



Thanh niên - Phụ nữ T07

Tạp san điện tử

T07 Youth and Women e-Bulletin

KỶ NGUYÊN CÔNG NGHỆ SỐ:

DẤU ẤN

TRÍ TUỆ NHÂN TẠO

The Digital Era: A Milestone of Artificial Intelligence



HỌC VIỆN KỸ THUẬT VÀ CÔNG NGHỆ AN NINH



Số 01 - Năm 2025



Thanh niên - Phụ nữ T07

Tạp san điện tử

T07 Youth and Women e-Bulletin

SỐ 01
ISSUE. 01

MỤC LỤC

01

THƯ NGỎ
OPEN LETTER

CHÍNH LUẬN - HỌC THUẬT

03

AI VÀ AN NINH QUỐC GIA: TỪ PHÒNG THỦ BỊ ĐỘNG ĐẾN CHỦ ĐỘNG KIẾN TẠO THỂ TRẬN AN NINH MỚI
AI and national security: From reactive defense to proactively constructing a new security paradigm

GUƠNG SÁNG ĐOÀN VIÊN, HỘI VIÊN

19

HOẠT ĐỘNG TRI ÂN, GIÁO DỤC TRUYỀN THỐNG CỦA ĐOÀN THANH NIÊN HỌC VIỆN KỸ THUẬT VÀ CÔNG NGHỆ AN NINH TẠI PHƯỜNG NINH XÁ
Ninh Xa commemoration and traditional education program of the Youth Union of the Academy of Security Engineering and Technology

24

ĐẠI ÚY NGUYỄN QUỲNH TRANG: TẤM GUƠNG GIẢNG VIÊN TIÊU BIỂU CỦA HỌC VIỆN KỸ THUẬT VÀ CÔNG NGHỆ AN NINH
Captain Nguyen Quynh Trang – An exemplary lecturer of the Academy of Security Engineering and Technology

28

HÀNH TRÌNH TỪ TRÁI TIM: DẤU ẤN TÌNH NGUYỆN CỦA TUỔI TRẺ HỌC VIỆN KỸ THUẬT VÀ CÔNG NGHỆ AN NINH
Journey from the heart: The mark in volunteer spirit of youth at the Academy of Security Engineering and Technology

VĂN HOÁ - NGHỆ THUẬT - ĐỜI SỐNG

34

THƠ: EM LÀ CHIẾN SĨ CÔNG AN & THƯ GỬI MẸ

35

TRỞ VỀ NƠI THANH XUÂN BẮT ĐẦU
Return to the dawning of Youth

GÓC THƯ GIẢN

38

HỌC VIỆN KỸ THUẬT VÀ CÔNG NGHỆ AN NINH - NHỮNG CHẶNG ĐƯỜNG PHÁT TRIỂN

40

EDUCATION QUIZ



Những tháng cuối năm 2025 đã ghi dấu một cột mốc lịch sử đầy tự hào và ý nghĩa đối với Học viện Kỹ thuật và Công nghệ an ninh. Đây là thời khắc chúng ta không chỉ nhìn lại chặng đường 15 năm phát triển đầy thành tựu dưới tên gọi cũ - Trường Đại học Kỹ thuật - Hậu cần Công an nhân dân (21/10/2010 - 21/10/2025), mà còn hân hoan chào đón một sự kiện mang tính lịch sử khi Nhà trường được chính thức chuyển đổi thành Học viện Kỹ thuật và Công nghệ an ninh (kể từ ngày 17/10/2025). Đây là dấu mốc quan trọng, có tính bước ngoặt, thể hiện tầm nhìn chiến lược, quyết tâm của Đảng, Nhà nước, Đảng ủy Công an Trung ương, Bộ Công an về xây dựng Học viện thành trung tâm đào tạo khoa học - kỹ thuật - công nghệ an ninh xứng tầm, đáp ứng yêu cầu, nhiệm vụ trong tình hình mới; mở ra chương mới đối với sự phát triển mạnh mẽ của Học viện trong những năm tiếp theo, trở thành nôi đào tạo nhân lực bảo đảm chủ quyền số, an ninh mạng, an ninh dữ liệu, an toàn thông tin không chỉ trong CAND mà cả hệ thống chính trị, phục vụ đắc lực phát triển các ngành công nghiệp, công nghệ chiến lược của đất nước.

Để hiện thực hóa tinh thần tiên phong và sự kế thừa di sản ấy, Đoàn Thanh niên, Hội Phụ nữ và Câu lạc bộ Tiếng Anh E4A đã phối hợp chung tay xây dựng sáng kiến ***“Tập san điện tử Thanh niên - Phụ nữ T07”***. Tập san là một diễn đàn số mở để đoàn viên thanh niên, hội viên phụ nữ của Học viện chia sẻ thông tin, lan tỏa tri thức và phát huy sức sáng tạo trong học tập, công tác; tạo môi trường thực tiễn để rèn luyện và nâng cao các kỹ năng nghiên cứu, biên tập, truyền thông và ngoại ngữ. Đây cũng chính là nơi giúp đoàn viên, hội viên thể hiện khả năng tư duy, sáng tạo, góp phần lan tỏa mạnh mẽ các giá trị tri thức, tinh thần xung kích trong kỷ nguyên phát triển mới của Học viện.

Số đầu tiên này ra mắt với chủ đề: ***“KỶ NGUYÊN CÔNG NGHỆ SỐ: DẤU ẤN TRÍ TUỆ NHÂN TẠO”*** mang đến những bài viết, phân tích và chia sẻ thực tiễn về vai trò của công nghệ số trong học tập, công tác và đời sống thông qua các chuyên mục về Chính luận - Học thuật, Gương sáng, Văn hóa - Nghệ thuật - Đời sống, và Góc thư giãn.

Kính mời Quý độc giả đón đọc, tích cực tương tác và đồng hành cùng Ban Biên tập để tô thắm thêm những trang sử vàng của Học viện Kỹ thuật và Công nghệ an ninh trong giai đoạn phát triển mới.

Trân trọng!



The final months of 2025 have marked a proud and meaningful historical milestone for the Academy of Security Engineering and Technology. This is a moment when we not only look back on 15 years of remarkable development under the former name - People's Public Security University of Technology and Logistics (October 21, 2010 - October 21, 2025), but also joyfully welcome a historic event - the official renaming of the institution as the Academy of Security Engineering and Technology (since October 17, 2025). This is an important turning point, reflecting the strategic vision and determination of the Party, the State, the Central Public Security Party Committee, and the Ministry of Public Security in establishing the Academy as a centre of security science, technology, and engineering that meets the demands and tasks of the new era. It opens a new chapter for the strong development of the Academy in the coming years, aiming to become a centre for training human resources to ensure digital sovereignty, cybersecurity, data security, and information safety, not only for the Public Security Forces but also for the entire political system, contributing effectively to the development of the country's strategic industries and technologies.

To realize the pioneering spirit and inheritance of this legacy, the Youth Union, Women's Union, and the E4A English Club have collaborated to launch the initiative **"T07 Youth and Women e-Bulletin"**. This serves as an open digital forum for the Academy's youth members and women members to share information, spread knowledge, and promote creativity in learning and work. It creates a practical environment for honing research, editorial, communication, and language skills. Through this platform, T07 cadets can express their creative thinking, contributing to the widespread dissemination of knowledge values and the spirit of dynamism in the new era of the Academy's development.

The inaugural issue launches with the theme: **"THE DIGITAL ERA: A MILESTONE OF ARTIFICIAL INTELLIGENCE"**, offering articles, analyses, and practical insights on the role of digital technology in education, work, and life across sections such as Political - Academic Insights, Exemplary Figures, Culture - Arts - Lifestyle, and Relaxation Corner.

We invite readers to enjoy the journal, actively engage, and accompany the Editorial Board in enriching the golden pages of the Academy of Security Engineering and Technology during the new stage of development.

Respectfully!

TỪ PHÒNG THỦ BỊ ĐỘNG ĐẾN CHỦ ĐỘNG KIẾN TẠO THỂ TRẬN AN NINH MỚI

Sự trỗi dậy của Trí tuệ nhân tạo (AI) không chỉ mang đến những đột phá về công nghệ mà còn đang tạo ra một thể hệ nguy cơ an ninh quốc gia hoàn toàn mới. Khi AI có thể tấn công một quốc gia từ cả bên ngoài lẫn bên trong, từ các chiến dịch thông tin giả quy mô lớn cho đến những sai lầm trong chính sách công, tư duy phòng thủ truyền thống giờ đây đã không còn phù hợp. Bài viết sẽ phân tích các mối đe dọa cốt lõi và luận giải sự cấp thiết của việc chuyển đổi sang một thể trận an ninh chủ động, nơi chúng ta không chỉ đối phó mà còn phải dự báo và làm chủ cuộc chơi.

Đầu năm 2021, một sự kiện chấn động chính trường châu Âu đã xảy ra: toàn bộ nội các chính phủ Hà Lan đã phải từ chức. Nguyên nhân không đến từ một cuộc tấn công mạng làm rò rỉ bí mật trọng yếu quốc gia, hay một bê bối chính trị thông thường, mà xuất phát từ chính một thuật toán Trí tuệ nhân tạo (AI) do cơ quan thuế triển khai. Với mục đích tốt là phát hiện gian lận trợ cấp trẻ em, hệ thống AI này, do được huấn luyện trên dữ liệu có sẵn định kiến và vận hành như một "hộp đen" không thể giải trình, đã tự động kết tội oan hàng chục nghìn gia đình, đẩy họ vào cảnh phá sản và tan vỡ. Thảm kịch này là một hồi chuông cảnh tỉnh đanh thép, cho thấy một sự thật quan trọng của Kỷ nguyên số: AI có thể đe dọa an ninh quốc gia mà không cần một dòng mã độc nào, không cần một cuộc tấn công mạng nào.

Thảm kịch chính trị ở Hà Lan không phải là một trường hợp cá biệt, mà là minh chứng điển hình cho một chiều hướng tấn công hoàn toàn mới trong kỷ nguyên số. Nó cho thấy, các mối đe dọa đối với an ninh quốc gia giờ

đây không chỉ đến từ bên ngoài - qua các chiến dịch thông tin giả hay các cuộc tấn công mạng tinh vi do AI hỗ trợ. Nguy hiểm hơn, chúng còn có thể trỗi dậy từ chính bên trong - khi việc triển khai AI một cách thiếu thận trọng trong các hệ thống quản trị nhà nước tự nó trở thành nguồn cơn gây ra khủng hoảng niềm tin và bất ổn xã hội. Để hiểu rõ toàn bộ bức tranh phức tạp này, trước hết cần nhận diện và phân tích sâu sắc từng lớp nguy cơ cốt lõi đang định hình nên bối cảnh an ninh mới.

Nhận diện các lớp nguy cơ trong Kỷ nguyên AI

Thứ nhất, và có lẽ là nguy hiểm nhất, là nguy cơ gây bất ổn chính trị - xã hội từ việc lạm dụng AI như một "vũ khí" thông tin có khả năng can thiệp trực tiếp vào các quy trình dân chủ và châm ngòi cho khủng hoảng. Các công nghệ AI tạo sinh như Deepfake không còn là công cụ đơn lẻ, mà đã trở thành những khí tài trong các chiến dịch thông tin được vận hành ở quy mô công nghiệp. Bằng cách phân tích dữ liệu lớn về tâm lý và hành vi của từng nhóm cộng đồng, các hệ thống này có thể tự động tạo ra những nội dung giả mạo được 'may đo' riêng cho từng đối tượng, tối ưu hóa khả năng gây kích động và hoài nghi. Các nghiên cứu công bố trong năm 2024 từ Viện An ninh mạng Stanford (thuộc Đại học Stanford, Mỹ) đã lượng hóa sức mạnh này, chỉ ra rằng các chiến dịch thông tin sử dụng AI tạo sinh không chỉ có tốc độ lan truyền nhanh hơn tới 70% mà còn có chi phí chỉ bằng 1/10 so với các chiến dịch truyền thống.

Nguy cơ này không còn là lý thuyết suông, mà đã được chứng minh qua từng yếu tố. Trong những năm gần đây, nhiều quốc gia ở châu Á đã trở thành nạn nhân của các chiến

dịch thông tin sai lệch quy mô lớn, dẫn đến những hậu quả chính trị nghiêm trọng. Cuộc tổng tuyển cử năm 2024 tại Indonesia là một ví dụ điển hình, nơi trong suốt chiến dịch, rất nhiều video, hình ảnh và âm thanh deepfake đã lan truyền mạnh mẽ, từ việc "hồi sinh" các nhà lãnh đạo quá cố để kêu gọi bỏ phiếu cho đến bóp méo phát biểu của các ứng cử viên. Mức độ ảnh hưởng của chúng đã được chỉ ra trong một cuộc khảo sát của Viện Nghiên cứu ISEAS-Yusof Ishak Institute (Singapore), cho thấy có tới 28.2% số người được hỏi tin rằng một video deepfake về ứng cử viên là thật, dù nó mô tả một sự kiện không có thực.

Tuy nhiên, mối đe dọa thực sự nằm ở kịch bản cộng hưởng ba chiều, nơi sự can thiệp của AI kết hợp với sự bất ổn xã hội và sự bất lực của hệ thống quản trị. Sự kiện khủng hoảng chính trị tại Bangladesh vào giữa năm 2024 đã cho thấy tốc độ đáng sợ mà một phong trào do giới trẻ và đặc biệt là sinh viên dẫn dắt được huy động và lan truyền qua mạng xã hội có thể leo thang dẫn đến sự sụp đổ của chính phủ trong thời gian ngắn. Mối nguy càng trầm trọng khi chính phủ các nước gặp khó khăn trong việc quản lý các nền tảng mạng xã hội xuyên quốc gia. Ví dụ điển hình là Nepal (tháng 9/2025), khi Chính phủ đã cố gắng đối phó với tình trạng tin giả bằng cách thực thi chính sách cấm hàng loạt mạng xã hội. Hành động cực đoan này lại bị coi là bịt miệng Gen Z, do đó đã châm ngòi cho một làn sóng biểu tình quy mô lớn và đẩy đất nước vào khủng hoảng chính trị trầm trọng hơn. Những ví dụ này cảnh báo về một thảm họa tiềm tàng cho an ninh quốc gia: khi AI tạo sinh can thiệp để dẫn dắt, cá nhân hóa nội dung kích động và cung cấp công cụ cho giới trẻ và đặc biệt là sinh viên để tạo, phát tán thông tin giả mạo một cách tinh vi (như đã thấy ở Indonesia), kết hợp với tốc độ huy động xã hội cao (như ở Bangladesh) và sự bất lực, phản ứng cực đoan của chính phủ (như ở Nepal) thì nguy cơ châm ngòi cho các cuộc bạo loạn và khủng

hoảng chính trị sẽ trở nên không thể kiểm soát.

Điều này tạo ra một cuộc cạnh tranh thông tin bất đối xứng, nơi các kênh truyền thông chính thống của Nhà nước, vốn vận hành theo các quy trình kiểm chứng nghiêm ngặt, trở nên lép vế và bị nhấn chìm trong một "cơn lũ" thông tin giả được sản xuất hàng loạt. Hậu quả là niềm tin vào các thiết chế nhà nước bị suy yếu, xã hội bị phân cực sâu sắc, và năng lực định hướng, quản lý thông tin của Nhà nước bị thách thức một cách trực tiếp.

Thứ hai, và có lẽ là sự thay đổi mang tính cấu trúc nhất, là sự "dân chủ hóa" năng lực tấn công tinh vi. Nếu trước đây, các hoạt động tấn công phức tạp đòi hỏi nguồn lực và trình độ của các cơ quan tình báo, thì giờ đây AI đã hạ thấp rào cản kỹ thuật và tài chính, trao năng lực tương tự vào tay các chủ thể phi nhà nước. Báo cáo của các hãng an ninh mạng công bố trong giai đoạn 2024-2025 cho thấy các bộ công cụ AI tự động tạo mã độc, vốn hoạt động theo mô hình kinh doanh cho thuê như một dịch vụ (Malware-as-a-Service), đang được rao bán trên các diễn đàn tin tặc với giá chỉ từ vài trăm đô la. Hậu quả trực tiếp là, theo báo cáo thường niên "Cost of a Data Breach" của Tập đoàn công nghệ đa quốc gia IBM (Hoa Kỳ), một cuộc tấn công bằng mã độc tổng tiền được AI tối ưu hóa có thể gây thiệt hại trung bình trên 5 triệu USD.

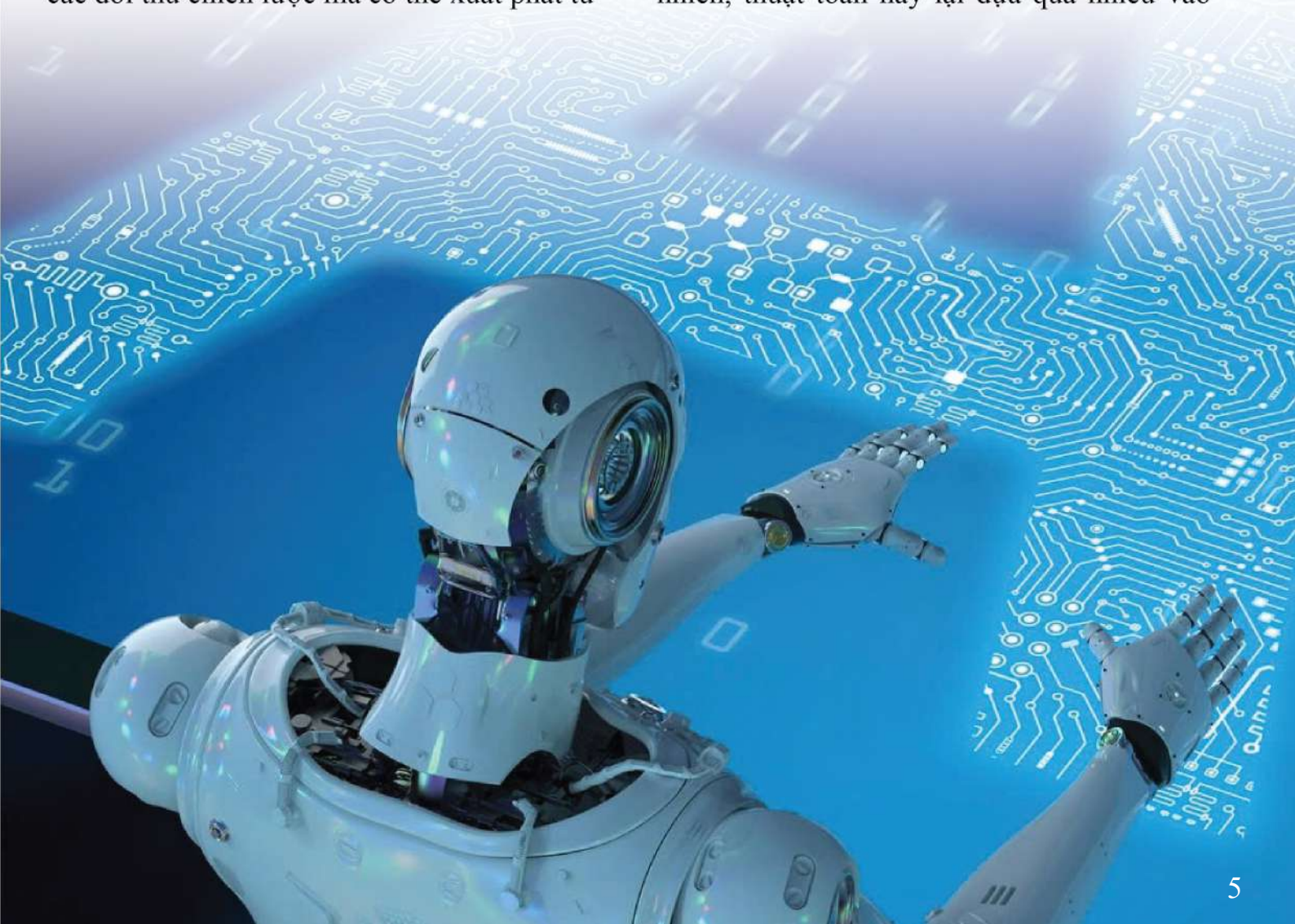
Tuy nhiên, nguy cơ đối với an ninh quốc gia không chỉ dừng lại ở thiệt hại tài chính. Các báo cáo phân tích mối đe dọa từ những công ty hàng đầu như Microsoft và Dragos (một công ty của Hoa Kỳ chuyên về an ninh cho hệ thống công nghiệp) trong giai đoạn 2024-2025 đã cảnh báo rằng các nhóm tin tặc đang tích cực phát triển các công cụ AI có khả năng tự động tìm kiếm và khai thác lỗ hổng trong các Hệ thống điều khiển công nghiệp (ICS) - bộ não vận hành của các hạ tầng trọng yếu như lưới điện, nhà máy nước và hệ thống giao thông. Một AI đủ tinh vi có thể "học" cách

vận hành bình thường của một lưới điện để tính toán thời điểm và phương thức tấn công hiệu quả nhất, gây ra sự sụp đổ trên diện rộng. Chính sự leo thang từ việc gây thiệt hại kinh tế sang khả năng làm tê liệt hạ tầng quốc gia trọng yếu này đã biến các cuộc tấn công do AI hỗ trợ trở thành một mối đe dọa an ninh quốc gia trực tiếp.

Với chi phí thấp và hiệu quả cao, một nhóm tội phạm nhỏ giờ đây có thể dùng AI để tự động viết ra các dòng mã độc đa hình có khả năng thay đổi liên tục để né tránh hệ thống phòng thủ; phân tích dữ liệu không gian và thời gian thực để lên kế hoạch cho một vụ tấn công vật lý với độ chính xác cao; hay nguy hiểm hơn là triển khai các cuộc tấn công phối hợp bằng đàn drone tự hành, có khả năng tự ra quyết định và áp đảo các hệ thống bảo vệ truyền thống. Điều này khiến cho bối cảnh an ninh trở nên phân mảnh và khó lường hơn bao giờ hết, khi mối đe dọa không còn chỉ đến từ các đối thủ chiến lược mà có thể xuất phát từ

bất kỳ đâu.

Thứ ba là nguy cơ dẫn đến sai lầm chính sách công từ các "hộp đen" thuật toán. Vụ bê bối ở Hà Lan là minh chứng rõ nét cho thấy một hệ thống AI, đặc biệt là các mạng nơ-ron sâu, có thể vận hành như một "hộp đen". Cơ chế ra quyết định của nó phức tạp đến mức ngay cả các kỹ sư tạo ra nó cũng không thể giải thích đầy đủ tại sao nó lại đưa ra một kết luận cụ thể. Nguy cơ này không chỉ là lý thuyết mà đã trở thành hiện thực đau đớn ở nhiều quốc gia. Vụ bê bối trợ cấp tại Hà Lan là bài học kinh điển về sự thất bại trong thực thi chính sách, nơi một hệ thống AI được thiết kế để tăng hiệu quả lại trở thành công cụ gây bất công. Tương tự, sự cố với thuật toán chấm thi A-level tại Vương quốc Anh lại là một thất bại trong hoạch định chính sách. Theo phân tích của đài BBC vào năm 2020, do các kỳ thi bị hủy vì đại dịch, chính phủ Anh đã sử dụng một thuật toán AI để dự đoán điểm. Tuy nhiên, thuật toán này lại dựa quá nhiều vào



thành tích lịch sử của ngôi trường, dẫn đến việc hạ điểm một cách có hệ thống đối với những học sinh xuất sắc ở các trường công lập, tạo ra một làn sóng phản đối dữ dội và buộc chính phủ phải hủy bỏ kết quả. Những trường hợp này đều khẳng định một chân lý quan trọng trong kỷ nguyên số: một sai sót kỹ thuật trong hệ thống AI do Nhà nước triển khai có thể nhanh chóng trở thành một thất bại nghiêm trọng về quản trị quốc gia, làm xói mòn niềm tin của người dân và gây ra những hệ lụy chính trị - xã hội khó lường.

Cuối cùng, một rủi ro mang tính nền tảng là sự phụ thuộc chiến lược vào chuỗi cung ứng công nghệ toàn cầu. Năng lực của mọi hệ thống AI đều được xây dựng trên ba trụ cột: dữ liệu, thuật toán và hạ tầng tính toán. Hiện nay, hệ sinh thái AI toàn cầu đang bị chi phối bởi một số ít tập đoàn công nghệ Hoa Kỳ như NVIDIA, vốn kiểm soát hơn 80% thị phần chip AI cho các trung tâm dữ liệu, và ba gã khổng lồ điện toán đám mây là Amazon Web

Services, Microsoft Azure, và Google Cloud, chiếm gần 70% thị phần toàn cầu. Sự tập trung quyền lực này tạo ra các "điểm nghẽn chiến lược", trao cho một vài chủ thể khả năng kiểm soát hạ tầng số của nhiều quốc gia. Nguy cơ này đã bị "vũ khí hóa" trong thực tế qua cuộc đối đầu công nghệ Mỹ - Trung, nơi Hoa Kỳ đã và đang sử dụng các lệnh cấm vận, hạn chế quyền truy cập vào công nghệ chip AI tiên tiến như một công cụ chính sách đối ngoại để gây áp lực và kìm hãm đối thủ chiến lược. Cuộc đối đầu này không chỉ diễn ra một chiều. Để đáp trả, Trung Quốc cũng đã bắt đầu sử dụng "quân bài" của riêng mình khi áp đặt các biện pháp hạn chế xuất khẩu Gali và Germani - hai vật liệu bán dẫn tối quan trọng, và đặc biệt là đất hiếm, tài nguyên mà họ gần như độc quyền và là thành phần không thể thiếu trong việc sản xuất các chip công nghệ cao. Điều này đe dọa trực tiếp đến chủ quyền số và năng lực tự chủ trong việc hoạch định chính sách kinh tế - an ninh quốc gia của các nước phụ thuộc.

Kiến tạo thể trận an ninh chủ động

Những phân tích trên đã chỉ ra một sự thật không thể phủ nhận: các nguy cơ từ Trí tuệ nhân tạo có tốc độ và quy mô vượt xa các mối đe dọa truyền thống. Chính vì vậy, tư duy an ninh dựa trên "Phòng thủ phản ứng" (Reactive Defense) đã tỏ ra hoàn toàn bất lực và lỗi thời. Yêu cầu cấp thiết là phải thực hiện một sự dịch chuyển mang tính học thuyết để kiến tạo nên một "thể trận an ninh mới" đúng như tiêu đề bài viết đã đề cập.

Trên thế giới hiện đang định hình hai học thuyết lớn đối lập nhau để kiến tạo nên thể trận này. Mô hình thứ nhất, được dẫn dắt bởi các quốc gia phương Tây, có nền tảng là "Năng lực chống chịu an ninh mạng" (Cyber Resilience). Theo định nghĩa của Viện Tiêu chuẩn và Kỹ thuật quốc gia Hoa Kỳ (NIST), học thuyết này không chỉ tập trung vào phòng thủ, mà là kiến tạo năng lực dự báo, chống chịu và phục hồi trong một môi trường số mở. Học thuyết này đã trở thành nền tảng trong các chiến lược quốc gia của các cường quốc: Hoa Kỳ đã thể chế hóa nó thông qua Chỉ thị Chính sách của Tổng thống PPD-21 do Tổng thống Barack Obama ban hành năm 2013; Vương quốc Anh và Singapore đều đặt nó làm trụ cột trong các Chiến lược An ninh mạng quốc gia của mình; và Liên minh châu Âu (EU) đã đưa nó vào các khung pháp lý chung như Chỉ thị NIS2 và Đạo luật về Sức chống chịu hoạt động kỹ thuật số (DORA).

Tuy nhiên, một mô hình đối trọng có sức ảnh hưởng không kém đang được định hình bởi Trung Quốc, dựa trên học thuyết về "Chủ quyền không gian mạng" (Cyber Sovereignty) - một khái niệm được Chủ tịch Tập Cận Bình nhiều lần nhấn mạnh và coi là nền tảng. Thay vì chấp nhận một không gian mạng mở và xây dựng năng lực chống chịu từ bên trong, học thuyết của Trung Quốc lại nhấn mạnh quyền của nhà nước trong việc kiểm soát toàn diện không gian mạng như một "vùng lãnh thổ" mới. Mô hình này được thực thi thông qua việc

xây dựng các hệ thống tường lửa kiên cố, kiểm soát chặt chẽ dòng chảy dữ liệu, và đặc biệt là chiến lược quốc gia về tự chủ công nghệ như "Made in China 2025" nhằm giảm thiểu tối đa sự phụ thuộc vào nước ngoài. Đây là một thể trận an ninh dựa trên sự phòng thủ từ xa, kiểm soát chặt chẽ và củng cố sức mạnh nội tại.

Trong bối cảnh đó, Việt Nam đang đứng trước những cơ hội và thách thức đan xen, hay nói đúng hơn là một ngã ba đường chiến lược. Là một quốc gia có nền kinh tế số đang phát triển nhanh, hạ tầng công nghệ ngày càng hiện đại và nguồn nhân lực trẻ, năng động, Việt Nam cũng phải đối mặt trực diện với cả bốn lớp nguy cơ an ninh từ AI đã được phân tích. Vị thế của một "người đi sau" mang đến một lợi thế chiến lược: chúng ta có cơ hội quan sát, học hỏi từ cả thành công và thất bại của những quốc gia tiên phong để định vị con đường của riêng mình giữa hai mô hình có sức ảnh hưởng lớn.

Mô hình "Chủ quyền không gian mạng" của Trung Quốc, với sự nhấn mạnh vào kiểm soát và tự chủ, chắc chắn cung cấp những bài học quý báu về việc duy trì sự ổn định và an ninh từ biên giới. Tuy nhiên, trong bối cảnh Việt Nam đang ngày càng hội nhập sâu rộng vào nền kinh tế toàn cầu, thúc đẩy đổi mới sáng tạo và tham gia vào các chuỗi cung ứng công nghệ quốc tế, học thuyết "Năng lực chống chịu an ninh mạng" của phương Tây lại tỏ ra có những ưu điểm phù hợp hơn. Nó không chỉ cung cấp một khuôn khổ để bảo vệ an ninh trong một môi trường số vốn dĩ mở và kết nối, mà còn thúc đẩy sự linh hoạt, thích ứng và khả năng phục hồi nhanh chóng - những yếu tố sống còn cho sự phát triển bền vững trong kỷ nguyên số. Chính vì vậy, thay vì đi theo lối mòn phòng thủ bị động, Việt Nam hoàn toàn có thể ở trong tâm thế chủ động đón đầu xu thế, xây dựng "thể trận an ninh mới" của mình trên nền tảng học thuyết "Năng lực chống chịu an ninh mạng". Để làm

được điều đó, việc nghiên cứu kinh nghiệm quốc tế thông qua ba trụ cột chiến lược dưới đây là một yêu cầu cấp thiết.

Trụ cột đầu tiên là chủ động về công nghệ, lấy công nghệ để trị công nghệ. Mũi nhọn đầu tiên trong việc lấy công nghệ để trị công nghệ chính là phát triển năng lực "chủ động săn lùng mối nguy" (Proactive Threat Hunting). Đây không phải là hoạt động "tuần tra" tự động thông thường, mà là một nghiệp vụ chuyên sâu, đòi hỏi các chuyên gia an ninh mạng trình độ cao. Họ sử dụng các công cụ AI và phân tích dữ liệu lớn không phải để chờ cảnh báo, mà để chủ động tìm kiếm các dấu hiệu bất thường, các hành vi ẩn náu của những nhóm tấn công tinh vi (thường được gọi là APTs - Advanced Persistent Threats) đã xâm nhập và nằm vùng trong hệ thống. Thực tiễn này đã được các quốc gia có nền an ninh mạng phát triển nhất áp dụng. Các cơ quan đầu ngành như Cơ quan An ninh mạng và An ninh Cơ sở hạ tầng Hoa Kỳ (CISA) hay Trung tâm An ninh mạng Quốc gia Anh (NCSC) đều xây dựng các đội "Threat Hunting" chuyên trách, coi đây là tuyến phòng thủ bậc cao để đối phó với các mối đe dọa phức tạp nhất.

Song song với việc "săn lùng", mũi nhọn thứ hai là nâng tầm năng lực "dự báo" bằng các công nghệ phân tích tiên tiến. Thay vì chỉ cảnh báo sớm khi một cuộc tấn công đã bắt đầu, các quốc gia tiên tiến đang sử dụng Trí tuệ nhân tạo và Học máy để phân tích các bộ dữ liệu khổng lồ. Các dữ liệu này bao gồm từ lưu lượng mạng bất thường, thông tin tình báo, cho đến các xu hướng lan truyền thông tin trên mạng xã hội. Mục đích là để nhận diện các quy luật ẩn, từ đó dự báo các vector tấn công mới có thể được khai thác, hoặc các điểm nóng xã hội có nguy cơ bùng phát thành khủng hoảng thông tin, cho phép các cơ quan chức năng hành động trước một bước. Năng lực này được thể hiện rõ nét qua hoạt động của các trung tâm phân tích mối đe dọa thuộc các tập đoàn công nghệ lớn như Microsoft

(Microsoft Threat Intelligence Center) hay Google (Threat Analysis Group). Họ thường xuyên công bố các báo cáo dự báo về chiến dịch tấn công của các nhóm tin tặc do nhà nước bảo trợ, cung cấp những thông tin tình báo chiến lược giúp các chính phủ và doanh nghiệp trên toàn cầu có sự chuẩn bị.

Tuy nhiên, cả hai năng lực "săn lùng" và "dự báo" nói trên phải được xây dựng trên một nền tảng chiến lược: sự tự chủ về công nghệ. Kinh nghiệm quốc tế cho thấy một quốc gia không thể thực sự "chống chịu" nếu các hạ tầng số cốt lõi của họ phụ thuộc hoàn toàn vào chuỗi cung ứng của nước ngoài. Như đã phân tích ở Nguy cơ 4, sự phụ thuộc này tạo ra các "điểm nghẽn chiến lược" có thể bị "vũ khí hóa" bất cứ lúc nào. Để đối phó trực diện với nguy cơ này, Liên minh châu Âu (EU) đang theo đuổi một chiến lược dài hạn về "Chủ quyền số". Chiến lược này được cụ thể hóa qua các sáng kiến quy mô lớn như GAIA-X, một dự án nhằm xây dựng hạ tầng dữ liệu chung cho châu Âu để giảm sự phụ thuộc vào các gã khổng lồ đám mây của Hoa Kỳ, và Đạo luật Chips châu Âu (European Chips Act), một nỗ lực hàng chục tỷ euro để tăng cường năng lực sản xuất và thiết kế bán dẫn ngay tại châu Âu. Điều này cho thấy, đối với các quốc gia tiên tiến, tự chủ công nghệ không phải là làm tất cả, mà là xác định và làm chủ những lĩnh vực nền tảng có ảnh hưởng quyết định đến an ninh và chủ quyền quốc gia.

Trụ cột thứ hai là chủ động về thể chế và pháp lý, kiến tạo một hành lang an toàn.

Nền tảng của một thể trận an ninh mới không chỉ dựa vào năng lực công nghệ để chống lại các mối đe dọa từ bên ngoài, mà còn phải dựa trên một hành lang pháp lý vững chắc để ngăn chặn các nguy cơ gây bất ổn từ bên trong và xây dựng niềm tin xã hội. Kinh nghiệm quốc tế sắc bén nhất trong lĩnh vực này chính là Đạo luật về Trí tuệ nhân tạo (AI Act) của Liên minh châu Âu (EU), được thông qua vào năm 2024. Đây là khung pháp lý toàn diện, mang

tính ràng buộc đầu tiên trên thế giới về AI. Thay vì cấm đoán cực đoan hoặc thả nổi thị trường, EU theo đuổi một triết lý quản trị tinh vi: tiếp cận dựa trên rủi ro (a risk-based approach). Đạo luật này phân loại các ứng dụng AI vào bốn nhóm chính: rủi ro không thể chấp nhận (bị cấm hoàn toàn, ví dụ như các hệ thống "chấm điểm công dân" - social scoring), rủi ro cao, rủi ro hạn chế, và rủi ro tối thiểu. Các hệ thống có rủi ro càng cao thì nghĩa vụ pháp lý càng chặt chẽ. Ví dụ, các hệ thống AI được sử dụng trong hạ tầng trọng yếu, tuyển dụng, cho điểm tín dụng, hay thực thi pháp luật đều bị xếp vào nhóm rủi ro cao và phải tuân thủ các quy định nghiêm ngặt trước khi được đưa ra thị trường.

Để giải quyết trực diện bài toán "hộp đen" và ngăn chặn các thảm họa chính sách như đã xảy ra ở Hà Lan, Đạo luật AI đặt ra các nghĩa vụ bắt buộc đối với các hệ thống rủi ro cao. Các nghĩa vụ này bao gồm yêu cầu về tính minh bạch (người dùng phải biết họ đang tương tác với AI), sự giám sát của con người (hệ thống phải có cơ chế để con người can thiệp hoặc dừng lại bất cứ lúc nào), và chất lượng dữ liệu (dữ liệu dùng để huấn luyện thuật toán phải đủ chất lượng và không chứa các định kiến có thể gây phân biệt đối xử).

Tuy nhiên, mục tiêu của EU không chỉ dừng lại ở việc quản lý rủi ro. Bằng cách tạo ra một tiêu chuẩn pháp lý rõ ràng và đáng tin cậy, họ đang muốn kiến tạo một hệ sinh thái "AI đáng tin cậy" (Trustworthy AI). Họ coi đây là một lợi thế cạnh tranh chiến lược trong cuộc đua công nghệ toàn cầu, giúp thu hút đầu tư, bảo vệ quyền lợi công dân, và quan trọng nhất là thúc đẩy sự chấp nhận của toàn xã hội đối với một công nghệ đầy tiềm năng nhưng cũng không ít rủi ro.

Trụ cột thứ ba, và cũng là nền tảng quyết định, là chủ động về con người. Ở cấp độ toàn xã hội, mục tiêu là xây dựng một "hệ miễn dịch số" quốc gia. Để chống lại các

chiến dịch thông tin giả do AI vận hành, cách hiệu quả nhất là trang bị cho mỗi người dân năng lực tư duy phản biện và kiểm chứng thông tin. Mô hình thành công nhất trên thế giới là của Phần Lan. Vốn là quốc gia có kinh nghiệm lịch sử về chiến tranh thông tin, Phần Lan từ lâu đã được công nhận là quốc gia có sức chống chịu với tin giả tốt nhất châu Âu. Thành công này không đến từ công nghệ, mà từ một chiến lược quốc gia về giáo dục truyền thông và tư duy phản biện, được tích hợp sâu rộng vào hệ thống giáo dục từ cấp tiểu học. Hơn thế nữa, họ còn tiên phong trong việc giáo dục AI cho toàn dân, với các sáng kiến như khóa học online miễn phí "Elements of AI" thu hút hàng triệu người tham gia trên toàn thế giới.

Song song với việc nâng cao sức đề kháng cho toàn xã hội, các quốc gia hàng đầu cũng tập trung xây dựng một lực lượng nòng cốt tinh nhuệ. Thế hệ chuyên gia an ninh mới này không chỉ cần giỏi về công nghệ, mà phải là những người có tư duy liên ngành: sự sắc bén của một nhà khoa học dữ liệu, sự nhạy bén của một nhà tâm lý học hành vi để hiểu và đối phó với các chiến dịch tác động tâm lý, và một nền tảng vững chắc về đạo đức AI. Mô hình đào tạo nhân tài này được thể hiện qua cách tiếp cận của Canada, quốc gia đã lặng lẽ vươn lên thành một "bộ não" của cuộc cách mạng AI. Thay vì chạy đua về ứng dụng thương mại, họ tập trung vào nghiên cứu nền tảng và nuôi dưỡng nhân tài thông qua các viện nghiên cứu danh tiếng thế giới như Mila ở Montreal và Vector Institute ở Toronto. Tương tự, Hàn Quốc nổi tiếng với chương trình "Best of the Best" (BoB) do chính phủ bảo trợ, một "lò luyện" khắc nghiệt để đào tạo ra những hacker mũ trắng và chuyên gia an ninh mạng xuất sắc nhất cho tương lai. Sự kết hợp giữa một xã hội có năng lực miễn dịch số cao và một lực lượng chuyên gia tinh nhuệ sẽ tạo ra tuyến phòng thủ xã hội vững chắc và toàn diện nhất.

Thay cho lời kết: Những câu hỏi định hình tương lai

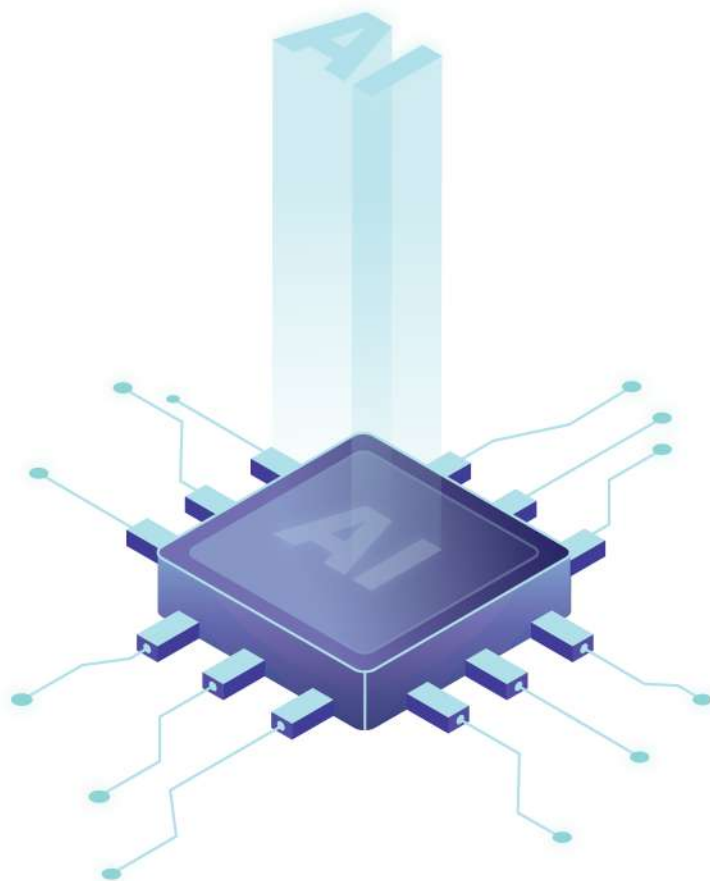
Trí tuệ nhân tạo không chỉ thay đổi bộ mặt công nghệ mà còn đang định hình lại toàn bộ bản chất của an ninh quốc gia. Những phân tích xuyên suốt bài viết đã cho thấy một sự thật không thể đảo ngược: các mối đe dọa thể hệ mới có tốc độ, quy mô và tính chất phức tạp đến mức khiến cho tư duy phòng thủ truyền thống giờ đây đã không còn phù hợp. Chính vì vậy, việc chuyển đổi sang một thể trận an ninh mới không còn là một lựa chọn, mà đã trở thành một yêu cầu mang tính sống còn. Thể trận này đòi hỏi một sự thay đổi toàn diện: từ tư duy phòng thủ bị động sang năng lực chống chịu chủ động; từ việc chỉ dựa vào công nghệ sang việc kiến tạo một hành lang pháp lý an toàn và đáng tin cậy; và quan trọng nhất, là đầu tư vào yếu tố con người - tuyến phòng thủ sâu sắc và bền vững nhất.

Tuy nhiên, việc áp dụng các bài học quốc tế này vào bối cảnh cụ thể của Việt Nam sẽ mở ra những bài toán chiến lược, những sự đánh đổi phức tạp chưa từng có tiền lệ. Đó không còn là bài toán đơn thuần về kỹ thuật, mà là sự lựa chọn con đường chiến lược giữa một mô hình mở, kết nối dựa trên "Năng lực chống chịu" và một mô hình có kiểm soát, tự chủ dựa trên "Chủ quyền không gian mạng". Điều này đặt ra những câu hỏi nền tảng: Làm thế nào để vạch ra lằn ranh đỏ nhằm bảo vệ quyền tự do và riêng tư của công dân khi chúng ta trao cho nhà nước và lực lượng Công an sử dụng những công cụ AI mạnh mẽ? Đó là câu hỏi chiến lược về con đường tự chủ công nghệ của riêng mình, vừa tận dụng sức mạnh toàn cầu, vừa bảo vệ được chủ quyền số trước nguy cơ bị "vũ khí hóa"? Hơn thế nữa, nó đòi hỏi sự thay đổi sâu sắc trong chính lực lượng Công an nhân dân, khi vai trò của người chiến sĩ không chỉ là thực thi, mà còn là người giữ quyền phán quyết cuối cùng trước những đề xuất về an ninh

quốc gia mà AI có thể đưa ra trong vài mili giây? Và khi lựa chọn của cỗ máy đó đang tiến tới lằn ranh của đạo đức, phẩm chất nào của con người - trực giác, kinh nghiệm, bản lĩnh, hay sự thấu cảm - sẽ trở thành điểm tựa cốt lõi và là thước đo trách nhiệm cho sự lựa chọn hành động của chính mình?

Đối mặt với những thách thức mang tầm vóc lịch sử này, vai trò, trách nhiệm và cũng là vinh quang của người chiến sĩ Công an nhân dân trong sứ mệnh giữ vững an ninh quốc gia lại càng được khẳng định và mang một ý nghĩa to lớn hơn bao giờ hết.

Bùi Hữu Sang, LT07



FROM REACTIVE DEFENSE TO PROACTIVELY CONSTRUCTING A NEW SECURITY PARADIGM

The rise of Artificial Intelligence (AI) has brought not only technological breakthroughs but also an entirely new generation of national security threats. As AI can strike a nation from both outside and within, from large-scale disinformation campaigns to policy failures, traditional defensive thinking is no longer sufficient. This article analyzes the core layers of AI-enabled threats and explains the urgency of shifting from reactive defense to a proactive national-security formation, where the objective is not only to respond but to anticipate and take the lead in current affairs.

From early 2021, an unprecedented political shock struck Europe: the entire Dutch cabinet resigned. The cause was neither a cyber-attack nor a conventional political scandal. Instead, it stemmed from an AI algorithm deployed by the tax authority to detect child-care-benefit fraud. Trained on biased data and operating as an inscrutable black box, the system wrongfully accused tens of thousands of innocent families, pushing many to bankruptcy and ruin. This disaster revealed a fundamental truth of the digital era: AI can threaten national security without a single line of malicious code or a large-scale cybersecurity assault.

This political tragedy in the Netherlands is not an isolated case, but a typical example of a completely new vector of attack in the digital era. It demonstrates that threats to national security no longer come solely from the outside - via disinformation campaigns or sophisticated AI-powered cyberattacks. More dangerously, they can also arise from within

- when the incautious deployment of AI in state governance systems itself becomes the source of crises of trust and social instability. To understand this entire complex picture, it is necessary to identify and deeply analyze each of the core risk layers shaping the new situation of security.

Identifying Risk Layers in the AI Era

First, and perhaps most dangerously, is the risk of socio-political destabilization from the misuse of AI as an information "weapon" capable of directly interfering in democratic processes and igniting crises. Generative AI technologies like Deepfake are no longer standalone tools but have become assets in information campaigns operating on an industrial scale. By analyzing big data on the psychology and behavior of specific community groups, these systems can automatically generate 'tailored' counterfeit content, which is optimized for incitement and sowing doubt. Studies published in 2024 by the Stanford Cyber Policy Center (at Stanford University, USA) quantified this power, showing that information campaigns using generative AI not only spread up to 70% faster but also cost only one-tenth of traditional campaigns.

This risk is no longer a mere theory but has been demonstrated through concrete evidence. In recent years, many countries in Asia have fallen victim to large-scale disinformation campaigns, leading to serious political consequences. The 2024 general election in Indonesia is a prime example, where throughout the campaign, a massive number of deepfake videos, images, and audio clips spread rampantly - from "resuscitating" deceased leaders to urge votes for certain parties to

distorting the speeches of candidates. Their impact was highlighted in a survey by the ISEAS-Yusof Ishak Institute (Singapore), which revealed that up to 28.2% of respondents believed a deepfake video of a candidate was real, even though it depicted a fictional event.

However, the real threat lies in the three-dimensional resonance scenario, where AI intervention combines with social instability and the ineffectiveness of the governance system. The political crisis in Bangladesh in mid-2024 demonstrated the frightening speed at which a movement led by the youth, and particularly students, mobilized and spread via social media, could escalate, leading to the collapse of a government in a short time. The danger is exacerbated when governments struggle to manage transnational social media platforms. A prime example is Nepal (September 2025), where the government attempted to counter misinformation by enforcing a blanket ban on social media. This extreme action was, in turn, perceived as muzzling Gen Z, thus igniting a wave of large-scale protests and plunging the country into a more severe political crisis. These examples warn of a potential disaster for national security: when generative AI intervenes to guide, personalize incendiary content, and provide tools for the youth, especially students, to create and disseminate sophisticated fake information (as seen in Indonesia), combined with high-speed social mobilization (as in Bangladesh) and the impotence and extreme reactions of the government (as in Nepal), the risk of triggering riots and political crises becomes uncontrollable.

This creates an asymmetric information competition, where the state's official media channels, which operate under rigorous verification processes, become disadvantaged and drowned in a "flood" of mass-produced fake information. The consequence is the

erosion of public trust in state institutions, deep social polarization, and a direct challenge to the state's capacity to guide and manage information.

Secondly, and perhaps the most structurally transformative change, is the "democratization" of sophisticated offensive capabilities. Whereas complex attacks once required the resources and expertise of intelligence agencies, AI has now lowered the technical and financial barriers, placing similar power in the hands of non-state actors. Reports from cybersecurity firms published in the 2024-2025 period reveal that automated AI-powered malware kits, operating on a Malware-as-a-Service (MaaS) business model, are being sold on hacker forums for as little as a few hundred dollars. A direct consequence, according to the annual "Cost of a Data Breach" report by IBM (USA), is that an AI-optimized ransomware attack can cause a loss of an average of over \$5 million.

However, the risk to national security extends beyond financial loss. Threat analysis reports from leading companies like Microsoft and Dragos (a U.S. company specializing in industrial system security) during the 2024-2025 period have warned that hacker groups are actively developing AI tools capable of automatically discovering and exploiting vulnerabilities in Industrial Control Systems (ICS) – the operational brains of critical infrastructure such as power grids, water treatment plants, and transportation systems. A sufficiently sophisticated AI could "learn" the normal operation of a power grid to calculate the most effective time and method for an attack, causing widespread collapse. It is this escalation from causing economic damage to possessing the ability to paralyze critical national infrastructure that transforms AI-assisted attacks into a direct national security threat.

With low cost and high efficiency, a small criminal group can now use AI to automatically write polymorphic malware

that continuously mutates to evade defense systems; analyze real-time spatial and temporal data to plan a highly precise physical attack; or, more dangerously, deploy coordinated swarms of autonomous drones capable of independent decision-making to overwhelm traditional protection systems. This renders the security landscape more fragmented and unpredictable than ever, as threats no longer emanate solely from strategic rivals but can originate from anywhere.

Third is the risk of public policy failures stemming from algorithmic "black boxes". The scandal in the Netherlands clearly demonstrates how an AI system, particularly deep neural networks, can operate as a "black box." Its decision-making mechanism is so complex that even the engineers who created it cannot fully explain why it reaches a specific conclusion. This risk is not merely theoretical

but has become a painful reality in many countries. The Dutch benefits scandal is a classic lesson in policy implementation failure, where an AI system designed to increase efficiency became an instrument of injustice. Similarly, the A-level grading algorithm incident in the United Kingdom was a failure in policy formulation. According to a BBC analysis in 2020, after exams were cancelled due to the pandemic, the UK government used an AI algorithm to predict grades. However, this algorithm relied too heavily on a school's historical performance, leading to the systematic downgrading of high-achieving students from public schools, sparking widespread protests and forcing the government to scrap the results. These cases affirm an important truth in the digital age: a technical flaw in a state-deployed AI system can rapidly escalate into a significant failure of national governance,



eroding public trust and triggering unforeseeable socio-political repercussions.

Finally, a fundamental risk is the strategic dependency on the global technology supply chain. The capability of any AI system is built on three pillars: data, algorithms, and computing infrastructure. Currently, the global AI ecosystem is dominated by a handful of U.S. technology giants such as NVIDIA, which controls over 80% of the market for AI data center chips, and the three cloud computing behemoths—Amazon Web Services, Microsoft Azure, and Google Cloud—which account for nearly 70% of the global market share. This concentration of power creates strategic "chokepoints," granting a few entities potential control over the digital infrastructure of many nations. This risk has been weaponized in practice through the U.S.-China tech rivalry, where the U.S. has employed embargoes and

restrictions on access to advanced AI chips as a tool of foreign policy to pressure and contain its strategic competitor. This confrontation is not one-sided. In response, China has also begun to play its own cards by imposing export controls on Gallium and Germanium—two critical semiconductor materials—and, notably, on rare earth elements, a resource they virtually monopolize and which is indispensable for manufacturing high-tech chips. This directly threatens the digital sovereignty and the autonomous capacity for national economic and security policy formulation of dependent countries.

Constructing a proactive security formation

The analyses above reveal an undeniable truth: the risks posed by Artificial Intelligence emerge with a speed and scale far exceeding traditional threats. As a result, the conventional



mindset of Reactive Defense has become inadequate and outdated. What is urgently required is a doctrinal shift toward constructing a “new security posture,” as emphasized in the title of this article.

Across the world, two contrasting doctrinal models are now shaping this security architecture. The first model, led by Western nations, is grounded in the concept of Cyber Resilience. According to the U.S. National Institute of Standards and Technology (NIST), this doctrine extends far beyond mere defense; it emphasizes prediction, resistance, and recovery in an inherently open digital environment. Cyber resilience has become a strategic foundation for major powers: the United States institutionalized it through Presidential Policy Directive PPD-21 issued by President Barack Obama in 2013; the United Kingdom and Singapore both place it at the core of their National Cybersecurity Strategies; and the European Union has adopted it in key regulatory frameworks such as the NIS2 Directive and the Digital Operational Resilience Act (DORA).

In contrast, an equally influential counter-model is being defined by China through the doctrine of Cyber Sovereignty, a concept repeatedly emphasized by President Xi Jinping as foundational. Instead of accepting an open cyberspace and building resilience from within, the Chinese doctrine underscores the state’s authority to comprehensively control cyberspace as a new form of “territory.” This model is implemented through robust digital firewalls, strict regulation of data flows, and national technological self-reliance strategies such as Made in China 2025, aimed at minimizing external dependence. It represents a security posture that prioritizes extended-range defense, tight control, and internal consolidation.

Within this context, Vietnam stands at a strategic crossroads filled with both opportunities and challenges. As a rapidly developing digital

economy with an increasingly modern technological infrastructure and a young, dynamic workforce, Vietnam faces all four layers of AI-driven security risks previously discussed. Yet our position as a “latecomer” offers a strategic advantage: we have the opportunity to analyze, learn from, and adapt the successes and failures of pioneering nations in order to define our own path between these two influential models.

China’s cyber sovereignty model, with its emphasis on control and self-reliance, provides valuable lessons in maintaining stability and securing the digital frontier. However, as Vietnam continues to integrate deeply into the global economy, promote innovation, and participate in international technology supply chains, the Western doctrine of cyber resilience offers advantages that align more closely with the nation’s development trajectory. It supplies a framework for safeguarding security within an inherently open and interconnected digital environment, while enhancing flexibility, adaptability, and rapid recovery—crucial elements for sustainable development in the digital era.

Therefore, instead of adhering to passive, defensive approaches, Vietnam can strategically position itself to anticipate global trends and construct its own “new security posture” on the foundation of cyber resilience. To achieve this, studying international experience through the following three strategic pillars is essential.

The first pillar is proactiveness in technology—using technology to govern technology. The foremost spearhead in this approach is the development of “Proactive Threat Hunting” capabilities. This is not ordinary automated “patrolling,” but a specialized professional discipline requiring highly skilled cybersecurity experts. They employ AI tools and large-scale data analytics not to wait for alerts, but to actively search for anomalies and hidden

behaviors of sophisticated threat groups—commonly referred to as Advanced Persistent Threats (APTs)—that have infiltrated and are residing within systems. This practice has been adopted by nations with the most advanced cybersecurity infrastructures. Leading agencies such as the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the UK’s National Cyber Security Centre (NCSC) have established dedicated Threat Hunting teams, treating this as a top-tier defensive line against the most complex threats.

Alongside “hunting,” the second spearhead is elevating “prediction” capabilities through advanced analytical technologies. Instead of merely issuing early warnings once an attack has already begun, advanced nations are now using Artificial Intelligence and Machine Learning to analyze massive datasets. These datasets range from abnormal network traffic and intelligence information to trends in the spread of information on social media. The goal is to identify hidden patterns in order to forecast new attack vectors that may be exploited, or potential social flashpoints likely to escalate into information crises, thereby enabling authorities to act one step ahead. This capability is clearly demonstrated through the work of threat-analysis centers belonging to major technology corporations such as Microsoft (Microsoft Threat Intelligence Center) and Google (Threat Analysis Group). They regularly publish predictive reports on attack campaigns conducted by state-sponsored hacker groups, providing strategic intelligence that helps governments and businesses worldwide prepare themselves.

However, both “hunting” and “prediction” capabilities must be built upon a strategic foundation: technological autonomy. International experience shows that no nation can truly be “resilient” if its core digital infrastructures are entirely dependent on foreign supply chains.

As analyzed in Risk No. 4, such dependence creates “strategic chokepoints” that can be “weaponized” at any time. To confront this risk directly, the European Union (EU) is pursuing a long-term strategy of “Digital Sovereignty.” This strategy is materialized through large-scale initiatives such as GAIA-X, a project aimed at building a shared European data infrastructure to reduce dependence on U.S. cloud giants, and the European Chips Act, a multibillion-euro effort to enhance semiconductor design and manufacturing capabilities within Europe. This demonstrates that for advanced nations, technological autonomy does not mean doing everything, but identifying and mastering foundational domains that have a decisive influence on national security and sovereignty.

The second pillar is proactive institutional and legal capacity, creating a safe governance corridor. The foundation of a new security posture relies not only on technological capability to counter external threats, but also on a solid legal corridor to prevent internal sources of instability and to build societal trust. The sharpest international experience in this field is the European Union’s Artificial Intelligence Act (AI Act), adopted in 2024. This is the world’s first comprehensive and binding legal framework governing AI. Instead of extreme prohibition or laissez-faire market freedom, the EU pursues a sophisticated governance philosophy: a risk-based approach. The Act categorizes AI applications into four groups: unacceptable risk (completely banned, such as “social scoring” systems), high risk, limited risk, and minimal risk. The higher the risk level, the stricter the legal obligations. For example, AI systems used in critical infrastructure, recruitment, credit scoring, or law enforcement are classified as high risk and must comply with stringent requirements before they are placed on the market.

To address the “black box” problem and prevent policy disasters like the one that occurred in the Netherlands, the AI Act imposes mandatory obligations on high-risk systems. These obligations include requirements for transparency (users must know when they are interacting with an AI system), human oversight (systems must include mechanisms that allow humans to intervene or shut them down at any time), and data quality (the data used to train algorithms must be of sufficient quality and free from biases that could lead to discrimination).

However, the EU’s objective goes beyond risk management. By establishing a clear and trustworthy legal standard, it aims to build an ecosystem of “Trustworthy AI.” The EU considers this a strategic competitive advantage in the global technological race, helping attract investment, protect citizens’ rights, and, most importantly, foster society-wide acceptance of a technology full of potential but also significant risks.

The third pillar, and also the decisive foundation, is proactiveness in human capital. At the societal level, the goal is to build a national “digital immune system.” To counter AI-driven disinformation campaigns, the most effective approach is to equip every citizen with critical-thinking skills and the ability to verify information. The most successful model in the world is Finland’s. Having historical experience with information warfare, Finland has long been recognized as the nation with the strongest resilience against fake news in Europe. This success does not come from technology, but from a national strategy of media-literacy education and critical thinking, deeply integrated into the school system from the primary level. Moreover, Finland is a pioneer in nationwide AI education, with initiatives such as the free online course “Elements of AI,” which has attracted millions of participants worldwide.

Alongside strengthening society’s immunity, leading nations also focus on building an elite core workforce. This new generation of security professionals must not only excel in technology but also possess interdisciplinary thinking: the analytical sharpness of a data scientist, the behavioral insight of a psychologist to understand and counter influence operations, and a strong foundation in AI ethics. This talent-development model can be seen in the approach of Canada, a nation that has quietly risen to become an “intellectual hub” of the AI revolution. Instead of racing in commercial applications, Canada focuses on foundational research and nurturing talent through world-renowned institutes such as Mila in Montreal and the Vector Institute in Toronto. Similarly, South Korea is well-known for its government-backed “Best of the Best” (BoB) program, a rigorous “forging ground” for training top white-hat hackers and cybersecurity experts for the future. The combination of a society equipped with strong digital immunity and an elite expert force will create the most solid and comprehensive social defense line.

In place of a conclusion: The questions that will define the future

Artificial intelligence is not merely transforming the technological current circumstances; it is reconfiguring the very nature of national security. The analyses presented throughout this article have revealed an irreversible reality: next-generation threats possess such speed, scale, and complexity that traditional defensive mindsets are no longer adequate. Accordingly, the shift toward a new security architecture is no longer optional but has become an existential imperative. This architecture demands a comprehensive transformation: from passive defense to proactive resilience; from reliance solely on technology to the construction of a

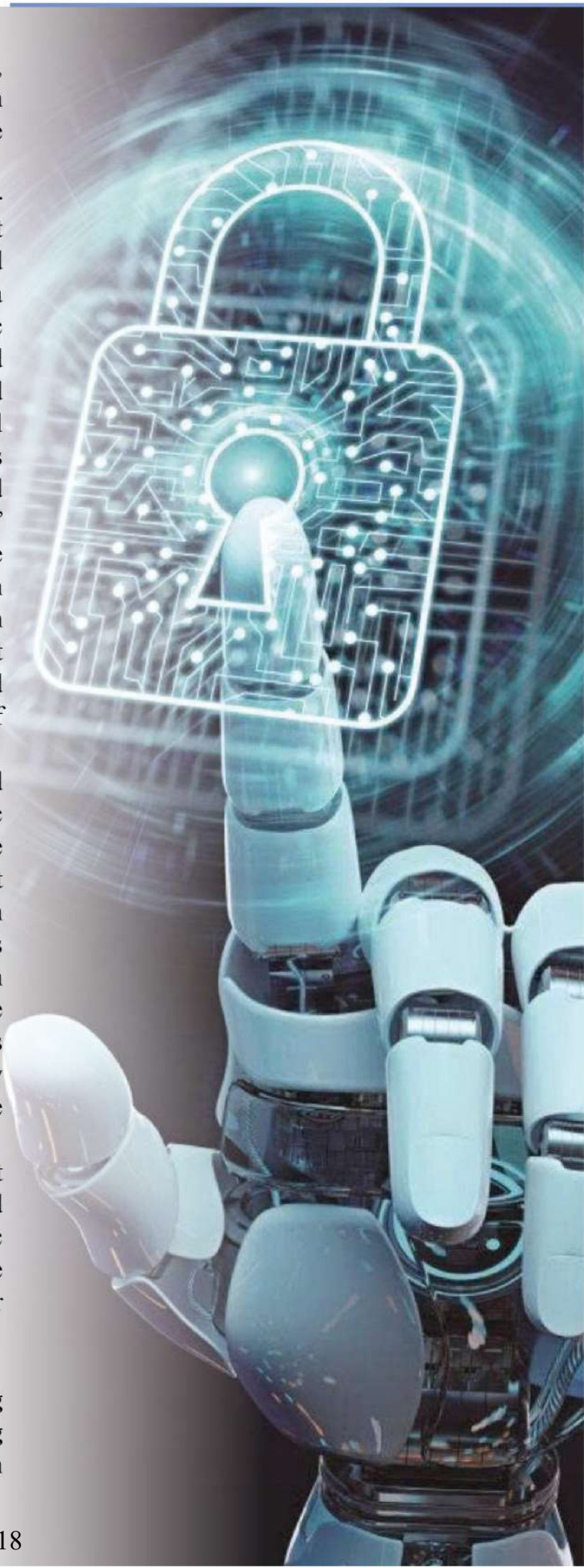
safe and trustworthy legal framework; and, most importantly, to investment in human capital — the deepest and most enduring line of defense.

However, the application of these international lessons to Vietnam’s specific context will give rise to strategic dilemmas and unprecedented trade-offs. This is no longer a purely technical question but a matter of strategic choice between an open, interconnected model premised on “resilience capacity” and a more controlled, autonomous model grounded in “cyberspace sovereignty.” This prompts fundamental inquiries: How can red lines be delineated to safeguard citizens’ freedoms and privacy when the state and the police are entrusted with powerful AI-driven tools? What is the strategic pathway for Vietnam to attain technological autonomy — one that both harnesses global capabilities and preserves digital sovereignty against the risk of “weaponization”?

Furthermore, it necessitates profound transformation within the People’s Public Security forces themselves, for the role of the officer is no longer limited to enforcement but extends to serving as the final arbiter in national security decisions that AI systems may generate within milliseconds. And when the machine’s recommendations approach the boundaries of ethics, which human qualities — intuition, experience, courage, or empathy — will constitute the essential anchor and the moral benchmark guiding one’s decisions?

Confronted with these historically significant challenges, the role, responsibility, and indeed the honor of the officers of the People’s Public Security in safeguarding national security are further underscored and imbued with greater significance than ever before../

Author: Bùi Hữu Sang
Translator: Đỗ Chí Công
Nguyễn Xuân Thành



Thực tế chính trị tại

Ninh Xá

HOẠT ĐỘNG TRI ÂN, GIÁO DỤC TRUYỀN THỐNG CỦA ĐOÀN THANH NIÊN HỌC VIỆN KỸ THUẬT VÀ CÔNG NGHỆ AN NINH TẠI PHƯỜNG NINH XÁ – BẮC NINH

Trong khuôn khổ chương trình công tác Đoàn và phong trào thanh niên năm học 2025, Đoàn Thanh niên Học viện Kỹ thuật và Công nghệ An ninh đã tổ chức đợt hoạt động tri ân và tình nguyện tại phường Ninh Xá, tỉnh Bắc Ninh dành cho học viên khóa D12 và D13. Chương trình do Đoàn Thanh niên Nhà trường phát động và trực tiếp triển khai, với sự phối hợp của chính quyền địa phương và các đơn vị chức năng trên địa bàn. Hoạt động hướng đến mục tiêu giáo dục truyền thống “Uống nước nhớ nguồn”, tăng cường trách nhiệm cộng đồng, đồng thời rèn luyện tác phong, ý thức kỷ luật và tinh thần xung kích của đoàn viên – học viên trong môi trường Công an nhân dân.

Điểm đến đầu tiên của đoàn là Nghĩa trang Liệt sĩ Nguyệt Đức, một địa chỉ đỏ có ý nghĩa lịch sử sâu sắc, nơi an nghỉ của nhiều liệt sĩ đã hy sinh trong các cuộc kháng chiến bảo vệ Tổ quốc. Dưới sự phân công của Đoàn Thanh niên Nhà trường, đoàn học viên D12 và D13 nhanh chóng ổn định

đội hình để thực hiện nghi lễ dâng hương tưởng niệm. Nghi lễ diễn ra trang trọng, thể hiện lòng biết ơn đối với các thế hệ cha anh đã cống hiến trọn đời cho độc lập dân tộc và sự bình yên hôm nay. Ban quản lý nghĩa trang đã giới thiệu thêm về lịch sử hình thành, số lượng liệt sĩ đang an táng và quá trình quy hoạch, chỉnh trang khu vực tưởng niệm tại địa phương.

Sau phần lễ, học viên được triển khai các phần việc tình nguyện như quét dọn khuôn viên nghĩa trang, vệ sinh lối đi, gom lá khô, lau rửa bia mộ và sắp xếp lại các khu vực thờ tự. Từng tổ nhóm phối hợp nhịp nhàng, thực hiện công việc đúng quy định, đảm bảo trang nghiêm và hiệu quả. Các thầy cô trong Ban Chấp hành Đoàn Thanh niên nhà trường trực tiếp theo dõi, hỗ trợ và động viên học viên thực hiện nhiệm vụ. Ban quản lý địa phương đánh giá cao tinh thần tích cực, ý thức tổ chức kỷ luật và thái độ làm việc nghiêm túc của đoàn học viên trong suốt quá trình vệ sinh, chỉnh trang nghĩa trang.



Trong khuôn khổ chương trình công tác Đòan và phong trào thanh niên năm học 2025, Đòan Thanh niên Học viện Kỹ thuật và Công nghệ An ninh đã tổ chức đợt hoạt động tri ân và tình nguyện tại phường Ninh Xá, tỉnh Bắc Ninh dành cho học viên khóa D12 và D13. Chương trình do Đòan Thanh niên Nhà trường phát động và trực tiếp triển khai, với sự phối hợp của chính quyền địa phương và các đơn vị chức năng trên địa bàn. Hoạt động hướng đến mục tiêu giáo dục truyền thống “Uống nước nhớ nguồn”, tăng cường trách nhiệm cộng đồng, đồng thời rèn luyện tác phong, ý thức kỷ luật và tinh thần xung kích của đòan viên – học viên trong môi trường Công an nhân dân.

Điểm đến đầu tiên của đòan là Nghĩa trang Liệt sĩ Nguyệt Đức, một địa chỉ đỏ có ý nghĩa lịch sử sâu sắc, nơi an nghỉ của nhiều liệt sĩ đã hy sinh trong các cuộc kháng chiến bảo vệ Tổ quốc. Dưới sự phân công của Đòan Thanh niên Nhà trường, đòan học viên D12 và D13 nhanh chóng ổn định



Bên cạnh đó, đòan còn tiến hành thăm hỏi, trò chuyện và động viên một số thương binh tại các phòng điều trị. Các thầy cô trong Ban Chấp hành Đòan nhà trường đại diện tặng quà, gửi lời chúc sức khỏe và bày tỏ niềm tri ân sâu sắc. Thông qua hoạt động giao lưu, học viên khóa D12 và D13 được nghe giới thiệu về lịch sử chiến đấu, những khó khăn trong quá trình trị thương và tinh thần kiên cường của các bác thương binh – những nhân chứng sống góp phần giáo dục trực tiếp về giá trị của hòa bình, lòng dũng cảm và trách nhiệm của thế hệ trẻ.

Kết thúc chương trình, Đòan Thanh niên Nhà trường tiến hành họp rút kinh nghiệm, đánh giá chất lượng hoạt động. Qua tổng kết, hoạt động lần này được đánh giá cao về tính tổ chức, tinh thần tham gia của học viên, thái độ nghiêm túc và sự hỗ trợ tích cực của địa phương. Hoạt động đã góp phần thiết thực nâng cao nhận thức chính trị – xã hội của đòan viên, tăng cường sự gắn kết giữa nhà trường với địa phương, đồng thời khẳng định vai trò nòng cốt của Đòan Thanh niên trong công tác giáo dục truyền thống và phát triển phong trào tại học viện.

Chương trình tình nguyện và tri ân tại Nghĩa trang Liệt sĩ Nguyệt Đức và Trung tâm Điều dưỡng Thương binh Thuận Thành (phường Ninh Xá) được xem là một trong những điểm nhấn quan trọng trong hoạt động của Đòan Thanh niên Học viện Kỹ thuật và Công nghệ An ninh năm 2025. Không chỉ mang ý nghĩa xã hội thiết thực, hoạt động còn tạo môi trường rèn luyện phẩm chất, bản lĩnh và nhân cách cho học viên khóa D12 và D13 – những chiến sĩ công an tương lai, tiếp tục phát huy truyền thống “Vì nước quên thân, vì dân phục vụ”.

Fieldtrip

Ninh Xá

COMMEMORATION AND TRADITIONAL EDUCATION PROGRAM OF THE YOUTH UNION OF THE ACADEMY OF SECURITY ENGINEERING AND TECHNOLOGY

As part of the Youth Union's work plan and youth activities for the academic year 2025, the Youth Union of the Academy of Security Engineering and Technology organized a gratitude and volunteer program in Ninh Xá Ward, Bắc Ninh Province, for students of cohorts D12 and D13. The program was launched and directly carried out by the Academy's Youth Union, in coordination with local authorities and relevant units in the area. The activity aimed to promote the tradition of "When drinking water, remember its source," foster a sense of social responsibility, and cultivate professional discipline, proper working manners, and the proactive spirit of Youth Union members and students within the environment of the People's Public Security.

The first destination of the delegation was the Nguyệt Đức Martyrs' Cemetery, a site of profound historical significance and the resting place of many fallen heroes who sacrificed their lives in

in the resistance wars for national independence and peace. Under the direction of the Academy's Youth Union, students of cohorts D12 and D13 quickly assembled in formation to conduct the incense-offering ceremony. The ceremony was carried out solemnly, expressing deep gratitude to previous generations who devoted their lives to the nation's freedom and today's security. The cemetery management board introduced the history of the site, the number of martyrs buried there, and the ongoing planning and restoration efforts conducted by the local authorities.

After the ceremonial activities, the students undertook volunteer tasks such as cleaning the cemetery grounds, tidying pathways, collecting fallen leaves, washing tombstones, and arranging the worship areas. Each group worked in a coordinated and disciplined manner, ensuring both respectfulness and effectiveness. Members of the Academy's Youth Union Executive Committee were present to



supervise, support, and encourage the students throughout the activities. The local management board highly appreciated the students' positive spirit, sense of discipline, and serious attitude during all tasks related to cleaning and maintaining the cemetery.

In the afternoon of the same day, the delegation proceeded to the Thuận Thành Rehabilitation Center for Wounded Soldiers, also located in Ninh Xá Ward, Bắc Ninh Province. The Center is responsible for providing care and medical rehabilitation for



severely injured and seriously ill veterans—those who continue to bear the long-term physical consequences of war and require extended treatment and daily support at the facility. This was an important destination within the program, allowing students to gain a deeper understanding of the silent sacrifices made by wounded veterans, while fostering compassion and a sense of responsibility among young members of the People's Public Security. In the afternoon of the same day, the delegation proceeded to the



the Thuận Thành Rehabilitation Center for Wounded Soldiers, also located in Ninh Xá Ward, Bắc Ninh Province. The Center is responsible for providing care and medical rehabilitation for severely injured and seriously ill veterans—those who continue to bear the long-term physical consequences of war and require extended treatment and daily support at the facility. This was an important destination within the program, allowing students to gain a deeper understanding of the silent sacrifices made by wounded veterans, while

fostering compassion and a sense of responsibility among young members of the People's Public Security

In addition, the delegation visited, conversed with, and encouraged several wounded veterans in the treatment wards. On behalf of the Academy, members of the Youth Union Executive Committee presented gifts, offered well-wishes, and expressed profound gratitude for their sacrifices. Through these interactions, students of cohorts D12 and D13 learned about the veterans' combat histories, the hardships they endured during treatment, and their remarkable resilience—living witnesses whose stories provide meaningful and direct lessons on the value of peace, courage, and the responsibilities of the younger generation.

At the conclusion of the program, the Academy's Youth Union held a review meeting to assess the quality and effectiveness of the activities. According to the evaluation, this volunteer and commemoration program was highly appreciated for its organizational quality, the active participation of the students, their disciplined attitude, and the strong support provided by the local authorities. The activity made a practical contribution to enhancing the socio-political awareness of Youth Union members, strengthening the bond between the Academy and the local community, and reaffirming the core role of the Youth Union in traditional education and the development of youth movements at the Academy.

The volunteer and commemoration program at the Nguyệt Đức Martyrs' Cemetery and the Thuận Thành Rehabilitation Center for Wounded Soldiers (Ninh Xá Ward) is regarded as one of the key highlights of the Youth Union's activities at the Academy of Security Engineering and Technology in 2025. Beyond its meaningful social impact, the program also provided an environment for students of cohorts D12 and D13 to develop personal qualities, resilience, and moral character—preparing them to become future officers of the People's Public Security who will continue upholding the tradition of “Sacrificing oneself for the nation; serving the people wholeheartedly.”



Đại úy NGUYỄN QUỲNH TRANG

TẤM GƯƠNG GIẢNG VIÊN TIÊU BIỂU CỦA HỌC VIỆN KỸ THUẬT VÀ CÔNG NGHỆ AN NINH



Trong những năm qua, Học viện Kỹ thuật và Công nghệ an ninh không ngừng khẳng định vị thế trong đào tạo nguồn nhân lực chất lượng cao về công nghệ thông tin, an toàn thông tin và kỹ thuật điện tử viễn thông, đóng góp quan trọng vào công tác phòng chống tội phạm công nghệ cao của lực lượng Công an nhân dân. Góp phần làm nên những thành tựu ấy là sự đóng góp thầm lặng, tâm huyết của đội ngũ cán bộ, giảng viên – những người luôn tận tụy với sự nghiệp "trồng người". Trong số đó, thạc sĩ, đại úy Nguyễn Quỳnh Trang, giảng viên Khoa Khoa học cơ bản và Ngoại ngữ, là một tấm gương tiêu biểu về tinh thần trách nhiệm, năng lực chuyên môn và đổi mới sáng tạo. Cô là tấm gương đẹp cho thế hệ giảng viên trẻ, vừa "hồng" vừa "chuyên," sẵn sàng vượt qua mọi khó khăn để hoàn thành xuất sắc nhiệm vụ được giao.

Sinh ra và lớn lên trong một gia đình truyền thống hiếu học, cô Nguyễn Quỳnh Trang sớm nuôi dưỡng niềm đam mê với ngôn ngữ và khát vọng được đứng trên bục giảng. Sau khi tốt nghiệp chuyên ngành sư phạm tiếng Anh tại Trường Đại học Ngoại ngữ - Đại học Quốc gia Hà Nội- một trong những cái nôi đào tạo chuyên ngành ngoại ngữ hàng đầu của đất nước, cô đã nộp đơn ứng tuyển làm giảng viên vào Học viện Kỹ thuật và Công nghệ an ninh..

Mong muốn của cô không chỉ dừng lại ở việc truyền đạt kiến thức, mà còn là được cống hiến sức trẻ và chuyên môn của mình để nâng cao năng lực tiếng Anh cho học viên trường CAND, giúp họ đủ tự tin làm chủ công nghệ, tham gia các chương trình hợp tác quốc tế. Với nền tảng học thuật vững chắc, sự cẩn mẫn trong nghiên cứu và phương pháp làm việc nghiêm túc, khoa học, cô Nguyễn Quỳnh Trang đã nhanh chóng khẳng định bản lĩnh của một giảng viên trẻ, chuyên môn vững vàng, có tư duy đổi mới và khát khao sáng tạo.

Giảng viên Nguyễn Quỳnh Trang luôn tâm niệm rằng, trong bối cảnh toàn cầu hóa, tiếng Anh không chỉ là một môn học mà còn là công cụ hỗ trợ và nâng cao năng lực chuyên môn của người cán bộ kỹ thuật. Vì vậy, cô luôn lấy người học làm trung tâm, chú trọng rèn luyện cho học viên năng lực tư duy độc lập và kỹ năng thực hành ngoại ngữ gắn liền mật thiết với nghiệp vụ chuyên ngành. Phương pháp giảng dạy của cô là sự kết hợp linh hoạt, khoa học giữa lý thuyết và



Đại úy Nguyễn Quỳnh Trang đạt giải Ba tại Hội thi giảng viên dạy giỏi cấp Bộ, năm học 2024-2025

thực hành ứng dụng. Cô không ngừng truyền tải những kiến thức bổ ích về tiếng Anh giao tiếp, tiếng Anh chuyên ngành cho học viên mà còn biến những tiết học căng thẳng thành các buổi thảo luận sôi nổi, tích cực giúp học viên hứng thú hơn với bộ môn tiếng Anh – để giao tiếp, để nghiên cứu, để phục vụ nhiệm vụ an ninh trong kỷ nguyên công nghệ số.

Đặc biệt, cô Trang là một trong những giảng viên tiên phong ứng dụng công nghệ trí tuệ nhân tạo vào giảng dạy, phát triển các tài liệu số để hỗ trợ học viên tự học, tự nghiên cứu sau giờ lên lớp. Sự đổi mới này góp phần nâng cao đáng kể hiệu quả đào tạo, đáp ứng nhu cầu của một Học viện Kỹ thuật hàng đầu. Một thành tích ấn tượng vào tháng 9 năm 2025, cô đạt giải Ba trong Hội thi giáo viên dạy giỏi cấp Bộ, ghi dấu ấn bằng phong thái tự tin, kiến thức sâu rộng và khả năng sư phạm tinh tế – thành tích không chỉ của riêng cô, mà đó còn là niềm tự hào của tập thể Khoa và toàn Học viện.

Không chỉ giỏi chuyên môn, cô Quỳnh Trang còn là gương mặt tiêu biểu trong mọi hoạt động phong trào Đoàn – Hội của Học viện. Cô là ủy viên Ban Chấp hành Đoàn trường, luôn nhiệt huyết, sáng tạo trong tổ chức các phong trào và hoạt động ngoại khóa. Ở vai trò này, cô là cầu nối giữa giảng viên và học viên, là người khơi dậy sức trẻ, truyền lửa cho những hoạt động của Đoàn, đặc biệt trong Câu lạc bộ Tiếng Anh – nơi cô cùng học viên tạo nên môi trường học tập cởi mở, sáng tạo và tràn đầy năng lượng sau những buổi học căng thẳng.

Dưới sự hướng dẫn chỉ dạy của cô Trang, tôi đã học hỏi ở cô rất nhiều về lòng nhiệt tình, tinh thần trách nhiệm, chăm chỉ học hành. Có những lúc áp lực do học tập căng thẳng khiến tôi mệt mỏi nhưng nghĩ tới cô Trang tôi lại thấy mình như được tiếp thêm sức mạnh để làm việc tốt hơn. Sự lan tỏa tích cực đó không chỉ dừng lại ở tinh thần. Cô Trang thường xuyên tổ chức các buổi chia sẻ kinh nghiệm về cách làm chủ 4 kỹ năng Tiếng Anh: nghe, nói, đọc, viết và những kinh nghiệm trong các công tác Đoàn thể. Sự chủ động, sự chuyên nghiệp và cách cô cân bằng giữa công tác chuyên môn và hoạt động Đoàn đã trở thành nguồn cảm hứng lớn, giúp học viên không ngừng nâng cao chất lượng học tập và đạt được hiệu quả cao nhất. Cô chính là hạt nhân lan tỏa văn hóa làm việc chuyên nghiệp, tận tâm vì sự nghiệp giáo dục trong lòng lực lượng CAND.

Thành tích và sự cống hiến của cô Nguyễn Quỳnh Trang là minh chứng rõ ràng nhất cho tinh thần nỗ lực không ngừng, dám nghĩ dám làm và hết lòng vì học viên. Cô chính là tấm gương sáng, là niềm tự hào của Học viện Kỹ thuật và Công nghệ an ninh, góp phần không nhỏ vào việc xây dựng lực lượng cán bộ kỹ thuật, nghiệp vụ tinh nhuệ, đáp ứng yêu cầu bảo vệ an ninh quốc gia trong tình hình mới.

Captain NGUYEN QUYNH TRANG

AN EXEMPLARY LECTURER OF THE ACADEMY OF SECURITY ENGINEERING AND TECHNOLOGY



In recent years, the Academy of Security Engineering and Technology has consistently affirmed its position as a leading institution in training high-quality human resources in IT, cybersecurity, and electronics and telecommunications engineering, which directly bolsters the People's Public Security Forces in their mission against cybercrime. Contributing to these achievements is the silent yet dedicated effort of the Academy's officers and lecturers—individuals who remain devoted to the mission of education, shaping the future of the People's Public Security Forces (PPSF). Among them, Captain Nguyen Quynh Trang, M.A., a lecturer at the Department of Basic Sciences and Foreign Languages, stands out as a shining role model of responsibility, professional competence, and pedagogical innovation. She embodies the model of young lecturers who are both “vibrant” and “talented,” always ready to overcome challenges to excel in every assigned task.

Born into a family with a tradition of reverence for learning, Ms. Nguyen Quynh Trang nurtured a passion for linguistics and found her calling to the classroom. After graduating in English Language Teacher Education from the University of Languages and International Studies – Vietnam National University, Hanoi – one of the country's top institutions for foreign-language training, she applied to become a lecturer at the Academy of Security Engineering and Technology.

Her desire does not stop at merely imparting knowledge, she also wishes to devote her youth and expertise to improving the foreign-language capacity of cadets, enabling them to confidently master technology and participate effectively in international cooperation programmes. With a solid academic foundation, diligence in research, and a serious, scientific working method, Ms. Nguyen Quynh Trang quickly proved herself as a young lecturer with strong professional qualifications, an innovative mindset, and a passion for creativity.

Captain Nguyen Quynh Trang firmly believes that in an era of globalization, English is not only an academic subject but also an essential tool for security-engineering officers in their professional duties. For that reason, she always adopts a learner-centred



Captain Nguyễn Quỳnh Trang won the Third Prize at the Ministry of Public Security's excellent teaching competition for the academic year 2024–2025

approach, focuses on developing independent thinking and practical language-in-use skills closely aligned with the cadets' major. Her teaching methodology is a flexible and systematic combination of theoretical instruction and applied practice. She continuously updates her lessons with relevant knowledge in general English, communicative English, and technical English, turning what could be stress lessons into engaging discussions and dynamic learning experiences. She helps students approach English as a living tool—for communication, research, and fulfilling professional responsibilities in the digital era.

Notably, Ms. Trang is among the pioneer lecturers applying artificial intelligence technologies in teaching, developing digital learning resources to support students' self-study and research beyond classroom hours. This breath of fresh air has significantly enhanced training effectiveness, meeting the demands of a leading technical academy. A remarkable milestone was achieved in September 2025, when she won the Third Prize at the Ministry of Public Security's excellent teaching competition for the academic year 2024–2025, earning recognition for her confident presentation, extensive knowledge, and refined pedagogical skill—a success that brought pride not only to herself but also to her Faculty and the entire Academy.

In addition to her professional excellence, Ms. Quynh Trang, M.A is an active and exemplary figure in Youth Union activities. She serves as a member of the Academy's Youth Union Executive Committee, consistently demonstrating enthusiasm and creativity in organizing movements and extracurricular activities. In this role, she acts as a bridge between lecturers and students, inspiring youthful energy and fostering dynamic engagement—especially within the English Club, where she works with students to build an open, creative, and highly energetic learning environment after stressful lessons

Under Ms. Trang's guidance, I have learned much from her about enthusiasm, responsibility, and diligence in studying. There were times when the heavy workload made me feel exhausted, but thinking of Ms. Trang gave me motivation to keep striving. That positive influence extends far beyond morale. Ms. Trang regularly organizes experience sharing sessions on how to master all four English skills: listening, speaking, reading, writing, and experiences in Union activities. Her proactiveness, professionalism, and ability to balance academic duties with social activities have become a great source of inspiration, helping us continually improve work quality and achieve the highest effectiveness. Ms. Nguyen Quynh Trang is truly a driving force, spreading a culture of professionalism and dedication to educational excellence within the PPSF education system. The achievements and contributions of Captain Nguyen Quynh Trang, M.A., serve as a vivid testament to her constant effort, courage to innovate, and wholehearted devotion to her learners. She is among the role models and a source of pride for the Academy of Security Engineering and Technology, significantly contributing to the development of a highly skilled, elite technical force capable of meeting the demands of safeguarding national security in the new era.

HÀNH TRÌNH TỪ TRÁI TIM:

ĐẤU ẮN TÌNH NGUYỆN CỦA TUỔI TRẺ HỌC VIỆN KỸ THUẬT VÀ CÔNG NGHỆ AN NINH

Trong dòng chảy mạnh mẽ của phong trào “Vì nhân dân phục vụ”, tuổi trẻ Học viện Kỹ thuật và Công nghệ an ninh (T07) đã và đang viết nên những câu chuyện đẹp bằng hành động giản dị mà giàu ý nghĩa. Từ những điểm trường vùng cao Yên Bái, những giọt máu hồng đầy nghị lực, đến những ngày tiếp sức mùa thi trong mưa gió hay những giờ phút lặng lòng trước anh linh các anh hùng liệt sĩ... tất cả đã tạo nên bản sắc riêng: bản lĩnh - kỷ luật - nhân văn - trách nhiệm của thế hệ học viên Công an nhân dân.

Lan tỏa yêu thương giữa mùa đông Tây Bắc



Ngày 17/01/2025, chương trình “Tình nguyện mùa Đông 2024 – Xuân tình nguyện 2025” đã đưa bước chân đoàn công tác Nhà trường lên với xã Phúc Sơn, thị xã Nghĩa Lộ, Yên Bái.

Dưới sự dẫn đoàn của Đại tá, TS Nguyễn Mạnh Cường- Phó Hiệu trưởng Nhà trường, đoàn đã trao:

- 30 suất học bổng (15 triệu đồng) cho học sinh tiểu học;
 - 180 suất quà cho hộ nghèo (90 triệu đồng);
 - 4 tấn xi măng hỗ trợ bê tông hóa đường vào Trường Mầm non;
 - 200 áo khoác ấm cho học sinh;
 - 90 bộ áo dài tặng phụ nữ địa phương;
- Nhiều phần quà ý nghĩa khác, tổng giá trị khoảng 130 triệu đồng.

Trong cái lạnh vùng cao, hơi ấm từ màu áo xanh tình nguyện đã mang đến niềm vui, sự động viên thiết thực cho người dân. Đây cũng là bài học sống động về lòng nhân ái, tinh thần sẻ chia đối với mỗi học viên CAND.

Giọt máu hồng - trao hy vọng, lan tỏa sự sống

Sáng 15/4/2025, T07 phối hợp Bệnh viện 19/8 tổ chức hiến máu tình nguyện với chủ đề “Giọt máu hồng, trao hy vọng”. Gần 300 cán bộ, giảng viên, học viên tham dự; 235 đơn vị máu được tiếp nhận - con số biết nói thể hiện tinh thần trách nhiệm và tấm lòng nhân văn của tuổi trẻ CAND. Phát biểu tại chương trình, Đại tá Vũ Việt Anh, Phó Hiệu trưởng, khẳng định: “*Hiến máu là nghĩa cử cao đẹp, là biểu hiện tinh thần ‘vì Nhân dân phục vụ’ của người chiến sĩ Công an nhân dân.*”



“Nâng bước em tới trường” – nâng niu những ước mơ nhỏ

Ngày 13/5/2025, Đoàn Thanh niên Nhà trường phối hợp Đoàn Thanh niên phường Hồ (Thuận Thành, Bắc Ninh) trao quà cho 03 em học sinh có hoàn cảnh khó khăn. Những lời thăm hỏi, động viên chân thành; những phần quà nhỏ bé nhưng chan chứa yêu thương đã tiếp thêm nghị lực để các em tiếp tục nỗ lực, nuôi dưỡng ước mơ trở thành công dân có ích cho xã hội. Đó cũng là cách tuổi trẻ T07 gieo những “hạt mầm” tốt đẹp trong lòng cộng đồng.



Tiếp sức mùa thi – ánh sáng giữa những ngày mưa

Ngày 21–22/6/2025, giữa cơn mưa lớn bất chợt tại Bắc Ninh, các học viên T07 vẫn ướt đầm áo, tay cầm ô nhỏ, sẵn sàng hướng dẫn gần 200 thí sinh đến làm thủ tục dự thi văn bằng 2 khóa 4. Ánh mắt thân thiện, lời nói nhẹ nhàng, từng bước chân nhanh nhẹn của các chiến sĩ trẻ đã xua tan căng thẳng, tạo nên điểm tựa tinh thần vững chắc cho thí sinh.

Một ngôi trường sáng lên giữa trời mưa – không phải bằng ánh đèn, mà bằng trái tim của những người đang sống và học tập tại nơi đây.



Tiếp sức mùa thi – Kỳ thi đánh giá năng lực Bộ Công an 2025

Ngày 05–06/7/2025, hàng trăm đoàn viên, học viên T07 được huy động tại các vị trí trọng điểm: cổng trường, phòng thi, phân luồng giao thông, hậu cần.

Với phương châm “Mỗi học viên là một tình nguyện viên gương mẫu”, lực lượng tình nguyện đã góp phần đảm bảo kỳ thi diễn ra an toàn – nghiêm túc – đúng quy định, để hàng nghìn thí sinh thêm tự tin trên hành trình trở thành chiến sĩ Công an nhân dân tương lai.

Hành trình cống hiến – hành trình trưởng thành
Nhìn lại chuỗi hoạt động trong năm 2024–2025, có thể thấy rõ: Mỗi chương trình tình nguyện không chỉ mang lại giá trị cho cộng đồng, mà còn là hành trình rèn luyện bản lĩnh, kỷ luật và nhân văn cho thế hệ học viên CAND. T07 hôm nay không chỉ là nơi đào tạo đơn thuần, mà còn là cái nôi nuôi dưỡng: Trái tim giàu tình thương; Khối óc bản lĩnh; Ý thức trách nhiệm với Nhân dân; Phẩm chất người chiến sĩ Công an nhân dân trong thời đại mới.

“Ngày Chủ nhật xanh” – dấu ấn công dân trẻ vì môi trường

Dù thời tiết mưa gió, trong ngày 22/6/2025, Đoàn Thanh niên T07 vẫn đồng loạt ra quân thực hiện “Ngày Chủ nhật xanh”: thu gom rác, phát quang cây cỏ, chỉnh trang cảnh quan. Tinh thần cống hiến lặng lẽ nhưng bền bỉ ấy đã lan tỏa thông điệp đẹp: “Sống xanh - sống trách nhiệm - sống vì cộng đồng.”

Uống nước nhớ nguồn Ngọn lửa tri ân luôn thấp sáng



Chung tay khắc phục hậu quả bão lũ – khi Nhân dân cần, T07 có mặt



Nhân 78 năm Ngày Thương binh – Liệt sĩ (27/7/1947 – 27/7/2025), Đoàn Thanh niên và Hội Phụ nữ Nhà trường đã tổ chức:

- Dọn dẹp môi trường tại Trung tâm Điều dưỡng thương binh Thuận Thành và Nghĩa trang liệt sĩ.

- Tham gia Lễ thấp nến tri ân tại hai nghĩa trang liệt sĩ ở Thuận Thành và Trạm Lộ.

Những ngọn nến lung linh, những phút giây lặng trang nghiêm đã nhắc nhở mỗi học viên về trách nhiệm kế thừa truyền thống “đền ơn đáp nghĩa”, sống xứng đáng với sự hy sinh của các thế hệ đi trước.

Trước thiệt hại nặng nề do bão số 10 và 11, đoàn cán bộ – học viên do Đại tá, TS Nguyễn Mạnh Cường làm Trưởng đoàn đã đến hỗ trợ Nhân dân xã Hợp Thịnh và xã Hoàng Vân (Bắc Ninh):

- Dọn vệ sinh môi trường, thu dọn rác, tường bao đổ sập;
- Hỗ trợ các gia đình neo đơn, thương binh, liệt sĩ;
- Thăm hỏi và trao quà động viên gia đình các đồng chí hy sinh khi làm nhiệm vụ.

Những chiếc áo xanh tình nguyện đã thấm dầm mồ hôi và nước mưa, nhưng sáng lên tinh thần “Vì Nhân dân phục vụ” – sẵn sàng đối mặt khó khăn để chung tay cùng cộng đồng.

TỪ NHỮNG VIỆC LÀM NHỎ – TẠO NÊN SỨC MẠNH LỚN

Hành trình tình nguyện của tuổi trẻ Học viện Kỹ thuật và Công nghệ an ninh trong thời gian qua đã khẳng định: Nơi nào Nhân dân cần, nơi ấy có bước chân của học viên T07. Với sức trẻ, trí tuệ và lòng nhiệt thành, các chiến sĩ trẻ vẫn đang tiếp tục viết tiếp những trang đẹp đẽ của lực lượng CAND – những trang viết bằng hành động, trách nhiệm và trái tim.

JOURNEY FROM THE HEART:

THE MARK IN VOLUNTEER SPIRIT OF YOUTH AT THE ACADEMY OF SECURITY ENGINEERING AND TECHNOLOGY

In the powerful flow of the movement “Serving the People,” the youth of the Academy of Security Engineering and Technology (T07) have been and are continuing to write beautiful stories through simple yet meaningful actions. From remote schools in Yên Bái, courageous blood donations, to supporting the entrance exam on a rainy day or solemn moments honoring fallen heroes—these all reflect the unique identity of Public Security students: bravery – discipline – humanity – responsibility.

Spreading love in the Northwestern Winter



On January 17, 2025, the program “Winter Volunteer 2024 – Spring of Volunteering 2025” brought the school’s delegation to Phuc Son commune, Nghia Lo town, Yen Bai province.

Led by Colonel, Dr. Nguyen Manh Cuong – Vice President of the Academy, the delegation delivered:

- 30 scholarships (worth 15 million VND) for primary school students;
- 180 gift packages for poor households (worth 90 million VND);
- 4 tons of cement to help pave the road to kindergartens;
- 200 warm jackets for students;
- 90 traditional dresses (ao dai) for local women;
- Many other meaningful gifts, totaling about 130 million VND

In the cold of the highlands, the warmth from the blue volunteer shirts brought joy and practical encouragement to the local people. This also served as a vivid lesson in compassion and sharing spirit for every Public Security student.

The Red Blood Drop - giving Hope, spreading Life

On the morning of April 15, 2025, T07 collaborated with the 19/8 Hospital to organize a voluntary blood donation program titled "The Red Blood Drop, Giving Hope." Nearly 300 officers, lecturers, and students participated; 235 units of blood were collected – a telling number demonstrating the responsible spirit and humane heart of the Public Security youth. Speaking at the event, Colonel Vu Viet Anh, Vice President of the Academy, affirmed: “Blood donation is a noble gesture, a manifestation of the ‘Serving the People’ spirit of Public Security soldiers”



“Lifting Young Steps to school”- Nurturing Little Dreams

On May 13, 2025, the T07 Youth Union, in coordination with the Ho Town’s Youth Union (Thuan Thanh, Bac Ninh), presented gifts to 3 disadvantaged students. Sincere inquiries and encouragement, together with small but love-filled gifts gave the children more strength to keep striving and nurturing their dreams of becoming useful citizens for society. This was also how T07's youth planted beautiful "seeds" of goodness in the community.



Exam Support – A Light in the Rain

On June 21–22, 2025, amid sudden heavy rains in Bac Ninh, T07 students—soaked and holding umbrellas—guided nearly 200 candidates through registration procedures for the 4th second-degree entrance exam. Friendly eyes, gentle words, and swift steps of the young officers eased the tension, becoming a solid source of support for the candidates.

A school shining in the rain—not with lights, but with the hearts of those living and studying there.



Exam Support – Ministry of Public Security’s 2025 Competency Assessment

On July 5–6, 2025, hundreds of T07 students were mobilized to key positions: school gates, exam rooms, traffic coordination, logistics.

With the motto “Every student is a model volunteer,” the team helped ensure the exam was safe, serious, and in accordance with regulations, helping thousands of candidates feel more confident on their way to becoming future People's Public Security officers.

A Journey of Dedication – A Journey of Growth

Looking back at the series of activities in 2024-2025, it is clear to see: Each volunteer program not only brings value to the community but is also a journey to cultivate bravery, discipline, and humanity for a generation of Public Security students.

T07 today is not merely a training institution, but also a cradle that nurtures: A heart full of love; A courageous mind; A sense of responsibility towards the people; The qualities of a People's Public Security soldier in the new era.

"Green Sunday" – The Mark of Young Citizens for the Environment

Despite the rainy weather on June 22, 2025, T07 Youth Union launched the "Green Sunday" campaign: collecting trash, clearing vegetation, and beautifying the campus.

This quiet yet persistent spirit of service spread a powerful message: "Live green – live responsibly – live for the community."

When drinking water, remember its source The flame of gratitude always burns bright



On the 78th anniversary of War Invalids and Martyrs Day (July 27, 1947 – July 27, 2025), the Academy's Youth Union and Women's Union organized:

- Environmental cleanup at Thuan Thanh War Invalids Nursing Center and local cemeteries
- Participation in candlelight tribute ceremonies at two military cemeteries in Thuan Thanh and Tram Lo

The flickering candles and solemn moments reminded every student of their duty to uphold the tradition of "repaying gratitude" and to live worthy of the sacrifices of previous generations.

Joining hands to overcome storm damage – When the people need, T07 responds



In response to severe damage caused by Storms No. 10 and 11, a delegation of officers and students led by Colonel, Dr. Nguyen Manh Cuong came to support the people of Hop Thinh and Hoang Van communes (Bac Ninh):

- Cleaning the environment, removing debris and collapsed walls
- Assisting lonely elderly, war invalids, and martyr families;
- Visiting and bringing gifts to families of officers who lost their lives while on duty.

The blue volunteer shirts were soaked with sweat and rain, yet they shone with the spirit of "Serving the People" – ready to face hardship to join hands with the community.

FROM SMALL ACTS – COMES GREAT STRENGTH

The volunteer journey of the Academy of Security Engineering and Technology's youth in recent times has affirmed: Wherever the people are in need, there the footsteps of T07 students will be.

With youth, intellect and passion, the young officers continue to write beautiful pages in the story of People's Public Security force – pages written with action, responsibility and heart.

Em là chiến sỹ Công an

"Hôm nay tạm biệt quê hương
Em về học dưới mái trường thân yêu
Em chăm chỉ học sớm chiều
Luyện rèn vất vả vượt nhiều gian lao
Chiến trường bớt đổ máu đào
Mồ hôi chẳng quản đổ thao trường nhiều
Có thầy cô hết mực thương yêu
Tận tâm dìu dắt vượt bao điều khó khăn
Rèn em từ mỗi bước chân
Tinh thần võ thuật – hàng quân thẳng đều
Mồ hôi thầy đổ đã nhiều
Thao trường bao buổi bấy nhiêu thân tình
Chúng em như một gia đình
Bên nhau bè bạn thân tình anh em
Ước mơ chiến sĩ Công an
Vì dân, vì nước gian nan chẳng từ
Sáu điều Bác dạy năm xưa
Nguyện xin ghi tạc nắng mưa luyện rèn
Ở trường học tập chăm ngoan
Em là chiến sĩ Công an mai này!"

-L.T.H-

02 Bài thơ sau, tác giả muốn dành đến tất cả các bạn, các em tân sinh viên, khi bước đến môi trường học tập mới, phải xa gia đình, xa quê hương, những nơi thân thương quen thuộc, tạm gác lại những tháng ngày miệt mài đèn bút và chuẩn bị hành trang để đi huấn luyện tại K02. Bài thơ này vừa là nhật ký của tác giả vừa là lời để các em nhắn nhủ đến gia đình, chúc các em luôn vững bước trên hành trình mà bản thân đã chọn

Thư gửi mẹ

Từ ngày con bước vào trường
Nhờ nhà, nhớ mẹ, quê hương đêm ngày
Chúng con rèn luyện hăng say
Tinh mơ đã dậy xếp ngay thẳng hàng
Trật tự nội vụ gọn gàng
Phẳng phiu vuông góc, chắn màn tinh tươm
Thể dục chẳng ngại gió sương
Tung bùng khí thể thao trường hô vang
Tập xà, bơi lội, xếp hàng
Quên đi giá rét, sức càng dẻo dai
Tập võ khổ lắm mẹ ơi
Ngã sấp, ngã ngửa khắp người tấy sưng
Chân tay chai sọ như sừng
Vẫn vui, vẫn tập tung bùng hăng say
Vững vàng, rắn chắc chân tay
Đến khi lâm trận diệt ngay kẻ thù
Quần chi bão táp mây mù
Con giờ đã lớn chẳng như ngày nào
Trên đầu lấp lánh mũ sao
Mẹ ơi, mẹ hãy tự hào vì con

Tác giả - Lê Tuấn Hưng

Đứng trước cổng Học viện Kỹ thuật và Công nghệ an ninh, tôi bỗng thấy lồng ngực mình rung lên một nhịp lạ. Hình ảnh hàng cây xanh, dãy giảng đường uy nghiêm và những tòa ký túc xá thân quen như một dòng suối ngược đưa tôi trở về những năm tháng thanh xuân rực rỡ - thuở tôi còn khoác trên vai đôi cầu vai đồ đầy kiêu hãnh của người học viên Công an nhân dân.

Hôm nay, tôi quay lại không chỉ để tiếp tục con đường học tập, mà còn để chứng kiến sự chuyển mình kỳ diệu của mái trường thân yêu, nơi đã sẵn sàng bước vào một hành trang mới với tên gọi: Học viện Kỹ thuật và Công nghệ An ninh, với tên quốc tế là Học viện Trần Quốc Hoàn.

Thật đặc biệt, bởi đúng vào thời điểm kỷ niệm 15 năm kể từ ngày thành lập (21/10/2010-21/10/2025), ngôi trường thân yêu nay chính thức bước sang một chặng đường lịch sử mới - một hành trình trưởng thành, hội nhập, mang theo niềm tự hào vô bờ của biết bao thế hệ thầy cô và học viên.

Nhìn sự chuyển mình ấy, tôi vừa ngỡ ngàng, vừa dâng trào tự hào. Mái trường Đại học Kỹ thuật - Hậu cần CAND năm nào giờ đây không chỉ còn là nơi ươm mầm cho những cán bộ kỹ thuật công an mà đã vươn lên trở thành cái nôi đào tạo nhân lực chiến lược cho nền an ninh - công nghệ của đất nước. Tôi thực sự xúc động khi nghe thầy cô chia sẻ về định hướng tương lai: Y - Dược, Kỹ thuật bán dẫn, Công nghệ cao, Trí tuệ nhân tạo... Những ngành học tiên phong này không chỉ bắt kịp hơi thở thời đại mà còn minh chứng cho khát vọng tự chủ và làm chủ công nghệ trong lĩnh vực an ninh, sẵn sàng đối phó với những thách thức phi truyền thống, chấp cánh cho nhà trường vươn tầm quốc tế, xứng đáng với tên gọi Học viện.

Trở về nơi Thanh xuân bắt đầu

Học viên Đỗ Thị Phụng
Lớp LT09

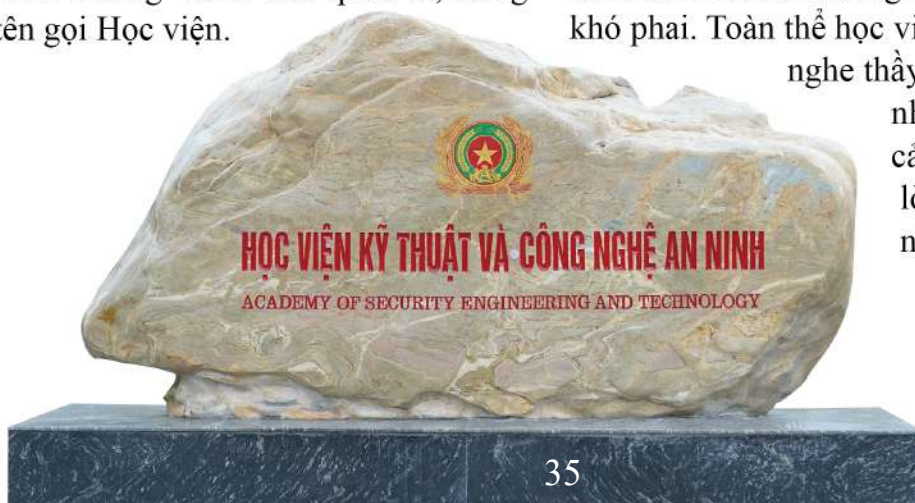
Học viện Kỹ thuật và Công nghệ An ninh

Những ký ức về một thời học viên lại cuộn cuộn ùa về trong tôi. Đó là nơi kỷ luật bắt đầu từ tiếng còi báo thức đồng đặc trong sương sớm, nơi hàng hàng lớp lớp học viên cùng hô vang khẩu hiệu rèn luyện thân thể - "khỏe để học, khỏe để xây dựng và bảo vệ Tổ quốc." Là những giờ học lý thuyết sâu sắc, là những đêm ánh đèn tri thức thao thức bên trang sách, đối diện với thử thách phòng thí nghiệm. Nhưng đáng nhớ hơn cả là những buổi thao luyện dưới trưa nắng gắt, nơi mồ hôi thấm đẫm vai áo, nơi ý chí được tôi luyện trong lửa để bền bỉ vượt qua mọi hành trình gian khổ. Tất cả tạo nên một thước phim ký ức không phai về những chàng trai, cô gái mười tám đôi mươi ấy: mạnh mẽ trong màu áo xanh, dịu dàng trong những giấc mơ, vẫn còn nguyên vẹn và tươi mới như hơi thở.

Và tôi không thể quên những buổi chào cờ đầu tuần. Tiếng trống, tiếng hiệu lệnh nghiêm trang vang lên, cả sân trường cùng vang vọng tiếng "Xin thề! Xin thề! Xin thề!" đồng thanh, hùng hồn của lớp lớp học viên. Tiếng thề ấy như thấm vào từng viên gạch, từng hàng cây, chứa đựng trọn vẹn nhiệt huyết và sức trẻ, đồng thời nhắc nhở mỗi học viên về kỷ luật thép, về trách nhiệm cao cả, và về niềm tự hào bất diệt khi khoác trên vai màu áo Công an nhân dân.

Hay những buổi sinh hoạt đọc báo tối âm áp dưới ánh đèn sân trường cũng để lại bao kỷ niệm khó phai. Toàn thể học viên ngồi xếp hàng lắng nghe thầy cô đọc những bài báo,

những câu chuyện truyền cảm hứng, xen lẫn những lời tâm sự chân tình, hay những tiết mục văn nghệ ngẫu hứng đầy tài hoa.



Tất cả đã bồi đắp nên một nét văn hóa, tinh đồng chí, tinh đồng đội sâu đậm và một thanh xuân không thể nào quên dưới mái trường này.

Tôi thấy trong niềm tự hào về mái trường là cả một chặng đường dài mà biết bao thế hệ thầy cô, học viên đã dốc sức vun đắp. Và hơn hết, tôi thấy lòng mình rung rung - vì được chứng kiến mái trường xưa trưởng thành, lớn mạnh, mang trong mình khát vọng vươn tầm cao mới.

Tôi chợt nhận ra, cũng như chính mình, mái trường đã lớn lên, trưởng thành và đổi thay theo dòng chảy thời gian. Nhưng dù tên gọi có thay đổi thế nào, nơi này vẫn mãi là ngôi nhà thứ hai - nơi đã dạy tôi bài học đầu tiên về kỷ luật, bản lĩnh, và lòng trung thành tuyệt đối với Tổ quốc.

Bước qua cánh cổng trường, giữa những âm thanh quen thuộc của sân thao luyện, tôi mỉm cười. Mười lăm năm trôi qua kể từ ngày thành lập, tôi lại được trở về. Lần trở về này không chỉ là để học thêm, mà là để cống hiến và viết tiếp hành trình thanh xuân còn dang dở, cùng mái trường mang tên mới, nhưng vẫn đầy ắp tình xưa, nghĩa cũ.

Mái trường năm ấy, dù mang tên gì, vẫn mãi là nơi tôi thuộc về – nơi đã dạy tôi bài học đầu tiên về kỷ luật, về lòng trung thành, và về niềm tự hào được khoác lên mình sắc phục CAND. Tôi luôn trân trọng từng ngày được sống, được học, được rèn luyện nơi đây. Bởi không có kỷ ức nào đẹp hơn những ngày khoác trên mình màu áo học viên, sáng tập thể dục trong sương, chiều thao luyện dưới nắng, tối miệt mài bên trang sách.

Mái trường hôm nay đã lớn mạnh, mang khát vọng vươn tầm quốc tế, nhưng vẫn giữ nguyên vẹn ngọn lửa truyền thống và tinh thần kiên cường của người chiến sĩ Công an nhân dân. Và tôi tin, tôi - một học viên trở lại - sẽ là cầu nối vững chắc giữa truyền thống rực rỡ và khát vọng vươn tầm. Trong từng viên gạch, từng hàng cây, tôi cảm nhận được nhịp đập quen thuộc của những thế hệ học viên đã từng đi qua - trong đó có tôi, người nay lại đứng trước cổng trường, lòng rộn ràng và tự hào như gặp lại chính mình của những ngày đầu tiên ấy./.

Return to the Dawning of Youth

Author: Do Thi Phuong

Class: LT09

Academy of Security Engineering and Technology

Translator: Ngo Viet Hoa

Standing in front of the gate of the People's Public Security University of Technology and Logistics, I suddenly felt a strange beat in my chest. The image of the green trees, the majestic lecture halls, and the familiar dormitory buildings seemed like a reverse stream, bringing me back to the bright years of my youth - the time when I proudly wore the red epaulettes of a public security cadet.

Today, I return not only to continue my educational journey but also to witness the remarkable transformation of the university, which is about to take on a new name - Academy of Security Engineering and Technology, internationally known as Tran Quoc Hoan Academy.

It's truly special because, on the 15th anniversary of its founding (October 21, 2010 - October 16, 2025), this beloved institution is officially entering a new historical chapter - a journey of maturity, integration, and immense pride for generations of teachers and students.

Witnessing this transformation, I am both surprised and overwhelmed with pride. The university of my past is no longer just a place nurturing technical police officers; it has risen to become a strategic human resources training center for the nation's security and technology sector. I was truly moved when teachers shared the future orientation: Medicine and Pharmacy, Semiconductor Technology, High Technology, Artificial Intelligence, etc. These pioneering fields not only keep pace with the times but also demonstrate the aspiration for technological

self-reliance and mastery in the security sector, ready to confront non-traditional challenges, elevating the university to international stature, living up to the prestigious name of an Academy. Memories of my time as a cadet came rushing back to me. It was the place where discipline started with the loud sound of the alarm in the early morning mist, where rows upon rows of cadets would chant slogans to train their bodies - "Strong to study, strong to build and protect the homeland." It was the hours of deep theoretical lessons, the nights when the light of knowledge flickered beside the pages of books, facing the challenges of the laboratory. But what stands out the most are the training sessions under the scorching midday sun, where sweat soaked through the shoulders of our uniforms, and where our willpower was forged in the fire to persist through every arduous journey. All of this forms a vivid memory of those young men and women, strong in their green uniforms, gentle in their dreams, still intact and as fresh as the very breath of life.

And I can never forget the flag-raising ceremonies every Monday morning. The drumbeats and the commanding signals rang out, and the whole schoolyard resounded with the synchronized, powerful chant of "I swear! I swear! I swear!" from row upon row of cadets. That oath seemed to seep into every brick, every tree, carrying the passion and youth of each cadet, while also reminding everyone of the steel discipline, the noble responsibility, and the unyielding pride of wearing the Public security force uniform.

The warm evening newspaper-reading sessions under the courtyard lights also left countless unforgettable memories. All the students would sit in formation, listening to teachers read inspiring articles and stories, interspersed with sincere confessions and impromptu, talented cultural performances. All of this nurtured a deep culture, camaraderie, and an unforgettable youth under the roof of this school.

I see that the pride I feel for the university encompasses a long journey that countless generations of teachers and students have dedicated themselves to building. And more than anything, my heart swells - for witnessing my old school grow, mature, and harbor the aspiration to reach new heights. I suddenly realize that, like myself, the school has grown, matured, and changed with the flow of time. But no matter what the name changes to, this place will always be my second home - the place that taught me the first lessons about discipline, bravery, and absolute loyalty to the homeland.

Stepping through the school gate, amidst the familiar sounds of the training ground, I smile. Fifteen years since its establishment, I get to return. This return is not just to learn more, but to contribute and continue the unfinished journey of my youth, alongside the school with its new name, but still full of old affection and comradeship.

The school of my past, whatever its name, will always be where I belong - the place that taught me the first lesson about discipline, loyalty, and the pride of wearing the Public security force uniform. I always cherish every day I lived, studied, and trained here. Because no memory is more beautiful than the days wearing the cadet uniform, exercising in the morning mist, training under the afternoon sun, and working diligently late into the night over my books.

The university today has grown stronger, embracing the aspiration to reach international stature, yet still preserving the integrity of its tradition and the unwavering spirit of a People's public security officers. And I believe that I - a returning student - will be a solid bridge between the brilliant tradition and the ambition for greater reach. In every brick, every tree, I feel the familiar pulse of the generations of students who have passed through - including me, who now stands once again at the university gate, my heart filled with the same excitement and pride as meeting my own self from those very first days./.

Học viện Kỹ thuật và Công nghệ an ninh - Những chặng đường phát triển

Trải qua gần 70 năm xây dựng, cống hiến và trưởng thành, Học viện Kỹ thuật và Công nghệ an ninh đã chính thức bước vào một chặng đường lịch sử mới đầy tự hào. Ngày 17 tháng 10 năm 2025, Phó Thủ tướng Chính phủ đã ký Quyết định số 2288/QĐ-TTg đổi tên Trường Đại học Kỹ thuật - Hậu cần Công an nhân dân thành Học viện Kỹ thuật và Công nghệ an ninh. Với tên giao dịch quốc tế là Học viện Trần Quốc Hoàn, Nhà trường đã bước vào một giai đoạn phát triển mới, mang trên mình tầm vóc, vị thế và sứ mệnh lịch sử to lớn hơn.

Đây không chỉ là sự thay đổi về tên gọi, mà còn là sự khẳng định cho một định hướng chiến lược, chuyên sâu, đáp ứng yêu cầu cấp thiết của nhiệm vụ bảo vệ an ninh quốc gia trong thời kỳ cách mạng công nghiệp 4.0. Để hiểu rõ hơn về bước chuyển mình mang tính bước ngoặt này, chúng ta hãy cùng nhìn lại những chặng đường phát triển vẻ vang đã tạo nên nền tảng vững chắc cho Học viện hôm nay.

Chặng 1: Cội nguồn từ những lớp học đầu tiên (1956 - 1984)

Nền móng của Học viện được hình thành từ hai đơn vị tiền thân, ra đời trong bối cảnh đất nước vừa kháng chiến, vừa kiến quốc, với những nhiệm vụ đặc biệt quan trọng.

Đầu tiên là Trường Trung học Thông tin liên lạc, với ngày truyền thống được tính từ 01/6/1956, khi Bộ Công an khai giảng Lớp đào tạo cán bộ báo vụ đầu tiên. Lớp học gồm 52 học viên, ra đời với sứ mệnh đào tạo lực lượng nòng cốt cho công tác thông tin, đảm bảo "mạch máu" liên lạc được thông suốt, thống nhất, phục vụ đắc lực cho sự nghiệp bảo vệ chính quyền cách mạng.

Mười một năm sau, trước yêu cầu bảo mật tuyệt đối trong chỉ đạo, Trường Cơ yếu Công an nhân dân ra đời, đánh dấu bằng sự kiện khai giảng Lớp đào tạo cán bộ cơ yếu đầu tiên vào ngày 20/5/1967. Lớp học gồm 45 học viên, được đào tạo với tinh thần mà Bộ trưởng Trần Quốc Hoàn đã chỉ thị: "Công tác Cơ yếu cũng là một công tác phản gián".

Hai đơn vị tiền thân, dù ra đời ở hai thời điểm khác nhau, nhưng cùng chung một mục tiêu là đào tạo những người chiến sĩ công an vừa "hồng", vừa "chuyên", đáp ứng yêu cầu đặc thù của công tác kỹ thuật nghiệp vụ.

Chặng 2: Hợp nhất và phát triển dưới mái trường Trung cấp (1984 - 2010)

Giai đoạn này được đánh dấu bằng hai cột mốc lịch sử quan trọng. Mốc son đầu tiên là ngày 08/9/1984, khi Bộ trưởng Bộ Nội vụ ra Quyết định số 92/QĐ-BNV, nâng cấp cả hai trường hạ sỹ quan Thông tin và Cơ yếu lên bậc Trung học chuyên nghiệp. Sự kiện này khẳng định sự trưởng thành vượt bậc về chất lượng đào tạo và sau này Ngày 08/9 hằng năm đã được chọn làm Ngày Truyền thống vẻ vang của Nhà trường.

Cột mốc thứ hai là ngày 14/10/1993, theo Quyết định số 402/QĐ-BNV, hai trường tiền thân chính thức sáp nhập thành Trường Trung học Kỹ thuật nghiệp vụ Công an nhân dân. Sự hợp nhất này đã tạo ra sức mạnh tổng hợp, tập trung nguồn lực, thống nhất chương trình đào tạo, đặt nền móng vững chắc cho sự phát triển toàn diện của Nhà trường trong giai đoạn tiếp theo.

Chặng 3: Vươn tầm Đại học (2010 - 2025)

Trước đòi hỏi của thực tiễn về nguồn nhân lực chất lượng cao, ngày 21/10/2010, Thủ tướng Chính phủ đã ban hành Quyết định lịch sử số 1945/QĐ-TTg, thành lập Trường Đại học Kỹ thuật - Hậu cần Công an nhân dân. Đây là một bước tiến vượt bậc, đưa Nhà trường lên một tầm cao mới.

Trong 15 năm dưới tên gọi này, Nhà trường đã đạt được những thành tựu rực rỡ: khai giảng khóa đại học chính quy đầu tiên (D1) vào năm 2011, xây dựng cơ sở vật chất hiện đại, khang trang tại thị xã Thuận Thành, tỉnh Bắc Ninh, và vinh dự được Đảng, Nhà nước trao tặng nhiều phần thưởng cao quý như Huân chương Quân công hạng Nhì (2014) và nhiều lần nhận Cờ thi đua của Chính phủ.

Chặng 4: Bước ngoặt mới - Học viện Kỹ thuật và Công nghệ an ninh (Từ 16/10/2025)

Quyết định đổi tên trường một lần nữa khẳng định tầm nhìn chiến lược của Đảng ủy Công an Trung ương và lãnh đạo Bộ Công an. Trong bối cảnh khoa học kỹ thuật và công nghệ phát triển như vũ bão, tội phạm sử dụng công nghệ cao ngày càng tinh vi và nguy hiểm, Bộ Công an cần có một học viện đào tạo, nghiên cứu chuyên sâu để đáp ứng những yêu cầu nhiệm vụ mới trong bối cảnh hiện nay.

Tên gọi mới "Học viện Kỹ thuật và Công nghệ an ninh" đã thể hiện rõ sứ mệnh và tầm vóc đó. Chữ "Học viện" khẳng định vị thế là một trung tâm đào tạo, nghiên cứu khoa học đầu ngành, trong khi cụm từ "Kỹ thuật và Công nghệ an ninh" nhấn mạnh định hướng chuyên sâu vào các lĩnh vực mũi nhọn, phù hợp với xu hướng toàn cầu về chuyển đổi số và an ninh mạng.

Đặc biệt, tên giao dịch quốc tế "Học viện Trần Quốc Hoàn" là một sự vinh danh mang ý nghĩa sâu sắc, nhằm tri ân đồng chí Trần Quốc Hoàn - vị Bộ trưởng đầu tiên của Bộ Công an, người đã đặt nền móng cho cả hai đơn vị tiền thân của Học viện. Việc mang tên ông là sự khẳng định cho việc kế thừa di sản, tầm nhìn chiến lược trong công tác kỹ thuật nghiệp vụ và là lời tri ân đối với một tấm gương sáng về trí tuệ, bản lĩnh và tinh thần kiên trung với sự nghiệp cách mạng.

Hành trang của Học viện Kỹ thuật và Công nghệ an ninh hôm nay là gần 70 năm lịch sử hào hùng. Sứ mệnh trong giai đoạn mới sẽ tập trung vào việc đào tạo các chuyên gia hàng đầu, đồng thời mở ra các chuyên ngành mới, bắt kịp xu thế như: Khoa học dữ liệu và trí tuệ nhân tạo, Công nghệ điện tử vi mạch và bán dẫn, An toàn thông tin và bảo mật hệ thống thông tin... để trở thành "thanh bảo kiếm" sắc bén trên mặt trận đối phó với các thách thức an ninh phi truyền thống và tội phạm công nghệ cao.

Nhìn lại chặng đường đã qua, các thế hệ lãnh đạo, cán bộ, giảng viên, học viên Nhà trường đều có quyền tự hào về một di sản lịch sử truyền thống vẻ vang đó. Hướng tới tương lai, với tên gọi và sứ mệnh mới, Học viện Kỹ thuật và Công nghệ an ninh chắc chắn sẽ tiếp tục viết nên những trang sử vàng, tiếp nối xứng đáng truyền thống của các thế hệ đi trước, hoàn thành xuất sắc mọi nhiệm vụ mà Đảng, Nhà nước và Nhân dân giao phó.

Trải qua gần 70 năm lịch sử với những chặng đường đầy tự hào, từ những lớp học nghiệp vụ đầu tiên thời gian khó đến một Học viện hiện đại, bề dày truyền thống đó đã hun đúc nên bản sắc và vị thế của Học viện Kỹ thuật và Công nghệ an ninh hôm nay.

Đề cùng nhìn lại và khắc sâu hơn những cột mốc đáng nhớ trên hành trình vẻ vang đó, Ban Biên tập đã chuẩn bị một thử thách nhỏ. Bạn đã sẵn sàng kiểm tra xem mình hiểu về lịch sử Nhà trường đến đâu chưa?

Hãy quét mã QR bên cạnh để tham gia bài trắc nghiệm vui "Thử thách Lịch sử T07" và xem bạn ghi được bao nhiêu điểm nhé!



EDUCATION QUIZ

Hey, future tech experts! Ready for a fun challenge? Let's see how well you know the world of education. Below are some tricky riddles related to your academic journey. Choose the correct answer from the options provided for each question. Put on your thinking caps and test your knowledge!

1. I hold facts, theories, and sometimes secrets. I can be opened in silence or searched in seconds. Whether in print or on a screen, I guard knowledge faithfully. What am I?

- A. Textbook B. Library card C. Notebook D. Tablet

2. I test your memory, logic, and patience. You meet me often, but never by choice. Yet I'm the one who helps prove your competence. What am I?

- A. Survey B. Exam C. Worksheet D. Assignment

3. I stand at the front, but my goal is to push you forward. I ask tough questions so you can become tougher people. Who am I?

- A. Coach B. Lecturer C. Librarian D. Monitor

4. I require teamwork, planning, and clear communication. I can build both skills and friendships. In university, I feel a bit like a mission briefing. What am I?

- A. Lecture notes B. Final exam C. Solo assignment D. Group project

5. I start with curiosity and end with understanding. I help officers make informed, responsible decisions. Without me, learning stops. What am I?

- A. Memorization drills B. Physical training
C. Critical thinking D. Time management

Select the correct answer for each question and see how well you do! Can you guess how many people will answer all questions correctly? Those who get it right will receive a prize! Don't forget to share with your friends and challenge them to beat your score!