114年「國際海事公約及趨勢動態掌握與因應分析」

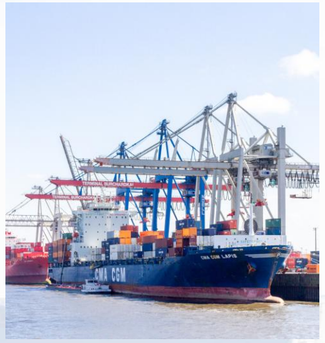
7月趨勢報告

海事網路安全與韌性：策略與挑戰

7/31/2025

Center for International Maritime Convention Studies
國立高雄科技大學
國際海事公約研究中心

大綱 Content



- 海事網路安全為何重要
- 常見的海事網路威脅
- 國際海事組織 (IMO) 的角色
- 其他國際標準與框架的應用
- 港口社群的網路安全
- 台灣在網路韌性方面的戰略轉型與實踐
- 結論與建議

海事網路安全為何重要
Why is Maritime Cyber Security important

海事網路安全是指保護船上和岸上的電腦與數位系統，使其免受可能損害數位資料和流程的機密性、完整性或可用性的網路威脅。這包括導航系統、通訊網路、推進控制、貨物管理以及船員福利平台等關鍵系統。

海事產業是全球貿易的基石，超過90%的貨物運輸依賴海運，而現代航運的運作則高度依賴互連的IT（資訊科技）和OT（營運科技）系統。保護海事網路安全至關重要，因為一旦發生攻擊事件，將導致嚴重後果，例如：

- **運輸延誤：** 影響全球供應鏈。
- **船舶遭劫持或改道：** 因導航系統被操縱。
- **貨物艙單洩露：** 導致貨物損失或盜竊。
- **敏感的船員和旅客資料外洩。**
- **港口營運停擺：** 造成巨大經濟損失。
- 網路攻擊事件甚至可能對人員、船舶、環境、公司、貨物和聲譽產生「廣泛的破壞性潛力」。

海事產業並非獨立存在，它與全球物流、石油和天然氣、國防甚至旅遊業相互關聯。
因此，海事網路安全的漏洞可能會對該行業以外的關鍵基礎設施和國家經濟造成嚴重影響。

海事網路安全為何重要
Why is Maritime Cyber Security important

資訊科技 (Information Technology, IT) 與 操作技術(Operational Technology, OT)系統的區別與互聯性：

資訊科技 (IT) 系統主要管理資料和支援業務功能，例如員工使用的個人電腦、行動電話、辦公周邊設備，以及旅客使用的公共 Wi-Fi 路由器和連線。它專注於利用資料作為資訊，包括軟體、硬體和通訊技術。

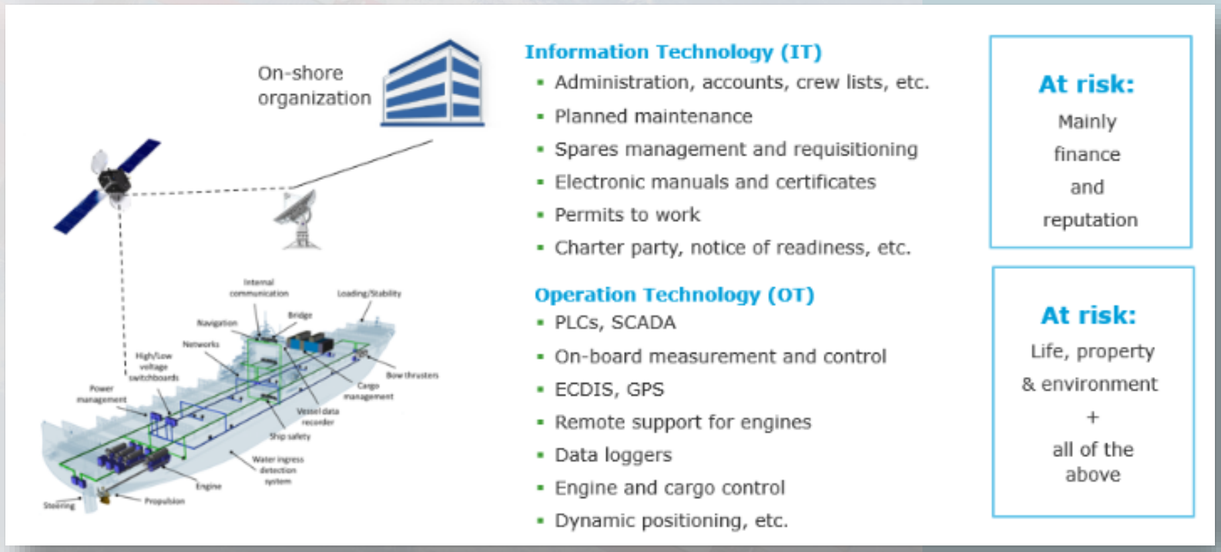
操作技術 (OT) 系統則是直接監控或控制實體設備和流程的硬體和軟體，是船舶不可或缺的一部分，必須獨立於 IT 系統運行。範例包括監控引擎性能的工業控制系統、導航系統、推進與機械管理系統、貨物處理系統、安全與存取控制系統、以及船上其他關鍵系統。

傳統上，IT 和 OT 系統是分離的，但隨著數位化和網路連接的增加，**IT/OT**兩者之間的界線變得模糊。

而兩者的融合更說明網路安全產生新的挑戰，像是：

- **攻擊面擴大：** 系統之間的連接性增加，使得潛在的網路攻擊更容易入侵
- **漏洞暴露：** OT 系統可能無法像 IT 系統那樣頻繁更新或運行防病毒軟體，一旦連接到 IT 網路，其漏洞可能會暴露。
- **操作安全風險：** OT 系統的破壞可能對船上人員的安全、環境保護和船舶營運造成重大風險。
- **供應鏈風險：** 供應商和外部各方對 OT 系統的遠端存取和維護也可能引入未知的漏洞。

因此，必須確保 IT 和 OT 系統之間有足夠的防火牆保護，並對 OT 系統的潛在漏洞保持警惕，因為這些漏洞可能因此暴露於 IT 網路。



Source: DNV, Maritime Cyber Security.

常見的海事網路威脅
Common Cyber threat in Maritime

海事產業面臨多種網路威脅，尤其針對複雜的網路：

- **網路釣魚 (Phishing) 和魚叉式網路釣魚 (Spear Phishing)：** 透過針對船員來取得未經授權的存取權限。
- **勒索軟體 (Ransomware)：** 加密系統並要求贖金才能解鎖。
- **阻斷服務 (DoS) 攻擊：** 癱瘓系統導致營運中斷。
- **內部威脅 (Insider Threats)：** 船員惡意或疏忽行為造成的漏洞。
- **惡意軟體 (Malware)：** 損壞或竊取船上系統的資料。
- **GPS 欺騙 (GPS Spoofing)：** 誤導導航系統關於位置和航向。

近年來網路攻擊事件顯著增加。像是2024年上半年，全球已有超過1,800艘船舶成為目標，檢測到23,400次惡意軟體，發生178次勒索軟體攻擊，以及超過500億次防火牆事件。新興威脅還包括AI驅動程式的惡意軟體、利用物聯網設備的殭屍網路以及結合實體和網路戰術的混合威脅。
(Nautilus shipping, Maritime Cybersecurity: Essential Strategies and Insights)

常見的海事網路威脅
Common Cyber threat in Maritime

海事產業因其多方利害關係人、頻繁的人員變動、老舊系統的使用、與岸上系統的互聯性，以及網路安全文化仍有提升空間等特性，使其成為網路攻擊的易受攻擊目標。

- **網路攻擊的類型與階段：**攻擊可分為**非針對性攻擊**（如 航運公司遭受NotPetya勒索軟體攻擊）和針對性攻擊。常見的攻擊手法包括惡意軟體（勒索軟體、病毒）、水坑攻擊、掃描、網路釣魚、魚叉式網路釣魚、憑證填充和阻斷服務（DoS/DDoS）等攻擊。網路攻擊通常會經歷偵察、傳遞、突破和樞轉四個階段，攻擊者可能長時間不被偵測。
- **針對 OT 系統的威脅：**儘管針對 OT 系統的攻擊相對較少被公開，但其風險不容低估。OT 系統的潛在威脅包括透過軟體更新（線上或 USB 隨身碟）引入的惡意軟體，或未經授權的人員操作。像是一艘新造船的 ECDIS（電子海圖顯示與資訊系統）感染病毒，導致數天延誤並造成數十萬美元損失，其來源被追溯到維修技術人員使用受感染的 USB 隨身碟。
- **針對 IT 系統的威脅：**IT 系統的攻擊更容易量化，儘管通常不直接造成人身傷害或環境污染，但可能導致嚴重的經濟損失和營運中斷，甚至影響安全，例如無法即時取得危險品清單。近期4月，萬海航運證實其資訊網站遭遇駭客攻擊，儘管營運未受影響，但再次凸顯航運供應鏈的數位脆弱性，尤其是航運系統包含大量高價值資訊，成功攻擊可能導致跨國供應鏈中斷。

國際海事組織 (IMO) 海事網路安全管理中的角色
Role of the International Maritime Organization (IMO)

際海事組織 (IMO) 在全球海事網路安全領域扮演著關鍵角色。

2017年6月，海事安全委員會第98屆會議(MSC 98) 通過MSC.428(98)號決議- 《安全管理系統中的海事網路風險管理》(*Maritime Cyber Risk Management in Safety Management Systems*)鼓勵各國政府確保在船舶的安全管理系統 (SMS) 中適當處理網路風險，並要求所有船舶營運者最遲在2021年1月1日後的首次公司符合證明年度驗證時遵守此規定。

此外，IMO 也發布了 **MSC-FAL.1/Circ.3 號通函**《海事網路風險管理準則》*Guidelines on maritime cyber risk management*，提供高層次建議，以協助船舶防範當前和新興的網路威脅和漏洞。

這些指引文件強調了網路風險管理的五個功能要素，可整合到現有的風險管理流程中，與 IMO 已建立的安全和保安管理實踐相輔相成：

- **識別 (Identify)：** 確定對船舶和船/港各方面造成的網路風險。
- **保護 (Protect)：** 實施風險控制流程和措施，並制定應急計劃。
- **偵測 (Detect)：** 發展、實施和練習及時偵測網路事件所需的活動。
- **應變 (Respond)：** 發展、實施和練習提供韌性以及恢復因網路事件受損的系統所需的活動和計劃。
- **恢復 (Recover)：** 識別和實施恢復船上電腦系統（包括網路）所需的措施。

這些指南旨在提高海事利益相關者對網路風險的意識，並支持安全和穩定的航運，使其對網路風險具有營運韌性。

Home

其他國際標準與框架的應用

- **NIST 網路安全框架**：美國國家標準與技術研究院 (NIST) 的網路安全框架（識別、保護、偵測、回應、復原）被廣泛接受，為降低關鍵基礎設施的網路風險提供指導。該框架鼓勵企業持續評估威脅、脆弱性、可能性和影響，並將其融入風險評估流程。例如，洛杉磯港的網路安全營運中心每月阻擋約 4000 萬次未經授權的入侵嘗試，並在網路內部使用多層入侵偵測。
- ISO/IEC 27001：一項資訊安全管理系統（ISMS）國際標準規範。
  符合 ISO/IEC 27001 意味著組織已建立系統來管理與公司擁有或處理的資料安全相關的風險，並符合最佳實踐和原則。促進對資訊安全的整體方法，包括人員、政策和技術，並被視為風險管理、網路韌性和卓越營運的工具。
- IACS 統一要求：國際船級社協會 (IACS) 已發布針對新造船的統一要求Unified Requirements (UR) E26（船舶網路彈性）側重於船舶的網路韌性營運層面和 UR E27（船載系統與設備網路彈性）針對船載系統和設備的網路韌性技術規範，要求自2024年7月1日起對新建船舶強制執行，但現有船舶可自願採用。
- 港口社區網路安全：IAPH 的2020年報告指出，數位化提高了港口社區的網路安全風險。該報告強調了使用通用語言來解決網路安全問題的重要性，提倡建立一套共同術語，並將網路風險管理與財務績效掛鉤，同時強調網路風險管理的責任是共享的，而非僅由「IT 人員」負責。缺乏港口社區政策、可見性不足、不願分享資訊和資源匱乏是港口網路防禦的常見問題。

其他相關海事安全規範與應用

- **歐盟指令 2016/1148 (NIS 指令) 與 NIS 2 指令**：**歐盟**這些指令將港口社區識別為關鍵基礎設施，並將海事營運商定義為基本服務營運商，強調了詳細解決海事網路安全問題的必要性。
- 美國海岸警衛隊 (USCG) 導航和船舶檢查通告 (NVIC) 01-20：這項指引針對《海事運輸安全法案 (MTSA)》規定設施的網路風險提出建議，指出海事領域中日益增加的網路技術應用引入了新的漏洞。
- 英國交通部《港口和港口系統網路安全良好實踐指南》：這份指南為港口金融和營運管理、與第三方合約安排、員工行為政策、港口規範/設計/建造/維護以及特定安全任務（包括事件應變）相關的各方提供建議。
- 法國驗船協會 (Bureau Veritas) NR 659 規則：由法國驗船協會(BV)開發的一項網路安全框架，旨在幫助船東遵守相關規定。另外還開發了一套 CHART (Cyber Health Assessment Report Tool) 的工具，用於評估船舶網路安全韌性。
- 國際海事無線電委員會 (CIRM) 海事電子設備和服務供應商網路風險行為準則：這項準則為製造商和服務提供商提供了實施有效且具成本效益的網路安全最佳實踐的指引。
- 數位貨櫃航運協會 (DCSA) 船舶網路安全實施指南 v1.0：這項準則為製造商和服務提供商提供了實施有效且具成本效益的網路安全最佳實踐的指引。

台灣在網路韌性方面的戰略轉型與實踐

台灣正積極應對日益升高的網路威脅，尤其是在地緣政治緊張的背景下，將網路安全視為國家安全的重要組成部分。

- 第七期國家網路安全發展計畫 (2025-2028)：台灣在 2025 年 5 月公布了這項四年計畫，投入新台幣 88 億元（約3.01 億美元）資源。該計畫由數位發展部 (MODA) 協調，並圍繞四個核心支柱進行戰略轉型：
  1. **國家準備度：**將地方政府、公立學校和非營利機構納入國家網路安全規劃，實現分散式風險擁有。
  2. **基礎設施風險降低：**MODA 和 ACS 將發布量身定制的安全基準，並進行實時模擬演習，以測試能源、醫療保健和電信等關鍵部門的營運準備情況。
  3. **網路安全產業發展：**將網路安全產業與全球技術標準對齊，如台積電與 SEMI 合作制定 SEMI E187 標準，加強供應鏈信任度。
  4. **人工智慧 (AI) 應用：**部署 AI 驅動的工具進行異常偵測、行為分析和預測性威脅建模，提升回應速度和精確度。這標誌著 AI 從輔助角色轉變為台灣防禦規劃的核心功能。

Source: Eryk Waligora, *Global Taiwan Brief Vol. 10, Issue 14*.

台灣在網路韌性方面的戰略轉型與實踐

- **不斷升級的威脅情勢：**2025 年 5 月，台灣數位發展部報告了 8,655 起網路安全事件，較上月增加 13.7%，較去年同期增加 13.2%，其中近 60% 涉及網路釣魚或惡意連結活動。這顯示威脅日益複雜，也反映了偵測能力的提升。
- **社會媒體素養的迫切需求：**隨著社群媒體在台灣青少年日常生活中佔據主導地位，他們日益暴露於資訊戰和虛假訊息的風險中。研究顯示，超過 80% 的台灣民眾遭遇過虛假資訊，但只有不到 10% 接受過媒體素養課程。台灣正在擴大現有計畫，賦予非政府組織和專家權力，並培訓教育工作者，以提升數位素養，特別是識別來自中國的敘事和資訊操控。
- **國防韌性的多層次應對：**面對中國日益複雜的「灰色地帶」威脅，台灣強調強化預警、監控與應處的主動機制，包括：
  - **情報交流：**深化與友邦的情報合作，監測中共透過方便旗船隻破壞海纜或部署監測設備等隱蔽干擾行為。
  - **軍事與海巡聯防：**加強海域監控，主動登檢可疑船隻，防範中共將商船和漁船用於軍事或權益主張。
  - **關鍵基礎設施防護：**推動資通訊設備升級、強化海纜建設與備援機房，並運用多元的中低軌衛星系統備援，打造多層次太空通訊網路。
  - **公私協力：**深化與電信業者的合作，完善海纜維修與備援機制，提升國家通訊網路的韌性。

Source: Eryk Waligora, *Global Taiwan Brief Vol. 10, Issue 14*.

HOME

港口社群的網路安全

Port Society cyber security

港口作為國際貿易的關鍵基礎設施，其網路安全日益受到關注：

- **港口作為協調者：**港口當局應發揮其固有的協調作用，促進整個港口生態系統內的對話，並推動全面的網路安全方法，包括貿易利害關係人、城市和區域政府機構，以及負責國家安全和防禦的部門。
- **共同語言與金融基礎：**為有效管理網路風險，港口社群需要建立一套共同的術語，並將網路風險管理與金融術語結合，以便決策者能以一致的方式做出投資決策。
- **社群網路防禦的不足：**當前港口社群的網路防禦通常缺乏社群方法，各利益關係者常因只專注於保護自身系統，與其他成員的協調有限。這導致港口社群無法從集體力量中受益，面臨更大風險。

結論與建議

CONCLUTION

全球海事產業正處於數位轉型的前沿，這既帶來了前所未有的營運效率，也伴隨著日益嚴峻的網路安全挑戰。從船舶到港口，每一個互聯的環節都可能成為攻擊面，威脅著貨物安全、人身安全和經濟穩定。國際組織如 IMO、IAPH 和產業工會 BIMCO 等，已積極發布詳細指南和要求，強調將網路風險管理整合到現有安全管理體系中，並涵蓋從識別威脅、實施保護措施到偵測、回應和復原的全生命週期。這些指南強調了 IT 和 OT 系統的區別、供應鏈網路安全的重要性以及培訓人員意識的關鍵作用。

台灣在應對這些挑戰方面採取了前瞻性的國家戰略，透過「國家網路安全發展計畫」的戰略轉型，將 AI 技術、供應鏈安全和跨部門協作置於其防禦核心。同時，台灣也認識到提升全民數位素養和加強國際合作的重要性，這對於抵禦外部資訊戰和網路攻擊至關重要。

總體而言，海事網路安全已不再是單一企業或組織的責任，而是一個需要全球各方協調一致、共同努力的「共享責任」。透過採納和實施國際標準與最佳實踐、投資於技術解決方案、培養具備網路安全意識的人力、以及促進跨行業和跨國界的資訊共享與合作，才能建立一個真正具有韌性的全球海事生態系統，確保國際貿易的順暢和安全。

結論與建議

CONCLUTION

- 現今的航運業需要一套全面的網路安全方案。數位化在提升效率的同時，也為前所未有的網路威脅打開了大門。正如2024年所表明的那樣，網路事件的頻率和嚴重程度都在上升。保障船舶和系統的安全需要採取全面、主動且符合標準的方法。海員、營運商、原始設備製造商和監管機構必須攜手合作，建構一個強大的航運網路安全生態系統。不作為會導致潛在的安全漏洞，其代價高昂—無論是經濟上、營運上或人道上，因此保障航運安全至關重要。
- 「船舶網路資安指南」在IMO法規的基礎上，整合了NIST框架的風險管理流程，並鼓勵參考ISO/IEC 27001和IACS統一要求等技術標準，形成了一個全面且多層次的網路風險管理策略。
- 就如同船舶設計不僅要遵循IMO的強制性安全規範，還要借鑒其他國家(美國國家標準局的最佳實踐方法)或其他專業機構參考國際船級社協會的具體建造標準，並吸取其他航運公司在營運中的經驗教訓，以確保船舶在日益複雜的網路環境中既合法合規，又具備穩健的防禦能力。
- 港口是全球貿易的關鍵基礎設施，並且日益數位化和互聯。港口社區的網路安全問題不僅影響單個實體，還可能導致整個供應鏈的重大中斷。缺乏社區合作、可見性和資訊共享意願是港口網路防禦的常見問題。
- 為了建立彈性的港口社區網路安全政策，應採用協作、連貫和協調的方法。NIST的五步框架（識別、保護、檢測、響應、恢復）可作為指導。建立共同的術語、將對話建立在財務基礎上，並明確網路風險管理的共同責任是至關重要的。

參考資料

- BIMCO. 2024. THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS.
- Nautilus shipping, Maritime Cybersecurity: Essential Strategies and Insights. June 11, 2025.
- Eryk Waligora, *Global Taiwan Brief Vol. 10, Issue 14*.
- IACS. IACS adopts new requirements on cyber safety.
- IAPH. 2020. PORT COMMUNITY CYBER SECURITY.
- IMO. MSC.428(98), Maritime Cyber Risk Management in Safety Management Systems.
- IMO. MSC-FAL.1/Circ.3. Guidelines on maritime cyber risk management.
- Txone network. 2024. Future Cybersecurity Threats in Ports: Protecting Global Trade from Rising Maritime Risks.
- DNV, Maritime cyber security https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/
- US maritime-cybersecurity. https://www.maritime-cybersecurity.com/
- US maritime-cybersecurity. https://www.maritime-cybersecurity.com/National_Maritime_Cybersecurity_Plan.html
- Watchsoft，從萬海到全球：航運供應鏈的數位韌性建設 04.25.2025。

Thank You!