Tạp chí Lý Luận Chính Trị Và Truyên Thông

Tạp chí điện tử tiếng Việt - Tập 32, Số 9 (2026)

Hợp tác đa phương trong phòng, chống tội phạm mạng và tội phạm công nghệ cao

Ngày nhận bài: 21/07/2026 | **Ngày phản biện:** 03/08/2026 | **Ngày xuất bản:** 10/09/2026

Tác giả: Nguyễn Hà Tâm (Văn phòng Học viện Cảnh sát nhân dân)

Tóm tắt: Tội phạm mạng và tội phạm công nghệ cao có tính xuyên biên giới, vận hành theo mạng lưới và khai thác chênh lệch pháp luật, năng lực thực thi giữa các quốc gia. Vì vậy, hợp tác đa phương ngày càng giữ vai trò trung tâm trong hình thành chuẩn mực chung, chia sẻ thông tin, bảo toàn chứng cứ là dữ liệu điện tử, phối hợp điều tra và thu hồi tài sản. Bài viết khảo sát các cơ chế của Liên hợp quốc, Tổ chức Cảnh sát hình sự quốc tế (INTERPOL) và Hiệp hội các quốc gia Đông Nam Á (ASEAN), đồng thời đánh giá sự tham gia của Việt Nam. Kết quả cho thấy khuôn khổ đa phương đã tạo ra những kết quả thực tiễn đáng kể, song vẫn bị giới hạn bởi "độ trễ" pháp lý, khác biệt thủ tục, sự không đồng đều về năng lực và tốc độ biến đổi của công nghệ. Từ đó, bài viết đề xuất các giải pháp nâng cao hiệu quả tham gia và thực thi hợp tác đa phương của Việt Nam trong giai đoạn mới.

1. Đặt vấn đề

Tội phạm trên không gian mạng đang gây thiệt hại lớn và vượt khỏi khả năng xử lý riêng lẻ của từng quốc gia. Năm 2024, Việt Nam thiệt hại hơn 18.900 tỷ đồng do tội phạm hoạt động trên không gian mạng, gấp hai lần năm 2023. Cơ quan Phòng, chống Ma túy và Tội phạm của Liên hợp quốc (UNODC) ước tính thiệt hại do lừa đảo tại Đông Á, Đông Nam Á, Australia và New Zealand năm 2025 ở mức 88,3-114,1 tỷ USD (UNODC, 2026). Thực tiễn này đặt ra yêu cầu tăng cường hợp tác đa phương để thống nhất chuẩn mực, chia sẻ thông tin, thu thập chứng cứ là dữ liệu điện tử và phối hợp xử lý tài sản do phạm tội mà có.

Về học thuật, tội phạm phụ thuộc vào công nghệ chỉ có thể được thực hiện thông qua hệ thống công nghệ thông tin. Tội phạm được công nghệ hỗ trợ là tội phạm truyền thống được công nghệ làm gia tăng quy mô, tốc độ hoặc phạm vi (Wall, 2007). Đây là cách phân loại theo vai trò của công nghệ, không phải hai tội danh độc lập. Trong bài viết này, "tội phạm mạng" bao quát hành vi mà hệ thống, dữ liệu hoặc không gian mạng là mục tiêu, công cụ hay môi trường thực hiện. "Tội phạm công nghệ cao" là thuật ngữ thường dùng trong thực tiễn Việt Nam, có phạm vi giao thoa lớn với tội phạm mạng nhưng còn bao gồm hành vi sử dụng công nghệ tiên tiến không nhất thiết diễn ra hoàn toàn trên mạng.

Hợp tác đa phương là một bộ phận của hợp tác quốc tế, được tổ chức giữa từ ba quốc gia trở lên trên cơ sở nguyên tắc, thể chế hoặc quy trình chung (Ruggie, 1992). Bài viết tập trung vào các cơ chế của Liên hợp quốc, INTERPOL, ASEAN và Hiệp hội Cảnh sát các quốc gia Đông Nam Á (ASEANAPOL); hợp tác song phương chỉ được xem xét như phương thức bổ trợ. Mục tiêu nghiên cứu là làm rõ cơ sở khoa học, thực tiễn, kết quả và hạn chế của hợp tác đa phương, từ đó đề xuất giải pháp nâng cao hiệu quả tham gia của Việt Nam.

2. Phương pháp nghiên cứu

Bài viết sử dụng ba nhóm phương pháp: Phương pháp phân tích tài liệu được dùng để khai thác văn bản pháp luật, báo cáo và dữ liệu chính thức của Việt Nam, Liên hợp quốc, UNODC, INTERPOL và ASEAN; làm rõ cơ sở pháp lý, thẩm quyền và giới hạn của từng cơ chế hợp tác. Phương pháp tổng hợp được sử dụng để hệ thống hóa kết quả, nhận diện vấn đề và xây dựng kiến nghị. Số liệu được lựa chọn từ nguồn chính thức, có thời điểm công bố và phạm vi thống kê xác định; vì vậy được dùng để phản ánh xu hướng và quy mô, không suy rộng thành tỷ lệ tuyệt đối cho toàn bộ tội phạm ẩn.

Phương pháp so sánh được thực hiện theo ba tầng: cơ chế toàn cầu của Liên hợp quốc, cơ chế phối hợp nghiệp vụ toàn cầu của INTERPOL và cơ chế khu vực ASEAN/ASEANAPOL. Các tiêu chí đối chiếu gồm phạm vi thành viên, nền tảng pháp lý, tốc độ phản ứng, công cụ hợp tác và giới hạn thực thi. Bài viết đồng thời so sánh kết quả của Chiến dịch HAECHI V năm 2024 với Chiến dịch Secure năm 2025 để

nhận diện khác biệt giữa phối hợp điều tra tội phạm tài chính trực tuyến và triệt phá hạ tầng kỹ thuật độc hại.

3. Kết quả và thảo luận

3.1. Kết quả nghiên cứu

3.1.1. Hợp tác đa phương là yêu cầu khách quan trong phòng, chống tội phạm mạng và tội phạm công nghệ cao

Tội phạm mạng có thể được thực hiện tại một quốc gia, sử dụng máy chủ ở quốc gia thứ hai, chiếm đoạt tiền của nạn nhân tại quốc gia thứ ba và chuyển tài sản qua nhiều trung gian tài chính hoặc tài sản mã hóa. Trong khi đó, thẩm quyền điều tra và các biện pháp ngăn chặn vẫn bị giới hạn bởi yếu tố lãnh thổ. Chứng cứ là dữ liệu điện tử dễ thay đổi, bị xóa hoặc phân tán tại các nhà cung cấp dịch vụ khác nhau; tài sản có thể được chuyển đi chỉ trong thời gian rất ngắn. Mâu thuẫn giữa tính xuyên biên giới của hành vi và tính lãnh thổ của quyền lực nhà nước làm phát sinh nhu cầu hợp tác.

Tính khách quan của hợp tác đa phương còn thể hiện ở quy mô của tội phạm. INTERPOL cho biết đến tháng 3/2025, nạn nhân bị mua bán vào các trung tâm lừa đảo đến từ 66 quốc gia; 74% trong số họ bị đưa tới các trung tâm ở Đông Nam Á (INTERPOL, 2025a). Các đối tượng sau đó tiếp tục thực hiện lừa đảo trực tuyến, mua bán người, rửa tiền, cưỡng bức lao động và các tội phạm liên quan đến tham nhũng. Cơ chế chuyên trách một loại tội phạm hoặc giới hạn trong một quốc gia không thể nhận diện đầy đủ cấu trúc, dòng tiền và hạ tầng của hệ sinh thái tội phạm đó.

3.1.2. Khuôn khổ pháp lý và thể chế của hợp tác đa phương

Ở cấp độ toàn cầu, Đại hội đồng Liên hợp quốc thông qua Công ước Liên hợp quốc về chống tội phạm mạng theo Nghị quyết 79/243 ngày 24/12/2024. Công ước được mở ký tại Hà Nội ngày 25-26/10/2025. Văn kiện quy định về hình sự hóa, biện pháp tố tụng, hợp tác quốc tế, hỗ trợ kỹ thuật và chia sẻ chứng cứ là dữ liệu điện tử đối với tội phạm nghiêm trọng (Đại hội đồng Liên hợp quốc, 2024). Đến nay, Công ước có 81 quốc gia ký, 3 bên tham gia và chưa có hiệu lực vì Điều 65 yêu cầu 40 văn kiện phê chuẩn, chấp thuận, phê duyệt hoặc gia nhập (United Nations Treaty Collection,

2026).

Bên cạnh khuôn khổ điều ước, INTERPOL cung cấp mạng lưới liên lạc cảnh sát, cơ sở dữ liệu, thông báo nghiệp vụ và cơ chế điều phối chiến dịch. Ở khu vực, Tuyên bố ASEAN về phòng ngừa và chống tội phạm mạng năm 2017 khẳng định nhu cầu hợp tác, xây dựng năng lực và chia sẻ thông tin (ASEAN, 2017). Tuyên bố số Bangkok về kỹ thuật số năm 2025 tiếp tục nhấn mạnh Nhóm công tác ASEAN về chống lừa đảo trực tuyến, phối hợp thực thi pháp luật, chia sẻ thông tin và phát triển năng lực ứng cứu sự cố khu vực (ASEAN, 2025); ASEANAPOL bổ sung kênh phối hợp cảnh sát giữa các nước thành viên. Các cơ chế này tạo thành mạng lưới nhiều tầng, trong đó chuẩn mực toàn cầu, điều phối nghiệp vụ và hợp tác khu vực hỗ trợ lẫn nhau.

Ở Việt Nam, nền tảng trong nước cho hợp tác được củng cố bởi Luật Dữ liệu số 60/2024/QH15, Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15, Luật Dẫn độ số 100/2025/QH15, Luật Tương trợ tư pháp về hình sự số 103/2025/QH15 và Luật An ninh mạng số 116/2025/QH15. Các văn bản này điều chỉnh quản trị dữ liệu, bảo vệ dữ liệu cá nhân, dẫn độ, tương trợ tư pháp hình sự và an ninh trên không gian mạng. Trọng tâm hiện nay là bảo đảm tính tương thích giữa các luật, thiết lập quy trình phối hợp và tổ chức thực thi nhất quán.

3.1.3. Các hình thức hợp tác đa phương chủ yếu

Thứ nhất, hợp tác xây dựng chuẩn mực giúp các quốc gia thu hẹp khác biệt về tội danh, thẩm quyền, thu thập dữ liệu và tương trợ tư pháp. Công ước Liên hợp quốc về chống tội phạm mạng tạo nền tảng toàn cầu cho chia sẻ chứng cứ là dữ liệu điện tử trong điều tra tội phạm nghiêm trọng. Văn kiện đồng thời đặt ra yêu cầu bảo đảm quyền con người và chủ quyền quốc gia. Các tuyên bố, kế hoạch hành động của ASEAN tuy chủ yếu mang tính định hướng nhưng hỗ trợ chuyển hóa chuẩn mực toàn cầu thành ưu tiên của khu vực.

Thứ hai, hợp tác chia sẻ thông tin và phối hợp chiến dịch cho phép đồng thời xử lý đối tượng, tài khoản, máy chủ và tên miền tại nhiều nước. Chiến dịch HAECHI V do INTERPOL điều phối năm 2024 có sự tham gia của 40 quốc gia và vùng lãnh thổ. Kết quả gồm hơn 5.500 vụ bắt giữ, trên 400 triệu USD bị thu giữ, 8.309 vụ việc được giải quyết và 1.023 tài khoản của nhà cung cấp dịch vụ tài sản ảo bị phong tỏa

(INTERPOL, 2024). Dữ liệu từ một vụ việc được đối chiếu trên nhiều hệ thống, qua đó phát hiện chủ thể và tài sản mà từng quốc gia khó tự xác định.

Thứ ba, hợp tác triệt phá hạ tầng kỹ thuật tập trung vào nguồn lực giúp tội phạm hoạt động ở quy mô lớn. Trong Chiến dịch Secure năm 2025, cơ quan thực thi pháp luật tại 26 quốc gia đã triệt phá hơn 20.000 địa chỉ giao thức Internet (IP) và tên miền độc hại, tương đương 79% số hạ tầng đáng ngờ được xác định. Chiến dịch còn thu giữ 41 máy chủ, hơn 100 gigabyte (GB) dữ liệu và bắt giữ 32 đối tượng; riêng lực lượng Công an Việt Nam bắt giữ 18 nghi phạm (INTERPOL, 2025b). Triệt phá hạ tầng làm gián đoạn phương tiện phạm tội dùng chung và có tác dụng phòng ngừa đối với nhiều hành vi chưa xảy ra.

Thứ tư, hợp tác về chứng cứ là dữ liệu điện tử, tương trợ tư pháp, dẫn độ, điều tra tài chính và thu hồi tài sản tạo cơ sở để kết quả nghiệp vụ được chuyển hóa thành chứng cứ có giá trị tố tụng. Cùng với đó là đào tạo, diễn tập, hỗ trợ kỹ thuật, nghiên cứu xu hướng và hợp tác công – tư với ngân hàng, doanh nghiệp viễn thông, nền tảng số, nhà cung cấp dịch vụ đám mây và tài sản ảo. Các hình thức này có quan hệ liên hoàn: thông tin nghiệp vụ giúp phát hiện; thủ tục pháp lý giúp sử dụng chứng cứ hiệu quả; phối hợp tài chính giúp ngăn chặn dòng tiền và hoàn trả cho nạn nhân.

3.1.4. Giá trị và đóng góp thực tiễn của các cơ chế đa phương

Kết quả so sánh cho thấy cơ chế Liên hợp quốc có phạm vi thành viên rộng nhất và ưu thế về xây dựng chuẩn mực pháp lý chung. Khi có hiệu lực, Công ước có thể giảm "khoảng trống" do các hệ thống pháp luật khác nhau và tạo cơ sở ổn định hơn cho hợp tác về chứng cứ là dữ liệu điện tử. Đổi lại, quá trình ký, phê chuẩn, nội luật hóa và thực hiện điều ước cần nhiều thời gian; thủ tục chính thức khó đáp ứng được yêu cầu khẩn cấp của dữ liệu dễ mất hoặc dòng tiền dịch chuyển tức thời. Do đó, giá trị của cơ chế này nằm ở tính hợp pháp và bền vững, không phải tốc độ phản ứng tức thì.

INTERPOL có lợi thế về tốc độ, mạng lưới đầu mối và khả năng điều phối chiến dịch toàn cầu. HAECHI V tập trung vào dòng tiền và mạng lưới lừa đảo tài chính, qua đó thực hiện hơn 5.500 vụ bắt giữ. Secure tập trung vào hạ tầng mã độc; số vụ bắt giữ thấp hơn nhưng hơn 20.000 địa chỉ IP và tên miền độc hại đã bị loại bỏ. Sự khác biệt về chỉ số đầu ra phản ánh hai phương thức can thiệp: xử lý đối tượng, tài sản và vô

hiệu hóa hạ tầng. Tuy nhiên, phối hợp cảnh sát không thay thế tương trợ tư pháp hoặc yêu cầu về tính hợp pháp và khả năng được chấp nhận của chứng cứ tại tòa án.

Trong khi đó, ASEAN và ASEANAPOL có ưu thế về sự gần gũi địa lý, mức độ tương đồng về tình hình tội phạm và khả năng xây dựng lòng tin giữa các đầu mối trong khu vực. Cơ chế khu vực thuận lợi cho đào tạo chung, trao đổi thông tin về trung tâm lừa đảo và điều phối các vụ việc liên quan đến nước láng giềng. Hạn chế là nhiều văn kiện còn mang tính "luật mềm", quyết định dựa trên đồng thuận và năng lực thực thi giữa các thành viên không đồng đều.

Đối với Việt Nam, tham gia đồng thời ba tầng cơ chế giúp mở rộng khả năng tiếp cận thông tin, nâng cao vị thế trong kiến tạo chuẩn mực và tăng cơ hội phối hợp vụ án. Việc đăng cai lễ mở ký Công ước tại Hà Nội, ký và sớm phê chuẩn thể hiện vai trò chủ động. Kết quả lực lượng Công an Việt Nam bắt giữ 18 nghi phạm trong Chiến dịch Secure cho thấy sự tham gia đã có sản phẩm nghiệp vụ cụ thể (INTERPOL, 2025b). Tuy nhiên, đóng góp chỉ bền vững khi các cam kết được chuyển thành quy trình trong nước, đầu mối đủ thẩm quyền và năng lực xử lý chứng cứ là dữ liệu điện tử theo chuẩn thống nhất.

3.1.5. Một số hạn chế

Một là, khuôn khổ pháp lý đa phương chưa tạo được mức độ ràng buộc đồng đều. Khác biệt về tội danh, thẩm quyền, điều kiện cung cấp dữ liệu và bảo vệ quyền riêng tư làm tăng chi phí pháp lý, kéo dài thời gian xử lý và có thể khiến chứng cứ mất giá trị sử dụng.

Hai là, công tác đấu tranh, triệt phá chưa tương xứng với quy mô và khả năng tái hình thành của các đường dây tội phạm. Các chiến dịch đa phương thường bị giới hạn về thời gian, địa bàn và đối tượng. Vì vậy, số vụ bắt giữ hay tên miền bị vô hiệu hóa chỉ phản ánh kết quả trực tiếp, chưa đủ để chứng minh tác động bền vững đối với tỷ lệ tội phạm và thiệt hại gây ra cho xã hội.

Ba là, kênh trao đổi thông tin nhanh và thủ tục tư pháp chính thức chưa liên thông đầy đủ. Thông tin có thể giúp xác định tài khoản hoặc máy chủ nhưng muốn phong tỏa tài sản, khám xét, dẫn độ hay sử dụng dữ liệu trước tòa án vẫn phải đáp ứng quy định của

quốc gia liên quan. Sự khác nhau về biểu mẫu, ngôn ngữ, quy trình thu thập, bảo quản và thời hạn lưu trữ dữ liệu làm phát sinh khoảng trống giữa "biết thông tin" và "chứng minh được hành vi". Hệ quả là đối tượng có thời gian xóa dữ liệu, dịch chuyển tài sản hoặc thay đổi hạ tầng trước khi biện pháp tố tụng được thi hành.

Bốn là, năng lực thực thi giữa các quốc gia còn chênh lệch. Hơn một nửa số quốc gia được khảo sát cho biết tội phạm mạng chiếm trên 30% tổng số tội phạm được ghi nhận (INTERPOL, 2026). Quốc gia thiếu nhân lực điều tra số, công cụ phân tích, cơ sở giám định hoặc đầu mối trực 24/7 có thể làm chậm toàn bộ chuỗi phối hợp. Hạn chế này có tính hệ thống, bởi hiệu quả mạng lưới phụ thuộc vào khả năng đáp ứng của từng thành viên.

Năm là, cơ chế đánh giá còn thiên về đầu ra hoạt động, chưa phản ánh đầy đủ hiệu quả phòng ngừa và bảo vệ nạn nhân. Trong khi đó, thời gian phản hồi, tỷ lệ dữ liệu được bảo toàn, tài sản hoàn trả cho nạn nhân, mức độ giảm tái phạm và tính hợp pháp của chứng cứ ít được công bố đồng bộ. Việc thiếu bộ chỉ số chung hạn chế khả năng so sánh giữa các chiến dịch, nhận diện khâu yếu và phân bổ nguồn lực.

3.2. Thảo luận

3.2.1. Những vấn đề đặt ra đối với hợp tác đa phương

Một là, cần giải quyết đồng bộ xung đột thẩm quyền và khác biệt pháp luật. Một vụ việc có thể đồng thời liên quan nơi cư trú của nạn nhân, nơi đặt máy chủ, trụ sở nhà cung cấp dịch vụ, nơi mở tài khoản và nơi đối tượng hiện diện. Công ước Liên hợp quốc tạo cơ sở hội tụ nhưng chưa có hiệu lực tại thời điểm nghiên cứu. Đối với Việt Nam, vấn đề đặt ra là xác định rõ thẩm quyền, nguyên tắc tham vấn và mức độ tương thích giữa Công ước với pháp luật về an ninh mạng, dữ liệu, tố tụng hình sự, dẫn độ và tương trợ tư pháp.

Hai là, cần rút ngắn khoảng cách giữa tốc độ dịch chuyển của dữ liệu, tài sản với thời gian thực hiện thủ tục. Dữ liệu có thể bị xóa theo chính sách lưu giữ; tài khoản có thể bị rút sạch hoặc tài sản mã hóa được chuyển qua nhiều ví trước khi yêu cầu chính thức hoàn tất. Nếu kênh cảnh sát và kênh tư pháp không được kết nối, thông tin phát hiện sớm sẽ không được chuyển hóa thành chứng cứ và biện pháp ngăn chặn hợp pháp.

Đây là vấn đề trực tiếp quyết định khả năng bảo toàn dữ liệu và thu hồi tài sản.

Ba là, cần khắc phục tình trạng phối hợp mang tính phản ứng và phân tán theo từng vụ việc. Tội phạm vận hành theo mạng lưới, dùng chung hạ tầng, tài khoản trung gian và phương thức rửa tiền; trong khi dữ liệu điều tra thường nằm tại nhiều đơn vị, địa phương và quốc gia. Kết quả khác nhau của HAECHI V và Secure chứng minh mục tiêu chiến dịch phải được xác định từ đầu: xử lý đối tượng, thu hồi tài sản hoặc vô hiệu hóa hạ tầng.

Bốn là, cần kiểm soát dòng tiền và huy động có trách nhiệm nguồn lực ngoài nhà nước. Hiện nay, cơ quan chức năng gặp nhiều khó khăn trong phát hiện giao dịch, phong tỏa khẩn cấp, truy vết tài sản mã hóa và hoàn trả tài sản cho nạn nhân. Ngân hàng, trung gian thanh toán, doanh nghiệp viễn thông, nền tảng số và nhà cung cấp dịch vụ tài sản ảo nắm giữ dữ liệu thiết yếu, do vậy việc chia sẻ dữ liệu phải có căn cứ, mục đích, phạm vi và cơ chế bảo vệ rõ ràng.

Năm là, cần xử lý sự câu kết giữa tội phạm mạng và tội phạm có tổ chức xuyên quốc gia bằng cơ chế điều phối liên ngành, liên khu vực. Nạn nhân được ghi nhận đến từ 66 quốc gia; 74% trong số họ bị đưa tới các trung tâm lừa đảo ở Đông Nam Á (INTERPOL, 2025a). Dữ liệu này cho thấy lừa đảo trực tuyến có thể đồng thời gắn với mua bán người, cưỡng bức lao động và rửa tiền. Cơ chế hợp tác phải kết nối lực lượng an ninh mạng, cảnh sát hình sự, cơ quan tài chính, xuất nhập cảnh và tư pháp, đồng thời phát huy vai trò điều phối của ASEAN, ASEANAPOL và INTERPOL.

Sáu là, cần thu hẹp khoảng cách năng lực và quản trị rủi ro công nghệ. INTERPOL ghi nhận 135.000 cuộc tấn công bằng mã độc tống tiền tại khu vực trong năm 2024. Số cuộc tấn công từ chối dịch vụ phân tán tăng 92%; thảo luận về nội dung giả mạo sâu tăng 600%; 66,7% quốc gia được khảo sát đã sử dụng công cụ trí tuệ nhân tạo (AI) trong ứng phó (INTERPOL, 2026). Hỗ trợ kỹ thuật vì vậy phải đi cùng đào tạo nhân lực, tiêu chuẩn kiểm thử công cụ, bảo mật, kiểm soát truy cập và trách nhiệm giải trình.

3.2.2. Giải pháp nâng cao hiệu quả hợp tác đa phương của Việt Nam

Một là, xây dựng kế hoạch quốc gia thực thi Công ước Liên hợp quốc về chống tội phạm mạng sau phê chuẩn. Đây là giải pháp trực tiếp để giải quyết xung đột về thẩm quyền và khác biệt pháp luật nêu trên. Kế hoạch cần phân công cơ quan đầu mối, xác định lộ trình rà soát pháp luật và chuẩn bị quy trình nghiệp vụ. Việc rà soát phải đối chiếu đồng bộ Luật An ninh mạng, Luật Dữ liệu, Luật Bảo vệ dữ liệu cá nhân, Luật Dẫn độ và Luật Tương trợ tư pháp về hình sự. Mỗi đề xuất sửa đổi phải được đánh giá về hiệu quả điều tra, khả năng hợp tác và bảo đảm quyền con người.

Hai là, kiện toàn đầu mối phối hợp 24/7 theo mô hình liên ngành để xử lý độ trễ của dữ liệu và thủ tục. Đầu mối phải có khả năng tiếp nhận, phân loại và chuyển ngay yêu cầu khẩn cấp. Biểu mẫu và quy trình cần thống nhất các khâu bảo toàn dữ liệu, xác thực nguồn, duy trì chuỗi bảo quản chứng cứ là dữ liệu điện tử, chuyển yêu cầu sang kênh tương trợ tư pháp và phản hồi cho đối tác. Hệ thống quản lý vụ việc cần ghi nhận thời gian từng khâu, trạng thái yêu cầu và căn cứ pháp lý, qua đó nâng cao tốc độ xử lý và trách nhiệm giải trình.

Ba là, chuyển từ hợp tác phản ứng theo vụ việc sang hợp tác dựa trên thông tin nghiệp vụ và đấu tranh chuyên án chung. Việt Nam cần chủ động cung cấp chỉ dấu tấn công, tài khoản trung gian, ví tài sản mã hóa, tên miền và phương thức hoạt động; đề xuất chuyên án chung đa quốc gia đối với mạng lưới có liên quan đến Việt Nam. Kinh nghiệm HAECHI V và Secure cho thấy kế hoạch phải xác định rõ mục tiêu ưu tiên: bắt giữ đối tượng, phong tỏa tài sản hoặc triệt phá hạ tầng. Trên cơ sở đó, cơ quan điều phối lựa chọn chỉ số đánh giá phù hợp, tránh đồng nhất số vụ bắt giữ với toàn bộ hiệu quả phòng ngừa.

Bốn là, tăng cường hợp tác điều tra tài chính, thu hồi tài sản và hợp tác công - tư. Cần thiết lập cơ chế phối hợp nhanh giữa cơ quan thực thi pháp luật, ngân hàng, trung gian thanh toán, doanh nghiệp viễn thông, nền tảng số và nhà cung cấp dịch vụ tài sản ảo. Cơ quan chức năng cần phát triển năng lực lần theo giao dịch chuỗi khối, yêu cầu phong tỏa khẩn cấp và thực hiện thu hồi xuyên biên giới. Thỏa thuận hợp tác công - tư phải quy định rõ căn cứ, mục đích, phạm vi dữ liệu, thời hạn lưu giữ, bảo mật và cơ chế kiểm tra. Giá trị tài sản được hoàn trả cho nạn nhân cần được xác định là một chỉ số kết quả chủ yếu.

Năm là, phát huy vai trò chủ động tại Liên hợp quốc, INTERPOL, ASEAN và ASEANAPOL để xử lý các chuỗi tội phạm liên ngành, liên khu vực. Việt Nam có thể đề xuất cơ chế khu vực về bảo toàn chứng cứ là dữ liệu điện tử, diễn tập chung để xử lý các trung tâm lừa đảo. Việc xây dựng chuẩn mực cần gắn với tổng kết thực tiễn trong nước, nhất là kinh nghiệm điều tra lừa đảo trực tuyến, bảo vệ trẻ em và triệt phá hạ tầng mã độc.

Sáu là, đầu tư có trọng tâm cho nhân lực, công nghệ và cơ chế kiểm soát. Cần phát triển đội ngũ kết hợp kiến thức điều tra, pháp luật quốc tế, ngoại ngữ, dữ liệu và tài sản số; duy trì đào tạo chung, kiểm tra năng lực định kỳ và mạng lưới chuyên gia có thể huy động nhanh. Công cụ AI phục vụ phân tích phải được kiểm thử, giám sát sai lệch và lưu vết quyết định. Bộ chỉ số hợp tác cần phản ánh thời gian phản hồi, tỷ lệ yêu cầu được đáp ứng, dữ liệu được bảo toàn, tài sản bị phong tỏa hoặc thu hồi và hạ tầng bị vô hiệu hóa.

4. Kết luận

Hợp tác đa phương là phương thức không thể thiếu để thu hẹp khoảng cách giữa tính xuyên biên giới của tội phạm mạng với giới hạn lãnh thổ của quyền tài phán quốc gia. Phân loại tội phạm phụ thuộc vào công nghệ và tội phạm được công nghệ hỗ trợ giúp nhận diện vai trò của công nghệ trong hành vi. Các khái niệm tội phạm mạng và tội phạm công nghệ cao trong tiêu đề phản ánh phạm vi nghiên cứu và thực tiễn sử dụng thuật ngữ tại Việt Nam. Việc làm rõ các tầng khái niệm giúp lựa chọn đúng công cụ hợp tác, từ triệt phá hạ tầng kỹ thuật đến điều tra tội phạm truyền thống được số hóa. Đây cũng là điều kiện để chuyển cam kết chính trị thành năng lực phòng ngừa, phát hiện và xử lý tội phạm, góp phần chủ động phòng ngừa nguy cơ từ sớm, từ xa, bảo đảm an ninh quốc gia, giữ gìn trật tự, an toàn xã hội./.

Tài liệu tham khảo

ASEAN. (2017, November 14). ASEAN declaration to prevent and combat cybercrime. https://asean.org/asean-declaration-to-prevent-and-combat-cybercrime/

ASEAN. (2025, January 17). Bangkok Digital Declaration. https://asean.org/wp-content/uploads/2025/01/14-ENDORSED-BANGKOK-DIGITAL-DECLARATION.pdf

INTERPOL. (2024, November 27). INTERPOL financial crime operation makes record 5,500 arrests, seizures worth over USD 400 million. https://www.interpol.int/News-and-Events/News/2024/INTERPOL-financial-crime-operation-makes-record-5-500-arrests-seizures-worth-over-USD-400-million

INTERPOL. (2025a, June 11). 20,000 malicious IPs and domains taken down in INTERPOL infostealer crackdown. https://www.interpol.int/News-and-Events/News/2025/20-000-malicious-IPs-and-domains-taken-down-in-INTERPOL-infostealer-crackdown

INTERPOL. (2025b, June 30). INTERPOL releases new information on globalization of scam centres. https://www.interpol.int/News-and-Events/News/2025/INTERPOL-releases-new-information-on-globalization-of-scam-centres

INTERPOL. (2026). INTERPOL Asia and South Pacific cyber threat assessment report 2025/2026. https://www.interpol.int/content/download/24327/file/CYBER_ASP%20Cyber%20Threat%20Assessment%20Report

Luật An ninh mạng (Số 116/2025/QH15, 2025). Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam. https://vanban.chinhphu.vn/?classid=1&docid=216499&orggroupid=1&pageid=27160

Luật Bảo vệ dữ liệu cá nhân (Số 91/2025/QH15, 2025). Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam. https://vanban.chinhphu.vn/?classid=1&docid=214590&pageid=27160&typegroupid=3

Luật Dẫn độ (Số 100/2025/QH15, 2025). Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam. https://vanban.chinhphu.vn/?classid=1&docid=216574&pageid=27160&typegroupid=3

Luật Dữ liệu (Số 60/2024/QH15, 2024). Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam. https://vanban.chinhphu.vn/?classid=1&docid=212488&orggroupid=1&pageid=27160

Luật Tương trợ tư pháp về hình sự (Số 103/2025/QH15, 2025). Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam. https://vanban.chinhphu.vn/?classid=1&docid=216570&orggroupid=1&pageid =27160

Nghị quyết về Công ước Liên hợp quốc về chống tội phạm mạng (A/RES/79/243, 2024). Đại hội đồng Liên hợp quốc. https://documents.un.org/doc/undoc/gen/n24/426/74/pdf/n2442674.pdf

Ruggie, J. G. (1992). Multilateralism: The anatomy of an institution. International Organization, 46(3), 561-598. https://doi.org/10.1017/S0020818300027831

United Nations Office on Drugs and Crime. (2026). An interconnected criminal ecosystem: Transnational organized crime threat assessment for South-East Asia. https://doi.org/10.18356/ 9789211577891

United Nations Treaty Collection. (n.d.). United Nations Convention against Cybercrime. Retrieved August 22, 2026, from https://treaties.un.org/pages/ViewDetails.aspx?chapter=18&clang=_en&mtdsg_no=XVIII-16&src=TREATY

Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity Press.