HIỆP HỘI AN NINH MẠNG QUỐC GIA

TẠP CHÍ ĐIỆN TỬ
AN NINH MẠNG VIỆT NAM
CƠ QUAN NGÔN LUẬN CỦA HIỆP HỘI AN NINH MẠNG QUỐC GIA

SỐ TẾT BÍNH NGỌ
2026

KIẾN TẠO TƯƠNG LAI SỐ AN TOÀN VÀ TỰ CHỦ

NCA
HIỆP HỘI AN NINH MẠNG QUỐC GIA

TẠP CHÍ ĐIỆN TỬ
AN NINH MẠNG VIỆT NAM
CƠ QUAN NGÔN LUẬN CỦA HIỆP HỘI AN NINH MẠNG QUỐC GIA

NGƯỜI BẠN ĐỒNG HÀNH TRONG KỶ NGUYÊN SỐ

> Vì một Việt Nam
> an toàn trên không gian mạng

LỜI TOÀ SOẠN

AN NINH MẠNG NỀN TẢNG CỦA NIỀM TIN SỐ QUỐC GIA

Xuân Bính Ngọ 2026 đến trong thời điểm đất nước bước vào một giai đoạn phát triển mới, năm đầu tiên triển khai Nghị quyết Đại hội đại biểu toàn quốc lần thứ XIV của Đảng. Chuyển đổi số không còn là lựa chọn, mà đã trở thành động lực trung tâm, định hình phương thức phát triển, quản trị và kết nối của Việt Nam trong kỷ nguyên số.

Trong quá trình ấy, không gian mạng ngày càng hiện diện rõ nét như một trụ cột của kinh tế số, xã hội số và quản trị quốc gia hiện đại. An ninh mạng vì thế không còn là câu chuyện kỹ thuật thuần túy, mà đã trở thành vấn đề chiến lược, gắn chặt với chủ quyền số, trật tự an toàn xã hội và niềm tin của người dân. Những nguy cơ tấn công mạng, lừa đảo trực tuyến, tội phạm công nghệ cao ngày càng tinh vi, xuyên biên giới, đặt ra yêu cầu mới về tư duy quản trị, sự phối hợp liên ngành và hợp tác quốc tế sâu rộng.

Năm 2025 ghi dấu bước tiến quan trọng khi Việt Nam chủ động tham gia và đóng góp trách nhiệm vào việc xây dựng các khuôn khổ hợp tác quốc tế về phòng, chống tội phạm mạng. Những nỗ lực đó không chỉ khẳng định vị thế và uy tín quốc gia, mà còn thể hiện tầm nhìn dài hạn trong bảo vệ lợi ích quốc gia trên không gian số.

Từ thực tiễn ấy, báo chí chuyên ngành an ninh mạng mang trên mình sứ mệnh đặc biệt: cung cấp thông tin chính xác, phân tích có chiều sâu, cảnh báo kịp thời và định hướng nhận thức xã hội. **Tạp chí An ninh mạng Việt Nam** tiếp tục kiên định vai trò là diễn đàn tin cậy, nơi kết nối chính sách với thực tiễn, công nghệ với con người, góp phần xây dựng không gian mạng an toàn, lành mạnh và đáng tin cậy.

Ấn phẩm Xuân Bính Ngọ 2026 là lời chào năm mới, đồng thời gửi đi thông điệp về một Việt Nam số phát triển bền vững trên nền tảng an ninh và niềm tin.

Tổng Biên tập

Nguyễn Tất Hồng Dương

MỤC LỤC

TÒA SOẠN

TỔNG BIÊN TẬP

Nguyễn Tất Hồng Dương

THƯ KÝ TÒA SOẠN

Phí Thanh Hường

Lê Phan Thủy Nguyên

THIẾT KẾ

Trần Thúy Quỳnh

LIÊN HỆ

Tạp chí An ninh mạng Việt Nam

38 Phan Đình Phùng, Ba Đình, Hà Nội
0928.773.838
toasoan@tcanninhmang.vn
https://tcanninhmang.vn
www.facebook.com/tcanninhmang

Giấy phép xuất bản:

Số 116/GP-XBĐS cấp ngày 23/12/2025

Phát hành qua mạng lưới Bưu điện Việt Nam và trực tiếp tại Tòa soạn Tạp chí An ninh mạng Việt Nam

KỶ NGUYÊN VƯƠN MÌNH

★ 1. Phát huy sức mạnh toàn dân xây dựng thế trận an ninh mạng vững chắc

★ 2. Đóng góp của Bộ Công an trong việc tổ chức thành công Lễ mở ký Công ước của Liên hợp quốc về chống tội phạm mạng

★ 3. An ninh mạng trong kỷ nguyên mới - Lá chắn số cho Khát vọng vươn mình

★ 4. Hợp lực quốc gia hiện thực hóa Nghị quyết 57-NQ/TW trong Kỷ nguyên chủ quyền số

Phát huy sức mạnh Toàn dân xây dựng thế trận an ninh mạng vững chắc

Đại tướng Lương Tam Quang

Ủy viên Bộ Chính trị, Bộ trưởng Bộ Công an , Chủ tịch Hiệp hội An ninh mạng quốc gia

> **Không gian mạng đã trở thành không gian chiến lược gắn trực tiếp với lợi ích quốc gia - dân tộc. Bảo đảm an ninh mạng là nhiệm vụ bảo vệ nền tảng của quản trị quốc gia, của tăng trưởng kinh tế và của niềm tin xã hội trong kỷ nguyên số.**
>
> *Đại tướng Lương Tam Quang*
> *Ủy viên Bộ Chính trị, Bộ trưởng Bộ Công an ,*
> *Chủ tịch Hiệp hội An ninh mạng quốc gia*

LỜI TÒA SOẠN

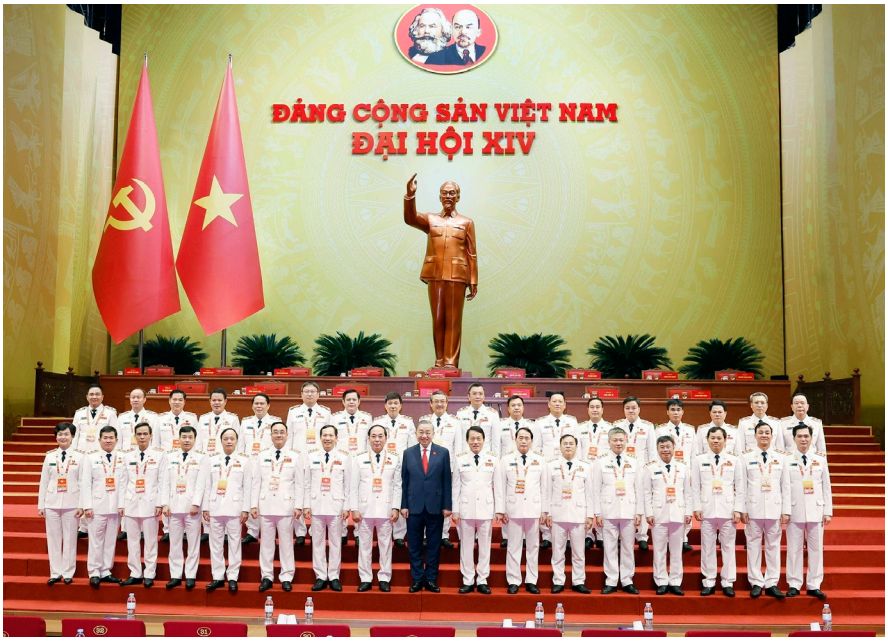
Nhân dịp Xuân Bính Ngọ 2026, Đại tướng Lương Tam Quang - Ủy viên Bộ Chính trị, Bộ trưởng Bộ Công an, Chủ tịch Hiệp hội An ninh mạng quốc gia, dành riêng cho Tạp chí An ninh mạng Việt Nam bài viết "Phát huy sức mạnh toàn dân xây dựng thế trận an ninh mạng vững chắc".

Tạp chí An ninh mạng Việt Nam trân trọng giới thiệu cùng bạn đọc.

Bước sang năm 2026, chúng ta bước vào một giai đoạn mà không gian mạng đã trở thành "không gian chiến lược" gắn chặt với lợi ích quốc gia - dân tộc. Dữ liệu là tài nguyên mới, hạ tầng số là huyết mạch vận hành của Nhà nước, doanh nghiệp và đời sống xã hội; niềm tin số là điều kiện quyết định cho phát triển bền vững. Từ đó, bảo đảm an ninh mạng trở thành nhiệm vụ bảo vệ nền tảng của quản trị quốc gia, tăng trưởng kinh tế, trật tự xã hội và quyền, lợi ích chính đáng, hợp pháp của người dân trong kỷ nguyên số. Bảo đảm an ninh mạng phải tạo nền tảng thực hiện thắng lợi nhiệm vụ trọng tâm mà Nghị quyết Đại hội XIV của Đảng đã đề ra *"xác lập mô hình tăng trưởng mới..., lấy khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số làm động lực chính".*

Nhìn sâu vào bản chất các mối đe dọa hiện nay, có thể thấy an ninh mạng không còn là câu chuyện "tấn công - phòng thủ". Tấn công mạng ngày càng đa dạng, tinh vi, xuyên biên giới; kết hợp kỹ thuật với thao túng tâm lý; khai thác điểm yếu từ con người, quy trình, chuỗi cung ứng đến hệ thống. Những nguy cơ như xâm phạm dữ liệu cá nhân, phá hoại hạ tầng trọng yếu, lừa đảo trực tuyến quy mô lớn... không chỉ gây thiệt hại kinh tế mà còn tác động trực tiếp tới ổn định chính trị - xã hội và năng lực quản trị quốc gia trong môi trường số.

Bối cảnh đó đòi hỏi nhiệm vụ an ninh mạng sự chuyển dịch mạnh mẽ ngay từ những ngày đầu năm 2026: Từ tư duy "xử lý sự cố" sang tư duy "quản trị rủi ro liên tục", từ "phòng thủ bị động" sang "phòng ngừa chủ động", từ "an toàn ở tầng kỹ thuật" sang "an toàn là kỷ luật vận hành". An ninh mạng phải được tích hợp ngay từ khâu thiết kế hệ thống và quy trình; phải được đo lường kiểm tra, diễn tập, đánh giá độc lập; phải gắn với trách nhiệm cụ thể của người đứng đầu. Khi an ninh mạng trở thành năng lực quản trị, quốc gia mới có thể đi nhanh mà không chệch hướng, doanh nghiệp mới có thể mở rộng mà không trả giá bằng rủi ro hệ thống.



Tổng Bí thư Tô Lâm, Chủ tịch Đoàn Chủ tịch chụp ảnh cùng Đoàn Đảng ủy Công an Trung ương dự Đại hội XIV của Đảng

Nâng cao năng lực tự chủ, phát triển an ninh mạng gắn với bảo vệ chủ quyền

Muốn bảo vệ chủ quyền số một cách thực chất, yêu cầu nâng cao năng lực tự chủ về thể chế, công nghệ, nhân lực và công nghiệp an ninh mạng đặt ra cấp thiết. Tự chủ không có nghĩa là khép kín, tách rời hợp tác quốc tế, mà là làm chủ những năng lực cốt lõi để không bị lệ thuộc, không bị động và có khả năng tự bảo vệ trước mọi tình huống. Đó là nền tảng để vừa giữ vững an ninh quốc gia, vừa thúc đẩy phát triển kinh tế - xã hội trong môi trường số.

Tự chủ trước hết phải bắt đầu từ hành lang pháp lý. Năm 2026, yêu cầu hoàn thiện thể chế không chỉ để "xử lý vi phạm", mà sâu xa hơn là để thiết lập kỷ luật số và trật tự số; bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân: tạo môi trường minh bạch, ổn định cho đổi mới sáng tạo và phát triển kinh tế số. Tinh thần đó cũng được cụ thể hóa bằng việc Quốc hội đã thông qua Luật An ninh mạng (Luật số 116/2025/QH15), có hiệu lực từ ngày 01/7/2026, thay thế các quy định trước đây, hướng tới tăng cường bảo vệ không gian mạng và năng lực quản lý trong bối cảnh số hóa mạnh mẽ.

Pháp luật chỉ thực sự có giá trị khi đi cùng năng lực thực thi và cơ chế bảo đảm. Bởi vậy, cùng với thể chế, cần thúc đẩy các điều kiện để triển khai đồng bộ: Trách nhiệm quản trị dữ liệu, cơ chế tài chính cho công tác bảo vệ an ninh mạng, chuẩn mực kỹ thuật, cơ chế phối hợp chia sẻ thông tin và khuyến khích phát triển - sử dụng sản phẩm, dịch vụ an ninh mạng của Việt Nam. Chính sự thống nhất giữa "khuôn khổ pháp lý" và "năng lực thực thi" sẽ tạo nên điểm tựa bền vững cho chuyển đổi số an toàn.

Song song với hoàn thiện thể chế là yêu cầu xây dựng nền công nghiệp an ninh hiện đại, tự chủ. Việc hình thành Quỹ đầu tư phát triển công nghiệp an ninh và Tổ hợp công nghiệp an ninh quốc gia mang ý nghĩa chiến lược, tạo nguồn lực dài hạn cho nghiên cứu, phát triển, ứng dụng sản phẩm, giải pháp an ninh mạng "Make in Vietnam", phục vụ trực tiếp nhiệm vụ bảo vệ an ninh quốc gia và chủ quyền số. Đây là cách biến năng lực phòng thủ thành năng lực cạnh tranh, biến yêu cầu bảo vệ thành động lực phát triển một ngành kinh tế chiến lược của quốc gia.

Trong kỷ nguyên trí tuệ nhân tạo, bảo vệ bí mật Nhà nước đặt ra yêu cầu đặc biệt nghiêm ngặt. Công nghệ AI đem lại năng suất mới, nhưng cũng đặt ra nguy cơ mới nếu bị lạm dụng để thu thập, suy luận, tái cấu trúc thông tin nhạy cảm. Cần kiên quyết không cho phép bất kỳ hành vi nào sử dụng hệ thống trí tuệ nhân tạo để xâm phạm bí mật Nhà nước; đồng thời phải tháo gỡ các rào cản không cần thiết để chuyển đổi số trong cơ quan nhà nước diễn ra thông suốt, an toàn, hiệu quả. Ở đây, điều cốt lõi là cân bằng đúng: bảo vệ nghiêm ngặt những gì phải bảo vệ, nhưng tạo dòng chảy thông suốt cho dữ liệu hợp pháp phục vụ quản trị và phát triển.

Nếu pháp luật và công nghiệp là "xương sống", thì sức mạnh xã hội, sức mạnh toàn dân là "hệ tuần hoàn" của thế trận an ninh mạng. Bảo vệ không gian mạng không thể chỉ dựa vào lực lượng chuyên trách. An ninh mạng bền vững phải được xây dựng như một "thế trận" nhiều tầng, nhiều lớp, trong đó mỗi người dân là một chủ thể an toàn, mỗi tổ chức là một mắt xích kỷ luật. Khi tri thức an toàn số được chuyển hóa thành hành vi thường nhật - biết kiểm tra, biết xác minh, biết dừng lại đúng lúc trước đường link lạ, biết bảo vệ danh tính số, biết báo cáo khi bị tấn công - thì bề mặt bị tấn công thu hẹp, chi phí xã hội cho việc chống tội phạm mạng giảm, và năng lực phòng vệ cộng đồng tăng

lên một cách tự nhiên.

Từ góc độ chiến lược quốc gia, đây chính là bản chất của "thế trận an ninh mạng toàn dân": không phải là một khẩu hiệu, mà là một cấu trúc sức mạnh xã hội được tổ chức và dẫn dắt, tạo ra khả năng tự vệ rộng lớn cho nền kinh tế và xã hội số. Đó là sức mạnh tổng hợp của Nhà nước, doanh nghiệp, giới chuyên gia, tổ chức xã hội và mỗi công dân - thống nhất trong nhận thức, đồng bộ trong hành động, và bền bỉ trong kỷ luật.

Hoàn thiện pháp luật trong nước đi đôi với tăng cường hợp tác quốc tế

Không một quốc gia nào có thể đơn độc ứng phó hiệu quả trước tội phạm mạng xuyên biên giới. Bởi vậy, cùng với việc hoàn thiện hệ thống pháp luật về an ninh mạng, an toàn thông tin, bảo vệ dữ liệu, Việt Nam đã rất chủ động, tích cực tham gia các cơ chế hợp tác quốc tế về phòng, chống tội phạm mạng. Lễ mở ký Công ước của Liên hợp quốc về chống tội phạm mạng diễn ra tại Hà Nội trong các ngày 25-26/10/2025 là minh chứng rõ nét cho uy tín, vị thế và trách nhiệm ngày càng cao của Việt Nam trong nỗ lực chung bảo đảm an ninh mạng toàn cầu.

Thông điệp Việt Nam gửi tới cộng đồng quốc tế là nhất quán: xây dựng không gian mạng dựa trên luật pháp; tăng cường hợp tác; tôn trọng chủ quyền; đồng thời bảo đảm hài hòa giữa yêu cầu an ninh, quyền con người và lợi ích chính đáng của các quốc gia. Không gian mạng cần trở thành không gian của hòa bình, ổn định và phát triển bền vững, chứ không phải là "vùng xám" cho các hành vi vi phạm pháp luật. Khi đặt luật pháp và lòng tin chiến lược làm nền, hợp tác quốc tế sẽ đi vào thực chất: chia sẻ thông tin, phối hợp điều tra, nâng cao năng lực, hỗ trợ kỹ thuật - đặc biệt với các nước đang phát triển - để không ai bị bỏ lại phía sau trong cuộc chiến chống tội phạm mạng.

Phát huy sức mạnh toàn dân - vai trò nòng cốt của Hiệp hội An ninh mạng quốc gia

Trong tổng thể thế trận an ninh mạng toàn dân, Hiệp hội An ninh mạng quốc gia giữ vai trò hạt nhân kết nối và tổ chức sức mạnh xã hội; là cầu nối quan trọng giữa

Đoàn Đảng ủy Công an Trung ương dự Đại hội XIV của Đảng

chủ trương, chính sách của Đảng và Nhà nước với thực tiễn triển khai trong cộng đồng doanh nghiệp, giới chuyên gia và người dân. Hiệp hội không chỉ là tổ chức xã hội - nghề nghiệp, mà còn là một thiết chế phối hợp "mềm", góp phần chuyển hóa định hướng chiến lược thành hành động cụ thể, lan tỏa rộng khắp trong toàn xã hội.

Vai trò của Hiệp hội cần được nhìn nhận như một "điểm hội tụ" của hệ sinh thái: nơi quy tụ trí tuệ chuyên gia, năng lực công nghệ của doanh nghiệp, kinh nghiệm thực tiễn của các chủ thể vận hành và nhu cầu bảo vệ cụ thể của xã hội. Từ đó, Hiệp hội có thể kiến tạo "lá chắn số" nhiều tầng, nhiều lớp; thúc đẩy hợp tác công - tư; chia sẻ chuẩn mực, kinh nghiệm; hỗ trợ đào tạo, truyền thông kết nối quốc tế; hỗ trợ kỹ thuật cho các tổ chức, doanh nghiệp trong phòng ngừa phát hiện, ứng phó sự cố. Quan trọng hơn, Hiệp hội góp phần hình thành một kỷ luật xã hội mới trong môi trường số: kỷ luật tuân thủ, kỷ luật bảo vệ dữ liệu, kỷ luật an toàn vận hành.

Trong ý nghĩa sâu xa đó, Hiệp hội chính là đầu mối kết nối sức mạnh toàn dân trong kỷ nguyên số: từ cơ quan quản lý nhà nước, lực lượng chuyên trách, doanh nghiệp cung cấp hạ tầng và dịch vụ số, đến từng tổ chức xã hội và mỗi người dân. Khi Hiệp hội làm tốt vai trò kết nối, chuẩn hóa và lan tỏa, "thế trận an ninh mạng toàn dân" không còn là một khái niệm, mà trở thành năng lực thực tế của quốc gia - thống nhất, đồng bộ và có sức đề kháng cao trước mọi biến động.

Năm 2026 cũng là năm bản lề, gắn với những nhiệm vụ phát triển lớn của đất nước trong kỷ nguyên mới, trong đó phát triển khoa học - công nghệ, đổi mới sáng tạo và chuyển đổi số tiếp tục được xác định là động lực quan trọng để phát triển nhanh, bền vững. Đại hội đại biểu toàn quốc lần thứ XIV của Đảng đặt ra yêu cầu rất cao về việc tạo đột phá chiến lược, đồng thời xác lập rõ vị trí của an ninh mạng, an ninh dữ liệu như điều kiện tiên quyết để kiến tạo niềm tin số quốc gia.

Khi mỗi cơ quan, tổ chức và doanh nghiệp coi an ninh mạng, an ninh dữ liệu là nền tảng vận hành; mỗi người dân tự trang bị kỹ năng an toàn số như một kỹ năng sống; Hiệp hội An ninh mạng quốc gia phát huy vai trò nòng cốt trong kết nối, dẫn dắt, chuẩn hóa và lan tỏa. Khi sức mạnh toàn dân được tổ chức đúng cách, khi thể chế được hoàn thiện đồng bộ, khi công nghiệp an ninh được đầu tư đúng hướng, khi hợp tác quốc tế đi vào chiều sâu... Việt Nam chắc chắn sẽ bảo vệ vững chắc chủ quyền số, không gian mạng quốc gia trong mọi tình huống, củng cố niềm tin số và tạo động lực mới cho phát triển nhanh, bền vững trong kỷ nguyên số./.

L.T.Q

Đại tướng Lương Tam Quang - Ủy viên Bộ Chính trị, Bí thư Đảng ủy Công an Trung ương, Bộ trưởng Bộ Công an, Chủ tịch Hiệp hội An ninh mạng quốc gia phát biểu tại phiên Bế mạc Lễ mở ký công ước của Liên hợp quốc về chống tội phạm mạng

Chủ tịch nước Lương Cường, Phó Thủ tướng Bùi Thanh Sơn và các đại biểu Việt Nam tham dự Lễ mở ký Công ước Hà Nội

Đóng góp của Bộ Công an trong việc tổ chức thành công Lễ mở ký Công ước của Liên hợp quốc về chống tội phạm mạng

Thượng tướng Phạm Thế Tùng

Uỷ viên Trung ương Đảng, Thứ trưởng Bộ Công an, Phó Chủ tịch Thường trực Hiệp hội An ninh mạng quốc gia

Trong bối cảnh thế giới bước vào giai đoạn chuyển đổi số sâu rộng, không gian mạng đã trở thành một không gian phát triển chiến lược gắn liền với an ninh quốc gia, ổn định xã hội và quan hệ quốc tế của mỗi quốc gia. Việc cộng đồng quốc tế thống nhất lựa chọn Hà Nội làm nơi mở ký Công ước của Liên hợp quốc về chống tội phạm mạng (Công ước Hà Nội) trong hai ngày 25–26/10/2025 không chỉ là một sự kiện đối ngoại đa phương quan trọng, mà còn đánh dấu bước phát triển mới trong hợp tác toàn cầu nhằm ứng phó với các thách thức an ninh phi truyền thống ngày càng phức tạp.

Thành công của Lễ mở ký Công ước Hà Nội là kết quả của quá trình chuẩn bị công phu, trách nhiệm và bền bỉ, trong đó Bộ Công an giữ vai trò nòng cốt, xuyên suốt - từ tham gia xây dựng nội dung, vận động quốc tế, tổ chức thực hiện, đến bảo đảm tuyệt đối an ninh, an toàn và định hướng triển khai Công ước sau mở ký. Đây cũng là minh chứng rõ nét cho uy tín quốc tế ngày càng được khẳng định của Việt Nam trong lĩnh vực an ninh mạng và phòng, chống tội phạm xuyên quốc gia.

Chủ động, trách nhiệm từ sớm trong toàn bộ quá trình chuẩn bị và vận động quốc tế

Công ước Hà Nội được hình thành trong bối cảnh tội phạm mạng gia tăng nhanh chóng cả về quy mô, tính chất và mức độ gây hại. Các hành vi lừa đảo trực tuyến, tấn công hệ thống thông tin trọng yếu, xâm phạm dữ liệu cá nhân, chiếm đoạt tài sản qua mạng không còn bị giới hạn bởi biên giới quốc gia, trong khi cơ chế hợp tác quốc tế về pháp lý và thực thi vẫn còn những khoảng trống đáng kể.

Nhận thức rõ yêu cầu đó, Bộ Công an Việt Nam đã tham gia tích cực, thực chất vào tiến trình đàm phán, xây dựng Công ước, đồng thời chủ động phối hợp với các bộ, ngành liên quan tham mưu cho Đảng, Nhà nước về chủ trương đăng cai Lễ mở ký tại Hà Nội. Việc vận động để Hà Nội trở thành địa điểm mở ký Công ước không chỉ xuất phát từ điều kiện tổ chức, mà còn từ mong muốn đóng góp trách nhiệm của Việt Nam vào việc kiến tạo một chuẩn mực hợp tác toàn cầu công bằng, cân bằng và tôn trọng chủ quyền quốc gia.

Trong quá trình chuẩn bị, Bộ Công an đã phối hợp chặt chẽ với các cơ quan của Liên hợp quốc, các tổ chức quốc tế, các quốc gia thành viên và đối tác song phương để thống nhất nội dung, chương trình, nghi thức và các yêu cầu tổ chức. Công tác chuẩn bị được triển khai sớm, bài bản và khoa học, bảo đảm sự đồng bộ giữa nội dung chính trị - pháp lý, công tác đối ngoại và các điều kiện tổ chức thực tế. Đây là nền tảng quan trọng để Lễ mở ký diễn ra đúng kế hoạch, đạt được sự đồng thuận và đánh giá cao của cộng đồng quốc tế.

Tổ chức Lễ mở ký tại Hà Nội - dấu ấn về năng lực, uy tín và trách nhiệm quốc gia

Trong hai ngày 25 -26/10/2025, Hà Nội trở thành điểm hội tụ của đông đảo đoàn đại biểu quốc tế, đại diện các quốc gia, tổ chức quốc tế, các cơ quan của Liên hợp quốc và giới chuyên gia về an ninh mạng. Lễ mở ký Công ước được tổ chức trang trọng, đúng chuẩn mực nghi thức ngoại giao đa phương, đồng thời bảo đảm hiệu quả, thiết thực và phù hợp với thông lệ quốc tế.

Bộ Công an đã chủ trì, phối hợp xây dựng các phương án tổng thể về tổ chức, bảo đảm an ninh, an toàn, hậu cần và truyền thông cho sự kiện. Công tác bảo vệ được triển khai ở mức cao nhất, với sự phối hợp đồng bộ giữa các lực lượng, không để xảy ra bất kỳ tình huống bị động, bất ngờ nào. Lễ mở ký diễn ra an

Chiều ngày 25/10, trong khuôn khổ Lễ mở ký Công ước của Liên hợp quốc về chống tội phạm mạng, Thượng tướng Phạm Thế Tùng phát biểu tại phiên thảo luận toàn thể

toàn, thông suốt, đúng kế hoạch, qua đó khẳng định năng lực tổ chức và bản lĩnh của Việt Nam trong việc đăng cai các sự kiện đối ngoại đa phương quy mô lớn, có yêu cầu cao về an ninh.

Thành công của sự kiện còn được thể hiện qua sự tham gia tích cực và ủng hộ rộng rãi của cộng đồng quốc tế. Nhiều quốc gia đã trực tiếp ký Công ước ngay tại Hà Nội, thể hiện niềm tin vào khuôn khổ pháp lý mới cũng như vai trò điều phối, dẫn dắt của Việt Nam trong tiến trình này. Đây là sự ghi nhận rõ nét đối với những đóng góp thực chất của Bộ Công an Việt Nam trong phòng, chống tội phạm mạng và thúc đẩy hợp tác quốc tế trong lĩnh vực còn nhiều thách thức này.

Lan tỏa thông điệp Việt Nam - đất nước hòa bình, thân thiện, đối tác tin cậy

Vượt ra ngoài khuôn khổ một sự kiện pháp lý - đối ngoại, Lễ mở ký Công ước Hà Nội đã lan tỏa mạnh mẽ thông điệp về Việt Nam là một quốc gia hòa bình, ổn định, thân thiện và có trách nhiệm với cộng đồng quốc tế. Việc hàng trăm đoàn đại biểu quốc tế, trong đó có nhiều đoàn cấp cao, đến Hà Nội tham dự và làm việc trong môi trường an toàn, cởi mở và chuyên nghiệp đã tạo nên những ấn tượng sâu sắc về hình ảnh đất nước và con người Việt Nam.

Công tác tổ chức chu đáo, tinh thần hợp tác thiện chí, cùng việc bảo đảm an ninh, an toàn tuyệt đối đã góp phần xây dựng "không gian của niềm tin", nơi các quốc gia với những khác biệt về thể chế, trình độ phát triển và lợi ích có thể cùng đối thoại, tìm kiếm tiếng nói chung trước các thách thức an ninh phi truyền thống mang tính toàn cầu. Hà Nội, trong những ngày cuối thu năm 2025, không chỉ là địa điểm mở ký một Công ước quốc tế, mà còn trở thành biểu tượng của đối thoại, hợp tác và trách nhiệm chung.

Thông điệp mà Việt Nam gửi đi qua sự kiện này là rõ ràng và nhất quán: bảo đảm an ninh mạng không đối lập với hòa bình, hợp tác và phát triển, mà chính là điều kiện để bảo vệ con người, thúc đẩy kinh tế số và củng cố niềm tin trong quan hệ quốc tế. Với cách tiếp cận cân bằng, tôn trọng luật pháp quốc tế và quyền con người, Việt Nam tiếp tục khẳng định vai trò là đối tác tin cậy, thành viên tích cực và có đóng góp thực chất trong cộng đồng quốc tế.

Từ cam kết quốc tế đến hành động cụ thể

Lễ mở ký Công ước Hà Nội là điểm khởi đầu cho giai đoạn triển khai thực thi Công ước trên thực tế. Ngay sau sự kiện, Bộ Công an xác định rõ trọng tâm là tổ chức thực hiện hiệu quả các cam kết quốc tế, gắn kết chặt chẽ giữa

hội nhập quốc tế và hoàn thiện thể chế, nâng cao năng lực quốc gia về phòng, chống tội phạm mạng.

Các nhiệm vụ trọng tâm bao gồm: tăng cường hợp tác quốc tế trong tố tụng hình sự, hỗ trợ tư pháp và dẫn độ; xây dựng, hoàn thiện các cơ chế chia sẻ thông tin, chứng cứ điện tử; đào tạo, bồi dưỡng nguồn nhân lực chuyên sâu về điều tra tội phạm mạng và hợp tác quốc tế; đồng thời tiếp tục rà soát, hoàn thiện hệ thống pháp luật trong nước để bảo đảm tính thống nhất, đồng bộ và phù hợp với Công ước.

Việc Quốc hội Việt Nam thông qua Luật An ninh mạng (sửa đổi) năm 2025, có hiệu lực từ 1/7/2026, là minh chứng rõ nét cho quyết tâm chính trị trong

Thượng tướng Phạm Thế Tùng, Thứ trưởng Bộ Công an đã tiếp Thứ trưởng Bộ Nội vụ Kazakhstan Baurzhan Alenov, ngày 26/10 một ngày sau lễ mở ký

việc tạo dựng nền tảng pháp lý vững chắc để thực thi các cam kết quốc tế. Đây cũng thể hiện cách tiếp cận nhất quán của Việt Nam: kết hợp chặt chẽ giữa bảo đảm an ninh mạng và thúc đẩy phát triển kinh tế số, xã hội số một cách an toàn, bền vững.

Dấu mốc Hà Nội và giá trị lâu dài của hợp tác toàn cầu

Việc gắn tên Hà Nội với một Công ước đa phương toàn cầu về chống tội phạm mạng mang ý nghĩa vượt ra ngoài khuôn khổ một sự kiện đối ngoại đơn lẻ. Công ước Hà Nội trở thành biểu tượng của nỗ lực chung, của tinh thần hợp tác và trách nhiệm trong ứng phó với những thách thức an ninh mới của thời đại số.

Trong dấu mốc đó, đóng góp của Bộ Công an

> **Việc cộng đồng quốc tế lựa chọn Hà Nội làm nơi mở ký Công ước của Liên hợp quốc về chống tội phạm mạng là sự ghi nhận đối với vai trò, uy tín và trách nhiệm của Việt Nam trong kiến tạo một khuôn khổ hợp tác toàn cầu dựa trên pháp quyền và niềm tin.**

Việt Nam là trụ cột xuyên suốt, từ quá trình hình thành, tổ chức Lễ mở ký đến triển khai thực hiện sau này. Đây không chỉ là thành công của một sự kiện, mà là đóng góp lâu dài của Việt Nam vào việc kiến tạo một trật tự an ninh mạng toàn cầu công bằng, hiệu quả, dựa trên hợp tác, thượng tôn pháp luật và niềm tin số.

Trong không khí mùa Xuân - mùa của khởi đầu và hy vọng - nhìn lại chặng đường đã qua, có thể khẳng định rằng Công ước Hà Nội mở ra một chương mới trong hợp tác toàn cầu về chống tội phạm mạng. Một chương trong đó Việt Nam, với vai trò chủ động và trách nhiệm, tiếp tục đồng hành cùng cộng đồng quốc tế vì một không gian mạng an toàn, tin cậy, phục vụ hòa bình, ổn định và phát triển bền vững của mỗi quốc gia và của toàn thể nhân loại.

Sáng 21-10, tại Hà Nội, Thượng tướng Phạm Thế Tùng - Thứ trưởng Bộ Công an, Trưởng Tiểu ban An ninh - Y tế/An ninh, trật tự Lễ mở ký Công ước của Liên hợp quốc về chống tội phạm mạng (Lễ mở ký) đã chủ trì Phiên họp đánh giá công tác bảo đảm an ninh, trật tự và y tế lễ mở ký

AN NINH MẠNG TRONG KỶ NGUYÊN MỚI

Lá chắn số cho khát vọng vươn mình

Trung tướng, Tiến sĩ Lê Xuân Minh

Cục trưởng Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao,
Phó Chủ tịch Điều hành Hiệp hội An ninh mạng quốc gia

Lịch sử 4.000 năm dựng nước và giữ nước của dân tộc ta là lịch sử của những cuộc trường kỳ kháng chiến bảo vệ bờ cõi. Từng trang sử được viết bằng xương máu của lớp lớp người Việt Nam đánh đổi từng tấc đất liền, từng bước sóng cả trên lãnh thổ biển khơi. Nhưng hôm nay, bờ cõi Việt Nam không chỉ nằm ở dải đất hình chữ S, mà còn trải dài vô tận trên không gian số. Đây là một không gian không có cột mốc biên cương hữu hình, nơi các cuộc tấn công có thể diễn ra trong tích tắc từ cách nửa vòng trái đất, nhắm trực tiếp vào hạ tầng trọng yếu và – nguy hiểm hơn là nhắm vào nhận thức của 100 triệu đồng bào. An ninh mạng vì thế trở thành "mặt trận mới" mà thành bại trên mặt trận này có ý nghĩa sống còn với sự ổn định và phát triển bền vững của mỗi quốc gia.

Chủ quyền không chỉ là những cột mốc hữu hình

Không gian mạng đã trở thành một thế giới phẳng không có cột mốc biên cương hữu hình, nơi chúng ta đang phải đối mặt với ba thách thức khốc liệt mang tính toàn cầu.

Một là, sự bùng nổ của các cuộc tấn công mạng có chủ đích và gián điệp mạng. Không còn là những hành vi phá hoại đơn lẻ, các chiến dịch tấn công hiện nay nhắm trực tiếp vào hạ tầng trọng yếu và chuỗi cung ứng toàn cầu. Các nhóm tin tặc nước ngoài đang đẩy mạnh tấn công vào các ban, bộ, ngành, địa phương, đặc biệt là các tập đoàn kinh tế lớn về tài chính, công nghệ và năng lượng. Việc thu thập, mua bán dữ liệu trái phép diễn ra ở quy mô công nghiệp, biến thông tin trở thành một loại vũ khí có thể làm tê liệt hoạt động của cả một quốc gia trong tích tắc.

Hai là, sự bùng nổ của thông tin xấu độc và sự thao túng của Trí tuệ nhân tạo (AI). Chỉ tính riêng năm 2025, lực lượng chức năng đã phát hiện 16 trang mạng, blog cùng hơn 7.400 tài khoản, fanpage và kênh Youtube, Tiktok đăng tải hơn 31.200 bài viết, video có nội dung độc hại. Đáng lo ngại hơn, các đối tượng đã triệt để lợi dụng AI như ChatGPT, Gemini, Deepseek hay Grok để ngụy tạo hình ảnh, tiếng nói (Deepfake) của lãnh đạo cấp cao nhằm lừa đảo và phá hoại tư tưởng, làm xói mòn niềm tin xã hội.

Ba là, tội phạm mạng xuyên quốc gia với thủ đoạn tinh vi. Năm 2025, chúng ta đã phát hiện, xử lý gần 5.000 vụ việc lừa đảo qua mạng với thiệt hại lên đến

Chủ quyền số không chỉ là những cột mốc hữu hình

hơn 3.400 tỷ đồng. Các thủ đoạn "bắt cóc online", giả danh lực lượng chức năng hay "tín dụng đen" trực tuyến diễn ra nhức nhối, nhắm trực tiếp vào những người yếu thế và sự bình an của mỗi gia đình.

Trước những thách thức này, quyết tâm chính trị của Đảng tại các văn bản chỉ đạo, đặc biệt là Chỉ thị số 57-CT/TW đã xác lập một quan điểm nhất quán: An ninh mạng là vấn đề chiến lược, có ý nghĩa sống còn. "Công cuộc chuyển đổi số đặt ra yêu cầu cấp bách đối với công tác bảo đảm an ninh thông tin,an ninh dữ liệu, an ninh mạng quốc gia trong tình hình mới". Tức là chúng ta không chọn cách đóng cửa không gian mạng để giữ an toàn, vì điều đó đồng nghĩa với việc tự tước đi cơ hội phát triển. Thay vào đó, chúng ta chọn cách hành động quyết liệt để biến không gian này thành một "vùng xanh" cho sự sáng tạo và phát triển của người dân.

Với vai trò người bảo vệ, Cục An ninh mạng và Phòng, chống tội phạm sử dụng công nghệ cao đã chọn cách hành động quyết liệt và hiệu quả dựa trên tư duy "Chủ động phòng thủ - Tích cực kiến tạo". Bảo vệ không gian mạng chính là bảo vệ sự bình yên của mỗi mái nhà, sự trong sáng trong tâm hồn của mỗi trẻ em và sự vững vàng trong niềm tin của mỗi công dân vào sự phát triển Đất nước.

Lá chắn số và vùng xanh sáng tạo cho khát vọng vươn mình

Năm 2025 là thời điểm mà lực lượng an ninh mạng chuyển mình mạnh mẽ từ vị thế "đấu tranh phòng ngự" sang "chủ động kiến tạo". Mục tiêu không chỉ dừng lại ở việc ngăn chặn tội phạm, mà cao hơn là xây dựng một môi trường số đủ an toàn để trở thành mảnh đất lành cho những khát vọng sáng tạo của người Việt vươn xa. Để hiện thực hóa mục tiêu này, lực lượng an ninh mạng đã triển khai đồng bộ 8 nhóm biện pháp quyết liệt.

Thứ nhất, chuyển dịch từ quản lý kỹ thuật đơn thuần sang dự báo chiến lược và quản trị rủi ro. Thay vì chỉ ứng phó khi sự cố xảy ra, lực lượng đã chủ động thu thập thông tin trên "đa địa bàn, đa lĩnh vực, đa mục tiêu" để phục vụ hoạch định chính sách của Đảng và Nhà nước. Hệ thống giám sát an ninh mạng quốc gia (NOC) thế hệ mới, sử dụng hoàn toàn giải pháp công nghệ trong nước, hiện có khả năng phân tích dữ liệu lớn để dự báo sớm các xu hướng tấn công từ khi chúng còn là mầm mống.

Thứ hai, thiết lập lá chắn bảo vệ tuyệt đối hạ tầng thông tin quốc gia. Hiện nay, lực lượng chuyên trách đang tổ chức giám sát an ninh mạng thường xuyên cho 37 hệ thống của 27 đơn vị chủ quản trọng yếu, xử lý trung bình mỗi ngày trên 218.000 cảnh báo tấn công mạng. Với năng lực này, tỷ lệ ngăn chặn thành công các cuộc tấn công vào hệ thống dữ liệu quốc gia đạt mức 99,8%. Đồng thời, trong hai năm qua, an ninh mạng đã được bảo đảm tuyệt đối cho 28 hội nghị và sự kiện chính trị quan trọng nhất của đất nước.

Thứ ba, đột phá trong đấu tranh phòng chống tội phạm mạng xuyên quốc gia. Năm qua, lực lượng đã triệt phá thành công 35 chuyên án lớn, khởi tố 1.597 vụ án với 1.712 bị can. Đặc biệt, chúng ta đã lần đầu

Trung tướng Lê Xuân Minh - Cục trưởng Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05, Bộ Công an), Phó Chủ tịch Điều hành Hiệp hội An ninh mạng quốc gia

tiên mở rộng phạm vi đấu tranh ra ngoài lãnh thổ khi cử các tổ công tác đặc biệt phối hợp với Cảnh sát Thái Lan, Lào, Campuchia bắt giữ hàng trăm đối tượng lừa đảo và đánh bạc trực tuyến. Những chiến dịch như "CleanNet 24/25" đã xóa sổ hơn 3.200 trang web giả mạo, thu hồi tài sản trị giá hơn 8.500 tỷ đồng cho người dân.

Thứ tư, đổi mới sáng tạo trong xây dựng thế trận an ninh nhân dân trên không gian mạng. Với tư duy "lấy dân làm gốc", chọn hướng đi "Gần dân nhất", chiến dịch truyền thông "Không Một Mình" đã đạt con số kỷ lục 1,5 tỷ lượt xem trên mạng xã hội và tiếp cận trực tiếp hơn 40 triệu người dân. Tại các địa phương, mô hình "Tổ an ninh mạng cộng đồng" đã hướng dẫn kỹ năng tự bảo vệ cho hơn 20 triệu lượt người dân. Đặc biệt, Hội nghị KOL Summit 2025 đã quy tụ gần 300 người có ảnh hưởng lớn để lan tỏa các giá trị nhân văn, hình thành Liên minh "Niềm tin số" bảo vệ cộng đồng khỏi những nội dung sai lệch. Tuyên truyền ANM đã trở thành " bình dân học vụ số".

Thứ năm, tiên phong làm chủ công nghệ lõi và hiện đại hóa lực lượng. Hệ sinh thái Signet do lực lượng tự nghiên cứu đã trở thành nền tảng bảo mật then chốt với hơn 377.000 tài khoản sử dụng thường xuyên. Các giải pháp "Phòng họp không giấy" và quản lý thiết bị di động an toàn đã giúp xóa bỏ hoàn toàn nguy cơ lộ lọt tài liệu mật, tạo điểm nhấn về năng lực công nghệ "Make in Vietnam".

Thứ sáu, thúc đẩy đa phương hóa hoạt động hợp tác quốc tế. Việt Nam không chỉ đào tạo và phối hợp thực thi pháp luật với các nước Úc, Nhật Bản, Hàn Quốc mà còn xúc tiến thành lập Trung tâm phòng, chống tội phạm mạng khu vực của Liên hợp quốc tại Việt Nam. Sự kiện chủ trì tổ chức Lễ mở ký Công ước Hà Nội với sự tham gia của 119 quốc gia đã khẳng định vị thế dẫn dắt của Việt Nam trong việc xây dựng chuẩn mực an ninh toàn cầu.

Thứ bảy, quyết liệt tháo gỡ điểm nghẽn về thể chế và hành lang pháp lý. Việc tham mưu ban hành Luật Bảo vệ dữ liệu cá nhân (có hiệu lực từ 1/1/2026) cùng Luật An ninh mạng 2025 và Chỉ thị 57 của Ban Bí thư đã tăng cường hoàn thiện hệ thống pháp luật an ninh mạng. Đây là bước ngoặt quan trọng để bảo vệ nhóm yếu thế và củng cố niềm tin số, góp phần kiến tạo môi trường kinh doanh an toàn – nơi các doanh nghiệp trong nước tăng trưởng 25% ngay trong năm đầu thực thi.

Thứ tám, gương mẫu đi đầu trong cải cách thủ tục hành chính phục vụ nhân dân. Từ tháng 3/2025, khi chức năng quản lý Nhà nước về an toàn thông tin được thống nhất đầu mối về lực lượng an ninh mạng, các quy trình đã được tối ưu hóa mạnh mẽ. Thủ tục cấp giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin hiện đã được rút ngắn tới 62% thời gian, giúp tiết kiệm đáng kể chi phí cho doanh nghiệp và kiến tạo môi trường kinh doanh minh bạch.

Nhờ những biện pháp đồng bộ này, kinh tế số Việt Nam năm 2025 đã đóng góp khoảng 20% GDP. Khi người dân không còn lo sợ bị lừa đảo hay xâm phạm dữ liệu, họ sẽ dấn thân sâu hơn vào nền kinh tế tri thức, biến không gian mạng thành động lực thực sự cho khát vọng vươn mình của dân tộc.

Từ Công ước Hà Nội đến Luật An ninh mạng 2025 và Chỉ thị 57 – bước tiến dài vì Việt Nam tự cường, tự chủ

Nhìn lại hành trình đã qua, việc mở ký Công ước Hà Nội không đơn thuần là một sự kiện ngoại giao; đó là biểu tượng về bản lĩnh Việt Nam trên trường quốc tế. Việc chúng ta chủ động đề xuất và thúc đẩy Công ước đã biến Việt Nam từ một "người tham gia" trở

thành "người thiết lập luật chơi". Ngay sau đó, Luật An ninh mạng 2025 được thông qua, cùng với sự ra đời của Chỉ thị số 57-CT/TW ngày 31/12/2025 của Ban Bí thư như một "mệnh lệnh chiến lược", yêu cầu tăng cường bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong toàn hệ thống chính trị.

Bám sát tinh thần Báo cáo chính trị trình Đại hội XIV, Luật An ninh mạng 2025 được xây dựng dựa trên nguyên lý: An ninh là để phục vụ phát triển, và phát triển phải dựa trên sự an toàn của con người. Lấy nhân dân làm trung tâm, xây dựng thế trận an ninh nhân dân, Luật không chỉ ngăn chặn tội phạm mạng, mà còn bảo vệ quyền riêng tư, quyền được tiếp cận thông tin sạch, quyền được phát triển toàn diện của mỗi cá nhân trên không gian số.

Lá chắn số và vùng xanh sáng tạo cho khát vọng vươn mình

Chỉ thị 57 khẳng định: An ninh mạng phải được đặc biệt coi trọng trong quá trình chuyển đổi số quốc gia, triển khai Chính phủ điện tử. Lực lượng ninh mạng thực thi Chỉ thị này không bằng các khẩu hiệu, mà bằng phương châm: "Lựa chọn đúng - Triển khai nhanh - Làm đến nơi đến chốn - Đo lường bằng kết quả". Chúng ta đã biến các cam kết quốc tế thành hành động cụ thể: tỷ lệ tin giả, thông tin độc hại nhắm vào Việt Nam đã giảm mạnh 40% trong năm đầu thực thi. An ninh mạng lúc này không còn là những dòng mã khô khan, mà là sự bảo vệ bình an cho tư duy và tình cảm của từng gia đình, đặc biệt là bảo vệ trẻ em trước các thuật toán thao túng hành vi.

Hành trình giữ vững "vùng xanh" số trong năm 2025 đã cho thấy một bài học quý giá: An ninh mạng không chỉ là công việc của lực lượng chuyên trách, mà là sự hiệp đồng giữa công nghệ, pháp luật và sự đồng lòng của nhân dân. Những chiến dịch đã triển khai, những con số đã đạt được mới chỉ là khởi đầu. Chúng ta sẽ tiếp tục kiên trì với con đường bảo vệ nhân tính và quyền tự chủ của người Việt trên không gian mạng, để mỗi bước đi trên con đường số đều là bước đi của phát triển bền vững và khát vọng vươn mình.

Sự kiên định đồng lòng và bản lĩnh, trí tuệ của cán bộ, chiến sĩ lực lượng ninh mạng sẽ là nền móng vững chắc cho những sáng kiến tầm vóc hơn trong tương lai – nơi Hà Nội không chỉ là tên của một Thủ đô ngàn năm văn hiến, mà còn là tên của một chuẩn mực về An ninh mạng nhân văn cho thế giới khi bước vào kỷ nguyên của trí thông minh nhân tạo – cũng là lúc mà nhân tính và phẩm giá nguyên bản của con người đứng trước những thách thức chưa từng có.

Hành trình vươn mình của dân tộc bắt đầu từ sự vững vàng của từng bit dữ liệu, từ sự an toàn của từng ý nghĩ và từ niềm tin sắt đá vào một nước Việt Nam tự chủ, tự tôn, tự lực, tự cường trên mọi không gian.

Lá chắn số và vùng xanh sáng tạo cho khát vọng vươn mình

Hợp lực quốc gia hiện thực hóa Nghị quyết 57-NQ/TW trong Kỷ nguyên chủ quyền số

Lam Nguyên - Thu Uyên (Thực hiện)

Tổng Bí thư Tô Lâm phát biểu chỉ đạo tại Hội nghị tổng kết công tác năm 2025 và nhiệm vụ, giải pháp trọng tâm năm 2026 của Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số.

Chuyển đổi số đang trở thành trục tái thiết mô hình phát triển quốc gia, gắn trực tiếp với chủ quyền số, tự chủ công nghệ và năng lực cạnh tranh dài hạn của Việt Nam. Sau hơn một năm triển khai Nghị quyết 57-NQ/TW của Bộ Chính trị, những chuyển động căn bản về tư duy quản trị, hoàn thiện thể chế, bảo đảm an ninh mạng – an ninh dữ liệu và vai trò dẫn dắt của doanh nghiệp đang dần định hình một mô hình phát triển mới, trong đó hợp lực quốc gia được xác lập là điều kiện tiên quyết. Sau giai đoạn chạy đà của năm đầu triển khai, Nghị quyết 57 đang bước vào giai đoạn đòi hỏi tăng tốc, lấy mục tiêu, sản phẩm và hiệu quả thực chất làm thước đo. Nhân dịp Xuân Bính Ngọ 2026, Tạp chí An ninh mạng Việt Nam có cuộc trao đổi với ông Nguyễn Huy Dũng, Ủy viên dự khuyết Ban Chấp hành Trung ương Đảng, Ủy viên Ban Chỉ đạo Trung ương về chuyển đổi số, Phó Chủ tịch Hiệp hội An ninh mạng quốc gia về chuyển đổi số, xoay quanh những vấn đề mang tính nền tảng và chiến lược trong hiện thực hóa Nghị quyết 57-NQ/TW.

Chuyển đổi số - nền tảng tái thiết mô hình phát triển quốc gia

- Sau hơn một năm triển khai Nghị quyết 57-NQ/TW, đâu là chuyển biến quan trọng nhất trong tư duy quản trị phát triển quốc gia?

Ông Nguyễn Huy Dũng: Chuyển biến quan trọng nhất không nằm ở việc tăng thứ hạng trên các bảng xếp hạng, mà ở sự thay đổi căn bản trong cách tiếp cận khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số trong quản trị quốc gia.

Tư duy quản trị đã chuyển từ "tin học hóa, ứng dụng công nghệ" sang tái thiết mô hình phát triển dựa trên tri thức và dữ liệu. Nghị quyết 57 xác định rõ khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số là đột phá chiến lược hàng đầu để phát triển lực lượng sản xuất hiện đại, hoàn thiện quan hệ sản xuất và nâng cao năng lực cạnh tranh quốc gia. Chuyển đổi số, vì thế, không còn là câu chuyện mua sắm công nghệ, mà là sắp xếp lại cách quản trị, cách vận hành toàn bộ nền kinh tế, xã hội trên nền tảng số.

Cùng với đó, tư duy "người dân và doanh nghiệp là trung tâm, là chủ thể" được đặt ở vị trí trung tâm. Nhà nước chuyển mạnh sang vai trò kiến tạo, dẫn dắt và thiết lập luật chơi; doanh nghiệp và giới khoa học trở thành lực kéo chính của đổi mới sáng tạo. Chỉ trong hơn một năm qua, Quốc hội và Chính phủ đã ban hành hoặc quyết định 17 luật, gần 60 nghị định và hơn 60 thông tư liên quan trực tiếp đến khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số.

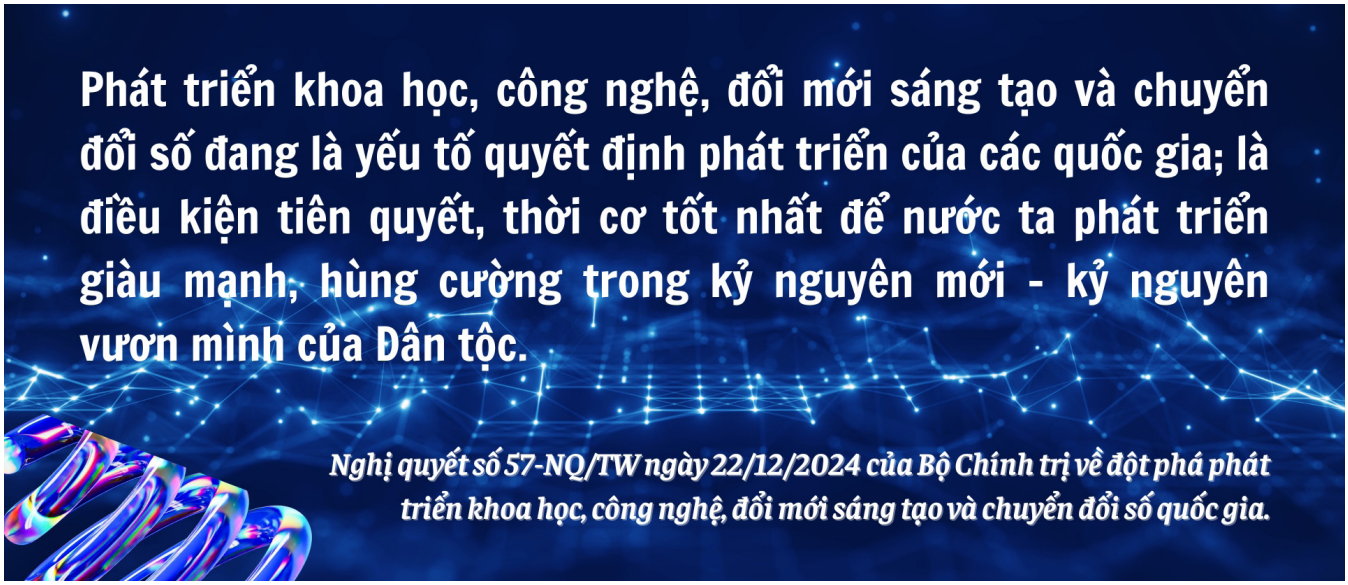
Đặc biệt, chủ quyền số, tự chủ công nghệ và an ninh dữ liệu được xác lập là yêu cầu xuyên suốt. Nghị quyết 57 khẳng định rõ: bảo đảm chủ quyền quốc gia trên không gian mạng, an ninh mạng và an ninh dữ liệu là điều kiện không thể tách rời của phát triển. Đây là bước tiến quan trọng về tư duy chiến lược: an ninh không đi sau phát triển, mà được tích hợp ngay trong thiết kế tổng thể của mô hình phát triển quốc gia.

"Làm nhanh - vá sau" và những rủi ro hệ thống

Nghị quyết 57-NQ/TW xác lập quan điểm coi an toàn, an ninh mạng và an ninh dữ liệu là điều kiện tiên

Ông Nguyễn Huy Dũng

Ủy viên dự khuyết Ban Chấp hành Trung ương Đảng, Ủy viên Ban Chỉ đạo Trung ương về chuyển đổi số, Phó Chủ tịch Hiệp hội An ninh mạng quốc gia.



quyết của chuyển đổi số. Những rủi ro lớn nhất sẽ phát sinh nếu tiếp cận theo tư duy "làm nhanh - vá sau"?

Ông Nguyễn Huy Dũng: Nếu chuyển đổi số được triển khai theo tư duy "làm nhanh - vá sau", sẽ xuất hiện ba nhóm rủi ro mang tính hệ thống.

Thứ nhất là rủi ro về kiến trúc và hạ tầng. Việc triển khai chắp vá, thiếu thiết kế tổng thể tạo ra nhiều điểm yếu, đặc biệt trước các hình thức tấn công chuỗi cung ứng, ransomware hoặc chiếm quyền điều khiển hệ thống trọng yếu. Dữ liệu không được chuẩn hóa, phân tán và thiếu mô hình quản trị thống nhất rất dễ dẫn đến lộ lọt dữ liệu cá nhân, dữ liệu định danh và dữ liệu tài chính.

Thứ hai là rủi ro phụ thuộc công nghệ. Việc triển khai vội vàng trên các nền tảng và công nghệ lõi nước ngoài, trong khi thiếu chiến lược nội địa hóa và đánh giá đầy đủ rủi ro dữ liệu xuyên biên giới, sẽ khiến nền kinh tế số rơi vào trạng thái lệ thuộc và bị "khóa" trong hệ sinh thái của bên thứ ba.

Thứ ba là rủi ro xã hội và niềm tin số. Dịch vụ số triển khai nhanh nhưng không an toàn sẽ khiến người dân trở thành đối tượng của lừa đảo, mạo danh, deepfake..., từ đó làm suy giảm niềm tin vào chính quyền số và nền kinh tế số.

Vì vậy, an toàn thông tin và bảo vệ dữ liệu cá nhân phải được tích hợp ngay từ khâu quy hoạch, thiết kế kiến trúc và lựa chọn công nghệ, chứ không phải "gắn thêm" ở giai đoạn cuối. Hệ thống pháp luật mới đang được hoàn thiện theo hướng quản lý để phát triển, đặt ra các tiêu chuẩn rõ ràng về xử lý dữ liệu, AI an toàn, trách nhiệm của các chủ thể tham gia; đồng thời thúc đẩy các nguyên tắc như zero trust, quản trị danh tính số và từng bước nội địa hóa các hạ tầng, dữ liệu và dịch vụ an ninh mạng trọng yếu nhằm bảo đảm chủ quyền số.

Hợp lực quốc gia - kiến tạo hệ sinh thái phòng thủ số thống nhất

"Hợp lực quốc gia" trong lĩnh vực an ninh mạng và an toàn dữ liệu cần được tổ chức như thế nào để hình thành một hệ sinh thái phòng thủ số thống nhất, thưa ông?

Ông Nguyễn Huy Dũng: Tinh thần cốt lõi của Nghị quyết 57 là huy động và tổ chức sức mạnh của toàn xã hội. Trong lĩnh vực an ninh mạng và an toàn dữ liệu, hợp lực quốc gia cần được tổ chức theo cấu trúc nhiều tầng, gắn kết chặt chẽ.

Ở tầng chiến lược, Nhà nước giữ vai trò kiến trúc sư, thống nhất kiến trúc phòng thủ số quốc gia, gắn chặt an ninh mạng, an ninh dữ liệu với triển khai Nghị quyết 57 và hệ thống pháp luật liên quan; đồng thời xây dựng tiêu chuẩn, chuẩn mực kỹ thuật, cơ chế chia sẻ dữ liệu an toàn và phương thức phối hợp ứng phó sự cố trên không gian mạng.

Ở tầng triển khai, doanh nghiệp và các đơn vị chuyên môn giữ vai trò nòng cốt. Các doanh nghiệp công nghệ số và doanh nghiệp an ninh mạng trực tiếp thiết kế, vận hành, giám sát và ứng cứu. Các trung tâm SOC, CERT, trung tâm dữ liệu và nền tảng số cần được kết nối thành mạng lưới thống nhất, chia sẻ theo thời gian thực các mối đe dọa và chỉ dấu tấn công.

Ở tầng cộng đồng, các hiệp hội nghề nghiệp và tổ chức xã hội đóng vai trò cầu nối giữa Nhà nước, doanh

nghiệp, xã hội; từ xây dựng tiêu chí niềm tin số, đào tạo nhân lực đến truyền thông nâng cao nhận thức. Mỗi người dân cũng là một mắt xích quan trọng trong việc bảo vệ không gian mạng an toàn, lành mạnh.

Doanh nghiệp Make in Vietnam và bài toán làm chủ công nghệ lõi

Vậy thưa ông, trong tiến trình hiện thực hóa Nghị quyết 57-NQ/TW, đâu là những nút thắt lớn nhất mà doanh nghiệp công nghệ số Make in Vietnam cần vượt qua?

Ông Nguyễn Huy Dũng: Doanh nghiệp công nghệ số Make in Vietnam được xác định là lực lượng nòng cốt trong hiện thực hóa các mục tiêu lớn của đất nước. Tuy nhiên, để tham gia sâu vào chuỗi giá trị số toàn cầu, cần nhìn thẳng vào những nút thắt căn bản.

> **An ninh mạng không chỉ là một lĩnh vực kỹ thuật, mà là một phần danh dự nghề nghiệp trong kỷ nguyên chủ quyền số.**
>
> **Ông Nguyễn Huy Dũng**
> *Ủy viên dự khuyết Ban Chấp hành Trung ương Đảng, Ủy viên Ban Chỉ đạo Trung ương về chuyển đổi số, Phó Chủ tịch Hiệp hội An ninh mạng quốc gia.*

Trước hết là công nghệ lõi và sự phụ thuộc vào hạ tầng nước ngoài, từ hệ điều hành, vi mạch, nền tảng cloud đến nền tảng AI. Nếu không từng bước làm chủ các thành tố này, rất khó nâng cao giá trị gia tăng và khả năng chống chịu trước các biến động địa chính trị, thương mại và công nghệ toàn cầu.

Thứ hai là năng lực an toàn, bảo mật theo tư duy "by design". An toàn thông tin phải được coi là lợi thế cạnh tranh, không chỉ là chi phí. Việc tuân thủ các chuẩn mực quốc tế về bảo vệ dữ liệu cá nhân, an ninh thông tin và AI có trách nhiệm là điều kiện tiên quyết để sản phẩm công nghệ Việt Nam bước ra thị trường toàn cầu.

Thứ ba là nhân lực chuyên sâu và vốn dài hạn cho các lĩnh vực công nghệ lõi như bán dẫn, trí tuệ nhân tạo và an ninh mạng. Đây không chỉ là bài toán của doanh nghiệp, mà là thước đo năng lực tự chủ số và sức cạnh tranh dài hạn của nền kinh tế Việt Nam.

Trách nhiệm thế hệ trong kỷ nguyên chủ quyền số

Trong bối cảnh Nghị quyết 57-NQ/TW đang bước vào giai đoạn triển khai quyết liệt và toàn diện, ông đặt kỳ vọng gì đối với thế hệ trẻ và cộng đồng công nghệ – an ninh mạng Việt Nam?

Yếu tố quyết định trong giai đoạn tới không chỉ nằm ở cơ chế hay nguồn lực đầu tư, mà ở ý thức trách nhiệm và tinh thần dấn thân của con người, đặc biệt là thế hệ trẻ và cộng đồng công nghệ, an ninh mạng Việt Nam. Trọng tâm triển khai từ năm 2026 không còn là "đã làm gì", mà là "tạo ra giá trị gì" cho tăng trưởng, năng suất và đời sống xã hội.

Chủ quyền quốc gia ngày nay không chỉ được xác lập trên đất liền, trên biển, mà còn trên không gian mạng và trong từng dòng dữ liệu. Không gian số đã trở thành một mặt trận phát triển gắn liền với bảo vệ Tổ quốc, tác động trực tiếp tới an ninh, kinh tế và tương lai dài hạn của đất nước.

Tôi cho rằng, làm chủ công nghệ phải luôn song hành với đạo đức số và trách nhiệm xã hội. Việc bảo vệ người dùng, bảo vệ dữ liệu cá nhân và giữ gìn niềm tin xã hội cần được coi là chuẩn mực nghề nghiệp trong kỷ nguyên số.

Xin trân trọng cảm ơn ông!

CÔNG ƯỚC HÀ NỘI DẤU ẤN VIỆT NAM TRÊN BẢN ĐỒ AN NINH MẠNG TOÀN CẦU

★ 1. Công ước Hà Nội và dấu ấn ngoại giao Việt Nam trong kiến tạo khuôn khổ hợp tác quốc tế về an ninh mạng và phòng, chống tội phạm mạng

★ 2. Công ước Hà Nội: Từ dấu mốc đa phương đến cơ hội kiến tạo niềm tin số cho Việt Nam

★ 3. Công ước Hà Nội: Nền tảng mới cho một không gian số an toàn

★ 4. Từ phân mảnh pháp lý đến đồng thuận toàn cầu về an ninh mạng

★ 5. Công ước của Liên hợp quốc về chống tội phạm mạng

Công ước Hà Nội và dấu ấn ngoại giao Việt Nam trong kiến tạo khuôn khổ hợp tác quốc tế về an ninh mạng và phòng, chống tội phạm mạng

Đặng Hoàng Giang
Thứ trưởng Bộ Ngoại giao

Việc Liên hợp quốc thông qua Công ước về chống tội phạm mạng và lựa chọn Hà Nội làm nơi tổ chức Lễ mở ký không chỉ là một sự kiện pháp lý quốc tế, mà còn là dấu mốc ngoại giao đa phương đặc biệt quan trọng. Trong tiến trình đó, Việt Nam đã thể hiện vai trò chủ động, trách nhiệm và xây dựng, góp phần thúc đẩy đồng thuận toàn cầu về quản trị không gian mạng, trên cơ sở tôn trọng luật pháp quốc tế, chủ quyền quốc gia và quyền con người.

Ông Đặng Hoàng Giang - Thứ trưởng Bộ Ngoại giao

Hà Nội đăng cai Lễ mở ký Công ước Liên hợp quốc về chống tội phạm mạng từ ngày 25 đến 26/10/2025.

Bước sang năm 2026, trong bối cảnh thế giới tiếp tục biến động sâu sắc dưới tác động đan xen của cạnh tranh chiến lược, xu thế toàn cầu hóa và chuyển đổi số, bảo đảm an ninh, an toàn không gian mạng đã trở thành một trong những yêu cầu lớn nhất đối với mỗi quốc gia và cộng đồng quốc tế. Không gian mạng, từ chỗ là công cụ hỗ trợ phát triển, đã trở thành không gian chiến lược mới, gắn chặt với an ninh quốc gia, trật tự xã hội, niềm tin của người dân và sự vận hành ổn định của nền kinh tế số toàn cầu. Những thách thức an ninh phi truyền thống mới, trong đó có tội phạm mạng, đang nổi lên với mức độ tinh vi ngày càng cao, phạm vi tác động ngày càng rộng và tính chất xuyên biên giới ngày càng rõ nét.

Trong bối cảnh đó, việc Liên hợp quốc thông qua Công ước Liên hợp quốc về chống tội phạm mạng và quyết định tổ chức Lễ mở ký Công ước tại Hà Nội (Công ước Hà Nội) không chỉ đánh dấu một sự kiện pháp lý quốc tế quan trọng, mà còn thể hiện sự ghi nhận đối với vai trò, uy tín và trách nhiệm ngày càng cao của Việt Nam trong việc tham gia và định hình các khuôn khổ hợp tác quốc tế về an ninh mạng và phòng, chống tội phạm mạng.

Công ước Hà Nội và dấu ấn của Việt Nam

Công ước Hà Nội là văn kiện pháp lý đầu tiên ở cấp độ toàn cầu, điều chỉnh toàn diện các vấn đề liên quan đến phòng, chống tội phạm mạng, thiết lập một khuôn khổ hợp tác quốc tế thống nhất, dựa trên các nguyên tắc cơ bản của luật pháp quốc tế, bao gồm tôn trọng chủ quyền quốc gia, toàn vẹn lãnh thổ và quyền con người.

Tiến trình đàm phán Công ước được khởi động theo Nghị quyết 74/247 của Đại hội đồng Liên hợp quốc năm 2019 là một trong những tiến trình phức tạp nhất trong nhiều năm qua. Với sự tham gia đàm phán của hơn 150 quốc gia cùng các tổ chức quốc tế liên chính phủ, phi chính phủ, và đặc biệt là các tập đoàn công nghệ, các bên đã phải đối mặt với nhiều bất đồng sâu sắc liên quan đến phạm vi điều chỉnh, nội dung hình sự hóa hành vi phạm tội và cơ chế bảo đảm quyền con người. Tuy nhiên, với tinh thần đối thoại và trách nhiệm, các quốc gia đã từng bước thu hẹp khác biệt để tiến tới đồng thuận, thông qua toàn văn Công ước vào cuối năm 2024.

Nhận thức rõ những nguy cơ và thách thức từ tội phạm mạng, Việt Nam từ sớm đã có chủ trương nhất quán ủng hộ việc xây dựng một khuôn khổ pháp lý quốc tế

mang tính phổ quát, đặt dưới sự điều phối của Liên hợp quốc, nhằm tạo nền tảng hợp tác bình đẳng, hiệu quả giữa các quốc gia trong phòng, chống tội phạm mạng. Với phương châm tích cực, chủ động tham gia vào định hình các khuôn khổ pháp lý, bảo đảm tốt nhất lợi ích của Việt Nam, Bộ Ngoại giao đã giữ vai trò nòng cốt trong tham mưu chiến lược, điều phối liên ngành và triển khai ngoại giao đa phương, phối hợp chặt chẽ với Bộ Công an, các bộ, ngành liên quan và Phái đoàn Việt Nam tại Liên hợp quốc, tham gia thương lượng Công ước từ những ngày đầu tiên. Trong suốt quá trình đàm phán, Việt Nam đã phát huy vai trò chủ động, tích cực và xây dựng, với tinh thần tôn trọng khác biệt, thúc đẩy đồng thuận và tìm kiếm giải pháp. Việt Nam đã góp phần quan trọng thúc đẩy nhiều nội dung then chốt của Công ước, cân bằng giữa an ninh và phát triển, giữa tôn trọng chủ quyền và bảo vệ quyền con người trên không gian chung, đồng thời, thúc đẩy hỗ trợ kỹ thuật, thu hẹp khoảng cách số và nâng cao năng lực cho các nước đang phát triển. Những đóng góp của Việt Nam được đánh giá cao, bởi tính thực tiễn, cân bằng, hài hòa, phản ánh tiếng nói và quan tâm chính đáng của các nước, đặc biệt các nước đang phát triển.

Hà Nội- điểm hội tụ của cam kết quốc tế

Lễ mở ký Công ước Hà Nội được tổ chức vào ngày 25-26/10/2025 tại Hà Nội, dưới sự chủ trì của Chủ tịch nước Lương Cường, sự tham dự của Tổng Thư ký Liên hợp quốc và Nguyên thủ, Lãnh đạo Chính phủ, lãnh đạo bộ, ngành của 119 quốc gia thành viên Liên hợp quốc. Việc 72 quốc gia ký Công ước ngay tại Lễ mở ký (đến nay có 74 nước đã ký Công ước) cho thấy sự hưởng ứng rộng rãi và niềm tin của cộng đồng quốc tế đối với khuôn khổ pháp lý mới này.

Phát biểu tại Lễ mở ký, Tổng Thư ký Liên hợp quốc António Guterres khẳng định "Việt Nam là một trụ cột quan trọng trong hệ thống đa phương", đánh giá cao việc Việt Nam đăng cai Lễ mở ký Công ước Hà Nội, cho rằng đây là biểu hiện rõ nét của một quốc gia thành viên tích cực, có trách nhiệm trong hệ thống đa phương, đã nhiều lần đóng góp thực chất vào các tiến trình then chốt của Liên hợp quốc. Tổng Thư ký nhấn mạnh rằng Việt Nam không chỉ tham gia, mà còn chủ động thúc đẩy đối thoại, xây dựng đồng thuận và tạo không gian hợp tác bao trùm giữa các quốc gia có trình độ phát triển và

"Việc Liên hợp quốc lựa chọn Hà Nội làm nơi tổ chức Lễ mở ký Công ước không chỉ đánh dấu một sự kiện pháp lý quốc tế quan trọng, mà còn thể hiện sự ghi nhận đối với vai trò, uy tín và trách nhiệm ngày càng cao của Việt Nam trong việc tham gia và định hình các khuôn khổ hợp tác quốc tế về an ninh mạng và phòng, chống tội phạm mạng."

Sáng 25_10_2025 tại Hà Nội, các đại biểu tham dự tại Lễ mở ký Công ước của Liên hợp quốc về chống tội phạm mạng

quan điểm khác nhau. Tổng Giám đốc Văn phòng Liên hợp quốc về Ma túy và Tội phạm (UNODC) ghi nhận vai trò nổi bật của Việt Nam trong suốt tiến trình xây dựng Công ước, từ tham gia đàm phán, đóng góp nội dung đến việc đăng cai Lễ mở ký, qua đó góp phần củng cố niềm tin vào các cơ chế đa phương do Liên hợp quốc dẫn dắt. Theo lãnh đạo UNODC, việc Hà Nội được lựa chọn là địa điểm tổ chức Lễ mở ký phản ánh sự tin cậy cao của cộng đồng quốc tế đối với năng lực điều phối, tinh thần hợp tác và cam kết lâu dài của Việt Nam đối với các nỗ lực chung của Liên hợp quốc.

Trong bối cảnh đó, Hà Nội không chỉ là điểm hội tụ của cam kết toàn cầu, mà còn là biểu tượng cho tiếng nói và đóng góp ngày càng rõ nét của các nước đang phát triển và khu vực ASEAN trong kiến tạo luật chơi quốc tế về an ninh mạng.

Hướng tới tương lai: Từ ký kết đến triển khai hiệu quả

Lễ mở ký Công ước vượt qua ý nghĩa của một sự kiện đối ngoại để truyền tải thông điệp về tinh thần hành động toàn cầu, mở ra tương lai mới của đối thoại, hợp tác và niềm tin. Với Việt Nam, đây không chỉ là cơ hội mà còn là trách nhiệm tiên phong trong việc thúc đẩy hiện thực hóa các cam kết toàn cầu bằng những hành động cụ thể. Trong thời gian tới, Việt Nam sẽ tập trung triển khai ba định hướng lớn:

Một là, tiếp tục hoàn thiện khuôn khổ pháp lý và thể chế pháp luật trong nước về phòng chống tội phạm mạng, phù hợp với các chuẩn mực quốc tế; nâng cao năng lực thực thi, tăng cường nhận thức cộng đồng, hướng tới không gian mạng an toàn, bảo vệ quyền và lợi ích chính đáng của người dân, đặc biệt là các nhóm dễ bị tổn thương, trên môi trường số.

Hai là, thúc đẩy hợp tác quốc tế thực chất về chia sẻ dữ liệu, hỗ trợ kỹ thuật, đào tạo nguồn nhân lực, chuyển giao công nghệ; kết nối chính phủ, trung tâm, viện nghiên cứu, doanh nghiệp và tổ chức quốc tế, phát triển hành lang hợp tác công-tư về an ninh mạng và an toàn dữ liệu.

Ba là, phát huy vai trò tiên phong của Việt Nam trong định hình các quy tắc, chuẩn mực đạo đức và khung pháp lý quốc tế về công nghệ, thúc đẩy các sáng kiến khu vực và toàn cầu gắn thực thi Công ước với hợp tác an ninh mạng, chuyển đổi số, kinh tế số, quản trị dữ liệu.

Công ước Hà Nội không chỉ là kết tinh trí tuệ và nỗ lực của các quốc gia, mà còn là lời cam kết chung của cộng đồng quốc tế về một thế giới an toàn, hợp tác và nhân văn hơn trong kỷ nguyên số. Từ trang mở ký Công ước Hà Nội, một chương mới của đối thoại và hợp tác đang mở ra, nơi các quốc gia cùng chung tay xây dựng tương lai số an toàn cho con người và vì con người, phấn đấu cho hòa bình và thịnh vượng chung của toàn nhân loại.

Trong bối cảnh không gian mạng trở thành không gian chiến lược mới, ngoại giao đa phương không còn chỉ xoay quanh các vấn đề truyền thống, mà ngày càng mở rộng sang những lĩnh vực phi truyền thống như an ninh mạng và quản trị công nghệ. Quá trình hình thành Công ước Hà Nội là minh chứng điển hình cho xu thế đó, khi các quốc gia phải tìm kiếm đồng thuận giữa an ninh, phát triển, chủ quyền quốc gia và bảo vệ quyền con người. Việt Nam, với cách tiếp cận cân bằng, xây dựng và thực chất, đã tham gia tích cực từ sớm, góp phần thúc đẩy đối thoại, thu hẹp khác biệt và hình thành một khuôn khổ hợp tác quốc tế mang tính bao trùm, phản ánh lợi ích chính đáng của cả các nước phát triển và đang phát triển.

Công ước Hà Nội: Từ dấu mốc đa phương đến cơ hội kiến tạo niềm tin số cho Việt Nam

Trung tướng Nguyễn Minh Chính

Phó Chủ tịch Hiệp hội An ninh mạng quốc gia

Nâng tầm vị thế bằng năng lực thực thi và niềm tin quốc tế

Tội phạm mạng có đặc tính ẩn danh, xuyên biên giới, không bị giới hạn bởi thời gian và không gian; hạ tầng kỹ thuật phân tán; chứng cứ điện tử có thể bị xóa chỉ trong một cú nhấn phím. Trong bối cảnh ấy, không một quốc gia đơn lẻ nào có thể đối phó hiệu quả nếu thiếu cơ chế hợp tác quốc tế, thiếu nền tảng chia sẻ thông tin và thiếu "ngôn ngữ pháp lý chung" để cùng hành động. Công ước Hà Nội vì vậy tạo ra một hành lang quan trọng để hợp tác đi vào thực chất, khả năng phối hợp và năng lực thực thi.

Công ước Hà Nội mở ra cơ hội quan trọng để nâng tầm vị thế chính trị - đối ngoại của Việt Nam; khẳng định Việt Nam là một thành viên tích cực, có trách nhiệm trong cộng đồng quốc tế, không chỉ giải quyết các vấn đề trong nước, mà còn chủ động tham gia vận động, ký kết và cùng cộng đồng quốc tế xử lý những thách thức chung về an ninh mạng.

Việc đăng cai Lễ mở ký cũng khẳng định năng lực tổ chức các sự kiện quốc tế đa phương lớn của Việt Nam. Thành công của sự kiện không chỉ mang ý nghĩa nhất thời, mà còn mở ra cơ hội để Việt Nam tiếp tục đăng cai các sự kiện lớn khác của Liên hợp quốc trong tương lai, qua đó gia tăng vai trò và tiếng nói trên các diễn đàn đa phương.

Công ước Hà Nội là cơ hội để thúc đẩy hoàn thiện thể chế và nâng cao năng lực thực thi. Việt Nam sẽ nội luật hóa các quy định của Công ước, bảo đảm phù hợp với thông lệ quốc tế trong đấu tranh chống tội phạm mạng. Quá trình này đòi hỏi cách tiếp cận thận trọng, bài bản, hài hòa giữa yêu cầu điều tra, xử lý tội phạm với bảo vệ dữ liệu cá nhân và bảo đảm chủ quyền quốc gia. Chỉ khi

Chiều 26/10, trong khuôn khổ Lễ mở ký Công ước Liên hợp quốc về chống tội phạm mạng tại Hà Nội, Hiệp hội An ninh mạng quốc gia và Cơ quan Phát triển và Hợp tác kinh tế, Cộng hoà Áo đã có buổi làm việc và ký biên bản hợp tác, thiết chặt mối quan hệ ngoại giao giữa hai quốc gia.

Công ước Hà Nội mở ra một giai đoạn mới không chỉ cho hợp tác quốc tế, mà còn đặt ra yêu cầu cấp thiết về năng lực thực thi trong nước. Từ công tác tổ chức, bảo đảm an ninh tuyệt đối cho Lễ mở ký đến triển khai sau ký kết, Việt Nam đang từng bước khẳng định năng lực điều phối, thực thi và kết nối hệ sinh thái an ninh mạng, biến cam kết quốc tế thành nền tảng bảo vệ không gian số an toàn và tin cậy.

Trung tướng Nguyễn Minh Chính, Phó Chủ tịch Hiệp hội An ninh mạng quốc gia

nội luật hóa đi cùng với nâng cao năng lực thực thi, Công ước mới thực sự trở thành công cụ hữu hiệu chứ không chỉ dừng lại ở một văn kiện ký kết.

Công ước Hà Nội cũng tạo điều kiện nâng cao năng lực kỹ thuật, nguồn nhân lực và năng lực tổ chức của Việt Nam trong giai đoạn hậu ký kết. Năng lực phòng, chống tội phạm mạng không chỉ thuộc về các cơ quan chuyên trách, mà là năng lực tổng thể của cả hệ sinh thái, từ hạ tầng kỹ thuật, quy trình phối hợp, chuẩn nghiệp vụ thu thập - bảo quản chứng cứ điện tử, đến đội ngũ nhân lực có khả năng làm việc trong môi trường hợp tác xuyên biên giới. Đây cũng là thời điểm thuận lợi để quảng bá hình ảnh Việt Nam như một điểm đến hòa bình, ổn định, an ninh và an toàn, thúc đẩy hợp tác công nghệ, dịch vụ số và đầu tư cho kinh tế số.

Công ước còn góp phần nâng cao nhận thức của hệ thống chính trị, người dân và doanh nghiệp về an ninh, an toàn không gian mạng. Nhận thức đúng sẽ dẫn đến hành vi số đúng, qua đó giảm thiểu rủi ro và chi phí xã hội do tội phạm mạng gây ra, tạo nền tảng cho chuyển đổi số bền vững.

Những thách thức và yêu cầu đặt ra để thành công trọn vẹn

Trước hết là quá trình vận động và đàm phán quốc tế để đưa Lễ mở ký về Hà Nội, bởi đây là lần đầu tiên một sự kiện ký kết của Liên hợp quốc được tổ chức bên ngoài trụ sở. Quá trình này đòi hỏi sự kiên trì, lập luận thuyết phục và uy tín quốc gia, thể hiện rõ tính chủ động và chuyên nghiệp của Việt Nam.

Thứ hai là công tác tổ chức một sự kiện quốc tế lớn với nhiều đoàn cấp cao và doanh nghiệp lớn tham dự, bảo đảm tuyệt đối an ninh, trật tự; bảo đảm tài chính, hậu cần bởi nước chủ nhà sẽ phải chủ động mời và hỗ trợ các đoàn đến từ những quốc gia, vùng lãnh thổ gặp khó khăn về kinh phí tham dự; bảo đảm các sự kiện bên lề diễn ra thành công. Đây là khâu chuẩn bị khổng lồ, đòi hỏi phối hợp đồng bộ và nhịp nhàng giữa Ban Chỉ đạo và tất cả các cơ quan liên quan, đặc biệt là Bộ Công an với vai trò chủ trì, sự phối hợp chặt chẽ của Bộ Ngoại giao và sự tham gia tích cực của Hiệp hội An ninh mạng quốc gia.

Thứ ba là nội luật hóa. Mỗi quốc gia có hệ thống pháp luật riêng liên quan đến chủ quyền, thu giữ tài sản, quy trình tố tụng, dẫn độ. Bên cạnh đó là các vấn đề phức tạp trong chính Công ước, liên quan đến tố tụng, phát hiện tội phạm, thu thập chứng cứ điện tử; đồng thời phải bảo đảm các nguyên tắc bảo vệ dữ liệu cá nhân.

Thứ tư về hạ tầng kỹ thuật và nguồn nhân lực. Chúng ta phải chuẩn bị kỹ lưỡng hệ thống thông tin để quảng bá sự kiện, truyền tải thông điệp và hình ảnh Việt Nam ra thế giới một cách thông suốt và an toàn. Trong thế giới số, mỗi "điểm nghẽn" kỹ thuật có thể trở thành một rủi ro truyền thông và một lỗ hổng an ninh. Vượt qua thách thức này chính là một phần quan trọng của năng lực quốc gia.

VAI TRÒ KẾT NỐI CỦA HIỆP HỘI AN NINH MẠNG QUỐC GIA

Trong tiến trình vận động, tổ chức và triển khai Công ước Hà Nội, Hiệp hội An ninh mạng quốc gia giữ vai trò "kết nối mềm" giữa Nhà nước, doanh nghiệp và các đối tác quốc tế. Không chỉ tham gia vận động quốc tế đưa Lễ mở ký về Hà Nội, Hiệp hội còn góp phần quảng bá năng lực công nghệ an ninh mạng của Việt Nam, thúc đẩy hợp tác công - tư và chuẩn bị nền tảng xã hội cho việc triển khai Công ước sau ký kết. Vai trò này cho thấy an ninh mạng không còn là nhiệm vụ riêng của cơ quan chuyên trách, mà là trách nhiệm chung củatoàn bộ hệ sinh thái số.

Vai trò của Hiệp hội An ninh mạng quốc gia trong vận động quốc tế và kiến tạo nền tảng triển khai

Quá trình đàm phán và vận động quốc tế để đưa Lễ mở ký Công ước về Hà Nội là một nỗ lực lớn. Cần nhấn mạnh rằng đây là ý tưởng và sự chỉ đạo của Đại tướng Lương Tam Quang - Ủy viên Bộ Chính trị, Bộ trưởng Bộ Công an, Chủ tịch Hiệp hội An ninh mạng quốc gia. Ý tưởng xuất phát từ mong muốn khẳng định Việt Nam coi trọng hợp tác quốc tế trong phòng, chống tội phạm mạng và xem đây là một vấn đề an ninh quốc gia; đồng thời thể hiện Việt Nam có đủ vị thế, vai trò, uy tín và khả năng để phối hợp với các quốc gia khác.

Trên cơ sở phân công của Ban Chỉ đạo, Hiệp hội An ninh mạng quốc gia được giao phối hợp cùng Bộ Ngoại giao và Bộ Công an tham gia các hội nghị của Liên hợp quốc, vận động các quốc gia ủng hộ đưa lễ mở ký về Việt Nam. Mỗi lần tiếp xúc với các đối tác, phải xây dựng thông điệp, chuẩn bị trình chiếu, xây dựng trang web và cung cấp thông tin để giải thích vì sao Việt Nam có thể đăng cai một lễ ký kết lớn như vậy; đồng thời khẳng định Việt Nam ổn định về chính trị, yêu chuộng hòa bình, có trách nhiệm, có năng lực bảo đảm an ninh, an toàn và có khả năng xử lý các vấn đề quốc tế. Những nỗ lực ấy góp phần tạo sự đồng thuận, gia tăng niềm tin và thúc đẩy quyết định lựa chọn Hà Nội cho sự kiện lịch sử này.

Bên cạnh vai trò vận động quốc tế, Hiệp hội An ninh mạng quốc gia còn trực tiếp tham gia kiến tạo nền tảng triển khai Công ước tại Việt Nam thông qua hàng loạt hoạt động cụ thể, mang tính tổ chức và điều phối. Hiệp hội phối hợp tiếp đón các đoàn quốc tế đến khảo sát, làm việc trước thời điểm Công ước diễn ra, bảo đảm cung cấp đầy đủ thông tin về điều kiện tổ chức, năng lực bảo đảm an ninh, an toàn và hạ tầng kỹ thuật.

Đối với các đoàn chính thức tham dự lễ mở ký, Hiệp hội tham gia chuẩn bị chu đáo các khâu triển khai, từ nội dung làm việc, hậu cần, lễ tân đến phối hợp tổ chức các phiên làm việc, ký kết bên lề Công ước.

Một điểm nhấn quan trọng là vai trò chủ trì của Hiệp hội trong việc tổ chức các triển lãm công nghệ an ninh mạng trong khuôn khổ Công ước. Thông qua các không gian trưng bày, Hiệp hội đã giới thiệu một cách có hệ thống năng lực, giải pháp và hệ sinh thái an ninh mạng của doanh nghiệp Việt Nam, từ phòng, chống tội phạm mạng, bảo vệ dữ liệu, an toàn hạ tầng số đến các ứng dụng trí tuệ nhân tạo trong giám sát, phân tích và ứng phó sự cố. Hoạt động này không chỉ quảng bá năng lực công nghệ trong nước, mà còn thể hiện cam kết thực chất của Việt Nam trong việc gắn nghĩa vụ quốc tế với năng lực kỹ thuật và nguồn lực xã hội, tạo nền tảng cho việc thực thi Công ước một cách hiệu quả và bền vững.

Trong khuôn khổ Lễ mở ký và Hội nghị Cấp cao, Hiệp hội đã chủ động tổ chức và thúc đẩy các phiên

Hiệp hội An ninh mạng Quốc gia làm việc với các đối tác Hà Lan về an ninh chuỗi khối và tài sản số

làm việc, ký kết hợp tác song phương và đa phương với các quốc gia, tổ chức quốc tế và đối tác chuyên ngành. Các nội dung hợp tác tập trung vào chia sẻ kinh nghiệm, nâng cao năng lực điều tra số, đào tạo nguồn nhân lực, phối hợp kỹ thuật và xây dựng không gian số an toàn, đáng tin cậy. Với vai trò "kết nối mềm", Hiệp hội đã góp phần chuyển hóa các cam kết chính trị - pháp lý của Công ước thành các chương trình hợp tác cụ thể, có khả năng triển khai lâu dài sau ký kết..

Trên cả hai trục - kiến tạo chuẩn mực ở tầm quốc tế và hỗ trợ triển khai ở tầm thực tiễn, Hiệp hội An ninh mạng quốc gia đã khẳng định vai trò là lực lượng nòng cốt trong hệ sinh thái an ninh mạng Việt Nam, góp phần quan trọng vào việc biến dấu mốc ngoại giao của Công ước Hà Nội thành nền tảng hợp tác thực chất, lâu dài, phục vụ mục tiêu xây dựng không gian mạng an toàn, tin cậy và bảo vệ vững chắc chủ quyền quốc gia trong kỷ nguyên số.

Nhiệm vụ trọng tâm của Hiệp hội An ninh mạng quốc gia sau ký kết

Hiệp hội An ninh mạng quốc gia ra đời trong bối cảnh cuộc cách mạng khoa học công nghệ diễn ra mạnh mẽ và Việt Nam bước vào kỷ nguyên chuyển đổi số. Hiệp hội có vai trò quan trọng trong việc "phát huy sức mạnh tổng hợp, kết nối cơ quan nhà nước với cộng đồng doanh nghiệp công nghệ và người dân".

Thứ nhất, nâng cao nhận thức xã hội và thúc đẩy phối hợp Nhà nước - doanh nghiệp - người dân trong phòng, chống tội phạm mạng, thông qua truyền thông, đào tạo và phổ biến kỹ năng an toàn số một cách bền bỉ, thực chất.

Thứ hai, huy động nguồn lực doanh nghiệp hội viên, đội ngũ chuyên gia và hạ tầng kỹ thuật để tăng cường năng lực phòng thủ, dự báo, ứng cứu và phục hồi trước các mối đe dọa mạng ngày càng tinh vi.

Thứ ba, tham gia tổ chức các hoạt động, diễn đàn bên lề, tạo không gian đối thoại công - tư, kết nối nguồn lực xã hội và đưa Công ước vào đời sống.

Lễ mở ký Công ước Hà Nội là điểm khởi đầu, còn thành công phụ thuộc vào triển khai sau ký kết, với trọng tâm là hoàn thiện thể chế, nâng cao năng lực kỹ thuật, phát triển nhân lực và xây dựng văn hóa an toàn số.

Với vai trò chủ trì của Bộ Công an, sự phối hợp của Bộ Ngoại giao và sự vào cuộc của Hiệp hội An ninh mạng quốc gia cùng doanh nghiệp, Việt Nam có thể biến dấu mốc này thành lợi thế chiến lược, củng cố niềm tin số và thúc đẩy kinh tế số bền vững.

Công ước Hà Nội Nền tảng mới cho một không gian số an toàn

Joshua James

Chuyên gia Văn phòng Liên hợp quốc về Ma túy và Tội phạm,
Khu vực Đông Nam Á và Thái Bình Dương

Tội phạm mạng đang gây ra những thiệt hại chưa từng có cho kinh tế, xã hội và an ninh toàn cầu, với quy mô lên tới hàng nghìn tỷ USD mỗi năm. Trong bối cảnh đó, sự ra đời của Công ước Hà Nội đánh dấu lần đầu tiên cộng đồng quốc tế có một công cụ pháp lý toàn cầu, toàn diện và mang tính ràng buộc, tạo nền tảng chung cho hợp tác phòng, chống tội phạm mạng và chia sẻ chứng cứ điện tử xuyên biên giới.

Tội phạm mạng - mối đe dọa toàn cầu với thiệt hại hàng nghìn tỷ USD

Trong khi các hình thức lừa đảo gia tăng, các quốc gia đang phải đối mặt với một loạt các hoạt động tội phạm mạng như: truy cập trái phép vào các hệ thống công nghệ thông tin (CNTT); nghe lén trái phép các liên lạc; can thiệp vào dữ liệu và hạ tầng số; tạo ra và phân phối các công cụ độc hại nhằm phục vụ việc thực hiện tội phạm mạng... đe dọa cá nhân, doanh nghiệp và chính phủ.

Đặc biệt, vấn nạn xâm hại và bóc lột tình dục trẻ em trên không gian mạng tiếp tục là một mối đe dọa ngày càng nghiêm trọng. Theo nghiên cứu của Childlight, mỗi năm có hơn 300 triệu trẻ em là nạn nhân của các hành vi bóc lột và xâm hại tình dục được hỗ trợ bởi công nghệ, ảnh hưởng đến khoảng 12,6% trẻ em trên toàn cầu. Ngoài ra, khoảng 300 triệu trẻ em, đã từng bị dụ dỗ tình dục trực tuyến.

Các dạng tội phạm mạng truyền thống như tấn công ransomware đã tăng hơn 40% trong năm 2024 so với năm 2023, đặc biệt nhắm vào các lĩnh vực y tế, giáo dục và hạ tầng trọng yếu. Thiệt hại toàn cầu liên quan đến ransomware trong năm 2024 đã vượt 60 tỷ USD, với chi phí trung bình cho mỗi sự cố (bao gồm khắc phục và thời gian ngừng hoạt động) lên tới 5 triệu USD. Tội phạm mạng ngày càng tận dụng triệt để AI làm công cụ tấn công. AI khiến các cuộc tấn công mạng diễn ra nhanh hơn và khó bị vô hiệu hóa hơn.

Công ước Hà Nội - một công cụ pháp lý toàn cầu chống tội phạm mạng

Công ước Liên hợp quốc về chống tội phạm mạng; tăng cường hợp tác quốc tế trong đấu tranh chống một số tội phạm được thực hiện thông qua hệ thống công nghệ thông tin và truyền thông, cũng như trong việc chia sẻ chứng cứ điện tử của các tội phạm nghiêm trọng, đã được Đại hội đồng Liên hợp quốc thông qua tại Nghị quyết 79/243 ngày 24/12/2024. Đây là hiệp ước về tư pháp hình sự đầu tiên của Liên hợp quốc được thông qua trong hơn 20 năm qua, đồng thời là hiệp ước toàn cầu đầu tiên về tội phạm mạng và trao đổi chứng cứ điện tử đối với các tội phạm nghiêm trọng. 9 chương của Công ước đã giải quyết một cách toàn diện vấn đề toàn cầu về tội phạm mạng.

Lễ mở ký Công ước Liên hợp quốc về chống tội phạm mạng tại Hà Nội (ngày 25 - 26/10/2025) mang ý nghĩa lịch sử đặc biệt. Lần đầu tiên, một hiệp ước của Liên hợp quốc được ký tại một thành phố của Việt Nam, một minh chứng mạnh mẽ cho vị thế ngày càng gia tăng của Việt Nam trên trường quốc tế. Tính đến nay, Công ước đã có 74 quốc gia ký kết, cho thấy sự đồng thuận đa phương trong quản trị không gian mạng toàn cầu, qua đó thu hẹp các khoảng trống pháp lý quốc tế trong kỷ nguyên số.

Phạm vi của Công ước xác định rõ những nghĩa vụ mà các quốc gia thành viên phải thực hiện. Phạm vi này bao gồm hai trụ cột:

Thứ nhất, liên quan đến các hành vi phạm tội được quy định trong các điều từ 7 đến 17 của Công ước. Theo đó, các quốc gia thành viên phải nội luật hóa các hành vi phạm tội này trong pháp luật hình sự quốc gia, thực thi các quy định đó thông qua điều tra và truy tố, đồng thời áp dụng các biện pháp phòng ngừa nhằm giải quyết các nguyên nhân gốc rễ. Các quốc gia thành viên cũng phải phong tỏa, tịch thu và sung công các khoản thu từ tội phạm, đồng thời hoàn trả cho các chủ sở hữu hợp pháp.

Thứ hai, liên quan đến chứng cứ điện tử. Các quốc gia thành viên được yêu cầu thiết lập các biện pháp tố tụng ở cấp quốc gia nhằm trao quyền cho cơ quan có thẩm quyền trong việc thu thập, tiếp cận và bảo quản chứng cứ điện tử đối với bất kỳ hành vi phạm tội nào theo pháp luật quốc gia. Điều này bảo đảm khả năng chấp nhận chứng cứ điện tử trước tòa án và thiết lập các năng lực kỹ thuật để tạo thuận lợi cho hợp tác quốc tế trong việc chia sẻ chứng cứ điện tử.

Ở cấp độ quốc tế, các quốc gia thành viên cam kết hợp tác với các quốc gia khác trong việc bảo quản, thu thập và tiếp cận chứng cứ điện tử nằm trong lãnh thổ của mình, qua đó chia sẻ các chứng cứ này đối với cả các hành vi phạm tội theo Công ước lẫn các tội phạm nghiêm trọng khác.

Công ước cũng kế thừa các biện pháp tố tụng đã tồn tại trong các điều ước trước đây, như phong tỏa và tịch thu tài sản, thiết lập hồ sơ tiền án, cũng như các biện pháp bảo vệ nạn nhân và nhân chứng.

Đầu mối cho hợp tác quốc tế về chứng cứ điện tử là mạng lưới 24/7, một mạng lưới các điểm liên lạc quốc gia cung cấp hỗ trợ tức thời 24 giờ mỗi ngày, 7 ngày mỗi tuần.

Mạng lưới 24/7 tạo điều kiện, hoặc nếu pháp luật trong nước cho phép thì trực tiếp cung cấp tư vấn kỹ thuật cho các quốc gia thành viên khác, có thể nhanh chóng bảo quản dữ liệu; bảo quản thông tin về vị trí của các nhà cung cấp dịch vụ liên quan, nhằm hỗ trợ quốc gia yêu cầu trong việc gửi yêu cầu đến cơ quan có thẩm quyền. Ngoài ra, trong một số trường hợp, mạng lưới 24/7 có thể hỗ trợ xác định vị trí của nghi phạm và cung cấp dữ liệu nhằm ngăn chặn các tình huống khẩn cấp.

Bên cạnh đó, Công ước còn bao gồm các biện pháp hợp tác quốc tế truyền thống nhằm tạo thuận lợi cho các thủ tục tố tụng hình sự nước ngoài, bao gồm dẫn độ, chuyển giao người bị kết án hoặc hồ sơ vụ án hình sự, hợp tác thực thi pháp luật, điều tra chung và hợp tác trong thu hồi tài sản.

Đáng chú ý, Công ước là hiệp ước tư pháp hình sự đầu tiên tích hợp các biện pháp bảo đảm quyền con người mang tính xuyên suốt. Công ước hình sự hóa một dạng bạo lực đối với phụ nữ và trẻ em gái, cập nhật khuôn khổ về xâm hại và bóc lột trẻ em

TỘI PHẠM MẠNG - MỐI ĐE DỌA TOÀN CẦU KHÔNG BIÊN GIỚI

Tội phạm mạng đang gây ra những thiệt hại kinh tế - xã hội ở quy mô chưa từng có, với hàng nghìn tỷ USD bị thất thoát mỗi năm. Từ lừa đảo tài chính, tấn công ransomware đến xâm hại trẻ em trên không gian mạng, các hành vi phạm tội ngày càng tinh vi, tận dụng công nghệ mới như trí tuệ nhân tạo và tiền mã hóa. Đặc điểm xuyên biên giới, ẩn danh và tốc độ cao khiến tội phạm mạng vượt quá khả năng ứng phó của bất kỳ quốc gia đơn lẻ nào, đặt ra nhu cầu cấp thiết về một công cụ pháp lý toàn cầu để phối hợp hành động.

Ngày 25-26_10_2025 tại Hà Nội diễn ra Lễ mở ký và Hội nghị cấp cao, Công ước của Liên Hợp Quốc về chống tội phạm mạng

trên không gian mạng, bảo đảm cơ chế bảo vệ và bồi thường cho nạn nhân của tội phạm mạng, đồng thời đưa ra khuôn khổ phòng ngừa với sự tham gia của nhiều bên liên quan. Biện pháp này có ý nghĩa then chốt trong việc bảo đảm an toàn và nhân phẩm cho các nạn nhân của những hành vi được mô tả trong các điều khoản đó.

Công ước có một chương riêng về các biện pháp phòng ngừa, theo đó các quốc gia thành viên cam kết ngăn chặn tội phạm mạng. Các quốc gia thành viên thừa nhận rằng phòng ngừa là nỗ lực của nhiều bên liên quan và khu vực tư nhân, xã hội dân sự và giới học thuật cần phối hợp với chính phủ để ngăn chặn tội phạm mạng. Các biện pháp phòng ngừa được đề xuất bao gồm tăng cường an ninh cho các dịch vụ, công nghệ và người sử dụng; cập nhật các tiến bộ công nghệ và theo dõi xu hướng hoạt động tội phạm; nâng cao nhận thức của công chúng về việc sử dụng an toàn các công nghệ số; thúc đẩy các biện pháp bảo vệ trẻ em, cũng như phòng, chống bạo lực trên cơ sở giới được thực hiện thông qua các hệ thống công nghệ thông tin và truyền thông.

Tương tự như các điều ước trước đây, hỗ trợ kỹ thuật là một yếu tố quan trọng trong việc triển khai Công ước thông qua các biện pháp như đào tạo, nâng cao năng lực về kỹ thuật điều tra; trao đổi thông tin về các tiến bộ công nghệ; khuôn khổ pháp lý; chuyển giao công nghệ; thu thập dữ liệu và xu hướng. Tuy nhiên, cần lưu ý rằng các quốc gia thành viên đã thừa nhận tầm quan trọng của việc cung cấp hỗ trợ không chỉ thông qua đào tạo mà còn, tùy theo tình hình, bằng việc cung cấp trang thiết bị và công nghệ có thể được sử dụng trong công tác phòng, chống tội phạm mạng.

Các quốc gia thành viên của Công ước cũng cần hỗ trợ lẫn nhau trong việc thu thập dữ liệu liên quan đến tội phạm mạng như một phương thức tăng cường trao đổi thông tin về hiện tượng này.

Nỗ lực của UNODC trong phòng, chống tội phạm mạng

Văn phòng Liên hợp quốc về Ma túy và Tội phạm (UNODC) giữ vai trò trung tâm trong việc hình thành Công ước Liên hợp quốc về chống tội phạm mạng. Với vai trò là Ban Thư ký chuyên môn, UNODC đã dẫn dắt quá trình đàm phán, soạn thảo kỹ thuật và tham vấn các bên liên quan, bao gồm sự tham gia của các chính phủ, xã hội dân sự, giới học thuật và khu vực tư nhân. UNODC sẽ hỗ trợ các quốc gia trong quá trình phê chuẩn, chuyển hóa các cam kết thành pháp luật quốc gia, xây dựng hạ tầng kỹ thuật và giám sát việc thực thi, với trọng tâm là tác động bền vững, các tiêu chuẩn pháp quyền và sự phù hợp với quyền con người.

Chương trình Toàn cầu về Tội phạm mạng của UNODC, phối hợp với Văn phòng Khu vực Đông Nam Á và Thái Bình Dương (ROSEAP) và Văn phòng UNODC tại Việt Nam, cam kết hỗ trợ Việt Nam trong việc nâng cao năng lực phòng, chống tội phạm mạng. Chúng tôi tiến hành tham vấn và đánh giá hằng năm với Việt Nam để xác định các khoảng trống và nhu cầu sắp tới. Từ kết quả đánh giá này, chúng tôi xây dựng các kế hoạch công tác chung nhằm bảo đảm Chính phủ nhận được nguồn lực tại những lĩnh vực có tác động lớn nhất trong việc phòng ngừa và ứng phó với tội phạm mạng. Chúng tôi cũng đầu tư vào việc phát triển đội ngũ chuyên gia trong nước thông qua các chương trình như đào tạo giảng viên về điều tra tội phạm mạng. Chúng tôi luôn tìm kiếm cơ hội hợp tác với các học viện và trường đại học để đưa nội dung về chứng cứ số và tội phạm mạng vào chương trình giảng dạy.

UNODC đã xây dựng một danh mục đầy đủ các khóa đào tạo nâng cao năng lực dành cho các quốc gia thành viên nhằm phòng ngừa và đấu tranh chống tội phạm mạng, và đã triển khai các khóa học này trên toàn cầu trong hơn 12 năm qua. Quan trọng hơn, chúng tôi cũng phối hợp với các đối tác để nâng cao nhận thức về an ninh mạng cho người dân, đặc biệt là các nhóm dễ bị tổn thương.

CÔNG ƯỚC HÀ NỘI - KHUÔN KHỔ PHÁP LÝ TOÀN DIỆN ĐẦU TIÊN

Công ước Hà Nội là hiệp ước tư pháp hình sự toàn cầu đầu tiên điều chỉnh toàn diện các vấn đề liên quan đến tội phạm mạng và chứng cứ điện tử. Không chỉ hình sự hóa các hành vi phạm tội, Công ước còn thiết lập cơ chế hợp tác quốc tế, chia sẻ dữ liệu và bảo đảm tính chấp nhận của chứng cứ điện tử trước tòa án. Đáng chú ý, Công ước tích hợp các nguyên tắc bảo vệ quyền con người, đặc biệt đối với phụ nữ và trẻ em, cho thấy nỗ lực cân bằng giữa yêu cầu bảo đảm an ninh và bảo vệ các giá trị nhân văn trong kỷ nguyên số.

Từ phân mảnh pháp lý đến đồng thuận toàn cầu về an ninh mạng

Ban biên tập

Từ một không gian pháp lý phân mảnh, thế giới đang tiến gần hơn tới đồng thuận toàn cầu về an ninh mạng với sự ra đời của Công ước Hà Nội. Việc một địa danh của Việt Nam được gắn với một Công ước quốc tế quan trọng không chỉ mang ý nghĩa biểu tượng, mà còn phản ánh sự ghi nhận của cộng đồng quốc tế đối với vai trò, uy tín và cách tiếp cận cân bằng, có trách nhiệm của Việt Nam trong quản trị không gian mạng toàn cầu.

Chủ tịch nước Lương Cường và các đại biểu dự lễ mở ký Công ước Hà Nội ngày 25-26_10_2025

"Ngôn ngữ pháp lý chung" cho an ninh mạng

Internet là môi trường không biên giới, nơi dữ liệu có thể ra đời ở một quốc gia, lưu trữ tại quốc gia thứ hai và bị khai thác, tấn công từ một quốc gia thứ ba. Chính đặc điểm này khiến việc truy vết, bắt giữ tội phạm mạng trở nên phức tạp hơn rất nhiều so với các loại tội phạm truyền thống, vốn gắn với không gian lãnh thổ cụ thể. Cùng với sự phát triển mạnh mẽ của trí tuệ nhân tạo (AI), Internet vạn vật (IoT) và dữ liệu lớn, rào cản giữa thế giới thực và thế giới ảo ngày càng mờ nhạt, kéo theo sự bùng nổ của các loại hình tội phạm mới như giả mạo nhân dạng, lừa đảo, tống tiền bằng deepfake, hoặc thao túng thông tin qua mạng xã hội. Năm 2025, thiệt hại do tội phạm mạng gây ra có thể chạm mốc 10.500 tỷ USD, tương đương GDP các cường quốc kinh tế hàng đầu.

Để thiết lập cơ chế hợp tác quốc tế khi xử lý vụ việc xuyên biên giới, một số thỏa thuận đa phương đã được khởi xướng. Trong đó Công ước Budapest về Tội phạm mạng (2001) do Hội đồng châu Âu thúc đẩy, hiện có hơn 70 thành viên, là điều ước quốc tế đầu tiên về phòng, chống tội phạm mạng, quy định về tội danh, thủ tục tố tụng và hợp tác quốc tế. Nghị định thư thứ hai bổ sung Công ước Budapest cung cấp thêm cơ chế tiếp cận dữ liệu điện tử xuyên biên giới và hỗ trợ pháp lý giữa thành viên.

Đại hội đồng Liên Hợp Quốc thông qua Công ước Hà Nội với tỷ lệ đồng thuận cao

Ở cấp khu vực, Liên minh châu Âu (EU) ban hành Chỉ thị NIS2 (áp dụng từ năm 2024) nhằm nâng cao khả năng chống chịu của các tổ chức hạ tầng thiết yếu, yêu cầu báo cáo sự cố trong vòng 24h và tăng cường chế tài xử phạt. ASEAN, dù chưa có điều ước ràng buộc, đã xây dựng Chiến lược Hợp tác an ninh mạng khu vực ASEAN (2021-2025), nhấn mạnh tầm quan trọng của chia sẻ thông tin, nâng cao năng lực và diễn tập chung. Tại châu Phi, Liên minh châu Phi thông qua Công ước Malabo (2014) nhằm bảo vệ các giao dịch điện tử, bảo vệ dữ liệu và an ninh mạng, nhưng tiến độ phê chuẩn còn chậm...

Các tổ chức quốc tế, bao gồm Liên hợp quốc và NATO, đã thông qua những văn kiện khuyến nghị về những nguyên tắc của luật pháp quốc tế áp dụng trong không gian mạng. Tuy nhiên, theo các chuyên gia, những văn bản đó mới chỉ đưa ra được những nguyên tắc chung, việc áp dụng cụ thể các nguyên tắc đó còn nhiều điểm chưa rõ ràng, phân mảnh. Dù đã ra đời hơn 20 năm, Công ước Budapest không có sự tham gia của Nga, Trung Quốc, Ấn Độ và nhiều quốc gia Nam bán cầu, trong khi đây lại là những điểm nóng về tấn công mạng và hạ tầng dịch vụ số. Mặt khác, một số cơ chế đa biên hoặc song phương nhiều lúc không thể phát huy tác dụng do căng thẳng chính trị giữa các nước.

Nhận thức rõ những bất cập và yêu cầu cấp bách đó, Việt Nam cùng một số thành viên Liên hợp quốc chủ chốt ủng hộ sáng kiến xây dựng một công ước của Liên hợp quốc về chống tội phạm mạng. Với vị thế là quốc gia đang phát triển có uy tín cao trên trường quốc tế, Việt Nam đã tiên phong hiện thực hóa ý tưởng này tại các diễn đàn Liên hợp quốc, APEC và ASEAN.

Từ năm 2020, quá trình xây dựng công ước bước vào giai đoạn tích cực. Kể từ đó, Việt Nam đã phát huy vai trò chủ động, thể hiện qua việc tổ chức nhiều hội thảo quốc tế, quy tụ các chuyên gia từ UNDP và UNODC để định hình nội dung công ước.

Quá trình đàm phán, Việt Nam đảm nhiệm vai trò điều phối thương lượng một số điều khoản quan trọng. Sau gần 5 năm thảo luận với sự tham gia của hơn 180 quốc gia và tổ chức quốc tế, công ước được Đại hội đồng Liên hợp quốc thông qua ngày 24/12/2024 với tỷ lệ đồng thuận cao.

Để hiện thực hóa các mục tiêu đề ra, Công ước có một khung nội dung đồ sộ nhưng chặt chẽ và khả thi. Nội dung Công ước gồm 9 chương, 71 điều. Công ước hướng tới 3 trụ cột chính: phòng ngừa và chống các hành vi phạm tội được quy định trong văn kiện; thu hồi tài sản do phạm tội mà có; và tăng cường hợp tác quốc tế, đặc biệt trong chia sẻ và tiếp cận bằng chứng điện tử xuyên biên giới. Một điểm đáng chú ý là công

ước yêu cầu các quốc gia thành viên bảo đảm rằng những tội phạm "ngoại tuyến" truyền thống đã được quy định trong các công ước và nghị định thư khác của Liên hợp quốc cũng phải được hình sự hóa khi được thực hiện "trực tuyến".

Công ước nhấn mạnh nghĩa vụ của các quốc gia thành viên phải tuân thủ luật pháp quốc tế, bao gồm tôn trọng nhân quyền và các quyền tự do cơ bản như tự do ngôn luận, tự do tư tưởng, tín ngưỡng, hội họp, đồng thời bảo đảm nguyên tắc bình đẳng về chủ quyền và toàn vẹn lãnh thổ của các quốc gia.

Công ước yêu cầu các quốc gia thành viên xây dựng khuôn khổ hình sự đối với các hành vi phạm tội được thực hiện thông qua hệ thống thông tin và truyền thông (ICT). Công ước thiết lập các nguyên tắc linh hoạt nhưng rõ ràng để ngăn chặn việc lợi dụng các khoảng trống về quyền tài phán...

Hà Nội – biểu tượng của tinh thần đoàn kết quốc tế

Khi quá trình thương lượng về Công ước đi đến giai đoạn quyết định, một vấn đề quan trọng lập tức được đặt ra là việc lựa chọn quốc gia đăng cai lễ mở ký. Đây không chỉ là quyết định mang tính tổ chức, mà còn là lựa chọn có ý nghĩa chính trị - biểu tượng sâu sắc. Điểm đến được lựa chọn phải đáp ứng những tiêu chí then chốt: phải là quốc gia có đóng góp thực chất trong tiến trình đàm phán, có uy tín quốc tế và năng lực điều phối, đồng thời có khả năng kết nối để thu hút sự tham gia rộng rãi nhất của các quốc gia thành viên Liên hợp quốc. Trong bối cảnh đó, Việt Nam đã chủ động triển khai một chiến dịch vận động ngoại giao bài bản, đồng bộ và quyết liệt trên phạm vi rộng rãi; làm rõ vai trò xây dựng, lập trường cân bằng và cam kết lâu dài của Việt Nam đối với hợp tác quốc tế trong lĩnh vực an ninh mạng. Kết quả là Đại hội đồng Liên hợp quốc đã nhất trí lựa chọn Hà Nội làm nơi tổ chức lễ mở ký, đồng thời chính thức gọi văn kiện này là "Công ước Hà Nội".

Lần đầu tiên một địa danh của Việt Nam được gắn với một điều ước quốc tế toàn cầu, đánh dấu bước tiến có ý nghĩa lịch sử trong ngoại giao đa phương của đất nước. Tên gọi "Công ước Hà Nội" không chỉ là niềm tự hào, mà còn là minh chứng rõ nét cho sự ghi nhận quốc tế đối với những đóng góp chủ động, có trách nhiệm và mang tính xây dựng của Việt Nam trong tiến trình hình thành một khuôn khổ pháp lý rộng khắp quan trọng.

Với Công ước Hà Nội, Việt Nam một lần nữa chứng minh mình là một đối tác tin cậy, tiếp tục khẳng định nỗ lực và cam kết mạnh mẽ trong thúc đẩy chủ nghĩa đa phương. Điều đó phù hợp với chủ trương của Đảng và Nhà nước về chủ động hội nhập quốc tế sâu rộng trong kỷ nguyên mới. Bên cạnh ý nghĩa chính trị - ngoại giao, việc tổ chức thành công lễ ký Công ước cũng mang lại cơ hội "vàng" về khoa học, công nghệ và kinh tế. Sự kiện diễn ra đúng vào dịp kỷ niệm thiết lập quan hệ Việt Nam - Liên hợp quốc, được thiết kế như một diễn đàn đa phương quy mô lớn về an ninh mạng.

Vì vậy, không chỉ dừng lại ở giá trị pháp lý, Công ước Hà Nội còn mang ý nghĩa biểu tượng sâu sắc.

TỪ PHÂN MẢNH PHÁP LÝ ĐẾN ĐỒNG THUẬN TOÀN CẦU

Trong nhiều năm, quản trị không gian mạng toàn cầu tồn tại tình trạng phân mảnh, với các điều ước khu vực, sáng kiến song phương và khuyến nghị không mang tính ràng buộc. Công ước Hà Nội ra đời trong bối cảnh đó, như một nỗ lực tập thể nhằm xây dựng "ngôn ngữ pháp lý chung" cho hợp tác quốc tế về an ninh mạng. Việc đạt được đồng thuận trong một lĩnh vực nhạy cảm, phức tạp và liên quan trực tiếp đến chủ quyền quốc gia cho thấy giá trị của chủ nghĩa đa phương và đối thoại trong giải quyết các thách thức toàn cầu.

Công ước Hà Nội có những điều khoản chặt chẽ để bảo vệ trẻ em trên không gian mạng

Hà Nội, cùng với Geneva, Paris hay Vienna, giờ đây trở thành một "địa danh pháp lý" của luật pháp quốc tế. Việc gắn tên Hà Nội với một công ước toàn cầu về chống tội phạm mạng cũng cho thấy cộng đồng quốc tế đánh giá cao cách tiếp cận cân bằng, có trách nhiệm và mang tính xây dựng của Việt Nam trong các vấn đề quốc tế.

Nhận xét về Công ước Hà Nội, Tổng thư ký Liên hợp quốc Antonio Guterres nêu rõ đây là văn kiện quan trọng nhất của Liên hợp quốc góp phần phòng, chống tội phạm mạng và tăng cường hợp tác quốc tế.

Ở cấp độ rộng hơn, Công ước Hà Nội là minh chứng cho khả năng của các quốc gia đang phát triển trong việc đóng góp chủ động vào quản trị toàn cầu thay vì thụ động quan sát như trước. Đây là thông điệp có ý nghĩa lớn trong bối cảnh thế giới đang đối mặt với nguy cơ phân mảnh, chủ nghĩa đơn phương và cạnh tranh chiến lược gay gắt.

HÀ NỘI - BIỂU TƯỢNG CỦA NIỀM TIN VÀ TRÁCH NHIỆM QUỐC TẾ

Việc gắn tên Hà Nội với một công ước toàn cầu về chống tội phạm mạng không chỉ mang ý nghĩa danh xưng, mà còn là biểu tượng của niềm tin quốc tế đối với Việt Nam. Từ một nước đang phát triển, Việt Nam đã vươn lên trở thành chủ thể đóng góp tích cực vào quản trị toàn cầu, với cách tiếp cận cân bằng, có trách nhiệm và hướng tới con người. Công ước Hà Nội vì vậy không chỉ là dấu mốc pháp lý, mà còn là thông điệp chính trị, đối ngoại sâu sắc về vai trò và vị thế của Việt Nam trong kỷ nguyên số.

Lễ mở ký Công ước của Liên hợp quốc về chống tội phạm mạng

Đăng Khoa - Thu Uyên

Chủ tịch nước Lương Cường đón tiếp Tổng thư ký Liên hợp quốc António Guterres tới tham dự Lễ mở ký Công ước Liên hợp quốc về chống tội phạm mạng

Chủ tịch nước Lương Cường tiếp đón Tổng Bí thư, Chủ tịch nước Lào Thongloun Sisoulith tới tham dự Lễ mở ký Công ước Hà Nội

Chủ tịch nước Lương Cường và Tổng thư ký Liên hợp quốc vào khán phòng chính chuẩn bị cho phiên khai mạc Lễ mở ký Công ước Hà Nội

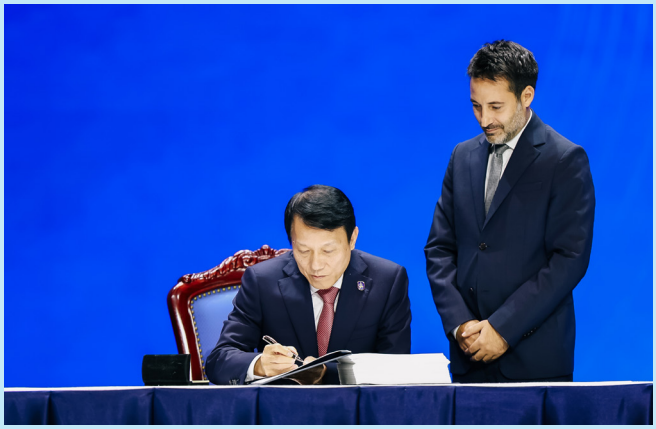
Chủ tịch nước Lương Cường, Tổng thư ký Liên hợp quốc António Guterres cùng đại diện các quốc gia tới tham dự Lễ mở ký Công ước Hà Nội chụp ảnh lưu niệm

Khai mạc Lễ mở ký Công ước Liên hợp quốc về chống tội phạm mạng

Chủ tịch nước Lương Cường phát biểu khai mạc

Tổng thư ký Liên hợp quốc António Guterres có bài phát biểu tại Lễ khai mạc, trong đó ông cảm ơn Việt Nam đã đăng cai Lễ mở ký kết này và vì vai trò lãnh đạo và kết nối của Việt Nam trong việc đưa các quốc gia đến với Lễ mở ký kết.

Bà Ghada Waly, Tổng Giám đốc Văn phòng Liên hợp quốc về Ma tuý và Tội phạm (UNODC) phát biểu tại Lễ mở ký Công ước Hà Nội



Đại tướng Lương Tam Quang, Uỷ viên Bộ Chính trị, Bộ trưởng Bộ Công an thay mặt nước chủ nhà Việt Nam ký vào bản Công ước của Liên hợp quốc về chống tội phạm mạng

Đại diện nước Cộng hoà Dân chủ Nhân dân Lào ký Công ước

Bộ trưởng Bộ Kinh tế và Xã hội kỹ thuật số Thái Lan Chaichanok Chidchob ký Công ước

Đại diện Thường trực của Burkina Faso tại Liên hợp quốc , bà Maïmounata Ouattara ký Công ước Hà Nội

Đại diện Thường trực của Burkina Faso tại Liên hợp quốc, bà Maïmounata Ouattara ký Công ước Hà Nội

Bà Vuysiwa Tulelo - Đại sứ Nam Phi tại Việt Nam ký vào Công ước

Toàn cảnh Lễ mở ký Công ước Liên hợp quốc về chống tội phạm mạng

Tổng thư ký Liên hợp quốc António Guterres và Thủ tướng Phạm Minh Chính tổ chức họp báo sau Lễ mở ký Công ước Hà Nội. Tại đây, Tổng thư ký Liên hợp quốc đã nhấn mạnh: " Trong không gian mạng, không ai an toàn cho đến khi tất cả mọi người đều an toàn. Đó là lý do tại sao chúng ta cần một phản ứng mạnh mẽ, tập thể và toàn cầu".

Thủ tướng Chính phủ Phạm Minh Chính nhấn mạnh: "Không có an ninh mạng vững chắc sẽ không có xã hội số an toàn".

Đại diện Bộ Công an và Bộ Ngoại giao tại Họp báo bên lề Lễ ký Công ước Liên hợp quốc về chống tội phạm mạng

Trung tướng Lê Xuân Minh, Cục trưởng Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao phát biểu tại toạ đàm trong khuôn khổ Lễ mở ký Công ước Hà Nội

Phó Thủ tướng Bùi Thanh Sơn và lãnh đạo một số quốc gia tham gian hàng triển lãm của Hiệp hội An ninh mạng quốc gia

A05 - THANH GƯƠM SẮC BÉN TRÊN KHÔNG GIAN MẠNG

★ 1. Những dấu ấn nổi bật năm 2025 của Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao

★ 2. "Không Một Mình" sức mạnh cộng đồng trong xây dựng thế trận an ninh nhân dân trên không gian mạng

★ 3. Chiêu trò lừa đảo bằng AI: Nhận diện và phòng ngừa

Những dấu ấn nổi bật năm 2025 của Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao

Năm 2025, trong bối cảnh chuyển đổi số quốc gia và cuộc Cách mạng công nghiệp lần thứ tư diễn ra mạnh mẽ, không gian mạng đã vượt ra khỏi phạm vi một hạ tầng kỹ thuật đơn thuần để trở thành không gian chiến lược, gắn chặt với an ninh, chủ quyền quốc gia và sự phát triển bền vững của đất nước. Cùng với cơ hội lớn cho phát triển kinh tế - xã hội, không gian mạng cũng đang đặt ra những nguy cơ, thách thức phi truyền thống ngày càng phức tạp, từ tấn công mạng, gián điệp mạng, chiến tranh thông tin đến các hoạt động lợi dụng không gian mạng xâm phạm an ninh quốc gia, trật tự an toàn xã hội.

Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05), với vai trò là "Tư lệnh" hệ lực lượng an ninh mạng và phòng, chống tội phạm công nghệ cao, đã phát huy rõ nét vai trò trụ cột, nòng cốt trong bảo đảm an ninh mạng, bảo vệ chủ quyền số, lợi ích quốc gia trên không gian mạng; qua đó góp phần giữ vững ổn định chính trị, tạo nền tảng vững chắc cho phát triển đất nước trong kỷ nguyên số.

Tạo hành lang pháp lý vững chắc cho bảo vệ không gian mạng

Một trong những dấu ấn nổi bật của Cục A05 trong năm 2025 là vai trò chủ trì, tham mưu xây dựng và hoàn thiện hệ thống pháp luật về bảo đảm an ninh mạng, an toàn thông tin và bảo vệ bí mật nhà nước trên không gian mạng. Trên cơ sở nghiên cứu, đánh giá toàn diện tình hình an ninh mạng trong nước và quốc tế, Cục A05 đã tham mưu cho Đảng, Nhà nước và Bộ Công an ban hành nhiều chủ trương, chính sách chiến lược, qua đó hình thành hành lang pháp lý đồng bộ, thống nhất, đáp ứng yêu cầu thực tiễn mới.

Nổi bật là việc chủ trì tham mưu xây dựng, trình Quốc hội thông qua Luật Bảo vệ dữ liệu cá nhân và Luật An ninh mạng năm 2025; tham mưu Chính phủ ban hành Nghị định quy định chi tiết thi hành Luật Bảo vệ dữ liệu cá nhân; đồng thời tiếp tục nghiên cứu, xây dựng các Nghị định hướng dẫn thi hành Luật An ninh mạng. Đây là những văn bản có ý nghĩa đặc biệt quan trọng, góp phần nâng cao hiệu lực, hiệu quả quản lý nhà nước về an ninh mạng, an toàn thông tin trong bối cảnh dữ liệu và công nghệ số trở thành tài nguyên chiến lược.

Chủ động tham mưu chiến lược, điều phối quốc gia về an ninh mạng

Phát huy vai trò nòng cốt, tiên phong trong chuyển đổi số quốc gia, Cục A05 đã tham gia xây dựng và triển khai hiệu quả nhiều Chỉ thị, Nghị quyết,

Một trong những dấu ấn nổi bật trong năm 2025 của Cục an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an là tham mưu xây dựng và hoàn thiện hệ thống pháp luật về bảo đảm an ninh mạng, an toàn thông tin và bảo vệ bí mật nhà nước trên không gian mạng

Đề án, Dự án chiến lược của Trung ương và Bộ Công an trong lĩnh vực an ninh mạng. Đặc biệt, việc triển khai Kế hoạch thực hiện Chương trình hành động theo Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị đã khẳng định rõ vai trò của lực lượng an ninh mạng trong đột phá phát triển khoa học - công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia.

Với vai trò là Cơ quan thường trực của Ban Chỉ đạo An ninh mạng quốc gia, Cục A05 đã tham mưu Thủ tướng Chính phủ ban hành Quyết định kiện toàn Ban Chỉ đạo, sửa đổi Quy chế hoạt động; hướng dẫn Công an các địa phương kiện toàn Ban Chỉ đạo cấp tỉnh; tổ chức sơ kết 6 năm thực hiện Nghị quyết số 30 của Bộ Chính trị về Chiến lược An ninh mạng quốc gia. Đặc biệt, việc tham mưu tổ chức thành công Lễ kỷ niệm Ngày An ninh mạng Việt Nam lần thứ I (6/8/2025) đã tạo dấu mốc quan trọng trong nâng cao nhận thức xã hội và định hình bản sắc an ninh mạng Việt Nam.

Song song đó, Cục A05 thực hiện tốt vai trò điều phối, định hướng hoạt động của Hiệp hội An ninh mạng quốc gia, qua đó thúc đẩy liên kết nhà nước - doanh nghiệp - xã hội trong bảo đảm an ninh mạng và phòng, chống tội phạm công nghệ cao.

Bảo vệ vững chắc chủ quyền quốc gia trên không gian mạng

Trong bối cảnh không gian mạng trở thành "mặt trận" mới gắn liền với an ninh, quốc phòng và đối ngoại, công tác đấu tranh với các hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia được Cục A05 triển khai chủ động, bài bản và hiệu quả. Lực lượng thường trực nắm tình hình 24/7 trên không gian mạng được duy trì, bảo đảm an ninh, an toàn thông tin tuyệt đối cho các sự kiện chính trị – xã hội trọng đại của đất nước như Lễ kỷ niệm 50 năm Ngày Giải phóng miền Nam, thống nhất đất nước (A50); Kỷ niệm 80 năm Cách mạng Tháng Tám và Quốc khánh 2/9 (A80); Đại hội đại biểu toàn quốc lần thứ XIV của Đảng.

Cục A05 đã kiểm soát chặt chẽ các mục tiêu, hội nhóm chống phá; kịp thời phát hiện, vô hiệu hóa âm mưu, hoạt động của các tổ chức, đối tượng phản động trên không gian mạng. Đồng thời, tổ chức giám sát, bảo vệ an ninh mạng đối với các hệ thống thông tin trọng yếu quốc gia; truy vết, phân tích hoạt động của các nhóm tin tặc, gián điệp mạng; phát hiện và xử lý nhiều dòng mã độc mới, qua đó góp phần bảo vệ vững chắc chủ quyền và lợi ích quốc gia trên không gian mạng.

Chủ lực trong đấu tranh phòng, chống tội phạm công nghệ cao

Trước sự gia tăng cả về số lượng, quy mô và mức độ tinh vi của tội phạm công nghệ cao, Cục A05 tiếp tục giữ vai trò chủ lực trong công tác phòng ngừa, phát hiện, đấu tranh và xử lý các loại tội phạm này. Thông qua việc áp dụng đồng bộ các biện pháp nghiệp vụ, kỹ thuật chuyên sâu, lực lượng đã tập trung xử lý có trọng tâm, trọng điểm các loại tội phạm nổi cộm như lừa đảo chiếm đoạt tài sản, tấn công mạng, đánh cắp dữ liệu, tổ chức đánh bạc, rửa tiền và tội phạm xuyên quốc gia.

Bảo vệ vững chắc chủ quyền quốc gia trên không gian mạng

Đáng chú ý, bên cạnh đấu tranh trực diện, Cục A05 đặc biệt coi trọng công tác phòng ngừa xã hội. Hàng trăm phóng sự, video tuyên truyền, cảnh báo phương thức, thủ đoạn tội phạm mạng được triển khai trên các nền tảng báo chí và mạng xã hội. Nổi bật là chiến dịch "Chống bắt cóc trực tuyến – KHÔNG MỘT MÌNH" thu hút hơn 2.000 điểm trường trên cả nước; các chiến dịch phối hợp với Google, TikTok như "An toàn hơn cùng Bộ Công an và Google", "Chống lừa đảo trực tuyến 2025", góp phần nâng cao nhận thức cộng đồng và hiệu quả phòng, chống tội phạm công nghệ cao.

Nâng cao năng lực bảo vệ hệ thống thông tin trọng yếu

Cục A05 đã tổ chức thẩm định, kiểm tra, đánh giá an ninh mạng đối với hàng chục đề án, dự án ứng dụng CNTT trong và ngoài lực lượng CAND; triển khai hàng trăm đoàn kiểm tra việc chấp hành quy định về bảo đảm an ninh mạng, bảo vệ bí mật nhà nước và dữ liệu cá nhân. Đồng thời, chủ động điều phối, hỗ trợ các cơ quan, đơn vị xử lý nhiều sự cố an ninh mạng nghiêm trọng; phát hành hàng trăm thông báo, điện mật, hướng dẫn nghiệp vụ về ứng phó, khắc phục tấn công mạng, góp phần nâng cao năng lực phòng vệ không gian mạng quốc gia.

Làm chủ công nghệ, phục vụ chuyển đổi số

Một điểm sáng nổi bật là việc Cục A05 tự chủ nghiên cứu, làm chủ và ứng dụng công nghệ. Nền tảng liên lạc an toàn SIGNET do Cục A05 phát triển đã đủ năng lực thay thế các ứng dụng OTT nước ngoài, được triển khai rộng rãi trong lực lượng CAND và nhiều địa phương. Bên cạnh đó, việc ứng dụng các công nghệ mới như Big Data, AI, điện toán đám mây, mã hóa lượng tử, UAV, camera thông minh... đã nâng cao hiệu quả công tác bảo vệ an ninh quốc gia trong không gian số.

Tiếp tục giữ vững vai trò trụ cột trong giai đoạn mới

Thời gian tới, trước những diễn biến phức tạp của an ninh mạng toàn cầu, Cục A05 tiếp tục phát huy vai trò trụ cột, chủ động nắm tình hình, nâng cao năng lực dự báo; tăng cường bảo vệ hệ thống thông tin trọng yếu; đẩy mạnh đấu tranh với tội phạm công nghệ cao; hoàn thiện cơ chế, chính sách pháp luật về an ninh mạng, an ninh dữ liệu và trí tuệ nhân tạo; xây dựng thế trận an ninh mạng toàn dân, góp phần bảo đảm vững chắc chủ quyền quốc gia trên không gian mạng trong tình hình mới.

19/12/2025 Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an đã tổ chức hoạt động diễn tập an ninh mạng nhằm sẵn sàng ứng phó, xử lý những nguy cơ, thách thức từ không gian mạng của lực lượng chuyên trách bảo vệ an ninh mạng trực thuộc Bộ Công an

"Chiến dịch là minh chứng sống động cho tinh thần hợp tác, lan tỏa thông điệp nhân văn: Không một trẻ em nào bị bỏ lại một mình trước những rủi ro trên mạng" - Trung tướng Lê Xuân Minh khẳng định.

"Không Một Mình" sức mạnh cộng đồng trong xây dựng thế trận an ninh nhân dân trên không gian mạng

Không gian mạng ngày nay đã trở thành một phần quen thuộc của đời sống xã hội, nơi con người kết nối, học tập, làm việc, sáng tạo và mở rộng cơ hội phát triển. Tuy nhiên, đi cùng với những tiện ích đó là hàng loạt rủi ro ngày càng phức tạp như lừa đảo trực tuyến, tin giả, bạo lực mạng, xâm hại trẻ em và các loại tội phạm công nghệ cao mang tính xuyên biên giới. Những nguy cơ này không còn là những vụ việc đơn lẻ, mà đang dần hình thành các thách thức an ninh có tính hệ thống, tác động trực tiếp đến trật tự an toàn xã hội, đặt ra yêu cầu cấp thiết phải xây dựng những cơ chế bảo vệ chủ động, bền vững và dựa trên sức mạnh của cộng đồng.

Liên minh Niềm Tin Số - huy động sức mạnh cộng đồng trên không gian mạng

Thực tiễn cho thấy, không một lực lượng chuyên trách nào có thể đơn độc kiểm soát toàn bộ không gian mạng rộng lớn, linh hoạt và biến đổi không ngừng. Đặc thù của không gian số đòi hỏi một cách tiếp cận toàn diện hơn, trong đó người dân không chỉ là đối tượng được bảo vệ, mà còn là chủ thể tham gia bảo vệ chính mình và cộng đồng. Từ yêu cầu đó, xây dựng thế trận an ninh nhân dân trên không gian mạng trở thành một nhiệm vụ mang tính chiến lược, gắn liền với sự ổn định và phát triển bền vững của xã hội trong kỷ nguyên số.

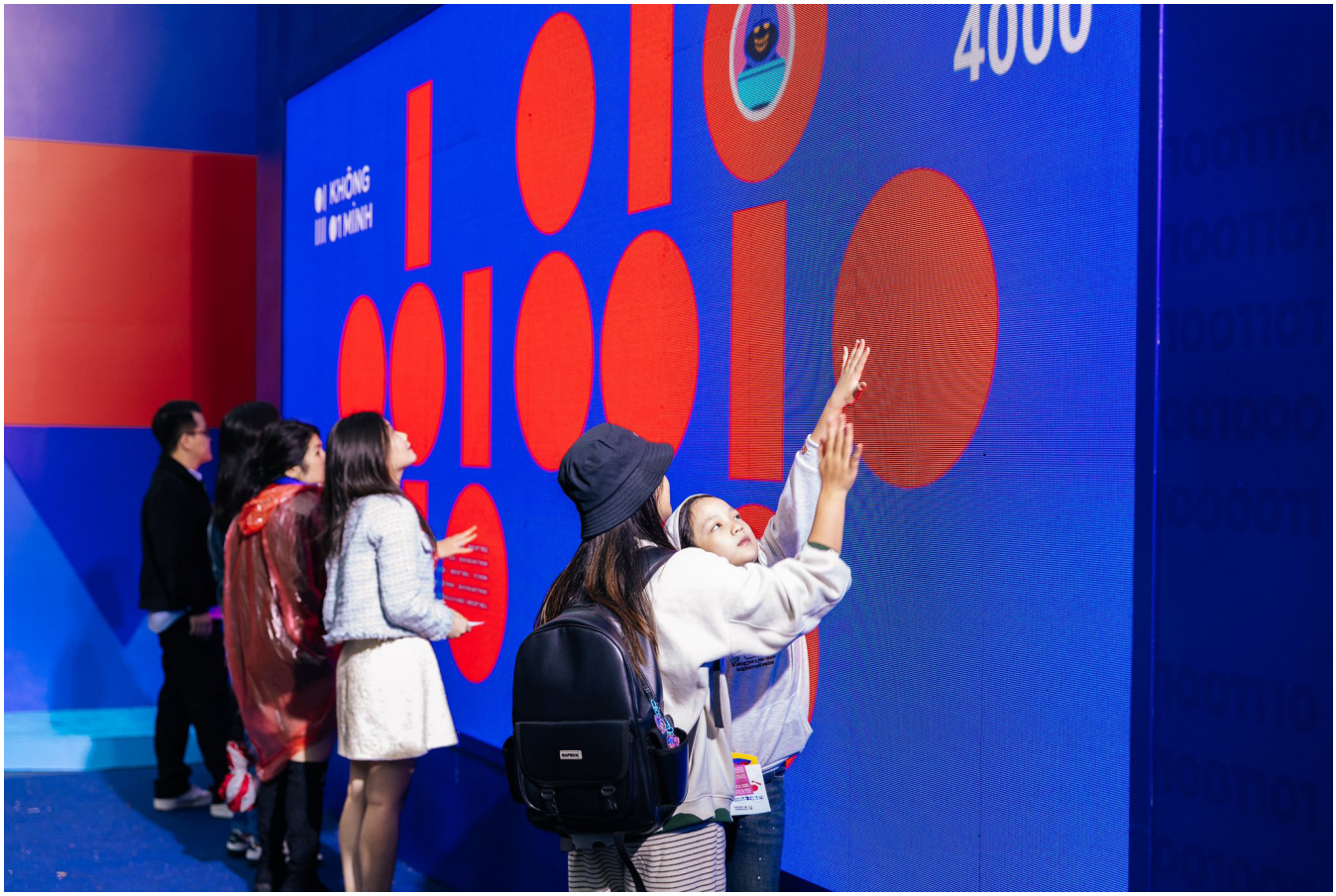
Trong bối cảnh ấy, Chiến dịch "Không Một Mình" do Liên minh Niềm Tin Số khởi xướng đã được triển khai như một mô hình tiêu biểu trong huy động sức mạnh cộng đồng, tổ chức nguồn lực xã hội và chuyển hóa phòng ngừa tội phạm mạng thành hành động toàn dân. Không chỉ là một hoạt động truyền thông, chiến dịch từng bước kiến tạo một không gian kết nối rộng khắp, nơi cơ quan quản lý, nhà trường, doanh nghiệp, nền tảng số, nhà sáng tạo nội dung, KOL, KOC và hàng triệu người dân cùng tham gia xây dựng môi trường mạng an toàn, nhân văn và đáng tin cậy.

Từ một thông điệp giản dị nhưng giàu ý nghĩa - "Không Một Mình" - chiến dịch đã lan tỏa thành một phong trào xã hội có chiều sâu. Hơn 40 triệu người dân Việt Nam đã được tiếp cận nội dung chiến dịch, tạo ra hơn 1.5 tỷ lượt xem và tương tác trên các nền tảng số. Giá trị cốt lõi không chỉ nằm ở những con số truyền thông, mà ở

Trung tướng Lê Xuân Minh - Cục trưởng Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05, Bộ Công an), Phó Chủ tịch Điều hành Hiệp hội An ninh mạng quốc gia phát biểu khai mạc phiên tọa đàm bên lề Lễ mở ký Công ước của Liên hợp quốc về chống tội phạm mạng, với chủ đề "Vai trò của nền tảng trực tuyến trong bảo vệ trẻ em và thanh thiếu niên trước tội phạm mạng"

Chiều 01/11/2025, tại phố đi bộ hồ Hoàn Kiếm, Hà Nội, Ngày hội An toàn trực tuyến "Không Một Mình" chính thức được khai mạc, chung tay hướng tới một không gian mạng an toàn, lành mạnh cho trẻ em và thanh thiếu niên.

sự chuyển biến trong vai trò và nhận thức của cộng đồng. Từ chỗ là những người tiếp nhận thông tin thụ động, nhiều người đã trở thành chủ thể chủ động lan tỏa cảnh báo, chia sẻ kinh nghiệm tự bảo vệ và hỗ trợ những người từng gặp rủi ro. Không gian mạng vì thế dần hình thành một mạng lưới cảnh báo xã hội, nơi phòng ngừa không còn là nhiệm vụ riêng của cơ quan chức năng, mà trở thành hành vi thường xuyên của chính người dân.



Tại không gian triển lãm số đa giác quan, khách tham quan sẽ được trải nghiệm hệ thống tương tác ánh sáng, âm thanh và công nghệ ấn tượng

Sức sống của chiến dịch còn thể hiện ở khả năng kết nối nhiều tầng lớp xã hội vào cùng một mục tiêu chung. Nhà trường trở thành tuyến giáo dục nền tảng, nơi học sinh được trang bị kỹ năng an toàn số thông qua những hình thức sáng tạo, gần gũi và dễ tiếp nhận. Gia đình đóng vai trò điểm tựa, đồng hành cùng trẻ em trong việc hình thành thói quen sử dụng mạng an toàn và có trách nhiệm. Báo chí, nhà sáng tạo nội dung, nghệ sĩ và những người có ảnh hưởng góp phần chuyển tải thông điệp theo cách giàu cảm xúc, truyền cảm hứng và phù hợp với giới trẻ. Doanh nghiệp công nghệ và các nền tảng số xuyên biên giới tham gia hỗ trợ lan tỏa nội dung, tăng cường cảnh báo rủi ro và phối hợp xử lý các hành vi vi phạm, qua đó góp phần mở rộng "vòng bảo vệ" cộng đồng mạng tại Việt Nam trong một không gian mạng không có ranh giới địa lý.

Ở quy mô cơ sở, chiến dịch đã được triển khai tại hàng nghìn điểm trường trên khắp 34 tỉnh, thành phố, tiếp cận hàng triệu học sinh, sinh viên, giáo viên và phụ huynh. Những buổi sinh hoạt chuyên đề, hoạt động ngoại khóa, chương trình truyền thông cộng đồng tại khu dân cư, khu công nghiệp và tổ dân phố đã đưa kiến thức, kỹ năng an toàn mạng đến gần hơn với người dân ở mọi lứa tuổi. Những thay đổi tưởng như nhỏ trong hành vi cá nhân - như cẩn trọng hơn khi chia sẻ thông tin, chủ động hơn khi phát hiện dấu hiệu lừa đảo, sẵn sàng hơn trong việc cảnh báo và hỗ trợ người khác - khi được nhân rộng trên quy mô xã hội đã tạo thành một "lá chắn cộng đồng" hiệu quả trên không gian mạng.

Định hướng hợp tác với các nền tảng số xuyên biên giới - bước đi chiến lược

Trong bối cảnh tội phạm mạng mang tính xuyên quốc gia, việc mở rộng phối hợp với các nền tảng số xuyên biên giới là một bước đi có ý nghĩa chiến lược. Thông qua cơ chế hợp tác này, các thông điệp an toàn trực tuyến được lan tỏa sâu rộng hơn, các nguy cơ liên quan đến lừa đảo, xâm hại và nội dung độc hại được phát hiện và xử lý kịp thời hơn, qua đó nâng cao năng lực bảo vệ người dùng Việt Nam trong không gian mạng toàn cầu. Đây cũng là cách tiếp cận phù hợp với bản chất không biên giới của môi trường số hiện đại, nơi các mối đe dọa không chỉ bó hẹp trong ranh giới lãnh thổ.

Để một phong trào cộng đồng có thể phát huy hiệu quả lâu dài, vai trò định hướng chuyên môn và điều phối nguồn lực là yếu tố then chốt. Trong tiến trình

này, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an (Cục A05) đã góp phần quan trọng trong việc định hướng nội dung, kết nối các chủ thể xã hội và bảo đảm các hoạt động của chiến dịch bám sát mục tiêu phòng ngừa, bảo vệ người dân trên không gian mạng. Vai trò ấy được thể hiện qua định hướng nhất quán, kết nối bền bỉ và việc từng bước xây dựng các nền tảng hợp tác lâu dài, bảo đảm sức mạnh cộng đồng được phát huy đúng hướng, đúng trọng tâm và có chiều sâu.

"Không Một Mình" - hướng đi mới của cách tiếp cận lấy dân làm gốc

Giá trị cốt lõi của Chiến dịch "Không Một Mình" nằm ở việc chuyển hóa "Thế trận An ninh nhân dân trên không gian mạng" thành những hành vi cụ thể trong đời sống hằng ngày. Khi một học sinh biết từ chối lời mời đáng ngờ, khi một phụ huynh chủ động đồng hành cùng con trong thế giới số, khi một người lao động kịp thời nhận diện chiêu trò lừa đảo và cảnh báo người khác, hay khi một cộng đồng sẵn sàng chia sẻ thông tin và hỗ trợ nạn nhân, thì "Thế trận An ninh nhân dân" không còn là một khẩu hiệu, mà đã trở thành một thực thể sống động trong đời sống xã hội. Ở đó, mỗi người dân là một điểm tựa an toàn, mỗi gia đình là một tuyến phòng vệ, mỗi cộng đồng là một lớp bảo vệ, và toàn xã hội hợp thành một mạng lưới phòng ngừa linh hoạt, hiệu quả.

Từ góc nhìn chiến lược, Chiến dịch "Không Một Mình" cho thấy một chân lý có tính lâu dài trong bảo đảm an ninh mạng: công nghệ và nghiệp vụ là điều kiện quan trọng, nhưng sức mạnh cộng đồng mới là

Sáng 11/10, sự kiện Cyber Day 2025 - Being Well, Being Me được tổ chức tại Hệ thống Trường Phổ thông Liên cấp Song ngữ Quốc tế Wellspring - đơn vị tiên phong hưởng ứng chiến dịch "Không Một Mình - Cùng nhau an toàn trực tuyến", lan tỏa tinh thần Công ước Hà Nội 2025. Đây là sáng kiến của Liên hợp Quốc về xây dựng không gian mạng nhân văn, an toàn và bao trùm cho mọi thế hệ.

nền tảng bền vững nhất. Khi người dân được trang bị tri thức, khi cộng đồng được kết nối, khi các nền tảng cùng chia sẻ trách nhiệm và khi các cơ quan chuyên trách giữ vai trò định hướng, thế trận an ninh nhân dân trên không gian mạng sẽ ngày càng phát huy sức mạnh, chủ động và có chiều sâu chiến lược.

"Không Một Mình" vì thế không chỉ là tên gọi của một chiến dịch, mà là biểu tượng cho một cách tiếp cận mới trong bảo vệ an ninh quốc gia trên không gian mạng - lấy người dân làm gốc, lấy cộng đồng làm nền, và lấy sự đồng lòng làm sức mạnh cốt lõi. Trong một không gian số rộng lớn và không ngừng biến đổi, chính tinh thần cộng đồng, trách nhiệm xã hội và sự kết nối bền chặt giữa các chủ thể sẽ là nền tảng quan trọng để gìn giữ một môi trường mạng an toàn, nhân văn và đáng tin cậy.

Chiêu trò lừa đảo bằng AI: Nhận diện và phòng ngừa

Đăng Khoa

1 THỰC TRẠNG LỪA ĐẢO DỰA TRÊN AI

- AI đang bị tội phạm mạng khai thác ngày càng nhiều cho các chiêu trò lừa đảo tinh vi
- Giả mạo giọng nói, hình ảnh, tin nhắn giống hệt người thật
- Nạn nhân khó phân biệt thật giả chỉ trong vài giây

2 CÁC THỦ ĐOẠN LỪA ĐẢO PHỔ BIẾN

- **Giả giọng nói AI:** Sao chép giọng nói của lãnh đạo hoặc người thân để yêu cầu chuyển tiền khẩn cấp
- **Video, hình ảnh Deepfake:** Tạo cuộc gọi video trực tiếp sử dụng khuôn mặt của người quen
- **Email, tin nhắn gửi bởi AI:** Tin nhắn do AI tạo, ngôn ngữ tự nhiên, chính tả đúng, cá nhân hóa cao
- **Chatbot chăm sóc khách hàng giả mạo:** Mạo danh ngân hàng, sàn thương mại điện tử để chiếm đoạt mã OTP, mật khẩu
- **Lừa đảo đầu tư và tình cảm:** Tài khoản giả sử dụng AI trò chuyện, dụ dỗ chuyển tiền

3 DẤU HIỆU LỪA ĐẢO AI

- Yêu cầu hành động khẩn cấp, tạo áp lực thời gian
- Lý do nghe có vẻ hợp lý nhưng khó xác minh
- Tránh việc xác minh qua các kênh quen thuộc khác
- Biết nhiều thông tin cá nhân nhưng thiếu chi tiết thực tế
- Giọng nói, video có điểm bất thường (ngữ điệu, cử động miệng)

4 PHƯƠNG PHÁP PHÒNG NGỪA HIỆU QUẢ

- Luôn xác minh qua nhiều kênh trước khi chuyển tiền
- Tránh chia sẻ công khai quá nhiều hình ảnh cá nhân hoặc bản ghi âm giọng nói
- Bật Xác thực đa yếu tố (MFA) cho tài khoản của bạn
- Trang bị kỹ năng số cho bản thân và doanh nghiệp
- Báo cáo ngay hoạt động khả nghi cho ngân hàng, nền tảng hoặc cơ quan chức năng

NÂNG CAO NĂNG LỰC TỰ CHỦ CÔNG NGHỆ

★ 1. An ninh mạng 2025: Bức tranh đa màu sắc từ người dùng cá nhân - doanh nghiệp

★ 2. Nền tảng pháp lý – trụ cột của năng lực tự chủ công nghệ quốc gia

★ 3. Công nghiệp an ninh mạng nền tảng tự chủ công nghệ và năng lực cạnh tranh quốc gia

★ 4. Bảo đảm an ninh mạng Nền tảng phát triển bền vững của ngành ngân hàng trong kỷ nguyên mới

★ 5. AI và bài toán làm chủ công nghệ trong bảo vệ không gian mạng

★ 6. Lưu ký tài sản số và yêu cầu an ninh hạ tầng trong kinh tế số

★ 7. Bảo vệ dữ liệu cá nhân -nền tảng của niềm tin số và tự chủ công nghệ

★ 8. An ninh mạng trong kỷ nguyên AI: Khi đổi mới phải đi đôi với năng lực phục hồi

★ 9. Nguồn nhân lực an toàn, an ninh thông tin - trụ cột của tự chủ công nghệ

An ninh mạng 2025: Bức tranh đa màu sắc từ người dùng cá nhân - doanh nghiệp

Ban Nghiên cứu, tư vấn, phát triển công nghệ và Hợp tác quốc tế của Hiệp hội An ninh mạng quốc gia

Hiệp hội An ninh mạng Quốc gia (NCA) vừa công bố Báo cáo nghiên cứu, khảo sát an ninh mạng năm 2025 với sự tham gia của 60.300 người dùng cá nhân và hơn 5.300 đơn vị, tổ chức tại Việt Nam. Dữ liệu được công bố ghi nhận những chuyển biến trái chiều trong bức tranh an ninh mạng 2025: số vụ tấn công và số nạn nhân lừa đảo trực tuyến có xu hướng giảm, song mức độ tinh vi và thiệt hại lại gia tăng.

Từ người dùng cá nhân đến các cơ quan, doanh nghiệp, các mối đe dọa trên không gian mạng đang chuyển dịch theo hướng có chọn lọc, khai thác sâu dữ liệu và tạo ra những rủi ro ngày càng phức tạp, đặt ra yêu cầu cấp thiết về nâng cao năng lực phòng thủ và quản trị an ninh mạng...

Chiêu thức lừa đảo biến đổi và ngày càng tinh vi tấn công người dùng cá nhân

Đối với người dùng cá nhân, lần đầu tiên sau nhiều năm, số nạn nhân của lừa đảo trực tuyến ghi nhận xu hướng giảm. Tuy nhiên, sự cải thiện về số lượng không đồng nghĩa với việc mức độ rủi ro đã được kiểm soát hoàn toàn, khi các hình thức tấn công mạng tiếp tục biến đổi nhanh chóng và ngày càng tinh vi.

Theo kết quả khảo sát, tỷ lệ người dùng trở thành nạn nhân của lừa đảo trực tuyến trong năm 2025 giảm rõ rệt so với năm trước. Cụ thể, cứ khoảng 555 người tham gia khảo sát thì có 1 người cho biết từng bị lừa đảo, tương đương tỷ lệ 0,18%. Trong khi đó, năm 2024, tỷ lệ này ở mức 0,45%, tức khoảng 220 người thì có 1 người là nạn nhân.

Nhận định về kết quả trên, Hiệp hội An ninh mạng quốc gia cho rằng đây là chuyển biến rất tích cực, phản ánh hiệu quả bước đầu của các biện pháp phòng, chống lừa đảo được triển khai đồng bộ trong thời gian qua. Đặc biệt, các chuyên án triệt phá ổ nhóm tội phạm lừa đảo trực tuyến do Bộ Công an triển khai cao điểm cả trong và ngoài nước đã góp phần làm suy giảm

Ảnh minh hoạ

đáng kể hoạt động của các đường dây phạm tội có tổ chức. Song song với đó, công tác tuyên truyền, phổ biến kiến thức nhận diện lừa đảo tới người dân tiếp tục được đẩy mạnh với nhiều hình thức đa dạng, giúp nâng cao mức độ cảnh giác trong cộng đồng.

Một yếu tố quan trọng khác góp phần tạo ra "rào cản kỹ thuật" đối với tội phạm lừa đảo là các quy định mới của Ngân hàng Nhà nước về xác thực sinh trắc học đối với tài khoản cá nhân và doanh nghiệp. Việc siết chặt định danh đã khiến các đối tượng không còn dễ dàng sử dụng tài khoản "rác", không xác thực danh tính như giai đoạn trước năm 2024. Các ngân hàng cũng tăng cường kết nối, chia sẻ thông tin với Ngân hàng Nhà nước và Bộ Công an về các tài khoản có dấu hiệu liên quan đến lừa đảo, qua đó hỗ trợ kịp thời việc theo dõi, phong tỏa và ngăn chặn dòng tiền bị chiếm đoạt.

Tuy vậy, theo ông Vũ Ngọc Sơn Trưởng ban Nghiên cứu, tư vấn, phát triển công nghệ và Hợp tác quốc tế của Hiệp hội An ninh mạng quốc gia, người dùng không thể chủ quan. "Lừa đảo trực tuyến vẫn vô cùng phức tạp. Các đối tượng sẽ tìm cách ứng dụng công nghệ mới, thậm chí thử nghiệm những thủ đoạn, hình thức mới nhằm qua mặt các biện pháp phòng, chống. Nguy cơ đối với người dùng vẫn thường trực trên không gian mạng", ông Sơn cảnh báo.

Thực tế cho thấy, dù tỷ lệ nạn nhân giảm, thiệt hại do lừa đảo trực tuyến vẫn ở mức rất lớn. Theo thống kê của Bộ Công an, trong 11 tháng đầu năm 2025, tổng thiệt hại do tội phạm lừa đảo trực tuyến gây ra ước tính trên 6.000 tỷ đồng.

Về hình thức lừa đảo, khảo sát năm 2025 cho thấy các đối tượng vẫn chủ yếu sử dụng những kịch bản quen thuộc như mạo danh cơ quan, tổ chức; giả mạo trúng thưởng; giả shipper; giả người quen; kết bạn tình cảm hoặc mời gọi đầu tư tài chính. Tuy nhiên, điểm khác biệt là các chiêu trò này ngày càng được "nâng cấp" về kịch bản, công nghệ và tâm lý, khiến người dùng khó phân biệt thật - giả hơn trước.

Trong đó, hình thức mạo danh công an nổi lên là loại hình lừa đảo phổ biến nhất năm 2025. Các đối tượng thường dựng kịch bản cáo buộc người dùng liên quan đến vụ án hình sự, yêu cầu giữ liên lạc để tạo áp lực tâm lý, sau đó chúng yêu cầu "chuyển tiền chứng minh trong sạch" hoặc cài đặt phần mềm giả mạo với danh nghĩa "phục vụ điều tra" nhằm chiếm đoạt tài sản. Đáng chú ý, nhiều vụ việc cho thấy các đối tượng còn dàn dựng trụ sở công an giả, sử dụng nhiều người đóng vai khác nhau và thao túng nạn nhân qua video call để tăng độ tin cậy.

Thủ đoạn lừa thông báo trúng thưởng, nhận quà để chiếm đoạt tiền đứng thứ hai về mức độ phổ biến. Trong khi đó, hình thức mời gọi đầu tư với lợi nhuận cao đã giảm xuống vị trí thứ ba, cho thấy người dân dần cảnh giác hơn với các lời hứa hẹn làm giàu nhanh chóng từng bùng nổ mạnh mẽ trong năm trước. Các hình thức khác như giả

shipper hay kết bạn, giao lưu tình cảm tiếp tục xếp ở các vị trí tiếp theo, tồn tại dai dẳng dù không phải là thủ đoạn mới.

Một vấn đề đáng lo ngại khác là thói quen trình báo khi gặp lừa đảo của người dân chưa được cải thiện rõ rệt. Chỉ 32,12% nạn nhân cho biết đã báo cáo sự việc với cơ quan chức năng. Phần lớn còn lại chỉ cảnh báo cho người thân, bạn bè, thậm chí 12,03% chấp nhận mất tiền mà không có bất kỳ hành động nào tiếp theo. Và việc không trình báo khiến cơ quan chức năng thiếu dữ liệu để điều tra, xử lý và đưa ra cảnh báo sớm cho cộng đồng, trở thành rào cản lớn trong công tác phòng, chống lừa đảo.

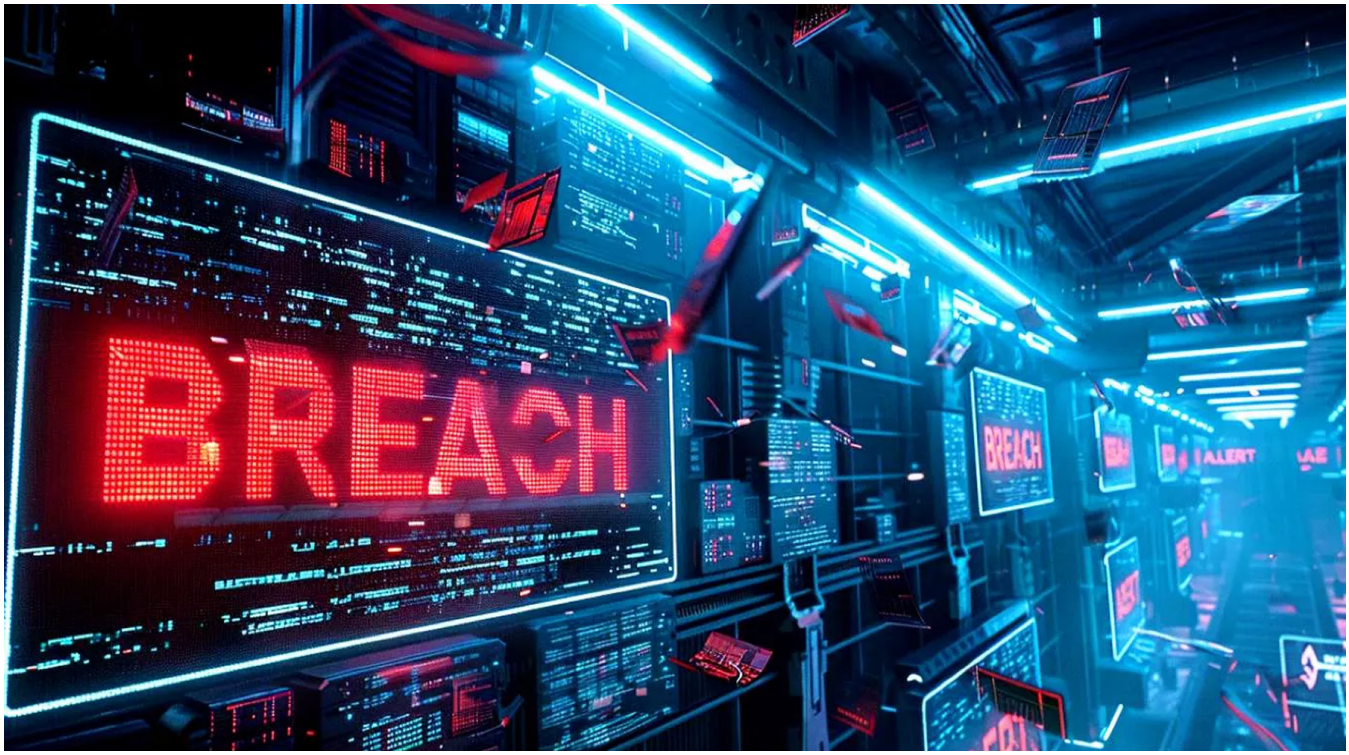
An ninh mạng người dùng cá nhân: mảng tối - sáng đan xen

Bên cạnh lừa đảo, mã độc tiếp tục là mối đe dọa lớn đối với người dùng cá nhân. Khảo sát cho thấy trong năm 2025 có tới 34,13% người dùng từng gặp ít nhất một sự cố liên quan đến mã độc, tăng mạnh so với mức 23,40% của năm 2024. Điều này phản ánh thực tế các hình thức tấn công ngày càng tinh vi và khó nhận biết hơn, đặc biệt trên môi trường số quen thuộc với người dùng.

Hệ thống phòng, chống lừa đảo nTrust của Hiệp hội An ninh mạng quốc gia ghi nhận 62.952 loại mã độc mới trên điện thoại di động được phát hiện tại Việt Nam trong năm 2025. Đáng chú ý, trong số này có 931 loại phần mềm giả mạo các ứng dụng phổ biến, nhằm đánh cắp thông tin hoặc chiếm quyền điều khiển thiết bị, gây ra nhiều rủi ro về an ninh dữ liệu và tài chính cá nhân. Xu hướng này cho thấy tội phạm mạng đang ngày càng tập trung khai thác nền tảng di động - nơi người dùng lưu trữ nhiều dữ liệu nhạy cảm.

Song song với đó, tình trạng lộ và sử dụng trái phép dữ liệu cá nhân vẫn diễn ra phổ biến. Có tới 88,05% người dùng phản ánh từng bị mời chào dịch vụ dù không có nhu cầu hay chưa từng đăng ký nhận thông tin. Những con số này cho thấy nguy cơ mất an ninh dữ liệu cá nhân vẫn ở mức đáng báo động.

Ở chiều tích cực, ý thức và kỹ năng an ninh mạng của người dùng đã có sự cải thiện rõ rệt. Nếu như năm 2024, nhiều người còn thờ ơ với quyền truy cập của ứng dụng, thì đến năm 2025 đã có 83,23% người tham gia khảo sát cho biết họ chú ý đọc các quyền khi cài đặt ứng dụng, đặc biệt với các ứng dụng liên quan đến ngân hàng. Hơn một nửa người dùng (56,80%) cho biết họ thường xuyên kiểm tra lại thông tin trước khi chuyển tiền hoặc



Ảnh minh hoạ

cung cấp dữ liệu cá nhân.

Bên cạnh đó, 83,20% người dùng đã chủ động sử dụng mật khẩu mạnh và kích hoạt xác thực hai yếu tố cho các tài khoản quan trọng. Đáng chú ý, 60,20% người tham gia khảo sát cho biết đã tìm hiểu hoặc tham gia các khóa học nâng cao kỹ năng an ninh mạng, cao hơn rõ rệt so với năm 2024. Theo các chuyên gia, đây là tín hiệu tích cực cho thấy nhu cầu tự bảo vệ trên không gian mạng của người dân đang ngày càng gia tăng trong bối cảnh chuyển đổi số diễn ra mạnh mẽ.

Tổ chức, doanh nghiệp: Tấn công giảm về lượng, gia tăng thiệt hại và rủi ro dữ liệu

Trong năm 2025, các hệ thống thông tin tại Việt Nam phải đối mặt với khoảng 552.000 cuộc tấn công mạng, giảm 19,38% so với năm 2024. Diễn biến này cho thấy những nỗ lực đầu tư cho an ninh mạng của các cơ quan, tổ chức, doanh nghiệp đã bước đầu phát huy hiệu quả, khiến các hình thức tấn công không còn dễ dàng như trước.

Tuy nhiên, sự sụt giảm về số lượng không đồng nghĩa với việc mức độ rủi ro giảm đi. Khảo sát cho thấy 52,30% cơ quan, doanh nghiệp từng ghi nhận chịu tổn hại do tấn công mạng trong năm, tăng so với mức 46,15% của năm 2024. Điều này cho thấy tin tặc đang chuyển sang chiến lược tấn công có chọn lọc, tập trung vào từng mục tiêu cụ thể với mức độ chuẩn bị và khai thác sâu hơn.

Năm hình thức tấn công phổ biến nhất trong năm 2025 gồm: tấn công từ chối dịch vụ (DDoS); chèn link quảng cáo cờ bạc, cá độ; tấn công gián điệp có chủ đích (APT); tấn công đánh cắp dữ liệu; và mã hóa dữ liệu tống tiền. Đáng chú ý, các hình thức này thường được kết hợp đan xen trong những kịch bản tấn công phức tạp, nhằm đánh lạc hướng và khai thác tối đa điểm yếu của hệ thống.

Ông Vũ Ngọc Sơn nhận định, tin tặc có xu hướng triển khai các cuộc tấn công kép, xâm nhập và nằm vùng trong hệ thống để đánh cắp dữ liệu trước, chỉ tiến hành mã hóa dữ liệu khi không còn khả năng khai thác thêm nhằm tống tiền nạn nhân. Nếu như năm 2024, mã hóa dữ liệu tống tiền là mối đe dọa chủ đạo, thì sang năm 2025, các cuộc tấn công xâm phạm và đánh cắp dữ liệu lại gây ra hậu quả nghiêm trọng hơn. Tin tặc ngày càng coi dữ liệu là tài sản có giá trị cao để khai thác lâu dài thông qua mua bán, trao đổi trên các thị trường ngầm.

Công tác phòng thủ: Còn nhiều khoảng trống trong khối tổ chức, doanh nghiệp

Năm 2025 cũng ghi nhận những chuyển biến tích cực về nhận thức an ninh mạng trong khối tổ chức, doanh nghiệp. Tỷ lệ đơn vị tổ chức đào tạo nâng cao nhận thức an ninh mạng đạt 75,93%. Khoảng 51,45% đơn vị đã tổ chức diễn tập an ninh mạng, trong khi 51,65% cho biết đã triển khai hoặc vận hành Trung tâm giám sát an ninh mạng (SOC). Đặc biệt, 76,35% doanh nghiệp đã xây dựng hệ thống sao lưu dữ liệu dự phòng, sẵn sàng hơn cho các kịch bản phục hồi sau sự cố.

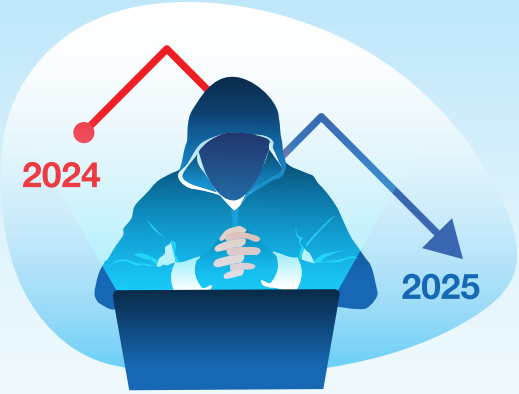
Dù vậy, phía sau những con số tích cực này vẫn còn nhiều khoảng trống đáng lo ngại. Gần một nửa số cơ quan, doanh nghiệp (47,72%) vẫn thiếu hụt nhân sự an ninh mạng. Có tới 27,80% đơn vị chưa triển khai bất kỳ tiêu chuẩn an ninh mạng nào trong nội bộ. Hơn một nửa số đơn vị chưa có phần mềm phòng, chống mã độc quản lý tập trung, trong khi 8,71% hoàn toàn không sử dụng phần mềm diệt virus. Đáng chú ý, 9,38% cơ quan, doanh nghiệp cho biết không có biện pháp kiểm soát truy cập Internet như tường lửa tại cửa ngõ hệ thống.

Nhìn tổng thể, so với năm 2024, an ninh mạng năm 2025 cho thấy những bước tiến rõ rệt về nhận thức, song mức độ đầu tư về giải pháp kỹ thuật và nhân lực vẫn chưa tương xứng với tốc độ và mức độ tinh vi của các cuộc tấn công. Thực tế này là lời cảnh báo rõ ràng rằng an ninh mạng không còn là vấn đề kỹ thuật đơn lẻ, mà đã trở thành bài toán quản trị, chiến lược và phát triển bền vững đối với cả người dùng cá nhân lẫn các tổ chức, doanh nghiệp trong kỷ nguyên số.

LỪA ĐẢO TRỰC TUYẾN GIẢM NHƯNG CHƯA THỂ CHỦ QUAN

Tỷ lệ nạn nhân
1/220 người

0,45%



0,18%

Tỷ lệ nạn nhân
1/555 người

Đây là chuyển biến rất tích cực sau nhiều năm, nhờ vào các biện pháp quyết liệt của cơ quan chức năng và công tác tuyên truyền, phổ biến kiến thức cộng đồng. Tuy nhiên lừa đảo trực tuyến vẫn vô cùng phức tạp, người dùng cần tiếp tục nâng cao cảnh giác.

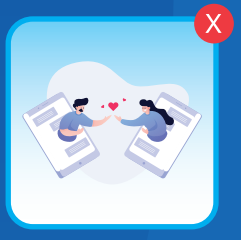
CÁC HÌNH THỨC LỪA ĐẢO PHỔ BIẾN NHẤT

1 | Mạo danh công an

2 | Lừa thông báo trúng thưởng, nhận quà

3 | Mời gọi đầu tư lợi nhuận cao

4 | Giả danh shipper



5 | Kết bạn, giao lưu tình cảm

AN NINH MẠNG

34,13%

Người dùng từng gặp sự cố mã độc

62.952

loại mã độc mới trên điện thoại di động

931

phần mềm giả mạo được phát hiện bởi Hệ thống phòng chống lừa đảo nTrust của NCA

NGƯỜI DÙNG CÁ NHÂN

83,23%

Người dùng đã chú ý đọc các quyền khi cài đặt ứng dụng

56,80%

thường kiểm tra lại thông tin

83,20%

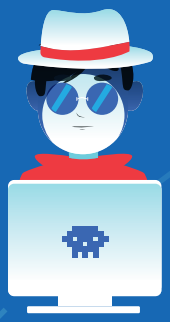
chủ động sử dụng mật khẩu mạnh, kích hoạt xác thực hai yếu tố (2FA)

60,20%

cho biết đã tìm hiểu hoặc tham gia các khóa học nâng cao kỹ năng an ninh mạng

Theo NCA, những tiến bộ tích cực trong ý thức của người dùng là tín hiệu đáng mừng, đặc biệt trong bối cảnh chuyển đổi số và ứng dụng công nghệ đang diễn ra mạnh mẽ

DỰ BÁO AN NINH MẠNG 2026



Các hình thức lừa đảo trực tuyến sẽ ngày càng tinh vi hơn với việc ứng dụng công nghệ như:

Giả mạo nhân dạng bằng Deepfake

Tạo mã độc bằng trí tuệ nhân tạo (AI)

NĂM 2026 ĐƯỢC KỲ VỌNG

Sẽ ghi nhận những cải thiện

Trong công tác bảo vệ dữ liệu cá nhân khi hàng loạt quy định pháp luật mới có hiệu lực.

Song song với đó, việc nâng cao nhận thức, kỹ năng số cho người dân sẽ tiếp tục là yếu tố then chốt

nhằm giảm thiểu rủi ro an ninh mạng.

Nền tảng pháp lý – trụ cột của năng lực tự chủ công nghệ quốc gia

Trung tướng, GS.TS Nguyễn Xuân Yêm

Viện trưởng Viện An ninh phi truyền thống , Trường Quản trị và Kinh doanh, Đại học Quốc gia Hà Nội

Nguyên Giám đốc Học viện Cảnh sát nhân dân, Bộ Công an

Luật Chuyển đổi số: Trụ cột hạ tầng thể chế cho tiến trình chuyển đổi số

Luật Chuyển đổi số gồm 8 chương, 48 điều, được xây dựng theo mô hình "luật khung"- quy định các nguyên tắc, yêu cầu và định hướng lớn. Dù không đi sâu vào các quy định thuộc phạm vi điều chỉnh của luật chuyên ngành nhưng đóng vai trò "trụ cột hạ tầng thể chế" cho toàn bộ tiến trình chuyển đổi số quốc gia, khi lần đầu tiên luật hóa các khái niệm nền tảng: Chuyển đổi số, hệ thống số, dữ liệu số, hạ tầng số, nền tảng số, Chính phủ số, kinh tế số, xã hội số.

Luật đã tháo gỡ các khó khăn chung về chuyển đổi số của các bộ, ngành, địa phương, tạo khung pháp lý thống nhất cho chuyển đổi số quốc gia, bảo đảm chuyển đổi số đúng hướng, an toàn, hiệu quả, khắc phục tình trạng "cát cứ" số, manh mún, chia cắt nền tảng, tạo ra môi trường cho đổi mới sáng tạo, thúc đẩy Chính phủ số, kinh tế số và xã hội số; chính thức hóa việc ban hành chương trình chuyển đổi số quốc gia, khung kiến trúc tổng thể quốc gia số, khung quản trị dữ liệu, khung năng lực số, bộ chỉ số đo lường chuyển đổi số quốc gia.

Luật Chuyển đổi số được xây dựng trên quan điểm lấy người sử dụng làm trung tâm, coi đây là nền tảng cho mọi hoạt động số hóa; bảo đảm tính thuận tiện, dễ tiếp cận, dễ dùng, phù hợp với nhiều nhóm đối tượng, bao gồm người yếu thế và các nhóm đối tượng dễ bị tổn thương.

Một điểm nhấn quan trọng là nguyên tắc "khai báo một lần là mặc định", tăng cường kết nối, chia sẻ và sử dụng lại dữ liệu; dữ liệu phải được thu thập, quản lý, chia sẻ, khai báo một lần và sử dụng hiệu quả để nâng cao chất lượng ra quyết định và chất lượng dịch vụ. Hệ thống phải được thiết kế dựa trên chuẩn mở, kiến trúc mở, hỗ trợ kết nối, tích hợp ngay từ đầu, giao diện lập trình ứng dụng theo chuẩn tạo thuận lợi cho chia sẻ dữ liệu và liên thông giữa các hệ thống.

Luật Chuyển đổi số yêu cầu bảo vệ dữ liệu và quyền riêng tư theo quy định; triển khai linh hoạt, thích ứng với sự phát triển nhanh của công nghệ; đồng thời bảo đảm tính bao trùm, minh bạch và trách nhiệm giải trình đối với mọi quyết định dựa trên công nghệ số. Để bảo đảm hiệu quả triển khai, Luật quy định cơ quan quản lý nhà nước về chuyển đổi số có trách nhiệm xây dựng và công bố bộ chỉ số đánh giá mức độ chuyển đổi số thống nhất, xây dựng, quản lý, vận hành Nền tảng thống kê, đo lường, giám sát, đánh giá triển khai chuyển đổi số; định kỳ hằng năm tổ chức đánh giá mức độ chuyển đổi số của quốc gia, các bộ, ngành, địa phương; kết quả đánh giá được công bố công khai và là căn cứ xếp hạng, khen thưởng, điều chỉnh chính sách... Các cơ quan nhà nước có trách nhiệm cung cấp dịch vụ công, quản trị nội bộ và điều hành trên môi trường số, trừ trường hợp pháp luật quy

Tại Kỳ họp thứ 10, Quốc hội khóa XV (tháng 12/2025) đã thông qua Luật Chuyển đổi số và Luật An ninh mạng (sửa đổi). Đây là bước đi quan trọng nhằm tạo hành lang pháp lý đồng bộ cho lĩnh vực an ninh mạng và chuyển đổi số; tạo ra khuôn khổ pháp lý toàn diện, thống nhất cho quốc gia số, xử lý những vấn đề mới về chính phủ số, kinh tế số, xã hội số.

Luật Chuyển đổi số(Luật số 148/2025/QH15) được Quốc hội Việt Nam thông qua vào ngày 11 tháng 12 năm 2025 và chính thức có hiệu lực thi hành kể từ ngày 01 tháng 7 năm 2026

định khác. Các hoạt động chỉ đạo, điều hành phải dựa trên dữ liệu số đầy đủ, chính xác và kịp thời. Quy trình nghiệp vụ phải được rà soát, chuẩn hóa, tái cấu trúc, bảo đảm tinh gọn, không trùng lặp và tăng cường tự động hóa.

Luật Chuyển đổi số thể hiện quyết tâm xây dựng nền tảng pháp lý đồng bộ, tạo động lực cho phát triển kinh tế số, xã hội số, hướng tới Chính phủ số hoạt động hiệu quả, phục vụ người dân và doanh nghiệp.

Luật An ninh mạng: Tăng cường bảo đảm an ninh, chủ quyền số

An ninh mạng và an toàn thông tin mạng trở thành vấn đề cấp thiết đối với mỗi quốc gia.

An ninh mạng thường được hiểu là các biện pháp bảo vệ hệ thống mạng khỏi các cuộc tấn công nhằm xâm nhập, phá hoại hoặc lấy cắp dữ liệu. Đây là yếu tố then chốt để bảo vệ các hạ tầng kỹ thuật quan trọng của đất nước khỏi sự đe dọa từ các hành vi tội phạm mạng.

An toàn thông tin mạng lại liên quan đến việc đảm bảo tính bảo mật, toàn vẹn và khả dụng của thông tin trong quá trình truyền tải qua mạng. Điều này không chỉ bao gồm các biện pháp bảo vệ dữ liệu mà còn là việc ngăn ngừa sự truy cập trái phép và đảm bảo thông tin không bị thay đổi một cách bất hợp pháp.

Dù hai khái niệm an ninh mạng và an toàn thông tin mạng có sự khác biệt nhất định, nhưng chúng lại có mối quan hệ mật thiết và bổ sung cho nhau trong việc bảo vệ không gian mạng. Thực tế thời gian qua cho thấy hệ thống thông tin của mỗi quốc gia luôn đối mặt với nguy cơ từ các mối đe dọa mạng, từ tin tặc, các tổ chức tội phạm cho đến các mối nguy hại đến từ các yếu tố bên ngoài. Các mối đe dọa trên không gian mạng ngày càng tinh vi và khó lường. Vì vậy, một hệ thống pháp lý thống nhất sẽ giúp các cơ quan chức năng dễ dàng hơn trong việc phát hiện, ngăn chặn và xử lý các hành vi vi phạm.

Luật An ninh mạng (sửa đổi) - Luật An ninh mạng 2025, gồm 8 chương, 45 điều, có hiệu lực thi hành từ ngày 1/7/2026, cơ bản kế thừa các quy định của Luật An toàn thông tin mạng 2015 và Luật An ninh mạng 2018. Việc hợp nhất 2 luật này nhằm phù hợp với chức năng, nhiệm vụ mới của Bộ Công an về an ninh mạng; tạo ra một khuôn khổ pháp lý đồng bộ và rõ ràng hơn trong việc quản lý các vấn đề an ninh và an toàn mạng. Điều này sẽ giúp giảm thiểu sự chồng chéo trong các quy định, đồng thời nâng cao hiệu quả thực thi.

Luật An ninh mạng 2025 đã hợp nhất khung pháp lý, chuẩn hóa khái niệm, thẩm quyền, quy trình thiết lập, quản trị rủi ro theo chuẩn quốc tế, đồng thời, bảo đảm nguyên tắc cần thiết, tương xứng, minh bạch và bảo vệ quyền, lợi ích hợp pháp của tổ chức và cá nhân.

Ảnh minh hoạ

Theo đó, Luật quy định rõ Bộ Công an chịu trách nhiệm trước Chính phủ chủ trì, phối hợp thực hiện quản lý nhà nước về an ninh mạng. Bộ Quốc phòng chịu trách nhiệm quản lý hệ thống thông tin quân sự; Ban Cơ yếu Chính phủ quản lý hệ thống thông tin cơ yếu và mật mã. Quy định này nhằm giải quyết tình trạng chồng chéo, đảm bảo sự chỉ huy, điều phối thống nhất trong bối cảnh các mối đe dọa an ninh mạng mang tính toàn cầu.

Mở rộng phạm vi và đối tượng bảo vệ, Luật bổ sung quy định cụ thể về bảo vệ nhóm người yếu thế trên không gian mạng. Bên cạnh trẻ em, Luật mở rộng bảo vệ đối với người cao tuổi và người gặp khó khăn về nhận thức; quy định chi tiết về trách nhiệm của cơ quan, tổ chức, doanh nghiệp và gia đình trong việc ngăn chặn thông tin xâm hại, thiết lập công cụ kỹ thuật hỗ trợ và xử lý nghiêm các hành vi xâm hại trẻ em trên không gian mạng.

Việc kịp thời cập nhật, bổ sung các hành vi vi phạm trong luật đã khắc phục khoảng trống pháp lý, bảo vệ người dân và củng cố niềm tin vào môi trường của công nghệ số; là dấu mốc quan trọng trong hoàn thiện khuôn khổ pháp lý cho quản lý an ninh mạng, góp phần bảo vệ chủ quyền số, trật tự an toàn xã hội và lợi ích của người dân, doanh nghiệp trong môi trường mạng.

Về bảo đảm an ninh dữ liệu, Luật quy định cụ thể việc xây dựng chính sách, áp dụng biện pháp kỹ thuật, sử dụng mật mã và kiểm soát dữ liệu xuyên biên giới. Khái niệm "An ninh dữ liệu" cũng được định nghĩa rõ ràng, nhấn mạnh vào bảo đảm chất lượng và bảo vệ dữ liệu phục vụ phát triển kinh tế – xã hội.

Hệ thống thông tin được phân loại theo 5 cấp độ căn cứ vào mức độ tổn hại tới an ninh quốc gia, trật tự an toàn xã hội nếu bị sự cố. Quy định này giúp xác định trọng tâm bảo vệ và áp dụng các biện pháp quản lý tương xứng. Hiện nay, hầu hết các hệ thống thông tin của các cơ quan, tổ chức, doanh nghiệp đều có sự kết nối, liên thông để thực hiện công tác quản lý, cung cấp dịch vụ, giao dịch trực tuyến... Do vậy, khi một hệ thống thông tin bị tấn

công, chiếm quyền điều khiển thì không chỉ ảnh hưởng đến hệ thống thông tin của cơ quan, tổ chức, doanh nghiệp đó mà còn ảnh hưởng đến an ninh, an toàn của toàn bộ hệ thống thông tin trong phạm vi cả nước hoặc toàn cầu. Vì vậy, Luật nghiêm cấm hành vi tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng, tội phạm sử dụng công nghệ cao; Xâm nhập trái phép vào mạng viễn thông, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của người khác...

Một điểm mới quan trọng của Luật An ninh mạng 2025 là đã nội luật hóa các quy định tại Công ước của Liên hợp quốc về chống tội phạm mạng (Công ước Hà Nội, ký ngày 25/10/2025) mà Việt Nam là thành viên, tạo hành lang pháp lý cho việc chia sẻ thông tin, phối hợp điều tra và phòng chống tội phạm mạng xuyên biên giới.

Công ước Hà Nội, với tính ràng buộc pháp lý trên toàn cầu, đã ghi nhận mỗi quốc gia thành viên chỉ định một đầu mối liên lạc sẵn sàng 24/7 nhằm bảo đảm việc cung cấp sự hỗ trợ ngay lập tức cho các hoạt động điều tra, truy tố, xét xử hoặc cho việc thu thập chứng cứ là dữ liệu điện tử. Theo phân công, Bộ Công an là cơ quan đầu mối của Việt Nam có nhiệm vụ tổ chức thực hiện Công ước.

Luật An ninh mạng 2025 đã khẳng định vai trò tiên phong của Việt Nam trong hợp tác pháp lý đa phương của Liên hợp quốc, bảo vệ chủ quyền số dữ liệu quốc gia và xây dựng môi trường số an toàn, minh bạch vì con người và phát triển bền vững. Công ước Hà Nội là dấu mốc pháp lý toàn cầu trong quản trị an ninh mạng, phản ánh xu hướng gắn kết giữa an ninh phát triển và quyền con người. Việc nội hóa các quy định cốt lõi của công ước vào Luật An ninh mạng 2025 không chỉ giúp đảm bảo tương thích quốc tế mà còn tạo cơ sở để nước ta trở thành trung tâm khu vực về quản trị không gian mạng an toàn, tin cậy của nhân dân.

Luật An ninh mạng 2025 không chỉ đáp ứng yêu cầu cấp bách trong bảo vệ chủ quyền, an ninh quốc gia trên không gian mạng mà còn thể hiện tư duy quản trị hiện đại, hài hòa giữa bảo đảm an ninh và thúc đẩy phát triển. Với cách tiếp cận phù hợp chuẩn mực quốc tế, đề cao hợp tác, chia sẻ và trách nhiệm chung, đạo luật này được kỳ vọng sẽ trở thành nền tảng xây dựng môi trường số an toàn, củng cố lòng tin xã hội và tạo động lực mới cho tăng trưởng kinh tế số bền vững.

Luật An ninh mạng 2025 đã nội luật hóa các quy định tại Công ước của Liên hợp quốc về chống tội phạm mạng ký ngày 25/10/2025 mà Việt Nam là thành viên, tạo hành lang pháp lý cho việc chia sẻ thông tin, phối hợp điều tra và phòng chống tội phạm mạng xuyên biên giới

Công nghiệp an ninh mạng nền tảng tự chủ công nghệ và năng lực cạnh tranh quốc gia

Trung tướng, GS.TS Nguyễn Minh Đức

Phó Chủ nhiệm Uỷ ban Quốc phòng, An ninh và Đối ngoại của Quốc hội

An ninh mạng là nền tảng của kinh tế số

Trong bối cảnh thế giới bước vào giai đoạn chuyển đổi số sâu rộng, không gian mạng đã trở thành một không gian phát triển chiến lược gắn liền với an ninh quốc gia, ổn định xã hội và quan hệ quốc tế của mỗi quốc gia. Việc cộng đồng quốc tế thống nhất lựa chọn Hà Nội làm nơi mở ký Công ước của Liên Hợp quốc về chống tội phạm mạng (Công ước Hà Nội) trong hai ngày 25–26/10/2025 không chỉ là một sự kiện đối ngoại đa phương quan trọng, mà còn đánh dấu bước phát triển mới trong hợp tác toàn cầu nhằm ứng phó với các thách thức an ninh phi truyền thống ngày càng phức tạp.

Kinh tế số - động lực tăng trưởng quan trọng của Việt Nam

Kinh tế số là tổng thể các hoạt động kinh tế được hình thành, vận hành và phát triển dựa trên công nghệ số, dữ liệu số và không gian mạng, trong đó các yếu tố số trở thành đầu vào, phương tiện và động lực chủ yếu của quá trình tạo ra giá trị kinh tế. Theo cách tiếp cận hiện đại, kinh tế số không chỉ bao gồm các ngành công nghệ thông tin, truyền thông, mà còn bao trùm quá trình số hóa toàn diện các ngành, lĩnh vực của nền kinh tế - xã hội.

Công nghiệp an ninh mạng là tập hợp các hoạt động nghiên cứu, phát triển, sản xuất, cung cấp sản phẩm, dịch vụ và giải pháp kỹ thuật nhằm bảo đảm an ninh, an toàn cho không gian mạng, hệ thống thông tin, dữ liệu và hạ tầng số, phục vụ đồng thời mục tiêu phát triển kinh tế - xã hội và bảo đảm an ninh quốc gia. Theo cách tiếp cận hiện đại, công nghiệp an ninh mạng không chỉ là một lĩnh vực kỹ thuật, mà là một phân ngành công nghiệp công nghệ cao, có vai trò nền tảng trong hệ sinh thái công nghệ số và kinh tế số. Công nghiệp an ninh mạng là bộ phận cấu thành của kinh tế số, giữ vai trò nền tảng và điều kiện, bảo đảm sự an toàn, tin cậy và phát triển bền vững của toàn bộ hệ sinh thái kinh tế số.

Kinh tế số đang trở thành động lực tăng trưởng quan trọng của Việt Nam[1], hoạt động sản xuất, kinh doanh, cung cấp dịch vụ, quản trị xã hội và đời sống người dân ngày càng phụ thuộc sâu sắc vào hạ tầng số, dữ liệu và các nền tảng trực tuyến. Cùng với đó, các mối đe dọa an ninh mạng gia tăng cả về quy mô, cường độ và mức độ tinh vi, tác động trực tiếp đến ổn định kinh tế – xã hội, an ninh quốc gia và niềm tin của thị trường. Thực tiễn này đặt ra yêu cầu cấp thiết phải xây dựng một khuôn khổ pháp lý đầy đủ, thống nhất và phù hợp với sự phát triển của công nghệ số, vừa bảo đảm an ninh mạng, vừa tạo điều kiện cho kinh tế số phát triển bền vững. Luật An ninh mạng 2025 được ban hành trong bối cảnh đó, thể hiện tư duy tiếp cận mới của Đảng và Nhà nước Việt Nam coi an ninh mạng không chỉ là vấn đề bảo vệ, phòng ngừa rủi ro, mà còn là một yếu tố cấu thành của năng lực cạnh tranh quốc gia và động lực phát triển công nghiệp công nghệ cao.

Luật An ninh mạng là bước hoàn thiện quan trọng của hành lang pháp lý cho công nghiệp an ninh mạng trong bối cảnh phát triển kinh tế số

An ninh mạng và công nghiệp an ninh mạng không tồn tại tách rời, mà hình thành một mối quan hệ biện sinh, đặc biệt rõ nét trong bối cảnh kinh tế số. Trong nền kinh tế số, mối quan hệ giữa an ninh mạng và công nghiệp an ninh mạng không dừng lại ở quan hệ một chiều, mà diễn ra quá trình chuyển hóa lẫn nhau, cụ thể:

An ninh mạng là nền tảng của kinh tế số: Kinh tế số chỉ có thể phát triển khi môi trường mạng đủ an toàn, tin cậy; các giao dịch điện tử, thanh toán số, thương mại điện tử, dịch vụ công trực tuyến hay nền kinh tế dữ liệu đều phụ thuộc vào khả năng bảo đảm an ninh, an toàn thông tin. Một sự cố an ninh mạng nghiêm trọng có thể gây gián đoạn chuỗi cung ứng, làm tê liệt hoạt động doanh nghiệp và gây tổn thất lớn về kinh tế; do đó, an ninh mạng ngày càng được khẳng định như một loại "hạ tầng mềm" của nền kinh tế số, có vai trò tương tự hạ tầng giao thông hay năng lượng trong nền kinh tế truyền thống.

Công nghiệp an ninh mạng là

[1] *Báo cáo kết quả phát triển kinh tế - xã hội của Chính phủ nhiệm kỳ 2021-2025 tại Kỳ họp thứ 10, Quốc hội Khoá XV: Với giá trị đạt khoảng 72,1 tỷ USD (trong đó doanh thu ngành công nghiệp an ninh mạng đạt khoảng xấp xỉ 320–350 triệu USD vào năm 2025. Tỷ trọng giá trị tăng thêm của kinh tế số trong GDP liên tục tăng trong giai đoạn 2021-2025, từ 12,87% GDP năm 2021 lên 14,02% GDP năm 2025; đây là những nhóm ngành bao gồm: sản xuất sản phẩm điện tử, máy tính; viễn thông; lập trình máy tính và xử lý dữ liệu.*

Dịch vụ giám sát an ninh ATTT CMC SOC của công ty CMC Cyber Security

trụ cột mới của công nghiệp công nghệ cao: Đây là lĩnh vực có hàm lượng khoa học, công nghệ cao, tốc độ đổi mới nhanh và tính lưỡng dụng rõ nét, vừa phục vụ nhiệm vụ bảo vệ an ninh quốc gia vừa tham gia trực tiếp vào thị trường dân sự; việc phát triển công nghiệp an ninh mạng nội địa không chỉ giúp tăng cường năng lực tự chủ về công nghệ, mà còn mở ra một thị trường mới, tạo việc làm chất lượng cao và đóng góp tích cực cho tăng trưởng kinh tế số.

Luật An ninh mạng 2025 được xây dựng trên cơ sở tổng kết thực tiễn thi hành các quy định pháp luật về an toàn thông tin mạng, an ninh mạng trước đây và tiếp thu kinh nghiệm quốc tế, khẳng định vai trò của việc bảo đảm an ninh mạng như một yếu tố nền tảng trong kinh tế số, đặt mối quan hệ giữa an ninh mạng – công nghiệp an ninh mạng – kinh tế số vào hệ thống pháp luật, cụ thể:

Hoàn thiện khung pháp lý thống nhất về an ninh mạng: Luật quy định theo hướng toàn diện hơn, bao quát từ bảo vệ hệ thống thông tin quan trọng, bảo vệ dữ liệu, phòng ngừa và xử lý sự cố an ninh mạng, đến trách nhiệm của các chủ thể tham gia không gian mạng. Việc hình thành một đạo luật có tính thống nhất, rõ ràng và ổn định là điều kiện tiên quyết để các doanh nghiệp, đặc biệt là doanh nghiệp công nghệ và an ninh mạng có cơ sở pháp lý yên tâm đầu tư dài hạn.

Tạo lập nhu cầu và tiêu chuẩn cho thị trường an ninh mạng: Đây là nội dung quan trọng của Luật bằng việc xác lập các yêu cầu, tiêu chuẩn bắt buộc về bảo đảm an ninh mạng đối với nhiều loại hệ thống thông tin, nền tảng số và dịch vụ trực tuyến; các quy định này không chỉ mang tính quản lý nhà nước, mà còn tạo ra nhu cầu thị trường ổn định và lâu dài cho các sản phẩm, dịch vụ an ninh mạng. Chính nhu cầu đó là "đầu ra" quan trọng để thúc đẩy doanh nghiệp đầu tư nghiên cứu, phát triển và thương mại hóa các giải pháp an ninh mạng, qua đó hình thành và mở rộng ngành công nghiệp an ninh mạng trong nước.

Định hướng khuyến khích nghiên cứu, phát triển và sử dụng các sản phẩm, giải pháp an ninh mạng do doanh nghiệp trong nước làm chủ; đây là cơ sở pháp lý quan trọng để giảm dần sự phụ thuộc vào công nghệ nước ngoài, đồng thời nâng cao năng lực tự chủ, tự cường về an ninh mạng. Định hướng này phù hợp với chiến lược phát triển kinh tế số và công nghiệp công nghệ cao, trong đó an ninh mạng được coi là một lĩnh vực ưu tiên.

Vai trò, ý nghĩa đối với phát triển công nghiệp an ninh mạng và kinh tế số

Luật An ninh mạng 2025 với nhiều nội dung mới được bổ sung và sửa đổi, cùng với các luật khác có liên quan đóng vai trò quan trọng đối với công nghiệp an ninh mạng, tạo:

Cơ sở pháp lý cho hình thành hệ sinh thái công nghiệp an ninh mạng: Thông qua việc xác lập rõ các yêu cầu, tiêu chuẩn và cơ chế quản lý an ninh mạng, Luật An ninh mạng 2025 cùng với các quy định pháp luật có liên quan[2] góp phần hình thành một hệ sinh thái công nghiệp an ninh mạng bao gồm: cơ quan quản lý nhà nước, doanh nghiệp công nghệ, tổ chức nghiên cứu – đào tạo và người sử dụng. Sự gắn kết giữa các chủ thể này trên nền tảng pháp lý thống nhất sẽ tạo điều kiện thuận lợi để chuyển giao công nghệ, thương mại hóa kết quả nghiên cứu và nâng cao năng lực cạnh tranh của doanh nghiệp an ninh mạng Việt Nam.

Thúc đẩy đổi mới sáng tạo và làm chủ công nghệ lõi: Một ngành công nghiệp an ninh mạng phát triển không thể chỉ dựa vào nhập khẩu công nghệ, cùng với các chính sách và quy định của pháp luật liên quan, các quy định của Luật đã tạo cơ sở để Nhà nước ưu tiên đầu tư cho nghiên cứu, phát triển và đổi mới sáng tạo trong lĩnh vực an ninh mạng; việc làm chủ các công nghệ lõi như phát hiện tấn công, phân tích mã độc, bảo vệ dữ liệu, trí tuệ nhân tạo (AI) trong an ninh mạng sẽ quyết định năng lực cạnh tranh dài hạn của doanh nghiệp và của cả nền kinh tế số.

Phát triển nguồn nhân lực an ninh mạng chất lượng cao: Gián tiếp thúc đẩy phát triển nguồn nhân lực an ninh mạng thông qua việc mở rộng nhu cầu xã hội đối với các dịch vụ, giải pháp an ninh mạng; nguồn nhân lực chất lượng cao là yếu tố then chốt để công nghiệp an ninh mạng phát triển bền vững và có khả năng hội nhập quốc tế; công nghiệp an ninh mạng là lĩnh vực có cường độ tri thức cao, việc mở rộng thị trường an ninh mạng dưới tác động của Luật tạo động lực mạnh mẽ cho đổi mới sáng tạo, tất yếu kéo theo nhu cầu lớn về nguồn nhân lực chất lượng cao, sẽ có tác động tích cực đến toàn bộ hệ sinh thái khoa học, công nghệ và giáo dục, đào tạo.

Luật An ninh mạng 2025 có ý nghĩa kinh tế quan trọng đối với quá trình phát triển kinh tế số của Việt Nam, đó là:

Tăng cường niềm tin và an toàn cho thị trường số: Một môi trường pháp lý rõ ràng, minh bạch về an ninh mạng sẽ giúp doanh nghiệp và người dân yên tâm hơn khi tham gia các hoạt động kinh tế số; niềm tin số là yếu tố nền tảng để thương mại điện tử, tài chính số, dịch vụ công trực tuyến và kinh tế dữ liệu phát triển.

Giảm thiểu rủi ro và chi phí kinh tế do sự cố an ninh mạng: Các sự cố an ninh mạng gây ra thiệt hại kinh tế lớn, cả trực tiếp và gián tiếp; việc nâng cao mức độ an toàn, chủ động phòng ngừa và ứng phó sự cố thông qua khung pháp lý hiệu quả sẽ giúp giảm thiểu chi phí xã hội, bảo đảm sự ổn định của nền kinh tế số.

Hình thành ngành kinh tế mới có giá trị gia tăng cao: Công nghiệp an ninh mạng được bảo vệ bởi Luật An ninh mạng cùng với các luật có liên quan sẽ hỗ trợ trở thành một ngành kinh tế có giá trị gia tăng cao, đóng góp trực tiếp cho tăng trưởng GDP, tạo việc làm chất lượng cao và nâng cao vị thế của Việt Nam trong chuỗi giá trị công nghệ toàn cầu.

Một số vấn đề đặt ra và kiến nghị

Để Luật An ninh mạng 2025 thực sự phát huy vai trò là cơ sở pháp lý cho phát triển công nghiệp an ninh mạng và phát triển kinh tế số hiện nay và thời gian tới, cần chú trọng một số vấn đề sau:

Thứ nhất, các cơ quan chức năng, cần khẩn trương hoàn thiện các văn bản hướng dẫn thi hành, đặc biệt là các tiêu chuẩn, quy chuẩn kỹ thuật về an ninh mạng; cơ chế đánh giá, kiểm định, chứng nhận sản phẩm và dịch vụ an ninh mạng; cơ chế phối hợp giữa Nhà nước với doanh nghiệp, tổ chức nghiên cứu trong phát triển sản phẩm, dịch vụ an ninh mạng; trách nhiệm pháp lý của các chủ thể trong nền kinh tế số..

Thứ hai, triển khai đồng bộ các quy định của Luật với các chính sách phát triển công nghiệp an

2 Luật Công nghiệp quốc phòng, an ninh và động viên công nghiệp; Luật Công nghiệp công nghệ số; Luật Trí tuệ nhân tạo; Luật Công nghệ; Luật Dữ liệu;...gồm: sản xuất sản phẩm điện tử, máy tính; viễn thông; lập trình máy tính và xử lý dữ liệu.

ninh mạng, công nghiệp nghệ số với công nghiệp quốc phòng, an ninh; phát triển thị trường và hệ sinh thái công nghiệp an ninh mạng nhằm ưu tiên sử dụng sản phẩm, dịch vụ an ninh mạng trong nước; hình thành chuỗi giá trị công nghiệp an ninh mạng nội địa, từ nghiên cứu, sản xuất đến cung cấp dịch vụ; tạo thị trường đầu ra ổn định cho doanh nghiệp nghiên cứu, sản xuất công nghiệp an ninh mạng.

Thứ ba, cụ thể hoá chính sách nghiên cứu, phát triển và tự chủ công nghệ an ninh mạng, gắn với phát triển nguồn nhân lực an ninh mạng chất lượng cao; nâng cao nhận thức và tuân thủ pháp luật về an ninh mạng; tăng cường hợp tác quốc tế trong lĩnh vực an ninh mạng; tăng cường đầu tư cho nghiên cứu – phát triển (R&D) trong lĩnh vực an ninh mạng; thúc đẩy chuyển giao công nghệ và hợp tác đối tác công – tư; quy định rõ chính sách ưu đãi cụ thể về đầu tư, thuế, nghiên cứu – phát triển đối với doanh nghiệp an ninh mạng trong nước; doanh nghiệp làm chủ công nghệ lõi, sản phẩm chiến lược để phục vụ bảo đảm an ninh quốc gia, nâng cao giá trị gia tăng và vị thế của công nghiệp an ninh mạng trong nền kinh tế số.

Tóm lại, Luật An ninh mạng 2025 không chỉ là công cụ pháp lý bảo đảm an ninh, an toàn trên không gian mạng, mà còn là nền tảng quan trọng để xây dựng và phát triển ngành công nghiệp an ninh mạng ở Việt Nam; thông qua việc tạo lập hành lang pháp lý rõ ràng, ổn định và định hướng phát triển, Luật góp phần thúc đẩy chiến lược phát triển kinh tế số Việt Nam an toàn, bền vững, bảo đảm an ninh quốc gia và nâng cao năng lực cạnh tranh quốc gia trong kỷ nguyên số.

An ninh mạng phải là nền tảng trong công cuộc chuyển đổi số quốc gia

Bảo đảm an ninh mạng - Nền tảng phát triển bền vững của ngành ngân hàng trong kỷ nguyên mới

Phạm Tiến Dũng

Phó Thống đốc Ngân hàng Nhà nước Việt Nam, Phó Chủ tịch Hiệp hội An ninh mạng quốc gia

Trong bối cảnh nền kinh tế Việt Nam bước vào năm 2026 với những kỳ vọng tăng trưởng mới, ngành Ngân hàng tiếp tục khẳng định vai trò tiên phong trong chuyển đổi số quốc gia. Tuy nhiên, sự phát triển nhanh chóng của công nghệ cũng đặt ra những yêu cầu cấp thiết về bảo đảm an ninh mạng. Đối với ngành Ngân hàng, việc bảo đảm an ninh mạng, xây dựng "niềm tin số" là yếu tố then chốt để phát triển nhanh và bền vững.

Chuyển đổi số ngân hàng: Cơ hội lớn đi cùng bảo đảm an ninh mạng

Năm 2025 ghi nhận những kết quả nổi bật trong hoạt động chuyển đổi số của ngành Ngân hàng. Đến cuối năm 2025, hơn 87% người trưởng thành tại Việt Nam đã sở hữu tài khoản thanh toán; tại nhiều ngân hàng thương mại, tỷ lệ giao dịch trên kênh số đạt tới 90%, tỷ lệ các quyết định giải ngân khoản vay nhỏ lẻ, vay tiêu dùng được thực hiện theo hướng số hóa, tự động có thể đạt tới 42.7%. Cùng với đó, thanh toán không dùng tiền mặt tiếp tục tăng trưởng mạnh: so với năm 2024, năm 2025 tăng 42,21% về số lượng và 22,65% về giá trị, ước gấp khoảng 28 lần GDP. Đồng thời, các dịch vụ ngân hàng ngày càng được triển khai, tích hợp qua các nền tảng và tiện ích trực tuyến (như cho vay, tiền gửi, bảo lãnh...). Những con số này cho thấy, quá trình chuyển đổi số đã thực sự mang lại cho người dân, doanh nghiệp dịch vụ ngân hàng thuận tiện, an toàn và tin cậy.

Bên cạnh những thành tựu đạt được, ngành Ngân hàng đang phải đối mặt với các thách thức an ninh mạng ngày càng phức tạp và khó lường. Một mặt, gia tăng các hình thức tấn công có chủ đích nhằm xâm nhập hệ thống để chiếm đoạt dữ liệu và tài sản của tổ chức, đánh cắp dữ liệu khách hàng, chiếm quyền truy cập tài khoản/hệ thống, cài mã độc, mã hóa dữ liệu đòi tiền chuộc hoặc phá hoại hệ thống thông tin. Mặt khác, các hành vi lừa đảo trực tuyến nhắm vào khách hàng vẫn còn diễn ra với nhiều thủ đoạn tinh vi, phức tạp. Đặc biệt, sự phát triển nhanh của công nghệ trí tuệ nhân tạo (AI) và Deepfake đang tạo ra công cụ mới cho tội phạm, cho phép tội phạm giả mạo khuôn mặt, giọng nói để vượt qua các hàng rào xác thực sinh trắc học thông thường.

Quan điểm xuyên suốt của Ngân hàng Nhà nước trong giai đoạn vừa qua cũng như trong thời gian tới là lấy người dân, doanh nghiệp làm trung tâm và an toàn thông tin, an ninh mạng là yếu tố then chốt, xuyên suốt, không thể tách rời trong quá trình chuyển đổi số ngành Ngân hàng. Từ sản phẩm, phần mềm, hệ thống thông tin đến quy trình triển khai, tất cả đều phải bảo đảm an toàn, an ninh ngay từ giai đoạn thiết kế và trong suốt quá trình vận hành, nhằm bảo vệ lợi ích hợp pháp của khách hàng, đồng thời bảo đảm sự phát triển bền vững và hiệu quả 2 của toàn hệ thống ngân hàng Việt Nam. Ngành Ngân hàng đã triển khai đồng bộ các giải pháp từ hoàn thiện khuôn khổ pháp lý đến ứng dụng công nghệ nhằm bảo đảm an toàn hệ thống ngân hàng.

Về mặt pháp lý, hệ thống văn bản quy phạm pháp luật về an toàn, an ninh mạng trong hoạt động ngân hàng ngày càng được hoàn thiện, qua đó tạo cơ sở để ngành Ngân hàng chủ động ứng phó với các rủi ro mới, đặc biệt là xu hướng tấn công có chủ đích nhằm chiếm đoạt dữ liệu, tài sản hoặc phá hoại, gây gián đoạn các hệ thống thông tin. Trên cơ sở yêu cầu bảo đảm vận hành an toàn, liên tục đối với các hệ thống trọng yếu, NHNN đã ban hành và cập nhật các quy định về an toàn hệ thống thông tin trong ngành, trong đó nổi bật là các văn bản như Thông tư 09/2020/TT-NHNN, Thông tư 50/2024/TT-NHNN, Thông tư 77/2025/TT NHNN... nhằm chuẩn hóa yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ, yêu cầu an toàn, bảo mật khi cung cấp dịch vụ trực tuyến trong ngành Ngân hàng. Đồng thời, NHNN cũng đã ban hành, sửa đổi, bổ sung các Thông tư hướng dẫn Nghị định 52/2024/NĐ-CP về thanh toán không dùng tiền mặt. Trong đó, nổi bật là việc quy định bắt buộc khách hàng chỉ được rút tiền, thực hiện giao dịch thanh toán bằng phương tiện điện tử khi đã hoàn thành việc đối chiếu khớp đúng giấy tờ tùy thân và thông tin sinh trắc học; yêu cầu khớp đúng thông tin sinh trắc học khi thực hiện các giao dịch giá trị cao đã phát huy hiệu quả thực tế trong việc phòng chống gian lận, lừa đảo trực tuyến.

Về các giải pháp kỹ thuật, năm 2025 là giai đoạn tăng tốc củng cố chất lượng dữ liệu nhằm hạn chế gian lận giao dịch trên môi trường số. Ngành Ngân hàng đã phối hợp với Bộ Công an triển khai có hiệu quả Đề án 06 để làm sạch dữ liệu quy mô lớn. Tính đến cuối năm 2025, các tổ chức tín dụng, trung gian thanh toán đã hoàn thành đối chiếu sinh trắc học, làm sạch hơn 143 triệu hồ sơ khách hàng cá nhân và hơn 1,5 triệu hồ sơ khách hàng tổ chức thông qua CCCD gắn chip hoặc ứng dụng VNeID (tương đương trên 100% số lượng tài khoản phát sinh giao dịch trên kênh số). Ngân hàng Nhà nước đã đối soát khoảng 57 triệu hồ sơ khách hàng trong cơ

sở dữ liệu thông tin tín dụng quốc gia; đồng thời làm sạch toàn bộ 154 triệu tài khoản và 36 triệu hồ sơ khách hàng trong cơ sở dữ liệu phòng, chống rửa tiền, tài trợ phổ biến vũ khí hủy diệt hàng loạt. Bên cạnh đó, các tổ chức tín dụng cũng thực hiện triển khai các giải pháp rà soát, đối chiếu số điện thoại của khách hàng đăng ký sử dụng trong giao dịch điện tử để bảo đảm số điện thoại là chính chủ và khớp với thông tin chủ tài khoản. Việc chuẩn hóa dữ liệu không chỉ nâng chất lượng quản trị, mà còn trực tiếp góp phần loại bỏ tài khoản ảo, qua đó góp phần làm giảm hơn 59% số vụ việc lừa đảo trong thanh toán so với năm 2024, thu hẹp kẽ hở và tăng khả năng bảo vệ khách hàng.

Đặc biệt, trong năm 2025 NHNN đã đưa vào vận hành hệ thống thông tin hỗ trợ quản lý, giám sát và phòng ngừa rủi ro gian lận (SIMO), hệ thống đã trở thành công cụ đắc lực trong việc chia sẻ thông tin rủi ro giữa các tổ chức tín dụng. Đến 3 ngày 15/01/2026, hệ thống này đã kết nối 149 đơn vị, ghi nhận hơn 600.000 bản ghi tài khoản nghi ngờ, hỗ trợ cảnh báo cho hơn 2,68 triệu lượt khách hàng, trong đó có hơn 850 nghìn lượt khách hàng đã tạm dừng/hủy bỏ giao dịch sau khi nhận cảnh báo với tổng số tiền giao dịch tương ứng là hơn 3,29 nghìn tỷ đồng.

Ngành Ngân hàng cũng đã phối hợp với các cơ quan báo chí thực hiện hàng loạt các tin, bài, phóng sự truyền hình hoặc tổ chức các chương trình, sự kiện trong đó có nội dung phổ biến kiến thức, hướng dẫn người dân, doanh nghiệp hiểu rõ và sử dụng các sản phẩm, dịch vụ ngân hàng trên nền tảng số một cách an toàn, đúng quy định pháp luật; đồng thời tuyên truyền, nâng cao nhận thức, cảnh giác của người dân về những rủi ro an ninh, an toàn thông tin, các thủ đoạn, hành vi tội phạm, lừa đảo phổ biến mới xuất hiện liên quan đến hoạt động ngân hàng.

Bên cạnh đó, hàng năm, NHNN (Cục CNTT) đã phối hợp với Bộ Công an (Cục A05) tổ chức các đoàn kiểm tra chuyên đề công tác đảm bảo an ninh, an toàn thông tin để kịp thời chấn chỉnh, chỉ đạo các tổ chức tín dụng, trung gian thanh toán nâng cao công tác bảo đảm an ninh, an toàn thông tin.

Tổng thể, kết quả năm 2025 cho thấy "Niềm tin số" được hình thành không chỉ từ sự phát triển dịch vụ, mà từ nền tảng dữ liệu sạch hơn, cơ chế giám sát tốt hơn và công tác bảo đảm an toàn, an ninh mạng được tăng cường.

Hợp lực nhà nước - doanh nghiệp - người dân trong xây dựng niềm tin số

Để xây dựng một không gian mạng an toàn cho tài chính số, Ngân hàng Nhà nước xác định cần có sự hợp lực chặt chẽ giữa ba chủ thể: Nhà nước, Doanh nghiệp và Người dân.

Về phía Nhà nước, Ngân hàng Nhà nước tiếp tục thực hiện vai trò kiến tạo, duy trì hành lang pháp lý và cơ chế giám sát chặt chẽ trong công tác bảo đảm an ninh, an toàn thông tin ngành Ngân hàng. Ngoài ra, sự phối hợp giữa Ngân hàng Nhà nước, Bộ Công an, Hiệp hội An ninh mạng Quốc gia, các đơn vị, tổ chức có liên quan sẽ tiếp tục được đẩy mạnh để chia sẻ thông tin và ứng phó kịp thời sự cố xảy ra.

Đối với các tổ chức tín dụng và trung gian thanh toán, yêu cầu đặt ra là phải chuyển đổi tư duy từ phòng vệ thụ động sang chủ động dự báo ngăn chặn rủi ro; phân bổ nguồn lực tương xứng cho an ninh mạng, thúc đẩy ứng dụng công nghệ mới, đặc biệt là AI, để nâng cao năng lực phòng vệ. Các tổ chức tín dụng và trung gian thanh toán cũng cần chủ động thiết lập, duy trì cơ chế phối hợp thường xuyên, chặt chẽ với các đơn vị chuyên trách về an ninh mạng trong và ngoài ngành để hỗ trợ giám sát, điều tra và xử lý sự cố phát sinh (nếu có).

Về phía người dân, việc nâng cao nhận thức và kỹ năng an toàn thông tin là yếu tố không thể thiếu. "Niềm tin số" chỉ có thể bền vững khi được xây dựng trên nền tảng của sự hiểu biết và cảnh giác. Mỗi người dân khi tham gia vào hệ sinh thái số cần trang bị kiến thức để tự bảo vệ mình trước các thủ đoạn lừa đảo ngày càng tinh vi.

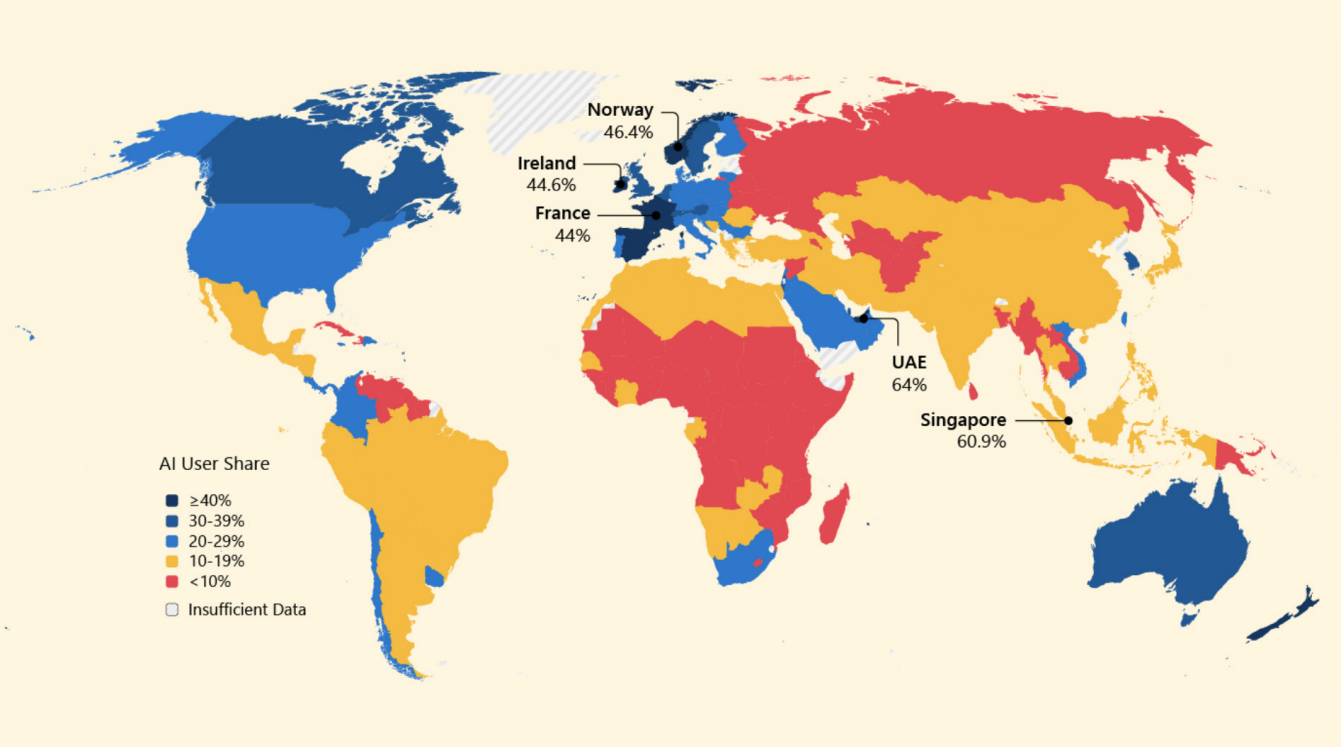
Bước sang năm 2026, với nền tảng hạ tầng công nghệ đang dần được củng cố và hành lang pháp lý ngày càng hoàn thiện, ngành Ngân hàng kiên định mục tiêu phát triển hệ sinh thái số an toàn, lành mạnh, góp phần vào sự thịnh vượng chung của nền kinh tế đất nước./.

An toàn tài chính số

AI và bài toán làm chủ công nghệ trong bảo vệ không gian mạng

Thái Hà

AI không phải là khái niệm mới trong lĩnh vực công nghệ. Nhưng phải đến cuối năm 2022 - thời điểm ứng dụng ChatGPT xuất hiện và nhanh chóng được phổ cập trên toàn cầu, AI mới thực sự trở thành một công cụ đại chúng và tác động trực tiếp đến đời sống xã hội. Chỉ sau quãng thời gian ngắn, các mô hình ngôn ngữ lớn (LLM) và AI tạo sinh (GenAI) đã cho thấy khả năng vượt trội trong việc viết văn bản, lập trình, phân tích dữ liệu, tạo hình ảnh, âm thanh và video với chất lượng ngày càng tiệm cận con người. Giờ đây, AI được tích hợp nhanh chóng vào các nền tảng email, công cụ tìm kiếm, mạng xã hội, hệ thống chăm sóc khách hàng, tài chính ngân hàng, y tế và cả các hạ tầng quan trọng. Tuy nhiên, AI đang mang lại cả cơ hội và rủi ro.



Biểu đồ ứng dụng AI của các quốc gia trên thế giới năm 2025 (nguồn_ Microsoft)

Tội phạm thời AI tinh vi hơn, nguy hiểm hơn

Đầu năm 2024, giới tài chính công nghệ toàn cầu từng choáng váng khi cảnh sát Hong Kong điều tra vụ công ty đa quốc gia ARUP bị lừa 25 triệu USD trong một giao dịch duy nhất do deepfake. Kẻ lừa đảo giả mạo "giám đốc tài chính" ARUP, liên lạc với nhân viên thủ quỹ từ trụ sở chính ở Anh để yêu cầu anh này tham gia một cuộc gọi video bàn bạc công việc. Khi nhân viên vào phòng họp trực tuyến, anh nhìn thấy các gương mặt đều là lãnh đạo công ty, bao gồm "giám đốc tài chính". Bởi vậy, khi được "giám đốc" lệnh chuyển tiền, người này lập tức làm theo. Hơn một năm trôi qua, khoản tiền khổng lồ nêu trên vẫn bặt vô âm tín. Mới đây, tháng 4/2025, cảnh sát Tây Ban Nha thông báo bắt giữ 6 người đứng sau một chiến dịch lừa đảo quy mô lớn sử dụng công nghệ deepfake để dụ nạn nhân đầu tư vào tiền ảo. Qua điều tra, hàng trăm nạn nhân trên toàn thế giới đã "sập bẫy" chiêu trò này, với tổng thiệt hại ước tính 21 triệu USD.

Nhưng đây chỉ là vài vụ việc bị cảnh sát các nước phát giác. Số liệu của deepstrike.io chỉ ra rằng, số lượng tệp tin dạng deepfake bị phát hiện đã tăng từ 500.000 (năm 2023) lên khoảng 8 triệu trong năm 2025. Không chỉ người dùng thông thường, deepfake còn được tội phạm sử dụng để nhắm mục tiêu tới nhân sự các công ty công nghệ hàng đầu. Theo Công ty bảo mật Eftsure có trụ sở ở Australia, năm 2024, nhân viên công ty an ninh mạng LastPass suýt bị lừa hàng triệu USD khi nhận cuộc gọi, tin nhắn và thư thoại từ một người mạo danh CEO trên ứng dụng nhắn tin WhatsApp. Khi kiểm tra lại, các chuyên gia an ninh mạng phát hiện kẻ tội phạm sử dụng hình ảnh của CEO thật được đăng tải trên Youtube để huấn luyện AI. Công ty bảo mật đám mây Wiz cũng từng đối mặt với một cuộc tấn công deepfake vào cuối năm 2024. Tội phạm lợi dụng AI sao chép giọng nói của CEO Assaf Rappaport và sau đó gửi tin nhắn thoại tới hàng chục nhân viên yêu cầu họ cung cấp thông tin đăng nhập.

Mức độ tự động hóa trong tội phạm mạng đang tăng nhanh. Theo công ty trí tuệ nhân tạo Anthropic, hoạt động này sử dụng hệ thống AI để điều hướng các chiến dịch tấn công mạng và tham gia vào nhiều khâu khác nhau của một cuộc tấn công. Trong một số vụ hack, AI thay con người "thực hiện 80-90%" lượng công việc. Báo cáo của Anthropic cũng cho biết, các nhóm tội phạm quy mô lớn, công ty tin tặc hoặc các thiết chế khác đang khai thác tiềm năng của AI, sử dụng công nghệ này để tự động hóa và tinh vi hóa các cuộc tấn công mạng, phát tán thông tin sai lệch mang tính kích động, cũng như xâm nhập các hệ thống nhạy cảm. Chẳng hạn, AI có thể biến những email lừa đảo viết vụng về thành tiếng Anh trôi chảy, hoặc tạo ra các bản sao kỹ thuật số, giả mạo thành viên cấp cao trong chính phủ để thực hiện hành vi lừa đảo.

Cũng có dấu hiệu AI bắt đầu được sử dụng trong các cuộc tấn công mạng nhắm vào một quốc gia đối thủ. Tháng 9/2025, Microsoft cảnh báo rằng, các đối thủ nước ngoài của Mỹ đang tận dụng AI để nâng cao hiệu quả các chiến dịch tấn công mạng, đồng thời giảm đáng kể công sức và chi phí triển khai các chiến dịch tấn công đó. Chủ tịch Ủy ban An toàn và An ninh của OpenAI, cơ quan có thẩm quyền giám sát và ngăn chặn những hướng phát triển AI rủi ro của nhà sản xuất ChatGPT, xác nhận các hệ thống AI mới giúp tin tặc "đạt những năng lực vượt trội hơn rất nhiều".

Ở quy mô nhỏ, sự phát triển của AI giúp các nhóm hacker nhỏ và hacker đơn độc khắc phục rào cản kỹ thuật (AI có thể giúp những kẻ "tay mơ" lập trình, soát lỗi lập trình hoặc tìm kiếm điểm yếu trong hệ thống mục tiêu), theo Adam Arellano, Giám đốc công nghệ hiện trường tại Harness, một công ty công nghệ sử dụng AI để giúp khách hàng tự động hóa quá trình phát triển phần mềm. "Tốc độ và khả năng tự động hóa mà trí tuệ nhân tạo mang lại là điều hơi đáng sợ. Thay vì một người có kỹ năng thành thạo cố gắng xâm nhập vào các hệ thống được bảo mật cao, AI đang đẩy nhanh các quy trình đó và vượt qua các trở ngại một cách nhất quán hơn", Arellano nói. Các chuyên gia cũng phát hiện các tên tội phạm can thiệp vào các hệ thống AI sẵn có để tạo ra mô hình AI chuyên sản xuất nội dung lừa đảo, giả mạo. Công ty an ninh mạng McAfee chỉ ra hai mô hình AI "khét tiếng" là WormGPT và FraudGPT.

AI trong vai trò tuyến phòng thủ mới của an ninh mạng

Trong khi AI bị kẻ xấu lợi dụng, đặc điểm nhanh, liên tục và chính xác của AI cũng mang đến một công cụ mạnh mẽ để chuyên gia an ninh mạng có thể sử dụng để chống lại những mối đe dọa an ninh mạng.

Trước hết, AI có thể phát hiện

và ngăn chặn phần mềm độc hại bằng cách liên tục phân tích các mẫu dữ liệu và hành vi bất thường, qua đó nhận diện sớm những mối đe dọa mới mà các giải pháp truyền thống dễ bỏ sót. Theo chuyên gia của McAfee và Eftsure, nhờ AI, các công cụ phân tích hành vi, học máy (ML) và học sâu (DL) có thể sàng lọc lượng lớn dữ liệu, nhận diện mẫu tấn công bất thường và phản ứng ngay lập tức. AI giúp giám sát liên tục, phân tích dấu hiệu nguy hiểm trong thời gian thực và đưa ra cảnh báo trước khi thiệt hại lớn xảy ra. Điều này làm giảm đáng kể thời gian phản ứng đối với sự cố, đồng thời hỗ trợ trong việc truy vết nguồn gốc tấn công và phục hồi hệ thống. Theo khảo sát an ninh mạng năm 2024 của KPMG, 66% các nhà lãnh đạo an ninh coi tự động hóa dựa trên AI là rất quan trọng để luôn đi trước các mối đe dọa mới và tăng cường sự linh hoạt cũng như khả năng phản ứng của các trung tâm điều hành an ninh của họ. Từ việc xác định các lỗ hổng đến ngăn chặn các cuộc tấn công mạng trong thời gian thực, AI có tiềm năng cách mạng hóa cách chúng ta bảo vệ các hệ thống trực tuyến. Reuters mới đây cho biết, nhiều công ty công nghệ lớn hay các nhà sản xuất dịch vụ diệt virus máy tính như McAfee đều đã ứng dụng AI để phát triển các sản phẩm mới, giúp vô hiệu hóa nhiều mối đe dọa.

Lợi ích tiếp theo của AI là nó không chỉ phản ứng với các mối đe dọa đã biết mà còn có thể dự đoán các chiến lược tấn công mới dựa trên dữ liệu quá khứ và hiện tại. Điều này giúp đội ngũ an ninh mạng chủ động xây dựng biện pháp phòng ngừa, từ đó giảm đáng kể thời gian phản ứng và thiệt hại. AI vượt trội rõ ràng so với con người trong việc sàng lọc lượng dữ liệu khổng lồ; có khả năng đọc, lọc và giám sát email; tự động phát hiện, cách ly các thư điện tử đáng ngờ, giúp giảm đáng kể nguy cơ lừa đảo. Các thuật toán AI liên tục giám sát nhật ký hệ thống và hành vi người dùng để phát hiện những sai lệch so với các chuẩn mực đã thiết lập. Chúng còn có thể xác định chính xác các hoạt động bất thường như các nỗ lực truy cập trái phép hoặc đánh cắp dữ liệu trong thời gian thực. Việc cảnh báo tức thì này cho phép các nhóm bảo mật điều tra và giảm thiểu các vi phạm tiềm tàng trước khi chúng leo thang.

Không dừng lại ở đó, AI cho phép phân tích tức thời các mối đe dọa bằng cách nhanh chóng phát hiện các mô hình và sai lệch trong lưu lượng mạng. Nhờ vậy, các tổ chức có thể hành động ngay lập

Bức ảnh được tạo bởi một công cụ AI khi được yêu cầu "mô tả tác động hai mặt của AI với vấn đề an ninh mạng"

tức nhằm hạn chế tác động của những cuộc tấn công có thể xảy ra. Khi sự cố an ninh phát sinh, AI có khả năng tự động hóa quy trình ứng phó. Bằng cách tự động hóa những tác vụ lặp đi lặp lại như giám sát nhật ký hay phân tích lưu lượng mạng, AI giúp giải phóng nguồn lực con người để tập trung vào các vấn đề an ninh phức tạp hơn, đòi hỏi con người trực tiếp giám sát, ra quyết định.

Theo các chuyên gia, một ưu điểm nổi bật khác là khả năng điều chỉnh (mở rộng, thu hẹp) hoạt động của hệ thống an ninh mạng gần như tức thời theo nhu cầu. Các giải pháp dựa trên AI có thể đáp ứng khối lượng công việc ngày càng tăng mà không đòi hỏi đầu tư lớn vào phần cứng hay nhân sự. Khi yêu cầu bảo mật của tổ chức gia tăng, hệ thống AI có thể dễ dàng thích ứng và phát triển tương ứng, mang lại giải pháp hiệu quả về chi phí cho mọi quy mô doanh nghiệp. Khả năng tích hợp linh hoạt với hạ tầng bảo mật sẵn có cũng giúp giảm thiểu gián đoạn và tối ưu hóa nguồn nhân lực, vật lực. Cuối cùng, AI đóng vai trò quan trọng trong bảo mật đám mây và thiết bị đầu cuối, giúp bảo vệ dữ liệu và hệ thống trước môi trường mối đe dọa ngày càng phức tạp.

Nhờ những ưu điểm đó, AI ngày càng được ứng dụng rộng rãi hơn trong lĩnh vực an ninh mạng. Khảo sát của hãng nghiên cứu thị trường IDC và công ty an ninh mạng Fortinet (Mỹ) được thực hiện với 550 lãnh đạo phụ trách công nghệ và an ninh mạng tại 11 thị trường châu Á - Thái Bình Dương, trong đó có Việt Nam, trong năm 2025 cho thấy, gần 90% doanh nghiệp lớn tại khu vực đã chủ động ứng dụng AI để bảo vệ hệ thống. Hầu hết ứng dụng AI trong môi trường an ninh để tự động hóa ứng phó, dự đoán mối đe dọa, chủ động ứng phó sự cố và phân tích hành vi. AI tạo sinh cũng dần được chấp nhận tại môi trường doanh nghiệp, chủ yếu là tác vụ nhẹ như vận hành kịch bản, cập nhật quy tắc và chính sách, phát hiện tấn công lừa đảo xã hội, viết quy tắc phát hiện và hỗ trợ điều tra...

Bài toán quản trị trong kỷ nguyên số

Từ những thuận lợi và thách thức đặt ra với an ninh mạng từ AI, nhiều chuyên gia đã liên tục nêu tính cấp thiết của việc xây dựng khuôn khổ đạo đức, pháp lý để quản lý và quản trị AI nhằm hạn chế tối đa những tác động tiêu cực, bảo vệ an toàn thông tin, giúp AI thực sự phát huy giá trị vì con người, vì sự phát triển an toàn. Ngay cả khi AI mang lại tiềm năng lớn trong việc tăng cường bảo vệ tài sản số, công nghệ này chỉ thực sự phát huy giá trị khi được triển khai có trách nhiệm, với cam kết mạnh mẽ trong bảo vệ quyền riêng tư, ngăn ngừa lạm dụng và hạn chế thiên lệch. Tổ chức Giáo dục, Khoa học và Văn hóa Liên hợp quốc (UNESCO) tin rằng, các chính phủ cần giải quyết không chỉ câu hỏi công nghệ có thể làm gì, mà cần tìm ra "AI nên làm gì?" và "Chúng ta nên sử dụng AI như thế nào để

mang lại lợi ích cho con người, chứ không gây tổn hại?".

Bài toán đặt ra với các nhà hoạch định chính sách an ninh mạng là cần chủ động đề ra những nguyên tắc cho việc triển khai AI một cách có trách nhiệm, bảo đảm các hệ thống được thiết kế và vận hành trên cơ sở tôn trọng quyền riêng tư, đề cao tính công bằng và minh bạch. Trong đó, yêu cầu then chốt là thiết lập các tiêu chuẩn rõ ràng về thu thập, lưu trữ và khai thác dữ liệu. Các tổ chức phải công khai dữ liệu nào được thu thập, mục đích thu thập và cách thức sử dụng, qua đó giúp cá nhân có thêm quyền kiểm soát đối với thông tin cá nhân của mình. Trách nhiệm giải trình là yếu tố không thể thiếu của bất kỳ khuôn khổ pháp lý hoặc đạo đức nào. Khi AI ngày càng có mức độ tự chủ cao hơn, việc xác định rõ ai chịu trách nhiệm đối với các quyết định do hệ thống AI đưa ra càng trở nên quan trọng. Điều này đòi hỏi phải tích hợp các cơ chế bảo đảm sự giám sát của con người, đồng thời khiến quá trình ra quyết định của AI trở nên minh bạch và có thể giải thích được.

Song song với đó, vai trò của khung pháp lý là yếu tố then chốt đảm bảo AI được sử dụng hợp pháp và hợp lý, với sự điều tiết và quản lý của Nhà nước. Các chính phủ và các tổ chức quốc tế theo đó cần tính toán xây dựng và thực thi những quy định điều chỉnh việc ứng dụng AI trong lĩnh vực an ninh, xác lập ranh giới rõ ràng đối với thu thập dữ liệu cá nhân, hoạt động giám sát và các thuật toán ra quyết định. Những quy định này cần hướng tới thúc đẩy tính minh bạch và công bằng, đồng thời vẫn tạo điều kiện để AI phát huy hiệu quả trong ứng phó với các mối đe dọa mạng phức tạp.

Hiện nhiều quốc gia, tổ chức quốc tế đã có những chính sách nhằm đưa AI vào triển khai có khuôn khổ và có trách nhiệm. Ở quy mô toàn cầu, năm 2024, Đại hội đồng Liên Hợp Quốc (LHQ) đã thông qua nghị quyết đầu tiên liên quan tới lĩnh vực AI với các điều khoản thúc đẩy các hệ thống AI hoạt động "an toàn, bảo mật và đáng tin cậy" nhằm mang lại lợi ích là sự phát triển bền vững cho tất cả mọi người. Trong văn kiện, Đại hội đồng đã nêu bật tầm quan trọng của việc tôn trọng, bảo vệ và thúc đẩy nhân quyền trong quá trình thiết kế, phát triển, triển khai và sử dụng AI, đồng thời kêu gọi tất cả các quốc gia thành viên và các bên liên quan "kiềm chế hoặc chấm dứt việc sử dụng các hệ thống AI không phù hợp với luật nhân quyền quốc tế hay gây ra những rủi ro quá mức đối với việc thực hành nhân quyền".

Tháng 6/2024, Liên minh châu Âu (EU) đã thông qua đạo Luật AI Act. Đây hiện là bộ luật đầu tiên và toàn diện nhất, có nhiều sáng kiến nhằm đối phó với nguy cơ từ AI. Điểm nhấn của Luật AI Act là việc nó dựa trên rủi ro của các mô hình AI để điều chỉnh luật pháp theo hướng tương ứng, cùng với đó là khung pháp lý thử nghiệm (sandbox) và cách tiếp cận 'mềm hóa' về đạo đức, độ tin cậy và tính trách nhiệm.

Tại Mỹ, chính quyền cựu Tổng thống Mỹ Joe Biden đã ban hành sắc lệnh hành pháp nhằm giảm thiểu những rủi ro mà công nghệ AI có thể gây ra, thiết lập các tiêu chuẩn mới về an toàn và bảo mật, bảo vệ quyền riêng tư của người dùng, thúc đẩy đổi mới và cạnh tranh trong lĩnh vực AI. Tháng 11/2025, Tổng thống Donald Trump ký sắc lệnh hành pháp nhằm thiết lập bộ tiêu chuẩn quản lý thống nhất ở cấp liên bang cho lĩnh vực AI.

Trung Quốc và Nhật Bản cũng là hai quốc gia có nhiều bước tiến trong việc phát triển AI có trách nhiệm. Năm 2019, Trung Quốc đã ban hành bốn nguyên tắc, tập trung vào người xây dựng mô hình, người sử dụng, quản trị AI và định hướng phát triển AI trong tương lai. Trung Quốc chọn cách vừa tự chủ phát triển AI, vừa đẩy mạnh quản trị trong nước, còn Nhật Bản hướng tới bộ quy tắc AI lấy con người làm trung tâm và vẫn đảm bảo tham gia được các diễn đàn quốc tế.

Nhìn từ những kinh nghiệm và cách tiếp cận khác nhau đó, có thể thấy không tồn tại một "khuôn mẫu" duy nhất cho mọi quốc gia trong quản trị AI, đặc biệt là trong lĩnh vực an ninh mạng, vốn thay đổi từng ngày, từng giờ. Điều quan trọng là mỗi nước cần chủ động nghiên cứu thực tiễn, tham khảo có chọn lọc các mô hình, khung pháp lý và chuẩn mực quốc tế, từ đó xây dựng chính sách phù hợp với trình độ phát triển, hệ sinh thái công nghệ và bối cảnh xã hội của mình. Quản trị AI không chỉ là bài toán kỹ thuật hay pháp lý, mà còn là lựa chọn mang tính chiến lược về cách đặt con người, quyền riêng tư và giá trị nhân văn ở vị trí trung tâm. Khi được định hướng và kiểm soát đúng đắn, AI sẽ thực sự phát huy vai trò như một công cụ giúp bảo đảm an ninh mạng, thúc đẩy đổi mới sáng tạo và phục vụ sự phát triển bền vững.

Lưu ký tài sản số và yêu cầu an ninh hạ tầng trong kinh tế số

Phan Đức Trung

Chủ tịch Hiệp hội Blockchain Việt Nam

Trong giai đoạn Việt Nam triển khai thí điểm thị trường tài sản mã hóa, "lưu ký" (custody) cần được nhìn nhận như một cấu phần an toàn - an ninh cốt lõi của hạ tầng tài chính số, thay vì chỉ là vấn đề kỹ thuật giữa ví nóng và ví lạnh. Thực tiễn từ Coinbase - sàn giao dịch tài sản mã hóa lớn nhất tại Mỹ với vốn hóa trên 60 tỷ USD - cho thấy rủi ro hiện đại không còn nằm ở thuật toán hay công nghệ lõi, mà chủ yếu phát sinh từ danh tính số, yếu tố con người và chuỗi cung ứng dịch vụ. Điều này đặt ra yêu cầu tiếp cận custody theo tư duy "chuỗi kiểm soát" (chain of control), thay vì chỉ tập trung vào lưu trữ khóa bí mật.

Bài học quản trị rủi ro từ Coinbase

Việt Nam đang từng bước xây dựng hành lang pháp lý thí điểm cho thị trường tài sản mã hóa. Trong bối cảnh đó, việc thiết kế tiêu chuẩn an toàn - an ninh cho mô hình sàn giao dịch tập trung (CEX) đòi hỏi phải mở rộng cách hiểu về custody.

Nếu trước đây, custody thường bị giản lược thành việc quản lý private key và lựa chọn giữa ví nóng - ví lạnh, thì thực tiễn tại các định chế lớn cho thấy rủi ro hiện đại hiếm khi đến từ việc phá vỡ thuật toán mật mã. Blockchain được thiết kế để khiến việc "bẻ khóa" gần như bất khả thi. Ngược lại, toàn bộ chuỗi vận hành xung quanh blockchain lại tồn tại nhiều điểm có thể bị thỏa hiệp: từ hành vi người dùng, sai sót thao tác, tấn công nội bộ đến khai thác đối tác thứ ba.

Nói cách khác, custody trong kỷ nguyên tài sản số không chỉ là giữ khóa, mà là kiến trúc quyền sở hữu và quyền kiểm soát, được bảo đảm đồng thời bởi công nghệ, quy trình quản trị và cơ chế pháp lý.

Sự cố tại Coinbase trong giai đoạn tháng 3 - 5/2021 - khi khoảng 6.000 khách hàng bị rút sạch tài sản là minh chứng điển hình. Thành lập năm 2012 tại San Francisco, Coinbase là doanh nghiệp đầu tiên trong lĩnh vực tài sản mã hóa niêm yết trực tiếp trên Nasdaq (mã COIN) vào tháng 4/2021, đồng thời đóng vai trò "kho tài sản số" cho nhiều tổ chức lớn. Vị thế này càng được củng cố khi SEC phê duyệt các quỹ ETF Bitcoin giao ngay đầu năm 2024, với Coinbase được lựa chọn làm đơn vị lưu ký cho nhiều nhà phát hành quỹ.

Chính vai trò trung tâm đó khiến Coinbase trở thành mục tiêu của các cuộc tấn công tinh vi nhất, đồng thời phơi bày một xu hướng rõ ràng: rủi ro dịch chuyển từ tấn công kỹ thuật sang tấn công quy trình.

Danh tính số - mắt xích yếu trong chuỗi kiểm soát

Các sự cố liên quan đến Coinbase cho thấy một khuôn mẫu nhất quán: kẻ tấn công không phá blockchain, mà tìm cách thỏa hiệp danh tính và quy trình xác thực. Nhiều trường hợp chiếm quyền tài khoản (account takeover) bắt nguồn từ lỗ hổng trong cơ chế khôi phục bằng SMS. Với người dùng cuối, tài khoản đăng nhập chính là ví. Khi xác thực yếu như SMS bị vượt qua bằng kỹ thuật SIM-swapping, hệ thống có thể mặc nhiên công nhận kẻ tấn công là chủ sở hữu hợp pháp.

Điều này khẳng định an ninh danh tính (identity security) là một phần không thể tách rời của custody. Các nền tảng muốn đạt mức bảo vệ cao buộc phải chấp nhận đánh đổi một phần trải nghiệm người dùng để triển khai xác thực mạnh hơn: từ phần cứng bảo mật, xác thực đa yếu tố nâng cao, đến các cơ chế kiểm soát hành vi như giới hạn rút tiền, thời gian chờ và "làm nguội" các thay đổi nhạy cảm.

Rủi ro nội bộ và yêu cầu kiến trúc zero trust

Ở chiều ngược lại, rủi ro không chỉ đến từ người dùng mà còn đến từ nội bộ. Tháng 2/2023, một nhóm tin tặc (được cho là liên quan đến nhóm 0ktapus) đã mở chiến dịch tấn công hàng loạt nhân viên Coinbase. Chúng gửi tin nhắn SMS mạo danh bộ phận IT yêu cầu nhân viên đăng nhập vào một đường link giả mạo để "nhận thông báo khẩn". Các chiến dịch phishing tinh vi nhắm vào nhân viên cho thấy tin tặc không cần phá lớp phòng vệ kỹ

Trong giai đoạn Việt Nam triển khai thí điểm thị trường tài sản mã hóa, "lưu ký" (custody) cần được nhìn nhận như một cấu phần an toàn - an ninh cốt lõi của hạ tầng tài chính số, thay vì chỉ là vấn đề kỹ thuật giữa ví nóng và ví lạnh

Danh tính số - mắt xích yếu trong chuỗi kiểm soát

thuật, mà chỉ cần khai thác sơ suất để chiếm thông tin xác thực truy cập.

Trong các mô hình custody hiện đại, việc kiểm soát quyền truy cập nội bộ quan trọng không kém gì cơ chế bảo vệ ví. Kẻ tấn công chỉ cần thỏa hiệp được một tài khoản nội bộ hoặc lợi dụng sai sót thao tác là có thể tiến sâu vào chuỗi hệ thống. Vì vậy, một mô hình custody trưởng thành phải được thiết kế theo nguyên tắc "zero trust" (không tin cậy mặc định), phân vùng hệ thống, áp dụng đặc quyền tối thiểu và cơ chế kiểm soát nhiều lớp để đảm bảo rằng ngay cả khi một tài khoản nội bộ bị xâm nhập, kẻ tấn công vẫn không thể chạm tới "lõi custody" - nơi sở hữu quyền ký hoặc kiểm soát luồng tài sản.

Chuỗi cung ứng - điểm mở rộng của rủi ro

Từ năm 2024 đến nay, bức tranh rủi ro tiếp tục mở rộng sang chuỗi cung ứng và dữ liệu KYC. Khi dữ liệu định danh bị rò rỉ từ nhà thầu phụ hoặc đối tác bên thứ ba, nó trở thành "nguyên liệu" cho các cuộc tấn công kỹ nghệ xã hội. Khi đó, sự cố không còn là câu chuyện của ví, mà là câu chuyện của dữ liệu, quy trình hỗ trợ khách hàng và quản trị đối tác.

Điểm chung của các rủi ro này là kẻ tấn công tìm cách phá vỡ chuỗi kiểm soát, thay vì tấn công trực tiếp khóa bí mật. Do đó, phòng thủ hiệu quả không nằm ở việc dựng thêm "tường kỹ thuật", mà ở thiết kế quy trình sao cho không một lỗi đơn lẻ nào có thể dẫn đến mất mát lớn.

Từ quản trị rủi ro đến yêu cầu an ninh hạ tầng

Trong bối cảnh Việt Nam, những bài học trên cần được đặt trong nền tảng chính sách mới. Luật Công nghiệp công nghệ số năm 2025 (hiệu lực từ 1/1/2026) đã xác định tài sản mã hóa là một loại tài sản số, được bảo hộ theo Bộ luật Dân sự 2015. Đây là bước then chốt, cho phép định danh, định giá và quy trách nhiệm ngay cả khi hệ thống văn bản dưới luật chưa hoàn thiện đầy đủ.

Cùng với đó, Quyết định 2815/QĐ-TTg xác định blockchain là công nghệ chiến lược ưu tiên triển khai. Thông điệp chính sách rất rõ: blockchain và custody không chỉ là dịch vụ fintech, mà là một phần của hạ tầng tài chính số quốc gia, cần được đầu tư, chuẩn hóa và bảo vệ như hạ tầng trọng yếu.

Trong khuôn khổ thí điểm theo Nghị quyết 05/

BÀI HỌC CHO VIỆT NAM TRONG GIAI ĐOẠN THÍ ĐIỂM

Việt Nam cần tiếp cận lưu ký như một cấu phần an toàn - an ninh của hạ tầng tài chính số.

Tiêu chuẩn lưu ký không nên chỉ dừng ở vốn lớn hay công nghệ mạnh, mà phải được thiết kế theo chuỗi kiểm soát toàn trình, để sai sót của con người không thể làm tổn hại đến lõi tài sản và niềm tin thị trường.

NQ-CP, yêu cầu vốn điều lệ lớn và tiêu chuẩn an toàn hệ thống thông tin cấp độ cao là cần thiết. Tuy nhiên, bài học từ Coinbase cho thấy các yêu cầu này chỉ thực sự có ý nghĩa khi được cụ thể hóa bằng chuỗi kiểm soát toàn trình: từ KYC, khôi phục tài khoản, kiểm soát nhân sự, quản trị đối tác thứ ba, đến giám sát liên tục và kiểm toán định kỳ.

Có thể nói, trong kỷ nguyên số, custody không còn là câu chuyện cất giữ khóa bí mật trong "két sắt". Custody là một bài toán quản trị rủi ro và an ninh hạ tầng, trả lời cho câu hỏi: ai được phép làm gì, trong điều kiện nào, qua bao nhiêu lớp phê duyệt và để lại dấu vết kiểm toán ra sao.

Một hệ thống an toàn không phải là hệ thống không có sai sót, mà là hệ thống đủ khả năng cô lập rủi ro, để sai sót của con người - dù là người dùng, nhân viên hay đối tác - không thể xâm phạm đến lõi tài sản. Sau cùng, thứ được lưu ký không chỉ là tài sản số, mà là niềm tin của thị trường đối với tính toàn vẹn của hạ tầng tài chính quốc gia.

Lưu ký tài số không đơn thuần là cất giữ

Bảo vệ dữ liệu cá nhân - nền tảng của niềm tin số và tự chủ công nghệ

Kim Jin - Wook

Ủy viên Ủy ban Bảo vệ Dữ liệu Cá nhân Hàn Quốc

Bảo vệ dữ liệu cá nhân là trụ cột của chuyển đổi số bền vững

Chuyển đổi số đang diễn ra với tốc độ và quy mô chưa từng có, trở thành xu thế tất yếu của mọi quốc gia trong thế kỷ XXI. Công nghệ số không chỉ làm thay đổi phương thức vận hành của nền kinh tế, mà còn tái định hình mô hình quản trị nhà nước và đời sống xã hội nói chung. Từ chính phủ điện tử, tài chính số, thương mại điện tử cho tới y tế và giáo dục thông minh, dữ liệu đã trở thành nền tảng trung tâm của mọi hoạt động phát triển.

Bảo vệ dữ liệu cá nhân – trụ cột của chuyển đổi số bền vững

Dữ liệu cá nhân ngày càng được thu thập, xử lý và khai thác với quy mô lớn, tần suất cao và mức độ phức tạp ngày càng gia tăng. Nếu thiếu vắng các cơ chế quản lý và bảo vệ phù hợp, dữ liệu cá nhân có thể trở thành nguồn rủi ro nghiêm trọng, dẫn đến xâm phạm quyền riêng tư, lạm dụng thông tin, gia tăng các hành vi gian lận, lừa đảo, đồng thời làm suy giảm niềm tin của người dân đối với môi trường số.

Vì vậy, bảo vệ dữ liệu cá nhân không còn là vấn đề mang tính lựa chọn hay bổ trợ, mà đã trở thành yêu cầu mang tính nền tảng, là điều kiện tiên quyết để chuyển đổi số được triển khai một cách bền vững, có trách nhiệm và lấy con người làm trung tâm.

Trong bối cảnh đó, việc Việt Nam ban hành Luật Bảo vệ Dữ liệu Cá nhân, đồng thời thành lập Ủy ban Bảo vệ Dữ liệu Cá nhân, mang ý nghĩa hết sức sâu sắc. Đây là bước đi kịp thời, thể hiện quyết tâm chính trị và cam kết pháp lý mạnh mẽ của Việt Nam trong việc bảo vệ quyền và lợi ích hợp pháp của người dân, cũng như trong việc xây dựng một môi trường số an toàn, minh bạch và đáng tin cậy trên hành trình phát triển kinh tế số.

Kinh nghiệm của Hàn Quốc trong việc hoàn thiện hệ thống bảo vệ dữ liệu cá nhân

Năm 2011, Hàn Quốc ban hành Luật Bảo vệ Dữ liệu Cá nhân trong bối cảnh xã hội thông tin và kinh tế số đang phát triển nhanh chóng. Tuy nhiên, thực tiễn cho thấy việc ban hành luật chỉ là điểm khởi đầu của một quá trình dài và phức tạp.

Trong hơn 10 năm qua, Hàn Quốc đã trải qua nhiều giai đoạn thử nghiệm, điều chỉnh và hoàn thiện

chính sách, song hành với sự phát triển nhanh chóng của công nghệ và mô hình kinh doanh số. Thông qua những va vấp và bài học thực tiễn, Hàn Quốc từng bước củng cố khung pháp lý, nâng cao năng lực quản lý và tăng cường hiệu quả thực thi.

Kết quả của quá trình này là việc hình thành một hệ thống bảo vệ dữ liệu cá nhân mang tính toàn diện, cân bằng hài hòa giữa bảo vệ quyền và lợi ích của cá nhân với việc thúc đẩy đổi mới, sáng tạo và phát triển kinh tế. Hiện nay, Hàn Quốc được cộng đồng quốc tế đánh giá là một trong những quốc gia có hệ thống bảo vệ dữ liệu cá nhân hoàn thiện và tiên tiến hàng đầu. Để đạt được điều này, phải đảm bảo các nguyên tắc sau:

Thứ nhất, khung nguyên tắc nền tảng và cơ sở pháp lý rõ ràng. Một trong những trụ cột quan trọng của hệ thống bảo vệ dữ liệu cá nhân tại Hàn Quốc là việc thiết lập một khung nguyên tắc pháp lý rõ ràng, nhất quán và có tính khả thi cao. Trọng tâm của khung này là bảo đảm quyền của chủ thể dữ liệu xuyên suốt toàn bộ vòng đời xử lý dữ liệu cá nhân, từ thu thập, sử dụng, lưu trữ, cung cấp cho bên thứ ba cho đến hủy bỏ dữ liệu.

Các quyền cơ bản của chủ thể dữ liệu, bao gồm quyền được thông báo, quyền đồng ý, quyền truy cập, quyền chỉnh sửa, quyền xóa và quyền phản đối việc xử lý dữ liệu, được xác định rõ ràng và bảo đảm bằng các cơ chế thực thi cụ thể. Song song với đó, vai trò và trách nhiệm của các tổ chức, doanh nghiệp cũng như của từng cá nhân trực tiếp tham gia xử lý dữ liệu được quy định một cách minh bạch.

Cách tiếp cận này góp phần hình thành văn hóa quản lý dữ liệu cá nhân dựa trên nguyên tắc trách nhiệm giải trình, minh bạch và tôn trọng quyền con người trong toàn xã hội.

Thứ hai, chuẩn hóa các biện pháp bảo vệ kỹ thuật và quản lý. Hàn Quốc đặc biệt chú trọng đến việc chuẩn hóa các biện pháp bảo vệ dữ liệu cá nhân về mặt kỹ thuật và quản lý. Các tiêu chuẩn này được cụ thể hóa thông qua các văn bản dưới luật và tài liệu hướng dẫn, nhằm hỗ trợ các tổ chức áp dụng một cách thống nhất và hiệu quả trong thực tiễn.

Các biện pháp bảo vệ cốt lõi bao gồm kiểm soát quyền truy cập, xác thực người dùng, mã hóa dữ liệu, phi định danh và ẩn danh hóa thông tin cá nhân. Trong số đó, việc ghi nhận và quản lý lịch sử xử lý dữ liệu cá nhân giữ vai trò đặc biệt quan trọng.

Việc ghi nhận đầy đủ và liên tục các hoạt động xử lý dữ liệu không chỉ cho phép phát hiện sớm các dấu hiệu bất thường, mà còn đóng vai trò là cơ sở khách quan để truy vết, điều tra và xác định trách nhiệm trong trường hợp xảy ra sự cố xâm phạm dữ liệu. Đồng thời, các bản ghi này cũng là công cụ quan trọng phục vụ công tác kiểm tra, đánh giá và chứng nhận mức độ tuân thủ

Bảo vệ dữ liệu cá nhân cùng nhau kiến tạo không gian an toàn và đáng tin cậy

Ảnh minh hoạ

của tổ chức.

Thứ ba, củng cố hệ thống quản lý nội bộ và trách nhiệm tổ chức. Hàn Quốc cũng đặc biệt nhấn mạnh vai trò của quản trị nội bộ trong bảo vệ dữ liệu cá nhân. Việc bắt buộc chỉ định người phụ trách bảo vệ dữ liệu cá nhân (CPO) giúp xác lập rõ ràng trách nhiệm, thẩm quyền và vai trò điều phối trong tổ chức.

Bên cạnh đó, cơ chế Đánh giá Tác động Bảo vệ Dữ liệu Cá nhân được áp dụng đối với các hệ thống hoặc dịch vụ mới có nguy cơ cao, nhằm nhận diện và kiểm soát rủi ro ngay từ giai đoạn thiết kế. Cách tiếp cận mang tính phòng ngừa này giúp giảm thiểu rủi ro và nâng cao mức độ an toàn của hệ thống ngay từ đầu.

Thứ tư, cơ chế kiểm chứng và nâng cao mức độ tuân thủ. Hàn Quốc triển khai đồng thời các cơ chế kiểm chứng đối với cả khu vực công và khu vực tư nhân. Các cơ quan nhà nước được đánh giá định kỳ, trong khi doanh nghiệp có thể tham gia các chương trình chứng nhận về quản lý an toàn thông tin và bảo vệ dữ liệu cá nhân.

Những cơ chế này không chỉ nhằm mục tiêu giám sát tuân thủ pháp luật, mà còn khuyến khích các tổ chức liên tục cải thiện năng lực quản lý, qua đó nâng cao mức độ trưởng thành của toàn bộ hệ sinh thái bảo vệ dữ liệu cá nhân.

Thứ năm, thực thi pháp luật hiệu quả, cân bằng và có trách nhiệm. Một hệ thống pháp luật chỉ thực sự phát huy giá trị khi được thực thi một cách hiệu quả. Hàn Quốc đã từng bước hoàn thiện cơ chế xử phạt và chế tài theo hướng hợp lý, bảo đảm tính răn đe, công bằng và tương xứng với mức độ vi phạm. Đồng thời, các chính sách hỗ trợ, tư vấn và hướng dẫn cũng được triển khai song song, nhằm giúp các tổ chức nâng cao năng lực tuân thủ trên cơ sở tự nguyện và bền vững.

Cùng nhau kiến tạo tương lai số an toàn và đáng tin cậy

Những kinh nghiệm mà Hàn Quốc tích lũy trong hơn một thập kỷ qua có thể trở thành nguồn tham khảo hữu ích cho Việt Nam trong quá trình xây dựng và hoàn thiện hệ thống bảo vệ dữ liệu cá nhân. Việt Nam hoàn toàn có thể rút ngắn lộ trình phát triển bằng cách tiếp thu có chọn lọc những bài học phù hợp với điều kiện thực tiễn của mình.

Trên tinh thần đó, chúng tôi mong muốn thúc đẩy hợp tác chặt chẽ với Việt Nam trong việc chia sẻ mô hình, cơ chế và kinh nghiệm, từ xây dựng chính sách, triển khai biện pháp bảo vệ kỹ thuật, phát triển hệ thống quản lý cho đến đào tạo nguồn nhân lực chuyên sâu. Bảo vệ dữ liệu cá nhân không chỉ là vấn đề pháp lý hay chế tài, mà còn là nền tảng quan trọng để xây dựng niềm tin số, thu hút đầu tư và tham gia sâu rộng hơn vào nền kinh tế số toàn cầu.

Trong kỷ nguyên số, với sự hợp tác và tin cậy lẫn nhau, Hàn Quốc và Việt Nam hoàn toàn có thể cùng nhau kiến tạo một tương lai số an toàn, minh bạch và bền vững, đồng thời đóng góp tích cực vào việc nâng cao chuẩn mực bảo vệ dữ liệu cá nhân trong khu vực châu Á.

An ninh mạng trong kỷ nguyên AI: Khi đổi mới phải đi đôi với năng lực phục hồi

Eugene Kaspersky

Thế giới đang bước vào một giai đoạn mang tính bước ngoặt, là thời điểm mà sự bùng nổ của công nghệ và các yêu cầu về an ninh mạng đang trực tiếp đối chọi nhau. AI từng chỉ được giới hạn trong các nghiên cứu học thuật và trí tưởng tượng về tương lai, nay đã trở thành động cơ quan trọng nhằm thúc đẩy đổi mới sáng tạo trên toàn cầu. Trong các lĩnh vực từ y tế, sản xuất đến tài chính, logistic, AI đang tái định nghĩa phương thức vận hành của các tổ chức thông qua việc thúc đẩy hiệu quả, đẩy nhanh chu kỳ đổi mới và tạo ra những lợi thế cạnh tranh mới.

Tại Việt Nam, từ việc phát hiện gian lận trong lĩnh vực fintech đang tăng trưởng nóng cho đến hệ thống logistic thông minh tại các cảng biển và sân bay, AI đang tái cấu trúc cách các doanh nghiệp vận hành, cạnh tranh và mở rộng quy mô. Tuy nhiên, tương tự các công nghệ đột phá khác, AI cũng tiềm ẩn nhiều rủi ro không lường trước được. Sức mạnh ngày càng lớn của công nghệ này không chỉ mang lại lợi ích cho các doanh nghiệp, tổ chức mà còn đang tiếp tay cho cả tội phạm mạng.

Chúng ta đang chứng kiến sự gia tăng mạnh mẽ về cả quy mô lẫn tốc độ tấn công của tội phạm mạng khi chúng tận dụng công nghệ AI. Đáng chú ý, những công cụ và kỹ thuật vốn đòi hỏi trình độ chuyên môn cao thì nay đang trở nên phổ biến, dễ tiếp cận với ngay cả những kẻ không chuyên hoặc ít kinh nghiệm. Các chiến dịch lừa đảo ngày càng trở nên tinh vi và thuyết phục hơn, công nghệ deepfake ngày càng chân thực, trong khi các mô hình cung cấp mã độc tống tiền dưới dạng dịch vụ (RaaS) lại không ngừng mở rộng. Những diễn biến này không chỉ đặt ra mối đe dọa trực tiếp đối với các doanh nghiệp tư nhân, mà còn ảnh hưởng đến an ninh quốc gia, sự ổn định kinh tế và niềm tin vào hệ sinh thái kỹ thuật số.

Trong một báo cáo gần đây về các rủi ro liên quan đến AI, gần 50% số người tham gia khảo sát nhận định rằng phần lớn các cuộc tấn công nhắm vào tổ chức của họ trong năm qua đều có sự can thiệp của AI. Tại Việt Nam, thực trạng này đặc biệt đáng báo động: hơn 50% doanh nghiệp và tổ chức cho biết đã đối mặt với các mối đe dọa mạng được hỗ trợ bởi AI trong cùng kỳ. Trong đó, hơn một nửa nhận thấy quy mô đe dọa tăng gấp đôi, thậm chí 30% số đơn vị ghi nhận mức tăng gấp ba lần. Những hình thức tấn công này không chỉ khó phát hiện hơn mà còn triệt để khai thác các kẽ hở trong khâu giám sát, khung quản trị cũng như quy trình vận hành nội bộ.

Ba trụ cột an ninh mạng trong kỷ nguyên AI: Công nghệ - Quy trình - Con người

Việc ứng dụng AI vào mục đích phòng thủ cũng đang gia tăng mạnh mẽ. Tại Việt Nam, có tới hơn 80% tổ chức đã đưa AI vào vận hành trong hệ thống an ninh mạng. Tuy nhiên, tốc độ triển khai thần tốc này không phải lúc nào cũng đi đôi với các biện pháp quản trị rủi ro tương xứng. Một nghiên cứu mới đây chỉ ra rằng, trong khi 66% tổ chức coi AI là yếu tố "thay đổi

Sự bùng nổ của trí tuệ nhân tạo (AI) đang mở ra những cơ hội chưa từng có cho đổi mới sáng tạo và tăng trưởng kinh tế. Tuy nhiên, song hành với đó là làn sóng tấn công mạng ngày càng tinh vi, khi AI không chỉ trở thành công cụ phòng thủ mà còn bị lợi dụng để gia tăng sức mạnh cho tội phạm mạng. Trong bối cảnh ấy, bài toán cân bằng giữa đổi mới và an toàn đang đặt ra thách thức lớn cho doanh nghiệp, tổ chức và cả các nhà hoạch định chính sách.

cuộc chơi" lớn nhất về an ninh mạng năm nay, thì một thực tế đáng báo động là chỉ có khoảng 1/3 trong số đó thực hiện các bước đánh giá công cụ AI trước khi sử dụng. Sự mất kết nối giữa tốc độ áp dụng và nhận thức rủi ro chính là rào cản lớn đối với an ninh mạng hiện nay, đòi hỏi vai trò điều phối then chốt từ phía chính phủ để tháo gỡ.

Sự giao thoa giữa các công nghệ mới nổi, tình trạng bất ổn địa chính trị, những lỗ hổng trong chuỗi cung ứng cùng sự thiếu hụt nhân lực an ninh mạng trình độ cao đang khiến bối cảnh đe dọa mạng trở nên phức tạp và biến động hơn bao giờ hết. Đối với các nhà lãnh đạo công nghệ, thách thức chưa bao giờ lớn như hiện nay. Họ phải đối mặt với bài toán khó: vừa phải nắm bắt đổi mới sáng tạo để duy trì lợi thế cạnh tranh, vừa phải chủ động ứng phó với những hiểm họa không ngừng biến chuyển. Đây là sự cân bằng đầy thách thức, đòi hỏi một chiến lược vừa có tính chủ động, vừa có khả năng phục hồi nhanh chóng. Để vượt qua giai đoạn này, các tổ chức cần kiện toàn hệ thống an ninh mạng dựa trên ba trụ cột cốt lõi: công nghệ, quy trình và con người.

Khi các đối tượng tấn công không ngừng cải tiến phương thức, năng lực phòng thủ cũng cần phát triển tương ứng để kịp thời ứng phó. Xét về khía cạnh công nghệ, việc đầu tư vào các giải pháp bảo mật tiên tiến là yếu tố then chốt để phát hiện sớm các nguy cơ, giúp doanh nghiệp có thêm thời gian xử lý trước khi tổn thất xảy ra. Bên cạnh đó, các công cụ tự động hóa đóng vai trò quan trọng trong việc xử lý các tác vụ lặp đi lặp lại, giúp đội ngũ chuyên gia an ninh tập trung nguồn lực vào những sự cố trọng yếu có mức độ ưu tiên cao hơn. Việc tiếp cận kịp thời các báo cáo tình báo về mối đe dọa cũng quan trọng không kém, qua đó cung cấp cái nhìn sâu sắc về các phương thức tấn công mới cũng như chiến thuật và quy trình của tin tặc. Ngoài ra, khả năng giám sát theo thời gian thực

AI - động lực đổi mới vừa là "chất xúc tác" cho các mối đe dọa mạng

Ông Eugene Kaspersky là một chuyên gia an ninh mạng hàng đầu thế giới và là người sáng lập kiêm Giám đốc điều hành (CEO) của Kaspersky Lab - công ty bảo mật thông tin toàn cầu nổi tiếng với các giải pháp chống phần mềm độc hại và bảo vệ người dùng trên Internet.

đối với hành vi của kẻ tấn công sẽ cho phép đưa ra các quyết định ứng phó nhanh chóng và chính xác hơn.

Tuy nhiên, ngay cả những công nghệ tiên tiến nhất cũng không thể phát huy hiệu quả nếu thiếu đi những nền tảng vận hành vững chắc. Việc thiết lập các quy trình bảo mật rõ ràng cũng như việc thực hiện chúng một cách thuần thục là yếu tố then chốt. Nếu thiếu đi các quy tắc bảo mật được xây dựng bài bản và kiểm tra thường xuyên, các tổ chức rất dễ rơi vào tình trạng lúng túng và phản ứng chậm trễ khi đối mặt với các sự cố nghiêm trọng. Dù là đối phó với mã độc tống tiền, các mối đe dọa nội bộ hay tấn công chuỗi cung ứng, các đội ngũ vận hành vẫn luôn cần những quy trình thực thi cụ thể để định hướng quyết định ngay cả dưới áp lực lớn. Các quy trình chặt chẽ sẽ giúp giảm thiểu sự xáo trộn trong các thời điểm khủng hoảng, đẩy nhanh tốc độ ứng phó và duy trì sự hoạt động liên tục của doanh nghiệp.

Yếu tố con người vẫn đóng vai trò then chốt không thể thay thế. Ngay cả trong kỷ nguyên AI, đội ngũ chuyên gia lành nghề vẫn là nền tảng và trụ cột của mọi hệ thống phòng thủ hiệu quả. Vì vậy, việc chú trọng đào tạo, nâng cấp kỹ năng và giữ chân nhân lực ngành an ninh mạng phải được đặt lên hàng đầu. Đây cũng chính là cầu nối để các nhà hoạch định chính sách, doanh nghiệp và giới học thuật đẩy mạnh hợp tác.

Các giải pháp AI mang tính đột phá cần được đón nhận một cách tự tin nhưng cũng đầy thận trọng. Dù những tiến bộ đạt được là không thể phủ nhận, song AI vẫn chưa thực sự tạo ra những bước nhảy vọt để thay đổi hoàn toàn các quy tắc vận hành cốt lõi của lĩnh vực an ninh mạng. Tuy nhiên, việc bám sát các diễn biến không ngừng của công nghệ này đóng vai trò hết sức quan trọng, bởi những bước tiến xa hơn trong tương lai có thể tạo ra những tác động vô cùng sâu rộng. Song song đó, việc đẩy mạnh hợp tác quốc tế nhằm chia sẻ thông tin, kết quả nghiên cứu và dữ liệu tình báo về các rủi ro bảo mật liên quan đến AI là một yêu cầu cấp thiết. Nỗ lực này cũng đồng thời hỗ trợ các sáng kiến nâng cao năng lực, cung cấp cho các chính phủ và doanh nghiệp những kiến thức cùng công cụ cần thiết để triển khai các hệ thống AI một cách an toàn.

Bên cạnh đó, chính sách an ninh mạng cần phải phát triển song hành cùng với sự chuyển dịch của công nghệ. Mặc dù đổi mới sáng tạo phần lớn được dẫn dắt bởi khu vực tư nhân, chính phủ lại giữ một vị thế đặc biệt để thiết lập các điều kiện cho việc áp dụng công nghệ một cách an toàn và có trách nhiệm. Bằng cách định hình các khung quản trị AI và điều chỉnh các quy định quốc gia phù hợp với tiêu chuẩn toàn cầu, chính phủ nên hợp tác với nhau và với các bên liên quan để tránh tình trạng chính sách bị chia cắt giữa các quốc gia, đồng thời bảo vệ các quyền con người cơ bản.

Sau cùng, cả các cơ quan chính phủ và các tổ chức tư nhân đều cần xây dựng những chiến lược có tầm nhìn xa và khả năng ứng phó linh hoạt, những chiến lược vừa khuyến khích đổi mới, vừa tăng cường hợp tác đa ngành, nhằm đảm bảo rằng khi các hệ thống kỹ thuật số trở nên thông minh hơn, chúng cũng phải trở nên an toàn hơn.

Nguồn nhân lực an toàn, an ninh thông tin - trụ cột của tự chủ công nghệ

TS. Hoàng Đức Thọ

Chủ nhiệm Khoa An toàn thông tin- Học viện Kỹ thuật mật mã

Thế giới đang chứng kiến một bước chuyển mang tính bản lề với sự trỗi dậy mạnh mẽ của Trí tuệ nhân tạo (AI). Không chỉ là một công nghệ mới, AI đang trở thành lực lượng sản xuất quan trọng, làm thay đổi căn bản phương thức vận hành của nền kinh tế - xã hội toàn cầu, đồng thời tái định hình cục diện an toàn, an ninh thông tin.

Trong bối cảnh đó, Nghị quyết số 57-NQ/TW của Bộ Chính trị về "Đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia" đã đặt ra yêu cầu có tính chiến lược đối với hệ thống giáo dục đại học: đào tạo nguồn nhân lực chất lượng cao, có khả năng làm chủ công nghệ lõi, bảo đảm an ninh, an toàn cho quốc gia trên không gian số.

Tuy nhiên, thực tiễn cho thấy mô hình đào tạo nguồn nhân lực an toàn, an ninh thông tin (ATANTT) theo cách tiếp cận truyền thống đang bộc lộ những giới hạn rõ rệt, chưa theo kịp sự biến đổi nhanh chóng, đa chiều và khó lường của môi trường an ninh mạng trong kỷ nguyên AI. Điều này đặt ra yêu cầu cấp thiết phải đổi mới tư duy và chiến lược đào tạo một cách căn cơ.

AI và môi trường an ninh mạng: "Con dao hai lưỡi"

Những năm gần đây, môi trường an ninh mạng đã chuyển từ trạng thái ổn định tương đối sang trạng thái biến động sâu sắc về chất. AI đóng vai trò như một "con dao hai lưỡi", vừa mở ra năng lực phòng thủ vượt trội, vừa tạo ra các mối đe dọa phi truyền thống.

Ở chiều tích cực, AI trở thành nền tảng của an ninh mạng chủ động và thông minh. Với khả năng xử lý dữ liệu lớn và nhận diện các mẫu hành vi phức tạp, AI và Học máy đang cách mạng hóa phương thức phòng thủ: phát hiện sớm hành vi bất thường, tự động hóa ứng phó sự cố, phân tích mã độc thế hệ mới với tốc độ và quy mô vượt xa khả năng con người. Trong bối cảnh đó, người làm ATANTT không còn chỉ là người vận hành hệ thống, mà phải trở thành nhà phân tích, kiến trúc sư và giám sát các hệ thống thông minh.

Ngược lại, chính sức mạnh của AI cũng làm gia tăng rủi ro. Các cuộc tấn công được hỗ trợ bởi AI đang trở

nên tinh vi hơn, từ tự động dò quét lỗ hổng đến tạo mã độc thích nghi. Đặc biệt, sự bùng nổ của AI tạo sinh đã khiến các hình thức lừa đảo, giả mạo lãnh đạo, xuyên tạc chính sách bằng deepfake ngày càng khó nhận diện, đe dọa trực tiếp đến niềm tin xã hội và an ninh tư tưởng.

Nguy hiểm hơn, các hệ thống AI - nhất là trong những lĩnh vực hạ tầng trọng yếu như tài chính, y tế, giao thông thông minh - đã trở thành đối tượng tấn công. Các kỹ thuật như đầu độc dữ liệu hay tấn công mẫu đối kháng có thể khiến hệ thống AI đưa ra quyết định sai lệch, gây hậu quả nghiêm trọng.

Trong khi đó, tình trạng thiếu hụt nhân lực an ninh mạng vẫn là bài toán toàn cầu. Trong kỷ nguyên AI, thách thức không chỉ nằm ở số lượng, mà còn ở chất lượng nhân lực đó là cần những người vừa vững nền tảng ATANTT, vừa hiểu dữ liệu, mô hình AI, triển khai hệ thống và có tư duy quản trị rủi ro, tuân thủ.

Khoảng trống trong đào tạo và yêu cầu tái cấu trúc tư duy

Thực tiễn đào tạo tại nhiều cơ sở giáo dục đại học hiện nay cho thấy một "độ trễ" đáng kể so với yêu cầu thực tiễn. Phần lớn chương trình đào tạo vẫn tách biệt giữa ATANTT và khoa học dữ liệu/AI. Sinh viên ATANTT thường thiếu kiến thức nền về AI để đối phó với các mối đe dọa thông minh; trong khi kỹ sư AI lại chú trọng hiệu suất mô hình mà chưa coi trọng đầy đủ các nguyên tắc bảo mật.

Sự "lệch pha" này khiến người học thiếu một lăng kính tích hợp để nhìn nhận AI vừa là công cụ phòng thủ, vừa là đối tượng cần bảo vệ, đồng thời cũng có thể là vũ khí của đối phương. Đây chính là lỗ hổng lớn trong năng lực của nguồn nhân lực ATANTT tương lai.

Mô hình đào tạo tích hợp - thực chiến - liên ngành

Để khắc phục những hạn chế trên, các cơ sở giáo dục đại học cần chuyển dịch từ mô hình đào tạo đơn ngành sang mô hình tích hợp - thực chiến - sáng tạo, dựa trên ba trụ cột chính.

Thứ nhất, tái cấu trúc chương trình theo tư duy "an ninh tích hợp". AI cần được xem là thành tố nền tảng trong cấu trúc kiến thức ATANTT, không chỉ là môn học bổ trợ. Chương trình cần tích hợp các nội dung như an ninh cho học máy,

bảo mật mô hình AI, mật mã học trong kỷ nguyên AI, giúp người học phát triển tư duy song hành: sử dụng AI để phòng thủ và bảo vệ chính các hệ thống AI.

Thứ hai, chuyển đổi phương pháp đào tạo từ hàn lâm sang thực chiến. Cần đầu tư xây dựng các thao trường mạng thế hệ mới, mô phỏng các kịch bản tấn công - phòng thủ phức tạp với sự tham gia của AI. Sinh viên phải được rèn luyện trong môi trường đối kháng, áp lực cao, qua đó hình thành tư duy phản biện và khả năng ra quyết định chính xác. Đồng thời, tăng cường hợp tác nhà trường - doanh nghiệp để đưa các bài toán thực tiễn vào giảng dạy, rút ngắn khoảng cách giữa đào tạo và nhu cầu thị trường.

Thứ ba, giáo dục đạo đức nghề nghiệp và trách nhiệm xã hội. Trong kỷ nguyên số, khi ranh giới giữa sáng tạo và lạm dụng công nghệ ngày càng mong manh, yếu tố con người trở thành chốt chặn cuối cùng. Giáo dục ATANTT không chỉ đào tạo kỹ năng, mà còn phải định hình nhân cách, bản lĩnh chính trị, ý thức pháp luật và trách nhiệm xã hội cho người học, đặc biệt trong các vấn đề đạo đức AI và an ninh mạng.

Sứ mệnh kiến tạo tương lai

An toàn, an ninh thông tin trong kỷ nguyên AI không còn là vấn đề thuần kỹ thuật, mà đã trở thành trụ cột của kinh tế số và chủ quyền quốc gia. Định hướng chiến lược đã được Đảng và Nhà nước xác lập, vấn đề còn lại là cụ thể hóa thành hành động đào tạo thực chất.

Chúng ta không đào tạo con người để cạnh tranh với máy móc, mà để làm chủ và dẫn dắt công nghệ. Mục tiêu là xây dựng đội ngũ nhân lực ATANTT có tư duy khoa học sắc bén, phẩm chất đạo đức vững vàng và khả năng ứng phó với các thách thức phi truyền thống.

Điều đó đòi hỏi sự quyết tâm đổi mới từ chính các cơ sở đào tạo, cùng với mạng lưới hợp tác chặt chẽ giữa nhà trường - doanh nghiệp - hiệp hội nghề nghiệp. Chỉ khi đó, Việt Nam mới có thể từng bước hiện thực hóa chiến lược tự chủ công nghệ, bảo đảm an ninh, an toàn trên không gian số và biến thách thức của kỷ nguyên AI thành cơ hội bứt phá.

NCA - HỢP LỰC VÌ NIỀM TIN SỐ QUỐC GIA

★ 1. Kiến tạo niềm tin số - hành trình trách nhiệm của Hiệp hội An ninh mạng quốc gia trong kỷ nguyên vươn mình

★ 2. Phương Nam kết nối - kiến tạo an ninh số Việt Nam

★ 3. Hiệp hội An ninh mạng Quốc gia và chiến lược xây dựng "lá chắn" bảo vệ người dùng trên không gian mạng

★ 4. Sinh viên an ninh mạng và sứ mệnh bảo vệ Chủ quyền số quốc gia

★ 5. Chiến dịch "Không một mình" từ cảnh báo rủi ro số đến tái thiết năng lực bảo vệ trẻ em của xã hội

Kiến tạo niềm tin số - hành trình trách nhiệm của Hiệp hội An ninh mạng quốc gia trong kỷ nguyên vươn mình

Vũ Duy Hiền

Phó Tổng thư ký, Chánh văn phòng Hiệp hội An ninh mạng quốc gia

Đại tướng Lương Tam Quang

Ủy viên Bộ Chính trị, Bộ trưởng Bộ Công an, Chủ tịch Hiệp hội An ninh mạng quốc gia chỉ đạo Sơ kết hoạt động 6 tháng đầu năm 2025 và ra mắt Chi hội phía Nam của Hiệp hội An ninh mạng quốc gia

Năm 2025 khép lại trong bối cảnh không gian mạng ngày càng trở thành không gian sống, không gian kinh tế và không gian lợi ích thiết yếu của quốc gia. Chuyển đổi số diễn ra sâu rộng mang lại nhiều cơ hội phát triển, nhưng đồng thời cũng đặt ra những thách thức mới, phức tạp và đa chiều về an ninh mạng, an toàn thông tin và bảo vệ con người trên môi trường số. Trong bối cảnh đó, trách nhiệm của các tổ chức xã hội - nghề nghiệp hoạt động trong lĩnh vực an ninh mạng trở nên rõ nét và nặng nề hơn bao giờ hết.

Ông Vũ Duy Hiền - Phó Tổng thư ký Chánh Văn phòng Hiệp hội An ninh mạng Quốc gia

Đối với Hiệp hội An ninh mạng quốc gia, năm 2025 không chỉ là một năm gia tăng về quy mô và mật độ hoạt động, mà quan trọng hơn, là giai đoạn chuyển tiếp mang tính bản lề: từ quá trình định hình tổ chức sang khẳng định vai trò bằng hành động cụ thể, có chiều sâu và tạo tác động lan tỏa trong xã hội. Trên hành trình đó, Hiệp hội kiên trì theo đuổi một mục tiêu xuyên suốt: góp phần kiến tạo niềm tin số cho quốc gia trong kỷ nguyên vươn mình của dân tộc.

Trong toàn bộ tiến trình này, Hiệp hội An ninh mạng quốc gia không đặt mình vào vai trò cơ quan quản lý nhà nước, cũng không thay thế doanh nghiệp hay cộng đồng, mà xác định rõ vị trí là không gian kết nối trung gian. Đó là nơi các chủ trương, chính sách của Nhà nước được đối thoại với thực tiễn triển khai; nơi doanh nghiệp được hỗ trợ để hiểu, tuân thủ và từng bước nâng cao năng lực phòng vệ; đồng thời là cầu nối để người dân tiếp cận tri thức, công cụ và kỹ năng tự bảo vệ mình trong không gian số. Chính vai trò trung gian này giúp các nỗ lực bảo đảm an ninh mạng không dừng lại ở quy định hay khẩu hiệu, mà từng bước đi vào đời sống xã hội một cách thực chất và bền vững.

Tham gia Lễ mở ký Công ước Hà Nội - trách nhiệm quốc gia trong không gian mạng toàn cầu

Một trong những dấu ấn nổi bật của năm 2025 là việc Hiệp hội An ninh mạng quốc gia tham gia trực tiếp công tác chuẩn bị và phối hợp tổ chức Lễ mở ký Công ước của Liên Hợp Quốc về phòng, chống tội phạm mạng (Công ước Hà Nội) dưới sự chủ trì của Chủ tịch nước Lương Cường, sự tham dự của Tổng Thư ký Liên hợp quốc và Nguyên thủ, Lãnh đạo Chính phủ, lãnh đạo bộ, ngành của 119 quốc gia thành viên Liên hợp quốc. Việc 72 quốc gia ký Công ước ngay tại Lễ mở ký (đến nay có 74 nước đã ký Công ước) cho thấy sự hưởng ứng rộng rãi và niềm tin của cộng đồng quốc tế đối với khuôn khổ pháp lý mới này. Việc Công ước được mở ký tại Hà Nội không chỉ mang ý nghĩa đối ngoại, mà còn phản ánh sự tin cậy của cộng đồng quốc tế đối với vai trò và trách nhiệm của Việt Nam trong lĩnh vực an ninh phi truyền thống.

Trong tiến trình đó, Hiệp hội tham gia với tinh thần đồng hành và hỗ trợ chuyên môn, phát huy vai trò kết nối giữa các cơ quan quản lý, cộng đồng chuyên gia, doanh nghiệp công nghệ và các tổ chức liên quan trong và ngoài nước. Cách tiếp cận của Hiệp hội không đặt trọng tâm vào hình thức, mà hướng tới việc làm rõ nội hàm, ý nghĩa và tác động lâu dài của Công ước đối với công tác phòng, chống tội phạm mạng trong nước, cũng như chuẩn bị các điều kiện cần thiết cho giai đoạn thực thi.

Trước thời điểm Lễ mở ký, Cuộc thi "Sinh viên với Công ước Hà Nội" được triển khai như một hoạt động hưởng ứng có tính định hướng rõ nét. Thông qua cách tiếp cận mềm, gần gũi với sinh viên, các nội dung pháp lý và tinh thần hợp tác quốc tế được "dịch" sang ngôn ngữ dễ tiếp cận, giúp thế hệ trẻ hình thành nhận thức sớm về trách nhiệm quốc gia trong không gian mạng. Đây cũng là cách Hiệp hội góp phần chuẩn bị nguồn lực con

người cho quá trình thực thi Công ước một cách lâu dài và bền vững.

Ngay sau Lễ mở ký, Hiệp hội kịp thời chuyển trọng tâm sang giai đoạn "hậu cam kết", tập trung hỗ trợ việc đưa các chuẩn mực quốc tế vào thực tiễn thông qua tọa đàm, diễn đàn chính sách, hoạt động đào tạo và truyền thông. Các hoạt động này nhận được sự quan tâm và tham gia ngày càng tích cực của đội ngũ chuyên gia, nhà quản lý và doanh nghiệp, cho thấy nhu cầu đối thoại chính sách và chia sẻ kinh nghiệm thực tiễn trong lĩnh vực an ninh mạng đang ngày càng rõ nét.

Tham mưu chính sách - khi an ninh mạng trở thành mối quan tâm chung của xã hội

Song hành với vai trò đối ngoại, năm 2025 tiếp tục đặt ra cho Hiệp hội yêu cầu phải tham gia sâu hơn vào quá trình tham mưu chính sách và nâng cao nhận thức xã hội về an ninh mạng. Trên thực tế, nhiều rủi ro trên không gian mạng không xuất phát từ lỗ hổng kỹ thuật thuần túy, mà từ khoảng trống nhận thức, quy trình vận hành và thói quen sử dụng công nghệ thiếu an toàn.

Với nhận thức đó, Hiệp hội đã tổ chức chuỗi hội thảo, tọa đàm chuyên đề tập trung vào những vấn đề sát với đời sống số của người dân và doanh nghiệp, như phòng, chống lừa đảo trực tuyến; bảo vệ dữ liệu cá nhân; mức độ trưởng thành an ninh mạng của doanh nghiệp; tiêu chuẩn, quy chuẩn kỹ thuật; cũng như góp ý hoàn thiện các dự thảo luật quan trọng chuẩn bị có hiệu lực trong giai đoạn tới.

Điểm đáng chú ý là các diễn đàn này thu hút sự quan tâm ngày càng rộng rãi của đội ngũ chuyên gia, nhà quản lý, doanh nghiệp công nghệ và các cơ quan báo chí. Nhiều ý kiến trao đổi không chỉ dừng ở phân tích học thuật, mà phản ánh trực tiếp những khó khăn, vướng mắc trong công tác quản lý, vận hành và bảo vệ hệ thống thông tin. Chính sự tham gia đa chiều này cho thấy an ninh mạng đang dần trở thành mối quan tâm chung của xã hội, đồng thời khẳng định vai trò của Hiệp hội như một diễn đàn trung gian tin cậy - nơi các góc nhìn khác nhau có thể gặp nhau, đối thoại và cùng tìm kiếm giải pháp phù hợp với bối cảnh Việt Nam.

Ngày 15/07/2025, Hiệp hội An ninh mạng quốc gia chính thức ra mắt Tạp chí An ninh mạng Việt Nam - cơ quan ngôn luận của Hiệp hội

Ngày 08/12 tại TPHCM, Hiệp hội An ninh mạng quốc gia (NCA) tổ chức Lễ ra mắt Chi hội phía nam và triển khai kế hoạch công tác năm 2026.

Các khảo sát quy mô lớn do Hiệp hội An ninh mạng quốc gia thực hiện trong năm 2025 đã cung cấp những dữ liệu thực tiễn quan trọng cho thảo luận chính sách. Khảo sát trên hơn 5.000 cơ quan, tổ chức và doanh nghiệp cho thấy, các hệ thống thông tin tại Việt Nam phải đối mặt với khoảng hơn 550.000 cuộc tấn công mạng mỗi năm. Đáng chú ý, trên 52% đơn vị ghi nhận từng chịu thiệt hại do tấn công mạng, phản ánh mức độ rủi ro ngày càng hiện hữu đối với hoạt động sản xuất, kinh doanh và cung cấp dịch vụ số.

Khảo sát cũng cho thấy những chuyển biến tích cực về nhận thức và đầu tư phòng vệ: khoảng 75% cơ quan, doanh nghiệp đã tổ chức đào tạo nâng cao nhận thức an ninh mạng; trên 50% đơn vị triển khai diễn tập ứng phó sự cố hoặc vận hành trung tâm giám sát an ninh mạng (SOC); và hơn 76% có cơ chế sao lưu dữ liệu dự phòng. Tuy nhiên, gần 48% tổ chức, doanh nghiệp vẫn thiếu hụt nhân lực an ninh mạng chuyên trách, cho thấy khoảng trống đáng kể giữa yêu cầu bảo vệ hệ thống và năng lực thực tế.

Những con số này không chỉ phản ánh thực trạng, mà còn là cơ sở quan trọng để cảnh báo sớm rủi ro hệ thống, đồng thời định hướng các giải pháp chính sách, kỹ thuật và nguồn lực phù hợp, gắn với yêu cầu phát triển kinh tế số, xã hội số an toàn và bền vững.

Bảo vệ con người - khi cộng đồng trở thành chủ thể của niềm tin số

Lấy con người làm trung tâm là định hướng xuyên suốt trong hoạt động của Hiệp hội An ninh mạng quốc gia. Năm 2025, định hướng này được thể hiện rõ qua các chiến dịch cộng đồng hướng tới bảo vệ những nhóm dễ bị tổn thương trên không gian mạng, đặc biệt là trẻ em và thanh thiếu niên.

Các chương trình như "Không Một Mình", "Ngày hội An toàn trực tuyến" đã nhận được sự quan tâm và đồng hành tích cực của báo chí, nhà trường, phụ huynh và đông đảo người dân. Nhiều phản hồi từ cộng đồng cho thấy nhu cầu tiếp cận kiến thức an toàn số là rất thực tế và cấp thiết. Chính sự tham gia và phản hồi này giúp Hiệp hội điều chỉnh thông

điệp, cách tiếp cận và công cụ hỗ trợ theo hướng gần gũi, dễ hiểu hơn, qua đó nâng cao hiệu quả lan tỏa và tính bền vững của các hoạt động bảo vệ con người trên không gian mạng.

Việc ra mắt phần mềm phòng, chống lừa đảo nTrust là một bước đi cụ thể nhằm chuyển vai trò bảo vệ an ninh mạng từ "bị động" sang "chủ động". Thông qua cơ chế cộng đồng cùng tham gia cảnh báo, người dân không chỉ là đối tượng thụ hưởng, mà trở thành một phần của mạng lưới phòng vệ xã hội, góp phần hình thành "lá chắn nhận thức" – tuyến phòng thủ bền vững nhất trong không gian số.

Từ kết nối sang thực chiến - củng cố năng lực phòng vệ

Trong bối cảnh các cuộc tấn công mạng ngày càng tinh vi, có chủ đích và hướng vào các hệ thống thông tin quan trọng, Hiệp hội sớm xác định yêu cầu phải nâng cao năng lực phòng vệ theo hướng thực chất, lấy khả năng ứng phó thực tế làm thước đo hiệu quả.

Việc phối hợp với Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05) tham gia tổ chức Diễn tập An ninh mạng Quốc gia, ra mắt Liên minh ứng phó, khắc phục sự cố an ninh mạng quốc gia và triển khai mô hình Red Team - Blue Team trên hệ thống thật đã thể hiện rõ bước chuyển từ kết nối, trao đổi sang hỗ trợ thực chiến. Thông qua các kịch bản tấn công giả định, các đơn vị tham gia có điều kiện rà soát năng lực, quy trình phối hợp và mức độ sẵn sàng ứng phó trong điều kiện gần với thực tế.

Các hoạt động thực chiến này không chỉ giúp phát hiện lỗ hổng kỹ thuật, mà còn làm rõ vai trò, trách nhiệm và cơ chế phối hợp giữa cơ quan quản lý, doanh nghiệp và đội ngũ chuyên gia. Qua đó, năng lực phòng vệ của hệ thống từng bước được củng cố, góp phần nâng cao niềm tin của xã hội vào khả năng bảo đảm an ninh mạng trong bối cảnh chuyển đổi số.

Làm chủ truyền thông - mở rộng không gian trách nhiệm xã hội

Năm 2025 đánh dấu bước hoàn thiện quan trọng về hạ tầng truyền thông chuyên ngành của Hiệp hội An ninh mạng quốc gia với việc ra mắt Tạp chí An ninh mạng Việt Nam, cơ quan ngôn luận của Hiệp hội. Trong bối cảnh an ninh mạng ngày càng trở thành vấn đề công chúng, việc hình thành một kênh thông tin chính thống, chuyên sâu và có trách nhiệm là yêu cầu tất yếu, nhằm bảo đảm việc cung cấp thông tin kịp thời, chính xác và có chiều sâu cho xã hội.

Thông qua Tạp chí, Hiệp hội chủ động tổ chức và dẫn dắt không gian thông tin chuyên ngành, tập trung phản ánh các vấn đề thực tiễn, cảnh báo sớm rủi ro và phân tích chính sách theo hướng khoa học, cân bằng và thận trọng. Tạp chí An ninh mạng Việt

Gian triển lãm của Hiệp hội An ninh mạng quốc gia tại triển lãm quốc tế trong khuôn khổ Lễ mở ký Công ước của Liên hợp quốc về chống tội phạm mạng (Công ước Hà Nội)

Nam đã từng bước trở thành kênh thông tin chuyên ngành tin cậy, góp phần kết nối chuyên môn an ninh mạng với báo chí và công chúng, qua đó hỗ trợ hiệu quả cho công tác truyền thông chính sách và nâng cao nhận thức xã hội.

Trên nền tảng đó, sự phối hợp, đồng hành của các cơ quan báo chí trung ương, địa phương và đội ngũ nhà báo đã góp phần mở rộng phạm vi lan tỏa thông tin, đưa các vấn đề an ninh mạng đến gần hơn với người dân, doanh nghiệp và các chủ thể trong nền kinh tế số. Cách tiếp cận này cho thấy, bên cạnh năng lực chuyên môn, việc làm chủ và sử dụng có trách nhiệm không gian truyền thông là một cấu phần quan trọng trong nỗ lực kiến tạo niềm tin số quốc gia.

Mở rộng không gian trách nhiệm - bám sát thực tiễn phát triển

Cuối năm 2025, việc ra mắt Chi hội phía Nam

tại TP.HCM đánh dấu bước phát triển quan trọng trong quá trình mở rộng không gian hoạt động của Hiệp hội. Đây là khu vực tập trung nhiều doanh nghiệp công nghệ, startup, hạ tầng số và dữ liệu, đồng thời cũng là nơi các rủi ro và thách thức an ninh mạng phát sinh sớm và đa dạng.

Sự hiện diện của Chi hội phía Nam giúp Hiệp hội tiếp cận sát hơn với thực tiễn thị trường, kịp thời nắm bắt nhu cầu của doanh nghiệp và địa phương, từ đó triển khai linh hoạt hơn các hoạt động hỗ trợ, đào tạo, kết nối chuyên gia và nâng cao năng lực phòng vệ. Ở bình diện rộng hơn, Chi hội đóng vai trò cầu nối giữa định hướng chính sách và yêu cầu thực tiễn, góp phần rút ngắn khoảng cách giữa chiến lược và triển khai.

Hướng tới năm 2026 - hành động để niềm tin số được củng cố

Bước sang năm 2026, trên nền tảng những kết quả đã đạt được, Hiệp hội An ninh mạng quốc gia xác định rõ yêu cầu chuyển trọng tâm từ khẳng định vai trò sang tạo ra tác động thực chất, lấy niềm tin số làm thước đo xuyên suốt. Đồng hành thực thi Công ước Hà Nội, nâng cao năng lực phòng vệ theo hướng thực chiến, phát triển nguồn nhân lực, mở rộng hệ sinh thái công - tư và tăng cường hiệu quả truyền thông chính sách là những định hướng trọng tâm.

Sự quan tâm và đồng hành ngày càng rộng rãi của đội ngũ chuyên gia, nhà quản lý, báo chí và người dân chính là điều kiện quan trọng để Hiệp hội tiếp tục phát huy vai trò kết nối, đưa các nỗ lực bảo đảm an ninh mạng đi vào chiều sâu và bền vững. Trên hành trình đó, Hiệp hội An ninh mạng quốc gia tiếp tục đồng hành cùng Nhà nước, doanh nghiệp và xã hội, góp phần xây dựng một Việt Nam số an toàn, tự tin và phát triển bền vững trong kỷ nguyên vươn mình của dân tộc.

Tại Lễ mở ký Công ước của Liên hợp quốc về chống tội phạm mạng, Hiệp hội An ninh mạng Quốc gia (NCA) đã có buổi làm việc với Tổ chức Japan Anti-Abuse Working Group (JPAAWG), một trong những tổ chức tiên phong của Nhật Bản trong lĩnh vực phòng chống lạm dụng trực tuyến và bảo đảm an ninh mạng toàn cầu.

Phương Nam kết nối - kiến tạo an ninh số Việt Nam

Thiếu tướng, Tiến sĩ Lê Minh Mạnh

Chi hội trưởng Chi hội phía Nam Hiệp hội An ninh mạng quốc gia

Thiếu tướng Lê Minh Mạnh - Chi hội trưởng Chi hội phía Nam - Hiệp hội An ninh mạng Quốc gia

Ngày 8/12/2025, Hiệp hội An ninh mạng Quốc gia ra mắt Chi hội phía Nam tại TP.HCM, sự kiện này không đơn thuần là mở rộng tổ chức, mà là bước đi chiến lược mang tính thực tiễn cao. Chi hội được thành lập để bám sát thực tế của khu vực có các hoạt động chuyển đổi số mạnh mẽ và phát triển kinh tế số năng động nhất cả nước; nơi tập trung đông đảo doanh nghiệp công nghệ, tài chính, thương mại điện tử và an toàn an ninh mạng. Tuy nhiên, bên cạnh những ưu điểm vượt trội cũng tồn tại các yếu tố rủi ro về an ninh mạng và các hoạt động xâm phạm an ninh quốc gia, trật tự an toàn xã hội trên không gian mạng. Chi hội phía Nam sẽ đóng vai trò cầu nối chính sách - doanh nghiệp - chuyên gia, góp phần nâng cao năng lực phòng thủ mạng, thúc đẩy chuẩn mực an toàn thông tin và kiến tạo niềm tin số cho quá trình chuyển đổi số, phát triển kinh tế số khu vực và quốc gia.

Phía Nam - đầu tàu kinh tế số và mặt trận an ninh mạng mới

Khu vực phía Nam, với hạt nhân là Thành phố Hồ Chí Minh cùng các tỉnh, thành thuộc vùng kinh tế trọng điểm, đang giữ vai trò đầu tàu trong phát triển kinh tế số của cả nước. Các hệ thống tài chính - ngân hàng, logistics, thương mại điện tử, công nghiệp công nghệ cao, đô thị thông minh... được triển khai với quy mô lớn, mức độ liên thông sâu và tốc độ đổi mới nhanh chưa từng có.

Tuy nhiên, khi giao dịch số diễn ra liên tục, khi nền tảng số trở thành "huyết mạch" vận hành kinh tế - xã hội, khi dữ liệu trở thành tài sản chiến lược thì không gian mạng cũng đồng thời trở thành địa bàn tác chiến mới của tội phạm công nghệ cao. Các cuộc tấn công mạng, lừa đảo số, khai thác dữ liệu, giả mạo danh tính, deepfake... không còn là hiện tượng cá biệt, mà đã trở

Thiếu tướng, Tiến sĩ Lê Minh Mạnh
Chi hội trưởng Chi hội phía Nam Hiệp hội An ninh mạng quốc gia

thành thách thức thường trực, có tổ chức, có chủ đích và xuyên biên giới.

Thực tiễn cho thấy, nhiều điểm yếu và sự cố an ninh mạng không chỉ xuất phát từ lỗ hổng kỹ thuật phức tạp, mà bao gồm cả những yếu tố bắt nguồn từ con người, nhất là những vấn đề liên quan đến nhận thức, kiến thức về an ninh mạng. Khi các thủ đoạn lừa đảo được "cá nhân hóa" nhờ dữ liệu và trí tuệ nhân tạo, chỉ một mắt xích yếu cũng có thể tạo thành sự cố lớn, kéo theo thiệt hại tài chính, gián đoạn dịch vụ và suy giảm niềm tin xã hội. Điều đó đặt ra yêu cầu phải nhìn an ninh mạng như một vấn đề tổng thể, gắn với con người, quy trình, công nghệ và văn hóa vận hành.

Thành lập Chi hội phía Nam - từ nhu cầu thực tiễn đến thiết chế hành động

Trong bối cảnh đó, Chi hội phía Nam được thành lập là một bộ phận quan trọng của Hiệp hội An ninh mạng Quốc gia nhằm hình thành một thiết chế phối hợp thực chất tại khu vực phía Nam. Chi hội được xác định là cánh tay nối dài của Hiệp hội An ninh mạng Quốc gia, đồng thời là điểm hội tụ của các cơ quan quản lý, doanh nghiệp, viện - trường và cộng đồng chuyên gia trong lĩnh vực an ninh mạng, an toàn thông tin và bảo vệ dữ liệu.

Mục tiêu xuyên suốt là kết nối chính sách với thực tiễn, kết nối chuyên môn với hành động, kết nối phòng ngừa với ứng phó. Thay vì tập trung vào ứng cứu và xử lý sự cố khi đã xảy ra, Chi hội hướng tới cách tiếp cận phòng ngừa từ gốc, hỗ trợ các tổ chức và doanh nghiệp nâng cao nhận thức, kiến thức về an ninh mạng và năng lực quản trị rủi ro số; xây dựng hệ thống phòng thủ bền vững ngay từ khâu thiết kế, vận hành và đào tạo con người.

Chi hội phía Nam vì vậy không chỉ là nơi sinh hoạt hội viên, mà là không gian để chia sẻ kinh nghiệm thực tiễn, lan tỏa tri thức, chuẩn hóa quy trình... góp

phần hình thành hệ sinh thái an toàn an ninh mạng và những giá trị văn hóa trong cộng đồng công dân số.

Hành động ngay từ đầu - thước đo giá trị của tổ chức

Giá trị của một tổ chức không nằm ở tên gọi, mà ở hành động và hiệu quả. Ngay sau khi ra mắt, Chi hội phía Nam đã tham gia và chủ trì những hoạt động chuyên môn quy mô lớn, phản ánh rõ định hướng đi vào thực chất.

Một trong những hoạt động tiêu biểu là việc đồng hành tổ chức các chương trình diễn tập thực chiến ứng phó sự cố an toàn thông tin mạng tại TP.HCM và khu vực lân cận vào ngày 25, 26/12/2025. Các chương trình này không nhằm phô diễn công nghệ, mà tập trung đánh giá năng lực ứng cứu thực tế, rà soát quy trình phối hợp liên ngành, phát hiện những điểm yếu trong tổ chức và con người - những yếu tố thường khó nhận diện nếu chỉ nhìn an ninh mạng từ góc độ kỹ thuật.

Cùng với đó, ngày 18/12/2025, Chi hội đã chỉ đạo tổ chức Hội thảo về nhận diện và phòng, chống lừa đảo qua ứng dụng ngân hàng số, trong bối cảnh các hành vi lừa đảo công nghệ cao đang gia tăng và gây thiệt hại lớn cho người dân. Một thông điệp xuyên suốt được nhấn mạnh tại hội thảo là: báo chí và truyền thông phải trở thành tuyến phòng ngừa đầu tiên. Trong kỷ nguyên AI và deepfake, tội phạm không còn tấn công trực diện vào hệ thống lõi, mà chủ yếu nhắm vào người dùng – mắt xích dễ tổn thương nhất. Khi đó, truyền thông nâng cao nhận thức, hướng dẫn kỹ năng số an toàn và cảnh báo sớm trở thành một phần không thể tách rời của an ninh mạng.

Hai hoạt động này cho thấy một cách tiếp cận thống nhất: an ninh mạng không thể chỉ dựa vào công nghệ, mà phải là sự phối hợp của nhiều lực lượng, trong đó con người và nhận thức đóng vai trò quyết định.

Đồng hành dài hạn, kiến tạo niềm tin số

Bước sang năm 2026, Chi hội phía Nam xác định phương châm hoạt động là đồng hành lâu dài - hỗ trợ thực chất - phát triển bền vững. Trọng tâm không chỉ là tổ chức sự kiện, mà là xây dựng năng lực phòng vệ số mang tính hệ thống cho khu vực phía Nam.

Chi hội sẽ tập trung kiện toàn tổ chức, chuẩn hóa cơ chế vận hành; tham gia tư vấn, phản biện chính sách và phổ biến pháp luật về an ninh mạng, bảo vệ dữ liệu; tổ chức các hội thảo chuyên đề, hội thảo quốc tế để cập nhật xu hướng và thông lệ tốt; triển khai các chương trình đào tạo, bồi dưỡng nguồn nhân lực, đặc biệt là thế hệ trẻ; thúc đẩy hợp tác trong nước và quốc tế, mở rộng mạng lưới hội viên và đối tác.

Xuyên suốt các hoạt động đó là một quan điểm nhất quán: an ninh mạng không phải là rào cản của đổi mới sáng tạo, mà là nền tảng để đổi mới sáng tạo diễn ra an toàn và bền vững. Khi an ninh mạng được đặt đúng vị trí trong chiến lược phát triển, niềm tin số sẽ được củng cố, và kinh tế số mới có thể phát triển lâu dài.

Xuân mới - kết nối mới - niềm tin số mới

Xuân là thời điểm của hy vọng và khởi đầu. Với Chi hội phía Nam, Xuân mới cũng là lời cam kết cho một chặng đường hành động nghiêm túc, bài bản và trách nhiệm. Chúng tôi tin rằng, với sự chỉ đạo của Hiệp hội an ninh mạng Quốc gia và sự kết nối chặt chẽ giữa các cơ quan Nhà nước - doanh nghiệp - giới chuyên gia - báo chí - cộng đồng, an ninh mạng sẽ không còn là "vùng kỹ thuật thuần tuý", mà trở thành hệ sinh thái an ninh số.

Phương Nam, với sức sống năng động và tinh thần hội nhập, sẽ tiếp tục là nơi khởi nguồn cho những sáng kiến, hợp tác và hành động thiết thực trong lĩnh vực an ninh mạng. Từ đó, góp phần cùng cả nước kiến tạo không gian mạng Việt Nam an toàn, lành mạnh, bảo vệ chủ quyền số và thúc đẩy kinh tế số phát triển bền vững trong năm mới và những năm tiếp theo.

Ngày 15/07/2025 Hiệp hội An ninh mạng quốc gia chính thức công bố quyết định thành lập Chi hội phía Nam

Hiệp hội An ninh mạng Quốc gia và chiến lược xây dựng "lá chắn" bảo vệ người dùng trên không gian mạng

Hiền Mai

Với vai trò phát triển nguồn nhân lực, nâng cao năng lực và nhận thức cộng đồng về phòng chống tội phạm, thúc đẩy một môi trường số an toàn, minh bạch, Hiệp hội An ninh mạng quốc gia (NCA) đã triển khai nhiều sáng kiến chiến lược quan trọng. Nổi bật trong số đó là nền tảng đào tạo trực tuyến nCademy và Phần mềm phòng chống lừa đảo nTrust - hai trụ cột thể hiện rõ cách tiếp cận toàn diện: kết hợp giữa đào tạo - nâng cao nhận thức và cung cấp công cụ công nghệ để bảo vệ người dùng trên không gian mạng.

nCademy - Nâng cao "kháng thể số" cho cộng đồng

nCademy là nền tảng đào tạo trực tuyến do NCA phát triển và vận hành, chính thức được triển khai ngày 11/4/2025. Nền tảng được xây dựng với mục tiêu hình thành một cộng đồng học tập mở, hỗ trợ từ nâng cao nhận thức phổ cập đến nghiên cứu chuyên sâu về an ninh mạng, góp phần phát triển nguồn nhân lực chất lượng cao cho xã hội số. Các khóa học trên nCademy được thiết kế, xây dựng bởi các tổ chức, doanh nghiệp an ninh mạng uy tín, là thành viên của Hiệp hội, bảo đảm tính chính xác, cập nhật và bám sát thực tiễn.

Ông Vũ Ngọc Sơn - Trưởng Ban Nghiên cứu, tư vấn, phát triển công nghệ và Hợp tác quốc tế của NCA cho hay, chuỗi khóa học "Cẩm nang an ninh mạng" mang tính tuyên truyền, phổ cập kiến thức được cung cấp hoàn toàn miễn phí. Người dùng chỉ cần có thiết bị kết nối Internet là có thể tham gia học tập ở mọi nơi, mọi lúc. Với các khóa học chuyên sâu hơn, yêu cầu môi trường thực hành hoặc có giảng viên hướng dẫn trực tiếp, sẽ được tổ chức theo hình thức thu phí để duy trì hạ tầng kỹ thuật và phát triển nội dung đào tạo. Hiệp hội đang cung cấp ba khóa học thu phí gồm: An ninh mạng cơ bản (dành cho cán bộ, nhân viên văn phòng); An ninh mạng cho nhà quản lý; Chuyên gia an ninh mạng (dành cho cán bộ phụ trách vận hành hệ thống).

Cẩm nang an ninh mạng là các khoá học ngắn

Hai ngày sau khi chính thức mở khóa học đầu tiên (06_05_2025)), nền tảng đào tạo trực tuyến nCademy do Hiệp hội An ninh mạng quốc gia phát triển, ghi nhận hơn 34.900 người tham gia khóa học miễn phí "Cẩm nang an ninh mạng".

- dễ hiểu - dễ nhớ, dưới dạng các bài trắc nghiệm ngắn. Mỗi tháng Hiệp hội xây dựng năm tình huống khác nhau, xoay quanh các chủ đề sát với đời sống số hằng ngày. Năm 2025, các bài trắc nghiệm này đã thu hút và đào tạo cho hơn 1 triệu lượt người dùng khác nhau. Cách tiếp cận này không chỉ giúp nâng cao nhận thức mà còn từng bước hình thành thói quen ứng xử an toàn trên không gian mạng, biến kiến thức an ninh mạng trở thành kỹ năng sống thiết yếu của mỗi người dân.

Hiệp hội cũng đặc biệt chú trọng đào tạo kỹ năng an ninh mạng cho cán bộ, nhân viên văn phòng - những người trực tiếp tham gia vào hệ thống công nghệ thông tin của các cơ quan, tổ chức, doanh nghiệp. Với mục tiêu giúp người học có kỹ năng thực hành cao, đủ để tự bảo vệ thiết bị cá nhân và góp phần bảo vệ hệ thống mà mình tham gia vận hành, bộ tài liệu đào tạo có nội dung chuyên sâu và quy trình đánh giá khắt khe hơn. Sau mỗi bài học, người học phải thực hiện bài kiểm tra mới được tiếp tục học các nội dung tiếp theo.

Đào tạo an ninh mạng cho đội ngũ nhà quản lý đóng vai trò then chốt trong việc bảo vệ an ninh mạng của tổ chức. Việc trang bị kiến thức an ninh mạng giúp nhà quản lý hiểu rõ các mối đe dọa, tuân thủ quy định và phân bổ nguồn lực một cách hợp lý. Khi nhà quản lý có nhận thức đúng và đầy đủ, khả năng phòng ngừa và ứng phó với sự cố an ninh mạng sẽ được nâng cao đáng kể

Ở cấp độ chuyên sâu nhất, Hiệp hội triển khai các khóa đào tạo dành cho cán bộ, chuyên viên an ninh mạng phụ trách vận hành hệ thống theo hình thức đặt hàng từ các cơ quan, tổ chức, qua đó trang bị cho các chuyên viên những kỹ năng cần thiết để bảo vệ hệ thống.

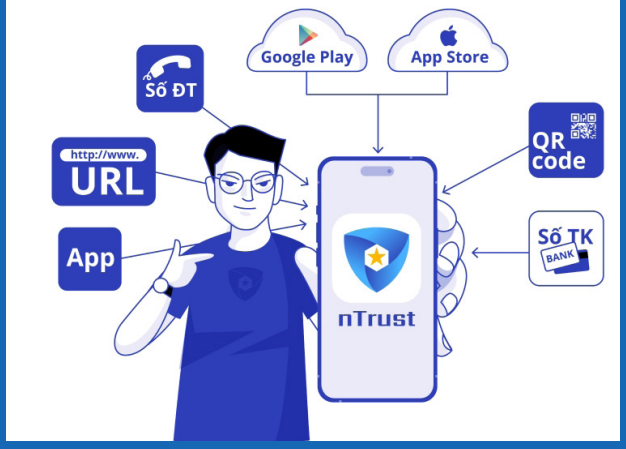
An ninh mạng là trách nhiệm của toàn xã hội vì vậy thời gian tới, NCA sẽ tiếp tục mở rộng hoạt động đào tạo sang các nhóm đối tượng học sinh, sinh viên. Với sinh viên, NCA hướng tới vừa đào tạo định hướng tham gia ngành công nghiệp an ninh mạng. Với học sinh, các chương trình phổ cập kiến thức và kỹ năng cơ bản sẽ góp phần bảo vệ nhóm đối tượng yếu thế trước các nguy cơ trên không gian mạng.

nTrust - từ công cụ bảo vệ cá nhân đến cộng đồng phòng chống lừa đảo trên không gian mạng

nTrust là phần mềm chống lừa đảo hoàn toàn miễn phí, không thu thập bất kỳ thông tin hay dữ liệu cá nhân nào của người dùng. Khi cài đặt ứng dụng, người dùng hoàn toàn chủ động trong việc chia sẻ các dấu hiệu nguy hại hoặc thông tin liên quan đến lừa đảo về Trung tâm. Hiện đã có khoảng 250.000 người thường xuyên dùng nTrust; đó không chỉ là số lượng người cài đặt ứng dụng, mà còn là 250.000 "hạt nhân" ban đầu của một cộng đồng phòng chống lừa đảo đang từng bước được hình thành trên không gian mạng Việt Nam.

NCA xác định sứ mệnh của nTrust là xây dựng cộng đồng cùng tham gia phát hiện, cảnh báo và ngăn chặn các hành vi lừa đảo trực tuyến. Mỗi người dùng nTrust, ngoài vai trò là đối tượng được

Cẩm nang nTrust do Hiệp hội An ninh mạng quốc gia phát triển



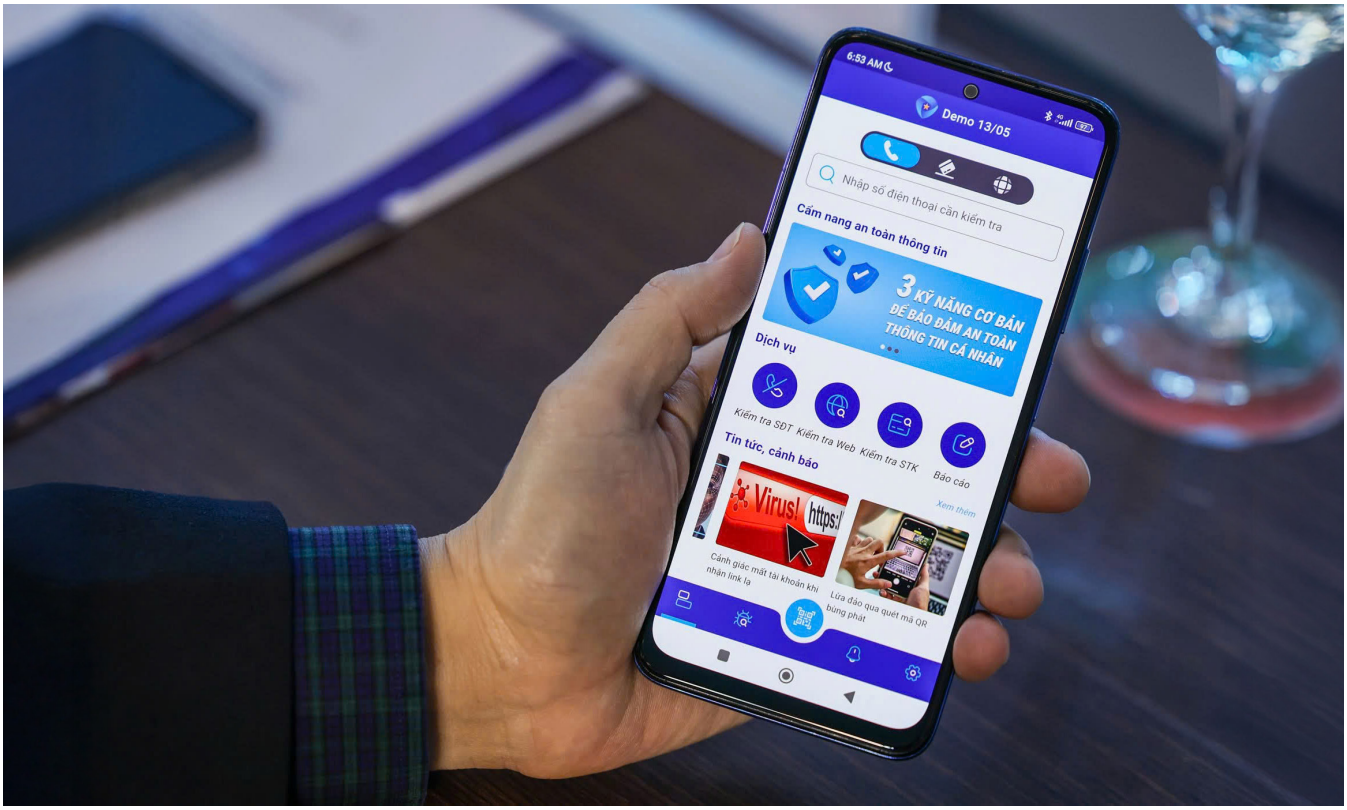
Ngày 30_07_2024, Hiệp hội An ninh mạng quốc gia chính thức ra mắt Phần mềm phòng chống lừa đảo nTrust

bảo vệ, còn đồng thời trở thành một "cảm biến" an ninh mạng, hằng ngày chủ động đóng góp các thông tin như số điện thoại nghi vấn lừa đảo, địa chỉ website giả mạo, đường link độc hại hay các ứng dụng có dấu hiệu mã độc.

Với 250.000 người dùng thường xuyên, không chỉ là người thụ hưởng mà còn là những "đại sứ" lan tỏa, giới thiệu ứng dụng tới bạn bè, đồng nghiệp và người thân; không những thế đây còn là 250.000 "cảm biến" được phân bổ rộng khắp trên không gian mạng. Trên cơ sở các thông tin do người dùng cảnh báo, các cơ quan, tổ chức liên quan có thể đưa ra những cảnh báo phù hợp tới cộng đồng người dùng trên không gian mạng Việt Nam. Đây cũng là cơ sở quan trọng để các đơn vị nghiên cứu, phát triển tiếp tục cập nhật, hoàn thiện các giải pháp công nghệ, giúp các phần mềm, hệ thống an ninh mạng của Việt Nam có khả năng phát hiện và xử lý hiệu quả hơn các mối nguy cơ mới. Các dữ liệu này không chỉ phục vụ riêng cho phần mềm nTrust mà còn được NCA chia sẻ tới các cơ quan quản lý nhà nước, các đơn vị thành viên của Hiệp hội để cùng phối hợp ứng phó các mối đe dọa trên không gian mạng. Với đặc điểm không thu thập dữ liệu cá nhân, cùng nhiều tính năng thiết thực như kiểm tra số điện thoại, tài khoản, website, cảnh báo cuộc gọi rác, tránh truy cập các đường link lừa đảo, nTrust đang dần trở thành một công cụ bảo vệ cần thiết đối với người dùng phổ thông.

Cùng với việc phát huy vai trò cộng đồng, nTrust còn liên tục được nâng cấp tính năng và hiệu quả hoạt động khi số lượng người dùng ngày càng tăng. Trong năm qua, nhiều cải tiến nằm ở "phần phía sau" của ứng dụng, trên hệ thống máy chủ, đã giúp nâng cao khả năng xử lý, phân tích và phản hồi các mối nguy cơ an aninh mạng. Vì vậy, nTrust được kỳ vọng sẽ tiếp tục là một người bạn đồng hành, một công cụ hữu ích đối với người dùng Việt Nam trong quá trình sử dụng không gian mạng.

Ông Vũ Ngọc Sơn - Trưởng Ban Nghiên cứu, tư vấn, phát triển công nghệ và Hợp tác quốc tế của Hiệp hội An ninh mạng quốc gia (NCA), giới thiệu nCademy



Ứng dụng chống lừa đảo nTrust hiện có khoảng 250.000 người sử dụng thường xuyên

Sinh viên an ninh mạng và sứ mệnh bảo vệ Chủ quyền số quốc gia

Đại tá, Tiến sĩ Nguyễn Hồng Quân

Phó Cục trưởng cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an,
Ủy viên Ban Chấp hành, Trưởng ban An ninh dữ liệu và Bảo vệ dữ liệu cá nhân,
Hiệp hội An ninh mạng quốc gia

Trung tướng Lê Xuân Minh - Cục trưởng Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an, Phó Chủ tịch Điều hành Hiệp hội An ninh mạng quốc gia trao giải nhất cho Học viện Công nghệ Bưu chính Viễn thông trong Cuộc thi Sinh viên an ninh mạng 2025

Trong bối cảnh chuyển đổi số quốc gia được triển khai mạnh mẽ trên mọi lĩnh vực của đời sống kinh tế – xã hội, không gian mạng đã trở thành mặt trận mới gắn liền với chủ quyền, an ninh và lợi ích cốt lõi của quốc gia. Các nghị quyết, chiến lược của Đảng và Nhà nước, tiêu biểu là Nghị quyết số 52-NQ/TW của Bộ Chính trị và Chiến lược An ninh mạng quốc gia, đã nhất quán khẳng định yêu cầu bảo đảm an ninh, an toàn không gian mạng phải song hành với quá trình phát triển và chuyển đổi số. Trong đó, việc xây dựng năng lực tự chủ, phòng vệ trên không gian mạng, lấy con người làm trung tâm, được coi là yếu tố then chốt nhằm bảo vệ vững chắc chủ quyền số trước các mối đe dọa phi truyền thống.

Không gian mạng - mặt trận mới gắn với chủ quyền, an ninh và lợi ích quốc gia

Thực tiễn thời gian qua cho thấy, các mối đe dọa trên không gian mạng ngày càng đa dạng, tinh vi và mang tính chiến lược, từ tấn công vào hạ tầng thông tin trọng yếu, xâm phạm dữ liệu cá nhân, thao túng dư luận, cho tới các hoạt động gián điệp mạng và phá hoại có chủ đích. Những thách thức này không chỉ đặt ra yêu cầu cấp bách đối với lực lượng chuyên trách của Nhà nước, mà còn đòi hỏi sự tham gia của nguồn nhân lực trẻ, có tri thức, bản lĩnh chính trị vững vàng và trình độ công nghệ cao. Đặc biệt là thế hệ trẻ - lực lượng sinh viên, với lợi thế về tư duy sáng tạo, khả năng tiếp cận nhanh công nghệ mới và tinh thần dấn thân, đang trở thành một trong những trụ cột quan trọng của hệ sinh thái bảo vệ an ninh mạng quốc gia.

Từ góc độ đó, việc đào tạo, bồi dưỡng và rèn luyện thế hệ nhân lực an ninh mạng trẻ không chỉ nhằm đáp ứng nhu cầu thị trường lao động, mà còn mang ý nghĩa chuẩn bị lực lượng bảo vệ chủ quyền số của quốc gia trong dài hạn. Cuộc thi Sinh viên An ninh mạng 2025 được tổ chức chính là một bước đi cụ thể, thể hiện quyết tâm chuyển hóa các chủ trương, chiến lược lớn thành hành động thực tiễn trong công tác xây dựng lực lượng.

Cuộc thi do Hiệp hội An ninh mạng quốc gia chủ trì tổ chức, dưới sự bảo trợ của Bộ Công an và Bộ Giáo dục và Đào tạo, với sự phối hợp trực tiếp của Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05). Chủ đề "An ninh dữ liệu và bảo vệ dữ liệu cá nhân" là một minh chứng sinh động cho việc gắn đào tạo nguồn nhân lực trẻ với nhiệm vụ bảo vệ chủ quyền số quốc gia.

Với quy mô 328 đội thi, quy tụ 1.248 sinh viên đến từ hàng chục cơ sở đào tạo trong nước và quốc tế, cuộc thi không chỉ là một sân chơi học thuật, mà còn là mô hình huấn luyện thực chiến, phản ánh đúng tính chất phức tạp, khốc liệt của các mối đe dọa an ninh mạng hiện nay.

Cuộc thi Sinh viên An ninh mạng 2025 - mô hình huấn luyện thực chiến bảo vệ chủ quyền số

Sau hơn hai tháng triển khai, cuộc thi đã lựa chọn 76 đội xuất sắc nhất vào vòng Chung khảo, diễn ra ngày 15/11/2025 tại Hà Nội, cùng sự tham gia của các đội thi đến từ ASEAN và Nhật Bản, đã tạo nên một môi trường cạnh tranh có chiều sâu. Đây không chỉ là sự so tài về kỹ thuật, mà còn là dịp để sinh viên Việt Nam đặt năng lực của mình trong tương quan quốc tế, qua đó kiểm chứng khả năng tham gia bảo vệ không gian mạng quốc gia trong bối cảnh hội nhập sâu rộng.

Cấu trúc thi đấu của vòng Chung khảo phản ánh rõ tư duy tác chiến bảo vệ chủ quyền số. Bảng A (Attack – Defense) đặt các đội thi vào tình huống phải bảo vệ hệ thống thông tin trước các đợt tấn công liên tục, đồng thời chủ động phát hiện và vô hiệu hóa điểm yếu của đối phương trong môi trường giả lập trung tâm dữ liệu. Đây chính là mô hình thu nhỏ của nhiệm vụ bảo vệ các hệ thống thông tin quan trọng quốc gia – nơi mọi sai sót đều có thể dẫn đến hậu quả nghiêm trọng. Bảng B (Jeopardy CTF nâng cao) tập trung vào các kỹ năng điều tra, phân tích và xử lý sự cố, phản ánh yêu cầu về chiều sâu chuyên môn và khả năng làm chủ công nghệ lõi trong bảo vệ chủ quyền không gian mạng.

Thông qua cấu trúc và nội dung thi đấu, cuộc thi đã góp phần hình thành cho sinh viên tư duy tiếp cận các bài toán an ninh mạng từ góc độ bảo vệ lợi ích quốc gia, chứ không đơn thuần là giải quyết các vấn đề kỹ thuật rời rạc. Việc đặt sinh viên vào các kịch bản sát với thực tiễn bảo vệ hạ tầng số, dữ liệu và hệ thống thông tin đã giúp các em từng bước làm quen với áp lực, trách nhiệm và yêu cầu kỷ luật của công tác bảo vệ an ninh mạng trong môi trường nhà nước và xã hội. Đây chính là quá trình "tập dượt chiến lược" cần thiết để chuẩn bị nguồn nhân lực tham gia bảo vệ các hệ thống thông tin phục vụ quản lý nhà nước, phát triển kinh tế – xã hội và bảo đảm an ninh quốc gia.

Thực tiễn thi đấu cho thấy sinh viên không chỉ làm chủ kỹ thuật, mà còn thể hiện rõ tư duy phòng thủ quốc gia trong cách tiếp cận bài toán. Suốt 88 hiệp thi đấu liên tiếp kéo dài gần 8 giờ, các đội luôn duy trì trạng thái sẵn sàng cao độ, liên tục điều chỉnh chiến thuật trước những tình huống bất ngờ. Trong nhiều thời điểm khó khăn, khi hệ thống bị khai thác, điểm số tụt giảm hoặc chiến thuật chưa phát huy hiệu quả, các đội vẫn kiên trì bám trụ, phối hợp chặt chẽ và chiến đấu

đến phút cuối cùng. Điều này thể hiện một tinh thần đồng đội, kỷ luật và ý chí chiến đấu bền bỉ –những phẩm chất không thể thiếu của lực lượng bảo vệ chủ quyền quốc gia trên không gian mạng – nơi các mối đe dọa không đến theo từng đợt ngắn hạn, mà có thể kéo dài, âm thầm và phức tạp.

Kết quả chung cuộc với chiến thắng của đội PTIT.CBS (Học viện Công nghệ Bưu chính - Viễn thông) tại Bảng A, đội UIT-Reze (Trường Đại học Công nghệ Thông tin – Đại học Quốc gia TP.HCM) tại Bảng B, cùng sự hiện diện nổi bật của các đội đến từ Nhật Bản, cho thấy năng lực của sinh viên Việt Nam không hề thua kém trong một sân chơi có tính quốc tế, tạo niềm tin vững chắc vào khả năng tự chủ về nhân lực trong bảo vệ không gian mạng quốc gia.

Hình thành thế hệ "chiến sĩ số" vững kỹ thuật, bản lĩnh chính trị và trách nhiệm quốc gia

Điều quan trọng hơn cả mà Cuộc thi Sinh viên An ninh mạng 2025 mang lại không chỉ nằm ở kết quả xếp hạng hay giải thưởng, mà ở việc hình thành nhận thức đúng đắn về sứ mệnh bảo vệ chủ quyền số. Mỗi sinh viên tham gia cuộc thi đều được đặt trong một thông điệp xuyên suốt: an ninh mạng không phải là trò chơi công nghệ, mà là trách nhiệm quốc gia. Mỗi dòng mã, mỗi công cụ, mỗi kỹ năng nếu không được định hướng đúng đắn sẽ tiềm ẩn nguy cơ bị lợi dụng, gây tổn hại cho Nhà nước, doanh nghiệp và người dân. Vì vậy, việc gắn kỹ năng công nghệ với đạo đức nghề nghiệp, pháp luật và bản lĩnh chính trị là yêu cầu bắt buộc đối với sinh viên an ninh mạng.

Cuộc thi Sinh viên An ninh mạng 2025 đã góp phần phát hiện, bồi dưỡng và định hướng lực lượng kế cận cho công tác bảo vệ an ninh, an toàn không gian mạng. Đây là kênh quan trọng để kết nối giữa cơ quan quản lý, cơ sở đào tạo và sinh viên, từng bước hình thành hệ sinh thái nhân

Các thí sinh tham gia Cuộc thi Sinh viên An ninh mạng 2025.

lực an ninh mạng gắn với lợi ích quốc gia. Những mô hình đào tạo thông qua thi đấu, thực hành và tình huống giả lập như cuộc thi này cần tiếp tục được nhân rộng, nâng tầm và gắn chặt hơn nữa với yêu cầu chiến lược về bảo vệ chủ quyền số.

Trong bối cảnh tình hình an ninh mạng quốc tế diễn biến phức tạp, các nguy cơ tấn công mạng, đánh cắp dữ liệu, thao túng thông tin ngày càng gia tăng, nguồn nhân lực an toàn, an ninh mạng chất lượng cao chính là "lá chắn vững chắc" bảo vệ không gian mạng quốc gia. Đảng, Nhà nước và Bộ Công an luôn quan tâm, chỉ đạo sát sao việc phát triển nguồn nhân lực công nghệ thông tin và an ninh mạng, coi đây là nhiệm vụ trọng tâm, lâu dài. Từ những sân chơi trí tuệ như Cuộc thi Sinh viên An ninh mạng 2025, sẽ tiếp tục hình thành một thế hệ "chiến sĩ số" vừa giỏi chuyên môn, vừa vững bản lĩnh chính trị, đủ năng lực bảo vệ không gian mạng, bảo vệ dữ liệu, bảo vệ niềm tin số và góp phần giữ vững chủ quyền số quốc gia trong kỷ nguyên mới.

Đội sinh viên Học viện Công nghệ Bưu chính viễn thông chụp ảnh lưu niệm trước khi bước vào Vòng Chung khảo Cuộc thi Sinh viên An ninh mạng 2025

Cuộc thi Sinh viên An ninh mạng 2025 là sân chơi học thuật - thực hành quy mô quốc gia, được bảo trợ bởi Bộ Công an và Bộ Giáo dục và Đào tạo, do Hiệp hội An ninh mạng quốc gia phối hợp với Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao tổ chức. Cuộc thi hướng tới mục tiêu tạo cầu nối giữa đào tạo - nghiên cứu - thực tiễn, qua đó phát hiện, bồi dưỡng nguồn nhân lực an ninh mạng chất lượng cao cho Việt Nam.

Vòng Sơ khảo diễn ra ngày 18/10/2025, thu hút 1.265 sinh viên thuộc 327 đội thi trên cả nước và quốc tế, thi trực tuyến trong 8 giờ liên tục với 21 thử thách thuộc 5 nhóm chủ đề: Web Security, Reverse, Pwnable, Crypto và Forensic. Từ kết quả sơ khảo, 20 đội xuất sắc nhất bước vào Vòng Chung khảo tổ chức ngày 15/11/2025.

Vòng Chung khảo được tổ chức trực tiếp, gồm hai bảng thi: Bảng A - Attack/Defense với 20 đội (17 đội thi trực tiếp, 3 đội quốc tế thi online) và Bảng B - Jeopardy CTF nâng cao. Điểm nhấn của mùa giải 2025 là việc lồng ghép thông điệp Công ước Hà Nội vào các thử thách, lan tỏa tinh thần hợp tác, trách nhiệm và phát triển bền vững trong không gian mạng.

Trung tướng Lê Xuân Minh
Cục trưởng Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05, Bộ Công an),
Phó Chủ tịch Điều hành Hiệp hội An ninh mạng quốc gia phát biểu khai mạc lễ phát động Chiến dịch "Không một mình".

Chiến dịch "Không một mình" Từ cảnh báo rủi ro số đến tái thiết năng lực bảo vệ trẻ em của xã hội

Thu Uyên

Lễ tổng kết Chiến dịch "Không Một Mình 2025 - Cùng nhau an toàn trực tuyến"

Chưa bao giờ trẻ em và thanh thiếu niên Việt Nam được bước vào không gian số với mức độ tự do và cường độ lớn như hiện nay. Một chiếc điện thoại thông minh không chỉ mở ra thế giới học tập, giải trí và kết nối xã hội, mà còn vô tình đẩy các em vào những vùng rủi ro vượt xa khả năng tự vệ của chính mình. Khi ranh giới giữa đời thực và đời ảo bị xóa nhòa, những mối nguy hiểm không còn hiện diện bằng hình hài cụ thể, mà ẩn mình trong tin nhắn, thuật toán và các mối quan hệ tưởng như vô hại.

Trong bối cảnh đó, bảo vệ trẻ em không còn là câu chuyện của riêng gia đình hay nhà trường, mà trở thành bài toán an ninh con người trên không gian mạng. Chiến dịch "Không một mình" ra đời không chỉ như một lời cảnh báo về rủi ro số, mà như một nỗ lực tái thiết năng lực bảo vệ trẻ em của toàn xã hội - nơi người lớn không đứng ngoài quan sát, còn trẻ em không bị buộc phải tự xoay xở một mình giữa thế giới số đầy cạm bẫy.

Hồi chuông từ "bắt cóc trực tuyến" và yêu cầu cấp bách về an ninh con người trên không gian mạng

Năm 2025 đánh dấu một bước chuyển đáng lo ngại trong cấu trúc tội phạm công nghệ cao tại Việt Nam. Nếu trước đây, lừa đảo trực tuyến chủ yếu nhằm chiếm đoạt tài sản, thì nay, mục tiêu ngày càng dịch chuyển sang chiếm đoạt con người thông qua thao túng tâm lý - hình thức được gọi là 'bắt cóc trực tuyến'. Đây không còn là hành vi phạm tội thuần túy về kinh tế, mà là mối đe dọa trực tiếp tới an ninh con người trong môi trường số.

Theo thống kê của Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Bộ Công an, hơn 77% trẻ em và thanh thiếu niên Việt Nam truy cập Internet hằng ngày. Chỉ trong 6 tháng đầu năm 2025, lực lượng chức năng đã ghi nhận hàng chục vụ việc lừa đảo, dụ dỗ, thao túng tâm lý và bắt cóc trực tuyến liên quan đến học sinh, sinh viên. Nhiều vụ việc gây thiệt hại tài chính lên tới hàng tỷ đồng, song hậu quả nghiêm trọng hơn là những tổn thương tâm lý kéo dài, ảnh hưởng sâu sắc đến học tập, nhân cách và tương lai của người trẻ.

Phát biểu tại lễ phát động Chiến dịch "Không Một Mình", Trung tướng Lê Xuân Minh - Cục trưởng Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Bộ Công an nhận định, khác với các hình thức phạm tội truyền thống, bắt cóc trực tuyến không cần tiếp xúc trực tiếp. Tội

phạm lợi dụng mạng xã hội, ứng dụng nhắn tin, trò chơi trực tuyến để gieo sợ hãi, đe dọa, ép nạn nhân cắt đứt liên lạc với gia đình và bạn bè, từ đó khống chế, thao túng và cô lập các em về mặt tâm lý từ xa, nhằm tống tiền hoặc phục vụ các mục đích phi pháp khác.

Từ góc độ an ninh xã hội, bảo vệ trẻ em trên không gian mạng vì thế không thể chỉ dừng ở giải pháp kỹ thuật hay xử lý vi phạm đơn lẻ. Đây là yêu cầu cấp bách về đạo đức, trách nhiệm xã hội và sự tham gia đồng bộ của toàn cộng đồng.

Khi an toàn số không còn là việc riêng: "Không Một Mình" và sức mạnh của hành động cộng đồng

Xuất phát từ thực tiễn đấu tranh phòng, chống tội phạm công nghệ cao, Trung tá Nguyễn Tiến Cường, Trưởng phòng 3 - Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Bộ Công an, chỉ ra rằng "điểm mù" lớn nhất mà tội phạm mạng khai thác không nằm ở công nghệ, mà ở việc phá vỡ sự kết nối xã hội của nạn nhân. Khi bị đe dọa, nhiều em lựa chọn im lặng vì sợ hãi hoặc xấu hổ, trong khi gia đình và nhà trường không nhận ra những nguy cơ âm thầm đang diễn ra trên không gian mạng.

Chính từ nhận thức đó, Chiến dịch "Không Một Mình" được khởi xướng và triển khai trên quy mô toàn quốc với một triết lý nhất quán: khôi phục và củng cố sự kết nối giữa trẻ em với gia đình, nhà trường và cộng đồng. Thông điệp gửi tới trẻ em rất rõ ràng: 'các em không đơn độc trên không gian mạng'. Đồng thời, chiến dịch cũng đặt ra trách nhiệm cho người lớn: không thể bảo vệ trẻ em bằng cấm đoán hay giám sát cứng nhắc, mà bằng sự hiện diện, lắng nghe và đồng hành liên tục.

Chiến dịch do Liên minh Niềm Tin Số khởi xướng và dẫn dắt, dưới sự bảo trợ của UNODC, UNICEF, cùng sự phối hợp của Bộ Công an, Bộ Giáo dục và Đào tạo, Bộ Y tế, UBND TP Hà Nội, Hiệp hội An ninh mạng quốc gia và nhiều tổ chức xã hội. Đối tượng hướng tới không chỉ là khoảng 12 triệu thanh thiếu niên trong độ tuổi 12 - 24, mà còn mở rộng tới 22 triệu học sinh, sinh viên, hàng triệu phụ huynh và giáo viên là những "lá chắn đầu tiên" trong bảo vệ trẻ em.

Điểm đáng chú ý của "Không Một Mình" là sử dụng những hình thức gần gũi với giới trẻ: âm nhạc, nghệ thuật, hoạt động cộng đồng và ngôn ngữ tích cực. Ngày hội An toàn Trực tuyến "Không Một

Ngày hội An toàn trực tuyến "Không Một Mình" chính thức khai mạc tại Quảng trường Đông Kinh Nghĩa Thục, Hoàn Kiếm (Hà Nội)

Mình" tổ chức tại Quảng trường Đông Kinh Nghĩa Thục đã đưa câu chuyện an toàn mạng ra giữa không gian công cộng, khẳng định đây không phải vấn đề nội bộ của ngành chức năng, mà là mối quan tâm chung của toàn xã hội.

Từ chiến dịch truyền thông đến cam kết dài hạn: không để trẻ em đơn độc trong thế giới số

Sau hơn hai tháng triển khai từ 06/10 đến 30/11/2025, Chiến dịch "Không Một Mình" ghi nhận hiệu ứng lan tỏa sâu rộng hiếm có. Trên các nền tảng mạng xã hội, chiến dịch đạt hơn 1,5 tỷ lượt xem, tiếp cận trên 40 triệu người dân, với sự đồng hành của hơn 1.000 KOL và hàng triệu nội dung sáng tạo lan tỏa thông điệp qua các hashtag #khongmotminh và #NiemTinSo.

Song song với hoạt động trực tuyến, chiến dịch được triển khai trực tiếp tại hơn 6.100 điểm trường, 113.000 lớp học thuộc 34 tỉnh, thành phố, với 2.500 lượt chuyên gia tham gia tập huấn, giảng dạy. Hơn 8 triệu học sinh, sinh viên, giáo viên và phụ huynh đã được trang bị kiến thức, kỹ năng an toàn trực tuyến thông qua các chương trình ngoại khóa, tọa đàm và hình thức học tập sáng tạo.

Sáng 11/01/2026, Lễ tổng kết Chiến dịch "Không Một Mình - Cùng nhau an toàn trực tuyến" năm 2025 đã khép lại một hành trình, đồng thời mở ra một chặng đường mới. Những hình ảnh tại buổi lễ - từ triển lãm tranh do chính học sinh sáng tác, đến những chậu sen đá nhỏ xinh mang thông điệp "Cùng nhau an toàn trực tuyến" cho thấy an toàn mạng không còn là khái niệm khô cứng, mà đã trở thành giá trị nhân văn được sẻ chia và gìn giữ.

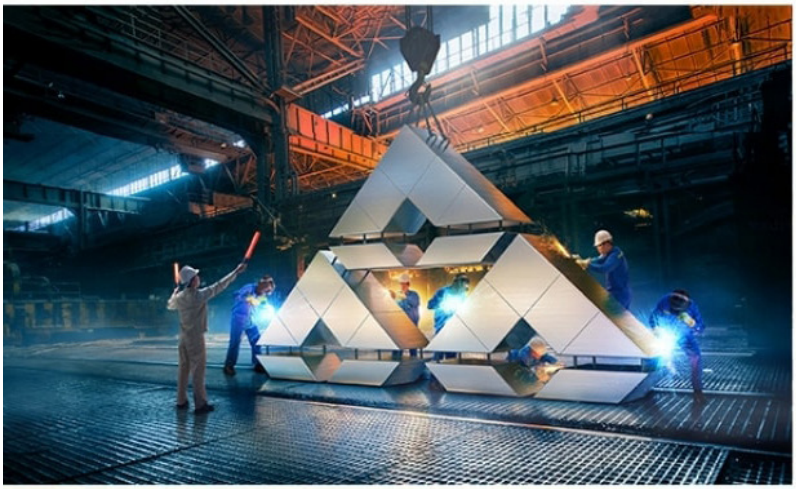
Tại sự kiện, Ban Tổ chức công bố Chiến dịch "Không Một Mình" sẽ tiếp tục trở lại trong năm 2026, với trọng tâm phòng, chống xâm hại trực tuyến, khẳng định đây không phải chiến dịch ngắn hạn, mà là cam kết xã hội dài hạn trong bảo vệ trẻ em trên không gian số.

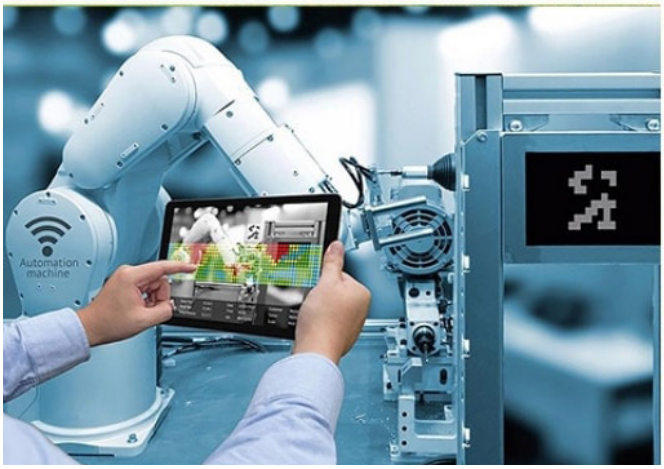
Chiến dịch "Không Một Mình" vì thế không chỉ khép lại bằng những con số ấn tượng hay các hoạt động truyền thông lan tỏa, mà mở ra một chuẩn mực mới trong cách xã hội tiếp cận vấn đề bảo vệ trẻ em trên không gian mạng. Ở đó, an toàn số được khẳng định là năng lực tổng hợp của xã hội trong việc phát hiện sớm, nâng đỡ kịp thời và bảo vệ con người trước những mối đe dọa vô hình.

Khi tội phạm công nghệ cao chuyển từ chiếm đoạt tài sản sang thao túng tâm lý và chiếm đoạt con người, thước đo của an ninh không thể chỉ dừng ở số vụ án được phá, mà phải được tính bằng khả năng trẻ em dám lên tiếng, gia đình đủ hiểu biết để nhận diện nguy cơ, nhà trường đủ năng lực đồng hành và cộng đồng đủ trách nhiệm để không quay lưng. Một xã hội an toàn trên không gian mạng là xã hội không để nỗi sợ trở thành công cụ cô lập trẻ em, cũng không để sự im lặng biến các em thành nạn nhân vô hình.

Tinh thần "Không Một Mình", vì vậy, không chỉ là thông điệp của một chiến dịch hay một năm hành động, mà là lời cam kết dài hạn về an ninh con người trong kỷ nguyên số. Bởi trong thế giới nơi công nghệ liên tục thay đổi, giá trị bền vững nhất vẫn là sự hiện diện của con người bên cạnh con người. Và chỉ khi không đứa trẻ nào bị buộc phải đối mặt một mình với hiểm họa trên không gian mạng, xã hội số mới thực sự an toàn và nhân văn.

SỨC MẠNH CỦA DOANH NGHIỆP VIỆT





★ 1. An ninh mạng - nền tảng phát triển bền vững của MobiFone

★ 2. Từ an ninh mạng đến hạ tầng số quốc gia: Dấu ấn của EVN trong giai đoạn mới

★ 3. Tự chủ công nghệ an ninh mạng - trụ cột chiến lược trong tầm nhìn Trung tâm số và AI của VNPT

★ 4. FPT góp phần kiến tạo "lá chắn số" quốc gia trong kỷ nguyên mới

★ 5. AI Trong Chuyển Đổi Số: Mặt Trận An Ninh Mạng Mới Của Nhà Nước Và Doanh Nghiệp

★ 6. Lá chắn bảo vệ cơ sở hạ tầng trọng yếu quốc gia

An ninh mạng - nền tảng phát triển bền vững của MobiFone

Tổng công ty Viễn thông MobiFone luôn xác định an ninh mạng là nền tảng bảo đảm cho phát triển bền vững và chủ quyền số của doanh nghiệp. Cách tiếp cận theo hướng thận trọng, bài bản, kế thừa những giá trị đã chứng minh hiệu quả, phù hợp với thực tiễn Việt Nam.

Duy trì ổn định hệ thống, giảm thiểu rủi ro trong môi trường số phức tạp

Năm 2025, hoạt động bảo đảm an toàn, an ninh mạng của MobiFone tập trung vào việc duy trì ổn định hệ thống và giảm thiểu rủi ro.

Ở phạm vi nội bộ, doanh nghiệp tiếp tục rà soát, củng cố các biện pháp bảo vệ hạ tầng và hệ thống thông tin, tăng cường giám sát, phát hiện sớm và xử lý kịp thời các nguy cơ mất an toàn thông tin. Công tác vận hành an ninh mạng được thực hiện chặt chẽ, tuân thủ quy trình, chú trọng nâng cao nhận thức và trách nhiệm của cán bộ, người lao động trong sử dụng hệ thống công nghệ thông tin.

Với góc độ cung cấp dịch vụ, MobiFone từng bước hoàn thiện các dịch vụ an toàn, an ninh mạng dựa trên năng lực sẵn có; giải pháp được triển khai theo hướng phù hợp quy mô, dễ tiếp cận, hỗ trợ khách hàng nâng cao mức độ an toàn cho hệ thống thông tin của mình.

Đặc biệt, MobiFone cũng có các sản phẩm dịch vụ an ninh mạng như: SOC, Đánh giá an toàn thông tin, tư vấn hồ sơ cấp độ, giải pháp về tường lửa MobiSafe Smart Firewall cung cấp ra thị trường. Hệ sinh thái an ninh mạng của MobiFone được xây dựng theo hướng đồng bộ, có trọng tâm và phù hợp với thực tiễn của các cơ quan, doanh nghiệp tại Việt Nam, trên nền tảng năng lực sẵn có của một doanh nghiệp viễn thông lớn.

Về cấu trúc, hệ sinh thái được tiếp cận theo nhiều lớp bảo vệ, gồm: bảo vệ hạ tầng mạng và kết nối; bảo vệ hệ thống CNTT và ứng dụng; giám sát, phát hiện và ứng cứu sự cố; cùng với các dịch vụ tư vấn, đánh giá, tuân thủ về an toàn thông tin. Các thành phần này có thể triển khai độc lập hoặc kết hợp, tùy theo quy mô và mức độ sẵn sàng của từng khách hàng; bảo đảm tính ổn định, dễ vận hành và hiệu quả lâu dài, giúp doanh nghiệp có thể đáp ứng các yêu cầu cơ bản về ATTT. Thời gian tới, hệ sinh thái an ninh mạng của MobiFone sẽ phát triển theo hướng gắn chặt với nhu cầu chuyển đổi số, hỗ trợ thiết thực cho khách hàng trong việc bảo đảm an toàn, ổn định cho hệ thống thông tin.

Các giải pháp an ninh mạng của MobiFone được xây dựng và triển khai trên cơ sở tận dụng hạ tầng viễn thông, nền tảng dữ liệu và kinh nghiệm vận hành dịch vụ số sẵn có, từ đó tạo ra sự gắn kết tự nhiên.

MobiFone chú trọng quản lý và bảo vệ dữ liệu xuyên suốt vòng đời. Các giải pháp an ninh mạng được thiết kế để phù hợp

Lãnh đạo và nhân viên Tổng công ty viễn thông MobiFone tại hội thảo "AI & Cyber Security – Kiến tạo tương lai bảo mật thông minh"

với hệ thống dữ liệu hiện có, hỗ trợ phân quyền, giám sát truy cập và phát hiện các hành vi rủi ro, qua đó góp phần bảo vệ dữ liệu khách hàng và dữ liệu nghiệp vụ một cách thực chất.

Đối với các dịch vụ số, an ninh mạng được tích hợp ngay trong quá trình cung cấp và vận hành dịch vụ, bảo đảm yêu cầu an toàn thông tin là một phần của chất lượng dịch vụ. Điều này giúp khách hàng dễ tiếp cận, giảm chi phí triển khai và thuận lợi trong vận hành.

Trách nhiệm bền bỉ vì an ninh mạng quốc gia

MobiFone xác định trách nhiệm và sứ mệnh của mình trong xây dựng năng lực an ninh mạng quốc gia theo hướng bền bỉ và đặt lợi ích chung lên trên hết với 4 yêu cầu:

Thứ nhất, là bảo đảm an toàn, ổn định cho hạ tầng viễn thông và hệ thống thông tin do mình quản lý. Đây là nền tảng thiết yếu của nền kinh tế số và đời sống xã hội. Việc giữ cho hệ thống vận hành an toàn, liên tục, không gián đoạn chính là đóng góp trực tiếp và thiết thực nhất cho an ninh mạng quốc gia.

Thứ hai, tích lũy, làm chủ và chia sẻ năng lực an ninh mạng. Trên cơ sở kinh nghiệm vận hành mạng quy mô lớn, doanh nghiệp từng bước xây dựng đội ngũ, quy trình và công nghệ an ninh mạng, đồng thời chuyển hoá những năng lực này thành các dịch vụ, giải pháp hỗ trợ cơ quan, doanh nghiệp khác nâng cao mức độ an toàn thông tin.

Thứ ba, coi trọng vai trò kết nối và phối hợp trong hệ sinh thái an ninh mạng; chủ động phối hợp với cơ quan quản lý, các đơn vị chuyên trách, các doanh nghiệp công nghệ trong nước để chia sẻ thông tin, kinh nghiệm và cùng ứng phó với các mối đe doạ trên không gian mạng, góp phần hình thành thế trận phòng thủ chung.

Thứ tư, xây dựng năng lực an ninh mạng quốc gia là một quá trình lâu dài, đòi hỏi sự kiên trì và kỷ luật, vì vậy cần đầu tư có trọng tâm, ưu tiên con người, tôn trọng chuẩn mực và pháp luật, từng bước nâng cao năng lực nội tại.

Năm 2026, MobiFone xác định các ưu tiên chiến lược trong lĩnh vực an ninh mạng theo hướng tập trung, thực chất và phù hợp với vai trò của một doanh nghiệp viễn thông - công nghệ nhà nước, đồng thời bám sát nhu cầu thực tế của thị trường.

Về công nghệ, tiếp tục củng cố nền tảng an ninh mạng cốt lõi, bảo đảm an toàn, ổn định; hoàn

thiện năng lực giám sát, phát hiện và ứng phó sự cố theo hướng hiệu quả, dễ vận hành; từng bước ứng dụng các công nghệ mới như tự động hoá, phân tích thông minh một cách chọn lọc, có kiểm soát; tăng mức độ làm chủ công nghệ trong vận hành và tích hợp hệ thống.

Về thị trường, MobiFone xác định tập trung vào các phân khúc khách hàng có nhu cầu thực, đặc biệt là cơ quan nhà nước, doanh nghiệp hạ tầng, doanh nghiệp đang chuyển đổi số nhưng còn hạn chế về nguồn lực an ninh mạng. Các dịch vụ an ninh mạng tiếp tục được phát triển theo hướng gắn với hạ tầng viễn thông và dịch vụ số sẵn có, dễ triển khai, dễ sử dụng và phù hợp quy mô từng khách hàng.

Về nhân lực, MobiFone ưu tiên xây dựng đội ngũ an ninh mạng ổn định, có chiều sâu, kết hợp giữa kinh nghiệm thực tiễn và năng lực tiếp cận công nghệ mới và khả năng làm chủ hệ thống trong thực tế vận hành.

Trung tâm mạng lưới MobiFone, Tổng công ty viễn thông MobiFone

Từ an ninh mạng đến hạ tầng số quốc gia: Dấu ấn của EVN trong giai đoạn mới

Nguyễn Xuân Tuấn, Phan Thế Đại

Để đảm bảo an ninh mạng và chuyển đổi số toàn diện phục vụ sản xuất, kinh doanh, Tập đoàn Điện lực Việt Nam (EVN) đã triển khai đồng bộ các giải pháp. Trong đó, lấy con người làm trung tâm, kết hợp quản trị, công nghệ và hợp tác, EVN đang từng bước khẳng định vai trò doanh nghiệp nhà nước nòng cốt trong kiến tạo hạ tầng số an toàn, tin cậy cho quốc gia trong giai đoạn phát triển mới.

Thách thức an ninh mạng đặc thù ngành điện

Trong bối cảnh an ninh mạng toàn cầu ngày càng phức tạp, ngành điện sẽ phải đối mặt bối cảnh kép: quá trình chuyển đổi số diễn ra song song với sự gia tăng của các nguy cơ rủi ro cao về an ninh mạng, các mối đe dọa ngày càng tinh vi nhắm vào hạ tầng trọng yếu. Các chiến dịch tấn công có chủ đích (APT) như Volt Typhoon nhắm vào chuỗi cung ứng và hệ thống công nghệ vận hành (OT) và hệ thống điều khiển công nghiệp (ICS); mã độc tống tiền (Ransomware), tấn công từ chối dịch vụ (DDoS) kiểu GhostRedirector, khai thác tiền điện tử (Cryptojacking), lợi dụng điện toán đám mây; các cuộc tấn công được hỗ trợ bởi trí tuệ nhân tạo (AI-powered) khiến mối đe dọa khó lường hơn. Hệ thống OT/ICS cũ tiềm ẩn rủi ro thiếu nguyên tắc bảo mật từ thiết kế (secure by design), sự hội tụ giữa công nghệ thông tin (IT) và OT xóa bỏ vùng an toàn (air-gap) vật lý truyền thống, chuỗi cung ứng phần mềm chưa kiểm định chặt chẽ.

Trong chuỗi này, con người là khâu tiềm ẩn nhiều rủi ro và nguy cơ cao. Các hình thức lừa đảo qua email (phishing) tinh vi, vi phạm quy trình, và đặc biệt sử dụng trái phép công cụ trí tuệ nhân tạo công cộng (Shadow AI) có thể gây sự cố lan rộng, tê liệt vận hành hệ thống điện quốc gia.

Chiến lược đào tạo ba tầng

Nhận diện được các nguy cơ an ninh mạng phải đối mặt là các mối đe dọa từ cả bên ngoài và các khoảng trống bảo mật bên trong, EVN đã triển khai hệ thống đào tạo ba tầng, kết hợp lý thuyết - thực hành - diễn tập, lồng ghép vào văn hóa tổ chức:

Thứ nhất, Chương trình học trực tuyến hàng năm cho 100% cán bộ, công nhân viên, tập trung rủi ro hàng ngày như lừa đảo qua email, mật khẩu yếu, sử dụng trái phép AI. Nội dung ngắn gọn, tương tác cao qua video minh họa, bài kiểm tra tình huống thực tế.

Thứ hai, Dành cho vị trí quan trọng, nhấn mạnh quy trình ứng phó, phân tích các trường hợp tấn công thực tế vào ngành năng lượng. Bao gồm hội thảo phối hợp

EVN ứng dụng công nghệ hiện đại trong vận hành các nhà máy điện

giữa IT và OT.

Thứ ba, Đào tạo cho đội ngũ an toàn thông tin (ATTT) với mô phỏng lừa đảo qua email thực chiến, diễn tập red team/blue team, phân tích thông tin tình báo mối đe dọa. Hợp tác với các viện nghiên cứu, doanh nghiệp trong lĩnh vực ATTT.

Các đơn vị thành viên của EVN đã chuyển hóa từ nhận thức thành văn hóa doanh nghiệp qua các biện pháp cụ thể: Truyền thông nội bộ (Bản tin hàng tuần, hình ảnh minh họa rủi ro mới; Hội thảo định kỳ; Đào tạo chéo giữa lĩnh vực OT và IT. Những sáng kiến này giúp nâng cao kỹ năng nhận diện rủi ro và từng bước xây dựng "Văn hóa ATTT ".

Đi đầu kiến tạo mô hình vận hành số trong ngành năng lượng

Đến hết năm 2025, EVN cơ bản hoàn thành các nhiệm vụ chuyển đổi số giai đoạn 2021 - 2025. Hiện 100% dịch vụ điện được cung cấp trực tuyến mức độ 4 trên Cổng Dịch vụ công Quốc gia và các cổng dịch vụ công địa phương; tỷ lệ thanh toán không dùng tiền mặt đạt trên 96%, với giá trị tiền thu chiếm gần 99%. Gần như toàn bộ yêu cầu dịch vụ điện được tiếp nhận, xử lý qua các nền tảng số. Các hệ thống lõi dùng chung được đầu tư, nâng cấp đồng bộ, tiêu biểu là hệ thống quản lý thông tin khách hàng CMIS 4.0, cùng việc đẩy mạnh lắp đặt công tơ điện tử (đạt gần 90% toàn EVN) - tạo nền tảng dữ liệu tập trung phục vụ quản lý, điều hành và hoạch định chính sách nội bộ.

Trong quản trị doanh nghiệp, EVN từng bước hình thành hệ sinh thái số EVNConnect, kết nối thông suốt với hạ tầng số của Chính phủ, các bộ, ngành và địa phương, qua đó khai thác hiệu quả dữ liệu dùng chung, nâng cao năng lực điều hành trên cơ sở dữ liệu thời gian thực.

Ở lĩnh vực đầu tư - xây dựng, việc ứng dụng công nghệ khảo sát, thiết kế 3D, BIM, chữ ký số, hồ sơ dự án điện tử, nhật ký thi công điện tử... đã làm thay đổi căn bản phương thức quản lý dự án. Từ năm 2021, 100% các gói thầu của EVN được tổ chức đấu thầu qua mạng, góp phần tăng tính minh bạch, hiệu quả và chuẩn hóa quy trình.

Trong sản xuất - vận hành, EVN đẩy mạnh ứng dụng trí tuệ nhân tạo (AI), tin học hóa công tác sửa chữa theo phương pháp RCM/CBM, xây dựng đồng

Đại diện Tổng Công ty Điện lực miền Nam nhận giải thưởng chuyển đổi số Việt Nam 2024

bộ 63/63 trung tâm điều khiển xa; tỷ lệ trạm biến áp 220 - 110kV không người trực đạt tới 97%. Đây là bước tiến quan trọng trong hiện đại hóa lưới điện, hướng tới mô hình lưới điện thông minh, an toàn và tin cậy.

Chuyển đổi số gắn với ghi nhận, tôn vinh và lan tỏa giá trị sáng tạo

Thành tựu chuyển đổi số của EVN đã được ghi nhận bằng các giải thưởng Chuyển đổi số Việt Nam, Giải thưởng Sao Khuê, sản phẩm "Make in Viet Nam"... Đặc biệt, đầu năm 2025, EVN được cơ quan đại diện chủ sở hữu vốn nhà nước đánh giá là đơn vị dẫn đầu trong 19 tập đoàn, tổng công ty nhà nước về chuyển đổi số, với mức độ trưởng thành đạt 4/5.

Tuy nhiên, giá trị cốt lõi và bền vững hơn cả chính là nguồn lực con người. Thông qua các phong trào thi đua, đặc biệt là chương trình "10 nghìn sáng kiến" hưởng ứng lời kêu gọi "1 triệu sáng kiến" của Tổng Liên đoàn Lao động Việt Nam, nhiều nhân tố tiêu biểu đã được phát hiện, bồi dưỡng và lan tỏa.

Trong giai đoạn 2025 - 2030, công cuộc chuyển đổi số tại EVN tiếp tục được triển khai bám sát tinh thần Nghị quyết số 57-NQ/TW của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia. EVN đang từng bước khẳng định vai trò doanh nghiệp nhà nước tiên phong trong ứng dụng khoa học công nghệ, đổi mới sáng tạo, không chỉ bảo đảm an ninh năng lượng quốc gia mà còn đồng hành, "trợ lực" cho tiến trình phát triển bền vững của đất nước trong kỷ nguyên số.

Tự chủ công nghệ an ninh mạng - trụ cột chiến lược trong tầm nhìn Trung tâm số và AI của VNPT

Thủy Nguyên - Thanh Hường

Chuyển đổi số đang đưa Việt Nam bước vào một giai đoạn phát triển mới, nơi dữ liệu, nền tảng số và trí tuệ nhân tạo trở thành nguồn lực cốt lõi của tăng trưởng. Trong bức tranh đó, an ninh mạng đã vươn lên thành điều kiện tiên quyết bảo đảm sự vận hành an toàn, liên tục và tin cậy của Chính phủ số, kinh tế số và xã hội số. Đối với VNPT, an ninh mạng được xác định là trụ cột chiến lược, gắn chặt với tầm nhìn xây dựng Trung tâm số và triển khai chiến lược AI-first trong giai đoạn phát triển mới.

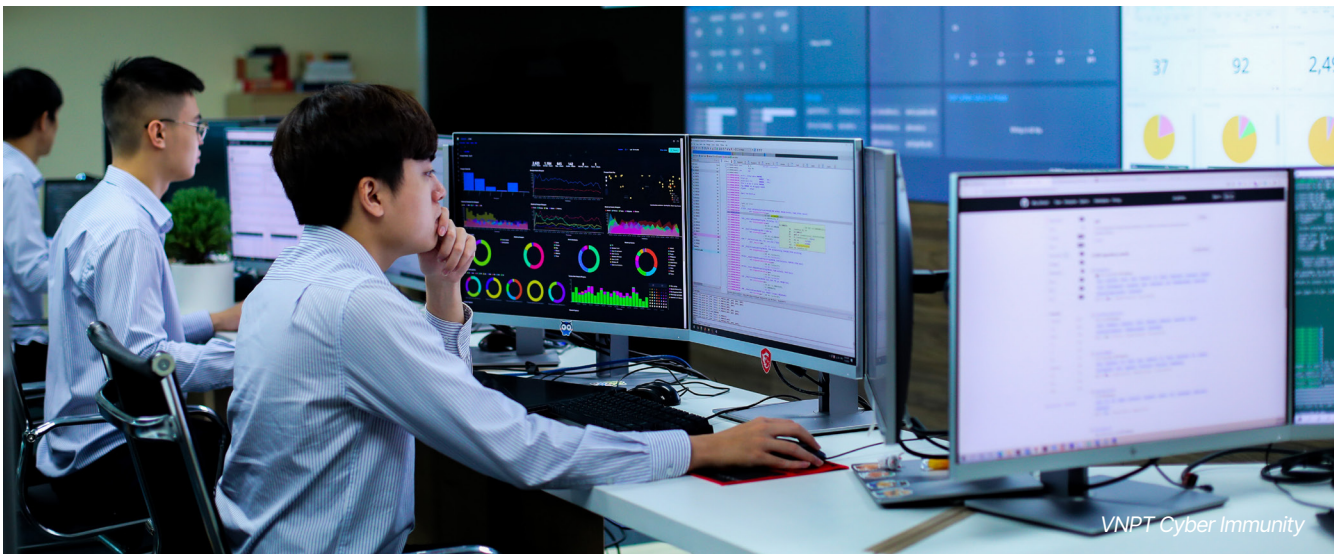
An ninh mạng trong kỷ nguyên AI: từ rủi ro kỹ thuật đến thách thức chiến lược

Sự bùng nổ của trí tuệ nhân tạo, đặc biệt là Generative AI, đang làm thay đổi sâu sắc cấu trúc không gian mạng. AI mở ra khả năng tự động hóa, tối ưu vận hành và sáng tạo ở quy mô chưa từng có, song đồng thời cũng trở thành "chất xúc tác" khiến các mối đe dọa mạng gia tăng cả về mức độ tinh vi lẫn tốc độ lan truyền. Những rào cản kỹ thuật từng khiến tấn công mạng trở nên khó khăn nay bị hạ thấp đáng kể khi AI có thể hỗ trợ tạo mã độc biến thể, dựng kịch bản lừa đảo tinh vi, hay tổ chức các chiến dịch tấn công có chủ đích với chi phí thấp nhưng hiệu quả cao.

Thực tiễn quốc tế cho thấy, ransomware quy mô lớn và tấn công chuỗi cung ứng đang nổi lên như hai mối đe dọa mang tính hệ thống. Không chỉ gây gián đoạn hoạt động của từng tổ chức, các cuộc tấn công này còn có khả năng tạo hiệu ứng lan truyền, làm tê liệt cả một hệ sinh thái số. Trong bối cảnh đó, an ninh mạng không còn là câu chuyện của từng đơn vị riêng lẻ, mà trở thành vấn đề an ninh kinh tế, an ninh xã hội và an ninh quốc gia.

Tự chủ công nghệ an ninh mạng là nền tảng của chủ quyền số

Trung tâm số không đơn thuần là tập trung hạ tầng, dữ liệu và nền tảng công nghệ. Cốt lõi của Trung tâm số là khả năng vận hành an toàn, tin cậy và bền bỉ trước mọi kịch bản rủi ro trên không gian mạng. Một Trung tâm số chỉ thực sự có giá trị khi an ninh mạng được thiết kế ngay từ đầu như năng lực nội sinh, chứ


VNPT Cyber Immunity

không phải lớp gia cố bổ sung.

Điều này đòi hỏi tư duy chiến lược mới: an ninh mạng không đi sau chuyển đổi số, mà đồng hành và dẫn dắt chuyển đổi số. Trong kiến trúc Trung tâm số của VNPT, các lớp phòng thủ được tích hợp sâu vào hạ tầng, nền tảng và dịch vụ, bảo đảm dữ liệu được bảo vệ xuyên suốt vòng đời - từ thu thập, lưu trữ, xử lý đến khai thác bằng AI.

Trong bối cảnh cạnh tranh công nghệ toàn cầu ngày càng gay gắt, VNPT xác định tự chủ công nghệ an ninh mạng là nền tảng của chủ quyền số. Phụ thuộc vào công nghệ lõi bên ngoài không chỉ tiềm ẩn rủi ro về an toàn dữ liệu, mà còn hạn chế khả năng phản ứng nhanh trước các mối đe dọa đặc thù của từng quốc gia.

VNPT lựa chọn con đường phát triển hệ sinh thái an ninh mạng Make in Vietnam, trong đó các giải pháp được xây dựng dựa trên sự am hiểu sâu sắc đặc thù dữ liệu, hành vi người dùng và bối cảnh vận hành tại Việt Nam. Trọng tâm của hệ sinh thái này là VNPT Cyber Immunity, thương hiệu an ninh mạng của Tập đoàn, với định hướng xây dựng "hệ miễn dịch số" cho các hệ thống trọng yếu.

Khác với mô hình phòng thủ truyền thống dựa trên các công cụ rời rạc, cách tiếp cận "Cyber Immunity" coi an ninh mạng như một cơ thể sống - có khả năng tự phát hiện, tự thích ứng và tự phục hồi trước các mối đe dọa ngày càng phức tạp.

Trong chiến lược AI-first của VNPT, trí tuệ nhân tạo không chỉ được ứng dụng để tạo ra dịch vụ mới, mà còn đóng vai trò lõi công nghệ cho an ninh mạng. AI phòng thủ (AI for Defense) được triển khai nhằm phát hiện sớm các hành vi bất thường, phân tích tương quan sự kiện ở quy mô lớn và tự động hóa quy trình ứng cứu sự cố.

Việc rút ngắn thời gian phát hiện và phản ứng - yếu tố quyết định trong các cuộc tấn công hiện đại - giúp giảm thiểu thiệt hại và tăng khả năng phục hồi của hệ thống. AI phòng thủ cũng cho phép VNPT chuyển từ mô hình bảo mật phản ứng sang bảo mật dự báo, chủ động nhận diện rủi ro trước khi sự cố xảy ra.

Từ thực tiễn triển khai, VNPT Cyber Immunity định hình mô hình bảo mật mới cho khách hàng dựa trên năm trụ cột: Zero Trust - "không bao giờ tin tưởng, luôn luôn xác thực"; AI phòng thủ; diễn tập thực chiến gắn với yếu tố con người; bảo hiểm an ninh mạng như công cụ quản trị rủi ro tài chính; và năng lực phục hồi sau thảm họa. Đây không chỉ là bộ giải pháp kỹ thuật, mà là khung tư duy an ninh mạng phù hợp với kỷ nguyên AI.

Kết hợp hạ tầng viễn thông và an ninh mạng thành lợi thế chiến lược

Thực tế thời gian qua cho thấy các cuộc tấn công mạng thường nhắm vào "mắt xích yếu nhất", vốn là cá nhân và các đơn vị cơ sở với hạ tầng mỏng và nguồn lực hạn chế.

Vì vậy, trong chiến lược phát triển, VNPT mở rộng tầm nhìn an ninh mạng từ bảo vệ hệ thống sang bảo vệ con người trên không gian số, với định hướng Cyber Wellness - An sinh số. Theo đó, an ninh mạng

trở thành dịch vụ thiết yếu cho từng cá nhân, hộ gia đình và cộng đồng. Các giải pháp an ninh mạng được tích hợp sẵn trên thuê bao di động và đường truyền Internet, giúp người dùng được bảo vệ một cách tự nhiên, xuyên suốt trong mọi trải nghiệm số. Đặc biệt, các nhóm dễ bị tổn thương như trẻ em, người cao tuổi, người dân vùng sâu, vùng xa được đặt ở vị trí trung tâm của chiến lược an sinh số.

VNPT cũng đẩy mạnh mô hình an toàn thông tin cấp cơ sở, đưa các dịch vụ bảo mật tinh gọn, chuẩn hóa xuống tận xã, phường và đơn vị địa phương. Thay vì những hệ thống cồng kềnh, các giải pháp được cung cấp dưới dạng dịch vụ, dễ triển khai, dễ vận hành nhưng vẫn đáp ứng tiêu chuẩn quốc gia.

Một lợi thế nổi bật của VNPT là sự kết hợp giữa hạ tầng viễn thông quy mô quốc gia và năng lực an ninh mạng nội sinh. Các lớp phòng thủ được triển khai ngay tại cửa ngõ mạng, tích hợp khả năng chống tấn công từ xa trước khi luồng truy cập độc hại chạm tới hệ thống khách hàng. Vì vậy hàng chục triệu thuê bao của VNPT không chỉ cung cấp kết nối mà luôn được bảo vệ an toàn.

Đối với doanh nghiệp, mô hình Managed Security Services giúp giải quyết bài toán thiếu hụt nhân lực an ninh mạng chuyên trách. Doanh nghiệp có thể tiếp cận tiêu chuẩn bảo mật quốc tế với chi phí tối ưu, được vận hành bởi đội ngũ chuyên gia Việt Nam am hiểu sâu sắc bối cảnh trong nước.

Make in Vietnam và tầm nhìn vươn ra toàn cầu

Tự chủ công nghệ không chỉ phục vụ thị trường trong nước, mà còn là nền tảng để VNPT từng bước vươn ra thị trường quốc tế. Hiện nay, phần lớn danh mục sản phẩm cốt lõi của VNPT Cyber Immunity được làm chủ công nghệ lõi bởi đội ngũ kỹ sư Việt Nam, thể hiện rõ triết lý: muốn bảo vệ chủ quyền số, phải sở hữu công nghệ do chính mình làm chủ.

Vì vậy, VNPT triển khai chiến lược Cyber Global, xuất khẩu tri thức an ninh mạng thông qua dịch vụ giám sát và ứng cứu sự cố, tham gia các bài kiểm thử quốc tế khắt khe, đồng thời tiếp thu xu hướng tấn công mới để làm giàu thêm "hệ miễn dịch số" trong nước.

Trong tổng thể chiến lược phát triển, VNPT Cyber Immunity không chỉ là nhà cung cấp giải pháp kỹ thuật, mà là đồng hành cùng quốc gia trên bốn trụ cột: lá chắn cho Chính phủ số; dẫn dắt hệ sinh thái Make in Vietnam; đào tạo nguồn nhân lực an ninh mạng chất lượng cao; và phổ cập an ninh mạng cho toàn dân thông qua Cyber Wellness.

Sự hội tụ của các trụ cột này đang từng bước hình thành hệ miễn dịch số quốc gia, nơi an ninh mạng không chỉ là phòng thủ, mà trở thành động lực kiến tạo niềm tin số, tạo nền tảng để Việt Nam phát triển tự chủ, an toàn và bền vững trong kỷ nguyên AI.

FPT góp phần kiến tạo "lá chắn số" quốc gia trong kỷ nguyên mới

Trong kỷ nguyên số, chủ quyền quốc gia không chỉ là đường biên địa lý, mà còn cả trên không gian mạng - nơi dữ liệu, hạ tầng số và niềm tin số trở thành tài sản chiến lược. Vì vậy, làm chủ công nghệ chiến lược đã trở thành điều kiện sống còn để mỗi quốc gia đứng vững, tự chủ và phát triển bền vững.

Là tập đoàn công nghệ, chiến lược phát triển của FPT cũng xác định thay đổi vai trò từ nhà cung cấp dịch vụ công nghệ sang chủ thể kiến tạo năng lực số quốc gia, tham gia trực tiếp vào cấu trúc bảo vệ chủ quyền trong kỷ nguyên mới.

Làm chủ công nghệ chiến lược để giữ chủ quyền số quốc gia

Thế giới đang chứng kiến sự tái cấu trúc sâu sắc của quyền lực công nghệ. Trí tuệ nhân tạo (AI) không chỉ tự động hóa lao động mà đang can dự trực tiếp vào quá trình ra quyết định; dữ liệu trở thành nguồn tài nguyên mới có giá trị chiến lược; chip bán dẫn trở thành nền tảng của mọi ngành kinh tế số; an ninh mạng quyết định khả năng tồn tại an toàn của các hệ thống trọng yếu quốc gia.

Trong bối cảnh ấy, một quốc gia không làm chủ hạ tầng số, không kiểm soát dữ liệu cốt lõi và không tự chủ công nghệ lõi sẽ đối diện nguy cơ phụ thuộc chiến lược, dù thị trường nội địa có lớn đến đâu. Chủ quyền số vì thế không còn là khái niệm trừu tượng, mà là tổng hòa của quyền kiểm soát dữ liệu, quyền vận hành hạ tầng số và quyền tự phát triển - tự bảo vệ các nền tảng công nghệ.

Nếu như giai đoạn trước, chuyển đổi số chủ yếu tập trung vào số hóa quy trình, tối ưu vận hành và nâng cao trải nghiệm dịch vụ, thì trong bối cảnh mới yêu cầu đặt ra cao hơn nhiều: phải làm chủ công nghệ chiến lược để hình thành năng lực nội sinh, bảo vệ chủ quyền số và nâng vị thế quốc gia trong chuỗi giá trị toàn cầu.

"Làm chủ" không đơn thuần là triển khai, mà là sở hữu đầy đủ năng lực thiết kế, phát triển, vận hành, bảo vệ hệ thống theo các chuẩn mực cao nhất; làm chủ dữ liệu, công nghệ lõi và đội ngũ

Ông Trương Gia Bình
Chủ tịch HĐQT FPT

nhân lực; đồng thời hình thành hệ sinh thái sản phẩm, dịch vụ đủ mạnh để triển khai ở quy mô quốc gia.

Một đặc trưng nổi bật của phòng thủ số là tốc độ và tính liên thông. Tấn công mạng không chờ quy trình; rủi ro có thể lan truyền theo chuỗi cung ứng và chỉ một điểm yếu nhỏ cũng có thể gây đứt gãy toàn hệ thống. Vì vậy, mô hình "mỗi bên làm một phần" đã không còn phù hợp.

Tư duy công - tư đồng kiến tạo ngày càng được khẳng định: Nhà nước kiến tạo thể chế, đặt hàng và định chuẩn; doanh nghiệp đầu tư R&D, phát triển nền tảng, vận hành dịch vụ; trường - viện đào tạo nguồn nhân lực; xã hội nâng cao nhận thức và kỹ năng số.

Dấu ấn "lá chắn số" Việt Nam tại Lễ mở ký Công ước Hà Nội

Lễ mở ký Công ước của Liên hợp quốc về chống tội phạm mạng (Công ước Hà Nội) tổ chức tại Hà Nội vào tháng 10/2025 đã trở thành một dấu mốc đặc biệt. Không chỉ mang ý nghĩa pháp lý quốc tế, sự kiện còn gửi đi thông điệp mạnh mẽ về vai trò chủ động và năng lực thực chất của Việt Nam trong kiến tạo không gian số an toàn, có trách nhiệm.

Việc Tập đoàn FPT tham gia Triển lãm quốc tế bên lề Lễ mở ký Công ước Hà Nội mang ý nghĩa vượt lên trên hoạt động giới thiệu sản phẩm. Đây là dịp để doanh nghiệp công nghệ hàng đầu của Việt Nam trình diễn năng lực "lá chắn số" được kiến tạo từ công nghệ lõi, trí tuệ Việt và tư duy phòng thủ chủ động, chứng minh doanh nghiệp Việt Nam có đủ năng lực tham gia giải quyết các bài toán an ninh mạng ở tầm quốc gia và quốc tế.

Chia sẻ tại sự kiện, Chủ tịch HĐQT FPT Trương Gia Bình khẳng định khi con người sống, làm việc và giao tiếp trong không gian số, an toàn – an ninh mạng trở thành vấn đề sống còn của mọi tổ chức và quốc gia. Bảo vệ an ninh mạng quốc gia không chỉ là trách nhiệm của Nhà nước, mà là sứ mệnh chung của cộng đồng doanh nghiệp công nghệ; trong đó, mô hình công – tư đồng kiến tạo chính là chìa khóa bảo vệ chủ quyền Việt Nam trên không gian số.

Hệ sinh thái bảo mật chủ động bằng AI: Nền tảng của lá chắn số

Với triết lý bảo mật chủ động, FPT đầu tư dài hạn cho nghiên cứu và phát triển, hình thành hệ sinh thái an ninh mạng ứng dụng sâu rộng AI, từ tư vấn, đào tạo đến sản phẩm, giải pháp và vận hành. Mỗi năm, doanh nghiệp triển khai hơn 1.500 dự án an ninh mạng; các giải pháp tự động hóa giúp tăng khoảng 400% tốc độ xử lý sự cố, giảm thiểu rủi ro và thiệt hại.

Hệ thống quản trị bảo mật của FPT đáp ứng nhiều tiêu chuẩn quốc tế khắt khe; các trung tâm điều hành an ninh mạng (SOC) vận hành 24/7 theo chuẩn toàn cầu; nền tảng giám sát thông minh ứng dụng AI giúp chuyển trạng thái phòng thủ từ bị động sang chủ động, cảnh báo sớm và dự báo rủi ro.

Các nền tảng, giải pháp do FPT phát triển không tồn tại rời rạc mà được thiết kế như các lớp phòng thủ bổ trợ lẫn nhau: từ giám sát, cảnh báo sớm, quản trị bề mặt tấn công, dịch vụ chuyên gia 24/7; kiểm soát định danh ra vào, đến phần cứng và chip do doanh nghiệp Việt Nam thiết kế, góp phần tăng cường tự chủ công nghệ.

Lá chắn số quốc gia chỉ bền vững khi được xây dựng trên năng lực nội sinh. Làm chủ công nghệ chiến lược không chỉ để phát triển mà để tự chủ; không chỉ để hội nhập mà để đứng vững. Đó chính là con đường để Việt Nam bảo vệ chủ quyền số, kiến tạo niềm tin số và khẳng định vị thế trong kỷ nguyên mới.

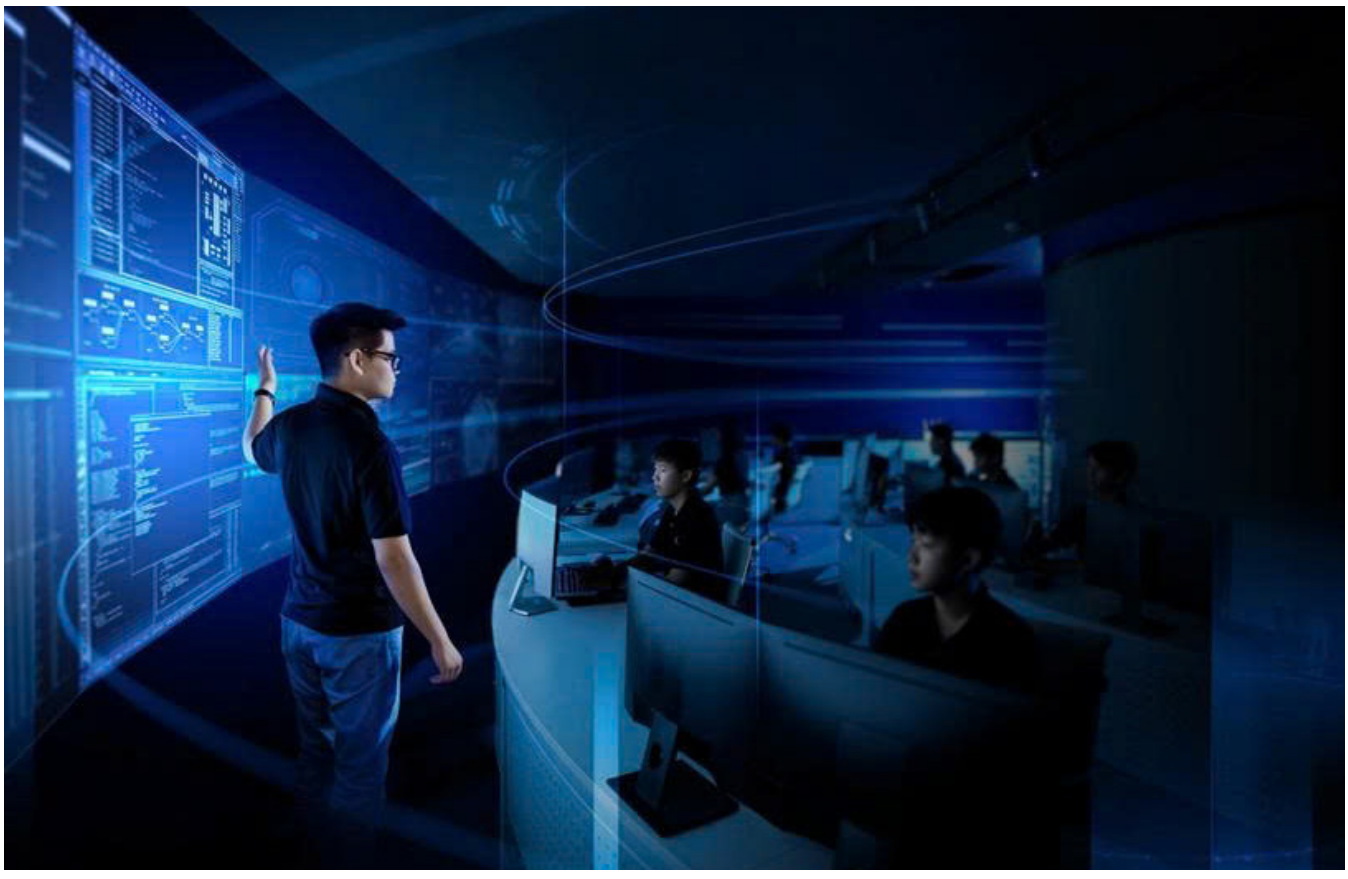
Tại Triển lãm quốc tế trong khuôn khổ Lễ mở ký và hội nghị cấp cao Công ước của Liên hợp quốc về chống tội phạm mạng (Công ước Hà Nội), Phó Thủ tướng Bùi Thanh Sơn và Phó Tổng thống Ecuador thăm gian triển lãm của FPT

AI Trong Chuyển Đổi Số: Mặt Trận An Ninh Mạng Mới Của Nhà Nước Và Doanh Nghiệp

Trí tuệ nhân tạo (AI) đang được triển khai ngày càng sâu vào quản lý nhà nước và vận hành doanh nghiệp tại Việt Nam. Khi AI đi vào lõi dữ liệu và tham gia trực tiếp vào quá trình ra quyết định, rủi ro an ninh mạng cũng mở rộng theo cấp số nhân. Nếu chuyển đổi AI không đi kèm quản trị rủi ro và an ninh ngay từ thiết kế, hệ thống số của tổ chức có thể trở nên mong manh hơn thay vì thông minh hơn.

AI đi vào lõi chuyển đổi số trong khuôn khổ pháp lý ngày càng rõ nét

Năm 2025 đánh dấu bước chuyển quan trọng của chuyển đổi số gắn với trí tuệ nhân tạo tại Việt Nam, khi AI đã vượt qua giai đoạn thử nghiệm để đi vào vận hành thực tế trong hoạt động của cơ quan nhà nước và doanh nghiệp. Theo nghiên cứu "Khai phá tiềm năng AI của Việt Nam" do Amazon Web Services phối hợp Strand Partners công bố năm 2025, khoảng 18% doanh nghiệp đã triển khai AI, với tốc độ tăng trưởng ứng dụng đạt 39% so với năm trước. Đáng chú ý, phần ớn không dừng ở thử nghiệm mà đã tích hợp AI vào các hoạt động cốt lõi như phân tích dữ liệu, tự động hóa quy trình, chăm sóc khách hàng và hỗ trợ ra quyết định. Trong nhóm doanh nghiệp



Hệ thống SOC của CMC Cyber Security ứng dụng AI hỗ trợ các tổ chức phát hiện sớm và xử lý hiệu quả các hành vi tấn công mạng ngày càng tinh vi

này, 61% ghi nhận doanh thu tăng trung bình 16%, trong khi 58% kỳ vọng tiết kiệm chi phí khoảng 20%.

Quá trình triển khai AI tại Việt Nam diễn ra trong khuôn khổ pháp lý ngày càng rõ nét, với Luật An ninh mạng 2025, Luật Bảo vệ Dữ liệu cá nhân, Luật Trí tuệ nhân tạo 2025 và định hướng từ Nghị quyết 57-NQ/TW, trong đó khoa học – công nghệ và chuyển đổi số được xác định là động lực phát triển quốc gia gắn chặt với yêu cầu bảo đảm an ninh, an toàn thông tin. Điều này cho thấy AI được thúc đẩy song hành với kiểm soát rủi ro, thay vì phát triển bằng mọi giá.

Khi AI mở ra cơ hội, rủi ro an ninh cũng nhân lên

AI mang lại lợi thế về tốc độ và khả năng khai thác dữ liệu quy mô lớn, nhưng đồng thời tạo ra các "điểm tấn công" mới. Rủi ro có thể đến từ dữ liệu (lộ lọt, sai lệch, sử dụng sai mục đích), từ mô hình (bị thao túng đầu vào, đánh cắp mô hình, đầu độc dữ liệu huấn luyện), hoặc từ vận hành (tự động hóa thiếu kiểm soát dẫn đến sai lệch lan truyền trên toàn hệ thống).

Nhận định về thực tế này, ông Trần Quốc Chính – Phó Chủ tịch Tập đoàn Công nghệ CMC, Tổng giám đốc CMC Cyber Security nhấn mạnh: "Khi AI xử lý dữ liệu ở quy mô lớn và can thiệp trực tiếp vào vận hành, rủi ro không còn dừng ở từng lỗ hổng riêng lẻ. Một sai sót trong thiết kế dữ liệu, phân quyền hay kiểm soát đầu vào có thể tạo hiệu ứng dây chuyền trên toàn hệ thống. Nếu bài toán an ninh không được đặt ra ngay từ khâu thiết kế và quản trị, AI rất dễ trở thành điểm khuếch đại rủi ro, thay vì là động lực phát triển."

Từ góc nhìn chiến lược, Chủ tịch Tập đoàn Công nghệ CMC Nguyễn Trung Chính cho biết định hướng đến năm 2028 của CMC là trở thành "một công ty chuyển đổi AI quy mô toàn cầu (A Global AI-X Company)". Theo ông, an ninh, an toàn thông tin là một mũi đột phá quan trọng trong chiến lược này, đặc biệt với các sản phẩm, dịch vụ ứng dụng AI. Khi AI đi sâu vào dữ liệu lõi và quy trình ra quyết định, "an ninh phải được thiết kế ngay từ đầu", nhằm bảo vệ niềm tin số và tạo nền tảng để mở rộng ứng dụng AI một cách an toàn.

Quản trị và kiểm soát rủi ro AI: tiếp cận theo chuẩn mực quốc tế

Quản lý rủi ro AI không thể chỉ dừng ở yêu cầu tuân thủ, mà cần được nhìn nhận như nền tảng cốt lõi bảo đảm độ tin cậy của hệ thống thông tin và dịch vụ số. Theo thông lệ quốc tế, vấn đề không chỉ là bảo mật từng công nghệ AI riêng lẻ, mà là xây dựng Hệ thống quản lý an ninh và rủi ro AI (AIMS) như một khung quản trị tổng thể, tích hợp giữa công nghệ, con người và quy trình.

Các chuẩn mực như ISO/IEC 42001:2023 xác định quản lý rủi ro là trọng tâm, bao trùm toàn bộ vòng đời AI – từ hoạch định, thiết kế, triển khai đến vận hành và cải tiến liên tục – nhằm bảo đảm rủi ro được nhận diện, đánh giá và kiểm soát một cách có hệ thống, phù hợp với mục tiêu kinh doanh, yêu cầu pháp lý và cam kết dịch vụ.

Trong thực tiễn, AIMS được triển khai theo chu trình PDCA. Giai đoạn Hoạch định (Plan) tập trung xây dựng chính sách, quy trình và xác định khẩu vị rủi ro AI. Thực thi (Do) triển khai các kiểm soát quản trị và kỹ thuật, quản lý dữ liệu, mô hình, hạ tầng, đánh giá tác động AI và giám sát an ninh. Kiểm tra (Check) theo dõi, đo lường hiệu quả vận hành và mức độ tuân thủ. Cải tiến (Act) khắc phục sai lệch, cập nhật chính sách và tinh chỉnh mô hình nhằm giảm rủi ro.

Cách tiếp cận này giúp tổ chức đáp ứng các khung quản trị AI quốc tế như AI TRiSM, NIST AI RMF và ISO/IEC 42001, đồng thời đưa quản trị rủi ro AI vào vận hành thực chất, có thể đo lường. Qua đó, AI không chỉ được bảo vệ, mà trở thành nền tảng đáng tin cậy cho chuyển đổi số bền vững.

CMC Cyber Security: Đồng hành bảo vệ chuyển đổi số và chuyển đổi AI an toàn

Trong bối cảnh AI trở thành "hạ tầng" của chuyển đổi số, an ninh được nhìn nhận không chỉ là bảo vệ từng hệ thống CNTT riêng lẻ, mà là bảo vệ dữ liệu, mô hình AI và toàn bộ quy trình vận hành. Theo hướng tiếp cận "tham gia từ sớm", CMC Cyber Security cho biết đơn vị đồng hành cùng cơ quan, doanh nghiệp ngay từ giai đoạn đánh giá và thiết kế để nhận diện rủi ro; đồng thời tăng cường năng lực giám sát, kiểm thử, phát hiện bất thường và phòng chống các hình thức tấn công mới với sự hỗ trợ của AI.

THẾ GIỚI CÔNG NGHỆ

Tinh thần kỵ binh trên chiến trường an ninh mạng

Nguyễn Khánh

Chiến tranh hiện đại không còn chỗ cho vó ngựa tung bụi trên chiến trường. Nhưng "tinh thần kỵ binh" - tốc độ, cơ động, trinh sát và đột kích chưa từng biến mất. Nó chỉ chuyển hóa, từ bánh xích và cánh quạt trực thăng đến những thuật toán trí tuệ nhân tạo (AI) đang rút ngắn thời gian ra quyết định xuống còn vài giây.

Khi chiến trường mở rộng sang không gian mạng, kỵ binh không còn là một binh chủng cụ thể, mà trở thành một tư duy tác chiến: Nhìn thấy sớm hơn, phản ứng nhanh hơn và hành động trước đối phương trong môi trường nén thời gian và bão hòa thông tin.

Khi vó ngựa nhường chỗ cho bánh xích

Trong nhiều thế kỷ, kỵ binh là biểu tượng của ưu thế chiến trường. Từ các đội kỵ sĩ châu Âu thời trung cổ, những đạo quân du mục Á - Âu cho đến kỵ binh thời cận đại, ngựa không chỉ là phương tiện di chuyển mà là nền tảng chiến thuật: trinh sát xa, đánh thọc sườn, truy kích và tạo cú sốc tâm lý. Ở những thời kỳ mà thông tin còn khan hiếm, ai nắm được tốc độ và khả năng cơ động thường làm chủ cục diện.

Tuy nhiên, đầu thế kỷ XX đã khép lại thời đại ấy. Thế chiến I với chiến tranh chiến hào, súng máy, pháo binh hạng nặng và khí độc đã phơi bày giới hạn không thể vượt qua của kỵ binh truyền thống. Không gian mở, điều kiện sống còn của kỵ binh, bị bóp nghẹt bởi thép gai và hỏa lực dày đặc. Những đợt xung phong trên yên ngựa, từng là biểu tượng của lòng dũng cảm, nhanh chóng trở thành thảm họa.

Sự suy tàn của kỵ binh không đến vì con người mất đi tinh thần chiến đấu, mà vì môi trường tác chiến đã đổi nền. Chiến tranh của kỷ nguyên công nghiệp không còn chỗ cho sinh thể mong manh như ngựa đối diện hỏa lực cơ giới. Dẫu vậy, quá trình chuyển đổi không diễn ra ngay lập tức. Trong giai đoạn giữa hai cuộc thế chiến, nhiều quân đội vẫn do dự giữa "ngựa hay xe tăng", phản ánh bản chất của một thời kỳ chuyển tiếp, cái cũ đã bộc lộ giới hạn, cái mới chưa hoàn thiện.

Đến Thế chiến II, câu trả lời trở nên dứt khoát. Bánh xích, động cơ và thép giáp thay thế vó ngựa trong vai trò mũi nhọn tiến công. Kỵ binh cưỡi ngựa rút khỏi tuyến đầu, nhường chỗ cho thiết giáp, cơ giới và không quân. Vó ngựa lùi vào lịch sử, nhưng tinh thần kỵ binh thì không.

Tinh thần kỵ binh trong những hình hài mới

Khi ngựa rời chiến trường, các nhiệm vụ cốt lõi của kỵ binh vẫn

còn nguyên: trinh sát, bảo đảm an ninh, đột kích, khai thác thắng lợi và truy kích đối phương. Điều thay đổi là phương tiện và nhịp độ ra quyết định.

Trong nửa sau thế kỷ XX, thiết giáp và cơ giới trở thành "kỵ binh mới". Trực thăng đưa cơ động lên chiều không gian thứ ba, cho phép triển khai lực lượng nhanh chóng vượt địa hình và phòng tuyến. Chiến tranh hiện đại lúc này được quyết định bởi tốc độ triển khai và khả năng tập trung lực lượng đúng thời điểm.

Bước sang thế kỷ XXI, một lần nữa, chiến tranh lại chứng kiến sự dịch chuyển mang tính bản lề. Lần này, không phải từ ngựa sang động cơ, mà từ con người sang thuật toán. Drone và các hệ thống không người lái nổi lên đúng vai trò vốn thuộc về kỵ binh: trinh sát nhanh, đánh sâu, gây bất ngờ và làm rối loạn đối phương. Chi phí thấp hơn, rủi ro nhân mạng thấp hơn, nhịp độ nhanh hơn, đó là "kỵ binh" của thời đại số.

Cuộc xung đột tại Ukraine cho thấy rõ sự "robot hóa" của tinh thần kỵ binh. Drone trinh sát, drone lảng vảng, drone cảm tử được sử dụng để phát hiện mục tiêu, tấn công chính xác và đánh vào hậu cần sâu. Đáng chú ý, nhiều hệ thống không còn phụ thuộc hoàn toàn vào liên lạc vệ tinh, mà được tích hợp thị giác máy và khả năng tự dẫn, giúp duy trì hiệu quả ngay cả trong môi trường tác chiến điện tử bị gây nhiễu mạnh. Điều đó cho thấy, ưu thế chiến trường ngày nay không còn nằm ở số lượng binh lực, mà ở khả năng làm chủ dữ liệu, thuật toán và nhịp độ ra quyết định.

Ở đây, tốc độ không còn là tốc độ di chuyển, mà là tốc độ ra quyết định. AI rút ngắn chu trình quan sát - định hướng - quyết định - hành động, biến ưu thế thông tin thành ưu thế tác chiến. Những gì kỵ binh xưa làm bằng kinh nghiệm và bản năng, nay được thuật toán hóa thành dữ liệu, mô hình và xác suất.

Ai sẽ cầm "dây cương"?

Sự phát triển của vũ khí tự hành gây chết người đẩy tinh thần kỵ binh lên một nấc mới, đồng thời làm dấy lên những tranh luận gay gắt. Khi máy móc có thể nhận dạng mục tiêu và thực hiện hành động với tốc độ vượt quá khả năng phản ứng của con người, câu hỏi đặt ra không chỉ là hiệu quả tác chiến, mà là đạo đức, pháp lý và kiểm soát.

Một nghịch lý ngày càng rõ: chính những hệ thống được ca ngợi vì độ chính xác cao lại có nguy cơ khiến chiến tranh trở nên "dễ dãi" hơn trong tính toán chính trị. Khi chi phí nhân mạng của bên sử dụng giảm xuống, ngưỡng sử dụng vũ lực có thể bị hạ thấp. Đây là mối nguy lớn của chiến tranh tương lai: rẻ hơn về chi phí trước mắt, nhưng đắt hơn về hệ quả lâu dài.

Dù vậy, dòng chảy công nghệ khó có thể đảo ngược. Các quân đội đều tìm cách tích hợp AI, tự động hóa và hệ thống không người lái vào học thuyết tác chiến, không phải để thay đổi bản chất chiến tranh, mà để giành ưu thế trong môi trường ngày càng phức tạp và nén thời gian.

Tinh thần kỵ binh trong lực lượng an ninh mạng Việt Nam

Sự chuyển hóa của tinh thần kỵ binh không chỉ diễn ra trên các chiến trường vật lý, mà còn thể hiện rõ trong cách tổ chức và vận hành lực lượng an ninh mạng Việt Nam.

Không gian mạng là nơi ranh giới giữa thời bình và xung đột bị xóa nhòa. Một cuộc tấn công mạng có thể diễn ra trong vài phút, lan rộng trong vài giờ và để lại hệ quả lâu dài nếu không được phát hiện kịp thời. Trong bối cảnh đó, tốc độ phát hiện, khả năng cơ

động kỹ thuật và sự linh hoạt trong điều hành trở thành yếu tố sống còn - đúng với tinh thần trinh sát và đột kích của kỵ binh xưa.

Thực tiễn cho thấy, phòng thủ thụ động không còn đủ. Các cuộc tấn công có chủ đích, chiến dịch lừa đảo quy mô lớn, tấn công chuỗi cung ứng hay việc lạm dụng AI để tạo nội dung giả mạo đều đòi hỏi năng lực chủ động phát hiện, truy vết và khoanh vùng rủi ro từ sớm. Đây chính là biểu hiện hiện đại của tinh thần kỵ binh: đi trước nguy cơ, không chờ sự cố xảy ra mới phản ứng.

Điểm đáng chú ý là sự thích ứng này không chỉ nằm ở công nghệ, mà ở tư duy tác chiến và kỷ luật vận hành. Trong không gian mạng, mối đe dọa có thể đến từ bên ngoài, nhưng cũng có thể bắt nguồn từ sai sót nội bộ, yếu tố con người hoặc chuỗi cung ứng dịch vụ. Vì vậy, tinh thần kỵ binh thời số không đồng nghĩa với liều lĩnh, mà là nhanh nhưng có kiểm soát, cơ động trong khuôn khổ kỷ luật.

Việc ứng dụng AI, tự động hóa và phân tích dữ liệu lớn giúp rút ngắn mạnh mẽ chu trình "phát hiện - đánh giá - can thiệp". Tuy nhiên, cách tiếp cận nhấn mạnh vai trò kiểm soát cuối cùng của con người. AI là công cụ tăng tốc và hỗ trợ ra quyết định, không thay thế trách nhiệm con người trong các quyết định liên quan đến an ninh, pháp lý và xã hội.

"KỴ BINH" TRÊN KHÔNG GIAN MẠNG

Tinh thần kỵ binh trong an ninh mạng được thể hiện qua bốn năng lực cốt lõi:

***Trinh sát sớm:** giám sát liên tục, phân tích tình báo mạng.*

***Cơ động kỹ thuật:** khả năng cô lập, phân vùng và tái cấu hình hệ thống nhanh.*

***Can thiệp nhanh:** phản ứng sự cố tốc độ cao, hạn chế lan truyền.*

***Khai thác sau sự cố:** điều tra số, vá lỗ hổng, nâng cao ngưỡng phòng thủ.*

AI giúp tăng tốc, nhưng mọi hành động phải đặt trong khuôn khổ pháp luật và kỷ luật vận hành.

Từ vó ngựa đến thuật toán AI, lịch sử cho thấy một quy luật xuyên suốt: môi trường tác chiến thay đổi, nhưng nhu cầu về tốc độ, cơ động và ưu thế thông tin thì không. Kỵ binh truyền thống đã hoàn thành sứ mệnh lịch sử của mình, song tinh thần kỵ binh vẫn tiếp tục chuyển hóa để thích ứng với mỗi giai đoạn phát triển của chiến tranh và an ninh.

Trong kỷ nguyên số, thách thức lớn nhất không nằm ở việc tạo ra những hệ thống nhanh và thông minh hơn, mà ở việc bảo đảm con người vẫn giữ quyền kiểm soát cuối cùng. Nếu tinh thần kỵ binh trong lịch sử gắn liền với danh dự và trách nhiệm của người kỵ sĩ, thì trong thời đại AI, giá trị ấy cần được kế thừa bằng kỷ luật, minh bạch và trách nhiệm trong không gian mạng - nơi niềm tin số đang trở thành nền tảng của an ninh và phát triển quốc gia.

AI: Chìa khoá vạn năng hay quả bom hủy diệt?

Nguyễn Khánh

Trong hành trình vươn tới những nấc thang văn minh cao hơn, nhân loại chưa bao giờ sở hữu một công cụ mạnh mẽ như Trí tuệ Nhân tạo (AI). Qua lăng kính của thang đo Kardashev, AI không đơn thuần là một phát minh công nghệ, nó xuất hiện như một "hàm số gia tốc" có thể đẩy nhanh tốc độ tiến hóa của văn minh, nhưng đồng thời cũng mang đến một nghịch lý sâu sắc. Liệu nó sẽ là chìa khóa mở cánh cửa nâng cấp nền văn minh hay chính là quả bom năng lượng kích hoạt một cuộc khủng hoảng sinh thái toàn cầu?

Thang đo Kardashev và vấn đề năng lượng

Thang đo Kardashev do nhà thiên văn học Xô viết Nikolai Kardashev đề xuất năm 1964, phân loại các nền văn minh dựa trên khả năng khai thác và sử dụng năng lượng. Một nền văn minh Cấp I có thể khai thác toàn bộ năng lượng hành tinh mình sinh sống. Cấp II là nền văn minh làm chủ toàn bộ năng lượng của một ngôi sao, trong khi nền văn minh Cấp III vận hành ở quy mô năng lượng của một thiên hà. Theo tính toán của nhà thiên văn học Carl Sagan, nhân loại mới chỉ ở khoảng 0,73 trên thang đo này. Nghĩa là chúng ta vẫn còn ở dạng một nền văn minh phụ thuộc vào các nguồn năng lượng hóa thạch hữu hạn và chưa thể quản lý hoàn toàn hệ sinh thái trên Trái Đất. Sự trỗi dậy của AI đang đóng vai trò như một "hàm số gia tốc" đối với hành trình này. Tuy nhiên, sự thúc đẩy này không chỉ có hiệu quả mà còn có thể phải trả giá.

AI đang tạo ra một làn sóng tiêu thụ điện năng chưa từng có tiền lệ trong lịch sử. Theo Cơ quan Năng lượng Quốc tế (IEA), các trung tâm dữ liệu phục vụ AI tiêu tốn tới 460-500 TWh trong năm 2024, tương đương với tiêu thụ điện của cả nước Đức (nước tiêu thụ điện năng trong top 10 thế giới). IEA cũng dự đoán, sản lượng tiêu thụ này sẽ tăng gấp đôi vào năm 2030. Kể từ khi thương mại hoá mô hình AI đầu tiên là Chat GPT vào tháng 2/2023, tiêu thụ điện toàn cầu đã gia tăng thêm 1,5% mỗi năm so với mức trung bình thập kỷ trước đó.

Dữ liệu ngôn ngữ lớn tạo nên sức mạnh của AI và cũng là nguyên nhân khiến cho nó tiêu tốn năng lượng hơn. Một truy vấn đơn giản gửi đến ChatGPT cũng tiêu tốn 2,9 Wh điện, gấp gần 10 lần so với một lượt tìm kiếm Google thông thường. Để hoàn thành cùng một nhiệm vụ, AI có thể sử dụng năng lượng gấp 33 lần so với phần mềm truyền thống. Ba gã khổng lồ Microsoft, Google và Meta cũng thừa nhận, lượng khí thải nhà kính tăng vọt kể từ năm 2020, nguyên nhân chủ yếu đến từ việc mở rộng các trung tâm dữ liệu AI. Giám đốc điều hành Nano Nuclear Energy, ông James Walker cho biết: "Một số trung tâm dữ liệu mới có thể cần tới 2 GW – tương đương mức tiêu thụ của cả một thành phố nhỏ". Sự gia tăng theo cấp số nhân của các trung tâm này đang đặt ra gánh nặng lên hệ thống hạ tầng năng lượng toàn cầu, vốn đã chịu áp lực từ quá trình điện khí hóa gần đây.

Cơn khát năng lượng bùng phát

Khi AI bùng nổ, hậu quả đầu tiên và trực tiếp nhất là sự quá tải của hệ thống lưới điện. Tại các khu vực công nghệ trọng điểm như California hay Arizona của Mỹ, lưới điện đã bộc lộ dấu hiệu căng thẳng. Ở cấp độ toàn cầu, cơn khát này còn làm trầm trọng thêm bài toán bất bình đẳng. Các quốc gia đang phát triển như tại ASEAN, nơi có nhu cầu năng lượng phục vụ phát triển, dự kiến tăng 5% mỗi năm và nhu cầu xây dựng trung tâm dữ liệu tăng hai con số như hiện nay đang đối mặt với thách thức tài chính khổng lồ. Ước tính riêng khu vực này cần tới 200 tỷ USD trong thập kỷ tới để nâng cấp hạ tầng lưới điện. Sự phát triển ồ ạt của AI trong bối cảnh hạ tầng năng lượng chưa sẵn sàng không chỉ làm trầm trọng thêm tình trạng thiếu điện tại nhiều nơi, mà còn có nguy cơ kéo dài sự phụ thuộc vào các nguồn năng lượng gây ô nhiễm, nhất là khi 60% sản lượng điện toàn cầu vẫn đến từ nhiên liệu hóa thạch.

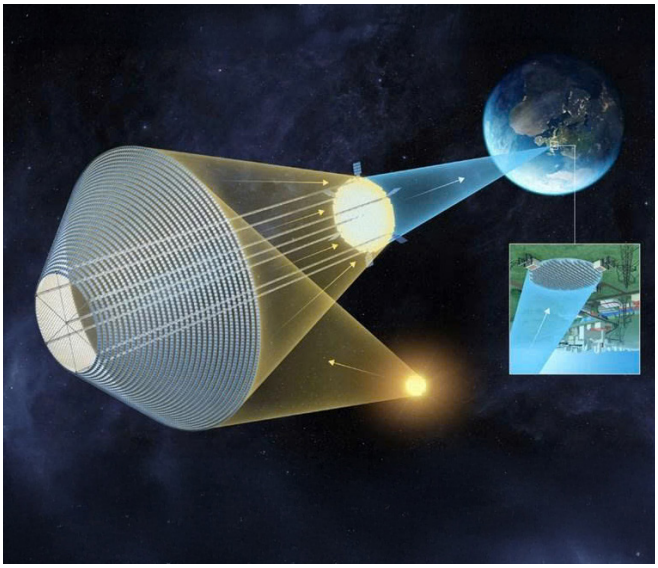
Tác động môi trường từ cơn khát năng lượng này cũng đáng báo động. Lượng khí thải carbon từ các trung tâm dữ liệu toàn cầu được dự báo sẽ chạm mốc 2,5 tỷ tấn CO_2 vào năm 2030, tương đương 40% lượng phát thải hàng năm của Mỹ. Nếu ngành công nghệ được xem như một quốc gia riêng biệt, nó sẽ lập tức trở thành nước phát thải lớn thứ 5 thế giới, vượt xa cả Brazil. Bên cạnh khí thải, AI còn "khát" nước. Các hệ thống máy chủ tiêu tốn lượng nước khổng lồ làm mát. Một trung tâm dữ liệu trung bình có thể dùng hơn 1,2 triệu lít nước/ ngày. Tình trạng này đã buộc Chính phủ Ireland, nơi có hơn 80 trung tâm dữ liệu, phải ra lệnh cấm tạm thời các dự án mới do lo ngại về an ninh nguồn nước.

Sự bùng nổ tiêu thụ năng lượng và tài nguyên này diễn ra trong một bối cảnh hết sức mong manh, khi "ngân sách carbon" của Trái Đất theo Công ước Paris đã gần cạn kiệt và AI trở thành một nhân tố đẩy nhanh quá trình đó. Nếu không được kiểm soát, chính công cụ được kỳ vọng sẽ dẫn dắt tương lai có thể trở thành tác nhân đẩy nhanh cuộc khủng hoảng sinh thái, khiến nhân loại mãi mắc kẹt trong những vấn đề của một nền văn minh cấp thấp.

Những niềm hy vọng

Tuy nhiên, bức tranh không chỉ có màu xám. Ở chiều ngược lại, nhiều học giả và nhà lãnh đạo công nghệ tin rằng AI chính là công cụ tối quan trọng để giải quyết những thách thức mà chính nó gây ra, đồng thời đẩy nhanh hành trình tiến tới ngưỡng văn minh Cấp I. Lời nhận định của nhà nghiên cứu Aditya Mohan, nhà sáng lập Robometrics, khiến chúng ta phải suy nghĩ: "Khi chúng ta cung cấp năng lượng cho AI, nó sẽ hoặc nâng cao sự phối hợp của chúng ta thành một trí tuệ hành tinh, hoặc khuếch đại sự hỗn loạn của chúng ta".

Nếu chọn con đường đầu tiên, AI có thể trở thành bộ não toàn cầu, tối ưu hóa việc sử dụng mọi nguồn lực hành tinh, nền tảng cốt lõi của một nền văn minh Cấp I.



Bước đột phá về năng lượng trong tương lai sẽ đến từ bên ngoài trái đất.

Trước hết, AI có tiềm năng thay đổi cách con người quản lý và phân phối năng lượng, biến hệ thống năng lượng toàn cầu thành một thể thống nhất và hiệu quả hơn. Diễn đàn Kinh tế Thế giới (WEF) chỉ ra rằng AI có thể giúp giảm tiêu thụ năng lượng tới 60% trong một số hệ thống nhờ vào khả năng tối ưu hóa lưu trữ và quản lý lưới điện thông minh. Nó có thể dự báo chính xác sản lượng từ các nguồn năng lượng tái tạo không ổn định như gió và mặt trời, điều phối tải một cách linh hoạt và giảm thiểu tổn thất truyền tải. Chính AI cũng đang được sử dụng để thiết kế những tấm pin mặt trời và các tua-bin gió tối ưu hơn. Các tập đoàn lớn xem sự phát triển của nguồn điện hạt nhân ổn định và linh hoạt thông qua các lò phản ứng module nhỏ (SMR) là phương án tối ưu để cấp điện cho các trung tâm dữ liệu của họ. AI đóng vai trò then chốt trong việc thiết kế, mô phỏng và vận hành an toàn những hệ thống phức tạp này.

Thứ hai, AI là vũ khí mạnh mẽ chưa từng có để giải quyết những vấn đề phức tạp ở quy mô hành tinh, như biến đổi khí hậu. Với khả năng xử lý và phân tích khối lượng dữ liệu khổng lồ, AI có thể tạo ra các mô hình dự báo khí hậu chính xác và tối ưu hóa các chiến lược giảm thiểu carbon trên toàn cầu. Nó cũng đang thúc đẩy nghiên cứu đột phá trong các lĩnh vực như vật liệu mới, thu giữ carbon và thậm chí là phản ứng nhiệt hạch. Bằng cách cung cấp những công cụ mạnh mẽ để chống lại biến đổi khí hậu, AI giúp nhân loại đủ khả năng "quản lý hoàn toàn hệ sinh thái trên Trái Đất", một đặc điểm của văn minh Cấp I mà hiện tại chúng ta muốn đạt tới.

Cùng với đó, AI chính là động lực và công cụ thúc đẩy khám phá không gian, bước tiến tất yếu để vượt qua giới hạn của hành tinh và hướng tới các cấp độ văn minh cao hơn. Khi nhu cầu năng lượng của nhân loại đạt đến giới hạn lý thuyết của Trái Đất (khoảng 173.000 terawatt), các khái niệm từng là viễn tưởng như khai thác năng lượng mặt trời trực tiếp từ không gian là lộ trình cần cân nhắc. AI sẽ đóng vai trò cốt lõi trong việc thiết kế, vận hành và bảo trì những hệ thống siêu phức tạp như vậy. Ngay ở thời điểm hiện tại, AI đã là trợ thủ đắc lực trong việc phân tích dữ liệu thiên văn, điều khiển tàu vũ trụ tự hành và tìm kiếm các nguồn tài nguyên ngoài hành tinh. Nó chính là công nghệ nền tảng sẽ biến giấc mơ chinh phục không gian, bước đệm để tiến từ văn minh Cấp I lên Cấp II, thành hiện thực.

Cuộc cách mạng AI đã đặt nhân loại trước một ngã rẽ lịch sử, được phản chiếu rõ nét qua lăng kính của Thang đo Kardashev. Một con đường dẫn tới tương lai đã mở mà ở đó AI là "công cụ tối ưu hóa vĩ đại", giúp chúng ta giải quyết vấn đề, quản lý hành tinh, mở ra kỷ nguyên khám phá vũ trụ, từng bước tiến tới văn minh mới. Con đường thứ hai lại vẽ nên một viễn cảnh u ám, nơi AI trở thành "gã khổng lồ ngốn tài nguyên", làm trầm trọng thêm khủng hoảng sinh thái, củng cố sự phụ thuộc vào nhiên liệu hóa thạch và khoét sâu hố ngăn cách giàu nghèo toàn cầu. Sự lựa chọn giữa hai kịch bản này không được định đoạt bởi số phận hay thuật toán, mà phụ thuộc vào ý chí, tầm nhìn và hành động tập thể của con người ngày hôm nay.

Hành trình tiến tới những nấc thang văn minh cao hơn không chỉ được đo bằng số terawatt năng lượng mà bằng trí tuệ và trách nhiệm mà con người sử dụng để kiến tạo tương lai đó. AI chỉ là công cụ; còn người sử dụng nó là ai và vì mục đích gì, mới là câu hỏi quyết định số phận của nhân loại.

AI được coi là điểm nổ cho nền văn minh của chúng ta

PHẦN KẾT

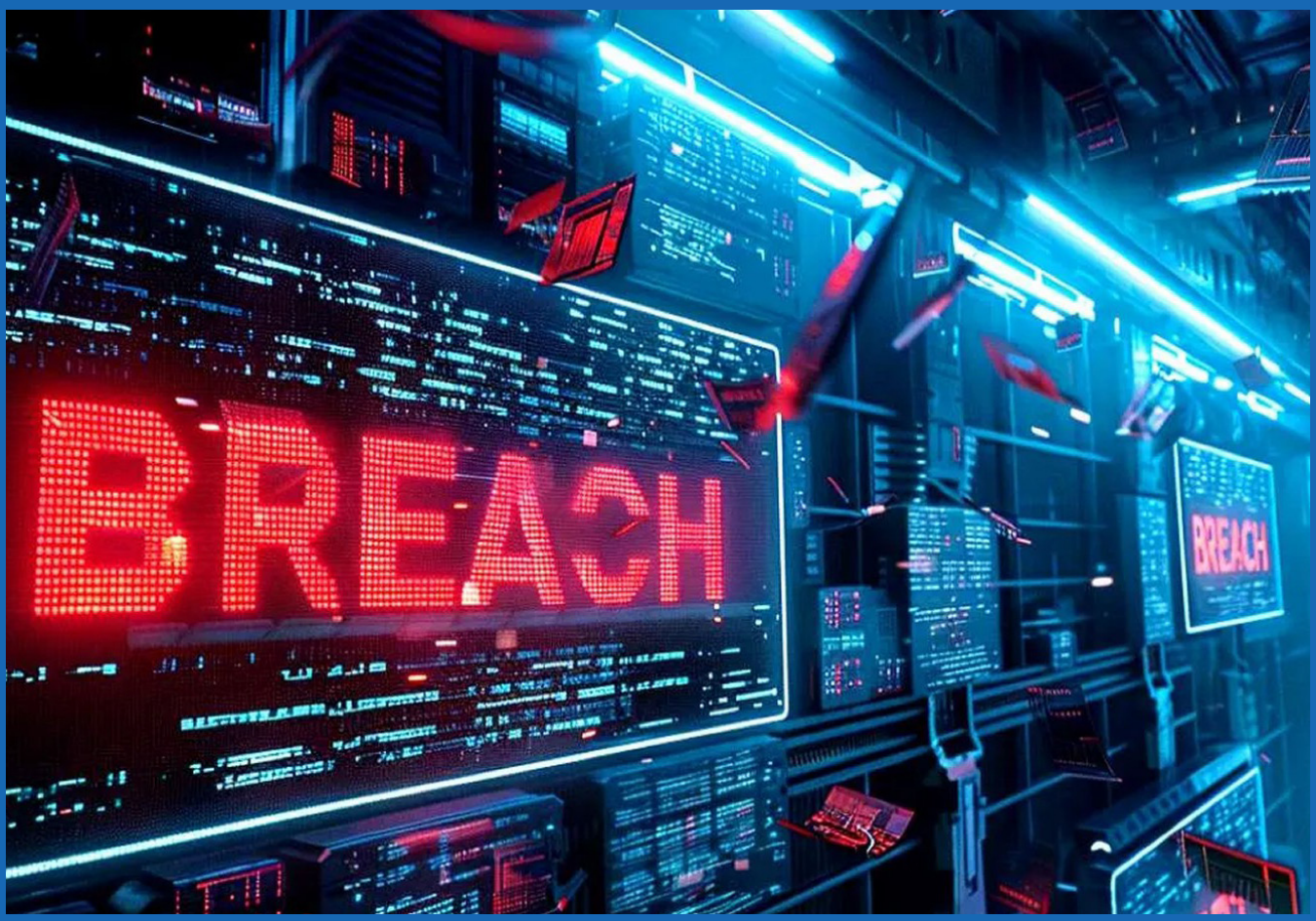
★
1. Xu hướng an ninh mạng thế giới 2026 và định hướng của Việt Nam

★
2. Năng lực thực thi- nền tảng của ổn định & phát triển Sau đại hội XIV

★
3. Xây dựng lá chắn quốc gia trên không gian mạng để đất nước phát triển bền vững

Xu hướng an ninh mạng thế giới 2026 và định hướng của Việt Nam

Ban Biên tập



Năm 2026, an ninh mạng toàn cầu bước vào một giai đoạn mới với những đặc trưng rất rõ nét: tốc độ tấn công tăng vọt, ranh giới giữa kỹ thuật, kinh tế, địa chính trị ngày càng xóa nhòa, còn trí tuệ nhân tạo (AI) trở thành "chất xúc tác" vừa giúp nâng cao năng lực phòng thủ, vừa khiến các mối đe dọa trở nên tinh vi và khó lường hơn bao giờ hết. Trong bối cảnh đó, an ninh mạng không còn là "bức tường kỹ thuật" phía sau phòng máy, mà đã trở thành một phần cốt lõi của chiến lược quốc gia, chiến lược kinh doanh và nền tảng của niềm tin xã hội vào không gian số.

AI và cuộc chạy đua vũ trang mới trên không gian mạng

Nếu phải chọn một từ khóa định hình bức tranh an ninh mạng 2026, đó chính là AI. AI không chỉ là công cụ hỗ trợ, mà đang trở thành hạ tầng trí tuệ được tích hợp sâu vào mọi lĩnh vực: tài chính, ngân hàng, y tế, giao thông, sản xuất và quản trị nhà nước.

Ở phía tấn công, AI cho phép các nhóm tội phạm mạng mở rộng quy mô và tốc độ vượt xa khả năng phản ứng thủ công của con người. Lừa đảo trực tuyến không còn những dấu hiệu thô sơ như email, tin nhắn, giọng nói và hình ảnh giả mạo được cá nhân hóa cao độ, dựa trên dữ liệu thu thập được về từng nạn nhân. Những gì trước đây đòi hỏi đội ngũ kỹ thuật lành nghề, nay có thể được tự động hóa, giúp các nhóm nhỏ hoặc cá nhân triển khai các chiến dịch tấn công có độ thuyết phục cao.

Ở chiều ngược lại, AI cũng mở ra một thế hệ trung tâm điều hành an ninh mới, nơi những chương trình AI có khả năng tự phân tích, ra quyết định và thực hiện hành động trong hệ thống có thể sàng lọc, tương quan dữ liệu và đề xuất phương án ứng phó gần như theo thời gian thực. Tuy nhiên, khi AI trở thành "thành viên" trong hệ thống, nó cũng tạo ra những rủi ro mới. Các "shadow AI agents", tác tử AI vận hành ngoài tầm quản trị chính thức, đang nổi lên như một điểm mù nguy hiểm, làm gia tăng nguy cơ rò rỉ dữ liệu, thao túng kết quả và các hình thức tấn công tinh vi thông qua prompt injection - hình thức tấn công thao túng AI bằng các chỉ dẫn được cài cắm trong dữ liệu đầu vào.

Địa chính trị, tội phạm mạng và chuỗi cung ứng số

AI không vận hành trong chân không, mà giao thoa với một thế giới đang phân mảnh mạnh mẽ về địa chính trị. Không gian mạng ngày càng trở thành mặt trận vùng xám giữa chiến tranh và hòa bình, nơi các chiến dịch do nhà nước bảo trợ, các nhóm APT và các băng nhóm tội phạm mạng xuyên quốc gia cùng tồn tại.

Tấn công mạng trong bối cảnh này không nhất thiết gây ra những thiệt hại vật lý tức thời, nhưng đủ sức làm tê liệt niềm tin vào hệ thống ngân hàng, nền tảng thanh toán, chuỗi logistics hay các dịch vụ thiết yếu. Ransomware và tống tiền dữ liệu tiếp tục vận hành như một "ngành công nghiệp", kết hợp mã hóa, đánh cắp dữ liệu, đe dọa công bố và gây áp lực đa chiều lên tổ chức, khách hàng và đối tác.

Đặc biệt, chuỗi cung ứng số trở thành điểm yếu mang tính hệ thống. Một lỗ hổng ở phần mềm, nền tảng đám mây hay tầng ảo hóa có thể tạo hiệu ứng domino, kéo theo hàng loạt tổ chức bị ảnh hưởng. Với các nền kinh tế đang số hóa nhanh, nguy cơ này không còn mang tính giả định, mà là vấn đề thời điểm.

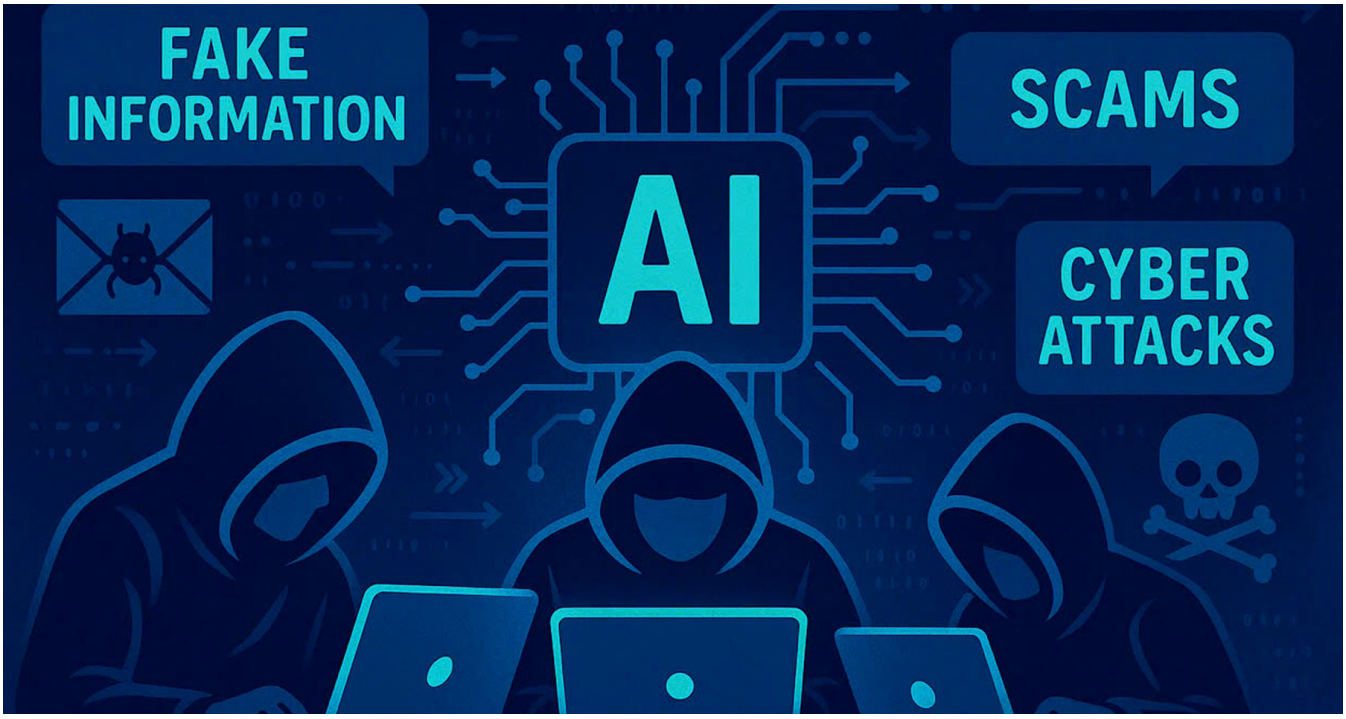
Dịch chuyển chiến lược: từ "tường lửa" sang khả năng chống chịu

Trước mức độ phức tạp ngày càng gia tăng của rủi ro, các mô hình phòng thủ truyền thống bộc lộ giới hạn. Xu hướng nổi bật của năm 2026 là dịch chuyển sang khả năng chống chịu mạng (cyber resilience) - chấp nhận rằng xâm nhập có thể xảy ra, nhưng hệ thống phải duy trì được hoạt động thiết yếu, phát hiện nhanh, khoanh vùng chính xác và khôi phục hiệu quả.

Theo đó, an ninh mạng được đưa lên bàn nghị sự của lãnh đạo cấp cao và hội đồng quản trị, được đo lường như một rủi ro chiến lược, thay vì chỉ là vấn đề kỹ thuật. Mô hình identity-first và Zero Trust trở thành hướng tiếp cận chủ đạo, coi danh tính của con người, máy móc, ứng dụng và cả tác tử AI là trung tâm của mọi quyết định truy cập.

Việt Nam 2026: dữ liệu và AI trở thành tâm điểm rủi ro

Đặt trong bối cảnh Việt Nam, năm 2026 cho thấy một sự dịch chuyển rất rõ về trọng tâm an ninh mạng. Nếu như trước đây, mối lo lớn nhất là gián đoạn hệ thống, thì nay mất kiểm soát dữ liệu mới là nguy cơ mang tính chiến lược. Dữ liệu cá nhân, dữ liệu khách hàng và dữ liệu vận hành đã trở thành "mỏ vàng" để các nhóm tội phạm mạng khai thác, đặc biệt khi AI cho phép chúng xây dựng các kịch bản tấn công có độ thuyết phục cao,



nhắm trúng từng cá nhân, từng tổ chức cụ thể.

Thực tế cho thấy, ngay cả khi hệ thống kỹ thuật được khôi phục sau sự cố, hậu quả từ việc bị xâm phạm dữ liệu vẫn có thể kéo dài, ảnh hưởng trực tiếp đến uy tín, trách nhiệm pháp lý và niềm tin của người dân, khách hàng và đối tác. Điều này khiến an ninh mạng không còn là bài toán kỹ thuật thuần túy, mà đã trở thành vấn đề quản trị và phát triển bền vững.

Trong bối cảnh chuyển đổi số diễn ra sâu rộng, năm 2026 cũng đánh dấu bước chuyển quan trọng về các chính sách liên quan đến an ninh mạng. Việc Luật Bảo vệ dữ liệu cá nhân có hiệu lực từ ngày 1/1/2026 xác lập dữ liệu cá nhân là đối tượng được bảo vệ bằng pháp luật, gắn với quyền và lợi ích hợp pháp của người dân trong kỷ nguyên số. Tiếp đó, Luật An ninh mạng 2025, có hiệu lực từ ngày 1/7/2026, hoàn thiện khung pháp lý tổng thể cho bảo vệ không gian mạng quốc gia, đặt nền tảng cho cách tiếp cận quản trị rủi ro theo cấp độ, bảo vệ hạ tầng. Với hai luật quan trọng này có hiệu lực thi hành, cho thấy, việc tuân thủ pháp luật về an ninh mạng và bảo vệ dữ liệu cá nhân không còn là lựa chọn mang tính đối phó, mà trở thành yêu cầu sống còn đối với các cơ quan, tổ chức và doanh nghiệp. Các chủ thể nắm giữ và khai thác dữ liệu buộc phải đầu tư tương xứng cho bảo vệ an ninh, an toàn thông tin.

Tuy nhiên, công nghệ và pháp lý dù quan trọng đến đâu cũng không thể thay thế vai trò của con người. Từ sự tỉnh táo của người sử dụng, trách nhiệm của doanh nghiệp đến vai trò kiến tạo và dẫn dắt của Nhà nước, an ninh mạng trong giai đoạn mới đòi hỏi cách tiếp cận toàn xã hội.

Nhìn tổng thể, bức tranh an ninh mạng thế giới năm 2026 cho thấy rõ một điều: lợi thế không thuộc về bên có nhiều công cụ nhất, mà thuộc về bên xây dựng được năng lực chống chịu vững chắc, quản trị dữ liệu hiệu quả và tận dụng AI một cách có trách nhiệm. Đối với Việt Nam, điều đó đồng nghĩa với việc coi an ninh mạng là nền tảng của niềm tin số, là điều kiện để chuyển đổi số, kinh tế số và xã hội số phát triển bền vững.

Ban Chấp hành Trung ương Đảng Cộng sản Việt Nam khoá XIV ra mắt Đại hội. Ảnh_ TTXVN

Năng lực thực thi- nền tảng của ổn định và phát triển sau Đại hội XIV

Tiến sĩ Nguyễn Sĩ Dũng

Nguyên Phó Chủ nhiệm Văn phòng Quốc hội

Đại hội đại biểu toàn quốc lần thứ XIV của Đảng đã mở ra một giai đoạn phát triển mới của đất nước với những mục tiêu cao, tầm nhìn dài hạn và yêu cầu hành động rất rõ ràng. Tuy nhiên, nhìn từ chiều sâu quản trị quốc gia, điểm mới có ý nghĩa nền tảng nhất của Đại hội không chỉ nằm ở những mục tiêu được xác lập, mà ở một thông điệp xuyên suốt và rất thực chất: *năng lực thực thi đã trở thành thước đo trung tâm của quyền lực và là điều kiện cốt lõi để bảo đảm ổn định và phát triển bền vững.*

Tinh thần ấy được cụ thể hóa rõ nét trong các chỉ đạo gần đây của Tổng bí thư Tô Lâm, với yêu cầu xuyên suốt: *nói đi đôi với làm, làm phải có kết quả, và kết quả phải đo lường được.* Tổng Bí thư nhiều lần nhấn mạnh việc khắc phục bằng được tình trạng "nói nhiều, làm ít", "nói hay, làm dở", "chủ trương đúng nhưng tổ chức thực hiện yếu", coi đây không chỉ là hạn chế trong quản lý, mà là nguy cơ trực tiếp làm suy giảm hiệu lực cầm quyền và niềm tin xã hội.

Trong bối cảnh thế giới biến động nhanh, cạnh tranh chiến lược gia tăng, các thách thức an ninh truyền thống và phi truyền thống đan xen, ổn định không thể được duy trì chỉ bằng ý chí hay tuyên bố chính trị. Ổn định chỉ bền vững khi các quyết sách đúng đắn được tổ chức thực hiện hiệu quả, đồng bộ và đến nơi đến chốn trong đời sống xã hội.

Khi thực thi được đặt vào trung tâm của tư duy lãnh đạo

Một chuyển động rất đáng chú ý của Đại hội XIV là sự dịch chuyển rõ ràng từ tư duy "đề ra chủ trương đúng" sang tư duy "tổ chức thực hiện cho bằng được chủ trương đúng". Thành công của lãnh đạo không còn được đánh giá chủ yếu ở việc ban hành bao nhiêu nghị quyết, mà ở việc nghị quyết ấy có đi vào cuộc sống hay không, có tạo ra chuyển biến thực chất hay không.

Trong tinh thần chỉ đạo mới, thực thi không còn được xem là khâu cuối cùng mang tính kỹ thuật, mà trở thành trung tâm của năng lực cầm quyền. Tổng Bí thư yêu cầu phải chấm dứt tư duy "ban hành xong là hoàn thành nhiệm vụ", thay vào đó là tư duy theo dõi, đôn đốc, kiểm tra và chịu trách nhiệm đến cùng về kết quả cuối cùng.

Đây là một sự điều chỉnh rất căn bản. Bởi lẽ, trong thực tiễn quản trị, khoảng cách giữa "đúng về chủ trương" và "đúng trong vận hành" chính là nơi dễ phát sinh trì trệ, méo mó chính sách và bào mòn niềm tin xã hội. Đại hội XIV đã đặt thẳng vấn đề vào khoảng cách ấy và coi việc thu hẹp nó là nhiệm vụ trọng tâm của giai đoạn phát triển mới.

Năng lực thực thi- nền tảng của ổn định chính trị và trật tự xã hội

Thực tiễn trong nước và kinh nghiệm quốc tế cho thấy, bất ổn xã hội hiếm khi bắt đầu từ việc thiếu chủ trương, mà thường khởi phát từ sự yếu kém trong tổ chức thực hiện. Khi chính sách đúng nhưng triển khai chậm, thiếu đồng bộ hoặc không rõ trách nhiệm, khoảng trống quản lý sẽ xuất hiện; từ đó nảy sinh bức xúc, khiếu kiện, thậm chí xung đột lợi ích.

Ngược lại, khi pháp luật và chính sách được thực thi nghiêm minh, nhất quán và hiệu quả, trật tự xã hội được giữ vững ngay từ gốc. Người dân và doanh nghiệp có thể dự đoán được hành vi của bộ máy công quyền, yên tâm đầu tư, sản xuất và tuân thủ pháp luật. Chính năng lực thực thi ấy tạo nên một "tuyến phòng thủ mềm" nhưng bền chắc cho an ninh quốc gia.

Vì vậy, từ góc độ quản trị hiện đại, năng lực thực thi không chỉ là vấn đề hành chính, mà là một trụ cột của ổn định chính trị- xã hội. Đại hội XIV đã làm rõ mối liên hệ này khi coi việc nâng cao hiệu lực, hiệu quả tổ chức thực hiện là điều kiện tiên quyết để giữ vững ổn định trong bối cảnh phát triển nhanh và hội nhập sâu.

Năng lực thực thi như một dạng kỷ luật của quyền lực

Đại biểu biểu quyết thông qua Nghị quyết Đại hội XIV của Đảng. Ảnh_ TTXVN

Một điểm nhấn rất đáng chú ý trong tư duy chỉ đạo của Tổng Bí thư thời gian qua là yêu cầu chấm dứt tình trạng né tránh, đùn đẩy trách nhiệm, sợ sai không dám làm trong một bộ phận cán bộ, công chức. Theo tinh thần đó, không thể vin vào khó khăn, vướng mắc hay quy trình để trì hoãn hành động; càng không thể để "an toàn cá nhân" làm tê liệt năng lực thực thi của bộ máy.

Thông điệp ở đây rất rõ ràng: không hành động đúng lúc cũng là một dạng vi phạm trách nhiệm quyền lực. Bộ máy công quyền được tổ chức không phải để né rủi ro, mà để giải quyết vấn đề; không phải để đứng ngoài thực tiễn, mà để dẫn dắt, tháo gỡ các điểm nghẽn của phát triển.

Tổng Bí thư đặc biệt nhấn mạnh yêu cầu xác định rõ trách nhiệm cá nhân, nhất là trách nhiệm của người đứng đầu, trong tổ chức thực hiện các chủ trương, chính sách lớn sau Đại hội XIV. Thực thi không còn là trách nhiệm chung chung của tập thể, mà phải gắn với địa chỉ cụ thể, công việc cụ thể và kết quả cụ thể. Làm tốt phải được ghi nhận; làm không đạt yêu cầu phải được chấn chỉnh, xử lý kịp thời. Kỷ luật không chỉ để xử lý vi phạm, mà để bảo đảm bộ máy luôn vận hành đúng nhịp và đúng hướng.

Đại biểu biểu quyết thông qua Nghị quyết Đại hội XIV của Đảng. Ảnh_ TTXVN

Những yêu cầu mới đối với bộ máy nhà nước sau Đại hội XIV

Đặt năng lực thực thi vào vị trí trung tâm cũng đồng nghĩa với việc đặt ra những yêu cầu mới, cao hơn đối với tổ chức và hoạt động của bộ máy nhà nước.

Trước hết, việc tinh gọn bộ máy phải đi vào thực chất, tránh hình thức, tránh "tinh gọn cơ học". Tổng Bí thư yêu cầu tinh gọn không phải để giảm đầu mối cho đẹp con số, mà để nâng cao năng lực hành động, giảm trung gian, rút ngắn thời gian xử lý công việc và tăng hiệu quả phục vụ người dân, doanh nghiệp. Tinh gọn vì thế gắn chặt với mục tiêu nâng cao năng lực thực thi, chứ không phải là một cuộc sắp xếp thuần túy về tổ chức.

Thứ hai, phân cấp, phân quyền phải đi đôi với năng lực thực tế và cơ chế kiểm soát hữu hiệu. Trao quyền mà không bảo đảm năng lực thực thi và trách nhiệm giải trình sẽ tạo ra rủi ro mới cho trật tự quản lý và pháp quyền. Do đó, yêu cầu đặt ra không chỉ là "trao quyền", mà là "trao quyền có kiểm soát và có trách nhiệm".

Thứ ba, chuẩn mực cán bộ sau Đại hội XIV không dừng lại ở việc "đúng quy trình", mà phải là làm được việc và chịu trách nhiệm về kết quả công việc. Đây là tiêu chuẩn rất cụ thể, rất thực chất, đồng thời cũng là thách thức lớn, nhưng là điều kiện không thể thiếu để nâng cao năng lực thực thi của cả hệ thống.

Năng lực thực thi- điều kiện bảo đảm cho phát triển bền vững

Đại hội XIV không chỉ đặt ra mục tiêu phát triển cao cho giai đoạn trước mắt, mà còn hướng tới những mục tiêu dài hạn đến năm 2045. Những mục tiêu ấy chỉ có thể trở thành hiện thực nếu được nâng đỡ bởi một nền tảng vững chắc của ổn định chính trị- xã hội và một bộ máy nhà nước có năng lực thực thi cao.

Có thể thấy rõ rằng, thông điệp sâu xa mà Tổng Bí thư gửi gắm sau Đại hội XIV không chỉ là lời kêu gọi đổi mới, mà là mệnh lệnh hành động đối với toàn bộ hệ thống chính trị: phải làm cho được, làm cho đến nơi đến chốn, và làm bằng kết quả cụ thể.

Khi năng lực thực thi được đặt đúng vị trí trung tâm; khi kỷ luật, trách nhiệm và hành động trở thành chuẩn mực vận hành của quyền lực; thì ổn định chính trị- xã hội sẽ không chỉ được giữ vững, mà còn trở thành nền tảng chủ động cho phát triển nhanh và bền vững. Đó chính là ý nghĩa cốt lõi, thiết thực và quyết liệt của giai đoạn phát triển mới sau Đại hội XIV.

Xây dựng lá chắn quốc gia trên không gian mạng để đất nước phát triển bền vững

Nguyễn Tất Hồng Dương

Tổng Biên tập Tạp chí An ninh mạng Việt Nam

Dữ liệu giờ đây đã trở thành tài nguyên chiến lược, trí tuệ nhân tạo phát triển nhanh chóng, không gian mạng trở thành không gian tác chiến mới, công tác bảo đảm an ninh mạng, an ninh dữ liệu, bảo mật thông tin không chỉ là nhiệm vụ kỹ thuật mà là vấn đề an ninh quốc gia, chủ quyền quốc gia, ổn định chính trị, xã hội và năng lực cạnh tranh quốc gia. Do đó, bảo vệ chủ quyền số cần được tiếp cận như một nhiệm vụ tổng hợp, những nguy cơ, thách thức về an ninh mạng phải được nhận diện và xử lý từ sớm, từ xa, sẵn sàng có các biện pháp phòng vệ tương xứng để răn đe, vô hiệu hoá các nguy cơ, bảo vệ lợi ích quốc gia - dân tộc.

Tăng tốc thực thi gắn với yêu cầu bảo đảm chủ quyền số

Nghị quyết 57/NQ-TW, ngày 22/12/2024, của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia đã xác định an ninh mạng, an ninh dữ liệu, an toàn thông tin là yêu cầu xuyên suốt, không thể tách rời trong quá trình chuyển đổi số.

Khi dữ liệu trở thành tài nguyên chiến lược, các cơ sở dữ liệu quốc gia, nền tảng số và hệ thống định danh điện tử được kết nối, chia sẻ ở quy mô lớn, thì an ninh mạng gắn trực tiếp với hiệu lực quản lý nhà nước, niềm tin của người dân và môi trường phát triển của doanh nghiệp. Do đó, bảo vệ chủ quyền số cần được tiếp cận như một nhiệm vụ tổng hợp, kết hợp giữa năng lực kỹ thuật, khung pháp lý và cơ chế phối hợp liên ngành.

Tại Hội nghị tổng kết công tác năm 2025 và triển khai nhiệm vụ năm 2026 của Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số, Tổng Bí thư Tô Lâm yêu cầu đẩy mạnh phát triển các ứng dụng, sản phẩm cụ thể phục vụ phát triển kinh tế - xã hội và người dân. Mọi chính sách, nền tảng và dịch vụ, tiện ích phải đáp ứng yêu cầu phục vụ người dân và doanh nghiệp; sự hài lòng của người dân doanh nghiệp là thước đo kết quả thực hiện. Tổng Bí thư cũng đề cập đến bảo đảm an toàn thông tin, an ninh mạng và chủ quyền số, đây là điều kiện tiên quyết để phát

Tổng Bí thư Tô Lâm phát biểu chỉ đạo tại Hội nghị tổng kết công tác năm 2025 và nhiệm vụ, giải pháp trọng tâm năm 2026 của Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số.

triển bền vững.

Ngay trước thềm Đại hội XIV của Đảng, ngày 31/12/2025, Thay mặt Ban Bí thư, đồng chí Trần Cẩm Tú, Ủy viên Bộ Chính trị, Thường trực Ban Bí thư đã ký ban hành Chỉ thị số 57-CT/TW về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị.

Cùng với Luật An ninh mạng 2025, Nghị quyết 57/NQ-TW, Chỉ thị 57- CT/TW thêm một lần khẳng định Đảng, Nhà nước đặc biệt coi trọng an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong quá trình chuyển đổi số quốc gia, triển khai Chính phủ điện tử, góp phần nâng cao hiệu lực, hiệu quả hoạt động của các cơ quan, tổ chức trong hệ thống chính trị sau sắp xếp, sáp nhập, hợp nhất, điều chỉnh địa giới hành chính và thực hiện mô hình chính quyền địa phương 2 cấp.

An ninh mạng là nền tảng để phát triển trong thời đại số

Khi trí tuệ nhân tạo làm biến đổi bản chất của tấn công mạng, khi không gian số gắn chặt với an ninh kinh tế và an ninh con người, lá chắn quốc gia phải được thiết kế để chống chịu, thích ứng và phục hồi, chứ không chỉ để ngăn chặn.

Trong kỷ nguyên mà một sự cố mạng có thể làm gián đoạn dịch vụ thiết yếu, tê liệt chuỗi cung ứng hoặc gây hoang mang xã hội chỉ trong vài giờ, an ninh mạng không còn là một hợp phần kỹ thuật nằm phía sau chuyển đổi số, mà đã trở thành năng lực cốt lõi của quản trị quốc gia, là điều kiện tiên quyết của năng lực phát triển quốc gia. Một quốc gia có thể đi nhanh đến đâu không chỉ phụ thuộc vào tốc độ số hóa, mà phụ thuộc vào khả năng bảo vệ hệ thống ấy trước các cú sốc công nghệ, tấn công xuyên biên giới và sự xói mòn niềm tin xã hội.

Năng lực ấy được đo không chỉ bằng số vụ tấn công bị ngăn chặn, mà bằng việc người dân có thể yên tâm sống, làm việc, giao dịch và tin tưởng vào tương lai số của đất nước; là cơ sở bảo đảm quốc gia có thể tăng tốc phát triển mà không phải trả giá bằng gián đoạn, mất dữ liệu hay xói mòn niềm tin xã hội.

Vì vậy, xây dựng lá chắn quốc gia trên không gian mạng là lựa chọn chiến lược mang tính chiến lược: đầu tư cho năng lực chống chịu dài hạn, cho khả năng phục hồi khi xảy ra sự cố, và cho một không gian số nơi người dân, doanh nghiệp và Nhà nước có thể cùng vận hành trên nền tảng tin cậy.

Lá chắn quốc gia trên không gian mạng phải là kiến trúc hành động thống nhất của cả hệ thống chính trị và xã hội, được vận hành đồng bộ trên bốn trụ cột.

Thứ nhất, thể chế và kỷ luật trách nhiệm, mỗi nhiệm vụ đều phải gắn với mục tiêu, lộ trình, nguồn lực và trách nhiệm rõ ràng.

Thứ hai, công nghệ và hạ tầng phòng thủ đa tầng. Công nghệ là lớp phòng thủ cứng, nhưng chỉ phát huy hiệu quả khi gắn với mục tiêu đo lường cụ thể: thời gian phát hiện, thời gian phản ứng, khả năng khôi phục và mức độ duy trì dịch vụ thiết yếu. Phòng thủ số không đo bằng số thiết bị, mà đo bằng năng lực chống chịu.

Thứ ba, cơ chế phối hợp và thế trận thống nhất. Một lá chắn quốc gia đòi hỏi sự liên thông giữa Nhà nước, doanh nghiệp, hạ tầng trọng yếu, các ngành kinh tế chủ lực. Khi sự cố xảy ra, phối hợp phải vận hành như một quy trình tác chiến, chứ không phải như một chuỗi công văn hành chính.

Thủ tướng Phạm Minh Chính thăm một số gian hàng khởi nghiệp sáng tạo tại TECHFEST Việt Nam 2025 - Ảnh: VGP

Thứ tư, con người và niềm tin số. Lá chắn quốc gia chỉ thực sự vững chắc khi người dân an toàn trên không gian mạng, dữ liệu cá nhân được bảo vệ, dịch vụ thiết yếu không gián đoạn, và sự hài lòng của Nhân dân trở thành thước đo cuối cùng của hiệu quả quản trị.

Do đó, năm 2026 là năm xác lập chuẩn vận hành mới cho an ninh mạng quốc gia: lựa chọn đúng, triển khai nhanh, làm đến nơi đến chốn, đo lường bằng kết quả; không để một ngày lãng phí, một tuần chậm trễ trong bảo vệ chủ quyền số và niềm tin xã hội.

Khi chuẩn mực ấy được thực thi nhất quán, lá chắn quốc gia trên không gian mạng sẽ không chỉ là tuyến phòng thủ trước các mối đe dọa, mà trở thành nền tảng vững chắc để Việt Nam bước vào kỷ nguyên số với tư thế chủ động, năng lực chống chịu và niềm tin bền vững.

Trong cấu trúc ấy, báo chí chuyên ngành an ninh mạng không đứng ngoài cuộc. Trách nhiệm của báo chí không chỉ là phản ánh chính sách hay cảnh báo rủi ro, mà là góp phần hình thành nhận thức xã hội đúng về an ninh mạng, thúc đẩy kỷ luật thực thi và lan tỏa tinh thần hành động trong toàn xã hội.

Tạp chí An ninh mạng Việt Nam xác định rõ vai trò đồng hành và kiến tạo diễn đàn chính sách, như một cam kết nghề nghiệp trước yêu cầu phát triển mới của đất nước.

Agribank – "Lá chắn" tin cậy giúp khách hàng bảo toàn hàng chục tỷ đồng trước vấn nạn lừa đảo số

Trong bối cảnh chuyển đổi số bùng nổ, bên cạnh những tiện ích vượt trội, gia tăng nhanh lượng giao dịch số, các thủ đoạn lừa đảo trực tuyến cũng ngày càng tinh vi. Năm 2025, với tinh thần chủ động và trách nhiệm, cán bộ Agribank trong toàn hệ thống đã kịp thời ngăn chặn nhiều vụ lừa đảo, bảo vệ an toàn hơn 17 tỷ đồng cho khách hàng, đặc biệt là nhóm yếu thế tại khu vực nông thôn.

Chuyển đổi số mang lại nhiều tiện lợi nhưng cũng trở thành "mảnh đất màu mỡ" cho tội phạm công nghệ cao. Các đối tượng liên tục thay đổi phương thức, từ giả danh cơ quan công an, viện kiểm sát để đe dọa; mời chào đầu tư tài chính lợi nhuận cao; giả mạo người thân nhờ chuyển tiền gấp; đến các kịch bản làm quen qua mạng, hứa tặng quà, đặt đơn hàng lớn hoặc lừa tiền đặt cọc.

Thực tế cho thấy, dù đã được cảnh báo rộng rãi, nhiều người dân vẫn "mắc bẫy", đặc biệt là người cao tuổi và người sinh sống tại khu vực nông thôn. Trong năm 2025, riêng Agribank Chi nhánh Thanh Hóa đã phát hiện 4 vụ việc với tổng số tiền suýt bị lừa gần 1,85 tỷ đồng; Chi nhánh Yên Bái phát hiện 5 vụ với tổng số tiền gần 700 triệu đồng.

Với thủ đoạn phổ biến là làm quen, kết thân qua mạng rồi "tặng quà". Đối tượng thường giả danh quân nhân nước ngoài, xây dựng mối quan hệ tình cảm, sau đó viện cớ gặp vướng mắc thủ tục để yêu cầu nạn nhân chuyển tiền. Trong năm qua, các giao dịch viên Agribank đã kịp thời phát hiện 7 vụ việc, giúp khách hàng tránh bị chiếm đoạt gần 1 tỷ đồng. Điển hình là tại Phòng giao dịch Hợp Minh – Chi nhánh Yên Bái, nơi giao dịch viên đã nhanh trí ngăn chặn việc chuyển 650 triệu đồng cho kẻ lừa đảo. Một thủ đoạn khác đánh vào lòng tham của người dân là giả đặt đơn hàng lớn, dẫn dụ chuyển tiền đặt cọc qua bên thứ ba. Tại Agribank Chi nhánh Bắc Quang (Hà Giang), cán bộ ngân hàng đã kịp thời phát hiện, bảo toàn gần 450 triệu đồng cho khách hàng.

Agribank – "Lá chắn đa lớp" bảo vệ tài sản khách hàng

Xác định bảo vệ tài sản của khách hàng là ưu tiên hàng đầu, Agribank đã triển khai đồng bộ nhiều giải pháp từ con người đến công nghệ. Đội ngũ giao dịch viên được đào tạo bài bản để nhận diện các dấu hiệu bất thường về tâm

lý và hành vi của khách hàng. Nhiều vụ việc đã được phát hiện ngay tại quầy giao dịch khi khách hàng có biểu hiện lo lắng, vội vã, liên tục nghe điện thoại và yêu cầu chuyển tiền gấp.

Song song với yếu tố con người, Agribank đẩy mạnh ứng dụng công nghệ nhằm tăng cường an toàn giao dịch. Các giải pháp xác thực sinh trắc học, hệ thống cảnh báo sớm giao dịch có yếu tố rủi ro được triển khai rộng khắp, giúp phát hiện và ngăn chặn rủi ro ngay từ khi giao dịch mới phát sinh. Đặc biệt, ngày 04/12/2025, Agribank và Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (Bộ Công an) ký kết chương trình phối hợp nhằm nâng cao năng lực phòng ngừa, phát hiện và xử lý rủi ro, chuyển từ thế bị động sang chủ động kiểm soát nguy cơ.

Cùng với đó, công tác truyền thông, cảnh báo cũng được Agribank chú trọng. Thông qua các kênh chính thức và tại quầy giao dịch, khách hàng được khuyến cáo không cung cấp mã OTP, mật khẩu; cảnh giác với cuộc gọi, tin nhắn lạ; xác minh kỹ thông tin trước khi chuyển tiền và liên hệ ngay với ngân hàng hoặc cơ quan công an khi có dấu hiệu nghi ngờ. Các thông điệp này đã lan tỏa rộng khắp, đặc biệt tại khu vực nông thôn thông qua mạng lưới chi nhánh và tổ vay vốn.

Có thể khẳng định, hơn 17 tỷ đồng được bảo toàn trong năm 2025 không chỉ là giá trị tài chính mà còn là minh chứng cho niềm tin của người dân đối với Agribank – ngân hàng luôn gắn bó, đồng hành và bảo vệ khách hàng trong kỷ nguyên số. Trong bối cảnh tội phạm công nghệ cao không ngừng biến đổi, sự chủ động của ngân hàng cùng với nâng cao nhận thức của người dân chính là "lá chắn" vững chắc để xây dựng môi trường tài chính an toàn, minh bạch và bền vững.

NCS
PROTECT YOUR SUCCESS

CÔNG TY CỔ PHẦN CÔNG NGHỆ AN NINH MẠNG QUỐC GIA VIỆT NAM

An ninh mạng vững chắc là nền tảng cho thành công bền vững.

CyStack Endpoint - Giải pháp DLP giúp các tổ chức chủ động ngăn chặn rò rỉ dữ liệu nội bộ

CyStack Endpoint - Giải pháp DLP giúp các tổ chức chủ động ngăn chặn rò rỉ dữ liệu nội bộ

83% doanh nghiệp từng gặp sự cố bảo mật xuất phát từ nhân sự nội bộ, không phải từ tấn công bên ngoài. Phần lớn tổ chức thiếu ngân sách, thiếu đội ngũ chuyên trách, trong khi nhiều giải pháp nước ngoài không phù hợp với bối cảnh vận hành tại Việt Nam và gần như không có hỗ trợ bản địa kịp thời.

Được phát triển để giải quyết vấn đề này, CyStack Endpoint là giải pháp quản lý thiết bị đầu cuối và bảo vệ dữ liệu nội bộ tiên phong tại Việt Nam, đồng thời thuộc nhóm hiếm hoi trong khu vực đáp ứng tốt cả yêu cầu kỹ thuật, pháp lý và vận hành thực tế. Sản phẩm cho phép tự động hóa quản lý máy tính và thiết bị di động của nhân sự, dễ triển khai - mở rộng, phù hợp với đa dạng quy mô và ngành nghề.

CyStack Endpoint giúp các tổ chức:

Bảo vệ dữ liệu nội bộ (DLP): Ngăn chặn rò rỉ dữ liệu nhạy cảm qua email, ứng dụng nhắn tin, thiết bị lưu trữ gắn ngoài; truy vết vòng đời dữ liệu (người tạo, chỉnh sửa, chia sẻ); sao lưu và khôi phục tài liệu.

Thiết lập & Thực thi chính sách bảo mật từ xa: Chặn website và ứng dụng trái phép; giám sát mức độ tuân thủ; ngăn chặn tấn công.

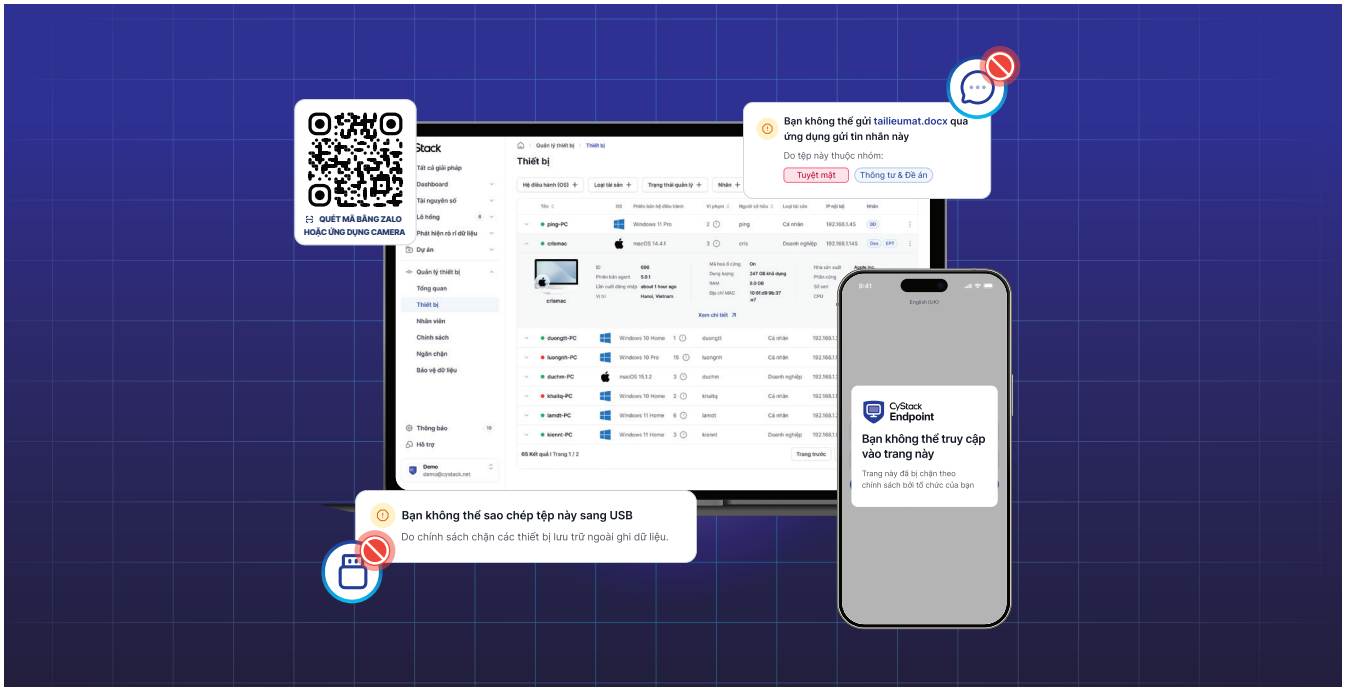
Quản lý thiết bị tập trung: Theo dõi và kiểm soát, giúp cấp phát thiết bị mới và cập nhật tình trạng nhanh chóng, minh bạch.

Định danh thiết bị gán với người dùng cùng công nghệ VPN thế hệ mới

CyStack Endpoint được xây dựng dựa trên hành vi sử dụng thực tế của người dùng Việt Nam, phát triển bởi CyStack - doanh nghiệp an ninh mạng Việt Nam được công nhận rộng rãi trong nước và quốc tế. Giải pháp nằm trong Top 10 Giải thưởng Make in Viet Nam, đạt Sao Khuê 5 sao, và được lựa chọn giới thiệu trên Cổng thông tin Nghị quyết 57 như một sản phẩm công nghệ tiêu biểu của quốc gia.

Bên cạnh đó, CyStack là thành viên được chứng nhận của CREST - tổ chức uy tín toàn cầu trong lĩnh vực an ninh mạng, bảo chứng cho năng lực kỹ thuật, quy trình, và đạo đức nghề nghiệp theo chuẩn toàn cầu.

Khám phá CyStack Endpoint qua mã QR dưới đây



Check Point - Giải pháp bảo vệ thế giới siêu kết nối trong kỷ nguyên AI

Bước vào kỷ nguyên chuyển đổi số toàn diện, không gian mạng đã trở thành một phần không thể tách rời của hạ tầng quốc gia. Cùng với cơ hội phát triển mạnh mẽ, các rủi ro an ninh mạng ngày càng gia tăng về quy mô, mức độ tinh vi và tính tổ chức, đặt ra yêu cầu cấp thiết về một nền tảng bảo mật an toàn, chủ động và tự chủ.

Trong bối cảnh đó, **Check Point** – tập đoàn an ninh mạng hàng đầu thế giới – tự hào đồng hành cùng Chính phủ, các tổ chức và doanh nghiệp Việt Nam trong hành trình **kiến tạo tương lai số an toàn.** Với hơn 30 năm kinh nghiệm và sự hiện diện tại hơn 150 quốc gia, Check Point mang đến các giải pháp bảo mật toàn diện, bảo vệ xuyên suốt từ hạ tầng mạng, trung tâm dữ liệu, cloud đến người dùng cuối.

Điểm khác biệt cốt lõi của Check Point nằm ở cách tiếp cận **bảo mật hợp nhất,** cùng khả năng ứng dụng trí tuệ nhân tạo, học máy (AI/Machine Learning) và hệ thống thông tin mối đe doạ toàn cầu (Threat Intelligence) cho phép các tổ chức quản lý, vận hành và giám sát toàn bộ hệ sinh thái công nghệ thông tin trên một nền tảng duy nhất. Từ hạ tầng mạng truyền thống, trung tâm dữ liệu, môi trường đám mây, thiết bị đầu cuối đến người dùng và ứng dụng, mọi lớp bảo mật đều được hợp nhất trong một kiến trúc thống nhất, giúp giảm độ phức tạp, tăng khả năng hiển thị và kiểm soát rủi ro một cách chủ động. Cách tiếp cận này không chỉ nâng cao hiệu quả phòng thủ, mà còn giúp tối ưu nguồn lực, giảm thiểu tối đa chi phí vận hành, giúp tạo nền tảng vững chắc cho **chuyển đổi số an toàn, linh hoạt và tự chủ trong dài hạn.**

Không chỉ cung cấp các giải pháp công nghệ, Check Point còn cam kết đồng hành lâu dài, chia sẻ tri thức, phát triển hệ sinh thái an ninh mạng và góp phần nâng cao năng lực tự chủ bảo mật cho Việt Nam. Đây chính là nền tảng quan trọng để bảo vệ dữ liệu, đảm bảo hoạt động liên tục của các hệ thống trọng yếu và giữ vững chủ quyền số quốc gia.

Nhân dịp Xuân mới, Check Point trân trọng đồng hành cùng Tạp chí trong Ấn phẩm Tết với chủ đề **"Kiến tạo tương lai số an toàn và tự chủ",** cùng lan tỏa thông điệp về vai trò then chốt của an ninh mạng – chìa khóa cho chuyển đổi số bền vững và thịnh vượng.

Lá chắn bảo vệ cơ sở hạ tầng trọng yếu quốc gia

Trong kỷ nguyên chuyển đổi số toàn diện, khi hạ tầng số đã trở thành "hệ thần kinh" của nền kinh tế và bộ máy quản trị quốc gia, an ninh mạng không còn là câu chuyện thuần túy kỹ thuật. Đó là bài toán bảo vệ chủ quyền số, bảo đảm sự vận hành liên tục của các hệ thống trọng yếu và gìn giữ niềm tin của xã hội vào không gian số - nền tảng cho sự phát triển bền vững của đất nước.

Tại Việt Nam, các lĩnh vực then chốt như tài chính, ngân hàng, năng lượng, quốc phòng, giao thông, sản xuất công nghiệp và hệ thống thông tin của các cơ quan nhà nước đang ngày càng phụ thuộc sâu vào công nghệ số. Song song với quá trình đó, bề mặt tấn công mạng mở rộng nhanh chóng, trong khi các mối đe dọa ngày càng tinh vi, ẩn sâu và khó phát hiện hơn. Thực tiễn cho thấy, nhiều sự cố nghiêm trọng xuất phát từ những "điểm vào" tưởng như an toàn: một tệp tin được trao đổi nội bộ, một thiết bị USB phục vụ vận hành kỹ thuật, hay một thành phần trong chuỗi cung ứng công nghệ.

Khi "điểm vào" trở thành mặt trận then chốt của an ninh hạ tầng

Trong môi trường vận hành của cơ sở hạ tầng trọng yếu, việc trao đổi dữ liệu và kết nối thiết bị là điều tất yếu. Tuy nhiên, chính các điểm giao tiếp này lại đang trở thành mục tiêu khai thác hàng đầu của tin tặc, đặc biệt trong bối cảnh mã độc đa hình, tấn công không dùng mã độc và việc lạm dụng trí tuệ nhân tạo ngày càng phổ biến.

Một tệp tin bị cài cắm mã độc tinh vi có thể vượt qua các biện pháp kiểm tra thông thường, âm thầm xâm nhập vào hệ thống điều khiển công nghiệp, hệ thống ngân hàng lõi hoặc mạng lưới điều hành giao thông thông minh. Khi đó, hậu quả không chỉ dừng ở gián đoạn kỹ thuật, mà có thể ảnh hưởng trực tiếp đến an ninh kinh tế, trật tự xã hội và uy tín quốc gia. Vì vậy, kiểm soát chặt chẽ các điểm xâm nhập đầu tiên của hệ thống được xem là yêu cầu nền tảng trong chiến lược xây dựng "lá chắn tự chủ" cho hạ tầng số quốc gia.

OPSWAT - Bảo vệ hạ tầng trọng yếu từ gốc rễ rủi ro

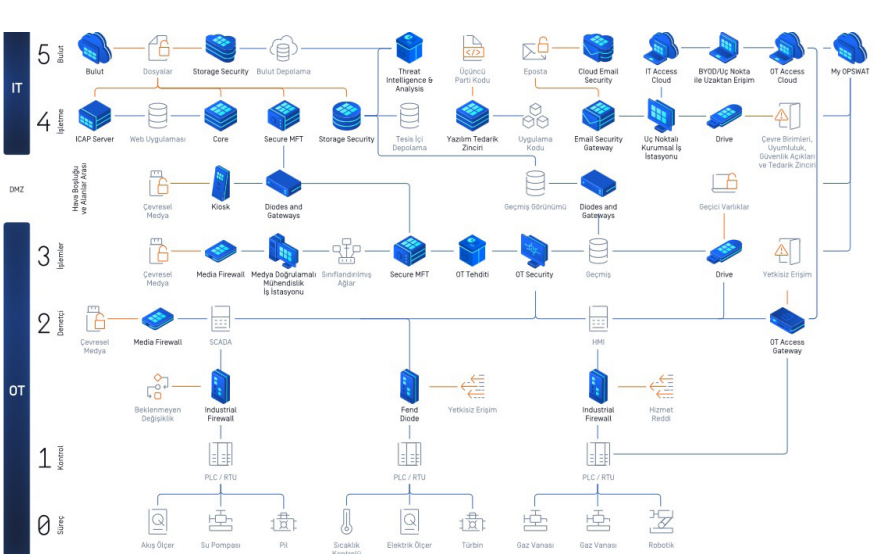
Với cách tiếp cận tập trung vào bảo vệ điểm xâm nhập, OPSWAT mang đến một hướng đi chiến lược, bổ trợ hiệu quả cho mô hình phòng thủ nhiều lớp của các hệ thống trọng yếu. Thay vì chỉ tập trung phát hiện và xử lý sự cố khi tấn công đã xảy ra, OPSWAT đặt trọng tâm vào việc ngăn chặn rủi ro tại mọi thời điểm tệp tin, thiết bị và dữ liệu tiếp cận hệ thống.

Theo đuổi triết lý "Không tin tưởng bất kỳ tập tin nào, thiết bị nào", các giải pháp của OPSWAT cho phép kiểm tra, phân tích và làm sạch tệp tin, thiết bị và dữ liệu trước khi chúng được phép đi vào hạ tầng cốt lõi. Thông qua việc kết hợp nhiều công nghệ phát hiện mã độc tiên tiến, phân tích sâu nội dung và tái cấu trúc dữ liệu an toàn, các mối đe dọa ẩn giấu được loại bỏ ngay từ đầu, đồng thời vẫn đảm bảo tính toàn vẹn và khả dụng của thông tin. Cách tiếp cận phòng thủ chủ động này đặc biệt phù hợp với các lĩnh vực trọng yếu, nơi tính an toàn, liên tục và ổn định của hệ thống luôn được đặt lên hàng đầu.

Minh chứng cho vai trò trong hệ sinh thái an ninh mạng Việt Nam

Những đóng góp của OPSWAT trong lĩnh vực bảo mật và an toàn thông tin đã được cộng đồng công nghệ Việt Nam ghi nhận. Tháng 10 năm 2025, OPSWAT Việt Nam vinh dự được Hiệp hội Phần mềm và Dịch vụ CNTT Việt Nam cùng Ban Tổ chức Chương trình Top 10 Doanh nghiệp Công nghệ & Bản đồ Doanh nghiệp Công nghệ số Việt Nam 2025 trao tặng nhiều giải thưởng danh giá. Đặc biệt, OPSWAT đã được xếp Hạng 1 trong Top 10 Doanh nghiệp Bảo mật, An toàn thông tin, khẳng định vị thế hàng đầu về năng lực công nghệ và chuyên môn trong lĩnh vực an ninh mạng.

Với năng lực công nghệ đã được kiểm chứng, đội ngũ R&D hùng hậu tại Việt Nam và cách tiếp cận phòng thủ từ gốc rễ rủi ro, OPSWAT đang đồng hành cùng hệ sinh thái an ninh mạng Việt Nam trong nỗ lực kiến tạo một không gian số an toàn, tự chủ và bền vững - nền tảng vững chắc để đất nước vươn mình mạnh mẽ trong kỷ nguyên mới.



CT Group gây ấn tượng với hai dự án UAV và LAE lớn nhất ASEAN

Với sự chứng kiến của những kênh truyền thông lớn nhất, thế giới sững sờ với bước nhảy vọt của công nghệ Việt Nam khi CT Group công bố cùng lúc hai dự án UAV và LAE lớn nhất ASEAN.

Ông Nguyễn Quốc Dũng - Đại diện CT Group công bố quyết định đầu tư Khu liên hợp UAV lớn nhất ASEAN

Ngày 29-12-2025, tại Hà Nội, trước sự chứng kiến của hơn 600 khách mời là lãnh đạo các bộ, ngành, tỉnh, thành cùng đại diện các viện nghiên cứu, các tập đoàn lớn trong nước và quốc tế, CT Group đã công bố đầu tư đồng thời hai dự án trọng điểm: Khu liên hợp UAV lớn nhất ASEAN và Trung tâm Kinh tế Không gian Tầm thấp lớn nhất ASEAN.

CT Group đã tiếp cận theo góc nhìn mới lạ để trả lời câu hỏi *"Cơ sở khoa học nào để một Tập đoàn Việt Nam đầu tư 2 dự án Công nghệ lớn của thế giới?"*. Đây không chỉ là một câu hỏi thẳng thắn mà còn là lời giải chiến lược cho các Tập đoàn khác đang tiến theo Nghị quyết 57-NQ/TW.

Thứ nhất, nắm toàn bộ các công nghệ lõi trong ngành UAV. CT Group với công ty thành viên là CT UAV đã đạt tỷ lệ nội địa hóa trung bình 87,5% trên 6 nhóm công nghệ lõi trong ngành UAV: Điện tử - Vi mạch, AI, Điều khiển & Tự hành; Vật liệu Composite, Pin; An ninh & Viễn Thông. Trong đó, hai nhóm công nghệ quan trọng nhất là Điện tử - Vi mạch và AI & Phần mềm đều đạt mức tự chủ 95%.

Thứ hai, CT UAV đã tiết lộ 3 công nghệ có tính cách mạng do chính CT UAV phát triển. Đó là công nghệ "chổi thần – cánh quạt nào cũng bay được" với khả năng tự lập trình siêu cấp, UAV có thể bay ổn định ngay với 4 cánh quạt hoàn toàn khác nhau trong khi các UAV thông thường thì cả 4 cánh quạt phải giống nhau và phải cân chỉnh rất chính xác. Công nghệ an toàn đa cấp cho phép UAV duy trì khả năng kiểm soát và hạ cánh an toàn ngay cả khi một cánh quạt gặp sự cố. Công nghệ chữa cháy tự động bằng bầy đàn UAV độc quyền. Đặc biệt là làm chủ được công nghệ khó nhất và cũng là phân khúc cao cấp nhất trong ngành - UAV chở hành khách.

Thứ ba, Tập đoàn có khả năng thích nghi linh hoạt cao tạo ra nhiều lợi thế cạnh tranh cao so với các doanh nghiệp cùng ngành trên thế giới.

Thứ tư, CT Group đã có kinh nghiệm sản xuất chế tạo, vận hành quy mô lớn với chuỗi 5 nhà máy sản xuất UAV hiện đại đang được vận hành (trên đại lộ DT743, gần ĐHQG-HCM) và để tiếp tục đáp ứng nhu cầu lớn của thị trường trong nước và quốc tế, CT Group quyết định đầu tư Khu liên hợp UAV lớn nhất ASEAN với tổng vốn đầu tư dự kiến 2 tỷ USD trong 10 năm. Đây là một thành phố công nghệ với chuỗi các nhà máy sản xuất cấu kiện UAV, viện nghiên cứu, sân bay huấn luyện – thử nghiệm, trường đại học cùng hệ sinh thái thu hút nhân tài.

Xây dựng và vận hành nhà máy thông minh: An ninh mạng là điều kiện tiên quyết!

Hiền Trâm

Trong bối cảnh ngành lọc hóa dầu chịu sức ép lớn từ biến động thị trường, xu hướng chuyển dịch năng lượng và yêu cầu ngày càng cao về chất lượng sản phẩm, an toàn và môi trường, Công ty Cổ phần Lọc hóa dầu Bình Sơn (BSR) đang đẩy mạnh chuyển đổi số theo hướng tích hợp, đồng bộ và gắn chặt với bảo đảm an toàn an ninh mạng.

Chuyển đổi số - trụ cột trong chiến lược phát triển của BSR

Chuyển đổi số ngày càng giữ vai trò quan trọng và trở thành một trong những trụ cột trong chiến lược phát triển của BSR. Mục tiêu chuyển đổi số được BSR xác định rõ ràng, hướng tới tăng trưởng doanh thu bền vững ở mức hai con số mỗi năm, đồng thời giải quyết các thách thức vận hành cụ thể trong bối cảnh doanh nghiệp phải đối mặt với nhiều thách thức như: áp lực chuyển dịch năng lượng và chuyển đổi xanh; yêu cầu tối ưu sử dụng năng lượng, giảm phát thải; tối ưu chi phí và nguồn lực; yêu cầu nâng cao năng suất lao động, tăng tính linh hoạt trong vận hành và bảo đảm tuân thủ...

Nhờ triển khai đồng bộ các sáng kiến số, BSR đã xây dựng nền tảng làm việc hợp tác hiệu quả trên toàn công ty; đồng bộ kế hoạch kinh doanh thương mại với kế hoạch sản xuất theo thời gian thực; vận hành Trung tâm Điều hành an ninh an toàn tích hợp sản xuất tập trung; tối ưu sản lượng và cơ cấu chế biến nhằm gia tăng doanh thu, lợi nhuận. Công tác giám sát hoạt động nhà máy và tình trạng thiết bị theo thời gian thực giúp phát hiện sớm bất thường, chủ động phòng ngừa rủi ro, đồng thời hỗ trợ giám sát phát thải và tối ưu năng lượng.

Với tầm nhìn rõ ràng, kế hoạch triển khai nhất quán, bảo đảm nguồn lực thực thi, những năm qua, đặc biệt năm 2025, BSR đã lập kỷ lục về sản lượng sản xuất, hiệu quả sử dụng năng lượng, doanh thu và lợi nhuận; bảo đảm tuyệt đối an toàn - an ninh - môi trường; chế biến thành công 12 loại sản phẩm mới, trong đó có

các sản phẩm phục vụ quốc phòng. Đến nay, công ty đã cán mốc gần 55 triệu giờ công an toàn.

An ninh mạng - Yếu tố "sống còn" trong vận hành nhà máy lọc hóa dầu thông minh

Đối với nhà máy lọc hóa dầu, rủi ro an ninh mạng không chỉ dừng lại ở mất dữ liệu hay gián đoạn các dịch vụ CNTT, gián đoạn sản xuất mà còn có thể dẫn đến những hậu quả nghiêm trọng như cháy nổ, hư hại lớn về thiết bị, ảnh hưởng môi trường trên diện rộng và thậm chí đe dọa tính mạng con người.

Theo ông Hoàng Ngọc Tú - Phó Giám đốc Nhà máy Lọc dầu Dung Quất (đơn vị trực thuộc BSR), để bảo đảm an toàn, an ninh mạng, các yếu tố phải được triển khai đồng bộ, cải tiến liên tục. Trong đó bao gồm: hệ thống chính sách và quản trị rủi ro; quy trình vận hành; năng lực-ý thức tuân thủ đội ngũ quản trị khai thác; kiến trúc bảo mật theo hướng phân lớp phân vùng; lựa chọn và triển khai công nghệ theo chuỗi giải pháp (tránh rời rạc); quản lý nhận diện thiết bị và người dùng; quản lý truy cập; chuẩn hóa cấu hình an toàn và kiểm soát thay đổi; bảo vệ dữ liệu, hệ thống cùng phương án sao lưu khôi phục; giám sát liên tục để phát hiện sớm; và luôn sẵn sàng kịch bản, quy trình và lực lượng ứng phó trước các mối nguy, sự cố.

Trên cơ sở đó, BSR đã ứng dụng AI trong công tác bảo đảm an ninh mạng đến từng thiết bị và người dùng, giám sát toàn diện các mối nguy từ xa, đồng thời phối hợp với các đơn vị an ninh mạng chuyên nghiệp để triển khai giám sát tập trung nhằm phát hiện sớm, ngăn chặn và xử lý kịp thời các nguy cơ tấn công.

Trung tâm điều hành An ninh - An toàn: Nền tảng quản trị hợp nhất cho nhà máy thông minh

Trong bối cảnh nhà máy vận hành ở công suất cao với chế độ vận hành linh hoạt, trong khi thiết bị ngày càng già cỗi, việc thành lập Trung tâm điều hành An ninh - An toàn và ứng phó tình huống khẩn cấp, đồng thời tích hợp quản trị nhà máy thông minh, đã giải quyết căn bản các điểm nghẽn về tập trung dữ liệu - thông tin, giám sát liên tục đồng bộ, cũng như phối hợp và ra quyết định nhanh, hiệu quả.

Ông Hoàng Ngọc Tú cho biết, Trung tâm giúp công tác quản lý, điều hành nhà máy hiệu quả hơn nhờ cơ chế phối hợp nhanh chóng, chặt chẽ và đồng bộ giữa các lực lượng và bộ phận: vận hành, bảo dưỡng, kiểm soát an toàn - chất lượng và đảm bảo an ninh. Qua đó, các vấn đề được phát hiện sớm, xử lý nhanh, hạn chế tối đa tình trạng đứt gãy thông tin hoặc xử lý rời rạc giữa lực lượng bảo vệ, giám sát an toàn, vận hành và bảo dưỡng sửa chữa.

Trung tâm đã tích hợp các mảng vốn rời rạc như đảm bảo an ninh, đảm bảo an toàn, vận hành sản xuất, bảo dưỡng sửa chữa, quản lý nhân sự, quản lý tài sản, thông tin chuyển tiếp... thành một nền tảng duy nhất. Mô hình này đã góp phần quan trọng giúp nhà máy duy trì gần 55 triệu giờ công an toàn và hiện thực hóa mục tiêu "4 không": Không có sự cố tai nạn lao động mất ngày công; Không có sự cố cháy nổ, mất an toàn công nghệ; Không có sự cố an ninh; Không vi phạm quy định về đảm bảo môi trường.

Đối với mô hình nhà máy thông minh, việc ứng dụng AI và dữ liệu lớn đã trở thành nền tảng cốt lõi để bảo đảm vận hành an toàn, ổn định và hiệu quả. BSR đang ứng dụng dữ liệu lớn và AI trong việc xây dựng mô hình Digital Twin để mô phỏng, đánh giá toàn diện về kỹ thuật, an toàn, chất lượng sản phẩm, hiệu quả kinh tế trước khi áp dụng vào sản xuất; Ứng dụng AI và Digital Twin vào tối ưu sản xuất, gia tăng lợi nhuận từ sản xuất theo thời gian thực; Ứng dụng dữ liệu lớn hợp nhất để xây dựng hệ thống báo cáo quản trị thông minh theo thời gian thực trên mọi lĩnh vực ở cấp Công ty, Ban chức năng.

Trung tâm điều hành tích hợp cũng là nền tảng để BSR phát triển và kết nối các trung tâm vệ tinh chuyên sâu về sản xuất, bảo dưỡng, kinh doanh thương mại trong tương lai gần để hướng tới mô hình quản trị hợp nhất, hiện đại và bền vững.


VINCOM
VINCOM MEGA MALL
THIÊN MÃ KHAI NIÊN
Đón Xuân viên mãn

Tập Đoàn Tuấn Dung là một doanh nghiệp hoạt động trong lĩnh vực bất động sản và phát triển dự án, được thành lập từ ngày 10/12/2004 với trụ sở chính tại xã Ninh Hiệp, huyện Gia Lâm, thành phố Hà Nội.

Tập đoàn hoạt động đa dạng trong các mảng như: Mua bán và cho thuê nhà đất; Phát triển dự án bất động sản nhà ở, khu đô thị, khu du lịch nghỉ dưỡng; Xây dựng và đầu tư hạ tầng cho các dự án quy mô lớn

Trong nhiều năm hoạt động, Tuấn Dung Group không chỉ tập trung vào thị trường Hà Nội mà còn mở rộng đầu tư tại nhiều địa phương khác nhau trên cả nước. Đơn cử như việc cùng các đối tác trúng thầu dự án Khu đô thị và du lịch An Quang quy mô hơn 89 ha tại Bình Định - một minh chứng cho tầm nhìn chiến lược và năng lực phát triển dự án lớn.

Các dự án do công ty triển khai hoặc đầu tư thường hướng tới việc tạo dựng không gian sống tiện nghi, giá trị gia tăng bền vững cho cộng đồng cư dân và nhà đầu tư, góp phần tích cực vào sự phát triển đô thị và kinh tế - xã hội của các khu vực mà doanh nghiệp tham gia.

Với gần hai thập kỷ kinh nghiệm, Tuấn Dung Group đã khẳng định vị thế của mình trong lĩnh vực bất động sản như một thương hiệu am hiểu thị trường và cam kết tạo ra những giá trị sống chất lượng.

Tổ hợp APEC Phú Quốc: Những kỷ lục mới sẽ đưa Việt Nam lên bản đồ MICE thế giới

Trung tâm Hội nghị và Triển lãm với phần mái cong lấy cảm hứng từ sóng nước.

Tổ hợp APEC Phú Quốc: Dấu ấn mới đưa Việt Nam lên bản đồ MICE[1] thế giới

Với quy mô và tiêu chuẩn chưa từng có, Tổ hợp Trung tâm Hội nghị – Triển lãm và Nhà biểu diễn đa năng APEC tại Phú Quốc, do Sun Group đầu tư xây dựng, đang xác lập những kỷ lục mới về hạ tầng hội nghị – biểu diễn. Công trình không chỉ phục vụ một sự kiện đối ngoại quan trọng của quốc gia, mà còn đặt nền móng để Việt Nam vươn lên vị thế mới trên bản đồ MICE toàn cầu.

Ballroom lớn nhất thế giới

Trung tâm Hội nghị và Triển lãm APEC có tổng diện tích sàn xây dựng 157.375 m², gồm 4 tầng nổi và 1 tầng hầm, là trung tâm hội nghị lớn nhất từng được xây dựng cho một kỳ APEC tại Việt Nam. Điểm nhấn nổi bật là không gian hội nghị – triển lãm vượt nhịp 81 m không cột, diện tích 11.050 m², được xác lập là ballroom lớn nhất thế giới, vượt kỷ lục của Caesars Forum (Las Vegas, Mỹ).

So với các ballroom hàng đầu khu vực như Sands Grand Ballroom (Singapore) hay các trung tâm MICE lớn tại Thái Lan, Indonesia, không gian tại Phú Quốc thuộc nhóm lớn nhất toàn cầu, đủ điều kiện tổ chức hội nghị cấp nguyên thủ, triển lãm và sự kiện quốc tế quy mô rất lớn.

Không gian Dinner Show độc đáo trong hệ sinh thái MICE

Một điểm khác biệt hiếm có của Trung tâm Hội nghị APEC Phú Quốc là không gian Dinner Show chuyên biệt, với sức chứa 2.000 chỗ ngồi. Không gian này cho phép tổ chức tiệc tối kết hợp trình diễn nghệ thuật quy mô lớn, vượt ra ngoài mô hình gala dinner truyền thống.

Trên thế giới, phần lớn các trung tâm hội nghị lớn thường tách biệt không gian tiệc với nhà hát

[1] *MICE là từ viết tắt tiếng Anh của 4 thuật ngữ: Meeting (Hội họp), Incentive (Khen thưởng), Conference/Convention (Hội nghị/Hội thảo) và Exhibition/Event (Triển lãm/Sự kiện).*

hoặc sân khấu biểu diễn độc lập. Việc tích hợp một không gian Dinner Show chuẩn biểu diễn quốc tế ngay trong trung tâm hội nghị, được đầu tư đồng bộ về sân khấu, âm thanh và ánh sáng, là mô hình rất hiếm trong hệ thống MICE toàn cầu. Đáng chú ý, Dinner Show tại đây được định hướng dàn dựng với sự tham gia của Cirque du Soleil, cho phép vận hành các show diễn nghệ thuật chuyên nghiệp, dài hạn.

Nhà biểu diễn đa năng quy mô hàng đầu Đông Nam Á

Bên cạnh trung tâm hội nghị, Nhà biểu diễn đa năng APEC Phú Quốc là một trong những công trình biểu diễn có quy mô lớn nhất Đông Nam Á, với 4.094 chỗ ngồi. Quy mô này vượt xa phần lớn các nhà hát trong khu vực và tiệm cận tiêu chuẩn của nhiều trung tâm biểu diễn hiện đại tại châu Á.

Công trình được tư vấn thiết kế bởi SOM (Mỹ) và Apeiro, giúp nhà hát không chỉ lớn về quy mô mà còn được định vị ngay từ đầu cho việc vận hành các show diễn quốc tế dài hạn, thay vì chỉ phục vụ biểu diễn định kỳ.

Từ một sự kiện đến chiến lược dài hạn

Sau APEC, tổ hợp Trung tâm Hội nghị – Biểu diễn tại Phú Quốc được kỳ vọng sáng đèn quanh năm, trở thành điểm đến của các đại nhạc hội, show diễn quốc tế, liên hoan phim và các hội nghị toàn cầu. Với những kỷ lục về quy mô và chuẩn vận hành, công trình không chỉ phục vụ một kỳ sự kiện, mà mở ra hướng phát triển mới cho ngành MICE Việt Nam, đưa Phú Quốc và Việt Nam từng bước ghi dấu trên bản đồ MICE thế giới.

Nhà biểu diễn đa năng với phần mái lấy cảm hứng từ vảy rồng cùng 50 cột trụ, gợi nhắc truyền thuyết Con Rồng cháu Tiên của Việt Nam.

Công ty cổ phần Công Nghệ - Viễn Thông Sài Gòn hiện hành chi nhánh Thái Nguyên (The Branch Of Saigon Telecommunication & Technologies Corporation In Thai Nguyen Province) tên chi nhánh viết tắt: CN - SGT - TN.

Địa chỉ: Số nhà 381, đường Lương Ngọc Quyến, Phường Hoàng Văn Thụ, Thành Phố Thái Nguyên, Tỉnh Thái Nguyên, Việt Nam.

Ngành nghề kinh doanh của chi nhánh: Khai thác, xử lý và cung cấp nước; lắp đặt hệ thống điện; lắp đặt hệ thống xây dựng khác như lắp đặt vật tư, thiết bị truyền dẫn, đầu nối, thiết bị bảo vệ phục vụ ngành thông tin; hoạt động dịch vụ hỗ trợ kinh doanh khác còn lại chưa được phân vào đâu.


ECO RETREAT
Rừng Mai
MÙA LỄ HỘI ĐẦU TIÊN
MỘT SẢN PHẨM CỦA NHÀ SÁNG LẬP ECOPARK
TẠI BẾN LỨC, TÂY NINH

Công ty Cổ phần Xây dựng ASK Sông Lam là đơn vị cung cấp các dịch vụ về Đầu tư xây dựng, kinh doanh bất động sản - Hỗ trợ phát triển dự án - Môi giới chuyển nhượng dự án.

Với phương châm làm việc chuyên nghiệp, trách nhiệm, tận tâm kết hợp với sự hiểu biết sâu sắc về từng lĩnh vực bất động sản tại Việt Nam cũng như đặt nhu cầu, lợi ích của khách hàng lên hàng đầu, Công ty chúng tôi mong muốn góp phần vào sự thành công của quý Khách hàng!


VinWonders
Vạn Sắc
Kỳ Quan
Tết
Ngàn Trải Nghiệm
Website
vinwonders.com
19006677

VNPT

Vững bước TIÊN PHONG

Trong kỷ nguyên vươn mình của đất nước, VNPT tự hào thực hiện vai trò nòng cốt trong việc xây dựng hạ tầng số, mở ra cuộc sống hạnh phúc, kết nối, thịnh vượng muôn màu đến cho tất cả mọi người.

Hiệp hội An ninh mạng quốc gia (NCA) là tổ chức xã hội - nghề nghiệp hoạt động trong lĩnh vực an ninh mạng, được thành lập theo định hướng chiến lược của Nhà nước, với sứ mệnh kết nối, dẫn dắt và phát huy sức mạnh tổng hợp của Nhà nước - doanh nghiệp - chuyên gia – cộng đồng trong bảo đảm an ninh mạng và chủ quyền số quốc gia. NCA là tổ chức xã hội – nghề nghiệp đầu tiên ở Việt Nam hoạt động chuyên sâu trong lĩnh vực an ninh mạng ở quy mô quốc gia, giữ vai trò:

- Cầu nối chiến lược giữa cơ quan quản lý nhà nước, cộng đồng doanh nghiệp, giới chuyên gia và đối tác quốc tế;
- Diễn đàn chuyên môn có uy tín, tham gia tư vấn, phản biện chính sách và hoàn thiện hành lang pháp lý;
- Nền tảng hợp lực, thúc đẩy phát triển hệ sinh thái an ninh mạng đồng bộ, bền vững và hội nhập quốc tế.

NCA

Địa chỉ

38 Phan Đình Phùng,
Ba Đình, Hà Nội

Email

info@nca.org.vn

Bảo đảm an ninh mạng theo định hướng, chiến lược về an ninh mạng góp phần bảo vệ Tổ quốc và thúc đẩy phát triển kinh tế - xã hội của đất nước

- Nghiên cứu, phát triển công nghệ
- Tư vấn chính sách, pháp luật
- Đào tạo, phát triển, hỗ trợ hội viên
- Hợp tác quốc tế
- Vận động nguồn lực
- Truyền thông