CÔNG ƯỚC HÀ NỘI NĂM 2025 VÀ TRIỂN VỌNG TĂNG CƯỜNG HỢP TÁC ASEAN TRONG PHÒNG, CHỐNG TỘI PHẠM MẠNG

THE HANOI CONVENTION AND PROSPECTS FOR STRENGTHENING ASEAN COOPERATION IN COMBATING CYBERCRIME

Trần Thị Ngọc Sương*, Lê Thị Hồng Ngọc

Trường Đại học Ngoại ngữ - Đại học Đà Nẵng, Việt Nam[1]

*Tác giả liên hệ / Corresponding author: ttnsuong@ufl.udn.vn

(Nhận bài / Received: 01/3/2026; Sửa bài / Revised: 11/4/2026; Chấp nhận đăng / Accepted: 17/4/2026)

DOI: 10.31130/ud-jst.2026.24(5B).267

Tóm tắt - Sự ra đời của Công ước Liên Hợp Quốc (LHQ) về chống tội phạm mạng năm 2025 (Công ước Hà Nội) phản ánh nỗ lực toàn cầu mạnh mẽ trong việc thiết lập một khuôn khổ pháp lý thống nhất có tính ràng buộc cho hợp tác phòng, chống tội phạm mạng. Công ước đem lại những cơ hội xen lẫn các thách thức đối với Hiệp hội các quốc gia Đông Nam Á (Association of Southeast Asian Nations - ASEAN) trong việc xây dựng nền tảng pháp lý chung, nâng cao hiệu quả thực thi, phát triển năng lực và thúc đẩy hợp tác đa bên trong lĩnh vực này. Trong bối cảnh đó, Việt Nam cần chủ động hoàn thiện pháp luật trong nước, tích cực tham gia và đề xuất các sáng kiến hợp tác phù hợp với các chuẩn mực của Công ước. Đồng thời, cần chú trọng bảo đảm hài hòa giữa tăng cường hợp tác quốc tế và bảo vệ chủ quyền quốc gia, qua đó góp phần củng cố cơ chế hợp tác của ASEAN trong phòng, chống tội phạm mạng.

Từ khóa - Công ước Hà Nội; ASEAN; tội phạm mạng; hợp tác; Việt Nam

Abstract - The adoption of the United Nations Convention against Cybercrime in 2025 (the Hanoi Convention) represents a significant global effort to establish a comprehensive legally binding framework for cooperation in preventing and combating cybercrime. The Convention offers both opportunities and challenges for the Association of Southeast Asian Nations (ASEAN) in strengthening a common legal basis, improving enforcement effectiveness, enhancing capacity-building, and fostering multi-stakeholder cooperation in this domain. In this context, Viet Nam should further develop its domestic legal framework and play a more active role in promoting cooperative mechanisms in line with the Convention. At the same time, it is important to strike an appropriate balance between deepening international cooperation and safeguarding national sovereignty, thereby contributing to the consolidation of ASEAN's regional mechanisms for combating cybercrime.

Key words - Hanoi Convention; ASEAN; cybercrime; cooperation; Viet Nam

1. Đặt vấn đề

Tội phạm mạng đang nổi lên như một thách thức an ninh phi truyền thống nghiêm trọng, đặc biệt trong bối cảnh chuyển đổi số và kết nối internet ngày càng sâu rộng [1]. Tại Đông Nam Á, sự phát triển nhanh chóng của nền kinh tế số đã dẫn đến sự gia tăng các hành vi tấn công mạng, lừa đảo trực tuyến, đánh cắp dữ liệu và các loại tội phạm sử dụng công nghệ cao [2]. Vì vậy, tăng cường hợp tác quốc tế, đặc biệt là trong khuôn khổ ASEAN, là yêu cầu cấp thiết nhằm nâng cao hiệu quả phòng, chống tội phạm mạng.

Trong bối cảnh đó, việc ký kết Công ước Hà Nội đánh dấu bước tiến quan trọng trong việc thiết lập khuôn khổ pháp lý quốc tế nhằm thúc đẩy hợp tác giữa các quốc gia [3]. Công ước không chỉ góp phần hoàn thiện các chuẩn mực pháp lý toàn cầu, mà còn mở ra những cơ hội mới để các quốc gia ASEAN tăng cường chia sẻ thông tin, hỗ trợ pháp lý và nâng cao năng lực thực thi pháp luật.

Trên cơ sở các phương pháp phân tích - tổng hợp, logic - lịch sử, so sánh - đối chiếu và dự báo, bài viết làm rõ các quy định cốt lõi của Công ước Hà Nội và đánh giá triển vọng hợp tác ASEAN trên các phương diện: xây dựng và thực thi pháp luật, thúc đẩy năng lực và hợp tác đa bên trong phòng, chống tội phạm mạng. Từ đó, bài viết đề xuất một số định hướng đối với Việt Nam nhằm phát huy vai trò chủ động thúc đẩy hợp tác khu vực trong bối cảnh chuyển đổi số và hội nhập quốc tế ngày càng sâu rộng.

2. Sự ra đời và nội dung chính của Công ước Hà Nội

2.1. Bối cảnh ra đời của Công ước Hà Nội

Trong những thập niên gần đây, sự phát triển nhanh chóng của công nghệ thông tin và internet đã thúc đẩy mạnh mẽ kinh tế - xã hội, nhưng đồng thời cũng làm gia tăng đáng kể các loại tội phạm mạng trên phạm vi toàn cầu như tấn công mạng, lừa đảo trực tuyến, đánh cắp dữ liệu và phát tán mã độc [4]. Với tính chất xuyên biên giới, các hành vi này đã gây nhiều khó khăn cho hoạt động điều tra, truy tố và xét xử, từ đó đặt ra nhiều thách thức nghiêm trọng đối với hệ thống tư pháp hình sự của các quốc gia.

Trước khi Công ước Hà Nội ra đời, Công ước Budapest năm 2001 được xem là khuôn khổ pháp lý quốc tế đầu tiên và quan trọng nhất về phòng, chống tội phạm mạng [5]. Tuy nhiên, do được xây dựng chủ yếu trong phạm vi châu Âu và thiếu sự tham gia rộng rãi của các nước đang phát triển [6], [7], nên Công ước Budapest đã dần bộc lộ nhiều hạn chế, đặc biệt liên quan đến vấn đề chủ quyền số và chia sẻ dữ liệu xuyên biên giới [8].

[1] The University of Danang - University of Foreign Language Studies, Vietnam (Tran Thi Ngoc Suong, Le Thi Hong Ngoc)

Trong bối cảnh đó, nhu cầu xây dựng một khuôn khổ pháp lý mang tính toàn cầu ngày càng trở nên cấp thiết. Năm 2019, Đại hội đồng LHQ đã thông qua Nghị quyết 74/247 nhằm khởi động tiến trình đàm phán một điều ước quốc tế mới với sự tham gia rộng rãi của các quốc gia dưới sự điều phối của Cơ quan phòng chống ma túy và tội phạm của LHQ (United Nations Office on Drugs and Crime - UNODC) [9] [10]. Tiến trình này đã dẫn đến việc thông qua Công ước về chống tội phạm mạng, được mở ký tại Hà Nội vào ngày 25 - 26/10/2025, qua đó thiết lập một khuôn khổ pháp lý toàn diện đầu tiên của LHQ trong lĩnh vực này [11].

2.2. Các nội dung chính của Công ước Hà Nội

2.2.1. Các nghĩa vụ về chống tội phạm mạng

a. Xác định các loại tội phạm mạng

Công ước Hà Nội xác định các nhóm tội phạm liên quan đến công nghệ thông tin và truyền thông (Information and Communication Technologies - ICT) mà các quốc gia cần phải xử lý về mặt hình sự, bao gồm: truy cập và can thiệp trái phép hệ thống ICT, dữ liệu và đường truyền; lạm dụng thiết bị; giả mạo, trộm cắp hoặc gian lận liên quan đến hệ thống ICT; tội phạm liên quan đến lạm dụng tình dục trẻ em trực tuyến; phát tán hình ảnh nhạy cảm không có sự đồng thuận; và rửa tiền từ các hành vi này (Điều 7 -17) [3]. Nhìn chung, các quy định này đã phản ánh thực tiễn gia tăng của tội phạm trong môi trường số, đồng thời tạo cơ sở chung để các quốc gia nội luật hóa, từ đó tăng cường hiệu quả hợp tác quốc tế trong phòng, chống tội phạm mạng.

b. Hình sự hóa trong pháp luật quốc gia

Công ước Hà Nội yêu cầu các quốc gia thành viên phải hình sự hóa các hành vi tội phạm mạng trong pháp luật quốc gia. Theo Chương II, các quốc gia phải ban hành hoặc sửa đổi pháp luật để bảo đảm rằng các hành vi sử dụng ICT để thực hiện tội phạm được quy định là tội phạm, đồng thời thiết lập cơ sở pháp lý cho việc điều tra, truy tố các vụ việc có yếu tố xuyên biên giới [3].

Đồng thời, Công ước cũng khuyến khích tăng cường năng lực thể chế và pháp lý, thúc đẩy hài hòa hóa quy định hình sự và thiết lập các cơ chế hợp tác như dẫn độ, tương trợ tư pháp hình sự và chia sẻ chứng cứ điện tử theo quy định tại Chương V [3]. Như vậy, Công ước hướng tới việc nâng cao tính tương thích giữa các hệ thống pháp luật và tăng cường hiệu quả hợp tác quốc tế trong phòng, chống tội phạm mạng.

c. Thực hiện nguyên tắc đảm bảo chủ quyền quốc gia và quyền con người

Công ước nhấn mạnh nguyên tắc tôn trọng chủ quyền quốc gia và không can thiệp vào công việc nội bộ, qua đó góp phần củng cố lòng tin giữa các quốc gia trong lĩnh vực an ninh mạng (Điều 5) [3]. Đồng thời, Công ước còn yêu cầu đảm bảo quyền con người trong toàn bộ quá trình phòng, chống tội phạm mạng. Các biện pháp điều tra và hợp tác quốc tế phải phù hợp với luật pháp quốc tế, đặc biệt về quyền riêng tư, tự do biểu đạt và xét xử công bằng; tuân thủ nguyên tắc hợp pháp, cần thiết và tương xứng, dưới sự giám sát của pháp luật quốc gia (Điều 6) [3]. Đây là những nguyên tắc từng gây tranh luận trong quá trình đàm phán Công ước Hà Nội, nhưng lại được xem là yếu tố quan trọng để bảo đảm tính chính danh và khả năng được chấp nhận rộng rãi của Công ước [12].

2.2.2. Các biện pháp hợp tác quốc tế

Hợp tác quốc tế là yêu cầu bắt buộc trong việc xử lý các tội phạm mạng xuyên biên giới. Theo đó, các biện pháp hợp tác quốc tế mà Công ước Hà Nội quy định bao gồm:

a. Tương trợ tư pháp hình sự

Công ước Hà Nội thiết lập cơ chế tương trợ tư pháp hình sự nhằm hỗ trợ quá trình điều tra, truy tố và xét xử tội phạm mạng. Theo Điều 36, các quốc gia thành viên có nghĩa vụ hợp tác với nhau ở mức độ rộng nhất; Điều 37 cho phép quốc gia đề xuất hoặc cung cấp hỗ trợ pháp lý trong các hoạt động tố tụng như thu thập chứng cứ, lấy lời khai, xác định danh tính và cung cấp thông tin tài khoản, giao dịch điện tử [3]. Như vậy, các biện pháp này sẽ tạo điều kiện cho các cơ quan thực thi pháp luật vượt qua các rào cản về thẩm quyền lãnh thổ khi xử lý các vụ án tội phạm mạng xuyên biên giới.

b. Trao đổi thông tin và chứng cứ điện tử

Điều 39 quy định các quốc gia thành viên có thể trao đổi thông tin về các phương thức, thủ đoạn, xu hướng tội phạm mạng và các biện pháp phòng ngừa [3], qua đó góp phần nhận diện sớm và xử lý hiệu quả các mối đe dọa. Ngoài ra, Điều 40 khuyến khích các quốc gia thiết lập các cơ chế pháp lý và kỹ thuật để thu thập, bảo quản và chuyển giao chứng cứ điện tử phục vụ quá trình điều tra và truy tố, vốn rất dễ bị thay đổi hoặc xóa bỏ nhanh chóng trong môi trường số [3].

c. Hợp tác điều tra và dẫn độ

Công ước Hà Nội cũng thúc đẩy các hình thức hợp tác sâu rộng hơn như hợp tác điều tra và dẫn độ tội phạm mạng. Theo Điều 41, các hành vi phạm tội trong Công ước có thể được sử dụng làm cơ sở pháp lý cho việc dẫn độ, phù hợp với pháp luật quốc gia và điều ước quốc tế liên quan [3], nhằm tránh việc tội phạm lợi dụng sự khác biệt giữa các hệ thống pháp luật để trốn tránh trách nhiệm hình sự.

Bên cạnh đó, Điều 42 cho phép thiết lập các nhóm điều tra chung hoặc tiến hành các hình thức hợp tác điều tra khác trong những vụ án xuyên biên giới [3], qua đó tăng cường hiệu quả phát hiện, xử lý tội phạm mạng và phối hợp giữa các cơ quan thực thi pháp luật của các quốc gia.

d. Các biện pháp hợp tác khác

Bên cạnh các cơ chế hợp tác ràng buộc trong tố tụng hình sự, Công ước cũng khuyến khích các hình thức hợp tác linh hoạt nhằm tăng cường hiệu quả phòng ngừa và ứng phó với tội phạm mạng. Cụ thể, Điều 54 - 56 nhấn mạnh nghĩa vụ thúc đẩy chia sẻ thông tin, hỗ trợ kỹ thuật, nâng cao năng lực cho các quốc gia đang phát triển và thiết lập mạng lưới đầu mối liên lạc 24/7 để phản ứng nhanh trước các sự cố và hành vi phạm tội trên không gian mạng [3].

Ngoài ra, Công ước Hà Nội cũng đề cao hợp tác đa bên, bao gồm khu vực tư nhân và các chủ thể phi nhà nước trong bảo đảm an ninh mạng toàn cầu. Điều 55(1) khuyến khích phối hợp giữa cơ quan hành pháp, cơ quan tư pháp với các doanh nghiệp cung cấp dịch vụ và hạ tầng công nghệ số [3], qua đó tăng cường hiệu quả phát hiện, ngăn chặn và xử lý tội phạm mạng. Trong bối cảnh phần lớn hạ tầng và dữ liệu là do tư nhân quản lý [13], sự phối hợp công - tư trở thành yếu tố then chốt nhằm phát hiện, ngăn chặn và xử lý tội phạm mạng một cách hiệu quả. Cách tiếp cận này phản

ánh xu hướng quản trị không gian mạng dựa trên mô hình đa chủ thể, trong đó Nhà nước, doanh nghiệp và xã hội cùng hợp tác xây dựng môi trường mạng an toàn, ổn định và bền vững [13], [14].

Nhìn chung, Công ước Hà Nội năm 2025 đã thiết lập một khuôn khổ pháp lý quốc tế tương đối toàn diện cho hợp tác phòng, chống tội phạm mạng, tạo nền tảng quan trọng để tăng cường phối hợp giữa các quốc gia, trong đó có các nước ASEAN.

3. Thực trạng hợp tác phòng, chống tội phạm mạng ở ASEAN

3.1. Tình hình tội phạm mạng ở ASEAN

Trong những năm gần đây, tội phạm mạng đã gia tăng nhanh chóng ở Đông Nam Á và trở thành thách thức an ninh phi truyền thống nổi bật đối với các quốc gia ASEAN. Các hành vi như lừa đảo trực tuyến, gian lận tài chính, đánh cắp dữ liệu và tấn công mạng ngày càng phổ biến, với sự tham gia ngày càng nhiều của các mạng lưới tội phạm xuyên quốc gia [15]. Năm 2023, thiệt hại từ các hoạt động lừa đảo trực tuyến tại Đông Á và Đông Nam Á đã lên đến 18 - 37 tỷ USD [16], [17]. Đặc biệt, sự phát triển của các công nghệ mới như trí tuệ nhân tạo, nội dung giả mạo (deepfake) và tiền điện tử đã tiếp tục làm gia tăng mức độ tinh vi của tội phạm mạng [17], trong đó số lượng deepfake ở Đông Nam Á đã tăng đến hơn 600% trong nửa đầu năm 2024 [18]. Thêm vào đó, các đường dây tội phạm công nghệ cao được tổ chức ngày càng có quy mô và chặt chẽ, từ khâu tấn công cho đến rửa tiền [19].

Đồng thời, đặc điểm xuyên biên giới đã khiến các hoạt động tội phạm mạng thường liên quan đến nhiều quốc gia. Cụ thể, các mạng lưới tội phạm có thể đặt cơ sở hoạt động tại một quốc gia, sử dụng hạ tầng kỹ thuật số ở quốc gia khác và tấn công vào các nạn nhân trên phạm vi toàn cầu [20]. Điều này cho thấy Đông Nam Á đang trở thành một điểm nóng về tội phạm mạng, và do vậy đặt ra yêu cầu cấp thiết về tăng cường hợp tác khu vực và quốc tế nhằm ứng phó hiệu quả với loại tội phạm này.

3.2. Các văn kiện và cơ chế hợp tác của ASEAN về phòng, chống tội phạm mạng

3.2.1. Các văn kiện về hợp tác chống tội phạm mạng

Cho đến nay, mặc dù chưa ký kết một điều ước khu vực riêng về tội phạm mạng, nhưng ASEAN đã ban hành nhiều văn kiện thúc đẩy hợp tác như: Kế hoạch hành động chống tội phạm xuyên quốc gia (1999) [21], Tuyên bố Kuala Lumpur về chống tội phạm xuyên quốc gia (2015) [22] và Kế hoạch hành động chống tội phạm xuyên quốc gia giai đoạn 2016 - 2025 (2017) [23]. Đặc biệt, Tuyên bố ASEAN năm 2017 về phòng, chống tội phạm mạng tái khẳng định cam kết tăng cường hợp tác và hoàn thiện khuôn khổ quốc gia nhằm ứng phó với việc lạm dụng không gian mạng [24].

Bên cạnh đó, Kế hoạch Tổng thể số ASEAN 2025 (2021) đã xác định an ninh mạng là một trụ cột của chuyển đổi số, nhấn mạnh chia sẻ thông tin, nâng cao năng lực ứng phó và hài hòa chính sách, pháp luật giữa các quốc gia thành viên [25]. Đồng thời, Chiến lược hợp tác an ninh mạng ASEAN giai đoạn 2021 - 2025 (2022) đề ra định hướng tăng cường năng lực phòng thủ, chia sẻ tình báo và phối hợp xử lý sự cố, với cách tiếp cận hợp tác đa bên giữa nhà nước, doanh nghiệp và các tổ chức quốc tế [26].

3.2.2. Các cơ chế hợp tác chống tội phạm mạng

Trên cơ sở các tuyên bố và kế hoạch hành động, ASEAN đã thiết lập nhiều cơ chế hợp tác phòng, chống các loại tội phạm xuyên quốc gia, trong đó có tội phạm mạng. Nổi bật nhất là Hội nghị Bộ trưởng ASEAN về phòng, chống tội phạm xuyên quốc gia (ASEAN Ministerial Meeting on Transnational Crime - AMMTC) với vai trò điều phối các sáng kiến hợp tác khu vực trong phòng, chống tội phạm xuyên quốc gia [27]. Ngoài ra còn có một số cơ chế khác như: Hội nghị Quan chức cấp cao ASEAN về tội phạm xuyên quốc gia (Senior Officials Meeting on Transnational Crime - SOMTC) [28], Nhóm công tác ASEAN về tội phạm mạng (ASEAN Working Group on Cybercirme - AWGC) [29], Hiệp hội Cảnh sát các nước Đông Nam Á (ASEAN Chiefs of Police - ASEANAPOL) [30], Ủy ban điều phối an ninh mạng ASEAN (ASEAN Cybersecurity Coordinating Committee) [31], và Bàn điều phối hoạt động chống tội phạm mạng ASEAN (ASEAN Cybercrime Operations Desk) [32],… Thông qua các cơ chế này, các quốc gia ASEAN thường xuyên trao đổi thông tin, chia sẻ kinh nghiệm, xây dựng chương trình hợp tác nhằm ứng phó với các loại tội phạm mới, trong đó tội phạm mạng được xem là lĩnh vực ưu tiên [21].

Nhìn chung, thông qua việc ký kết các văn kiện và xây dựng các cơ chế hợp tác liên chính phủ, ASEAN đã từng bước thiết lập nền tảng hợp tác khu vực tương đối toàn diện trong phòng, chống tội phạm mạng.

3.3. Các hoạt động hợp tác ASEAN trong phòng, chống tội phạm mạng

Các quốc gia ASEAN đã thiết lập các kênh trao đổi thông tin, cảnh báo sớm và các chương trình đào tạo nhằm tăng cường phối hợp điều tra và xử lý các loại tội phạm mạng. Một số chiến dịch quốc tế cho thấy hiệu quả rõ rệt như Operation HAECHI V do INTERPOL điều phối với sự tham gia của nhiều nước ASEAN, với hơn 5.500 vụ bắt giữ và khoảng 400 triệu USD bị tịch thu [33]. Trong khuôn khổ ASEANAPOL, các trung tâm chống lừa đảo trực tuyến được thành lập để thúc đẩy chia sẻ thông tin - dữ liệu và phối hợp điều tra giữa các quốc gia, góp phần thu hồi hàng trăm nghìn USD từ các mạng lưới lừa đảo xuyên biên giới [34].

Bên cạnh đó, ASEAN còn triển khai các sáng kiến hợp tác quản trị và vận hành không gian mạng như Trung tâm An ninh mạng Xuất sắc ASEAN - Singapore và Trung tâm Xây dựng năng lực an ninh mạng ASEAN - Nhật Bản nhằm triển khai huấn luyện, diễn tập an ninh mạng, điều tra số, phân tích mã độc và ứng phó sự cố mạng [35], [36]. Đáng chú ý, ASEAN cũng đẩy mạnh hợp tác với các đối tác ngoài khu vực và các tổ chức quốc tế như Microsoft, INTERPOL, UNODC và Liên minh Viễn thông quốc tế nhằm hỗ trợ kỹ thuật, đào tạo chuyên môn và thúc đẩy các chiến dịch phối hợp điều tra tội phạm mạng xuyên quốc gia [37], [38]. Những nỗ lực này đã góp phần tăng cường năng lực thực thi pháp luật và thúc đẩy sự hình thành mạng lưới chuyên gia an ninh mạng trong khu vực.

4. Triển vọng tăng cường hợp tác ASEAN trong phòng, chống tội phạm mạng theo Công ước Hà Nội

4.1. Về xây dựng pháp luật phòng, chống tội phạm mạng

Có thể thấy rằng, mặc dù ASEAN đã ban hành nhiều văn kiện về hợp tác an ninh mạng và quản trị mạng, nhưng các văn kiện này chủ yếu mang tính định hướng, chưa thiết lập được các nghĩa vụ ràng buộc chặt chẽ, đồng thời vẫn thiếu một khuôn khổ pháp lý chung về tội phạm mạng. Trong bối cảnh đó, Công ước Hà Nội, vốn đã được 8/11 quốc gia thành viên ASEAN ký kết (tính đến ngày 28/2/2026) [39], có thể đóng vai trò là chuẩn mực tham chiếu quan trọng nhất nhằm thúc đẩy hoàn thiện pháp luật trong nước và từng bước hài hòa hệ thống pháp lý khu vực về tội phạm mạng. Điều này sẽ góp phần thu hẹp sự khác biệt trong pháp luật quốc gia về định nghĩa tội phạm mạng, thẩm quyền tài phán và thu thập chứng cứ điện tử, qua đó tạo thuận lợi cho hợp tác điều tra và tương trợ tư pháp trong các vụ việc xuyên biên giới [40].

Bên cạnh đó, các chuẩn mực pháp lý của Công ước Hà Nội còn góp phần củng cố các cơ chế hợp tác hiện hành của ASEAN về tội phạm mạng, giảm thiểu xung đột pháp lý và tạo cơ sở triển khai hiệu quả các cơ chế như dẫn độ tội phạm, tương trợ tư pháp và chia sẻ chứng cứ điện tử. Tuy nhiên, việc thúc đẩy một nền tảng pháp lý thống nhất chung giữa các nước ASEAN theo Công ước Hà Nội sẽ đối mặt với nhiều thách thức, đặc biệt là sự chênh lệch về trình độ pháp lý và năng lực thực thi giữa các nước thành viên [41]. Mặt khác, đặc trưng của "Phương thức ASEAN" (ASEAN Way), với trọng tâm là nguyên tắc đồng thuận và tôn trọng chủ quyền quốc gia [42], có thể làm chậm tiến trình hài hòa hóa pháp luật trong các lĩnh vực nhạy cảm như chia sẻ thông tin điều tra, trao đổi dữ liệu điện tử hay phối hợp truy tố tội phạm mạng [43].

4.2. Về thực thi pháp luật phòng, chống tội phạm mạng

Tính chất xuyên quốc gia của tội phạm mạng, với sự liên quan đến nhiều hệ thống pháp luật [20], đã khiến cho hợp tác xuyên biên giới giữa các cơ quan thực thi pháp luật trở thành điều kiện then chốt để xử lý hiệu quả các mạng lưới tội phạm ngày càng mở rộng [44]. Trong bối cảnh đó, Công ước Hà Nội mở ra triển vọng tăng cường hợp tác thực thi pháp luật trong ASEAN. Các quy định về tương trợ tư pháp hình sự, dẫn độ và hợp tác điều tra sẽ góp phần thúc đẩy sự phối hợp, chuẩn hóa quy trình và rút ngắn thời gian xử lý các vụ án xuyên quốc gia, đặc biệt đối với các tội phạm phổ biến như lừa đảo trực tuyến, tấn công mạng, rửa tiền và các tội phạm công nghệ cao khác [44].

Tuy nhiên, hợp tác thực thi trong ASEAN vẫn đối mặt với nhiều thách thức, khi các cơ chế khu vực hiện hành như AMMTC hay SOMTC thường tập trung chủ yếu vào việc trao đổi thông tin và điều phối chính sách, trong khi phần lớn hoạt động điều tra và truy tố vẫn phụ thuộc vào hợp tác song phương [45]. Bên cạnh đó, sự chênh lệch về năng lực kỹ thuật, nguồn nhân lực và hệ thống pháp luật giữa các quốc gia thành viên cũng ảnh hưởng đến hiệu quả phối hợp điều tra và chia sẻ thông tin trong các vụ án xuyên biên giới [41].

4.3. Về xây dựng năng lực phòng, chống tội phạm mạng

Công ước Hà Nội nhấn mạnh tầm quan trọng của xây dựng năng lực, yêu cầu các quốc gia phát triển chuyên môn và nguồn lực cần thiết để phòng, chống tội phạm mạng [3]. Thông qua các biện pháp cụ thể về hỗ trợ kỹ thuật, chia sẻ kinh nghiệm và đào tạo, Công ước góp phần nâng cao năng lực điều tra, thu thập chứng cứ điện tử và xử lý tội phạm mạng [3]. Do đó, Công ước đã bổ sung những khoảng trống trong các sáng kiến hợp tác hiện hành của ASEAN, vốn chủ yếu tập trung vào quản trị mạng và an ninh mạng mà chưa chú trọng đầy đủ đến các kỹ năng chuyên sâu về tội phạm mạng (như kỹ thuật điều tra chuyên biệt, bảo quản chứng cứ điện tử, hay bảo vệ nạn nhân và nhân chứng) [45]. Điều này mở ra cơ hội đáng kể cho các quốc gia ASEAN, đặc biệt là các nước đang phát triển trong việc thu hẹp khoảng cách về hạ tầng số, trình độ nhân lực và năng lực thực thi.

Đối với ASEAN, các cơ chế hợp tác và hỗ trợ xây dựng năng lực theo Công ước tạo điều kiện tiếp cận nguồn lực, công nghệ và các chương trình đào tạo quốc tế. Hiện tại, ở khu vực Đông Nam Á vẫn tồn tại nhiều sáng kiến được triển khai ngoài khuôn khổ ASEAN như Dự án Phát triển năng lực mạng của INTERPOL do Bộ Ngoại giao Mỹ tài trợ [46]. Tuy nhiên, sự chênh lệch về trình độ phát triển giữa các quốc gia thành viên, cùng với mức độ phụ thuộc vào hỗ trợ bên ngoài, có thể ảnh hưởng đến hiệu quả và tính bền vững, cũng như đặt ra yêu cầu về tăng cường tính tự chủ của khu vực.

4.4. Về hợp tác đa bên trong phòng, chống tội phạm mạng

Do phần lớn hạ tầng và dữ liệu số do khu vực tư nhân vận hành và quản lý [13], nên nỗ lực phòng, chống tội phạm mạng đòi hỏi sự tham gia của các chủ thể phi nhà nước như doanh nghiệp, tổ chức quốc tế và giới học thuật. Định hướng hợp tác đa bên này của Công ước Hà Nội vì vậy sẽ góp phần thúc đẩy ASEAN chuyển dịch từ mô hình hợp tác chủ yếu trong khuôn khổ các cơ chế liên chính phủ như SOMTC - nơi các nội dung thảo luận và kế hoạch hành động chưa được công khai đầy đủ - sang một cách tiếp cận bao trùm và thực chất hơn, với sự tham gia rộng rãi của các chủ thể liên quan [45].

Ngoài ra, hợp tác đa bên còn giúp ASEAN tận dụng nguồn lực và chuyên môn từ khu vực tư nhân, đồng thời tăng cường kết nối với các mạng lưới quốc tế, qua đó nâng cao khả năng phát hiện và ứng phó với các mối đe dọa an ninh mạng [47]. Tuy nhiên, việc thúc đẩy hợp tác đa bên trong ASEAN cũng sẽ gặp thách thức do sự khác biệt về pháp luật quốc gia, đặc biệt trong vấn đề bảo vệ dữ liệu, chia sẻ thông tin và cân bằng giữa an ninh mạng và quyền riêng tư và dữ liệu cá nhân.

5. Một số định hướng đối với Việt Nam về thúc đẩy hợp tác ASEAN trong phòng, chống tội phạm mạng

Những phân tích trên đã cho thấy Công ước Hà Nội vừa mở ra nhiều cơ hội, vừa đặt ra không ít thách thức đối với hợp tác ASEAN về phòng, chống tội phạm mạng. Trong bối cảnh đó, với tư cách là một thành viên tích cực của ASEAN và nước đăng cai ký kết Công ước, Việt Nam có nhiều điều kiện thuận lợi để chủ động thúc đẩy hợp tác khu vực trong lĩnh vực này. Từ đó, có thể đưa ra một số định hướng nhằm nâng cao vai trò của Việt Nam như sau:

5.1. Tiếp tục hoàn thiện pháp luật quốc gia

Trong thời gian qua, Việt Nam đã từng bước hoàn thiện

pháp luật về an ninh mạng và phòng, chống tội phạm công nghệ cao. Bộ luật Hình sự năm 2015 (sửa đổi, bổ sung năm 2017) quy định về việc xử lý các hành vi xâm phạm an toàn mạng máy tính, mạng viễn thông và phương tiện điện tử tại các điều 287 - 290 [48]. Bên cạnh đó, Luật An ninh mạng năm 2018 thiết lập các nguyên tắc bảo đảm an ninh mạng, đồng thời quy định trách nhiệm của các cơ quan nhà nước, tổ chức và doanh nghiệp trong việc phòng ngừa và xử lý vi phạm pháp luật trên không gian mạng [49].

Tuy nhiên, trước tính chất ngày càng phức tạp và xuyên biên giới của tội phạm mạng, cần phải tiếp tục rà soát và cập nhật khuôn khổ pháp luật hiện hành phù hợp với yêu cầu hợp tác quốc tế. Việc nội luật hóa cần được thực hiện theo hướng chọn lọc, đảm bảo tương thích với hệ thống pháp luật trong nước và cân bằng giữa yêu cầu điều tra với việc bảo vệ quyền con người. Trên cơ sở đó, Việt Nam có thể chủ động thúc đẩy quá trình phê chuẩn và thực thi Công ước trong ASEAN, đồng thời chia sẻ kinh nghiệm và tăng cường hợp tác với các quốc gia thành viên, qua đó góp phần thúc đẩy hài hòa hóa pháp luật khu vực [50].

5.2. Xây dựng các sáng kiến nâng cao năng lực thực thi

Việt Nam cần chủ động lồng ghép việc thực thi Công ước Hà Nội vào các cơ chế hợp tác hiện hành của ASEAN, đặc biệt trong khuôn khổ AMMTC và SOMTC, nhằm thúc đẩy trao đổi kinh nghiệm và điều chỉnh hợp tác khu vực phù hợp với các chuẩn mực mới [51]. Trên cơ sở đó, Việt Nam có thể đóng vai trò cầu nối trong việc tăng cường phối hợp liên ngành giữa các cơ quan thực thi pháp luật, cơ quan tư pháp và cơ quan quản lý an ninh mạng khu vực theo hướng tiếp cận đa ngành mà Công ước đã đặt ra [52].

Đồng thời, Việt Nam có thể nghiên cứu đề xuất một số sáng kiến như: thành lập nhóm công tác chuyên trách thuộc SOMTC về thực thi Công ước, cơ chế trao đổi thường niên về điều tra số; thiết lập các cơ chế chia sẻ thông tin và phối hợp điều tra (chẳng hạn như đầu mối liên lạc 24/7 hoặc cơ chế cảnh báo sớm), nhằm nâng cao hiệu quả xử lý tội phạm mạng xuyên biên giới và củng cố vai trò chủ động của Việt Nam trong hợp tác an ninh mạng khu vực [53].

Mặt khác, Việt Nam cần tích cực tham gia các chương trình đào tạo, diễn tập chung và chia sẻ kinh nghiệm về điều tra tội phạm mạng, thu thập và xử lý chứng cứ điện tử, cũng như ứng dụng công nghệ mới trong phòng, chống tội phạm mạng. Những hoạt động này sẽ góp phần thu hẹp khoảng cách năng lực giữa các quốc gia ASEAN [41]. Ngoài ra, việc chủ động tiếp nhận, điều phối và chia sẻ các nguồn hỗ trợ kỹ thuật từ các tổ chức quốc tế và các nước đối tác phát triển sẽ giúp nâng cao năng lực trong nước, đồng thời tạo nền tảng cho hợp tác khu vực bền vững và hiệu quả hơn.

5.3. Bảo đảm cân bằng giữa hợp tác khu vực và chủ quyền quốc gia

Việc duy trì sự cân bằng giữa hợp tác hiệu quả và tôn trọng chủ quyền là điều kiện tiên quyết để các nước ASEAN có thể phê chuẩn và thực thi Công ước Hà Nội, phù hợp với nguyên tắc đồng thuận và không can thiệp vào công việc nội bộ [53]. Vì vậy, hợp tác điều tra và chia sẻ dữ liệu cần được thực hiện trên cơ sở pháp lý chặt chẽ, minh bạch và xây dựng lòng tin giữa các quốc gia. Việt Nam có thể thúc đẩy cách tiếp cận linh hoạt, từng bước, ưu tiên các lĩnh vực có sự đồng thuận cao như chia sẻ thông tin về phương thức, thủ đoạn phạm tội hoặc đào tạo nâng cao năng lực, trước khi mở rộng sang các nội dung nhạy cảm hơn như truy cập dữ liệu xuyên biên giới theo thời gian thực.

Thông qua việc kết hợp hài hòa giữa chuẩn mực toàn cầu của Công ước Hà Nội và nguyên tắc vận hành đặc thù của ASEAN, Việt Nam có thể góp phần định hình mô hình hợp tác khu vực hiệu quả, tôn trọng sự đa dạng pháp lý và lợi ích quốc gia, từ đó nâng cao vai trò và hiệu quả đóng góp trong đảm bảo an ninh mạng và trật tự pháp lý khu vực.

6. Kết luận

Công ước Hà Nội đánh dấu một bước phát triển quan trọng trong việc thiết lập khuôn khổ pháp lý chung nhằm thúc đẩy hợp tác quốc tế trong điều tra, truy tố và xử lý các hành vi phạm tội trên không gian mạng. Đối với ASEAN, Công ước góp phần tăng cường hợp tác khu vực thông qua hài hòa hóa pháp luật, nâng cao hiệu quả hợp tác thực thi, xây dựng năng lực và thúc đẩy hợp tác đa bên trong quản trị an ninh mạng. Tuy nhiên, quá trình này sẽ vẫn chịu tác động đáng kể của sự chênh lệch về trình độ phát triển, năng lực kỹ thuật giữa các quốc gia thành viên và đặc thù của "Phương thức ASEAN".

Trong bối cảnh đó, Việt Nam cần chủ động phát huy vai trò tích cực trong việc triển khai và thúc đẩy hợp tác ASEAN phù hợp với các chuẩn mực của Công ước Hà Nội. Việc hoàn thiện pháp luật quốc gia, nâng cao năng lực thực thi và thúc đẩy các sáng kiến hợp tác khu vực sẽ góp phần nâng cao hiệu quả phòng, chống tội phạm mạng, đồng thời củng cố vai trò của Việt Nam trong các cơ chế hợp tác an ninh mạng của ASEAN và cộng đồng quốc tế.

TÀI LIỆU THAM KHẢO

[1] M. I. Abuja, "UNODC Warns of Cybercrime Threat to Nigeria", *Voice of Nigeria*, December 12, 2025. [Online]. Available: https://von.gov.ng/unodc-warns-of-cybercrime-threat-to-nigeria/ [Accessed January 20, 2026].

[2] M. N. Sari, "Cybercrime in Association of Southeast Asian Nations: Regional Effort and Its Effectiveness", *scholarlypublishingcollective.org*, September 19, 2024. [Online]. Available: https://scholarlypublishingcollective.org/psup/information-policy/article/doi/10.5325/jinfopoli.14.2024.0016/390841/Cybercrime-in-Association-of-Southeast-Asian [Accessed January 20, 2026].

[3] United Nations Office on Drugs and Crime, *United Nations Convention against Cybercrime*. Hanoi: Oct. 25-26, 2025.

[4] United Nations, *Basic facts about the global cybercrime treaty*. [Online]. Available: https://www.un.org/en/peace-and-security/basic-facts-about-global-cybercrime-treaty [Accessed January 20, 2026].

[5] Council of Europe, *Budapest Convention on Cybercrime*, ETS 185 Budapest, November 23, 2001. [Online]. Available: https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf [Accessed January 20, 2026].

[6] N. L. Chat and W. Golfred, "Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'". *Computer Law & Security Review*, vol. 40, 105521, 2021. https://doi.org/10.1016/j.clsr.2020.105521

[7] H. Makhija and A. Roy, "The Hanoi Convention and the Contest to Shape Global Cybercrime Norms", *ORF Middle East*, 25 November, 2025. [Online]. Available: https://orfme.org/research/the-hanoi-convention-and-the-contest-to-shape-global-cybercrime-norms/ [Accessed January 20, 2026].

[8] United Nations Office on Drugs and Crime, *Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime*, UNODC/CCPCJ/EG.4/2017/4, Vienna, April 24, 2017. [Online]. Available: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2017/Cybercrime_report_2017/Report_Cyber_E.pdf [Accessed January 20, 2026].

[9] United Nations General Assembly, *Resolution 74/247: Countering the use of information and communications technologies for criminal purposes,* December 27, 2019. [Online]. Available: https://undocs.org/A/RES/74/247 [Accessed December 20, 2025].

[10] United Nations Office on Drugs and Crime, *Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*, A/DEC/76/552, January 20, 2022. [Online]. Available: https://digitallibrary.un.org/record/3956024?ln=en&v=pdf [Accessed February 02, 2026].

[11] United Nations Office on Drugs and Crime, *United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes.* [Online]. Available: https://www.unodc.org/unodc/en/cybercrime/convention/home.html [Accessed February 02, 2026].

[12] A. Kazakova, "The UN process to negotiate the cybercrime convention: Key takeaways from the fifth session", *Diplo*, April 03, 2024. [Online]. Available: https://www.diplomacy.edu/blog/the-un-process-to-negotiate-the-cybercrime-convention-key-takeaways-from-the-fifth-session/ [Accessed January 21, 2026].

[13] Cybersecurity and Infrastructure Security Agency, *Partnerships and Collaboration.* [Online]. Available: https://www.cisa.gov/topics/partnerships-and-collaboration [Accessed February 02, 2026].

[14] A. Adeyeri and H. Abroshan, "Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era", *Information,* vol. 15, no. 11, 682, 2024. https://doi.org/10.3390/info15110682

[15] United Nations Office on Drugs and Crime, *Darknet Cybercrime Threats to Southeast Asia 2020*, 2021. [Online]. Available: https://www.unodc.org/roseap/uploads/archive/documents/Publications/2021/Darknet_Cybercrime_Threats_to_Southeast_Asia_report.pdf [Accessed February 28, 2026].

[16] Technode Global Staff, "UNODC Estimates Financial Losses between $18B and $37B from scams in East and Southeast Asia in 2023", *TnGlobal,* October 8, 2024. [Online]. Available: https://technode.global/2024/10/08/unodc-estimates-financial-losses-between-18b-and-37b-from-scams-in-east-and-southeast-asia-in-2023 [Accessed February 25, 2026].

[17] S. Rogers, "Cyber-Fraud, Underground Banking, and Technological Innovation Fuels Crime in SE Asia", *UNODC Report*, Dec 17, 2024. [Online]. Available: https://www.gasa.org/post/unodc-cyber-fraud-underground-banking-and-technological-innovation-fuels-crime-in-se-asia [Accessed February 23, 2026].

[18] M. Khomeriki, "UN report increase in Cybercrime and Illegal Gambling in Southeast Asia", *SBC Eurasia*, October 15, 2024. [Online]. Available: https://sbceurasia.com/en/2024/10/15/un-reports-increase-in-cybercrime-and-illegal-gambling-in-southeast-asia/ [Accessed February 22, 2026].

[19] M. B. Manantan, "Cyber Diplomacy Co-operation on Cybercrime between Southeast Asia and Commonwealth Countries: Realities, Responses and Recommendations", *Commonwealth Cybercrime Journal*, 2023. [Online]. Available: https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/s3fs-public/2023-03/D19156-CCJ-1-1-Cyber-Diplomacy-Cybercrime-SE-Asia-Commonwealth--Manantan.pdf [Accessed February 25, 2026].

[20] P. Thamrong-ajariyakun, "Is ASEAN Becoming a Breeding Ground for Cybercrime?", *Bangkok BIZ Newspaper,* vol. 38(12896), May 7, 2025. [Online]. Available: https://www.itd.or.th/en/itd-data-center/68_32/ [Accessed February 25, 2026].

[21] ASEAN Secretariat, *ASEAN Plan of Action to Combat Transnational Crime*, 1999. [Online]. Available: https://asean.org/wp-content/uploads/2012/05/ASEAN-Plan-of-Action-to-Combat-Transnational-Crime.pdf [Accessed February 25, 2026].

[22] ASEAN Secretariat, *Kuala Lumpur Declaration in Combating Cybercrime*, September 13, 2015. [Online]. Available: https://asean.org/wp-content/uploads/2021/01/KL-declaration-in-combating-tnC-1.pdf [Accessed February 25, 2026].

[23] ASEAN Secretariat, *ASEAN Plan of Action to Combat Transnational Crime (2016-2025)*, September 20, 2017. [Online]. Available: https://asean.org/wp-content/uploads/2012/05/ASEAN-Plan-of-Action-to-Combat-Transnational-Crime.pdf [Accessed February 21, 2026].

[24] ASEAN Secretariat, *ASEAN Declaration to Prevent and Combat Cybercrime*, November 13, 2017. [Online]. Available: https://asean.org/wp-content/uploads/2017/11/ASEAN-Declaration-to-Combat-Cybercrime.pdf [Accessed February 23, 2026].

[25] ASEAN Secretariat, *ASEAN Digital Masterplan 2025: Towards ASEAN's Digital Future,* 2021. [Online]. Available: https://asean.org/wp-content/uploads/2021/08/ASEAN-Digital-Masterplan-2025.pdf [Accessed February 28, 2026].

[26] ASEAN Secretariat, *ASEAN Cybersecurity Cooperation Strategy (2021-2025)*, 2022. [Online]. Available: https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf [Accessed February 28, 2026].

[27] ASEAN Secretariat, *ASEAN Ministerial Meeting on Transnational Crime-AMMTC.* [Online]. Available: https://asean.org/our-communities/asean-political-security-community/transnational-crime/ [Accessed February 28, 2026].

[28] ASEAN Secretariat, *ASEAN Senior Officials Meeting on Transnational Crime (SOMTC).* [Online]. Available: https://asean.org/senior-officials-meeting-on-transnational-crime-somtc/ [Accessed February 28, 2026].

[29] ASEAN Senior Officials Meeting on Transnational Crime, *ASEAN Working Group on Cybercrime*, 2014. [Online]. Available: https://asean.org/wp-content/uploads/2021/01/DOC-8-Adopted-TOR-ASEAN-Cybercrime-Working-Group.pdf [Accessed February 28, 2026].

[30] ASEANAPOL, "43rd ASEANAPOL Conference convenes in Bangkok, Thailand", *asean.org*, November 7, 2025. [Online]. Available: https://asean.org/43rd-aseanapol-conference-convenes-in-bangkok-thailand/ [Accessed February 28, 2026].

[31] Cyber Security Brunei, "Cyber Security Brunei participates in the ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC) meeting", *Press Release*, November 6, 2020. [Online]. Available at: https://www.csb.gov.bn/cyber-security-brunei-participates-asean-cybersecurity-coordinating-committee-asean-cyber-cc [Accessed February 01, 2026].

[32] N. G. Miralis, "INTERPOL's ASEAN Cybercrime Operations Desk: Addressing the rising threat of cybercrime in Southeast Asia", *Lexology*, May 19, 2023. [Online]. Available: https://www.lexology.com/library/detail.aspx?g=4a45c2f9-6e35-4de9-849b-4228fd174f96 [Accessed February 25, 2026].

[33] INTERPOL, "INTERPOL financial crime operation makes record 5,500 arrests, seizures worth over USD 400 million", *Interpol,* November 27, 2024. [Online]. Available: https://www.interpol.int/News-and-Events/News/2024/INTERPOL-financial-crime-operation-makes-record-5-500-arrests-seizures-worth-over-USD-400-million [Accessed February 28, 2026].

[34] VNA, "ASEANAPOL enhances crackdown on scam call centres", *VietnamPlus*, January 21, 2025. [Online]. Available: https://en.vietnamplus.vn/aseanapol-enhances-crackdown-on-scam-call-centres-post308678.vnp [Accessed February 28, 2026].

[35] Cybil, *ASEAN-Singapore Cybersecurity Centre of Excellence*, [Online]. Available: https://cybilportal.org/projects/asean-singapore-cybersecurity-centre-for-excellence-ascce/ [Accessed February 28, 2026].

[36] ASEAN-Japan Cybersecurity Capacity Building Centre, Calendar and Courses. [Online]. Available: https://ajccbc.ncsa.or.th/courses/ [Accessed February 28, 2026].

[37] Microsoft, "Working together to build a more diverse cybersecurity workforce", *Microsoft Vietnam Communication*, November 13, 2022. [Online]. Available: https://news.microsoft.com/vi-vn/2022/11/13/cung-chung-tay-xay-dung-mot-luc-luong-lao-dong-an-ninh-mang-da-dang-hon/ [Accessed February 28, 2026].

[38] T. Thi, "ASEAN discusses solutions to deal with high-tech crimes", *Lao Dong Newspaper*, August 20, 2025. [Online]. Available:

https://news.laodong.vn/xa-hoi/asean-ban-giai-phap-doi-pho-toi-pham-cong-nghe-cao-1560698.ldo [Accessed February 28, 2026].

[39] United Nations Treaty Collection, *United Nations Convention against Cybercrime; Strenthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communication Technology System and for the Sharing of Evidence in Electronic Form of Serious Crime*, Status As at 28-02-2026. [Online]. Available: https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-16&chapter=18&clang=_en [Accessed February 28, 2026].

[40] United Nations Office on Drugs and Crime, *Global Programme on Cybercrime - Training Catalogue,* 2024. [Online]. Available: https://www.unodc.org/documents/Cybercrime/Web_Global_Program_on_Cybercrime_Training_Catalog.pdf?v=4.3 [Accessed February 28, 2026].

[41] International Telecommunication Union, *Global Cybersecurity Index,* 5th edition, 2024. [Online]. Available: ttps://www.itu.int/epublications/publication/global-cybersecurity-index-2024 [Accessed December 10, 2025].

[42] N. T. Trung, "ASEAN Way", *International Studies*, March 12, 2016. [Online]. Available: https://nghiencuuquocte.org/2016/03/12/phuong-thuc-asean-asean-way/ [Accessed December 10, 2025].

[43] R. Broadhurst and Y. Chang, "Cybercrime in Asia: Trends and Challenges", in L. Jianhong, B. Hebonton and J. Susan (eds), *Handbook of Asian Criminology*. New York: Springer, 2013, pp. 49-63. https://doi.org/10.2139/ssrn.2118322

[44] INTERPOL, *Asia and South Pacific Cyberthreat Assessment Report*, 2024. [Online]. Available: https://www.interpol.int/content/download/22308/file/Asia%20and%20South%20Pacific%20Cyberthreat%20Assessment%20Report%202024-4.pdf [Accessed December 10, 2025].

[45] H. Y. Huang, "UN Cybercrime Convention: Relevance to ASEAN", *RSIS Commentary Series*, January 16, 2024. [Online]. Available: https://rsis.edu.sg/rsis-publication/rsis/un-cybercrime-convention-relevance-to-asean/ [Accessed January 21, 2026].

[46] INTERPOL, "C3DP: Fostering regional cooperation against cybercrime in Southeast Asia", *C3DP-Cyber Capacities & Capacity Development Project*. [Online]. Available: https://www.interpol.int/Crimes/Cybercrime/Projects/C3DP-Cyber-Capabilities-Capacity-Development-Project [Accessed January 28, 2026].

[47] World Economic Forum, "Global Cybersecurity Outlook 2026", *Insight Report*, January 2026. [Online]. Available: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf [Accessed February 20, 2026].

[48] National Assembly, *Criminal Code of Viet Nam*, No. 100/2015/QH13, 2015.

[49] National Assembly, *Law on Cybersecurity of Viet Nam*, No. 116/2025/QH15, 2018.

[50] B. Dieu, "Prospects for the Implementation of the Hanoi Convention in the Southeast Asia Region", *baophapluat.vn,* October 26, 2025. [Online]. Available: https://baophapluat.vn/trien-vong-thuc-thi-cong-uoc-ha-noi-tai-khu-vuc-dong-nam-a.html [Accessed December 10, 2025].

[51] C. Tuan and T. Trung, "ASEAN promotes cooperation in preventing and combating transnational crime", *bocongan.gov.vn*, September 10, 2025. [Online]. Available: https://bocongan.gov.vn/bai-viet/asean-thuc-day-hop-tac-phong-chong-toi-pham-xuyen-quoc-gia-1757497310 [Accessed January 20, 2026].

[52] Government of Viet Nam, "The Hanoi Convention: Establishing a global legal framework - a major turning point in multilateral cooperation on the prevention and combat of cybercrime", *chinhphu.vn*, November 22, 2025. [Online]. Available: https://xaydungchinhsach.chinhphu.vn/cong-uoc-ha-noi-thiet-lap-khuon-kho-phap-ly-toan-cau-buoc-ngoat-quan-trong-trong-hop-tac-da-phuong-ve-phong-chong-toi-pham-mang-119251122084808112.htm [Accessed January 21, 2026].

[53] Cyble, "United Against Cybercrime: ASEAN Ministers Forge New Security Pathways", *cyble.com*, January 27, 2025. [Online]. Available: https://cyble.com/blog/united-against-cybercrime-asean-ministers-forge-new-security-pathways/ [Accessed December 15, 2025].