CÔNG ƯỚC CỦA LIÊN HỢP QUỐC VỀ CHỐNG TỘI PHẠM MẠNG VÀ TÁC ĐỘNG ĐỐI VỚI VIỆT NAM

TRẦN THĂNG LONG(*)

Ngày nhận bài: 11/3/2025 Ngày thẩm định: 19/3/2025 Ngày duyệt đăng: 20/6/2025

Tóm tắt: *Bài viết nghiên cứu vai trò của Công ước Liên hợp quốc về chống tội phạm mạng năm 2024 như một khung pháp lý quốc tế toàn diện nhằm chống tội phạm mạng, đồng thời đánh giá tác động của Công ước đối với Việt Nam trong bối cảnh chuyển đổi số; làm rõ ý nghĩa của Công ước trong việc chuẩn hóa luật pháp, thúc đẩy hợp tác quốc tế và bảo vệ chủ quyền quốc gia trên không gian mạng; thảo luận những thách thức mà Việt Nam phải đối mặt khi triển khai, đồng thời đề xuất giải pháp để tận dụng tối đa lợi ích từ khung pháp lý này, hỗ trợ mục tiêu phát triển kinh tế số và an ninh mạng quốc gia.*

Từ khóa: *an ninh mạng; chống tội phạm mạng; chủ quyền quốc gia; chuyển đổi số; Công ước Liên hợp quốc*

1. Giới thiệu

Sự phát triển vượt bậc của công nghệ số đã mở ra một kỷ nguyên mới với những cơ hội chưa từng có cho tăng trưởng kinh tế, kết nối xã hội và đổi mới sáng tạo. Từ thương mại điện tử, dịch vụ công trực tuyến đến các nền tảng tài chính số, thế giới đang chứng kiến sự chuyển đổi sâu rộng trong cách con người tương tác và vận hành. Tuy nhiên, cùng với đó là sự gia tăng đáng lo ngại của tội phạm mạng - mối đe dọa không chỉ gây thiệt hại tài chính, mà còn đe dọa an ninh quốc gia và ổn định xã hội. Các hình thức tấn công của tội phạm mạng, như mã độc tống tiền, lừa đảo trực tuyến, đánh cắp dữ liệu hay khai thác trẻ em trên mạng, đã trở thành vấn đề toàn cầu, với thiệt hại ước tính lên tới 8 nghìn tỷ USD mỗi năm[1]. Đặc trưng xuyên biên giới của tội phạm mạng, kết hợp với sự khác biệt về pháp lý và kỹ thuật giữa các quốc gia đã tạo ra những lỗ hổng lớn mà tội phạm dễ dàng khai thác.

Nhận thức được tính cấp bách này, ngày 24/12/2024, Đại hội đồng Liên hợp quốc đã thông qua Công ước Liên hợp quốc về chống tội phạm mạng (sau đây gọi tắt là Công ước) - văn kiện pháp lý quốc tế đầu tiên tập trung toàn diện vào vấn đề này. Công ước không chỉ nhằm mục tiêu chuẩn hóa luật pháp, mà còn thúc đẩy hợp tác giữa các quốc gia, nâng cao năng lực kỹ thuật và bảo vệ quyền con người trong không gian mạng. Dự kiến, Công ước sẽ

(*) PGS, TS, Trường Đại học Luật Thành phố Hồ Chí Minh

được mở ký tại Hà Nội, Việt Nam vào năm 2025, đánh dấu một cột mốc quan trọng trong nỗ lực toàn cầu nhằm xây dựng một không gian mạng an toàn và bền vững[2].

Đối với Việt Nam, một quốc gia đang nỗ lực thúc đẩy chuyển đổi số để đạt mục tiêu kinh tế số chiếm 20% GDP vào năm 2025 theo Nghị quyết số 52-NQ/TW ngày 27/9/2019 của Bộ Chính trị "về một số chủ trương, chính sách chủ động tham gia cuộc Cách mạng công nghiệp lần thứ tư", Công ước mang ý nghĩa đặc biệt. Sự phát triển nhanh chóng của thương mại điện tử (đạt doanh thu 25 tỷ USD vào năm 2023[3], cùng với việc ứng dụng công nghệ rộng rãi trong các lĩnh vực, như y tế, giáo dục và dịch vụ công đang tạo ra động lực mạnh mẽ cho nền kinh tế. Đến năm 2025, Việt Nam sẽ có 100 triệu người sử dụng internet, trong đó, 23 triệu trẻ em tiếp cận internet[4]. An toàn thông tin mạng trở thành vấn đề cần được quan tâm hơn bao giờ hết. Tuy nhiên, các mối đe dọa mạng cũng gia tăng tương ứng. Đơn cử, năm 2023, Việt Nam hứng chịu hơn 13.000 cuộc tấn công mạng, tăng 10% so với năm trước[5]. Thiệt hại từ lừa đảo trực tuyến năm 2024 ước tính 18.900 tỷ đồng[6]. Những sự cố như vụ tấn công ransomware[7] hay các chiến dịch lừa đảo nhằm vào người dùng thương mại điện tử đã cho thấy những điểm yếu trong hệ thống an ninh mạng của Việt Nam.

Khung pháp lý hiện hành, chủ yếu dựa trên Luật An ninh mạng năm 2018, dù đã đặt nền móng cho việc quản lý không gian mạng, nhưng vẫn còn nhiều hạn chế. Đặc biệt, Luật này chưa có các quy định đầy đủ để xử lý tội phạm xuyên quốc gia, trong khi năng lực kỹ thuật của Việt Nam tuy có những tiến bộ vượt bậc nhưng vẫn chưa đủ để cạnh tranh với các quốc gia dẫn đầu khu vực, như Indonesia, Thái Lan, Singapore hay Hàn Quốc[8]. Trong bối cảnh đó, Công ước mang đến cơ hội chiến lược để Việt Nam khắc phục những điểm yếu này, đồng bộ hóa với tiêu chuẩn quốc tế và bảo vệ quá trình chuyển đổi số. Vai trò tích cực của Việt Nam trong quá trình đàm phán Công ước và việc đăng cai lễ ký kết tại Hà Nội là cơ hội để khẳng định vị thế trong quản trị an ninh mạng toàn cầu.

Bài viết đặt ra hai mục tiêu chính: (1) Phân tích ý nghĩa toàn cầu của Công ước trong việc thiết lập một khung pháp lý để chống tội phạm mạng; (2) Đánh giá tác động của Công ước đối với Việt Nam từ góc độ bảo vệ chủ quyền quốc gia trên không gian mạng và thảo luận các giải pháp, qua đó, Việt Nam tận dụng Công ước để bảo vệ chủ quyền quốc gia và thúc đẩy chuyển đổi số.

2. Công ước Liên hợp quốc về chống tội phạm mạng

Công ước Liên hợp quốc về chống tội phạm mạng được thông qua là một bước tiến mang tính lịch sử trong nỗ lực đối phó với tội phạm mạng - vấn đề đang gây ra thiệt hại kinh tế khổng lồ và đe dọa an ninh toàn cầu. Thiệt hại từ tội phạm mạng dự kiến sẽ tăng lên 10,5 nghìn tỷ USD vào năm 2025 nếu không có biện pháp hiệu quả[9]. Được khởi xướng từ Nghị quyết 74/247 năm 2019 do Nga và Trung Quốc đề xuất, Công ước là kết quả của hơn 05 năm đàm phán căng thẳng giữa các quốc gia thành viên Liên hợp quốc. Ngày 24/12/2024, Đại hội đồng đã thông qua Công ước với Nghị quyết 79/243, đánh dấu lần đầu tiên 193 quốc gia đạt được đồng thuận về một khung pháp lý quốc tế để xử lý vấn đề này. Công ước gồm 09 chương và 71 điều, cụ thể: Chương II - Hình sự hóa tội phạm mạng, Chương III - Thẩm quyền, Chương IV - Thủ tục điều tra và thu thập bằng chứng, Chương VI - Phòng ngừa, Chương VII - Chia sẻ thông tin và hỗ trợ kỹ thuật và Chương VIII - Cơ chế thực thi. Công ước sẽ có hiệu lực 90 ngày sau khi quốc gia thứ 40 phê chuẩn, mở ra kỷ nguyên mới trong quản trị an ninh mạng toàn cầu.

Các mục tiêu chính của Công ước bao gồm: (1) Tăng cường hiệu quả xử lý các

mối đe dọa mạng, như ransomware, lừa đảo trực tuyến, gian lận tiền điện tử và rửa tiền số; (2) Thiết lập các cơ chế chia sẻ bằng chứng điện tử và hỗ trợ pháp lý xuyên biên giới để truy tố tội phạm hiệu quả; (3) Hỗ trợ các quốc gia đang phát triển nâng cao năng lực kỹ thuật và pháp lý để đối phó với tội phạm mạng; (4) Bảo đảm cân bằng giữa an ninh mạng và bảo vệ quyền con người trong không gian số. So với Công ước Budapest năm 2001 - vốn chỉ thu hút 78 quốc gia thành viên, chủ yếu từ phương Tây, Công ước có phạm vi bao phủ rộng, tạo ra sự đồng thuận toàn cầu hiếm có từ trước đến nay. *Ý nghĩa quốc tế của Công ước thể hiện ở 04 nội dung* sau:

Thứ nhất, một trong những thách thức lớn nhất trong việc đối phó với tội phạm mạng là sự không đồng bộ giữa hệ thống pháp luật quốc gia. Chương II của Công ước yêu cầu các quốc gia thành viên hình sự hóa các hành vi phạm tội phổ biến, như truy cập trái phép hệ thống, phát tán mã độc, gian lận tiền điện tử và khai thác trẻ em trực tuyến. Sự chuẩn hóa này giúp khắc phục tình trạng tội phạm mạng thường lợi dụng để hoạt động xuyên biên giới mà không bị truy tố. Ví dụ, một vụ lừa đảo trực tuyến bắt nguồn từ Đông Âu nhằm vào các ngân hàng Mỹ có thể không bị truy tố nếu quốc gia nguồn không coi hành vi đó là bất hợp pháp. Công ước bảo đảm rằng các hành vi này được hình sự hóa đồng bộ, tạo ra một mặt trận pháp lý thống nhất trên toàn cầu. Điều này không chỉ tăng cường hiệu quả truy tố, mà còn gửi đi một thông điệp mạnh mẽ rằng không có nơi nào là "vùng miễn nhiễm" cho tội phạm mạng. Công ước đã tạo ra một bộ tiêu chuẩn pháp lý thống nhất, giảm thiểu các "thiên đường an toàn" cho tội phạm mạng.

Thứ hai, tính chất xuyên quốc gia của tội phạm mạng đòi hỏi sự phối hợp chặt chẽ giữa các quốc gia - điều mà các Công ước Budapest hay các hiệp định song phương chưa thể đáp ứng đầy đủ. Chương IV của Công ước thiết lập một mạng lưới thực thi pháp luật hoạt động 24/7, các giao thức chia sẻ bằng chứng điện tử và cơ chế dẫn độ, giúp các quốc gia phản ứng nhanh chóng và hiệu quả hơn trước các mối đe dọa. Vụ tấn công ransomware vào Colonial Pipeline và JBS tại Mỹ năm 2021 là một minh chứng rõ ràng về sự cần thiết của hợp tác quốc tế[10]. Cuộc tấn công này làm gián đoạn nguồn cung nhiên liệu cho toàn bộ bờ Đông nước Mỹ, nhưng các tội phạm từ nước ngoài rất khó bị truy tố do thiếu sự phối hợp pháp lý giữa các quốc gia. Công ước cung cấp các công cụ để giải quyết những vấn đề như vậy, từ việc chia sẻ thông tin tình báo, thời gian thực hiện đến hỗ trợ pháp lý lẫn nhau. Hơn nữa, hợp tác quốc tế không chỉ dừng lại ở việc truy tố, mà còn mở rộng sang lĩnh vực chia sẻ công nghệ và kinh nghiệm. Các quốc gia phát triển, như Mỹ, Nhật Bản hay Đức, có thể hỗ trợ các quốc gia đang phát triển như Việt Nam xây dựng năng lực an ninh mạng, tạo ra mạng lưới toàn cầu vững mạnh hơn để đối phó với tội phạm mạng.

Thứ ba, khác với nhiều khung pháp lý trước đây chỉ tập trung vào truy tố sau khi tội phạm xảy ra, Công ước đặt trọng tâm vào phòng ngừa thể hiện ở Chương VI (giáo dục cộng đồng, hợp tác với khu vực tư nhân) và Chương VII (hỗ trợ kỹ thuật cho các quốc gia đang phát triển). Với 67,4% dân số thế giới kết nối internet vào năm 2023[11], việc ngăn chặn mối đe dọa ngay từ đầu là yếu tố sống còn để giảm thiểu thiệt hại. Công ước khuyến khích các quốc gia hợp tác với các công ty công nghệ, như Google, Microsoft hay Kaspersky để phát triển các công cụ phòng ngừa tiên tiến, như phần mềm phát hiện mã độc hoặc hệ thống cảnh báo lừa đảo. Đối với các quốc gia đang phát triển, hỗ trợ kỹ thuật từ Công ước bao gồm đào tạo nhân lực, cung cấp thiết bị và chuyển

giao công nghệ góp phần thu hẹp khoảng cách với các quốc gia dẫn đầu, ngăn chặn nguy cơ trở thành "mắt xích yếu" trong chuỗi an ninh mạng toàn cầu.

Thứ tư, không gian mạng ngày nay được xem là "lãnh thổ thứ năm" của mỗi quốc gia[12], nơi các mối đe dọa không chỉ đến từ tội phạm tư nhân, mà còn từ các tác nhân nhà nước. Công ước củng cố chủ quyền quốc gia thông qua ba khía cạnh chính: (1) Công ước cho phép các quốc gia áp dụng luật nội địa để truy tố các hành vi tội phạm mạng bắt nguồn từ nước ngoài, mở rộng phạm vi tài phán thông qua cơ chế pháp lý chung. Điều này đặc biệt quan trọng với các quốc gia như Việt Nam, nơi tội phạm mạng đang có khuynh hướng gia tăng về quy mô và loại hình[13]; (2) Công ước cung cấp các công cụ kỹ thuật và thông tin để bảo vệ hạ tầng quan trọng, như ngân hàng, lưới điện hay hệ thống y tế trước các mối đe dọa xuyên biên giới. Vụ tấn công vào hệ thống Colonial Pipeline hay vụ ransomware nhằm vào bệnh viện ở Đức năm 2020 khiến một bệnh nhân thiệt mạng do không được cấp cứu kịp thời[14] cho thấy, mức độ nghiêm trọng của những mối đe dọa này; (3) Công ước tạo sự linh hoạt để các quốc gia điều chỉnh các tiêu chuẩn toàn cầu theo bối cảnh nội địa, tránh bị áp đặt bởi các cường quốc công nghệ, như Mỹ, Trung Quốc. Chẳng hạn, Ấn Độ có thể tích hợp các quy định của Công ước vào luật bảo vệ dữ liệu cá nhân, trong khi vẫn giữ quyền yêu cầu các công ty công nghệ nước ngoài lưu trữ dữ liệu trong nước. Sự linh hoạt này bảo đảm rằng các quốc gia vừa có thể hợp tác quốc tế, vừa duy trì quyền kiểm soát trên không gian mạng, yếu tố then chốt trong bối cảnh cạnh tranh địa chính trị ngày càng gay gắt. Đây là điểm đáng chú ý, phù hợp với quan điểm của Đảng và Nhà nước Việt Nam về bảo vệ chủ quyền quốc gia trên không gian mạng như một yêu cầu trong bối cảnh mới[15].

3. Tác động đối với Việt Nam: Bảo vệ chủ quyền và thúc đẩy chuyển đổi số

Thứ nhất, thực trạng an ninh mạng tại Việt Nam

Việt Nam đang bước vào giai đoạn chuyển đổi số mạnh mẽ. Sự phát triển của thương mại điện tử cùng với việc triển khai các dịch vụ công trực tuyến và ứng dụng công nghệ trong y tế, giáo dục đã tạo ra động lực cho nền kinh tế. Tuy nhiên, sự gia tăng của tội phạm mạng đang đe dọa nghiêm trọng đến quá trình này. Sự gia tăng các cuộc tấn công mạng, khá nhiều vụ trong số đó xuất phát từ nước ngoài[16], gây thiệt hại lớn, làm phức tạp hóa quá trình truy tố do thiếu cơ chế hợp tác quốc tế hiệu quả.

Những sự cố nghiêm trọng đã chỉ rõ những điểm yếu trong hệ thống an ninh mạng của Việt Nam. Chỉ trong 06 tháng đầu năm 2022, Kaspersky đã phát hiện và ngăn chặn 56.392 cuộc tấn công giả mạo nhằm vào ngân hàng[17]. Thiệt hại do lừa đảo trực tuyến ước tính 18.900 tỷ đồng năm 2024[18]. Các chiến dịch lừa đảo trực tuyến nhằm vào người dùng thương mại điện tử, đặc biệt trên các nền tảng, như Shopee, Lazada cũng ngày càng gia tăng với mức thiệt hại ước tính chiếm 05% doanh thu của ngành[19].

Khung pháp lý hiện hành của Việt Nam, chủ yếu dựa trên Luật An ninh mạng năm 2018, đã tạo ra một số nền tảng cơ bản để quản lý không gian mạng. Luật này yêu cầu các công ty công nghệ lưu trữ dữ liệu tại Việt Nam và cho phép chính phủ giám sát các hoạt động trực tuyến, nhằm bảo vệ an ninh quốc gia. Tuy nhiên, Luật vẫn bộc lộ nhiều hạn chế khi đối mặt với tội phạm xuyên quốc gia. Chẳng hạn, Luật An ninh mạng năm 2018 không có quy định cụ thể về dẫn độ hay chia sẻ bằng chứng điện tử với các quốc gia khác, dẫn đến việc chỉ có 25% vụ án xuyên biên giới được giải quyết[20]. Sự hạn chế về nhân lực an ninh mạng cũng là một vấn đề lớn. Việt Nam

hiện đang thiếu hụt nhân sự chất lượng cao phục vụ cho 100 triệu dân[21].

Thứ hai, lợi ích từ Công ước đối với Việt Nam

- Công ước mang lại cho Việt Nam các công cụ để truy tố tội phạm mạng xuyên quốc gia - một điểm yếu mà Luật An ninh mạng năm 2018 còn hạn chế. Với mạng lưới thực thi pháp luật hoạt động 24/7 và các giao thức dẫn độ, Việt Nam có thể xử lý hiệu quả các vụ tấn công từ nước ngoài, ví dụ, các mạng lưới lừa đảo từ Campuchia hay ransomware từ Đông Âu vốn khó truy tố do thiếu cơ chế hợp tác thì giờ đây có thể bị đưa ra ánh sáng nhờ các quy định của Công ước. Điều này không chỉ tăng cường khả năng tự vệ pháp lý, mà còn giúp Việt Nam khẳng định quyền tài phán trong không gian mạng, giảm sự phụ thuộc vào các khung pháp lý khu vực như trường hợp các quốc gia thành viên Công ước Budapest ở châu Âu.

- Luật An ninh mạng năm 2018 đã xác định dữ liệu là tài sản quốc gia cần được bảo vệ. Công ước hỗ trợ mục tiêu này thông qua các biện pháp phòng ngừa (Chương VI) và hỗ trợ kỹ thuật (Chương VII), giúp Việt Nam xây dựng năng lực bảo vệ các hệ thống trọng yếu, như ngân hàng, năng lượng hay y tế trước các cuộc tấn công từ bên ngoài. Hỗ trợ kỹ thuật từ Văn phòng Liên hợp quốc về ma tuý và tội phạm (UNODC), đào tạo nhân lực và chuyển giao công nghệ, giúp Việt Nam giảm phụ thuộc vào các giải pháp công nghệ nước ngoài - yếu tố quan trọng để duy trì tự chủ kỹ thuật và chủ quyền số. Các cuộc tấn công mạng có thể được ngăn chặn hoặc giảm thiểu thiệt hại nếu Việt Nam có hệ thống cảnh báo sớm tiên tiến hơn, điều mà Công ước có thể hỗ trợ thông qua các chương trình hợp tác với các quốc gia, như Mỹ, Nhật Bản. Việc bảo vệ hạ tầng không chỉ bảo đảm an ninh quốc gia, mà còn duy trì sự ổn định kinh tế trong bối cảnh chuyển đổi số.

- Chuyển đổi số đòi hỏi một không gian mạng an toàn để triển khai các dịch vụ công trực tuyến, thương mại điện tử và tài chính số. Sự phát triển của hạ tầng công nghệ số, sự an toàn của các nền tảng vận hành trên đó là những tiền đề thiết yếu cho sự vận hành của thương mại điện tử. Bởi lẽ, thương mại điện tử gắn liền với người dùng internet và thiết bị điện tử. Sự an toàn của người dùng là cơ sở để thương mại điện tử tồn tại và phát triển. Công ước mang lại các công cụ chiến lược để Việt Nam đạt được điều này. Hỗ trợ kỹ thuật (Chương VII) có thể giúp Việt Nam mở rộng đội ngũ chuyên gia an ninh mạng và triển khai các công nghệ giám sát tiên tiến, như trí tuệ nhân tạo (AI). Các chương trình đào tạo của Văn phòng Liên hợp quốc về ma túy và tội phạm (UNODC), hỗ trợ cho các quốc gia châu Phi giai đoạn 2020 - 2023 chống lại các hành vi tội phạm mạng, là minh chứng cho tiềm năng của cách tiếp cận này. Không gian mạng an toàn cũng tăng niềm tin của người dân và doanh nghiệp vào các nền tảng số. Đối với Việt Nam, việc bảo vệ dữ liệu cá nhân sẽ giúp các nền tảng thương mại điện tử, như Zalo hay Tiki tăng cường sự tin cậy, từ đó thúc đẩy sự tham gia của người dùng - yếu tố quan trọng để đạt mục tiêu "nuôi dưỡng doanh nghiệp công nghệ số"[22]. Ví dụ, nếu các vụ lừa đảo trên Shopee hay Lazada được giảm thiểu nhờ các biện pháp phòng ngừa của Công ước, người dùng sẽ yên tâm hơn khi tham gia mua sắm trực tuyến, từ đó thúc đẩy doanh thu thương mại điện tử.

- Công ước giảm thiểu rủi ro từ tội phạm mạng, bảo vệ các lĩnh vực trọng yếu, như thương mại điện tử, tài chính số và dịch vụ công trực tuyến, từ đó củng cố niềm tin của nhà đầu tư và người dùng. Tuy nhiên, thiệt hại 500 triệu USD từ lừa đảo trực tuyến và các vụ gian lận nhằm vào doanh nghiệp nhỏ, chiếm 40% báo cáo sự cố mạng theo VCCI (năm 2023) đang đe dọa sự ổn định của lĩnh vực này. Công ước giúp giảm rủi

ro thông qua các biện pháp phòng ngừa (Chương VII) và truy tố hiệu quả (Chương III). Ví dụ, bảo vệ các nền tảng thương mại điện tử hàng đầu, như Shopee khỏi gian lận có thể tiết kiệm hàng trăm triệu USD mỗi năm, tăng niềm tin của nhà đầu tư. Một không gian mạng an toàn cũng thu hút FDI, dự kiến 20 tỷ USD vào năm 2025[23], hỗ trợ mục tiêu 20% GDP từ kinh tế số. Với 70 triệu người dùng internet tại Việt Nam, sự tham gia tích cực vào các dịch vụ số sẽ tạo động lực cho tăng trưởng kinh tế dài hạn.

- Việc đăng cai lễ ký kết Công ước tại Hà Nội vào năm 2025 không chỉ là một sự kiện ngoại giao, mà còn là cơ hội để Việt Nam định hình các chuẩn mực quốc tế theo hướng có lợi cho mình. Tham gia tích cực vào quá trình đàm phán, Việt Nam có thể thúc đẩy các điều khoản bảo vệ quyền tự quyết trong không gian mạng, đặc biệt cho các quốc gia đang phát triển, tránh bị áp đặt bởi các cường quốc công nghệ. Bằng cách tận dụng Công ước, Việt Nam có thể tiếp cận tài trợ từ Văn phòng Liên hợp quốc về ma tuý và tội phạm để xây dựng một trung tâm đào tạo an ninh mạng tại Hà Nội, với mục tiêu đào tạo 2.000 chuyên gia mỗi năm đến năm 2027. Điều này không chỉ tăng cường nội lực, mà còn biến Việt Nam thành một "điểm đến số" trong khu vực Đông Nam Á, điểm nóng của tội phạm mạng. Điều này tạo điều kiện thu hút đầu tư công nghệ, hợp tác quốc tế và dẫn dắt các sáng kiến số khu vực, củng cố nền tảng cho chiến lược chuyển đổi số quốc gia.

- Đối phó với các cuộc tấn công mạng đến từ nước ngoài, hợp tác quốc tế là yếu tố sống còn để Việt Nam bảo vệ không gian mạng. Chương III của Công ước thiết lập mạng lưới thực thi pháp luật 24/7, cơ chế chia sẻ bằng chứng điện tử và giao thức dẫn độ, giúp Việt Nam giải quyết các mối đe dọa xuyên biên giới hiệu quả hơn. Ví dụ, Việt Nam có thể hợp tác với Mỹ hoặc Singapore trong khuôn khổ ASEAN Cyber Shield 2023 để truy vết và truy tố tội phạm mạng nhanh chóng, tăng tỷ lệ giải quyết vụ án xuyên biên giới. Hợp tác quốc tế không chỉ giảm thiểu rủi ro, mà còn tạo điều kiện thuận lợi cho hội nhập kinh tế số toàn cầu. Chẳng hạn, sự phối hợp với các quốc gia ASEAN, như Malaysia, Thái Lan có thể giúp Việt Nam xây dựng một "lá chắn mạng" khu vực, bảo vệ các dịch vụ xuyên biên giới, như thương mại điện tử và thanh toán số.

Thứ ba, những thách thức đối với Việt Nam trong việc thực thi Công ước

- *Về nguồn lực:* Việt Nam sẽ đối mặt với thách thức về tài chính và nhân sự để đáp ứng các yêu cầu kỹ thuật của Công ước. Ngân sách an ninh mạng cần được tăng cường do nhu cầu triển khai các hệ thống công nghệ cao để giám sát mạng đòi hỏi các khoản đầu tư lớn. Công ước yêu cầu các quốc gia nâng cấp hạ tầng để chia sẻ bằng chứng điện tử và phản ứng nhanh, nhưng với nguồn lực hiện tại, Việt Nam khó có thể đáp ứng. Sự thiếu hụt nhân lực là một rào cản lớn. Nếu không tăng đầu tư, Việt Nam có thể không tận dụng được hỗ trợ từ Công ước, làm chậm quá trình chuyển đổi số và tiềm ẩn nguy cơ phụ thuộc vào công nghệ nước ngoài.

- *Quan ngại đối với vấn đề quyền riêng tư*: Các quy định giám sát trong Chương IV của Công ước có thể dẫn đến quan ngại về quyền riêng tư tại Việt Nam, vốn dĩ đã là vấn đề nhạy cảm vào thời điểm ban hành Luật An ninh mạng năm 2018. Việc Công ước yêu cầu thu thập và chia sẻ bằng chứng điện tử có thể dẫn đến việc tăng cường các biện pháp và cơ chế giám sát dữ liệu người dùng. Thậm chí, việc áp dụng Chương IV có thể làm gia tăng lo ngại về nguy cơ lạm dụng, thiếu kiểm soát vượt quá mục tiêu chống tội phạm mạng. Với 70 triệu người dùng internet và 100 triệu người trong tương lai, bất kỳ hành vi xâm phạm quyền riêng tư mà không được xử

lý thích đáng đều có thể gây mất niềm tin vào các nền tảng số, từ dịch vụ công trực tuyến đến thương mại điện tử. Các hiệp định tự do thương mại EVFTA yêu cầu tuân thủ tiêu chuẩn dữ liệu cao, thậm chí, các đối tác thương mại có thể áp đặt hạn chế thương mại hoặc công nghệ nếu vấn đề bảo vệ dữ liệu người dùng không được giải quyết minh bạch.

- *Pháp lý và thể chế chưa hoàn thiện, đồng bộ:* Khung pháp lý hiện tại của Việt Nam chưa đồng bộ với Công ước, trong khi sự phân mảnh thể chế làm chậm khả năng triển khai. Luật An ninh mạng năm 2018 thiếu quy định về dẫn độ và chia sẻ bằng chứng điện tử (hai yêu cầu quan trọng của Chương III) dẫn đến khó khăn trong hợp tác đấu tranh đối với loại tội phạm xuyên biên giới. Sự phối hợp giữa Bộ Khoa học và Công nghệ với Bộ Công an còn thiếu hiệu quả, với thời gian phản ứng trung bình 72 giờ cho các sự cố lớn[24]. Công ước đòi hỏi các cơ quan chức năng cần phối hợp phản ứng nhanh hơn, nhưng cơ cấu quản lý hiện tại không đủ linh hoạt để đáp ứng. Nếu không cải cách pháp lý kịp thời, Việt Nam có thể không tận dụng được cơ chế hợp tác quốc tế, làm giảm hiệu quả truy tố các mối đe dọa xuyên biên giới như lừa đảo từ Campuchia hay ransomware từ Đông Âu. Điều này không chỉ ảnh hưởng đến an ninh mạng, mà còn đe dọa khả năng tự chủ trong không gian số.

4. Khuyến nghị

Thứ nhất, cần xem xét thành lập Quỹ An ninh mạng quốc gia với cơ chế đóng góp hỗn hợp từ ngân sách nhà nước, doanh nghiệp công nghệ và đối tác quốc tế. Khuyến khích mô hình đầu tư theo giai đoạn, ưu tiên hệ thống hạ tầng mạng theo yêu cầu kỹ thuật của Công ước, thúc đẩy hợp tác công - tư trong phát triển hạ tầng, cho phép doanh nghiệp công nghệ trong nước cùng phát triển giải pháp, vừa tiết kiệm chi phí vừa tăng cường năng lực nội địa. Việt Nam cần đầu tư tăng ngân sách cho an ninh mạng. Nguồn kinh phí này sẽ sử dụng vào việc đào tạo các chuyên gia mới về an ninh mạng, xây dựng một trung tâm an ninh mạng có chức năng điều phối và phối hợp hoạt động. Đồng thời, Việt Nam có thể yêu cầu hỗ trợ từ các cơ quan chuyên trách của Liên hợp quốc để thiết lập hạ tầng ban đầu, như hệ thống AI giám sát mạng và mạng lưới thực thi pháp luật 24/7. Điều này sẽ tăng gấp đôi lực lượng chuyên gia, giảm phụ thuộc vào công nghệ nước ngoài và bảo đảm đáp ứng các tiêu chuẩn kỹ thuật của Công ước.

Thứ hai, cần có cơ chế minh bạch bảo đảm sự hài hòa giữa bảo đảm an ninh mạng và tôn trọng quyền riêng tư. Chính phủ cần xúc tiến xây dựng khung quản trị dữ liệu quốc gia minh bạch, quy định cụ thể về cân bằng giữa an ninh và quyền riêng tư, đặt giới hạn rõ ràng về phạm vi thu thập dữ liệu và thời lượng lưu trữ. Việt Nam cần ban hành quy định thực thi Chương IV của Công ước, thành lập hội đồng giám sát độc lập bao gồm đại diện từ Chính phủ (Bộ Khoa học và Công nghệ, Bộ Công an); chuyên gia độc lập. Hội đồng này sẽ kiểm tra các hoạt động giám sát, công bố báo cáo tuân thủ hằng năm và thiết lập đường dây nóng để người dân khiếu nại. Các biện pháp này sẽ tăng tính minh bạch, duy trì niềm tin công chúng và tránh xung đột với các đối tác quốc tế.

Thứ ba, khắc phục sự chưa đồng bộ về luật pháp và cơ chế. Việt Nam cần sửa đổi, bổ sung Luật An ninh mạng năm 2018 và các văn bản hướng dẫn thi hành để tích hợp các giao thức trong Chương IV của Công ước, như dẫn độ tội phạm mạng (quy định "dẫn độ trong 30 ngày nếu có bằng chứng xác thực") và chia sẻ bằng chứng điện tử. Đặt Bộ Khoa học và Công nghệ làm đầu mối điều phối, hợp nhất vai trò với Bộ Công an, thành lập một đơn vị chuyên trách để giảm thời gian phản ứng từ 72 giờ

xuống 24 giờ. Điều này sẽ tăng hiệu quả truy tố các mối đe dọa xuyên biên giới, bảo vệ hạ tầng số và củng cố chủ quyền quốc gia trong không gian mạng. Việc tham gia Công ước đòi hỏi sự cập nhật và điều chỉnh nhằm bảo đảm tương thích giữa các đạo luật khác với nhau, như Luật Tố tụng hình sự, Luật Dẫn độ, chứng cứ và điều tra hình sự bảo đảm tuân thủ các cam kết của Việt Nam trong các hiệp định tương trợ tư pháp về hình sự với các nước khác.

5. Kết luận

Công ước Liên hợp quốc về chống tội phạm mạng là khung pháp lý toàn cầu mang tính biến đổi, đối phó với mối đe dọa từ tội phạm mạng toàn cầu. Với Việt Nam, Công ước không chỉ là công cụ để bảo vệ kinh tế số và chủ quyền quốc gia, mà còn là cơ hội để nâng cao vị thế trong quản trị toàn cầu. Tuy nhiên, để tận dụng tối đa lợi ích, Việt Nam cần đầu tư mạnh mẽ vào nguồn lực, cải cách pháp lý và bảo đảm minh bạch trong triển khai. Chỉ khi vượt qua những thách thức này, Việt Nam mới có thể biến Công ước thành đòn bẩy cho sự phát triển bền vững trong thời đại số, đồng thời khẳng định vai trò trên trường quốc tế ❑

(1) và (9) Cybersecurity Ventures, 'Cybercrime Damage Costs to Hit $10.5 Trillion Annually by 2025' (2023), https://byvn.net/AZ9s

(2) và (11) Sam Lê, *Công ước Liên hợp quốc về chống tội phạm mạng*, https://nhandan.vn, ngày 04/01/2025

(3) Hữu Tuấn, *Thương mại điện tử đạt doanh thu 25 tỷ USD*, https://baodautu.vn, ngày 29/12/2024

(4) Hữu Tuấn, *Thị trường an ninh mạng 500 triệu USD: Miếng bánh trong tầm tay*, https://baodautu.vn, ngày 20/12/2022

(5) Minh Huyền, *An toàn thông tin mạng tại Việt Nam vì nền kinh tế số bền vững và phát triển*, https://consosukien, ngày 25/02/2025

(6) Khắc Lãm, Tiểu Vy, *Lừa đảo trực tuyến: Mối đe dọa ngày càng tinh vi trong thời đại số*, https://congan.com, ngày 14/01/2025

(7) Minh Hà, *Việt Nam xếp thứ 3 Đông Nam Á với hơn 57.000 cuộc tấn công ransomware trong năm 2022*, https://vneconomy.vn, ngày 14/3/2023

(8) T.H., *Việt Nam được xếp vào nhóm 1 các quốc gia an toàn thông tin mạng*, https://consosukien.vn, ngày 16/9/2024

(10) Đăng Thứ, *Câu chuyện của năm 2021: Ransomware*, https://antoanthongtin.gov.vn, ngày 27/01/2022

(12) và (15) Đại tướng, GS, TS. Tô Lâm, *Chủ quyền không gian mạng: Yêu cầu thời đại và nghĩa vụ quốc gia*, Nxb Công an nhân dân, Hà Nội, 2021, tr.184 và 184-185

(13) NCS Group, *Tổng kết An ninh mạng Việt Nam năm 2023 và dự báo 2024*, https://ncsgroup.vn, ngày 20/02/2024

(14) Báo Thanh niên, *Một phụ nữ ở Đức tử vong do bệnh viện bị tấn công ransomware*, https://thanhnien.vn, ngày 19/9/2020

(16) VietnamNet, *Số vụ tấn công mạng nhắm tới Việt Nam nhiều thứ 3 Đông Nam Á*, https://vietnamnet.vn, ngày 20/02/2024

(17) An An, *Nửa đầu năm 2022: Hàng chục ngàn vụ tấn công giả mạo ngân hàng tại Việt Nam*, *Tạp chí Tự động hóa ngày nay,* https://tudonghoangaynay.vn, ngày 30/10/2022

(18) HM, *Thiệt hại do lừa đảo trực tuyến ước tính 18.900 tỷ đồng năm 2024*, https://baochinhphu.vn, ngày 16/12/2024

(19) VECOM, *Báo cáo Thương mại Điện tử Việt Nam 2023*, https://www.vecom.vn, ngày 18/4/2023

(20) Bộ Thông tin và Truyền thông, *Báo cáo Tình hình An ninh mạng Việt Nam 2023*, https://mic.gov.vn, ngày 26/9/2020

(21) Bộ Nội vụ, *Đánh giá thực trạng chế độ hỗ trợ đối với cán bộ, công chức, viên chức và người làm công tác chuyên trách về chuyển đổi số, an toàn, an ninh mạng*, https://shorturl.at/lqo2A, ngày 26/01/2025

(22) Bộ Thông tin và Truyền thông, *Tờ trình Dự thảo Luật Công nghiệp công nghệ số năm 2024*, mục I.2.4

(23) Nguyễn Mại, *Triển vọng thu hút FDI năm 2025: Cơ hội và thách thức*, Tạp chí Kinh tế và Dự báo, https://kinhtevadubao.vn, ngày 26/01/2025

(24) MIC, *Báo cáo Tình hình An ninh Mạng Việt Nam 2023*, https://mic.gov.vn, ngày 26/9/2020