**An toàn, an ninh mạng năm 2020:**

**Mục tiêu kép, Bảo vệ nhiều lớp phục vụ Chính phủ điện tử**

Năm 2019, mỗi giây trên không gian mạng toàn cầu trung bình có **108** cuộc tấn công mạng và **32** mã độc mới được tạo ra. Mỗi giây trên không gian mạng Việt Nam trung bình lại có **92** thông tin tiêu cực mới xuất hiện, chiếm tỷ lệ khoảng **8%**. Tỷ lệ này năm 2020 dự báo sẽ tăng. Việt Nam đang bước vào tiến trình chuyển đổi số, phát triển chính phủ số, kinh tế số, xã hội số. Vì vậy, ATANM là điều kiện cơ bản, là yếu tố sống còn, không thể tách rời. Trong nhiều tình huống, ATANM cần phải đi trước một bước.

**1. KẾT QUẢ ĐẠT ĐƯỢC ĐẾN NĂM 2019**

Năm 2019 đã ghi nhận nhiều chuyển biến tích cực. Có được kết quả này nhờ sự quyết liệt chỉ đạo của Thủ tướng Chính phủ, sự vào cuộc của các cơ quan, tổ chức, cá nhân và cộng đồng. Thủ tướng đã ban hành Chỉ thị số 14 ngày 07/6/2019 để chỉ đạo đồng bộ từ Trung ương đến địa phương, **lần đầu tiên** chỉ rõ trách nhiệm của **người đứng đầu**, đưa ra mô hình bảo vệ chuyên nghiệp theo **4 lớp**, yêu cầu các dự án CNTT phải dành tối thiểu **10%** kinh phí cho ATANM.

Trong bảng xếp hạng toàn cầu do ITU đánh giá, Việt Nam vươn lên mạnh mẽ, từ thứ **hạng 100** năm 2017 lên thứ **hạng 50** năm 2019. Việt Nam cũng được đánh giá về mã độc di động thấp thứ **2** Đông Nam Á, chỉ sau Singapore. Mạng lưới đơn vị chuyên trách về ATANM với sự tham gia rộng khắp của gần **200** cơ quan, tổ chức tại Việt Nam, đặt dưới sự điều phối chung, thống nhất của Trung tâm VNCERT thuộc Cục ATTT. Việt Nam có những chuyên gia hàng đầu thế giới đang làm ở trong nước và nước ngoài.

Cục ATTT đã triển khai một số hệ thống kỹ thuật quy mô quốc gia:

- **Hệ thống theo dõi, phát hiện xu hướng thông tin trên không gian mạng**: Cho phép theo dõi, phát hiện xu hướng thông tin nóng; phân loại thông tin theo sắc thái tích cực, tiêu cực, nguồn phát tán thông tin; giúp phát hiện, dự báo sớm biểu tình, kêu gọi tụ tập đông người.

- **Hệ thống điều phối, xử lý nguồn phát tán thông tin vi phạm pháp luật:** Kết nối với đầu mối của toàn bộ **11** nhà cung cấp dịch vụ viễn thông, Internet (ISPs) lớn của Việt Nam để điều phối, xử lý tức thời.

- **Hệ thống theo dõi, thống kê tình hình lây nhiễm mã độc**: Cho phép theo dõi, thống kê tình hình lây nhiễm mã độc đến từng máy tính.

- **Hệ thống chia sẻ và giám sát ATANM phục vụ chính phủ điện tử:** Cho phép giám sát theo hình thức gián tiếp hoặc trực tiếp (đặt cảm biến bên trong hệ thống được giám sát); cho phép chia sẻ thông tin giám sát phục vụ phân tích, cảnh báo sớm nguy cơ mất ATANM. Hệ thống đã kết nối, chia sẻ thông tin với hệ thống của **05** doanh nghiệp lớn là Viettel, VNPT, FPT, BKAV và CMC; giám sát gián tiếp cho **20/30** bộ, ngành, **51/63** địa phương; giám sát trực tiếp tại **43** điểm cho **29** cơ quan, tổ chức.

Công tác phối hợp, hiệp đồng tác chiến giữa 3 lực lượng Quốc phòng, Công an, Thông tin và Truyền thông đã có những bước tiến độ đáng kể, xử lý hiệu quả các tình huống ATANM phát sinh.

**2. BA ĐIỂM TỒN TẠI, HẠN CHẾ**

Thứ nhất, TTgCP yêu cầu nâng cao trách nhiệm của người đứng đầu, quán triệt nguyên tắc Thủ trưởng trực tiếp chịu trách nhiệm. Tuy nhiên, đến hết 2019, chỉ có **05/30** bộ, ngành, **08/63** địa phương có sự quan tâm chỉ đạo, tham gia trực tiếp của người đứng đầu. Ở cấp đơn vị chuyên trách, chỉ có **18/30** thủ trưởng đơn vị chuyên trách về CNTT của các bộ, ngành, **20/63** Giám đốc Sở TT&TT có sự quan tâm chỉ đạo, tham gia trực tiếp trong công tác ATANM.

Thứ hai, TTgCP yêu cầu mỗi cơ quan, tổ chức dành tối thiểu **10%** tổng kinh phí chi cho công nghệ thông tin để chi cho ATANM. Tuy nhiên, năm 2019, vẫn có **08/30** bộ, ngành, **37/63** tỉnh, thành phố có tỷ lệ này ở mức dưới **10%** (trong đó có **20** tỉnh, thành phố có tỷ lệ dưới **5%**).

Thứ ba, không tính Bộ Công an, Bộ Quốc phòng, gần như **100%** các bộ, ngành, địa phương hiện nay đều chưa triển khai bảo đảm ATANM theo tinh thần **“4 lớp”** như chỉ đạo của TTgCP.

Đa số các cơ quan, tổ chức dành nhiều kinh phí để mua sắm sản phẩm, giải pháp của nước ngoài nhưng không khai thác một cách hiệu quả, thậm chí không sử dụng. Đáng lưu ý, một số bộ, ngành, địa phương đã và đang triển khai dự án đầu tư trung tâm điều hành, giám sát ATANM (SOC) với kinh phí lớn, nhưng chủ yếu chỉ mua sắm thiết bị nước ngoài, dẫn đến nguy cơ lãng phí, không có đủ đội ngũ nhân lực để vận hành, khai thác hiệu quả.

**3.** **NĂM ĐỊNH HƯỚNG TRIỂN KHAI NĂM 2020**

M**ục tiêu kép**: Nâng cao mức độ bảo đảm ATANM của các cơ quan tổ chức gắn với việc thúc đẩy phát triển hệ sinh thái, làm chủ công nghệ.

**Thứ nhất, ATANM ngay từ đầu, nâng cao sức “đề kháng”**

Cơ quan, tổ chức triển khai ATANM ngay từ đầu, từ khâu thiết kế, xây dựng hệ thống, coi đây là nhiệm vụ thường xuyên, liên tục trong suốt quá trình quản lý, khai thác, vận hành hệ thống.

Nếu như cách làm cũ là: Triển khai ATANM sau khi đưa hệ thống vào vận hành hoặc sau khi xảy ra sự cố; đầu tư lớn vào giải pháp, trang thiết bị; chủ yếu mua sắm giải pháp nước ngoài. Thì cách làm mới là: ATANM ngay từ đầu, từ khi thiết kế xây dựng; tối thiểu 10% kinh phí; đầu tư hài hoà giữa giải pháp, trang thiết bị và quy trình, nhân sự; ưu tiên mua sắm giải pháp trong nước sản xuất được, có dịch vụ hỗ trợ kỹ thuật tại chỗ, kịp thời.

Nếu như cách làm cũ là: Mất bò mới lo làm chuồng. Thì cách làm mới là: Phòng bệnh hơn chữa bệnh. Người dùng cuối luôn là điểm yếu nhất của hệ thống. Chỉ cần mỗi tổ chức, cá nhân có ý thức phòng ngừa, có thói quen, kỹ năng bảo đảm ATANM tốt là đã có thể phòng ngừa đến hơn **80%** nguy cơ, rủi ro.

**Thứ hai, triển khai bảo đảm an toàn, an ninh mạng đồng bộ, nhiều lớp**

- “4 lớp” kỹ thuật: (1) Lớp mạng, (2) Lớp hệ điều hành và cơ sở dữ liệu, (3) Lớp ứng dụng và (4) Lớp thiết bị đầu cuối.

- “4 lớp” tổ chức: (1) Lực lượng tại chỗ, (2) Tổ chức hoặc doanh nghiệp giám sát, bảo vệ chuyên nghiệp, (3) Tổ chức hoặc doanh nghiệp độc lập kiểm tra, đánh giá định kỳ, (4) Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia.

**Thứ ba, triển khai giải pháp phòng chống mã độc hiệu quả**

Việc triển khai giải pháp phòng chống mã độc hiện nay vẫn chưa hiệu quả. Tỷ lệ lây nhiễm mã độc ở mức cao. Đây là nguồn gốc của các sự cố, lộ lọt thông tin. Việt Nam có những giải pháp phòng chống mã độc, phòng chống tấn công có chủ đích (APT) rất tốt, cụ thể là: BKAV, Viettel, CMC và CyRadar.

**Thứ tư, triển khai hệ thống SOC hiệu quả**

Việc triển khai hệ thống giám sát, điều hành ATANM tập trung (SOC) cho một bộ, ngành, địa phương là hết sức cần thiết. Tuy nhiên, ngay từ khi triển khai, cần nhận thức rất rõ: Việc triển khai một hệ thống SOC hiệu quả mấu chốt nằm ở đội ngũ nhân sự phân tích, vận hành, khai thác theo quy trình chuyên nghiệp. Lực lượng nhân sự này chủ yếu nằm ở các doanh nghiệp. Vì vậy, việc triển khai hệ thống SOC cần được cân nhắc trên quan điểm tổng thể, tránh việc chỉ đơn giản đầu tư, mua sắm giải pháp, trang thiết bị mà không khai thác, vận hành hiệu quả.

- Đối với các bộ, ngành, địa phương đã có dự án đầu tư, đang triển khai: Đề nghị tham vấn ý kiến của Bộ TT&TT về thiết kế kỹ thuật, bảo đảm sự hoạt động liên thông, kết nối, chia sẻ thông tin với Trung tâm Giám sát an toàn KGM quốc gia, Cục ATTT. Lựa chọn đối tác có đủ năng lực về ATANM để triển khai.

- Đối với các bộ, ngành, địa phương chưa có dự án đầu tư: Đề nghị ưu tiên triển khai theo hình thức thuê dịch vụ của doanh nghiệp một cách phù hợp, trừ những hệ thống có lưu trữ, xử lý thông tin bí mật nhà nước hoặc hệ thống không thể thuê dịch vụ của doanh nghiệp theo quy định của pháp luật. Đối với những hệ thống thông tin này, đề nghị lựa chọn một trong các đơn vị chuyên trách thuộc Bộ TT&TT, Bộ Quốc phòng, Bộ Công an để thực hiện giám sát, bảo vệ.

- Đối với các bộ, ngành, địa phương chưa có dự án đầu tư, chưa thể có kinh phí thuê dịch vụ: Đề nghị liên hệ với Cục ATTT để được tư vấn, hỗ trợ triển khai một cách phù hợp.

**Thứ năm, phát triển hệ sinh thái Việt Nam, làm chủ công nghệ**

Bộ TT&TT đã cấp phép cho **84** doanh nghiệp kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng, trong đó nổi bật là Viettel, VNPT, BKAV, CMC và FPT. Bộ TT&TT đã quy hoạch phát triển hệ sinh thái sản phẩm an toàn, an ninh mạng Việt Nam gồm **8** nhóm với **24** dòng sản phẩm chủ lực, cơ bản tạo thành một hệ sinh thái đầy đủ cho Chính phủ điện tử. Việt Nam hoàn toàn có đủ năng lực làm chủ hệ sinh thái sản phẩm ATANM.

Bộ TT&TT đã thành lập Liên minh sản xuất sản phẩm ATANM gồm khoảng **20** doanh nghiệp. Trong năm 2020, Bộ TT&TT sẽ tổ chức đánh giá, kiểm định sản phẩm ATANM nói riêng và sản phẩm công nghệ thông tin nói chung; xây dựng quy định ưu tiên đầu tư, mua sắm dùng ngân sách nhà nước; triển khai xây dựng Trung tâm R&D Quốc gia về an toàn không gian mạng.

Việc phát triển hệ sinh thái Việt Nam, làm chủ công nghệ, chính là phát triển **lá chắn thép** để bảo vệ không gian mạng quốc gia. Việt Nam không thể có ATANM bằng công nghệ của người khác.

**4.** **SỨ MỆNH, TRÁCH NHIỆM CỦA CÁC ISPs**

Thứ nhất, bảo đảm ATANM khi cung cấp dịch vụ, cần sớm hoàn thành triển khai giải pháp kỹ thuật (DPI) cho phép xử lý hiệu quả các nguồn phát tán thông tin vi phạm pháp luật, triển khai giải pháp quản lý trải nghiệm người dùng đến từng trạm thu phát sóng.

Thứ hai, thực hiện các biện pháp ngăn chặn tin nhắn rác, cuộc gọi rác, thư điện tử rác, tên miền độc hại theo sự điều phối của Cục ATTT.

Thứ ba, tích hợp sẵn dịch vụ tư vấn, kiểm tra, đánh giá về ATANM khi cung cấp dịch vụ truy nhập Internet cho thuê bao sử dụng, không để người dùng sử dụng sẵn cài đặt mặc định của nhà sản xuất thiết bị; tự động cảnh báo và hướng dẫn xử lý khi thiết bị của thuê bao Internet bị lây nhiễm mã độc; có cơ chế tạm thời ngắt kết nối đối với các thuê bao bị lây nhiễm mã độc đã nhận cảnh báo quá 3 lần mà không có biện pháp xử lý, khắc phục.

**5. ĐỀ XUẤT VỚI CÁC BỘ, NGÀNH, ĐỊA PHƯƠNG**

Đề xuất người đứng đầu các bộ, ngành, địa phương trực tiếp quan tâm, chỉ đạo công tác ATANM theo đúng chỉ đạo của Thủ tướng Chính phủ, có thể phân công một Lãnh đạo cấp phó giúp theo dõi, điều hành, tuy nhiên, cần bảo đảm:

- Khẩn trương kiện toàn tổ chức, bộ máy về ATANM trong phạm vi cơ quan, tổ chức, địa phương mình. Tối thiểu **01 lần / 1 năm** chủ trì một cuộc họp chuyên đề để chỉ đạo triển khai công tác bảo đảm ATANM. Chỉ đạo tổ chức và tham dự Ngày ATTT hàng năm trong phạm vi cơ quan, tổ chức, địa phương mình.

- Chỉ đạo triển khai hoàn thành việc xác định, phê duyệt hồ sơ cấp độ đối với các hệ thống thông tin từ cấp độ 3 trở lên trước 30/5/2020.

- Bố trí tối thiểu **10%** ngân sách chi cho công nghệ thông tin để chi cho ATANM. Trong đó, các bộ, ngành, địa phương chưa có các biện pháp bảo đảm ATANM tối thiểu có thể bố trí từ **20-30%** ngân sách chi cho CNTT để chi cho ATANM. Chỉ đạo các đơn vị trực thuộc sử dụng sản phẩm, dịch vụ do doanh nghiệp Việt Nam làm chủ, được Bộ TT&TT công bố đáp ứng yêu cầu sử dụng.

**6. ĐỀ XUẤT VỚI THỦ TƯỚNG CHÍNH PHỦ**

- Chỉ đạo Bộ Kế hoạch và Đầu tư, Bộ Tài chính bố trí nguồn kinh phí triển khai các dự án, hoạt động bảo đảm ATANM cho các bộ, ngành, địa phương tương xứng với tầm quan trọng của không gian mạng; tinh thần là bảo đảm chi cho ATANM tối thiểu **10%** ngân sách cấp cho công tác CNTT.

- Chỉ đạo Bộ Kế hoạch và Đầu tư, Bộ Tài chính, Bộ Nội vụ ưu tiên bố trí nguồn lực đầu tư nâng cao năng lực, cả về cơ sở vật chất, trang thiết bị lẫn biên chế cho 3 lực lượng nòng cốt bảo đảm ATANM ở Bộ Quốc phòng, Bộ Công an và Bộ TT&TT. Có cơ chế như nhau cho cả 3 lực lượng. Hiện nay, trong 3 lực lượng, Cục ATTT thuộc Bộ Thông tin và Truyền thông hiện được đầu tư ít nhất. Kính đề xuất Thủ tướng Chính phủ:

+ Chỉ đạo Bộ Tài chính, Bộ Kế hoạch và Đầu tư cấp đủ kinh phí cho các dự án đã được phê duyệt để nâng cao năng lực cho Cục ATTT.

+ Chỉ đạo Bộ Nội vụ sớm thẩm định, trình bổ sung biên chế cho Cục ATTT (đã trình TTg tại Tờ trình tối mật số 514/TTr-BTTTT ngày 06/12/2019).

- Giao Bộ TT&TT xây dựng Đề án kiện toàn bộ máy QLNN về ATTT từ TW đến địa phương theo hướng mỗi cơ quan chuyên trách về CNTT/ATTT của mỗi bộ, tỉnh đều có 1 phòng ATTT và mỗi cơ quan, tổ chức có quản lý, vận hành hệ thống thông tin phải có ít nhất 1 cán bộ chuyên trách về ATTT.

**CỤC AN TOÀN THÔNG TIN**