MỐI ĐE DỌA AN NINH TRUYỀN THÔNG TRONG KỶ NGUYÊN SỐ

ThS. NGUYỄN VĂN THUẬT
Bộ Văn hóa, Thể thao và Du lịch

● **Tóm tắt:** *Công nghệ số và trí tuệ nhân tạo (AI) đã tạo ra những thay đổi cơ bản về mọi mặt của đời sống xã hội, góp phần nâng cao năng suất, hiệu quả lao động, cải thiện chất lượng cuộc sống của con người, song cũng đặt ra không ít thách thức, kéo theo các mối đe dọa tiềm ẩn đối với an ninh truyền thông. Bài viết làm rõ khái niệm và các mối đe dọa an ninh truyền thông, nguy cơ các thế lực thù địch, phản động lợi dụng không gian mạng để chống phá Đảng và Nhà nước ta; đề xuất giải pháp nhằm phòng, chống các mối đe dọa an ninh truyền thông trong kỷ nguyên số thời gian tới.*

● **Từ khóa:** *An ninh truyền thông; AI; Trí tuệ nhân tạo; Kỷ nguyên số.*

Ngày 22-5-2025, Chính phủ đã ban hành Nghị quyết số 147/NQ-CP Chiến lược tổng thể quốc gia phòng ngừa, ứng phó với các đe dọa an ninh phi truyền thống đến năm 2030, tầm nhìn đến năm 2045. Trong đó, chỉ rõ: "Tác động từ các đe dọa an ninh phi truyền thống phải được đánh giá, nhận diện đầy đủ, khách quan, hạn chế thấp nhất rủi ro, đe dọa đến lợi ích, an ninh quốc gia"[1]. Trong bối cảnh toàn cầu hóa hiện nay, một trong những phạm trù quan trọng của an ninh quốc gia trong kỷ nguyên số là an ninh truyền thông. Hiện nay, có nhiều quan điểm khác nhau về mối đe dọa an toàn, an ninh truyền thông. Theo tài liệu của Tổ chức Tiêu chuẩn quốc tế về quản lý rủi ro, mối đe dọa an toàn thông tin là bất kỳ yếu tố nào có thể làm suy giảm tính bảo mật, toàn vẹn hoặc khả dụng của thông tin[2]. Liên minh Viễn thông quốc tế (ITU) cho rằng, an ninh truyền thông là việc bảo vệ thông tin và hệ thống truyền thông khỏi các nguy cơ như truy cập trái phép, giả mạo, gián đoạn hoặc lộ lọt dữ liệu[3].

Có thể hiểu, an ninh truyền thông là trạng thái ổn định và bảo đảm an toàn của hệ thống thông tin và truyền thông trong việc bảo đảm tính bảo mật, toàn vẹn, khả dụng và chính xác của dữ liệu, đồng thời phòng ngừa và ứng phó với các mối đe dọa có thể gây tổn hại do truy cập trái phép, giả mạo, lộ lọt hoặc từ chối dịch vụ; qua đó, bảo đảm cho quá trình trao đổi thông tin diễn ra thông suốt, tin cậy, phục vụ hiệu quả cho tiến trình phát triển và hội nhập của đất nước.

Các hình thức đe dọa an ninh truyền thông

Trên thực tế đã xuất hiện một số hình thức đe dọa an ninh truyền thông phổ biến như: 1) Tấn công mạng (Cyber Attack) - hành động xâm nhập vào hệ thống thông tin nhằm đánh cắp dữ liệu, phá hoại hoặc gây gián đoạn hoạt

động của các nền tảng truyền thông, nghe lén, đánh cắp thông tin cá nhân thông qua email, website giả mạo; 2) Lan truyền tin giả (Fake News), thông tin sai lệch hoặc bị bóp méo nhằm gây hiểu lầm, hoang mang hoặc thao túng dư luận; 3) Gây rò rỉ dữ liệu (Data Breach), làm lộ những thông tin quan trọng do lỗ hổng bảo mật hoặc bị đánh cắp, ảnh hưởng đến quyền riêng tư của tổ chức hoặc cá nhân; 4) Tấn công từ chối dịch vụ (DDoS), làm tê liệt hệ thống truyền thông bằng cách gửi một lượng lớn yêu cầu truy cập, gây quá tải và gián đoạn dịch vụ; 5) Thực hiện hành vi gián điệp truyền thông (Media Espionage) nhằm theo dõi, nghe lén hoặc thu thập thông tin từ các phương tiện truyền thông để trục lợi hoặc phục vụ mục đích chính trị, gây ra các cuộc chiến tranh thông tin (Information Warfare) để thao túng, định hướng dư luận, gây bất ổn trong xã hội...

Mục tiêu, phương thức chống phá của các thế lực thù địch, phản động

Mục tiêu chống phá: Các thế lực thù địch, phản động luôn tận dụng mọi sơ hở để chống phá nhằm phủ định chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh. Chúng cho rằng, nền tảng, nguyên tắc tổ chức và hoạt động của Đảng Cộng sản Việt Nam theo các quan điểm của chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh đã lỗi thời, không còn phù hợp trong thế kỷ XXI. Đồng thời, chúng ra sức "bác bỏ vai trò lãnh đạo của Đảng Cộng sản Việt Nam, hòng xóa bỏ thành quả cách mạng, phủ nhận con đường đi lên chủ nghĩa xã hội của Đảng và nhân dân ta, hướng lái Việt Nam phát triển đi theo quỹ đạo tư bản chủ nghĩa"[4].

Phương thức chống phá: Các thế lực thù địch, phản động thường sử dụng truyền thông đại chúng, đặc biệt là các xuất bản phẩm, sản phẩm báo chí ở nước ngoài với nội dung chống phá và chuyển về phát tán trong nước. Chúng thường tài trợ cho một số cơ quan báo chí nước ngoài chuyên chống phá Việt Nam (VOA tiếng Việt, RFA, RFI, BBC...) để tuyên truyền xuyên tạc, nói xấu, bôi nhọ Đảng và Nhà nước Việt Nam. Thủ đoạn của chúng là lợi dụng những sơ hở, sai sót trong công tác quản lý, điều hành phương tiện truyền thông xã hội để phát tán thông tin chống phá, kích động bạo lực, biểu tình trái phép, gây bạo loạn chính trị hòng lật đổ chính quyền... Các thế lực thù địch, phản động thường sử dụng thủ đoạn tung tin giả (fake news) và xuyên tạc thông tin chính thống, nhất là trước các sự kiện trọng đại của đất nước hay các vụ việc thu hút sự quan tâm của đông đảo các tầng lớp nhân dân... Điển hình như: Vụ việc ở xã Đồng Tâm (huyện Mỹ Đức, Hà Nội), mặc dù đã được các cơ quan chức năng tích cực đối thoại, giải quyết thỏa đáng, song lợi dụng vấn đề này, các thế lực thù địch, phần tử cơ hội chính trị, phản động đã xuyên tạc, kích động người dân chống đối khiến vụ việc diễn biến ngày càng phức tạp, các đối tượng cố tình chống phá, gây rối trật tự công cộng, sử dụng vũ khí, chống người thi hành công vụ[5]. Ngoài ra, các thế lực thù địch, phản động thường tìm các lỗ hổng bảo mật để tấn công mạng bằng cách phát tán mã độc, đánh cắp thông tin cá nhân, phá hoại hạ tầng dữ liệu của các cơ quan, tổ chức trong nước. Không chỉ dừng lại ở đó, chúng còn mua chuộc, lôi kéo một số cá nhân bất mãn trong xã hội, lợi dụng sự thiếu hiểu biết hoặc tâm lý dễ bị kích động, biến họ thành công cụ phục vụ cho mục đích chống phá. Nhiều tài khoản giả mạo, trang web trá hình được chúng lập ra nhằm lan truyền luận điệu "đa nguyên, đa đảng", phủ nhận vai trò lãnh đạo của Đảng Cộng sản Việt Nam, gây hoang mang dư luận, chia rẽ nội bộ, từ đó dẫn đến cuộc chiến tâm lý trên không gian mạng hòng làm suy giảm lòng tin của Nhân dân vào chế độ.

Sự phát triển nhanh chóng của internet, công nghệ số và AI - nguy cơ đối với an ninh truyền thông

Thực tế cho thấy, sự phát triển bùng nổ của internet, đặc biệt là các nền tảng mạng xã hội đã mang đến nhiều cơ hội trên mọi lĩnh vực, ngành nghề, song với đặc tính mở, không có ranh giới giữa "thực" và "ảo" lại tiềm ẩn những rủi ro lớn về an ninh mạng.

Xu hướng phát triển nhanh chóng và mạnh mẽ của internet, mạng xã hội đã tạo ra "mảnh đất" màu mỡ cho các thế lực thù địch, phản động lợi dụng để chống phá Đảng, Nhà nước, phá hoại khối đại đoàn kết toàn dân tộc. Các thế lực thù địch, phản động triệt để sử dụng hệ thống thông tin để tác động, can thiệp nội bộ, hướng lái chính sách, thao túng dư luận, thúc đẩy "cách mạng màu". Chúng sử dụng không gian mạng để đăng tải nhiều thông tin tiêu cực, xấu độc... nhằm công kích, bôi nhọ lãnh đạo Đảng, Nhà nước, xuyên tạc chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước; đồng thời, bịa đặt, bóp méo sự thật về tình hình nội bộ Đảng đang bị chia rẽ nhằm bôi nhọ, hạ uy tín và gieo rắc nỗi hoài nghi về lập trường chính trị... Mặt khác, các thế lực thù địch, phản động thường sử dụng AI (ChatGPT, Midjourney, Deepfake...) để phát động các chiến dịch truyền thông chống phá cũng như thực hiện các cuộc tấn công mạng.

Theo ông Vũ Ngọc Sơn, Trưởng Ban Nghiên cứu, tư vấn, phát triển và hợp tác quốc tế - Hiệp hội An ninh mạng quốc gia: Trong năm 2024, các doanh nghiệp tại Việt Nam đã "hứng chịu" khoảng 659.000 cuộc tấn công mạng, chưa tính những vụ nhỏ lẻ không được báo cáo[6]. Theo số liệu thống kê, chỉ trong quý I-2025, Việt Nam đã ghi nhận hơn 257.000 cuộc tấn công từ chối dịch vụ (DDoS), phát hiện 36 lỗ hổng bảo mật nghiêm trọng, cùng với hơn 4,5 triệu tài khoản bị đánh cắp, chiếm 12,9% toàn cầu. Ngoài ra, có tới 911 tên miền độc hại, 746 trang web lừa đảo và 48 vụ rao bán dữ liệu, với tổng số 155 triệu bản ghi, dung lượng lên tới 24,65GB[7]... trên không gian mạng. Điều này cho thấy, mức độ phổ biến và nguy hiểm của các hình thức tấn công lừa đảo trên không gian mạng hiện nay là rất đáng báo động.

Thiếu tướng Lê Minh Mạnh, Phó Cục trưởng Cục An ninh mạng và phòng, chống tội phạm công nghệ cao - Bộ Công an (A05) đánh giá, Việt Nam là một trong những quốc gia đối mặt với nhiều thách thức trên không gian mạng. Tình hình tội phạm mạng diễn biến phức tạp, có tổ chức, hoạt động với tần suất ngày càng gia tăng cũng như quy mô ngày càng lớn[8]. Ví dụ điển hình như, trong vụ tấn công khủng bố tại Đắk Lắk ngày 11-6-2023, nhóm khủng bố đã nhận sự chỉ đạo và hậu thuẫn từ một số tổ chức phản động lưu vong ở nước ngoài, trong đó có tổ chức Fulro lưu vong nhằm thành lập "*Nhà nước Đề ga*", "*Hội những người miền núi*" (MFI), "*Nhân quyền người Thượng*" (MHRO), "*Người Thượng thống nhất*" (UMP)... Các thế lực thù địch, phản động đã lợi dụng các nền tảng trực tuyến để liên lạc, chỉ đạo và tuyển mộ thành viên; đồng thời, sử dụng mạng xã hội và các kênh truyền thông khác nhằm tuyên truyền, lôi kéo, kích động tư tưởng ly khai, tự trị[9]. Để thực hiện âm mưu này, một mặt, các đối tượng cầm đầu đã liên kết với các tổ chức phản động khác, kêu gọi sự ủng hộ từ một số tổ chức, cá nhân ở nước ngoài; mặt khác, lợi dụng các diễn đàn nhằm xuyên tạc, vu cáo Việt Nam vi phạm nhân quyền, quốc tế hóa vấn đề dân tộc thiểu số ở Tây Nguyên...

Các đối tượng thù địch, phản động đã khai thác triệt để tiện ích của không gian mạng để chống phá Đảng và Nhà nước Việt Nam với những thủ đoạn tinh vi, nguy hiểm như: Biến không thành có, biến ít thành nhiều, biến hiện tượng thành bản chất. Các quan điểm được lồng ghép trong các bài viết đa tầng thông tin, đa quan điểm, đánh tráo khái niệm, ngụy tuyên truyền nhằm lan truyền thông tin xấu, độc, sai sự thật.

Thực tế cho thấy, sự phát triển của công nghệ AI vẫn phụ thuộc vào các thuật toán, dữ liệu đầu vào do con người cung cấp, vì vậy, tiềm ẩn những tác động tiêu cực như: Nguy cơ mất an toàn thông tin, mất an ninh trật tự... Mặt khác, nguồn lực bảo đảm an ninh thông tin, cả về con người, tài chính và hạ tầng cơ sở kỹ thuật, công nghệ chưa đáp ứng yêu cầu trong tình hình mới. Hiệu lực, hiệu quả quản lý nhà nước về an ninh thông tin chưa cao; năng lực phát hiện, xử lý các hoạt động xâm hại an ninh thông tin, sự cố gây mất an ninh thông tin của các cơ quan, đơn vị còn hạn chế; ứng dụng khoa học kỹ thuật trong bảo đảm an ninh thông tin chưa đáp ứng được yêu cầu, đòi hỏi của tình hình mới...

Giải pháp phòng, chống các mối đe dọa an ninh truyền thông

Một là, hoàn thiện thể chế, chính sách. Trong bối cảnh các mối đe dọa an ninh truyền thông ngày càng đa dạng và phức tạp, việc rà soát, cập nhật và hoàn thiện hệ thống pháp luật là nhiệm vụ trọng tâm và cấp thiết. Trước hết, cần rà soát các văn bản quy phạm pháp luật hiện hành liên quan đến an ninh mạng, an ninh thông tin, hoạt động báo chí, truyền thông số và dữ liệu số nhằm phát hiện những bất cập, chồng chéo hoặc không còn phù hợp với thực tiễn.

Từng bước sửa đổi, bổ sung hoặc ban hành mới các văn bản pháp luật (Luật Báo chí, Luật Công nghệ thông tin...) theo hướng đồng bộ, hiện đại và hiệu quả. Tăng cường chế tài xử lý các hành vi vi phạm pháp luật trên không gian mạng, đặc biệt là hành vi phát tán tin giả, xuyên tạc, kích động, tấn công mạng hoặc khai thác dữ liệu trái phép. Việc nâng cao hiệu lực cưỡng chế pháp luật sẽ tạo sức răn đe; đồng thời, củng cố niềm tin của các tầng lớp nhân dân vào hệ thống pháp luật bảo đảm an ninh truyền thông quốc gia. Chú trọng nâng cao năng lực công nghệ số quốc gia như: Đầu tư vào hạ tầng kỹ thuật, công nghệ và nguồn nhân lực chất lượng cao về an toàn, an ninh thông tin...

Hai là, nâng cao nhận thức và trách nhiệm xã hội cho công chúng. Trong bối cảnh không gian mạng ngày càng trở thành môi trường chính để người dân tiếp nhận, chia sẻ và tương tác thông tin, việc nâng cao nhận thức và trách nhiệm xã hội cho công chúng là giải pháp then chốt để ngăn ngừa các mối đe dọa an ninh truyền thông.

Trước hết, cần triển khai rộng rãi các chiến dịch truyền thông giáo dục cộng đồng, thông qua nhiều hình thức như: Báo chí, mạng xã hội, truyền hình, nền tảng số... Các chiến dịch này cần tập trung truyền tải thông điệp rõ ràng, dễ tiếp cận, phù hợp với từng nhóm đối tượng mục tiêu để truyền thông cho đúng và trúng vấn đề. Nội dung tuyên truyền không chỉ dừng lại ở việc phòng, chống tin giả, mà còn giúp công chúng nhận thức đầy đủ về quyền và nghĩa vụ, ý thức, trách nhiệm khi chia sẻ thông tin trên mạng. Đặc biệt, cần trang bị kỹ năng số cơ bản như: Kỹ năng bảo mật tài khoản, quản lý thông tin cá nhân, xử lý tình huống truyền thông khủng hoảng và đặc biệt là kỹ năng phân biệt tin thật - giả…

Ngoài ra, cần lồng ghép các chuyên đề về "an ninh truyền thông" trong chương trình giáo dục phổ thông và đại học, đặc biệt đối với các ngành liên quan đến báo chí, công nghệ thông tin, luật, chính trị, xã hội... Việc nâng cao nhận thức cần được thực hiện đồng bộ với việc tạo lập các công cụ hỗ trợ tra cứu thông tin chính thống, phản ánh tin giả và báo cáo nội dung xấu độc, từ đó tạo dựng hệ sinh thái truyền thông an toàn, minh bạch và có trách nhiệm.

Ba là, phát triển nền tảng số nội địa an toàn. Một trong những thách thức lớn đối với an ninh truyền thông hiện nay là sự lệ thuộc quá mức vào các nền tảng số xuyên biên giới như: Facebook, YouTube, TikTok, X (Twitter)... khiến việc kiểm soát nội dung, xử lý vi phạm và bảo vệ chủ quyền số gặp nhiều khó khăn.

Để khắc phục tình trạng này, Việt Nam cần chủ động xây dựng và phát triển hệ sinh thái thông tin số quốc gia với sự tham gia tích cực của các doanh nghiệp công nghệ, các cơ quan báo chí, truyền thông và các tổ chức xã hội... Hệ sinh thái này bao gồm các nền tảng mạng xã hội nội địa, công cụ tìm kiếm, ứng dụng chia sẻ và hệ thống phân tích dữ liệu truyền thông. Đồng thời, đẩy mạnh đầu tư nghiên cứu và ứng dụng các công cụ quản lý số hiện đại, có khả năng rà quét, phân tích dữ liệu lớn (big data), theo dõi xu hướng dư luận, đánh giá mức độ lan tỏa, độ tin cậy và tác động của thông tin trên không gian mạng. Các công cụ này không chỉ cảnh báo sớm nguy cơ từ tin giả, nội dung xấu độc... mà còn giúp đo lường hiệu quả hoạt động truyền thông, từ đó điều chỉnh chính sách truyền thông một cách linh hoạt, kịp thời và có cơ sở dữ liệu thực chứng. Việc làm chủ công nghệ và dữ liệu sẽ giúp Việt Nam giảm thiểu phụ thuộc, tăng khả năng chủ động bảo đảm an ninh truyền thông quốc gia trong thời đại số.

Bốn là, đẩy mạnh hợp tác quốc tế một cách thiết thực, hiệu quả. Trên thực tế, an ninh mạng và truyền thông ngày càng mang tính xuyên biên giới, việc một quốc gia đơn độc ứng phó với các mối đe dọa là không hiệu quả. Do đó, Việt Nam cần chủ động, tích cực tham gia vào các diễn đàn đa phương và hiệp ước quốc tế liên quan đến an ninh mạng, quản trị không gian mạng, truyền thông toàn cầu và bảo vệ dữ liệu... Hoạt động này không chỉ giúp Việt Nam tiếp cận kịp thời với các xu hướng, công nghệ và quy chuẩn quốc tế, mà còn là cơ hội để đóng góp ý kiến, bảo vệ lợi ích quốc gia trên các diễn đàn toàn cầu. Cụ thể, Việt Nam cần phát huy vai trò trong các tổ chức như: Liên minh Viễn thông quốc tế (ITU), Hội nghị toàn cầu về Không gian mạng (GCCS)... Ngoài ra, thông qua hợp tác quốc tế, Việt Nam có thể tiếp nhận các mô hình quản trị không gian mạng tiên tiến; đồng thời, khẳng định vị thế quốc gia có trách nhiệm, sẵn sàng tham gia xây dựng không gian mạng toàn cầu ■

---

[1] Chính phủ, *Nghị quyết số 147/NQ-CP ngày 22-5-2025 ban hành Chiến lược tổng thể quốc gia phòng ngừa, ứng phó với các đe dọa an ninh phi truyền thống đến năm 2030, tầm nhìn đến năm 2045*.

[2] Xem: International Organization for Standardization, *ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements*, https://www.iso.org/standard/82875.html

[3] Xem: International Telecommunication Union, *Global Cybersecurity Index (GCI) 2018*, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf?utm

[4] Vũ Thị Hường, *Kiên quyết đấu tranh, bác bỏ các âm mưu, thủ đoạn, luận điệu sai trái phủ nhận vai trò lãnh đạo của Đảng Cộng sản Việt Nam, phủ nhận những thành quả cách mạng Việt Nam*, https://www.tapchicongsan.org.vn, ngày 14-9-2023.

[5] Xem: Lê Thế Cương, *Cảnh giác âm mưu, thủ đoạn lợi dụng vụ việc Đồng Tâm để kích động chống phá*, https://hvctcand.bocongan.gov.vn, ngày 13-1-2020.

[6, 7, 8] Xem: Bảo Lâm, *Nhân sự an ninh mạng Việt Nam thiếu 700.000 người*, https://vnexpress.net, ngày 24-5-2025.

[9] Xem: *Nhận diện, đấu tranh làm thất bại âm mưu của các tổ chức phản động FULRO lưu vong qua vụ khủng bố xảy ra ngày 11-6-2023 tại huyện Cư Kuin*, https://congan.daklak.gov.vn, ngày 31-7-2023.