

Vai trò của báo chí trong bảo vệ an ninh quốc gia trên không gian số tại Việt Nam

Role of the press in safeguarding national security in Vietnam's digital space

Font chữ UTM sử dụng
bảng mã UNICODE
để thiết lập lại
tính điều khiển bản phẩm

TS. NGUYỄN ĐĂNG KHANG

Báo Đại đoàn kết; Email: dangkhangcand@gmail.vn

Ngày nhận bài: 11/05/2026

Ngày phản biện: 17/05/2026

Ngày duyệt đăng: 20/6/2026

Chủ đề của bài viết thuộc lĩnh vực: Báo chí truyền thông.

Tóm tắt: Bài viết nghiên cứu vai trò chủ lực của báo chí cách mạng Việt Nam trong việc bảo vệ nền tảng tư tưởng của Đảng, giữ vững chủ quyền thông tin và ứng phó với các thách thức phi truyền thống như tin giả, công nghệ deepfake và các chiến dịch thao túng dư luận. Bằng phương pháp phân tích tài liệu và tiếp cận từ thuyết sinh thái học truyền thông, thuyết an ninh hóa, nghiên cứu bước đầu cho thấy báo chí đang từng bước đảm nhiệm chức năng phản gián thông tin trong môi trường số. Kết quả nghiên cứu cho thấy năng lực thực hiện vai trò bảo vệ an ninh quốc gia của báo chí Việt Nam hiện nay đang chịu tác động đáng kể từ hai thách thức cơ bản: sự suy giảm nguồn lực kinh tế của các cơ quan báo chí và mức độ phụ thuộc ngày càng lớn vào các nền tảng truyền thông số xuyên biên giới trong hoạt động phân phối nội dung. Từ đó, bài viết đề xuất các giải pháp nhằm củng cố năng lực phòng vệ thông tin quốc gia thông qua bảo đảm nguồn lực phát triển báo chí, nâng cao mức độ tự chủ công nghệ, hoàn thiện thể chế quản trị không gian số và tăng cường năng lực hiểu biết truyền thông của công chúng.

Từ khóa: an ninh quốc gia; báo chí cách mạng; chủ quyền số; phản gián thông tin; an ninh không gian mạng.

Abstract: This article examines the leading role of Vietnam's revolutionary press in defending the Party's ideological foundation, protecting information sovereignty, and addressing non-traditional security challenges such as fake news, deepfake technology, and public opinion manipulation campaigns. Employing document analysis and drawing upon media ecology theory and securitization theory, the study provides preliminary evidence that the press is increasingly assuming the function of information counterintelligence in the digital environment. The findings indicate that the Vietnamese press's capacity to safeguard national security is currently constrained by two major challenges: the declining financial resources of press organizations and their growing dependence on cross-border digital media platforms for content distribution. Accordingly, the article proposes measures to strengthen national information security by ensuring sustainable resources for press development, enhancing technological autonomy, improving the governance framework for cyberspace, and promoting public media literacy.

Keywords: national security; revolutionary press; digital sovereignty; information counterintelligence; cybersecurity.

1. Đặt vấn đề

Bảo vệ an ninh quốc gia (ANQG) là nhiệm vụ trọng yếu, thường xuyên, là điều kiện tiên quyết để phát triển đất nước bền vững. Trong văn kiện Đại hội XIII, Đảng Cộng sản Việt Nam đã khẳng định việc mở rộng nội hàm ANQG, không chỉ giới hạn ở bảo vệ biên giới lãnh thổ mà còn bao gồm cả an ninh truyền thống và an ninh phi truyền thống, trong đó an ninh mạng và chủ quyền thông tin giữ vị trí đặc biệt quan trọng (Nguyễn Văn Thành & Lục Anh

Tuấn, 2024). Trong bối cảnh không gian mạng trở thành một môi trường cạnh tranh thông tin ngày càng phức tạp, báo chí cách mạng Việt Nam tiếp tục giữ vai trò quan trọng trong định hướng dư luận xã hội, bảo vệ nền tảng tư tưởng của Đảng và củng cố niềm tin công chúng đối với các chủ trương, chính sách của Nhà nước.

Tuy nhiên, kỷ nguyên số với sự trỗi dậy của các công nghệ thuật toán và trí tuệ nhân tạo (AI) đã tạo ra những thách thức chưa từng có. Những năm gần đây, không gian

mạng tại Việt Nam chứng kiến sự gia tăng nhanh chóng của các dạng thông tin sai lệch, giả mạo và kích động cảm xúc xã hội. Theo Báo cáo nghiên cứu, khảo sát an ninh mạng năm 2025 của Hiệp hội An ninh mạng Quốc gia, [các hình thức lừa đảo trực tuyến, giả mạo danh tính và phát tán thông tin sai lệch tiếp tục diễn biến phức tạp, gây thiệt hại lớn về kinh tế và tác động tiêu cực đến niềm tin xã hội (NCA, 2025). Khác với giai đoạn trước, các chiến dịch gây nhiễu hiện nay không còn tồn tại dưới dạng tin giả đơn lẻ mà được tổ chức theo hướng có chủ đích, tận dụng thuật toán phân phối nội dung của mạng xã hội để mở rộng mức độ lan truyền. Trong nhiều vụ việc, tốc độ lan tỏa của thông tin sai lệch thậm chí vượt xa khả năng phản hồi của báo chí chính thống. Thực tế cho thấy, tin giả và công nghệ deepfake ngày càng được sử dụng trong các hoạt động thao túng thông tin và gây ảnh hưởng tới niềm tin xã hội. Theo Hiệp hội An ninh mạng Quốc gia (NCA, 2025), [chỉ trong 11 tháng đầu năm 2025, người dùng Internet tại Việt Nam đã thiệt hại hơn 6.000 tỷ đồng do các hoạt động lừa đảo trực tuyến. Chẳng hạn, nhiều vụ giả mạo người thân qua video call trên Facebook và Zalo trong năm 2025 đã cho thấy khả năng AI tạo sinh bị lợi dụng để tạo dựng niềm tin giả đối với nạn nhân.

Bài viết tập trung phân tích vai trò của báo chí Việt Nam trong bảo vệ an ninh quốc gia trên không gian số, nhận diện những thách thức đặt ra đối với hoạt động báo chí trong môi trường truyền thông số và đề xuất một số giải pháp nhằm nâng cao hiệu quả thực hiện nhiệm vụ này trong giai đoạn hiện nay.

2. Phương pháp nghiên cứu

Để đảm bảo tính khoa học và chiều sâu lý luận, nghiên cứu áp dụng cách tiếp cận định tính kết hợp với phân tích dữ liệu thứ cấp từ các tổ chức uy tín.

Phương pháp phân tích tài liệu: Tác giả tiến hành rà soát, hệ thống hóa và phân tích các văn bản quy phạm pháp luật liên quan như Luật An ninh mạng 2018, Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, Luật Dữ liệu 2024 cùng các báo cáo chiến lược về an ninh mạng và truyền thông số (Chính phủ, 2023; NCA, 2025; Quốc hội, 2024). Việc phân tích các nghị quyết chuyên đề của Đảng, đặc biệt là Nghị quyết số 35-NQ/TW của Bộ Chính trị (Ban Tuyên giáo Trung ương, 2018) cũng giúp xác định định hướng chính trị cốt lõi của hoạt động báo chí.

Phương pháp phân tích nội dung: Nghiên cứu tiến hành phân tích các xu hướng thông tin sai lệch, mô hình lan truyền tin giả và các sản phẩm deepfake tiêu biểu trên các nền tảng số xuyên biên giới trong giai đoạn 2024 - 2025 nhằm nhận diện đặc điểm vận hành, cơ chế khuếch

tán và tác động của các hình thức thao túng thông tin trong môi trường truyền thông số.

Nghiên cứu không hướng tới đo lường định lượng hiệu quả hoạt động báo chí mà tập trung phân tích vai trò, xu hướng và những thách thức đặt ra đối với báo chí Việt Nam trong bảo vệ an ninh quốc gia trên không gian số.

3. Kết quả nghiên cứu

3.1. Những thách thức đối với bảo vệ an ninh quốc gia trên không gian số

3.1.1. Sự gia tăng các mối đe dọa thông tin trong môi trường số

Sự phát triển nhanh chóng của công nghệ số, đặc biệt là trí tuệ nhân tạo tạo sinh (Generative AI), đang làm xuất hiện nhiều hình thức đe dọa mới đối với an ninh quốc gia trên không gian số. Theo Trần Thành Nam (2026), [công nghệ AI tạo sinh cho phép sản xuất các nội dung giả mạo dưới dạng hình ảnh, âm thanh và video với mức độ chân thực ngày càng cao, gây khó khăn cho quá trình nhận diện thông tin xác thực của công chúng. Trong thực tế, nhiều vụ lừa đảo gần đây đã sử dụng công nghệ giả giọng nói và hình ảnh để tạo dựng lòng tin đối với nạn nhân thông qua các cuộc gọi video trên mạng xã hội. Một số trường hợp giả danh người thân hoặc cán bộ cơ quan nhà nước đã gây thiệt hại đáng kể về tài chính và tạo tâm lý bất an trong xã hội.

Theo Báo cáo nghiên cứu, khảo sát an ninh mạng năm 2025 của Hiệp hội An ninh mạng Quốc gia, [thiệt hại do lừa đảo trực tuyến tại Việt Nam vẫn ở mức cao mặc dù tỷ lệ nạn nhân có xu hướng giảm nhờ các biện pháp xác thực sinh trắc học (NCA, 2025). Hồng Đạt (2026) nhận định rằng [các đối tượng lừa đảo đang ngày càng sử dụng AI để cá nhân hóa nội dung tấn công, qua đó nâng cao khả năng thuyết phục và mức độ nguy hiểm của các hành vi lừa đảo trên không gian mạng.

3.1.2. Sự lan truyền của thông tin sai lệch và thao túng nhận thức

Bên cạnh các hình thức lừa đảo công nghệ cao, không gian số còn chứng kiến sự gia tăng của các chiến dịch phát tán thông tin sai lệch có tổ chức. Khác với giai đoạn trước, các nội dung gây nhiễu hiện nay không còn tồn tại dưới dạng tin giả đơn lẻ mà được khuếch tán thông qua các mạng lưới tài khoản liên kết, tận dụng thuật toán của nền tảng số để mở rộng phạm vi ảnh hưởng. Trong nhiều trường hợp, tốc độ lan truyền của thông tin sai lệch vượt xa tốc độ kiểm chứng và phản hồi của các cơ quan truyền thông chính thống. Điều này không chỉ gây nhiễu loạn môi trường thông tin mà còn tác động tiêu cực đến niềm tin xã hội và hiệu quả quản trị quốc gia trên không gian mạng.

Theo Pauwels (2024), [sự kết hợp giữa thuật toán nền

tăng, các hệ thống tự động hóa và công nghệ AI tạo sinh đang làm gia tăng khả năng khuếch đại thông tin sai lệch trên môi trường số. Một đặc điểm đáng chú ý của môi trường truyền thông số hiện nay là vai trò ngày càng lớn của thuật toán phân phối nội dung và các mạng lưới tài khoản tự động (bot). Nhiều nghiên cứu cho thấy các hệ thống thuật toán thường ưu tiên những nội dung có khả năng tạo tương tác cao, đặc biệt là các thông tin gây tranh cãi, kích động cảm xúc hoặc tạo ra phản ứng mạnh từ người dùng. Trong khi đó, các mạng lưới bot có thể được sử dụng để khuếch đại nhân tạo mức độ phổ biến của một thông tin, tạo cảm giác về sự đồng thuận xã hội đối với những nội dung chưa được kiểm chứng. Quá trình này góp phần hình thành các buồng vọng âm (echo chamber) (Kolotaev, 2026), nơi người dùng chủ yếu tiếp xúc với các quan điểm tương đồng và ít có cơ hội tiếp cận các nguồn thông tin đa chiều. Hệ quả là nhận thức xã hội có thể bị dẫn dắt theo những khuynh hướng sai lệch, làm gia tăng nguy cơ phân cực thông tin và gây khó khăn cho hoạt động định hướng dư luận của báo chí chính thống.

3.2. Vai trò của báo chí trong bảo vệ an ninh quốc gia trên không gian số

3.2.1. Báo chí định hướng dư luận và kiểm chứng thông tin

Trong các tình huống khủng hoảng thông tin, công chúng thường tìm đến các nguồn tin chính thống để kiểm chứng các nội dung lan truyền trên mạng xã hội. Theo Nguyễn Văn Thành và Lục Anh Tuấn (2024), báo chí giữ vai trò quan trọng trong định hướng dư luận xã hội, đấu tranh với các thông tin sai lệch và củng cố niềm tin của nhân dân đối với Đảng và Nhà nước. Trong thực tiễn nhiều cơ quan báo chí chủ lực như Báo Nhân Dân, Thông tấn xã Việt Nam và Đài Truyền hình Việt Nam đã xây dựng các chuyên mục chuyên trách nhằm phát hiện, phân tích và phản bác thông tin sai trái trên không gian mạng.

3.2.2. Báo chí thực hiện chức năng phản gián thông tin

Sự phát triển của chiến tranh thông tin đòi hỏi báo chí không chỉ thực hiện chức năng truyền tải thông tin mà còn phải tham gia chủ động vào quá trình phát hiện và hạn chế các chiến dịch thao túng nhận thức xã hội. Hiện nay, báo chí Việt Nam đang từng bước chuyển từ mô hình phản ứng sau khi thông tin sai lệch xuất hiện sang hướng chủ động cảnh báo sớm, nhận diện xu hướng thông tin bất thường và hỗ trợ công chúng nâng cao năng lực tự kiểm chứng thông tin. Đây cũng là cơ sở thực tiễn để nghiên cứu bước đầu tiếp cận khái niệm phản gián thông tin (Information Counter-Intelligence - ICI) trong hoạt động báo chí.

Phản gián thông tin (ICI) trong báo chí không phải là một thuật ngữ tự thân của ngành báo chí mà là sự giao thoa giữa báo chí và an ninh học. Trong phạm vi nghiên cứu này, tác giả đề xuất cách tiếp cận ban đầu về khái niệm: ICI trong báo chí là hệ thống các hoạt động nghiệp vụ (theo dõi, giải mã và phản bác) nhằm phát hiện sớm các chiến dịch thao túng nhận thức của các chủ thể tiến hành thao túng thông tin và hạn chế tác động lan truyền của các mạng lưới tin giả có tổ chức trước khi chúng tạo ra rủi ro truyền thông và bất ổn xã hội trên diện rộng. Khác với hoạt động fact-checking vốn chủ yếu tập trung vào xác minh tính đúng sai của từng nội dung cụ thể, ICI hướng tới nhận diện cấu trúc vận hành, động cơ và phương thức lan truyền của các chiến dịch thao túng thông tin có tổ chức. Do đó, ICI không chỉ mang tính phản ứng nội dung mà còn bao gồm yếu tố dự báo và phòng ngừa trong môi trường truyền thông số. Khái niệm này hiện vẫn mang tính gợi mở và cần được tiếp tục kiểm chứng thông qua các nghiên cứu thực nghiệm.

Để làm rõ, ICI cần được phân biệt với ba khái niệm liên quan:

Chống tin giả: Mang tính kỹ thuật và bị động, tập trung vào việc đính chính một mẫu tin cụ thể (fact-checking) (Pauwels, 2024).

Truyền thông chiến lược: Tập trung vào việc chủ động xây dựng và lan tỏa thông điệp tích cực của Nhà nước (Nguyễn Văn Thành & Lục Anh Tuấn, 2024).

Chiến tranh thông tin: Là phạm trù bao trùm, bao gồm cả tấn công và phòng thủ thông tin trên quy mô quốc gia (Kolotaev, 2026).

Ngược lại, ICI trong báo chí tập trung vào việc giải mã nguồn gốc và động cơ của thông tin sai lệch có chủ đích, góp phần bảo vệ nhận thức công chúng. Mặc dù ICI là khái niệm mới, tuy nhiên một số hoạt động mang tính chất của cách tiếp cận này đã xuất hiện trong thực tiễn báo chí Việt Nam. Chẳng hạn, chiến dịch "Chống lừa đảo trực tuyến 2025" với sự tham gia của nhiều cơ quan báo chí đã góp phần nâng cao nhận thức cộng đồng và giảm tỷ lệ người dùng trở thành nạn nhân của các hình thức lừa đảo trực tuyến (NCA, 2025).

3.3. Những rào cản đối với việc phát huy vai trò của báo chí

3.3.1. Suy giảm nguồn lực kinh tế báo chí

Theo HTV Tin tức (2024), doanh thu quảng cáo của báo in và báo điện tử tại Việt Nam năm 2024 đạt hơn 8.000 tỷ đồng, giảm 6,1% so với năm trước. Xu hướng suy giảm nguồn thu đang tạo áp lực đáng kể đối với hoạt động chuyển đổi số, đầu tư công nghệ và phát triển nguồn nhân

lực của các cơ quan báo chí. Đồng thời, xu hướng dịch chuyển doanh thu quảng cáo số sang các nền tảng xuyên biên giới đang tạo thêm áp lực cạnh tranh đối với các cơ quan báo chí trong nước.

3.3.2. Hạn chế về tự chủ công nghệ và phụ thuộc nền tảng

Bên cạnh vấn đề kinh tế, sự phụ thuộc ngày càng lớn vào các nền tảng số xuyên biên giới cũng đang đặt ra những thách thức đáng kể đối với báo chí Việt Nam. Phần lớn lưu lượng truy cập và phân phối nội dung hiện nay được thực hiện thông qua các nền tảng mạng xã hội và công cụ tìm kiếm nước ngoài. Điều này làm giảm mức độ chủ động của các cơ quan báo chí trong tiếp cận công chúng, đồng thời tiềm ẩn nguy cơ bị chi phối bởi các thuật toán phân phối nội dung nằm ngoài khả năng kiểm soát của Việt Nam. Trong bối cảnh đó, tự chủ công nghệ và chủ quyền nền tảng đang trở thành những điều kiện quan trọng để báo chí phát huy hiệu quả vai trò bảo vệ an ninh quốc gia trên không gian số.

4. Thảo luận kết quả nghiên cứu

- Về lý thuyết An ninh hóa (Securitization Theory):

Trường phái Copenhagen cho rằng an ninh không phải là một trạng thái khách quan mà được hình thành thông qua "phát ngôn an ninh" (speech act), trong đó "một vấn đề được kiến tạo như một mối đe dọa cần có biện pháp can thiệp đặc biệt" (Buzan et al., 1998). Khi vấn đề bảo vệ nền tảng tư tưởng và chủ quyền thông tin được đặt trong khuôn khổ an ninh quốc gia, báo chí trở thành một trong những chủ thể tham gia kiến tạo diễn ngôn an ninh trên không gian truyền thông. Trong thực tế "nếu báo chí chạy theo xu hướng thương mại hóa nội dung hoặc ưu tiên các chiến lược thu hút tương tác cực đoan (clickbait), vai trò định hướng và tính chính danh của báo chí trong môi trường thông tin số có thể bị suy giảm" (Nguyễn Văn Thành & Lục Anh Tuấn, 2024). Quá trình an ninh hóa thông tin đòi hỏi sự phối hợp giữa báo chí, cơ quan quản lý và công chúng nhằm hình thành cơ chế pháp lý, công nghệ và truyền thông đủ khả năng ứng phó với các rủi ro trên không gian số.

- Về lý thuyết Sinh thái học truyền thông (Media Ecology):

Theo McLuhan (1964), "bản thân môi trường truyền thông có khả năng định hình cách thức con người tiếp nhận và diễn giải thông tin". Từ góc độ này, tác động của các nền tảng số xuyên biên giới không chỉ nằm ở nội dung được truyền tải mà còn ở cơ chế thuật toán, hình thức tương tác và cấu trúc phân phối thông tin mà các nền tảng đó thiết lập đối với người dùng. Trong bối cảnh hiện nay, việc báo chí Việt Nam ngày càng phụ thuộc vào cơ chế phân phối nội dung của các nền tảng số xuyên biên giới

cho thấy ảnh hưởng ngày càng lớn của các hệ sinh thái nền tảng đối với quá trình tiếp nhận thông tin của công chúng. Từ góc độ sinh thái học truyền thông, sự phụ thuộc vào các nền tảng xuyên biên giới đặt ra yêu cầu tăng cường năng lực tự chủ về hạ tầng truyền thông số và bảo đảm chủ quyền thông tin quốc gia trong môi trường số.

Bài viết bước đầu đề xuất cách tiếp cận phản gián thông tin (Information Counter-Intelligence - ICI) như một hướng nghiên cứu mở nhằm lý giải sự mở rộng chức năng của báo chí trước các thách thức an ninh phi truyền thống trên không gian mạng. Tuy nhiên, đây mới chỉ là một đề xuất lý thuyết ban đầu và cần tiếp tục được kiểm chứng thông qua các nghiên cứu thực nghiệm trong tương lai.

5. Giải pháp

Từ các kết quả nghiên cứu về những thách thức đối với bảo vệ an ninh quốc gia trên không gian số, vai trò của báo chí và các rào cản trong quá trình thực hiện nhiệm vụ này, bài viết đề xuất bốn nhóm giải pháp trọng tâm sau:

Về thể chế và chính sách: Trong bối cảnh các thách thức an ninh thông tin trên không gian số ngày càng gia tăng, cần tiếp tục hoàn thiện hệ thống pháp luật và cơ chế quản trị nhằm bảo đảm chủ quyền thông tin quốc gia. Trọng tâm là nâng cao trách nhiệm của các nền tảng số xuyên biên giới trong lưu trữ dữ liệu, kiểm soát nội dung vi phạm pháp luật và phối hợp xử lý thông tin sai lệch trên môi trường mạng. Đồng thời, Nhà nước cần có cơ chế hỗ trợ tài chính phù hợp đối với các cơ quan báo chí thực hiện nhiệm vụ chính trị - xã hội nhằm tăng cường năng lực đầu tư công nghệ, phát triển hạ tầng số và nâng cao khả năng cạnh tranh của báo chí chính thống trong môi trường truyền thông số.

Về hạ tầng và công nghệ: Cần đẩy mạnh đầu tư xây dựng các hệ thống quản trị tòa soạn điện tử dùng chung (CMS), nền tảng dữ liệu lớn và các giải pháp công nghệ số do doanh nghiệp trong nước phát triển nhằm nâng cao năng lực tự chủ hạ tầng truyền thông. Trong bối cảnh tin giả, deepfake và các chiến dịch thao túng thông tin ngày càng tinh vi, việc ứng dụng AI trong phát hiện sớm nội dung sai lệch, phân tích xu hướng lan truyền và hỗ trợ kiểm chứng thông tin đang trở thành yêu cầu quan trọng đối với các cơ quan báo chí hiện đại. Bên cạnh đó, công nghệ Blockchain cũng có thể được nghiên cứu áp dụng trong xác thực nguồn gốc và tính toàn vẹn của nội dung báo chí, qua đó góp phần nâng cao độ tin cậy của thông tin chính thống trong môi trường truyền thông số đa nền tảng.

Về con người và đạo đức nghề nghiệp: Tsui và Lee (2021) cho rằng "những thay đổi của công nghệ số đang

đặt ra yêu cầu mới về năng lực bảo mật dữ liệu, bảo vệ nguồn tin và thích ứng công nghệ đối với hoạt động báo chí. Trên cơ sở đó, cần xây dựng chiến lược đào tạo đội ngũ nhà báo đa kỹ năng, kết hợp giữa năng lực nghiệp vụ báo chí, hiểu biết công nghệ số và khả năng bảo vệ dữ liệu, nguồn tin trong môi trường truyền thông số có mức độ giám sát và rủi ro an ninh mạng ngày càng cao. Trong bối cảnh AI tạo sinh, deepfake và thao túng thông tin phát triển nhanh, nhà báo không chỉ đóng vai trò sản xuất nội dung mà còn phải có năng lực kiểm chứng, phân tích và nhận diện các nguy cơ sai lệch thông tin trên không gian mạng. Đồng thời, cần tăng cường thực thi các chuẩn mực đạo đức nghề nghiệp báo chí, kiểm soát tình trạng thương mại hóa nội dung và hiện tượng "báo chí hóa" các trang thông tin điện tử nhằm hạn chế nguy cơ làm suy giảm độ tin cậy của môi trường thông tin xã hội.

Về giáo dục cộng đồng: Cần từng bước đưa nội dung hiểu biết truyền thông (media literacy), kỹ năng số và an toàn thông tin vào chương trình giáo dục quốc gia nhằm nâng cao khả năng nhận diện và xử lý thông tin sai lệch của công chúng trong môi trường số (UNESCO, 2023). Trong bối cảnh các nền tảng mạng xã hội ngày càng chi phối hành vi tiếp nhận thông tin, năng lực tư duy phản biện, kỹ năng kiểm chứng nguồn tin và trách nhiệm khi chia sẻ nội dung trực tuyến trở thành những yếu tố quan trọng đối với an toàn thông tin xã hội. Adewale-Ojo và Baderin (2025) cho rằng, "việc nâng cao hiểu biết truyền thông góp phần tăng cường khả năng chống chịu của xã hội trước các chiến dịch gây ảnh hưởng và thao túng thông tin trong môi trường số". Trên cơ sở đó, việc nâng cao hiểu biết truyền thông không chỉ giúp giảm nguy cơ lan truyền tin giả, deepfake và các hình thức thao túng nhận thức mà còn góp phần xây dựng khả năng chống chịu của xã hội trước các chiến dịch gây ảnh hưởng trên không gian mạng.

6. Kết luận

Thực tiễn cho thấy bảo vệ an ninh quốc gia trên không gian số không còn là nhiệm vụ riêng của các cơ quan chuyên trách mà đòi hỏi sự tham gia của toàn bộ hệ thống chính trị, trong đó báo chí giữ vai trò đặc biệt quan trọng trong định hướng dư luận và củng cố niềm tin xã hội. Trong bối cảnh thông tin sai lệch, deepfake và thao túng truyền thông ngày càng tinh vi, báo chí cần được nhìn nhận không chỉ như một thiết chế truyền thông mà còn là một thành tố của năng lực phòng vệ xã hội trên không gian số. Tuy nhiên, để thực hiện hiệu quả vai trò này, báo chí Việt Nam cần giải quyết đồng thời nhiều vấn đề về nguồn lực kinh tế, năng lực công nghệ và chất lượng nhân lực truyền thông trong không gian số.

TÀI LIỆU THAM KHẢO

- Adewale-Ojo, T. O., & Baderin, A. G. (2025). Evaluating the role of the media in enhancing national security: A case study of Nigeria. *LALICO Journal of Languages, Literature, and Communication*, 3(3), trang 44-59.
- Ban Tuyên giáo Trung ương (2018). *Nghị quyết số 35-NQ/TW về tăng cường bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác các quan điểm sai trái, thù địch trong tình hình mới*.
- Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner Publishers, https://www.riennner.com/title/Security_A_New_Framework_for_Analysis, truy cập ngày 03/5/2026.
- Chính phủ (2023). *Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 quy định về bảo vệ dữ liệu cá nhân*, <https://vanban.chinhphu.vn>, truy cập ngày 10/3/2026.
- Hồng Đạt (2026). *Người dùng Việt Nam thiệt hại hơn 6.000 tỷ đồng do lừa đảo trực tuyến trong năm 2025*, Tạp chí An toàn thông tin, <https://antoanthongtin.vn>, truy cập ngày 07/5/2026.
- HTV Tin tức (2024). *Doanh thu báo chí năm 2024 sụt giảm mạnh: Thách thức và hướng đi* [Video], YouTube, <https://www.youtube.com>, truy cập ngày 07/5/2026.
- Kolotaev, Yu. Yu. (2026). Digital securitization: How online platforms change the security landscape, *Russia in Global Affairs*, 24(1), trang 81-97, DOI: 10.31278/1810-6374-2026-24-1-81, <https://eng.globalaffairs.ru/articles/digital-securitization-kolotaev/>, truy cập ngày 07/5/2026.
- McLuhan, M. (1964). *Understanding Media: The Extensions of Man*. New York: McGraw-Hill Book Company, <https://archive.org/details/understandingmed00mclu>, truy cập ngày 07/5/2026.
- NCA (2025). *Báo cáo nghiên cứu, khảo sát an ninh mạng năm 2025 khu vực người dùng cá nhân*, Hiệp hội An ninh mạng quốc gia, <https://nca.org.vn>, truy cập ngày 03/3/2026.
- Nguyễn Văn Thành và Lục Anh Tuấn (2024). Bảo đảm an ninh con người trong tiến trình đẩy mạnh phát triển toàn diện đất nước hiện nay, *Tạp chí Quản lý nhà nước*, số 341, trang 18-23.
- Pauwels, E. (2024). *Preparing for next-generation information warfare with generative AI*, CIGI Paper No. 310, Centre for International Governance Innovation (CIGI), <https://www.cigionline.org/publications/preparing-for-next-generation-information-warfare-with-generative-ai/>, truy cập ngày 07/5/2026.
- Quốc hội (2024). *Luật Dữ liệu số 60/2024/QH15*, ban hành ngày 30/11/2024, <https://vanban.chinhphu.vn>, truy cập ngày 03/3/2026.
- Trần Thành Nam (2026). *Cảnh báo lừa đảo deepfake giả giọng giả hình người quen dịp Tết*, Thông tấn xã Việt Nam, <https://vnanet.vn>, truy cập ngày 03/3/2026.
- Tsui, L., & Lee, F. (2021). How journalists understand the threats and opportunities of new technologies: A study of security mind-sets and its implications for press freedom, *Journalism*, 22(3), trang 714-731, <https://doi.org/10.1177/1464884919849418>, truy cập ngày 07/5/2026.
- UNESCO (2023). *Guidelines for the Governance of Digital Platforms*, UNESCO Publishing, <https://unesdoc.unesco.org>, truy cập ngày 03/3/2026.