

Quan niệm của thế giới và Việt Nam về an ninh mạng

PGS, TS NGUYỄN THỊ TRƯỜNG GIANG

Học viện Báo chí và Tuyên truyền; Email: truonggiangptth.ajc@gmail.com

Nhận ngày 30 tháng 9 năm 2022; chấp nhận đăng tháng 11 năm 2022.

Tóm tắt: Sau sự ra đời vào nửa sau thế kỷ XIX, Internet không ngừng phát triển mạnh mẽ trong những thập kỷ gần đây, đã cung cấp rất đa dạng các dịch vụ, đáp ứng nhu cầu đa dạng của cá nhân, gia đình, đến tổ chức, quốc gia. Với sự gia tăng việc sử dụng Internet và các dịch vụ liên quan, mọi người được trao nhiều quyền hơn, đặc biệt là tự do ngôn luận, vượt qua khỏi những khoảng cách địa lý và thúc đẩy lan tỏa thông tin. Tuy nhiên, sự phát triển không cân xứng, bất cập trong quy tắc và trật tự bất bình đẳng trên không gian mạng ngày càng rõ ràng, tạo khoảng cách giữa các quốc gia và khu vực đang ngày càng rộng. Bên cạnh đó, nhiều hoạt động trên không gian mạng để lại những hậu quả nặng nề, nghiêm trọng cho xã hội, đặt ra bài toán nan giải về an ninh mạng cho các quốc gia và cộng đồng quốc tế.

Từ khóa: an ninh; an ninh mạng; an ninh quốc gia; không gian mạng.

Abstract: Since its birth in the second half of the 19th century, the Internet has been developing strongly in recent decades, providing a variety of services to meet the diverse needs of individuals, families, organizations, and countries. With the increasing use of the Internet and related services, people are empowered with more rights, especially freedom of expression, to overcome geographical distances and promote the spread of information. However, the disproportionate development, the inadequacy in regulations and unequal order in cyberspace are increasingly evident, creating a widening gap among countries and regions. In addition, a great number of activities in cyberspace have left serious consequences on society, posing a dilemma of cybersecurity for countries and the international community.

Keywords: security; network security; national security; cyberspace.

1. Tầm quan trọng của việc quản lý, kiểm soát không gian mạng

Internet đã trở thành một không gian chứa nhiều mối đe dọa với các chính phủ và một mặt trận tranh giành ảnh hưởng của nhiều quốc gia lớn. Việc kiểm duyệt Internet trở thành một công cụ cần thiết trong việc kiểm soát nội dung, định hướng dư luận, ngăn chặn nguy cơ các làn sóng trong xã hội và gây những bất ổn sâu sắc trong đất nước. Clark et al (2017) nhận định rằng, các hoạt động kiểm duyệt Internet của nhà nước ngày càng đan xen với các động lực chính trị, được sử dụng để thúc đẩy các mục tiêu chính trị và cản trở các chính sách của các nhà nước đối thủ⁽¹⁾. Chẳng hạn, khi xung đột địa chính trị song phương và khu vực gia tăng, nhiều nhà nước đang thực hiện

các chính sách kiểm duyệt để chặn nội dung liên quan đến xung đột có nguồn gốc từ các nhà nước đối trọng với họ.

Vai trò của các chính sách kiểm soát an ninh mạng ngày càng được nâng cao, có thể tóm gọn vì những lý do như sau:

Một là, kiểm soát không gian mạng để Internet có thể tồn tại, phát triển và hoạt động theo các chức năng của mình. Với bản chất không có người kiểm soát, tự vận hành của Internet, vẫn cần có sự điều tiết cần thiết của nhà nước để nó hoạt động và phát triển. Những thủ thuật công nghệ hay hoạt động từ các đối tượng không thân thiện hoàn toàn có thể gây nên những cản trở cho việc vận hành mạng Internet, ảnh hưởng đến cuộc sống của nhiều người.

Hai là, các hoạt động trên không gian ảo nhưng lại có tác động mạnh mẽ đến thế giới thực. Internet là địa hạt và phương tiện để nhiều cá nhân, tổ chức lạm dụng dữ liệu, tạo ra sự bất ổn, giành lợi thế so với đối thủ cạnh tranh hoặc phổ biến thông điệp gây thù hằn chính trị, sắc tộc, tôn giáo, khuyến khích chiến tranh, khủng bố. Do đó, nhà nước cần phải mở rộng các hoạt động kiểm soát và điều chỉnh hành vi của các nhóm chủ thể. Hầu hết các quốc gia đã có quy định pháp luật nhằm ngăn chặn các dòng thông tin xấu như thông tin về khiêu dâm, lạm dụng trẻ em, về khủng bố, kỳ thị chủng tộc, tôn giáo... ảnh hưởng đến sự an toàn đối với cuộc sống của công dân nước.

Ba là, những vấn đề liên quan đến an ninh quốc gia. Hiện nay, nhiều quốc gia khai thác không gian mạng như một phương tiện nhằm đạt được lợi thế chiến lược và quân sự so với các quốc gia khác. Các hoạt động trên không gian mạng luôn gắn với chủ quyền của các chủ thể cụ thể được xác lập thông qua các mối quan hệ tài chính được bảo vệ bởi hệ thống pháp luật của các quốc gia. Do đó, các quốc gia phải kiểm soát hoạt động này như một vấn đề an ninh quốc tế⁽²⁾.

Sự khác biệt trong việc áp dụng kiểm duyệt trên mạng Internet với các chính phủ không phải là hoạt động kiểm duyệt, mà là mức độ áp dụng các quy tắc kiểm soát một cách công khai, dân chủ, công bằng thông qua một cơ quan tư pháp độc lập. Việc tạo ra công cụ pháp lý nhằm bảo đảm cho mọi cá nhân và tổ chức được bảo vệ quyền truy cập, sử dụng mà không bị làm hại hay gây hại cho chủ thể khác là vô cùng cần thiết. Các quốc gia khác nhau có những cách tiếp cận khác nhau về triết lý, nguyên tắc, cách thức vận hành, cơ quan chủ quản trong hoạt động giám sát và quản lý an ninh mạng. Trong khi một số quốc gia có kiểm duyệt Internet ở mức độ vừa phải, các quốc gia khác lại hạn chế việc tiếp cận thông tin, đặc biệt vào thời điểm các sự kiện lớn trong nước diễn ra như bầu cử, biểu tình và bạo loạn. Phản ứng với việc kiểm duyệt Internet cũng khác nhau. Trong một cuộc khảo sát của Hiệp hội Internet năm 2012, 71% người được hỏi đồng ý rằng “kiểm duyệt nên tồn tại dưới một số hình thức trên Internet”. Trong cùng một cuộc khảo sát, 83% đồng ý rằng “quyền truy cập Internet nên được coi là quyền cơ bản của con người” và

86% đồng ý rằng “quyền tự do ngôn luận cần được đảm bảo trên Internet”⁽³⁾.

2. Quan niệm của các quốc gia về an ninh mạng

a. Trung Quốc

Khái niệm chủ quyền không gian mạng bắt đầu có ảnh hưởng lớn hơn trên chính trường quốc tế vào năm 2015 khi Chủ tịch Trung Quốc Tập Cận Bình có bài phát biểu tại Hội nghị Internet thế giới (World Internet Conference) kêu gọi tất cả các nước tôn trọng chủ quyền không gian mạng. Ông nhấn mạnh vào việc tôn trọng quyết định của tất cả các quốc gia trong lựa chọn phát triển và quản lý Internet. Các quốc gia không nên cố gắng can thiệp vào công việc nội bộ của các quốc gia khác và gây nguy hiểm cho an ninh mạng của các quốc gia khác, cũng như không quốc gia nào nên cố gắng nắm giữ sức mạnh độc tôn trên Internet⁽⁴⁾. Bằng chứng của tuyên bố này là Bắc Kinh đi đầu trong việc khẳng định “chủ quyền không gian mạng” - đặt sự kiểm soát của chính phủ đối với cách Internet được vận hành và sử dụng, cũng như dữ liệu người dùng - một nguồn tài nguyên vô cùng quý giá trong nền kinh tế kỹ thuật số.

Điều này đặc biệt quan trọng với quốc gia sở hữu một trong những cơ sở mạng lớn nhất và tiên tiến nhất trên thế giới, không ngừng tăng cường tích hợp big data, điện toán đám mây và trí tuệ nhân tạo (AI). Đến năm 2025, Trung Quốc sẽ chiếm gần 30% tổng lượng dữ liệu của thế giới với nhiều kiểu dữ liệu phong phú⁽⁵⁾. Đảng Cộng sản Trung Quốc đã cố gắng duy trì quyền kiểm soát không gian mạng, đồng thời tận dụng nó như đòn bẩy cho tăng trưởng kinh tế và tiến bộ công nghệ⁽⁶⁾. Sự mở rộng của nền kinh tế dựa vào mạng Internet của Trung Quốc trên nhiều mặt của đời sống góp phần thúc đẩy tăng trưởng quốc gia, đồng thời cung cấp cho chính quyền Trung Quốc các công cụ mới để giám sát và kiểm duyệt.

Cụ thể, Trung Quốc là nước có chính sách quản lý mạng Internet chặt nhất trên thế giới. Các công cụ cụ thể mà chính quyền Trung Quốc sử dụng để đẩy mạnh quyền lực trên Internet của mình là: Luật An ninh mạng, Cơ quan Quản lý không gian mạng Trung Quốc (中华人民共和国国家互联网信息办公室-Cyberspace Administration of China), Dự án khiên vàng (Great Firewall, chữ Hán: 金盾工程; bính âm: jīndùn gōngchéng), Binh đoàn Ngũ Mao

Đảng (五毛党) hay hệ thống thu thập thông tin và theo dõi người dùng qua các ứng dụng công nghệ. Trong đó, Luật An ninh mạng đã được ban hành bởi Ủy ban Thường vụ Đại hội Đại biểu Nhân dân Toàn quốc Cộng hòa Nhân dân Trung Hoa vào ngày 07 tháng 11 năm 2016 và được thực hiện vào ngày 01 tháng 6 năm 2017, yêu cầu các nhà khai thác mạng lưu trữ dữ liệu trong phạm vi Trung Quốc và cho phép chính quyền Trung Quốc tiến hành kiểm tra tại chỗ đối với các hoạt động mạng của công ty⁽⁷⁾. Trung Quốc cũng kiểm soát luồng thông tin bên trong biên giới của mình, và “Great Firewall of China”, hay “Dự án Khiên vàng” - công cụ giúp nước này kiểm soát và ngăn chặn truy cập vào các trang web nước ngoài được chọn và làm chậm lưu lượng truy cập Internet xuyên biên giới⁽⁸⁾, cũng như giảm các thông tin bất lợi cho chính phủ xâm nhập vào môi trường truyền thông trong nước. Luật bảo mật dữ liệu (DSL) có hiệu lực vào tháng 6.2021 như một trụ cột mới trong khuôn khổ pháp lý của Trung Quốc về bảo mật thông tin và bảo vệ quyền riêng tư dữ liệu. Luật tập trung vào các yêu cầu về bản địa hóa dữ liệu, xuất dữ liệu và bảo vệ dữ liệu⁽⁹⁾.

Các nỗ lực có cả yếu tố nội địa và quốc tế của Trung Quốc nhằm hướng đến một mạng Internet được kiểm soát chặt chẽ hơn. Chính phủ Trung Quốc đảm bảo rằng các dịch vụ xã hội và tìm kiếm được sử dụng rộng rãi nhất của họ đều thuộc sở hữu trong nước và luật pháp của nước này hiện yêu cầu bất kỳ dịch vụ Internet nào cũng phải chia sẻ dữ liệu với chính quyền. Thông tin, tài liệu, hình ảnh, video, các cụm từ tìm kiếm cụ thể được coi là mối đe dọa đối với sự ổn định chính trị, có thể kích động bất ổn xã hội cũng bị ngăn chặn, như tham nhũng, kinh tế, các vụ bê bối về sức khỏe và môi trường, các nhóm tôn giáo nhất định và xung đột sắc tộc. Các đề cập liên quan đến các vấn đề cụ thể như: Tây Tạng hoặc Khu tự trị Tân Cương của Trung Quốc, nơi sinh sống của nhóm thiểu số Duy Ngô Nhĩ theo đạo Hồi và phong trào võ Pháp Luân Công cũng được chú ý ngăn chặn (Xu & Albert, 2017)⁽¹⁰⁾.

Lập trường rõ ràng của Trung Quốc về chủ quyền không gian mạng phù hợp với xu hướng rộng lớn hơn trong chính sách đối ngoại của nước này - chủ quyền mạng là một phần của lĩnh vực an ninh thông tin lớn hơn, quan trọng để duy trì các giá trị cốt lõi

quốc gia. Khái niệm “chủ quyền trên không gian mạng” của Trung Quốc liên quan đến nhu cầu kiểm soát các luồng thông tin về chính phủ và đảng phái, với trọng tâm là kiểm soát và quản lý những nội dung trên Internet. Việc đề cao lập trường này là tương xứng với sự tự định vị Trung Quốc như là một cường quốc có trách nhiệm trên chính trường thế giới.

Tuy nhiên, vào cuối năm 2016, lập trường của Bắc Kinh có phần dịu đi khi các quan chức Trung Quốc đưa ra và công nhận thuật ngữ “quản trị đa bên” (multiparty governance) là sự thay thế cho khái niệm “đa bên liên quan” (multi-stakeholder). Ý tưởng về chủ quyền không gian mạng này được nhấn mạnh lại trong “Chiến lược hợp tác quốc tế về không gian mạng” (International Strategy of Cooperation on Cyberspace) năm 2017, trong đó nhấn mạnh sự cần thiết của cả quản trị đa phương đối với Internet và sự tham gia của nhiều bên trong lĩnh vực - bao gồm các công ty, tổ chức và cộng đồng các công ty công nghệ⁽¹¹⁾.

b. Liên bang Nga

Coi vấn đề an ninh mạng là một ưu tiên trong chính sách an ninh quốc gia nên Nga đã xây dựng chiến lược về an ninh mạng 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 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 nhắm 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⁽¹²⁾.

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.

Để bảo đảm an ninh mạng 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 mạng của quốc gia này⁽¹³⁾. Các cơ quan này được trao thẩm quyền lớn trong bảo vệ an ninh mạng. 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.

c. Hoa Kỳ

Theo Schia và Gjesvik (2017), với việc thúc đẩy chủ quyền mạng trở thành một chương trình nghị sự quan trọng của Trung Quốc, Hoa Kỳ bày tỏ lo ngại rằng Trung Quốc sử dụng các chính sách về chủ quyền mạng như một vỏ bọc cho việc kiểm duyệt, chủ nghĩa bảo hộ và gián điệp⁽¹⁴⁾.

Trong chính sách đối nội của Hoa Kỳ, chính sách thông tin đóng một vai trò quan trọng, kể từ thời của cựu Tổng thống Bill Clinton, theo Nguyễn Việt Lâm (2019)⁽¹⁵⁾. Đến thời tổng thống George W. Bush, chính sách kiểm soát trên không gian mạng đã được thúc đẩy và trở thành một chương trình nghị sự, đặc biệt sau cuộc tấn công khủng bố ngày 11.9.2001. Chính quyền Bush đã cố gắng thiết lập sự kiểm soát thông tin không chỉ ở cấp quốc gia mà còn trên toàn cầu.

Chính quyền Barack Obama xác định ưu tiên trong lĩnh vực an ninh thông qua Chiến lược quốc tế về không gian mạng⁽¹⁶⁾, bao gồm hai phần: (I) Thịnh vượng, an ninh và sự cởi mở trong thế giới mạng và (II) Chiến lược của Bộ Quốc phòng về hoạt động trong không gian mạng, trong sự phối hợp với các đối tác quốc tế. Chiến lược này của chính phủ dưới thời Barack Obama cho thấy một ý định rõ ràng về việc xây dựng một trật tự mới trong không gian mạng quốc tế, với vai trò đi đầu của nước Hoa kỳ. Trong thư mở đầu của chiến lược, ông Obama nhấn mạnh cam kết tham gia của Hoa kỳ với các đối tác trong nước và quốc tế để bảo vệ những thuộc tính của mạng Internet - tự tổ chức, có sự tham gia quản lý của nhiều bên (nhà nước, người dân, xã hội dân sự, giới học thuật, khu vực tư nhân...). Trong Sắc lệnh mới về An ninh mạng của Hoa kỳ ngày 11.5.2017 dưới thời Tổng thống Donald Trump⁽¹⁷⁾, mục tiêu chính sách của Hoa kỳ trong vấn đề an ninh mạng là thúc đẩy một không gian rộng mở, đáng tin cậy và an toàn nhằm tăng cường tính hiệu quả, sáng tạo, giao lưu và thịnh vượng kinh tế; đồng thời tôn trọng quyền riêng tư và chống lại sự gián đoạn các dịch vụ mạng, gian lận và trộm cắp trên không gian mạng. Bên cạnh đó, Hoa kỳ cũng thúc đẩy phát triển nguồn nhân lực trong lĩnh vực không gian mạng.

Như thế, có thể thấy Hoa kỳ đã có những động thái siết chặt hơn kiểm soát trên không gian mạng, chống lại sự tấn công của những tác nhân nước ngoài. Tuy nhiên, Hoa kỳ chưa từng công khai thể hiện sự ủng hộ với việc rạch ròi một biên giới trên không gian mạng. Chính sách của Hoa kỳ trên không gian mạng luôn là tăng cường sự hợp tác quốc tế, nhằm bảo vệ tính cởi mở, an toàn và thịnh vượng của mạng Internet, với trách nhiệm của một cường quốc trong cam kết về các vấn đề trên không gian mạng. Những giá trị cốt lõi mà Hoa kỳ đề cao trên Internet là: tự do ngôn luận, tự do liên kết, quyền riêng tư, và dòng chảy tự do của thông tin. Đây là điều khác biệt cơ bản trong cách tiếp cận về không gian mạng giữa hai cường quốc Hoa kỳ và Trung Quốc.

d. Các quốc gia khác

Nhiều chính phủ trên khắp thế giới, coi Internet là mối đe dọa đối với quyền riêng tư, bình đẳng, văn hóa địa phương, thông tin chính thống và bình ổn quốc gia. Trong thư ngày 12 tháng 9 năm 2011 của

Đại diện thường trực 4 nước gồm Trung Quốc, Liên bang Nga, Tajikistan và Uzbekistan gửi Liên hợp quốc cụ thể là Tổng thư ký Ban Ki-moon, đề nghị phát thảo Bộ quy tắc ứng xử quốc tế về an ninh thông tin đã được soạn bởi các quốc gia này, coi đó là tài liệu chính thức của kỳ họp thứ 66 của Đại hội đồng và kêu gọi các quốc gia thảo luận thêm về văn kiện này trong khuôn khổ Liên hợp quốc để đạt được sự đồng thuận về các chuẩn mực và quy tắc quốc tế liên quan đến thông tin và không gian mạng⁽¹⁸⁾. Cho đến nay, các nỗ lực để đạt được các thỏa thuận quốc tế nhằm xây dựng bộ quy tắc ứng xử trên không gian mạng vẫn tiếp tục được nhấn mạnh.

Việc ban hành các quy định và luật cho phép chính phủ tăng cường quyền kiểm soát đối với Internet không chỉ có ở Trung Quốc hay Nga. Theo Tổ chức Freedom House, trong năm 2018, “ít nhất 17 quốc gia đã thông qua hoặc đề xuất luật hạn chế phương tiện truyền thông trực tuyến dưới danh nghĩa chống lại “tin tức giả mạo” và “thao túng trực tuyến”⁽¹⁹⁾. Thế giới đã đi đến nhiều đồng thuận trong việc cần phải bảo vệ chủ quyền quốc gia trên không gian mạng nhưng vẫn chưa đi đến thống nhất để xây dựng, thiết lập các nguyên tắc pháp lý mang tính quốc tế đối với các hoạt động này. Các nước châu Âu như Anh, Ba Lan và Hungary cũng đã có những động thái tương tự, là biểu hiện rằng ranh giới “dân chủ” - “không dân chủ” về vấn đề kiểm duyệt trên Internet đã không còn rõ ràng như trước. Liên minh châu Âu có Công ước Budapest năm 2001 nhằm thiết lập khuôn khổ pháp lý chung cho các quốc gia châu Âu trong công tác phòng chống tội phạm mạng. Đến nay công ước đã được đàm phán và mở rộng cho các quốc gia thành viên ở châu Á như: Nhật Bản, Philippines. Cách tiếp cận này cũng được ưa chuộng ở các quốc gia đang phát triển, những nước đang gặp bất lợi về kỹ thuật số và dễ bị ảnh hưởng bởi toàn cầu hóa.

Các nước ASEAN cũng ngày càng tăng cường phối hợp trong một cộng đồng với nhu cầu đảm bảo an ninh mạng, phối hợp tổng thể thông qua các diễn đàn khu vực và các cuộc họp cấp cao. Tuy nhiên, theo Nguyễn Việt Lâm (2019)⁽²⁰⁾, các nước có các cách tiếp cận khác nhau đối với vấn đề này: Việt Nam và Myanmar có xu hướng kiểm soát chặt chẽ nhằm ngăn các nội dung xấu, độc hại; còn các quốc gia

khác như Thái Lan, Philippines lại nói lỏng hơn với các việc kiểm soát thông tin trên mạng.

Cho đến nay, thế giới mới chỉ có các thỏa thuận riêng lẻ giữa các quốc gia trong từng khu vực liên quan đến đảm bảo an ninh mạng mà chưa có các quy chuẩn pháp lý mang tính quốc tế để điều chỉnh các hoạt động trên lĩnh vực này. Việc thiếu cơ sở pháp lý mang tính quốc tế khiến cho việc thực hiện các hoạt động bảo vệ chủ quyền trên không gian mạng của quốc gia gặp nhiều khó khăn, cũng như các hoạt động hợp tác, phối hợp trong bảo vệ chủ quyền của các quốc gia sẽ không được thúc đẩy trên thực tế.

3. Quan niệm của Việt Nam về an ninh mạng

Chính phủ Việt Nam triển khai các hoạt động bảo vệ chủ quyền quốc gia trên không gian mạng, triển khai các hoạt động quản lý nhà nước về an ninh mạng không đi ngược lại tinh thần bảo vệ các quyền cơ bản của con người đã được ghi nhận trong hệ thống luật nhân quyền quốc tế, trong Hiến pháp, pháp luật quốc gia. Tuy nhiên, những thách thức chúng ta cần đối diện trên không gian mạng ngày càng tăng. Thời gian qua, Việt Nam cũng chịu nhiều đợt tấn công nhằm vào các hệ thống thông tin quốc gia, phát tán thông tin sai sự thật để lừa đảo, chiếm đoạt tài sản. Kể từ năm 2020, do ảnh hưởng từ dịch Covid-19, người dùng chuyển dần các hoạt động lên không gian mạng trực tuyến nhiều hơn - mỗi ngày, trung bình một người Việt Nam trực tuyến trên Internet khoảng gần 7 giờ. Đối tượng sử dụng mạng giờ đã mở rộng ra cả trẻ em và người chưa thành niên, đây là công cụ giúp các em duy trì việc học tập, giải trí, giữ liên hệ với bạn bè. Thời lượng này sẽ tiếp tục tăng lên và người sử dụng Internet ngày càng nhiều, đồng nghĩa với nguy cơ mất an toàn an ninh mạng sẽ cao và ngày càng phức tạp hơn. Trung tâm Công nghệ thông tin và Giám sát an ninh mạng, Ban Cơ yếu Chính phủ, trong 6 tháng đầu 2022 đã ghi nhận 48.646 cuộc tấn công mạng vào các hệ thống công nghệ thông tin trọng yếu của các cơ quan chính phủ⁽²¹⁾.

Chính phủ Việt Nam đã có nhiều chủ trương, chính sách đẩy mạnh ứng dụng, phát triển công nghệ thông tin phục vụ phát triển kinh tế - xã hội, bảo đảm quốc phòng, an ninh. Bảo vệ an ninh quốc gia trên không gian mạng được coi là một ưu tiên liên quan đến chế độ chính trị và Nhà nước, độc lập, chủ quyền,

thống nhất, toàn vẹn lãnh thổ Việt Nam trên không gian mạng; nhằm bảo vệ an ninh về tư tưởng và văn hóa, khối đại đoàn kết toàn dân tộc, quyền lợi và lợi ích hợp pháp của các cơ quan, tổ chức, cá nhân trên không gian mạng. Không gian mạng quốc gia được hiểu là không gian mạng do Nhà nước xác lập, quản lý và kiểm soát. Nhiều chính sách, pháp luật được ban hành như Luật An ninh mạng, Luật An toàn thông tin mạng, Luật Bảo vệ bí mật nhà nước và các văn bản hướng dẫn thi hành.

Luật An ninh mạng được Quốc hội thông qua thể hiện nỗ lực của Đảng và Nhà nước trong việc tạo ra công cụ pháp lý nhằm bảo đảm cho mọi cá nhân và tổ chức được bảo vệ quyền truy cập, sử dụng mạng cho mục đích cá nhân của mình mà không bị làm hại hay gây hại cho chủ thể khác. Theo Luật An ninh mạng: “Nhà nước áp dụng các biện pháp để bảo vệ không gian mạng quốc gia; phòng ngừa, xử lý hành vi xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng”⁽²²⁾. Nhà nước Việt Nam áp dụng các biện pháp và ban hành các bộ luật để bảo vệ không gian mạng quốc gia; phòng ngừa, xử lý hành vi xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng.

Nghị quyết số 52-NQ/TW, ngày 27.9.2019, của Bộ Chính trị, “Về một số chủ trương, chính sách chủ động tham gia cuộc Cách mạng công nghiệp lần thứ tư”, cũng nhấn mạnh các chủ trương về bảo vệ Tổ quốc trên không gian mạng, bảo vệ an ninh mạng quốc gia nhằm nâng cao tiềm lực khoa học, công nghệ cũng như năng lực bảo đảm an ninh mạng, phòng, chống chiến tranh mạng. Nghị định số 53/2022/NĐ-CP cũng quy định hoàn thiện phương án bảo đảm an ninh mạng đối với hệ thống thông tin của cơ quan nhà nước. Điều đó cho thấy sự quan tâm tích cực của chính phủ Việt Nam trong hoạt động bảo vệ an ninh mạng, đặc biệt là cơ quan nhà nước.

Tuy nhiên, cũng có thể khẳng định, các khung pháp lý về dữ liệu và quyền riêng tư của các cá nhân, tổ chức ở Việt Nam vẫn còn hạn chế. Sự phát triển của các loại hình tội phạm trên mạng đòi hỏi không chỉ đầu tư quy trình, thiết bị và con người mà còn phải nắm bắt kịp thời các xu thế tấn công, chủ động phòng ngừa, để đảm bảo an toàn và bền vững của hệ

thống thông tin. Hoàng Thị Quyên (2021) chỉ ra một số thách thức cơ bản trong tiến trình phát triển nhận thức cũng như hoạt động mà các quốc gia đã triển khai nhằm bảo vệ chủ quyền của mình trên không gian mạng, đặc biệt là ở Việt Nam, chẳng hạn như thiếu cơ sở pháp lý cũng như các cơ chế hợp tác quốc tế để bảo vệ chủ quyền quốc gia trên không gian mạng, năng lực thực thi của các quốc gia. Tại nước ta, nhiều người cũng đặt ra câu hỏi là: liệu Việt Nam có nên thiết lập một hệ thống mạng riêng cho người Việt giống như những gì mà Trung Quốc đang thực hiện? Bên cạnh đó, cũng phải thừa nhận thách thức trong việc xác định ranh giới giữa hoạt động bảo vệ chủ quyền quốc gia trên không gian mạng với các hoạt động được coi là vi phạm quyền tự do cơ bản của con người⁽²³⁾.

4. Kết luận

Với những tiến bộ về công nghệ - khoa học kỹ thuật được ứng dụng trong lĩnh vực truyền thông xã hội, vai trò của các nền tảng truyền thông trong quan hệ quốc tế, chính trị, xã hội ngày càng được nâng cao. Với tầm nhìn xa về mối quan hệ giữa mạng xã hội và tuyên truyền, Trung Quốc đã nhanh tay khởi động các chính sách, các điều luật và dự án, lãnh đạo trong việc đề cao xu thế chủ quyền mạng. Trung Quốc đã xây dựng được một thương hiệu quốc gia về vấn đề chủ quyền không gian mạng và an ninh mạng. Khái niệm an ninh mạng đã có nhiều phát triển từ khái niệm “an ninh quốc gia” truyền thống, hay khái niệm “an ninh phi truyền thống”, tuy nhiên vẫn là chủ đề gây tranh cãi, từ đó chưa thể xây dựng, thiết lập các nguyên tắc pháp lý mang tính quốc tế đối với các hoạt động bảo đảm an ninh thông tin quốc tế và hòa bình trên không gian mạng.

Ở Việt Nam cũng đã có những nỗ lực trong công tác quản lý tài nguyên mạng xã hội, rõ nhất là mốc ngày 01.01.2019, Luật An ninh mạng bắt đầu chính thức có hiệu lực. Điều đó cho thấy những mối đe dọa từ mạng Internet, việc nâng cao ý thức bảo vệ chủ quyền quốc gia trên không gian mạng trong thời đại công nghệ số và những khuôn khổ pháp lý kịp thời, hợp lý, hiệu quả. Tuy nhiên, cũng cần có những chủ trương mới, bắt kịp với xu hướng phát triển không ngừng của Internet, nhằm bảo vệ quyền lợi của người dùng và lợi ích quốc gia./.

* Bài viết là kết quả nghiên cứu trong khuôn khổ Đề tài cấp nhà nước KX04.32: “*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) Clark, J. D., Faris, R. M., Morrison-Westphal, R. J., Noman, H., Tilton, C. B., & Zittrain, J. L. (2017). The shifting landscape of global internet censorship. *Berkman Klein Center*, 17-38.

(2) Hoàng Thị Quyên. 2021. Bảo vệ chủ quyền quốc gia trên không gian mạng trong thời đại công nghệ số. Tạp chí Lý luận chính trị, truy cập ngày 15 tháng 4 năm 2021. <<http://lyluanchinhtri.vn/home/index.php/dien-dan/item/3385-bao-ve-chu-quyen-quoc-gia-tren-khong-gian-mang-trong-thoi-dai-cong-nghe-so.html>>

(3) “Global Internet User Survey 2012”. Archived 14 March 2013, Internet Society, 20 November 2012, truy cập ngày 20 tháng 4 năm 2021. <https://web.archive.org/web/20130314063616/https://www.internetsociety.org/sites/default/files/GIUS2012-GlobalData-Table-20121120_0.pdf>

(4) Remarks by H.E. Xi Jinping President of the People’s Republic of China At the Opening Ceremony of the Second World Internet Conference, 16 December 2015. https://www.fmprc.gov.cn/eng/wjdt_665385/zyjh_665391/201512/t20151224_678467.html

(5) Yi Wu (2022). Understanding China’s Digital Economy: Policies, Opportunities, and Challenges. <https://www.china-briefing.com/news/understanding-chinas-digital-economy-policies-opportunities-and-challenges/>

(6) Katja Drinhausen and John Lee (2021). The CCP in 2021: smart governance, cyber sovereignty and tech supremacy. <https://merics.org/en/ccp-2021-smart-governance-cyber-sovereignty-and-tech-supremacy>

(7) Wagner, Jack. (ngày 1 tháng 6 năm 2017). “China’s Cybersecurity Law: What You Need to Know”. <https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/>

(8) Mozur, Paul (13 September 2015). “Baidu and Cloud-Flare Boost Users Over China’s Great Firewall”. The New York Times. Archived from the original on 24 January 2019.

(9) Abby Chen (2021). A Close Reading of China’s Data Security Law, in Effect Sept. 1, 2021. <https://www.china-briefing.com/news/a-close-reading-of-chinas-data-security-law-in-effect-sept-1-2021/>

(10) Xu, B. & Albert E., 2017, “Media Censorship in China”, Council on Foreign Relations, ngày 17 tháng 02, truy cập ngày 21 tháng 04 năm 2021. <https://www.cfr.org/backgrounder/media-censorship-china>

(11) Xinhuanet (2017). International Strategy of Cooper-

ation on Cyberspace. http://www.xinhuanet.com/english/china/2017-03/01/c_136094371_2.htm

(12) 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.

(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, Hà Nội, tr. 61.

(14) Schia, N., Gjesvik, L. 2017. China’s cyber sovereignty. Norwegian Institute for International Affairs , NUPI, truy cập ngày 14 tháng 04 năm 2021. <<http://www.jstor.com/stable/resrep07952>>

(15) 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.

(16) The White House, 2011, ‘International strategy for cyberspace: prosperity, security, and openness in a networked world’, truy cập ngày 11 tháng 04 năm 2021. <https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>

(17) A Presidential Document by the Executive Office of the President on 05.16.2017, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. <https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure>

(18) Ministry of Foreign Affairs, the People’s Republic of China (2011). China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations. https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zjjg_663340/jks_665232/jkxw_665234/201109/t20110914_599206.html

(19) Shahbaz, A. 2017, “The Rise of Digital Authoritarianism”, *Freedom House*, truy cập ngày 20 tháng 04 năm 2021. <<https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism>>

(20) 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.

(21) 6 tháng đầu năm 2022 ghi nhận hơn 48.600 cuộc tấn công vào các hệ thống CNTT trọng yếu. <http://antoanthongtin.vn/chinh-sach-chien-luoc/6-thang-dau-nam-2022-ghi-nhan-hon-48600-cuoc-tan-cong-vao-cac-he-thong-cntt-trong-yeu-108183>

(22) <https://pbgdpl.moj.gov.vn/qt/tintuc/Lists/ToGap/Attachments/323/To%20gap%2003.pdf>

(23) Hoàng Thị Quyên 2021, “Bảo vệ chủ quyền quốc gia trên không gian mạng trong thời đại công nghệ số”, *Tạp chí Lý luận chính trị online*, truy cập ngày 01 tháng 03 năm 2021. <<http://lyluanchinhtri.vn/home/index.php/dien-dan/item/3385-bao-ve-chu-quyen-quoc-gia-tren-khong-gian-mang-trong-thoi-dai-cong-nghe-so.html>>.