

THAM LUẬN

Công tác đảm bảo an ninh mạng trên địa bàn tỉnh Quảng Bình

*Trung tá Trần Anh Tuấn
Trưởng Phòng PA05, Công an tỉnh*

Trong những năm qua, Quảng Bình đã chú trọng đẩy mạnh việc chuyển đổi số bao gồm xây dựng, phát triển chính quyền số, kinh tế số và xã hội số. Trong điều kiện kinh tế - xã hội của tỉnh còn rất nhiều khó khăn, nhất là bối cảnh đại dịch Covid-19 diễn biến phức tạp và ảnh hưởng nghiêm trọng nhưng cơ bản các nhiệm vụ trọng tâm đề ra tại Nghị quyết số 17/NQ-CP ngày 07/3/2019 của Chính phủ về một số nhiệm vụ, giải pháp trọng tâm phát triển Chính phủ điện tử giai đoạn 2019-2020, định hướng đến 2025; Kế hoạch số 262/KH-UBND ngày 01/3/2021 của UBND tỉnh về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước, phát triển chính quyền số và bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Quảng Bình đều đạt khá.

Nhìn chung, cơ sở hạ tầng kỹ thuật phục vụ công tác chuyển đổi số được xây dựng khá đồng bộ. Tại Quảng Bình, 100% sở ngành cấp tỉnh, UBND cấp huyện và UBND cấp xã đã thiết lập mạng LAN và kết nối Internet cho máy tính của cán bộ, công chức; Mạng diện rộng (WAN) của tỉnh được triển khai trên nền tảng Mạng truyền số liệu chuyên dùng đã kết nối đến 100% sở, ban ngành cấp tỉnh, UBND cấp huyện và 80% UBND cấp xã, tạo nền tảng cho chuyển đổi số tại địa phương.

Để phục vụ cho các hệ thống thông tin quan trọng của tỉnh, Trung tâm dữ liệu điện tử của tỉnh đặt tập trung tại Sở Thông tin và Truyền thông, được đầu tư xây dựng phần lõi của nền tảng tích hợp, chia sẻ dữ liệu cấp tỉnh LGSP, kết nối, chia sẻ dữ liệu giữa các hệ thống thông tin, cơ sở dữ liệu của tỉnh và liên thông với nền tảng dữ liệu quốc gia NGSP. Tại đây khai thác, ứng dụng 10 hệ thống thông tin, cơ sở dữ liệu dùng chung của tỉnh như dịch vụ công trực tuyến, phản ánh hiện trường, giám sát an toàn trật tự, an toàn giao thông, giám sát thông tin xấu, độc trên không gian mạng; quản lý, vận hành 01 Cổng thông tin điện tử tỉnh, hơn 200 trang thông tin điện tử của các cơ quan Đảng, Nhà nước trên địa bàn tỉnh. Ngoài ra, một số sở, ngành có đầu tư các hệ thống thông tin riêng phục vụ nhiệm vụ chuyên môn, chính trị của đơn vị mình.

Có thể nhận thấy, kinh tế số tại địa phương đã dần được hình thành, phát triển nhanh, ngày càng trở thành bộ phận quan trọng của nền kinh tế; công nghệ số được áp dụng trong các ngành công nghiệp, nông nghiệp và dịch vụ; xuất hiện ngày càng nhiều hình thức kinh doanh, dịch vụ mới dựa trên nền tảng công nghệ số và Internet đang tạo nhiều cơ hội việc làm, thu nhập, tiện ích, nâng cao chất lượng cuộc sống của người dân. Việc xây dựng chính quyền điện tử, tiến tới chính quyền số, đô thị thông minh và cải cách hành chính được triển khai quyết liệt, bước đầu đạt được nhiều kết quả tích cực.

Tuy nhiên, song song với sự tăng trưởng, phát triển xuất hiện một số nguy cơ làm mất an toàn, an ninh mạng trong thời kỳ chuyển đổi số, đó là:

Thứ nhất, hoạt động lợi dụng chuyển đổi số, nội dung số để thực hiện các hành vi phạm tội có chiều hướng gia tăng, diễn biến phức tạp trên địa bàn.

Chuyển đổi số giúp thu hẹp khoảng cách về không gian và thời gian, ngoài những lợi ích mang lại thì người dân cũng phải đối mặt với nhiều nguy cơ về tội phạm, tệ nạn xã hội được truyền tải bằng nhiều hình thức qua nội dung số. Thống kê cho thấy, tội phạm lừa đảo chiếm đoạt tài sản, đánh bạc và tổ chức đánh bạc, vi phạm bản quyền, sở hữu trí tuệ, buôn bán hàng giả, hàng cấm, truyền bá văn hóa phẩm đồi trụy và các hành vi vi phạm pháp luật khác... trong thời kỳ chuyển đổi số tại địa phương diễn biến phức tạp. Các đối tượng hoạt động phạm tội ngày càng tinh vi, sử dụng các thủ đoạn mới để che giấu hành vi phạm tội của mình, gây khó khăn cho lực lượng chức năng trong công tác quản lý, đấu tranh, phòng chống loại tội phạm này.

Thứ hai, chuyển đổi số là thành tựu nhưng cũng là thách thức trong công tác bảo vệ an ninh mạng trong tình hình hiện nay.

Chuyển đổi số làm xuất hiện một loại hình đối tượng mới cần bảo vệ an ninh, an toàn, đó là hệ thống thông tin. Trong thời gian qua, qua Trung tâm giám sát an toàn thông tin phát hiện nhiều đợt rà quét tấn công các hệ thống thông tin của các cơ quan, đơn vị, địa phương trên địa bàn tỉnh. Mặc dù chưa phát sinh vụ việc tấn công mạng quy mô lớn nhưng các đợt tấn công đã gây ảnh hưởng không nhỏ đến sự hoạt động ổn định của các hệ thống thông tin, cơ sở dữ liệu dùng chung của tỉnh. Trên địa bàn cũng ghi nhận tình trạng các máy tính bị nhiễm mã độc và trở thành máy tính ma trong hệ thống botnet khi bọn tội phạm kích hoạt các cuộc tấn công mạng có chủ đích nhắm vào hệ thống thông tin của cơ quan Đảng, Nhà nước.

Bên cạnh đó, nhiều hệ thống thông tin quan trọng của tỉnh do các cơ quan, đơn vị chuyên môn xây dựng, quản lý, vận hành còn tồn tại nhiều điểm yếu, lỗ hổng bảo mật trong tình trạng đáng báo động về bảo mật an toàn thông tin. Những lỗ hổng, điểm yếu bảo mật này dễ dẫn đến nguy cơ về an ninh mạng như: tấn công khai thác, sử dụng trái phép các cơ sở dữ liệu quan trọng của tỉnh, thay đổi giao diện hiển thị, chèn virus, mã độc để thực hiện tấn công mạng, thay đổi thông tin xấu, độc vào các cổng/trang thông tin chính thống của cơ quan Đảng, Nhà nước.

Thứ ba, tình trạng thông tin xấu, độc hại, thông tin giả truyền tải qua nội dung số diễn ra phổ biến trên không gian mạng.

Trong những năm qua, thông tin xấu, độc hại, thông tin giả truyền tải qua nội dung số bắt đầu xuất hiện phổ biến, lan truyền đến nhiều tầng lớp nhân dân trên địa bàn tỉnh. Một số bộ phận người dân nhận thức còn hạn chế, không kiểm chứng thông tin mà vô tư lan truyền, chia sẻ trên mạng xã hội. Bên cạnh đó, công tác quản lý về nội dung số gặp rất nhiều khó khăn, vướng mắc, đặc biệt nảy sinh nhiều vấn đề xuất phát từ hoạt động của các công ty công nghệ đa quốc gia khiến cho diễn biến tình hình trở nên phức tạp, gây hoang mang dư luận, ảnh hưởng trực tiếp đến an ninh trật tự, phát triển kinh tế, xã hội của địa phương.

Thứ tư, tình trạng lộ, mất dữ liệu cá nhân và mua, bán dữ liệu cá nhân trên không gian mạng diễn biến phức tạp trong quá trình chuyển đổi số.

Nguy cơ lộ, mất và tình trạng mua, bán dữ liệu cá nhân ngày càng gia tăng trong quá trình chuyển đổi số, trở thành một vấn đề đe dọa đối với quyền và lợi ích hợp pháp của cá nhân, tổ chức. Vấn nạn này có thể gây ra thiệt hại về tài chính, làm mất quyền riêng tư và ảnh hưởng đến danh tính của cá nhân, tổ chức trên môi trường không gian mạng. Những năm qua, lực lượng Công an đã phát hiện, triệt phá nhiều đường dây mua bán thông tin cá nhân với số lượng vô cùng lớn trên phạm vi cả nước, trong đó đã xuất hiện các hoạt động vi phạm pháp luật liên quan hoạt động mua, bán dữ liệu cá nhân trên địa bàn tỉnh Quảng Bình.

Nắm bắt được những nguy cơ trên, Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Công an tỉnh Quảng Bình đã chủ động triển khai các mặt công tác nghiệp vụ, tiến hành các biện pháp phòng ngừa vi phạm, tội phạm trong chuyển đổi nền kinh tế số và đảm bảo an ninh thông tin mạng đối với dịch vụ nội dung số tại Việt Nam, cụ thể là:

- *Thực hiện công tác tham mưu, hướng dẫn, phối hợp kịp thời, có hiệu quả:* Tham mưu cho Tỉnh ủy, UBND tỉnh nhiều nội dung quan trọng, nổi bật là tham mưu thành lập Tiểu ban An toàn, an ninh mạng tỉnh Quảng Bình thống nhất chỉ đạo công tác bảo đảm an toàn, an ninh mạng trên địa bàn toàn tỉnh. Trên cơ sở đó, xây dựng các nội dung, chương trình công tác, phân công nhiệm vụ cụ thể cho các cơ quan có liên quan để thực hiện có hiệu quả công tác phòng ngừa tội phạm, các hành vi vi phạm pháp luật và bảo đảm an ninh thông tin mạng trong quá trình chuyển đổi số tại địa phương.

- *Tổ chức công tác nắm tình hình trên không gian mạng, đấu tranh có hiệu quả với tội phạm mạng:* Triển khai các biện pháp nghiệp vụ, các hoạt động trinh sát trên không gian mạng kết hợp với công tác nắm tình hình theo tuyến, lĩnh vực, địa bàn để nắm chắc tình hình hoạt động của các đối tượng trọng điểm, các loại tội phạm mạng và các hành vi vi phạm pháp luật trên địa bàn tỉnh. Từ năm 2021 đến nay, Phòng PA05 đã chủ trì, phối hợp với các đơn vị nghiệp vụ, Công an các địa phương đấu tranh thành công, khởi tố 33 vụ/97 bị can liên quan đến các hành vi phạm tội sử dụng công nghệ cao như lừa đảo chiếm đoạt tài sản, đánh bạc và tổ chức đánh bạc, “tín dụng đen”, mua bán, công khai hóa tài khoản ngân hàng... trên không gian mạng. Nổi bật, Phòng PA05 đã chủ trì các chuyên án lớn đấu tranh với nhiều đường dây, ổ nhóm tội phạm công nghệ cao với nhiều phương thức, thủ đoạn mới, hoạt động có tổ chức, có tính chất liên tỉnh, xuyên quốc gia được các cấp lãnh đạo Bộ Công an, Tỉnh ủy, UBND tỉnh và quần chúng Nhân dân ghi nhận, đánh giá cao.

- *Tổ chức rà quét, phát hiện lỗ hổng bảo mật, bảo vệ an toàn thông tin:* Thường xuyên theo dõi hoạt động hệ thống thông tin của các cơ quan Đảng, Nhà nước; các tổ chức chính trị; báo, đài của Đảng, Nhà nước; các tập đoàn kinh tế, doanh nghiệp nhà nước đóng tại địa phương để phòng ngừa, phát hiện các lỗ hổng, điểm yếu bảo mật, tình trạng lộ, mất BMNN trên không gian mạng và các hành vi vi phạm pháp luật khác. Đã rà soát, phát hiện và hướng dẫn xử lý đối với 7.104 điểm yếu, lỗ hổng bảo mật tại các cổng, trang thông tin điện tử, phần mềm phục vụ công tác chuyên môn thuộc hệ thống thông tin của các cơ quan Đảng, Nhà nước; tham mưu xử lý 02 vụ việc liên quan đăng tải tài liệu thuộc bí mật nhà nước, tài liệu mang nội dung không đăng tải trên các phương tiện thông tin đại chúng.

- *Tăng cường phối hợp với các đơn vị có liên quan; Tuyên truyền, nâng cao nhận thức bảo vệ an ninh mạng trong thời kỳ chuyển đổi số:* Tham mưu cho

Công an tỉnh xây dựng và ban hành nhiều quy chế phối hợp giữa Công an tỉnh với các cơ quan có liên quan nhằm nâng cao hiệu quả trong công tác phòng ngừa tội phạm, các hành vi vi phạm pháp luật và bảo đảm an ninh thông tin mạng trong quá trình chuyển đổi số tại địa phương. Công tác tuyên truyền và phát động phong trào toàn dân bảo vệ an ninh Tổ quốc trên không gian mạng được thực hiện trên tinh thần đổi mới, ứng dụng các thành tựu của khoa học - công nghệ, gắn với nhiệm vụ xây dựng thế trận An ninh nhân dân trên không gian mạng tại địa bàn tỉnh, nâng cao sức đề kháng của quần chúng nhân dân trước tác động của các nguy cơ xấu trong thời kỳ chuyển đổi số.

Để nâng cao hiệu quả công tác phòng ngừa vi phạm, tội phạm trong chuyển đổi nền kinh tế số và đảm bảo an ninh thông tin mạng đối với dịch vụ nội dung số tại Việt Nam nói chung và tại Quảng Bình nói riêng, chúng tôi đề ra một số giải pháp và kiến nghị sau:

Một là, tiếp tục hoàn thiện cơ chế, chính sách, pháp luật liên quan đến chuyển đổi số, nội dung số như sửa đổi, bổ sung Luật Viễn thông, Luật Công nghệ thông tin, ban hành Nghị định quy định xử lý vi phạm hành chính trên lĩnh vực An ninh mạng và các văn bản pháp luật khác... Đây là hành lang pháp lý quan trọng để tổ chức có hiệu quả công tác bảo đảm an ninh thông tin mạng đối với dịch vụ nội dung số. Trên cơ sở hoàn thiện hệ thống pháp luật, tăng cường các chế tài xử lý các hành vi vi phạm pháp luật trên không gian mạng đủ sức răn đe, thể hiện tính nghiêm minh của pháp luật đối với lĩnh vực này.

Hai là, tăng cường phát triển hạ tầng kỹ thuật phục vụ công tác bảo đảm an ninh, an toàn thông tin trong thời kỳ chuyển đổi số. Trong đó quan tâm đầu tư, xây dựng phát triển nền tảng số phục vụ chuyển đổi số, triển khai hệ thống giám sát an toàn thông tin, cảnh báo nguy cơ, điều phối ứng cứu sự cố an toàn, an ninh mạng đối với hệ thống thông tin của chính quyền điện tử, đô thị thông minh...

Ba là, đẩy mạnh công tác công an, kịp thời phát hiện sớm âm mưu, phương thức, thủ đoạn hoạt động của các thế lực thù địch và các loại tội phạm trong thời kỳ chuyển đổi số. Tiếp tục xây dựng lực lượng chính quy, tinh nhuệ, bản lĩnh chính trị vững vàng, đầu tư trang thiết bị hiện đại, cơ sở hạ tầng tốt nhất, đáp ứng được yêu cầu nhiệm vụ đảm bảo an ninh mạng, phát hiện và điều tra tội phạm mạng, bảo vệ an toàn các mục tiêu.

Bốn là, nâng cao năng lực và trách nhiệm các cơ quan Đảng, Nhà nước; các tổ chức chính trị; báo, đài của Đảng, Nhà nước; các tập đoàn kinh tế, doanh

nghiệp nhà nước trong thực hiện công tác bảo vệ an toàn, an ninh mạng. Chủ động thực hiện các biện pháp bảo vệ an toàn, an ninh mạng trong thời kỳ chuyển đổi số như hoàn thiện quy chế làm việc nội bộ; quy định an toàn, an ninh mạng nghiêm ngặt; thường xuyên rà soát hệ thống thông tin để phát hiện lỗ hổng bảo mật; cập nhật các bản vá lỗi cho hệ điều hành và các ứng dụng trên máy chủ; bảo vệ dữ liệu cá nhân thu thập được thông qua các hoạt động chuyên môn, nghiệp vụ...

Năm là, thực hiện tuyên truyền nâng cao nhận thức, ý thức bảo đảm an toàn, an ninh mạng cho các cán bộ, đảng viên và quần chúng nhân dân, nhất là thế hệ trẻ trên địa bàn. Xây dựng phong trào toàn dân bảo vệ an ninh Tổ quốc theo hướng thay đổi cách thức, phương pháp tiếp cận và triển khai thực hiện. Trong đó, cần chú ý đẩy mạnh ứng dụng thành tựu khoa học - công nghệ, tính lan truyền mạnh mẽ của mạng Internet và báo chí điện tử, tâm lý quần chúng nhân dân để tuyên truyền một cách chủ động với trạng thái cao nhất là xây dựng thành công thế trận An ninh nhân dân trên không gian mạng./.
