Kinh nghiệm một số quốc gia ở châu Á trong bảo đảm an ninh truyền thông

PGS, TS. NGUYỄN THỊ TRƯỜNG GIANG
Học viện Báo chí và Tuyên truyền; Email: truonggiangptth.ajc@gmail.com

Nhận ngày 15 tháng 5 năm 2023; chấp nhận đăng tháng 6 năm 2023.

Tóm tắt: *Bảo đảm an ninh truyền thông luôn được coi là một trong những nhiệm vụ quan trọng trong chiến lược bảo vệ nền an ninh, ổn định chính trị và phát triển kinh tế của các quốc gia, trong đó có Việt Nam. Đứng trước tính chất và diễn biến ngày càng phức tạp của những mối đe dọa an ninh truyền thông, các quốc gia đã và đang ban hành nhiều đạo luật và triển khai chương trình hành động nhằm đấu tranh, đẩy lùi sự xâm phạm từ trong nước và nước ngoài. Kinh nghiệm của một số quốc gia châu Á trong đảm bảo an ninh truyền thông là cơ sở thực tiễn để Việt Nam bổ sung, hoàn thiện và thực thi hiệu quả chính sách, pháp luật ban hành.*
Từ khóa: *an ninh truyền thông; châu Á; chính sách; luật; báo chí; truyền thông.*

Abstract: *Ensuring communication security is always considered as one of the important tasks in the strategy of protecting security, political stability and economic development of countries, including Vietnam. Facing the increasingly complexity and evolution of communication security threats, countries have been promulgating many laws and implementing action plans to fight and repel intrusions domestically and abroad. The experience of some Asian countries in ensuring communication security is a practical basis for Vietnam to supplement, perfect and effectively implement promulgated policies and laws.*
Keywords: *communication security; Asia; policy; law; press; communication.*

Theo tập đoàn công nghệ IBM, tội phạm mạng có thể gây thiệt hại cho nền kinh tế thế giới khoảng 10 nghìn tỷ USD mỗi năm cho đến năm 2025. Trong thời đại bùng nổ của Internet, chỉ tính đến các dịch vụ mạng xã hội, châu Á là khu vực có lượng người dùng cao nhất thế giới, theo sau đó lần lượt là các quốc gia thuộc khu vực châu Mỹ, châu Âu, châu Phi[1],...Đây là cơ hội để các tội phạm mạng thực hiện hành vi phạm pháp, đồng thời tạo ra thách thức đối với việc quản lý thông tin, xuất bản trên không gian mạng. Nhận thức được tầm quan trọng của an ninh truyền thông đối với sự ổn định chính trị và phát triển kinh tế, tới nay đã có khoảng 140 quốc gia xây dựng và ban hành các quy định cụ thể liên quan đến đảm bảo an ninh mạng, quản lý thông tin trên các kênh báo chí, truyền thông và hoạt động của tổ chức và cá nhân trên Internet. Các quốc gia châu Á như Trung Quốc, Nhật Bản từ cuối những năm 90 của thế kỷ XX đã xây dựng hệ thống chính sách, pháp luật nhằm tăng cường công tác đảm bảo an ninh truyền thông trước sự phát triển của công nghệ, toàn cầu hoá, biến động trong quan hệ chính trị giữa các quốc gia và các vấn đề nội tại.

1. Trung Quốc

Trung Quốc là một trong những quốc gia quản lý chặt chẽ và nghiêm ngặt các hoạt động báo chí, xuất bản, thông tin, truyền thông trên Internet. Sau 30 năm cải cách đổi mới, Trung Quốc từng bước hoàn thiện hành lang pháp lý quản lý báo chí, truyền thông mang đặc sắc Trung Quốc theo nguyên tắc: Đảng lãnh đạo, Chính phủ quản lý, doanh nghiệp kinh doanh hợp pháp, lấy báo Đảng làm trọng tâm, phát triển theo cơ chế thị trường xã hội chủ nghĩa[2]. Chính phủ Trung Quốc không cho phép báo chí tư nhân hoạt động, các cơ quan truyền

thông nước ngoài phải có tổng biên tập mang quốc tịch Trung Quốc, sống tại Trung Quốc. Đồng thời, chính quyền Trung Quốc được phép có cổ phần đặc biệt để trở thành thành viên trong hội đồng quản trị của chi nhánh đặt tại Trung Quốc.

Về hoạt động xuất bản, theo báo cáo của Bộ Thông tin và Truyền thông năm 2022[3], các nhà xuất bản ở Trung Quốc hoạt động dưới nhiều loại hình tổ chức như: Cơ quan xuất bản của Đảng, nhà xuất bản là doanh nghiệp, trong đó có mô hình tập đoàn xuất bản phụ trách cả báo chí, truyền thông. Điều 4 Điều lệ quản lý xuất bản do Quốc vụ viện Trung Quốc công bố quy định: "Hoạt động xuất bản phải đặt lợi ích xã hội lên hàng đầu, thực hiện sự kết hợp giữa lợi ích xã hội với lợi ích kinh tế." Hoạt động xuất bản phải kiên định định hướng phục vụ nhân dân, phục vụ Chủ nghĩa xã hội, thực hiện quan điểm phát triển, truyền bá tích lũy tri thức khoa học, công nghệ và văn hóa, thúc đẩy giao lưu văn hóa quốc tế, làm phong phú đời sống tinh thần của nhân dân[4].

Đối với báo chí truyền thống, cuộc cải tổ được bắt đầu từ thời kỳ cải cách kinh tế do Đặng Tiểu Bình khởi xướng vào cuối những năm 1970. Hệ thống cơ quan báo chí truyền thống của Trung Quốc bao gồm các tờ báo, đài phát thanh - truyền hình từ trung ương tới địa phương và được phép mở rộng về số lượng tờ báo, kênh truyền hình - phát thanh nhằm đem đến cho công chúng nhiều sự lựa chọn hơn. Bắt đầu từ báo in được quản lý theo kiểu doanh nghiệp và cơ chế thị trường, sau đó là đến phát thanh, truyền hình. Các tờ báo tự tổ chức phân phối sản phẩm của mình thay vì phân phối báo chí độc quyền qua bưu điện như trước đây.

Từ năm 1997, Chính phủ Trung Quốc đã ban hành nhiều chính sách quan trọng nhằm quản lý và kiểm duyệt Internet và mạng xã hội, trong đó ban hành Quy chế "Quy định về việc quản lý và đảm bảo an toàn an ninh mạng và thông tin máy tính", chỉ đạo Bộ Công an Trung Quốc triển khai và giám sát việc thực hiện quy chế này. Trung Quốc cũng thực hiện dự án Golden Shield (tạm dịch là "Lá chắn vàng") để giám sát và kiểm duyệt thông tin của người sử dụng Internet. Dự án được khởi công năm 1998 và đưa vào hoạt động năm 2003. Khi phát hiện những nội dung, thông tin nhạy cảm được đăng tải trên Internet hoặc gửi qua thư điện tử, hệ thống "Lá chắn vàng" sẽ yêu cầu cơ quan quản lý nhà nước chuyên ngành can thiệp[5]. Các nội dung nhạy cảm về chính trị trên mạng điện thoại di động ở Trung Quốc cũng được yêu cầu sàng lọc và xóa bỏ.

Nằm trong khuôn khổ Dự án "Lá chắn vàng", năm 1998, Bộ Công an Trung Quốc đã triển khai dự án "Great Firewall" (Phòng hỏa trường thành hay Tường lửa vĩ đại) nhằm điều chỉnh Internet trong nước. Great Firewall phát huy hiệu quả trong ngăn chặn việc truy nhập tới nội dung không được phép, đồng thời giám sát và kiểm duyệt người dùng mạng Internet.

Bên cạnh việc quản lý nội dung trên Internet luật pháp và công nghệ, Bộ Công an Trung Quốc còn thành lập đội "Cảnh sát mạng" và "tình nguyện viên cảnh sát mạng" nhằm tăng cường kiểm duyệt các nội dung nhạy cảm, tiêu cực, tác động xấu đến xã hội như gian lận, lừa đảo, khiêu dâm, đặc biệt là tội phạm, khủng bố trên không gian mạng. Hiện có khoảng 50.000 cảnh sát mạng và gần 2 triệu tình nguyện viên đồng hành, thậm chí có cả nhân viên ở nước ngoài hỗ trợ theo dõi và hướng dẫn việc sử dụng Internet của người dân; giúp các cơ quan bảo mật mạng kịp thời phát hiện các lỗ hổng; ngăn chặn các chủ đề, hình ảnh độc hại và góp phần lan toả những thông tin tích cực; hỗ trợ cảnh sát bảo vệ an ninh mạng. Bộ Công an Trung Quốc còn lập các đơn vị cảnh sát an ninh mạng tại các tập đoàn công nghệ lớn như Alibaba, Tencent, Baidu nhằm hỗ trợ các công ty này quản lý an ninh mạng.

Chính phủ Trung Quốc còn tuyển dụng nhiều chuyên gia để theo dõi và giám sát hoạt động của các phương tiện truyền thông, mạng xã hội, thường xuyên gửi các báo cáo về các nội dung, bài viết trên mạng, các từ khoá được tìm kiếm nhiều nhất...

Tháng 11/2016, "Đạo luật về an ninh mạng" (Cybersecurity Law) được Quốc hội Trung Quốc thông qua và có hiệu lực từ ngày 01/6/2017 đã giúp cho không gian mạng của Trung Quốc được kiểm soát rất chặt chẽ. Toàn bộ hệ thống mạng Internet ở Trung Quốc đã trở thành "Chinternet" do nhà

nước kiểm soát chặt cả về nội dung, mạng lưới kết nối, dịch vụ, ứng dụng và các kênh giao tiếp. Người dùng mạng xã hội chia sẻ thông tin và bình luận nhạy cảm, sai sự thật có thể bị phạt tù từ 5 ngày đến 11 năm tuỳ vào mức độ nghiêm trọng của vụ việc. Các công ty nước ngoài phải lắp đặt máy chủ tại Trung Quốc. Người dùng Internet phải đăng ký các dịch vụ trên mạng với tài khoản định danh, và dự kiến được kết nối hệ thống chấm điểm công dân.

Ngoài ra, Trung Quốc còn tăng cường sử dụng những KOL (Key Leader Opinion - những người có tầm ảnh hưởng) như người nổi tiếng, các chính khách để họ trao đổi, nói chuyện, dẫn dắt dư luận trên các diễn đàn, blog, nhằm hình thành "kỷ luật tự giác" của người sử dụng mạng.

Song song với hệ thống báo chí, truyền thông phục vụ nhu cầu trong nước, hệ thống báo chí đối ngoại của Trung Quốc cũng góp phần đưa hình ảnh Trung Quốc ra thế giới, góp phần đảm bảo an ninh truyền thông.

2. Nhật Bản

Ở Nhật Bản, Chính phủ không có cơ quan chuyên trách quản lý báo chí nhưng về phương diện nghề nghiệp, *Hiệp hội báo chí Nhật Bản* lại phát huy chức năng giám sát, uốn nắn, rút kinh nghiệm nếu có tờ báo hay nhà báo nào vi phạm đạo đức nghề báo.

Liên quan đến an ninh mạng, Nhật Bản đã ban hành nhiều đạo luật như: Đạo luật Cấm truy cập máy tính trái phép năm 1999; Đạo luật Bảo vệ thông tin cá nhân năm 2003; Đạo luật cơ bản về an ninh mạng năm 2014; Các đạo luật này quy định các nguyên tắc cơ bản của chính sách an ninh mạng quốc gia; trách nhiệm của Chính phủ Nhật Bản, chính quyền địa phương và các bên liên quan khác cũng như các vấn đề quan trọng về chính sách an ninh mạng. Ngoài các đạo luật trên, Nhật Bản còn ban hành Luật Cơ bản về An ninh mạng nhằm ứng phó với những thay đổi trong nước và các vấn đề toàn cầu, trong đó có có sự gia tăng của các mối đe dọa liên quan đến an ninh mạng, xây dựng hệ thống Internet và hệ thống thông tin, truyền thông hiện đại khác. Luật này quy định các nguyên tắc cơ bản của chính sách an ninh mạng quốc gia thông qua việc làm rõ trách nhiệm của các bên liên quan như: nhà cung cấp hạ tầng thông tin trọng yếu, các cơ quan, tổ chức có hoạt động sản xuất, kinh doanh liên quan đến không gian mạng và các doanh nghiệp khác, các tổ chức nghiên cứu và giáo dục, công dân Nhật Bản trong bảo vệ an ninh mạng[6]. Nội dung đạo luật này cũng hướng đến việc xây dựng chiến lược an ninh mạng, thành lập Ban Chiến lược An ninh mạng.

Bên cạnh việc tạo hành lang pháp lý cho hoạt động bảo vệ an ninh mạng, Nhật Bản cũng tập trung đầu tư cho yếu tố con người. Kể từ năm 2017, Nhật Bản cung cấp một khoản hỗ trợ cho các chuyên gia an ninh mạng, yêu cầu các cơ quan chính phủ đề ra kế hoạch bồi dưỡng về an ninh mạng. Các chuyên gia ưu tú sẽ được chuyển đến Trung tâm An ninh mạng Nội các (NISC), các doanh nghiệp tư nhân để thực hiện nhiệm vụ giám sát các hoạt động tấn công mạng nhằm vào Chính phủ Nhật Bản[7].

3. Hàn Quốc

Hàn Quốc là một trong những quốc gia có hệ thống cơ quan báo chí, truyền thông và Internet phát triển mạnh nhưng không nằm ngoài sự kiểm duyệt chặt chẽ của Chính phủ. Điều 5 và 7, *Luật An ninh Quốc gia* cấm lưu trữ, tái xuất bản các ấn phẩm có ảnh hưởng tiêu cực đến an ninh quốc gia. Theo Điều 47 của *Luật Truyền thông Điện tử*, việc sản xuất và lưu hành các bài báo sai sự thật là vi phạm pháp luật và có thể bị phạt tù từ 4 năm. Hàn Quốc nghiêm cấm đăng tải, lan truyền các thông tin liên quan đe dọa đến an ninh quốc gia và người dân trên không gian mạng, kể cả khi những thông tin này là chính xác[8].

Để kiểm soát các thông tin xấu, độc, có nội dung chống phá chính quyền trên Internet, Chính phủ Hàn Quốc yêu cầu các doanh nghiệp cung cấp dịch vụ Internet và mạng xã hội phải chặn các website "đen" trong danh sách của Chính phủ; các cơ sở cung cấp dịch vụ truy cập Internet công cộng phải cài đặt các phần mềm lọc nội dung.

Bên cạnh đó, Hàn Quốc cũng bảo vệ nghiêm ngặt thông tin cá nhân của công dân. Theo Luật Bảo vệ thông tin cá nhân năm 2011, tất cả các công

ty cung cấp dịch vụ viễn thông phải lưu trữ dữ liệu cá nhân người dùng trong nước. Tất cả các cá nhân, tổ chức, công ty, thậm chí là các cơ quan nhà nước sử dụng thông tin cá nhân vì mục đích kinh doanh đều bị xử lý theo quy định của luật này.

Để quản lý chặt chẽ hoạt động truyền thông, đặc biệt là hoạt động truyền thông mới, Hàn Quốc trao thẩm quyền quản lý cho nhiều cơ quan quản lý nhà nước chuyên ngành như Bộ Thông tin, Văn phòng Phủ Tổng thống về các vấn đề chính trị, Văn phòng Người phát ngôn của Tổng thống và Ủy ban Phát thanh truyền hình. Bên cạnh đó, để bảo đảm thông tin đưa đến người dân khách quan, trung thực, minh bạch và công bằng, Chính phủ Hàn Quốc đã thành lập Ủy ban Thẩm định truyền hình - truyền thông vào năm 1981. Nhiệm vụ chính của Ủy ban Thẩm định truyền hình - truyền thông là thẩm định tính công bằng, chính trực về nội dung của các sản phẩm truyền hình - truyền thông; phòng, chống các nội dung thiếu đạo đức trên Internet; nghiên cứu, đề xuất và xây dựng các chính sách quản lý, giám sát truyền hình - truyền thông Hàn Quốc; phát triển các dự án truyền thông hợp tác trong nước, quốc tế. Ngoài nhiệm vụ quan trọng trên, Ủy ban tổ chức các khóa đào tạo, vận động và các hoạt động khác liên quan[9]. Chính sự phối hợp chặt chẽ giữa các cơ quan quản lý nhà nước về truyền thông đã góp phần phát triển báo chí - truyền thông và bảo đảm an ninh truyền thông tại Hàn Quốc.

4. Một số quốc gia Đông Nam Á

Nhận thức rõ tầm quan trọng của an ninh truyền thông, đặc biệt trong bối cảnh hội nhập quốc tế và cách mạng công nghệ 4.0, các quốc gia thành viên của ASEAN đã xây dựng chiến lược và tăng cường thực hiện các biện pháp bảo đảm an ninh truyền thông. Nhìn chung, chiến lược bảo vệ an ninh truyền thông của các quốc gia ASEAN đều tập trung vào những nội dung cơ bản sau:

Một là, tăng cường ban hành hệ thống văn bản quy phạm pháp luật điều chỉnh hoạt động thông tin, truyền thông, tạo cơ sở pháp lý cho hoạt động bảo đảm an ninh truyền thông.

Singapore là một trong những trung tâm truyền thông được đánh giá cao, là nguồn thông tin đáng tin cậy trong khu vực châu Á - Thái Bình Dương, có hai đạo luật chính là Luật Báo in và các ấn phẩm in và Luật Phát thanh truyền hình. Singapore quản lý báo chí, các nhà cung cấp dịch vụ Internet theo hình thức cấp giấy phép hoạt động và đánh giá lại hiệu quả thực hiện hằng năm, với cơ quan chủ quản là Bộ Truyền thông và Thông tin. Các loại hình báo chí gây ảnh hưởng tiêu cực đến an ninh quốc gia, đến Chính phủ, đến các dân tộc trong nước, đến Malaysia và các nước lân cận... sẽ bị xử phạt theo các quy định của pháp luật[10]. Báo chí cần phải đưa tin chính xác, khách quan và có trách nhiệm, đặc biệt cần trọng khi đưa tin liên quan đến vận mệnh của đất nước; cần khuyến khích công chúng tôn trọng thể chế nhà nước, các cơ quan tư pháp, hành pháp và thi hành pháp luật.

Ngày 5/2/2018, Quốc hội Singapore đã thông qua Luật An ninh mạng về tăng cường bảo vệ cơ sở hạ tầng thông tin trọng yếu (CII) thiết lập khung pháp lý để ngăn chặn nguy cơ tấn công mạng trong nước. Luật này cho phép cơ quan an ninh mạng Singapore theo dõi, quản lý an toàn không gian mạng của đất nước. Các lĩnh vực thuộc CII bao gồm: Năng lượng, Nước, Ngân hàng và Tài chính, Y tế, Giao thông vận tải (bao gồm Đất đai, Hàng hải và Hàng không), Thông tin liên lạc, Truyền thông, Dịch vụ An ninh và Khẩn cấp, và Chính phủ[11]... Bên cạnh đó, Singapore cũng ban hành các đạo luật khác để bảo vệ an ninh truyền thông ở nhiều lĩnh vực khác nhau như: Luật Kiểm soát thư rác, Luật Giao dịch điện tử, Luật Bảo vệ dữ liệu cá nhân.

Tại Thái Lan, ngày 16/12/2016, Quốc hội đã thông qua Luật Tội phạm máy tính, theo đó hành vi đăng tải thông tin sai sự thật để phá hoại an ninh quốc gia, an toàn công cộng, ổn định kinh tế quốc dân, gây hoang mang dư luận… là vi phạm pháp luật và phải chịu mức án lên tới 5 năm tù.

Ở Indonesia, Chính phủ Indonesia quản lý báo chí bằng Luật Báo chí và các quy định khác dưới luật, trong đó quy định tất cả những ai viết, xuất bản, trưng bày các tài liệu tiêu cực, xúi giục hay tạo nên sự căm ghét Chính phủ Indonesia, với các nhóm dân tộc trong nước đều bị xử phạt, thậm chí có thể bị phạt tù. Năm 2016, Indonesia cũng ban

hành Luật Giao dịch điện tử và thông tin để điều chỉnh các giao dịch điện tử ở quốc gia này, trong đó quy định rõ chế tài với hành vi xâm phạm an ninh trong lĩnh vực này.

Lào đã thông qua Luật Phòng, chống tội phạm mạng năm 2015, trong đó nghiêm cấm việc đăng tải những nội dung không phù hợp, tin giả chống lại Đảng Nhân dân cách mạng Lào, phá hoại hòa bình, độc lập, chủ quyền, sự thống nhất và thịnh vượng của Lào. Sau đó hai năm, Lào chính thức ban hành Luật Bảo vệ dữ liệu nhằm bảo đảm an toàn cho dữ liệu điện tử của người sử dụng.

Ở Malaysia, nhiều đạo luật về an ninh truyền thông đã được ban hành như: Luật Tội phạm máy tính (năm 1997); Luật Truyền thông và đa phương tiện (năm 1998); Luật Bảo vệ dữ liệu cá nhân (năm 2010); Luật An ninh mạng (năm 2017).

Năm 2013, Myanmar đã ban hành Luật Thông tin truyền thông nhằm quản lý Internet (luật này đã được sửa đổi, bổ sung vào năm 2015) và Luật Bảo vệ quyền riêng tư và an ninh của người dân (năm 2017).

Hai quốc gia theo chế độ quân chủ là Brunei và Campuchia hiện nay đều chưa có các đạo luật riêng về an ninh truyền thông nói chung và bảo vệ dữ liệu cá nhân nói riêng. Hai quốc gia này vẫn đang áp dụng: Luật Cấm nói xấu Hoàng gia (của Brunei) và Luật Cấm nói xấu, bình luận không hay về Hoàng gia và Chính phủ (của Campuchia) trong quản lý lĩnh vực truyền thông và Internet.

Đông Timor hiện nay mới ban hành duy nhất Luật Thông tin truyền thông năm 2012 liên quan đến quản lý Internet[12].

Hai là, tổ chức lực lượng chuyên trách bảo vệ an ninh truyền thông quốc gia. Nhận thức được tầm quan trọng của việc bảo vệ an ninh truyền thông, các quốc gia trong khu vực ASEAN đều thành lập hoặc giao nhiệm vụ bảo vệ an ninh truyền thông cho các cơ quan chuyên trách.

Ở Indonesia, Bộ Thông tin và Truyền thông là cơ quan chịu trách nhiệm quản lý, xử lý đối với những tin tức độc hại, tin giả, liên quan đến vấn đề chính trị, bạo lực cực đoan.

Năm 2015, cùng với việc ban hành Chiến lược quốc gia về an ninh mạng, Singapore đã thành lập Cơ quan chuyên trách về an ninh mạng (CSA). Cơ quan này còn được trao thẩm quyền kiểm soát các dịch vụ liên quan đến an ninh mạng ở khu vực tư nhân như hệ thống thanh toán tài chính.

Ở Thái Lan, Ủy ban An ninh mạng quốc gia (NCSC) được thành lập năm 2019 với chức năng chủ trì, soạn thảo chính sách và kế hoạch hành động nhằm củng cố an ninh mạng quốc gia. Ủy ban này có đầy đủ quyền hạn thực hiện các hoạt động giám sát kết nối Internet, yêu cầu gỡ các nội dung không phù hợp và tịch thu các máy tính vi phạm mà không cần sự cho phép của tòa án. NCSC cũng được phép tiếp cận các máy tính của cá nhân hoặc của các công ty tư nhân, sao chép thông tin và truy cập các tài sản cá nhân mà không cần lệnh của tòa án; triệu tập các doanh nghiệp hoặc cá nhân để thẩm vấn và yêu cầu trình báo, giao nộp những thông tin cần thiết. Ngoài ra, Thái Lan còn thành lập Ủy ban Giám sát an ninh mạng do Bộ trưởng phụ trách kinh tế kỹ thuật số và xã hội điều hành[13].

Ba là, tăng cường hợp tác quốc tế trong lĩnh vực an ninh truyền thông.

Năm 2002, Hội nghị thượng đỉnh lần thứ 6 giữa các nước ASEAN và Trung Quốc tại Phnôm Pênh (Campuchia) đã ra Tuyên bố chung ASEAN - Trung Quốc về hợp tác trên lĩnh vực an ninh phi truyền thống. Tuyên bố này xác định các vấn đề an ninh phi truyền thống ngày càng diễn biến phức tạp như: buôn bán trái phép chất ma túy, đưa người trái phép, trong đó có buôn bán phụ nữ và trẻ em, cướp biển, khủng bố, buôn lậu vũ khí, rửa tiền, tội phạm kinh tế quốc tế và tội phạm mạng. Kể từ đó, các nước ASEAN đã triển khai hợp tác với các quốc gia Trung Quốc, Nhật Bản, Hàn Quốc, Mỹ, EU, các tổ chức quốc tế trong đấu tranh phòng, chống tội phạm xuyên quốc gia và lĩnh vực an ninh phi truyền thống.

Các quốc gia trong khu vực ASEAN đã tiến hành diễn tập về ứng phó với sự cố an ninh mạng trên quy mô toàn khu vực Đông Nam Á với sự tham gia của các CERT (Đội phản ứng nhanh sự cố máy tính) của các nước trong khu vực.

Singapore - một trong những quốc gia được đánh giá cao về những nỗ lực trong bảo đảm an

ninh truyền thông nói chung và an ninh mạng nói riêng đã thành lập Quỹ xây dựng năng lực an ninh mạng ASEAN (ACCP) để giúp các thành viên trong khu vực xây dựng hành lang pháp lý, mua sắm trang thiết bị, thuê chuyên gia, huấn luyện nhân sự… bảo vệ an ninh mạng.

Có thể khẳng định, mặc dù các quốc gia ASEAN có chênh lệch về trình độ kỹ thuật công nghệ thông tin, sự khác biệt trong chính sách an ninh truyền thông, hạn chế về nhân lực và tài chính... nhưng đều tích cực hợp tác với quốc gia trong khu vực để bảo đảm an ninh truyền thông của quốc gia và khu vực.

Việt Nam là một quốc gia luôn sẵn sàng lắng nghe, học hỏi các bài học kinh nghiệm của các quốc gia trên thế giới một cách chọn lọc và phù hợp. Trong bối cảnh an ninh truyền thông trên không gian mạng gặp nhiều thách thức, Việt Nam đã kịp thời đưa ra các đường lối, chính sách hợp lý. Từ năm 1997, Bộ Nội vụ (nay là Bộ Công an) đã có Quyết định số 848/1997/QĐ-BNV (A11) quy định về biện pháp và trang thiết bị kiểm tra, kiểm soát bảo đảm an ninh quốc gia trong hoạt động Internet tại Việt Nam. Năm 2005, Ban Bí thư Trung ương Đảng đã ban hành Chỉ thị số 52-CT/TW về "Phát triển và quản lý báo điện tử ở nước ta hiện nay. Nghị định số 72/NĐ-CP về "quản lý, cung cấp sử dụng dịch vụ Internet và thông tin trên mạng", Nghị định số 142/2016/NĐ-CP năm 2016 về ngăn chặn xung đột thông tin trên mạng. Đặc biệt, năm 2018, Quốc hội đã thông qua và ban hành Luật An ninh mạng… Gần đây, khi an ninh truyền thông bị thách thức lớn bởi tin giả, Bộ Thông tin và Truyền thông Việt Nam đã xây dựng và công bố Cẩm nang về phòng chống tin giả, tin sai sự thật trên mạng là một phần trong nhóm các giải pháp quản lý nhà nước. Bên cạnh đó, Việt Nam cũng đã tổ chức ra các cơ quan chuyên trách về vấn đề an ninh truyền thông, an ninh mạng như Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng thẩm định an ninh mạng đối với hệ thống thông tin quân sự; Ban Cơ yếu Chính phủ thẩm định an ninh mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ[14].

Tuy vậy, sự biến động không ngừng của không gian mạng, sự phát triển của khoa học công nghệ kèm theo hệ quả là sự phát triển tinh vi của các tội phạm công nghệ cao, Việt Nam rất cần những kinh nghiệm quý báu từ các quốc gia để hoàn thiện hơn nữa thể chế, luật pháp nhằm ứng phó hiệu quả với các vấn đề an ninh truyền thông, an ninh mạng phù hợp với thông lệ quốc tế và bối cảnh Việt Nam./.

* Bài viết là kết quả nghiên cứu trong khuôn khổ Đề tài cấp nhà nước KX04.32/21-25: *"Vấn đề an ninh phi truyền thống, trọng tâm là an ninh mạng trong nền an ninh quốc gia"* thuộc Chương trình khoa học xã hội trọng điểm cấp quốc gia giai đoạn 2021-2025 "Nghiên cứu khoa học lý luận chính trị giai đoạn 2021-2025" (mã số KX.04/21-25)

(1) Statista (2023), Number of social network users worldwide in 2022, by region, truy cập tại link https://www.statista.com/statistics/454772/number-social-media-user-worldwide-region/ ngày 31/5/2023

(2), (3) Bộ Thông tin và Truyền thông (2022), Báo cáo thuyết minh Quy hoạch phát triển mạng lưới cơ sở báo chí, phát thanh, truyền hình, thông tin điện tử, cơ sở xuất bản thời kỳ 2021 - 2030, tầm nhìn đến 2050.

(4) Điều lệ quản lý xuất bản ngày 25/12/2001 theo Nghị định số 343 của Hội đồng Nhà nước Cộng hòa Nhân dân Trung Hoa)

(5) Nguyễn Thị Trường Giang (2020), Pháp luật và đạo đức báo chí, Nxb. Đại học Quốc gia Hà Nội.

(6) Đạo luật cơ bản về An ninh mạng Nhật Bản (The Basic Act on Cybersecurity) số 014 ngày 12 tháng 11 năm 2014

(7) Bộ Công an (2017), Thông tin về tình hình an ninh mạng một số nước, Hà Nội.

(8) Doãn Thị Thuận, *Kinh nghiệm quản lý báo chí điện tử ở một số quốc gia trên thế giới*, Tạp chí Tuyên giáo số 3/2016

(9) Hà Huy Phượng (2020), Bức tranh đa chiều về truyền thông Hàn Quốc, Tạp chí Người làm báo, truy cập tại link https://nguoilambao.vn/buc-tranh-da-chieu-ve-truyen-thong-han-quoc-ky-ii-n11229.html ngày 31/5/2023.

(10) Hoàng Mạnh Thắng (2016), *Quản lý xã hội đối với hoạt động truyền thông đại chúng ở tỉnh Đắk Nông hiện nay*, Luận văn thạc sĩ, HVBCTT.

(11) CSC Singapore, Cybersecurity Act, truy cập tại link https://www.csa.gov.sg/legislation/Cybersecurity-Act ngày 31/5/2023

(12), (13) Nguyễn Việt Lâm (2019), *Chính sách an ninh mạng trong quan hệ quốc tế hiện nay và đối sách của Việt Nam*, Nxb. Chính trị quốc gia Sự thật, H., tr. 105-108, 110.

(14) Theo Luật an ninh mạng Việt Nam, ban hành năm 2018, có hiệu lực năm 2019.