TẠP CHÍ ISSN: 1859-316X, e-ISSN:3093-3161
KHOA HỌC CÔNG NGHỆ HÀNG HẢI
JOURNAL OF MARINE SCIENCE AND TECHNOLOGY

AN NINH MẠNG HÀNG HẢI TRƯỚC CÁC THÁCH THỨC TỪ HOẠT ĐỘNG GÂY NHIỄU, GIẢ MẠO VÀ CÁC GIẢI PHÁP CÔNG NGHỆ

MARITIME CYBER SECURITY AGAINST CHALLENGES FROM JAMMING, SPOOFING, AND TECHNOLOGICAL SOLUTIONS

NGUYỄN THANH SƠN*

Khoa Hàng hải, Trường Đại học Hàng hải Việt Nam

**Email liên hệ: nguyenthanhson@vimaru.edu.vn*

DOI: https://doi.org/10.65154/jmst.1179

Tóm tắt

Trong bối cảnh ngành vận tải biển phụ thuộc lớn vào Hệ thống Vệ tinh Dẫn đường Toàn cầu (GNSS) để thu thập dữ liệu về Vị trí, Điều hướng và Thời gian (PNT), bản thảo này phân tích các lỗ hổng an ninh mạng phát sinh do tín hiệu vệ tinh yếu và dễ bị tổn thương. Cụ thể, nghiên cứu làm rõ cơ chế hoạt động của hai mối đe dọa vô tuyến nguy hiểm nhất hiện nay là gây nhiễu làm mất hoàn toàn khả năng định vị và giả mạo đánh lừa máy thu để thao túng tọa độ và thời gian của tàu. Những rủi ro này trực tiếp đe dọa đến an toàn hàng hải và sự phát triển của công nghệ tàu tự hành (MASS).

Để ứng phó, bài viết rà soát các khung quản lý rủi ro từ Tổ chức Hàng hải Quốc tế và đề xuất hướng đi chiến lược nhằm xây dựng nền tảng PNT có khả năng phục hồi. Các giải pháp công nghệ trọng tâm bao gồm hệ thống định vị dự phòng (như STL, eLoran), công nghệ bảo vệ máy thu bằng ăng-ten mảng thích ứng, cùng các công nghệ đột phá tương lai hoàn toàn độc lập với vệ tinh như quang học laser và định vị lượng tử. Nghiên cứu kết luận rằng việc áp dụng một kiến trúc phòng thủ theo chiều sâu là yếu tố then chốt để đảm bảo an ninh tuyệt đối cho chuỗi cung ứng hàng hải toàn cầu.

Từ khóa: *An ninh mạng hàng hải, Hệ thống Vệ tinh Dẫn đường Toàn cầu, Gây nhiễu, Giả mạo, PNT có khả năng phục hồi.*

Abstract

In the context of the maritime industry's heavy reliance on the Global Navigation Satellite System (GNSS) to acquire Position, Navigation, and Time (PNT) data, this manuscript analyzes the cybersecurity vulnerabilities arising from weak and vulnerable satellite signals. Specifically, the research clarifies the operating mechanisms of the two most dangerous radio threats today: jamming, which causes a complete loss of positioning capabilities, and spoofing, which deceives the receiver to manipulate the ship's coordinates and time. These risks directly threaten maritime safety and the development of Maritime Autonomous Surface Ships (MASS) technology.

In response, the article reviews risk management frameworks from the International Maritime Organization (IMO) and proposes strategic directions to build a Resilient PNT foundation. Key technological solutions include backup positioning systems (such as STL, eLoran), receiver protection technologies using adaptive antenna arrays, as well as future breakthrough technologies entirely independent of satellites, such as laser optics and quantum navigation. The study concludes that the implementation of a defense-in-depth architecture is the key factor in ensuring absolute security for the global maritime supply chain.

Keywords: *Maritime Cyber Security, GNSS, Jamming, Spoofing, Resilient PNT.*

1. Mở đầu

Trong bối cảnh toàn cầu hóa và cuộc cách mạng công nghiệp lần thứ tư, ngành vận tải biển tiếp tục khẳng định vai trò là xương sống của nền kinh tế thế giới. Việc đảm bảo các tiêu chuẩn hàng hải khắt khe không chỉ quyết định sự an toàn của con tàu, thuyền bộ và hàng hóa mà còn đóng vai trò sống còn trong việc bảo vệ môi trường biển. Hiện nay, hoạt động thương mại hàng hải và quân sự phụ thuộc rất lớn vào Hệ thống Vệ tinh Dẫn đường Toàn cầu (Global Navigation Satellite System - GNSS), bao gồm GPS (Mỹ), GLONASS (Nga), BeiDou (Trung Quốc) và Galileo (Châu Âu), nhằm thu thập dữ liệu về Vị trí, Điều hướng và Thời gian (Position, Navigation, and

TẠP CHÍ ISSN: 1859-316X, e-ISSN: 3093-3161
KHOA HỌC CÔNG NGHỆ HÀNG HẢI
JOURNAL OF MARINE SCIENCE AND TECHNOLOGY

Time - PNT). Dữ liệu PNT cho phép các thiết bị thu trên tàu xác định vị trí với độ chính xác cao, tạo lập khả năng định hướng hành trình và đồng bộ hóa thời gian tuyệt đối. Hiệu suất của các hệ thống GNSS được đánh giá qua bốn tiêu chí cốt lõi: độ chính xác (accuracy), tính toàn vẹn (integrity), tính liên tục (continuity) và tính sẵn sàng (availability).

Tuy nhiên, sự phụ thuộc tuyệt đối vào nền tảng kỹ thuật số và kết nối vệ tinh đã làm bộc lộ những lỗ hổng an ninh mạng nghiêm trọng. Tín hiệu GNSS phát ra từ vệ tinh có công suất tương đối thấp, khiến chúng dễ bị tổn thương trước các nguồn nhiễu sóng dù là yếu nhất. Sự phát triển của các công nghệ tác chiến điện tử (Electronic Warfare - EW) từ các tác nhân nhà nước và phi quốc gia đã biến việc vô hiệu hóa hoặc can thiệp dữ liệu PNT thành một mối đe dọa chiến lược mang tính đột phá. Các hành vi can thiệp này đe dọa trực tiếp đến an toàn hàng hải toàn cầu, hệ thống tài chính, chuỗi cung ứng logistics và mạng lưới thông tin liên lạc. Trong đó, hai hình thức tấn công phổ biến và nguy hiểm nhất là gây nhiễu (jamming) và giả mạo (spoofing).

Gây nhiễu là việc sử dụng sóng vô tuyến có cường độ mạnh để áp đảo tín hiệu GNSS yếu, khiến thiết bị thu mất khả năng theo dõi tín hiệu xác thực và dẫn đến mất khả năng định vị. Tinh vi hơn, tấn công giả mạo (spoofing) liên quan đến việc phát sóng các tín hiệu GNSS giả mạo nhưng có cấu trúc giống hệt tín hiệu thật nhằm đánh lừa thiết bị thu. Kẻ tấn công có thể thao túng dữ liệu để hệ thống của tàu tin rằng nó đang ở một vị trí hoặc một thời điểm hoàn toàn khác so với thực tế. Sự phức tạp của giả mạo còn được thể hiện qua các kỹ thuật như giả mạo phép đo (measurement spoofing), thay đổi thời gian hoặc tần số đến của tín hiệu và giả mạo dữ liệu (data spoofing) can thiệp vào dữ liệu kỹ thuật số được hệ thống sử dụng để tính toán PNT. Đặc biệt, kỹ thuật tấn công "carry-off" cho phép kẻ thù đồng bộ hóa tín hiệu giả với tín hiệu thật, sau đó tăng dần công suất để chiếm quyền kiểm soát thiết bị thu của tàu một cách vô hình.

Trong những năm gần đây, việc vũ khí hóa tín hiệu hàng hải đã trở thành một hiện tượng địa chính trị đáng báo động. Các cường quốc trên thế giới đang tích hợp năng lực tác chiến điện tử vào chiến lược an ninh mạng để chối bỏ, làm suy giảm hoặc thao túng không gian thông tin. Đơn cử, hệ thống thao túng GPS đã tạo ra các "vòng tròn giả mạo" (spoofing circles) tại các cảng dầu chiến lược, làm sai lệch dữ liệu Hệ thống Nhận dạng Tự động (AIS) của tàu thương mại nhằm che giấu việc nhập khẩu dầu trái phép. Đồng thời, các đội tàu cá cũng thường xuyên tắt hoặc giả mạo tín hiệu AIS để thực hiện các hoạt động đánh bắt bất hợp pháp, không báo cáo và không được quản lý (IUU) tại các khu vực bảo tồn biển. Tại Trung Đông, có lực lượng đã sử dụng thiết bị gây nhiễu GPS và giả mạo liên lạc vô tuyến tại khu vực eo biển Hormuz để dẫn dụ các tàu thương mại đi lạc vào lãnh hải, từ đó tạo cớ bắt giữ tàu, như trong sự kiện của tàu Stena Impero. Tương tự, việc triển khai năng lực giả mạo GNSS, không chỉ để bảo vệ các cơ sở chiến lược và các yếu nhân mà còn ứng dụng trong các vùng chiến sự nhằm từ chối không phận và áp chế thiết bị điện tử dân sự cũng như quân sự.

Từ góc độ pháp lý quốc tế, các hành vi gây nhiễu và giả mạo vi phạm nghiêm trọng các công ước hiện hành. Quy chế Vô tuyến của Liên minh Viễn thông Quốc tế (ITU) nghiêm cấm mọi trạm vô tuyến thực hiện các hành vi gây nhiễu có hại (harmful interference), đồng thời cấm phát các tín hiệu sai lệch, gây nhầm lẫn hoặc không có nhận dạng. Việc gây nhiễu hoặc giả mạo tín hiệu làm gián đoạn nghiêm trọng dịch vụ an toàn hàng hải và vô tuyến, đe dọa sự an toàn của sinh mạng con người trên biển. Nhằm ứng phó với thực trạng này, Tổ chức Hàng hải Quốc tế (IMO) đã thông qua Nghị quyết MSC.428(98), chính thức yêu cầu các bên liên quan phải tích hợp quản lý rủi ro không gian mạng vào hệ thống quản lý an toàn của tàu. Cùng với đó, IMO cũng ban hành Hướng dẫn Quản lý Rủi ro Không gian mạng Hàng hải, thiết lập khuôn khổ dựa trên năm yếu tố chức năng: Nhận dạng, Bảo vệ, Phát hiện, Ứng phó và Phục hồi (Identify, Protect, Detect, Respond, Recover). Ngoài ra, các tiêu chuẩn hiệu suất cho thiết bị thu vô tuyến đa hệ thống cũng được IMO thiết lập nhằm tăng khả năng chống nhiễu và cung cấp dữ liệu PNT có độ tin cậy cao.

Sự xuất hiện của công nghệ tàu tự hành mặt nước (Maritime Autonomous Surface Ships - MASS) càng làm tăng tính cấp thiết của việc bảo vệ tín hiệu PNT. Các tàu tự hành, đặc biệt là ở cấp độ tự chủ cao, phụ thuộc hoàn toàn vào các trung tâm vận hành từ xa (ROCs) và các thuật toán Trí tuệ Nhân tạo (AI) để đưa ra quyết định điều hướng thay cho con người. Nếu tín hiệu điều hướng bị tấn công, sự sai lệch dữ liệu sẽ dẫn đến nguy cơ va chạm hoặc thảm họa môi trường nghiêm trọng.

Dựa trên bối cảnh nêu trên, nghiên cứu này được thực hiện nhằm mục đích hệ thống hóa và phân tích chuyên sâu về bản chất, cơ chế hoạt động của các mối đe dọa gây nhiễu và giả mạo tín hiệu GNSS trong ngành hàng hải. Bài báo sẽ đánh giá lỗ hổng

của các hệ thống định vị hiện tại dưới tác động của chiến tranh điện tử, đồng thời rà soát khung pháp lý quốc tế (UNCLOS, ITU, IMO) đang được áp dụng để quản lý rủi ro. Trọng tâm của nghiên cứu là đề xuất và phân tích các giải pháp công nghệ tiên tiến nhằm xây dựng nền tảng PNT có khả năng phục hồi (Resilient PNT). Các giải pháp này bao gồm việc ứng dụng công nghệ Thời gian và Vị trí Vệ tinh (STL), thiết bị hỗ trợ đo lường quán tính (IMU), ăng-ten mảng thích ứng triệt tiêu nhiễu, công nghệ quang học laser, và đặc biệt là hệ thống điều hướng lượng tử (quantum navigation) hoàn toàn độc lập với vệ tinh. Qua đó, nghiên cứu kỳ vọng đóng góp cơ sở lý luận và thực tiễn thiết thực nhằm đảm bảo sự phát triển bền vững và an ninh, an toàn tuyệt đối cho chuỗi cung ứng hàng hải toàn cầu trong kỷ nguyên số.

2. Bản chất của Gây nhiễu (Jamming) và Giả mạo (Spoofing) tín hiệu định vị

Sự an toàn và hiệu quả của các hoạt động thương mại hàng hải hiện đại phụ thuộc gần như tuyệt đối vào Hệ thống Vệ tinh Dẫn đường Toàn cầu (GNSS) như GPS, GLONASS, BeiDou và Galileo. GNSS cung cấp dịch vụ cốt lõi về Vị trí, Điều hướng và Thời gian (PNT). Hiệu suất của GNSS được đánh giá dựa trên bốn tiêu chí nền tảng: độ chính xác, tính toàn vẹn, tính liên tục và tính sẵn sàng.

Tuy nhiên, do khoảng cách truyền xa từ không gian, tín hiệu GNSS khi đến bề mặt Trái Đất có công suất rất thấp. Điểm yếu vật lý này khiến hệ thống máy thu trên tàu biển vô cùng dễ bị tổn thương trước các nguồn nhiễu sóng (RF waveforms) từ các tác nhân bên ngoài. Sự can thiệp này, thường được thực hiện thông qua công nghệ tác chiến điện tử (EW), đang nổi lên như một mối đe dọa chiến lược mang tính phá hoại đối với an toàn hàng hải toàn cầu. Hai hình thức can thiệp phổ biến và nguy hiểm nhất là gây nhiễu và giả mạo.

2.1. Kỹ thuật gây nhiễu tín hiệu (Jamming)

Gây nhiễu là hình thức tấn công dựa trên việc phát ra các dải sóng vô tuyến có cường độ mạnh tại cùng dải tần số mà hệ thống GNSS sử dụng. Mục tiêu của gây nhiễu là áp đảo hoàn toàn tín hiệu vệ tinh yếu ớt, từ đó làm suy giảm hoặc từ chối hoàn toàn khả năng hoạt động của máy thu GNSS trên tàu.

Trong thực tiễn, tin tặc thường sử dụng kỹ thuật "gây nhiễu áp đảo" (brute force jamming), tạo ra các tín hiệu nhiễu loạn giống như tiếng ồn trắng (noise-like signals) để ngăn chặn máy thu bám sát các tín hiệu xác thực. Các thiết bị gây nhiễu rất đa dạng, có thể là các hệ thống tác chiến điện tử cấp quân sự hoặc chỉ đơn giản là các Thiết bị Bảo vệ Cá nhân (Personal Protection Devices - PPDs) có khả năng phát sóng vô tuyến. Khi bị tấn công gây nhiễu, hệ thống định vị của tàu sẽ báo lỗi mất tín hiệu hoàn toàn, khiến tàu bị "mù" định vị và phải chuyển sang các phương pháp hàng hải thủ công.

2.2. Kỹ thuật Giả mạo tín hiệu (Spoofing)

Khác với gây nhiễu mang tính chất phá hoại trực tiếp, tấn công giả mạo tinh vi, phức tạp và nguy hiểm hơn rất nhiều. Thay vì cắt đứt hoàn toàn tín hiệu, thủ phạm sẽ phát ra các tín hiệu giả mạo có cấu trúc giống hệt tín hiệu GNSS thật hoặc phát lại các tín hiệu xác thực đã được ghi lại từ một không gian hoặc thời gian khác. Kỹ thuật này lừa máy thu GNSS tin rằng tàu đang ở một vị trí khác với thực tế, hoặc ở đúng vị trí đó nhưng vào một mốc thời gian khác.

Về mặt học thuật, giả mạo được chia thành ba phương thức tấn công kỹ thuật số chính:

Giả mạo phép đo (Measurement spoofing): Kẻ tấn công can thiệp vật lý vào sóng vô tuyến, khiến máy thu mục tiêu tạo ra các phép đo sai lệch về thời gian truyền tín hiệu (time of arrival) hoặc tần số đến, từ đó làm sai lệch tọa độ tính toán.

TẠP CHÍ ISSN: 1859-316X, e-ISSN: 3093-3161
KHOA HỌC CÔNG NGHỆ HÀNG HẢI
JOURNAL OF MARINE SCIENCE AND TECHNOLOGY

Giả mạo dữ liệu (Data spoofing): Kẻ tấn công tiêm nhiễm dữ liệu kỹ thuật số sai lệch vào máy thu mục tiêu, làm sai lệch thuật toán xử lý dữ liệu PNT cốt lõi của tàu.

Tấn công "mang đi" (Carry-off attack): Đây là kỹ thuật vô hình và nguy hiểm nhất. Kẻ tấn công bắt đầu bằng việc phát sóng các tín hiệu giả mạo đồng bộ hoàn toàn với tín hiệu thật mà máy thu đang bắt được. Sau đó, chúng tăng dần công suất của tín hiệu giả để chiếm quyền kiểm soát máy thu. Khi hệ thống của tàu đã "bám" vào tín hiệu giả, kẻ tấn công từ từ thao túng dữ liệu để báo cáo vị trí chệch hướng dần so với quỹ đạo thực.

Việc sử dụng các kỹ thuật này không chỉ đe dọa sinh mạng trên biển mà còn vi phạm nghiêm trọng luật pháp quốc tế. Điều 15 của Quy chế Vô tuyến thuộc Liên minh Viễn thông Quốc tế (ITU) cấm hoàn toàn các đài phát thực hiện các hành vi truyền tín hiệu không cần thiết, truyền tín hiệu dư thừa, phát tín hiệu sai lệch, gây nhầm lẫn hoặc không có nhận dạng nhằm gây can thiệp có hại (harmful interference) đến các dịch vụ vô tuyến và hàng hải. Dù bị cấm, sự trỗi dậy của EW khiến các vụ giả mạo và gây nhiễu đang trở thành vùng xám an ninh cần được Tổ chức Hàng hải Quốc tế (IMO) và các cường quốc hàng hải khẩn trương giải quyết.

Số lượng các cuộc tấn công không gian mạng nhằm vào ngành vận tải biển quốc tế đã gia tăng đáng kể, từ 0 vụ vào năm 2003 lên 3 vụ vào năm 2013 và chạm mốc 64 vụ vào năm 2023. Các cuộc tấn công này chủ yếu thông qua việc can thiệp vào Hệ thống Vệ tinh Dẫn đường Toàn cầu (GNSS) và Hệ thống Nhận dạng Tự động (AIS).

3. Khung quản lý rủi ro và các sáng kiến quốc tế

Bảng 1. Bảng phân tích so sánh bản chất Gây nhiễu và Giả mạo

Tiêu chí	Gây nhiễu (Jamming)	Giả mạo (Spoofing)
Cơ chế hoạt động	Áp đảo tín hiệu bằng sóng vô tuyến công suất cao cùng tần số.	Đánh lừa máy thu bằng cách phát tín hiệu GNSS giả mạo hoặc ghi âm/phát lại tín hiệu thật.
Mục đích	Từ chối dịch vụ (Denial of Service), làm mất khả năng định vị.	Thao túng tọa độ, dẫn dụ tàu đi chệch hướng hoặc sai lệch thời gian.
Dấu hiệu nhận biết trên tàu	Mất tín hiệu hoàn toàn, báo động hệ thống mất kết nối vệ tinh.	Hệ thống vẫn báo nhận tín hiệu tốt nhưng tọa độ/thời gian thực tế bị sai lệch. Rất khó phát hiện.
Phân loại kỹ thuật	Gây nhiễu áp đảo (Brute force jamming).	Giả mạo phép đo, giả mạo dữ liệu, tấn công dẫn dụ (Carry-off).
Thiết bị thực hiện	Máy phá sóng quân sự, thiết bị PPDs.	Cần thiết bị giả lập tín hiệu và phần mềm tính toán thuật toán phức tạp (thường cấp quốc gia).

Để đối phó với sự gia tăng của các mối đe dọa không gian mạng nhắm vào các hệ thống định vị và hàng hải, cộng đồng quốc tế đã thiết lập các khuôn khổ quản lý rủi ro đa tầng, bao gồm sự can thiệp của Tổ chức Hàng hải Quốc tế (IMO), các sáng kiến từ ngành công nghiệp và các chính sách phòng vệ quốc gia.

3.1. Các sáng kiến của Tổ chức Hàng hải Quốc tế (IMO)

IMO đóng vai trò tiên phong trong việc thiết lập các tiêu chuẩn an toàn an ninh mạng trên biển. Năm 2017, Ủy ban An toàn Hàng hải (MSC) đã thông qua Nghị quyết MSC.428(98) nhằm nâng cao nhận thức về các mối đe dọa, lỗ hổng rủi ro không gian mạng và khuyến khích các cơ quan quản lý đảm bảo rằng rủi ro không gian mạng được xử lý thích hợp trong hệ thống quản lý an toàn của tàu. Bên cạnh đó, IMO cũng ban hành Hướng dẫn Quản lý Rủi ro Không gian mạng Hàng hải cung cấp các khuyến nghị cấp cao để bảo vệ ngành vận tải biển trước các mối đe dọa liên quan đến sự số hóa, tích hợp và tự động hóa. Khuôn khổ quản lý rủi ro này được xây dựng dựa trên năm yếu tố chức năng cốt lõi để đảm bảo khả năng phục hồi hoạt động: Nhận dạng (Identify), Bảo vệ (Protect), Phát hiện (Detect), Phản hồi (Respond) và Phục hồi (Recover). Về mặt công nghệ định vị, IMO đã thông qua Tiêu chuẩn hiệu suất cho thiết bị thu vô tuyến đạo hàng đa hệ thống trên tàu vào năm 2015. Hệ thống này cho phép sử dụng kết hợp tín hiệu từ hai hay nhiều hệ thống vệ tinh (GNSS), giúp cải thiện dữ liệu về Vị trí, Vận tốc, Thời gian (PVT)

và tăng cường khả năng chống lại nhiễu sóng vô tuyến có chủ đích hoặc không chủ đích. Đến năm 2017, IMO tiếp tục phê duyệt Hướng dẫn xử lý dữ liệu PNT trên tàu, tạo ra bộ nguyên tắc nhằm cung cấp dữ liệu PNT (Vị trí, Điều hướng và Thời gian) đáng tin cậy, an toàn và có khả năng chống lại sự can thiệp của các tác nhân độc hại.

3.2. Sáng kiến từ các tổ chức và ngành công nghiệp hàng hải

Nhiều tổ chức hàng hải hàng đầu như BIMCO, ICS, INTERCARGO, và INTERTANKO đã hợp tác phát triển các hướng dẫn và thực tiễn tốt nhất về an ninh mạng trên tàu. Đặc biệt, INTERTANKO đã phát hành hướng dẫn chi tiết về cách đối phó với hiện tượng gây nhiễu và giả mạo GNSS, yêu cầu các hoa tiêu thực hiện các bước phát hiện và giảm thiểu rủi ro như:

- Sử dụng hệ thống Radar và ECDIS (Hệ thống Thông tin và Hiển thị Hải đồ Điện tử) để phát hiện giả mạo khi có thể quan sát đất liền trên radar.

- Kiểm tra vị trí thường xuyên và đối chiếu thông qua phương pháp đo khoảng cách ước tính (DR) hoặc sử dụng máy đo độ sâu (echo sounder) để so sánh độ sâu thực tế.

- Giám sát chặt chẽ các chỉ số hiệu suất chính (KPI) của thiết bị thu GNSS nhằm phát hiện sự bất thường như các bước nhảy đồng hồ (clock jumps) hoặc sự khác biệt giữa mã và phép đo sóng mang. Ngành công nghiệp cũng đề xuất các biện pháp đối phó công nghệ cao như sử dụng ăng-ten mảng thích ứng (CRPA), hỗ trợ máy thu bằng Hệ thống Đo lường Quán tính (IMU), các thuật toán kiểm soát hiện tượng nhảy vọt vị trí, và sử dụng tín hiệu E-Loran làm hệ thống dự phòng nhằm phát hiện can thiệp.

3.3. Khung chính sách bảo vệ hạ tầng định vị của Hoa Kỳ

Hoa Kỳ đã triển khai một loạt các chính sách quốc gia toàn diện để bảo vệ hệ thống định vị khỏi mối đe dọa không gian mạng. Tháng 2 năm 2020, Sắc lệnh Hành pháp 13905 được ban hành nhằm bảo vệ các dịch vụ PNT, đảm bảo sự gián đoạn hoặc thao túng PNT không làm suy yếu các cơ sở hạ tầng trọng yếu của quốc gia. Kế hoạch Điều hướng Vô tuyến Liên bang (2021) của Hoa Kỳ yêu cầu người dùng GPS phải chuẩn bị sẵn sàng cho sự gián đoạn bằng cách áp dụng các thiết bị chống nhiễu và tích hợp nguồn PNT thay thế. Đồng thời, Bộ Quốc phòng Hoa Kỳ đang nỗ lực nâng cấp hệ thống GPS với tín hiệu M-code một loại tín hiệu quân sự được mã hóa và truyền trên dải tần rộng hơn, giúp tăng cường mạnh mẽ khả năng chống nhiễu và giả mạo so với các thiết bị thương mại. Bên cạnh đó, Kế hoạch R&D Quốc gia về Khả năng Phục hồi PNT và Bản ghi nhớ An ninh Quốc gia NSM-22 tập trung vào việc thiết lập các hệ thống phòng thủ theo chiều sâu, xây dựng các phương pháp phân tích tình báo theo thời gian thực và quản lý rủi ro trên toàn bộ các lĩnh vực cơ sở hạ tầng trọng yếu. Cuối cùng, Cục Hàng hải Hoa Kỳ (MARAD) thường xuyên ban hành các cảnh báo yêu cầu các tàu thương mại khi gặp sự cố gián đoạn GPS/GNSS phải lập tức báo cáo cho Trung tâm Điều hướng (NAVCEN) của Lực lượng Tuần duyên Hoa Kỳ cũng như các tổ chức giám sát hàng hải khu vực (như UKMTO) để điều tra và xử lý kịp thời.

4. Các giải pháp công nghệ giảm thiểu rủi ro

Sự gia tăng của các mối đe dọa không gian mạng đối với Hệ thống Vệ tinh Dẫn đường Toàn cầu (GNSS) đã thúc đẩy ngành hàng hải chuyển hướng sang khái niệm "PNT có khả năng phục hồi" (Resilient PNT). Khái niệm này là sự kết hợp giữa công nghệ cung cấp Vị trí, Điều hướng và Thời gian (PNT) truyền thống với các công nghệ phi truyền thống và công nghệ mới nổi nhằm phát hiện, bảo vệ và xác thực các lỗ hổng của GNSS trước các cuộc tấn công gây nhiễu và giả mạo. Các giải pháp công nghệ giảm thiểu rủi ro hiện nay có thể được phân loại thành bốn nhóm chiến lược cốt lõi.

4.1. Công nghệ định vị dự phòng và hệ thống thay thế phi truyền thống

Khi tín hiệu GNSS bị áp đảo hoặc thao túng, việc sở hữu các hệ thống độc lập để đối chiếu và thay thế là lớp phòng thủ đầu tiên. Nổi bật trong số đó là công nghệ Thời gian và Vị trí Vệ tinh (Satellite Time and Location - STL). STL hoạt động thông qua mạng lưới vệ tinh Iridium, cung cấp tín hiệu được mã hóa và có cường độ mạnh hơn tín hiệu GNSS tới 1000 lần, giúp hệ thống có khả năng chống lại cả gây nhiễu và giả mạo. Mặc dù độ chính xác của STL (30-50 mét) không bằng GNSS, nhưng nó đóng vai trò là một công cụ xác thực chéo tuyệt vời để kiểm tra tính chính xác của dữ liệu GNSS. Khi được kết hợp với Hệ thống Điều hướng Quán tính (Inertial Navigation System - INS), STL cung cấp các cập nhật về phạm vi và hiệu ứng Doppler, giúp giảm thiểu độ lệch của hệ thống quán tính và duy trì giải pháp điều hướng ngay cả trong những khoảng thời gian dài bị mất tín hiệu GNSS.

Bên cạnh đó, Hệ thống eLoran được đánh giá là một giải pháp thay thế hoàn hảo nhờ sự khác biệt hoàn toàn về bản chất vật lý so với GNSS. Trong khi

TẠP CHÍ ISSN: 1859-316X, e-ISSN: 3093-3161
KHOA HỌC CÔNG NGHỆ HÀNG HẢI
JOURNAL OF MARINE SCIENCE AND TECHNOLOGY

GNSS sử dụng vi sóng từ không gian với công suất thấp, eLoran sử dụng dải tần số thấp, phát xung công suất cao và dựa trên các trạm phát trên mặt đất. Sự khác biệt này đồng nghĩa với việc các thiết bị phá sóng được thiết kế để tấn công GNSS sẽ hoàn toàn vô tác dụng đối với eLoran, mang lại mức độ phục hồi cao cho an toàn hàng hải.

Để tự động hóa việc phát hiện, các Thiết bị Bảo vệ Điều hướng (Navigation Protection Devices - NPDs) như hệ thống Broad Shield của Orolia đã được phát triển. Các thiết bị này hoạt động độc lập với hệ thống điều hướng chính, liên tục giám sát, phân tích tín hiệu GNSS và giao tiếp với màn hình ECDIS để cảnh báo ngay lập tức cho hoa tiêu khi phát hiện các dải sóng lạ trong băng tần GNSS, hoặc khi dữ liệu GNSS có sự sai lệch so với các nguồn thay thế như STL hay eLoran.

4.2. Công nghệ bảo vệ máy thu và chống nhiễu chủ động

IMO đã thiết lập các tiêu chuẩn hiệu suất cho thiết bị thu vô tuyến đạo hàng đa hệ thống (multi-system receivers) nhằm gia tăng khả năng chống nhiễu vô ý và cố ý. Các thiết bị này phải có khả năng xử lý tín hiệu từ ít nhất hai hệ thống GNSS độc lập (như GPS, GLONASS, Galileo, BeiDou) và có khả năng tự chủ đánh giá tính toàn vẹn của dữ liệu. Hệ thống phải đáp ứng các tiêu chuẩn tính toán thời gian thực vô cùng khắt khe: cung cấp dữ liệu PNT trong vòng 5 phút ở trạng thái khởi động nguội (không có dữ liệu lịch vệ tinh - cold start), 1 phút ở trạng thái khởi động ấm (warm start), và chỉ 2 phút sau khi bị gián đoạn nguồn điện. Nếu mất tín hiệu hoàn toàn, hệ thống phải tự động xuất ra vị trí, tốc độ và hướng di chuyển hợp lý cuối cùng để duy trì điều hướng tạm thời.

Ở góc độ phần cứng, công nghệ ăng-ten mảng thích ứng (Adaptive antenna array), đặc biệt là ăng-ten có mô hình thu được kiểm soát (CRPA), đang được ứng dụng mạnh mẽ. Một ví dụ điển hình là hệ thống Veripos GAJT-710MS do Hexagon phát triển. Công nghệ này có khả năng tạo ra các "điểm mù" (nulls) trong mô hình độ lợi của ăng-ten, hướng chính xác vào vị trí của nguồn phát nhiễu, từ đó triệt tiêu sự can thiệp của sóng ngoại lai.

Về mặt phần mềm, các tổ chức như INTERTANKO khuyến nghị sử dụng thuật toán bánh đà (fly-wheel algorithms) để ngăn chặn hệ thống nhận diện các bước nhảy vọt bất hợp lý về vị trí và thời gian. Việc liên tục giám sát các chỉ số hiệu suất chính (KPI) của máy thu, chẳng hạn như hiện tượng nhảy đồng hồ hoặc tỷ lệ tín hiệu trên nhiễu bất thường, kết hợp với công nghệ mật mã, giúp phát hiện sớm các nỗ lực giả mạo. Ở cấp độ quân sự, Hoa Kỳ đang tích hợp tín hiệu M-code cho GPS, sử dụng dải tần số rộng hơn và mã hóa nâng cao, cung cấp khả năng chống nhiễu và giả mạo vượt trội cho các tàu thuyền quốc gia.

4.3. Công nghệ định vị và triệt tiêu nguồn tấn công

Không chỉ dừng lại ở phòng ngự, các giải pháp công nghệ hiện nay còn hướng tới việc chủ động tìm kiếm và vô hiệu hóa các thiết bị phá sóng. Công ty công nghệ Zephr của Mỹ đã thử nghiệm thành công một phần mềm đặc biệt cài đặt trên điện thoại di động thông minh nhằm định vị các thiết bị gây nhiễu. Bằng cách thiết lập một mạng lưới các thiết bị và đối chiếu khả năng thu nhận GPS của chúng, hệ thống có thể phát hiện thời điểm bị tấn công. Nâng cao hơn, công nghệ này cho phép tam giác đạc (triangulation) vị trí chính xác của nguồn gây nhiễu thông qua ba dữ liệu đầu vào: (1) ước tính khoảng cách dựa trên công suất sóng, (2) khoanh vùng khu vực bị ảnh hưởng, và (3) đo lường góc tới của tín hiệu. Điều này cho phép các tàu tránh xa khu vực nguy hiểm hoặc cung cấp tọa độ để lực lượng chức năng vô hiệu hóa nguồn phát.

4.4. Các công nghệ đột phá tương lai: Quang học Laser và Định vị Lượng tử

Để loại bỏ hoàn toàn rủi ro từ chiến tranh điện tử vô tuyến, các nhà khoa học đang phát triển các phương thức điều hướng không sử dụng sóng RF. Công nghệ laser đang nổi lên như một giải pháp thay thế an toàn. Cảm biến CyScan GeoLock của Wärtsilä sử dụng tia laser đo khoảng cách và phương vị đến các bộ phản xạ được tham chiếu địa lý. Thuật toán sẽ so sánh mô hình hình học thu được với cấu hình đã khảo sát để xác định vị trí tàu một cách chính xác tuyệt đối mà không có bất kỳ rủi ro nào về nhiễu hay giả mạo tín hiệu. Hơn nữa, các quốc gia như Pháp và Trung Quốc đang thử nghiệm mạng lưới giao tiếp laser không gian - mặt đất. Với băng thông rộng hơn vi sóng từ 10 đến 1000 lần và đặc tính truyền điểm-điểm, tia laser cung cấp độ bảo mật gần như tuyệt đối, rất khó bị đánh chặn hay phát hiện, và hoàn toàn miễn nhiễm với các quy định phân bổ tần số vô tuyến hiện tại.

Cuối cùng, đỉnh cao của sự phát triển PNT là Định vị Lượng tử (Quantum Navigation). Công ty SandboxAQ của Mỹ đang phát triển hệ thống AQNav kết hợp Trí tuệ Nhân tạo (AI) với các cảm

biến lượng tử siêu nhạy. AQNav hoạt động bằng cách đo lường từ trường ở lớp vỏ Trái Đất – một tín hiệu thụ động, đáng tin cậy và không thể bị thao túng. Công nghệ này cung cấp khả năng điều hướng thời gian thực ở các khu vực bị từ chối GPS, mang lại khả năng phục hồi 100% hoàn toàn độc lập với vệ tinh và không thể bị ảnh hưởng bởi bất kỳ hình thức gây nhiễu hay giả mạo nào.

Tóm lại, không có một giải pháp công nghệ đơn lẻ nào có thể giải quyết toàn diện mọi lỗ hổng của GNSS. Giải pháp tối ưu cho sự an toàn của ngành hàng hải nằm ở việc xây dựng một kiến trúc phòng thủ theo chiều sâu**.** Sự kết hợp đa tầng giữa các nguồn dữ liệu PNT (GNSS, STL, eLoran, Quán tính, Laser, Lượng tử), cùng với các thuật toán phát hiện bất thường và công nghệ ăng-ten tiên tiến, sẽ đảm bảo rằng ngay cả khi một hoặc nhiều điểm bị tấn công, tàu thương mại và quân sự vẫn có thể duy trì hoạt động an toàn và hiệu quả trên các vùng biển quốc tế.

5. Kết luận

Trong bối cảnh các cuộc tấn công không gian mạng nhằm vào ngành vận tải biển quốc tế ngày càng gia tăng về cả số lượng lẫn mức độ tinh vi, việc chỉ phụ thuộc vào GNSS làm nền tảng định vị và điều hướng đã không còn đảm bảo mức độ an toàn tuyệt đối. Các lỗ hổng vật lý cố hữu của GNSS trước các mối đe dọa như gây nhiễu và giả mạo đặt ra yêu cầu cấp thiết về một sự chuyển dịch mang tính chiến lược. Để giải quyết bài toán này, ngành hàng hải cần khẩn trương hướng tới việc xây dựng một hệ thống PNT có khả năng phục hồi. Khái niệm này đòi hỏi sự hợp nhất giữa nền tảng công nghệ PNT truyền thống với các công nghệ phi truyền thống và công nghệ mới nổi, nhằm khắc phục các khoảng trống về độ chính xác, tính sẵn sàng và tính ổn định, từ đó đảm bảo sự an toàn cho các hoạt động mang tính sống còn trên biển.

Để hiện thực hóa và duy trì được nền tảng PNT có khả năng phục hồi này, sự kết hợp đồng bộ giữa quản trị rủi ro an ninh mạng và đổi mới công nghệ là yếu tố tiên quyết. Trước tiên, các bên liên quan cần tuân thủ nghiêm ngặt việc đánh giá rủi ro an ninh mạng thường xuyên và thiết lập các kế hoạch ứng phó sự cố bài bản (tuân theo các tiêu chuẩn cốt lõi như Nhận dạng, Bảo vệ, Phát hiện, Phản hồi và Phục hồi) nhằm đảm bảo khả năng duy trì hoặc khôi phục hoạt động khi hệ thống bị xâm phạm.

Thứ hai, việc áp dụng nhanh chóng các giải pháp công nghệ tiên tiến và mang tính đột phá sẽ đóng vai trò là "chìa khóa" phòng vệ tối ưu. Điển hình có thể kể đến như: nâng cấp hệ thống tín hiệu mã hóa kháng nhiễu mạnh mẽ như M-code; triển khai các hệ thống cảm biến quang học laser cung cấp tham chiếu vị trí hoàn toàn độc lập và không bị ảnh hưởng bởi can thiệp vô tuyến; và đặc biệt là công nghệ định vị lượng tử, một giải pháp tiềm năng cho phép điều hướng theo thời gian thực tại các khu vực bị từ chối tín hiệu vệ tinh, tạo ra một năng lực kháng nhiễu và chống giả mạo tuyệt đối.

Tựu trung lại, sự kết hợp giữa các nguyên tắc phòng thủ theo chiều sâu trong quản trị an ninh mạng và các giải pháp định vị thế hệ mới sẽ là cấu trúc bảo vệ toàn diện nhất. Chỉ khi xây dựng được một khung năng lực như vậy, ngành hàng hải mới có thể bảo vệ an toàn cho tàu thuyền, thuyền bộ, hàng hóa và đảm bảo tính liên tục, không bị gián đoạn của chuỗi cung ứng giao thương toàn cầu trước các mối đe dọa trong kỷ nguyên chiến tranh điện tử.

TÀI LIỆU THAM KHẢO

[1] Androjna, M. Perkovič, I. Pavic, and J. Miškovič, "AIS Data Vulnerability Indicated by a Spoofing Case-Study," *Applied Sciences*, vol. 11, no. 11, p. 5015, 2021.

[2] E. N. Armelloni *et al.*, "AIS Data, a Mine of Information on Trawling Fleet Mobility in the Mediterranean Sea," *Marine Policy*, vol. 129, p. 104571, 2021.

[3] D. Bréhaut, *GMDSS: A User's Handbook*, 5th ed. Bloomsbury, 2013.

[4] J. Carson-Jackson, "Satellite AIS: Developing Technology or Existing Capability?" *Journal of Navigation*, vol. 65, no. 2, pp. 303–321, 2012.

[5] J. A. Creech and J. F. Ryan, "AIS, The Cornerstone of National Security?" *Journal of Navigation*, vol. 56, no. 1, pp. 31–44, 2003.

[6] C. Dupont *et al.*, "Exploring Uses of Maritime Surveillance Data for Marine Spatial Planning: A Review of Scientific Literature," *Marine Policy*, vol. 117, p. 103930, 2020.

[7] M. Fournier *et al.*, "Past, Present, and Future of the Satellite-Based Automatic Identification System: Areas of Applications (2004–2016)," *WMU Journal of Marine Affairs*, vol. 17, pp. 311–345, 2018.

[8] A. Goudossis and S. K. Katsikas, "Towards a Secure Automatic Identification System (AIS)," *Journal of Marine Science and Technology*, vol.

TẠP CHÍ ISSN: 1859-316X, e-ISSN: 3093-3161
KHOA HỌC CÔNG NGHỆ HÀNG HẢI
JOURNAL OF MARINE SCIENCE AND TECHNOLOGY

24, no. 6, pp. 410–423, 2019.

[9] A. Harati-Mokhtari *et al.*, "Automatic Identification Systems (AIS): Data Reliability and Human Error Implications," *Journal of Navigation*, vol. 60, no. 3, pp. 373–389, 2007.

[10] International Maritime Organization (IMO), "Guidelines on Automatic Identification of Shipping (AIS) Operational Matters: Note by the International Chamber of Shipping (ICS)," MSC 72/10/12, May 31, 2000.

[11] International Maritime Organization (IMO), "Adoption of Amendments to the International Convention for the Safety of Life at Sea, 1974, as Amended," MSC.99(73), Dec. 5, 2000.

[12] International Maritime Organization (IMO), "Revision of Chapter V of SOLAS: Transponders," MSC 72/10/8, Mar. 14, 2000.

[13] International Maritime Organization (IMO), "Guidelines for the Onboard Operational Use of Shipborne Automatic Identification Systems (AIS)," A 22/Res.917, Nov. 29, 2001.

[14] International Maritime Organization (IMO), "Adoption of Amendments to the International Convention for the Safety of Life at Sea, 1974, as Amended," MSC.202(81), May 19, 2006.

[15] International Maritime Organization (IMO), *Guide to Maritime Security and the ISPS Code*, 2012.

[16] International Maritime Organization (IMO), "Revised Guidelines for the Onboard Operational Use of Shipborne Automatic Identification Systems (AIS)," A 29/Res.1106, Annex, Dec. 14, 2015.

[17] International Maritime Organization (IMO), "Urging Member States and All Relevant Stakeholders to Promote Actions to Prevent Illegal Operations in the Maritime Sector by the 'Dark Fleet' or 'Shadow Fleet'," A 33/Res.1192, Dec. 11, 2023.

[18] International Maritime Organization (IMO), "Brief History of IMO," [Online]. Available: www.imo.org/en/About/HistoryOfIMO/Pages/Default.aspx.

[19] R. L. Kilpatrick, Jr., "Monitoring Sanctions Compliance at Sea," *Northwestern Journal of International Law and Business*, vol. 42, no. 2, pp. 221–251, 2022.

[20] R. L. Kilpatrick, Jr., "Sanctions Clause Redux," *Journal of International Maritime Law*, vol. 29, no. 4, p. 199, 2023.

[21] J. M. Krajewski, "Out of Sight, Out of Mind? A Case for Long Range Identification and Tracking of Vessels on the High Seas," *Naval Law Review*, vol. 56, pp. 219–249, 2008.

[22] N. Serra-Sogas *et al.*, "Using Aerial Surveys to Fill Gaps in AIS Vessel Traffic Data to Inform Threat Assessments, Vessel Management, and Planning," *Marine Policy*, vol. 133, p. 104765, 2021.

[23] R. L. Shelmerdine, "Teasing Out the Detail: How Our Understanding of Marine AIS Data Can Better Inform Industries, Developments, and Planning," *Marine Policy*, vol. 54, pp. 17–25, 2018.

[24] M. Svanberg *et al.*, "AIS in Maritime Research," *Marine Policy*, vol. 106, p. 103520, 2019.

[25] M. Vespe, H. Greidanus, and M. Alvarez Alvarez, "The Declining Impact of Piracy on Maritime Transport in the Indian Ocean: Statistical Analysis of 5-Year Vessel Tracking Data," *Marine Policy*, vol. 59, pp. 9–15, 2015.

[26] K. Wolsing *et al.*, "Anomaly Detection in Maritime AIS Tracks: A Review of Recent Approaches," *Journal of Marine Science and Engineering*, vol. 10, no. 1, p. 112, 2022.

Ngày nhận bài:	21/05/2026
Ngày nhận bản sửa:	02/06/2026
Ngày duyệt đăng:	06/06/2026