SỐ ĐẶC BIỆT
THÁNG 10/2025

Tạp chí
CÔNG DÂN & KHUYẾN HỌC
CƠ QUAN NGÔN LUẬN CỦA HỘI KHUYẾN HỌC VIỆT NAM

Dạy và Học NGÀY NAY

TODAY'S TEACHING & LEARNING MAGAZINE

ISSN 2815 - 5769

TẠP CHÍ CÔNG DÂN VÀ KHUYẾN HỌC

ẤT TỴ

SỐ ĐẶC BIỆT

THÁNG 10/2025

Học
Học nữa
Học mãi!

Tạp chí
CÔNG DÂN & KHUYẾN HỌC
CƠ QUAN NGÔN LUẬN CỦA HỘI KHUYẾN HỌC VIỆT NAM
Dạy và Học NGÀY NAY

SỐ ĐẶC BIỆT
THÁNG 10/2025

TỔNG BIÊN TẬP
Tô Quang Phán

BAN TẠP CHÍ IN
TRƯỞNG BAN
Trương Thị Thúy Hằng

PHÓ BAN
Nguyễn Thị Bính

TRÌNH BÀY
Ngô Tráng Kiện
Mạnh Hùng

Giá: 38.000 đ

MỤC LỤC/ CONTENTS

• Tòa soạn: Tòa nhà TueMy, số 29/67 Đỗ Quang, Phường Trung Hòa, Quận Cầu Giấy, Hà Nội
• Điện thoại: 2473.098.555 * DĐ: 0983081976 * dvh_nn@yahoo.com
• Tạp chí điện tử Công dân và Khuyến học * Email: toasoan@congdankhuyenhoc.vn
• Giấy phép xuất bản: Số 114/GP-BTTTT do Bộ Thông tin và Truyền thông cấp ngày 25/02/2022

GIẢI PHÁP TĂNG CƯỜNG AN NINH MẠNG GÓP PHẦN BẢO VỆ CHỦ QUYỀN SỐ QUỐC GIA HIỆN NAY

NGHIÊM CÔNG ĐĨNH
Khoa Giáo dục Quốc phòng, Đại học Mỏ địa chất

Ngày nhận bài: 03/9/2025; Ngày phản biện, biên tập và sửa chữa: 27/9/2025; Ngày duyệt đăng: 14/10/2025

ABSTRACT

In the context of digital transformation and deep international integration, cyber security has become a key factor in ensuring cyberspace safety and national digital sovereignty. This article analyzes the concept and current status of CSS in Vietnam, pointing out the challenges from cybercrime, cyber attacks, as well as gaps in institutions, infrastructure and human resources. On that basis, the article proposes key solutions: perfecting the legal framework, developing cyber defense infrastructure, training high-quality human resources, strengthening international cooperation, raising public awareness and applying new technologies. These are practical directions to contribute to protecting national digital sovereignty today.

Keywords: *Cyber security; national digital sovereignty; cyber attack; information security.*

Trong bối cảnh toàn cầu đang diễn ra cuộc cách mạng công nghiệp lần thứ tư, chuyển đổi số trở thành xu thế tất yếu, tác động sâu sắc đến mọi lĩnh vực của đời sống kinh tế, chính trị, xã hội. Ở Việt Nam, sự phát triển mạnh mẽ của công nghệ thông tin, Internet và các nền tảng số đã mở ra nhiều cơ hội trong quản lý nhà nước, phát triển kinh tế, nâng cao chất lượng đời sống nhân dân. Không gian mạng đã trở thành một phần không thể thiếu, vừa là môi trường hoạt động, vừa là "không gian sống" mới của quốc gia. Tuy nhiên, đi cùng với những thành tựu, ANM nổi lên như một vấn đề đặc biệt quan trọng, gắn liền trực tiếp với an ninh quốc gia và chủ quyền số. Nếu như trước đây chủ quyền quốc gia được thể hiện trên lãnh thổ, vùng biển, vùng trời thì ngày nay còn được mở rộng sang không gian mạng. Mọi nguy cơ tấn công, chiếm đoạt dữ liệu, thao túng thông tin hay phá hoại hạ tầng số đều có thể đe dọa nền tảng chính trị, kinh tế và sự ổn định xã hội.

Thực tiễn cho thấy, các cuộc tấn công mạng ngày càng gia tăng về quy mô, tính chất và thủ đoạn; tình trạng lộ lọt dữ liệu cá nhân, dữ liệu nhạy cảm; sự xuất hiện của chiến tranh không gian mạng trở thành thách thức toàn cầu. Trước những vấn đề đó, yêu cầu đặt ra cho Việt Nam là cần xây dựng và triển khai hệ thống giải pháp toàn diện, đồng bộ và hiệu quả nhằm tăng cường ANM, qua đó bảo vệ vững chắc chủ quyền số quốc gia trong thời kỳ hội nhập và phát triển.

An ninh mạng là một phạm trù rộng, có ý nghĩa đặc biệt trong bối cảnh toàn cầu hóa, chuyển đổi số và sự phát triển mạnh mẽ của công nghệ thông tin hiện nay. Theo Luật ANM Việt Nam năm 2018, ANM được định nghĩa là "sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội; không gây phương hại đến quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân". Như vậy, khái niệm ANM của Việt Nam vừa phản ánh bản chất chung của vấn đề bảo vệ hệ thống thông tin, dữ liệu, hạ tầng kỹ thuật, vừa khẳng định mối quan hệ mật thiết giữa ANM với lợi ích quốc gia, lợi ích xã hội và quyền lợi chính đáng của công dân. Trong phạm vi rộng, ANM không chỉ giới hạn ở việc phòng ngừa, phát hiện, ngăn chặn, xử lý các hành vi tấn công, xâm nhập, phá hoại hệ thống thông tin mà còn bao gồm các hoạt động bảo vệ chủ quyền, lợi ích quốc gia trong không gian mạng. Điều này đặc biệt quan trọng trong bối cảnh chiến tranh thông tin, tội phạm mạng và các hình thức khủng bố mạng ngày càng tinh vi, đa dạng.

Khái niệm chủ quyền số là sự mở rộng của khái niệm chủ quyền truyền thống (trên lãnh thổ, vùng trời, vùng biển) sang không gian mạng. Chủ quyền số quốc gia bao gồm các yếu tố cơ bản sau: 1- Chủ quyền trên không gian mạng: Đây là quyền kiểm soát, quản lý và bảo vệ không gian mạng trong phạm vi quốc gia, bao gồm các hệ thống mạng công cộng và mạng riêng của các cơ quan, tổ chức. Quốc gia có quyền đặt ra quy định, tiêu chuẩn, và có biện pháp bảo đảm an toàn hoạt động trên lãnh thổ mạng của mình. 2- Chủ quyền dữ liệu: Dữ liệu ngày nay được coi là "tài nguyên chiến lược" của quốc gia. Chủ quyền dữ liệu thể hiện ở quyền kiểm soát, sở hữu và bảo vệ dữ liệu của cơ quan nhà nước, doanh nghiệp và công dân. Nếu dữ liệu bị đánh cắp, thao túng hoặc phụ thuộc vào hệ thống lưu trữ bên ngoài, nguy cơ mất an ninh, mất chủ quyền là rất lớn. 3- Chủ quyền hạ tầng số: Bao gồm quyền kiểm soát và bảo đảm an toàn cho hạ tầng kỹ thuật số, từ trung tâm dữ liệu, hệ thống viễn thông, mạng Internet quốc gia cho đến các nền tảng số phục vụ quản lý và điều hành xã hội. Đây là nền tảng vật chất để bảo đảm cho các hoạt động trên không gian mạng diễn ra an toàn, ổn định và có kiểm soát. Có thể thấy, chủ quyền số là một khái niệm có nội hàm rộng, bao quát cả khía cạnh kỹ thuật, pháp lý, chính trị và an ninh quốc gia. Trong kỷ nguyên số, việc giữ vững chủ quyền số quốc gia có ý nghĩa tương tự như bảo vệ chủ quyền lãnh thổ, là nền tảng để quốc gia phát triển độc lập, tự chủ trong môi trường mạng toàn cầu.

Thực tiễn tại Việt Nam những năm gần đây cho thấy tình hình ANM diễn biến phức tạp với nhiều dạng thức. Các cuộc tấn công từ chối dịch vụ (DDoS), tấn công vào hệ thống máy chủ của cơ quan, tổ chức, doanh nghiệp nhằm làm tê liệt hoạt động diễn ra ngày càng nhiều. Một số cuộc tấn công nhắm vào các hệ thống trọng yếu, đe dọa trực tiếp đến hoạt động kinh tế, xã hội. Theo thống kê của các tổ chức ANM, mỗi năm có hàng chục nghìn máy tính tại Việt Nam bị nhiễm mã độc, trong đó có nhiều mã độc tống tiền (ransomware) gây hậu quả nghiêm trọng đối với dữ liệu cá nhân, dữ liệu doanh nghiệp. Hình thức lừa đảo qua email, mạng xã hội, ứng dụng giả mạo ngày càng phổ biến, gây thiệt hại lớn về tài chính và làm suy giảm niềm tin của người dân vào môi trường số. Nhiều vụ việc cho thấy tin tặc đã tấn công nhằm chiếm đoạt dữ liệu y tế, dữ liệu tài chính, thậm chí dữ liệu của cơ quan nhà nước. Đây là những thông tin đặc biệt quan trọng, nếu bị rò rỉ sẽ ảnh hưởng trực tiếp đến an ninh quốc gia và quyền lợi công dân.

Mặc dù còn nhiều khó khăn, nhưng Việt Nam đã đạt được những kết quả quan trọng trong việc xây dựng và phát triển năng lực bảo vệ ANM. Việc ban hành Luật An ninh mạng năm 2018, Chiến lược ANM quốc gia, cùng với nhiều nghị định, thông tư liên quan đã tạo nền tảng pháp lý quan trọng cho công tác bảo đảm ANM. Chính phủ đã ban hành Chiến lược an toàn, ANM quốc gia đến năm 2025, định hướng đến năm 2030; Chiến lược chuyển đổi số quốc gia; đồng thời tăng cường xây dựng các trung tâm giám sát an toàn không gian mạng (SOC) tại nhiều địa phương và ngành. Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia đã được thành lập và phát huy hiệu quả. Các đơn vị chuyên trách, trong đó có Cục An toàn thông tin (Bộ Thông tin và Truyền thông) và Bộ Tư lệnh Tác chiến không gian mạng (Bộ Quốc phòng) đã kịp thời xử lý nhiều vụ tấn công, ngăn chặn nguy cơ lan rộng. Việt Nam đã tham gia nhiều diễn đàn quốc tế về ANM, ký kết thỏa thuận hợp tác với các tổ chức, quốc gia nhằm trao đổi kinh nghiệm và phối hợp xử lý sự cố.

Bên cạnh những kết quả đạt được, thực trạng ANM tại Việt Nam vẫn đối mặt với nhiều hạn chế và thách thức. Nhiều hệ thống thông tin quan trọng của quốc gia chưa được trang bị đầy đủ giải pháp ANM tiên tiến. Việc phân bổ nguồn lực đầu tư cho hạ tầng bảo mật còn chênh lệch giữa các bộ, ngành, địa phương. Dù đã có nhiều cơ sở đào tạo chuyên ngành an toàn thông tin, nhưng đội ngũ chuyên gia, kỹ sư ANM có trình độ ngang tầm quốc tế vẫn còn hạn chế. Nhu cầu nhân lực lớn nhưng cung chưa đáp ứng đủ, tạo ra khoảng trống đáng lo ngại. Một bộ phận người dân, thậm chí cả cán bộ công chức, viên chức chưa nhận thức đầy đủ về tầm quan trọng

của ANM, còn chủ quan trong việc bảo vệ dữ liệu cá nhân, thông tin công vụ. Điều này tạo điều kiện cho tin tặc lợi dụng, thực hiện các hành vi xâm nhập, lừa đảo. Sự phát triển nhanh chóng của trí tuệ nhân tạo (AI), Internet vạn vật (IoT), điện toán đám mây… vừa mang lại lợi ích nhưng cũng mở ra những lỗ hổng an ninh mới. Việt Nam cần có chiến lược phù hợp để vừa tận dụng được cơ hội, vừa phòng ngừa rủi ro.

Trong bối cảnh chuyển đổi số và hội nhập quốc tế sâu rộng, việc bảo vệ ANM không chỉ đơn thuần là một nhiệm vụ kỹ thuật mà còn là vấn đề chiến lược, gắn liền với chủ quyền và lợi ích quốc gia. Để xây dựng một không gian mạng an toàn, lành mạnh, phục vụ đắc lực cho sự phát triển đất nước, cần triển khai đồng bộ các giải pháp sau:

Thứ nhất, tiếp tục hoàn thiện thể chế, pháp luật, cơ chế quản lý nhà nước

Trước sự phát triển nhanh chóng của công nghệ mới, khung pháp lý hiện hành về ANM cần được thường xuyên rà soát, cập nhật để phù hợp với thực tiễn. Bên cạnh Luật ANM năm 2018, cần bổ sung các quy định liên quan đến bảo mật dữ liệu cá nhân, an toàn thông tin trong thương mại điện tử, giao dịch tài chính số, cũng như những thách thức mới từ trí tuệ nhân tạo, Internet vạn vật (IoT) và điện toán đám mây. Song song với việc hoàn thiện luật pháp, Nhà nước cần xây dựng cơ chế phối hợp hiệu quả giữa các bộ, ngành, địa phương và doanh nghiệp. Một cơ chế quản lý thống nhất, phân công rõ trách nhiệm, tăng cường kiểm tra, giám sát sẽ giúp xử lý kịp thời các nguy cơ tấn công, hạn chế tình trạng chồng chéo trong quản lý. Ngoài ra, cần tăng cường chế tài xử lý nghiêm khắc các hành vi vi phạm ANM, từ việc phát tán mã độc, tấn công hệ thống thông tin đến buôn bán dữ liệu cá nhân trái phép. Chỉ khi pháp luật đủ mạnh và được thực thi nghiêm minh thì mới có thể răn đe, ngăn chặn các hành vi xâm hại ANM.

Thứ hai, xây dựng và phát triển hạ tầng an ninh mạng quốc gia

Một nền ANM vững chắc đòi hỏi phải có hạ tầng kỹ thuật hiện đại, đồng bộ và có khả năng chống chịu cao. Do đó, cần ưu tiên đầu tư hệ thống giám sát, cảnh báo và phòng thủ chủ động. Các trung tâm điều hành an ninh mạng (SOC) cần được phát triển ở cả cấp quốc gia và cấp ngành, địa phương, kết nối thành mạng lưới thống nhất để kịp thời phát hiện, phân tích và ứng phó với các mối đe dọa. Đặc biệt, phải chú trọng bảo vệ hạ tầng thông tin quan trọng của quốc gia như hệ thống viễn thông, tài chính - ngân hàng, năng lượng, giao thông, y tế, và cơ sở dữ liệu dân cư. Đây là những "mạch máu" vận hành xã hội, nếu bị tấn công sẽ gây hậu quả nghiêm trọng. Việc áp dụng các tiêu chuẩn an toàn thông tin tiên tiến, kiểm định định kỳ hệ thống và triển khai các giải pháp sao lưu, phục hồi dữ liệu là hết sức cần thiết. Ngoài ra, Việt Nam cần khuyến khích phát triển các doanh nghiệp công nghệ trong nước cung cấp sản phẩm, dịch vụ ANM, góp phần giảm phụ thuộc vào công nghệ nước ngoài và tăng cường năng lực tự chủ về hạ tầng ANM quốc gia.

Thứ ba, nâng cao năng lực đội ngũ chuyên trách và đào tạo nhân lực an ninh mạng

Con người là yếu tố trung tâm của mọi giải pháp ANM. Để ứng phó với các mối đe dọa ngày càng phức tạp, Việt Nam cần chú trọng đào tạo, bồi dưỡng lực lượng chuyên gia ANM có trình độ quốc tế. Các chương trình đào tạo phải bám sát thực tiễn, kết hợp lý thuyết với thực hành, chú trọng kỹ năng ứng dụng công nghệ mới. Bên cạnh lực lượng chuyên trách trong các cơ quan nhà nước, cần phát triển đội ngũ nhân lực ANM trong các doanh nghiệp, tổ chức xã hội. Việc kết hợp chặt chẽ giữa Nhà nước - doanh nghiệp - viện nghiên cứu - trường đại học là hết sức quan trọng. Mô hình "tam giác hợp tác" này sẽ giúp tận dụng thế mạnh của từng bên: Nhà nước định hướng và hỗ trợ, doanh nghiệp đầu tư công nghệ, còn viện - trường đào tạo nhân lực chất lượng cao. Ngoài ra, cần có chính sách đãi ngộ, khuyến khích để thu hút nhân tài trong lĩnh vực ANM, đồng thời xây dựng môi trường nghiên cứu, sáng tạo thuận lợi cho lực lượng trẻ.

Thứ tư, tăng cường hợp tác quốc tế trong lĩnh vực an ninh mạng

An ninh mạng mang tính toàn cầu, không một quốc gia nào có thể tự mình đối phó hiệu quả với mọi nguy cơ. Do đó, Việt Nam cần chủ động tham gia các hiệp ước, diễn đàn quốc tế về ANM, như ASEAN, Liên Hợp Quốc, APEC, cũng như các tổ chức chuyên ngành. Qua đó, Việt Nam có thể chia sẻ kinh nghiệm, học hỏi mô hình quản lý tiên tiến và tham gia xây dựng bộ quy tắc ứng xử chung trên không gian mạng. Đồng thời, cần đẩy mạnh trao đổi thông tin, phối hợp xử lý sự cố xuyên biên giới. Khi xảy ra tấn công mạng có nguồn gốc từ nước ngoài, sự phối hợp quốc tế sẽ giúp nhanh chóng xác định thủ phạm, ngăn chặn hậu quả lan rộng và truy vết đối tượng. Bên cạnh đó, hợp tác quốc tế còn giúp Việt Nam nâng cao năng lực nghiên cứu, tiếp cận công nghệ tiên tiến, đào tạo nhân lực chất lượng cao và tham gia chuỗi giá trị toàn cầu trong lĩnh vực ANM.

Thứ năm, nâng cao nhận thức cộng đồng, xây dựng "lá chắn xã hội"

An ninh mạng không chỉ là nhiệm vụ của các cơ quan chức năng mà còn là trách nhiệm của toàn xã hội. Để xây dựng một "lá chắn xã hội", cần đẩy mạnh tuyên truyền, giáo dục về ANM cho mọi tầng lớp nhân dân. Các chương trình truyền thông phải dễ hiểu, dễ tiếp cận, hướng dẫn cụ thể cách nhận diện và phòng tránh các mối nguy từ mạng Internet. Đặc biệt, việc phát triển kỹ năng số an toàn cho học sinh, sinh viên, cán bộ công chức và người lao động trong doanh nghiệp là yêu cầu cấp thiết. Đây chính là lực lượng trực tiếp sử dụng các nền tảng số, nếu có ý thức và kỹ năng bảo mật sẽ hạn chế tối đa nguy cơ lộ lọt dữ liệu và bị tấn công. Ngoài ra, các tổ chức xã hội, hiệp hội nghề nghiệp, doanh nghiệp công nghệ cần tích cực tham gia các chương trình nâng cao nhận thức cộng đồng, tạo nên một phong trào xã hội rộng lớn về bảo vệ ANM.

Thứ sáu, ứng dụng công nghệ tiên tiến trong bảo vệ không gian mạng

Sự phát triển nhanh chóng của khoa học - công nghệ đặt ra cả cơ hội lẫn thách thức cho công tác bảo đảm ANM. Để chủ động thích ứng, Việt Nam cần mạnh dạn ứng dụng các công nghệ tiên tiến như trí tuệ nhân tạo (AI), phân tích dữ liệu lớn (Big Data), công nghệ chuỗi khối (Blockchain) trong giám sát, phát hiện sớm và phòng ngừa tấn công mạng. AI có thể giúp tự động phân tích hàng triệu dữ liệu trong thời gian thực để phát hiện bất thường; Big Data hỗ trợ nhận diện xu hướng tấn công; còn Blockchain có thể tạo ra cơ chế lưu trữ, truyền tải dữ liệu minh bạch và khó bị giả mạo. Việc ứng dụng đồng bộ các công nghệ này sẽ tạo bước đột phá trong năng lực bảo vệ không gian mạng quốc gia. Bên cạnh đó, cần khuyến khích phát triển các sản phẩm ANM "Make in Vietnam". Đây không chỉ là giải pháp nâng cao năng lực tự chủ công nghệ, mà còn tạo động lực thúc đẩy ngành công nghiệp ANM trong nước phát triển, góp phần vào mục tiêu đưa Việt Nam trở thành quốc gia mạnh về công nghệ số.

Phải khẳng định, việc bảo đảm ANM gắn liền với bảo vệ chủ quyền số quốc gia là nhiệm vụ chiến lược, lâu dài. Những giải pháp nêu trên từ hoàn thiện thể chế pháp luật, phát triển hạ tầng, đào tạo nhân lực, hợp tác quốc tế, nâng cao nhận thức cộng đồng đến ứng dụng công nghệ tiên tiến cần được triển khai đồng bộ, liên tục và hiệu quả. Chỉ trên cơ sở đó, Việt Nam mới có thể xây dựng một không gian mạng an toàn, bền vững, bảo vệ vững chắc chủ quyền số, tạo nền tảng cho phát triển kinh tế - xã hội và hội nhập quốc tế trong kỷ nguyên số./.

TÀI LIỆU THAM KHẢO

[1] Tuyên giáo Tỉnh ủy Khánh Hòa (2025), "Bảo đảm chủ quyền quốc gia trên không gian mạng nhằm phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia trong kỷ nguyên mới", Cổng thông tin điện tử Ban Tuyên giáo Tỉnh ủy Khánh Hòa, ngày 31/7/2025. Truy cập tại: https://btgdvtukhanhhoa.vn/chuyen-doi-so/bao-dam-chu-quyen-quoc-gia-tren-khong-gian-mang-nham-phat-trien-khoa-hoc-cong-ng

[2] Bộ Công an - Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (2025), "Đảm bảo an ninh mạng, bảo vệ vững chắc chủ quyền số quốc gia trên không gian mạng", Cổng thông tin điện tử Bộ Công an, ngày 20/8/2025. Truy cập tại: https://bocongan.gov.vn/bai-viet/dang-bo-cuc-an-ninh-mang-va-phong-chong-toi-pham-su-dung-cong-nghe-cao-to-chuc-thanh-cong-dai-hoi-dai-bieu-lan-thu-ii-nhiem-ky-2025-2030-1755695704

[3] Báo Điện tử VOV (2025), "An ninh mạng - Thành trì bảo vệ chủ quyền số", Báo Điện tử VOV, ngày 06/8/2025. Truy cập tại: https://vov.vn/cong-nghe/an-ninh-mang-thanh-tri-bao-ve-chu-quyen-so-post1220594.vov