Bảo đảm an ninh mạng ở các nước Đông Nam Á

PGS.TS. PHẠM THỊ THANH BÌNH[1]
VŨ HOÀNG DŨNG[2]
[1] Trường Đại học Mở Hà Nội
[2] Viện Kinh tế và chính trị thế giới

● NGÀY NHẬN BÀI: 01/7/2023 ● NGÀY PHẢN BIỆN: 20/7/2023
● NGÀY DUYỆT ĐĂNG: 30 /8/2023

Tóm tắt: Đe dọa an ninh mạng là một trong những vấn đề an ninh toàn cầu hiện nay. Kinh tế số ASEAN phát triển nhanh, đóng góp lớn vào GDP khu vực nhưng kinh tế số cũng gây ra nhiều thách thức cho khu vực, mang đến nguy cơ mối đe doạ an ninh mạng. Bài viết tìm hiểu thực trạng vấn đề bảo đảm an ninh mạng ở Đông Nam Á (ASEAN) và phân tích nguyên nhân yếu kém của bảo đảm an ninh mạng Đông Nam Á và từ đó đề xuất giải pháp cho vấn đề đảm bảo an ninh mạng khu vực.

Từ khóa: *An ninh mạng, thực trạng, nguyên nhân, giải pháp, ASEAN.*

1. GIỚI THIỆU

Đông Nam Á (ASEAN) được coi là một trong những nền kinh tế số lớn nhất thế giới. Kinh tế số ASEAN có giá trị ước tính tạo ra 150 tỷ USD hàng năm và có tiềm năng đóng góp thêm 1 nghìn tỷ USD vào GDP khu vực (2025). Tuy nhiên, kinh tế số Đông Nam Á cũng đem đến nhiều nguy cơ về các mối đe dọa mạng. Rủi ro mạng có thể cản trở khả năng phục hồi kinh tế và cản trở Đông Nam Á đạt được tiềm năng kỹ thuật số tối đa. Hiện ASEAN là mục tiêu chính của các cuộc tấn công mạng và nằm trong số các quốc gia bị đe dọa phần mềm độc hại cao ở khu vực Châu Á - Thái Bình Dương.

2. THỰC TRẠNG VẤN ĐỀ AN NINH MẠNG Ở ASEAN

Khái niệm "An ninh mạng" lần đầu tiên xuất hiện bởi mạng toàn cầu (WWW - World Wide Web) năm 1989. "An ninh mạng là hoạt động bảo vệ máy tính, máy chủ, thiết bị di động, hệ thống điện tử và dữ liệu khỏi các cuộc tấn công nguy hiểm". Quá trình chuyển đổi số, kinh tế số đã góp phần giải quyết các khó khăn do dịch bệnh Covid-19 gây ra. Tuy nhiên, xu hướng phát triển kinh tế số cũng làm gia tăng thách thức về an ninh mạng đối với các nước ASEAN, trong đó nổi bật là hành vi tấn công mạng có chủ đích vào các cơ sở hạ tầng thông tin trọng yếu; giả mạo các trang, cổng thông tin điện

tử của cơ quan nhà nước, lực lượng Công an, tổ chức, doanh nghiệp để đánh cắp dữ liệu cá nhân, lừa đảo chiếm đoạt tài sản; tạo lập các sàn giao dịch, ứng dụng, website lừa đảo chiếm đoạt tài sản, mua bán, phát tán thông tin, dữ liệu cá nhân trái phép trên không gian mạng.

Đe dọa an ninh mạng mà thế giới và ASEAN đang phải đối diện chủ yếu được phân ra thành ba dạng sau:

Thứ nhất, tội phạm mạng được đặc trưng bởi các cá nhân hoặc nhóm phá hoại hệ thống mạng vì mục tiêu tài chính.

Thứ hai, tấn công mạng được xác định khi hành động nhằm mục tiêu chính trị và thường liên quan đến việc khai thác thông tin bất hợp pháp.

Thứ ba, chủ nghĩa khủng bố mạng phá hoại hệ thống điện tử với mục đích gây hoảng sợ hoặc sự hoang mang cho công chúng.

Do phụ thuộc ngày càng tăng của Đông Nam Á vào mạng Internet cùng với những tiến bộ công nghệ trong khu vực khiến cho vấn đề an ninh mạng vốn đã không ổn định trong khu vực càng trở nên trầm trọng hơn. Singapore là quốc gia an toàn nhất trong khu vực ASEAN nhưng cũng được coi là quốc gia dễ bị tấn công mạng nhiều nhất do quá phụ thuộc vào công nghệ. Là quốc gia có nền kinh tế phát triển nhất và có mức độ kết nối Internet cao, Singapore đặc biệt dễ bị ảnh hưởng bởi khủng bố mạng. Đối tượng của các cuộc tấn công mạng bao gồm các cá nhân, doanh nghiệp vừa và nhỏ, cơ sở hạ tầng thông tin quan trọng CII (Critical Information Infrastructure) như: chăm sóc sức khỏe và các lĩnh vực ngân hàng - tài chính. Trong năm 2017, Singapore đã ba lần trở thành mục tiêu chính của các cuộc tấn công mạng, đó là: Vụ vi phạm mạng của Bộ Quốc phòng (MINDEF Cyber Breach) vào tháng 2; Cuộc tấn công bằng mã độc (WannaCry Ransomware) vào tháng 5; Hoạt động của Petya Ransomware vào tháng 6. Cuộc tấn công WannaCry Ransomware không chỉ giới hạn ở Singapore mà còn ảnh hưởng đến phần còn lại của khu vực Đông Nam Á và tấn công Indonesia, Việt Nam, Thái Lan, Malaysia và Philippines. Singapore có mức thiệt hại bình quân đầu người cao nhất do tội phạm mạng với trung bình 1.158 đô la Singapore. Năm 2016, Việt Nam cũng bị tấn công mạng do nhóm hacker tấn công cướp màn hình thông tin và hệ thống âm thanh tại các sân bay và máy bay lớn nhất của Việt Nam. Trong giai đoạn (2018- 2019), Việt Nam ghi nhận 4.035 cuộc tấn công mạng, gây thiệt hại khoảng 12,3 nghìn tỷ đồng. Malaysia cũng bị thiệt hại khoảng 900 triệu USD giai đoạn 2007-2012 do tội phạm mạng, với trung bình 30 người là nạn nhân của tội phạm mạng mỗi ngày. Indonesia bị thiệt hại khoảng 2,7 tỷ USD do vấn đề an ninh mạng.

Đe dọa không gian mạng trong ASEAN cũng nảy sinh từ hành vi vi phạm bản quyền. Phần mềm vi phạm bản quyền thường dễ bị tấn công bởi phần mềm độc hại. Campuchia có tỷ lệ vi phạm bản quyền hơn 95%, tiếp theo là Việt Nam và Indonesia với tỷ lệ vi phạm bản quyền hơn 80%. Người tiêu dùng trong ASEAN sẽ phải chi 10,8 triệu USD để giải quyết vấn đề phần mềm độc hại do các chương trình vi phạm bản quyền. Rõ ràng, mối đe dọa mạng xuyên biên giới khiến an ninh quốc

gia và khu vực càng trở nên nguy hiểm hơn.

Không chỉ có nguy cơ bị tấn công mạng, Đông Nam Á còn là khu vực thường xuyên bị đe dọa lừa đảo tấn công giả mạo (Phishing threats). Tấn công giả mạo Phishing threats là loại tội phạm mạng khiến nạn nhân để bị mắc vào bẫy của thủ phạm thông qua cung cấp liên kết. Thủ phạm có thể sử dụng liên kết đó để lấy thông tin quan trọng từ nạn nhân. Năm 2019, Đông Nam Á có 14 triệu vụ tấn công lừa đảo phishing threats. Trong đó, Philippines, Indonesia, Malaysia và Việt Nam là những quốc gia có hoạt động kinh doanh lừa đảo Phishing threats lớn nhất.

Do trình độ kém phát triển hơn so với một số quốc gia thành viên khác của ASEAN, Myanmar rất dễ bị tấn công mạng. Chủ nghĩa tin tặc hacktivism cũng là một mối đe dọa mạng lan tràn ở Myanmar. Tin tặc sử dụng các kênh truyền thông xã hội như Facebook và các diễn đàn riêng khác để điều phối các cuộc tấn công. Hậu quả của những cuộc tấn công nhằm vào các thiết bị Internet of Things (IoT) đe dọa khiến Đông Nam Á mất tới 750 tỷ USD vốn hóa thị trường do các mối đe dọa rình rập.

Khu vực ASEAN có rất ít hình thức giáo dục về an ninh mạng. Thậm chí, số lượng các công trình nghiên cứu được công bố giữa các quốc gia thành viên ASEAN có rất ít công trình được thực hiện về chủ đề an ninh mạng. Trong giai đoạn (2014-2019), không có nghiên cứu nào được công bố về an ninh mạng ở Lào và Campuchia, tỷ lệ là 0%, trong khi Malaysia (9,33%), Myanmar (5,19%) và Singapore (5,18%). Điều này phản ánh sự thiếu hiểu biết và quan tâm đầy đủ đến các mối đe dọa mạng hiện có ở nhiều quốc gia Đông Nam Á và thiếu nỗ lực bảo vệ không gian mạng.

3. NGUYÊN NHÂN BẢO ĐẢM AN NINH MẠNG KÉM CỦA ASEAN.

Bảo đảm an ninh mạng ở Đông Nam Á yếu kém là do những nguyên nhân cơ bản sau:

Thứ nhất, do ASEAN chưa thực sự coi trọng việc bảo đảm an ninh mạng**.** Rủi ro lớn mà Đông Nam Á phải đối diện do chưa coi trọng việc bảo đảm an ninh mạng. Sự phát triển của CNTT ở các nước Đông Nam Á (Indonesia, Philippines, Malaysia) khá nhanh nhưng không kèm theo nhận thức về tầm quan trọng của việc bảo vệ CNTT khỏi các cuộc tấn công mạng. Myanmar chỉ đưa ra kế hoạch ngăn chặn các cuộc tấn công mạng. Hầu hết các nước ASEAN xếp các vấn đề về đe dọa mạng vào loại vấn đề phi chính trị hóa. Indonesia và Philippines hiểu rằng tấn công mạng có thể gây thiệt hại cho cơ sở hạ tầng công cộng, dữ liệu và thông tin liên quan đến an ninh quốc gia có thể bị truy cập. Tuy nhiên, thách thức đối với Inđonesia và Philippines là chưa có kế hoạch cụ thể để đối phó với các cuộc tấn công mạng. Tương tự như Indonesia và Philippines, Malaysia cũng đối diện với những khó khăn tương tự liên quan đến các kế hoạch và chiến lược cụ thể. Thách thức đối với Thái Lan là thiếu kiến thức liên quan đến các mối đe dọa mạng, mặc dù người dân Thái Lan đã quen thuộc với các công nghệ mạng như mạng xã hội và giao dịch điện tử. Nhưng nguồn nhân lực hiểu biết về lĩnh vực kỹ thuật cũng thiếu, do đó, không có cơ quan chức năng nào chịu trách nhiệm ngăn chặn và đưa ra phản ứng tức thời nếu mối đe dọa xảy ra.

Thứ hai, mức chi tiêu bảo đảm an ninh mạng trong khu vực thấp. Mặc dù có nền kinh tế kỹ thuật số đang phát triển, nhưng ASEAN chi tiêu quá thấp cho an ninh mạng. Tình trạng càng trở nên trầm trọng hơn do khu vực thiếu chú ý đến các mối đe dọa mạng. Ngân sách nhà nước mà ASEAN chi cho bảo đảm an ninh mạng tương đối nhỏ, khoảng 0,06% GDP (1,9 tỷ USD). Thái Lan và Malaysia phân bổ cho bảo đảm an ninh mạng lần lượt 0,05% GDP và 0,08% GDP (2017). Tính trung bình, các nước thành viên ASEAN sử dụng 0,06% GDP cho an ninh mạng. Do vậy, ASEAN cần phải tăng ngân sách an ninh mạng của khu vực do những mối nguy hiểm đang bị đe dọa. Chi phí đầu tư cho việc bảo vệ dữ liệu có thể cao nhưng nếu bỏ qua có thể dẫn đến thiệt hại lớn hơn cho nền kinh tế và giảm lòng tin của xã hội. Trong ASEAN, Singapore đứng đầu về chi tiêu cho an ninh mạng, chiếm 0,22% tổng GDP (2017) và trở thành quốc gia duy nhất trong khu vực Đông Nam Á phân bổ ngân sách cho an ninh mạng nhiều hơn toàn cầu, bình quân 0,13% GDP. Singapore đã thành lập Quỹ Năng lực Không gian mạng ASEAN (ASEAN Cyber Capacity Fund) trị giá 10 triệu USD với mục đích cải thiện khả năng an ninh mạng của khu vực Đông Nam Á.

Thứ ba, thiếu năng lực quản trị và kỹ năng bảo vệ yếu kém của CNTT ở Đông Nam Á. Lỗ hổng bảo mật khiến tội phạm mạng nhắm mục tiêu vào Đông Nam Á như một cuộc tấn công. Nguy cơ bị tấn công mạng trong khu vực Đông Nam Á gây ra nhiều tổn thất. Báo cáo của AT Kearney, rủi ro an ninh mạng có thể khiến 1.000 công ty trong khu vực Đông Nam Á bị thiệt hại 750 tỷ đô la Mỹ. Indonesia thậm chí còn yếu kém hơn khi chưa có khuôn khổ để lập kế hoạch chống lại các cuộc tấn công mạng. Trong khi Indonesia là quốc gia có xu hướng phát triển ngành sử dụng CNTT khá cao. Các công ty khởi nghiệp như Gojek, Bukalapak, là những ngành công nghiệp kỹ thuật số lưu trữ dữ liệu người dùng, khiến Indonesia trở thành một trong những quốc gia dễ bị tổn thương nhất trong ASEAN và cũng sẽ bị tổn thất rất lớn nếu bị tấn công. Myanmar, ngoài việc thiếu công nghệ và cơ sở hạ tầng, cũng phải đối diện với thách thức lớn nhất là thiếu kiến thức, kỹ năng quản trị và nhận thức về an ninh mạng. Các luật liên quan đến không gian mạng của Myanmar còn nhiều bất cập.

Thứ tư, thiếu các chuyên gia trong lĩnh vực bảo đảm an ninh mạng. Ngành công nghiệp an ninh mạng của khu vực ASEAN gặp khó khăn để đáp ứng nhu cầu bảo đảm an ninh mạng vì khả năng và chuyên môn của nguồn nhân lực bảo đảm an ninh mạng còn thiếu. Với chất lượng và khả năng tiếp cận giáo dục khác nhau của các quốc gia ASEAN, đặc biệt là trong lĩnh vực an ninh mạng, các chuyên gia rất yếu trong vấn đề xử lý tình huống khó khăn và là vấn đề đáng báo động trong khu vực. Sự phát triển công nghệ nhanh tạo ra nhiều mối đe dọa nghiêm trọng. Việc giám sát và phản hồi khó khăn hơn, đặc biệt là với mã hóa mạnh mẽ hơn, như điện toán đám mây (cloud computing) và sự phát triển của Internet vạn vật (IoT). Nhiều nước Đông Nam Á thiếu tư duy chiến lược, chính sách và giám sát thể chế đối với an ninh mạng, dẫn đến chia rẽ nhiệm vụ giữa cảnh sát quốc gia (đối với tội phạm mạng) và Bộ nội vụ (đối với cơ sở

hạ tầng quan trọng). Có ít hoặc không có sự phối hợp giữa các cơ quan tổ chức. Do thiếu thống nhất thường dẫn đến không đầu tư cho việc bảo đảm an ninh mạng.

Thứ năm, chưa nhận thức được về rủi ro không gian mạng. Trong khu vực tư nhân, rủi ro không gian mạng được coi là do công nghệ thông tin (CNTT) chứ không phải là một vấn đề kinh doanh, vì vậy doanh nghiệp không có cách tiếp cận toàn diện đến vấn đề an ninh mạng. Các doanh nghiệp không coi an ninh mạng là ưu tiên kinh doanh nên không có cách tiếp cận tổng thể để chống lại sự phá hoại không gian mạng. Các quốc gia Đông Nam Á ít có sự chia sẻ. Hạn chế thông báo về mối đe dọa an ninh mạng thường là do không tin tưởng và thiếu minh bạch. Việc thiếu nhận thức của cộng đồng về các rủi ro mạng và sự cố an ninh mạng là một vấn đề đáng lo ngại. Khu vực ASEAN có nhận thức thấp hơn về an ninh mạng so với các quốc gia khác nơi luật vi phạm dữ liệu có hiệu lực. Vấn đề thiếu nhận thức về an ninh mạng của ASEAN đã ảnh hưởng đến nhịp độ, quan điểm của các nhà lập pháp trong khu vực Đông Nam Á để thực hiện các biện pháp an ninh mạng. Trong số các quốc gia ASEAN, chỉ có Singapore và Malaysia trang bị một số công cụ quản lý an ninh mạng tiên tiến. Philippines và Thái Lan đã bắt đầu thiết lập một số khuôn khổ quy định cần thiết để giải quyết vấn đề an ninh mạng. Mặc dù vậy, phần lớn các quốc gia thành viên ASEAN vẫn chưa xây dựng các quy tắc vững chắc hơn về an ninh mạng.

4. GIẢI PHÁP ĐẢM BẢO AN NINH MẠNG ASEAN

An ninh mạng đang ngày càng trở nên quan trọng để đảm bảo sự phát triển bền vững trong bối cảnh nền kinh tế ASEAN phát triển nhanh cùng với sự thâm nhập mạnh của các thiết bị thông minh và dữ liệu công nghệ mạng trong cuộc sống. Hiện Đông Nam Á là tổ chức khu vực duy nhất đã ký 11 chuẩn mực tự nguyện, không ràng buộc của Liên hợp quốc về hành vi có trách nhiệm của nhà nước trong không gian mạng. Đông Nam Á cần phát triển các chuẩn mực hành vi trên không gian mạng để duy trì sự ổn định khu vực. Trong bối cảnh dịch bệnh Covid-19 đang diễn biến ngày càng phức tạp ở các nước Đông Nam Á. Hội nghị Bộ trưởng ASEAN về an ninh mạng lần thứ 6 (10/2021) sẽ tạo cơ hội cho các cơ quan thực thi pháp luật ASEAN trao đổi kinh nghiệm, chia sẻ thông tin về các nguy cơ đe dọa an ninh mạng và các giải pháp phòng ngừa nhằm bảo đảm an toàn không gian mạng cho các nước ASEAN.

Thứ nhất, tiếp tục ban hành và thực thi pháp luật điều chỉnh tội phạm mạng**.** Trên toàn cầu, Công ước của Hội đồng Châu Âu (Council of Europe Convention on Cybercrime) về tội phạm mạng, được thừa nhận là "Công ước Budapest", là công ước quốc tế đầu tiên và duy nhất đề cập đến tội phạm mạng cho đến ngày nay. Công ước Budapest kết hợp cả các phần quy định về thủ tục, yêu cầu các bên ký kết hình sự hóa các hành vi vi phạm mạng chống lại tính bảo mật, tính toàn vẹn và tính khả dụng của dữ liệu máy tính. Những hành vi này bao gồm các tội danh như truy cập bất hợp pháp, chặn đường truyền không công khai, can thiệp vào dữ liệu và hệ thống máy tính cũng như sử dụng sai các thiết bị liên quan đến máy tính. Cho đến nay, vẫn chưa có bất kỳ quốc gia thành viên ASEAN nào ký và

hoặc phê chuẩn "Công ước Budapest" và chỉ có tám trong số mười quốc gia thành viên ASEAN (ngoại trừ Lào và Campuchia), đã ban hành một số hình thức pháp luật để điều chỉnh tội phạm mạng cùng những luật phù hợp với yêu cầu của "Công ước Budapest". Cho dù là một thực thể ASEAN thống nhất, luật pháp và các biện pháp chống khủng bố mạng của mỗi quốc gia thành viên cũng rất khác nhau. Do các thành viên ASEAN xây dựng chính sách an ninh mạng trong các giai đoạn khác nhau. Vì vậy, khu vực cần thành lập cơ quan chính phủ chính thức chịu trách nhiệm phát triển chính sách an ninh mạng để thúc đẩy sự phát triển các chuẩn mực mạng từ bên trong nội bộ quốc gia. Hiện ASEAN có bốn cơ chế để điều tra các đặc điểm khác nhau của an ninh mạng và tội phạm mạng: 1) Hội nghị Bộ trưởng ASEAN về Tội phạm Xuyên Quốc gia (AMMTC - ASEAN Ministerial Meeting on Transnational Crime); 2) Hội nghị Bộ trưởng Viễn thông và Công nghệ thông tin ASEAN (TELMIN - ASEAN Telecommunications and IT Ministers Meeting); 3) Diễn đàn Khu vực ASEAN (ARF - ASEAN Regional Forum); 4) Hội nghị Quan chức Cấp cao ASEAN về Tội phạm Xuyên Quốc gia (SOMTC – ASEAN Senior Oficials Meeting on Transnational Crime).

Thứ hai, nâng cao nhận thức về bảo đảm an ninh mạng và tăng cường năng lực cho lực lượng thực thi pháp luật**.** Nâng cao nhận thức về an ninh mạng là sáng kiến được đưa ra trong Kế hoạch tổng thể của ASEAN (ASEAN Master Plan) năm 2015 và năm 2020. Sự xuất hiện của dịch Covid-19 buộc ASEAN phải thích ứng với một nền tảng điện tử và phụ thuộc nhiều hơn vào mạng, như tăng cường phụ thuộc vào các giao dịch trực tuyến và thậm chí chuyển sang làm việc trực tuyến, tạo ra nhiều dữ liệu hơn để có thể tiếp xúc. Vì vậy, ASEAN phải thúc đẩy các nỗ lực tìm hiểu và chống lại các mối đe dọa mạng trong khu vực. Nâng cao giáo dục về an ninh mạng trong quần chúng, đặc biệt là ở trẻ em, những đối tượng tiềm năng dễ bị tổn thương nhất. Giáo dục về tầm quan trọng của việc giữ bí mật thông tin cá nhân. Các loại tội phạm về an ninh mạng đang thay đổi phương thức, thủ đoạn để tấn công trên nhiều lĩnh vực đòi hỏi ASEAN cần phải tăng cường nhận thức về an ninh mạng và nâng cao năng lực cho lực lượng thực thi pháp luật. Thúc đẩy việc thống nhất về nhận thức và hành động của các nước ASEAN đối với vấn đề an ninh mạng, tiến tới xây dựng các khuôn khổ pháp lý chung tạo thuận lợi cho việc phối hợp, hợp tác quốc tế trong lĩnh vực an ninh mạng.

Thứ ba, xây dựng trung tâm ứng cứu khẩn cấp ASEAN cho mục tiêu bảo đảm an ninh mạng**.** Hoạt động của trung tâm thông tin an ninh mạng giữa ASEAN và Singapore là một bước tiến mới để tăng cường năng lực về an ninh mạng. Việt Nam đã đăng ký 1,68 triệu khối IP Block (2016), nhờ đó ngăn chặn được một số cuộc tấn công nhằm vào các thiết bị Internet of Things (IoT) có nguồn gốc của tấn công mạng. Phối hợp chặt chẽ trong việc xây dựng Trung tâm ứng cứu khẩn An ninh mạng của ASEAN. Thiết lập cơ chế hợp tác đào tạo chung, dài hạn, chuyên sâu với sự hỗ trợ của các nước đối tác (Trung Quốc, Nhật Bản, Hàn Quốc...) trong lĩnh vực bảo

đảm an ninh mạng. Thiết lập cơ chế và xây dựng kế hoạch hợp tác đào tạo chung, dài hạn trong ASEAN theo hướng chuyên sâu, đào tạo chuyên gia và cán bộ nguồn; ưu tiên tập trung một số lĩnh vực quan trọng như: xây dựng pháp luật; điều tra số, phục hồi, phân tích dữ liệu, chứng cứ điện tử; phòng, chống tội phạm có tổ chức xuyên quốc gia trong lĩnh vực tài chính, ngân hàng, tội phạm rửa tiền; quản lý thông tin xấu độc; bảo vệ dữ liệu cá nhân... nhằm tiến tới xây dựng "không gian mạng tự cường trong ASEAN".

Thứ tư, thúc đẩy xây dựng Chiến lược hợp tác an ninh mạng khu vực ASEAN (2021-2025). An ninh mạng đã trở thành một trong những thách thức an ninh phi truyền thống lớn nhất đòi hỏi các nước ASEAN không ngừng nỗ lực nâng cao năng lực để đảm bảo an ninh toàn diện và ngăn chặn tội phạm mạng. Kế hoạch chi tiết về Cộng đồng Chính trị-An ninh ASEAN năm 2025 nhấn mạnh sự cần thiết phải chống lại tội phạm mạng bằng các phương thức hợp tác trong khu vực. Đề cao tăng cường hợp tác giữa tất cả các quốc gia thành viên ASEAN trong cuộc chiến chống khủng bố mạng, kêu gọi xây dựng và cải thiện luật pháp phù hợp để giải quyết tội phạm mạng cũng như tăng cường quan hệ đối tác công - tư nhằm tăng cường chia sẻ thông tin an toàn trong khu vực. Hợp tác khu vực cần được cập nhật và giám sát liên tục, cùng với sự giúp đỡ quốc tế đối với việc tăng cường thực tiễn an ninh mạng ASEAN. Thế giới tội phạm mạng và an ninh mạng đang có tốc độ phát triển nhanh hơn và điều quan trọng là sự hợp tác cần phải luôn đi trước hai bước. ASEAN tiếp tục tăng cường hợp tác nâng cao năng lực bảo vệ Cơ sở hạ tầng thông tin trọng yếu thông qua tổ chức diễn tập chung phòng, chống tấn công mạng, ứng cứu khắc phục sự cố an ninh mạng; tập huấn nâng cao năng lực cho các nhà quản lý, vận hành. Thúc đẩy xây dựng Chiến lược hợp tác an ninh mạng khu vực ASEAN (2021-2025) để thống nhất tầm nhìn, nhận thức và hành động chung của các nước ASEAN đối với vấn đề an ninh mạng; tiến tới xây dựng các khuôn khổ pháp lý khu vực nhằm tạo thuận lợi cho việc phối hợp, hợp tác quốc tế trong lĩnh vực an ninh mạng. Để tăng cường bảo vệ an ninh mạng, các thành viên ASEAN đang xem xét hợp tác trong bốn lĩnh vực chính: (i)Thực hiện hành động nhanh chóng khung bảo đảm an ninh mạng (RAC – Rapid Action Cyber) để nâng cao an ninh mạng trong chương trình chính sách khu vực. Khung RAC bao gồm Chương trình hành động 12 điểm hành động cho các chính phủ giải quyết những rạn nứt trong chính sách, chiến lược và luật pháp liên quan đến an ninh mạng; (ii) Duy trì cam kết về an ninh mạng, trong đó bao gồm việc giảm khoảng cách chi tiêu bảo đảm không gian mạng, sử dụng bảng điều khiển vệ sinh mạng để xác định và theo dõi số liệu; (iii) Khuyến khích các liên minh công - tư thúc đẩy tư duy lấy rủi ro làm trung tâm (risk-centric mindset) trong khu vực doanh nghiệp, tạo một nền văn hóa chia sẻ mối đe dọa mạng và giúp khả năng phục hồi không gian mạng cho chuỗi cung ứng; (iv) Giải quyết tình trạng thiếu kỹ năng an ninh mạng và tăng cường quan hệ đối tác toàn cầu-địa phương trong ngành công nghiệp. Bao gồm áp dụng nghiên cứu và phát triển công nghệ sáng tạo, là yếu tố

cần thiết để giải quyết những điều không lường trước được các mối đe dọa.

Đông Nam Á thúc đẩy các biện pháp hợp tác khu vực trên không gian mạng trong bối cảnh điều kiện bình thường mới, chú trọng các lĩnh vực hợp tác giữa các thành viên ASEAN và các đối tác đối thoại của khối, phối hợp các chính sách không gian mạng của khu vực, ứng phó với các sự cố trên không gian mạng từ quá trình số hóa nhanh do tác động của đại dịch Covid-19.

Tóm lại, an ninh mạng là thách thức thực sự đối với các nước ASEAN. Singapore với tư cách là nhân tố tích cực bảo vệ các vấn đề an ninh mạng ở khu vực Đông Nam Á. Hợp tác ASEAN đã khởi động Chương trình Năng lực Không gian mạng (Cyber Capacity Program) nhưng trên thực tế, nhiều nước Đông Nam Á vẫn chưa có kế hoạch và chiến lược đối phó với các mối đe dọa mạng, các nước Đông Nam Á chưa coi vấn đề mạng là một mối đe dọa nghiêm trọng. Vì vậy, nỗ lực bảo đảm an ninh mạng của các quốc gia trong khu vực Đông Nam Á chưa thực sự thành công. Các chính sách khu vực ASEAN về bảo đảm an ninh mạng của các quốc gia thành viên ASEAN còn hạn chế do việc xem xét không can thiệp vào quyền tự quyết của quốc gia. Các quốc gia ASEAN được khuyến khích cần mở rộng sự hiểu biết sâu sắc hơn về các mối đe dọa an ninh trong không gian mạng và hành động hợp tác nhanh hơn, học hỏi kinh nghiệm của các nước láng giềng để phát triển kinh tế và an toàn trong kỷ nguyên kỹ thuật số đang phát triển.

TÀI LIỆU THAM KHẢO

1. AT Kearney, "Cybersecurity in ASEAN: An Urgent Call to Action", AT Kearney, Tech. Report, 2018.

2. Chang L. Cybercrime and cyber security in ASEAN. Monash University, 2017. https://www.academia.edu/32258162/Cybercrime_and_Cyber_security_in_ASEAN (accessed 03.28.2020)

3. CNBC, "Southeast Asia is Hugely at Risk of Cyberattacks. It's Not Investing Nearly Enough in Security, report says", CNBC, 2018. Available: https://www.cnbc.com/2018/01/23/asean-need-to-increase-cybersecurity-spending-says-new-report.html (Accessed 12 August 2019)

4. Inda Mastika Permata (2021), The Securitization of cyber Issue in ASEAN, (researchgate.net)

5. Kaspersky. What is Cyber Security? https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security (accessed 11.04.2019)

6. Gnanasagaran A. The flip side of a digital ASEAN. The ASEAN Post, 10.02.2018. https://theaseanpost.com/article/flipside-digital-asean (accessed 11.27.2019)

7. Lê Phi (2021), ASEAN tăng cường hợp tác trong khu vực về an ninh mạng - Báo Cần Thơ Online (baocantho.com.vn)

8. Nguyễn Nhâm (2020), Các nước ASEAN tăng cường hợp tác an ninh mạng | VOV.VN

9. Shahar S.M., Ma'arif M.Y., Mizan N.S., Zatar N.S. 2019. CNDS-Cybersecurity: Issues and Challenges in ASEAN Countries. International Journal of Advanced Trends in Computer Science and Engineering. Vol. 8. No. 1.4.

10. Subhan A. Southeast Asia's cybersecurity an emerging concern. The ASEAN Post, 20.05.2018. https://theaseanpost.com/article/southeast-asias-cybersecurity-emerging-concern (accessed 10.19.2019)

11. Strengthening ASEAN's cybersecurity. 2018. https://theaseanpost.com/article/strengthening-aseans-cybersecurity (accessed 12.04.2019)

12. Xuân Tùng (2021), Thúc đẩy chiến lược hợp tác an ninh mạng khu vực ASEAN (mod.gov.vn).