

PHÁT HUY TIỀM NĂNG CÔNG NGHỆ VÀ TRÍ TUỆ NHÂN TẠO TRONG BẢO VỆ TỔ QUỐC VIỆT NAM XÃ HỘI CHỦ NGHĨA TRƯỚC NGUY CƠ AN NINH PHI TRUYỀN THỐNG

NGÔ VĂN HƯỞNG

Đại học Mở - Địa chất

Ngày nhận bài: 06/9/2025; Ngày phản biện, biên tập và sửa chữa: 28/9/2025; Ngày duyệt đăng: 10/10/2025

ABSTRACT

The article analyzes the context of the strong development of technology and artificial intelligence (AI), and points out non-traditional security risks that are directly threatening the sovereignty and stability of the socialist Fatherland of Vietnam. Based on the assessment of the current status of AI application in national security protection, the article proposes a number of key solutions such as: perfecting mechanisms and policies; investing in technology infrastructure; developing high-quality human resources; strengthening international cooperation; building an early warning system based on AI. These are important orientations to firmly protect the Fatherland in the context of integration and the digital age.

Keywords: Technology; artificial intelligence; non-traditional security; national defense; socialist Vietnam.

Trong kỷ nguyên Cách mạng công nghiệp 4.0, công nghệ và trí tuệ nhân tạo (AI) phát triển với tốc độ vượt bậc, tạo ra những cơ hội to lớn cho phát triển kinh tế, xã hội, đồng thời đặt ra nhiều thách thức đối với an ninh quốc gia. Cùng với lợi ích về tự động hóa, tối ưu hóa quản lý và nâng cao năng lực dự báo, AI cũng tiềm ẩn nguy cơ bị khai thác vào mục đích gây bất ổn chính trị, xâm phạm chủ quyền số, hoặc tiến hành các hoạt động chiến tranh phi truyền thống. Nguy cơ an ninh phi truyền thống bao gồm các mối đe dọa như an ninh mạng, chiến tranh thông tin, khủng bố công nghệ, tấn công AI và kiểm soát dữ liệu. Đây là những thách thức có tính chất phức tạp, khó lường, tác động trực tiếp tới nền tảng an ninh của mỗi quốc gia, trong đó có Việt Nam. Việc nghiên cứu, khai thác và phát huy tiềm năng của công nghệ và AI trong bảo vệ Tổ quốc Việt Nam xã hội chủ nghĩa trở thành yêu cầu cấp bách, nhằm xây dựng hệ thống phòng thủ hiện đại, chủ động và bền vững trước các nguy cơ an ninh mới trong bối cảnh hội nhập quốc tế sâu rộng.

Trí tuệ nhân tạo là tập hợp các công nghệ mô phỏng trí thông minh của con người cho phép hệ thống máy tính tự học hỏi, suy luận và đưa ra quyết định. Trong lĩnh vực an ninh - quốc phòng, AI được ứng dụng để phân tích dữ liệu lớn, dự báo nguy cơ, phát hiện tấn công mạng, giám sát không gian mạng và tối ưu hóa khả năng phản ứng trước các tình huống khẩn cấp. AI còn hỗ trợ xây dựng hệ thống phòng thủ thông minh, nâng cao hiệu quả quản lý, kiểm soát và bảo vệ các hạ tầng chiến lược của quốc gia. Sự phát triển của AI mang lại những tiện ích vượt trội nhưng cũng kéo theo nhiều thách thức, như: 1- Tấn công mạng, đánh cắp dữ liệu: Hệ thống AI có thể bị xâm nhập hoặc thao túng để khai thác thông tin mật, gây thiệt hại nghiêm trọng cho an ninh quốc gia và các cơ sở hạ tầng số. 2- Chiến tranh thông tin, thao túng nhận thức: Công nghệ AI có thể bị lợi dụng để sản xuất tin giả, thao túng dư luận xã hội, ảnh hưởng đến ổn định chính trị, kinh tế và an ninh văn hóa - tư tưởng. 3- Giám điệp công nghệ, phá hoại hạ tầng trọng yếu: AI có khả năng điều khiển các hệ thống công nghiệp, giao thông, năng lượng. Khi bị xâm nhập, chúng có thể bị phá hoại gây ra sự cố lớn, ảnh hưởng trực tiếp đến an ninh và phát triển quốc gia.

Trên thực tế, nhiều quốc gia tiên tiến đã triển khai AI trong các hệ thống phòng thủ và an ninh, như: Mỹ phát triển các nền tảng AI để giám sát không gian mạng, tự động phát hiện và phản ứng trước các cuộc tấn công; Israel ứng dụng AI trong phân tích tình báo, nhận dạng mối đe dọa tiềm ẩn từ dữ liệu lớn nhằm đưa ra phương án ngăn chặn sớm; Trung Quốc xây dựng hệ thống AI phục vụ giám sát hạ tầng trọng yếu, phát hiện bất thường trong các lĩnh vực năng lượng, giao thông, thông tin. Những kinh nghiệm này cho thấy, việc phát huy tiềm năng AI trong bảo vệ Tổ quốc là xu hướng tất yếu đòi hỏi Việt Nam cần nghiên cứu sâu, xây dựng chiến lược ứng dụng phù hợp với điều kiện, năng lực và yêu cầu bảo vệ an ninh quốc gia trong thời đại số.

Trong những năm gần đây, Việt Nam đã từng bước ứng dụng công nghệ hiện đại và AI vào công tác bảo vệ an ninh quốc gia,

đặc biệt trong phòng chống các nguy cơ an ninh phi truyền thống. Nổi bật nhất là việc hình thành hệ thống phòng thủ mạng quốc gia, do Bộ Thông tin và Truyền thông phối hợp với Bộ Quốc phòng và Bộ Công an triển khai nhằm phát hiện, cảnh báo sớm và ngăn chặn các cuộc tấn công mạng quy mô lớn. Các trung tâm an ninh mạng của Bộ Công an và Bộ Quốc phòng đã áp dụng công nghệ AI trong giám sát, phân tích hành vi bất thường trên không gian mạng, nhận diện sớm nguy cơ tấn công và truy vết nguồn gốc sự cố. AI cũng hỗ trợ lọc tin giả, chống chiến tranh thông tin, đặc biệt trong bối cảnh mạng xã hội phát triển mạnh và trở thành môi trường truyền bá nhiều thông tin sai lệch. Ngoài ra, một số doanh nghiệp công nghệ trong nước như Viettel, BKAV, VNPT cũng đã nghiên cứu và phát triển các giải pháp an ninh mạng tích hợp AI, giúp tăng cường khả năng tự chủ về công nghệ, giảm phụ thuộc vào các hệ thống ngoại nhập. Nhờ đó, năng lực bảo vệ hạ tầng số, dữ liệu quan trọng và hệ thống điều hành trọng yếu của quốc gia được nâng cao, góp phần giữ vững an ninh chính trị và trật tự xã hội trong thời đại số.

Mặc dù đã đạt được nhiều kết quả tích cực, nhưng việc ứng dụng công nghệ và AI trong bảo vệ Tổ quốc ở Việt Nam vẫn còn những hạn chế nhất định, xuất phát từ một số nguyên nhân chủ yếu sau:

Một là, nguồn lực tài chính còn hạn chế: Việc đầu tư vào các hệ thống AI tiên tiến đòi hỏi chi phí rất lớn, từ phần cứng, phần mềm đến bảo trì, cập nhật. Trong khi đó, ngân sách cho lĩnh vực này chưa thực sự tương xứng với yêu cầu bảo đảm an ninh quốc gia trong bối cảnh mới.

Hai là, nhân lực chất lượng cao còn thiếu: Đội ngũ chuyên gia về an ninh mạng, khoa học dữ liệu và AI còn mỏng, đặc biệt là các chuyên gia có khả năng nghiên cứu sâu và phát triển công nghệ lõi. Điều này ảnh hưởng trực tiếp đến khả năng triển khai các dự án AI quy mô lớn và duy trì hệ thống ở mức an toàn, ổn định.

Ba là, hạ tầng dữ liệu chưa đồng bộ: AI chỉ phát huy hiệu quả tối đa khi có nguồn dữ liệu lớn, đa dạng và được chuẩn hóa. Tuy nhiên, hiện nay dữ liệu quốc gia về an ninh vẫn phân tán, thiếu liên thông giữa các bộ, ngành và chưa có hệ thống chia sẻ an toàn, hiệu quả.

Bốn là, chính sách và hành lang pháp lý chưa hoàn thiện: Các quy định pháp luật về quản lý, sử dụng AI trong lĩnh vực an ninh quốc gia còn chưa đồng bộ. Vấn đề bảo vệ quyền riêng tư, an toàn thông tin cá nhân và an ninh dữ liệu trong ứng dụng AI vẫn đang được nghiên cứu, hoàn thiện.

Hệ thống phòng thủ mạng quốc gia đã nhiều lần phát hiện và ngăn chặn các chiến dịch tấn công mạng nhắm vào các cơ quan Đảng, Chính phủ, và hệ thống tài chính - ngân hàng, góp phần giảm thiểu rủi ro rò rỉ dữ liệu mật. Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) thuộc Bộ Thông tin và Truyền thông đã triển khai các giải pháp AI để phân tích hành vi tấn công, phát hiện mã độc và cảnh báo sớm các nguy cơ. Các trung tâm an ninh mạng của Bộ Công an và Bộ Quốc phòng đang phát triển hệ thống phân tích dữ liệu lớn (Big Data) kết hợp với AI để giám sát thông

tin trên không gian mạng, nhận diện và xử lý kịp thời các hoạt động chống phá, khủng bố mạng và gián điệp công nghệ. Doanh nghiệp công nghệ quân đội Viettel đã phát triển nhiều nền tảng AI phục vụ phân tích nguy cơ tấn công, mã hóa dữ liệu và bảo vệ hạ tầng thông tin chiến lược của quốc gia. Những kết quả đạt được cho thấy Việt Nam đang đi đúng hướng trong việc ứng dụng công nghệ và AI nhằm bảo vệ Tổ quốc trước các nguy cơ an ninh phi truyền thống. Tuy nhiên, để phát huy hết tiềm năng, cần có chiến lược tổng thể về phát triển AI trong an ninh - quốc phòng, đầu tư nguồn lực đồng bộ về tài chính, nhân lực và hạ tầng dữ liệu, đồng thời hoàn thiện hành lang pháp lý nhằm đảm bảo tính an toàn, minh bạch và hiệu quả trong triển khai.

Để phát huy tiềm năng công nghệ và AI bảo vệ Tổ quốc Việt Nam xã hội chủ nghĩa trong kỷ nguyên số, thời gian tới cần tập trung vào một số giải pháp chủ yếu sau đây:

Thứ nhất, hoàn thiện cơ chế, chính sách, chiến lược quốc gia về AI và an ninh phi truyền thống

Để phát huy tối đa tiềm năng công nghệ và AI, Việt Nam cần xây dựng một khung chính sách đồng bộ, mang tính dự báo dài hạn. Trước hết, cần hoàn thiện Chiến lược quốc gia về AI gắn với bảo vệ an ninh quốc gia, đảm bảo tích hợp yếu tố an ninh phi truyền thống vào các văn bản quy hoạch, chiến lược phát triển kinh tế - xã hội, quốc phòng - an ninh. Bên cạnh đó, cần bổ sung quy định pháp lý về quản lý, khai thác và bảo vệ dữ liệu chiến lược; xây dựng hành lang pháp lý chặt chẽ cho việc phát triển các hệ thống AI phục vụ giám sát, phòng thủ mạng, nhận diện rủi ro và ứng phó sớm với các hình thức chiến tranh công nghệ mới. Ngoài ra, cần thiết lập các chuẩn mực đạo đức và nguyên tắc sử dụng AI trong lĩnh vực an ninh - quốc phòng, ngăn ngừa nguy cơ lạm dụng công nghệ dẫn đến xâm phạm quyền con người hoặc tạo ra các mối đe dọa tiềm ẩn. Chính phủ nên thúc đẩy cơ chế phối hợp liên ngành, kết nối các cơ quan như Bộ Quốc phòng, Bộ Công an, Bộ Thông tin và Truyền thông, cùng các viện nghiên cứu, trường đại học và doanh nghiệp công nghệ nhằm triển khai đồng bộ chiến lược AI vì an ninh quốc gia.

Thứ hai, đầu tư hạ tầng công nghệ, xây dựng hệ thống AI tự chủ

Một trong những giải pháp then chốt là đầu tư phát triển hạ tầng số hiện đại, bao gồm trung tâm dữ liệu quốc gia, siêu máy tính phục vụ mô phỏng, phân tích nguy cơ và các nền tảng đám mây an toàn dành riêng cho quốc phòng - an ninh. Việc xây dựng hệ thống AI tự chủ không chỉ giúp Việt Nam chủ động trước các nguy cơ tấn công công nghệ cao mà còn tránh phụ thuộc vào giải pháp, phần mềm và thuật toán từ nước ngoài. Các hệ thống AI có thể được ứng dụng trong nhiều lĩnh vực, như: 1- Giám sát và phòng thủ mạng: AI hỗ trợ phát hiện bất thường, truy vết xâm nhập, phân tích hành vi tấn công trong thời gian thực. 2- Phân tích dữ liệu lớn về an ninh quốc gia: Thu thập, phân loại, dự báo xu hướng các mối đe dọa phi truyền thống. 3- Bảo vệ cơ sở hạ tầng trọng yếu: Các nhà máy điện, hệ thống viễn thông, tài chính, ngân hàng có thể được bảo vệ bằng các thuật toán AI dự đoán nguy cơ và tự động ứng phó trước khi thiệt hại xảy ra. Đầu tư vào công nghệ AI còn cần đi kèm chính sách ưu đãi tài chính và khuyến khích doanh nghiệp công nghệ trong nước tham gia nghiên cứu, phát triển sản phẩm phục vụ lĩnh vực quốc phòng - an ninh.

Thứ ba, phát triển nguồn nhân lực chất lượng cao về AI, an ninh mạng, phân tích dữ liệu lớn

Nguồn nhân lực là yếu tố quyết định trong mọi chiến lược ứng dụng AI. Việt Nam cần có các chương trình đào tạo chuyên sâu về AI quân sự, an ninh mạng, khoa học dữ liệu và quản trị rủi ro công nghệ. Các trường đại học, học viện quân đội, công an phải phối hợp với doanh nghiệp công nghệ để mở các ngành đào tạo mới, xây dựng các phòng thí nghiệm, trung tâm nghiên cứu về AI ứng dụng trong phòng thủ. Đồng thời, cần triển khai các chương trình bồi dưỡng cán bộ hiện có, đặc biệt là những người trực tiếp tham gia quản lý, vận hành hệ thống an ninh quốc gia. Bên cạnh đó, việc thu

hút chuyên gia công nghệ cao từ nước ngoài, khuyến khích du học sinh ngành AI trở về nước cũng là một hướng đi cần được thúc đẩy.

Thứ tư, tăng cường hợp tác quốc tế và chia sẻ dữ liệu an ninh

Trong bối cảnh nguy cơ an ninh phi truyền thống có tính toàn cầu, không một quốc gia nào có thể tự mình đối phó hiệu quả. Việt Nam cần mở rộng hợp tác quốc tế về công nghệ AI, đặc biệt với các quốc gia tiên tiến và tổ chức quốc tế trong lĩnh vực phòng thủ mạng, chống tội phạm công nghệ cao và nghiên cứu AI quân sự. Các hoạt động hợp tác bao gồm: Chia sẻ dữ liệu an ninh phục vụ cảnh báo sớm, phân tích xu hướng tấn công; tổ chức diễn tập an ninh mạng liên quốc gia để nâng cao khả năng phản ứng nhanh trước các tình huống khủng hoảng; học hỏi kinh nghiệm triển khai hệ thống AI trong bảo vệ hạ tầng trọng yếu của các quốc gia hàng đầu như Mỹ, Israel, Hàn Quốc, Singapore. Hợp tác quốc tế không chỉ mang lại lợi ích về kỹ thuật, công nghệ mà còn giúp Việt Nam tham gia vào mạng lưới cảnh báo nguy cơ toàn cầu, đồng thời nâng cao vị thế chiến lược trong khu vực và trên thế giới.

Thứ năm, xây dựng hệ thống cảnh báo sớm và phân tích nguy cơ bằng AI

Một trong những ứng dụng quan trọng của AI là xây dựng hệ thống cảnh báo sớm về các nguy cơ an ninh phi truyền thống. Hệ thống này sẽ sử dụng thuật toán học máy để thu thập, phân tích dữ liệu khổng lồ từ các nguồn: mạng xã hội, hệ thống tài chính, cơ sở hạ tầng trọng yếu và các báo cáo tình báo. Qua đó, có thể dự đoán được nguy cơ tấn công mạng, chiến dịch tung tin sai lệch hoặc các mối đe dọa công nghệ khác trước khi chúng xảy ra. Việc xây dựng hệ thống cảnh báo sớm cần được triển khai theo hướng phân lớp nguy cơ (nguy cơ thấp, trung bình, cao) và đề xuất phương án ứng phó tự động nhằm giảm thiểu thời gian xử lý. Đặc biệt, các hệ thống này phải được đặt trong trung tâm điều hành an ninh mạng quốc gia, kết nối trực tiếp với Bộ Quốc phòng, Bộ Công an, Bộ Thông tin và Truyền thông, cùng các địa phương, bộ ngành liên quan. Việc phát huy tiềm năng công nghệ và AI trong bảo vệ Tổ quốc Việt Nam xã hội chủ nghĩa là xu thế tất yếu và mang ý nghĩa chiến lược trong bối cảnh các nguy cơ an ninh phi truyền thống ngày càng phức tạp. Công nghệ và AI không chỉ là công cụ hiện đại giúp phát hiện, phân tích và dự báo nguy cơ mà còn là lực lượng đột phá trong việc xây dựng nền quốc phòng - an ninh thông minh, linh hoạt và hiệu quả.

Như vậy, bài viết đã đề xuất các giải pháp trọng tâm bao gồm: hoàn thiện cơ chế, chính sách và chiến lược quốc gia về AI; đầu tư hạ tầng công nghệ và hệ thống AI tự chủ; phát triển nguồn nhân lực chất lượng cao; tăng cường hợp tác quốc tế, chia sẻ dữ liệu; đồng thời xây dựng hệ thống cảnh báo sớm và phân tích nguy cơ bằng AI. Để bảo vệ vững chắc Tổ quốc trong kỷ nguyên số, cần triển khai đồng bộ, lâu dài và linh hoạt các giải pháp trên, bảo đảm vừa nắm bắt cơ hội, vừa ứng phó hiệu quả với các nguy cơ an ninh phi truyền thống, giữ vững độc lập, chủ quyền và toàn vẹn lãnh thổ./.

TÀI LIỆU THAM KHẢO

- [1] Thủ tướng Chính phủ (2021), Quyết định số 127/QĐ-TTg ban hành Chiến lược quốc gia về nghiên cứu, phát triển và ứng dụng Trí tuệ nhân tạo đến năm 2030, Hà Nội.
- [2] Thủ tướng Chính phủ (2022), Quyết định số 964/QĐ-TTg phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030, Hà Nội.
- [3] Tạp chí Cộng sản (2022), Nhận thức về an ninh phi truyền thống theo tinh thần Đại hội XIII của Đảng và những vấn đề đặt ra đối với pháp luật hình sự Việt Nam, mục Nghiên cứu.
- [4] Cục An toàn thông tin - Bộ TT&TT (2022), Chức năng, nhiệm vụ của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), thông tin phổ biến pháp luật.
- [5] Viettel Cyber Security (2023), Giải pháp an toàn thông tin/AI & an ninh mạng: Viettel Endpoint Security và hệ sinh thái an toàn thông tin, tài liệu giới thiệu dịch vụ/doanh nghiệp.