

Điều chỉnh chính sách an ninh thông tin của Nga trong bối cảnh mới và hàm ý cho Việt Nam

Đỗ Hồng Huyền¹

Ngày nhận bài: 22/7/2026 | Ngày gửi phản biện: 24/7/2026 | Ngày duyệt đăng: 25/8/2026

Tóm tắt: Những biến động của môi trường quốc tế, đặc biệt từ năm 2022, đã thúc đẩy Nga điều chỉnh chính sách an ninh thông tin theo hướng tăng cường chủ quyền số, bảo vệ hạ tầng thông tin trọng yếu, phát triển công nghệ trong nước và hoàn thiện cơ chế quản lý không gian mạng. Bài viết phân tích những điều chỉnh chủ yếu trong chính sách an ninh thông tin của Nga và thực tiễn triển khai chính sách. Trên cơ sở đó, bài viết đề xuất một số hàm ý tham khảo đối với Việt Nam trong quá trình hoàn thiện thể chế, phát triển nguồn lực, nâng cao năng lực bảo đảm an ninh thông tin, đáp ứng yêu cầu của quá trình chuyển đổi số và bảo vệ an ninh quốc gia trong môi trường số.

Từ khóa: An ninh thông tin, chủ quyền số, không gian mạng, Liên bang Nga, Việt Nam.

Adjustments to Russia's Information Security Policy in the new Context and Implications for Vietnam

Abstract: The profound shifts in the international environment, particularly since 2022, have driven Russia to adjust its information security (IS) policy toward reinforcing digital sovereignty, safeguarding critical information infrastructure, fostering domestic technological development, and perfecting cyberspace governance mechanisms. This article analyzes the major adjustments in Russia's IS policy alongside its practical implementation. On this basis, the paper proposes several policy implications for Vietnam in refining its institutional framework, developing resources, and enhancing IS assurance capabilities, thereby meeting the demands of the digital transformation process and safeguarding national security in the digital realm.

Keywords: Information security, digital sovereignty, cyberspace, Russian Federation, Vietnam.

1. Đặt vấn đề

Từ khi xung đột Nga - Ukraine bùng phát, những biến động của môi trường quốc tế cùng các biện pháp trừng phạt về công nghệ và thông tin đã đặt ra yêu cầu đối với Nga về việc phải điều chỉnh chính sách an ninh thông tin (ANTT) theo hướng tăng cường chủ quyền số, bảo vệ hạ tầng thông tin trọng yếu và phát triển các công nghệ trong nước. Nga đã từng bước hoàn thiện hệ thống pháp luật, nâng cao năng lực quản lý không gian mạng và giảm sự phụ thuộc vào công nghệ nước ngoài nhằm bảo đảm an ninh quốc gia trong điều kiện mới.

Tại Việt Nam, chuyển đổi số quốc gia đang được triển khai mạnh mẽ, đi cùng với yêu cầu bảo đảm an ninh, an toàn không gian mạng và bảo vệ chủ quyền số. Nghị quyết số 57-NQ/TW của Bộ Chính trị đã xác định phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số và bảo đảm an ninh mạng là những nhiệm vụ có ý nghĩa chiến lược (Báo Điện tử Chính phủ, 2026). Trong bối cảnh đó, việc nghiên cứu chính sách ANTT của Liên bang Nga giúp gợi mở chính sách có giá trị tham khảo cho Việt Nam trong quá trình hoàn thiện thể chế, phát triển nguồn lực và nâng cao năng lực bảo đảm ANTT.

¹ Thạc sĩ, Viện Nghiên cứu Châu Âu và Châu Mỹ; Email: honghuyen232@gmail.com

2. Điều chỉnh chính sách an ninh thông tin của Nga sau năm 2022

2.1. Cơ sở hình thành và hoàn thiện chính sách an ninh thông tin

Trong bối cảnh chuyển đổi số, sự phát triển của các công nghệ mới và mức độ phụ thuộc ngày càng lớn vào hạ tầng số đã làm gia tăng nguy cơ tấn công mạng, đánh cắp dữ liệu, can thiệp vào hệ thống thông tin trọng yếu và các hoạt động gây ảnh hưởng trên không gian mạng. Từ năm 2022, cùng với các biện pháp trừng phạt về công nghệ và việc nhiều doanh nghiệp công nghệ nước ngoài thu hẹp hoặc chấm dứt hoạt động tại Nga, yêu cầu bảo đảm chủ quyền số và tự chủ công nghệ trở thành một nội dung ưu tiên trong chính sách an ninh quốc gia Nga. Nga không còn nhìn nhận không gian mạng đơn thuần qua lăng kính quản trị kỹ thuật số, mà nâng tầm ANTT thành một cấu phần không thể tách rời của chiến lược an ninh quốc gia toàn diện.

Nền tảng pháp lý quan trọng cho những điều chỉnh về chính sách ANTT là Học thuyết ANTT của Liên bang Nga ban hành năm 2016, xác định các lợi ích quốc gia trên không gian thông tin, các nguy cơ đối với ANTT và định hướng xây dựng hệ thống bảo vệ quốc gia trong lĩnh vực này (President of the Russian Federation, 2016). Việc điều chỉnh chính sách ANTT được đặt trong tổng thể Chiến lược An ninh quốc gia năm 2021, trong đó, bảo đảm chủ quyền thông tin, phát triển công nghệ trong nước và bảo vệ hạ tầng thông tin quan trọng được xác định là những nhiệm vụ trọng tâm của quốc gia (President of the Russian Federation, 2021). Trên cơ sở đó, Nga tiếp tục hoàn thiện hệ thống văn bản điều chỉnh ANTT và an ninh mạng.

Kể từ năm 2022, nhiều chính sách mới được ban hành nhằm tăng cường khả năng tự chủ về công nghệ và bảo đảm hoạt động ổn định của hạ tầng số. Một trong những định hướng quan trọng là Chiến lược phát triển ngành truyền thông của Liên bang Nga đến năm 2035, được Chính phủ Nga phê duyệt năm 2023 (The Russian Government, 2023). Văn kiện đặt mục tiêu phát triển hạ tầng thông tin hiện đại, mở rộng ứng dụng công nghệ trong nước, nâng cao mức độ độc lập của các nền tảng số và tăng cường năng lực bảo vệ không gian thông tin quốc gia.

Việc triển khai chính sách ANTT được thực hiện thông qua sự phối hợp của nhiều cơ quan nhà nước. Hội đồng An ninh Liên bang Nga giữ vai trò tham mưu chiến lược về các vấn đề an ninh quốc gia; Cơ quan An ninh Liên bang chịu trách nhiệm bảo vệ hạ tầng thông tin trọng yếu và phòng, chống các mối đe dọa trên không gian mạng; Cơ quan Giám sát thông tin, công nghệ thông tin (CNTT) và truyền thông quản lý hoạt động trên không gian mạng, thực thi các quy định về dữ liệu và thông tin; Bộ Phát triển số, Truyền thông và Truyền thông đại chúng chịu trách nhiệm xây dựng chính sách phát triển hạ tầng số và CNTT. Cơ chế phối hợp này tạo điều kiện thống nhất giữa hoạch định chính sách, xây dựng pháp luật và tổ chức thực hiện trong lĩnh vực ANTT.

2.2. Những nội dung điều chỉnh chính sách an ninh thông tin

Thứ nhất, nâng cấp chiến lược “chủ quyền số”

Từ đầu năm 2022, trước bối cảnh đứt gãy chuỗi cung ứng công nghệ toàn cầu và sức ép từ các lệnh trừng phạt, Nga đã chuyển đổi chính sách “chủ quyền số” từ trạng thái phòng vệ sang các biện pháp pháp lý mang tính cưỡng chế. Dấu mốc quan trọng là Sắc lệnh của Tổng thống Liên bang Nga số 166 ngày 30/3/2022 “Về các biện pháp bảo đảm độc lập công nghệ và an ninh của hạ tầng thông tin trọng yếu”, quy định các cơ quan nhà nước và tổ chức vận hành hạ tầng thông tin trọng yếu không được mua sắm phần mềm của các nhà cung cấp thuộc các quốc gia “không thân thiện” từ năm 2022 và phải hoàn tất việc thay thế các sản phẩm này trước năm 2025. Tiếp đó, Sắc lệnh số 250 ngày 01/5/2022 “Về các biện pháp bổ sung nhằm bảo đảm an ninh thông tin của Liên bang Nga” yêu cầu các cơ quan nhà nước

và doanh nghiệp nhà nước xây dựng hệ thống quản trị an ninh mạng, bổ nhiệm lãnh đạo phụ trách an ninh thông tin, tăng cường giám sát sự cố và triển khai các giải pháp kỹ thuật do Nga phát triển.

Bên cạnh đó, Chính phủ Nga tiếp tục hoàn thiện khuôn khổ pháp lý về quản trị dữ liệu và nền tảng số trên cơ sở Luật Liên bang số 242-FZ về nội địa hoá dữ liệu, các sửa đổi đối với Luật số 149-FZ “Về thông tin, công nghệ thông tin và bảo vệ thông tin”, cùng các quy định tăng cường xử phạt các doanh nghiệp công nghệ không tuân thủ yêu cầu lưu trữ dữ liệu người dùng tại Nga. Trên nền tảng pháp lý này, nhà nước đồng thời triển khai chính sách hỗ trợ phát triển các nền tảng số trong nước như VKontakte, RuStore, hệ thống thanh toán Mir và các giải pháp điện toán, hệ điều hành nội địa nhằm giảm phụ thuộc vào các doanh nghiệp công nghệ phương Tây.

Như vậy, chính sách “chủ quyền số” của Nga sau năm 2022 không còn giới hạn ở mục tiêu bảo vệ dữ liệu hay bảo đảm hoạt động của hạ tầng thông tin trọng yếu, mà đã phát triển thành chiến lược xây dựng một hệ sinh thái số tương đối tự chủ, có khả năng duy trì hoạt động trong điều kiện bị cô lập về công nghệ và giảm thiểu rủi ro từ các sức ép bên ngoài (President of the Russian Federation, 2023).

Thứ hai, thiết lập hành lang bảo vệ hạ tầng thông tin trọng yếu

Sự gia tăng của các cuộc tấn công mạng nhắm vào Nga từ năm 2022 đã buộc chính phủ phải thay đổi cách tiếp cận đối với việc bảo vệ hạ tầng thông tin trọng yếu. Các hệ thống phục vụ năng lượng, tài chính, giao thông, viễn thông và dịch vụ công không còn được quản lý như các đối tượng kỹ thuật thông thường, mà được đặt vào trung tâm của an ninh quốc gia. Nga hoàn thiện cơ chế giám sát và ứng phó sự cố theo hướng tập trung hóa. Thông qua Trung tâm Phối hợp Quốc gia về Sự cố Máy tính do Cơ quan An ninh Liên bang quản lý, việc chia sẻ thông tin cảnh báo sớm giữa các cơ quan an ninh và doanh nghiệp vận hành hạ tầng được thực hiện thường xuyên hơn. Đồng thời, Chính phủ Nga chuyển từ cơ chế khuyến nghị sang áp đặt các tiêu chuẩn bảo mật bắt buộc: yêu cầu kiểm định an toàn định kỳ, sử dụng chuẩn mã hóa trong nước, và xây dựng kịch bản duy trì hoạt động cho các hệ thống cốt lõi ngay cả khi gặp sự cố ngắt kết nối với mạng quốc tế (TadViser, 2026).

Nga mở rộng phạm vi điều chỉnh của các quy định pháp luật hiện hành. Trên cơ sở Luật Liên bang số 187-FZ năm 2017 “Về an ninh của hạ tầng thông tin trọng yếu của Liên bang Nga”, Chính phủ Nga liên tục ban hành các văn bản hướng dẫn và sửa đổi quy định về phân loại đối tượng hạ tầng trọng yếu, chế độ giám sát an ninh mạng, chia sẻ thông tin sự cố và trách nhiệm của các đơn vị vận hành. Sắc lệnh số 250 của Tổng thống Nga (2022) đã bổ sung yêu cầu bắt buộc đối với các cơ quan nhà nước, doanh nghiệp nhà nước và tổ chức vận hành hạ tầng trọng yếu trong việc thiết lập hệ thống quản trị ANTT và triển khai các biện pháp kiểm soát rủi ro theo tiêu chuẩn thống nhất trên phạm vi toàn quốc.

Song song với việc hoàn thiện khuôn khổ pháp lý, Nga điều chỉnh cơ chế điều phối an ninh mạng theo hướng tập trung hơn thông qua Trung tâm Điều phối Quốc gia về Sự cố Máy tính (NCCC) thuộc Cơ quan An ninh Liên bang. Theo các quy định mới, các đơn vị vận hành hạ tầng thông tin trọng yếu có nghĩa vụ kết nối với hệ thống giám sát quốc gia, báo cáo sự cố an ninh mạng trong thời gian quy định và phối hợp với NCCC trong quá trình điều tra, khắc phục cũng như chia sẻ dữ liệu cảnh báo sớm.

Một điều chỉnh đáng chú ý là Nga chuyển từ mô hình khuyến nghị sang áp dụng các yêu cầu bắt buộc về bảo đảm an ninh đối với hạ tầng thông tin trọng yếu. Các cơ quan và doanh nghiệp thuộc diện điều chỉnh phải định kỳ đánh giá mức độ an toàn của hệ thống thông tin, sử dụng các phương tiện bảo mật và mật mã được cơ quan có thẩm quyền của Nga chứng nhận, xây dựng phương án duy trì hoạt động

liên tục và khôi phục hệ thống khi xảy ra sự cố hoặc trong trường hợp bị cô lập khỏi mạng internet toàn cầu. Những yêu cầu này được bổ sung đồng bộ với chính sách thay thế công nghệ nước ngoài bằng các giải pháp trong nước, giúp giảm thiểu nguy cơ bị gián đoạn hoạt động do các biện pháp trừng phạt hoặc các cuộc tấn công mạng từ bên ngoài.

Thứ ba, phát triển năng lực công nghệ

Trước nguy cơ đứt gãy nguồn cung thiết bị và giải pháp phần mềm từ nước ngoài, Nga đã ban hành chuỗi chính sách ưu đãi tài chính và thể chế nhằm tạo động lực bứt phá cho các doanh nghiệp công nghệ trong nước, ưu tiên ngân sách quốc gia cho các chương trình nghiên cứu và phát triển thuộc các lĩnh vực hạ tầng số cốt lõi. Chính phủ đã thành lập hệ thống các “Trung tâm Năng lực Công nghiệp” theo từng ngành kinh tế nhằm tập trung nguồn lực phát triển các phần mềm thay thế nhập khẩu, đặc biệt là hệ quản trị cơ sở dữ liệu, phần mềm thiết kế kỹ thuật và hệ điều hành nội địa (Grigorenko, D, 2026). Đồng thời, các cơ quan nhà nước và tập đoàn thuộc sở hữu nhà nước bắt buộc phải áp dụng tỷ lệ tối thiểu đối với việc mua sắm, sử dụng các sản phẩm phần mềm và thiết bị phần cứng nằm trong Danh mục Sản phẩm Công nghệ Quốc gia.

Ngoài ra, để giải quyết tình trạng thiếu hụt lao động trình độ cao và hạn chế nguy cơ “chảy máu chất xám” trong lĩnh vực công nghệ, Chính phủ Nga đã triển khai nhóm chính sách hỗ trợ nhân lực mang tính đặc thù. Các biện pháp này bao gồm: miễn thuế thu nhập doanh nghiệp cho các công ty CNTT, ban hành quy định hoãn nghĩa vụ quân sự đối với nhân sự làm việc trong lĩnh vực CNTT và an toàn thông tin.

Thứ tư, mở rộng hợp tác quốc tế trong lĩnh vực ANTT

Mạng lưới hợp tác quốc tế của Nga từ năm 2022 không còn duy trì theo phương thức đa phương truyền thống với các nước phát triển, mà chuyển hướng chiến lược sang củng cố liên minh với các nước Nam bán cầu và các tổ chức đa phương do Nga giữ vai trò nòng cốt.

Ở cấp độ toàn cầu, Nga duy trì quan điểm nhất quán về việc đa phương hóa quản trị internet dưới sự bảo trợ của Liên hợp quốc. Nga chủ động thúc đẩy các sáng kiến pháp lý quốc tế thông qua Tiến trình Nhóm Công tác về an ninh CNTT giai đoạn 2021-2025 (CADE, 2025). Mục tiêu của Nga là xây dựng một công ước quốc tế có tính ràng buộc pháp lý về chống tội phạm mạng và thiết lập các quy tắc ứng xử của quốc gia trên không gian mạng, dựa trên nguyên tắc tôn trọng tuyệt đối chủ quyền số và không can thiệp vào công việc nội bộ của các quốc gia khác. Ở cấp độ khu vực và các khối hợp tác mới nổi, Nga gia tăng tần suất hợp tác an ninh mạng trong khuôn khổ Tổ chức Hợp tác Thượng Hải (SCO) và khối BRICS. Thông qua các cơ chế này, Nga cùng các đối tác chia sẻ thông tin đe dọa an ninh mạng, xây dựng tiêu chuẩn kỹ thuật dùng chung và phối hợp bảo vệ hạ tầng dữ liệu liên vùng. Ngoài ra, Nga cũng điều chỉnh chính sách “ngoại giao công nghệ” đối với các đối tác tại châu Á, châu Phi và Latinh. Chính sách này tập trung vào việc xuất khẩu các giải pháp an toàn thông tin nội địa (như phần mềm diệt virus, giải pháp chống tấn công DDoS, công nghệ giám sát an ninh mạng), hỗ trợ kỹ thuật trong việc xây dựng hạ tầng số quốc gia và chuyển giao thông tin bảo mật. Điều chỉnh này giúp doanh nghiệp công nghệ Nga khai thác thị trường mới, và nâng cao sức đề kháng trước các nguy cơ an ninh mạng phi truyền thống.

3. Thực tiễn triển khai chính sách an ninh thông tin của Liên bang Nga

Sau khi hoàn thiện hệ thống định hướng chiến lược và khung pháp lý, Nga tập trung triển khai chính sách ANTT thông qua việc hoàn thiện hạ tầng số, phát triển công nghệ trong nước, tăng cường bảo vệ hạ tầng thông tin trọng yếu và xây dựng nguồn nhân lực. Các nhiệm vụ này được thực hiện đồng thời ở

cấp liên bang và địa phương, với sự tham gia của các cơ quan quản lý nhà nước, doanh nghiệp và các cơ sở nghiên cứu, đào tạo.

Tháng 11/2023, Chính phủ Liên bang Nga ban hành Chiến lược phát triển ngành truyền thông đến năm 2035, xác định các mục tiêu về hiện đại hóa hạ tầng viễn thông, phát triển mạng thông tin thế hệ mới, nâng cao năng lực sản xuất thiết bị và phần mềm trong nước, đồng thời, từng bước giảm sự phụ thuộc vào công nghệ nước ngoài. Chiến lược cũng yêu cầu các bộ, ngành xây dựng kế hoạch triển khai phù hợp với chức năng, nhiệm vụ của từng cơ quan nhằm bảo đảm tính thống nhất trong quá trình thực hiện chính sách.

Trong lĩnh vực bảo vệ hạ tầng thông tin trọng yếu, Nga tiếp tục hoàn thiện các quy định về an toàn thông tin đối với các hệ thống thông tin quan trọng của quốc gia. Cơ quan Kiểm soát Kỹ thuật và Xuất khẩu Liên bang (FSTEC) thường xuyên cập nhật các yêu cầu kỹ thuật về xây dựng, vận hành và bảo vệ hệ thống thông tin, tăng cường các biện pháp giám sát, phát hiện và ứng phó với nguy cơ mất an toàn thông tin đối với các lĩnh vực như tài chính, năng lượng, giao thông, viễn thông và dịch vụ công.

Bên cạnh đó, Nga chú trọng phát triển nguồn nhân lực phục vụ chuyển đổi số và ANTT. Chiến lược phát triển ngành truyền thông đến năm 2035 xác định đào tạo nhân lực chất lượng cao là một trong những điều kiện bảo đảm cho phát triển CNTT, an ninh mạng và truyền thông số, là điều kiện tiên quyết để duy trì “chủ quyền số”. Nga đã lồng ghép nhiệm vụ đào tạo chuyên gia an ninh thông tin vào Chương trình Mục tiêu Quốc gia “Kinh tế số Liên bang Nga”. Liên kết Viện - Trường - Doanh nghiệp thể hiện rõ qua việc Bộ Giáo dục và Khoa học Nga phối hợp điều chỉnh chỉ tiêu tuyển sinh đại học, tăng tỷ lệ chỉ tiêu ngân sách cho các ngành an ninh mạng, mật mã học và hệ thống thông tin tại các trường đại học trọng điểm.

Ngoài những kết quả đạt được, quá trình triển khai chính sách cũng đặt ra một số yêu cầu mới. Việc phát triển công nghệ trong nước cần nguồn lực đầu tư lớn và thời gian để hình thành hệ sinh thái công nghệ có khả năng thay thế các sản phẩm nhập khẩu. Đồng thời, quá trình chuyển đổi số làm gia tăng yêu cầu bảo đảm an toàn đối với các hệ thống thông tin quan trọng, đòi hỏi sự phối hợp chặt chẽ giữa cơ quan quản lý nhà nước, doanh nghiệp và các tổ chức nghiên cứu trong xây dựng tiêu chuẩn kỹ thuật, đào tạo nhân lực và nâng cao năng lực ứng phó với các rủi ro trên không gian mạng. Những yêu cầu này tiếp tục được Nga xác định là các nhiệm vụ ưu tiên trong quá trình thực hiện Chiến lược phát triển ngành truyền thông đến năm 2035.

4. Hàm ý đối với Việt Nam

Quá trình điều chỉnh và triển khai chính sách ANTT của Nga trong những năm gần đây cho thấy, nhiều kinh nghiệm có thể tham khảo trong quá trình hoàn thiện chính sách bảo đảm ANTT ở Việt Nam. Mặc dù điều kiện phát triển, thể chế chính trị và môi trường an ninh của hai quốc gia có nhiều khác biệt, song một số định hướng của Nga vẫn có giá trị tham khảo trong bối cảnh Việt Nam đang đẩy mạnh chuyển đổi số và xây dựng hạ tầng số quốc gia.

Một là, cần tiếp tục hoàn thiện hệ thống pháp luật và cơ chế điều phối về ANTT theo hướng đồng bộ giữa chuyển đổi số, phát triển kinh tế số và bảo đảm an ninh quốc gia. Việt Nam cần tiếp tục rà soát, hoàn thiện các quy định pháp luật về bảo vệ dữ liệu, an toàn hệ thống thông tin và bảo vệ hạ tầng số cần được gắn với yêu cầu phát triển Chính phủ số, kinh tế số và xã hội số.

Hai là, cần nâng cao năng lực tự chủ về công nghệ và phát triển hệ sinh thái số trong nước. Trong điều kiện công nghệ số trở thành yếu tố quyết định năng lực cạnh tranh quốc gia, việc từng bước làm chủ các công nghệ cốt lõi, phát triển doanh nghiệp công nghệ số, sản phẩm phần mềm và nền tảng số trong nước có ý nghĩa quan trọng đối với việc bảo đảm ANTT lâu dài. Đối với Việt Nam, phát triển năng lực nghiên cứu, đổi mới sáng tạo và thúc đẩy liên kết giữa Nhà nước, doanh nghiệp và các cơ sở nghiên cứu sẽ góp phần nâng cao khả năng tự chủ về công nghệ, giảm dần sự phụ thuộc vào các nền tảng và công nghệ nước ngoài trong những lĩnh vực quan trọng.

Ba là, cần ưu tiên bảo vệ hạ tầng thông tin trọng yếu và phát triển nguồn nhân lực chất lượng cao. Quá trình chuyển đổi số làm gia tăng mức độ phụ thuộc của các lĩnh vực tài chính, năng lượng, giao

thông, y tế và dịch vụ công vào hạ tầng số. Vì vậy, Việt Nam cần tiếp tục hoàn thiện các tiêu chuẩn bảo đảm an toàn thông tin, tăng cường năng lực giám sát, cảnh báo sớm và ứng phó sự cố, đồng thời chú trọng đào tạo đội ngũ chuyên gia về ANTT, an ninh mạng và công nghệ số đáp ứng yêu cầu phát triển trong giai đoạn mới.

Bốn là, tiếp tục mở rộng hợp tác quốc tế về ANTT trên cơ sở bảo đảm lợi ích quốc gia và phù hợp với đường lối đối ngoại của Việt Nam. Trong bối cảnh các nguy cơ trên không gian mạng có tính xuyên biên giới, hợp tác quốc tế vẫn là một yêu cầu khách quan. Việt Nam cần tăng cường trao đổi kinh nghiệm, đào tạo nhân lực, chia sẻ thông tin và hợp tác nghiên cứu với các đối tác quốc tế, đồng thời chủ động tham gia xây dựng các chuẩn mực và cơ chế hợp tác đa phương về an ninh mạng và quản trị không gian số.

5. Kết luận

Sau năm 2022, Liên bang Nga đã điều chỉnh chính sách ANTT theo hướng tăng cường bảo đảm chủ quyền số, bảo vệ hạ tầng thông tin trọng yếu và nâng cao năng lực tự chủ về công nghệ. Những điều chỉnh này được thể hiện thông qua việc hoàn thiện hệ thống văn bản chiến lược, phát triển hạ tầng số, thúc đẩy công nghệ trong nước và tăng cường năng lực bảo vệ các hệ thống thông tin quan trọng. Đối với Việt Nam, kinh nghiệm của Nga là nguồn tham khảo trong quá trình hoàn thiện chính sách ANTT gắn với chuyển đổi số quốc gia. Việc tiếp tục hoàn thiện thể chế, phát triển công nghệ số trong nước, bảo vệ hạ tầng thông tin trọng yếu, đào tạo nguồn nhân lực và mở rộng hợp tác quốc tế cần được triển khai phù hợp với điều kiện phát triển và yêu cầu bảo đảm quốc phòng, an ninh của Việt Nam. Những gợi mở này góp phần nâng cao hiệu quả quản lý nhà nước về ANTT và tăng cường khả năng bảo đảm an toàn không gian số trong giai đoạn tới.

Ghi chú: Bài viết là sản phẩm của Nhiệm vụ khoa học cấp cơ sở “Chiến tranh thông tin của Nga và những thách thức đặt ra cho châu Âu”, mã số Nhiệm vụ CACM/2026-05 do ThS. Đỗ Hồng Huyền làm chủ nhiệm.

Tài liệu tham khảo

1. Báo Điện tử Chính Phủ (2026). *Nghị quyết 57-NQ/TW về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia*. <https://xaydungchinhhsach.chinhphu.vn/toan-van-nghi-quyet-ve-dot-pha-phat-trien-khoa-hoc-cong-nghe-doi-moi-sang-tao-va-chuyen-doi-so-quoc-gia-119241224180048642.htm>
2. CADE (2025). *OEWG 2021-2025 adopts its Final Report*. <https://cadeproject.org/updates/oewg-2021-2025-adopts-its-final-report/>
3. Grigorenko, D (2026). *A new selection process has begun for particularly significant IT projects vying for grants*. <http://government.ru/news/58192/>
4. President of the Russian Federation (2016). *Doctrine of Information Security of the Russian Federation*. <http://kremlin.ru/acts/bank/41460>
5. President of the Russian Federation (2021). *Executive Order No. 400 on the National Security Strategy of the Russian Federation*. <http://publication.pravo.gov.ru/Document/View/0001202107030001>
6. President of the Russian Federation (2023). *Decree No. 231 on the Unified Digital Platform "GosTech"*. <https://rg.ru/documents/2023/04/04/fz231.html>
7. TadViser (2026). *Security of critical information infrastructure of the Russian Federation* https://tadviser.com/index.php/Article:Security_of_critical_information_infrastructure_of_the_Russian_Federation
8. The Russian Government (2023). *Mikhail Mishustin held a strategic session on the telecommunications industry development until 2035*. <http://government.ru/en/news/48806/>