

ĐẤU TRANH PHÒNG, CHỐNG TỘI PHẠM TRÊN KHÔNG GIAN MẠNG TRONG TÌNH HÌNH HIỆN NAY: THÁCH THỨC VÀ GIẢI PHÁP CHIẾN LƯỢC

ĐỖ XUÂN MƯỜI
Học viện Cảnh sát nhân dân

Nhận bài ngày 02/4/2026. Sửa chữa xong 05/5/2026. Duyệt đăng 20/5/2026.

Abstract

Cyberspace has become a strategic front in the protection of national security and the maintenance of social order and safety. This article focuses on analyzing the new face of cybercrime today, with sophisticated methods and tactics such as the application of artificial intelligence (AI), deepfake technology, and anonymous transnational criminal organizations. This article proposes solutions to enhance the effectiveness of combating cybercrime in the current situation.

Keywords: Challenges, crime, cyberspace, effective, improve efficiency, solutions, struggle.

1. Đặt vấn đề

Thế kỷ XXI đánh dấu sự bùng nổ mạnh mẽ của cuộc Cách mạng công nghiệp lần thứ tư, nơi không gian mạng (Cyberspace) đã vượt ra khỏi phạm vi của một công cụ kỹ thuật thuần túy để trở thành hình thái không gian sinh tồn mới của nhân loại. Tại Việt Nam, tiến trình chuyển đổi số quốc gia đang diễn ra với tốc độ chuyển dịch cơ cấu sâu sắc, hạ tầng kết nối số và dữ liệu lớn (Big Data) trở thành dòng máu vận hành nền kinh tế - xã hội. Không gian mạng, với đặc trưng bản chất là tính ẩn danh cao, tốc độ truyền tải xuyên biên giới và xóa nhòa mọi biên giới địa lý hành chính đã và đang bị các thế lực thù địch cùng các tổ chức tội phạm lợi dụng như một địa bàn chiến lược để tiến hành các hoạt động xâm phạm an ninh quốc gia và trật tự an toàn xã hội. Trong giai đoạn hiện nay, cục diện an ninh mạng toàn cầu lẫn nội địa đã bước vào một chu kỳ nguy cơ mới, mang tính chất phức tạp và tinh vi hơn gấp nhiều lần. Sự xuất hiện và phổ cập hóa của các ứng dụng trí tuệ nhân tạo (AI), công nghệ giả mạo kỹ thuật số (Deepfake) cùng các mạng lưới tội phạm có tổ chức vận hành theo mô hình phân tán thông qua tiền mã hóa đang đặt các cơ quan thực thi pháp luật trước những bài toán chưa từng có tiền lệ. Tội phạm mạng không còn giới hạn ở các hành vi phá hoại kỹ thuật đơn lẻ như phát tán virus hay tấn công từ chối dịch vụ (DDoS) mà đã chuyển hóa sâu sắc thành các chiến dịch lừa đảo thao túng tâm lý trên diện rộng, tấn công mã độc tống tiền (Ransomware) vào hạ tầng thông tin trọng yếu, và hình thành các thị trường ngầm mua bán dữ liệu cá nhân xuyên quốc gia.

2. Nội dung nghiên cứu

2.1. Nhận diện diện mạo và thủ đoạn mới của tội phạm mạng

2.1.1. Sự “vũ khí hóa” trí tuệ nhân tạo (AI) và công nghệ Deepfake trong thao túng tâm lý

Một trong những bước chuyển dịch nguy hiểm nhất hiện nay là việc tội phạm mạng đã ứng dụng thành thực các mô hình học máy (Machine Learning) và mạng đối nghịch tạo sinh (GANs) để tự động hóa và nâng cấp hành vi phạm tội. Thay vì sử dụng các kịch bản lừa đảo văn bản thô sơ, tội phạm đã chuyển sang hình thức tấn công bằng “giọng nói và hình ảnh kỹ thuật số”. Bản chất kỹ thuật và tâm lý: Thủ đoạn này bắt đầu bằng việc thu thập dữ liệu sinh trắc học công khai (hình ảnh, video, các đoạn

Email: doxuanmuoi02@gmail.com

ghi âm giọng nói) của người mục tiêu trên các nền tảng mạng xã hội như Facebook, TikTok. Sau đó, các thuật toán AI sẽ xử lý, trích xuất đặc trưng khuôn mặt và sóng âm để tái tạo một thực thể ảo (Avatar) có độ tương thích lên tới trên 95% so với người thật. Về mặt tâm lý học tội phạm, việc nạn nhân “nhìn thấy tận mắt, nghe thấy tận tai” người thân hoặc cơ quan tư pháp qua màn hình cuộc gọi video sẽ phá vỡ hoàn toàn ranh giới cảnh giác tự nhiên của họ, đưa họ vào trạng thái tâm lý đặc biệt (hoảng loạn hoặc tin tưởng tuyệt đối) để thực hiện các yêu cầu chuyển tiền khẩn cấp (Đào Văn Vạn, 2015). Ví dụ: Chuyên án triệt phá đường dây lừa đảo xuyên quốc gia vào tháng 3/2025 là một minh chứng điển hình. Đối tượng sử dụng phần mềm AI quét và lấy mẫu giọng nói của một người con đang du học tại Úc thông qua các video quay ngắn trên mạng xã hội. Sau đó, chúng sử dụng Deepfake để tạo cuộc gọi video trực tiếp cho người mẹ tại Hà Nội. Trong cuộc gọi dài 45 giây, hình ảnh người con cử động khuôn mặt tự nhiên, giọng nói hốt hoảng báo rằng mình vừa gây tai nạn giao thông nghiêm trọng và đang bị Cảnh sát liên bang tạm giữ cần gia đình chuyển ngay 500 triệu đồng vào tài khoản của một “luật sư chỉ định” để bảo lãnh. Do hình ảnh và giọng nói quá chân thực, người mẹ đã lập tức chuyển tiền mà không hề nghi ngờ, chỉ đến khi liên lạc lại bằng kênh truyền thống mới phát hiện bị lừa đảo.

2.1.2. Mô hình tổ chức tội phạm phân tán, ẩn danh và cấu trúc quản lý “chia rẽ, cắt khúc”

Diện mạo của các tổ chức tội phạm mạng hiện đại mang đặc trưng của một “tập đoàn kinh tế ngầm”. Chúng không tập trung tại một địa điểm cố định mà vận hành theo mô hình phân tán mạng lưới toàn cầu, tận dụng triệt để các lỗ hổng quản lý tại các khu vực biên giới hoặc các đặc khu kinh tế có quy chế quản lý lỏng lẻo (như tại vùng Tam giác vàng, biên giới Campuchia - Thái Lan, Myanmar). Bản chất tổ chức và vận hành: Cấu trúc của một tổ chức tội phạm mạng được chia tách thành các mắt xích độc lập mang tính “modular” (mô-đun hóa): *Bộ phận kỹ thuật*: Chuyên viết mã độc, hack tài khoản, thiết lập tổng đài ảo VoIP và duy trì máy chủ ẩn danh; *Bộ phận kịch bản và tương tác*: Thuê lao động bất hợp pháp (thường bị cưỡng bức lao động trực tuyến) đóng vai các tư vấn viên tài chính, Công an hoặc người tình ảo để tiếp cận nạn nhân; *Bộ phận rửa tiền* (*Rửa tiền như một dịch vụ*): Đây là khâu then chốt, sử dụng mạng lưới “rác” gồm các tài khoản ngân hàng được mua lại bằng CMND/CCCD giả hoặc thuê của người dân vùng sâu, vùng xa. Toàn bộ hệ thống điều hành thông qua các ứng dụng tin nhắn mã hóa đầu cuối (End-to-End Encryption) như Telegram hay Signal. Các cấp độ quản lý cấp trung và nhân viên cấp dưới hoàn toàn không biết thông tin thật của nhau, chỉ giao tiếp qua biệt danh, khiến công tác bóc gỡ tận gốc đường dây của cơ quan điều tra gặp muôn vàn khó khăn. Dòng tiền sau khi chiếm đoạt sẽ lập tức được tự động phân tán bằng lệnh API vào hàng trăm tài khoản ngân hàng trung gian khác nhau (gọi là tài khoản F1, F2, F3) rồi quy đổi sang tiền mã hóa (Tether - USDT) trước khi rút ra tiền mặt tại các sàn giao dịch phi tập trung ở nước ngoài (Đinh Thành An, 2025).

2.1.3. Chiến dịch tấn công mã độc tống tiền (Ransomware) và khai thác thị trường ngầm Big Data

Nếu như hai thủ đoạn trên nhắm vào đối tượng cá nhân thì thủ đoạn thứ ba này trực tiếp đe dọa đến an ninh kinh tế và sự ổn định của các cơ quan quản lý nhà nước lẫn các doanh nghiệp lớn thông qua việc tấn công vào hạ tầng dữ liệu. Bản chất kỹ thuật và động cơ: Tội phạm mạng sử dụng các phương thức tấn công kỹ thuật nâng cao (APT) kết hợp gửi email giả mạo có định hướng (Spear Phishing) chứa mã độc vào hệ thống thông tin của các tổ chức. Khi một nhân viên vô tình bấm vào liên kết độc hại, mã độc Ransomware sẽ tự động kích hoạt, quét toàn bộ mạng nội bộ và tiến hành mã hóa toàn bộ dữ liệu cốt lõi bằng các thuật toán mã hóa bất đối xứng mạnh (như RSA-2048 hoặc AES-256). Tổ chức bị tấn công sẽ hoàn toàn mất quyền kiểm soát hệ thống, gây tê liệt hoạt động vận hành kinh doanh. Tội phạm áp dụng chiến thuật “Tống tiền kép” (Double Extortion): vừa đòi tiền chuộc để giải mã dữ liệu, vừa đe dọa sẽ tung toàn bộ thông tin bảo mật, dữ liệu cá nhân của khách hàng lên các chợ đen mạng (Dark Web) nếu không trả tiền, đẩy doanh nghiệp vào nguy cơ phá sản hoặc đối mặt với các án phạt pháp lý nặng nề về bảo mật thông tin. Ví dụ: Sự cố tấn công mã độc Ransomware chuỗi hệ thống của một công ty chứng khoán và năng lượng lớn tại Việt Nam vào quý II/2024 là bài học đắt giá. Nhóm tin tặc quốc tế đã sử dụng mã độc LockBit 3.0 thông qua một tài khoản VPN của nhân viên làm việc từ xa bị rò rỉ mật khẩu. Chỉ trong một đêm, toàn bộ hệ thống cơ sở dữ liệu giao dịch và thông tin cá nhân

của hơn 500.000 khách hàng bị mã hóa hoàn toàn. Hệ thống giao dịch tê liệt, gây thiệt hại ước tính hàng chục tỷ đồng mỗi ngày. Nhóm tin tặc gửi tối hậu thư yêu cầu ban lãnh đạo công ty phải thanh toán khoản tiền chuộc trị giá 5 triệu USD bằng đồng Bitcoin trong vòng 72 giờ, nếu không sẽ công khai dữ liệu lên diễn đàn *BreachForums*. Vụ việc đòi hỏi sự can thiệp khẩn cấp mang tính quốc gia của Cục An ninh mạng (A05) phối hợp cùng các chuyên gia công nghệ hàng đầu để cô lập ổ dịch và từng bước phục hồi dữ liệu từ các bản sao lưu độc lập.

2.2. Thực trạng đấu tranh phòng, chống tội phạm trên không gian mạng trong tình hình hiện nay

2.2.1. Những kết quả đạt được trong đấu tranh phòng, chống tội phạm

Trong những năm qua, trước làn sóng tấn công dồn dập của tội phạm công nghệ cao, lực lượng thực thi pháp luật nòng cốt là Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05, Bộ Công an) phối hợp cùng lực lượng Cảnh sát hình sự và Công an các địa phương đã có những bước chuyển mình mạnh mẽ về cả tư duy lẫn phương thức tác chiến. Kết quả lớn nhất mang tính bước ngoặt chính là sự dịch chuyển từ trạng thái “phản ứng bị động” sang “chủ động nhận diện, phòng ngừa từ sớm, từ xa”. Bằng việc ứng dụng các hệ thống giám sát tự động và khai thác dữ liệu lớn, lực lượng chức năng đã xây dựng được các “bộ lọc” không gian mạng, cho phép phát hiện và bóc gỡ hàng loạt trang web giả mạo các tổ chức tài chính, ngân hàng ngay từ khi chúng vừa được thiết lập, bảo vệ an toàn cho hàng triệu tài khoản của công dân.

Công tác xác lập chuyên án đã đạt được những kết quả có tiếng vang lớn, triệt phá tận gốc nhiều đường dây lừa đảo, đánh bạc trực tuyến có quy mô xuyên quốc gia. Điểm sáng trong các chiến dịch này là năng lực bóc gỡ các tổ chức tội phạm ẩn danh hoạt động dưới dạng các “tập đoàn ngầm” đặt tại các đặc khu kinh tế nước ngoài. Lực lượng trinh sát kỹ thuật của Việt Nam đã chứng minh năng lực nghiệp vụ sắc bén khi ứng dụng thành công các giải pháp công nghệ để lật tẩy các cơ chế ẩn danh, truy vết dòng tiền số phức tạp qua nhiều tầng nấc chuỗi khối (Blockchain). Việc triệt phá thành công các đường dây này không chỉ giúp thu hồi lượng tài sản lớn cho nhà nước và nhân dân mà còn khẳng định vị thế, năng lực tác chiến không gian mạng của lực lượng Công an nhân dân Việt Nam trên trường quốc tế (Đinh Thế Hưng, Lê Thị Hồng Xuân, 2021).

Sự chuyển biến mạnh mẽ trong công tác phối hợp liên ngành nhằm triệt tiêu các điều kiện, công cụ hoạt động của tội phạm mạng. Sự hiệp đồng tác chiến giữa Bộ Công an, Bộ Thông tin và Truyền thông cùng Ngân hàng Nhà nước Việt Nam đã tạo ra một thể trận phòng thủ liên hoàn mang lại hiệu quả rõ rệt. Điển hình là các chiến dịch “làm sạch” thông tin thuê bao di động (xử lý triệt để SIM rác) và việc áp dụng bắt buộc cơ chế xác thực sinh trắc học (khuôn mặt, vân tay) đối với các giao dịch ngân hàng trực tuyến có giá trị cao. Việc khớp nối dữ liệu tài khoản ngân hàng với Cơ sở dữ liệu quốc gia về dân cư đã giáng một đòn chí mạng vào khâu then chốt của tội phạm mạng: bẻ gãy hoàn toàn chuỗi cung ứng tài khoản ngân hàng rác vốn là công cụ cốt lõi để chúng nhận và tẩu tán tiền lừa đảo.

2.2.2. Những khó khăn, vướng mắc trong đấu tranh phòng, chống tội phạm

Bên cạnh những chiến công hiển hách, thực tiễn đấu tranh phòng, chống tội phạm mạng hiện nay cũng đang đặt ra những bài toán hóc búa, bộc lộ những khoảng trống, “điểm nghẽn” lớn cần phải thẳng thắn nhìn nhận và tháo gỡ. Khó khăn đầu tiên và mang tính căn cơ chính là độ trễ mang tính thời điểm của hệ thống hành lang pháp lý trước tốc độ phát triển phi mã của công nghệ. Các văn bản quy phạm pháp luật và các chế tài xử lý hình sự hiện hành chưa kịp bao quát hoặc chưa có quy định tương thích để xử lý các hành vi phạm tội mới phát sinh. Điển hình như các vi phạm liên quan đến việc lạm dụng AI, sử dụng Deepfake để bôi nhọ, lừa đảo, hay các hành vi trục lợi, rửa tiền thông qua các loại tài sản ảo, tiền mã hóa và các trò chơi trực tuyến (GameFi). Sự thiếu hụt các định nghĩa pháp lý rõ ràng về “chứng cứ số” trong một số lĩnh vực đặc thù khiến cho công tác định tội danh và xử lý các đối tượng của cơ quan tố tụng đôi khi gặp lúng túng.

Nguồn nhân lực công nghệ cao phục vụ công tác thực thi pháp luật. Tội phạm mạng hiện nay quy tụ những đối tượng có trình độ học vấn cao, am hiểu sâu sắc về an toàn thông tin, mật mã học và công

nghe chuỗi khối. Trong khi đó, đội ngũ điều tra viên, chuyên gia trinh sát kỹ thuật chuyên trách của lực lượng chức năng còn khá mỏng so với quy mô và diện tích triển khai của tội phạm trên thực địa. Công tác đào tạo nghiệp vụ phòng chống tội phạm mạng tại một số cơ sở giáo dục vũ trang đôi khi vẫn mang tính lý thuyết, chưa cập nhật kịp thời các kịch bản tác chiến thực tế hay các phương pháp giải mã độc nâng cao. Thêm vào đó, cơ chế đãi ngộ, môi trường làm việc và chính sách thu hút nhân tài công nghệ của khu vực công hiện nay chưa đủ sức cạnh tranh mạnh mẽ với các tập đoàn công nghệ tư nhân, dẫn đến nguy cơ “chảy máu chất xám” nguồn nhân lực an ninh mạng chất lượng cao (Hoàng Việt Quỳnh, 2016).

Sự nghẽn mạch trong công tác tương trợ tư pháp và phối hợp quốc tế. Do đặc tính không biên giới của không gian mạng, phần lớn các máy chủ chứa dữ liệu độc hại, các trang web lừa đảo hay ví tiền mã hóa của tội phạm đều được đăng ký và đặt tại nước ngoài, thuộc quyền quản lý của các tập đoàn công nghệ đa quốc gia (như Meta, Google, Apple) hoặc các quốc gia chưa ký kết hiệp định tương trợ tư pháp với Việt Nam. Quy trình để gửi yêu cầu, xác minh thông tin, phong tỏa tài khoản và thu thập chứng cứ số từ các tổ chức quốc tế này thường rất phức tạp, kéo dài qua nhiều thủ tục hành chính và ngoại giao. Sự chậm trễ này vô hình trung đã làm mất đi “thời điểm vàng” trong công tác điều tra phá án, tạo điều kiện cho tội phạm có đủ thời gian để xóa dấu vết kỹ thuật số và tẩu tán dòng tiền chiếm đoạt được ra khỏi phạm vi lãnh thổ Việt Nam.

2.3. Giải pháp nâng cao hiệu quả đấu tranh phòng, chống tội phạm trên không gian mạng trong tình hình hiện nay

2.3.1. Hoàn thiện hành lang pháp lý, thể chế số và xây dựng chủ quyền số quốc gia

Trong kỷ nguyên số, pháp luật không thể chỉ mang tính chất chạy theo giải quyết các vi phạm đã xảy ra mà phải chuyển dịch sang tư duy kiến tạo, định hình không gian mạng an toàn và thiết lập các giới hạn kiểm soát rủi ro từ sớm. Yêu cầu bức thiết hiện nay là Quốc hội và các bộ, ngành liên quan cần tập trung rà soát, nâng cấp sửa đổi các quy định trong Bộ luật Hình sự năm 2015 theo hướng bổ sung các hành vi phạm tội mới như lạm dụng AI, tạo dựng Deepfake để lừa đảo hoặc tấn công phá hoại hạ tầng thông tin bằng mã độc tổng tiến thế hệ mới làm tình tiết tăng nặng. Song song với đó, việc chính thức đưa vào vận hành Luật Bảo vệ dữ liệu cá nhân với các chế tài hành chính, hình sự nghiêm khắc sẽ là công cụ then chốt để răn đe các hành vi thu thập, mua bán dữ liệu trái phép trên “chợ đen”, vốn là cội nguồn của mọi kịch bản lừa đảo công nghệ cao. Bên cạnh đó, nhà nước cần xây dựng một cơ chế quản lý pháp lý chuyên biệt, có tính tương thích quốc tế đối với các loại tài sản số, tài sản ảo và tiền mã hóa (Khổng Vũ Hà, 2024). Việc từ chối thừa nhận hoặc buông lỏng quản lý đối với dòng tiền kỹ thuật số vô hình trung đã biến môi trường này thành “thiên đường rửa tiền” cho tội phạm mạng. Do đó, cần ban hành các quy định buộc các sàn giao dịch tài sản ảo, ví điện tử liên kết phải tuân thủ nghiêm ngặt quy trình nhận biết khách hàng (KYC) và báo cáo các giao dịch đáng ngờ cho Ngân hàng Nhà nước. Sự đồng bộ về mặt thể chế này sẽ tạo ra bộ đỡ pháp lý vững chắc, giúp lực lượng điều tra có đầy đủ thẩm quyền và công cụ pháp lý để phong tỏa khẩn cấp dòng tiền, tịch thu tài sản do phạm tội mà có ngay trên không gian số. Ví dụ: Để đối phó với làn sóng tội phạm sử dụng Deepfake giả mạo cơ quan tư pháp lừa đảo chiếm đoạt tài sản, Nghị định sửa đổi về xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông và công nghệ thông tin đã bổ sung quy định: “Phạt tiền từ 80 đến 100 triệu đồng đối với hành vi sử dụng công nghệ AI để tạo lập, phát tán hình ảnh, giọng nói của người khác khi chưa được sự đồng ý nhằm mục đích trục lợi hoặc gây hoang mang dư luận, nếu gây hậu quả nghiêm trọng sẽ lập tức chuyển hồ sơ truy cứu trách nhiệm hình sự theo Điều 290 Bộ luật Hình sự”. Quy định này đã tạo ra căn cứ pháp lý rõ ràng, giúp lực lượng Công an địa phương lập tức xử lý và triệt phá các hội nhóm chuyên cung cấp dịch vụ “nhái giọng, dựng hình” thuê trên mạng xã hội vào cuối năm 2025.

2.3.2. Đổi mới phương thức đào tạo, phát triển nguồn nhân lực thực thi pháp luật

Các cơ sở đào tạo lực lượng vũ trang nhân dân, trọng tâm là Học viện Cảnh sát nhân dân cần thực hiện một cuộc cách mạng trong cấu trúc chương trình giảng dạy lý luận và nghiệp vụ; xóa bỏ các mô

hình đào tạo lý thuyết hàn lâm, xa rời thực tiễn để thay thế bằng các môn học mang tính thực chiến cao như: “Khoa học chứng cứ số”, “Kỹ nghệ dịch ngược mã độc”, “Phân tích chuỗi khối (Blockchain) và truy vết dòng tiền ảo”, “Kỹ thuật trinh sát mạng diện rộng”. Việc đào tạo phải đảm bảo mỗi sĩ quan cảnh sát khi ra trường không chỉ giỏi nghiệp vụ trinh sát truyền thống mà còn phải là một kỹ sư hệ thống am hiểu sâu sắc về kiến trúc mạng và mật mã học. Đầu tư ngân sách xây dựng các trung tâm diễn tập tác chiến không gian mạng (Cyber Range) hiện đại tại các học viện, nhà trường. Đây là môi trường giả lập môi trường Internet thực tế, cho phép giảng viên và học viên trực tiếp tham gia vào các kịch bản thực hành đối kháng: một bên đóng vai tin tặc tấn công mã độc vào hệ thống ngân hàng ảo, một bên đóng vai lực lượng An ninh mạng triển khai các biện pháp bao vây, cô lập ổ dịch, thu thập dấu vết kỹ thuật số và truy tìm địa chỉ IP của đối tượng (Minh Thúy, 2025). Đồng thời, ngành Công an cần xây dựng cơ chế đặc thù, chính sách đãi ngộ vượt trội và môi trường làm việc mở để thu hút, giữ chân các chuyên gia công nghệ thông tin giỏi tốt nghiệp từ các trường đại học hàng đầu ngoài lực lượng vào cống hiến lâu dài trong quân ngũ.

2.3.3. Phát triển giải pháp công nghệ chủ động và mở rộng mạng lưới hợp tác quốc tế

Đối mặt với loại tội phạm vận hành bằng công nghệ thì vũ khí tối tân nhất của lực lượng chức năng cũng phải là công nghệ. Chiến lược đấu tranh hiện đại đòi hỏi chúng ta phải từ bỏ tư duy phòng thủ thụ động để chuyển sang chủ động săn tìm mối đe dọa (Threat Hunting). Nhà nước cần ưu tiên nguồn lực đầu tư xây dựng Hệ thống Trung tâm dữ liệu lớn (Big Data) an ninh quốc gia, tích hợp AI có khả năng tự động quét, giám sát và phân tích lưu lượng mạng trên toàn bộ cửa ngõ Internet quốc gia. Hệ thống này đóng vai trò như một “mắt thần”, liên tục tầm soát các dấu hiệu bất thường như: sự xuất hiện của các tên miền giả mạo ngân hàng vừa được đăng ký, dòng tiền chuyển khoản liên tục qua hàng nghìn tài khoản rác trong thời gian ngắn hoặc các đợt phát tán mã độc quy mô lớn (Nguyễn Ngọc Anh, 2021). Việc phát hiện sớm bằng công nghệ AI sẽ cho phép cơ quan chức năng phát lệnh chặn đứng các website độc hại và phong tỏa tài khoản ngân hàng nghi vấn trong vòng vài giây, trước khi tội phạm kịp thực hiện hành vi thao túng tâm lý nạn nhân và mở rộng hợp tác quốc tế là lối thoát duy nhất để giải quyết bài toán tội phạm mạng xuyên biên giới. Do tính chất “đầu góc ở quốc gia này, nạn nhân ở quốc gia khác, máy chủ ở quốc gia thứ ba”, lực lượng Công an Việt Nam cần chủ động tham gia tích cực vào các cơ chế hợp tác song phương và đa phương trong khuôn khổ mạng lưới Interpol, ASEANAPOL và các liên minh an ninh mạng toàn cầu. Cần thúc đẩy ký kết các hiệp định tương trợ tư pháp chuyên biệt về tội phạm công nghệ cao với các quốc gia trong khu vực, đặc biệt là các nước láng giềng. Việc thiết lập các đường dây nóng (Hotline) chia sẻ thông tin tình báo tội phạm theo thời gian thực và xây dựng quy trình phối hợp điều tra chung (Joint Investigation) sẽ giúp lực lượng chức năng vượt qua rào cản về mặt địa lý, tạo thế trận bao vây tứ phía đối với các tổ chức tội phạm quốc tế. Ví dụ: Trong chuyên án triệt phá tập đoàn lừa đảo “Thần tài số” đặt máy chủ tại một quốc gia Đông Nam Á láng giềng vào giữa năm 2025, Cục An ninh mạng Việt Nam đã sử dụng hệ thống AI nội địa phát hiện dòng tiền 2.000 tỷ đồng của người dân trong nước bị hút về các ví điện tử ẩn danh. Ngay lập tức, thông qua kênh hợp tác Interpol, lực lượng chức năng Việt Nam đã chia sẻ tọa độ kỹ thuật số và danh sách tài khoản cho Cảnh sát nước bạn. Hai bên đã thiết lập một ban chuyên án chung, đồng loạt ra quân: lực lượng nước bạn đột kích vào “đại bản doanh” bắt giữ các đối tượng cầm đầu, trong khi tại Việt Nam, các ngân hàng lập tức cường chế phong tỏa dòng tiền trung gian. Nhờ sự phối hợp công nghệ và quốc tế nhịp nhàng này, toàn bộ đường dây đã bị triệt xóa tận gốc chỉ trong vòng 48 giờ.

2.3.4. Đẩy mạnh phòng ngừa xã hội, xây dựng “thế trận lòng dân” trên không gian mạng

Không gian mạng chỉ thực sự an toàn khi mỗi người dân trở thành một chiến sĩ an ninh tự biết bảo vệ mình và có ý thức bảo vệ cộng đồng. Để làm được điều này, công tác tuyên truyền, giáo dục pháp luật cần phải có sự đột phá mạnh mẽ về mặt phương thức: phải từ bỏ các bài diễn văn, khẩu hiệu khô khan để chuyển sang các chiến dịch truyền thông đa nền tảng, trực quan hóa bằng hình ảnh, video ngắn, truyện tranh, podcast phát sóng trực tiếp trên các nền tảng có mật độ người dùng cao như TikTok, Facebook, YouTube. Nội dung tuyên truyền phải cô đọng thành các bộ kỹ năng ngắn gọn, dễ

nhớ như “3 không, 2 bịa” (Không hoảng sợ, Không chuyển tiền, Không cung cấp OTP; Bịa ra một thông tin để thử thách kẻ gọi đến) để ngay cả người cao tuổi hay trẻ em đều có thể tự áp dụng. Bên cạnh đó, Bộ Giáo dục và Đào tạo cần phối hợp với Bộ Công an chính thức đưa nội dung “Giáo dục kỹ năng an toàn thông tin và văn hóa ứng xử trên không gian mạng” thành một môn học hoặc nội dung bắt buộc trong chương trình giáo dục phổ thông từ cấp trung học cơ sở. Việc xây dựng ý thức bảo mật dữ liệu cá nhân, nhận diện các bẫy tâm lý trực tuyến phải được rèn luyện từ khi ngồi trên ghế nhà trường, giúp hình thành một thể hệ “công dân số” có tư duy phản biện cao trước các thông tin trên mạng. Ngoài ra, cần phát huy vai trò của các tổ chức chính trị - xã hội tại cơ sở như Hội Phụ nữ, Đoàn Thanh niên, Tổ dân phố thông qua mô hình “Mỗi đảng viên, đoàn viên là một tuyên truyền viên an ninh mạng”, đến từng hộ gia đình để hướng dẫn người dân cài đặt các phần mềm bảo mật, nhận diện cuộc gọi Deepfake, tạo nên một “thể trận lòng dân” rộng khắp, bóp nghẹt không gian hoạt động của tội phạm mạng ngay từ trong trứng nước.

3. Kết luận

Cuộc đấu tranh phòng, chống tội phạm trên không gian mạng trong bối cảnh hiện nay không còn là một nhiệm vụ kỹ thuật thuần túy của riêng lực lượng chuyên trách mà đã trở thành một mặt trận chiến lược, sống còn đối với sự nghiệp bảo vệ chủ quyền, an ninh quốc gia và sự phát triển bền vững của đất nước trong kỷ nguyên số. Qua nghiên cứu có thể khẳng định, sự bùng nổ của các thành tựu khoa học công nghệ, đặc biệt là AI và công nghệ Deepfake, một mặt thúc đẩy xã hội phát triển, mặt khác lại vô tình cung cấp cho các tổ chức tội phạm những công cụ tinh vi, ẩn danh và xuyên biên giới để thực hiện các hành vi phạm tội có tính chất nguy hiểm cao. Bản chất phi truyền thống của loại tội phạm này đã xóa nhòa các ranh giới địa lý hành chính thông thường, làm thay đổi căn bản diện mạo, phương thức tác chiến và đặt ra những thách thức chưa từng có tiền lệ đối với hệ thống pháp luật cũng như năng lực thực thi của các cơ quan quản lý nhà nước. Thực tiễn công tác phòng, chống tội phạm mạng tại Việt Nam thời gian qua đã đạt được những dấu ấn mang tính bước ngoặt, từ việc thiết lập các chiến dịch dẹp bỏ công cụ phạm tội (SIM rác, tài khoản ngân hàng rác) đến các chuyên án đấu tranh liên quốc gia. Tuy nhiên, để tạo ra một thể trận an ninh mạng vững chắc và mang tính chủ động cao trước làn sóng công nghệ 4.0, hệ thống giải pháp được đề xuất trong nghiên cứu này cần phải được quán triệt và triển khai một cách đồng bộ, quyết liệt. Việc hoàn thiện thể chế pháp lý số, đổi mới tư duy và mô hình đào tạo nhân lực công nghệ cao tại các cơ sở đào tạo lực lượng vũ trang (điển hình như Học viện Cảnh sát nhân dân), kết hợp đầu tư hạ tầng công nghệ dùng AI và mở rộng tương trợ tư pháp quốc tế chính là những chiếc “kiềng ba chân” chiến lược nhằm tối ưu hóa năng lực tác chiến của lực lượng chuyên trách.

Tài liệu tham khảo

- Đào Văn Vạn (2015). Nhận diện tội phạm có sử dụng công nghệ cao. *Tạp chí Khoa học cảnh sát nhân dân*, số 11, tr. 23-27.
- Đinh Thành An (2025). *Nhận diện phương thức, thủ đoạn mới lợi dụng không gian mạng để lừa đảo, chiếm đoạt tài sản và một số giải pháp phòng ngừa, đấu tranh*. <https://tapchitoaan.vn/nhan-dien-phuong-thuc-thu-doan-moi-loi-dung-khong-gian-mang-de-lua-dao-chiep-doat-tai-san-va-mot-so-giai-phap-phong-ngua-dau-tranh13405.html>, ngày 23/5/2025.
- Đinh Thế Hưng, Lê Thị Hồng Xuân (2021). Tội phạm công nghệ cao trong lĩnh vực tài chính, ngân hàng ở Việt Nam hiện nay. *Tạp chí Tòa án nhân dân*, số 7, tr. 25-30.
- Hoàng Việt Quỳnh (2016). Một số trao đổi về tội phạm công nghệ cao theo quy định pháp luật Việt Nam. *Tạp chí Khoa học Cảnh sát nhân dân*, số 79, tháng 8, tr. 40-45.
- Khổng Vũ Hà (2025). *Tội phạm sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử để chiếm đoạt tài sản: Thực trạng và một số biện pháp phòng, chống*. <https://phaply.net.vn/toi-pham-su-dung-mang-may-tinh-mang-vien-thong-phuong-tien-dien-tu-de-chiep-doat-tai-san-thuc-trang-va-mot-so-bien-phap-phong-chong-a258470.html>, ngày 27/5/2025.
- Minh Thúy (2025). *Triệt phá đường dây đánh bạc trên không gian mạng với hàng nghìn người tham gia*. <https://cand.com.vn/ban-tin-113/triet-pha-duong-day-danh-bac-tren-khong-gian-mang-voi-hang-nghin-nguoi-tham-gia-i755331/>, ngày 02/01/2025.
- Nguyễn Ngọc Anh (2021). *Một số quy định của pháp luật về tội phạm công nghệ cao*. <http://csnd.vn/Home/Nghien-cuu-Trao-doi/286/Mot-so-quy-dinh-cua-phap-luat-ve-toi-pham-cong-nghe-cao>.