

# NHẬN DIỆN MỘT SỐ ĐẶC ĐIỂM TÂM LÝ TIÊU CỰC CỦA TỘI PHẠM XÂM NHẬP TRÁI PHÉP VÀO MẠNG MÁY TÍNH, MẠNG VIỄN THÔNG HOẶC PHƯƠNG TIỆN ĐIỆN TỬ CỦA NGƯỜI KHÁC PHỤC VỤ CÔNG TÁC PHÒNG NGỪA

Bùi Thị Liên, Ngô Tấn Khải  
Học viện An ninh nhân dân

**Tóm tắt:** Gần đây, tận dụng sự phát triển của khoa học và công nghệ, tội phạm công nghệ cao ngày càng trở nên phức tạp; đặc biệt là hành vi xâm nhập trái phép vào các mạng máy tính, mạng viễn thông hoặc thiết bị điện tử của người khác (hack). Với đặc điểm có trí tuệ cao và nhận thức tốt, hành vi tâm lý của loại tội phạm này rất đa dạng và khó nắm bắt. Do đó, việc nghiên cứu các đặc điểm tâm lý tiêu cực của những tội phạm xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc thiết bị điện tử là hết sức cần thiết. Điều này sẽ là cơ sở cho công tác điều tra và xác minh, đóng góp vào cuộc chiến chống tội phạm trong thời đại mới.

**Từ khóa:** đặc điểm tâm lý; hacker; tội phạm công nghệ cao

## IDENTIFYING SOME NEGATIVE PSYCHOLOGICAL CHARACTERISTICS OF OFFENDERS WHO ILLEGALLY INTRUDE INTO COMPUTER NETWORKS, TELECOMMUNICATION NETWORKS, OR ELECTRONIC DEVICES OF OTHERS TO SERVE PREVENTIVE WORK

Bui Thi Lien, Ngo Tan Khai  
People's Security Academy

**Abstract:** In recent times, taking advantage of the development of science and technology, high-tech crime has become increasingly complex; especially unauthorized intrusion into computer networks, telecommunications networks, or electronic devices of others (hacking). With the characteristics of having high intellectual capacity and awareness, the psychological behavior of this type of criminal is extremely diverse and difficult to grasp. Therefore, studying the negative psychological traits of criminals who illegally access computer networks, telecommunications networks, or electronic devices is essential. This serves as a foundation for investigation and verification efforts, contributing to the fight against crime in the new era.

**Key word:** psychological traits; hacker; high-tech crime

Nhận bài: 13/02/2025

Phản biện: 15/03/2025

Duyệt đăng: 19/03/2025

### I. ĐẶT VẤN ĐỀ

Cuộc cách mạng 4.0, hay còn gọi là Cách mạng công nghiệp 4.0, đề cập đến giai đoạn phát triển mới trong công nghệ sản xuất và quản lý, với sự tích hợp của công nghệ số, Internet of Things (IoT), trí tuệ nhân tạo (AI) và tự động hóa. Mặc dù sự phát triển của công nghệ đem lại nhiều lợi ích cho cuộc sống nhưng nó cũng mang kèm theo đó là những rủi ro và thách thức, trong đó có sự xuất hiện và hoạt động của tội phạm sử dụng công nghệ cao. Tội phạm xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác là loại tội phạm có những đặc trưng cơ bản nhất của tội phạm sử dụng công nghệ cao.

Thống kê năm 2024, ở Việt Nam đã phát hiện 83 chiến dịch tấn công mạng từ 45 nhóm tin tặc trong nước và quốc tế (tăng 30% so với năm 2023) với gần hơn 5000 chỉ dấu xâm nhập nhằm vào hệ thống thông tin trọng yếu. Các đối tượng thực hiện

hành vi xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác thường ẩn danh, khó phát hiện đối tượng cụ thể. Đặc điểm nhân cách, nhận thức và xu hướng hành vi của các đối tượng hacker thường khó nắm bắt, gây khó khăn cho việc phòng ngừa, phát hiện và đấu tranh với những đối tượng phạm tội loại này. Điều này đặt ra yêu cầu cần phải nghiên cứu, khái quát các đặc điểm tâm lý của các đối tượng này phục vụ cho các mặt công tác thực tiễn cũng như bổ sung các vấn đề lý luận có liên quan.

Bài viết nghiên cứu các biểu hiện tâm lý tiêu cực của tội phạm xâm nhập trái phép vào mạng máy tính, mạng viễn thông, nghiên cứu từ 30 trường hợp cụ thể được ghi nhận từ năm 2018 đến 2024. Trên cơ sở đó, bài viết đề xuất một số giải pháp nhằm phòng ngừa, đấu tranh với loại tội phạm này trong tình hình hiện nay.

## II. NỘI DUNG NGHIÊN CỨU

### 2.1. Nhận thức cơ bản về tâm lý tội phạm xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác

Trên thế giới và ở Việt Nam có nhiều cách phân loại các hành vi xâm nhập trái phép vào mạng máy tính, mạng viễn thông ... Phổ biến hiện nay là 4 hình thức hacking cơ bản, bao gồm: Xâm nhập (vật lý và phi vật lý), Kỹ nghệ xã hội (gửi tệp tin có gắn mã độc để làm thay đổi hoặc chiếm quyền kiểm soát tài khoản); Tấn công thay đổi giao diện; Từ chối dịch vụ (DoS) và từ chối dịch vụ phân tán (DDoS). Phương thức thủ đoạn của các đối tượng hacker ngày một tinh vi hơn, hacker có thể

Trong nghiên cứu tâm lý học cá nhân, có nhiều quan điểm và phương pháp phân tích khác nhau về đặc điểm tâm lý. Tâm lý con người được hiểu là các hiện tượng tinh thần diễn ra trong đầu óc con người, được hình thành thông qua hoạt động và giao tiếp, đồng thời được bộc lộ và điều chỉnh toàn bộ hoạt động ở mỗi cá nhân. Đặc điểm tâm lý cá nhân là tổ hợp những nét riêng biệt, đặc trưng riêng phản ánh sự khác nhau trên phương diện tâm lý giữa cá nhân này với cá nhân khác, nhóm người này với nhóm người khác. Đặc điểm tâm lý có thể được nhận diện theo các thuộc tính tâm lý trong nhân cách cá nhân, bao gồm: xu hướng (nhu cầu, động cơ, hứng thú, niềm tin, thể giới quan, lý tưởng, định hướng giá trị), tính cách, năng lực, khí chất; hoặc có thể được phân tích theo các đặc điểm về nhận thức, xúc cảm, hành vi, trạng thái tâm lý và diễn biến tâm lý.

Bài viết tập trung phân tích một số đặc điểm tâm lý tiêu cực của tội phạm xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác. Cụ thể, nghiên cứu sẽ làm rõ các biểu hiện liên quan đến nhận thức, trí tuệ, cảm xúc, ý chí, xu hướng cá nhân, nhu cầu, động cơ hành vi, tính cách và năng lực... Việc xem xét những đặc điểm tâm lý này có ý nghĩa quan trọng trong việc xây dựng các biện pháp phòng ngừa, phát hiện và xử lý hiệu quả loại tội phạm này trong bối cảnh hiện nay.

### 2.2. Thực trạng đặc điểm tâm lý tội phạm xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác.

Qua nghiên cứu 30 đối tượng liên quan đến hoạt động xâm nhập trái phép vào mạng máy tính trên không gian mạng điện hình, tổng hợp ý kiến của 100 cán bộ trình sát (CBTS) đã và đang trực tiếp đấu tranh với loại tội phạm này, có thể chỉ ra một số đặc điểm tâm lý tiêu cực của tội phạm loại này như sau:

*Thứ nhất, về nhận thức:* các đối tượng phạm tội liên quan đến hoạt động “xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác” là những người có trình độ cao, có hiểu biết đa dạng, phong phú ở nhiều lĩnh vực công nghệ thông tin và các ứng dụng công nghệ khác. Trong 100 phiếu khảo sát, có 86 ý kiến chiến sỹ Công an đồng tình với nhận định đặc điểm tâm lý nêu trên (chiếm 86%).

Đặc điểm tâm lý này thể hiện đầu tiên ở nhận thức, các đối tượng đa phần là những người có trình độ về công nghệ thông tin ở mức thành thạo. Mục tiêu các đối tượng hướng tới có thể là cá nhân, tổ chức, các doanh nghiệp,... Các đối tượng lợi dụng các lỗ hổng từ hệ thống bảo mật xâm nhập vào đánh cắp thông tin, phá hủy hệ thống cũng như các hành vi phá hoại khác gây ra hậu quả nghiêm trọng.

Về đặc điểm nhân thân, đa số các đối tượng ở trong độ tuổi từ 15-30 tuổi (chiếm 80% số đối tượng). Về nghề nghiệp, phần lớn các đối tượng hoạt động trong lĩnh vực công nghệ thông tin, một số đối tượng là sinh viên, hiện đang học tập tại các trường đại học, số còn lại không có nghề nghiệp ổn định, có đam mê tìm hiểu về công nghệ. Hầu hết các đối tượng đều biết rõ, nhận thức được hành vi phạm tội của mình nhưng có sự hạn chế hoặc không lường trước được hậu quả và hình phạt sẽ phải chịu trước pháp luật. Trong một số trường hợp nhất định, các đối tượng đã nhận thức được cả hai vấn đề những vì muốn thỏa mãn được nhu cầu, lợi ích cá nhân nên vẫn cố tình vi phạm pháp luật.

*Thứ hai, về động cơ hoạt động:* các đối tượng phạm xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác với nhiều động cơ khác nhau. Có những đối tượng thực hiện hành vi để thỏa mãn trí tò mò, có những đối tượng thực hiện vì mục đích thỏa mãn cái tôi, khẳng định năng lực, khả năng của bản thân. Tuy vậy, đa phần các đối tượng có động cơ gắn liền với nhu cầu vụ lợi vật chất. Nhiều đối tượng được trả tiền để thực hiện hành vi, hoặc hợp tác với các đối tượng lừa đảo xâm nhập đánh cắp thông tin cá nhân, lợi dụng danh tính cá nhân người khác để lừa đảo, chiếm đoạt tài sản của các nạn nhân. Đặc điểm này chiếm phần lớn ở đối tượng liên quan đến hoạt động phạm xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác được khảo sát (25/30, chiếm 83.3%). Các cán bộ, chiến sỹ công an được khảo sát đánh giá đây là một trong những động cơ phổ biến nhất của loại tội phạm này. Ngoài ra, một số ít đối tượng

có động cơ chính trị, thực hiện mục tiêu chính trị, tình báo như bô nhô cá nhân, thu thập thông tin đời tư, bí mật của cán bộ, công chức hoặc người có chức vụ nhằm trục lợi... Một số vụ việc được ghi nhận có động cơ xuất phát từ những mâu thuẫn của các nhóm hackers muốn thực hiện hành vi để khẳng định tầm ảnh hưởng của nhóm mình khi đối đầu với các nhóm hackers khác.

Sự hình thành động cơ phạm tội xuất phát từ các nhu cầu cá nhân. Các đối tượng thực hiện hành vi phạm tội xâm nhập trái phép vào phương tiện điện tử, mạng máy tính thường là những người hoạt động trong lĩnh vực công nghệ, có hiểu biết, thành thạo các thao tác về công nghệ thông tin. Do đó, các đối tượng có thể sử dụng những phương thức thủ đoạn vô cùng tinh vi và phức tạp, lợi dụng các lỗ hổng bảo mật, sự thiếu hiểu biết về công nghệ thông tin cũng như sự chủ quan của người dùng để thực hiện hành vi hacking với nhiều mục đích khác nhau.

*Thứ ba, về định hướng giá trị:* các đối tượng liên quan đến hoạt động “xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác” thường đề cao giá trị, lợi ích của bản thân hơn các giá trị, lợi ích của xã hội. Đặc điểm này được cán bộ, chiến sỹ Công an đánh giá xuất hiện ở 26/30(86,66%) đối tượng này. Trong hệ giá trị của các đối tượng, họ hoạt động vì bản thân của họ nhiều hơn là vì sự phát triển của xã hội dẫn đến những suy nghĩ tiêu cực, vì những lợi ích trước mắt.

*Thứ tư, về tính cách:* bên cạnh những đặc điểm riêng gắn với từng cá nhân, qua nghiên cứu, khảo sát cho thấy các đối tượng liên quan hoạt động “xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác” bộc lộ một số tính cách gây khó khăn cho công tác đấu tranh: có kiến thức về công nghệ thông tin, thận trọng, cảnh giác. Qua khảo sát cho thấy có (17/30, chiếm 56,66%) đối tượng bộc lộ tính cách này. Với phần lớn là những người có trình độ cao về công nghệ các đối tượng cho thấy sự hiểu biết về công nghệ sử dụng các phương thức thủ đoạn tinh vi, phức tạp để xóa dấu vết đánh lạc hướng gây khó khăn trong quá trình điều tra. Về kiểu loại tính cách, các nhận định của cán bộ trình sát, điều tra viên đều cho rằng kiểu loại tính cách của hacker thuộc nhóm hướng nội, lối sống khép kín, ít giao tiếp xã hội và nhút nhát trong ứng xử xã hội (26/30, chiếm 86,66%).

*Thứ năm, về mặt tình cảm:* trong cuộc sống hàng ngày, bao gồm cả mối quan hệ với gia đình và người thân, những người phạm tội liên quan

đến hoạt động “xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác” thường duy trì một thái độ cân bằng, kiểm soát tốt cảm xúc của mình. Đối với họ, gia đình đóng vai trò quan trọng, chi phối tới đời sống tình cảm cá nhân của họ. Họ thể hiện sự hợp tác và khai báo nhanh chóng khi được yêu cầu hợp tác trong điều tra, nhưng các bản khai thường thể hiện sự không trung thực và mâu thuẫn qua thời gian đấu tranh. Theo kết quả khảo sát, có 15/30 (50%) đối tượng liên quan đến hacker cho thấy đặc điểm tâm lý này, mặc dù mức độ biểu hiện ở nhiều mức độ khác nhau.

### **2.3 Một số lưu ý trong phòng ngừa tội phạm xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác**

Đối tượng sẽ gia tăng sử dụng nền tảng số, mạng xã hội, tích cực khai thác tiềm năng của không gian mạng để xây dựng mạng lưới “lừa đảo” trên không gian mạng. Các đối tượng núp bóng dưới những công ty tài chính, tạo ra các ứng dụng cho vay, giả danh các tổng đài viễn thông, ngân hàng,... để đưa ra những hình thức quảng cáo, lời chào mời hấp dẫn, các thao tác, thủ tục đơn giản, giải ngân nhanh chóng,... nhằm đánh vào tâm lý người dân. Môi trường mạng là điều kiện thuận lợi để tội phạm có thể thực hiện các thủ đoạn tinh vi, chiếm đoạt thông tin của công dân với mục đích vụ lợi. Do đó, để nâng cao hiệu quả công tác phòng ngừa tội phạm xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác, cần chú ý một số nội dung sau đây:

*Một là,* các cơ quan chức năng cần đẩy mạnh công tác tuyên truyền, đổi mới nội dung hình thức tuyên truyền, kết hợp giữa các phương tiện, biện pháp truyền thống với các kênh tương tác mới như mạng xã hội, báo điện tử, diễn đàn trên mạng về các phương thức, thủ đoạn hoạt động của tội phạm để nâng cao nhận thức trong nhân dân, phòng ngừa, ngăn chặn tội phạm. Tổ chức tuyên truyền cho người dân những kiến thức cơ bản về bảo vệ thông tin cá nhân khi truy cập trên không gian mạng; khi bị các đối tượng gọi điện đe dọa, quấy rối, xuyên tạc, vu khống, xúc phạm danh dự nhân phẩm, hoặc có những dấu hiệu giả danh các tổ chức chính thống như nhà đài, ngân hàng ... cần khai báo với cơ quan công an nơi gần nhất để xử lý theo quy định. Để chủ động phòng ngừa loại tội phạm này, cần phải bắt đầu ngay từ thay đổi nhận thức của người dân – những nạn nhân tiềm năng. Khi người dân đã nâng cao nhận thức về trách nhiệm công dân, trách nhiệm của bản thân

mình, họ sẽ tự giác và kịp thời tố giác tội phạm, cung cấp các thông tin cho cơ quan chức năng, góp phần giữ gìn, đảm bảo trật tự an toàn xã hội.

*Hai là*, các cơ quan chức năng cần tham mưu với Đảng, Nhà nước hoàn thiện các quy định pháp luật, tạo dựng hệ thống pháp luật về bảo mật mạng máy tính, mạng viễn thông hoặc phương tiện điện tử. Theo đó, tập trung rà soát hệ thống pháp luật hiện hành, phát hiện những sơ hở bất cập để tham mưu đề xuất xây dựng, sửa đổi, ban hành các quy định góp phần quản lý chặt chẽ và nâng cao hiệu quả công tác phòng ngừa, đấu tranh xử lý các loại tội phạm sử dụng công nghệ cao; nghiên cứu, đánh giá sửa đổi, bổ sung lý luận về tội phạm nói chung và tội phạm sử dụng công nghệ cao nói riêng. Ngoài ra, cần tạo ra những tổ chức, cơ quan có chức năng, nhiệm vụ bảo vệ thông tin, dữ liệu cá nhân của công dân Việt Nam trên không gian mạng, xử lý sự cố trước các cuộc tấn công nhắm vào người dùng mạng xã hội, các trang web của tổ chức, doanh nghiệp,...

*Ba là*, nâng cao hiệu quả công tác phối hợp trong phòng, chống tội phạm xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác giữa các đơn vị, địa phương, nhất là trong công tác chia sẻ thông tin, phối hợp xác minh, thu thập thông tin, tài liệu phục vụ công tác đấu tranh, xử lý với loại tội phạm này. Mỗi đơn vị, địa phương đều đóng một vai trò quan trọng trong đấu tranh phòng chống tội phạm nói chung và tội phạm liên quan đến công nghệ cao nói riêng. Các lực lượng như Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05), phòng PA05 các tỉnh thành cần thể hiện chủ động vai trò chủ trì, hướng dẫn trong công tác đấu tranh với các loại tội phạm công nghệ. Vậy nên, các chủ thể cần tăng cường phối hợp để có thể trao đổi, chỉ rõ nguyên nhân, điều kiện nảy sinh tội phạm, phát hiện tội phạm cũng như phát huy hơn nữa hiệu quả trong hoạt động phòng ngừa tội phạm xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác.

*Bốn là*, lực lượng Công an cần triển khai mạnh mẽ, quyết liệt các biện pháp nghiệp vụ, nắm tình hình các vụ, việc liên quan đến hoạt động xâm nhập trái phép trên không gian mạng. Lực lượng Công an cần chủ động nắm tình hình, thu thập thông tin các trang web, ứng dụng (app) có dấu hiệu vi phạm pháp luật trên không gian mạng; nắm tình hình, thu thập, phối hợp xử lý các thuê bao điện thoại có dấu hiệu phục vụ hoạt động lừa đảo, giả mạo; tăng cường nắm tình hình về các hội nhóm Zalo, Facebook, Weibo, Telegram, Deepweb... liên quan đến hoạt động mua bán trái phép thông tin cá nhân người dùng; nắm tình hình, ngăn chặn xử lý các cổng trung gian thanh toán trái phép, dịch vụ chuyển tiền trái phép tại địa phương phục vụ hoạt động rửa tiền của tội phạm công nghệ cao.

Năm là, nâng cao hiệu quả công tác tiếp nhận tin báo, tố giác của nhân dân, đổi mới hình thức tiếp nhận tin báo tố giác tội phạm. Thu thập, tổng hợp thông tin về các vụ việc tấn công mạng, xâm nhập trái phép vào các thiết bị điện tử, viễn thông của người bị hại, các phương thức, thủ đoạn, công cụ mà các đối tượng sử dụng để thực hiện cuộc tấn công mạng... và các thông tin liên quan khác nếu có. Trên cơ sở tài liệu thu thập được, nếu xác định có dấu hiệu tội phạm thì tiến hành tập trung lực lượng đấu tranh, điều tra khám phá nhanh các vụ án; phối hợp với Viện kiểm sát nhân dân, Tòa án nhân dân các cấp truy tố, xét xử lưu động một số vụ án điển hình liên quan đến tội phạm này để răn đe, phòng ngừa chung.

### III. KẾT LUẬN

Nhận diện đúng các đặc điểm tâm lý tiêu cực ở tội phạm xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác có ý nghĩa quan trọng, là cơ sở cho công tác điều tra, xác minh tội phạm, góp phần nâng cao hiệu quả công tác phòng ngừa các loại tội phạm nói chung và tội phạm liên quan đến sử dụng công nghệ cao trên không gian mạng nói riêng trong tình hình hiện nay.

### TÀI LIỆU THAM KHẢO

- [1] Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05) Bộ Công an, Báo cáo tình hình công tác đấu tranh phòng chống tội phạm (2019 – 2023).
- [2] Nghị quyết số 08/2021/NQ-UBTVQH15 của ỦY BAN THƯỜNG VỤ QUỐC HỘI về giải thích khoản 1 điều 289 của bộ luật hình sự
- [3] Trương Công Am, Giáo trình tâm lý học tội phạm, Học viện An ninh nhân dân, 2010.
- [4] Bộ luật hình sự năm 2015 sửa đổi, bổ sung năm 2017
- [5] Grainne Kirwan và Andrew Power, Cybercrime: The Psychology of Online Offenders, Nhà xuất bản Cambridge University Press