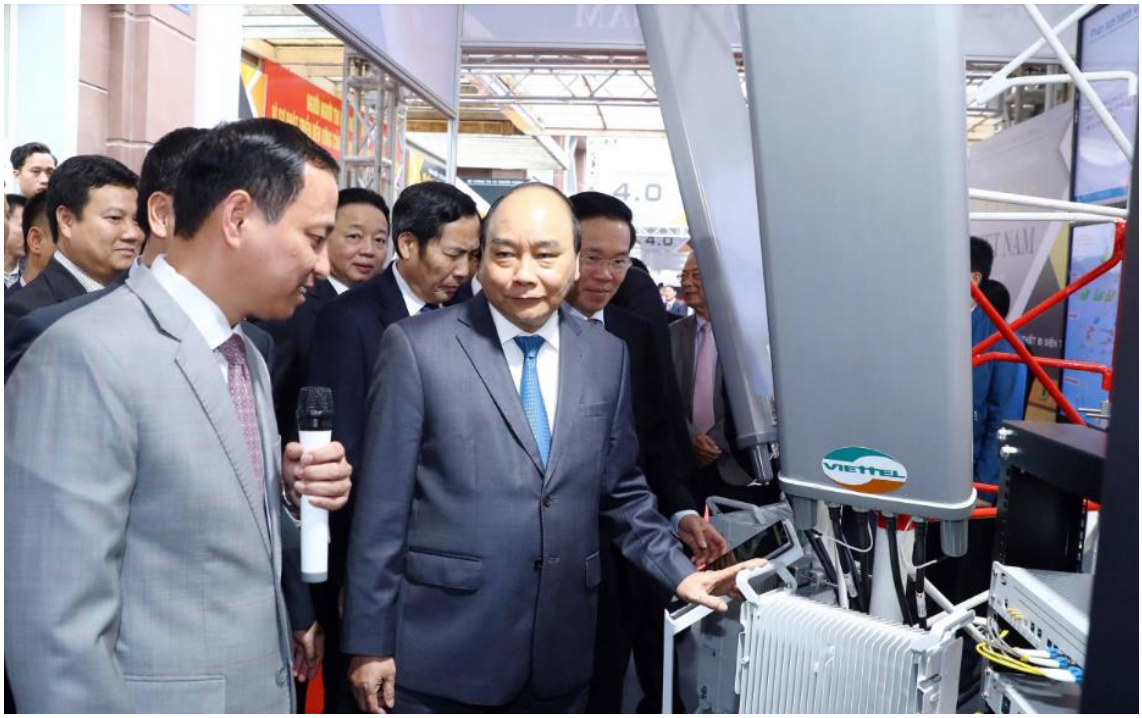
Bảo đảm an ninh mạng trong tình hình mới

GS, TS. TÔ LÂM
Đại tướng, Ủy viên Bộ Chính trị, Bộ trưởng Bộ Công an

10:23, ngày 10-08-2020 http://tapchicongsan.org.vn/web/guest/tin-tieu-diem/-/asset_publisher/s5L7xhQiJeKe/content/bao-dam-an-ninh-mang-trong-tinh-hinh-moi

TCCS - Thế giới bước vào cuộc Cách mạng công nghiệp lần thứ tư với sự phát triển mạnh mẽ của không gian mạng. Bên cạnh những lợi ích to lớn không thể phủ nhận, cách mạng số, không gian mạng kết nối toàn cầu với đặc tính không biên giới cũng đặt ra nhiều thách thức rất lớn đối với an ninh của các quốc gia trên thế giới, khiến cho an ninh mạng không còn là vấn đề của riêng một quốc gia, mà đã trở thành vấn đề toàn cầu. Chính vì vậy, bảo đảm an ninh mạng đang là ưu tiên hàng đầu được thể hiện rõ trong các quan điểm, chiến lược và hành động cụ thể của các quốc gia, trong đó có Việt Nam.



Bảo đảm an ninh mạng đang là ưu tiên hàng đầu của các quốc gia, trong đó có Việt Nam (Trong ảnh: Ủy viên Bộ Chính trị, Thủ tướng Chính phủ Nguyễn Xuân Phúc tham quan triển lãm công nghệ số) _Ảnh: TTXVN

Bảo đảm an ninh mạng là vấn đề toàn cầu

Với sự phát triển mạnh mẽ của không gian mạng, ngày nay, mọi hoạt động diễn ra trong thế giới thực đều có sự hỗ trợ đắc lực của các thiết bị thông minh; sự kết hợp giữa hệ thống ảo và thực thể đã làm thay đổi cách thức con người tiến hành công việc, tạo ra sản phẩm, từ đó tạo nên "cuộc cách mạng" về tổ chức các chuỗi sản xuất - giá trị, thúc đẩy phát triển kinh tế - xã hội. Bên cạnh những lợi

ích thiết thực, sự phát triển mạnh mẽ của không gian mạng cũng đặt ra những thách thức to lớn cho vấn đề bảo đảm an ninh mạng. Ngày 1-4-2015, Đại hội đồng liên minh Nghị viện thế giới lần thứ 132 đã thông qua Nghị quyết về "Chiến tranh mạng: mối đe dọa nghiêm trọng đến hòa bình và an ninh toàn cầu". Tháng 9-2019, trong khuôn khổ kỳ họp thứ 74 Đại hội đồng Liên hợp quốc ở Niu Oóc (Mỹ), 20 quốc gia đã ký thỏa thuận ngăn chặn lan truyền tin giả trực tuyến. Đây là những tiếng nói chung của cộng đồng quốc tế, là cơ sở để tiến tới xây dựng một điều ước quốc tế về bảo đảm an ninh mạng và phòng, chống tội phạm công nghệ cao.

Các chiến dịch tấn công mạng quy mô lớn nhằm vào hạ tầng công nghệ thông tin trọng yếu của các quốc gia..., gián điệp mạng, khủng bố mạng, kêu gọi tài trợ khủng bố, tội phạm mạng, tán phát tin giả liên tục diễn ra, gây ra những hậu quả khôn lường. Trên cương vị Tổng thống Mỹ, ông Ba-rắc Ô-ba-ma từng thừa nhận: "Đe dọa về an ninh mạng trở thành một trong các thách thức về kinh tế và an ninh quốc gia nguy hiểm nhất đối với nước Mỹ"(1). Bộ Quốc phòng Mỹ đã chính thức công nhận không gian mạng là một lãnh thổ mới, có tầm quan trọng ngang với các lãnh thổ khác trong chiến tranh, như trên đất liền, trên biển, trên không và trong không gian(2). Tổng thống Mỹ Đô-nan Trăm xác định, phát triển chiến lược an ninh mạng mới toàn diện hơn là một trong bốn ưu tiên hàng đầu của nước Mỹ và ban hành sắc lệnh an ninh mạng ngay trong 100 ngày cầm quyền đầu tiên.

Ở Nga, Tổng thống Nga Vla-đi-mia Pu-tin cho rằng, "Trong điều kiện hiện nay, "sức sát thương" của các cuộc tấn công thông tin có thể cao hơn bất kỳ loại vũ khí thông thường nào"(3) và ban hành học thuyết an ninh mạng mới vào ngày 5-12-2016. Nhằm bảo đảm hệ thống in-tơ-nét nội bộ của Nga hoạt động ổn định cả trong trường hợp nước này bị ngắt kết nối với kết cấu hạ tầng in-tơ-nét toàn cầu, Tổng thống Nga V. Pu-tin đã ký ban hành Luật In-tơ-nét 2019. Ngay sau khi Luật có hiệu lực, ngày 23-12-2019, Nga tiến hành thử nghiệm về độ tin cậy của kết cấu hạ tầng in-tơ-nét nội địa trong tình huống nước này bị ngắt in-tơ-nét trên toàn thế giới do bị tấn công mạng.

Với Trung Quốc, không gian mạng được coi là chiến trường thứ năm và là mặt trận tình báo mới. Chủ tịch Trung Quốc Tập Cận Bình khẳng định, "Không thể có an ninh quốc gia nếu không có an ninh mạng, in-tơ-nét và an ninh thông tin đã trở thành thách thức mới đối với Trung Quốc vì cả hai đều gắn liền với an ninh quốc gia và ổn định xã hội"(4). Bộ Quốc phòng Trung Quốc cũng xác định, "không gian mạng đã trở thành một trụ cột mới cho phát triển kinh tế - xã hội"(5). Để đáp ứng yêu cầu của công tác bảo đảm an ninh mạng, Trung Quốc liên tục có những thay đổi, bổ sung trong xây dựng, tạo lập chính sách và hành lang pháp lý cho lĩnh vực công tác này. Tháng 5-2019, Trung Quốc công bố dự thảo Luật An ninh mạng mới thay thế Luật An ninh mạng có hiệu lực từ tháng 6-2017. Đồng thời, ban hành quy định về "Phương pháp đánh giá an ninh mạng", gồm hệ thống các tiêu chí đánh giá về an ninh mạng và mức độ tin cậy của chuỗi cung ứng cho kết cấu hạ tầng thông tin quan trọng của đất nước; theo

đó, các hoạt động mua sắm sản phẩm, dịch vụ an ninh mạng phục vụ hạ tầng mạng quan trọng phải được đánh giá về an ninh mạng và chỉ được thực hiện sau khi vượt qua các đánh giá về an ninh mạng.

Bảo đảm an ninh mạng tại Việt Nam

Những năm qua, Đảng, Nhà nước ta đã có nhiều chủ trương, chính sách đẩy mạnh ứng dụng, phát triển công nghệ thông tin phục vụ nhiệm vụ phát triển kinh tế - xã hội, bảo đảm quốc phòng, an ninh và đã đạt được nhiều thành tựu rất quan trọng. Nhiều chính sách, pháp luật được ban hành nhằm thúc đẩy ứng dụng công nghệ thông tin vào phát triển kinh tế - xã hội, đồng thời bảo đảm an ninh mạng. Trong đó, nổi bật là Nghị quyết số 52-NQ/TW, ngày 27-9-2019, của Bộ Chính trị, "Về một số chủ trương, chính sách chủ động tham gia cuộc cách mạng công nghiệp lần thứ tư", Luật An ninh mạng, Luật An toàn thông tin mạng, Luật Bảo vệ bí mật nhà nước và các văn bản hướng dẫn thi hành... Kết cấu hạ tầng viễn thông ở nước ta được xây dựng khá đồng bộ; kinh tế số được hình thành và phát triển nhanh, ngày càng trở thành bộ phận quan trọng của nền kinh tế. Công nghệ số được áp dụng ở hầu hết các ngành; xuất hiện ngày càng nhiều hình thức kinh doanh, dịch vụ mới xuyên quốc gia, dựa trên nền tảng công nghệ số và in-tơ-nét. Việc triển khai chính phủ điện tử được thực hiện quyết liệt, đã đưa vào sử dụng hệ thống e-Ca-bi-net phục vụ các kỳ họp của Chính phủ, hệ thống Trục liên thông văn bản quốc gia. Năm 2019, chỉ số ứng dụng công nghệ thông tin, truyền thông của Việt Nam đã tăng từ hạng 95 (năm 2018) lên hạng 41 trên thế giới.

Tuy nhiên, bên cạnh những thuận lợi, nước ta cũng đang phải đối mặt với nhiều thách thức đối với an ninh quốc gia, trật tự, an toàn xã hội đến từ không gian mạng, nổi lên là:

Thứ nhất, hoạt động sử dụng không gian mạng để tuyên truyền phá hoại tư tưởng, chống Đảng, Nhà nước, kích động tập trung đông người gây rối an ninh, trật tự. Thời gian qua, phát hiện trên 3.000 trang web, blog, tài khoản mạng xã hội và gần 100 hội, nhóm trên mạng xã hội facebook thường xuyên đăng tải thông tin chống Đảng, Nhà nước, kích động gây rối an ninh, trật tự. Trong thời gian dịch bệnh Covid-19 bùng phát, không gian mạng tiếp tục là môi trường chủ yếu để các thế lực thù địch, đối tượng phản động, chống đối phát tán thông tin bịa đặt về tình hình dịch bệnh, xuyên tạc, đả kích sự chỉ đạo, điều hành trong phòng, chống dịch bệnh của Chính phủ và chính quyền các cấp; kích động, chia rẽ quan hệ đối ngoại của Việt Nam với một số nước; kích động công nhân đình công tập thể tại các công ty, khu công nghiệp có yếu tố nước ngoài. Càng gần đến Đại hội XIII của Đảng, hoạt động chống phá của các thế lực thù địch càng diễn ra quyết liệt, thông qua hàng trăm trang web và hàng nghìn nhóm, tài khoản mạng xã hội để tán phát thông tin xuyên tạc, đả kích lãnh đạo Đảng, Nhà nước; xuyên tạc, bịa đặt về công tác nhân sự Đại hội XIII của Đảng.

Thứ hai, hoạt động gián điệp mạng, tình trạng lộ bí mật nhà nước trên không gian mạng diễn biến ngày càng phức tạp. Chỉ tính riêng năm 2019, đã phát hiện hàng trăm trang web tên miền quốc gia bị tấn công; 127 trang và 349

cổng thông tin điện tử của nhiều cơ quan, đơn vị tồn tại các lỗ hổng bảo mật nghiêm trọng; 40 vụ lộ bí mật nhà nước qua in-tơ-nét với 241 đầu tài liệu. Đáng chú ý, tin tặc gia tăng tấn công mạng vào các cơ quan trọng yếu và các tập đoàn kinh tế lớn để thu thập, chiếm đoạt thông tin, tài liệu bí mật nhà nước. Các đối tượng này duy trì chiến dịch tấn công liên tục với các kỹ thuật tấn công mới, nâng cấp các dòng mã độc, bám sát tình hình chính trị, xã hội ở nước ta để thay đổi thủ đoạn tán phát mã độc cho đến khi xâm nhập thành công. Điển hình như, trong khi dịch bệnh Covid-19 diễn biến phức tạp, phòng, chống dịch bệnh là mối quan tâm chung của cả cộng đồng, tin tặc đã tán phát mã độc đính kèm thư điện tử giả mạo Chỉ thị của Thủ tướng Chính phủ về phòng, chống dịch Covid-19 nhằm đánh lừa người dùng nhấn mở tệp để lây nhiễm mã độc và đánh cắp thông tin, dữ liệu trên máy tính người dùng, đặc biệt là thông tin của Chính phủ, các bộ, ban, ngành.

Nước ta đang phải đối mặt với nhiều thách thức đối với an ninh quốc gia, trật tự, an toàn xã hội đến từ không gian mạng. _Ảnh minh họa

Thứ ba, sử dụng không gian mạng để thực hiện các hành vi phạm tội gia tăng cả về số vụ, tính chất, mức độ nghiêm trọng và bằng nhiều phương thức, thủ đoạn tinh vi, khiến nhiều nạn nhân bị chiếm đoạt số tiền rất lớn. Đặc biệt, thủ đoạn mạo danh các cơ quan thực thi pháp luật như công an, viện kiểm sát, tòa án gọi điện yêu cầu nạn nhân "cung cấp thông tin hỗ trợ điều tra" để đánh cắp thông tin tài khoản và chiếm đoạt tài sản xảy ra ở nhiều địa phương, chiếm đoạt tổng số tiền lên đến hàng trăm tỷ đồng. Tội phạm tổ chức đánh bạc, cá độ bóng đá trên mạng chủ yếu do các "nhà cái" ở nước ngoài móc nối với các đối tượng trong nước hình thành các đường dây, thiết lập hàng nghìn trang web, tên miền, ước tính sử dụng hàng triệu đô-la Mỹ mỗi ngày. Các trò chơi đổi thưởng, đánh bạc trá hình, hoạt động kinh doanh đa cấp biến tướng lừa đảo tiếp tục diễn

biến phức tạp. Hoạt động "tín dụng đen" trên mạng xuất hiện hình thức mới (cho vay ngang hàng - P2P Lending), tiềm ẩn nguy cơ bị lợi dụng để thực hiện đánh bạc qua mạng, lừa đảo, trốn thuế, rửa tiền, tài trợ cho tổ chức khủng bố hoặc huy động tài chính đa cấp. Tội phạm người nước ngoài sử dụng công nghệ cao có chiều hướng dịch chuyển mạnh địa bàn hoạt động sang Việt Nam, tập trung chủ yếu tại các thành phố lớn, khu du lịch. Tội phạm có tổ chức hoạt động trong lĩnh vực thương mại điện tử, thanh toán thẻ, thanh toán điện tử, tài chính, ngân hàng tiếp tục gia tăng. Xuất hiện nhiều đường dây mua bán vũ khí, công cụ hỗ trợ, các thiết bị nghe lén, định vị ngụy trang trên in-tơ-nét.

Trước tình hình trên, Bộ Công an đã tham mưu với Đảng, Nhà nước ban hành, triển khai thực hiện nhiều chủ trương, chính sách, pháp luật và các giải pháp kịp thời về bảo đảm an ninh mạng, nhất là khẩn trương xây dựng, đề xuất ban hành các văn bản hướng dẫn thi hành Luật An ninh mạng, các quy định về bảo vệ dữ liệu cá nhân, xử phạt vi phạm hành chính; đồng thời, tiếp tục rà soát những vấn đề mới đang đặt ra trong cuộc Cách mạng công nghiệp lần thứ tư để đề xuất hoàn thiện hệ thống chính sách, pháp luật. Mở rộng hợp tác quốc tế trên lĩnh vực an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao với các quốc gia, tập đoàn công nghệ lớn trên thế giới để tiếp thu công nghệ, học hỏi kinh nghiệm, đào tạo nguồn nhân lực và hợp tác đấu tranh phòng, chống tội phạm mạng. Chủ động phối hợp chặt chẽ với các bộ, ban, ngành, địa phương triển khai các giải pháp bảo vệ an ninh hệ thống mạng thông tin trọng yếu quốc gia, phòng, chống tấn công mạng; đấu tranh, phản bác kịp thời các quan điểm thù địch, sai trái trên không gian mạng; xử lý nghiêm các đối tượng có hành vi vi phạm pháp luật về quản lý, cung cấp, sử dụng in-tơ-nét và thông tin trên mạng. Chỉ trong 5 tháng đầu năm 2020, Bộ Công an đã điều tra, đề nghị xử lý hình sự 81 đối tượng, xử phạt vi phạm hành chính 353 trường hợp có hành vi tán phát thông tin sai sự thật trên không gian mạng. Vì vậy, thông tin sai sự thật trên không gian mạng đã giảm hẳn và hầu hết các tài khoản mạng xã hội trong nước đã chủ động gỡ bỏ thông tin sai sự thật. Trong đấu tranh phòng, chống tội phạm trên không gian mạng, trong năm 2019, Bộ Công an đã khởi tố 10 vụ với 116 bị can; bắt giữ và bàn giao cảnh sát các nước 555 đối tượng; phối hợp xử phạt hành chính và trục xuất 254 đối tượng.

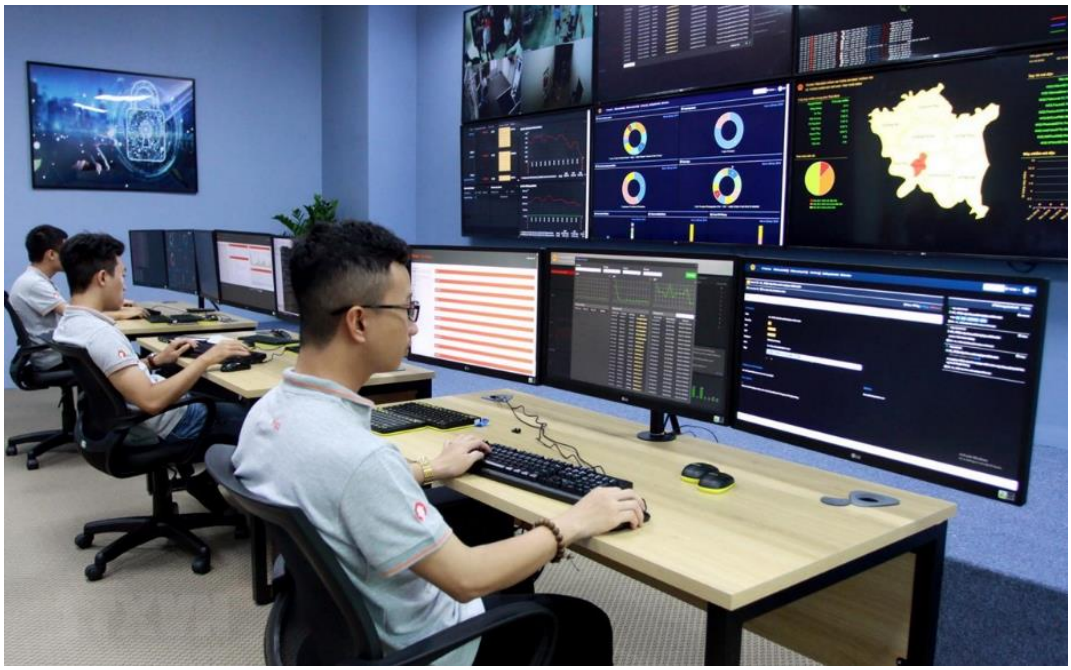
Giải pháp bảo đảm an ninh mạng thời gian tới

Thời gian tới, tình hình an ninh mạng sẽ tiếp tục có nhiều diễn biến phức tạp, không gian mạng tiếp tục là mục tiêu trọng yếu của các cuộc tấn công, là môi trường chủ yếu để tiến hành các hoạt động gián điệp, khủng bố, phá hoại, thực hiện các hành vi phạm tội; đặc biệt là tuyên truyền xuyên tạc, kích động chống Đảng, Nhà nước, nhất là từ nay đến Đại hội XIII của Đảng. Chủ động, tích cực tham gia cuộc Cách mạng công nghiệp lần thứ tư là yêu cầu tất yếu khách quan nhằm mang lại cơ hội cho phát triển kinh tế - xã hội, đồng thời đối phó có hiệu quả với những thách thức đối với an ninh của đất nước. Để nắm bắt kịp thời cơ hội và phòng ngừa, ứng phó, hạn chế tác động tiêu cực đối với an ninh đất nước từ không gian mạng, cần triển khai một số nhiệm vụ cấp bách sau:

Một là, tiếp tục tăng cường sự lãnh đạo của các cấp ủy đối với công tác bảo đảm an ninh mạng. Tập trung triển khai có hiệu quả các chủ trương, chỉ thị, nghị quyết của Đảng về ứng dụng, phát triển công nghệ thông tin đi đôi với bảo đảm an toàn thông tin, an ninh mạng, trọng tâm là Nghị quyết số 52-NQ/TW, ngày 27-9-2019, của Bộ Chính trị, "Về một số chủ trương, chính sách chủ động tham gia cuộc Cách mạng công nghiệp lần thứ tư", các chủ trương về bảo vệ Tổ quốc trên không gian mạng, bảo vệ an ninh mạng quốc gia nhằm nâng cao tiềm lực khoa học, công nghệ cũng như năng lực bảo đảm an ninh mạng, phòng, chống chiến tranh mạng.

Hai là, hoàn thiện chính sách, pháp luật và nâng cao hiệu lực, hiệu quả quản lý nhà nước về thông tin, truyền thông và an ninh mạng. Tổ chức thực hiện nghiêm Luật An toàn thông tin mạng, Luật An ninh mạng, Luật Bảo vệ bí mật nhà nước và các văn bản hướng dẫn thi hành; quản lý chặt chẽ các loại hình dịch vụ viễn thông, in-tơ-nét ở Việt Nam. Khẩn trương tham mưu cho Chính phủ xây dựng, ban hành Nghị định quy định chi tiết một số điều của Luật An ninh mạng, Nghị định quy định xử phạt vi phạm hành chính trong lĩnh vực an ninh mạng, Nghị định bảo vệ dữ liệu cá nhân. Tham khảo chính sách, pháp luật về an ninh mạng của các nước, đồng thời nghiên cứu, rà soát, phát hiện những bất cập trong chính sách, pháp luật của nước ta, những vấn đề mới đang đặt ra trong thực tiễn chưa được điều chỉnh bằng chính sách, pháp luật để tham mưu, đề xuất ban hành các chính sách, pháp luật về quản lý "tiền ảo", "tài sản ảo", dịch vụ trung gian thanh toán, chứng cứ điện tử, các rô-bốt trang bị trí tuệ nhân tạo,...

Ba là, xây dựng, hoàn thiện cơ chế phối hợp giữa Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông, Ban Tuyên giáo Trung ương và các bộ, ban, ngành, địa phương trong bảo đảm an ninh mạng. Tổ chức phổ biến, tập huấn để nâng cao nhận thức và năng lực bảo vệ an ninh mạng cho các tổ chức, cá nhân, trước hết là cán bộ lãnh đạo, cán bộ chuyên trách quản lý và vận hành hệ thống thông tin quan trọng về an ninh quốc gia. Nghiên cứu xây dựng mô hình hợp tác công - tư trong bảo đảm an ninh, phòng, chống tội phạm trên không gian mạng ở Việt Nam, tạo cơ chế phối hợp chặt chẽ giữa các cơ quan nhà nước với các doanh nghiệp nhằm khai thác tối đa nguồn lực xã hội trong hoạt động này. Tăng cường tuyên truyền, phổ biến, nâng cao nhận thức, cảnh giác của người dân trong phòng ngừa tội phạm và vi phạm pháp luật về an ninh mạng.



Quang cảnh Trung tâm điều hành an ninh mạng tỉnh Thái Bình _Nguồn: vietnamplus.vn

Bốn là, tiếp tục tăng cường thực hiện các giải pháp bảo đảm an ninh mạng và đấu tranh phòng, chống tội phạm trên không gian mạng. Triển khai đồng bộ các giải pháp để bảo đảm an ninh mạng cho hệ thống thông tin quan trọng về an ninh quốc gia; phát hiện, đấu tranh ngăn chặn sớm hoạt động tấn công mạng, gián điệp mạng, âm mưu, hoạt động chống phá của các thế lực thù địch, phản động trên mạng. Chủ động phòng ngừa và quyết liệt tấn công, trấn áp mạnh tội phạm mạng, nhất là những loại tội phạm diễn ra phổ biến thời gian qua, như tội phạm tổ chức đánh bạc, lừa đảo chiếm đoạt tài sản, tội phạm do người nước ngoài thực hiện...; kịp thời giải quyết các vấn đề phức tạp nổi lên về an ninh, trật tự trên không gian mạng.

Năm là, đẩy mạnh nghiên cứu, phát triển công nghệ thông tin, nhằm tự chủ về công nghệ và trang thiết bị, không để bị lệ thuộc vào nước ngoài. Có lộ trình phát triển các doanh nghiệp công nghệ thông tin và an ninh mạng, trong đó, lựa chọn các lĩnh vực mà Việt Nam có thế mạnh để ưu tiên phát triển. Hoàn thiện các chính sách nhằm khuyến khích, huy động mọi nguồn lực xã hội trong nghiên cứu khoa học, phát triển và ứng dụng công nghệ thông tin và an ninh mạng. Nghiên cứu các mô hình đổi mới, sáng tạo có hiệu quả trên thế giới để vận dụng phù hợp với điều kiện của Việt Nam nhằm khuyến khích các doanh nghiệp đầu tư, nghiên cứu, phát triển các sản phẩm công nghệ bảo đảm an ninh mạng.

Sáu là, chú trọng đào tạo, phát triển và thu hút nguồn nhân lực chất lượng cao về công nghệ thông tin và an ninh mạng làm việc trong các cơ quan, doanh nghiệp của Việt Nam, không để tình trạng "chảy máu chất xám" về công nghệ thông tin. Nâng cao chất lượng đào tạo về công nghệ thông tin và an ninh mạng tại các cơ sở đào tạo trong nước, đồng thời đẩy mạnh hợp tác với các quốc gia, các trường đại học, các tập đoàn công nghệ tiên tiến trên thế giới để tiếp thu

công nghệ mới và kinh nghiệm bảo đảm an ninh mạng nhằm đáp ứng yêu cầu của tình hình mới./.