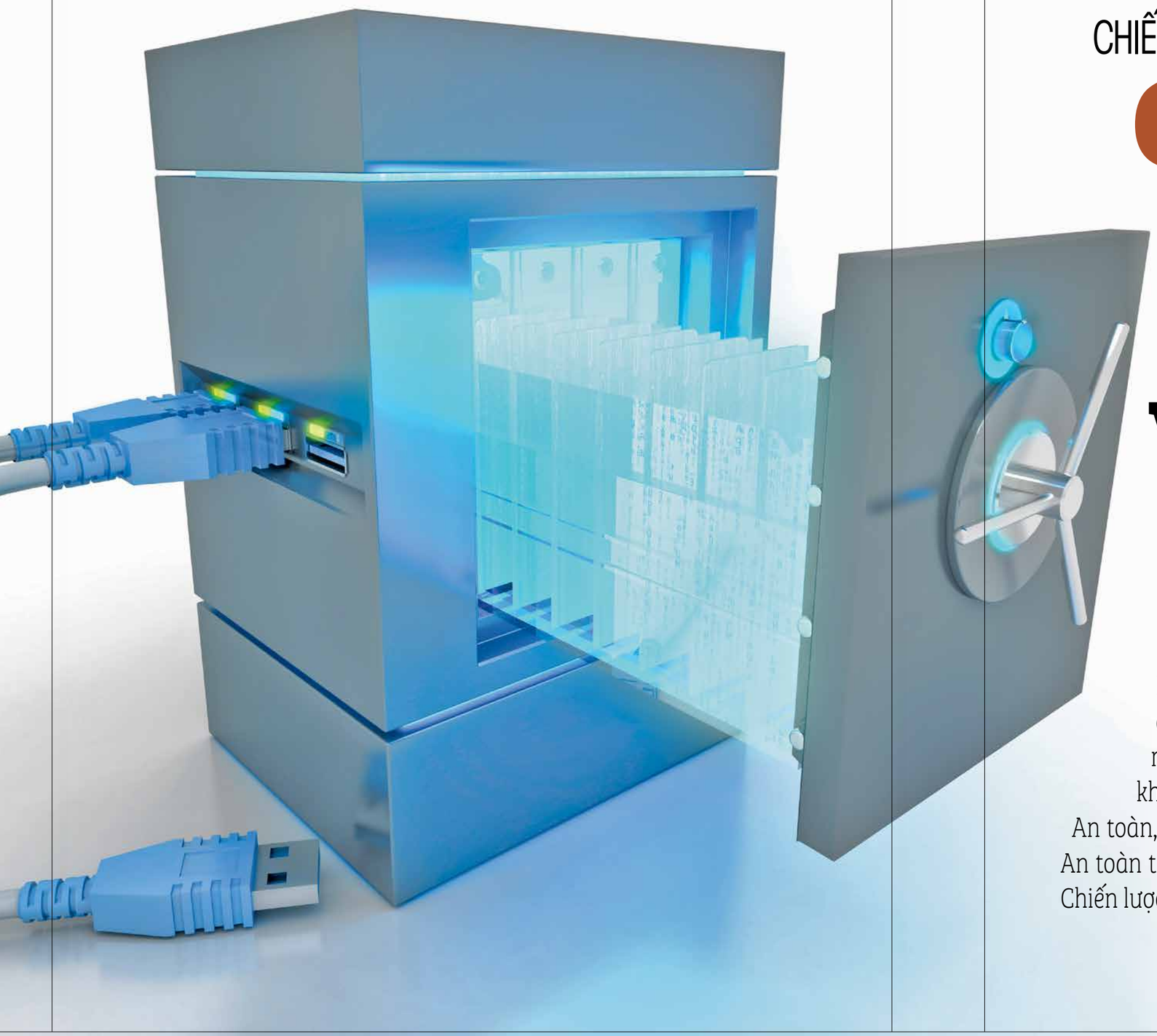

CHIẾN LƯỢC AN TOÀN, AN NINH MẠNG QUỐC GIA:

CHỦ ĐỘNG, SẴN SÀNG CHO MỘT VIỆT NAM SỐ

TRẦN ĐĂNG KHOA

Ngày 10/8/2022, Thủ tướng Chính phủ đã ban hành Quyết định số 964/QĐ-TTg phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030 (Chiến lược An toàn, An ninh mạng quốc gia). Đây là lần đầu tiên kể từ khi Luật An toàn thông tin mạng và Luật An ninh mạng có hiệu lực thi hành, Chiến lược An toàn, An ninh mạng quốc gia được ban hành.

Chiến lược nhằm bảo vệ sự thịnh vượng của Việt Nam trên không gian mạng

Việt Nam hướng tới trở thành quốc gia số, nước công nghiệp phát triển và thịnh vượng vào năm 2045. Đến nay, đã xác định được tầm nhìn quốc gia rõ ràng và kế hoạch hành động quốc gia cụ thể thông qua: 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; Chương trình Chuyển đổi số quốc gia; Chiến lược phát triển Chính phủ điện tử hướng tới Chính phủ số; và gần đây là Chiến lược quốc gia phát triển kinh tế số và xã hội số (các Quyết định của Thủ tướng Chính phủ số 749/QĐ-TTg ngày 03/6/2020, 942/QĐ-TTg ngày 15/6/2021, 441/QĐ-TTg ngày 31/3/2022).

Khi chuyển đổi số đưa hoạt động của cơ quan, tổ chức, doanh nghiệp và người dân lên môi trường mạng một cách toàn diện, được số hóa thì không gian mạng có thể coi là không gian sống mới. Nhưng không gian sống đó không an toàn, nhiều nguy cơ, thách thức trong khi nhận thức và kỹ năng tự bảo vệ của tổ chức, người dân còn hạn chế, chưa tương xứng. Điều này đặt ra yêu cầu Việt Nam cần có một nền tảng an toàn, an ninh mạng đủ mạnh, sẵn sàng và kiên cường ứng phó trước thách thức từ không gian mạng.

Trên thế giới, các cuộc tấn công mạng, vi phạm dữ liệu với quy mô lớn liên tiếp diễn ra nhằm vào chính phủ, tập đoàn lớn, các hệ thống, cơ sở hạ tầng quan trọng của các quốc gia để đánh cắp dữ liệu hoặc làm tê liệt hoạt động kinh tế, xã hội. Mức độ phức tạp của các mối đe dọa trên không gian mạng tăng lên do xu thế áp dụng các công nghệ mới như trí tuệ nhân tạo (AI), 5G, điện toán đám mây, Internet vạn vật (IoT),... và từ sự hợp tác chiến thuật chặt chẽ hơn giữa các nhóm tin tặc và tổ chức chính trị. Mới đây nhất, việc dữ liệu cá nhân của một tỷ người dân Trung Quốc bị tin tặc rao bán hay Albania phải đóng cửa các hệ thống chính phủ điện tử do tấn công mạng chính là lời cảnh tỉnh cho các quốc gia về tầm quan trọng của an toàn, an ninh mạng. Có thể nói, một quốc gia không an toàn nếu không gian mạng của quốc gia đó không an toàn.

Việt Nam cũng như nhiều nước trên thế giới, tầm quan trọng của Internet có thể sánh ngang với những nhu yếu phẩm cần thiết cho cuộc sống như điện, nước, xăng dầu, thực phẩm... Do đó, hơn lúc nào hết, Việt Nam cần ban hành và triển khai một chiến lược an toàn, an ninh mạng bài bản và tổng thể. Chiến lược sẽ giúp Việt Nam đối phó với những mối đe dọa ngày càng tăng trên không gian mạng.

Chiến lược An toàn, An ninh mạng quốc gia được ban hành là mảnh ghép quan trọng giúp hoàn thiện bức tranh tổng thể về một quốc gia số với Chính phủ số, kinh tế số và xã hội số. Chủ động đón nhận khi những cơ hội mới từ chuyển đổi số mở ra nhưng cũng cần sẵn sàng ứng phó trước những nguy cơ rủi ro, để bảo vệ những thành quả đạt được.

Với tầm nhìn trở thành quốc gia tự chủ về an toàn, an ninh mạng để bảo vệ sự phát triển thịnh vượng của Việt Nam trên không gian mạng, Chiến lược An toàn, An ninh mạng quốc gia đã đề ra 13 mục tiêu cụ thể đến năm 2025 và 8 mục tiêu cụ thể đến năm 2030 để hiện thực hóa tầm nhìn này. Cùng với đó, 12 nhóm nhiệm vụ, giải pháp cũng được đặt ra để triển khai thực hiện.

Quan điểm mới, rõ ràng và đột phá

Chiến lược An toàn, an ninh mạng quốc gia đưa ra 7 quan điểm chỉ đạo rõ ràng về an toàn, an ninh mạng. Trong đó, có những quan điểm mới, đột phá và phù hợp với đặc thù của Việt Nam. Những quan điểm này sẽ là kim chỉ nam cho công tác bảo đảm an toàn, an ninh mạng quy mô quốc gia cũng như trong hoạt động của các cơ quan, tổ chức, doanh nghiệp:

- An toàn, an ninh mạng là trọng tâm của quá trình chuyển đổi số, là trụ cột quan trọng tạo lập niềm tin số và sự phát triển thịnh vượng trong kỷ nguyên số. An toàn, an ninh mạng là nhiệm vụ trọng yếu, thường xuyên, lâu dài nhằm khởi tạo và duy trì môi trường mạng an toàn, lành mạnh, tin cậy cho các cơ quan, tổ chức, doanh nghiệp và mỗi người dân. Đầu tư cho an toàn, an ninh mạng là đầu tư cho phát triển bền vững và tạo ra giá trị.
- Phát huy sức mạnh của cả hệ thống chính trị và toàn xã hội, chủ động ứng phó từ sớm, từ xa với các nguy cơ, thách thức, hoạt động gây tổn hại tới chủ quyền, lợi ích, an ninh quốc gia trên không gian mạng và an toàn thông tin mạng quốc gia, trong đó cơ quan quản lý nhà nước giữ vai trò điều phối, gắn kết, chia sẻ thông tin.
- Chuyển đổi căn bản về nhận thức và cách làm để thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa an toàn, an ninh mạng (cyber resilience): Từ mô hình bảo vệ phân tán sang mô hình bảo vệ tập trung; từ bị động ứng cứu sự cố sang chủ động dự báo sớm, cảnh báo sớm, phòng ngừa và ứng phó hiệu quả; từ đơn độc bảo vệ, giấu kín thông tin bị tấn công mạng sang chủ động hợp tác, chia sẻ thông tin nhằm chủ động phòng ngừa và hỗ trợ xử lý sự cố, phục hồi hoạt động bình thường của hệ thống thông tin.
- Thúc đẩy chuyên gia, nghiên cứu, phát triển tự chủ về công nghệ, sản phẩm, dịch vụ an toàn, an ninh mạng Việt Nam là giải pháp căn cơ bảo đảm an toàn, an ninh mạng quốc gia.

Bảo vệ không gian mạng quốc gia

Không gian mạng quốc gia bao gồm toàn bộ hạ tầng số, nền tảng số, thiết bị, ứng dụng và dữ liệu do tổ chức, cá nhân Việt Nam tạo ra, sở hữu, quản lý. Bảo đảm không gian mạng quốc gia cũng chính là bảo đảm cho chủ quyền số quốc gia, bảo vệ sự thịnh vượng của Việt Nam trên không gian mạng.

Cơ sở hạ tầng không gian mạng quốc gia cần được bảo đảm an toàn, an ninh mạng trong quá trình lựa chọn, thiết kế, xây dựng, vận hành, khai thác; ưu tiên sử dụng sản phẩm an toàn, an ninh mạng Việt Nam.

Hạ tầng số là hạ tầng của nền kinh tế số và xã hội số. Các doanh nghiệp hạ tầng số có vị trí thuận lợi nhất để phòng, chống tấn công mạng, có sứ mệnh tiên phong bảo đảm an toàn không gian mạng quốc gia và bảo vệ cho người sử dụng. Vì vậy, doanh nghiệp hạ tầng số cần triển khai trung tâm điều hành an toàn thông tin mạng (SOC), kết nối với Nền tảng điều hành, chỉ huy an toàn thông tin mạng

tập trung do Bộ Thông tin và Truyền thông triển khai; công khai mức độ an toàn thông tin mạng và cung cấp dịch vụ viễn thông, Internet an toàn; bảo đảm an toàn thông tin mạng 5G và các thế hệ mạng tiếp theo; khắc phục, xử lý các điểm yếu, nguy cơ mất an toàn thông tin trên mạng lưới; Thúc đẩy phát triển và làm chủ công nghệ điện toán đám mây Make in Viet Nam và hạ tầng mạng IoT an toàn; ....

Các nền tảng số được xem là giải pháp đột phá để thúc đẩy nhanh quá trình chuyển đổi số. Toàn bộ dữ liệu, lịch sử hoạt động của người sử dụng trên nền tảng số đều được thu thập, xử lý, lưu trữ. Các doanh nghiệp nền tảng số có trách nhiệm quan trọng trong việc bảo đảm an toàn, an ninh mạng quốc gia. Nền tảng số khi xây dựng, phát triển cần xác định cấp độ an toàn thông tin và triển khai phương án bảo đảm an toàn hệ thống thông tin theo cấp độ. Các nền tảng số khi được phát triển cần có khả năng tự bảo vệ, có công cụ sàng lọc, xử lý thông tin vi phạm pháp luật. Cần tập trung bảo vệ và công khai chính sách thu thập, quản lý, sử dụng thông tin, dữ liệu của người sử dụng; cung cấp cơ chế cho người sử dụng cơ chế khiếu nại, phản ánh, xác minh thông tin; chủ động phát hiện, ngăn chặn, xử lý, xóa bỏ tin giả, thông tin vi phạm pháp luật.

Dữ liệu là tài nguyên số, là nguyên liệu cho nền kinh tế số. Dữ liệu số có nguy cơ mất an toàn do số lượng lớn người sử dụng Việt Nam đang sử dụng dịch vụ nền tảng số của các doanh nghiệp xuyên biên giới, thông tin, dữ liệu của người sử dụng Việt Nam không được lưu trữ tại Việt Nam. Chìa khóa của chủ quyền dữ liệu nằm ở các nền tảng số Make in Viet Nam. Cần phát triển các Trung tâm dữ liệu đạt tiêu chuẩn quốc tế tại Việt Nam và phát triển các nền tảng số Make in Viet Nam có hàng triệu người Việt Nam và quốc tế sử dụng. Bảo đảm an ninh mạng, an toàn thông tin mạng theo cấp độ cho các cơ sở dữ liệu quốc gia và cơ sở dữ liệu quan trọng của các ngành, lĩnh vực.

Bảo vệ hệ thống thông tin của các cơ quan Đảng, Nhà nước và các lĩnh vực quan trọng

Chủ quản hệ thống thông tin có trách nhiệm tự bảo vệ hệ thống thông tin, dữ liệu của mình. Cơ quan nhà nước phải đi đầu về việc tuân thủ quy định của pháp luật và tiêu chuẩn về an toàn, an ninh mạng. Các hệ thống thông tin thuộc 11 lĩnh vực quan trọng (Giao thông, Năng lượng, Tài nguyên và Môi trường, Thông tin, Y tế, Tài chính, Ngân hàng, Quốc phòng, An ninh, trật tự an toàn xã hội, Đô thị, Chỉ đạo điều hành của Chính phủ) là cơ sở hạ tầng quan trọng của nền kinh tế - xã hội hoặc nắm giữ lượng thông tin, dữ liệu quan trọng. Nếu xảy ra mất an toàn, an ninh mạng thì có thể ảnh hưởng đến an ninh quốc gia và sự phát triển của nền kinh tế, sự ổn định của xã hội. Bảo vệ hệ thống thông tin của các lĩnh vực quan trọng là hoạt động ưu tiên. Thực hiện bảo đảm an toàn hệ thống thông tin theo cấp độ và triển khai mô hình bảo vệ 4 lớp trước khi đưa vào sử dụng. Tăng cường triển khai các hoạt động diễn tập thực chiến để tăng cường năng lực của lực lượng bảo đảm an toàn, an ninh mạng. Phát triển Mạng lưới ứng cứu sự cố an toàn thông tin quốc gia, tập trung vào 11 lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng (CERT lĩnh vực).

Tạo lập niềm tin số và bảo vệ người dân trên không gian mạng

Việt Nam với hơn 70 triệu người dùng Internet, trung bình mỗi người sử dụng trực tuyến gần 7 giờ mỗi ngày, an toàn, an ninh mạng giờ đây là câu chuyện của mọi người dân. Tuy nhiên, nhận thức và kỹ năng về an toàn, an ninh mạng của đại đa số người dân còn hạn chế, chưa đủ để bảo vệ chính mình. Do đó, nguy cơ mất an toàn, an ninh mạng đối với người dân là rất lớn và bảo đảm an toàn cho người dân sẽ cần là nhiệm vụ trọng tâm. Trong đó, nâng cao nhận thức và thay đổi thói quen, hành vi trên không gian mạng của người dân sẽ là giải pháp căn bản.

Tạo lập niềm tin số, xây dựng môi trường mạng trung thực, văn minh, lành mạnh và phòng, chống vi phạm pháp luật trên không gian mạng được xác định là nội dung quan trọng của Chiến lược. Niềm tin số giúp cho người dân trải nghiệm đầy đủ cuộc sống an toàn, lành mạnh trên không gian mạng, giúp cho doanh nghiệp yên tâm đầu tư, phát triển hoạt động sản xuất kinh doanh trực tuyến, giúp cơ quan nhà nước chuyển toàn bộ hoạt động lên môi trường mạng an toàn, hiệu quả. Ứng dụng (app) Internet an toàn, nền tảng hỗ trợ bảo vệ trẻ em trên môi trường mạng sẽ được thúc đẩy phát triển nhằm bảo vệ người dân trên môi trường mạng. Quan điểm lấy cộng đồng làm trung tâm sẽ là phương thức để triển khai các chiến dịch tuyên truyền nâng cao nhận thức, phát triển cổng Khonggianmang.vn cung cấp cho tổ chức, cá nhân thông tin, cảnh báo, giải đáp thắc mắc, hỗ trợ công cụ, tiện ích và hướng dẫn xử lý sự cố an toàn thông tin mạng.

Một cơ chế phối hợp liên ngành, cùng với sự tham gia của các tổ chức, doanh nghiệp sẽ được triển khai để phòng ngừa, phát hiện, điều tra, xử lý các vi phạm pháp luật trên không gian mạng và chống khủng bố mạng.

Làm chủ, tự chủ công nghệ, sản phẩm, dịch vụ an toàn, an ninh mạng

Làm chủ, tự chủ về công nghệ, sản phẩm, dịch vụ an toàn, an ninh mạng là giải pháp căn bản bảo đảm an toàn không gian mạng quốc gia. Khuyến khích và tôn vinh tinh thần đổi mới sáng tạo về công nghệ, sản phẩm, dịch vụ an toàn, an ninh mạng. Sẽ phát triển 2 đến 3 Trung tâm nghiên cứu và phát triển (R&D), tạo môi trường thuận lợi cho nghiên cứu, thử nghiệm sản phẩm, dịch vụ an toàn thông tin mạng mới. Các doanh nghiệp an toàn, an ninh mạng được khuyến khích nghiên cứu, phát triển, làm chủ công nghệ, sản phẩm, dịch vụ bảo đảm an toàn, an ninh mạng.

Việc phát triển sản phẩm an toàn thông tin mạng sẽ được chuyển dịch từ chiều rộng sang chiều sâu: tập trung phát triển 3 - 5 sản phẩm trọng điểm, có thương hiệu quốc gia. Chuyển dịch từ sản phẩm lớn, chuyên dụng sang sản phẩm phổ cập: "bình dân hóa" sản phẩm an toàn thông tin mạng, phục vụ đối tượng người dân, hộ gia đình. Đặt nền móng cho công nghiệp an toàn thông tin mạng và Xây dựng nền công nghiệp an ninh mạng với công nghệ, sản phẩm, dịch vụ an ninh mạng tiên tiến.

Đào tạo và phát triển nguồn nhân lực

Nguồn nhân lực đóng vai trò quan trọng trong hoạt động an toàn, an ninh mạng. Chiến lược xác định chuyển đổi từ đào tạo cán bộ kỹ thuật trung bình sang phát triển đội ngũ chuyên gia giỏi, phát triển đội ngũ chuyên gia xuất sắc về an toàn, an ninh mạng để giải quyết các bài toán khó của đất nước cũng như góp phần giải quyết các vấn đề về an toàn, an ninh mạng trong công nghệ số của thế giới. Hướng dẫn, thúc đẩy triển khai quy định chuẩn kỹ năng an toàn thông tin mạng. Đưa nội dung về an toàn, an ninh mạng vào chương trình giáo dục phổ thông (chính khóa và ngoại khóa) cũng như đào tạo bậc đại học trở lên. Xây dựng đội ngũ kỹ sư an ninh mạng chất lượng cao, có khả năng nghiên cứu, chế tạo, sản xuất các sản phẩm, dịch vụ an ninh mạng, đóng vai trò quan trọng trong việc tiếp thu, chuyển giao tri thức về an ninh mạng, chính sách tôn vinh và đãi ngộ phù hợp.

Thông qua việc ban hành và triển khai Chiến lược, Việt Nam đã cho cộng đồng quốc tế thấy được tầm nhìn, mục tiêu, định hướng chiến lược của Việt Nam đối với công tác bảo đảm an toàn, an ninh mạng quốc gia, nâng cao uy tín và vị thế của quốc gia trên trường quốc tế, tạo đà cho sự bứt phá của chuyển đổi số quốc gia.■ THÔNG TIN & TRUYỀN THÔNG