Kinh nghiệm của Mỹ và một số quốc gia ở châu Âu trong bảo đảm an ninh truyền thông trên không gian mạng

20:12 05/07/2023

Tác giả: Đang cập nhật

Trong bối cảnh cách mạng khoa học công nghệ phát triển mạnh mẽ, thế giới bước vào quá trình chuyển đổi số toàn diện thì truyền thông đã không chỉ là công việc của các tổ chức, cơ quan, đơn vị và hãng thông tấn, báo chí mà còn liên quan đến các cá nhân (các tài khoản) trên không gian mạng. Sự gia tăng mạnh mẽ của truyền thông qua các nền tảng mạng xã hội trên không gian mạng đã đặt ra những vấn đề an ninh buộc các chính phủ phải điều chỉnh các chính sách có liên quan đến an ninh truyền thông và an ninh mạng. Bài viết khái quát hóa, hệ thống hóa các nội dung liên quan đến an ninh truyền thông trong mối quan hệ với an ninh mạng của Hoa Kỳ, Nga và một số quốc gia ở Liên minh châu Âu như những kinh nghiệm quý báu tham chiếu cho Việt Nam.

Nước Mỹ

Mỹ là cường quốc trên thế giới với một thể chế lâu đời và thường xuyên có những điều chỉnh phù hợp với sự phát triển của thời đại. Để đảm bảo an toàn truyền thông, Quốc hội Mỹ có Ủy ban liên bang về thông tin để phân tích và kiểm tra các thông tin trên báo chí. Ủy ban này được quyền ba năm một lần cấp giấy phép hoạt động cho các cơ quan báo chí dựa trên những đánh giá về hoạt động của nó. Ngoài ra, Mỹ cũng đã đưa ra chính sách liên quan đến hoạt động của các nhà báo là Quy tắc Báo chí, Quy tắc về Vô tuyến truyền hình mà các nhà báo hoạt động nghề nghiệp phải tuân thủ. Tuy nhiên, truyền thông trong bối cảnh phát triển của mạng xã hội lại buộc Mỹ đưa ra các thiết chế an ninh mạng. Chính phủ Mỹ giao nhiệm vụ cho các cơ quan: Bộ Tư pháp, Bộ An ninh nội địa (DHS) và Văn phòng Tình báo quốc gia, Cơ quan An ninh mạng và cơ sở hạ tầng Mỹ (CISA), Bộ Tư lệnh Không gian mạng Mỹ (USCYBERCOM)... Trong đó, Bộ Tư pháp, thông qua Cục Điều tra liên bang (FBI) và lực lượng đặc nhiệm chung điều tra mạng quốc gia (NCIJTF) có chức năng ngăn chặn những nguy cơ an ninh mạng trước khi vụ việc xảy ra. Bộ An ninh nội địa đảm nhiệm các vấn đề về kỹ thuật khi có sự cố, đồng thời đóng vai trò phối hợp liên ngành. Văn phòng Tình báo quốc gia cung cấp thông tin về các mối đe dọa an ninh mạng. Sự phân công nhiệm vụ rõ ràng như trên vừa bảo đảm sự phối hợp nhịp nhàng, đồng bộ, vừa tránh tình trạng chồng chéo chức năng giữa ba

cơ quan, góp phần bảo đảm hiệu quả xử lý tình huống đe dọa an ninh mạng nhanh chóng, kịp thời [1].

Mỹ ngày càng hoàn thiện thể chế của mình, trên cơ sở ba đạo luật an ninh mạng chính là (1) Đạo luật về trách nhiệm giải trình và khả năng chuyển đổi bảo hiểm sức khỏe (Health Insurance Portability and Accountability Act – HIPAA) năm 1996; (2) Đạo luật Gramm-Leach-Bliley năm 1999; (3) Đạo luật An ninh nội địa (Homeland Security Act năm 2002) bao gồm luật An ninh thông tin Liên bang (Federal Information Security Management Act - FISMA) và đạo luật tăng cường bảo vệ an ninh mạng quốc gia năm 2015 bổ sung cho Đạo luật An ninh Nội địa năm 2002. Cụ thể, ngày 27/10/2015, Thượng nghị viện Mỹ thông qua Luật Chia sẻ thông tin an ninh mạng (CISA); đồng thời, một số quy định về an ninh mạng không còn phù hợp đã được kịp thời sửa đổi, ban hành như: Đạo luật Tăng cường an ninh mạng, Đạo luật Tăng cường bảo vệ an ninh mạng quốc gia sửa đổi, Đạo luật Thông báo vi phạm dữ liệu trao đổi liên bang. Đạo luật Thông báo vi phạm dữ liệu trao đổi liên bang (Federal Exchange Data Breach Notification Act) năm 2015[2]. Tháng 9 năm 2018, Mỹ đã công bố Chiến lược An ninh mạng, trong đó xác định mối đe dọa về an ninh mạng là mối đe dọa hàng đầu đối với an ninh quốc gia; tuyên bố sẵn sàng đáp trả bằng các biện pháp quân sự nếu an ninh mạng quốc gia bị đe dọa, tấn công. Trước những báo cáo của Bộ Tư pháp, Cơ quan tình báo CIA và cả Cục điều tra liên bang Hoa Kỳ FBI, Tổng thống Obama đề xuất một Gói cải cách lập pháp an ninh mạng. Hạ viện Mỹ thông qua một dự luật chia sẻ thông tin và Thượng viện Mỹ phát triển một dự luật thỏa hiệp, để tìm kiếm sự cân bằng giữa an ninh quốc gia, bảo mật và lợi ích kinh doanh. Ngày 28/5/2020, Tổng thống Donal Trump đã ký một sắc lệnh hành chính nhằm tăng cường khả năng của chính phủ trong việc kiểm soát các nền tảng truyền thông xã hội (online platform)[3] . Đặc biệt, tháng 3 năm 2023, Nhà Trắng đã công bố chiến lược an ninh mạng quốc gia của chính quyền Tổng thống Joe Biden nhằm bảo đảm mọi người dân Mỹ được thừa hưởng “những lợi ích đầy đủ của một hệ sinh thái số an toàn” và tăng cường năng lực phòng thủ trên không gian mạng[4].

Như vậy, để bảo vệ an ninh truyền thông trên không gian mạng, Chính phủ Mỹ xây dựng một loạt các giải pháp đồng bộ: *một là*, xây dựng hệ thống các cơ quan chuyên trách vừa là mạng lưới phòng thủ cấp nhà nước vừa là xử lý các thách thức với an ninh truyền thông; *hai là*, hoàn thiện thể chế, chính sách đảm bảo an ninh truyền thông; *ba là*, đẩy mạnh liên kết công – tư trong đảm bảo an ninh thông tin; *bốn là*, triển khai các lớp bảo vệ[5].

Liên bang Nga

Liên bang Nga là một quốc gia luôn coi trọng an ninh truyền thông và an ninh mạng. Để bảo đảm

an ninh truyền thông quốc gia, Nga đã xây dựng hệ thống cơ quan gồm: Cơ quan An ninh liên bang Nga; Bộ Nội vụ; Bộ Quốc phòng và các cơ quan khác. Cơ quan An ninh liên bang có vai trò đứng đầu trong việc điều phối các công tác an ninh trên mạng, điều phối các chiến dịch truyền bá thông tin; kiểm soát các danh sách đen về thông tin và quản lý truyền thông. Bộ Nội vụ Nga phụ trách về tội phạm mạng. Bộ Quốc phòng phụ trách các vấn đề về an ninh quốc phòng và chiến tranh thông tin. Ngoài ra, các cơ quan bảo vệ liên bang và cơ quan tình báo nước ngoài của Nga cũng tham gia vào hệ thống bảo đảm an ninh truyền thông của quốc gia này[6]. Các cơ quan này được trao thẩm quyền lớn trong bảo vệ an ninh truyền thông. Trong một số trường hợp cần thiết, các cơ quan có thẩm quyền có thể đóng cửa toàn bộ các trang mạng được coi là cung cấp thông tin hoặc có nội dung không phù hợp mà không cần có quyết định của tòa án.

Coi vấn đề an ninh truyền thông là một ưu tiên trong chính sách an ninh quốc gia nên Nga đã xây dựng chiến lược về an ninh truyền thông từ năm 2000. Với Thuyết An ninh thông tin Liên bang Nga năm 2016, Chính phủ Nga đã bắt đầu tiến hành các biện pháp cụ thể để đấu tranh chống tội phạm mạng và bảo đảm an ninh truyền thông trên không gian mạng.

Trước hết, Liên bang Nga đã ban hành một khối lượng lớn các văn bản quy phạm pháp luật điều chỉnh hoạt động thông tin và truyền thông đại chúng. Nổi bật trong số đó là hai đạo luật: Luật số 149-FZ năm 2006 về thông tin, công nghệ thông tin và an ninh thông tin; Luật số 152-FZ năm 2006 về dữ liệu cá nhân. Năm 2014, để tăng cường công tác bảo vệ dữ liệu cá nhân cho phù hợp với tình hình chính trị trong và ngoài nước, đặc biệt trong bối cảnh các trang mạng xã hội bị lợi dụng trong các phong trào chống đối chính phủ, Nga đã ban hành Luật số 242-FZ về nội địa hóa dữ liệu. Nội dung đạo luật này tập trung vào chính sách quản lý mạng xã hội ở Nga. Theo đó, tất cả các công ty Internet, quản lý hộp thư điện tử, công cụ tìm kiếm, các mạng xã hội nội địa hoặc nước ngoài nhằm đến người dùng Nga phải ghi chép, hệ thống hóa, lưu trữ và xác định dữ liệu người dùng. Tất cả các thông tin của người sử dụng phải được lưu trữ tại máy chủ đặt tại Nga. Luật này cũng yêu cầu các công ty viễn thông và các nhà cung cấp dịch vụ Internet phải cắt giảm dịch vụ đối với người sử dụng nếu họ không đáp ứng yêu cầu của cơ quan thực thi pháp luật để xác định danh tính của họ khi họ sử dụng các dịch vụ viễn thông và dịch vụ online nói chung[7]. Tổng thống Vladimir Putin năm 2019 đã ban hành đạo luật mới có tên Luật về tin giả và thông tin xúc phạm chính quyền trên Internet nhằm kiểm soát và điều chỉnh hành vi con người trên không gian mạng. Đối tượng điều chỉnh là người dùng và nhà cung cấp dịch vụ. Mức phạt hành chính sẽ tăng dần theo 3 cấp độ: từ tạo ra mối đe dọa đến gây nhiễu loạn trong đời sống xã hội và cao nhất là gây chết người. Đối với doanh nghiệp cung cấp dịch vụ: trong 24 giờ không thực hiện yêu cầu của cơ

quan chức năng, trang web chứa thông tin vi phạm sẽ bị đóng[8].

Bên cạnh việc siết chặt các quy định về quản lý thông tin và truyền thông đại chúng bằng các đạo luật, Nga còn tập trung phát triển các công nghệ hiện đại như phần mềm tự động kiểm soát các trang mạng xã hội và các hiện tượng tiêu cực trên mạng Internet.

Tương tự như Mỹ, Nga rất quan tâm đến việc hình thành các cơ quan chuyên trách, hoàn thiện thể chế phòng, chống các thách thức an ninh truyền thông trên không gian mạng. Nga đã thể hiện rõ nhận thức của nhà nước về tầm quan trọng của an ninh truyền thông trên không gian mạng từ đó nhấn mạnh quyết tâm chính trị của mình trong cuộc chiến an ninh mạng về truyền thông nói riêng và an ninh mạng nói chung.

Các quốc gia trong Liên minh châu Âu

Với mục đích nâng cao an ninh truyền thông trên không gian mạng của các quốc gia trong khối, Liên minh châu Âu đã thành lập Cơ quan về an ninh mạng và an ninh thông tin (ENISA) vào năm 2004. Cơ quan này được thành lập với chức năng cung cấp các dịch vụ thuộc lĩnh vực không gian mạng cho các quốc gia thành viên của liên minh châu Âu, bao gồm: *một là*, khuyến nghị các quốc gia thành viên về các hành động đối với vi phạm an ninh mạng; *hai là*, xây dựng chính sách và hỗ trợ việc thực hiện các quy định về an ninh mạng cho tất cả các thành viên EU; *ba là*, trực tiếp làm việc với các đội, nhóm hoạt động trong lĩnh vực không gian mạng của EU[9].

Năm 2016, các quốc gia thành viên của EU được yêu cầu phải tạo ra một *chiến lược chỉ thị NIS* bao gồm các đội CSIRTs, các cơ quan có thẩm quyền quốc gia (NCAs) và các cơ quan điều phối (SPOCs). Những tổ chức này được trao trách nhiệm xử lý vi phạm an ninh mạng, bao gồm các biện pháp kỹ thuật phòng ngừa, quản lý rủi ro của hành vi vi phạm an ninh mạng. thành lập đơn vị không gian mạng chung của EU. Tháng 6 năm 2021, 27 quốc gia thành viên EU thống nhất thành lập Đơn vị không gian mạng chung để đối phó với tội phạm an ninh mạng ngày càng tăng và tinh vi hơn[10]. Bên cạnh đó là Europol có trụ sở tại The Hague, Hà Lan hỗ trợ 27 nước thành viên EU trong cuộc chiến chống tội phạm mạng và các hình thức tội phạm nghiêm trọng khác.

Để có thể ứng phó với an ninh truyền thống và an ninh mạng, EU hết sức quan tâm đến việc hoàn thiện thể chế. Đến tháng 5 năm 2016, EU cùng những nhà quản lý các mạng xã hội ký bộ quy tắc ứng xử nhằm chống lại các phát ngôn gây thù hận trên mạng. Theo đó, các nhà quản lý của Facebook, Microsoft, Twitter, YouTube cam kết sẽ ngăn chặn sự phát tán phát những bình luận thù hận trên mạng xã hội của họ, 24 giờ sau khi nhận được thông báo phải xét duyệt, xóa bỏ các phát

ngôn tiềm ẩn nội dung gây thù hận. Tháng 7 năm 2016, Nghị viện châu Âu đưa Chỉ thị về an ninh của mạng và hệ thống thông tin (chỉ thị NIS) có hiệu lực từ tháng 8 năm 2016. Mục đích của Chỉ thị NIS này là tạo ra một mức độ an ninh mạng tổng thể cao hơn trong EU. Ngày 25/5/2018, Luật An ninh mạng của EU chính thức có hiệu lực với những điều khoản không chỉ áp dụng cho các tổ chức hoạt động trong EU mà còn áp dụng cho các tổ chức xử lý dữ liệu của bất kỳ cư dân nào thuộc EU; đối tượng vi phạm có thể bị phạt tiền lên tới 20 triệu ơ-rô hoặc 4% doanh thu hằng năm[11]... Các quy định chung này nhằm mang lại một tiêu chuẩn duy nhất để bảo vệ dữ liệu giữa tất cả các nước thành viên trong EU. Tất cả các hành vi vi phạm dữ liệu, ảnh hưởng tới các quyền và sự tự do của những cá nhân cư trú tại EU phải được công bố trong vòng 72 giờ. Ban Bảo vệ dữ liệu của EU (EDP) phải chịu trách nhiệm về tất cả các giám sát theo quy định. Các công ty nắm giữ dữ liệu liên quan đến công dân EU phải cung cấp cho các công dân quyền được chia sẻ hoặc từ chối chia sẻ dữ liệu. Chiến lược An ninh mạng mới của EU được Ủy ban châu Âu (EC) và Đại diện cấp cao của Liên minh Chính sách an ninh và đối ngoại châu Âu thông qua vào tháng 12 năm 2020. Chiến lược có mục tiêu tổng quát là tăng cường năng lực bảo mật an ninh mạng, giúp châu Âu an toàn hơn trước các mối đe dọa trên không gian mạng[12]. Ngày 28/11/2022, EU đã thông qua Chỉ thị NIS2 về "Các biện pháp an ninh mạng thống nhất cao trên toàn EU". Năm 2023, Uỷ ban châu Âu (EC) đã công bố đề xuất Đạo luật Đoàn kết mạng của EU nhằm cải thiện sự chuẩn bị, khả năng phát hiện và ứng phó các sự cố an ninh mạng trên quy mô toàn khối.

Những hoạt động của EU cho thấy phản ứng thông minh, đầy kinh nghiệm trong ứng phó với các vấn đề liên quan đến an ninh mạng nói chung và an ninh truyền thông trong không gian mạng nói riêng. Một đặc điểm riêng có của EU là sự đầu tư mạnh mẽ và tính đồng thuận khá cao trong việc đảm bảo an ninh truyền thông, an ninh mạng.

Đức

Là một trong những quốc gia đầu tiên tại châu Âu thông qua Luật An ninh mạng năm 2014 và có hiệu lực từ tháng 7/2015. Theo đó yêu cầu các công ty cơ quan liên bang phải có tiêu chuẩn bảo mật mạng tối thiểu, phải được Văn phòng Bảo mật thông tin liên bang (BSI) chứng nhận; cấm người sử dụng Internet âm mưu sử dụng bạo lực để lật đổ chính quyền, xúi giục hành vi phạm tội. Từ ngày 1/9/2017, Luật cải tiến chấp pháp tại các mạng xã hội (NetzDG) đã được thông qua. Ban đầu luật này có hiệu lực từ ngày 1/10/2017, song Đức đã quyết định gia hạn đến ngày 1/1/2018 để các công ty có thời gian tự điều chỉnh việc kiểm duyệt. Để xây dựng các điều khoản của NetzDG, Đức đã sử dụng Bộ luật Hình sự để điều chỉnh hành vi người dùng trên mạng xã hội. NetzDG cũng

được sử dụng để ngăn chặn sự phát tán tin giả và phát ngôn gây thù hận, áp dụng cho bất cứ dịch vụ mạng xã hội nào có hơn hai triệu tài khoản người dùng, cụ thể hóa những khái niệm cũng như quy định rõ ràng về những điều bị cấm khi sử dụng mạng xã hội, như: Sử dụng phù hiệu hoặc biểu tượng các tổ chức trái với Hiến pháp (ví dụ như các biểu tượng liên quan đến Đức quốc xã hoặc các tổ chức khủng bố, cực đoan); âm mưu sử dụng bạo lực xâm hại an ninh quốc gia; hình thành các tổ chức tội phạm, khủng bố ở trong và ngoài nước; xúi giục bạo lực, kích động hận thù; phát tán các văn hóa phẩm có nội dung bạo lực; nhục mạ tín ngưỡng, tôn giáo cũng như tư tưởng; xúc phạm, phỉ báng, vu khống; xâm phạm các khu vực sinh sống cá nhân bằng cách chụp ảnh, quay phim; quấy rối tính dục trên mạng...[13] Theo quy định của đạo luật này, nếu những dịch vụ mạng xã hội tại Đức để xảy ra tình trạng người dùng đăng tải thông tin mang tính lăng mạ, gây thù hận hay phát tán tin tức giả mạo sẽ phải chịu hình phạt rất nghiêm khắc, có thể lên đến 50 triệu euro.

Pháp

Cũng là một trong những nước phát triển đi tiên phong xây dựng và áp dụng các biện pháp an ninh mạng quốc gia để ngăn chặn các cuộc tấn công mạng ngày càng dày đặc và tinh vi. Ngay từ tháng 7/2009, Pháp đã thành lập Cơ quan Quốc gia về an ninh thông tin (ANSSI) là cơ quan có thẩm quyền cao nhất về an ninh mạng quốc gia, có nhiệm vụ quản lý phòng ngừa và ứng phó với các cuộc tấn công máy tính chống lại các tổ chức, doanh nghiệp. ANSSI đóng vai trò là cơ quan phản ứng đầu tiên trong không gian mạng của Pháp với 600 nhân viên và vẫn tiếp tục tăng lên trong thời gian tới. Bên cạnh đó, Bộ Nội vụ là cơ quan có nhiệm vụ chiến đấu chống lại tội phạm mạng dưới mọi hình thức nhằm bảo vệ lợi ích quốc gia, các tác nhân kinh tế, các cơ quan công quyền và các cá nhân[14]. Đầu năm 2017 Bộ Tư lệnh phòng thủ không gian mạng (COMCYBER) thuộc Bộ Quốc phòng được thành lập, có nhiệm vụ kép là bảo vệ các mạng lưới thông tin nền tảng của quân đội và đưa kỹ thuật số thành trung tâm của các hoạt động quân sự.

Năm 2009, Pháp công bố Chiến lược về bảo mật hệ thống thông tin[15], năm 2015, Chiến lược an ninh mạng quốc gia đã được Pháp triển khai để hỗ trợ quá trình chuyển đổi kỹ thuật số. Chiến lược này đáp ứng những thách thức mới nảy sinh từ sự phát triển ứng dụng kỹ thuật số và các mối đe dọa liên quan, mục tiêu nhằm đảm bảo chủ quyền quốc gia, chống các hành vi gây hận thù trên mạng.

Tháng 6/2016, Pháp đi đầu trong thông qua Cam kết không gian mạng của Tổ chức Hiệp ước Bắc Đại Tây Dương (NATO) tại Hội nghị thượng đỉnh Vácsava. Tháng 5/2018, Pháp đã tổ chức hội nghị đầu tiên về cam kết này, công nhận không gian mạng là một lĩnh vực hoạt động của NATO, bên

cạnh các lĩnh vực truyền thống trên bộ, trên không và trên biển. Đầu năm 2017, nhằm tăng cường an ninh không gian mạng quân sự, Bộ Quốc phòng Pháp đã thành lập Bộ Tư lệnh phòng thủ không gian mạng (COMCYBER), có nhiệm vụ kép là bảo vệ các mạng lưới thông tin nền tảng của quân đội và đưa kỹ thuật số thành trung tâm của các hoạt động quân sự. Bên cạnh các luật và đạo luật chung về an ninh mạng, Pháp cũng đã có những quy định về an ninh truyền thông, chẳng hạn uốc hội đã thông qua "Luật về siết chặt kiểm soát thông tin trên mạng xã hội" vào tháng 12/2018. Mục đích ban hành đạo luật là nhằm hạn chế các thông tin thất thiệt có thể ảnh hưởng đến kết quả của các cuộc bầu cử tại Pháp. Mức phạt cho hành vi tung tin thất thiệt không chỉ bị phạt hành chính với mức phạt cao. Đạo luật quy định "hình sự hóa" tội danh tung tin thất thiệt, theo đó phạt tù đến 1 năm và phạt tiền đến 75.000 Euro đối với hành vi phát tán một cách có chủ ý và với số lượng lớn thông tin sai lệch ảnh hưởng đến kết quả bầu cử[16]

Những quan điểm, chính sách của các quốc gia trên thế giới đã cho thấy (1) sự quyết tâm của các chính phủ trong việc đảo bảo an toàn thông tin, truyền thông và không gian mạng (2) về cơ bản, các quốc gia đều tổ chức một bộ máy thực thi chuyên biệt gồm các cơ quan đến từ các bộ như an ninh - cảnh sát, quốc phòng, nội vụ chuyên trách về an ninh truyền thông và an ninh mạng. (3) các quốc gia đều coi vấn đề an ninh truyền thông, an ninh mạng là vấn đề được đặt lên hàng đầu trong chính sách hoặc chiến lược an ninh quốc gia (4) Các quốc gia cũng liên tục cập nhật và điều chỉnh các chính sách dưới dạng đạo luật, luật, văn bản quy phạm pháp luật liên quan đến an ninh truyền thông và an ninh mạng phù hợp với sự phát triển của quốc gia và thời đại, đặc biệt tính nghiêm khắc trong việc xử lý vi phạm được chú trọng. (5) Đầu tư kịp thời, đúng và đủ là điều kiện cần cho cuộc chiến an ninh truyền thông trên không gian mạng.

PGS, TS Nguyễn Thị Trường Giang

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] 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, Hà Nội, tr. 52.

[2] https://tapchitoaan.vn/bao-dam-an-ninh-mang-cua-mot-so-nuoc-tren-the-gioi

[3]https://ictvietnam.vn/xu-ly-thong-tin-gia-tren-the-gioi-va-khuyen-nghi-bai-hoc-cho-viet-nam-31434.html

[4]https://www.qdnd.vn/quoc-te/binh-luan/my-cong-bo-chien-luoc-an-ninh-mang-quoc-gia-720657

[5] Xem thêm Lê Văn Thắng (2019), *An ninh thông tin của Việt Nam trong điều kiện hiện nay: Thực trạng, vấn đề đặt ra và giải pháp*, Đề tài cấp nhà nước KX.04/16-20, tr. 68-70.

[6] 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, Hà Nội, tr. 61.

[7] Bộ Thông tin và Truyền thông (2022), *Báo cáo tổng hợp 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 năm 2050*, Hà Nội, tr. 354-357.

[8] https://www.sggp.org.vn/cac-nuoc-manh-tay-phong-chong-tin-gia-post633213.html

[9] 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, Hà Nội, tr. 84.

[10]https://www.tapchicongsan.org.vn/web/guest/the-gioi-van-de-su-kien/-/2018/825421/%C2%A0an-ninh-mang-o-lien-minh-chau-au-%C2%A0thuc-trang-va-giai-phap-chien-luoc.aspx

[11]https://nhandan.vn/bao-ve-an-ninh-mang-la-chinh-vi-loi-ich-quoc-giavi-loi-ich-moi-nguoi-post327327.html

[12]https://www.tapchicongsan.org.vn/web/guest/the-gioi-van-de-su-kien/-/2018/825421/%C2%A0an-ninh-mang-o-lien-minh-chau-au-%C2%A0thuc-trang-va-giai-phap-chien-luoc.aspx

[13] https://special.vietnamplus.vn/2019/03/28/bao-dam-an-ninh-mang/

[14]https://m.antoanthongtin.vn/chinh-sach---chien-luoc/thuc-trang-toi-pham-mang-o-phap-nhung-nam-gan-day-108789

[15] https://special.vietnamplus.vn/2019/03/28/bao-dam-an-ninh-mang/

[16]https://ictvietnam.vn/xu-ly-thong-tin-gia-tren-the-gioi-va-khuyen-nghi-bai-hoc-cho-viet-nam-31434.html

Link bài viết: https://nguoilambao.vn/kinh-nghiem-cua-my-va-mot-so-quoc-gia-o-chau-au-trong-bao-dam-an-ninh-truyen-thong-tren-khong-gian-mang