AIS假資訊之威脅與因應

海洋委員會自行研究報告

中華民國 113 年 11 月

AIS假資訊之威脅與因應

單位：海巡署教育訓練測考中心

研究人員：

于青雲 劉郁婕 呂佳龍

幸祠淵 曾柏瑋 黃祥閔

海洋委員會自行研究報告

中華民國 113 年 11 月

目次

AIS假資訊之脅因與威應

自行研究報告

表 次

圖 次

提要

一、研究緣起

近年來的海上案例顯示，AIS 假資訊及相關海上網域攻擊事件，已不再只侷限於常見的非法漁業、走私等議題，更延伸至軍事及執法等領域。類似狀況亦發生在我管轄海域內，例如近期便發現有大陸籍船舶冒用台灣地區識別碼或明明是我方遊艇，卻使用大陸地區識別碼在海上活動之情事，者些足以造成敵我不分之困擾，更對海域安全產生極大威脅。

二、研究目的

期盼經由本論文之研究成果，讓海巡同仁能系統化的認識到「AIS 假資訊」之危害及其延伸之威脅，並作為檢視及設計本中心各階段教育相關課程之依據。

三、研究方法及過程

(一) 本論文採用「文獻檢閱」、「案例分析」、「問卷調查」、「專家訪談」等研究方法，除廣泛蒐集國內外相關文獻外，並透過案例 (計 2010-2020 年國外 46 起海上網域攻擊事件及 5 起指標性事件)，從應然與實然之角度，檢視所欲研究的問題，同時也透過問卷調查及專家訪談，了解海巡學員，對船舶運用 AIS 進行不法行為態樣、模式及威脅等議題之看法，並藉由專家意見充實研究所見，不至於閉門造車。

(二) 過程

本研究參考系統理論，將研究過程區分為「資料及案例蒐整」、「資料處理及調整」、「研究產出」等階段。

四、重要發現及建議

(一) 重要發現

1. 在 AI 技術支援下，海上假資訊將更難於查證，應從「海上網域安全」的大格局，看待此一威脅所產生之挑戰。
2. 就案例所見，海上假資訊及海上網域安全事件，多可歸咎於「便宜行事」使然，故制定「網域衛生政策」(Cyber-hygiene policy) 有其迫切需要。

3. 問卷調查顯示，高達 84% 的學員(均為日後各階層領導幹部)不知道 AIS 假資訊是如何產生的，必須強化在職訓練。
4. AIS 銷售商為牟利起見，罔顧 IMO 規定，向客戶提供後門程式，使船方能製造假資訊，專家表示透過立法禁止，應有助於減少假資訊氾濫。

(二) 建議

1. 教育訓練
   (1) 透過師資、教材、建置海上假資訊教學模擬軟體設備及與時俱進的課程規劃，補強現行在職訓練機制不足之處。
   (2) 各分署應調派適員參加本中心機動輔訓，避免出公差性質，以提升同仁專業能力。
2. 法律

   透過立法程序，強制 20 噸以下之動力載具應加裝 AIS，以利建立海域空間透明度之優勢。
3. 勤務
   (1) 除建立正確心態之外，更要營造具有時刻提醒慎防假資訊之環境(例如第六巡防區的作法可為借鏡)。
   (2) 運用 AI 技術，建立海上假資訊辨識機制，以輔助巡防區勤務作業。

關鍵詞：認知戰、網域攻擊、海域空間透明度、Cyber-hygiene、Fake AIS

第一章　緒論

第一節　前言

壹、發展背景

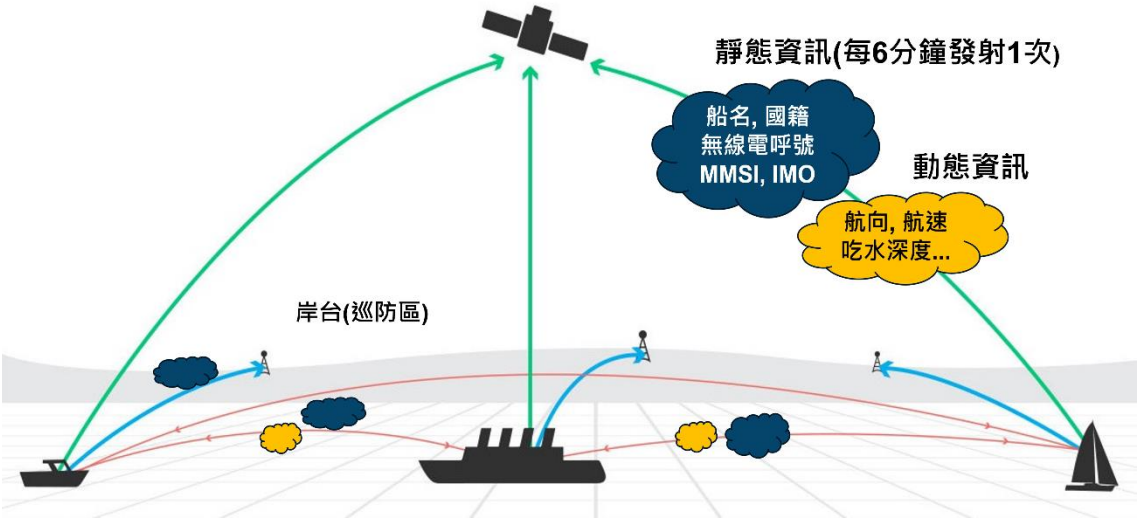
自 2002 年起，國際海事組織 (International Maritime Organization, IMO) 基於增進船舶航行安全之目的，與國際電信聯盟 (International Telecommunication Union, ITU) 合作開發「自動辨識系統」(Automatic Identification System, AIS) 並制定軟、硬體架構及通訊協定 (Protocol)。後續更在海上人命安全公約 (Safety of Life at Sea, SOLAS) 第 5 章，增加強制船舶裝設 AIS 之規定，使其運用取得法源依據。於 2008 年 7 月起，成為往來國際水域大小船舶所必配之航儀設備之一；而公約附帶的其他規定及 IMO 相關決議案，則具體規範了AIS 的操作方式、限制、資訊內容及數據交換協議等，逐漸形成現行的國際制度。就設計目的而言，AIS 可透過 VHF 無線電，利用專屬頻道 (計有 87B, 88B 二個頻道) 向外發射本船航行資訊，以利其他船舶、沿海國船舶動態監控中心 (以下稱 VTS 中心)[1] 識別本船身分及掌握航行動態，當所有船舶都在做相同動作時，各方行為者便能知道彼此所在位置及動態，藉此降低海上碰撞風險，且能強化各沿海國 VTS 中心掌握轄區海域內大小船舶動態之能力，所以 AIS 的資訊內容必須是真實數據，不允許偽造或錯誤輸入，故又稱為「榮譽式系統 」(Honor system)。

AIS 資訊分為靜態與動態兩種，前者為船舶身分識別依據，後者則隨航行狀態 (例如速度、航向等) 而改變 (如圖1-1)。理論上，AIS 可以減少船舶碰撞風險，增進航行安全，各國船舶理應積極擁護此一制度才對，但實際上，卻有許多裝設 AIS 之船舶，在航行時並未發射 AIS 資訊，究其原因幾乎都跟不法活動、意圖隱匿蹤跡或混淆視聽有關[2]，所以國際海事組織第 A.1106 (29) 決議案，強制要求船

[1] 沿海國依 IMO 規定，於岸際或港口所設置之船舶動態監控中心，該中心之軟、硬體設施及人員標準，都必須符合國際船舶交通服務規範的運作要求(Vessel Traffic Service, VTS)。

[2] Wawruch, R. (2017). Ability to test shipboard automatic identification system instability and inaccuracy on simulation devices. *Zeszyty Naukowe Akademii Morskiej w Szczecinie*, (52 (124), 128-134.

圖 1-1：AIS 資訊交流示意圖



舶在航行或錨泊時，都必須依規定，在間隔時間內發射 AIS 資訊，除非船長認為當前海域有航安顧慮，可以暫停 AIS 對外發訊 (必須登記在航行日誌)，其他航行階段都應保持 AIS 的正常發射；至於無線電接收範圍約在 30-50 浬不等，而收發訊效果則取決當時海象、天線高度及發射機的功率強度等因素。上圖所示，為 AIS 資訊交流之過程，當某船發出 AIS 資訊後，其週邊船舶及 VTS 中心都可接收到資訊，同時也可傳至低軌道衛星(Low Earth Orbit, LEO)，作為大區域船舶動態監控之依據，許多海事資訊服務公司(如 Findship, Fleetmon, MarineTraffic 等) 就是利用地面 AIS 接收站、衛星所獲得之相關數據，針對全球船舶的活動狀況進行大數據分析，並以使用者付費方式，提供各種客製化船舶資訊服務 (例如可依據客戶要求，於發現聯合國制裁名單內的船舶出現指定海域時，便立即通知客戶)。

貳、問題與威脅

儘管 AIS 設計立意良善，但科技本身就是一把雙面刃，不論行為者之動機良善與否，都能使用 AIS 逞其所欲，由於這套系統係著眼於減少船舶碰撞、提升船舶航行安全之需要所設計，在兼顧時效 (盡早掌握周邊船舶動態、身分) 及方便各國廠商開發與 AIS 資訊相容之其他航儀 (例如 VTS 雷達) 之要求下，具有「使用公

圖 1-2：船舶 AIS 資訊與 VTS 雷達之融合畫面

開之收發頻率」、「資訊內容不加密 (即明文顯示資訊原始內容)」、「開放性軟硬體架構 (例如資訊格式、交換方式及字數限制等)」三大開放性特色，也正因為如此， VTS 雷達才能在收到某船 AIS 資訊後，直接在螢幕上顯示其 IMO 碼[3]、MMSI 碼[4]、無線電呼號(Call sign)[5] 及船名等四大基本身分資料，圖 1-2 的 AIS 接收天線(紅圈所示)，於收到海上船舶發出的資訊後，送入轉換器並和納入雷達目標回跡(光點)[6]，只要雷達操作員將游標移至該光點，即可顯示目標之身分訊息。

一、問題

在整合式電子航儀系統尚未普及化之前，船舶依賴各自獨立運作的雷達、無線電裝備、視 (聽) 覺裝備 (例如探照燈、笛號或霧號等)、人力瞭望等方式維持航行安全，由於分工與專業不同，因此每一個航行值班的人數都較多，可在不同部位監控海面動態，相對提高航行安全。隨著整合式航儀系統普及化之後，船舶航行應當更加安全才對，但海難事件仍時有所聞，例如 2014 年 10 月海研五號 (於澎

[3] IMO 碼為英國HIS Maritime & Trade公司所研發之船舶身分辨識系統，是船舶永久身分碼 (7位數)，其功能如同民眾的出生證明，不因轉賣或變更國籍而改變，從2013年起開放漁船申請，凡是船身長12公尺或排水量超過100噸以上的漁船， 不論材質均須申請 IMO 碼，以便各區域性漁業組織識別漁船身分。

[4] MMSI 碼為船旗國所核發之國籍證明(，其功能如同民眾之護照。

[5] 為船舶的無線電呼叫號碼，其作用如同民眾使用的電話號碼。

[6] 雷達發現目標後所反射的回波，投射在雷達螢幕上以光點顯示目標之存在。

湖龍門海域沉沒)、2016 年 3 月德翔台北貨輪 (於石門海域擱淺造成油污染最終拆解)、2023 年 12 月巡護九號 (在澎湖七美海域與國籍貨輪發生碰撞) 等事故中，都有一定程度人為因素可以歸咎，畢竟操作航儀系統的是人，一旦人出了問題 (例如過勞、未按時保養裝備、人員證照過期等)，便會影響船舶安全，而這種影響往往是多面且互為牽動，近年來船員或駭客蓄意操縱 AIS 進行各類欺騙或隱匿數位(碼)足跡 (Digital footprint)[7] 的案例與日俱增，船舶以「假身分航行、不顯示目的地、全程關閉 AIS、對外顯示假位置」等現象，已不侷限於商、漁業海上活動，甚至已出現在軍事或執法等活動上，讓「利用 AIS 發射假資訊之欺騙行為」 (以下稱 AIS spoofing) 成為海事安全的重大議題，更被部分戰略研究者視為是認知作戰的型態之一。

假設圖1-2 所示之船舶遠在24浬外，在無法目視驗證之下，雷達操作人員只能從螢幕上所顯示的 AIS 資訊進行監控，但螢幕上的資訊，都是他方船舶所提供，在資訊內容操之於人的狀況下，我們顯然處於資訊不對稱劣勢，所以主筆作者於參與海巡署巡防區年度測考或授課時，必然會協助同仁建立以下基本認知：

(一) 如何確認船舶身分真假？(有可能是冒用他船身分航行)

(二) 雷達螢幕上的光點是否為實際存在的目標？(有可能是駭客置入的假目標)

(三) 光點若是目標的話會是怎麼樣的船？

(四) 一個光點真的是一艘船？或二艘併靠在一起的船？

(五) 雷達光點的位置和目標真正的船位有無誤差？

(六) AIS 資訊所顯示的 MMSI 碼有無多船共用一碼之狀況？

二、威脅

幾乎每一個沿海國在維護海域治安的工作上，都要面對以上問題所帶來的挑戰，鑑於海洋的遼闊與開放性，每日出沒的大小船舶眾多，更不乏有非法份子進

[7] 係指船舶在航行過程中，使用網路或無線電通訊時所留下的信號，足以讓其他方循線追蹤其動態，就如同民眾瀏覽網頁時，網站要求瀏覽者接受cookie (可儲存瀏覽紀錄方便下次搜尋)是相同道理，所以在數位世界活動，只要走過必留下足跡。

行各種 AIS spoofing 行為，真的很難做到毫無罅隙的海防標準，由於 AIS 的三大開放性特色，讓不法者皆可透過網路或在本機上操作的方式，輸(植)入假數據 (如裝載貨物、下一抵達港口等)，然後再向外發送，以達到掩蔽本船航跡或製造假目標 (所謂之Ghost ship) 混淆視聽之目的。研究小組將 AIS 問題 (因人為操縱) 所產生的威脅，歸納為傳統與非傳統二個面向 (如表1-1)：

(一) 傳統安全

就動機而言，AIS spoofing 行為目的，在影響敵對方決定國家安全或軍事議題之決策走向，例如在某國實際控制海域，製造敵方軍艦出現或滯留的數位足跡企圖製造恐慌心理、或在一個非核國家的領海製造一艘核動力船舶的 AIS 資訊。

(一) 非傳統安全

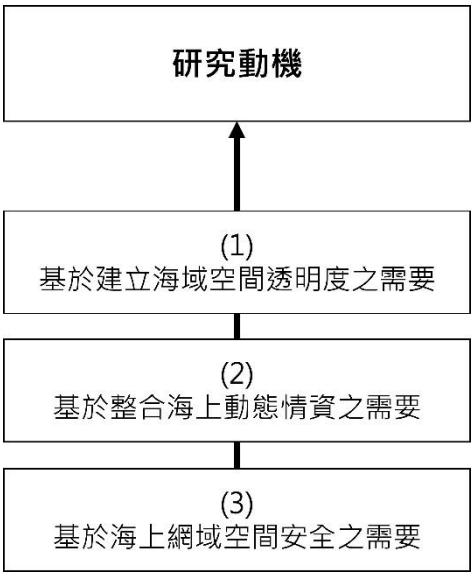
經歸納案例後，研究小組將出現在非傳統安全領域的 AIS spoofing 行為，區分為海洋經濟活動等五類，其中最常看到的便是違法捕撈，尤其是「非法、未經許可即不受節制」(Illegal, Unreported, Unregulated, IUU) 及闖入海洋保育區違法作業等，至於近年頻頻出現的海上接駁非法交易，則是常見的犯罪模式，這類的欺騙態樣多以關閉 AIS 為主，其次則是有心人士為掩護不法活動，安排船舶於偏遠海域故意發射遇險信號，引誘海上巡邏艦艇前往該處，造成責任區執法真空以逞不法企圖。

表 1-1：人為操縱 AIS 所形成之威脅

面向	受威脅領域
傳統安全 (Conventional security)	☑ 軍事 ☑ 海域秩序及執法
非傳統安全 (Non-conventional security)	☑ 海上交通管理 ☑ 海洋保育 ☑ 人命安全 ☑ 海洋環境保護 ☑ 海上經濟活動

第二節　研究動機與目的

壹、研究動機



一、建立海域空間透明度之需要

海域空間透明度 (Maritime Space Transparency, MST) 是完善海域執法的一項重要前提，最直接的說法就是，海域執法機關必須掌握，在我方管轄海域內所有的船舶動態，並能有效辨識其身分真假，換言之，海巡機關必須有能力接收和辨識 AIS 資訊內容真偽，同時也能掌握不明身分船舶之動態，這種能力就是所謂的 MST。

二、基於整合海上情資之需要

船舶在航行或錨泊時，都必須依規定，在間隔時間內發射 AIS 資訊，以利外界識別並採取必要之避碰措施 (如調整航向等)，雷達雖可發現船舶行蹤並進行動態監控，但其功能有可能會因電磁干擾、環境(如大雨)或人為操作不佳、目標判讀錯誤等因素而受到影響，由於船舶始終處於「移動」狀態下，所以結合雷達情資、AIS資訊顯示、海域水文狀況(如深度、潮流、海底質地等)、甚至目標查證等，才能滿足整合動態情資之需要。

三、基於海上網域安全 (Maritime cybersecurity) [8]之需要

駭客可經由網路從任何地方侵入某船或某 VTS 中心之 AIS 主機，強制接管並指使 AIS 進行各種欺騙行為；另一方面，由於現代船舶的管理與運作已經離不開網路作業方式，所以一旦駭客侵入 AIS 主機後，便有可能透過植入病毒或木馬程式等手段，破壞或監控與之連線的其他航儀系統，這種因為網路所形成之安全漏洞對海上船舶安全及海域監控均會造成極大之威脅，以下兩個案例類型即可一窺當前海上網域安全所面臨的威脅：

(一) 駭客侵入全球導航系統發送刻意加大誤差之 GPS 信號

2017 年至少約有 20 艘的各式商船在靠近黑海南部活動時，陸續發生導航系統所顯示的船舶當前位置和經緯度位置，出現極大誤差情況 (部分船舶的誤差甚至達到32公里)，此一事件顯然是駭客侵入全球導航系統[9] 傳送刻意加大誤差之 GPS 信號所造成[10]。

(二) 駭客侵入港口管理當局導致暫時失能事件

2018年7月、9月在美國的長堤港、聖地牙哥港，分別傳出工作人員點開駭客寄送電子郵件，啟動夾帶之 Ryuk 勒索軟體，將內部所有檔案強制加密而無法運作之事件[11]。

---

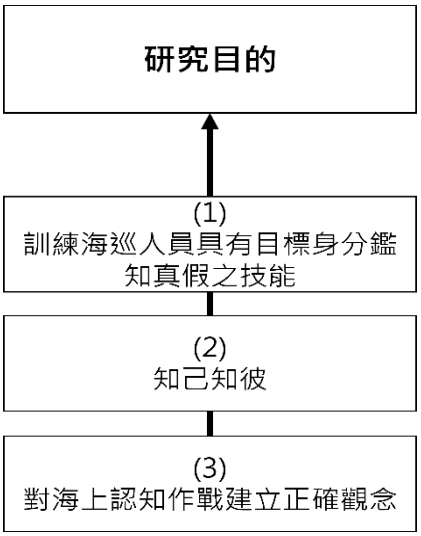
[8] Cyber 是指由整個網際空間，此一空間由不同條件、元素或軟硬體所組成，我們常說的網路只是工具之一，故本文稱為網域安全而非網路安全，因為前者已包括後者。

[9] 所謂的全球導航系統是一個統稱，它包括了美國GPS(我們最常聽到的系統)、俄國的格洛納斯系統(GLONASS)、中國大陸的北斗衛星導航系統(BDS)、歐盟的伽利略定位系統(Galileo)等。

[10] Polychronis, K.: Cybersecurity at Sea. In: Otto, L. (ed.) Global Challenges in Maritime Security. p. 243 Springer International Publishing (2020)

[11] Cimpanu, C.: US Coast Guard discloses Ryuk ransomware infection at maritime facility, 529 https://www.zdnet.com/article/us-coast-guard-discloses-ryuk-ransomware-infection-at-maritime-facility/, last accessed 2021/04/25

貳、研究目的



一、訓練海巡人員具有鑑知目標身分真假之技巧

基層人員流動率相對高，再加上升遷、受訓等必要之經管歷練，因此必須特別重視工作經驗傳承，尤其是涉及海事科技的部分，本研究案目的之一，便在經由系統化之資料蒐集、分析及案例比對方式，讓各級人員都能清楚理解 AIS spoofing 行為之態樣、模式及執行方式，有效掌握鑑知目標身分真假之技巧，避免被不法份子所矇騙 。

二、知己的同時也要做到真正的知彼

此處所稱之知己，指的是海巡人員對海域偵蒐系統 (主要是雷達) 軟硬體限制之了解，知彼則是當雷達螢幕出現可疑目標回跡之後，如何依據其 AIS 資訊研判是否為真？在資訊內容不全之狀況下，如何利用外界相關網站所提供之公開資訊進一步推敲其身分？

三、建立海上認知作戰之正確觀念

認知作戰是近年興起的名詞，主要是透過製造、散播或引領議題方式，讓民

眾相信假資訊進而做出自認為正確之行為[12]，某些國家甚至已將認知作戰當作是一種策略性工具。AIS spoofing 行為亦具備相同特性，其手法便是用假資訊達到欺騙(敵)之目的，所以北大西洋公約組織 (第二次世界大戰後西方陣營所成立的軍事同盟組織)及英國都將 AIS spoofing 行為視為海上認知作戰的範疇，而後者更將其納為海軍正規戰術的輔助措施，考量不法份子或敵方運用 AIS 假資訊干擾我方海域監控作業或透過網域攻擊，都是極有可能的手段之一，故研究小組才會帶入認知作戰之概念，期盼能藉由本研究案的發現，建立海巡同仁對此議題之正確認知。

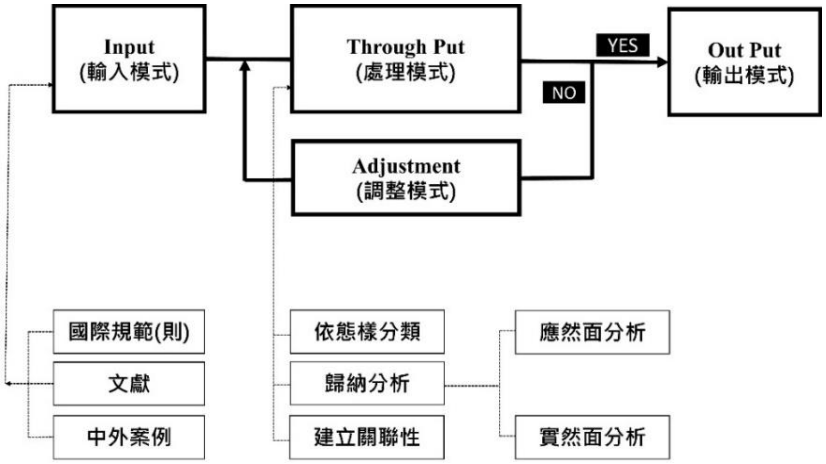
[12] Claverie, B., & Du Cluzel, F. (2022). "Cognitive warfare": The advent of the concept of "cognitics" in the field of warfare. *Cognitive Warfare: the future of cognitive dominance*, 2-1.

第三節　研究架構、方法與限制

壹、研究架構

鑑於研究主題與海域執法、相關部門對船舶動態監控資訊之分享與應用有關，主筆作者採用「系統理論」(System Theory)[13]作為本研究之架構，並以該理論的「輸入」(Input)、「處理」(Through put)、「輸出」(Output)及「調整」(Adjustment) 等模式進行研究。

圖 1-3：研究架構



一、輸入模式

跟研究主題有關的資料，包括「AIS 國際應用規定與決議案(以IMO制定為主)」、「AIS spoofing 期刊文獻」、「中外案例」(以上均稱為 Raw Data) 等，透過分工方式，由研究小組成員負責研讀並摘錄重點。

二、處理模式

本模式旨在經由每月一次之小組研討會，進行 Raw Data 研讀重點報告，並由

[13] 黃昆輝、張德銳、斐元領.(2000年12月).系統理論模式(System Theory Model).(國家教育研究院)2018年2月28日，擷取自雙語詞彙、學術名詞暨辭書資訊網：http://terms.naer.edu.tw/detail/1305926

研究計畫主持人進行總結，從案例角度檢視各成員提報內容並提出建議及編撰重點，藉此建立章節內容之關聯性，避免方向錯誤。

三、調整模式

人員於完成各章節初稿後，須納入小組研討會提出報告，同時依問卷調查(設定以113年度學資班隊為問卷對象)[14] 回收有效樣本之意見，進行必要修改。

四、輸出模式：即經由調整模式所得到之研究成果。

貳、研究方法

鑑於AIS spoofing 行為態樣的多元化，而且其影響層面幾乎涵蓋所有跟船舶有關之活動，更遑論涉及到當前各國高度關切的「海域網路安全(Maritime cybersecurity)」、「認知作戰 (Cognitive warfare)」等議題領域，因此在選用研究素材上，除以相關期刊文獻及中外案例為對象外，主筆作者將透過「歸納途徑」(deductive approach) 理解所欲探討的問題，過程中採用以下 4 種研究方法：

一、文獻檢閱

研究小組成員利用 Google scholar 學術性資料庫輸入 AIS spoofing、Fake AIS、Maritime Cybersecurity 等關鍵詞，搜尋自 2010-2020 年間與本研究主題相關之文獻，經小組成員檢視後，擇列出46起海上網路攻擊事件(如附件1)，至於跟 AIS 運用及管理方式之國際法規依據，則以國際海事組織、國際電信聯盟所制定之規定或決議案 (Resolution) 為主，具體作法則是透過「閱讀與整理」、「描述」、「分類」、「詮釋」等步驟進行分析。

二、案例研究

案例是真實呈現主事者，當時處理該事件或狀況的紀錄，每一個案例都有成

[14] 海洋委員會海巡署教育訓練測考中心學資班隊，係指學員為晉升上一級職務所開設之短期訓練班次。

功及失敗的關鍵因素，可作為後來者處理類似狀況時之參考依據。有感於 AIS spoofing 行為已對海域網路空間安全構成嚴重威脅，在缺乏相關機關(構)系統性研究之下，遂從案例著手，從應然及實然面理解 AIS spoofing 行為的動機、發生模式、危害程度，當有助於找出對應之策，研究小組所選用案例如下：

(一)指標性案例

時期	發生地點	案由	利用 AIS 之欺騙手法
2014	厄瓜多	2014年10月發生在格拉帕哥(Galapagos) 海洋保護區的非法漁撈事件	在岸際雷達偵蒐範圍外關閉 AIS 隱蔽航跡 (Go dark)
2017	台灣南部	國王之路號貨輪 (聯合國禁止入港之船舶) 滯留事件。	不斷變換身分混淆視聽以躲避雷達監控 (Identity switching)
2017	麻六甲海峽	二艘美國海軍驅逐艦因關閉 AIS 被商船撞毀事件。	關閉 AIS 成為不明目標 (AIS off)
2019	澎湖台灣灘	不明身分船舶發射假遇險信號。	調虎離山 (製造執法空窗期)
2022	黑海	駭客製造幽靈船恐嚇俄羅斯黑海艦隊	製造不存在之目標形成威脅 (Ghost ship)

(二) 2010-2020年海上網域攻擊事件

依據海事情報資訊廠商 Windward 公司之統計顯示[15]，不法份子透過網路進行 AIS spoofing 欺騙之行為模式，從2015年以後出現複合式手法，不單單只是常見的散播假資訊、隱匿蹤跡或關閉 AIS 等模式，還多了植入惡意軟體(例如2011-

[15] https://windward.ai/blog/gns-manipulation-2-0-practice-makes-perfect/

2013年重創南韓及日本海運業的 Icefog、2017 年造成航運巨人 Maersk 重大損失的 NotPetya、2018年癱瘓美國聖地牙哥港運作的 Ryuk 等勒贖軟體)和所謂的「衛星定位信號操縱」混和搭配運用，因此上述提到的46起海上網路攻擊事件足可作為實務上之分析對象。

(三) 問卷調查法

採用問卷調查法，統計海巡署教育訓練測考中心 2024 年各學資班隊受訓學員對「船舶運用 AIS 進行不法行為」態樣、模式及威脅等議題之看法及理解程度，由於學員均來自海巡署各單位，且至少都有 3 年以上工作經驗，因此所獲得之回饋，對提出問題解決對策(教育及實務訓練部分)，具有重要參考價值，具體作法如下：

1. 由研究小組專責人員，依全體成員共識下所訂定之問題，製作成問卷，並利用紙本或 以 Google 表單方式向，受訪者進行不記名問卷調查，使受訪者可於網路上作答，針對回收之有效問卷進行統計，以供研究小組運用並納入研究發現與建議。

2. 問卷對象

(1) 第 23 期海巡研究班(取得少校晉升中校之學歷)：學員26人。

(2) 第 40 期軍官正規班(取得上尉晉升少校之學歷)：學員49人。

(3) 第 27 期士官正規班(取得上士晉升士官長之學歷)：學員43人。

(4) 第 40 期海巡士官班(取得上等兵晉升下士之學歷)：學員46人。

(四)專家訪談

為從不同角度了解 AIS 科技發展及應用，經洽國內大小製造商，僅獲全科綜電股份有限公司 (WWW.ALLTEKMARINE.COM) 總經理同意，接受研究小組訪談，針對使用 AIS 的限制、不法運用模式、如何運用科技反制假資訊等議題進行專訪，以作為研究建議之參考。

參、研究限制

一、除少部分案例係出於主筆作者，以往任職前海岸巡防總局、金馬澎分署勤務指揮中心時期 (115年11月迄118年6月) 所處理過之案件外，118年以後之相關案例，均因涉及雷達運用、雷情分析等敏感性無法得見全貌，故大部分之案例仍以國際期刊文獻為研究題材。

二、參考文獻多取自 Google scholar 或 Researchgate.net ，由於本研究案並無單位預算支援，故部分重要文章無法購得，因此只能透過摘要，概略了解文章內容。

第二章　文獻檢閱

第一節　AIS 假資訊之應然與實然分析

研究小組於 112 年 12 月成立時，即有成員認為，從一線勤務作業之角度，海巡同仁最常聽到、也最熟悉的名詞莫過於「非法漁業、走私、偷渡」，若能將研究重點放在跟這些相關的案例上，當更能引起共鳴。對此論點，主筆作者認為，海巡五大核心任務所面對是各種海上狀況 (上述議題都只是其之一而已)，不論是哪一種的海上不法活動，都要用到船舶或飛行器，若只聚焦在同仁熟悉的議題上，恐怕研究結果會有「見樹不見林」之憾；而且隨著 COVID-19 結束後，國際局勢快速演變，不同陣營壁壘分明，尤其在 2022 年 2 月 24 日，俄烏戰爭開打後，認知作戰 (Cognitive warfare) 迅速成為各方話題，雖說國際社會對於認知作戰定義眾說紛紜，但許多研究者皆認為認，知作戰的主要手段，是透過散播不實、假造的資訊或利用網紅、名嘴等工具，引導議題風向進而達到掌握輿論之目的[16]，所以「打假」便成為反認知作戰的重要主題。事實上，海域空間 (Maritime domain) 也同樣存在著假資訊的問題，在近年的案例中，只要航行在海上的船舶多半都會採用第一章所提到的 AIS spoofing 行為，只是程度和手段之差別而已，綜合考量之餘，本論文研究重點決定放在「AIS 假資訊之威脅與挑戰」。

壹、為何要操縱 AIS 散播假資訊？

AIS 是為了降低船舶碰撞風險所開發之航行輔助系統，讓船舶在航行或錨泊階段，都能清楚「知道」彼此動態，其訊號接收及發射範圍會因天氣、海象、天線設置高度等因素而改變，一般而言約在 30-50公里之間。目前 AIS 已能和網路、無線電通訊、電腦、雷達，全球衛星定位系統、測深儀、電羅經等航儀信號銜接，形成一個整合式航行輔助系統，可對外發送本船航行動態資訊，如果所有航行船舶都能按規定使用的話，則對於海上航行安全、船舶動態掌握，可提供更佳

[16] Claverie, B., & Du Cluzel, F. (2022). "Cognitive warfare": The advent of the concept of "cognatic" in the field of warfare. *Cognitive Warfare: the future of cognitive dominance*, 2-1.

的保障[17]，然而實際狀況卻非如此。利用 AIS 發布假資訊或進行欺騙活動的行為者幾乎遍布各層面，各有不同動機，本文將之分為經濟及非經濟二種。前者為典型的「殺頭生意有人做、賠錢買賣無人做」，不法行為者在海上進行貿易時，為降低被發現風險必然會採取「隱匿航行蹤跡不讓外界發現」、「冒用他船身分從事不法勾當以便嫁禍他人」、「以身分不明的方式進行海上不法活動」等手段[18]，就主筆作者服務經驗所見，在台灣所轄海域，最常見到的不法態樣，無非是大陸籍船越界作業、漁民走私、盜採海砂等，這些不法活動都在求取不當之利；至於後者則多半跟政治、海上秩序、治安或特殊目的有關，不法態樣從以往案例可歸納為以下：

一、偷渡

近年較多案例顯示海峽偷渡者多是台灣民眾，例如因故滯留大陸多年之台灣民眾偷渡金門後再轉返台灣、或台灣民眾因案偷渡至大陸。

二、軍艦透過電子信號偽裝成商船

軍艦除了關閉 AIS 不顯示身分外，為加強偽裝效果，於航行時通常只會開啟商用雷達，讓沿海國電子情報偵蒐單位收到雷達信號後，誤以為是商船。

三、民兵船

民兵船外型跟漁船極像(甚至就是漁船)，即使它發射 AIS 資訊表明漁船身分時，外界亦無從研判到底是民兵船還是漁船[19]。

綜上所述，不論是從經濟或非經濟面而言，所有的 AIS spoofing 行為，都會間接或直接涉及到國家安全、邊境管制、海上治安及人命安全等議題，很難區分到底是屬於傳統或非傳統安全範疇之內[20]，這是目前最為棘手的狀況。

---

[17] 張樹波、唐強榮，基於AIS資料的船舶異常行為檢測方法，人工智慧與機器人研究，2015，4(4): 23-31。

[18] Kontopoulos, I., Spiliopoulos, G., Zissis, D., Chatzikokolakis, K., & Artikis, A. (2018, August). Countering real-time stream poisoning: An architecture for detecting vessel spoofing in streams of AIS data. In *2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)* (pp. 981-986). IEEE.

[19] Kennedy, C. M., & Erickson, A. S. (2017). China Maritime Report No. 1: China's Third Sea Force, The People's Armed Forces Maritime Militia: Tethered to the PLA.

[20] Lynch, T. F. (2019). The Military and Alternative Security: New "Missions" for Stable Conventional

貳、誰在從事 AIS spoofing 活動？

廣義而言，只要跟海域活動有關或依賴海事資訊營運的各行各業，都有可能是行為者，差別在使用手段及程度輕重而已。例如航商對所屬商輪動態保密，可防止競爭對手通過分析我方貨輪 AIS 資訊，掌握物流走向，因此關閉 AIS 不讓外界收到我方船隊動態資訊，便成為最有效的手段之一。各國海軍及海巡機關之艦艇在航行時，也都會採取相同作法以防範敵人及不法份子掌握我方艦艇動態。這種自我隱匿的作法，有可能為自身的航行安全帶來風險，以下案例適足以說明一二。

2017 年美國海軍二艘神盾級驅逐艦 (USS Fitzgerald, USS McCain) 因遵守「不發射 AIS 資訊對外告知本艦動態」之政策，分別和商船發生碰撞事故，造成重大損失，前者於 6 月 17 日在東京灣外海和菲律賓貨輪 (ACX Crystal) 相撞，造成7位船員當場殉職，作戰系統幾乎全毀，後者則於8月21日在麻六甲海峽和賴比瑞亞籍貨輪 (Alnic MC) 相撞，造成動力系統嚴重受損及10位船員殉職 (以上案例已納入第四章進行分析)，所以利用 AIS spoofing 進行各種隱匿、欺騙或偽裝活動的

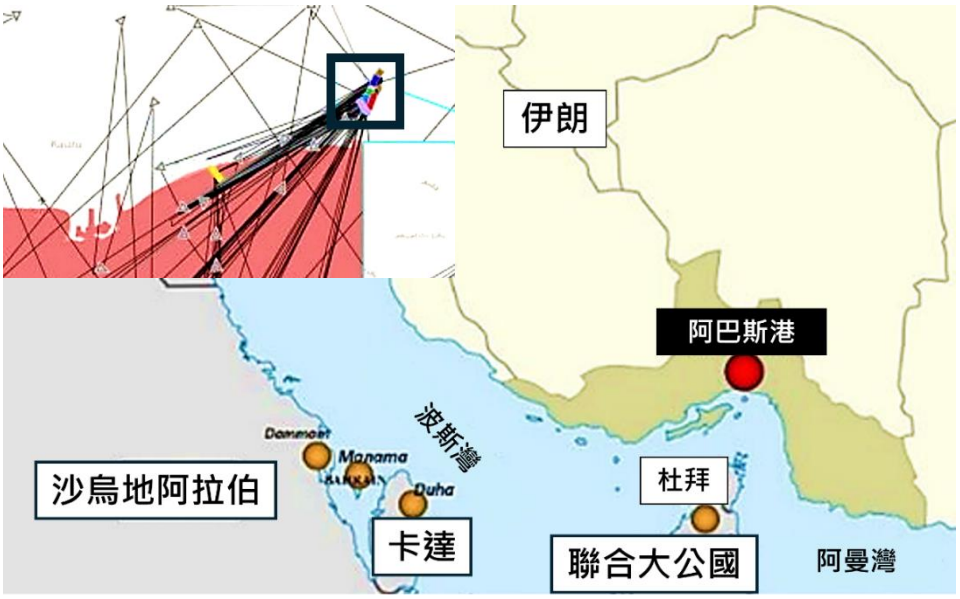
圖 2-1: 左為美艦 Fitzgerald 號、右為 McCain 號 (出處: CNN.COM)

同時，也必然會為自身安全帶來一定程度風險。從事 AIS spoofing 活動的眾多行為者中，國家級行為者 (例如俄羅斯、伊朗、朝鮮等) 也是經常被點名的對象，因為被聯合國制裁，民生受到重大影響，所以才更要透過各種利用 AIS 假資訊或駭

Security. In *Alternative Security* (pp. 7-42). Routledge.

客手法，掩護本國商船的海上動態。圖 2-2 是所示的阿巴斯港 (位於波斯灣荷姆茲海峽沿岸之城市) 是伊朗南部石油輸出重鎮，在聯合國持續多年的制裁下，阿巴斯港的商業活動可謂是門可羅雀，已不見當年風華，於是當局便在外海進行船對船的海上石油貿易，但為避免參與貿易的船舶，被聯合國發現而列入制裁黑名單內，伊朗駭客刻意在港口外海，透過網路植入許多的商船 AIS 假資訊 (左上圖黑框所示密密麻麻的黑點)，讓外界無法鎖定正在進行交易的船舶動態；另一個值得警惕的則是，軍艦以假亂真之案例，在2020年9月17日，英國海軍「伊莉莎白皇后號」(HMS Queen Elizabeth) 航艦戰鬥群(由 6 艘北約軍艦組成)，其船團的 AIS 位置顯示在愛爾蘭外海約 20 英里處，有好事者調閱歐盟「哨兵 2 號」(Sentinel-2) 衛星在同一天的空照圖，赫然發現，航艦戰鬥群根本不在該處水域，6 艘軍艦一直都待在港裡[21]，由此可見，從事 AIS spoofing 活動的對象，已經不再只限於不法份子了，所以誰都有可能是發動 AIS spoofing 活動的行為者。

圖 2-2: 伊朗使用 AIS 假資訊掩護阿巴斯港外的海上石油交易 (出處: Geollect)[22]



[21] *Warship positions faked including UK aircraft carrier*. (2021, August 3). Retrieved August 15, 2024, from BBC News briefing: https://www.bbc.com/news/technology-58027363

[22] https://www.tradewindsnews.com/news/ais-data-spoofed-to-move-60-ships-to-iran-s-bandar-abbas-airport/2-1-1464751

參、國際社會之態度

從近年的俄烏戰爭中，可發現無人機 (Unmanned Aerial Vehicle, UAV) 、無人艇 (Unmanned Surface Vehicle, USV) 在戰場運用上「小兵立大功」的價值，再加上低軌衛星優越的通訊及導航支援能力，將無人科技之應用提升到更高的境界。LEO 衛星位於地表上空約 500-2000 公里之間，從太空中俯瞰海面，可接收到更大區域範圍內的船舶 AIS 資訊，而且衛星信號下載速度快、衛星信號覆蓋率高，更有利於導引 UAV、USV 作業，但這些科技也同時可為不法份子所用。換言之，船舶可在科技的應用下，製造更多的欺騙花樣。對沿海國而言，除了要建立鑑別 AIS 資訊真假之能力外，還要防範駭客利用 AIS 三大公開特色(資訊不加密、架構公開、頻道公開) 侵入 AIS 主機及與之連線的其它航儀系統，發動惡意攻擊。

這些狀況的確讓國際社會，對不法份子運用 AIS 進行欺騙的行為感到同仇敵愾，盡管業界人士不斷呼籲 IMO 應採取更積極的態度解決問題(例如對收發資訊進行加密)，但 IMO 的專家技術委員會 (IMO Panel of Experts) 卻認為， AIS 從一開始便是針對提升船舶航行安全、減少碰撞風險所設計的輔助性系統，不是用來監控船舶動態、協助邊境安全管理或支援海域執法，所以不能混為一談。故 AIS spoofing 行為所造的挑戰與威脅，還是要由沿海國自行面對並研擬解決方案，在求人不如求己之下，一些國家已經開始做出具體的回應；例如新加坡、以色列等，便以立法方式，強制規定進入其管轄海域之大小船舶均須開啟 AIS 自我表明身分，這是著眼於減少不明身分目標的作法。另一種則是擴大 AIS 強制適用對象，例如美國依其聯邦法規 (Code of Federal Regulations) Title 33 (Part 164, § 164.46 Automatic Identification System) 的要求，具備動力之水上載具只要長度大於 26 英呎 (約 8.1公尺) 都必須加裝 A 型的 AIS[23]，並依 IMO 所規定的間隔時間內，對外發送本船 (艇) 航行資訊。

[23] https://www.navcen.uscg.gov/ais-requirements

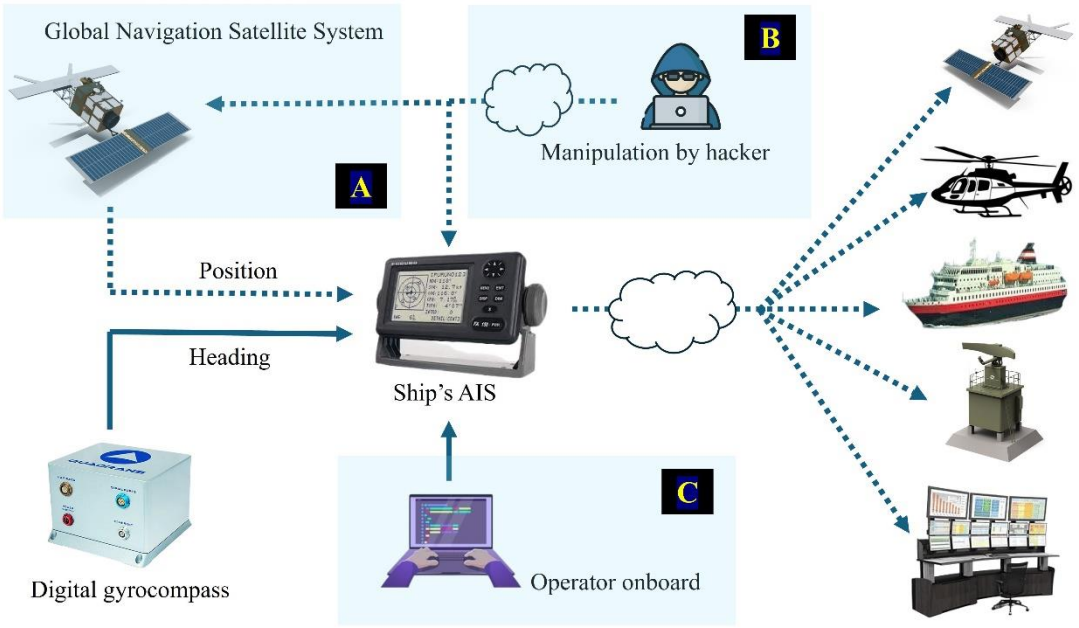
第二節　弱點與衝擊

AIS spoofing 是一個廣義名詞 (Umbrella term)，很難精準定義，因為所有涉及運用 AIS 假資訊的不法活動都屬之，而且應用範疇也從海上延伸至太空，例如在地球軌道上 (如圖 2-3)，裝有 AIS 的低軌道衛星 (分布於地表上空500-2000公里) 即可接收船舶所發出的航行資訊，又能在地面控制站的指揮下，向海面傳送各類資訊，若駭客侵入發射假資訊或傳送刻意加大誤差距離之定位信號的話，其所造成的威脅層面及破壞程度只會更大。在本研究所納入分析的 46 起海上資安事件中，就已經出現有案例顯示，不明身分行為者，利用操控衛星信號的方式傳送假的定位資訊，搭配 AIS 運用的事件。

圖 2-3: 衛星接收AIS資訊後可對海面船舶進行定位及數據交換(出處: OpenAI) [24]

[24] OpenAI. (2024). *ChatGPT* (4o) [Large language model]. https://chatgpt.com/c/964730ea-2914-4cf3-b70f-7fc503c97e1e

圖 2-4: 操縱 AIS 之模式



為能清楚說明可能之風險區域，作者彙整相關文獻研究所得後，繪製圖 2-4 並摘要說明如下：

一、可能的攻擊弱點

不論是哪一種資訊系統，都離不開網路，而網路本身就是一個既看不到、無邊界且不設防的電磁空間，所以各方資訊生產者都必須依賴協定 (Protocol) 才能在此一空間內完成交換。為保全資訊內容起見，一般做法都會先在發射端進行加密、然後於接收端解密，所以兩端都必須使用自家的編碼 (Encoder) 及解碼器 (Decoder)，才能安全的交換訊息。以上圖的 AIS 為例，它是身處在一個公開且無加密的網路空間中， A、B、C 可視為最容易受到控制、侵入或操縱之可能漏洞。

(一) A區 (AIS 接收全球導航衛星系統的座標資訊)

全球導航衛星系統 (Global Navigation Satellite System, GNSS) 為一通用名詞，例如美國 GPS、中國大陸的北斗系統、歐洲的加利略系統等都是 GNSS 的一種。

衛星可向地球表面發送最基本的座標資訊 (即經度、緯度) 供各式載具所使用，不論是定位、導航或通訊都需要 GNSS 的資訊才能知道現在的位置，像美國的 GPS ，它可提供高精準度(P-code)、低精準度 (C/A-code) 的導航信號[25]，前者為美國政府所屬單位使用其誤差可能只有幾公尺，後者則免費開放各國使用，然而天下無白吃的午餐，GPS 的管理者只要加大 GPS 信號誤差範圍(例如從5公尺增至5000公尺)，便可將船舶或飛機導引至錯誤或有危險之地方(例如淺灘)。

以下案例發生於 2019 年 9 月 5 日的大連港，一艘名為「金牛座」的商輪正在駛入港口(正常航跡為黃線)，突然出現 GPS 假訊號(紅色)，而且在進港最後階段，其位置已偏移到陸地上去形成紅色的圓圈，當時顯示的船速竟高達31節，在陸地上的橘色小圓圈則是 GPS 信號的干擾源所在位置，換言之，這是一起刻意操縱 GPS 信號，製造不實船舶位置的欺騙模式 (以下稱 GNSS manipulation)，這種手法需要大量的資源及人力才能發揮作用，所以必然是國家級的行為者。

圖 2-5: 利用操縱 GPS 製造船舶假位置 (出處: SKYTRUTH[26])

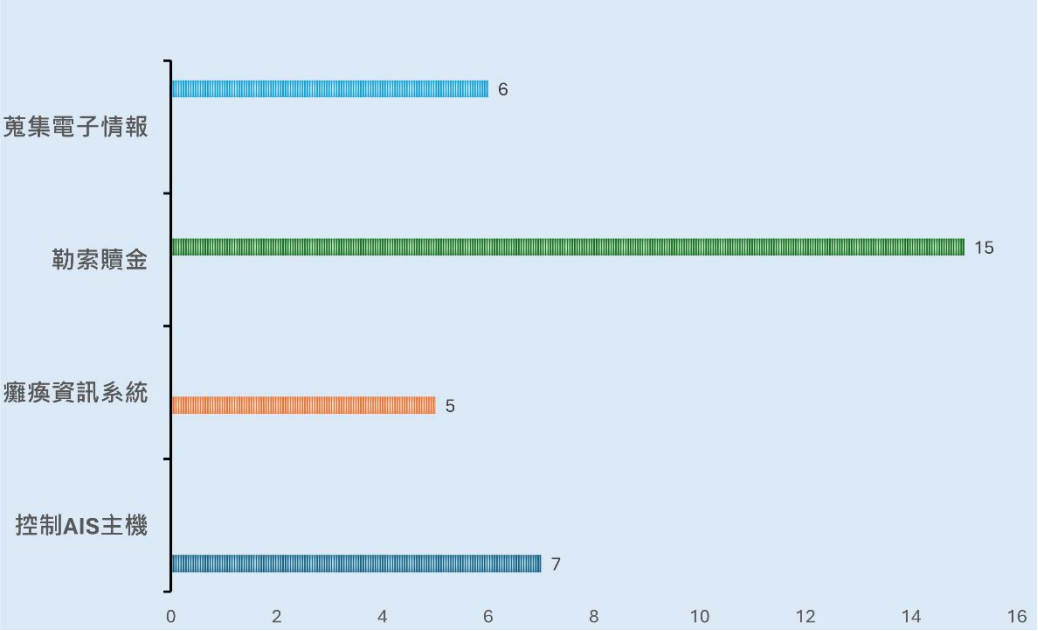
[25] Gustafson, D. E., Dowdle, J. R., Elwell, J. M., & Flueckiger, K. W. (2009). A nonlinear code tracking filter for GPS-based navigation. *IEEE Journal of Selected Topics in Signal Processing*, *3*(4), 627-638.
[26] SkyTruth 是一個關注於海上鑽井、石油洩漏、非法捕魚和棲息地變化等議題之非營利環境監管組織，利用衛星影像和遙感資料來識別和監控對地球自然資源的威脅。

鑑於所收到的衛星定位信號、AIS 資訊都是他方提供，接收方只能全盤接受，很難驗證資訊內容之真偽，在作者所檢視的 46 個案例中，全部都是受害者，這些受害對象包括船公司、官方海事機構、船舶、海運業者等。

(二) B區 (駭客通過網路侵入)

歹徒或不法 (有心) 份子利用網路侵入 AIS 主機、船舶或 VTS 中心主伺服器系統 (Main server)[27] 進行各類破壞、竊取或監控之行為，是較為常見的手法而且難度也較小，在 案列中，駭客攻擊船舶的模式，可歸納為「蒐集電子情報(駭入系統植入木馬程式)」、「植入勒贖軟體」、「癱瘓系統」、「控制 AIS 主機」等四類 (如圖2-6)。其中勒索贖金的案例竟有15個之多，以控制它船 AIS 主機的案例則多半是屬於「搞破壞、製造混亂、掩護不法活動」的性質，而值得注意的則是「蒐集電子情報」，通常是在一方實施海上演習或特別行動時，敵對陣營的船舶也正好滯留在附近海域，截收海上演習單位所發出的電磁信號。

圖 2-6：2010-2020 年駭客侵入船舶系統進行不法活動之統計及類別



[27] 伺服器 (Server) 是一台專門用來管理電腦的電腦，而主伺服器則是用來管理一般伺服器的大電腦，一旦被駭入，則該船或該機構所受到的損害可想而知。

例如北約海軍在 2014-2017 年期間，實施密集演習時，俄羅斯民船曾多次滯留在挪威外海，北約軍方便懷疑這些民船應該都是在蒐集電子情報，所以 B 區所受到的安全威脅，不會只有單純的侵入船舶 AIS 主機，一旦成功駭入後，便可造成各層面的破壞。

(三) C區 (船員輸入錯誤資訊以混淆外界視聽)

這個部份多是船員在船長授意下，於 AIS 主機故意輸入假資訊 (如假身分、不實之經緯度等) 或不發射本船資訊，以達成混淆外界視聽或隱匿航跡之目的，嚴格地說，這種欺騙模式雖然談不上科技，但可造成海域安全極大程度的威脅，而且也是最難防範的一種態樣。

二、衝擊

從以上案例所提到的 AIS spoofing 態樣來看，不法份子的手法已從單純的「本機操作」趨向多元化，其中又以 「GNSS 加上 AIS 」複合手法所產生的困擾最麻煩。主要是因為 AIS 無法自行產生船舶所在位置之經緯度，必須外接 GPS 定位信號，才能向外告知本船的位置 (如圖2-4)，一旦假的位置資訊送入某船的 AIS 主機或其他航儀系統的話，其所造成的衝擊將會是非常嚴重，很可能是某船早上 10 時的位置在高雄港，11 時又出現在新加坡海域，如此一來外界將無從確定「船舶真正所在位置」(Ship's actual whereabouts)。此外，駭客亦可透過衛星，向更廣大的海域範圍發送 AIS 假資訊，製造更大的欺騙效應，而且飛機、艦艇還無從防範起，就算關閉了 AIS 主機，衛星天線仍然還得接收衛星所發出的定位信號， 除非有不同的衛星信號來源可做驗證，否則在茫茫大海中，將無從判斷所收到的衛星定位信號，到底是真是假？對此可以下列假設狀況加以說明。

假設某巡邏艇在新北市林口區外海正西 10 浬處 (離岸約 18.6 公里) 執行勤務，為驗證 GPS 接收器所得到的船位信號有無被駭客惡意植入距離誤差，艇長在 1500 時，以雷達從二個方位觀測林口發電廠煙囪，分別取得二條方位線 (Bearing)，然後將其繪於海圖上，二線交叉於一點，該點的經緯度便是該艇 1500 時的船位，因為

林口發電廠煙囪是固定的地標，以它為標的定位的準確度最高，此時若 GPS 所顯示的船位不在正西，而是在西南方30浬海域的話，那信號可能就有問題了(有可能是造假、或被故意加大方位和距離誤差)，因為這個距離誤差太大。但若是在大洋航行時，船舶就只能依靠衛星所提供的信號掌握所在位置，此刻最好能使用不同來源的衛星信號 (例如低軌衛星、同步衛星) 進行比較，經由案例研析，主筆作者將 AIS spoofing 行為所造成的衝擊概分成以下幾種：

(一) 不利於建立海域空間透明度

本項所稱之安全 (Security) 即「邊境管理、海上治安及交通秩序維護」等議題領域所專注之安全，屬於傳統安全範疇。站在海域執法之立場，執法者當然希望海上船舶的動態及身分都能清楚呈現於眼前，所以非常強調「建立縱深」(即延伸監控縱深) 與「早期預警」之能力，唯有如此才能建立「海域空間透明度」落實安全維護；然而 AIS spoofing 行為卻以掩護不法活動，混淆外界認知為目的，企圖隱匿船舶蹤跡，透過假資訊製造更多的不確定性，其作法已嚴重妨礙海域空間透明度之形成，讓海域空間變得更不安全。

(二) 國際社會須建立標準化的海上網域安全共識及應變機制

海上網域安全相較於陸上網域安全，雖然談的都是跟資訊有關的安全，但落差很大，後者有各種嚴格的資安機制和法規，不論在軟體硬體的防護上都相對完整，這是因為一旦出現網路不安全狀況時，其嚴重程度和受損層面都會非常可觀，甚至釀成災難級的破壞，因為很多部門都有密切的連結關係。前者正好相反，船舶機動性高而且穿梭在國際之間，船員來自各方，缺乏類似陸域社會各行各業的緊密連結，因此國際社會對於海上網域安全並無一致性標準，而且各方行為者的防護概念也未必相同，這是為什麼，同質性的海上資安事件總會不斷重複上演的原因[28]。本研究案所檢視的網域安全事件，雖無法完整涵蓋所有的欺騙模式，但有一點可以確定的是，駭客有能力運用 AIS 的開放架構，通

[28] Tam, K., & Jones, K. D. (2018). Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. *Journal of Cyber Policy*, *3*(2), 147-164.

過公開的頻道從遠端侵入一艘船，港口管理中心或海事安全機構等，對其進行各類破壞活動。

不法份子或有心人士，一旦透過網路空間侵入目標內部時，通常會鎖定「資訊端」(Information technology, IT) 或是「維運端」 (Operation technology, OT) 兩個部門。攻擊資訊端之目的，在阻絕資訊流通，使其無法對外聯繫或停止內部資訊交換作業；後者則在癱瘓正常運作[29]。例如先前所提到的「操縱衛星訊號」就是一種對 OT 的攻擊模式，其所造成的危害更甚，因為航儀或武器系統，一旦使用錯誤的衛星座標信號之後，就會出現極大的準確度誤差，讓船舶駛向危險區域或讓武器系統打不到目標。現今已有越來越多的海洋事務學者，公開呼籲各沿海國，要更積極的參與海上網路安全工作[30]，因為海上的網路攻擊是不分軒輊，任何假資訊都有可能影響或威脅到海上船舶、飛機或沿海國的安全運作。

第三節　小結

透過文獻檢閱，研究小組對海上的 AIS spoofing 行為之動機、模式及可能造成的衝擊，均獲得較清晰之理解，我們也發現到，一些傳統的欺騙手法 (如船舶用假身分活動、關閉 AIS 等)，例如大陸籍漁船冒用我方 AIS 識別碼、我方漁船或遊艇使用中國大陸製造的 AIS 在海上活動，而被認為是大陸籍船舶的案例已多次出現，這種魚目混珠 (難以區分彼此) 的現象，讓已經不甚透明的海域動態變得更加複雜，因為在以往，僅憑 AIS 資訊所顯示的身分碼，就可以辨識船舶的身分，如今在大家都在使用假身分之情況下，顯然這已經嚴重涉及到邊境安全。

[29] Mraković, I., & Vojinović, R. (2019). Maritime cyber security analysis–how to reduce threats?. *Transactions on maritime science*, *8*(01), 132-139.
[30] Meland, P. H., Bernsmed, K., Wille, E., Rødseth, Ø. J., & Nesheim, D. A. (2021). A retrospective analysis of maritime cyber security incidents.

第三章　AIS假資訊之欺騙態樣與案例解析

第一節　欺騙態樣

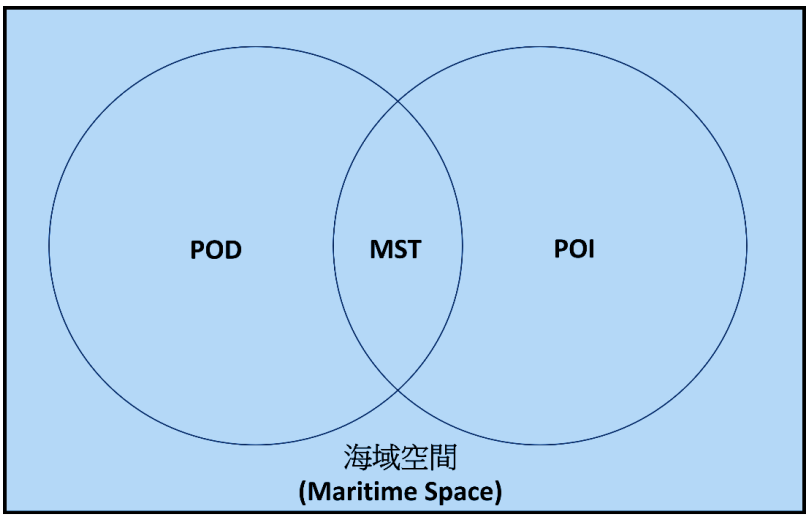
不法份子或有心人士利用 AIS 發射假資訊，無非是出於賺取暴利、掩護非法活動或軍事行為等動機，其行為就是要造成 AIS 資訊使用者的錯誤認知，以達到誤導或影響決策之目的。歸納近年相關文獻，可明顯發現，利用AIS從事欺騙行為之態樣持續翻新，從非傳統安全範疇 (如非法漁撈、海上交易、非法排放、盜採海砂等) 擴大至傳統安全領域 (如軍事、國防、外交等)、甚至跨越到所謂的「海上網域安全」，而行為者也不再局限於船上人員，任何人都能經由網路，駭入任何一(多)台AIS主機 (不論是安裝在船舶或VTS中心)，進行操控，對此國際社會對 AIS 多有質疑，認為是設計上的問題才會讓不法份子有機可乘。然而「國際海事組織」的技術委員會則另有見解，他們強調 AIS 係著眼於減少船舶碰撞、提升船舶航行安全之需要所設計，基於時效及方便各國廠商開發 AIS 周邊相關配套措施之要求，才會使用開放開放性架構，所以不能將AIS 之功能，與軍事或執法用途所需之目標追蹤和偵蒐混為一談。

壹、動機

AIS spoofing 之行為動機，和行為者所欲達成之目的直接有關，但其出發點未必都與不法活動有關，有可能只是保護自身利益使然。例如船公司為防範競爭者經由分析我方貨船的AIS資訊動態，掌握物流走向而要求所屬船隻使用假身分航行、某國商輪違反國際禁運在公海進行交易時所採取的關閉AIS行為、駭客為激化某國和敵對國之衝突，在其海域內製造敵對國船舶之AIS資訊等，這些行為動機雖不盡相同，但都必須運用AIS 手段才能達到目標，所以掌握船舶動向 (來自何處、駛往何方)，當有助於了解行為者之動機。對維護海域秩序的一方而言，有效執法的前提，就是出現在管轄海域內的大小船舶，都能被偵測到並可有效辨識其身分及動態，此即所謂之「海域空間透明度」(Maritime Space Transparency,

MST)[31]。重點在偵測 (發現可疑) 與辨識 (區分敵友及真假)，二者缺一不可而且必須產生交集，圖3-1所示之兩個圓圈，分別為偵測率 (Probability of Detection, POD) 和辨識率 (Probability of Identification, POI)，交集區域便是MST；換言之，只要出現在交集區內的海上目標，既要能被偵測的到又要能辨識其身分，而AIS資訊是當前辨識目標身分的重要依據，所以執法者對海上船舶製造假資訊及其危害不可不察。

圖3-1：海域空間透明度(Singh, 2010)



[31] Papadimitriou, A., Pangalos, K., Duvaux-Béchon, I., & Giannopapa, C. (2019). Space as an enabler in the maritime sector. *Acta Astronautica*, *162*, 197-206.

貳、欺騙態樣

本文蒐集 2010-2020 年間，所發生之相關案例、海事統計報告[32,33]及工作實務所見，表列為以下三大類：

表 3-1：AIS假資訊的欺騙類別及威脅

類別	威脅對象或模式	AIS 操縱手法	
		軟體	電磁信號
各類 AIS 欺騙	船舶	V	V
	導航設施	V	V
	搜救	V	V
	碰撞		V
	遇險信標 (Distress Beacons)		V
劫持 AIS 主機	船, 岸上監控中心	V	V
應用式干擾	插入空白碼 (Slot Starvation)		V
	跳頻 (Hopping Frequency)		V
	時間攻擊 (Timing Attack)		V

一、各類 AIS 欺騙

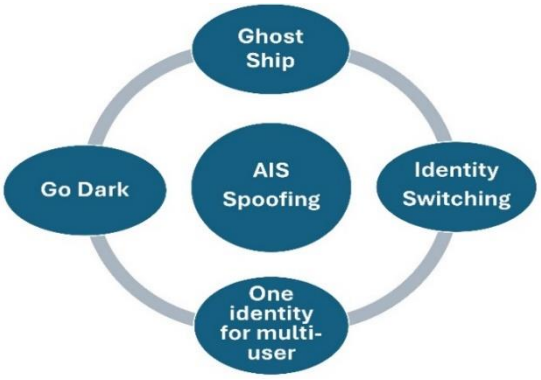
(一)以船舶為欺騙對象

行為者意在使他方船舶，誤認為所接收到的AIS資訊都是真的，而採取自認為正確動作，逐步走向行為者所設計的圈套。這種欺騙模式多半都是由船員透過後門程式，進入AIS主機竄改資訊然後再發射出去，雖然 IMO 有明文規定任何一方都不可更改 AIS 資訊，但在客戶要求下，幾乎所有的AIS製造廠商都會配合船東提供後門程式，這是一個很大的問題。

[32] https://www.hellenicshippingnews.com/wp-content/uploads/2014/10/AIS_Executive_Summary-Windward.pdf

[33] Meland, P. H., Bernsmed, K., Wille, E., Rødseth, Ø. J., & Nesheim, D. A. (2021). A retrospective analysis of maritime cyber security incidents.

圖3-2：船舶常見之欺騙態樣



1. 關閉AIS

關閉AIS (Go dark) 便可停止對外發射本船身分及航行資訊，讓外界或其他船舶無法得知本船身分，變成所謂的「身分不明目標」(Unknown target)。在巡防區的岸際雷達螢幕上，經常可發現此種身分不明的船舶，由於數量過多，因此在實務上，除非是航跡可疑，才會派遣巡邏艦艇就近查看，所以部分國家 (新加坡、以色列、加拿大等) 便透過立法程序強制規定，凡進入其鄰接區海域內之大小船舶，均應開啟AIS表明身分，以便於管理及監控作業，有的國家甚至還進一步擴大強制安裝 AIS 的對象。這種強制措施的確可發揮嚇阻作用，只要船舶關閉AIS，除將面臨處罰外亦將列為強制登檢對象[34]。在當前愈來愈多國家以法律強制之下，船舶在沿海國管轄海域關閉AIS以掩蔽身分之現象有明顯下降，但這種模式卻轉移到了公海之上，許多船舶仍然以不明身分活動，尤其是從事海上貿易或非法捕撈之船舶。

2. 多船共用一身分(One identity for multi-user)

多船共用一身分，對維護海上秩序的一方而言，必然是一大威脅[35]，例如第二巡防區某座雷達於 20 時，在基隆外海發現 A 船之身分碼為 315123456，但第七巡防區雷達 21 時在高雄外海，也出現一個相同身分碼的船舶，A 船不可能於一小時

[34] USCG. (2023, April 10). *NAV Systems and Services*. Retrieved May 27, 2024, from Navigation Center: https://www.navcen.uscg.gov/automatic-identification-system-overview
[35] Goudossis, A., & Katsikas, S. K. (2019). Towards a secure automatic identification system (AIS). *Journal of Marine Science and Technology*, *24*, 410-423.

內便駛抵高雄，類似非法態樣往往會造成海事安全單位的極大困擾，因為一旦發生海上危安事件或緊急狀況時，將無法鎖定誰才是真正的目標並確定其身分，後續亦將很難追查。

3. 幽靈船(Ghost ship)

顧名思義，幽靈船就是不存在，但卻顯示雷達螢幕上的類似船舶信號，這種欺騙手法往往著眼於更高層面之目的 (例如軍事、政治等)，操作模式也相對複雜，除使用駭客技術外、還須搭配假的衛星導航信號，所以專家學者又將此種模式稱為「全球導航衛星系統」(Global Navigation Satellite Systems, GNSS) 操縱模式[36]，換言之，就是將假的衛星定位座標加上幽靈船身分資料，整合成一筆 AIS 船舶資訊，然後再透過 VHF 無線電對外發送，在對方雷達螢幕上顯示出，一艘不存在船舶的位置 (甚至還有速度變化)，常見的案例，便是在某國敏感海域製造敵對國軍艦航跡、或在非核國海域內製造一艘核動力船舶之AIS資訊，以挑動國家間之衝突或提高區域緊張程度等。

4. 交互使用不同身分 (Identity Switching)

一艘不願真實身分曝光的船舶，於單一航程中，利用 AIS 發射不同的身分碼，企圖混淆外界視聽之作法，稱為「Identity Switching」。使用這種手法之目的，當然就是要混淆視聽，讓 VTS 中心誤以為有多艘船舶於轄區內活動，這就如同一個人擁有多張身分證進出公開場所一樣，根本無從鎖定[37]，若無法掌握可疑者身分的話，也將無法進行後續的偵查及監控作為。

5. 經由網路操縱導航設施、碰撞、搜救及遇險信標之欺騙措施

除了船員直接在船上製造假資訊外，有越來越多的案例顯示，網路操縱 AIS 已成為主流欺騙趨勢，駭客可從任何地方或處所，駭入某 (多) 艘船或岸置 VT S中

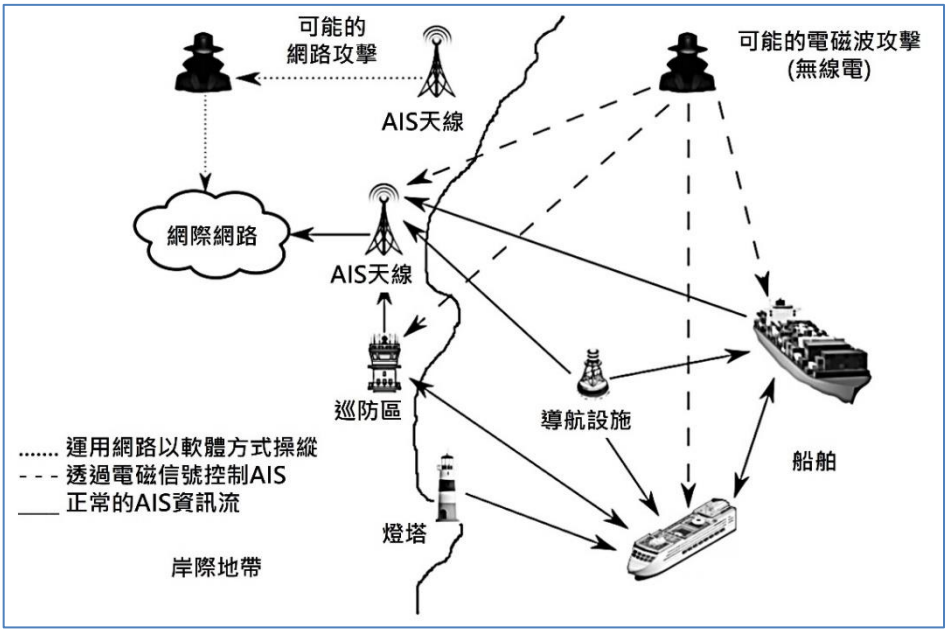
[36] Balduzzi, M., Pasta, A., & Wilhoit, K. (2014, December). A security evaluation of AIS automated identification system. In *Proceedings of the 30th annual computer security applications conference* (pp. 436-445).
[37] Zhou, M., van der Veen, A. J., & van Leuken, R. (2012, March). Multi-user LEO-satellite receiver for robust space detection of AIS messages. In *2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (pp. 2529-2532). IEEE.

心，一旦進入AIS 主機後，便以最高管理員身分指揮 AIS 主機，依其號令行事作業，進行以下欺騙：

(1) 駭入港口VTS中心發布假的航船公告

駭客一旦進入後，便可植入假的導航設施信號，誘使船舶駛往陷阱區，這種模式必須掌握AIS的最高管理員權限，一旦駭入系統後，便能強制接管VTS 中心的AIS 為其所用，此時就算VTS中心人員發現，也無法處理只能拔掉主機電源。

圖3-3：AIS操作手法示意圖



(2) 惡意更改碰撞預警設定

船舶航行期間總會遇到交會狀況，當兩(多)船相互接近時，必然會有最近距離點 (Closest Point Approach, CPA)，CPA 的距離越大越安全，而船上安裝的 AIS 具有 CPA 距離設定及警示功能，一旦對方接近設定距離時，便會發出警訊，提醒值班人員注意避碰。例如某船以 20 節 (時速 36 公里) 速率航行，設定 AIS 避碰預警距離為 3 浬(約5400公尺)，駭客侵入後將其預警距離變更為 500 公尺，縮短 CPA 距離，會讓某船陷入非常危險狀況，在此假想狀況下，AIS發出警訊後，某

船就只有1分鐘時間反應，將無法避免碰撞發生。

(3) 透過網路操縱導航設施

導航設施 (如浮標、雷達標竿、方向信標等) 之目的，在維持航道暢通及船舶行經導航服務區時之航行安全，所以導航設施也要加裝 AIS，並發出資訊告知外界注意航安。 一旦駭客自遠端透過無線電頻率侵入後，便可強制關閉導航設施的 AIS 使其不發射航安資訊，以達到誘導船舶航向危險區(例如淺灘)之目的。

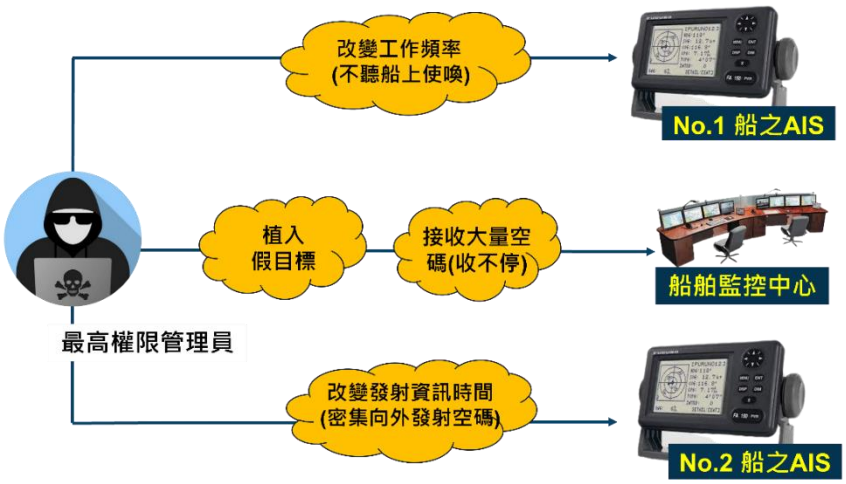
(4) 製造假遇險信號(調虎離山)

正常狀況下，海巡艦艇要負責海上責任區內的安全警戒，因此會在區域內巡邏，以防範可能的不法活動，在實務上，國內外曾有案例顯示，不法集團安排一艘誘餌船 (Decoy) 在偏遠海域，發出船舶遇險訊號，引誘巡邏艦艇離開巡邏區前往遇難地點查看，然後趁此空檔進行不法活動，這一招往往有效，因為人命無價，海上救難是船舶的義務。所以海上執法艦艇在面對類似狀況時，必須要密切和岸上指揮中心多方求證，並嘗試找出遇險信號中，有關 AIS 資訊的破綻，輕易相信的結果，除了白跑一趟外，還將製造了執法空窗，讓有心人士有機可乘。

二、劫持AIS主機

此種模式屬駭客行為，攻擊者可從任何地點發起，透過無線電、網際網路，駭入所選定之 AIS 主機 (艦艇或 VTS 中心的系統)，強制接管多部主機，供其所用，而被駭者即使發現亦無計可施，因為駭客一旦侵入系統後，便以最高管理員身分，於短短幾秒內變更系統原先所設定的帳號密碼，將船(岸)上值班人員拒之門外，換言之，此時的 AIS 已完全聽命於遠端的駭客，船(岸)上值班人員能做的便只有關閉 AIS 電源一途。圖 4-4 所示即為研究小組成員經由案例研析所歸納之手法。

圖 3-4：駭客劫持 AIS 進行資訊攻擊之示意圖



三、應用式干擾

(一)發射大量空白碼 (Slot starvation) 塞爆船舶 AIS 接收機

海事機關為避免船舶航行於其管轄海域時，過度接收AIS資訊造成飽和現象，因此都會在 AIS 資訊欄位中，預留部分空白欄位 (正常狀況下欄位內無資訊) 以便日後使用。當駭客侵入VTS中心AIS主機後，便可命令系統密集發射空白欄位，如此一來，船上 AIS 便會收到由中心發出的大量空白碼，塞爆 AIS 接收機，而真正重要資訊卻進不來，此種干擾目的就在癱瘓 AIS。

(二)轉換 AIS 工作頻率

在傳統的無線電通訊作業中，轉換通話頻率 (又稱為跳頻) 之功能行之已久，假設甲方、乙方在通訊時，為避免他方偷聽通訊內容，啟動跳頻功能，可讓通訊更安全，因為在短短數分鐘的通話時間內，雙方可能已經同步在上百個頻率中，不斷轉移通話頻率，想要偷聽的一方，將無從鎖定通話頻率，而能擺脫被偷聽之風險。然而運用在 AIS 時正好相反，AIS 本身就是要自動對外發出船舶資訊，不怕他方接收，因此工作頻率固定。不法份子為達控制 AIS 目的，於駭入 VTS 中心之 AIS 主機後，向特定或多艘船舶，發出轉換工作頻率之指令，一旦收到後，AIS 便會自動執行，轉移到駭客指定之頻率工作，脫離 AIS 正常的工作方式，而

且無法逆轉 (因為駭客是用最高管理員權限進入系統)，這種模式的發生時機，通常是在船舶駛入特定海域後(陷阱區)，讓受害船舶無法對外發送訊息[38]。

(三)時間攻擊

依據 IMO 於 2015 年 12 月所修訂的 AIS 使用指南 (GUIDELINES FOR THE AIS)[39]，船舶在不同速度下，發射 AIS 資訊的間隔時間也不同，例如某船速超過 23 節時，必須每2 秒鐘發射一次 AIS 資訊，當駭客控制某船後，可透過延遲發射間隔時間 (例如每 30 分鐘發射一次) 或縮短發射間隔時間 (變成每 0.5 秒鐘發射一次)的方式達成目的，前者可讓某船延遲 AIS 發射時間，防止該船航行資訊過於曝露，讓外界容易掌握其蹤跡，但假如在極短時間內密集發送航行資訊的話，將使各方 AIS 接收器收到海量般的資訊，進而達到癱瘓運作之目的。

第二節、案例解析

在上節中，已摘要說明利用 AIS spoofing 行為的態樣及手法，不論手法如何變，其最終目的在「掩護不法或激化敵對方彼此衝突」，換言之，就是讓資訊使用者，相信 AIS 所顯示的資訊，作出自認為正確之處置作為，落入惡意方所設下的陷阱，從而造成重大損失；所以北大西洋公約組織 (簡稱北約) 將 AIS spoofing 列為海上認知作戰的一種[40]，故海域執法者不能再用以往思維，看待現在的AIS spoofing，單純的認為，它只是不法漁業、走私行為者所慣用的掩護手段而已，為進一步說明起見，本文挑選較具代表性的 5 個案例進行解析，期能產生拋磚引玉之效果。

[38] Balduzzi, M., Pasta, A., & Wilhoit, K. (2014, December). A security evaluation of AIS automated identification system. In *Proceedings of the 30th annual computer security applications conference* (pp. 436-445).
[39] IMO. (2015, December 2). *AIS transponder*. Retrieved June 25, 2024, from Resolution A.1106(29): https://wwwcdn.imo.org/localresources/en/OurWork/Safety/Documents/AIS/Resolution%20A.1106(29).pdf
[40] Claverie, B., Prébot, B., Buchler, N., & Du Cluzel, F. (2022). Cognitive Warfare: The Future of Cognitive Dominance. *Bruxelles: NATO Science and Technology Organization*, 2022-03.

壹、國王之路號貨輪 (Kingsway)

一、概述

Kingsway 是專為載運油料及化學品所設計之貨船，船東為高雄航商，和台灣有深厚的地緣關係，但該船因違反聯合國制裁北韓禁運規定，被列入制裁船舶名單，不准進入各國港口 (有多次更改船名之紀錄)，目前已名列海巡署網頁的「制裁及關注船舶名單」中，同時也是各巡防區的監控對象，然而「道高一尺、魔高一丈」，該輪毫無疑問會窮盡諸般手段，以圖生存及謀取不法利益。

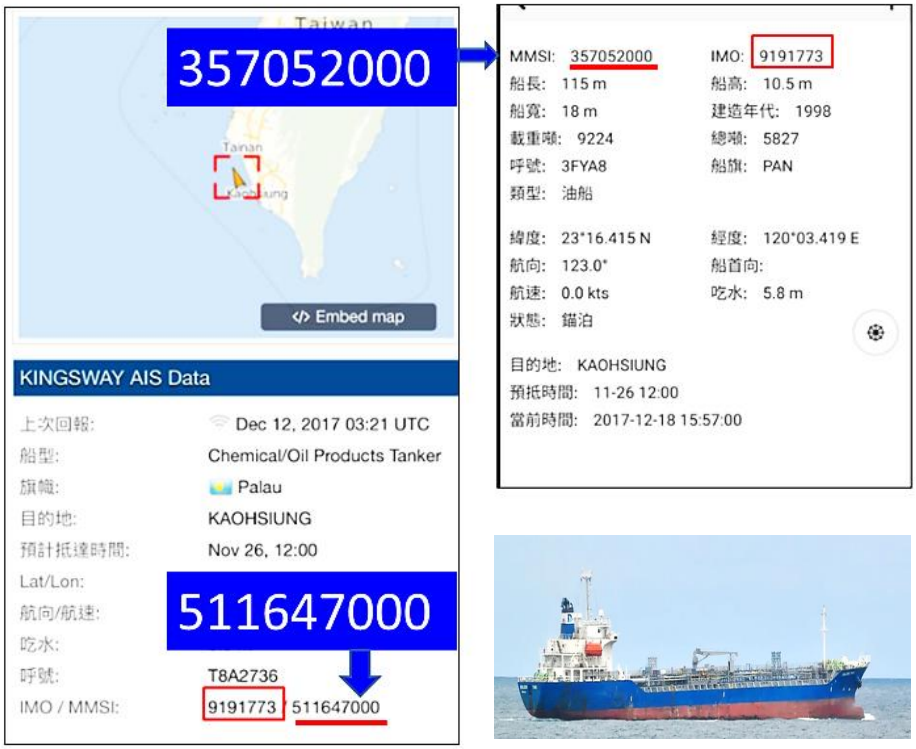


圖3-5： Kingsway滯留南台灣期間之AIS資訊

二、經過情形

2017年12月12日，Kingsway 於出現於屏東海域，當時 AIS 資訊所顯示的 MMSI 碼為511647000 (國籍為帛琉)，該輪以極緩慢速度 (1節) 向北航行到嘉義外海後，再折回屏東海域，如此循環七天，依據12月18日 AIS 資訊顯示，其國籍已

變更為巴拿馬 (MMSI碼：357052000)(佐證資料如圖3-5)，而且連無線電呼號也由原先的 T8A2736 變為 3FYA8，隨即消失蹤跡，約於二週後，該輪於公海被美方無人機發現，與北韓船舶進行海上交易。

三、解析

(一) Kingsway為何滯留並持續以極低速往返於南部海域？

Kingsway 已被禁止入港，故不論是哪一種類別的補給都只能在海上實施，而且也不能過於招搖，不難理解為何他要以近似滯留航速往返於屏東及嘉義之間海域，主筆作者認為這種慢速行進的態樣，應該是在進行海上補給，船東為降低風險，有可能僱用小型油船，在海上以邊走邊加油的方式補充油料，以供轉賣其他被制裁國家，為免小船跟不上，而且加油也有風險，因此才採取低速航行，再加上小型油船裝載量有限，所以得花費較長時間進行加油。

(二) Kingsway為何在滯留期間改變其身分？

屏東及嘉義之間海域分別為 4 個巡防區所守護，且配備相當數量之岸際雷達全天候監控海面，如果全程關閉 AIS 而且速度又是如此緩慢的話，將很容易被發現，為減少被發現風險，Kingsway 採取險招 (有別於常見的關閉 AIS，變成不明身分目標)，全程發射 AIS 資訊，讓本船蹤跡透明顯示在各巡防區雷達監視之下，其間透過變換身分，讓雷達操作人員誤以為，是不一樣的船舶南來北往，圖 3- 5 雖然只顯示了12月12日、12月18日這二天的 AIS 資訊，但這二天以外的日期，不排除 Kingsway 還有用到其欺騙模式進行更周全的掩護。

貳、不法集團施展調虎離山之計，企圖製造特定區域執法真空

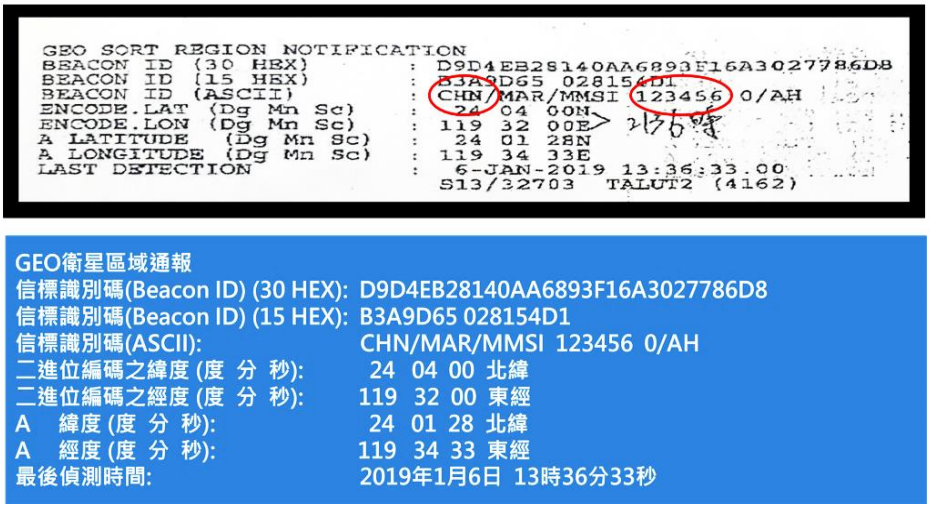
一、概述

各海巡隊每日派艇出海巡邏，維護轄區海域安全，除了海巡核心任務外，救生救難也是重點勤務之一，根據 SOLAS 要求，全世界航行中的船舶，在發現或接獲周遭出現海上遇險事件通報後，均應立刻參與救援，這是基於「我為人人、人人為我」的人道精神，但對不法份子而言，卻可能變成另一種不法之手段。

二、經過情形

主筆作者於金馬澎分署勤務指揮中心服務時，曾在2019年1月6日，接獲上級轉發之船舶遇險信文(如圖3-6)，這封信文是 GEO [41]衛星收到遇難船舶發出之信號後，轉給地面站，再送交國搜中心傳給海巡署處理，所顯示之遇難位置在澎湖周邊海域，故由金馬澎分署接手後續作業，所以勤指中心必須針對信文內容作出適當反應，並建議長官決定是否派艇前往救援，鑑於以往曾發生漁船 "誤觸" 遇險求救裝備，造成執法艦艇疲於奔波之情事發生，因此值勤人員對於這封信文採取較審慎之作法，最終認定信文內容有假，而未派艇前往現場。

圖3-6：遇難船舶所發送之GEO衛星遇險信文



三、解析

基於人道精神，金馬澎分署本當通報線上巡邏艇前往協助，然而這封遇險信文，從頭到尾只能用詭異二字形容，原因如下：

(一)遇險者的身分無法辨識

MMSI 碼是確認船舶國籍的重要依據，總共有 9 碼，前 3 碼被稱為「海事確認碼」 (Maritime Identification Digits, MIDs) 代表國籍，由「國際電信聯盟」(International Telecommunication Union, ITU) 統一制定[42]，例如：台灣碼為 416，第

[41] 稱為地球靜止軌道 (Geostationary Orbit) 衛星，位於地表上空約35789公里處，主要用於通信。
[42] https://www.itu.int/en/ITU-R/terrestrial/fmd/Pages/mid.aspx

一個數字 4 代表亞洲，16 則是區域碼，中國大陸有412、413、414 三個區域碼，換言之，只要船舶 MMSI前 3 碼為 412-414 都是大陸籍船舶。然而信文第 4 行的 MMSI 卻只有 6 碼，少了最重要的 MIDs，無法確認該船之身分證，有就查不出船名、無線電呼號等，更遑論和對方建立通訊，這是極為不合常理之處。因為一艘正常運作的船舶，在安裝遇難求救裝備前，供售廠家均會將該船的身分資訊輸入裝置內，而且還要經過測試無誤後，才能安裝在船舶上，一旦狀況發生時，便會向外發出預設的身分資訊，讓救援方能早早確認遇難船舶身分及位置，因此這封遇難信文的真實性令人可疑。

(二)無法確定遇難地點

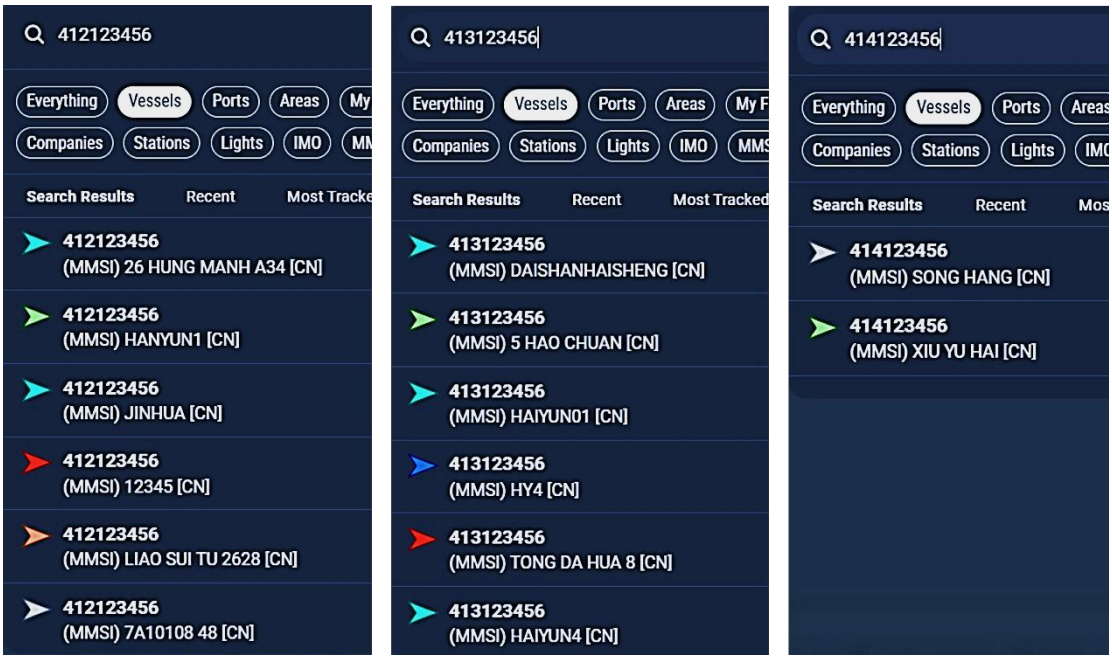
若按經緯度標示的話，該船遇難地點約在澎湖七美西南方60至70浬處，而且有 2 組經緯度座標，代表兩個地點都有可能是遇難地點，線上巡邏艇僅一艘，如何在廣大海域搜索遇難船舶，的確有實務上困難。

(三)有「多船共用一身分」之事實

信文第 4 行的 MMSI 只有 6 碼，少了最重要的前 3 碼，主筆作者抱著姑且一試心態，將 CHN 當成 China，便出現以下 3 組的MMSI：**412**123456、**413**123456、**414**123456，將此 3 組數字逐一輸入外網所得到查詢結果顯示，每一組 MMSI 都有多艘船舶使用，而且全都是中國大陸的船隻(如圖3-7)，也就是說，有多船同時使用一組身分證的事實存在，根本就無法確定到底是誰遇難了？

深度查詢之下(須具備會員資格方能使用)，這些船舶在事發當日全都不在遇難海域，因此可合理認定，這是不法集團的誘餌戰術，利用發射不完整的遇險信文，故意誘使巡邏艦艇離開責任區前往救難，達到調虎離山之目的，在經過以上分析後， 分署長官遂同意不派巡邏艇前往遇難地點，並向海巡署回報分析結果，因此結案。

圖3-7：透過 www.marinetraffic.com 查詢3組MMSI之結果



參、美國軍艦因為關閉 AIS 和商船發生碰撞之事件

一、概述

傳統上，關閉 AIS 是不法份子最常慣用的手法，可讓本船變成雷達上無法辨識身分之「不明目標」。這種目標對海上治安、救難及交通管制，均將造成極大之困擾，所以愈來愈多的沿海國才會立法，強制活動於其管轄海域之船舶，都必須開啟 AIS。試想在大多數船舶都有開啟 AIS 狀況下，執法行為者只要注意少數無 AIS 資訊顯示的目標，便可節省許多勤務成本，而且也可滿足優化海域空間透明度之要求，所以 SOLAS才會在相關章節對 AIS 之使用，做出各種強制性規定(包括安裝 AIS 對象、AIS 資發訊時間間隔等)，以減少海上撞船之風險。惟此強制性作法不適用於軍艦及執法艦艇，前者面對的是敵軍、後者則是不法之徒，除非是出於策略性考量，否則對本身航行蹤跡及位置都採取完全保密，於航行時只接收他船所發出的 AIS 資訊，而本身不發射航行資訊。

二、經過情形

美國海軍在 2017 年 6 及 8 月份，二艘神盾級驅逐艦 (*USS Fitzgerald, USS McCain)* [43]，分別和商船發生碰撞事故，造成重大損失[44]，前者於 6 月 17 日在東京灣外海和菲律賓貨輪 (ACX Crystal) 相撞，造成 7 位船員當場殉職，作戰系統幾乎全毀，後者則於8月21日在麻六甲海峽和賴比瑞亞籍貨輪 (Alnic MC) 相撞，此一事件造成動力系統嚴重受損及 10位船員殉職 (如圖3-8)。

三、解析

在美國國家運輸安全委員會所完成海事調查報告中，歸納出 8 點肇事原因，而其中一點則跟美國海軍的AIS資訊發射管制政策有關[45]。各國軍艦均配有AIS，但於航行時不主動發射AIS資訊，而且在 SOLAS 所制定的規定中，也排除了軍艦適用，所以軍艦不發射 AIS 資訊有其合法性，但這二起事件，卻突顯出不論基於何種原因，船舶關閉 AIS 企圖隱匿航跡，必然會帶來高度的航安風險，於是美軍在新修訂之政策下，允許軍艦在平時狀況，可以發射 AIS 資訊，但只顯示「我是美國軍艦及航向、航速」，這對於軍艦或執法艦艇而言，都是保平安的作法值得參考。

[43] 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.
[44] Demchak, C., Patton, K., & Tangredi, S. J. (2017). Why are our ships crashing? Competence, overload, and cyber considerations. *Center for International Maritime Security*.
[45] STAFF, U. N. (2019, August 6). *NTSB Accident Report on Fatal 2017 USS John McCain Collision off Singapore*. Retrieved February 13, 2024, from USNI News: https://news.usni.org/2019/08/06/ntsb-accident-report-on-fatal-2017-uss-john-mccain-collision-off-singapore

圖3-8：被撞後的*USS Fitzgerald* (上) 及 *USS McCain* 號軍艦

肆、駭客製造幽靈船恐嚇俄羅斯黑海艦隊

一、概述

傳統 AIS spoofing 手法，都須要在 AIS 主機上手動進行有其侷限性，但隨著網路化的普及化，運用駭客技術製造 AIS 假資訊，造成他方恐慌之手法已逐漸成為主流模式，而且也變得愈來越容易，只要有網路暢通，駭客或不法份子便可從任何地方、任何一部電腦，無差別或針對特定對象進行攻擊。通常這一類的作法，都著眼於更大層面之欺騙效果，例如在軍事敏感地區植入一艘敵艦資訊 (不實際存在，稱為幽靈船)，讓另一方的雷達偵測到此一威脅資訊，達到升高緊張程度

，引發擦槍走火之目的，或在交通繁忙海域，製造不存在的船舶遇難信號，讓沿海國執法艦艇疲於奔赴事故現場，近年發生的案例適足以說明，駭客作法已成為趨勢，尤其是在俄烏戰爭期間，發生於黑海的下列案例。

二、經過情形

2022年6月18日下午，兩艘隸屬北大西洋公約組織[46] 的英國「防衛者號」(Defender) 驅逐艦及荷蘭「艾沃生號」(Evertsen) 巡防艦，聯袂駛入烏克蘭奧德薩港進行整補作業，這兩艘軍艦一直待到19日下午均未出港，然而到19日凌晨，距離奧德薩港 180 公里外，俄羅斯黑海艦隊戰情中心的雷達上，突然出現這兩艘北約戰艦的 AIS 航跡 (如圖3-9)，而且距離自家港口僅 2 浬 (3.6公里) 之外，隨即下令所有待命艦艇緊急出港攔截，但忙了半天卻並未發現這兩艘軍艦的蹤跡，結果只是虛驚一場，這是一個典型的駭客利用 AIS 植入假資訊，企圖激化敵對雙方衝突之案例，同時也證明了，AIS spoofing 行為已被應用到了軍事領域。

圖 3-9：駭客製造的北約軍艦假航跡

[46] 為美蘇冷戰時期，由歐美國家，基於集體安全需要所組成的軍事性防禦組織，計32個成員國加入(統計至2024年3月24日)。

三、解析

根據 Marine Traffic 網站所公布的 AIS 航跡圖顯示，2021年6月19日，兩艘北約軍艦航向 (航跡為紫色線)，克里米亞島的俄羅斯黑海艦隊母港，其最後位置非常接近港口，對俄軍已造成極大威脅，所以當時俄軍才會動員所有待命艦艇出海攔截；反觀圖右側三個不同時段畫面(為港口監視系統所拍攝)，均顯示北約軍艦根本沒有出港，由此可證明，這完全是駭客的傑作，意在造成俄國艦隊的恐慌做出錯誤的決定。

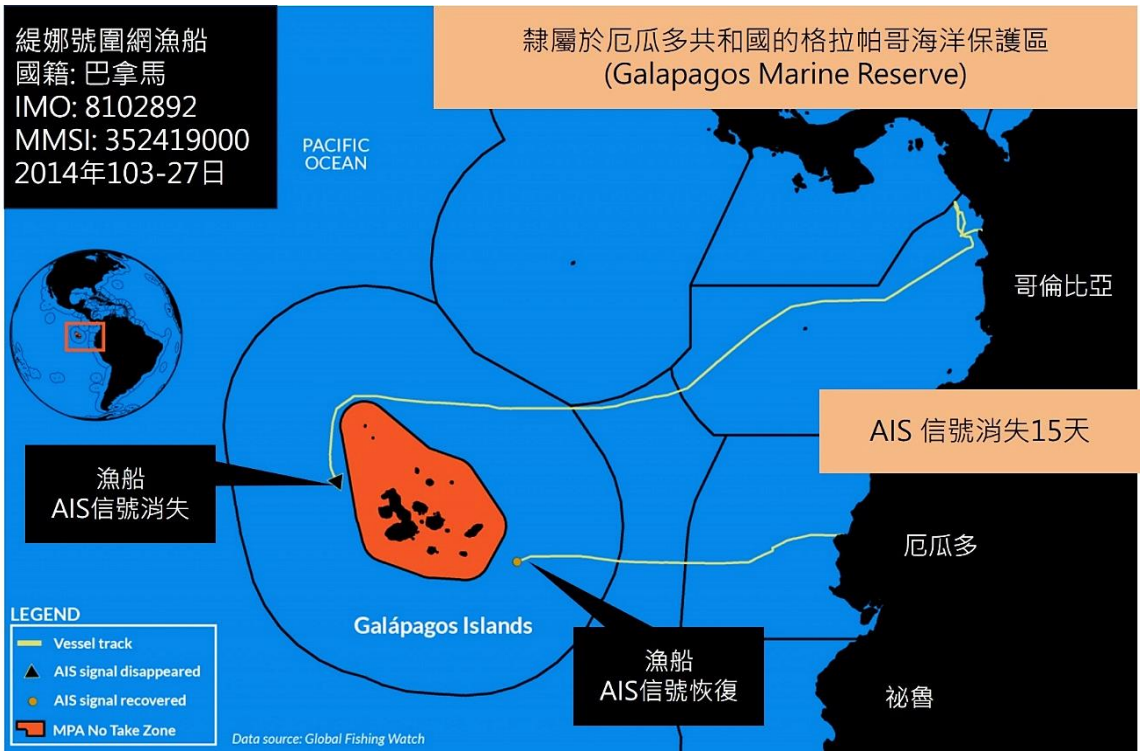
伍、2014 年10 月發生在格拉帕哥 (Galapagos) 海洋保護區的非法漁撈事件

一、概述

漁船關閉AIS侵入他國的海洋保護區進行非法捕撈活動，時有所聞，一些關注海洋保育議題之組織，如Global Fishing Watch、OCEANA等，都會密切監控這類行為並不時發布報告界以發出警訊。格拉帕哥 (Galapagos) 群島為厄瓜多共和國所有，是極具經濟價值的海洋保護區，以海洋生態多樣性及資源豐富著稱，更因英國生物學家達爾文 (Charles Darwin) 於1835年造訪後，受到啟發所完成的進化論而聞名於世，但它也深受盛名之苦，因為非法捕撈活動頻繁，一直困擾著厄瓜多政府。

圖3-10: 緹娜號圍網漁船檔案照片 (出處: Marine Traffic)

圖3-11：緹娜號在厄瓜多外海的非法漁業活動示意圖(出處: OCEANA)



二、經過情形

巴拿馬籍的圍網漁船「緹娜號」(Tiuna) (檔案照片如圖3-10) 於2014年10月3日自哥倫比亞出港，在接近格拉帕哥 (Galapagos) 海洋保護區西邊海域時，便失去 AIS 信號，使得外界無法掌握其行蹤。直到 15 天之後，其 AIS 再次發出信號，換言之，「緹娜號」有 15 天是處於行蹤不明的狀態下，從圖 3-11 所示，外界再次發現其蹤跡時，該船已出現在保護區的東側海域正航向厄瓜多。

三、解析

根據「全球漁業觀察組織」所公布的 AIS 航跡，「緹娜號」在格拉帕哥海洋保護區下方海域神秘消失的 15 天，雖然沒有直接證據顯示，該船有非法侵入海洋保護區進行捕撈作業的行為，但卻有高度嫌疑，否則其航跡從消失到再出現，也不會都圍繞在保護區周邊，相信明眼人都知道是怎麼回事。

第三節、小結

以上五個案例都跟運用 AIS 進行欺騙或隱匿船舶動態有關，使用的手段(法)未必相同但目的均相同，就是要以假亂真或無中生有的方式，讓外界或特定對象做出錯誤的反應，就本章所述，可歸納為以下四點：

壹、運用 AIS spoofing 之行為者已出現多元化趨勢

運用 AIS 進行欺騙之行為，除了在傳統的非法漁業、海上交通外，已擴大至各海事議題領域，尤其在「聯合國貿易禁運或制裁」、「潛在性區域衝突 (例如俄烏戰爭、南海主權爭議所產生之海上衝突或對立)」、「軍事及海域安全」等領域，任何船舶都有可能在其航行階段，運用到以上所提到的 AIS spoofing 伎倆，以維護國家安全或賺取暴利，例如英國海軍在 2020 年即已宣布，將AIS spoofing視為標準作戰模式之一。

貳、AIS假資訊已成為海上認知作戰的一種態樣

AIS spoofing的終極目的，就是要透過假資訊，讓收到資訊的一方信以為真做出自認為正確的反應(但實際上卻是錯誤反應)，造成重大損失，所以北約已將此一手法視為是海上認知作戰的態樣之一。

參、網路科技讓駭客得以綁架或從任何地方遙控AIS為其服務

駭客可以透過網路，控制或綁架任何一部 AIS 主機為其所用，或駭入某一 VTS 中心之 AIS 主機，再指揮它向外發布假資訊，甚至癱瘓該中心正常運作。

肆、嚴重威脅到海上網域安全

現今的船舶不論是大艦小艇，在導航、通信、雷達及射控 (Fire control) 系統的佈局，幾乎都已高度網路化，駭客一旦駭入某船的 AIS 主機後，就可循線進入其它系統大搞破壞，造成嚴的危安問題。

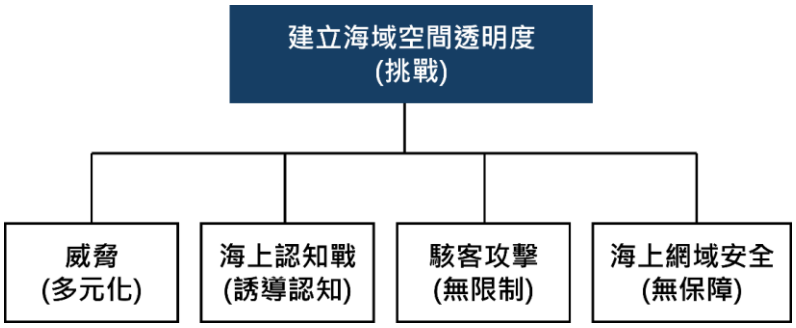
第四章　挑戰與機會

第一節　挑戰

岸際雷達是海巡署巡防區掌握海上船舶動態之利器，它整合了船舶所發出的AIS 資訊，作為了解其身分及航行動態之依據，但此一資訊是由他方所提供 (對方讓你看什麼你就只能看什麼，所以資訊來源操之於人)，因此執法者不能排除「資訊有假」(Fake AIS) 的可能性 (這也是本中心教官不斷在相關課程中強調的重點)。所以才要分辨資訊內容真假，而這也是最難的部分。

在研究本文鎖定的 4 6個涉及海事安全的案例中，有相當多的失敗案例都可歸咎於人的因素 (例如隨意開啟電子郵件夾帶的惡意軟體、亂插 USB 等)，因為人的疏忽或便宜行事，讓駭客得以伺機侵入而造成軟體 (重要資料被竊、勒贖) 或硬體 (如癱瘓資訊控制系統、偵測裝置及航儀系統等) 的損失。駭客入侵方式不外乎透過網際網路 (針對陸地單位)、AIS 公開頻率、衛星連線等管道進行攻擊行動，而且某些惡意軟體一旦侵入後並不立即發作，反而是進入潛伏狀態，直到接獲駭客指令後才會活化，有的則是透過密集傳送資訊封包 (Packet) 的方式 (這種攻擊模式的特性是資料可在不先建立連線狀況下，由一台電腦傳送給另一台，資料隨機傳送)，使電子航儀系統無法接收正常的運轉指令而達到癱瘓船舶運作之目的 (例如船舶在轉向時控制系統無法驅動舵機轉向指令)。作者將從法律及非法律之角度檢視，在當前海上假資訊充斥的環境下，欲建立海域空間透明度所須面對之挑戰 (如圖4-1)。

圖4-1: 建立海域空間透明度所面對之四大挑戰



壹、挑戰之一：海上假資訊所造成的多元威脅

海上假資訊之所以能從早期較單純的威脅 (例如船舶關閉AIS成為不明身分目標或於航行期間斷續發射AIS資訊等) 態樣演變成今日之多元威脅，主要是網路普及應用之所賜。網路本身並無好壞之分，重點是行為者之心態與動機。例如 2020 年 9 月英國研發團隊 (由普里茅斯大學和 IBM 公司組成) 研製的「五月花號無人船」(Mayflower Autonomous Ship, MAS)，於 40 天內成功航越大西洋至美國麻塞諸塞州之後[47] (如圖4-2)，無人化海上運輸成為不可擋之趨勢，但新的挑戰也隨之產生。

圖4-2: 歷時 40 天航行 5600 公里駛抵麻塞諸塞州的五月花號無人船
(出處: https://siliconsensing.com)

MAS 的順利首航，使用全自動化的航儀並搭配 AI 決策系統 (扮演船長角色)，但在穿越大西洋階段，船上系統仍須透過衛星通訊網路，進行程式更新及維護以便正常運作。日後無人海運一旦付諸實行後，大型無人貨輪在遠洋航行階段，船上系統，勢必也會碰到同樣狀況，萬一駭客透過網路傳送假資訊或從放置惡意軟體時，船上的主控系統如何能確認所下載的更新程式是否有害？再者，若駭客以最高權限管理員身分強行接管主系統[48]，要求關機、停船或更改航向的話又當如何應處？這都是國際航運界必須面對的新挑戰。其次，如 IMO 之要求，所有用於海上航行的通信電子、導航、救生(小到救生衣) 之設備，都必須符合「海上人

[47] O'Donncha, F., Sheehan, J. D., Touma, M., Zemouri, S., & High, R. H. (2024). Towards Intelligent Ship-Edge Computing Enabling Automated Configuration of Ship Models and Adaptive Self-Learning. In *State-of-the-Art Digital Twin Applications for Shipping Sector Decarbonization* (pp. 73-93). IGI Global.

[48] Mraković, I., & Vojinović, R. (2019). Maritime cyber security analysis–how to reduce threats?. *Transactions on maritime science*, *8*(01), 132-139.

命安全公約」(International Convention for the Safety of Life at Sea, SOLAS) 的安全規範並取得認證才能安裝在船上，此一制度已行之多年，但對裝備所涉及之軟體及資訊安全要求(尤其是前述無人船部分)至今尚未建立防範標準，所以國際海洋界近年來，才會一直不斷呼籲國際社會要重視海上網域安全的原因[49]。

一、法律面

眾所周知，法律是海洋治理 (Marine governance) 的必要工具之一[50]，國際組織要處理國際議題，就必須制定公約 (例如 1982 年聯合國海洋法公約) 以為各國遵循依據，惟公約必須經過國內法化[51] 之後，才能成為一個國家之法律產生實質約束力，然而國際公約往往是大國相互折衝之下的產物，未必能與時俱進滿足當代的需求，而且並無法兼顧每一個國家都利益，有的甚至還不認同公約 (例如美國不是聯合國海洋法公約的簽署國之一，卻經常借題發揮)；儘管海上假資訊對船舶本身保安、人員安全、海上交通、航運及海域治安等領域均已造成極大威脅，SOLAS 對當前發生在全球海域的 AIS spoofing 活動卻無其他闡述。有鑑於此，才會有國家自行立法，規定在其管轄海域內活動的船舶都要加裝 AIS 並須主動表明身分，否則將予以究責，這是基於建立「海域空間透明度」所須採取之必要手段。

二、非法律面

回顧臺海現況，如今的挑戰除了以往常見的越界捕魚、走私、偷渡之外，在所謂的「灰色地帶」(Gray zone) 策略[52] 之下，更多了來意不善的海上事件 (例如三無船舶[53]、民兵船、快艇侵入等活動)。就海上偵蒐而言，發現目標不難，難的是「如何確認其有涉及違法或危安事實」，因此首要之務便是掌握「對方身分、意圖、航行態樣及其行為」，在實務上，跟目標有關的種種情資，都應集中在一個綜合情資顯示平台上，平台具有特定海域水文及地理綜合圖資的背景資訊，能完

[49] 網域是一個廣義名詞，其範疇包括「網路 (Internet)、安全規定和策略、資訊設施、人員訓練、資訊戰、網路戰、駭客攻防等」，所以我們經常所提到的網路，只是網域安全的項目之一。

[50] Smythe, T. C., & McCann, J. (2018). Lessons learned in marine governance: Case studies of marine spatial planning practice in the US. *Marine Policy*, *94*, 227-237.

[51] 依司法院釋字第329號解釋，我國採取一元論學說(立法院決議經總統公布後，即視同國內法)。

[52] 吳東明. (2022). 現今灰色地帶策略於海事競技場域的探析域借鏡-中國與俄羅斯的應用案例研究. 於 吳東明, 海巡灰色地帶與海洋科學研究 (頁 008-023). 桃園: 五南. 2021年9月20日 擷取

[53] 指「無船名、無國籍及無相關證書」之船舶。

整顯現目標所在海域之水面 (如流向、流速) 及水下 (如等深線、深度、海底地形及地質等) 資訊，如此才有利於判斷目標的後續動態，若再加入我方執法資源配置及部署，便可形成所謂的共同作業圖像 (Common Operation Picture, COP)。作者根據曾經發生過的中外案例設定以下幾種想定狀況及其對應之挑戰：

狀況	內容	挑戰
1	一艘配備AIS之船舶，正逐漸接近約定地點，準備和對方進行不法交易，船長為避免被標記為雷達關注目標 (Red flag)，決定全程開啟AIS發射本船資訊，但使用的卻是假身分。	(一) 雷達監控人員如何能發現該船舶為可疑目標？ (二)如何辨識其身分為假？
2	某船的 AIS 資訊不完整，只有 MMSI 卻沒有 IMO 碼，出現在雷達監控海域且有滯留情形。	如何確認某船為聯合國制裁船舶之一？
3	某岸際雷達發現一目標 AIS 資訊，顯示為大陸籍，經通報巡邏艇查看後，發現該目標竟為我國籍遊艇。	該如何面對此種狀況？
4	不明身分船舶(經查無AIS資訊顯示)出現於我方海域並有滯留情形。	如何查證其身分？
5	某大陸籍小艇於進入我方鄰接區後，開啟 AIS 發射我國籍之船舶信號，並混入作業漁船中。	該如何面對此種狀況所帶來之挑戰？

貳、挑戰之二： AIS假資訊已成為海上認知戰的一部分

自從2022年俄烏戰爭爆發以來，北大西洋公約組織網站，便不斷放送「認知戰 」[54] 這個名詞，國際相關期刊也多有探討，但各學派見解不同，國際社會至今尚未統一定義，本文基於探究需要，採用北大西洋公約組織之定義即「某一方運

[54] NATO. (2022, June 22). *Cognitive Warfare*. Retrieved September 17, 2024, from NATO's Strategic Warfare Development Command: https://www.act.nato.int/activities/cognitive-warfare/

用不同權力工具，透過影響、保護、破壞等手段，改變個人、群體對某項議題之認知，進而付諸行動，為其行動爭取優勢，這種作為便是認知戰」[55]。認知戰在某種程度上和《戰國策·秦策二》(西漢、劉向所著)「曾參殺人」具有異曲同工之妙；換言之，就是透過權力工具 (如媒體、名嘴、網紅等) 不斷放話，經由以訛傳訛的方式，讓特定對象或群體，相信媒體所報導的內容都是真的，而達到控制認知之目的，當然最重要元素便是「假話」、「假新聞」或「假資訊」；在海域空間的假資訊，指的是駭客透過AIS公開頻道所植入的資訊、船上人員在AIS主機輸入的假資訊、或國家級的行為者利用衛星發送不實的定位資訊等，其目的都在誘導資訊使用者相信所接收到的假資訊。

一、法律面

國際社會對於以上行為並無相對之公約加以規範，各國關注焦點也多聚焦在跟傳統安全有關的事件 (例如第三章第二節所提及之駭客以偽造之北約軍艦航跡接近俄羅斯黑海艦隊大本營) 上，仍然缺乏全面性理解，猶如見樹不見林。

二、非法律面

作者在文獻檢閱階段，發現每個案例雖然性質不同但都有一些共同特徵，其中最常見的，便是警覺意識薄弱，船上人員在收到假資訊 (可能含有其他惡意軟體) 時，因為對 AIS 這套機制的信任，而未實施查證以致擴大災情；例如每一部 AIS 主機都有記憶卡或 USB 插孔(視機型之別)，可儲存所收到的資訊，船員往往在便宜行事之下，便將拔起來的 USB 再插到其他的航儀系統 (例如電子海圖) 上使用，導致其它系統也感染病毒。其次則是船舶的重要控制系統被惡意軟體侵入，造成失能或停機後，基於各種因素考量，未及時向外預警致使他方也跟著受損。對此國際社會已經有因應措施，例如「國際船東互保協會」(Club P&I)[56,57] 便公開

[55] Claverie, B., & Du Cluzel, F. (2022). The Cognitive Warfare Concept. *Innovation Hub Sponsored by NATO Allied Command Transformation*, *2*.

[56] Club, P&I. (2020, May 20). *Vessel monitoring and P&I insurance – ship's Automated Information System (AIS)*. Retrieved September 22, 2024, from https://www.igpandi.org/article/the-international-group-clubs-discuss-the-importance-of-ships-complying-with-the-requirement-to-use-a-ships-automated-information-system-ais/

[57] IGP&I. (2022, September). *Guidelines for Correspondents 2022*. Retrieved September 23, 2024, from

宣布，凡是船舶涉及操縱 AIS 散播假資訊，進行欺騙或知情不報等明顯危及海上安全之行為，經查屬實後，所造成他方及己方的損失，皆不在保險理賠之範圍。

叁、挑戰之三：駭客可透過網路從任何地方控制特定對象之 AIS

一、法律面

網際網路使用者透過協定 (Internet Protocol, IP) 便可由一點聯繫全世界的任何地方，因此各國都有制定相關法律，做為網路活動及資訊運用之規範。惟海上環境不同於陸地，所適用之法律也不盡相同，囿於現實，國際社會對於海上網域活動 (尤其施行認知戰之行為者) 尚未建立相對應之公約以為約束依據，所以在各國在面對假資訊或惡意軟體挑戰時，必須制定更明確的法律規範才行。

二、非法律面

不法份子操弄 AIS 進行欺騙、干擾 GNSS 提供錯誤導航定位之最終目的，在引導行為者做出錯誤決定以逞其企圖，作者於第三章第二節 (案例解析)，提出「不法集團製造假的遇險信號，企圖吸引特定區域之巡邏艇前往救援，藉以製造特定區域之執法真空」之案例，此案例跟先前所提到的「利用假資訊、建立被騙者錯誤認知」具有同樣性質，尤其假資訊內容往往又跟人命安全有關，決策者基於人命關天，在未經查證下便直接通報鄰近在航艦艇前往救援，結果很有可能就是被他人設計，直到抵達現場後，才發現並非如此 (有可能是對方誤觸遇險求救裝置)，所以在面對假資訊時，有很大程度是在挑戰主事者的決心下達、更是考驗勤指人員的應處專業。

肆、挑戰之四：對海上網域安全造成嚴重威脅

現今的船舶，幾乎所有的系統都已走向網路化及自動化，駭客必須透過無線電網路，才能侵入一艘航行中的船舶或 VTS 中心，進行各種不法或破壞活動。由於 AIS 主機具有二個公開 VHF 頻道，一旦駭入後便可控制該主機為其所用、遙控

https://static.igpandi.org/igpi_website/media/article_attachments/Correspondents_Guidelines_-_2022.pdf

VTS 中心之 AIS 主機，向外發布假資訊或不斷發送垃圾資訊，讓其它船舶一直處於收訊狀態，真正需要的航安資訊卻進不來，這是典型的飽和式資訊攻擊，意在讓對方無法正常作業。

一、法律面

在以上論述過程中，不管是哪一種挑戰，都缺乏相對應的國際公約或國內法，尤其在面對海上假資訊之際，必須建立一套法律規定作為執法依據，同時透過立法及補助措施，讓所有 20 噸以下的小型艇筏，都能加裝 B 型 AIS (只發射不接收) 以增進航行安全，同時也有助於分辨敵我，依據作者於專家訪談階段所獲資訊顯示，台灣地區至少有 20000 艘小型艇筏 (尚不包括浮具) 有待加裝 AIS。

二、非法律面

不法份子或有心人士，透過網路發送 Fake AIS 之行為，只是影響海上網域安全的手法之一，尤有甚者，如奈及利亞的 Cold galleon 駭客集團在 2017-2018 年之間，透過電子郵件夾帶病毒 (如Ryuk、Stuxnet、Icefog等惡意軟體) 攻擊海上鑽油平台船、跨國海運公司、港口 (如巴塞隆納港、聖地牙哥港[58]) 及美國海岸防衛隊的海運安全資訊中心[59]，其造成損失之大，不僅只是機密文件被盜 (通常會透過所謂的暗網進行交易) 而已，更會導致資訊系統或監控設備失能甚至停擺，對所有的政府及企業機構而言，這都是不可承受之損失。其次則是可能引發的邊境安全問題，在 2024 年海巡署曾發現多起明明是中國大陸船舶，但其 AIS 顯示卻是台灣籍 (識別碼為416) 的案例，更詭異的是，也有台灣籍的船舶使用大陸廠商製造的 AIS 主機，發出的竟是大陸地區的識別碼 (412、413、414)，這類「敵我不分」的案例，對邊境安全已造成更大威脅。

---

[58] *2018 Highlights: Major cyber attacks reported in maritime industry*. (2018, December 26). (USCG) Retrieved September 29, 2024, from SAFETY4SEA: https://safety4sea.com/cm-2018-highlights-major-cyber-attacks-reported-in-maritime-industry

[59] Blackmore, C. (2019, December 16). *Cyberattack Impacts MTSA Facility Operations*. (USCG) Retrieved September 29, 2024, from Marine Safety Information Bulletin: https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2019/MSIB_10_19.pdf

第二節　機會

以上所列四個面向，是建立「海域空間透明度」過程中，無可避免的挑戰，作者綜合研究所見及實務經驗，歸納出以下方向：

壹、提高海上目標偵測率及辨識率，以便獲得更佳的海域空間透明度

各巡防區岸際雷達可全天候監控海域動態、再加上艦艇的遠程及近程雷達協同偵蒐，已經具備了「早期預警」的基本條件，但對於小快目標的偵蒐能力，卻仍有精進之處，此等目標具雷達截面積小、雷達波反射率低之特性[60]，不容易被雷達發現，再加上背景雜訊干擾，更增加小快目標的辨識難度。於 2014 年，前海岸總局曾就雷達未能發現小快目標的 9 起案例進行過總檢討(如圖4-3)，其中有 6 案皆發生在近海區域，因目標體積低於雷達偵測規範所容許之最低偵測標準 (應大於 1 平方公尺) 而未被發現，如今雷達科技與當年科技已不可同日而語，功能上亦有明顯進步，惟在當前台海局勢未見和緩之前，仍應加強雷達人員對實際狀況之研判訓練，除了在教室內介紹案例外，更可考慮建置雷情模擬訓練機制。

圖4-3: 雷達無法發現小型快艇案例之查明情形

失即時反應妥處及攔截目標之先機，形成勤務罅隙，探討其實際無法監偵原因及擬定具體策進作為。

貳、查明情形：

經逐案查明 9 件案例，其中第 1 案為勤務交接時，未以人工作業鎖定微弱光點目標及完成交接，造成雷達目標漏鎖，第 3、4 案分別係因無法判定為海上目標及原已在盲區作業之工作船外，餘 6 案均屬雷達契約規範以外小船(船體截面積小於 1 平方公尺)及無動力漂浮之船隻，不利雷達偵蒐。近期海上可疑目標雷達監控未能鎖定例案，如附件。

[60] Tegowski, B., & Koelpin, A. (2024). Accuracy limitations of interferometric radar owing to the radar cross section of its antenna. *IEEE Transactions on Microwave Theory and Techniques*.

作者於 2019 年 6 月赴以色列、荷蘭進行博士論文研究時，也曾就上述威脅就教當地友人，發現大家所面臨的問題都大同小異，例如以色列要應付海上及陸上邊境的恐攻威脅，他們在邊境上廣設雷達站、無人機、機動及固定式紅外線/電子光學 (Electro Optical and Infrared, EO/IR) 等偵蒐系統，進行全天候監控，但仍免不了時有小快目標衝岸或闖入邊界騷擾，而且也多次是在當地民眾通報後，才開始採取反制行動。該國軍方鑑於一般雷達多有難於發現小快目標之限制，除維持既有偵蒐系統常態運作外，將重心置於提高闖入警戒區 (例如20公里內) 內小快目標之偵蒐及辨識能力，因此採用繫留式氣球 (Tethered Aerostat)，在其下方吊掛雷達、無線電中繼、Wi-Fi、EO/IR 等常用偵蒐及通信系統，隨氣球浮升於空中一定高度 (作業高度依裝備吊掛總重及氣球大小而定) ，對海 (地) 面進行全天候監控 (如圖4-4)，海 (地) 目標的一舉一動都能全程掌握 (如圖4-5)，因為從空中看地面沒有死角，而且誰在快速移動看得清清楚楚。據友人告知，此一機制建立後，小快目標衝岸的事件大幅減少，這種機制可部署於艦艇、車輛、建築物上，具有極佳的機動性，倘遇天候不佳時，可降低作業高度。相較於無人機，這種以氣球為浮力的空中滯留式監控系統，可滿足對責任區進行長時間的地面監控。

圖4-4：攜帶 EO/IR 於空中執行偵蒐任務的繫留式氣球 (出處：RT System)

圖4-5：攜帶 EO/IR 於空中執行偵蒐任務的繫留式氣球 (出處：RT System)

上圖所示，為空中滯留式監控系統的地面操控站，可顯示目標的活動路線及相對位置(如右上方的地圖)，並透過光學攝影機呈現目標所在附近之影像。

貳、善用AI系統驗證可疑資訊

利用假資訊去誤導另一方的認知，並據以做出錯誤決策以達到爭取優勢之目的，已被視為是認知戰一種。傳統的海上假資訊態樣，就是船員在本船的 AIS 主機上動手腳，對外發送不實船舶資訊，因為造假手法簡單，驗證上不困難。自從 AI 普及應用後，不法份子運用 AI 製造的假資訊將難於查證，主要是因為 AI 背後有大數據資料庫支持，透過邏輯運算模式，產出的結果幾乎已考慮到各種可能的因素。故利用 AI 製造的假資訊具有「深偽」(Deep fake) 之特徵[61]，換言之，AI 將各種可能的質疑都做了邏輯化處理，不怕使用者查證，照樣能達到混淆視聽及製造心理恐慌之目的，所以在這樣的威脅下，反而會刺激我們注意以下重點：

[61] 曾子軒. (2024年10月8日). 生成式AI，讓深偽與假資訊難防？Google高階主管：有解方. (遠見雜誌, 製作人) 2024年10月20日 擷取自 遠見高峰會: https://www.gvm.com.tw/article/116176

一、注意原始資料的品質及來源

AI 必須依賴數據庫內資料進行運算及匹配，所以透過資料校準 (Data calibration) 作業，可確保資料匯入 AI 系統的準確性和可靠性，除非原始資料是我方人員生成的，否則在開發 AI 系統時，應選擇來自可信賴且經驗證過的資料來源，避免使用社交媒體等可能摻假的資料。

二、運用具公正性之網路查核機制

當收到可疑資訊時，可上網檢查其內容之準確性，例如專門針對一般資訊提供內容驗證的 Snopes, PolitiFact, FactCheck.org、驗證文字型內容有無抄襲或查驗抄襲程度的 iThenticate, Turnitin, Grammarly Plagiarism Checker 等。

第三節　小結

壹、挑戰

本章就法律、非法律二個面向，檢視沿海國於建立海域空間透明度的過程中所將面臨之挑戰，謹採表列方式說明重點：

挑戰面	法律面	非法律面
海上假資訊所造成的多元威脅	透過自行立法，規定在國家司法權所及海域內活動的船舶，都要加裝AIS並須主動表明身分。	1. 確認船舶有無涉及違法或危安疑慮之首要之務，便是掌握「對方身分、意圖、航行態樣及其行為。 2. 建立共同作業圖像(COP) 當有助於落實達成海域空間透明度之要求。
AIS 假資訊已成為海上認知戰的一部分	國際社會目前並無相對之公約加以規範，各國關注焦點也多聚焦在跟傳統安全有關的事件上。	1. 就案例歸納，最常見的，便是警覺意識薄弱(應強化人員教育)。 2. 基於各種因素考量，未及時向外預警，致使他方也跟著受損。 3. 國際社會已經有因應措施，例如「國際船東互保協會」 便公開宣布，凡是船舶涉及操縱假資訊進行欺騙者，不在保險理賠之範圍。
駭客可透過網路從任何地方控制特定對象之 AIS	國際社會對於海上網域活動尚未建立相對應之公約以為約束依據，故在面對假資訊或惡意軟體挑戰時，須制定更明確的法律規範才行。	1. 操弄 AIS 最終目的，在引導行為者做出錯誤決定以逞其企圖。 2. 假資訊未經查證，便採取反應行動，很有可能落入他人陷阱，故在面對假資訊的同時，也是在挑戰主事者的決心下達、更是考驗勤指人員的應處專業。

對海上網域安全造成嚴重威脅	1. 面對海上假資訊之際，必須建立一套法律規範作為執法依據。 2. 透過立法及補助措施，讓所有的小型船艇筏都能加裝B型AIS (只發射不接收)以增進航行安全，有助於分辨彼此。	1. 發送 AIS 假資訊之行為，只是手法之一，新興方式，透過電子郵件夾帶病毒(如 Ryuk、Stuxnet、Icefog 等惡意軟體)攻擊海事產業所其造成損失更大。 2. 造成邊境安全問題，例如中國大陸船舶的 AIS 顯示為台灣籍，或台灣籍的船舶發出大陸地區的識別碼 (412、413、414)，已經隱約透露出「敵我不分」。

貳、機會

機會面	建議方向
提高海上目標偵測率及辨識率，以便獲得更佳的海域空間透明度	1. 除持續引進新式監偵系統外，還要在雷達專業訓練上與時俱進，應採取新思維規劃人員訓練方式，例如運用「情境模擬(模擬不同天候、海象下大小船舶的航行態樣)」。 2. 可參考荷蘭及以色列作法，整合各類偵蒐系統的情資，建立共同作業圖像並引進可持久性監控效能之工具。
善用AI系統驗證可疑資訊	不法份子運用AI製造的假資訊將難於查證，具有「深偽」(Deep fake) 之特徵，在這樣的威脅下，應注意以下重點： 1. 注意原始資料的品質及來源。 2. 運用具公正性之網路查核機制。

第五章　研究發現與建議

第一節　研究發現

在經歷11個月的資料研讀分析、教學 (提供研讀文獻列為雷達目標研判及辨識課程補充資料)、問卷調查 (利用 AI 軟體製作問卷調查) 及專家訪談等過程後，研究發現可歸納為以下五項：

壹、 海上假資訊之應用模式已多元化，在 AI 深偽技術支援下，將更難查證資訊內容。

海上假資訊已不單單只在 AIS 上作假，更出現了複合式的運用案例，例如不法份子製造假的 GPS 信號送入某船 AIS ，結合航行資訊對外發送，或駭客透過 AIS 公開頻道侵入特定目標內部網路，綁架或強制接管 AIS 主機，進行不法活動。近年來，人工智慧受惠於「大數據」(Big data) 運算方法及高階晶片應用而得以迅猛進步，在 AI 深度學習 (訓練機器像人類一般思考)下，利用「深偽技術」(Deep fake)[62] 所製作出來的資訊幾可亂真 (而且多以影片方式呈現更具說服力)，令人更難判斷其內容真假。

於 1980-1990 年代，大陸機帆船屢屢越界作業，在淡水至澎湖之間的海域，收到遇險求救信號乃是常事，主筆作者當時服務於瀋陽軍艦，每當接獲指揮中心傳來遇險信號通報時，本艦艦長總是第一時間加速前往遇難地點進行搜救，可往往到了現場卻不見遇難對象，如今回想應是被假資訊所欺騙，有可能是中了對方調虎離山之計。在第二章第二節中，作者納入類似案例，在經過查證後，確認收到的信號有假 (屬多船共用一身分之 AIS 欺騙模式)，意在誘使巡邏艇離開責任區造成執法真空，故面對海上資訊時，唯有多方查證，才有可能免於被騙。

[62] 是一種利用人工智慧技術(特別是深度學習)，來合成或操控資訊內容的技術，這種技術可以生成非常逼真的假影片、音頻或圖像，例如將一個人的面部特徵或聲音替換成另一個人，讓外界難以辨別真偽。

貳、應從網域安全之角度看待 AIS 假資訊所造成之潛在威脅。

2011 年 12 月主筆作者初任查緝員，於當時，只要發現有船舶運用 AIS 假資訊 (以下稱 Fake AIS)，冒充他船身分活動情事時，即屬關注性案件，如今不依規定使用 AIS、隨意關機 (IMO 規定只有航行在海盜或武裝搶劫出沒之海域時才能關機) 等現象早已司空見慣[63]。按理說，海巡同仁對 Fake AIS 應該不陌生才對，但依據問卷回復分析，許多同仁對「不法份子利用 Fake AIS 的欺騙模式、如何辨識身分真假」等作業仍多有不知之處，更遑論實務上的攻防，同樣的，在本文所歸納之 46 個案例中，也明顯發現，許多海上假資訊或遭到惡意軟體攻擊之當事人，往往基於面子或營運考量，不會主動對外揭露，因此實際發生的案例應該會更多，Fake AIS 所造成的潛在威脅，約可分為以下幾點：

(一) 隱蔽真實位置或製造假船位，進行各類海上非法活動。

(二) 可能導致航運交通管理作業之誤判，例如散佈假訊息造成航道堵塞、擱淺或發生碰撞等海上事故。

(三) AIS 傳訊作業不具備加密和驗證機制，再加上採用公開頻率，易受到網路攻擊，例如使用「社交工程」混淆訊息，或運用「分散式阻斷服務攻擊」(Distributed Denial of Service, DDoS)[64]，藉以達到癱瘓目標正常收訊作業之目的。

(四) Fake AIS 可能被軍艦、海上民兵船或不法份子，用以隱匿行蹤(例如北約、英國及俄羅斯等， 已將操弄 AIS 技巧納入海軍正規戰術)，或誤導執法資源用於錯誤地點，從而干擾海域執法或安全警戒之精準度。

(五) 現代化的船舶及VTS中心都具有資料庫，一旦假資訊透過內部網路存入 AIS 資料庫，不知情的工作人員極有可能誤用而造成再次擴散，例如在規劃航線時，因使用假資訊而做出錯誤的決策，導致增加航行安全風險。

---

[63] d'Afflisio, E., Braca, P., & Willett, P. (2021). Malicious AIS spoofing and abnormal stealth deviations: A comprehensive statistical framework for maritime anomaly detection. *IEEE Transactions on Aerospace and Electronic Systems*, *57*(4), 2093-2108.

[64] 駭客針對特定電腦系統進行飽和式攻擊(如惡意軟體)製造大量且密集的資訊請求服務或發送垃圾訊息讓對方電腦一直處於收信狀態況，進而達到癱瘓或中斷正常功能之目的。

參、惡意軟體 (Malware) 成為海上網域安全的首要威脅。

現代化船舶均設計在網路環境下作業，以節省人力及效率，相關的安全機制及各種使用規定亦屬完備。理論上，外界的惡意軟體應無法侵入才對，但從案例來看，卻可明顯發現應然和實然面的巨大差異，原因可歸咎於「人」的因素 (只有人才會便宜行事)。 如圖 5-1, 5-2 所示，在 2010-2020 年之間，海上假資訊及網域危安事件中的受害者中以「船舶」、「航商」最多，主要是工作人員所使用的 USB 及電子郵件所造成，後者通常會以附件方式夾帶惡意軟體，一旦收信人點閱後，惡意軟體便會透過網路，進入整個內部系統伺機破壞，這種經由三部曲 (網路、電子郵件、釋放惡意軟體) 造成實體系統受損的攻擊模式稱為「網域實體攻擊」(Cyber-physical attack)。其次，則是船員未依規定使用 USB ，例如拔出原先插在 AIS 主機上的 USB 後，再插入電子海圖系統使用，便將惡意軟體散布至其它系統，造成本單位更嚴重的傷害。

圖5-1: 2010-2020 年海上假資訊及網域危安事件受害者之類別

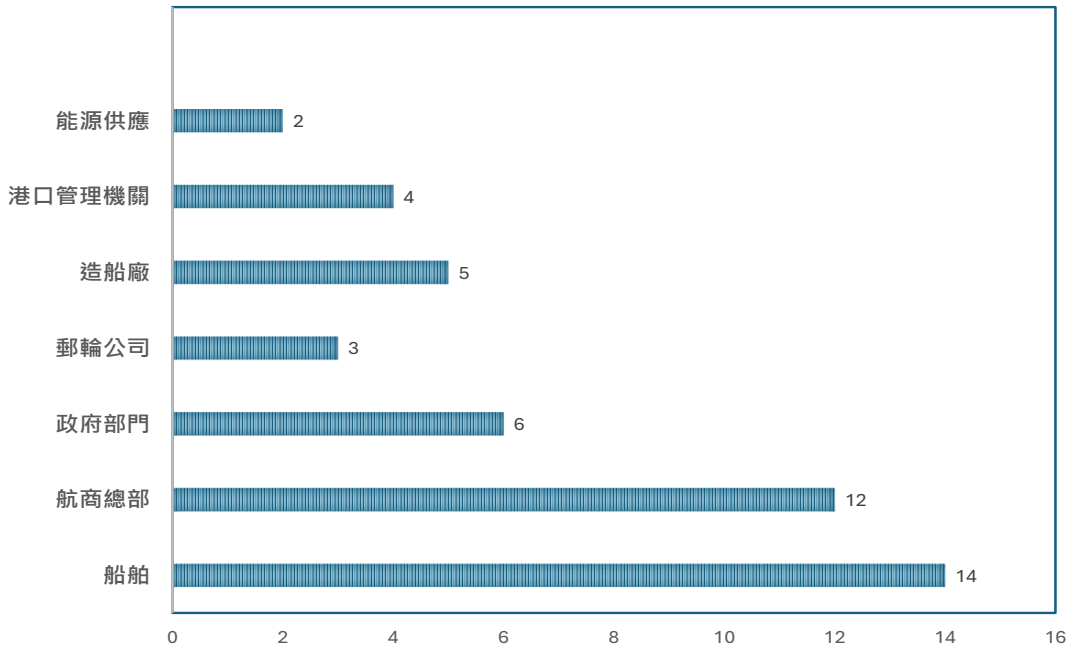
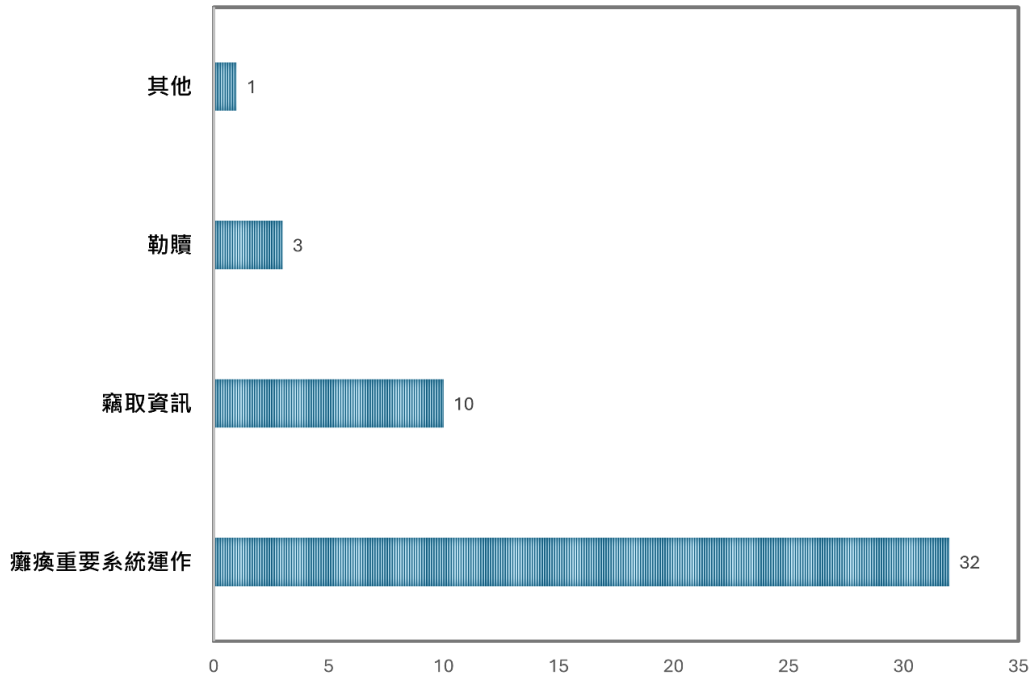


圖5-2: 2010-2020 年海上假資訊及網域危安事件之類別



根據美國學者 Gary C. Kessler 所做研究指出[65]， 惡意軟體對艦艇的航儀 (包括全球衛星定位系統、雷達、電子海圖及AIS) 及資訊系統威脅最大，所以他在 2019 年的「海上人命安全及保全月刊」(美國海岸防衛隊刊物) 特別撰文呼籲，必須制定所謂的「網域衛生政策」(Cyber-hygiene policy)[66] 以便對抗透過網域空間侵入系統的惡意軟體攻擊。

肆、海巡同仁對 Fake AIS 之威脅、操縱模式之認知程度亟待加強。

研究小組運用生成式 AI ，製作了一份有關 AIS 主題之問卷 (計 21 題)，請 5 個不同班次的 231員學 (平均年齡27歲、男女性各占 81%、19%，平均服務年資為 6 年以上)，進行不記名 Google 問卷調查，學員們對海巡勤務內容及執行都有一定程度理解和經驗，然而問卷結果 (如附件 2) 卻顯示，應然及實然面的明顯差異

[65] Kessler, G. C. (2019, March 25). Cybersecurity in the Maritime Domain. *The Coast Guard Journal of Safety & Security at Sea, Vol. 76* (1), pp. 34-39.
[66] 網路衛生是指使用者為了保護個人、組織或設備的網路安全，所進行的一系列日常或定期的安全措施與行為。

(如圖5-3)。

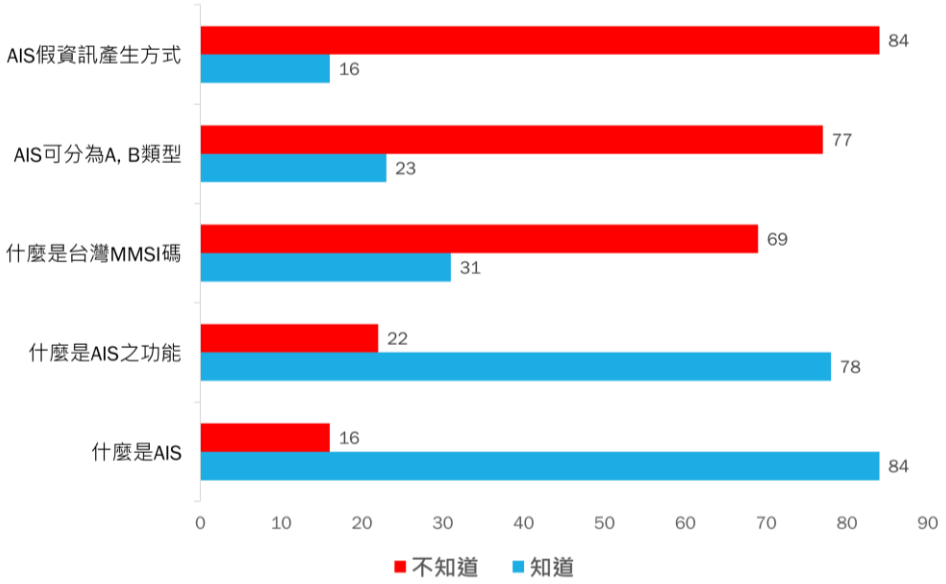
(一)為什麼知道 AIS 的人數 (84%) 多於知道 AIS 功能的人數 (78%)？

理論上，知道 AIS 的人應該也要知其功能才對，但兩者卻差了6%，這個差異可解釋為「從事跟 AIS 相關業務的人數較少，所以知道 AIS 功能的人也相對少」，畢竟大多數人的工作和 AIS 沒有直接關係，但運用 AIS 判別船舶身分是海巡人員應具備之基本知識之一，故可透過強化學習方式，增進這 6% 的人對 AIS 功能的了解。

(二) 不知道台灣 MMSI 碼的人數多於知道人數之差異分析。

AIS 資訊中，有一個名為「MMSI」的識別碼，它由 9 位數字組成，前 3 位數為國籍碼， 台灣的編號為 416，從問卷數據顯示，不知道的人竟高達 69%，這是令人無法理解的現象，如果海巡同仁連台灣船舶的身分都不知道如何辨識的話，那如何能勝任港口安檢、雷達操作或情資研判等工作？所以這突顯了在職訓練的問題。

圖5-3 : 問卷調查重點項目分析



(三) 知道和不知道 「AIS 可分為 A、B 兩種類型」的人數差異分析。

一般商船 (即符合 SOLAS 標準) 必須使用 A 型系統，其他小型船舶則使用 B 型系統，前者具有 AIS 資訊收發功能，後者只能發射本身的航行資訊，對此不知道的人數高達 77%，顯見大部分學員對運用 AIS 及相關規定都缺乏了解。

(四) 知道和不知道 Fake AIS 的產生方式之差異分析。

高達 84% 的學員不知道 Fake AIS 是如何產生的，鑑於這些人都將成為領導幹部，所以這又是一個令人擔心的現象，顯見某階段的在職訓練出現問題，必須瞭解不法行為的運用模式及手段，如此才能更有效率的識別海上船舶。

伍、專家訪談

一、 IMO 明令船舶禁止 AIS 資訊造假，但為何仍有船舶可發出假資訊？

受訪專家表示，這跟商業利益很有關係，很多 AIS 銷售商在不願得罪客戶之下，往往會罔顧規定，向客戶提供後門程式，所以船舶才能製造假資訊，除非國內通過立法強制執行，否則在利益考量下，船舶仍會持續製造假資訊。

二、 針對近期船舶冒用變造的 MMSI 碼(船舶的國籍碼)，有無解決辦法？

近期出現「明明是我國籍船舶，但其AIS資訊卻顯示為大陸籍」之案例，不難理解這類船舶使用的是大陸製造的AIS，換言之，這些船舶應已入中國籍，但船主有可能會再加裝一部由台灣主管機關核發 MMSI 碼的 AIS (以方便在海上活動)，如此一來，這艘船舶就會有二台 AIS，可隨時換用不同的身分在海上活動。另一類案例則更具威脅性，即「大陸籍船舶於海上活動時，發出的是台灣地區的 MMSI 碼」，藉以矇騙巡防區雷達監控，這個問題的危害程度更甚於前者，因為不知來者是何人(武裝船艇、漁船或民兵船) 專家認為，主政機關可要求在台灣地區販售的 AIS (不論是哪一國製造)，都必須加裝特別的識別碼產生器，當巡防區雷達收到海上船舶的 AIS 資訊時，即可檢視此一隱藏的識別碼，以確認船舶真

為台灣註冊之船舶。

三、不法份子如如何操弄 AIS 製造假訊息？

基本上只要符合國際海事組織 (IMO) 規範的 AIS 製造廠商，其生產的AIS主機，僅能於出廠前依照客戶需求設定 (一次) 船舶相關資訊 (後續廠商不會再協助客戶變更船舶資訊)；惟不遵循 IMO 規範所生產之 AIS 主機，則可運用外接資訊設備變造船舶相關資訊，或直接在主機上逕行設定。

四、如何防範駭客透過公開頻率侵入特定對象 AIS 主機進行操控？

(一) AIS 的設計是在「公開架構、公開頻道、內容不加密」的前提下運作，因此駭客只要具備適當設備，便可透過無線電頻道，攔截、接收和分析 AIS 數據，以此追蹤實際船舶船位並同時植入惡意軟體，在其指揮下進行破壞活動。

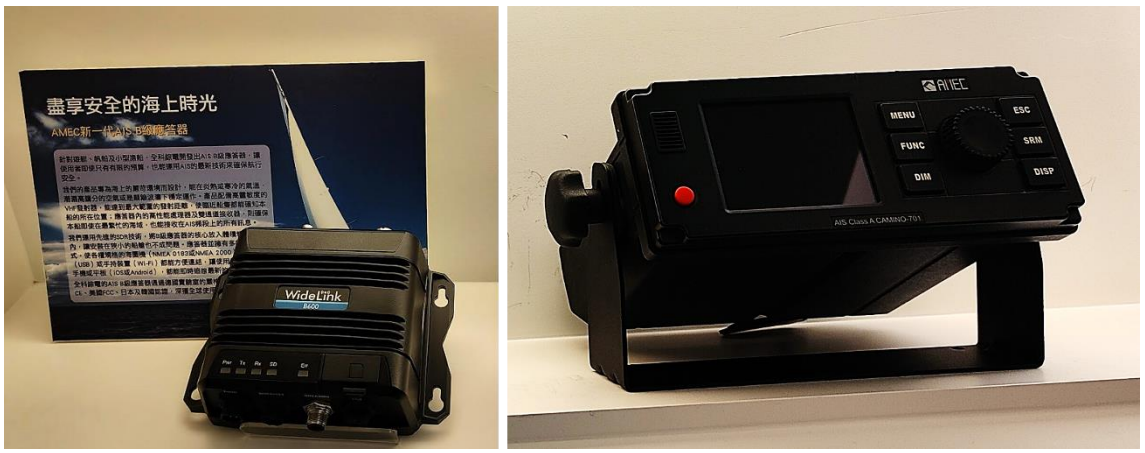
(二) 因為 AIS 是開放性系統，要防範駭客的確很難，曾有人提出對資訊加密之建議 (技術上沒有問題)，但接收方的 AIS 主機若沒有解密裝置，將無法解讀所收到的 AIS 資訊，如此將產生更大的航安風險。

五、有些國家為便於管理 20 噸以下小型艇筏，有規定要加裝型 AIS-B 型主機，我國海巡署也準備推動立法，請問 B 型功能和 A 型主要的差別何在？艇上的人能否更改資料? 一套 B 型 AIS 的成本約多少錢？

(一) AIS主機可區分為 Class A、Class B^+、Class B 等三種機型(如圖5-4)，前兩種機型可以發射與接收訊號，惟 Class B 僅能發射訊號，無法接收訊號。

(二) 船艇上人員可否操弄 AIS 主機製造假資訊，端視該主機是否為合法廠商所製(即係符合國際海事組織 IMO 規範，經由多國認證許可)，若然則無法任意變更船舶資訊，反之，艦艇上人員即可透過主機本身或藉由連結外部資訊設備竄改船舶資訊。

圖5-4：圖左為 AIS/B 型主機、右為 A 型主機其面板左半邊為 LCD 顯示，右為旋轉式按鈕可供使用者操作各項功能 (出處: 呂佳龍教官提供)



(三) 目前 B 型 AIS 主機安裝費用約為 2 萬元，即為我國漁業署目前「漁船筏裝設攜帶式船舶自動識別系統船載臺補助作業規範」所補助之金額，依報載目前全臺 20 噸以下船筏約近有 20000 艘，安裝率僅兩成。

第二節　建議

從問卷調查回收所做之分析中，可清楚發現高達 60% 以上的學員對於 Fake AIS 均缺乏完整理解，由於 AIS 制度行之有年，且關乎 IMO 全球航行安全政策及相關科技，實非研究小組所能置喙，因此本節僅聚焦以下三點，提出淺見以供參考。

壹、 改善現行在職訓練機制不足之處

欲建立學員對 Fake AIS 問題及衍生性海上安全問題之全面理解，應盡量滿足「師資、教材、情境教學模擬設備、適當課程規劃」等要求(且稱為四大要素)，才有可能達到最佳教學效果。主筆作者以「雷達目標辨識查證分析研判」課程為例略舉如下：

一、師資

上述課程涵蓋「雷達應用、回跡 (Echo) 辨識、海上船舶身分查證、行為動態分析、研判意圖、海圖判讀」等多個專業領域，理應由多位講座協同授課才對，然礙於各種因素限制，目前僅有一位老師授課，這位講座必須具備多方經驗及實務方能擔綱授課，但適當人選猶如鳳毛麟角且未必請得來，基於長遠計，必須培養自有師資才是治本之道；另一個重要條件，則是要有能力閱讀國際期刊相關文獻，原因如下：

(一)國內海上相關案例基於各種原因，往往不易取得完整資訊，尤其是在跨部門請求提供資料時，總會因為不明原因或程序而無法及時或取得完整資訊，進行客觀性案情分析，即使只是用於教學亦有相當難度。

(二)投書國際期刊之作者，多為學(業)界人士，在國外資訊分享制度化的環境下，文章所引用之案例相對完整而且還會經過匿名審查機制，故可信度高，有助於教學參考。

二、教材

教材是增進學習效果的必備項目之一，以本中心為例，前身為前海岸巡防總局之人員研習中心，當時每一個班次開訓前夕，均有專人在教室內的每一張課桌上，擺放一套基本文具及課本，2018 年組改後，本中心成為四級機構，配置人事、主計單位及編列獨立預算，教官也依規定逐年更新教案，但反而無足夠經費印製教材(主要是預算按比例逐年刪減)，只能給學員電子檔自行閱讀。爰建議，上級機關對教育訓練的重視，除政策指導外亦應給予更多的實質幫助 (例如不被刪減教育訓練預算、更新裝備時也要兼顧教學訓練單位之需求[67])。

三、充分運用情境教學模擬軟體設備

利用教學模擬設備 (不論是軟體或硬體) 強化學習效果已是趨勢所在，主筆作者於 2017 年曾就精進巡防區雷情目標辨識研判作業需要，參觀台北海洋科技大學海事專業教室內的 AIS、全球遇險安全系統 (Global Maritime Distress Safety System, GMDSS)、應急指位無線電信標 (EPIRB) 等模擬教學軟體設備 (實體仿真模擬亦為方法之一，但成本昂貴且有維護支出)，並親身體驗此種教學模式，在老師講解後，學生便可自行操作設定參數或製作假資訊，透過教室內部網路模擬海上發送場景，此種輔具教學可讓學生快速融入課程並建立深刻印象，較之本中心現行傳統教學方式(教官說、學生聽)，學習效果高下立判。

四、與時俱進的課程規劃

課程規劃範疇甚廣且涉及教學資源分配，長久以來，海巡各階教育課程都一律區分為「法律」與「專業」二類，主筆作者認為有失精準，難道法律不是專業項目嗎？其他以海巡勤務為主的專業課程中就沒有法律成分嗎？這種因應早年訓練需求的一刀切分法，無法突顯當今科技教育的重要性，爰建議應在現有的類別

[67] 例如在向海致敬專案中，海巡署交由東部分署統籌購置之遙控式動力救生圈就沒想到教學單位需求，以致於上課時必須向廠商或其他勤務單位商借使用，潛水設備(含潛水衣)也只配置4套，由於數量太少以致無法用於教學。

中，再分出「科技」類別，則相關課程 (如衛星通訊、電磁應用、海上資安、AI 應用、大數據運算等) 方可歸入正確類別，得到合理的教學資源分配，例如一個20小時的英語課程以外聘鐘點費計須 40000 元 (2000元/時)、「雷達目標辨識查證分析研判」課程為 4 小時卻只有鐘點費8000元，二者性質雖有不同，但英語說不好不會影響到國安，然雷達偵蒐及海上目標辨識分析研判作為，卻容不得半點失誤空間，因為直接攸關國安。

貳、對 20 噸以下之艇筏制定加裝 AIS 之法規，以利建立海域空間透明度之優勢。

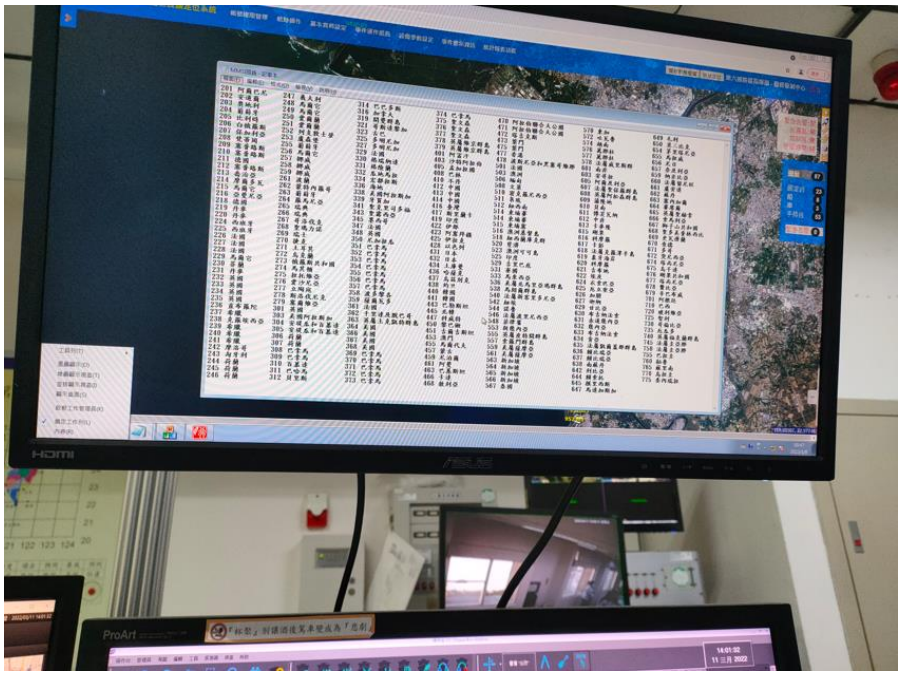
以往常有不明身分小型快艇侵入我方海域事件發生，然在前兩岸氛圍之下，同樣的事件卻多了國安顧慮，由於此類目標截面積小、速度快，儼然形成海域安全另類威脅，基於人命安全及海域維安之雙重考量，亦應將 20 噸以下之艇筏納入強制安裝 AIS 之對象[68]，如此，當雷達偵蒐海面目標時，只須針對無 AIS 資訊顯示之目標加強監偵，即可以建立更佳的海域空間透明度之優勢。當然這也不能只要求船舶加裝 AIS 而已，海上的各式導航裝置、定置漁網、風機等，也要納入加裝 AIS 的強制對象，才能在巡防區的共同作業圖像中，完整呈現海域內的各類行為者 (Actors) 的相對位置及動態。

參、建立正確心態之外更要營造具有時刻提慎防假資訊之環境

經由強化教育訓練方式，提升同仁對 Fake AIS 之認識與防制之道是正規作法，但在本文所參考的46個案例中，卻可發現許多的失誤都可歸咎於便宜行事心態或走捷徑的結果，畢竟建立正確認知是一回事，時刻警惕又是一回事，因此周遭環境的提醒機制扮演著重要作用。以主筆作者於 2022 年 3 月 11 日前往第六巡防區進行測考所見為例，當本中心帶隊官於現場，下達「不明身分海上目標辨識狀況」之後，作者明顯發現在某雷達席位上方，竟有電視面板時刻顯示各國船舶的國籍

[68] 交通部於2018年7月27日，已公告修訂後之「船舶設備規則」(於2019年7月起開始執行)，規定總噸位 20 以上的各式船舶須裝設 AIS，並在領海內活動時保持開啟狀態。

圖5-5：第六巡防區所設置的船舶國籍快速辨識表



辨識碼(如圖5-5)，此一提醒機制，讓雷達操作人員能有效避免錯誤辨識，進而影響海上監偵作業。

肆、各分署應善用機動輔訓機制，調派適員參訓以提升勤值同仁本職學能

機動輔訓是本中心承海巡署指導所建立之訓練機制，訓練對象皆為各地區分署之種子教官，自 2024 年起已將「雷達目標辨識查證分析研判」課程列為必訓科目之一。鑑於巡防區雷達作業小組，日後將回歸各分署岸巡隊，其在職訓練亦將由各分署接手，故於派員參加年度機動輔訓時，應以擔任相關工作者為主要參訓對象，以落實訓練成效。

伍、運用 AI 建立海上假資訊辨識機制以輔助巡防區勤務作業

以上建議，仍有其限制性，例如機動輔訓、各階班次的訓期都有固定時間及實施頻率，無法隨時滿足各巡防區要求，故分署建立自訓師資方為治本之道，但必須推出配套措施 (如經費、專責專人) 方有可能見效，這一步需要時間逐步建立無法揠苗助長。惟以下案例，可供未來設計提升海域偵監輔助機制之參考，主筆

作者回憶於 2016-2017 年任職前海岸總局勤指中心時，受命參與某委外案研究成果評鑑作業，該案要求承攬方，應透過「機器學習」之研究途徑(Approach)，蒐集各巡防區「易走私偷渡熱點區」內曾發生案例之雷達目標航跡，經過分析後，建立大數據資料庫，以供日後人發現可疑目標時，將其航跡匯入資料庫進行比對，以科學化數據做為情資研判之依據。如今 AI 技術突飛猛進，建立海上假資訊辨識機制應非難事。

附錄

一、AIS 假資訊及其衍伸性威脅 (2010-2020 年之 46 起案例)

編號	態樣	年度	概述及參考來源
01	惡意軟體	2010	建造中的鑽油平台完工後，準備從南韓駛往南美洲，於航前階段其主控制系統被駭客侵入並植入惡意軟體，被迫停機 19 天，損失約 70 萬美金。 Drougkas, A., Sarri, A., Kyranoudi, P., & Zisi, A. (2019). Port Cybersecurity. Good practices for cybersecurity in the maritime sector. *ENSISA*, *10*, 328515.
02	惡意軟體	2010-2011	駭客透過 WiFi 網路侵入某希臘航商總部，竊取該公司船運資料並提供亞丁灣海盜集團策劃不法之用。 Polychronis, K.: Cybersecurity at Sea. In: Otto, L. (ed.) Global Challenges in Maritime Security. p. 243 Springer International Publishing (2020).
03	惡意軟體	2011-2013	比利時 Antwerp 港務局的貨物追蹤系統被駭客侵入，用以協助槍毒走私(以南美洲香蕉名義作掩護)，此一非法活動持續二年才被發現。 Walker, J., Spencer, J.: Cyber Marine: Risks & Loss Scenarios, http://www.marineclaimsconference.com/imcc-docs/docs/Cyber%20workshop.pdf.
04	惡意軟體	2011-2013	名為冰霧 (Icefog)之惡意軟體(為蠕蟲病毒之一種)，於 2011-2013 年針對南韓、日本、烏克蘭等國家之大型企業及海運公司進行網路釣魚式攻擊，以竊取電子郵件、網路帳戶之密碼為目標。 GREAT: The Icefog APT: A Tale of Cloak and Three Daggers, https://papers.put.as/papers/malware/2013/icefog.pdf-apt-threat.pdf

05	惡意軟體	2011	伊朗 IRISL 海運公司遭病毒入侵，所有業務資料均被破壞，同時和所屬船舶的通信系統亦受波及無法使用，造成嚴重損失。 CyberKeel: Maritime Cyber-Risks, https://maritimecyprus.files.wordpress.com/2015/06/maritime-cyber-risks.pdf,
06	惡意軟體	2011	伊朗官方報導，一艘鑽油平台於波斯灣外海，遭惡意軟體攻擊(透過衛星天線侵入)，導致該船資訊系統停擺 15 天。 Singh, H. (2019). *CYBER SECURITY IN MARITIME INDUSTRY The Exposures, Risks, Preventions and Legal Scenario* (master's thesis).
07	惡意軟體	2012	澳洲海關及邊防局的「貨物轉運及查核系統」遭駭客置入蠕蟲病毒，可窺視該局之貨物安檢紀錄並進行竄改。 CyberKeel, Copenhagen, & Denmark (2014). MARITIME CYBER-RISKS.
08	惡意軟體	2012	駭客利用電子郵件夾帶病毒方式，侵入丹麥海事局並成功竊取機敏性資料。 Schwarz, M., Marx, M., & Federrath, H. (2021). A Structured Analysis of Information Security Incidents in the Maritime Sector. *ArXiv*. /abs/2112.06545
09	惡意軟體	2013	一艘美籍鑽油平台於墨西哥灣作業，因船員所攜帶之電腦及 USB 受病毒感染，於連線時感染船上動力系統，致無法航行達 3 天之久。 Knox, J.: Coast Guard Commandant on Cyber in the maritime domain, https://mariners.coastguard.dodlive.mil/2015/06/15/6152015-coast-guard-commandant-on-cyber-in-the-maritime-domain/
10	惡意軟體	2014	駭客透過電子郵件，置入 Stuxnet 蠕蟲病毒，竊取造船廠的銀行帳戶密碼，造成重大損失。 CyberKeel: Maritime Cyber-Risks, https://maritimecyprus.files.wordpress.com/2015/06/maritime-cyber-risks.pdf

11	AIS 假資訊	2012-2014	依據以色列海事資訊公司(Windward)2014 年年報統計，於 2012-2014 年全球船舶使用假身分航行者約有 1%，航行時不發射 AIS 資訊者約占 25%，後者態樣多半與走私、人口販運、恐怖活動等有關。 Windward: AIS Data on the High Seas: An Analysis of the Magnitude and Implications of Growing Data Manipulation at Sea. (2014).
12	偽造衛星導航信號	2016	疑似駭客利用「假衛星定位資料」(GNSS manipulation) 攻擊南韓釜山，致使 280 艘船舶導航系統故障或停機，事件發生後南韓政府查不出問題所在。 Polychronis, K.: Cybersecurity at Sea. In: Otto, L. (ed.) Global Challenges in Maritime Security. p. 243 Springer International Publishing (2020).
13	電子情報偵蒐	2014-2017	挪威海事局統計，2014-2017 年在其海域多次出現俄羅斯商、漁船異常滯留事件，時機均在北約軍事演訓期間，疑為從事電子信號偵蒐活動。 Schnelle, S.: Kartlegging av maritime hybride trusler. Kan bruk av stordata og sosial nettverksanalyse bidra til økt maritim situasjonsbevissthet? Forsvarets Høgskole (2018). Wallace, T., Mesko, F.: The Odessa Network Mapping Facilitators of Russian and Ukrainian Arms Transfers, https://globalinitiative.net/analysis/the-odessa-network-mapping-facilitators-of-russian-and-ukrainian-arms-transfers/
14	惡意軟體	2017	駭客透過電子郵件，置入 Stuxnet 蠕蟲病毒，竊取英國航商 Clarkson 公司機密文件並要求支付贖金。 Nguyen, L.: Collaboration in the Shipping Industry: Innovation and Technology, https://informaconnect.com/epaper-collaboration-in-the-shipping-industry-innovation-and-technology/
15	偽造衛星導航信號	2017	在黑海靠近 Novorossiysk 港口外海(俄羅斯南部港阜)，有 20 艘船舶的 GPS 導航定位出現 32 公里之誤差，疑似有駭客入侵 GPS 輸送假信號。 Hambling, D. (2017, August 10). *Ships fooled in GPS spoofing attack suggest Russian cyberweapon*. Retrieved September 26, 2024, from New Scientist: https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/#.

16	惡意軟體	2017	NotPetya 勒索軟體透過稅務會計軟體 MeDoc（在烏克蘭稅務會計師中廣泛使用）的更新修補程式，侵入全球航運巨頭馬士基 (Maersk) 之營運系統造成嚴重癱瘓，據該公司估計，此一攻擊事件對全球約 1/5 的航運業務造成了延宕，其中包括 76 座港口。 馬士基估計，該事件導致收入減少，造成經濟損失近 3 億美元，超過 4000 台伺服器、45000 台 PC 和 2500 個應用程式必須重新安裝。 Leovy, J. (2017, August 17). *Cyberattack cost Maersk as much as $300 million and disrupted operations for 2 weeks*. Retrieved September 26, 2024, from Los Angeles Times: https://www.latimes.com/business /la-fi-maersk-cyberattack- 20170817-
17	偽造衛星導航信號	2017	在上述同樣海域，一艘海上作業船舶發現其 GPS 顯示，船位竟在陸地上，這種假信號出現 3 次，每次都在 30 分鐘以上(據信是有不明國家在測試網路武器)。 Vold, L.B.: Den Norske Krigsforsikring for Skib, https://www.warrisk.no/,
18	惡意軟體	2018	疑似中國駭客侵入美國海軍承包商資料庫竊取機密文件。 Lubold, G., Volz, D.: Chinese Hackers Breach U.S. Navy Contractors - WSJ, https://www.wsj.com/articles/u-s-navy-is-struggling-to-fend-off-chinese-hackers-officials-say-11544783401,
19	惡意軟體	2018	美國海岸防衛隊海事運輸安全行動中心受到 (MTSA) Ryuk 惡意軟體攻擊，造成 IT 控制系統失能 30 小時，重要設施之攝影機控制系統無作用。 Blackmore, C. (2019, December 16). *Cyberattack Impacts MTSA Facility Operations*. (USCG) Retrieved September 29, 2024, from Marine Safety Information Bulletin: https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2019/MSIB_10_19.pdf

20	惡意軟體	2018	為上述惡意軟體攻擊事件之翻版，就「海事運輸安全行動中心」被攻擊後第 5 天，聖地牙哥港於 2018.12.25 也傳出相同攻擊事件。 *2018 Highlights: Major cyber attacks reported in maritime industry*. (2019, December 26). (USCG) Retrieved September 29, 2024, from SAFETY4SEA: https://safety4sea.com/cm-2018-highlights-major-cyber-attacks-reported-in-maritime-industry/
21	惡意軟體	2018	疑似伊朗駭客於 2018 年 10 月，運用 Ryuk 惡意軟體攻擊澳洲 Austal 造船廠，該廠主要承造澳洲及美國海軍艦艇。 *2018 Highlights: Major cyber attacks reported in maritime industry*. (2019, December 26). (USCG) Retrieved September 29, 2024, from SAFETY4SEA: https://safety4sea.com/cm-2018-highlights-major-cyber-attacks-reported-in-maritime-industry/
22	惡意軟體	2017-2017	駭客組織(Cold Galleon)針對南韓及日本造船廠、海運公司發動網路攻擊，以竊取造船設計相關資料為主，並於暗網 (Dark web) 販售。 Secure works: GOLD GALLEON: How a Nigerian Cyber Crew Plunders the Shipping Industry, https://www.secureworks.com/research/gold-galleon-how-a-nigerian-cyber-crew-plunders-the-shipping-industry,
23	惡意軟體	2018	中國遠洋運輸集團(COSCO)北美公司受到駭客攻擊，透過 email 將勒贖軟體置入資訊系統，封鎖該公司電子郵件伺服器達 5 天之久。 https://channel16.dryadglobal.com/maritime-cyber-security-threats-nov-2020-week-3
24	惡意軟體	2018	義大利石油業者 Saipem 公司在中東及北非的營運據點約有 400 台伺服器遭受勒贖軟體攻擊，所幸大部分資料都有備援，這次攻擊造成 5 天的停工。 Maritime Executive: Saipem's Servers Hit by Cyberattack, https://www.maritime-executive.com/article/saipem-s-servers-hit-by-cyberattack,

25	惡意軟體	2019	一艘大型船舶於接近紐約港時，其駕駛系統遭到惡意軟體攻擊，嚴重影響航行安全，事後經調查係因船員接收電子郵件時點閱夾帶之附件，致病毒侵入船上內部網路。 Lemos, R. (2019, July 10). *Coast Guard Warns Shipping Firms of Maritime Cyberattacks*. Retrieved May 25, 2024, from Dark Reading Logo: https://www.darkreading.com/vulnerabilities-threats/coast-guard-warns-shipping-firms-of-maritime-cyberattacks
26	偽造衛星導航信號	2018-2019	於 2018-2019 年期間，在挪威北部海域，發生多起 GPS 信號被干擾情形，造成船舶導航定位有極大誤差(類似第 15 項)。 Grant, A., Williams, P., Ward, N., & Basker, S. (2009). GPS jamming and the impact on maritime navigation. *The Journal of Navigation*, *62*(2), 173-187. Papadimitratos, P., & Jovanovic, A. (2008, October). Protection and fundamental vulnerability of GNSS. In *2008 IEEE International Workshop on Satellite and Space Communications* (pp. 167-171). IEEE.
27	惡意軟體	2019	美國加州長堤港遭 Ryuk 惡意軟體攻擊，造成港口重要基礎設施停擺 3 天。 Cimpanu, C. (2019, December 29). *US Coast Guard discloses Ryuk ransomware infection at maritime facility*. (ZD NET) Retrieved September 23, 2024, from https://www.zdnet.com/article/us-coast-guard-discloses-ryuk-ransomware-infection-at-maritime-facility/
28	惡意軟體	2019	依美國政府宣稱，針對其東南部地區天然氣輸送管路所發動惡意軟體攻擊，造成該區域供應斷氣 2 天，據信是由東歐的 ARKSIDE 網路犯罪組織所發動。 Christine Buurma, Alyza Sebenius. (2020, February 20). *Ransomware Shuts U.S. Natural Gas Compressor Facility for Two Days*. Retrieved Octomber 25, 2024, from Carrier Management: https://www.carriermanagement.com/news/2020/02/20/203485.htm Nakashima, E., Torbati, Y., & Englund, W. (2021). Ransomware attack leads to shutdown of major US pipeline system. *The Washington Post*, NA-NA.
29	惡意軟體	2019	英國老牌海事服務業者(James Fisher & SON)，因遭受 Ryuk 惡意軟體攻擊，未免災情擴大，關閉所有數位系統，致股市價值跌落 7% Cimpanu, C.: Ransomware Infection Cripples Shipping Giant COSCO's American Network, https://www.bleepingcomputer.com/news/security/ransomware-infection-cripples-shipping-giant-coscos-american-network/,

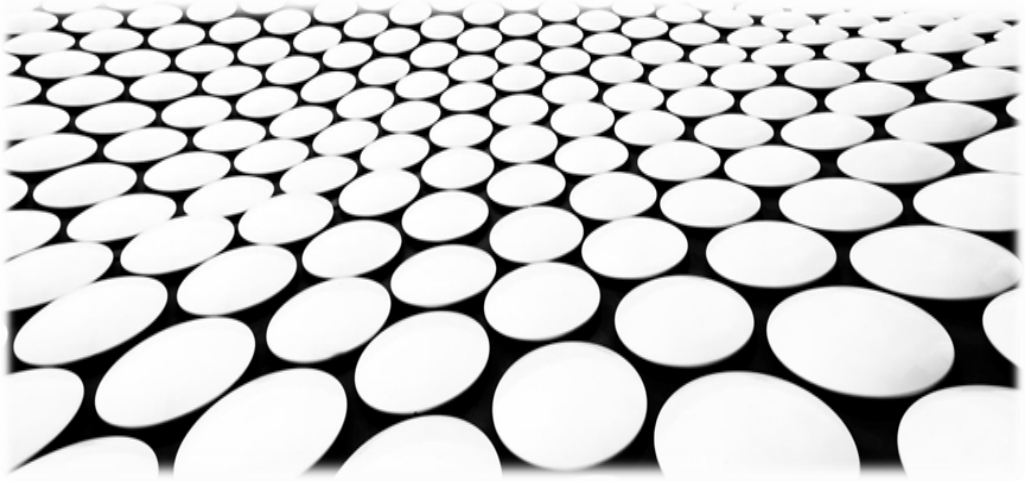
30	惡意軟體	2019	一艘油輪於駛入芬蘭 Naantali 港口時，其行政作業伺服器遭惡意軟體侵入，將資料完全鎖死，同時也清除了船上備份檔案，最後確認是船員不經意開啟電子郵件附件所致。 Danilin, G., Sokolov, S., Knysh, T., & Singh, V. (2021, May). Information security incidents in the last 5 years and vulnerabilities of automated information systems in the fleet. In *International Scientific Siberian Transport Forum* (pp. 1541-1550). Cham: Springer International Publishing.
31	惡意軟體	2019	義大利 Lentlugino 海運公司所屬二艘散裝貨輪，於地中海航行時，遭到 Hermes 2.1 型蠕蟲軟體攻擊，動力系統無法正常運轉，據信是透過 GMDSS 的電子郵件夾帶檔案侵入。 Meland, P. H., Bernsmed, K., Wille, E., Rødseth, Ø. J., & Nesheim, D. A. (2021). A retrospective analysis of maritime cyber security incidents.
32	惡意軟體	2020	一艘錨泊在英國 Tynemouth 港外的商船，遭到 Ryuk 惡意軟體攻擊，所有資料均被加密無法使用，船公司特地調派 IT 人員上船搶救，仍無法解密，最後只好重新安置電腦系統。 Soner, O., Kayisoglu, G., Bolat, P., & Tam, K. (2024). An investigation of ransomware incidents in the maritime industry: Exploring the key risk factors. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 1748006X241283093.
33	惡意軟體	2020	三艘美籍商船於靠港時，AIS 被駭客侵入，並安放 Sodinokibi 勒贖軟體，並盜取船上航行資料於暗網販售。 Datta, P. M., & Acton, T. (2023). From disruption to ransomware: Lessons From hackers. *Journal of Information Technology Teaching Cases*, *13*(2), 182-192.
34	惡意軟體	2020	地中海航運公司(全球首大海運航商)位於日內瓦的總部，遭受惡意軟體攻擊，造成 5 天暫停營業 Jones, K.D., Tam, K., Papadaki, M.: Threats and Impacts in Maritime Cyber Security. Engineering & Technology Reference. 1, 1, (2016). https://doi.org/10.1049/etr.2015.0123.

35	惡意軟體	2020	以色列駭客對伊朗 Shahid Rajaeee 港口發動網路攻擊(使用 Ryuk 等複合式惡意軟體)，癱瘓該港口管理中心作業達二週之久。 Warrick, J., Nakashima, E.: Officials: Israel linked to a disruptive cyberattack on Iranian port facility, https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html, (2020).
36	惡意軟體	2020	挪威 Vard 造船廠受到惡意軟體攻擊(經由電子郵件夾帶方式)，破壞工廠資訊系統致發生暫停營運狀況。 Team, E. (2020, June 11). *Vard shipbuilder experiences ransomware attack*. Retrieved October 29, 2024, from SAFETY4SEA: https://safety4sea.com/vard-shipbuilder-experiences-ransomware-attack/
37	惡意軟體	2019-2020	由英美合資的 Carnival Corporation & PLC 輪船旅遊公司，於 2019、2020 年二度遭遇駭客侵入竊取客戶個資及信用卡資料，公司並未說明公開說明損失情形。 Editoral, T. (2020, August 17). *Carnival Corporation Reports Ransomware Attack Accessed Data*. Retrieved October 15, 2024, from Maritime Executive: https://www.maritime-executive.com/article/carnival-corporation-reports-ransomware-attack-accessed-data
38	惡意軟體	2020	馬爾他(Malta)運輸部門，受到惡意軟體攻擊，被迫關閉線上服務達 5 天之久。 Azzopardi, K. (2020, October 29). *Transport Malta cyber attack investigation has not yet determined whether data was stolen*. Retrieved October 18, 2024, from Maltatoday: https://www.maltatoday.com.mt/news/national/105593/watch_transport_malta_cyber_attack_investigation_has_not_yet_determined_whether_data_was_stolen
39	惡意軟體	2020	希臘 Diana 船運公司，受到 Egregor 勒贖軟體攻擊，造成資訊系統被封鎖，被迫停止業務達二周之久。 Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. *Cyber resilience of systems and networks*, 1-25.

40	惡意軟體	2020	法國 CMA CGM 海運公司在中國的辦公室遭到 Ragner Locker 勒贖軟體攻擊，被迫關閉線上服務。 Aşan, C. THE ROLE OF CYBER SITUATIONAL AWARENESS OF HUMANS IN SOCIAL ENGINEERING CYBER ATTACKS ON THE MARITIME DOMAIN. *Mersin University Journal of Maritime Faculty*, *5*(2), 22-36.
41	惡意軟體	2020	聯合國國際海事組織(IMO)的資訊中心，遭到惡意軟體攻擊，據該組織表示，這次的攻擊行動的模式非常複雜。 Lemons, R. (2019, July 10). *Coast Guard Warns Shipping Firms of Maritime Cyberattacks*. Retrieved September 17, 2024, from Dark Reading : https://www.darkreading.com/vulnerabilities---threats/coast-guard-warns-shipping-firms-of-maritime-cyberattacks/d/d-id/1335198
42	惡意軟體	2020	英國的 Red Funnel 輪船旅遊公司遭到惡意軟體攻擊，資訊中心被迫關機，導致線上訂票作業失能，旅客只能現場購票。 Qamar, A., Karim, A., & Chang, V. (2019). Mobile malware attacks: Review, taxonomy & future directions. *Future Generation Computer Systems*, *97*, 887-909.
43	惡意軟體	2020	美國 MATSON 海運公司遭到惡意軟體攻擊，無法進行線上交易，部分資訊系統出現不穩定狀況。 Ussatova, O., Zhumabekova, A., Begimbayeva, Y., Matson, E. T., & Ussatov, N. (2022). Comprehensive DDoS Attack Classification Using Machine Learning Algorithms. *Computers, Materials & Continua*, *73*(1).
44	惡意軟體	2020	美國懷俄明州的 Kennewick 港管理中心遭到惡意軟體攻擊，資訊室無法運作，所有檔案都被駭客加密無法使用，駭客要求支付 20 萬美金贖款。 Senarak, C. (2024). Port cyberattacks from 2011 to 2023: a literature review and discussion of selected cases. *Maritime Economics & Logistics*, *26*(1), 105-130.

45	惡意軟體	2020	挪威 Hurtigruten 海上旅遊公司的資訊系統遭到惡意軟體攻擊，許多客戶的護照資料被竊取，該公司不得已遂關閉了一些主要系統以防災情擴大。 Soner, O., Kayisoglu, G., Bolat, P., & Tam, K. (2024). An investigation of ransomware incidents in the maritime industry: Exploring the key risk factors. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 1748006X241283093.
46	惡意軟體	2020	德國 AIDA 海上旅遊公司，設在 Rostock 的總部，被 Dopple Payme 勒贖軟體攻擊，導致主伺服器電腦停機，只好取消部分旅遊行程。 Sevim, A. Automation and Cybersecurity in Maritime Commerce. In *Global Maritime Geopolitics* (pp. 363-379). Transnational Press London.

對AIS系統操作與認知之研究



研究之問卷題目

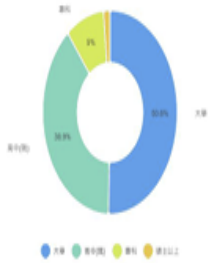
1. 請問您的性別?
2. 請問您的最高學歷?
3. 請問您的年齡?
4. 請問您的服務單位所屬機關?
5. 請問您目前受訓班隊?
6. 請問您的職務處所類別?
7. 請問您知道AIS系統嗎?
8. 請問您知道AIS系統的功用嗎?
9. 請問您目前執勤(工作)會運用AIS系統查詢資料嗎?
10. 請問您曾使用哪些系統查詢AIS相關資料?
11. 請問您知道AIS系統發出信號項目包括下列哪些?
12. 請問您知道MMSI編碼共幾碼?
13. 請問您知道MMSI前3碼，代表台灣的編碼號碼為何?
14. 請問您知道AIS信號可區分為A類與B類嗎?
15. 請問您知道AIS信號區分為A類與B類的差別為何?
16. 請問您知道總噸位多少以上的漁船需要裝設AIS系統嗎?
17. 請問您知道AIS假信息是如何產生的嗎?
18. 請問您知道如何發送AIS假信息的方式嗎?
19. 請問您在值班時有沒有碰到目標沒有AIS顯示的狀況?
20. 請問您如何看待使用AIS對於海事安全的貢獻程度?
21. AIS能用於船舶避免碰撞嗎?

問卷調查來源:針對在訓班隊5班隊等231員學生採線上問卷方式實施調查，對象均已至一線單位服務，具相當執勤經驗，實際年資已達最低1年至最高10年以上之年資，以符合調查參考數據。

1. 請問您的性別

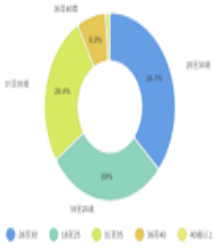
選項	填答數	百分比
男性	187	80.9%
女性	44	19%

2.請問您的最高學歷?



選項	填答數	百分比
大學	117	50.6%
高中(職)	90	38.9%
專科	21	9%
碩士以上	3	1.2%

3.請問您的年齡?



選項	填答數	百分比
26至30歲	85	36.7%
18至25歲	67	29%
31至35歲	61	26.4%
36至40歲	16	6.9%
40歲以上	2	0.8%

2.請問您的服務單位所屬機關?

選項	填答數	百分比
南部分署	64	27.7%
北部分署	48	20.7%
中部分署	35	15.1%
臺南市分署	29	12.5%
東南沙分署	21	9%
東部分署	19	8.2%
矯務分署	6	2.5%
海巡署	4	1.7%
教育訓練發考中心	3	1.2%
循隊分署	2	0.8%

5.請問您目前受訓班隊?

選項	填答數	百分比
海巡士官班	108	46.7%
士官長正規班	41	17.7%
軍官正規班	34	14.7%
海巡軍士官班	33	14.2%
海巡研究班	15	6.4%

6.請問您的職務處所類別?

選項	填答數	百分比
安檢所	108	46.7%
岸巡隊隊部	46	19.9%
機動巡防隊	29	12.5%
警備隊及所屬各中隊	13	5.6%
基本部各科室或分署本部各科室	9	3.8%
巡防區	8	3.4%
勤務指揮中心	7	3%
通資隊及所屬各中隊	5	2.1%
查緝隊	4	1.7%
特勤隊	2	0.8%

7.請問您知道AIS系統嗎?

選項	填答數	百分比
知道	193	83.5%
不知道	38	16.4%

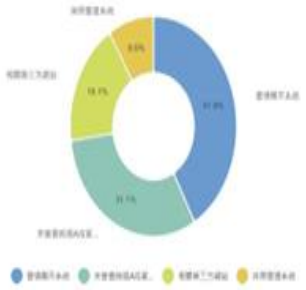
8.請問您知道AIS系統的功用嗎?

選項	填答數	百分比
知道	180	77.9%
不知道	51	22%

9.請問您目前執勤(工作)會運用AIS系統查詢資料嗎?

選項	填答數	百分比
不會	150	64.9%
會	81	35%

10.請問您曾使用哪些系統查詢AIS相關資料?



選項	填答數	百分比
雷情顯示系統	97	41.9%
未曾查詢過AIS資料	72	31.1%
相關第三方網站	42	18.1%
岸際管理系統	20	8.6%

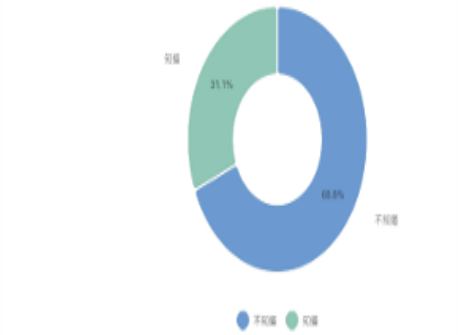
11.請問您知道AIS系統發出信號項目包括下列哪些?

選項	填答數	百分比
以上皆是	171	74%
不瞭解有何項目	34	14.7%
位置資訊	16	6.9%
船舶資料	8	3.4%
船舶類型	2	0.9%
航行狀態	0	0%

12.請問您知道MMSI編碼共幾碼?

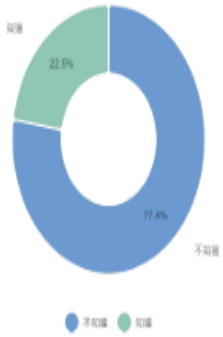
選項	填答數	百分比
不知道	120	51.9%
9碼	70	30.3%
8碼	24	10.3%
6碼	15	6.4%
7碼	2	0.8%

13.請問您知道MMSI前3碼，代表台灣的編碼號碼為何?



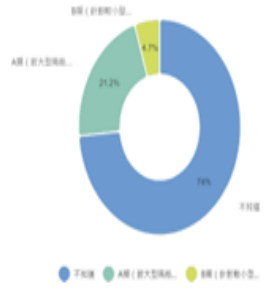
選項	填答數	百分比
不知道	159	68.8%
知道	72	31.1%

14.請問您知道AIS信號可區分為A類與B類嗎?



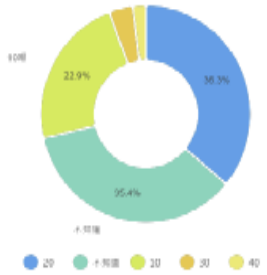
選項	填答數	百分比
不知道	179	77.4%
知道	52	22.5%

15.請問您知道AIS信號區分為A類與B類的差別為何?



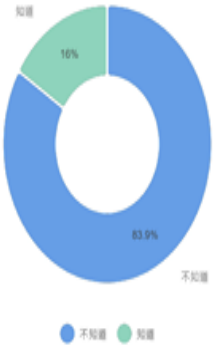
選項	填答數	百分比
不知道	171	74%
A類（對大型商船強制要求安裝，藉以提供全面的船舶相關數據）	49	21.2%
B類（針對較小型、非SOLAS公約規範的船舶，提供數據功能有限）	11	4.7%

16.請問您知道總噸位多少以上的漁船需要裝設AIS系統嗎?



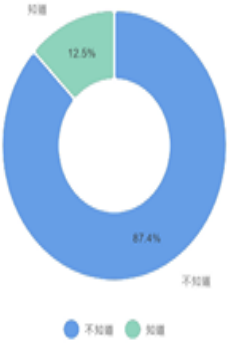
選項	填答數	百分比
20噸	84	36.3%
不知道	82	35.4%
10噸	53	22.9%
30噸	8	3.4%
40噸	4	1.7%

17.請問您知道AIS假信息是如何產生的嗎?



選項	填答數	百分比
不知道	194	83.9%
知道	37	16%

18.請問您知道如何發送AIS假信息的方式嗎?

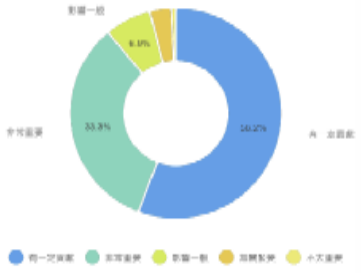


選項	填答數	百分比
不知道	202	87.4%
知道	29	12.5%

19.請問您在值班時有沒有碰到目標沒有AIS顯示的狀況?

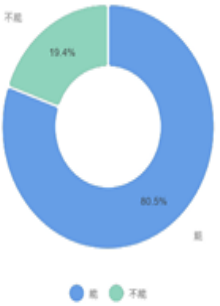
選項	填答數	百分比
有	121	52.3%
偶爾有	91	39.3%
經常有	25	10.8%

20.請問您如何看待使用AIS對於海事安全的貢獻程度?



選項	填答數	百分比
有一定貢獻	130	56.2%
非常重要	77	33.3%
影響一般	16	6.9%
無關緊要	7	3%
不太重要	1	0.4%

21. AIS能用於船舶避免碰撞嗎?



選項	填答數	百分比
能	186	80.5%
不能	45	19.4%

核判區分	主管	秘書	副主任	主任
				V

檔　　號:113/ 030304

保存年限：5

海洋委員會海巡署教育訓練測考中心　職員奉派出席會議情形報告單

密等及解密條件或保密期限：

會議事由：拜會全●綜電股份有限公司

召集機關及主席：全●綜電股份有限公司李●平副總經理

開會時間：113年9月20日(星期五)下午2時整

開會地點：全●綜電股份有限公司

本署參加人員：邱●讀主任教官、呂●龍教官

會議內容摘要：本次拜會由邱●讀主任教官偕呂●龍教官於1350時抵達全●綜電股份有限公司，該公司由李●平副總(總管理處)、劉●修副總(研發處)、游●豐副總(資訊部)、王●程業務經理、許●俊技術長全程接待，雙方主要針對當前AIS系統國際間與我國相關法律規範、AIS系統結合衛星運用最新發展趨勢、如何識別敵我海上目標、不法人士竄改AIS主機發射船舶資訊等實務現況詳加探討，全程交流時間約2小時30分，相關拜會照片(如附件1)與各類AIS主機介紹(如附件2)。

交流議題如下：

承辦單位	核(閱)稿	批示
[redacted] 0925 1445	[redacted] 0925 1640	
[redacted] 0925 1450	[redacted] 0925 1700	
[redacted] 0925 1555		
		[redacted] 0927 0725

副主任辦公室 9月25日16時30分收到

歸檔總頁數共　頁，附件共　頁

教官科 [redacted]

擬 副主任 [redacted] 文書電腦編號 [redacted]

秘書 [redacted] 主管 [redacted]

第1頁 共3頁

一、關於不法份子操弄AIS系統製造假訊息，請教在A型、B型兩種AIS主機上是如何進行?

答：原則只要符合國際海事組織(IMO)規範的AIS製造廠商，所生產AIS主機，僅能於出廠時依照客戶需求設定(一次)船舶相關資訊(後續廠商不會再協助客戶變更船舶資訊)；惟，不法廠商(此處多指中國大陸製，未符合國際海事組織規範廠商)所生產之AIS主機，可運用外接資訊設備操弄變更AIS主機內船舶相關資訊，更有甚者可直接在主機上設定變更船舶資訊，藉此隱匿船舶蹤跡，以遂行不法意圖。

二、AIS主機的信號是透過VHF頻率向外發射，目前已有衛星可以接收AIS信號，請問是哪一種衛星? 是否為低軌道衛星?

答：傳統接收AIS主機所發射的資訊，以AIS岸台為主，訊號接受範圍多為限制，超過通訊距離(20至40 浬)時，即失去船舶資訊之掌控，因此，近年全球多致力於低軌道 AIS衛星發展，於軌道中運行形成衛星網絡，以解決通訊距離受限之問題。

三、AIS信號係透過VHF頻率發送及接收，目前已經有案例顯示，駭客可透過上述公開頻段侵入特定對象的AIS主機進行操控藉此混淆，請問是否有防範方式?

答：目前全[redacted]綜電股份有限公司的資訊部門工程師已發展出一套獨特的數位演算加密方式，於本公司生產製造的AIS主機發射訊號時加密，可增加駭客於傳遞訊號過程中輕易竄改原始發射資訊的難度，以增加訊號傳輸安全。

四、部分國家為便於管理20噸以下船筏，已規範須加裝B型的AIS主機，目前我國海巡署亦準備協調漁業署推動立法，請教B型與A型主機，其功能主要差異為何? 船筏上人員可否擅自變更船舶資料?目前一套B型AIS主機價格大約多少?

答：

一、目前AIS主機可區分為Class A、Class B+、Class B等三種機型，前2種機型皆可發射與接收訊號，惟Class B機型設計僅能發射，無法接收訊號。

二、關於船筏上人員可否操作AIS主機，擅自變更船舶資訊，端視該主機是否為合法(即係符合國際海事組織IMO規範，經由

多國認證許可)廠商所製，如係合法廠商所生產，即無法任意變更船舶資訊(意即如欲變更資訊，則必須透過原廠操作，惟廠商為遵守法規，必定不會協助變更)；如係不法廠商所生產之AIS主機，船筏上人員即可能透過主機本身操弄，抑或藉由連結外部資訊設備竄改船舶資訊。

三、目前Class B型AIS主機安裝費用約為2萬元，即為我國漁業署公布「漁船筏裝設攜帶式船舶自動識別系統船載臺補助作業規範」所補助之金額。據中時新聞網報導目前全臺20噸以下船筏近2萬艘，安裝率約2成，意即目前不足4千艘小型船筏（20噸以下）已完成AIS主機安裝，仍有許多努力的空間。

處理建議：擬將本次會議資料納入本中心今年度自行研究案(AIS假資訊之威脅與因應)撰擬內容，並提供相關課程教案編修與教學使用。

附件 1

拜會全●綜電股份有限公司相關照片

由王●程業務經理實施簡報介紹(該公司組織架構、產品)

雙方針對 AIS 相關議題研討交流

拜會全●綜電股份有限公司相關照片

AIS SART、AIS MOB、Portable AIS Class B 產品陳列介紹

AIS Class A 產品陳列介紹

參考目錄

黃昆輝、張德銳、斐元領.(2000 年 12 月).系統理論模式(System Theory Model).(國家教育研究院)2018 年 2 月 28 日，擷取自雙語詞彙、學術名詞暨辭書資訊網：http://terms.naer.edu.tw/detail/1305926

張樹波、唐強榮，基於 AIS 資料的船舶異常行為檢測方法，人工智慧與機器人研究，2015，4(4): 23-31。

吳東明. (2022). 現今灰色地帶策略於海事競技場域的探析域借鏡-中國與俄羅斯的應用案例研究. 海巡灰色地帶與海洋科學研究 (頁 008-023). 桃園: 五南. 2021 年 9 月 20 日 擷取

曾子軒. (2024 年 10 月 8 日). 生成式 AI，讓深偽與假資訊難防？Google 高階主管：有解方. (遠見雜誌, 製作人) 2024 年 10 月 20 日 擷取自 遠見高峰會: https://www.gvm.com.tw/article/116176

2018 Highlights: Major cyber attacks reported in maritime industry. (2018, December 26). (USCG) Retrieved September 29, 2024, from SAFETY4SEA: https://safety4sea.com/cm-2018-highlights-major-cyber-attacks-reported-in-maritime-industry

Balduzzi, M., Pasta, A., & Wilhoit, K. (2014, December). A security evaluation of AIS automated identification system. In *Proceedings of the 30th annual computer security applications conference* (pp. 436-445).

Blackmore, C. (2019, December 16). *Cyberattack Impacts MTSA Facility Operations*. (USCG) Retrieved September 29, 2024, from Marine Safety Information Bulletin: https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2019/MSIB_10_19.pdf

Cimpanu, C.: US Coast Guard discloses Ryuk ransomware infection at maritime facility, 529 , https://www.zdnet.com/article/us-coast-guard-discloses-ryuk-ransomware-infection-at-maritime-facility/, last accessed 2021/04/25

Claverie, B., & Du Cluzel, F. (2022). “Cognitive warfare”: The advent of the concept of “cognitics” in the field of warfare. *Cognitive Warfare: the future of cognitive dominance*, 2-1.

Demchak, C., Patton, K., & Tangredi, S. J. (2017). Why are our ships crashing? Competence, overload, and cyber considerations. *Center for International Maritime Security*.

Club, P&I. (2020, May 20). *Vessel monitoring and P&I insurance – ship's Automated Information System (AIS)*. Retrieved September 22, 2024, from https://www.igpandi.org/article/the-international-group-clubs-discuss-the-importance-of-ships-complying-with-the-requirement-to-use-a-ships-automated-information-system-ais/

d'Afflisio, E., Braca, P., & Willett, P. (2021). Malicious AIS spoofing and abnormal stealth deviations: A comprehensive statistical framework for maritime anomaly detection. *IEEE Transactions on Aerospace and Electronic Systems*, *57*(4), 2093-2108.

Goudossis, A., & Katsikas, S. K. (2019). Towards a secure automatic identification system (AIS). *Journal of Marine Science and Technology*, *24*, 410-423.

IGP&I. (2022, September). *Guidelines for Correspondents 2022*. Retrieved September 23, 2024, from https://static.igpandi.org/igpi_website/media/article_attachments/Correspondents_Guidelines_-_2022.pdf

Gustafson, D. E., Dowdle, J. R., Elwell, J. M., & Flueckiger, K. W. (2009). A nonlinear code tracking filter for GPS-based navigation. *IEEE Journal of Selected Topics in Signal Processing*, *3*(4), 627-638.

IMO. (2015, December 2). *AIS transponder*. Retrieved June 25, 2024, from Resolution A.1106(29): https://wwwcdn.imo.org/localresources/en/OurWork/Safety/Documents/AIS/Resolution%20A.1106(29).pdf

Kennedy, C. M., & Erickson, A. S. (2017). China Maritime Report No. 1: China's Third Sea Force, The People's Armed Forces Maritime Militia: Tethered to the PLA.

Kessler, G. C. (2019, March 25). Cybersecurity in the Maritime Domain. *The Coast Guard Journal of Safety & Security at Sea, Vol. 76* (1), pp. 34-39.

Kontopoulos, I., Spiliopoulos, G., Zissis, D., Chatzikokolakis, K., & Artikis, A. (2018, August). Countering real-time stream poisoning: An architecture for detecting vessel spoofing in streams of AIS data. In *2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)* (pp. 981-986). IEEE.

USCG. (2023, April 10). *NAV Systems and Services*. Retrieved May 27, 2024, from Navigation Center: https://www.navcen.uscg.gov/automatic-identification-system-overview

Lynch, T. F. (2019). The Military and Alternative Security: New "Missions" for Stable Conventional Security. In *Alternative Security* (pp. 7-42). Routledge.

Meland, P. H., Bernsmed, K., Wille, E., Rødseth, Ø. J., & Nesheim, D. A. (2021). A retrospective analysis of maritime cyber security incidents.

Mraković, I., & Vojinović, R. (2019). Maritime cyber security analysis–how to reduce threats?. *Transactions on maritime science*, *8*(01), 132-139.

NATO. (2022, June 22). *Cognitive Warfare*. Retrieved September 17, 2024, from NATO's Strategic Warfare Development Command: https://www.act.nato.int/activities/cognitive-warfare/

O'Donncha, F., Sheehan, J. D., Touma, M., Zemouri, S., & High, R. H. (2024). Towards Intelligent Ship-Edge Computing Enabling Automated Configuration of Ship Models and Adaptive Self-Learning. In *State-of-the-Art Digital Twin Applications for Shipping Sector Decarbonization* (pp. 73-93). IGI Global.

Papadimitriou, A., Pangalos, K., Duvaux-Béchon, I., & Giannopapa, C. (2019). Space as an enabler in the maritime sector. *Acta Astronautica*, *162*, 197-206.

Polychronis, K.: Cybersecurity at Sea. In: Otto, L. (ed.) Global Challenges in Maritime Security. p. 243 Springer International Publishing (2020)

STAFF, U. N. (2019, August 6). *NTSB Accident Report on Fatal 2017 USS John McCain Collision off Singapore*. Retrieved February 13, 2024, from USNI News: https://news.usni.org/2019/08/06/ntsb-accident-report-on-fatal-2017-uss-john-mccain-collision-off-singapore

Smythe, T. C., & McCann, J. (2018). Lessons learned in marine governance: Case studies of marine spatial planning practice in the US. *Marine Policy*, *94*, 227-237.

Tam, K., & Jones, K. D. (2018). Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. *Journal of Cyber Policy*, *3*(2), 147-164.

Tegowski, B., & Koelpin, A. (2024). Accuracy limitations of interferometric radar owing to the radar cross section of its antenna. *IEEE Transactions on Microwave Theory and Techniques*.

Warship positions faked including UK aircraft carrier. (2021, August 3). Retrieved August 15, 2024, from BBC News briefing: https://www.bbc.com/news/technology-58027363

Wawruch, R. (2017). Ability to test shipboard automatic identification system instability and inaccuracy on simulation devices. *Zeszyty Naukowe Akademii Morskiej w Szczecinie*, (52 (124), 128-134.

Zhou, M., van der Veen, A. J., & van Leuken, R. (2012, March). Multi-user LEO-satellite receiver for robust space detection of AIS messages. In *2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (pp. 2529-2532). IEEE.