KHUNG PHÁP LÍ VỀ CƠ CHẾ HỢP TÁC PHÒNG CHỐNG TỘI PHẠM MẠNG TRONG KHU VỰC ASEAN

ĐỖ QUÍ HOÀNG *

Tóm tắt: *Tội phạm mạng là một dạng thức của tội phạm xuyên quốc gia, đòi hỏi có sự hợp tác giữa các quốc gia trong nhiều lĩnh vực, mà đặc biệt là về pháp luật và lĩnh vực kĩ thuật bảo mật. Quá trình hợp tác nhằm ngăn ngừa, phòng, chống loại hình tội phạm này không chỉ diễn ra trên phạm vi toàn cầu mà từng khu vực cũng cần tự trang bị cho mình cơ chế phù hợp. Bài viết làm rõ khung pháp lí điều chỉnh hoạt động hợp tác ngăn ngừa, phòng, chống tội phạm mạng của khu vực ASEAN, nhận diện một số hạn chế và đề xuất một số giải pháp nhằm thúc đẩy và thiết lập có hiệu quả cơ chế hợp tác trong phòng, chống tội phạm mạng.*

Từ khoá: ASEAN; hài hoà hoá pháp luật; tội phạm mạng; tội phạm công nghệ cao

Nhận bài: 20/7/2020 Hoàn thành biên tập: 07/4/2021 Duyệt đăng: 07/4/2021

LEGAL FRAMEWORK ON COOPERATION ABOUT CYBERCRIME PREVENTION IN ASEAN

Abstract: *Cybercrime is a form of transnational crime that requires cooperation from many aspects, especially in legal and specific security technology. The process of international cooperation to prevent this type of crime not only takes place in an -global scope, but it also needs to equip itself with appropriate mechanisms. The paper focuses on clarifying the legal framework governing the prevention of cybercrime within ASEAN, identify several limitations and propose solutions to promote and effectively establish a cooperation mechanism in preventing and combating cybercrime.*

Keywords: ASEAN; legal harmonization, cybercrime

Received: July 20th, 2020; Editing completed: Apr 7th, 2021; Accepted for publication: Apr 7th, 2021

1. Khái quát về tình hình tội phạm mạng tại khu vực ASEAN

Năm 2019, số lượng người dùng Internet ở tất cả các nước ASEAN đã gia tăng mạnh mẽ, đặc biệt là Brunei, Campuchia, Myanmar, Philippines, Singapore, Thái Lan và Việt Nam.(1) Internet đang mang đến những thay đổi toàn diện trong đời sống của con người. Việc sử dụng các ứng dụng Internet trên máy tính, thiết bị di động đã ngày càng trở nên phổ biến với mọi vùng miền, lứa tuổi. Bên cạnh tác động tích cực hiện hữu trong đời sống hằng ngày, không thể phủ nhận những hậu quả bất lợi do Internet hay bắt nguồn từ Internet, một trong số đó là sự xuất hiện và gia tăng của các hình thức tội phạm công nghệ cao, đặc biệt là tội phạm mạng. Trong bối cảnh đó, ASEAN không thể tự tách ra khỏi những ảnh hưởng tiêu cực của loại hình tội phạm này. Đa phần các nước ASEAN đã và đang trải qua các cuộc tấn công của tội phạm mạng. Ví dụ, cảnh sát của Malaysia

*** Thạc sĩ, Trường Đại học Luật Hà Nội**
E-mail: doquihoang@hlu.edu.vn

(1). https://dig.watch/updates/40-million-new-digital-users-southeast-asia-2020, truy cập 01/4/2021.

ghi nhận 24 trường hợp tấn công mạng của hacker giữa tháng 01 và tháng 9/2012, với thiệt hại ước tính lên tới 1,1 triệu đô la.(2) Indonesia đã có kinh nghiệm đối mặt với kế hoạch lừa đảo trực tuyến nghiêm trọng mà thiệt hại lên tới hơn 500 nghìn đô la.(3) Những vụ việc có thiệt hại trên 500 nghìn đô la tại Indonesia chiếm 40% trong tổng số 176 vụ việc liên quan đến tội phạm mạng trong năm 2013.(4) Chính phủ Campuchia đã chịu nhiều tổn thất từ các cuộc tấn công mạng trong quá khứ, đặc biệt phải kể tới một nhóm trộm ẩn danh trên mạng đã đánh cắp hơn 5.000 tài liệu từ Bộ Ngoại giao của nước này.(5) Singapore cũng không đứng ngoài xu hướng này khi có tới hơn 900 công dân là nạn nhân của hành vi lừa đảo trực tuyến trong lĩnh vực ngân hàng trong Quý I/2013.(6) Tại Brunei, theo ghi nhận của Dịch vụ Bảo vệ an ninh công nghệ thông tin, đã phát hiện hơn 2.000 cuộc tấn công mạng trong giai đoạn 2010 - 2012, trong đó bao gồm 62% cuộc tấn công bằng virus, 26% thông qua hình thức thư rác, l7% tới từ các hành vi giả mạo nội dung trang web (defacement) và lừa đảo thông qua gian lận, lừa đảo email là 04% (scams and phising)[7]. Thái Lan ghi nhận có đến 1.485 cuộc xâm nhập bất hợp pháp vào trang web của Chính phủ và hàng trăm cuộc tấn công, lừa đảo từ các phần mềm độc hại.(8) Thực tiễn này cho thấy, các quốc gia cho thấy ASEAN là khu vực dễ bị tổn thương trong việc đấu tranh phòng, chống tội phạm mạng.(9) Ngoài ra, dữ liệu của Microsoft đã chỉ ra rằng, trong giai đoạn từ tháng 7 đến tháng 12/2015, so với các quốc gia ở Đông Á, các quốc gia Đông Nam Á có tỉ lệ cao hơn trong việc gặp phải các phần mềm độc hại hay một mối đe dọa cụ thể.(10) Chỉ số nhiễm độc Malware 2016 cũng cho thấy, trong khu vực Châu Á Thái Bình Dương, các nước ASEAN nằm trong nhóm những quốc gia bị ảnh hưởng lớn từ các mối đe dọa do phần mềm độc hại, trong đó Indonesia xếp thứ hai trong danh sách sau Pakistan, Việt Nam, Philippines và Campuchia lần lượt xếp thứ 5, 6 và 7 trong khi Thái Lan, Malaysia và Singapore lần lượt xếp thứ 10, 11 và 12.(11)

Theo tác giả Michael Raska, tình trạng tội phạm mạng tại các nước ASEAN bắt

(2). https://jurnal.uns.ac.id/belli/article/viewFile/27366/18950, truy cập 01/4/2021.
(3). https://jurnal.uns.ac.id/belli/article/viewFile/27366/18950, truy cập 01/4/2021.
(4). https://jurnal.uns.ac.id/belli/article/viewFile/27366/18950, truy cập 01/4/2021.
(5). https://jurnal.uns.ac.id/belli/article/viewFile/27366/18950, truy cập 01/4/2021.
(6). https://jurnal.uns.ac.id/belli/article/viewFile/27366/18950, truy cập 01/4/2021.
(7). https://jurnal.uns.ac.id/belli/article/viewFile/27366/18950, truy cập 01/4/2021.
(8). https://jurnal.uns.ac.id/belli/article/viewFile/27366/18950, truy cập 01/4/2021.
(9). Bima Yudha Wibawa Manopo, Diah Apriani Atika Sari, *ASEAN Regional Forum - Realizing regional cyber security in ASEAN region*, p. 44 - 45. https://jurnal.uns.ac.id/belli/article/viewFile/27366/18950, truy cập 03/3/2021.
(10). Microsoft (2016b), *Microsoft Security Intelligence Report* (Vol. 20). Seattle: Microsoft, https://www.microsoft.com/en-us/download/details.aspx?id=52255, truy cập 03/3/2021.
(11). Microsoft (2016a), *Malware Infection Index 2016 highlights key threats undermining cybersecurity in Asia Pacific*: Microsoft, https://news.microsoft.com/apac/2016/06/07/malware-infection-index-2016-highlights-key-threats-undermining-cybersecurity-in-asia-pacific-microsoft-report/, truy cập 03/3/2021.

nguồn từ một số nguyên nhân phổ biến sau:[(12)] 1) Nhiều quốc gia Đông Nam Á đã không xây dựng đầy đủ chiến lược, chuẩn bị chính sách để đảm bảo an toàn an ninh mạng; 2) Trong khu vực tư nhân, rủi ro không gian mạng vẫn được coi là công nghệ thông tin chứ không phải là vấn đề kinh doanh, vì vậy các doanh nghiệp trong khu vực chưa thực sự có cách tiếp cận phù hợp đối với vấn đề an ninh mạng; 3) Ngành công nghiệp an ninh mạng trong khu vực phải đối mặt với những thách thức do hạn chế về năng lực ứng phó và đặc biệt là đội ngũ chuyên gia; 4) *C*ác quốc gia Đông Nam Á vẫn có sự thận trọng trong việc chia sẻ thông tin, đây là nguyên nhân xuất phát một phần do sự thiếu lòng tin và minh bạch; 5) Sự đẩy mạnh kết nối giữa các nền kinh tế Đông Nam Á làm gia tăng nhiều rủi ro mang tính hệ thống; 6) Sự phát triển nhanh chóng của công nghệ thông tin làm cho việc giám sát và ứng phó mối đe dọa trở nên khó khăn hơn, đặc biệt là các công nghệ liên quan đến điện toán đám mây và công nghệ vạn vật kết nối (Internet of Things - IoT).

2. Khung pháp lí-chính trị về hoạt động hợp tác ngăn ngừa, phòng chống tội phạm mạng của ASEAN

2.1. Khuôn khổ pháp lí - chính trị chung cho hoạt động hợp tác phòng, chống tội phạm mạng của ASEAN

Theo Kế hoạch hành động ASEAN về phòng, chống tội phạm xuyên quốc gia năm 1999 và Chương trình hành động thực hiện Kế hoạch hành động ASEAN về chống tội phạm xuyên quốc gia năm 2002, tội phạm mạng (loại hình tội phạm thứ 8) được ASEAN xếp vào nhóm tội phạm xuyên quốc gia cùng với các loại hình tội phạm khác là buôn bán ma tuý bất hợp pháp, cướp biển, buôn bán người, khủng bố, buôn lậu vũ khí, rửa tiền và tội phạm kinh tế.[(13)] Do đó, khuôn khổ pháp lí-chính trị đối với tội phạm mạng bao gồm những văn kiện về ngăn ngừa, phòng, chống tội phạm xuyên quốc gia nói chung và các văn kiện điều chỉnh riêng đối với loại tội phạm này.

2.1.1. Các văn kiện về ngăn ngừa, phòng, chống tội phạm xuyên quốc gia nói chung

Thứ nhất, Tuyên bố Kuala Lumpur về chống tội phạm xuyên quốc gia năm 2015

Tuyên bố Kuala Lumpur về chống tội phạm xuyên quốc gia được các Bộ trưởng phụ trách vấn đề tội phạm xuyên quốc gia của ASEAN thông qua năm 2015.[(14)] Nội dung của Tuyên bố tập trung vào các vấn đề về tăng cường thể chế trong phòng, chống tội phạm xuyên quốc gia của ASEAN như triệu tập Hội nghị Bộ trưởng ASEAN phụ trách vấn đề chống tội phạm xuyên quốc gia (ASEAN Ministerial Meeting on Transnational Crime - AMMTC) trên cơ sở các phiên họp hằng năm để tham vấn thường xuyên; triệu tập các phiên họp khẩn cấp khi cần thiết để

(12). Michael Raska, Benjamin Ang, *Cybersecurity in Southeast Asia,* Note de présentation n°5/8 de l'Observatoire Asie du Sud-Est, cycle 2018-2019 Mai 2018, https://centreasia.eu/wp-content/uploads/2018/12/NotePrésentation-AngRaska-Cybersecurity_180518.pdf, truy cập 12/4/2020.

(13). https://asean.org/?static_post=work-programme-to-implement-the-asean-plan-of-action-to-combat-transnational-crime-kuala-lumpur-17-may-2002, truy cập 03/02/2021.

(14). https://asean.org/kuala-lumpur-declaration-in-combating-transnational-crime/, truy cập 03/02/2021.

đáp ứng ngay lập tức và hiệu quả đối với các thách thức và mối đe dọa từ các tội phạm xuyên quốc gia; tăng cường năng lực của hệ thống tư pháp hình sự; tăng cường hợp tác và phối hợp giữa các cơ quan thực thi pháp luật ASEAN.

Thứ hai, Kế hoạch hành động ASEAN về phòng, chống tội phạm xuyên quốc gia (2016 - 2025)

Kế hoạch hành động ASEAN về phòng, chống tội phạm xuyên quốc gia - ASEAN Plan of Action in Combating Transnationl Criem (2016 - 2025) được thông qua năm 2017 nhằm triển khai các nội dung trước đó được ghi nhận trong Tuyên bố Kuala Lumpur về chống tội phạm xuyên quốc gia.(15) Qua đó, thúc đẩy sự hợp tác chặt chẽ giữa các quốc gia thành viên ASEAN để ngăn ngừa và chống tội phạm xuyên quốc gia, cũng như nâng cao năng lực của ASEAN để giải quyết các tội phạm xuyên quốc gia một cách hiệu quả và kịp thời. Các hành động, lĩnh vực ưu tiên được ghi nhận trong Kế hoạch hành động bao gồm:

- Xây dựng chiến lược hoặc kế hoạch quốc gia để ngăn ngừa và phòng, chống tội phạm xuyên quốc gia, trong đó tập trung vào một số vấn đề như thành lập các đơn vị, lực lượng đặc nhiệm trong cơ quan thực thi pháp luật khi thích hợp; cho phép sử dụng kĩ thuật điều tra đặc biệt khác như giám sát điện tử và hoạt động theo dõi bí mật; xây dựng hồ sơ tội phạm và cơ sở dữ liệu của các quốc gia thành viên ASEAN và vấn đề bảo vệ nhân chứng;

- Các vấn đề pháp lí bao gồm đàm phán xây dựng, kí kết điều ước quốc tế liên quan đến tội phạm xuyên quốc gia; phát triển công cụ pháp lí của khu vực; đẩy mạnh hoạt động hài hoà hoá chính sách, pháp luật của các quốc gia trong khu vực về tội phạm xuyên quốc gia;

- Trao đổi thông tin thông qua việc thiết lập kho lưu trữ dữ liệu khu vực về pháp luật của các quốc gia thành viên liên quan đến các tội phạm xuyên quốc gia tại Ban Thư kí ASEAN; xây dựng các điểm liên lạc trọng điểm quốc gia; tăng cường sử dụng công nghệ viễn thông cũng như sử dụng công cụ tích hợp sẵn có của INTERPOL như i-24/7;

- Thực thi pháp luật trên cơ sở tiến hành biện pháp tăng cường hợp tác và phối hợp trong trao đổi, chia sẻ thông tin, bảo vệ nhân chứng, bảo vệ, giúp đỡ nạn nhân cũng như tăng cường hợp tác với các bên liên quan; thực hiện các cuộc điều tra chung và sử dụng kĩ thuật điều tra đặc biệt khi thích hợp;

- Đào tạo và xây dựng năng lực thể chế thông qua việc phát triển các chương trình đào tạo và tiến hành hội thảo, các hoạt động nâng cao năng lực khác; sử dụng cũng như nâng cấp các trung tâm đào tạo của các quốc gia thành viên ASEAN.

2.1.2. Các văn kiện về tội phạm mạng

Do đặc thù của tội phạm mạng liên quan đến công nghệ nên bên cạnh các văn kiện quy định chung về tội phạm mạng với tính chất là loại tội phạm xuyên quốc gia, hoạt động ngăn ngừa, phòng, chống tội phạm mạng của ASEAN còn được điều chỉnh bằng

(15). https://asean.org/wp-content/uploads/2012/05/ASEAN-Plan-of-Action-in-Combating-TC_Adop ted-by-11th-AMMTC-on-20Sept17.pdf, truy cập 03/02/2021.

các văn kiện trong lĩnh vực công nghệ thông tin có liên quan đến an ninh mạng, cụ thể:

Thứ nhất, Tuyên bố ASEAN về ngăn ngừa và phòng, chống tội phạm mạng (ASEAN Declaration on the Prevention and Combat of Cyber Crime)

Năm 2017, các nhà lãnh đạo ASEAN đã thông qua Tuyên bố ASEAN về ngăn chặn và chống tội phạm mạng trong Hội nghị thượng đỉnh ASEAN lần thứ 31 tại Manila, Philippines.(16) Đây là văn kiện đầu tiên của ASEAN đề cập vấn đề tội phạm.

Theo đó, những biện pháp ngăn ngừa, phòng, chống tội phạm mạng được ASEAN thông qua bao gồm: 1) hài hoà hoá pháp luật liên quan đến tội phạm mạng và bằng chứng điện tử; 2) gia nhập hệ thống các văn kiện pháp lí khu vực và quốc tế hiện có trong lĩnh vực đấu tranh phòng, chống tội phạm mạng; 3) xây dựng kế hoạch hành động của từng quốc gia trong việc giải quyết vấn đề tội phạm mạng; 4) tăng cường hợp tác và phối hợp giữa các cơ quan của ASEAN, các quốc gia thành viên và hợp tác giữa ASEAN với cơ quan liên quan của quốc gia thành viên trong giải quyết các vấn đề về tội phạm mạng thông qua các hình thức như trao đổi thông tin, kinh nghiệm, tập huấn nghiệp vụ, nghiên cứu-giáo dục hay lĩnh vực hành chính-kĩ thuật và tăng cường nhận thức về tội phạm mạng; 5) tăng cường hợp tác quốc tế với các cơ quan, tổ chức có liên quan ở cấp khu vực và quốc tế như ASEANAPOL, EUROPOL và INTERPOL để tăng cường khả năng phòng ngừa, bảo vệ và ứng phó đối với các vấn đề an ninh mạng, trong đó đặc biệt là hành vi có liên quan đến tội phạm mạng, hệ thống mạng công nghệ cao.

Ngoài ra, Tuyên bố cũng nhấn mạnh việc phát triển năng lực của ASEAN trong hoạt động đấu tranh phòng, chống tội phạm mạng bằng cách hợp tác chặt chẽ hơn nữa với thiết chế "Tổ hợp INTERPOL toàn cầu về đổi mới" (The INTERPOL Global Complex for Innovation – IGCI),(17) thông qua việc cử các biệt phái viên cũng như thiết lập hệ thống chuyên gia chuyên trách về tội phạm mạng của ASEAN hoạt động trong IGCI. Với một bộ phận túc trực 24/7 để theo dõi và phối hợp với các quốc gia thành viên ASEAN nói riêng và châu Á nói chung để xử lí các vấn đề an ninh mạng, các tội phạm phát sinh tại chỗ cũng như khả năng sẵn sàng tiếp nhận nhân viên từ lực lượng cảnh sát các quốc gia thành viên trong khu vực gửi đến, IGCI là cơ hội hợp tác tốt giúp nâng cao năng lực ứng phó của các quốc gia ASEAN đối với các loại tội phạm công nghệ cao, trong đó có tội phạm mạng. Về nguyên tắc, IGCI không trực tiếp nhận tin báo tội phạm hay sự vụ từ công chúng. Đặc thù này xuất phát từ nguyên tắc hoạt động của Interpol về "không xâm phạm chủ quyền của các quốc gia thành viên".

(16). https://asean.org/asean-declaration-prevent-combat-cybercrime/, truy cập 02/3/2021.

(17). IGCI là cơ sở bổ sung cho Tổng hành dinh tọa lạc tại thành phố Lyon, Pháp, nhằm tăng cường sự hiện diện của Interpol ở châu Á. Hoạt động quan trọng nhất của IGCI là nghiên cứu và phát triển các công cụ mà cảnh sát sẽ dùng để nhận diện, phòng và chống tội phạm. IGCI cũng sẽ nghiên cứu, chế tạo các thiết bị cứu hộ khẩn cấp và kĩ thuật giám định pháp y để nhận diện nạn nhân trong các vụ thảm họa. Bên cạnh đó là hoạt động đào tạo, huấn luyện chuyên môn, xây dựng năng lực cho lực lượng cảnh sát của 190 quốc gia thành viên Interpol.

Điều này là hoàn toàn phù hợp với đặc thù hiện tại của các quốc gia ASEAN.

Thứ hai, Kế hoạch tổng thể về công nghệ thông tin ASEAN 2020 (ASEAN ICT Masterplan - AIM 2020)

Kế hoạch tổng thể về công nghệ thông tin ASEAN năm 2016 - 2020 đã được Hội nghị Bộ trưởng Viễn thông và Công nghệ thông tin ASEAN (The ASEAN Telecommunications and IT Ministers' Meeting - TELMIN) công bố năm 2015 với mục tiêu chính là chuyển đổi sang nền kinh tế kĩ thuật số, phát triển năng lực cần thiết cho con người để đáp ứng quá trình chuyển đổi này.(18) Để đạt được những mục tiêu này, ASEAN đã đề ra 08 chiến lược và một trong số đó là "Bảo mật và bảo đảm thông tin" (Chiến lược số 8) - chiến lược có liên quan mật thiết đến vấn đề an toàn an ninh mạng.(19) Chiến lược này bao gồm 2 sáng kiến sẽ được thực hiện trong toàn bộ kế hoạch tổng thể:

Sáng kiến đầu tiên là tăng cường an ninh thông tin trong ASEAN nhằm tạo ra nền kinh tế kĩ thuật số ASEAN đáng tin cậy dựa trên ba trọng điểm hành động: phát triển các nguyên tắc bảo vệ dữ liệu của khu vực; phát triển mạng lưới an ninh chung của khu vực cũng như việc phát triển cơ sở hạ tầng thông tin trong khu vực xuất phát từ thực tiễn thực hiện. Để đạt được điều này, sáng kiến đề xuất nhấn mạnh vào việc thiết lập những hướng dẫn khu vực, phát triển nguyên tắc cơ bản về bảo mật mạng lưới công nghệ thông tin cũng như tạo ra hệ thống cơ sở hạ tầng thông tin năng động và có tính tương tác cao.

Sáng kiến thứ hai là tăng cường hệ thống cảnh báo sớm về an ninh thông tin trong ASEAN với mục tiêu cải thiện các phản ứng và việc hợp tác trong những tình thế khẩn cấp trên không gian mạng của các quốc gia thành viên ASEAN, cũng như tăng cường hợp tác ứng phó khẩn cấp đối với sự cố mạng thông thường. Để đạt được mục đích này, sáng kiến sẽ khuyến khích hợp tác để tạo ra mạng lưới hoạt động hiệu quả với tên gọi "CERTs" (Computer Emergency Response Team) với khả năng phản hồi nhanh theo thời gian thực (real-time response) đối với các vi phạm về an ninh mạng.

2.2. Các thiết chế ngăn ngừa, phòng, chống tội phạm mạng của ASEAN

Tương tự như khuôn khổ pháp lí-chính trị, thiết chế chịu trách nhiệm trong lĩnh vực tội phạm công nghệ cao của ASEAN cũng bao gồm hai nhóm là các thiết chế chịu trách nhiệm chung trong phòng, chống tội phạm xuyên quốc gia và các thiết chế chịu trách nhiệm chuyên trách đối với loại tội phạm này.

Các thiết chế chịu trách nhiệm chung bao gồm: 1) Hội nghị Bộ trưởng ASEAN về tội phạm xuyên quốc gia (ASEAN Ministerial Meeting on Transnational Crime - AMMTC) là cơ quan hoạch định chính sách cao nhất về các vấn đề liên quan đến hoạt động hợp tác

(18). https://www.asean.org/storage/images/2015/November/ICT/15b%20--%20AIM%202020_Publication_ Final.pdf, truy cập 02/3/2021.

(19). Các chiến lược được đề ra trong Chiến lược tổng thể về công nghệ thông tin ASEAN năm 2020: 1) phát triển và chuyển đổi kinh tế; 2) hội nhập và trao quyền cho mọi người thông qua công nghệ thông tin; 3) đổi mới; 4) phát triển cơ sở hạ tầng công nghệ thông tin; 5) phát triển nguồn nhân lực; 6) vấn đề công nghệ thông tin trong một thị trường chung thống nhất; 7) phương tiện và nội dung mới; 8) vấn đề bảo mật và bảo đảm thông tin.

trong ngăn ngừa và phòng, chống tội phạm xuyên quốc gia của ASEAN; 2) Hội nghị quan chức cao cấp về tội phạm xuyên quốc gia (Senior Official Conference on Transnational Crime - SOMTC) là cơ quan hỗ trợ cho AMMTC trong việc thực hiện các chính sách và kế hoạch thông qua tại AMMTC, tăng cường hợp tác và phối hợp với các cơ quan khác của ASEAN, các cơ quan quốc tế có liên quan đến tội phạm xuyên quốc gia; 3) Hiệp hội Cảnh sát quốc gia ASEAN (ASEAN National Police Association - ASEANAPOL) là cơ quan phối hợp giữa các quốc gia thành viên trong lĩnh vực điều tra hình sự.

Nhóm thiết chế chuyên ngành trước tiên bao gồm Nhóm công tác về tội phạm mạng (Work Group on Cyber Crime - WGoCC), được thành lập theo quyết định của SOMTC lần thứ 13 năm 2013 trên cơ sở sáng kiến của Singapore nhằm cung cấp nền tảng cho các quốc gia thành viên trong việc xây dựng năng lực, đào tạo và chia sẻ thông tin liên quan đến chống tội phạm mạng cũng như xây dựng nền tảng cho quá trình thảo luận và thông qua cách tiếp cận phối hợp để đối phó với tội phạm mạng; theo dõi các khuyến nghị về tội phạm mạng từ các tổ chức có liên quan và tham gia hoạt động phối hợp với các bên đối thoại. WGoCC bao gồm đại diện của các quốc gia thành viên, họp định kì hàng năm và kết quả cuộc họp sẽ được báo cáo lên SOMTC.[(20)]

Phạm vi hoạt động của WGoCC bao gồm:

+ Tạo điều kiện cho hoạt động chia sẻ thông tin về tội phạm mạng như xu hướng, thực tiễn tốt nhất, công nghệ mới thông qua việc thiết lập khuôn khổ cho hoạt động chia sẻ thông tin giữa các thiết chế có liên quan của các quốc gia thành viên;

+ Thiết lập các điểm liên lạc thường xuyên trong hợp tác chống tội phạm mạng để tạo điều kiện cho việc phối hợp mạng lưới trong hợp tác thực thi và xây dựng năng lực;

+ Tăng cường năng lực trong phòng, chống tội phạm mạng thông qua việc phát triển các chương trình đào tạo khu vực và tổ chức các hội nghị định kì;

+ Xác định các lĩnh vực trọng tâm trong hoạt động phối hợp giữa ASEAN và các bên đối thoại liên quan đến tội phạm mạng và nghiên cứu những hoạt động hợp tác có thể tiến hành với các đối tác chiến lược tư nhân.

Ngoài WGoCC, do đặc thù của loại tội phạm mạng liên quan mật thiết với công nghệ - kĩ thuật cao nên bên cạnh các thiết chế hoạt động với tư cách là cơ quan về phòng, chống tội phạm còn bao gồm những cơ quan hoạt động trong lĩnh vực công nghệ thông tin với các nhiệm vụ có liên quan đến an ninh mạng, bao gồm:

Một là, Uỷ ban ASEAN về khoa học và công nghệ (ASEAN Committee for Science and Technology - COST), thành lập ngày 08/8/1967 với mục đích tăng cường hoạt động hợp tác và hỗ trợ lẫn nhau trong các vấn đề liên quan đến lợi ích chung về kinh tế, xã hội, văn hoá, khoa học, kĩ thuật, hành chính, đồng thời hỗ trợ đào tạo và tạo điều kiện cho hoạt động nghiên cứu về giáo dục, nghề nghiệp, kĩ thuật và quản lí hành chính. COST có nhiệm vụ: khởi xướng và tăng cường hợp tác khu vực trong các hoạt động

(20). *ASEAN Working Group on Cybercrime - Terms of reference,* http://ASEAN.org/storage/2012/05/DOC-8-Adopted-TOR-ASEAN-Cybercrime-Working-Group.pdf, truy cập 02/3/2021.

khoa học; xây dựng và thúc đẩy phát triển chuyên môn và nhân lực khoa học, công nghệ trong khu vực ASEAN; tạo điều kiện và thúc đẩy chuyển giao các phát triển khoa học, công nghệ giữa các nước ASEAN và từ các nước công nghiệp phát triển hơn sang khu vực ASEAN; trợ giúp, hỗ trợ trong việc áp dụng kết quả nghiên cứu và sử dụng hiệu quả nguồn tài nguyên thiên nhiên trong khu vực ASEAN cũng như hỗ trợ trong việc thực hiện những chương trình hiện tại và tương lai của ASEAN trong lĩnh vực khoa học, công nghệ.

Hai là Hội nghị Bộ trưởng Viễn thông và Công nghệ thông tin ASEAN (TELMIN), được thành lập năm 2001 chịu trách nhiệm chính trong việc xây dựng các chính sách, chương trình và hoạt động hợp tác về công nghệ thông tin trong ASEAN; thiết lập cơ sở hạ tầng công nghệ thông tin cho khu vực; phối hợp và hài hoà hoá các chương trình và chính sách viễn thông và công nghệ thông tin; thúc đẩy và phát triển nội dung viễn thông, kĩ thuật số; thúc đẩy sự tham gia của khu vực tư nhân và tăng cường hợp tác khu vực công - tư trong các chương trình và hoạt động hợp tác viễn thông khu vực; tăng cường hợp tác và tiếp cận chung trong việc giải quyết các vấn đề viễn thông và công nghệ thông tin trên phạm vi quốc tế và khu vực…[(21)] Hội nghị quan chức cao cấp về công nghệ thông tin và viễn thông ASEAN (ASEAN Telecom and Information Technology Senior Officials Meeting - TELSOM) và Hội đồng điều tiết viễn thông ASEAN (ASEAN Telecom Regulatory Council - ATRC) đảm nhiệm chức năng giám sát, phối hợp, thực hiện các chương trình, chính sách do TELMIN thông qua cũng như tư vấn cho cơ quan này.

2.3. Cơ chế hợp tác phòng, chống tội phạm mạng trong khuôn khổ ARF

Ngoài các thiết chế chịu trách nhiệm trực tiếp trong phòng, chống tội phạm mạng, Diễn đàn khu vực ASEAN (ASEAN Region Forrum - ARF) là kênh đối thoại chính thức ở cấp chính phủ nhằm thúc đẩy cơ chế đối thoại và tham vấn về các vấn đề an ninh, chính trị trong khu vực, được tạo ra bởi ASEAN và hiện có nhiều nỗ lực trong việc thúc đẩy các hoạt động hợp tác đấu tranh phòng, chống các loại hình tội phạm công nghệ cao trên thực tế. Một trong những mục đích của diễn đàn là tạo ra môi trường chính trị-an ninh ổn định; phát triển các biện pháp ngoại giao phòng ngừa và cũng không loại trừ hoạt động hợp tác đấu tranh phòng, chống tội phạm mạng, để ASEAN có thể trở thành khu vực vững mạnh hơn.

Hiện nay, ARF chưa hình thành được các văn kiện có giá trị ràng buộc, điều này xuất phát từ việc ARF không có đủ thẩm quyền và điều kiện cho phép khi chỉ tồn tại với tư cách là một diễn đàn hợp tác quốc tế. Song thực tế này không ảnh hưởng nhiều đến vai trò của ARF trong lĩnh vực đấu tranh phòng, chống tội phạm mạng. ARF hiện có 3 cơ chế để đấu tranh phòng, chống tội phạm mạng: *Một là* biện pháp xây dựng lòng tin (Confidence Building Measure - CBM) lẫn

(21). Ministerial Understanding on ASEAN Cooperation in Telecommunications and Information Technology Kuala Lumpur, 2001, https://ASEAN.org/?static_ post= ministerial-understanding-on-ASEAN-cooperation-in-telecommunications-and-information-technology-kuala-lumpur-13-july-2001, truy cập 10/4/2020.

nhau giữa các quốc gia thành viên ARF đối với tầm quan trọng của việc phát triển an ninh mạng; *Hai là* biện pháp ngoại giao phòng ngừa (Preventive Diplomacy - PD) nhằm tạo ra các biện pháp phòng ngừa đối với các mối đe dọa tiềm tàng của tội phạm mạng; *Ba là* biện pháp giải quyết xung đột (Conflict Resolutions - CR) nhằm mục đích tạo ra văn kiện điều chỉnh để giải quyết tranh chấp giữa các quốc gia hữu quan, trước mắt những văn kiện này có thể chỉ mang tính khuyến nghị nhưng các bên sẽ cố gắng tiệm cận dần đến tính ràng buộc về mặt pháp lí. Liên quan đến vấn đề an ninh mạng của khu vực có thể kể tới một số cam kết trong khuôn khổ ARF được thể hiện trong các văn kiện:

Thứ nhất, Tuyên bố ARF về đấu tranh phòng, chống tấn công mạng và tấn công khủng bố trái phép trên không gian mạng năm 2006 (ARF Statement On Fighting Cyber Attack And Terrorism Misuse Of Cyber Space 2006). Đây là tuyên bố chung của các quốc gia thành viên ARF nhằm nhấn mạnh các cam kết trong việc chung sức đồng lòng chiến đấu chống lại tất cả các dạng thức của khủng bố và tấn công mạng. Các quốc gia trong ARF đã nhận thấy rằng, tất cả các dạng thức hành động của khủng bố và tấn công mạng đều sử dụng không gian mạng làm công cụ để tiến hành hành vi phạm tội. Tuyên bố chung này còn nhấn mạnh vào hậu quả của việc sử dụng trái phép không gian mạng để tấn công nhằm vào hệ thống cơ sở hạ tầng thông tin truyền thông của các chính phủ. Khi đó, hậu quả không chỉ trực tiếp ảnh hưởng tới các chính phủ mà còn tác động gián tiếp tới nền kinh tế quốc dân nói chung và các cá nhân nói riêng. Vì vậy, văn kiện này cũng nhấn mạnh vào sự hợp tác giữa các quốc gia thành viên của ARF trong việc ngăn chặn các hành vi tội phạm và khủng bố có liên quan đến việc khai thác bất hợp pháp, lạm dụng nguồn tài nguyên khoa học, công nghệ và truyền thông mà chủ yếu là mạng internet.

Thứ hai, Tuyên bố chung của các Ngoại trưởng ARF về vấn đề hợp tác trong bảo đảm an ninh mạng năm 2012 (ARF Statement by The of Foreign Affairs On Cooperation In Ensuring Cyber Security)[22], 2012). Đây là văn kiện được tuyên bố bởi Bộ trưởng Bộ Ngoại giao của các quốc gia thành viên ARF với mục tiêu tái khẳng định những cam kết của quốc gia họ về vấn đề an ninh mạng. Thông qua văn kiện này, các quốc gia thành viên ARF thừa nhận rằng việc bảo đảm an toàn an ninh, bảo mật trong việc ứng dụng công nghệ thông tin là một trong những trụ cột chủ đạo trong quá trình tăng cường sự kết nối giữa các quốc gia thành viên. Chính vì thế, thực tế đòi hỏi một cam kết để khuyến khích, xây dựng và thực hiện các hành động nhằm kiểm soát, quản lí và loại trừ tất cả các dạng thức của tội phạm công nghệ mạng, góp phần đảm bảo an ninh mạng cho toàn khu vực. Văn kiện này cũng nhấn mạnh tới việc các quốc gia thành viên ARF khi thực hiện các hành động trong khuôn khổ tuyên bố chung phải đảm bảo phù hợp với các văn kiện trước đó, đặc biệt là Tuyên bố ARF về đấu tranh phòng, chống tấn công mạng và tấn công khủng bố trái phép trên không gian mạng năm 2006.

(22). https://aseanregionalforum.asean.org/wp-content/uploads/2019/01/ARF-Statement-on-Cooperation-in-Ensuring-Cyber-Security.pdf, truy cập 03/02/2021.

ARF là diễn đàn đối thoại sử dụng an ninh hợp tác như một cách tiếp cận để tăng cường mối quan hệ giữa các quốc gia thành viên ASEAN với các đối tác đối thoại của ASEAN. Phát triển quan hệ đối tác an ninh khu vực là một trong những chương trình nghị sự chính của ARF, trong đó quan hệ đối tác trong việc xây dựng trật tự an ninh dựa trên sự đồng thuận giữa các chính phủ trong công tác hợp tác xử lí các mối đe dọa an ninh đang hiện hữu. Để ARF trở thành diễn đàn trong việc tạo ra sự an toàn cho an ninh mạng ở khu vực ở Đông Nam Á, ASEAN cần tối ưu hoá vai trò của mình với các đối tác như Trung Quốc, Nhật Bản và Liên minh châu Âu... Trên thực tế, ASEAN hiện đã đạt được những kết quả hợp tác ban đầu với các đối tác như: Biên Bản ghi nhớ giữa ASEAN và Chính phủ Cộng hoà nhân dân Trung Hoa về hợp tác trong các vấn đề an ninh phi truyền thống năm 2009 (Cooperation in The Field of Non-Traditional Security Issues 2009);[(23)] Tuyên bố chung ASEAN-Nhật Bản về hợp tác chống khủng bố và tội phạm xuyên quốc gia năm 2014 (Declaration For Cooperation to Combat Terrorism and Transnational Crime 2014);[(24)] Tuyên bố Nuremberg về tăng cường quan hệ đối tác giữa EU-ASEAN năm 2007 (Nuremberg Declaration on an EU-ASEAN Enhanced Partnership 2007).[(25)]

3. Nhận định về hạn chế và kiến nghị một số giải pháp nâng cao hiệu quả công tác hợp tác đấu tranh, phòng chống tội phạm mạng của ASEAN

3.1. Hạn chế trong hợp tác đấu tranh phòng chống tội phạm mạng của ASEAN

Thứ nhất, trong lĩnh vực phòng, chống tội phạm mạng, ASEAN hiện chưa có điều ước quốc tế về vấn đề này. Tuyên bố của ASEAN về phòng, chống tội phạm mạng, xét về mặt pháp lí, là không phải văn bản có giá trị pháp lí ràng buộc. Xét về mặt nội dung, văn bản này chỉ mang tính chất định khung trong việc định hướng hoạt động của ASEAN. Trước mắt, đây được coi là cách tiếp cận tương đối linh hoạt của ASEAN để có thể tìm ra được những giải pháp chung cho các vấn đề quan trọng trong khi vẫn tồn tại những trở ngại từ vấn đề chủ quyền cũng như sự khác biệt trong quan điểm của các quốc gia về tội phạm công nghệ cao. Đây có thể không phải là vấn đề cần ưu tiên của các thành viên mới gia nhập và kém phát triển hơn. Trong khi các quốc gia thành viên phát triển hơn về kinh tế đang hưởng lợi ích lớn từ việc tiếp cận công nghệ tiên tiến nên rất quan tâm tới việc tập trung nguồn lực giải quyết loại tội phạm này.[(26)] Tuy vậy, xét trên phương diện pháp lí tổng thể, một văn bản khung không có giá trị pháp lí ràng buộc không thể là cơ sở nền tảng vững chắc cho hoạt động ngăn ngừa, phòng, chống các loại

(23). https://asean.org/storage/2012/05/MoU-ASEAN-China-on-NTS-2017-2023.pdf, truy cập 03/02/2021.

(24). https://www.asean.org/storage/images/pdf/ 2014_upload/ASEAN-Japan%20JD%20on%20 CTTC.pdf, truy cập 13/02/2021.

(25). https://ec.europa.eu/commission/presscorner/detail/en/PRES_07_54, truy cập 03/02/2021.

(26). *ASEAN Matters: Reflecting on the Association of Southeast Asian Nations*, edited by Yoong Yoong Lee, World Scientific Publishing Co Pte Ltd, 2014, tr. 83, ProQuest Ebook Central, http://ebookcentral. proquest. com/lib/monash/detail.action?docID= 840723, truy cập 03/4/2018.

hình tội phạm công nghệ cao của ASEAN. Các văn kiện khác về hoạt động đấu tranh phòng, chống tội phạm mạng phần nhiều là các tuyên bố chính trị không có tính ràng buộc đối với các quốc gia thành viên. Dù rằng các văn kiện "luật mềm" cũng có vai trò nhất định trong việc dẫn dắt xu hướng và định hình các quy phạm pháp luật trong tương lai, tuy nhiên, bằng cách này hay cách khác, chính điều này sẽ làm suy giảm đáng kể hiệu quả thực hiện các cam kết về phòng, chống tội phạm mạng trong ASEAN. Hơn nữa, khi đi sâu vào nội dung các cam kết được ghi nhận của các văn kiện này (bao gồm cả văn kiện pháp lí và văn kiện chính trị), các biện pháp phòng, chống tội phạm mạng được các bên cam kết cũng chỉ là cơ chế hợp tác mềm (soft mechanism of cooperation) như trao đổi thông tin, thiết lập mạng lưới, tập huấn, chia sẻ kinh nghiệm[(27)]...

Thứ hai, về mặt thiết chế, vai trò của các cơ quan tiến hành hoạt động đấu tranh, phòng, chống tội phạm mạng của ASEAN còn mờ nhạt, chưa thực sự phát huy tối đa khả năng của mình. Mặc dù đã có sự phân cấp các thiết chế có trách nhiệm chung và chuyên trách song do chưa được trao nhiều quyền hạn có tính thực chất[(28)] và việc hoạt động theo kì họp thông thường được tổ chức thường niên nên đa phần các thiết chế không đáp ứng được tính hiệu quả và cấp thiết trong trường hợp khẩn cấp, đặc biệt trong bối cảnh tội phạm mạng có thể diễn phức tạp, tinh vi và khả năng xoá dấu vết vô cùng nhanh chóng...

Thứ ba, về hoạt động hợp tác trao đổi thông tin liên quan đến tội phạm mạng giữa các quốc gia trong ASEAN và với các đối tác ngoài khu vực chưa được tiến hành thường xuyên. Điều này gây ra tác động tiêu cực đến công tác hợp tác đấu tranh phòng, chống tội phạm mạng, mà điển hình là sự thiếu cập nhật của hệ thống dữ liệu và không tối ưu hoá được vai trò của tổ chức trong mối quan hệ với các đối tác ngoại khối vốn có nhiều kinh nghiệm trong vấn đề này.

Thứ tư, về hài hoà hoá pháp luật hình sự về tội phạm mạng chưa nhận được sự quan tâm từ các quốc gia ASEAN. Hài hoá pháp luật về hình sự hiện nay tồn tại theo hai cấp độ. Theo mức độ phổ biến là hình sự hoá những hành vi nhất định để tạo cơ sở pháp lí cho việc truy cứu trách nhiệm hình sự cũng như tiến hành các hoạt động dẫn độ, tương trợ tư pháp hình sự khi cần thiết. Với các khu vực có cấp độ liên kết cao giữa các quốc gia thành viên, mức độ hài hoà hoá còn bao gồm cả hài hoà hoá về hình phạt, tức là quy định mức hình phạt tối thiểu đối với mỗi hành vi vi phạm nhất định nhằm tạo ngưỡng chung trong xử lí hình sự những hành vi tội phạm tại tất cả các quốc gia thành viên, điển hình ở mức độ này là Liên minh châu Âu.

(27). Michaeal J.Green & Bates Gill, *Asia's news multilateralism cooperation, competition and the search for Community,* Columbia Univeristy Press, New York, The United States of America, 2009, p. 35 - 38, https://books.google.ps/books?id=-FesAgAAQ B A J&printsec=frontcover&hl=vi#v=onepage&q&f= false, truy cập 03/3/2021.

(28). Bùi Thị Ngọc Lan, "Thực trạng và giải pháp nâng cao hiệu quả của hoạt động phòng, chống tội phạm xuyên quốc gia trong khuôn khổ Asean", *Tạp chí Nghiên cứu lập pháp* số 18 (394), tháng 9/2019 http://lapphap.vn/Pages/tintuc/tinchitiet.aspx?tintucid =210406, truy cập 01/4/2021.

Tuy nhiên, mức độ hài hoá pháp luật tại khu vực ASEAN hiện nay mới chỉ dừng lại ở cấp độ hình sự hóa các hành vi. Với cấp độ thứ nhất, hình sự hoá những hành vi để tạo cơ sở pháp lí cho việc truy cứu trách nhiệm hình sự, hiện đã có tới chín trên mười quốc gia ASEAN ban hành luật riêng về phòng chống tôi phạm mạng. Lào mới chỉ ban hành Luật về phòng chống tội phạm mạng vào tháng 9/2014 (law on prevention and combating cybercrime). Campuchia đến thời điểm này vẫn chưa ban hành luật riêng về phòng chống tội phạm mạng.

Trong trường hợp của Việt Nam, một số thuật ngữ có cùng nội hàm đã được sử dụng trong các văn bản pháp luật của Việt Nam hiện nay như: tội phạm công nghệ cao; tội phạm sử dụng công nghệ cao; tội phạm mạng; tội phạm an ninh mạng; tấn công mạng; khủng bố mạng; gián điệp mạng. Trong Luật An ninh mạng năm 2018, Điều 2 đã cắt nghĩa về loại hình "tội phạm mạng" và đặt trong mối tương quan với hàng loạt các hành vi vi phạm khác được tiến hành trên không gian mạng nhưng chưa có bất kì văn bản hướng dẫn nào giải thích, phân biệt làm sáng rõ hơn các loại hình vi phạm này cũng như mối tương quan trong việc áp dụng với các văn bản pháp luật khác có liên quan. Trong Bộ luật Hình sự năm 2015 không sử dụng thuật ngữ "tội phạm công nghệ cao" hay "tội phạm mạng" mà quy định theo cách thức liệt kê. Cách thức quy định theo phương pháp định dạng liệt kê như vậy hoàn toàn có khả năng bỏ sót các loại hình tội phạm công nghệ cao vốn đang có những biến tướng cực kì phức tạp và đặc biệt chưa tương thích với cách tiếp cận của các văn kiện pháp lí của ASEAN cũng như các văn bản luật khác có liên quan.

Cách tiếp cận về tội phạm công nghệ cao của Việt Nam có thể không khác biệt so với quy chuẩn trong các cam kết quốc tế của khu vực ASEAN, tuy nhiên việc không thống nhất trong việc sử dụng thuật ngữ cũng như phạm vi hình sự hoá chưa đảm bảo tính "bao phủ" sẽ phần nào ảnh hưởng tới quá trình hài hoà hoá pháp luật, cản trở việc thực thi các cam kết của Việt Nam với tư cách là quốc gia thành viên tham gia tích cực và có trách nhiệm trong các khuôn khổ hợp tác của ASEAN nói chung và hợp tác trong lĩnh vực phòng, chống tội phạm nói riêng.

3.2. Một số giải pháp nâng cao hiệu quả hoạt động đấu tranh, phòng, chống tội phạm mạng trong khuôn khổ ASEAN

Cho tới thời điểm hiện nay, ASEAN đã và đang từng bước xây dựng cơ chế về phòng, chống tội phạm mạng với hệ thống các văn kiện pháp lí, trong đó có những văn kiện có hiệu lực pháp lí ràng buộc và một số văn kiện mang tính khuyến nghị cũng như các cơ quan, thiết chế với sự phân định rõ ràng và cụ thể về chức năng, nhiệm vụ, quyền hạn. Trong tình hình mới, nền tảng của cơ chế này góp phần không nhỏ trong cuộc chiến phòng, chống tội phạm mạng nói riêng và các loại hình tội phạm công nghệ cao nói chung - vốn mang tính chất phức tạp và ngày càng tinh vi. Bên cạnh đó, công tác trao đổi thông tin cũng là một trong những "điểm sáng" trong hoạt động phòng, chống tội phạm mạng của ASEAN. ASEAN hiện đã xây dựng được hệ thống cơ sở dữ liệu về tội phạm xuyên quốc gia, trong đó có thư mục về tội phạm mạng, góp phần tạo thuận

lợi cho việc trao đổi thông tin giữa các cơ quan chức năng của các quốc gia hữu quan diễn ra một cách chính xác, thuận tiện và có độ bảo mật cao. Hiện nay, hệ thống cơ sở dữ liệu về tội phạm mạng trong ASEAN được xây dựng và nâng cấp trên cơ sở hệ thống cơ sở dữ liệu thông tin cảnh sát các nước ASEAN (ADS) đã có từ năm 1992. Vào năm 2006, theo sáng kiến của Singapore, ADS được nâng cấp thành hệ thống cơ sở dữ liệu điện tử (e-ADS) với nhiều sự lưu tâm hơn đối với các dạng thức tội phạm công nghệ cao nhằm hỗ trợ các quốc gia thành viên trao đổi và chia sẻ thông tin phòng, chống tội phạm mạng một cách nhanh chóng và kịp thời.(29)

Tuy nhiên với những hạn chế trong hợp tác phòng, chống tội phạm mạng đã phân tích ở trên, tác giả đề xuất một số giải pháp cho khu vực này để thúc đẩy và thiết lập có hiệu quả cơ chế hợp tác trong phòng, chống tội phạm mạng, cụ thể như sau:

Một là trong thời gian sắp tới, ASEAN cần thực hiện đồng bộ một số giải pháp liên quan đến việc tăng cường "pháp lí hoá" các văn kiện có tính chính trị hiện tại để tạo ra cam kết có tính ràng buộc về quyền và nghĩa vụ đối với các quốc gia thành viên ASEAN, tạo cơ sở vững chắc đối với hoạt động đấu tranh phòng, chống tội phạm mạng với mục tiêu hướng tới một văn kiện điều ước quốc tế khu vực điều chỉnh tổng quát về tội phạm mạng cũng như hoạt động hợp tác quốc tế phòng, chống loại hình tội phạm này.

Hai là ASEAN cần siết chặt hơn nữa cơ chế đảm bảo thực thi các cam kết hiện tại và trong tương lai của các quốc gia thành viên ASEAN liên quan đến phòng, chống tội phạm mạng thay vì cơ chế điều phối hiện thời; cùng với đó, tối ưu hoá công tác báo cáo hoạt động thực thi và tăng cường trách nhiệm của các quốc gia thành viên đối với các văn kiện pháp lí của khu vực. Đặc biệt, ASEAN sẽ phải củng cố hơn nữa vai trò của các thiết chế hiện hành trên cơ sở nguyên tắc "tăng quyền, giảm lập"; tức là hạn chế hình thành thiết chế mới, tránh làm "cồng kềnh" bộ máy mà hướng tới việc trao thêm quyền hạn cho những thiết chế hiện có thể hoạt động một cách thường trực, góp phần hỗ trợ cho các cơ quan hoạt động theo kì họp của ASEAN trong khoảng thời gian không diễn ra cuộc họp để ứng phó kịp thời với các tình huống khẩn cấp và quan trọng về phòng, chống tội phạm mạng nói riêng và các loại hình tội phạm công nghệ cao nói chung.

Ba là với diễn biến tinh vi, phức tạp của tội phạm, việc cập nhật thường xuyên hệ thống cơ sở dữ liệu tội phạm mạng thông qua việc nâng cấp hệ thống kĩ thuật là điều vô cùng quan trọng, góp phần tăng cường trao đổi thông tin thông qua những kênh liên lạc hiện có như cơ sở dữ liệu điện tử của ASEANAPOL, hệ thống cơ sở dữ liệu về tội phạm của INTERPOL, đồng thời thiết lập các kênh trao đổi thông tin mới hiệu quả hơn giữa các cơ quan hợp tác chuyên ngành của các quốc gia thành viên.

Tóm lại, để đạt được cấu trúc an ninh mạng vững mạnh cho toàn khu vực nhằm đương đầu với các thách thức an ninh phi

(29). Nguyễn Kim Ngân, Nguyễn Đức Phúc, "Hiệp hội cảnh sát các nước ASEAN - Mô hình hợp tác quốc tế đấu tranh chống tội phạm xuyên quốc gia", *Tạp chí Luật học*, số 9/2009, tr 27-33.

truyền thống đang hiện hữu, các quốc gia thành viên ASEAN cần xây dựng và triển khai khuôn khổ pháp lí toàn diện, có khả năng dự báo và có tính phối hợp linh hoạt hơn nữa. Để đạt được điều này, cần tới sự thấu hiểu, thông cảm và chia sẻ lẫn nhau giữa các quốc gia thành viên ASEAN về tầm quan trọng của việc đưa ARF trở thành tổ chức quốc tế có tư cách chủ thể luật quốc tế và có thẩm quyền pháp lí./.

TÀI LIỆU THAM KHẢO

1. Yoong Yoong Lee, *ASEAN Matters: Reflecting on the Association of Southeast Asian Nations*, World Scientific Publishing Co Pte Ltd, 2014.
2. Bima Yudha Wibawa Manopo, Diah Apriani Atika Sari, *ASEAN Regional Forum - Realizing regional cyber security in ASEAN region*, *Belli Ac Pacis*, 2015.
3. Michael Raska, Benjamin Ang, *Cybersecurity in Southeast Asia*, Note de présentation n°5/8 de l'Observatoire Asie du Sud-Est, cycle 2018-2019 Mai, 2018, https://centreasia.eu/wp-content/uploads/2018/12/NotePrésentation-AngRaska-Cybersecurity_180518.pdf.
4. Nguyễn Kim Ngân, Nguyễn Đức Phúc, "Hiệp hội cảnh sát các nước ASEAN - Mô hình hợp tác quốc tế đấu tranh chống tội phạm xuyên quốc gia", *Tạp chí Luật học*, số 9/2009.
5. Michaeal J.Green & Bates Gill, *Asia's news multilateralism cooperation, competition and the search for Community*, Columbia Univeristy Press, New York, The United States of America, 2009.

VAI TRÒ VÀ THÁCH THỨC ĐỐI VỚI VIỆT NAM... ***(tiếp theo trang 70)***

22. *Joint Statement of the U.S.-ASEAN Special Leaders' Summit: Sunnylands Declaration*, Sunnylands, California, February 15-16, 2016.
23. Lao Statistics Bureau, *Statistical Yearbook 2017*, Vientiane Capital, June 2018.
24. Ministry of Planning and Finance (The Government of the Republic of the Union of Myanmar), *2018 Myanmar Statistical Yearbook*.
25. Mohan Malik, *The East Asia Summit*, Australian Journal of International Affairs, Vol. 60, No. 2, 2006,.
26. Prashanth Parameswaran, *China, Not ASEAN, the Real Failure on South China Sea at Kunming Meeting*, The Diplomat, June 16, 2016.
27. *Prime Ministern (N. Modi)'s remarks at the 9th East Asia Summit*, Nay Pyi Taw, Myanmar, November 13, 2014.
28. *Remarks by the Prime Minister (N. Modi) at 12th India-ASEAN Summit*, Nay Pyi Taw, Myanmar, November 12, 2014.
29. Rodolfo C. Severino, *ASEAN and the South China Sea*, Security Challenges, Vol.6, No.2, 2010.
30. *Singapore Declaration of 1992 Singapore*, January 28, 1992.
31. *The 1992 ASEAN Declaration on the South China Sea*, Manila, July 22, 1992.
32. Võ Xuân Vinh, "Nguyên tắc đồng thuận của ASEAN: Vai trò và những thách thức đối với ngăn ngừa xung đột ở Biển Đông", *Tạp chí Nghiên cứu Đông Nam Á,* số 8/2017.