion)技術；若系統在進行座標格式轉換或多源數據解析時未具備完善的驗證機制，任何微小的定位偏差都將透過網路化設備產生連鎖反應。這種資訊不對稱性不僅會導致態勢感知的誤判，更將直接干擾避碰路徑規劃等核心航行決策，對整體航行安全構成實質性威脅。

為了更清楚說明 GNSS 接收器於 NMEA 0183 通訊架構下所使用之主要導航語句，本研究整理常見且具代表性的語句類型及其功能特性。各語句在系統中具有明確分工，例如提供即時定位資訊、航行狀態更新與衛星訊號品質評估等功能，並共同支持船舶導航系統之正常運作。表 1 彙整 NMEA 0183 標準中常見語句之名稱、識別符及主要功能說明，作為後續導航資料分析與系統脆弱性探討之基礎。

表 1 NMEA 0183 標準語句類型與功能說明

語句標識符	語句名稱	主要內容與功能說明
GPGGA	全球定位系統定位數據	提供時間、經緯度位置、定位品質指示、使用衛星數量及海拔高度等基礎定位資料。
GPRMC	建議最小特定 GNSS 資料	屬於綜合性導航語句，包含 UTC 時間、日期、狀態、經緯度、地面航速及地面航向等核心資料。
GPVTG	航向與航速資訊	提供船舶相對於地面的實際航向(True/Magnetic Course)與航速(節／公里每小時)。
GPGSA	衛星狀態與精度資訊	顯示當前定位模式(2D/3D)、參與計算之衛星編號以及精度稀釋度(HDOP/VDOP/PDOP)等參數。

語句標識符	語句名稱	主要內容與功能說明
GPGSV	可視衛星資訊	提供目前天空中可見衛星的總數、衛星編號、仰角、方位角及訊噪比(SNR)，用於評估收訊品質。
GPGLL	地理位置資訊	主要用於輸出經緯度位置座標及定位時間，格式較為精簡。

由表 1 可知，NMEA 0183 語句在功能設計上具有明確分工，不同語句分別負責定位資訊、導航狀態與衛星品質等資料傳輸，並共同構成完整之導航資訊鏈。在實務應用中，由於 AIS 系統多數依賴 GPS 所提供之 NMEA 資料進行船位更新與資訊廣播，因此上述語句內容之正確性與完整性將直接影響船舶導航判斷、態勢感知以及海上交通監控系統之可靠性。此一資料依賴關係亦凸顯在導航系統遭受干擾或欺騙情境下，進行資料層級分析與驗證的重要性，並為後續脆弱性分析提供關鍵基礎。

此外，GPS 輸出之經緯度座標具備多種表述型態，常見者包括：度分秒格式(DMS)、十進制度(DD)，以及 NMEA 標準規範之 ddmm.mmmm (或 dddmm.mmmm) 格式。在多設備整合與資料融合(Data Fusion)的環境下，不同格式間的精確轉換與統一解析，是確保航跡分析可靠度及系統資料一致性的關鍵。若解析機制未臻完善，極易產生定位偏差或資訊誤判，進而威脅導航安全。

整體而言，GPS 所提供之高精度定位能力已廣泛整合於電子海圖顯示與資訊系統(Electronic Chart Display and Information System, ECDIS)、雷達整合導航系統、自動舵以及智慧航行系統等多種船舶設備之中，成為現代航行決策與海上交通管理的重要基礎。然而，正因航運系統高度依賴 GPS 所提供之定位資訊，其訊號品質與可靠性亦直接影響船舶導航安全與海上交通管理效能。因此，深入理解 GPS 資料結構與其可能面臨之技術脆弱性，對於建立安全且具韌性之導航系統具有重要研究價值。

參、AIS 與 GPS 的脆弱性及其對航運安全的影響

儘管自動識別系統(AIS)與全球定位系統(GPS)已成為現代航運安全架構中不可或缺的重要技術，但其設計初期主要著重於資訊共享與導航效率提升，而非以資訊安全為核心考量，因此在面對惡意干預時仍存在一定程度的技術脆弱性。近年來，隨著低成本無線電設備與訊號模擬技術日益普及，針對 AIS 與 GPS 的欺騙(spoofing)與干擾(jamming)攻擊逐漸增加，對船舶航行安全、海上交通管理與海事保安造成潛在威脅。此類攻擊不僅影響單一船舶之導航能力，更可能透過資訊鏈結造成整體海域態勢判斷錯誤，進而引發連鎖性風險。

圖 1 與圖 2 分別從系統耦合關係與攻擊面分析兩個層面，說明 AIS 與 GPS 在導航架構中的風險傳遞機制。為了進一步說明 AIS 與 GPS 系統在實際航行環境中的資料依賴關係及其潛在攻擊面，本研究建立 AIS–GPS–ECDIS–VTS 之多層級資料流架構，如圖 2 所示。該架構顯示導航資料由 GNSS 層向上傳遞至船載整合系統與岸基監控系統，當底層資料遭受攻擊時，其影響可能沿著資料鏈向上擴散，形成連鎖式航行風險。

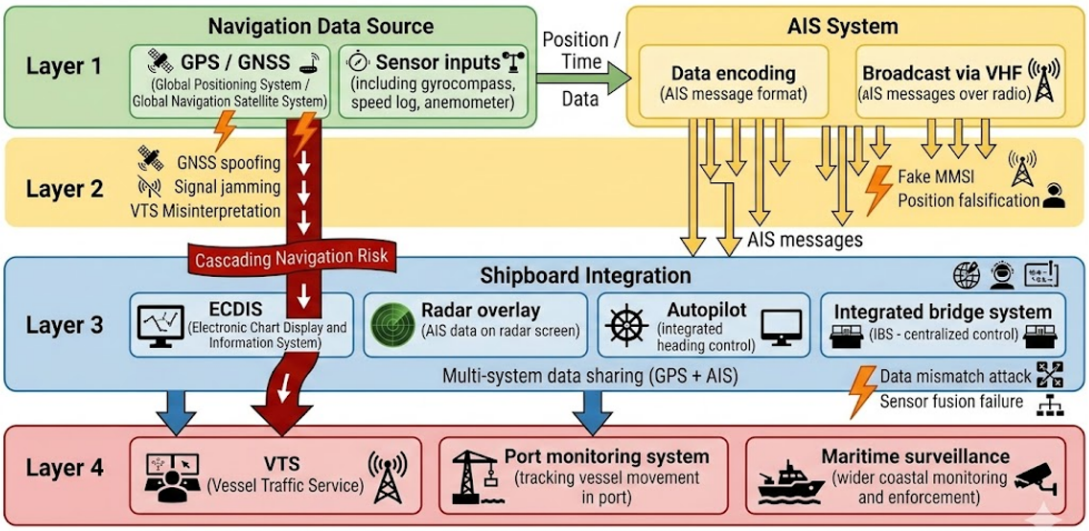

圖 2 海事導航系統中 AIS–GPS–ECDIS–VTS 資料依賴與攻擊面架構圖(本研究整理)

如圖 2 所示，AIS 與 GPS 系統並非獨立運作，而是透過多層級資料共享機制與船載導航系統及岸基監控系統形成高度耦合之網路。當 GNSS 訊號遭受欺騙或干擾時，其影響可能導致 AIS 訊息錯誤，進一步造成 ECDIS 顯示偏差或 VTS 誤判，最終形成級聯式(cascading)導航風險。此現象說明了現代海事導航系統中資料依賴結構所帶來之系統性脆弱性。

3.1 系統架構之形式化定義

為提升分析架構之可操作性與理論嚴謹性，本研究將 AIS–GPS–ECDIS–VTS 系統建模為一多層級有向圖(Directed Graph)：

$$G = (V, E)$$

其中，

V為節點集合，包含 GNSS 衛星、GPS 接收器、AIS transponder、ECDIS 系統與 VTS 中心；E為資料傳遞邊，表示導航資訊於各系統間之流動關係。

依據系統功能，本研究將節點劃分為三個層級：

(1) 感測層(GNSS Layer)：GNSS 衛星、GPS 接收器。

(2) 通訊層(AIS Layer)：AIS transponder、VHF 通訊鏈路。

(3) 應用層(Application Layer)：ECDIS、VTS 系統。

此多層級結構可用以描述導航資訊由底層感測來源逐層傳遞至決策與監控系統之過程。

此外，本研究進一步區分資料依賴邊之類型，包括：

(1) 強依賴(Strong Dependency)：如 GPS → AIS 定位資料輸入。

(2) 弱依賴(Weak Dependency)：如 AIS → VTS 輔助監控資訊。此區分有助於識別高風險傳遞路徑與關鍵節點。

為進一步提升本研究分析框架之可操作性與評估能力，本文引入以下形式化指標(metrics)以描述系統中風險傳遞之特性：

(1) 節點重要性(Node Criticality, C_i)：用以衡量節點 i在整體資料傳遞結構中的關鍵程度，特別是其失效對上層系統所造成之影響範圍。

(2) 路徑風險(Path Risk, R_p)：表示特定風險傳遞路徑上累積之風險程度，該值可隨著跨層級傳遞而逐步放大。

(3) 依賴權重(Dependency Weight, w_{ij})：用以表示節點 i與節點 j之間之依賴強度，其中強依賴關係具有較高之權重，代表其在風險傳遞中扮演更關鍵角色。

此外，需說明的是，本文所提出之節點重要性(C_i)、路徑風險(R_p)與依賴權重(w_{ij})等指標，主要用於建立系統化之分析架構，並作為導航系統風險評估與關鍵節點識別之基礎。惟本研究並未針對上述指標進行精確之數值估計或參數校準，其目的在於建構具解釋能力之概念模型。

未來研究可進一步結合實測資料與統計方法，對相關指標進行量化分析與驗證，以提升模型之預測能力與實務應用價值，並促進本研究架構向定量化分析模型之延伸。

3.2 AIS 脆弱性：訊號欺騙(Spoofing)

AIS 欺騙係指惡意行為者透過偽造或竄改 AIS 訊息，傳輸不正確的船舶位置、身份或航行狀態資料，使其他船舶或岸基監控系統接收到錯誤資訊。由於 AIS 設計目的在於提升資訊透明度，而非建立強化驗證機制，因此其訊息在傳輸過程中缺乏完整的加密與身分認證機制，使得系統較容易受到偽造訊號的影響。

在技術層面上，AIS 欺騙可能透過流氓應答器(rogue transponder)直接發送虛假訊號，或透過入侵合法 AIS 設備修改其輸出資料來實現。攻擊者可模仿真實船舶身份，甚至建立不存在的「虛擬船舶」，進一步干擾海上交通監控與態勢分析。AIS 欺騙對航運安全的影響主要包括以下幾個面向：

(1) 碰撞風險提升：船舶若依據被竄改之 AIS 資訊進行航行判斷，可能在不知情情況下與其他船舶或障礙物過度接近，增加碰撞可能性。

(2) 態勢感知能力下降：船員及海上交通服務(VTS)操作人員接收到錯誤資訊後，將難以準確掌握實際海況，降低決策品質。

(3) 搜救行動困難：當遇險船舶位置資訊遭到偽造或錯誤傳輸時，將直接影響搜救資源配置與救援效率。

(4) 海事保安威脅：AIS 欺騙亦可能被用於掩護非法活動，例如走私、非法捕撈或未經授權進入敏感水域，增加海上執法難度。

AIS 訊號欺騙所引發的連鎖反應，其影響力已遠遠跨越了電子導航的技術範疇，深度滲透進現代海事管理的行政與法律層面。對海上交通服務(VTS)中心而言，大規模的虛假資訊將導致行政決策癱瘓；對執法單位而言，身分偽裝技術則大幅提升了打擊走私與非法捕撈的難度。這種「技術性偏差」所誘發的「管理性失能」，對當前國際航運的運作模式構成了系統性挑戰。

這意味著，強化 AIS 系統的韌性已不再僅是航海儀器的升級議題，而是涉及國際公約、各國執法權限以及跨國保安合作的整體性戰略任務，此現象顯示技術層面之導航異常可能進一步影響管理決策效率與海事治理能力。

3.3 GPS 脆弱性：訊號干擾(Jamming)與訊號欺騙(Spoofing)

相較於 AIS，GPS 系統之主要脆弱性來自於衛星訊號在抵達地表時功率極低，因此容易受到外部無線電訊號干擾或偽造攻擊。由於現代航運導航系統高度依賴 GPS 提供之定位資訊，一旦訊號遭受破壞，將直接影響船舶航行安全。

(一)GPS 干擾(Jamming)

GPS 干擾係指透過發射與 GPS 相同頻率之無線電訊號，以壓制合法衛星訊號，使接收器無法正常追蹤衛星或完成定位計算。干擾設備通常成本低且易於取得，使其成為最常見的導航攻擊方式之一。GPS 干擾對航運安全可能造成以下影響：

(1) 定位能力喪失：船舶可能失去精確定位能力，被迫依賴推算航法或傳統導航方式，增加操作負擔。

(2) 導航系統失效：現代船舶之 ECDIS、雷達整合導航系統及自動航行設備多仰賴 GPS 資料，干擾可能導致系統顯示異常或功能失效。

(3) AIS 功能受影響：由於 AIS 通常依賴 GPS 提供位置資訊，GPS 訊號失效將導致 AIS 位置報告不準確甚至停止更新。

(4) 擱淺與碰撞風險增加：在狹窄水道或高密度航運區域中，失去可靠定位資訊可能導致船舶偏離安全航道。

(二)GPS 欺騙(Spoofing)

GPS 欺騙則是透過發射模擬之 GPS 訊號，使接收器誤判自身位置或時間資訊。與干擾不同，欺騙攻擊並非阻斷服務，而是刻意誤導導航系統，使船舶在不知情情況下偏離原有航線。其主要影響包括：

(1) 導航誤導：船舶可能被引導至危險水域或偏離既定航道。

(2) 電子海圖資訊錯誤：當 GPS 資訊遭竄改時，ECDIS 所顯示之船位將產生偏差，導致錯誤決策。

(3) 系統信任下降：頻繁發生欺騙事件可能削弱船員對電子導航系統之信任，影響操作行為與決策模式。

3.4 AIS 與 GPS 脆弱性之關聯性

值得注意的是，自動識別系統(Automatic Identification System, AIS)與全球定位系統(Global Positioning System, GPS)在實際航行應用中並非獨立運作，而是存在高度的功能耦合關係。AIS 應答器所傳輸之動態資訊(如船位、航向與航速)多數係由 GPS 接收器即

時提供之定位結果所驅動，因此 GPS 所產生之導航資訊可視為 AIS 資料鏈的重要基礎來源之一。換言之，AIS 系統本身雖負責船舶識別與資訊交換，但其核心位置資訊之正確性高度依賴 GPS 的定位精度與穩定性。

在此架構下，一旦 GPS 訊號遭受干擾(Jamming)或欺騙(Spoofing)等攻擊，AIS 所廣播之船位資訊亦可能同步產生偏差或錯誤，進而造成多層次之連鎖影響。例如，錯誤的定位資訊可能導致船舶間態勢感知(Situational Awareness)失真，使船舶避碰決策、航路規劃以及岸基監控系統之判斷產生誤差。此外，港口交通管理系統(Vessel Traffic Service, VTS)及海上監控單位亦可能因接收到錯誤之 AIS 資料而做出不適當的監控或調度決策，進一步放大航行風險。

從系統工程角度觀之，此種 AIS 與 GPS 之相依性代表導航資訊鏈具有明顯之單點脆弱特性(Single Point Vulnerability)。當核心定位來源失效時，不僅單一導航設備受到影響，整體資訊交換與海上交通管理架構亦可能產生系統性失效，形成跨層級的風險擴散效應。因此，AIS 與 GPS 之脆弱性問題已不再僅屬於單一技術層面的安全議題，而應被視為涉及導航安全(Navigation Safety)與海事保安(Maritime Security)之系統性風險。

基於上述分析，建立多層次防護機制(Multi-layer Defense)與提升導航系統韌性(Navigation System Resilience)已成為當前海事安全領域的重要研究方向，包括多源導航資訊交叉驗證、異常行為偵測機制，以及備援定位系統之導入等措施，均可有效降低單一系統失效所造成之整體風險。

為更清楚呈現 AIS 與 GPS 系統之脆弱性差異及其對航運安全與海事保安之影響，本文整理如表 2 所示之比較分析。

表 2 AIS 與 GPS 系統脆弱性比較分析

系統	主要功能	主要威脅類型	攻擊機制	對航運安全影響	對海事保安影響
AIS	船舶識別與資訊交換	訊號欺騙 (Spoofing)	偽造 AIS 訊息、建立虛擬船舶	增加碰撞風險、造成錯誤態勢感知	掩護非法活動、誤導監控系統
GPS	定位與導航	干擾 (Jamming)	同頻訊號壓制	喪失定位能力、導航功能失效	航道偏移、進入高風險區域
GPS	定位與導航	訊號欺騙 (Spoofing)	偽造衛星訊號	船舶偏離航線、錯誤海圖定位	可被利用進行誘導或導航干擾
AIS + GPS(耦合)	綜合導航資訊	系統連鎖失效	GPS 異常導致 AIS 資訊錯誤	多層導航系統同步失效	整體海域監控能力失真

3.5 連鎖失效路徑與關鍵節點分析

在圖 2 所示攻擊面架構基礎上，現代海事導航與監控系統中之 AIS 與 GPS 並非獨立運作，而是透過多層次資料依賴關係共同支撐船舶導航、電子海圖顯示系統(ECDIS)及海上交通服務系統(VTS)等核心功能。此類高度耦合之資訊鏈結構，使得單一節點異常可能沿資料流與決策流程向外擴散，進而引發連鎖式安全風險(cascading risk)。

在上述模型下，典型之系統失效路徑可表示如下：

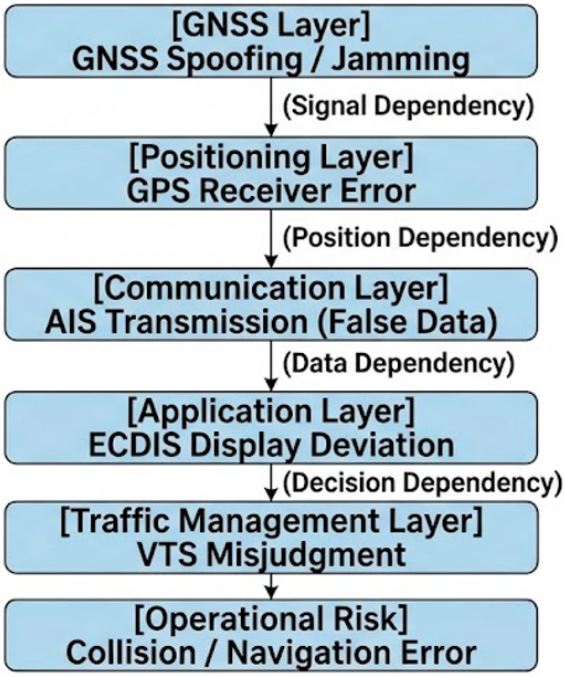

圖 3 AIS–GPS–ECDIS–VTS 系統之連鎖性失效傳遞架構示意圖(本研究整理)

如圖 3 所示，本研究所建構之多層級資料依賴架構可清楚呈現導航系統中錯誤訊號之傳遞路徑，並驗證連鎖性風險(cascading risk)之跨層級擴散機制。該連鎖失效路徑亦可視為一條沿有向圖 G = (V,E) 之關鍵傳遞路徑(critical propagation path)，其中各節點間之依賴關係對應不同類型之資訊依賴機制。

進一步而言，各層級之間之風險傳遞係透過不同類型之依賴關係所驅動，包括訊號依賴(signal dependency)、定位依賴(position dependency)、資料依賴(data dependency)及決策依賴(decision dependency)。不同依賴類型代表風險傳遞之機制差異，亦影響異常擴散之速度與影響範圍。

此一過程顯示，底層訊號異常可透過資料依賴鏈逐層放大，形成跨系統之連鎖性風險。以 GPS 作為主要定位與授時來源而言，其訊號若遭受干擾(jamming)或欺騙(spoofing)，將直接影響船舶定位精度，導致導航系統輸入資料產生偏差。由於 AIS 通常

依賴 GPS 提供之位置資訊進行訊息廣播，GPS 異常將進一步造成 AIS 所傳輸之動態資料失真，使其他船舶與岸基監控系統接收錯誤航行資訊。此類錯誤資訊若未被即時識別，將可能導致海上交通態勢感知失真，增加碰撞風險與航道誤判之可能性。

此外，ECDIS 與自動導航系統高度依賴 AIS 與 GPS 所提供之資料進行航線規劃與風險評估，一旦上游資料遭受操控，電子海圖顯示之船位與實際位置可能產生偏差，使船員在未察覺異常之情況下作出錯誤導航決策。另一方面，岸基 VTS 系統亦依賴 AIS 數據進行交通監控與指揮調度，若資料來源遭到偽造，可能導致監控中心對海域態勢產生誤判，進一步放大風險影響範圍。由此可見，導航異常所造成之影響並非侷限於單一設備或單一船舶，而是可能透過資料耦合結構擴散至整體航運監控與管理系統。

在此有向圖(Directed Graph)架構中，GPS 接收器被視為核心節點，具備顯著的單點失效(Single Point of Failure, SPoF)特性 。一旦該節點遭受攻擊或發生異常，其影響將沿著資料流向上層系統遞延，進而衝擊整體導航與監控資訊的正確性 。因此，GPS 接收器之可靠性與安全性，對於整體海事導航系統韌性具有決定性影響。從系統工程角度觀之，此種單點脆弱性不僅代表技術層面之失效風險，更意味著現代航運資訊鏈在缺乏足夠冗餘設計與交叉驗證機制時，極易因核心定位來源異常而產生系統性失效。

值得注意的是，連鎖風險之特性在於其跨層級傳遞效應，即單一技術層面之異常可逐步演變為操作層與管理層之系統性風險。例如，GPS 訊號異常原屬技術問題，但其後續影響可能延伸至船員決策錯誤、交通管理失效，甚至演變為海事事故或保安事件。因此，AIS 與 GPS 之脆弱性不應僅被視為單一設備之技術缺陷，而應從整體海事資訊系統之角度進行評估。

因此，本研究所揭示之連鎖風險可被理解為一種由底層訊號異常驅動、經由多層級依賴關係放大之跨層級風險傳遞過程。

綜上所述，AIS 與 GPS 所形成之高度依賴架構，使現代航運系統在提升效率與透明度的同時，也增加了系統性連鎖風險的可能性。未來海事安全治理應強化跨系統異常偵測能力，建立多來源資料驗證機制，並提升導航系統之冗餘設計，以降低單點失效所引發之連鎖影響，進而提升整體海事導航系統之安全性與韌性。

3.6 地緣政治環境下之導航風險擴展

在南海與台海等地緣政治高度敏感區域，導航訊號干擾與 AIS 異常事件已逐漸成為灰色地帶行動之一部分。相關研究指出，該區域可能存在非傳統電子干擾與訊號操控行為，對 GNSS 定位準確性與 AIS 資訊可信度造成潛在影響。此類干擾不僅影響單一

船舶導航安全，更可能透過資訊鏈傳遞影響區域航行秩序與海上監管決策。然而，由於相關事件多涉及國安與軍事敏感資訊，其公開資料有限，亦反映出現行國際治理機制在資訊透明與跨國通報方面仍存在顯著不足。

相較於一般航運環境，此類高風險區域具有「高干擾頻率」與「低資訊透明度」之特徵。由於相關事件往往涉及國家安全與軍事敏感資訊，其公開資料相對有限，導致導航異常事件難以被完整記錄與系統性分析。

此一現象顯示，目前國際導航安全治理體系在「資訊透明」、「風險通報」與「跨國資料共享」方面仍存在明顯制度性缺口，亦突顯建立全球導航異常監測與通報機制之必要性。

此外，該類導航異常事件亦反映出現行國際治理機制在面對灰色地帶衝突與非傳統安全威脅時之不足，包括缺乏即時通報機制、跨國協調困難以及資訊透明度不足等問題。未來應建立更完善之國際合作平台與資訊共享機制，以提升對導航異常事件之監測能力與應變效率，進而降低其對區域航行安全之影響。

3.7 Spoofing/Jamming 案例分析

本研究選取波斯灣 GNSS 干擾事件作為代表案例，並依據本研究所提出之多層級架構進行分析：

(1) 技術層：GNSS 訊號遭干擾，導致定位誤差。

(2) 資料層：AIS 廣播錯誤船位資訊。

(3) 應用層：ECDIS 顯示偏移。

(4) 管理層：VTS 判斷錯誤。

此案例顯示導航異常具有明顯跨層級擴散特性，驗證本文所提出之 cascading risk 機制。

3.7.1 多案例比較分析

為提升分析深度與實證支撐，本研究進一步比較不同區域之導航干擾與欺騙案例，以探討其在系統層級與治理層面之差異。

本研究選取三個具代表性案例進行比較分析，包括：

(1) 波斯灣 GNSS 干擾事件、

(2) 2017 年黑海 GNSS spoofing 事件，以及

(3) 南海疑似導航訊號異常事件。

上述案例涵蓋不同攻擊類型(jamming 與 spoofing)、不同地緣政治環境及不同政策回應模式，具有良好之比較價值。

表 3 多案例 spoofing / jamming 比較分析

案例	攻擊類型	影響層級	對 VTS 影響	政策回應
波斯灣	Jamming	GNSS → AIS → VTS	高	通報機制 + 航安警示
黑海(2017)	Spoofing	GNSS → ECDIS	中	學術研究主導
南海	不明干擾	GNSS → AIS	高	資訊不透明

表 4 層級案例評估與半量化比較框架

案例	攻擊類型	主要影響節點	關鍵傳遞路徑	影響層級	風險擴散層數	是否影響 VTS	政策回應成熟度
波斯灣	Jamming	GNSS、GPS 接收器、AIS、VTS	GNSS → AIS → ECDIS → VTS	高	4	Yes	3
黑海 (2017)	Spoofing	GNSS、GPS 接收器、ECDIS	GNSS → ECDIS	中	2	No	2
南海	不明干擾	GNSS、AIS	GNSS → AIS	高	2–3	Yes	1

進一步而言，上述案例亦可對應本研究所定義之節點重要性(C_i)、路徑風險(R_p)與依賴權重(w_{ij})等指標。例如，波斯灣事件中 GNSS 節點具有高度 C_i，且其失效導致高 R_p之跨層級傳遞；而在黑海案例中，風險主要集中於應用層，顯示不同攻擊型態在風險傳遞結構上具有顯著差異。

為強化案例分析之系統性與可比較性，本研究進一步建立多層級案例評估框架，將各案例依據統一之分析構面進行比較，包括攻擊類型、影響節點、關鍵傳遞路徑，以及對海上交通服務系統(VTS)之影響。

此外，本研究引入半量化指標，以提升分析之客觀性與可操作性。其中，「影響層級」依據對航運安全之衝擊程度區分為高、中、低；「風險擴散層數」代表異常訊號在系統中所跨越之層級數量；「政策回應成熟度」則以 1 至 3 表示各案例中相關治理措施之完整程度(1 = 初步或不足，3 = 相對完善)。

透過上述標準化分析框架，不僅可清楚比較不同導航攻擊事件之影響差異，亦可進一步驗證本研究所提出之多層級連鎖風險模型在實務案例中的適用性。

3.7.2 跨案例比較分析

由比較結果可知，不同導航攻擊事件在影響範圍與政策回應上呈現顯著差異：

(1) 在攻擊類型方面，jamming 通常造成系統失效，而 spoofing 則可能導致更隱蔽且持續性的導航誤導，對決策系統造成更高風險。

(2) 在影響層級上，當攻擊影響擴展至 AIS 與 VTS 層級時，其風險將由單一船舶擴散至整體海域，形成系統性安全問題。

(3) 在政策回應方面，波斯灣案例顯示已建立較完善之通報與警示機制，而黑海事件則主要由學術研究揭露；相較之下，南海相關事件則因資訊透明度不足，使得風險評估與治理回應面臨困難。

上述案例分析顯示，各類導航攻擊皆可對應至本文所建構之 GNSS 層、AIS 層與應用層之多層級架構，進一步驗證本研究所提出之 cascading risk 模型具有良好解釋能力與適用性。

綜合上述案例分析結果可知，本研究所提出之多層級風險傳遞架構與相關指標，能有效描述不同導航攻擊情境下之風險擴散特性，並驗證其於實務案例中的適用性與解釋能力。

肆、政策因應與國際合作

隨著 AIS 與 GPS 系統在全球航運中之廣泛應用，其所面臨的訊號欺騙與干擾威脅已逐漸從單純技術問題，演變為涉及航運安全、海事保安與國際治理的重要議題。由於航運活動具有高度跨國性，單一國家難以獨立應對導航系統所帶來的風險，因此國際組織與各國主管機關逐步建立相關政策框架與合作機制，以提升導航系統之安全性與

整體航運韌性 [6]。目前相關治理措施主要可分為國際標準制定、技術規範協調以及各國實務執行三個層面。

4.1 國際海事組織(IMO)

國際海事組織(International Maritime Organization, IMO)作為全球航運安全與海事治理之核心機構，在建立 AIS 制度與相關安全規範方面扮演關鍵角色。IMO 不僅負責制定國際航運安全標準，也透過公約與決議方式推動各會員國落實相關規範。

在制度層面上，IMO 透過《海上人命安全公約》(SOLAS)強制規範特定類型船舶必須搭載 AIS 設備，包括所有從事國際航行之 300 總噸以上船舶、非國際航行之 500 總噸以上貨船，以及所有客船。此一規定顯示 AIS 已被視為現代航運安全的重要基礎工具，其目的在於提升船舶可視性、降低碰撞風險並強化海上領域意識(Maritime Domain Awareness)。

IMO 亦透過發布決議與操作指南來提升 AIS 的安全使用，例如 A.1106(29) 決議即針對船載 AIS 系統的操作原則與限制進行說明，提醒海員應理解 AIS 資訊並非絕對可靠，需結合其他導航工具進行判斷。此類指南雖非直接針對資安威脅，但已間接反映對系統脆弱性的關注。

隨著數位化航運與智慧船舶概念發展，IMO 近年逐步將海事網路安全納入治理重點，提出海事網路風險管理相關指引，要求航運公司建立風險評估與管理機制，以降低導航與通訊系統遭受攻擊之可能性。此趨勢顯示，導航安全已由傳統操作層面延伸至整體資訊安全治理。

4.2 國際航標組織(IALA)

國際航標組織(International Organization for Marine Aids to Navigation, IALA)在全球航標標準與導航服務技術協調方面具有重要地位，其所制定之技術建議與指導文件，對 AIS 系統之部署與運作產生直接影響。

IALA 透過發布各項技術建議與指南，協助各國航標主管機關建立一致性之導航服務標準。例如 IALA 指南 1082 提供 AIS 系統整體運作概述，涵蓋設備部署、資料管理與數據完整性維護等內容，有助於提升系統可靠性與資訊品質。

此外，IALA 推動之虛擬航標(Virtual Aids to Navigation, V-AtoN)概念，透過 AIS 訊號傳送航標資訊，使航標服務由傳統實體設施延伸至數位化環境。此一發展雖提升導航

靈活性，但同時亦凸顯 AIS 資訊安全的重要性，若相關訊號遭到惡意操控，可能對航行安全造成直接影響。因此，IALA 在相關建議中亦強調資料完整性與系統安全管理的重要性。

整體而言，IALA 透過標準協調與技術規範建立，有助於降低不同國家系統差異所產生的安全漏洞，進一步提升全球航運通訊環境之互操作性與安全性。

4.3 各國海事主管機關與其他因應措施

除了國際組織之外，各國海事主管機關亦在實務層面扮演重要角色，透過法規制定、風險通報與技術研發等方式強化導航系統安全。例如美國海岸警衛隊(USCG)即依據國內法規(如 33 CFR §164.46)對 AIS 使用提出具體要求，明確規範船舶設備類型與操作方式，以確保航行安全與資訊一致性。

此外，面對近年來多起 GPS 干擾與 AIS 欺騙事件，部分國家機構如美國海事管理局(MARAD)與英國海事貿易行動中心(UKMTO)亦定期發布風險警示與航安通報，提醒船員在特定高風險區域提高警覺，並採取多重導航確認措施。此類即時資訊發布機制，有助於降低航行風險並提升業界對導航威脅之認知。

在技術發展方面，各國政府與研究機構亦積極投入相關研究，以提升 GNSS 與 AIS 系統韌性，包括發展替代性導航系統、改良訊號驗證機制以及建立更先進之干擾與欺騙偵測技術。透過技術創新與政策管理並行，逐步形成多層次防護架構，以應對日益複雜之導航安全挑戰。

表 5 國際導航安全政策與監管措施比較

組織／機關	主要規範或文件	政策重點	是否直接涉及 spoofing / jamming	主要限制
IMO	SOLAS、公約決議	AIS 強制搭載、航行安全	間接涉及	缺乏具體技術防護要求
IMO	Maritime Cyber Risk Guidelines	網路風險管理	部分涉及	偏原則性指引
IALA	Guideline 1082	AIS 技術運作建議	間接涉及	非強制性
IALA	V-AtoN 建議	數位航標應用	間接涉及	資訊驗證機制有限
USCG / 各國主管機關	國家法規與通報機制	AIS 操作要求、風險警示	部分涉及	各國標準不一致

為了系統性地檢視全球海事社群對導航安全之治理邏輯，本研究針對主要國際組織、技術標準制定機構及國家級主管機關，就其所頒布之規章制度、技術指南及監管

機制進行綜合評比。透過對比各單位在法律位階、政策範疇及對新興威脅(如訊號欺騙與干擾)之關注程度，藉以揭示當前國際導航安全架構中的共同趨勢與潛在治理缺口，具體比較內容詳見表 5 所示。

伍、結論與建議

隨著全球航運活動日益依賴數位化導航與通訊技術，自動識別系統(AIS)與全球定位系統(GPS)已成為現代國際航運運作不可或缺之核心基礎。兩者透過即時資訊交換與精確定位能力，不僅有效提升船舶航行安全與海上交通管理效率，也大幅強化海上態勢感知與國際航運治理能力。然而，隨著技術高度普及與系統相互依賴程度增加，其潛在脆弱性亦逐漸浮現，特別是在訊號欺騙(spoofing)與訊號干擾(jamming)等非傳統威脅日益頻繁的背景下，AIS 與 GPS 系統所面臨的安全風險已成為全球海事安全領域的重要議題。

本研究透過對 AIS 與 GPS 技術特性及其通訊架構之分析，探討其在航運安全中的關鍵角色，並進一步檢視兩者在實際運作中所面臨之系統性脆弱性及其可能造成的航行風險。此外，本文亦從國際治理角度出發，分析國際海事組織(IMO)、國際航標組織(IALA)及各國海事主管機關在政策與監管層面所採取之因應措施，藉此呈現當前國際社會在面對導航系統安全挑戰時的治理方向與合作模式。研究結果顯示，AIS 與 GPS 的風險具有高度關聯性，單一系統遭受攻擊可能導致多層次資訊鏈失效，進而對整體航運安全體系造成連鎖性影響，因此提升導航系統韌性與建立多重防護機制已成為未來發展的重要方向。基於上述分析結果，為強化國際航運之安全與穩定，本研究提出以下政策與技術建議：

(一)增強導航系統韌性

建議船舶逐步採用多重全球導航衛星系統(Multi-GNSS)架構，整合 Galileo、GLONASS、BeiDou 等不同衛星系統，以降低對單一導航來源之依賴。此外，應積極發展與部署替代性定位、導航與授時(PNT)技術，例如 eLoran 或視覺導航等方案，以作為 GNSS 失效時之備援機制，提升整體導航可靠性。

(二)改進異常偵測與通報機制

面對日益複雜的訊號攻擊形式，應強化欺騙與干擾偵測技術之研發，並將相關功能整合至船載導航設備與岸基監控系統中。同時，建立標準化且高效率之事件通報流

程，鼓勵航運公司與船員主動回報導航異常狀況，以利主管機關及早掌握風險並進行資訊共享。

(三)強化國際合作與資訊共享

由於航運活動具有跨國特性，單一國家難以獨立應對導航系統威脅，因此應加強國際組織、政府機構、航運產業與研究單位之合作，共同制定應對 AIS 與 GPS 威脅之技術標準與最佳實務。此外，建立全球性威脅情報共享平台，有助於即時通報攻擊模式與防範策略，提升整體風險應對能力。

(四)提升船員培訓與操作意識

導航系統安全不僅仰賴技術層面改善，也需透過人員訓練加以強化。建議在船員培訓課程中納入 AIS 與 GPS 脆弱性相關內容，包括辨識訊號異常、系統失效時之應變程序，以及傳統導航方法之運用能力，以避免過度依賴電子系統所帶來之操作風險。

(五)持續完善國際監管框架

面對快速演變的導航威脅，IMO 與 IALA 等國際組織應持續更新相關規範與技術指引，推動更嚴謹之設備認證制度，鼓勵導入抗干擾與抗欺騙功能，同時明確規範船舶在遭受導航攻擊時之法律責任與通報義務，以建立更完善之治理架構。

綜合而言，AIS 與 GPS 系統之安全性已不再僅屬技術層面問題，而是涉及國際治理、產業實務與人員操作等多面向之整體挑戰。唯有透過技術創新、政策完善、國際合作與教育訓練等多管齊下之策略，方能有效提升導航系統韌性，降低航運風險，並確保全球海上運輸體系之長期安全與穩定發展。

參考文獻

1 Skuld. (2025, August 18). AIS spoofing and jamming in the Persian Gulf. Retrieved from https://www.skuld.com/topics/ship/navigation/ais-spoofing-and-jamming-in-the-persian-gulf-a-growing-maritime-security-concern/，瀏覽日期 2026/01/20。

2 USCG Navigation Center. (n.d.). AIS Messages. Retrieved from https://www.navcen.uscg.gov/ais-messages，瀏覽日期 2026/01/20。

3 Reselman, B. (2021, June 29). An architect's guide to GPS and GPS data formats. Red Hat Blog. Retrieved from https://www.redhat.com/en/blog/architects-guide-gps-and-gps-data-formats ，瀏覽日期 2026/01/20。

4 IMO. (2004, December 31). AIS transponders. Retrieved from https://www.imo.org/en/ourwork/safety/pages/ais.aspx，瀏覽日期 2026/01/20。

5 Bueger, C. (2015). What is maritime security? Marine Policy, 53, 159–164.

6 Cabigon, J. V., & Doorey, T. J. (2020). PHILIPPINE NAVY MARITIME SITUATIONAL AWARENESS SYSTEM: CURRENT SITUATION, GAPS, AND POTENTIAL ROLE OF MARITIME SPECIAL OPERATIONS FORCES (Doctoral dissertation). Naval Postgraduate School, Monterey, CA.

7 Lee, E., Mokashi, A. J., Moon, S. Y., & Kim, G. (2019). The maturity of automatic identification systems (AIS) and its implications for innovation. Journal of Marine Science and Engineering, 7(9), 287.

8 Mallam, S. C., Nordby, K., Johnsen, S. O., & Bjørneseth, F. B. (2020). The digitalization of navigation: Examining the accident and aftermath of US Navy Destroyer John S. McCain. Proceedings of the Royal Institution of Naval Architects Damaged Ship V, 55–63.

9 Thomas, A., & Chiego, C. (2022). Maritime Cybersecurity: AIS Manipulation Motivations in the Maritime Domain.

10 Wilhoit, K., Balduzzi, M., & Pasta, A. (2016). Vulnerabilities in the Automatic Identification System (AIS) for Maritime Security. Presented at HITB Security Conference.

11 Kpler. (2024, July 10). AIS spoofing in the maritime industry: A growing risk and compliance challenge. Retrieved from https://www.kpler.com/blog/ais-spoofing-in-the-maritime-industry-a-growing-risk-and-compliance-challenge，瀏覽日期 2026/01/20。

12 London Maritime Academy. (2025). AIS spoofing: What it is, how it works, and why it matters. Retrieved from https://www.lmitac.com/articles/what-is-ais-spoofing，瀏覽日期 2026/01/20。

13 Seatrade Maritime. (2023). Asian Maritime Security in Q4. Retrieved from https://www.seatrade-maritime.com/piracy/asian-maritime-security-in-q4-ais-spoofing-and-crimes-at-sea ，瀏覽日期 2026/01/20。

14 Kang, H., et al. (2019). Development of noise reduction techniques to enhance data quality in Automatic Identification Systems (AIS). *Journal of Marine Data Processing, 22*(3), 45-59.

15 Mazzarella, F., et al. (2015). The potential of AIS data as a tool to analyze ship behavior in response to meteorological conditions. *Marine Navigation and Safety of Sea Transportation, 11*(1), 157-164.

16 Ngai, E.W.T., et al. (2012). AIS-based system to reduce collision risks in maritime transport. *Journal of Transport Management, 24*, 85-100.

17 Jalkanen, J.P., et al. (2014). Application of AIS data to monitor and control ship emissions in the maritime sector. *Environmental Monitoring and Assessment, 186*(10), 6525-6539.

18 Pallotta, G., Vespe, M., & Bryan, K. (2013). Vessel pattern knowledge discovery from AIS data: A framework for anomaly detection and route prediction. *Entropy, 15*(6), 2218-2245.

19 Carson-Jackson, J. (2012). AIS based synthetic aperture radar: Detection and identification of maritime targets. *International Journal of Remote Sensing, 33*(5), 1473-1492.

20 Robards, M., Silber, G., Adams, J., Arroyo, J., Lorenzini, D., Schwehr, K., & Amos, J. (2016). Conservation science and policy applications of the marine vessel Automatic Identification System (AIS)—A review. *Biological Conservation, 205*, 93-103.

21 Zhang, M. H. (2002). Study on AIS (Automatic Identification System). *Journal of Navigational Technology*, 2002(4), 31-35.

22 Danu, D., Sinha, A., Kirubarajan, T., et al. (2007). Fusion of over-the-horizon radar and automatic

identification systems for overall maritime picture. *Proceedings of the 10th International Conference on Information Fusion*, July 9-12, Candan, 2007.

23 Wang, M. N., & Hu, J. W. (2007). Research on AIS-based automatic ship identification and its application. *Journal of Marine Engineering*, 2007(2), 129-132.

24 Lin, Z. Q. (2003). Optimization of AIS identity recognition efficiency based on multi-fuzzy logic synthesis technology. *Journal of Angel Maritime University*, 2003, 29(1), 43-46.

25 Lin, Z. M. (2002). Research on data fusion methods for effective AIS identity recognition. *Chinese Journal of Navigation*, 2002(1), 22-25.

26 Rudnik, P., Cuntz, M., & Meurer, M. (2025). Effectiveness of detection methods for GNSS spoofing signals in the Eastern Mediterranean airspace: A flight study. https://doi.org/10.1109/plans61210.2025.11028279

27 Mistrapau, F., Clopot, R., Kosjer, V., & Ciobanu, C. (2025). *Towards resilient PNT: Developing and testing the Riptide Black Sea demonstrator*. Retrieved from https://www.ion.org/publications/abstract.cfm?articleID=20225，瀏覽日期 2026/01/20。

28 Androjna, A., Perkovič, M., & Pavić, I. (2021). *Cyber security challenges for safe navigation at sea*. Retrieved from https://www.researchgate.net/profile/David-Brcic/publication/358671686_Proceedings_14th_Annual_Baska_GNSS_Conference_Technologies_Techniques_and_Applications_Across_PNT_and_The_1st_Workshop_on_Smart_Blue_and_Green_Maritime_Technologies/links/620e72eeeb735c508adb3928/Proceedings-14th-Annual-Baska-GNSS-Conference-Technologies-Techniques-and-Applications-Across-PNT-and-The-1st-Workshop-on-Smart-Blue-and-Green-Maritime-Technologies.pdf#page=48，瀏覽日期 2026/1/20。

29 Balić, M., Radoš, K., & Blazevic, Z. (2024). GNSS spoofing attack in real-time static and dynamic scenarios (pp. 1–6). https://doi.org/10.23919/softcom62040.2024.10721889

30 Spanghero, M., & Papadimitratos, P. (2024). POSTER: Testing network-based RTK for GNSS receiver security. https://doi.org/10.48550/arxiv.2405.10906

31 Romaniuc, A. (2025). *Contributions to the security of satellite navigation systems using machine learning techniques*. Retrieved from https://doctorat.utcluj.ro/theses/view/HPLVKSPuGwoUSrCcLDqEXfcW9RjhPW3LeIOe1puZ.pdf，瀏覽日期 2026/01/11。

32 Farah, M. A. B., et al. (2022). Cyber security in the maritime industry: A systematic survey of recent advances and future trends. *Information, 13*(1), 22. https://doi.org/10.3390/info13010022

33 Marine Public. AIS Complete Guide: How It Works & Maritime Regulations. Retrieved from https://www.marinepublic.com/blogs/training/872993-ais-complete-guide-how-it-works-maritime-regulations ，瀏覽日期 2026/01/11。

34 國際海事組織(International Maritime Organization, IMO)，網址：http://www.imo.org ，瀏覽日期 2026/01/11。

35 國際航標組織(International Organization for Marine Aids to Navigation, IALA)，網址：http://www.iala-aism.org ，瀏覽日期 2026/01/11。

36 國際電信聯盟(International Telecommunication Union, ITU)，網址：http://www.itu.int ，瀏覽日期 2026/01/11。

37 國際海上人命安全公約 1974(Safety of Life at Sea 1974, SOLAS)，網址：https://www.imo.org/en/About/Conventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx ，瀏覽日期 2026/01/12。

38 VHF - Very High-Frequency，網址：https://en.wikipedia.org/wiki/Very_high_frequency ，瀏覽日期 2026/01/12。

39 自動識別系統 AIS - Automatic Identification System，網址：https://en.wikipedia.org/wiki/Automatic_identification_system ，瀏覽日期 2026/01/11。

40 人工智慧 AI - Artificial Intelligence，網址：https://en.wikipedia.org/wiki/Artificial_intelligence ，瀏覽日期 2026/01/12。

41 物聯網 IoT - Internet of Things，網址：https://en.wikipedia.org/wiki/Internet_of_things ，瀏覽日期 2026/01/12。