BẢO ĐẢM AN NINH MẠNG VÀ AN NINH DỮ LIỆU TRONG ĐỔI MỚI GIẢNG DẠY CÔNG NGHỆ THÔNG TIN Ở HỌC VIỆN CHÍNH TRỊ HIỆN NAY

Phùng Thị Lan
Khoa Ngoại ngữ, Học viện Chính trị

Tóm tắt: *Trong bối cảnh kỷ nguyên số, an ninh mạng, an ninh dữ liệu đã trở thành thách thức sống còn mang tính toàn cầu và quốc gia. Chuyển đổi số trong quân đội đặt ra yêu cầu cấp bách về bảo vệ chủ quyền dữ liệu, đặc biệt trong lĩnh vực giáo dục và đào tạo. Bài viết tiếp cận từ lý luận, thực trạng an ninh mạng gắn với sự đổi mới mạnh mẽ của chương trình giảng dạy công nghệ thông tin tại Học viện Chính trị hiện nay. Trên cơ sở đó, đề xuất 05 giải pháp đồng bộ nhằm góp phần nâng cao chất lượng đào tạo đội ngũ cán bộ chính trị cấp chiến dịch, chiến thuật, đáp ứng yêu cầu bảo vệ vững chắc Tổ quốc trên không gian mạng.*

Từ khóa: *An ninh mạng; an ninh dữ liệu; giảng dạy công nghệ thông tin; Học viện Chính trị.*

ENSURING CYBERSECURITY AND DATA SECURITY IN THE INNOVATION OF INFORMATION TECHNOLOGY TEACHING AT THE POLITICAL ACADEMY TODAY

Abstract: *In the context of the digital era, cybersecurity and data security have become vital challenges at both global and national levels. Digital transformation in the military has created an urgent need to safeguard data sovereignty, particularly in the field of education and training. This article approaches the issue from both theoretical and practical perspectives, examining the current state of cybersecurity in relation to the ongoing strong innovation of the information technology curriculum at the Political Academy. On that basis, it proposes five synchronized solutions to help improve the quality of training for political officers at the operational and tactical levels, thereby meeting the requirements of firmly safeguarding the Fatherland in cyberspace.*

Keywords: *Cybersecurity; data security; information technology teaching; Political Academy.*

Nhận bài: 26/02/2026 Phản biện: 20/03/2026 Duyệt đăng: 24/03/2026

I. ĐẶT VẤN ĐỀ

Không gian mạng hiện nay đã thực sự trở thành "lãnh thổ thứ năm", nơi diễn ra các cuộc đấu tranh gay gắt về ý thức hệ, đánh cắp thông tin chiến lược và chiến tranh thông tin. Theo Báo cáo An ninh mạng năm 2025, bức tranh toàn cầu và tại Việt Nam đang đối mặt với những thách thức khốc liệt: hệ thống thông tin nước ta phải hứng chịu khoảng 552.000 cuộc tấn công mạng, khiến 52,3% tổ chức, doanh nghiệp chịu tổn hại. Đặc biệt nguy hiểm, tin tặc đang chuyển hướng lạm dụng trí tuệ nhân tạo (AI) tăng 89%, với khả năng xuyên thủng hệ thống chỉ trong vỏn vẹn 27 giây, chủ yếu thông qua các cuộc tấn công phi mã độc (chiếm 82%) nhắm vào định danh người dùng. Nhận định về tình hình này, tại Phiên họp thứ I năm 2026 của Ban Chỉ đạo An ninh mạng quốc gia ngày 21/3/2026, Thủ tướng Chính phủ Phạm Minh Chính đã nhấn mạnh: *"Bảo vệ an ninh mạng là yêu cầu cấp bách, thường xuyên, trọng yếu"*.

Trong bối cảnh nguy cơ an ninh mạng ngày càng lớn, sự nghiệp đổi mới giáo dục, đào tạo của đất nước và Quân đội cũng đang đứng trước yêu cầu cấp bách phải chuyển đổi số. Nghị quyết số 71-NQ/TW của Bộ Chính trị và Nghị quyết số 290-NQ/QUTW của Quân ủy Trung ương đã đặt ra đột phá xây dựng các nhà trường quân đội thông minh. Học viện Chính trị, trung tâm hàng đầu về đào tạo cán bộ nghiên cứu, giảng dạy khoa học xã hội nhân văn, cán bộ chính trị cấp chiến dịch, chiến thuật cho toàn quân, việc đổi mới giảng dạy công nghệ thông tin đang diễn ra mạnh mẽ. Tuy nhiên, sự chuyển đổi từ giảng dạy kỹ năng tin học cơ bản sang ứng dụng công cụ số, trí tuệ nhân tạo cũng đồng thời mở ra những "lỗ hổng" tiềm ẩn về an toàn thông tin, tài liệu nội bộ và dữ liệu số mang tính bí mật quân sự, bí mật nhà nước. Do đó, nghiên cứu về bảo đảm an ninh mạng, an ninh dữ liệu trong đổi mới giảng dạy công nghệ thông tin tại Học viện Chính trị hiện nay là đòi hỏi tất yếu, cấp thiết cả về lý luận và thực tiễn.

II. NỘI DUNG NGHIÊN CỨU

2.1. Tính tất yếu bảo đảm an ninh mạng, an ninh dữ liệu trong đổi mới giảng dạy công nghệ thông tin ở Học viện Chính trị

Luật An ninh mạng năm 2025 định nghĩa: "An ninh mạng là sự ổn định, an ninh, an toàn của không gian mạng; bảo vệ hệ thống thông tin và bảo đảm thông tin, dữ liệu, hoạt động trên không

gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân". "An ninh dữ liệu là sự bảo đảm chất lượng dữ liệu và các hoạt động xử lý, sử dụng dữ liệu trên không gian mạng phục vụ phát triển kinh tế - xã hội, chuyển đổi số quốc gia, tránh bị truy cập, sử dụng, tiết lộ, sửa đổi trái phép, phá hoại hoặc hành vi khác đe dọa hoặc gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội". Như vậy, nói đến an ninh mạng, an ninh dữ liệu không chỉ là sự bảo đảm an toàn hệ thống, mà còn nhấn mạnh năng lực chủ động ứng phó với các mối đe dọa từ AI và Big Data. Trong điều kiện chuyển đổi số diễn ra mạnh mẽ, việc bảo vệ, bảo đảm an ninh mạng, an ninh dữ liệu có vai trò thường xuyên, trọng yếu, quyết định sự ổn định, phát triển bền vững của mỗi quốc gia, dân tộc và mỗi tổ chức, cá nhân. Đối với môi trường quân sự, việc bảo đảm an ninh mạng, an ninh dữ liệu là tổng thể các hoạt động lãnh đạo, chỉ đạo, quản lý và ứng dụng các biện pháp kỹ thuật, nghiệp vụ của cơ quan, đơn vị, các chủ thể thuộc Bộ Quốc phòng trong việc phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh mạng, an ninh dữ liệu, bảo đảm sự ổn định, an toàn của không gian mạng, bảo đảm chất lượng dữ liệu và các hoạt động xử lý, sử dụng dữ liệu, ngăn chặn mọi âm mưu tấn công, phá hoại, thâm nhập hoặc chiếm quyền điều khiển.

Nhận thức sâu sắc mức độ nguy hiểm, nguy cơ đe dọa an ninh mạng, an ninh dữ liệu từ phần mềm độc hại, phần cứng độc hại, tội phạm mạng, khủng bố mạng, gián điệp mạng, tấn công mạng hiện nay, Ban Bí thư đã ban hành Chỉ thị số 57-CT/TW (tháng 12/2025), coi bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị là "*nhiệm vụ trọng yếu, thường xuyên"*. Nghị quyết số 3488-NQ/QUTW của Quân ủy Trung ương yêu cầu: "Bảo đảm an ninh mạng, an ninh dữ liệu... là yêu cầu xuyên suốt, không thể tách rời trong quá trình phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số". Đối với lĩnh vực giáo dục, đào tạo ở các nhà trường quân đội, Nghị quyết số 290-NQ/QUTW cũng yêu cầu phải xây dựng môi trường số gắn liền với việc "*bảo đảm tuyệt đối bí mật*". Nghị định số 147/2024/NĐ-CP của Chính phủ quy định rõ chức năng, nhiệm vụ của các tổ chức, cá nhân trong việc bảo đảm an ninh mạng, an ninh dữ liệu. Trong đó, Bộ Quốc phòng và các cơ quan đơn vị thuộc Bộ, "trong phạm vi chức năng, nhiệm vụ, quyền hạn của mình có trách nhiệm bảo vệ chủ quyền quốc gia trên môi trường mạng, bảo đảm an toàn thông tin mạng, an ninh mạng, bảo vệ bí mật Nhà nước, bí mật quân sự; phối hợp với các cơ quan có thẩm quyền trong đấu tranh, phòng, chống tội phạm và vi phạm pháp luật trên môi trường mạng".

Đổi mới giảng dạy công nghệ thông tin ở Học viện Chính trị là yêu cầu tất yếu của quá trình giáo dục, đào tạo đội ngũ cán bộ chính trị cấp chiến thuật, chiến dịch cho Quân đội. Sự thay đổi trong giảng dạy công nghệ thông tin không phải là sự chắp vá hay nâng cấp đơn thuần về mặt công cụ, như việc cập nhật phần mềm, nâng cấp máy tính hay kỹ năng soạn thảo văn bản. Trong một môi trường chuyên sâu về đào tạo cán bộ lãnh đạo, chỉ đạo công tác đảng, công tác chính trị, đổi mới giảng dạy công nghệ thông tin là sự kết hợp chặt chẽ giữa yếu tố khoa học công nghệ hiện đại và khoa học xã hội nhân văn quân sự. Đó là quá trình chuyển đổi căn bản, toàn diện chương trình, nội dung, hình thức, phương pháp truyền thụ tri thức số, nhằm định hình "văn hóa số", "bản lĩnh số" và năng lực "tác chiến thông tin" cho đội ngũ cán bộ chính trị cấp chiến dịch, chiến thuật. Trang bị tư duy, phương pháp trong việc phân tích, chọn lọc, xử lý, bảo mật dữ liệu và phản bác các thông tin xấu độc. Việc đổi mới giảng dạy công nghệ thông tin còn hướng tới giúp học viên nắm chắc, thành thạo trong ứng dụng tiến hành công tác tư tưởng, chính trị, tham gia trực diện vào cuộc đấu tranh phản bác các quan điểm sai trái, thù địch trên không gian mạng.

Bảo đảm an ninh mạng, an ninh dữ liệu là bộ phận khăng khít, yếu tố quan trọng, quyết định sự thành bại của đổi mới giáo dục, đào tạo tại Học viện Chính trị nói chung và đổi mới giảng dạy công nghệ thông tin nói riêng. Nghị quyết số 290-NQ/QUTW của Quân ủy Trung ương, đặt ra yêu cầu là phải xây dựng môi trường sư phạm quân sự thông minh, hiện đại nhưng phải tuyệt đối an toàn về thông tin, dữ liệu. Nghị quyết số 3488-NQ/QUTW của Quân ủy Trung ương cũng nhấn mạnh: "Chuyển đổi số phải gắn liền với bảo đảm an toàn thông tin, an ninh mạng; coi đây là nhiệm vụ trọng tâm, xuyên suốt".

Quán triệt tinh thần đó, Văn kiện Đại hội đại biểu Đảng bộ Học viện Chính trị lần thứ XVII coi việc *"đẩy mạnh ứng dụng công nghệ thông tin, chuyển đổi số",* "đẩy mạnh cải cách hành chính và chuyển đổi số, xây dựng Học viện thông minh, hiện đại" gắn liền với bảo vệ an toàn thông tin là

một trong những khâu đột phá trọng tâm để nâng cao chất lượng giáo dục, đào tạo. Bảo đảm an ninh mạng, an ninh dữ liệu trong đổi mới giảng dạy công nghệ thông tin ở Học viện Chính trị đã có những bước tiến vững chắc. Điểm sáng nổi bật là sự chuyển biến mạnh mẽ trong nhận thức của Đảng ủy, Ban Giám đốc Học viện và cấp ủy, chỉ huy các cấp, đội ngũ giảng viên; hạ tầng mạng nội bộ (mạng truyền số liệu quân sự) được đầu tư mở rộng, đáp ứng nhu cầu khai thác học liệu số và mô phỏng các bài tập công nghệ thông tin gắn sát với các nội dung giảng dạy chính trị, quân sự. Hiện nay, Học viện đã đổi mới chương trình học phần công nghệ thông tin theo hướng tăng cả nội dung, thời gian và đa dạng các hình thức, phương pháp, phương tiện giảng dạy. Đặc biệt, nội dung đã cập nhật theo yêu cầu chuyển đổi số trong lĩnh vực quân sự. Nhiều nội dung mới đưa vào giảng dạy như: sử dụng phần mềm Microstation V8i soạn thảo văn kiện tác chiến; ứng dụng AI xây dựng học liệu số; kỹ năng tương tác trên môi trường số và đã đầu tư nâng cấp chuyên đề về bảo đảm an toàn thông tin, an ninh mạng. Tuy nhiên, vẫn còn một số hạn chế: ở một số ít cán bộ, học viên vẫn còn tâm lý chủ quan khi kết nối thiết bị ngoại vi, hoặc chưa tuân thủ triệt để các quy tắc bảo mật khi xử lý tài liệu trên không gian mạng; hạ tầng và công nghệ, hệ thống máy chủ lưu trữ tài liệu, dữ liệu chưa đồng bộ với các phần mềm thực hành trực tuyến; năng lực phòng thủ của hệ thống mạng nội bộ trước các kỹ thuật tấn công nâng cao cần được củng cố; học viên thực hành trên các công cụ AI, tương tác dữ liệu trên nền tảng đám mây khiến nguy cơ rò rỉ tài liệu nội bộ, dễ bị "tin tặc sử dụng AI" xâm nhập như Báo cáo An ninh mạng 2025 đã cảnh báo..... Những hạn chế này xuất phát từ cả nguyên nhân khách quan do tốc độ phát triển công nghệ, tính đặc thù hoạt động quân sự bảo mật, song nguyên nhân chủ quan là cơ bản.

2.2. Giải pháp cơ bản bảo đảm an ninh mạng, an ninh dữ liệu trong đổi mới giảng dạy công nghệ thông tin tại Học viện Chính trị hiện nay

Một là, nâng cao nhận thức, trách nhiệm và bản lĩnh chính trị về an ninh mạng gắn với đặc thù chương trình đào tạo mới. Tăng cường giáo dục cho cán bộ, giảng viên, học viên, nhân viên về những nội dung cơ bản của công nghệ thông tin. Tổ chức thực chất chương trình Bình dân học vụ số, đảm bảo 100% nắm được những kiến thức cơ bản về công nghệ số, chuyển đổi số và đặc biệt là hiểu về an ninh mạng, an ninh dữ liệu và việc bảo vệ nó. Kết hợp nhiều hình thức phương pháp của giáo dục chính trị, giáo dục pháp luật nhằm nâng cao nhận thức cho mọi chủ thể về các nghị quyết, chỉ thị của Đảng, pháp luật của nhà nước, quy định của quân đội về bảo đảm, bảo vệ an ninh mạng, an ninh dữ liệu. Trọng tâm là Nghị quyết 57, Nghị quyết 71, Chỉ thị 57 của Trung ương, các Nghị quyết 290, Nghị quyết 3488 của Quân ủy Trung ương, Luật An ninh mạng năm 2025, Nghị định 147 của Chính phủ, Thông tư 81 của Bộ Quốc phòng và các văn bản khác có liên quan. Trước thực trạng 82% các cuộc xâm nhập mạng hiện nay, lợi dụng kẽ hở từ định danh người dùng, việc thiết lập "bức tường lửa" trong tư duy là giải pháp nền tảng. Cụ thể hóa Chỉ thị số 57-CT/TW và các Nghị quyết của Quân ủy Trung ương, Học viện cần giáo dục cán bộ, giảng viên chuyển dịch tư duy từ phòng thủ bị động sang "Phòng thủ chủ động", "Phòng thủ tích cực". Khi đưa các nội dung mới như ứng dụng AI, Microstation V8i vào giảng dạy, giảng viên cần lồng ghép khéo léo các tình huống lộ lọt thông tin quân sự vào bài giảng, giúp học viên nhận thức rõ hậu quả khôn lường của sự chủ quan trên môi trường mạng.

Hai là, hoàn thiện quy chế quản lý, phân quyền và thiết lập cơ chế phản ứng nhanh về bảo mật dữ liệu học thuật. Học viện cần cụ thể hóa yêu cầu của Quân ủy Trung ương trong Nghị quyết số 290-NQ/QUTW về việc: "xây dựng cơ chế quản lý chặt chẽ, phân cấp bảo mật, ngăn ngừa nguy cơ rò rỉ dữ liệu". Thường xuyên quán triệt và cụ thể các văn bản pháp luật của cấp trên để xây dựng quy chế, quy định, hướng dẫn cụ thể phù hợp với đặc thù giáo dục, đào tạo của Học viện. Đồng thời bảo đảm, tạo điều kiện cho đổi mới giảng dạy, không vì tuyệt đối hóa yếu tố bảo mật mà không dám đổi mới giảng dạy, đổi mới nội dung, chương trình học tập. Các học liệu số, văn kiện tác chiến thực hành phải được gán nhãn bảo mật minh bạch. Đồng thời, cần rèn luyện cho đội ngũ giảng viên, học viên, nhân viên cơ chế phản ứng nhanh khi phát hiện vi phạm quy định bảo vệ dữ liệu, phải lập tức thông báo bằng văn bản cho Bộ Tư lệnh 86 và Cục Bảo vệ an ninh Quân đội trong vòng 72 giờ để có biện pháp ngăn chặn kịp thời sự lây lan của các mã độc thế hệ mới.

Ba là, hiện đại hóa hạ tầng kỹ thuật và ứng dụng các công nghệ bảo mật đa lớp gắn với thực tiễn thực hành công nghệ số. Việc đầu tư hạ tầng phải tuân thủ nguyên tắc "Bảo mật từ khâu thiết kế" theo Chỉ thị 57-CT/TW: "Hệ thống chưa bảo

đảm an toàn, an ninh thì kiên quyết chưa đưa vào sử dụng". Học viện cần hướng tới sử dụng giải pháp công nghệ không phụ thuộc vào các đối tác ngoài quân đội theo tinh thần Nghị quyết 3488-NQ/QUTW. Phối hợp với Bộ Tư lệnh 86 thiết kế kiến trúc mạng an toàn. Đặc biệt, để đáp ứng chương trình giảng dạy môn học như thực hành AI, tương tác số, Học viện phải xây dựng các vùng cách ly mạng ảo (Sandbox) độc lập, cho phép tự do thực nghiệm công nghệ mới mà không tạo ra lỗ hổng đe dọa mạng Truyền số liệu quân sự lõi.

Bốn là, bồi dưỡng, chuẩn hóa năng lực an ninh mạng và tư duy tác chiến không gian mạng cho đội ngũ giảng viên. Giảng viên công nghệ thông tin ở Học viện Chính trị không chỉ cần giỏi về công nghệ số, kỹ năng thuật toán mà phải có "nhãn quan chính trị số". Học viện phải thường xuyên cử giảng viên đi đào tạo, bồi dưỡng, tập huấn chuyên sâu tại các trung tâm, các cơ sở đào tạo về công nghệ thông tin, về an ninh mạng, an ninh dữ liệu hàng đầu. Giảng viên phải đủ năng lực giải mã các thủ đoạn lừa đảo Deepfake (đang gia tăng mạnh nhờ AI), chỉ ra nguyên lý phòng chống sự xâm nhập của tư tưởng thù địch qua các kẽ hở kết nối, biến mỗi giờ học công nghệ thông tin thành một cuộc rèn luyện bản lĩnh chiến đấu trên không gian số.

Năm là, tăng cường kiểm tra, giám sát công nghệ và thường xuyên tổ chức diễn tập ứng cứu sự cố không gian mạng. Học viện cần duy trì tổ chuyên trách giám sát 24/7 lưu lượng dữ liệu và rà quét lỗ hổng định kỳ tại các phòng máy thực hành. Cần đưa nội dung diễn tập ứng phó sự cố an ninh mạng vào chương trình học tập, bổ trợ để học viên có thể tham quan, tham gia có kiến thức thực tiễn. Các kịch bản giả định bám sát thực tiễn tấn công tốc độ cao như mã độc mã hóa dữ liệu chỉ trong vài phút, sẽ giúp cán bộ chính trị tương lai rèn luyện bản lĩnh chỉ huy, quản trị rủi ro đa ngành, sẵn sàng xử lý khủng hoảng ngay khi tốt nghiệp về công tác ở các cơ quan, đơn vị.

III. KẾT LUẬN

Bảo đảm an ninh mạng và an ninh dữ liệu là nhiệm vụ chính trị trọng yếu mang tính sống còn trong đổi mới giảng dạy công nghệ thông tin ở Học viện Chính trị. Bối cảnh tấn công mạng bùng nổ toàn cầu cùng sự dịch chuyển mạnh mẽ của chương trình đào tạo từ tin học cơ bản sang ứng dụng AI và tác chiến số đòi hỏi một "hàng rào" bảo mật tương xứng cả về công nghệ lẫn con người. Quán triệt sâu sắc các nghị quyết, chỉ thị của Đảng, Nhà nước và Quân ủy Trung ương, việc thực hiện đồng bộ 05 nhóm giải pháp trên sẽ tạo ra sức đề kháng nội sinh vững chắc. Qua đó, bảo đảm công cuộc chuyển đổi số trong giáo dục, đào tạo ở Học viện diễn ra an toàn tuyệt đối, kiến tạo nên thế hệ cán bộ chính trị tinh nhuệ về lý luận, sắc bén về công nghệ, đủ bản lĩnh bảo vệ vững chắc nền tảng tư tưởng của Đảng và không gian mạng quốc gia./.

TÀI LIỆU THAM KHẢO

Ban Bí thư (2025), *Chỉ thị số 57-CT/TW về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị,* Hà Nội, ngày 31/12/2025.

Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam (2025), *Nghị định số 147/2024/NĐ-CP quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng*, Hà Nội, ngày 09/11/2024, Điều 22.

Đảng bộ Học viện Chính trị (2025), *Văn kiện Đại hội đại biểu đảng bộ Học viện Chính trị lần thứ XVII nhiệm kỳ 2025 - 2030,* Hà Nội.

Quân ủy Trung ương (2025), *Nghị quyết số 3488-NQ/QUTW về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số trong Quân đội*, Hà Nội, ngày 29/01/2025.

Quân ủy Trung ương (2026), *Nghị quyết số 290-NQ/QUTW về đột phá phát triển giáo dục và đào tạo trong Quân đội,* Hà Nội, ngày 07/01/2026.

Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam (2025), *Luật An ninh mạng, Luật số 116/2025/QH15, ngày 10/12/2025, Khoản 1, Điều 2.*