

XÂY DỰNG “TUYẾN PHÒNG THỦ MỀM” TRÊN KHÔNG GIAN SỐ THÔNG QUA CÔNG TÁC GIÁO DỤC QUỐC PHÒNG VÀ AN NINH CHO SINH VIÊN

Nguyễn Văn Phúc¹, Đinh Văn Quyên¹

Email: phucnvan@huit.edu.vn

Ngày tòa soạn nhận được bài báo: 19/08/2025

Ngày phản biện đánh giá: 13/10/2025

Ngày bài báo được duyệt đăng: 24/10/2025

DOI: 10.59266/houjs.2025.764

Tóm tắt: Trong bối cảnh số hóa đa nền tảng, không gian số như “cánh cửa mở rộng vô tận”, nơi sinh viên (SV) có cơ hội tiếp cận kho tri thức toàn cầu nhưng cũng tiềm ẩn những “vùng tối” về an ninh phi truyền thống và chiến tranh thông tin. Nhiệm vụ bảo vệ Tổ quốc (BVTQ) trong tiến trình mới, bên cạnh “tuyến phòng thủ cứng” bằng biện pháp quân sự, khoa học công nghệ cần hình thành “tuyến phòng thủ mềm” như lớp lá chắn phi vật chất dựa trên bản lĩnh chính trị, năng lực tư tưởng và kỹ năng số. Giáo dục quốc phòng và an ninh (GDQP&AN) giữ vai trò nòng cốt, không dừng lại ở trang bị kiến thức quân sự quốc phòng mà còn rèn luyện bản lĩnh, kỹ năng xử lý thông tin, phản biện và phòng chống thông tin xấu độc trong bối cảnh “ô nhiễm thông tin” đồng thời xây dựng trách nhiệm công dân và ý thức BVTQ từ khi “nước chưa nguy”; hình thành “kháng thể tư tưởng”, nâng cao năng lực miễn dịch trước tác động tiêu cực trên không gian số. Xây dựng “tuyến phòng thủ mềm” cho SV là yêu cầu chiến lược nhằm củng cố thế trận lòng dân trong kỷ nguyên số. Đề xuất một số giải pháp xây dựng “tuyến phòng thủ mềm” cho SV thông qua GDQP&AN hình thành thể hệ tri thức trẻ vừa vững vàng lý tưởng vừa linh hoạt trong ứng xử số, trở thành lực lượng phòng thủ quan trọng, góp phần BVTQ từ sớm, từ xa.

Từ khóa: chiến tranh thông tin, giáo dục quốc phòng và an ninh, không gian số, sinh viên, tuyến phòng thủ mềm

I. Đặt vấn đề

Trong bối cảnh chiến tranh thông tin và các mối đe dọa an ninh phi truyền thống không ngừng lan rộng bởi những làn sóng hội nhập quốc tế sâu rộng và

toàn cầu hóa mạnh mẽ, không gian số dần trở thành một môi trường sống mới, gắn bó mật thiết với các hoạt động học tập, công tác nghiên cứu và giao tiếp xã hội của mỗi cá nhân. Đặc biệt, với SV là lực

¹ Trường Đại học Công Thương Thành phố Hồ Chí Minh

lượng trẻ kế tục sự nghiệp BVTQ trong thời đại mới, không gian số mang lại lợi ích như một kho tàng tri thức vô hạn, nơi nuôi dưỡng khát vọng sáng tạo, đồng thời đây cũng là dòng xoáy ngầm chứa đựng nhiều nguy cơ về an ninh phi truyền thống. Sự lan truyền của tin giả dễ thao túng nhận thức còn non trẻ, nguy cơ “ô nhiễm tư tưởng” và các hoạt động chiến tranh thông tin cũng như các tác động xuyên biên giới của các thế lực thù địch, chống phá đã và đang trực tiếp tác động đến lối sống, tư tưởng và nhận thức của thế hệ chủ nhân tương lai của đất nước.

Đại hội XIII khẳng định: *“Chủ động đấu tranh kịp thời, hiệu quả, từng bước đẩy lùi các loại tội phạm; phòng ngừa và ứng phó kịp thời với các mối đe dọa an ninh truyền thống và an ninh phi truyền thống; làm thất bại âm mưu và hoạt động “diễn biến hoà bình”, bạo loạn lật đổ của các thế lực thù địch, phản động”* [4, tr. 69]. Quan điểm trên nhấn mạnh yêu cầu mới trong nhiệm vụ BVTQ thời kỳ mới không chỉ dừng lại ở phương diện công nghệ hay biện pháp quân sự truyền thống mà còn nằm ở bình diện phi truyền thống đặc biệt là trên mặt trận không gian số, trước yêu cầu đó việc chú trọng xây dựng một “tuyến phòng thủ mềm” như một khả năng tự đề kháng về tư tưởng, chính trị, đạo đức, lối sống và kỹ năng số của mỗi cá nhân nhất là SV trở thành vấn đề cốt lõi trong chiến lược BVTQ trên “mặt trận số”.

Công tác GDQP&AN trong các cơ sở giáo dục giữ vị trí nòng cốt trong triển khai xây dựng tuyến phòng thủ này. Điều 19 Luật số: 30/2013/QH xác định nội dung phổ biến kiến thức QPAN cho toàn dân về: *“Những hiểu biết cần thiết về độc lập, chủ quyền, thống nhất và toàn vẹn lãnh thổ của Tổ quốc; âm mưu, thủ*

đoạn hoạt động chống phá của các thế lực thù địch; nhiệm vụ quốc phòng và an ninh trong từng thời kỳ; phòng thủ dân sự; trách nhiệm của công dân đối với sự nghiệp xây dựng và bảo vệ Tổ quốc Việt Nam xã hội chủ nghĩa” [5]. Điều này cho thấy công tác GDQP&AN không chỉ đóng vai trò truyền đạt kiến thức quân sự bên cạnh đó hướng đến việc hình thành bản lĩnh chính trị, nâng cao năng lực xử lý thông tin và xây dựng niềm tin vững chắc cho SV trước những biến động phức tạp của không gian số.

Từ những vấn đề trên có thể thấy, việc xây dựng “tuyến phòng thủ mềm” trên không gian số thông qua công tác GDQP&AN cho SV không đơn thuần là một yêu cầu nhất thời mà còn thể hiện tầm nhìn chiến lược lâu dài. Tham luận tập trung phân tích cơ sở lý luận và thực tiễn; làm rõ những thách thức hiện đại như chiến tranh thông tin, an ninh phi truyền thống trên không gian số; đồng thời đề xuất những định hướng và giải pháp nhằm phát huy vai trò của GDQP&AN trong xây dựng bản lĩnh, niềm tin và năng lực số cho SV. Qua đó, có thể nói SV không chỉ là đối tượng cần được bảo vệ mà còn đóng vai trò như một lực lượng nòng cốt trong sự nghiệp BVTQ từ sớm, từ xa trong kỷ nguyên số.

II. Cơ sở lý luận

2.1. Khái niệm “tuyến phòng thủ mềm” và nhiệm vụ bảo vệ Tổ quốc trên không gian số

Khái niệm “tuyến phòng thủ mềm” có thể hiểu là hệ thống rào chắn năng lực mềm hoặc một lớp “lá chắn phi vật chất”, nhằm chặn đứng sự xâm nhập của các dòng chảy thông tin độc hại, các thế lực chống phá, phòng ngừa các thủ đoạn phi truyền thống trên không gian số.

Bản chất của tuyến phòng thủ này là một sự kết hợp đa tầng, bao gồm bản lĩnh chính trị, nhận thức hành vi, phẩm chất đạo đức là lớp nền cứng cùng với kỹ năng số và năng lực ứng xử có trách nhiệm là mũi nhọn linh hoạt. Đây là nền tảng tạo nên sức đề kháng xã hội, một dạng “miễn dịch số” trước những nguy cơ thông tin sai lệch, xuyên tạc, “diễn biến hòa bình”, bạo loạn lật đổ, cách mạng màu thông qua không gian mạng,... vốn đã được Đảng ta chỉ rõ trong nhiều văn kiện là những thách thức chưa từng có về an ninh phi truyền thống trong bối cảnh số hóa.

Nội hàm của tuyến phòng thủ này có thể được hiểu đầy đủ khi đặt trong mối quan hệ hỗ trợ với “tuyến phòng thủ cứng” tức các giải pháp về kỹ thuật, pháp luật, cơ sở hạ tầng số và cơ chế quản lý của Nhà nước đối với không gian số hoặc các biện pháp quân sự truyền thống. Có thể thấy, khác với tuyến phòng thủ trên, “tuyến phòng thủ mềm” tạo nên nội lực xã hội, hình thành “miễn dịch số” ở cấp độ con người, đặc biệt là trong cộng đồng SV. Cần nhấn mạnh rằng “tuyến phòng thủ mềm” không mang tính thích ứng thụ động trước những biến đổi, đây là một tiến trình chủ động mang tính định hướng. Bao gồm trang bị kiến thức GDQP&AN cho SV theo Luật GDQP&AN và các chương trình đào tạo hiện hành như Thông tư 05/TT-BGDĐT [6]; hình thành kỹ năng ứng xử văn minh, có trách nhiệm trong môi trường số; nuôi dưỡng khả năng “tự đề kháng” trước thông tin xấu độc, qua đó biến mỗi SV trở thành một “tế bào khỏe mạnh” trong hệ miễn dịch xã hội. Chính nhờ sự bền vững từ bên trong, “tuyến phòng thủ mềm” mới có thể hỗ trợ cho “tuyến phòng thủ cứng” tạo thành hệ thống phòng thủ tổng hợp. Mối quan hệ này phản ánh quan điểm kết hợp chặt chẽ giữa “xây” và “chống”, giữa

“bảo vệ từ bên ngoài” và “củng cố từ bên trong”, đáp ứng yêu cầu nhiệm vụ BVTQ trong thời đại mới.

Ở góc độ lý thuyết, khái niệm “tuyến phòng thủ mềm” có thể đối chiếu và liên hệ với các tiếp cận hiện đại về an ninh phi truyền thống và sức mạnh mềm, nhấn mạnh sự ảnh hưởng bằng tư tưởng, văn hóa, tri thức. Có thể thấy, sức mạnh của một quốc gia trong kỷ nguyên số không chỉ phụ thuộc ở công nghệ hay tiềm lực quân sự mà còn phụ thuộc vào khả năng “miễn dịch” về nhận thức, văn hóa và bản lĩnh chính trị xã hội.

Vận dụng vào bối cảnh Việt Nam, khái niệm này gắn liền với quan điểm của Đảng về BVTQ “từ sớm, từ xa” và trên mọi không gian, trong đó không gian số được coi là một không gian sống mới. Trong văn kiện Đại hội XIII chỉ rõ yêu cầu: *“Chủ động ngăn ngừa các nguy cơ chiến tranh, xung đột từ sớm, từ xa; phát hiện sớm và xử lý kịp thời những nhân tố bất lợi, nhất là những nhân tố có thể gây đột biến; đẩy mạnh đấu tranh làm thất bại mọi âm mưu và hoạt động chống phá của các thế lực thù địch, phản động và cơ hội chính trị”* [4, tr. 117]. Đây là cơ sở chính trị, tư tưởng cho việc hình thành “tuyến phòng thủ mềm” trên không gian số.

Không gian số đối với SV như một sự tác động hai chiều. Một mặt, nó được xem là một đại dương mới của thời đại về tri thức, nơi sinh viên có thể ra khơi tìm kiếm tri thức mới, sáng tạo và giao lưu tiếp cận tri thức toàn cầu, qua đó trực tiếp góp phần thực hiện các định hướng chiến lược trong Nghị quyết số 57-NQ/TW và Nghị quyết số 71-NQ/TW. Mặt khác, đây cũng là “mặt trận” tiềm ẩn nhiều nguy cơ: tin giả, bạo lực ngôn từ, cách mạng màu, kích động cực đoan hay các hoạt động lợi

dụng “diễn biến hòa bình” nhằm tác động đến nhận thức, tư duy và nền tảng tư tưởng non trẻ của SV. Việc xây dựng “tuyên phòng thủ mềm” vì vậy không chỉ là yêu cầu mang tính cấp bách mà còn là nhiệm vụ giáo dục căn cơ trong thời đại số.

2.2. Sinh viên trên không gian số: từ mục tiêu tấn công lực lượng trong “tuyên phòng thủ mềm”

SV giữ một vị trí đặc biệt trong cấu trúc xã hội học tập số, là nhóm tiếp xúc thường xuyên với không gian số, từ học tập trực tuyến, mạng xã hội đến các diễn đàn trao đổi học thuật và các hoạt động xã hội. Điều này khiến SV trở thành đối tượng dễ bị tác động bởi các nguồn thông tin sai lệch, chưa kiểm chứng. Đồng thời, SV cũng là thành phần có khả năng trở thành lực lượng lan tỏa thông tin tích cực, có tiềm năng chuyển hóa thành nguồn lực bảo vệ an ninh tư tưởng gắn với nhiệm vụ BVTQ trên không gian mạng.

Tuy nhiên, thực trạng hiện nay cho thấy sự phân hóa khá lớn trong nhận thức và năng lực an ninh số của bộ phận SV. Một bộ phận có ý thức tốt về trách nhiệm công dân, nhưng cũng còn không ít SV thiếu khả năng kiểm chứng thông tin và chưa hiểu đầy đủ về trách nhiệm pháp lý khi tham gia không gian số. Bên cạnh đó là những thách thức hiện đại vô cùng lớn mà SV phải đối mặt trên không gian số: từ deepfake đến tác động xuyên biên giới. Các phương thức tấn công hiện đại không chỉ dừng ở “tin giả” đơn thuần mà đã tinh vi thành vũ khí hóa AI để tạo ra hình ảnh, video giả, sử dụng thuật toán để khuếch đại thông tin phân cực hay lợi dụng các nền tảng với thuật toán gợi ý nhằm tạo ra “bong bóng xác nhận”. Những kỹ thuật này khiến SV khó phân biệt thật giả, nhất là khi nội dung được trình bày hấp dẫn,

cảm xúc mạnh. Ngoài ra, tác nhân xuyên biên giới như nhóm lợi ích, các tổ chức tuyên truyền nước ngoài,... có thể khai thác các vấn đề xã hội nhạy cảm để khuấy động tâm lý giới trẻ. Thực tế quốc tế cho thấy, SV nhiều nước từng là tâm điểm của các cuộc vận động chính trị, xã hội. Tại Bangladesh, năm 2018 SV đã phát động phong trào biểu tình toàn quốc về an toàn giao thông, sử dụng mạng xã hội để tổ chức và lan tỏa thông điệp. Và mới đây nhất, năm 2025 ở Nepal, phong trào biểu tình GenZ là minh chứng cho việc thiếu bản lĩnh chính trị sẽ dẫn đến bị cuốn vào vòng xoáy bất ổn. Những ví dụ này phản ánh rõ nguy cơ và đồng thời khẳng định tầm quan trọng của việc xây dựng “tuyên phòng thủ mềm” cho SV Việt Nam trong bối cảnh toàn cầu hóa và hội nhập quốc tế.

Trên không gian số, SV là mục tiêu dễ bị lôi kéo, dễ bị tác động bởi các chiến dịch thông tin bởi các lý do cơ bản như: mức độ và tần suất sử dụng nền tảng số cao và hành vi chia sẻ nội dung nhanh và cảm tính; quá trình hình thành nhận thức vẫn đang diễn ra, nhất là nhận thức về chính trị, xã hội vẫn chưa hoàn thiện, do đó dễ bị ảnh hưởng bởi thông tin chưa được kiểm chứng; thiếu kỹ năng phân tích, kiểm chứng và thông tin trong môi trường có nội dung phức tạp. Song song đó, trong lịch sử dân tộc, SV luôn giữ vai trò tiên phong trong các phong trào cách mạng, từ cao trào đấu tranh chống thực dân đến sự nghiệp BVTQ và đổi mới. Bước vào kỷ nguyên số, vai trò này được đặt trong điều kiện mới, khi “mặt trận” không còn giới hạn trên chiến trường truyền thống mà mở rộng sang không gian số. Như vậy, SV với tư cách là lực lượng trẻ, năng động, giàu tiềm năng sáng tạo, tinh thần tham gia xã hội và khả năng lan tỏa cao khiến họ trở thành “tế bào” của “tuyên phòng

thủ mềm” và là nguồn lực có thể huy động để lan tỏa thông tin chính xác, ngăn chặn tin giả và hình thành văn hóa an ninh số nếu được trang bị đủ kỹ năng, kiến thức và bản lĩnh. Điều này phù hợp với quan điểm chiến lược của nước ta về phát huy và huy động sức mạnh toàn dân đồng thời coi trọng giáo dục và đào tạo nhân lực chất lượng cao bảo đảm độc lập, tự chủ và an ninh quốc gia theo Nghị quyết 71-NQ/TW và Nghị quyết 57-NQ/TW. Do đó, nhìn nhận SV không chỉ là “mục tiêu” mà còn là “lực lượng” là bước chuyển tư duy quan trọng để biến họ trở thành mắt xích then chốt của “tuyến phòng thủ mềm” trên không gian số là yêu cầu mang tính tất yếu trong bối cảnh mới.

2.3. Vai trò của công tác giáo dục quốc phòng và an ninh trong xây dựng “tuyến phòng thủ mềm”

Trong hệ sinh thái tri thức hiện đại, công tác GDQP&AN có vai trò như một mắt xích không thể thiếu, vừa mang tính nền tảng lý luận, vừa trực tiếp bồi dưỡng cho SV những năng lực cần thiết để tham gia BVTQ trong kỷ nguyên số. Theo quan điểm xuyên suốt Đảng ta luôn xác định quốc phòng toàn dân không chỉ là sự kết hợp sức mạnh chính trị, quân sự, tiềm lực kinh tế và văn hóa mà còn phải dựa trên “thế trận lòng dân”, nơi trách nhiệm và bản lĩnh của mỗi cá nhân chuyển hóa thành sức mạnh trước vận mệnh đất nước. Đại hội XIII chỉ ra rõ: *“hoàn thiện lý luận về quốc phòng, an ninh và tư duy mới về bảo vệ Tổ quốc từ sớm, từ xa, từ khi “nước chưa nguy” trên cơ sở xây dựng thế trận lòng dân vững chắc”* [4, tr. 100-101]. Từ đó có thể thấy, công tác GDQP&AN chính là một kênh quan trọng để xây dựng bản lĩnh chính trị, nuôi dưỡng ý chí tinh thần của SV, biến đây trở thành lực lượng tiên

phong trong “tuyến phòng thủ mềm” của đất nước.

Trước hết, GDQP&AN trang bị cho SV những kiến thức cơ bản và hệ thống về chính trị, quốc phòng và an ninh. Thông tư 05/2020/TT-BGDĐT quy định rõ mục tiêu của chương trình GDQP&AN là trang bị: *“kiến thức cơ bản về quan điểm của Đảng, chính sách, pháp luật của Nhà nước về quốc phòng và an ninh; xây dựng nền quốc phòng toàn dân, an ninh nhân dân, xây dựng thế trận quốc phòng toàn dân gắn với thế trận an ninh nhân dân, xây dựng lực lượng vũ trang nhân dân; bổ sung kiến thức về phòng thủ dân sự và kỹ năng quân sự; sẵn sàng thực hiện nghĩa vụ quân sự, nghĩa vụ công an bảo vệ Tổ quốc”*. Đây không chỉ là tri thức lý thuyết mà còn là hành trang để SV có thể nhận diện, phân tích và ứng xử trước những vấn đề thực tiễn trong đời sống số.

Thứ hai, công tác GDQP&AN có chức năng rèn luyện kỹ năng xử lý thông tin, phòng chống chiến tranh tâm lý và chiến tranh thông tin. Trong bối cảnh chiến tranh hiện đại ngày càng “phi tuyến tính”, không chỉ diễn ra bằng vũ khí mà còn bằng dòng chảy dữ liệu, tin tức giả mạo và thao túng dư luận, SV chính là đối tượng dễ bị tác động. Thực tế ở nhiều nước như Nepal, Bangladesh hay Ukraine cho thấy, SV vừa là lực lượng năng động nhất trong không gian số vừa dễ trở thành mục tiêu của các chiến dịch chiến tranh thông tin nhằm khơi dậy xu hướng cực đoan, bất mãn xã hội. Do đó, công tác GDQP&AN chú trọng đào tạo kỹ năng phản biện, chọn lọc thông tin, biết đặt câu hỏi đúng và kiểm chứng nguồn tin chính thống trở thành một yêu cầu cấp thiết. Có thể xem đây như quá trình xây dựng “lá chắn tinh thần”, giúp SV không bị cuốn

trôi bởi “ô nhiễm thông tin” hay các làn sóng tâm lý xã hội bất ổn.

Thứ ba, công tác GDQP&AN góp phần xây dựng bản lĩnh chính trị, trách nhiệm công dân và ý thức BVTQ từ xa. Như Đại hội XIII khẳng định, BVTQ trong tình hình mới phải đặt trên nền tảng “từ sớm, từ xa, từ khi nước chưa nguy”. Điều này có nghĩa là trách nhiệm của SV không chỉ thể hiện khi đất nước có xung đột, mà phải thể hiện ngay trong việc duy trì thái độ chính trị vững vàng, không bị lung lạc bởi quan điểm sai trái, thù địch. Thông qua công tác GDQP&AN, SV được giáo dục để trở thành những công dân “có kháng thể tư tưởng”, nghĩa là có khả năng tự miễn dịch trước những tác động tiêu cực trên không gian số, từ đó củng cố “tuyến phòng thủ mềm” bằng niềm tin, lý tưởng và trách nhiệm xã hội.

Cuối cùng, tác động cụ thể nhất của công tác GDQP&AN đối với SV chính là nâng cao “ý thức số”, khả năng ứng xử thông tin an toàn, khoa học, có trách nhiệm và nhân văn trong môi trường mạng. Không chỉ dừng lại ở việc hiểu biết các quy định pháp luật về an ninh mạng, SV cần được rèn luyện năng lực phân tích, phản biện và chọn lọc thông tin. Đây chính là kỹ năng sống còn trong bối cảnh chiến tranh thông tin đang diễn ra trên quy mô toàn cầu, nơi mà mỗi cú click chuột, mỗi lượt chia sẻ đều có thể tạo ra hiệu ứng xã hội sâu rộng.

Tóm lại, không dừng lại ở vai trò là học phần bắt buộc trong chương trình giáo dục, công tác GDQP&AN còn là một “hệ miễn dịch” chính trị tư tưởng cho SV trong kỷ nguyên số. Thông qua GDQP&AN, SV được cung cấp kiến thức, kỹ năng, được nuôi dưỡng bản lĩnh chính trị và tinh thần trách nhiệm từ đó có thể

phát triển thành lực lượng then chốt trong xây dựng “tuyến phòng thủ mềm” BVTQ từ khi “nước chưa nguy”.

2.4. Định hướng và giải pháp xây dựng “tuyến phòng thủ mềm” cho sinh viên thông qua công tác giáo dục quốc phòng và an ninh

Trong bối cảnh chiến tranh thông tin, tấn công mạng và các thách thức an ninh phi truyền thống ngày càng phức tạp, việc xây dựng “tuyến phòng thủ mềm” cho SV cần được xem như một nhiệm vụ chiến lược gắn với mục tiêu lâu dài của quốc phòng toàn dân. Trên cơ sở đó, một số định hướng và giải pháp có thể triển khai như sau:

Thứ nhất, nâng cao nội dung GDQP&AN theo hướng tích hợp giáo dục an ninh số

Không gian mạng vừa là môi trường học tập vừa là “mặt trận” mới trong BVTQ. Vì vậy, nội dung GDQP&AN trong nhà trường đại học cần được mở rộng, gắn với giáo dục về an ninh số, kỹ năng truyền thông số, nhận diện và phản bác thông tin sai lệch. Đây không chỉ là trang bị tri thức mà còn là rèn luyện bản lĩnh và thái độ ứng xử có trách nhiệm trên không gian mạng. Chẳng hạn, SV không chỉ học về âm mưu “diễn biến hòa bình” trên lý thuyết, mà còn được hướng dẫn cách kiểm chứng tin giả, phân tích nguồn tin, tránh bị thao túng bởi các chiến tranh tâm lý trên không gian số.

Thứ hai, ứng dụng công nghệ số trong giảng dạy và huấn luyện

Phương pháp giảng dạy GDQP&AN truyền thống cần được bổ sung bằng các công cụ giáo dục hiện đại hay “sự phạm công nghệ (EdTech pedagogy)”. Việc mô phỏng tình huống an ninh mạng, xây dựng

học liệu số, tạo diễn đàn đối thoại giúp SV trải nghiệm và xử lý vấn đề thực tế. Một số mô hình có thể vận dụng như:

(1) Mô hình Serious Games: Khác với game giải trí, Serious Games trong GDQP&AN có thể được thiết kế với mục tiêu nhận thức, hướng tới phát triển tư duy, ra quyết định, phản biện. Cho phép SV nhập vai vào các tình huống giả lập như xung đột thông tin, xung đột nhận thức, tự vệ mạng để diễn tập năng lực “phòng thủ mềm”. Ví dụ: Trò chơi “Thông tin thật giả” (Fact or Fake), có thể thiết kế để SV “chặn” các thông tin giả lan truyền trên mạng xã hội hoặc có thể đối phó với các luận điệu xuyên tạc của thế lực thù địch. Có thể thiết kế nhiều vòng chơi với nhiều mức độ khác nhau, qua mỗi vòng SV ngày càng nâng cấp được kỹ năng nhận định và phản biện. Có thể xem đây là mô hình “chuyên hóa tri thức thành hành vi”.

(2) Mô hình Mô phỏng thực tế ảo VR/AR: Mô hình này cho phép SV trải nghiệm các tình huống ảo hoá trong môi trường ba chiều, kết hợp hình ảnh, âm thanh và tương tác thời gian thực. Có thể vận dụng mô phỏng các tình huống tấn công mạng vào hệ thống hạ tầng thông tin của một cơ quan, đơn vị giả định hoặc tái hiện “khủng hoảng thông tin”, chiến dịch truyền thông xấu độc trên mạng xã hội, giả lập tình huống ứng phó với hành vi tuyên truyền sai trái,... SV sẽ nhập vai là “người bảo vệ an ninh mạng” hoặc “chuyên viên truyền thông chính thống” hoặc “công dân kỹ thuật số” để phân tích dữ liệu, ra quyết định nhanh và định hướng dư luận đúng hướng.

(3) Diễn đàn đối thoại số trên các nền tảng LMS: Một số nội dung có thể triển khai trên các nền tảng Edmodo, Moodle, Google Classroom hoặc Microsoft Teams

như Diễn đàn “Phòng tuyến thông tin” sinh viên phân tích, phản bác tin giả, luận điệu sai trái; thảo luận tình huống “Công dân số có trách nhiệm”, tranh luận về quyền tự do thông tin và giới hạn an ninh quốc gia; các buổi đối thoại trực tuyến với chuyên gia an ninh mạng, nhà nghiên cứu, giúp mở rộng tầm nhìn thực tiễn.

(4) Ứng dụng AI: Có thể mô phỏng chatbot “thế lực thù địch”, để AI vào vai “đối thủ” tạo ra các kịch bản tấn công thông tin, đưa ra các luận điểm sai lệch để SV phản biện; hoặc AI vào vai “người hướng dẫn” AI đánh giá bài phản biện của SV, chỉ ra điểm yếu trong lập luận từ đó cá nhân hóa quá trình rèn luyện tư duy phản biện.

Thứ ba, tăng cường phối hợp giữa nhà trường, gia đình và xã hội

Xây dựng “tuyến phòng thủ mềm” cho SV không thể chỉ đặt trên vai nhà trường. Cần có sự tham gia đồng bộ từ gia đình là chủ thể giáo dục định hướng giá trị, xã hội là chủ thể tạo môi trường lành mạnh và văn hóa mạng đồng thời có thể phối hợp các cơ quan quốc phòng an ninh để hướng dẫn kỹ năng nhận diện, cảnh báo nguy cơ, phối hợp bảo vệ thông tin cá nhân. Thông qua sự phối hợp này, SV sẽ được bảo vệ toàn diện cả về tri thức, kỹ năng và môi trường sống.

Thứ tư, phát huy vai trò chủ động và sáng tạo của sinh viên

SV không chỉ là đối tượng được bảo vệ mà cần trở thành “tác nhân phòng thủ mềm”. Điều này có nghĩa là SV phải tham gia chủ động vào các hoạt động nghiên cứu khoa học, xây dựng sản phẩm truyền thông số và hình thành các cộng đồng trực tuyến tích cực. Nhiều mô hình có thể triển khai như: đội SV xung kích an ninh mạng, nhóm truyền thông chống tin giả trong trường đại học hoặc câu lạc bộ nghiên cứu quốc phòng

an ninh trong kỷ nguyên số. Khi đó, mỗi SV không chỉ là người tiếp nhận tri thức mà còn là “chiến sĩ trên không gian số”, góp phần củng cố nền tảng tư tưởng, chính trị trong thời đại mới.

Thứ năm, kết nối kinh nghiệm quốc tế và bối cảnh toàn cầu

Thực tiễn các phong trào SV ở Nepal, Bangladesh hay “cách mạng màu” cho thấy, nếu thiếu định hướng chính trị và nền tảng tư tưởng vững vàng, SV rất dễ bị lôi kéo, biến thành công cụ cho các thế lực bên ngoài. Do đó, giải pháp cho Việt Nam không chỉ là “phòng thủ” mà còn là “chủ động hội nhập” học hỏi cách giáo dục an ninh số của các quốc gia tiên tiến, đồng thời giữ vững bản sắc và định hướng chính trị của Đảng.

Xây dựng “tuyến phòng thủ mềm” cho SV là một quá trình kết hợp chặt chẽ giữa giáo dục chính trị, tư tưởng với trang bị kỹ năng số hiện đại. Thông qua việc đổi mới GDQP&AN, ứng dụng công nghệ, tăng cường phối hợp đa chiều và phát huy vai trò chủ động của SV, chúng ta có thể hình thành một thể hệ trẻ vừa vững vàng về lý tưởng vừa linh hoạt trong ứng xử trên không gian mạng. Đó chính là lớp “lá chắn tinh thần” của quốc gia, góp phần BVTQ từ sớm, từ xa trong kỷ nguyên hội nhập và chuyển đổi số toàn cầu.

III. Phương pháp nghiên cứu

Để tiếp cận và làm sáng tỏ vấn đề nghiên cứu, bài viết sử dụng tổng hợp nhiều phương pháp nghiên cứu khoa học xã hội nhân văn, đảm bảo tính hệ thống, khách quan, phù hợp với yêu cầu lý luận và thực tiễn hiện nay. Trước hết, phương pháp phân tích tổng hợp được sử dụng để hệ thống hóa cơ sở lý luận của Đảng, Nhà nước về quốc phòng toàn dân, an ninh nhân dân cũng như các quan điểm

mới trong các nghị quyết, từ đó khái quát thành nền tảng khoa học cho việc phân tích vấn đề. Bên cạnh đó, phương pháp lịch sử logic vận dụng để khảo sát quá trình hình thành, phát triển của công tác giáo dục quốc phòng và an ninh trong hệ thống giáo dục đại học, qua đó chỉ ra tính tất yếu của việc gắn kết nội dung này với bối cảnh không gian số và những thách thức an ninh phi truyền thống. Ngoài ra, phương pháp so sánh đối chiếu được vận dụng để làm rõ điểm tương đồng, sự khác biệt và mối quan hệ bổ sung giữa “tuyến phòng thủ cứng” dựa trên tiềm lực quân sự, khoa học công nghệ và “tuyến phòng thủ mềm” dựa trên bản lĩnh chính trị, năng lực tư tưởng và ý thức công dân của sinh viên. Bài viết cũng sử dụng phương pháp phân tích tài liệu thứ cấp giúp khai thác các văn kiện chính trị, nghị quyết, công trình khoa học và nghiên cứu chuyên ngành, qua đó làm cơ sở tham chiếu khoa học. Đặc biệt, với việc kết hợp phương pháp tiếp cận liên ngành, bao gồm chính trị học, quốc phòng an ninh, truyền thông số và khoa học giáo dục, bài viết hướng đến xây dựng một cái nhìn đa chiều, không chỉ dừng lại ở mô tả hiện tượng mà còn lý giải bản chất, dự báo xu hướng, từ đó đề xuất giải pháp trong việc hình thành “tuyến phòng thủ mềm” trên không gian số thông qua công tác GDQP&AN cho SV.

IV. Kết quả nghiên cứu và thảo luận

Kết quả nghiên cứu cho thấy việc xây dựng “tuyến phòng thủ mềm” trên không gian số thông qua GDQP&AN cho SV không chỉ mang tính cấp thiết trước những nguy cơ chiến tranh thông tin và an ninh phi truyền thống mà còn có ý nghĩa chiến lược lâu dài trong củng cố “thế trận lòng dân”. Thực tiễn tại nhiều cơ sở giáo dục đại học ở Việt Nam, việc hình thành

“tuyển phòng thủ mềm” trong sinh viên không còn là vấn đề lý luận thuần túy mà đang diễn ra rõ nét trong thực tế học đường và không gian số. Điển hình, năm 2023 Đại học Duy Tân đã khai trương phòng Skills Lab về An ninh mạng đồng thời ra mắt chương trình “Vườn ươm Nhân tài An toàn - An ninh Mạng” hay còn được gọi là Dự án “Blue Rock”, hướng đến việc cung cấp cho xã hội một lực lượng SV mang ý thức BVTQ trên không gian số. Bên cạnh đó, năm 2023 Trường Đại học Nha Trang cũng đã khánh thành Phòng thực hành An ninh mạng, dự án này được coi như là một bước đi lớn trong xây dựng SV trở thành “lực lượng nòng cốt” trong “tuyển phòng thủ mềm” trên không gian số.

Phân tích lý luận cho thấy, tuyển phòng thủ này được hình thành từ sự kết hợp của tri thức, bản lĩnh chính trị, ý thức công dân và kỹ năng số, qua đó tạo nên một lớp “kháng thể tư tưởng” trong xã hội. So với một số tiếp cận quốc tế về an ninh phi truyền thống, có thể thấy sự tương đồng trong việc nhấn mạnh đến vai trò của “sức mạnh mềm” và an ninh tư tưởng; tuy nhiên, điểm khác biệt của Việt Nam nằm ở việc gắn trực tiếp khái niệm này với công tác GDQP&AN.

Thảo luận từ kết quả nghiên cứu cũng cho thấy một số vấn đề đặt ra. Thứ nhất, trong khi nhiều nghiên cứu quốc tế tập trung vào giải pháp công nghệ hoặc chính sách quản trị không gian số, nghiên cứu này bổ sung góc nhìn về con người, cụ thể là sinh viên - như một lực lượng lớn của tuyển phòng thủ mềm. Đây là sự đóng góp mới, làm rõ tính chủ động và sáng tạo của thế hệ trẻ trong BVTQ từ sớm, từ xa. Thứ hai, nghiên cứu đồng thời chỉ ra khoảng cách giữa mục tiêu giáo dục và thực tiễn: nội dung GDQP&AN hiện nay tuy đã có bước đổi mới theo Thông

tư 05/2020/TT-BGDĐT, nhưng vẫn chưa theo kịp tốc độ biến đổi của chiến tranh thông tin và công nghệ số. Điều này đặt ra yêu cầu tiếp tục tích hợp giáo dục an ninh số, kỹ năng phản biện và ứng xử thông tin vào chương trình đào tạo.

Đóng góp khoa học của nghiên cứu là khái quát hóa khái niệm “tuyển phòng thủ mềm” như một mô hình lý luận về an ninh phi truyền thống trong điều kiện số hóa. Về thực tiễn, nghiên cứu khẳng định GDQP&AN không chỉ dừng lại ở việc truyền đạt tri thức quân sự, chính trị mà còn góp phần nuôi dưỡng khả năng tự đề kháng, giúp sinh viên chuyển từ vị trí “mục tiêu dễ bị tác động” sang “lực lượng phòng thủ tích cực”. Tuy nhiên, nghiên cứu cũng thừa nhận hạn chế khi chưa đi sâu vào khảo sát định lượng hoặc phân tích so sánh trường hợp quốc tế một cách hệ thống. Đây sẽ là hướng tiếp theo nhằm củng cố luận điểm và mở rộng tính ứng dụng của kết quả.

V. Kết luận

Trong kỷ nguyên số, khi không gian mạng trở thành không gian sống song song thực tế, vấn đề an ninh phi truyền thống mà đặc biệt là an ninh thông tin và an ninh tư tưởng ngày càng nổi bật và phức tạp. Sự lan truyền của tin giả, chiến tranh thông tin và các hoạt động can thiệp xuyên biên giới đã cho thấy: BVTQ ngày nay không chỉ dựa vào tuyển phòng thủ cứng bằng công nghệ và sức mạnh quân sự mà còn cần đến một “tuyển phòng thủ mềm” được hun đúc từ sức mạnh tri thức, ý thức và nhận thức; ngoài ra được xây dựng từ bản lĩnh chính trị và trách nhiệm xã hội của cá nhân, trước hết là SV “mạch nguồn tri thức trẻ” của đất nước.

Công tác GDQP&AN chính là mắt xích không thể thiếu trong quá trình này. Thông qua việc trang bị kiến thức QPAN,

rèn luyện khả năng xử lý và phản biện thông tin, công tác GDQP&AN góp phần hình thành “kháng thể tư tưởng” và năng lực phòng thủ mềm cho SV trong bối cảnh chiến tranh thông tin hiện đại. Không dừng lại ở yêu cầu trước mắt nhằm chủ động đối phó với mối hiểm họa an ninh phi truyền thống bên cạnh đó còn mang ý nghĩa như một bước đi, một tầm nhìn mang tính chiến lược trong xây dựng “thế trận lòng dân” và BVTQ từ sớm, từ xa.

Những định hướng lớn của Đảng và Nhà nước về đổi mới giáo dục, phát triển khoa học, công nghệ, chuyển đổi số quốc gia và xây dựng thế trận quốc phòng toàn dân đã tạo cơ sở chính trị và pháp lý vững chắc để nâng cao chất lượng GDQP&AN trong các cơ sở giáo dục đại học. Nhiệm vụ đặt ra là phải tiếp tục đổi mới nội dung, phương pháp, gắn kết chặt chẽ giữa giảng đường và thực tiễn đời sống số; đồng thời phát huy vai trò chủ động, sáng tạo của SV, biến họ thành những lực lượng phòng thủ mềm trên không gian số.

Có thể khẳng định rằng, xây dựng “tuyến phòng thủ mềm” cho SV thông qua công tác GDQP&AN không chỉ bảo vệ chính thể hệ trẻ trước những tác động tiêu cực từ không gian mạng mà còn khơi dậy và phát huy sức mạnh của họ trong sự nghiệp BVTQ Việt Nam xã hội chủ nghĩa trong tình hình mới. Đây là con đường đúng đắn, lâu dài và bền vững kết hợp giữa “sức mạnh mềm” của con người Việt Nam với “sức mạnh cứng” của khoa học, công nghệ tạo thành một thế trận quốc phòng toàn diện trong thời đại số.

Tài liệu tham khảo

- [1]. Bộ Chính trị (2024). *Nghị quyết số 71-NQ/TW về đột phá phát triển giáo dục và đào tạo*. Hà Nội.
- [2]. Bộ Chính trị (2024). *Nghị quyết số 57-NQ/TW về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia*. Hà Nội.
- [3]. Bộ Chính trị (2024). *Kết luận số 91-KL/TW về tiếp tục thực hiện Nghị quyết số 29-NQ/TW, ngày 04/11/2013 về đổi mới căn bản, toàn diện giáo dục và đào tạo*. Hà Nội.
- [4]. Đảng Cộng sản Việt Nam. (2021). *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII (Tập I)*. NXB. Chính trị quốc gia Sự thật.
- [5]. Quốc hội (2013). *Luật Giáo dục quốc phòng và an ninh*. Hà Nội.
- [6]. Bộ Giáo dục và Đào tạo (2020). *Thông tư số 05/2020/TT-BGDĐT Ban hành chương trình giáo dục quốc phòng và an ninh trong trường trung cấp sư phạm, cao đẳng sư phạm và cơ sở giáo dục đại học*. Hà Nội.

BUILDING A “SOFT DEFENSE LINE” IN CYBERSPACE THROUGH NATIONAL DEFENSE AND SECURITY EDUCATION FOR STUDENTS

Nguyen Van Phuc², Dinh Van Quyen²

Abstract: *In the context of multi-platform digitalization, cyberspace emerges as an “infinite open door,” where students have the opportunity to access the global repository of knowledge but also face hidden “dark zones” of non-traditional security threats and information warfare. The mission of safeguarding the Fatherland in the new era, alongside the “hard defense line” built on military measures and science-technology, requires the establishment of a “soft defense line” as an intangible shield grounded in political will, ideological strength, and digital competencies. National Defense and Security Education plays a core role, not merely providing military and defense knowledge but also fostering resilience, skills in information processing, critical thinking, and resistance to harmful information within the context of “information pollution” while simultaneously cultivating civic responsibility and the awareness of protecting the Fatherland before the nation faces peril. It also contributes to forming “ideological antibodies” strengthening immunity against negative impacts in cyberspace. Building such a “soft defense line” for students is a strategic requirement to consolidate the “people’s defense posture” in the digital era. This paper proposes several solutions to strengthen the “soft defense line” for students through National Defense and Security Education, aiming to shape a young intellectual generation that is both firm in ideals and flexible in digital engagement, becoming an essential defensive force that contributes to safeguarding the Fatherland early and from afar.*

Keywords: *information warfare, national defense and security education, cyberspace, students, soft defense line*

² Ho Chi Minh City University of Industry and Trade