THỦ TƯỚNG CHÍNH PHỦ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do - Hạnh phúc
Số: 964/QĐ-TTg	*Hà Nội, ngày 10 tháng 8 năm 2022*

QUYẾT ĐỊNH
Phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030

THỦ TƯỚNG CHÍNH PHỦ

Căn cứ Luật Tổ chức Chính phủ ngày 19 tháng 6 năm 2015; Luật sửa đổi, bổ sung một số điều của Luật Tổ chức Chính phủ và Luật Tổ chức chính quyền địa phương ngày 22 tháng 11 năm 2019;

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị quyết số 30-NQ/TW ngày 25 tháng 7 năm 2018 của Bộ Chính trị về Chiến lược An ninh mạng quốc gia;

Căn cứ Nghị quyết số 22/NQ-CP ngày 18 tháng 10 năm 2019 của Chính phủ ban hành Chương trình hành động thực hiện Nghị quyết số 30-NQ/TW ngày 25 tháng 7 năm 2018 của Bộ Chính trị về Chiến lược An ninh mạng quốc gia;

Theo đề nghị của Bộ trưởng Bộ Công an và Bộ trưởng Bộ Thông tin và Truyền thông.

QUYẾT ĐỊNH:

Điều 1. Phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030 (sau đây gọi tắt là Chiến lược) với những nội dung chủ yếu sau đây:

I. QUAN ĐIỂM

1. Bảo đảm sự lãnh đạo toàn diện của Đảng, sự quản lý của Nhà nước trong công tác bảo đảm an toàn thông tin mạng và an ninh mạng (gọi tắt là an toàn, an ninh mạng), chủ động ứng phó với các thách thức từ không gian mạng. Xây dựng lực lượng bảo đảm an toàn, an ninh mạng hiện đại, chuyên nghiệp, có đủ nguồn nhân lực chất lượng cao đáp ứng yêu cầu thực tiễn.

2. An toàn, an ninh mạng là trọng tâm của quá trình chuyển đổi số, là trụ cột quan trọng tạo lập niềm tin số và sự phát triển thịnh vượng trong kỷ nguyên số. An toàn, an ninh mạng là nhiệm vụ trọng yếu, thường xuyên, lâu dài nhằm khởi tạo và duy trì môi trường mạng an toàn, lành mạnh, tin cậy cho các cơ quan, tổ chức, doanh nghiệp và mỗi người dân. Đầu tư cho an toàn, an ninh mạng là đầu tư cho phát triển bền vững và tạo ra giá trị.

3. Nắm bắt kịp thời, tận dụng hiệu quả các cơ hội do không gian mạng mang lại để phát triển kinh tế, xã hội, đồng thời chủ động phòng ngừa, sẵn sàng ứng phó để hạn chế các tác động tiêu cực, bảo đảm quốc phòng, chủ quyền, lợi ích, an ninh quốc gia, trật tự an toàn xã hội và tính bền vững của quá trình phát triển đất nước trong thời đại Cách mạng công nghiệp lần thứ tư.

4. Phát huy sức mạnh của cả hệ thống chính trị và toàn xã hội, chủ động ứng phó từ sớm, từ xa với các nguy cơ, thách thức, hoạt động gây tổn hại tới chủ quyền, lợi ích, an ninh quốc gia trên không gian mạng và an toàn thông tin mạng quốc gia, trong đó cơ quan quản lý nhà nước giữ vai trò điều phối, gắn kết, chia sẻ thông tin. Xác định nguồn lực nhà nước là quyết định, chiến lược, cơ bản lâu dài; sự tham gia của tổ chức, doanh nghiệp và phát huy sức mạnh của quần chúng nhân dân là quan trọng, đột phá. Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông chia sẻ thông tin giám sát không gian mạng nhằm phục vụ công tác bảo đảm an toàn, an ninh mạng và bảo vệ chủ quyền quốc gia trên không gian mạng.

5. Chuyển đổi căn bản về nhận thức và cách làm để thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa an toàn, an ninh mạng (cyber resilience): Từ mô hình bảo vệ phân tán sang mô hình bảo vệ tập trung; từ bị động ứng cứu sự cố sang chủ động dự báo sớm, cảnh báo sớm, phòng ngừa và ứng phó hiệu quả; từ đơn độc bảo vệ, giấu kín thông tin bị tấn công mạng sang chủ động hợp tác, chia sẻ thông tin nhằm chủ động phòng ngừa và hỗ trợ xử lý sự cố, phục hồi hoạt động bình thường của hệ thống thông tin.

6. Thúc đẩy chuyên gia, nghiên cứu, phát triển tự chủ về công nghệ, sản phẩm, dịch vụ an toàn, an ninh mạng Việt Nam là giải pháp căn cơ bảo đảm an toàn, an ninh mạng quốc gia; phát triển thị trường, doanh nghiệp, năng lực cạnh tranh về an toàn, an ninh mạng, đưa Việt Nam trở thành quốc gia có năng lực cao về bảo đảm an toàn, an ninh mạng.

7. Chủ động hội nhập quốc tế trong lĩnh vực an toàn, an ninh mạng trên tinh thần làm bạn, đối tác tin cậy, có trách nhiệm trong cộng đồng quốc tế, tôn trọng chủ quyền quốc gia trên không gian mạng của các nước khác, tuân thủ luật pháp quốc tế và các hiệp ước đa phương, song phương mà Việt Nam tham gia.

II. TẦM NHÌN ĐẾN NĂM 2030

Trở thành quốc gia tự chủ về an toàn, an ninh mạng để bảo vệ sự thịnh vượng của Việt Nam trên không gian mạng.

III. MỤC TIÊU

1. Mục tiêu tổng quát

Không gian mạng quốc gia được xây dựng, phát triển văn minh, lành mạnh, là động lực tham gia cuộc Cách mạng công nghiệp lần thứ tư. Năng lực quốc gia về bảo đảm an toàn, an ninh mạng được nâng cao, chủ động, sẵn sàng ứng phó với các nguy cơ, thách thức từ không gian mạng nhằm bảo vệ vững chắc chủ quyền, lợi ích, quốc phòng, an ninh quốc gia, trật tự an toàn xã hội; bảo vệ chủ quyền quốc gia trên không gian mạng và công cuộc chuyển đổi số quốc gia, quyền và lợi ích hợp pháp của tổ chức, cá nhân Việt Nam trên không gian mạng.

2. Mục tiêu cụ thể đến năm 2025

a) Duy trì thứ hạng 25 đến 30 về Chỉ số an toàn, an ninh mạng theo đánh giá của Liên minh Viễn thông quốc tế (Chỉ số GCI).

b) Xây dựng được hệ thống Thế trận An ninh nhân dân trên không gian mạng có khả năng chỉ huy, kết nối, chia sẻ thông tin, tiếp nhận và xử lý sớm các thông tin gây hại tới không gian mạng quốc gia từ các bộ, ngành, địa phương, các doanh nghiệp viễn thông, Internet, dịch vụ nội dung số.

c) Hình thành lực lượng bảo đảm an toàn, an ninh mạng tại các bộ, ngành, cơ quan nhà nước, các tổ chức chính trị - xã hội và các tập đoàn, tổng công ty nhà nước; đảm bảo mỗi cơ quan, tổ chức, doanh nghiệp nhà nước có một bộ phận được giao nhiệm vụ làm đầu mối, chịu trách nhiệm về công tác bảo đảm an toàn, an ninh mạng. Khuyến khích các doanh nghiệp khác có một đơn vị bảo đảm an toàn, an ninh mạng.

d) Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân tỉnh, thành phố trực thuộc trung ương, các tổ chức chính trị - xã hội, doanh nghiệp nhà nước, hiệp hội doanh nghiệp thực hiện bảo đảm an toàn, an ninh mạng theo quy định của pháp luật về an toàn thông tin và an ninh mạng.

đ) Bảo vệ cơ sở hạ tầng không gian mạng quốc gia, trọng tâm là hệ thống thông tin quan trọng về an ninh quốc gia theo quy định của pháp luật về an ninh mạng. Bảo vệ hệ thống thông tin của 11 lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng (theo Quyết định số 632/QĐ-TTg ngày 10 tháng 5 năm 2017 của Thủ tướng Chính phủ).

e) Phấn đấu 80% người sử dụng Internet có cơ hội tiếp cận hoạt động nâng cao nhận thức, kỹ năng và công cụ bảo đảm an toàn, an ninh mạng.

g) Đặt nền móng hình thành nền công nghiệp an ninh mạng và công nghiệp an toàn thông tin mạng. Xây dựng nền tảng chính sách phù hợp cho khởi nghiệp về an toàn, an ninh mạng.

h) Phát triển từ ba đến năm sản phẩm, dịch vụ an toàn thông tin trọng điểm, chiếm lĩnh thị trường trong nước, có khả năng cạnh tranh quốc tế.

i) Doanh thu thị trường an toàn, an ninh mạng hàng năm tăng trưởng từ 20 đến 30%.

k) Thành lập Hiệp hội An ninh mạng quốc gia.

l) Hình thành một trung tâm nghiên cứu, đổi mới, sáng tạo về an ninh mạng, thu hút được các nhà khoa học trên thế giới, nhà khoa học Việt Nam về nước để nghiên cứu, chế tạo, sản xuất sản phẩm.

m) Hình thành một Trung tâm Nghiên cứu và phát triển (R&D) về an toàn thông tin mạng, tạo môi trường thuận lợi cho nghiên cứu, thử nghiệm sản phẩm, dịch vụ an toàn thông tin mạng mới.

n) Kinh phí bảo đảm an toàn, an ninh mạng đạt tối thiểu 10% kinh phí chi cho khoa học công nghệ, chuyển đổi số, ứng dụng công nghệ thông tin.

3. Mục tiêu cụ thể đến năm 2030

a) Duy trì, nâng cao năng lực, thứ hạng về an toàn, an ninh mạng của Việt Nam trên bảng xếp hạng toàn cầu.

b) Xây dựng được Thế trận An ninh nhân dân trên không gian mạng với sự tham gia đông đảo, tích cực của quần chúng nhân dân.

c) Củng cố, tăng cường lực lượng bảo đảm an toàn, an ninh mạng.

d) Phấn đấu 90% người sử dụng Internet có cơ hội tiếp cận hoạt động nâng cao nhận thức, kỹ năng và công cụ bảo đảm an toàn, an ninh mạng.

đ) Hình thành trung tâm nghiên cứu, đổi mới, sáng tạo về an ninh mạng có danh tiếng trong khu vực và thế giới.

e) Hình thành hai đến ba Trung tâm Nghiên cứu và phát triển (R&D) về an toàn thông tin mạng, tạo môi trường thuận lợi cho nghiên cứu, thử nghiệm sản phẩm, dịch vụ an toàn thông tin mạng mới.

g) Việt Nam trở thành một trong những trung tâm bảo đảm an toàn, an ninh mạng hàng đầu châu Á. Hình thành được thị trường về bảo đảm an toàn, an ninh mạng, có sự cạnh tranh và ảnh hưởng trên toàn khu vực và thế giới.

h) Duy trì doanh thu thị trường an toàn, an ninh mạng hàng năm tăng trưởng từ 10 - 20%.

IV. NHIỆM VỤ, GIẢI PHÁP

1. Tăng cường vai trò lãnh đạo của Đảng, quản lý của Nhà nước

a) Thống nhất nhận thức từ trung ương tới địa phương về bảo đảm an toàn, an ninh mạng là trách nhiệm của cả hệ thống chính trị, trong đó Ban Chỉ đạo An toàn, An ninh mạng quốc gia điều phối chung sự phối hợp giữa 4 lực lượng (các Bộ: Công an, Quốc phòng, Thông tin và Truyền thông và Ban Tuyên giáo Trung ương). Các lực lượng này chủ động, phối hợp thực hiện theo chức năng, nhiệm vụ được giao.

b) Thường xuyên phổ biến, quán triệt chủ trương của Đảng, chính sách, pháp luật của Nhà nước về an toàn, an ninh mạng, coi đây là nhiệm vụ quan trọng của hệ thống chính trị.

c) Nâng cao nhận thức, trách nhiệm của các cấp ủy đảng, chính quyền, Mặt trận Tổ quốc, các tổ chức chính trị - xã hội, người dân, doanh nghiệp trong công tác bảo đảm an toàn, an ninh mạng. Người đứng đầu cấp ủy trực tiếp lãnh đạo, chỉ đạo và chịu trách nhiệm về công tác an toàn, an ninh mạng, chủ động rà soát, xác định rõ những vấn đề trọng tâm, trọng điểm để chỉ đạo thực hiện hiệu quả.

d) Phát huy sự tham gia có hiệu quả của quần chúng nhân dân trong công tác bảo đảm an toàn, an ninh mạng và chủ động ứng phó với các nguy cơ, thách thức từ không gian mạng.

đ) Hình thành Thế trận An ninh nhân dân trên không gian mạng kết hợp chặt chẽ với Thế trận Quốc phòng toàn dân trên không gian mạng.

e) Nhà nước ưu tiên chuyển giao và ứng dụng mạnh mẽ công nghệ, kỹ thuật an toàn, an ninh mạng; thúc đẩy nghiên cứu, tạo môi trường thuận lợi và hỗ trợ có trọng tâm, trọng điểm để tổ chức, cá nhân tham gia xây dựng công nghiệp an toàn thông tin mạng và công nghiệp an ninh mạng. Xây dựng cơ chế hợp tác giữa Nhà nước và các doanh nghiệp, hiệp hội doanh nghiệp trong xây dựng và thực thi các chính sách về an toàn, an ninh mạng. Đẩy mạnh phổ biến kỹ năng tham gia không gian mạng an toàn.

2. Hoàn thiện hành lang pháp lý

a) Bộ Công an

- Xây dựng, hoàn thiện chính sách, pháp luật về bảo vệ an ninh mạng đồng bộ, thống nhất từ trung ương đến địa phương theo định hướng điều chỉnh đầy đủ các lĩnh vực phát sinh hành vi sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự an toàn xã hội; nâng cao năng lực bảo vệ chủ quyền quốc gia trên không gian mạng theo chức năng, nhiệm vụ được giao.

- Xây dựng, hoàn thiện chính sách, pháp luật về bảo vệ dữ liệu quốc gia, dữ liệu cá nhân, quy định về hoạt động thu thập, lưu trữ, xử lý dữ liệu công dân Việt Nam và trách nhiệm của các tổ chức, doanh nghiệp trong và ngoài nước trong bảo vệ chủ quyền, an ninh quốc gia của Việt Nam trên không gian mạng.

- Nghiên cứu, rà soát, đề xuất sửa đổi, bổ sung văn bản quy phạm pháp luật về an ninh mạng để đồng bộ, thống nhất, toàn diện, đáp ứng được yêu cầu đấu tranh, xử lý vi phạm pháp luật về an ninh mạng.

- Xây dựng, hoàn thiện các văn bản hướng dẫn thi hành Luật An ninh mạng, các văn bản quy phạm pháp luật về điều kiện kinh doanh các sản phẩm, dịch vụ an ninh mạng, nhất là các sản phẩm, dịch vụ sử dụng trong hệ thống thông tin quan trọng về an ninh quốc gia, hệ thống thông tin của cơ quan nhà nước.

- Chủ trì, phối hợp với Bộ Thông tin và Truyền thông, Bộ Khoa học và Công nghệ nghiên cứu, áp dụng cơ chế khoán chi cho các đề tài khoa học về an toàn, an ninh mạng.

b) Bộ Thông tin và Truyền thông

- Xây dựng, hoàn thiện chính sách, pháp luật về an toàn thông tin mạng, nhất là các chế tài xử lý vi phạm pháp luật về an toàn thông tin mạng.

- Nghiên cứu, rà soát, đề xuất xây dựng, sửa đổi, bổ sung văn bản quy phạm pháp luật và văn bản hướng dẫn thi hành về bảo đảm an toàn thông tin mạng cho giao dịch điện tử, chuyển đổi số, hạ tầng số, nền tảng số, dữ liệu số, bảo vệ thông tin cá nhân trên mạng.

c) Bộ Quốc phòng

Xây dựng, hoàn thiện chính sách, pháp luật về lĩnh vực quốc phòng, bảo vệ Tổ quốc trên không gian mạng, bảo vệ chủ quyền quốc gia trên không gian mạng theo chức năng, nhiệm vụ được giao.

d) Các bộ, cơ quan liên quan theo chức năng, nhiệm vụ được giao tổ chức bảo vệ đội ngũ chuyên gia, trí thức, nhân sự đầu ngành, lĩnh vực tham gia xây dựng cơ chế, chính sách, pháp luật về an toàn, an ninh mạng và đội ngũ vận hành hệ thống thông tin quan trọng của Đảng, Nhà nước.

3. Bảo vệ chủ quyền quốc gia trên không gian mạng

a) Nghiên cứu, đề xuất ban hành chủ trương, chính sách, pháp luật về bảo vệ chủ quyền quốc gia trên không gian mạng phù hợp với tình hình thực tế của nước ta và chức năng, nhiệm vụ của các bộ, ngành có liên quan.

b) Xây dựng năng lực tự chủ, phản ứng trước các hoạt động xâm phạm chủ quyền quốc gia trên không gian mạng.

c) Chủ động tham gia các diễn đàn, tổ chức đa phương và song phương, văn bản và điều ước quốc tế về bảo vệ chủ quyền quốc gia trên không gian mạng.

d) Bộ Quốc phòng, Bộ Công an, Bộ Thông tin và Truyền thông và các bộ, cơ quan liên quan phối hợp bảo vệ chủ quyền quốc gia trên không gian mạng theo đúng chức năng, nhiệm vụ được giao.

4. Bảo vệ hạ tầng số, nền tảng số, dữ liệu số, cơ sở hạ tầng không gian mạng quốc gia

a) Bảo vệ cơ sở hạ tầng không gian mạng quốc gia

- Bảo đảm an toàn, an ninh mạng trong quá trình lựa chọn, triển khai các dịch vụ, công nghệ cho cơ sở hạ tầng không gian mạng quốc gia; ưu tiên sử dụng sản phẩm an toàn, an ninh mạng Việt Nam.

- Bảo đảm an toàn, an ninh mạng trong quá trình thiết kế, xây dựng, vận hành, khai thác cơ sở hạ tầng không gian mạng quốc gia. Giám sát, cảnh báo sớm các hành vi vi phạm pháp luật trên không gian mạng đối với cơ sở hạ tầng không gian mạng quốc gia.

- Nâng cao năng lực tự chủ về an toàn, an ninh mạng.

- Bảo đảm an toàn, an ninh mạng cho quá trình triển khai Chính phủ điện tử, chuyển đổi số.

- Xây dựng Bộ tiêu chí đánh giá rủi ro an ninh mạng và xếp hạng năng lực bảo đảm an ninh mạng đối với chủ quản hệ thống thông tin quan trọng về an ninh quốc gia.

b) Bảo vệ hạ tầng số

- Bộ Thông tin và Truyền thông:

+ Ban hành tiêu chuẩn, quy chuẩn kỹ thuật và tiêu chí kỹ thuật về an toàn thông tin mạng đối với hạ tầng, dịch vụ điện toán đám mây, thiết bị 5G và thiết bị Internet kết nối vạn vật (IoT).

+ Phát triển và làm chủ công nghệ điện toán đám mây Make in Viet Nam. Đánh giá, công bố các doanh nghiệp cung cấp dịch vụ điện toán đám mây đáp ứng tiêu chí an toàn thông tin mạng.

+ Chỉ đạo, kiểm tra, đánh giá các doanh nghiệp hạ tầng số thực thi trách nhiệm và sứ mệnh bảo đảm an toàn thông tin mạng quốc gia theo chức năng, nhiệm vụ được giao.

+ Phát triển Nền tảng điều hành, chỉ huy an toàn thông tin mạng tập trung với các yêu cầu:

. Có năng lực tiếp nhận và phân tích dữ liệu lớn từ hơn 100 trung tâm điều hành an toàn thông tin mạng (SOC) của các bộ, ngành, địa phương, các doanh nghiệp hạ tầng số, các tổ chức nước ngoài.

. Có năng lực dự báo, cảnh báo sớm các nguy cơ, rủi ro trên không gian mạng Việt Nam, các lỗ hổng bảo mật trên diện rộng, lộ lọt dữ liệu nghiêm trọng giúp các cơ quan, tổ chức, doanh nghiệp Việt Nam ngăn chặn kịp thời các cuộc tấn công mạng, giảm thiệt hại trên diện rộng.

. Có năng lực điều hành, chỉ huy và giám sát tuân thủ an toàn thông tin mạng 24/7 trên phạm vi toàn quốc.

+ Theo chức năng, nhiệm vụ được giao, thực hiện thu thập, tổng hợp, phân tích dữ liệu lưu lượng truy cập Internet trên môi trường mạng Việt Nam nhằm phát hiện các dấu hiệu, nguy cơ để dự báo sớm, kịp thời ngăn chặn hành vi tấn công mạng.

+ Phát triển hệ thống tên miền Internet (DNS) quốc gia an toàn sẵn sàng cho 5G, IoT, IPv6, ứng dụng các công nghệ, tiêu chuẩn bảo đảm an toàn cho hệ thống tên miền Internet quốc gia ".vn".

+ Tổ chức các Chiến dịch rà quét, xử lý bóc gỡ mã độc trên toàn quốc.

- Bộ Quốc phòng:

+ Chủ động chỉ đạo, kiểm tra các đơn vị trực thuộc, các doanh nghiệp có hoạt động liên quan tới lĩnh vực quốc phòng.

+ Chỉ đạo, kiểm tra, đánh giá các doanh nghiệp hạ tầng số thực thi trách nhiệm và sứ mệnh bảo vệ chủ quyền quốc gia trên không gian mạng, phòng chống chiến tranh thông tin, chiến tranh không gian mạng theo chức năng, nhiệm vụ được giao.

+ Phối hợp với Bộ Công an, Bộ Thông tin và Truyền thông và các bộ, cơ quan liên quan trong công tác chỉ đạo, kiểm tra, đánh giá các doanh nghiệp cung cấp dịch vụ nền tảng số thực thi trách nhiệm và sứ mệnh bảo đảm an toàn, an ninh mạng.

- Bộ Công an: Chỉ đạo, kiểm tra, đánh giá các doanh nghiệp hạ tầng số thực thi trách nhiệm và sứ mệnh bảo đảm an ninh mạng theo chức năng, nhiệm vụ được giao.

- Doanh nghiệp hạ tầng số:

+ Cung cấp dịch vụ viễn thông, Internet an toàn (Security by Default).

+ Bảo đảm an toàn thông tin mạng 5G và các thế hệ mạng tiếp theo trong toàn bộ quá trình thiết kế, xây dựng và vận hành, khai thác, bao gồm:

. Kiểm tra, đánh giá an toàn thông tin mạng (Pentest) và săn lùng mối nguy hại (Threat hunting). Xây dựng môi trường thử nghiệm (Test-bed) để diễn tập, nâng cao kỹ năng và tri thức cho chuyên gia an toàn thông tin của doanh nghiệp.

. Kiểm tra, đánh giá an toàn thông tin mạng đối với các thiết bị đầu cuối trước khi cung cấp cho người sử dụng. Ưu tiên sử dụng các thiết bị đầu cuối do doanh nghiệp trong nước sản xuất đã được kiểm tra, đánh giá, công bố về an toàn thông tin mạng theo quy định.

+ Khắc phục, xử lý hoặc thay thế thiết bị đầu cuối cung cấp cho người sử dụng (Modem, Router, Camera giám sát, các thiết bị IoT,…) có dấu hiệu mất an toàn thông tin mạng.

+ Triển khai trung tâm điều hành an toàn thông tin mạng (SOC).

+ Phát triển hạ tầng mạng IoT an toàn, bao gồm:

. Đánh giá, công bố đáp ứng tiêu chí kỹ thuật về an toàn thông tin đối với thiết bị IoT. Lựa chọn thiết bị IoT đã được đánh giá, công bố đáp ứng tiêu chí kỹ thuật về an toàn thông tin khi thiết lập hạ tầng mạng IoT.

. Phát triển các sản phẩm, giải pháp cổng kết nối thiết bị IoT (IoT Gateway) Make in Viet Nam bảo đảm an toàn thông tin cho thiết bị IoT.

+ Bảo đảm an toàn thông tin mạng cho hạ tầng điện toán đám mây, bao gồm: Phát triển hạ tầng điện toán đám mây Make in Viet Nam; kết nối các nền tảng cung cấp dịch vụ điện toán đám mây của Việt Nam (Multi Cloud), bảo đảm tính liên thông, an toàn, hiệu quả.

+ Công khai mức độ an toàn thông tin mạng của các dịch vụ hạ tầng số.

+ Ưu tiên sử dụng sản phẩm an toàn, an ninh mạng Make in Viet Nam.

- Tổ chức, cá nhân sử dụng dịch vụ:

+ Lựa chọn sử dụng dịch vụ viễn thông, Internet và dịch vụ hạ tầng số được công khai mức độ an toàn, an ninh mạng. Ưu tiên sử dụng sản phẩm an toàn, an ninh mạng Make in Viet Nam.

+ Chủ động thông báo cho lực lượng chức năng khi xảy ra các hành vi vi phạm pháp luật trên không gian mạng; thực hiện hoặc thông báo, phối hợp với doanh nghiệp hạ tầng số khắc phục, xử lý hoặc từng bước thay thế thiết bị đầu cuối có dấu hiệu mất an toàn thông tin mạng.

c) Bảo vệ nền tảng số

- Doanh nghiệp chủ quản nền tảng số:

+ Xác định cấp độ an toàn thông tin và triển khai phương án bảo đảm an toàn hệ thống thông tin theo cấp độ đối với nền tảng số.

+ Phát triển nền tảng số có khả năng tự bảo vệ; có các công cụ sàng lọc, phát hiện, xử lý, gỡ bỏ thông tin vi phạm pháp luật trên nền tảng số.

+ Công khai chính sách quản lý, sử dụng thông tin, dữ liệu của người sử dụng trên nền tảng số. Bảo đảm an toàn thông tin cá nhân, thông tin về tài khoản, mật khẩu tin nhắn, lịch sử giao dịch của người sử dụng dịch vụ nền tảng số.

+ Cung cấp cho người sử dụng cơ chế khiếu nại, phản ánh, xác minh tin giả, thông tin vi phạm pháp luật và tiến hành xử lý theo quy định.

+ Chủ động phát hiện, ngăn chặn, xử lý, xóa bỏ tin giả, thông tin vi phạm pháp luật hoặc cung cấp các bằng chứng để truy vết, xác định nguồn gốc thông tin; xử lý, xóa bỏ thông tin vi phạm pháp luật theo yêu cầu của cơ quan chức năng có thẩm quyền.

+ Không cung cấp hoặc ngừng cung cấp dịch vụ cho tổ chức, cá nhân đăng tải trên môi trường mạng thông tin có nội dung vi phạm pháp luật Việt Nam.

+ Phát triển các nền tảng số Make in Viet Nam có hàng triệu người Việt Nam và quốc tế sử dụng.

- Bộ Thông tin và Truyền thông: Chỉ đạo, kiểm tra, đánh giá các doanh nghiệp cung cấp dịch vụ nền tảng số thực thi trách nhiệm và sứ mệnh bảo đảm an toàn thông tin mạng quốc gia theo chức năng, nhiệm vụ được giao.

- Bộ Công an: Chỉ đạo, kiểm tra, đánh giá các doanh nghiệp cung cấp dịch vụ nền tảng số thực thi trách nhiệm và sứ mệnh bảo đảm an ninh mạng theo chức năng, nhiệm vụ được giao.

- Bộ Quốc phòng:

+ Chủ động chỉ đạo, kiểm tra các đơn vị trực thuộc, các doanh nghiệp có hoạt động liên quan tới lĩnh vực quốc phòng.

+ Chỉ đạo, kiểm tra, đánh giá các doanh nghiệp cung cấp dịch vụ nền tảng số thực thi trách nhiệm và sứ mệnh bảo vệ chủ quyền quốc gia trên không gian mạng, phòng chống chiến tranh thông tin, chiến tranh không gian mạng theo chức năng, nhiệm vụ được giao.

+ Phối hợp với Bộ Công an, Bộ Thông tin và Truyền thông và các bộ, cơ quan liên quan trong công tác chỉ đạo, kiểm tra, đánh giá các doanh nghiệp cung cấp dịch vụ nền tảng số thực thi trách nhiệm và sứ mệnh bảo đảm an toàn, an ninh mạng.

- Các bộ, ngành, địa phương: Chủ động giám sát, phát hiện và công bố hành vi vi phạm quy định pháp luật của Việt Nam thuộc phạm vi quản lý trên các nền tảng số. Xử lý theo thẩm quyền hoặc phối hợp với Bộ Công an, Bộ Thông tin và Truyền thông xử lý tổ chức, cá nhân vi phạm, gỡ bỏ thông tin vi phạm trên các nền tảng số.

- Tổ chức, cá nhân sử dụng dịch vụ:

+ Lựa chọn sử dụng dịch vụ nền tảng số an toàn, lành mạnh.

+ Thận trọng khi cung cấp thông tin, dữ liệu cá nhân trên nền tảng số; bảo mật tài khoản, mật khẩu để không bị lộ lọt, lợi dụng thực hiện hành vi vi phạm pháp luật.

+ Tuân thủ các quy tắc ứng xử, không đăng tải, lan truyền các nội dung vi phạm pháp luật trên môi trường mạng.

+ Chia sẻ, lan tỏa các thông tin tích cực; cảnh báo và phản ánh, tố giác các hành vi vi phạm pháp luật.

d) Bảo vệ dữ liệu của tổ chức, cá nhân

- Xây dựng chính sách, pháp luật về bảo vệ dữ liệu nhằm bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân, đặc biệt là dữ liệu quan trọng quốc gia.

- Phát triển các Trung tâm dữ liệu đạt tiêu chuẩn quốc tế tại Việt Nam và thúc đẩy các tổ chức, cá nhân thuê dịch vụ của các Trung tâm dữ liệu này.

- Kiểm tra, đánh giá các doanh nghiệp cung cấp dịch vụ xuyên biên giới đối với việc tuân thủ quy định của pháp luật Việt Nam về lưu trữ, xử lý dữ liệu của tổ chức, cá nhân Việt Nam.

- Bảo đảm an ninh mạng, an toàn thông tin mạng theo cấp độ cho các cơ sở dữ liệu quốc gia và cơ sở dữ liệu quan trọng của các ngành, lĩnh vực.

- Thiết lập cơ chế đánh giá rủi ro bảo mật dữ liệu tập trung, hiệu quả và có thẩm quyền; báo cáo, chia sẻ thông tin, giám sát và cảnh báo sớm; tăng cường thu thập, phân tích, nghiên cứu, phán đoán và cảnh báo sớm về thông tin rủi ro bảo mật dữ liệu. Xây dựng cơ chế phản ứng khẩn cấp trong trường hợp xảy ra sự cố bảo mật dữ liệu.

5. Bảo vệ hệ thống thông tin của các cơ quan Đảng, Nhà nước

a) Chủ quản hệ thống thông tin

- Nâng cao trách nhiệm tự bảo vệ hệ thống thông tin thuộc phạm vi quản lý. Gắn trách nhiệm của người đứng đầu cơ quan chủ quản hệ thống thông tin với trách nhiệm bảo đảm an toàn, an ninh mạng.

- Xây dựng, cập nhật, vận hành hệ thống thông tin theo tiêu chuẩn, quy chuẩn kỹ thuật về an toàn, an ninh mạng.

- Rà soát, lập hồ sơ đề nghị đưa các hệ thống thông tin trọng yếu, phù hợp với quy định của pháp luật vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

- Thực hiện nghiêm túc các quy định pháp luật về bảo vệ an ninh mạng; xác định cấp độ và trách nhiệm bảo đảm an toàn hệ thống thông tin theo từng cấp độ và triển khai mô hình bảo vệ 4 lớp trước khi đưa vào sử dụng.

- Chủ động giám sát, kịp thời phát hiện nguy cơ mất an toàn, an ninh mạng trong quá trình thi công, lắp đặt thiết bị trong các hệ thống thông tin. Ưu tiên sử dụng sản phẩm, giải pháp an toàn, an ninh mạng Make in Viet Nam.

- Đầu tư nguồn lực, thường xuyên nâng cấp hệ thống, cập nhật bản quyền, nâng cao nhận thức và kỹ năng an toàn, an ninh mạng cho cán bộ, công chức, viên chức và người lao động. Tối thiểu 1 năm/1 lần tổ chức diễn tập, hướng dẫn, kiểm tra, ứng phó và ứng cứu sự cố an toàn, an ninh mạng.

- Phối hợp với cơ quan chuyên trách về an ninh mạng của Bộ Công an để kết nối với Trung tâm An ninh mạng quốc gia để giám sát an ninh mạng.

b) Bộ Công an

- Xây dựng quy trình kiểm tra, đánh giá an ninh mạng đối với các thiết bị kỹ thuật, phương tiện điện tử, phần mềm sử dụng trong những hệ thống thông tin quan trọng về an ninh quốc gia trước khi đưa vào sử dụng, nhất là những thiết bị, phương tiện được nước ngoài, doanh nghiệp tài trợ hoặc tặng, cho.

- Xây dựng cơ chế phối hợp, tham gia tư vấn, thẩm định về an ninh mạng đối với các hệ thống thông tin quan trọng về an ninh quốc gia.

- Chủ động xây dựng kế hoạch, tổ chức kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia và hệ thống thông tin khác của các cơ quan Đảng, Nhà nước khi có đề nghị của chủ quản hệ thống thông tin. Tổ chức đánh giá, xếp hạng mức độ an ninh mạng đối với hệ thống thông tin của cơ quan nhà nước.

- Tổ chức diễn tập thực chiến về an ninh mạng cấp quốc gia, có sự tham gia của các chủ quản hệ thống thông tin quan trọng về an ninh quốc gia, cơ quan, tổ chức, doanh nghiệp bảo đảm an ninh mạng.

- Xây dựng, hình thành Mạng lưới ứng phó, khắc phục sự cố an ninh mạng, lấy lực lượng chuyên trách bảo vệ an ninh mạng làm trung tâm, phối hợp chặt chẽ với các cơ quan, tổ chức, cá nhân trong ứng phó, khắc phục sự cố an ninh mạng.

- Chủ trì, phối hợp với Bộ Quốc phòng, Bộ Thông tin và Truyền thông, các bộ, ngành có liên quan xây dựng cơ chế phối hợp, chia sẻ thông tin giám sát an toàn, an ninh mạng hệ thống thông tin của các bộ, ban, ngành, địa phương, tổ chức, doanh nghiệp trọng yếu.

- Phối hợp với chủ quản hệ thống thông tin khắc phục, xử lý nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật, phần cứng độc hại.

- Triển khai các biện pháp phòng ngừa, đấu tranh, xử lý hành vi xâm phạm an ninh mạng, hoạt động của các đối tượng, thế lực thù địch sử dụng không gian mạng xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự an toàn xã hội.

c) Bộ Quốc phòng

- Chủ động, kịp thời phát hiện và ngăn chặn các nguy cơ mất an toàn, an ninh mạng nhằm bảo vệ chủ quyền quốc gia trên không gian mạng, phòng chống chiến tranh thông tin, chiến tranh không gian mạng.

- Tổ chức lực lượng bảo đảm an toàn thông tin, an ninh mạng cho các hệ thống thông tin của cơ quan Đảng, Nhà nước, hệ thống thông tin quan trọng về an ninh quốc gia, hệ thống thông tin quân sự theo chức năng, nhiệm vụ được giao.

- Tham mưu, đề xuất xây dựng các hệ thống kỹ thuật nghiệp vụ, triển khai các biện pháp phòng ngừa, đấu tranh với hoạt động của các thế lực thù địch sử dụng không gian mạng xâm phạm quốc phòng, chủ quyền quốc gia trên không gian mạng.

d) Bộ Thông tin và Truyền thông

- Triển khai Nền tảng điện toán đám mây riêng của Chính phủ đáp ứng yêu cầu bảo đảm an toàn thông tin mạng, tạo cơ sở hạ tầng an toàn cho các ứng dụng Chính phủ điện tử dùng chung.

- Phát triển Nền tảng Điều hành, chỉ huy an toàn thông tin mạng tập trung, kết nối, phân tích dữ liệu lớn, chia sẻ thông tin rủi ro an toàn thông tin mạng với 100% SOC của các cơ quan nhà nước nhằm dự báo, cảnh báo sớm, giúp ngăn chặn, xử lý kịp thời sự cố an toàn thông tin mạng, tránh thiệt hại trên diện rộng.

- Phát triển Nền tảng rà quét lỗ hổng bảo mật nhằm phòng ngừa sự cố mất an toàn thông tin mạng cho các ứng dụng Chính phủ điện tử của các bộ, ngành, địa phương.

- Phát triển Nền tảng đào tạo, sát hạch trực tuyến kiến thức, kỹ năng an toàn thông tin cơ bản cho người sử dụng.

- Phát triển Phòng thử nghiệm mô phỏng, tái hiện sự cố an toàn thông tin mạng.

- Đánh giá và gán nhãn tín nhiệm mạng đối với website.

- Tổ chức đánh giá, xếp hạng mức độ an toàn thông tin của các cơ quan, tổ chức, doanh nghiệp nhà nước và các tổ chức, doanh nghiệp hoạt động trong các lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng.

- Phát triển Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia nhằm điều phối kịp thời, phối hợp đồng bộ, hiệu quả các lực lượng để bảo đảm an toàn thông tin mạng, tập trung vào 11 lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng (CERT lĩnh vực).

- Phát triển các hệ thống kỹ thuật khác phục vụ bảo đảm an toàn thông tin mạng quốc gia, bảo đảm an toàn thông tin cho quá trình chuyển đổi số quốc gia, phát triển Chính phủ số, kinh tế số, xã hội số.

đ) Ban Cơ yếu Chính phủ

- Triển khai các giải pháp dùng mật mã để bảo vệ thông tin trong hệ thống thông tin quan trọng quốc gia của các cơ quan Đảng, Nhà nước.

- Cung cấp dịch vụ và quản lý hệ thống chứng thực chữ ký số chuyên dùng phục vụ các cơ quan thuộc hệ thống chính trị, triển khai bảo mật ứng dụng công nghệ thông tin trong hoạt động của các cơ quan Đảng, Nhà nước, đáp ứng yêu cầu bảo mật và an toàn thông tin cho Chính phủ điện tử.

- Phối hợp với các cơ quan liên quan triển khai giám sát an toàn thông tin trên hệ thống thông tin quan trọng quốc gia của các cơ quan Đảng, Nhà nước.

e) Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông thực hiện giám sát, cảnh báo sớm để bảo vệ hệ thống thông tin của các cơ quan Đảng, Nhà nước theo chức năng, nhiệm vụ được giao.

6. Bảo vệ hệ thống thông tin của các lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin

a) Chủ quản hệ thống thông tin

- Triển khai phương án bảo đảm an toàn thông tin theo cấp độ và mô hình bảo vệ 4 lớp đối với hệ thống thông tin của các lĩnh vực quan trọng.

- Ưu tiên sử dụng sản phẩm, giải pháp an toàn thông tin mạng Make in Viet Nam trong các hệ thống thông tin quan trọng quốc gia.

- Đầu tư nâng cao nhận thức cho các tổ chức, cá nhân liên quan về bảo đảm an toàn thông tin mạng cho các hệ thống thông tin của các lĩnh vực quan trọng.

- Tối thiểu 1 năm/1 lần tổ chức diễn tập, hướng dẫn, kiểm tra, ứng phó và ứng cứu sự cố an toàn thông tin cho các lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin và hệ thống thông tin quan trọng quốc gia.

- Phát triển các Đội ứng cứu sự cố khẩn cấp của 11 lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng (CERT lĩnh vực) theo sự điều phối của Bộ Thông tin và Truyền thông, tham gia vào Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia.

b) Các cơ quan chuyên trách an toàn, an ninh mạng (Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông) chia sẻ thông tin về nguy cơ, rủi ro an toàn thông tin mạng cho chủ quản hệ thống thông tin thuộc 11 lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng.

c) Bộ Công an hướng dẫn, đôn đốc, kiểm tra công tác bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin quan trọng thuộc phạm vi quản lý.

d) Bộ Quốc phòng hướng dẫn, đôn đốc, kiểm tra công tác bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin quan trọng thuộc phạm vi quản lý.

đ) Bộ Thông tin và Truyền thông hướng dẫn, đôn đốc, kiểm tra công tác bảo đảm an toàn thông tin mạng và ứng cứu sự cố đối với các hệ thống thông tin thuộc 11 lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng (trừ các hệ thống thông tin thuộc phạm vi quản lý của Bộ Công an, Bộ Quốc phòng).

7. Tạo lập niềm tin số, xây dựng môi trường mạng trung thực, văn minh, lành mạnh và phòng, chống vi phạm pháp luật trên không gian mạng

a) Bộ Công an

- Xây dựng cơ chế, thiết lập đường dây nóng, hệ thống tiếp nhận, xử lý thông tin về tội phạm mạng từ không gian mạng để quần chúng nhân dân phản ánh kịp thời, trực tiếp thông tin, hành vi vi phạm pháp luật trên không gian mạng tới cơ quan chức năng có thẩm quyền.

- Đổi mới nội dung, hình thức, biện pháp xây dựng phong trào toàn dân bảo vệ an ninh Tổ quốc phù hợp với thực tiễn chuyển đổi số. Phát huy vai trò của Thế trận An ninh nhân dân trên không gian mạng để hình thành mô hình toàn dân bảo vệ an ninh Tổ quốc trên không gian mạng.

- Xây dựng cơ chế phối hợp liên ngành với các bộ, ngành, địa phương, giữa lực lượng chuyên trách bảo vệ an ninh mạng với các tổ chức, doanh nghiệp có liên quan theo quy định của pháp luật trong thực hiện công tác phòng ngừa, phát hiện, điều tra, xử lý các vi phạm pháp luật trên không gian mạng và chống khủng bố mạng.

- Nâng cấp, phát triển Trung tâm An ninh mạng quốc gia có khả năng giám sát, tổng hợp, thu thập, phân tích dữ liệu lớn toàn bộ hoạt động, hành vi vi phạm pháp luật trên không gian mạng, hành vi tấn công mạng, hỗ trợ xử lý kịp thời các nguy cơ, thách thức, hành vi xâm phạm an ninh mạng.

- Gắn hoạch định, thực hiện chính sách phát triển kinh tế, xã hội với công tác phòng, chống tội phạm mạng. Tăng cường giáo dục, bồi dưỡng kiến thức quốc phòng, an ninh mạng.

- Xây dựng hệ thống cảnh báo sớm quốc gia để kịp thời phát hiện, điều phối, ứng cứu cố sự an ninh mạng; thu thập, chia sẻ thông tin về an ninh mạng giữa Nhà nước và doanh nghiệp, trong nước và thế giới; xây dựng, hình thành nền tảng điều hành, giám sát an ninh mạng thống nhất.

b) Bộ Thông tin và Truyền thông

- Thúc đẩy phát triển ứng dụng (app) Internet an toàn nhằm bảo vệ người dân trên môi trường mạng.

- Phát triển ứng dụng (app) tuyên truyền, nâng cao nhận thức và phổ biến kiến thức về an toàn thông tin cho người sử dụng.

- Phát triển Nền tảng hỗ trợ bảo vệ trẻ em trên môi trường mạng.

- Hướng dẫn tổ chức, cá nhân thay đổi thói quen, hành vi trên môi trường mạng theo các chuẩn mực an toàn.

- Đổi mới phương thức tuyên truyền, nâng cao nhận thức, phổ biến kiến thức và thay đổi thái độ của người dân về an toàn thông tin với quan điểm lấy cộng đồng làm trung tâm qua các hình thức như: ứng dụng trên điện thoại, mạng xã hội. Cung cấp cho tổ chức, cá nhân thông tin, cảnh báo, giải đáp thắc mắc về an toàn thông tin mạng tại địa chỉ https://khonggianmang.vn; hỗ trợ công cụ, tiện ích và hướng dẫn xử lý sự cố an toàn thông tin mạng.

- Thiết lập kênh trao đổi, làm việc nhằm khuyến khích, hỗ trợ và xây dựng cẩm nang hướng dẫn các tổ chức, doanh nghiệp (nhất là doanh nghiệp vừa và nhỏ) triển khai giải pháp bảo đảm an toàn thông tin mạng.

- Triển khai Chương trình Bảo vệ và hỗ trợ trẻ em tương tác lành mạnh, sáng tạo trên môi trường mạng giai đoạn 2021 - 2025.

- Chỉ đạo doanh nghiệp nền tảng số xây dựng và triển khai cơ chế để người sử dụng phản ánh, xử lý tin giả, thông tin không đúng sự thực về đất nước, con người Việt Nam.

c) Bộ Quốc phòng

- Nghiên cứu nội dung, hình thức xây dựng Thế trận Quốc phòng toàn dân trên không gian mạng gắn với Thế trận An ninh nhân dân trên không gian mạng.

- Xây dựng hệ thống giám sát, phát hiện, cảnh báo sớm các nguy cơ xâm phạm quốc phòng, chủ quyền quốc gia trên không gian mạng, góp phần xây dựng không gian mạng an toàn, lành mạnh.

- Phát hiện, xử lý các hành vi đăng tải, lưu trữ, traođổi trái phép thông tin, tài liệu có nội dung bí mật nhà nước trong phạm vi quản lý.

- Phối hợp với các ban, bộ, ngành, địa phương thực hiện phòng ngừa, phát hiện, xử lý hành vi tấn công mạng, hành vi chống phá Đảng, Nhà nước; phòng, chống khủng bố mạng đối với các hệ thống thông tin trong phạm vi quản lý.

d) Các bộ, ngành, địa phương

- Giám sát, phát hiện và phối hợp với cơ quan chức năng và các doanh nghiệp nền tảng số xử lý tin giả, thông tin vi phạm pháp luật trong phạm vi quản lý.

- Phát triển các website, trang mạng xã hội, tài khoản trên môi trường mạng uy tín, nhiều tương tác để tuyên truyền, định hướng thông tin, dư luận và phản bác hiệu quả các thông tin tiêu cực về đất nước, con người Việt Nam.

8. Làm chủ, tự chủ công nghệ, sản phẩm, dịch vụ đủ khả năng chủ động ứng phó với các thách thức từ không gian mạng

a) Làm chủ, tự chủ công nghệ

- Bộ Thông tin và Truyền thông:

+ Nghiên cứu và phát triển:

. Chỉ đạo 2 đến 3 doanh nghiệp ICT lớn phát triển Trung tâm R&D về an toàn thông tin mạng, tạo môi trường thuận lợi cho nghiên cứu, thử nghiệm sản phẩm, dịch vụ an toàn thông tin mạng mới.

. Phát triển Hệ thống đánh giá, kiểm định an toàn thông tin và công bố các sản phẩm đạt chuẩn an toàn thông tin mạng.

. Hỗ trợ một số doanh nghiệp, cơ sở nghiên cứu có năng lực làm chủ và sáng tạo về giải pháp công nghệ để phát triển giải pháp an toàn thông tin mạng trọng điểm.

. Thúc đẩy các ý tưởng khởi nghiệp sáng tạo xuất sắc, phục vụ lợi ích quốc gia.

+ Hợp tác công tư:

. Định hướng, giao nhiệm vụ cho các doanh nghiệp giải quyết các vấn đề quốc gia về an toàn thông tin mạng.

. Thúc đẩy sứ mệnh của doanh nghiệp viễn thông giải quyết bài toán lớn của đất nước về an toàn thông tin mạng.

- Bộ Công an

+ Xây dựng chiến lược từng bước tiếp thu, kế thừa công nghệ, sản phẩm, dịch vụ an ninh mạng của nước ngoài thông qua đầu tư, chuyển giao công nghệ. Khuyến khích và tôn vinh tinh thần đổi mới sáng tạo về công nghệ, sản phẩm, dịch vụ an ninh mạng.

+ Xây dựng cơ chế thúc đẩy làm chủ, tự chủ có chọn lọc và lộ trình phù hợp về an ninh mạng, tiến tới làm chủ công nghệ cốt lõi về khoa học và công nghệ nhằm giải quyết những nguy cơ, thách thức về an ninh mạng và phục vụ cho sự nghiệp phát triển kinh tế, xã hội.

+ Xác định, chọn lọc công nghệ an ninh mạng có tầm chiến lược quốc gia, dài hạn, với một cơ chế hợp tác dân sự - an ninh:

. Nghiên cứu, xây dựng Mạng theo dõi không gian dựa trên các công nghệ xử lý thông tin trong mọi điều kiện thời tiết, thời điểm, có tốc độ truyền và xử lý cao, kết hợp công nghệ cảm biến, theo dõi, phân tích, nhận dạng, ứng dụng thời gian thực và có độ phân giải cao.

. Hình thành hệ thống thông tin an ninh mạng gồm: hệ thống chỉ huy, hệ thống thông tin chiến lược, hệ thống cảnh báo nguy cơ không gian, biển, không gian số, vũ khí mới, hệ thống bảo vệ vùng trời, hệ thống bảo vệ vùng biển, hệ thống bảo vệ môi trường sinh học và hệ thống bảo vệ không gian mạng quốc gia theo chức năng, nhiệm vụ được giao.

. Đầu tư cho các dự án bảo đảm an ninh mạng trong trí tuệ nhân tạo, xử lý dữ liệu lớn, thiết bị thông minh, mã hóa lượng tử và mạng lưới tính toán hiệu năng cao, hệ điều hành cho cấu trúc lai ghép tính toán lượng tử, mô phỏng não và máy tính số thông thường, các công nghệ xử lý lỗi, linh kiện và thiết bị ngoại vi, cảm biến lượng tử.

. Thúc đẩy ứng dụng song hành các sản phẩm, dịch vụ an ninh mạng vào quá trình xây dựng, phát triển kinh tế đất nước, như: xây dựng và bảo vệ quy hoạch đô thị thông minh, kế hoạch hóa đô thị, giải quyết vấn đề giao thông, an ninh xã hội, các giải pháp cảm biến, theo dõi, tối ưu, dự báo, xử lý dữ liệu, cảnh báo sớm; bảo đảm an ninh mạng trong ứng dụng các thành tựu khoa học công nghệ mới về công nghiệp giải trí và truyền thông.

. Xây dựng và đặt các Viện nghiên cứu về an ninh mạng vào một mạng lưới nghiên cứu sử dụng chung hạ tầng nhằm cùng nghiên cứu và phát triển sản phẩm, dịch vụ, công nghệ an ninh mạng. Các Viện cần có năng lực và được đầu tư hạ tầng, các phòng thí nghiệm tiên tiến để tích hợp công nghệ, tri thức khoa học, chuyển giao từ cơ sở đào tạo cho doanh nghiệp.

. Xây dựng và vận hành các phòng thí nghiệm quốc gia về an ninh mạng tiên tiến theo nguyên tắc cung cấp dịch vụ, hoạt động theo cơ chế mở, dùng chung. Có chính sách chia sẻ quyền sở hữu công bằng và hợp lý đối với kết quả nghiên cứu tại phòng thí nghiệm về an ninh mạng, sử dụng vốn ngân sách và sử dụng hỗn hợp ngân sách cùng với vốn đầu tư từ doanh nghiệp.

. Xây dựng cơ chế thu hút các doanh nghiệp, viện trường tham gia phát triển công nghệ về an ninh mạng. Đầu tư một số dự án nghiên cứu cơ bản hoặc phát triển công nghệ cốt lõi về an ninh mạng có tầm quan trọng chiến lược từ nguồn kinh phí quốc phòng - an ninh, theo cơ chế tài chính đặc biệt.

. Huy động và triển khai hoạt động nghiên cứu, sáng tạo của các doanh nghiệp thành viên "Hiệp hội An ninh mạng quốc gia", gồm các cá nhân, tổ chức hàng đầu của Việt Nam về công nghệ cốt lõi để trở thành "cánh tay nối dài" trong sự nghiệp làm chủ, tiến tới tự chủ, tự cường của đất nước.

. Xây dựng Danh mục công nghệ, sản phẩm, dịch vụ an ninh mạng ưu tiên làm chủ, tự chủ.

- Bộ Quốc phòng

+ Hình thành hệ thống thông tin phục vụ nhiệm vụ quân sự, quốc phòng trên không gian mạng, gồm: hệ thống chỉ huy, hệ thống thông tin chiến lược, hệ thống cảnh báo nguy cơ không gian, biển, không gian số, vũ khí mới, hệ thống bảo vệ vùng trời, hệ thống bảo vệ vùng biển, hệ thống bảo vệ môi trường sinh học và hệ thống bảo vệ không gian mạng quốc gia theo chức năng, nhiệm vụ được giao.

+ Tạo điều kiện về cơ chế, chính sách, ưu tiên đầu tư cho các Viện nghiên cứu về sản phẩm, dịch vụ an toàn, an ninh mạng gắn với thực hiện nhiệm vụ quốc phòng trên không gian mạng.

+ Thúc đẩy các cơ quan, đơn vị, doanh nghiệp trực thuộc nghiên cứu, sản xuất sản phẩm, dịch vụ an toàn, an ninh mạng phù hợp với định hướng phát triển công nghiệp quốc phòng.

- Doanh nghiệp an toàn, an ninh mạng

+ Nghiên cứu, phát triển, tiếp nhận chuyển giao và làm chủ công nghệ an toàn, an ninh mạng.

+ Khuyến khích nghiên cứu, giải mã, phát triển, làm chủ được các công nghệ, sản phẩm, dịch vụ bảo đảm an toàn, an ninh mạng, bao gồm: các sản phẩm, dịch vụ truyền tải viễn thông, Internet và cung cấp dịch vụ nội dung trên mạng; các sản phẩm, dịch vụ, biện pháp bảo đảm an toàn, an ninh mạng; phòng, chống khủng bố mạng; các hệ thống giám sát an toàn, an ninh mạng diện rộng; các sản phẩm, dịch vụ an toàn, an ninh mạng tham gia giải quyết bài toán của xã hội.

b) Đặt nền móng cho công nghiệp an toàn thông tin mạng, phát triển sản phẩm an toàn thông tin mạng

- Doanh nghiệp an toàn thông tin mạng:

+ Chuyển dịch từ chiều rộng sang chiều sâu: tập trung phát triển 3 - 5 sản phẩm trọng điểm, có thương hiệu quốc gia. Phát triển sản phẩm, dịch vụ bảo đảm an toàn cho người dân trên môi trường mạng.

+ Chuyển dịch từ sản phẩm lớn, chuyên dụng sang sản phẩm phổ cập: "bình dân hóa" sản phẩm an toàn thông tin mạng, phục vụ đối tượng người dân, hộ gia đình.

+ Phát triển dịch vụ viễn thông, Internet, dịch vụ nền tảng số an toàn: các dịch vụ an toàn thông tin mạng được tích hợp vào các dịch vụ viễn thông, Internet, dịch vụ nền tảng số.

- Bộ Thông tin và Truyền thông

+ Hỗ trợ phát triển 02 nhóm doanh nghiệp an toàn thông tin mạng chủ đạo:

. Nhóm doanh nghiệp lớn có tiềm lực đóng vai trò dẫn dắt thị trường.

. Nhóm doanh nghiệp khởi nghiệp sáng tạo có các ý tưởng, giải pháp xuất sắc.

+ Chỉ đạo, thúc đẩy thiết lập Trung tâm nghiên cứu, phát triển, thử nghiệm sản phẩm, dịch vụ an toàn thông tin mạng quốc gia tại các doanh nghiệp ICT lớn.

+ Thúc đẩy triển khai mô hình an toàn thông tin mạng như dịch vụ (Security as a Service).

c) Xây dựng nền công nghiệp an ninh mạng với công nghệ, sản phẩm, dịch vụ an ninh mạng tiên tiến

- Thúc đẩy, chuyển giao công nghệ sở hữu trí tuệ về an ninh mạng.

- Xây dựng mạng lưới dịch vụ công nghệ về an ninh mạng. Hình thành các tổ chức đánh giá, thẩm định, giám định, định giá công nghệ an ninh mạng và tài sản trí tuệ, tư vấn, môi giới chuyển giao công nghệ về an ninh mạng.

- Hình thành mạng lưới chuyển giao công nghệ về an ninh mạng, có khả năng tìm kiếm, nhận dạng công nghệ, đối tác, phân tích nhu cầu thị trường, liên kết nhu cầu giữa nhà phát triển và người sử dụng công nghệ.

- Thí điểm thành lập quỹ đầu tư mạo hiểm để hỗ trợ doanh nghiệp khởi nghiệp và các dự án công nghệ về an ninh mạng mới. Có chính sách huy động đầu tư mạo hiểm của tư nhân và doanh nghiệp.

- Hình thành các doanh nghiệp dẫn đầu về công nghệ, sản phẩm, dịch vụ an ninh mạng, có khả năng nghiên cứu, chế tạo, sản xuất sản phẩm, dịch vụ an ninh mạng, tập trung vào 02 nhóm: nhóm doanh nghiệp có tiềm năng, tiềm lực lớn, có khả năng bắt tay vào nghiên cứu, chế tạo các sản phẩm dịch vụ an ninh mạng và nhóm doanh nghiệp khởi nghiệp, có nguồn nhân lực chất lượng cao, sáng tạo, có giải pháp xuất sắc, phù hợp với thực tiễn.

- Xác định được danh mục các sản phẩm, dịch vụ an ninh mạng trọng tâm trong chuyển đổi số, Cách mạng công nghiệp lần thứ tư để hỗ trợ phát triển, đạt chứng nhận tiêu chuẩn quốc tế, tiêu chuẩn Việt Nam, tiến tới hình thành thị trường xuất khẩu sản phẩm, dịch vụ an ninh mạng và mở rộng, chiếm lĩnh thị trường trong nước và quốc tế.

- Xây dựng các cơ chế hợp tác giữa quốc phòng, an ninh với dân sự, giữa nhà nước và tư nhân để nghiên cứu, phát triển, ứng dụng và chuyển giao công nghệ an ninh mạng.

- Thúc đẩy nghiên cứu, chế tạo sản phẩm, dịch vụ an ninh mạng trong các doanh nghiệp khởi nghiệp và trường, viện nghiên cứu, trong giáo dục phổ thông và đại học, đặc biệt trong sinh viên, học sinh, doanh nghiệp vừa và nhỏ.

- Tập trung đầu tư cho một số đề án, dự án lớn về tự chủ an ninh mạng. Đầu tư và triển khai Đề án "Trung tâm nghiên cứu, giải mã, sản xuất, chế tạo sản phẩm, dịch vụ công nghệ an toàn, an ninh mạng".

9. Đào tạo và phát triển nguồn nhân lực

a) Bộ Thông tin và Truyền thông

- Triển khai Đề án "Đào tạo và phát triển nguồn nhân lực an toàn thông tin giai đoạn 2021 - 2025"; nghiên cứu, đề xuất phương án thúc đẩy hoạt động trong lĩnh vực này giai đoạn 2026 - 2030.

- Phát triển đội ngũ chuyên gia xuất sắc về an toàn thông tin mạng để giải quyết các bài toán khó của đất nước.

- Phát triển và liên kết nguồn nhân lực an toàn thông tin trong các doanh nghiệp công nghệ số và doanh nghiệp an toàn thông tin mạng.

- Hướng dẫn, thúc đẩy triển khai quy định chuẩn kỹ năng an toàn thông tin mạng.

- Tuyên dương, khen thưởng kịp thời đối với các cơ quan, tổ chức, doanh nghiệp, cá nhân có cống hiến cho an toàn thông tin mạng quốc gia.

b) Bộ Công an

- Xây dựng cơ chế, chính sách, pháp luật về đào tạo nguồn nhân lực về bảo đảm an ninh mạng.

- Xây dựng đội ngũ nhà khoa học về an ninh mạng chất lượng cao, có uy tín quốc tế, có chế độ đãi ngộ phù hợp với thực tiễn công tác bảo đảm an ninh mạng. Khuyến khích các nhà khoa học về an ninh mạng trong nước tham gia các dự án an ninh mạng về quốc tế đa phương hoặc song phương, đặc biệt là các dự án, nhiệm vụ mà nước ta chưa có điều kiện đầu tư.

- Xây dựng đội ngũ kỹ sư an ninh mạng chất lượng cao, có khả năng nghiên cứu, chế tạo, sản xuất các sản phẩm, dịch vụ an ninh mạng, đóng vai trò quan trọng trong việc tiếp thu, chuyển giao tri thức về an ninh mạng, chính sách tôn vinh và đãi ngộ phù hợp.

- Phát hiện, đào tạo tài năng trẻ về an ninh mạng. Có chính sách ưu tiên đào tạo các tài năng trẻ, tạo điều kiện để du học nước ngoài, tài trợ nghiên cứu ở nước ngoài để về nước phát triển nền an ninh mạng quốc gia. Tăng cường tổ chức các hội nghị, hội thảo về an ninh mạng quốc tế ở Việt Nam nhằm phát huy vai trò của các nhà khoa học về an ninh mạng đồng thời tạo môi trường phát triển cho các tài năng trẻ.

- Thúc đẩy việc cải cách chương trình giáo dục với tinh thần đổi mới sáng tạo, phổ cập và cập nhật các tri thức bảo đảm an ninh mạng trong nhà trường.

- Tạo môi trường phát triển cạnh tranh, bình đẳng giữa doanh nghiệp an ninh mạng trong nước và nước ngoài.

- Nghiên cứu, hoàn thiện chính sách, pháp luật về việc sử dụng kinh phí từ nguồn ngân sách nhà nước để mời hoặc thuê dài hạn các chuyên gia về an ninh mạng quốc tế, đặc biệt các chuyên gia gốc Việt hoặc có liên hệ với Việt Nam, làm việc, giảng dạy, nghiên cứu phát triển và tham gia các nhiệm vụ về an ninh mạng tại Việt Nam.

- Triển khai Đề án "Đào tạo nguồn nhân lực an ninh mạng đến năm 2025, tầm nhìn đến năm 2030".

- Tuyên dương, khen thưởng kịp thời đối với các cơ quan, tổ chức, doanh nghiệp, cá nhân có cống hiến về bảo đảm an ninh mạng.

c) Bộ Quốc phòng

- Chủ trì, phối hợp với các bộ, cơ quan liên quan xây dựng và triển khai thực hiện có hiệu quả các chương trình, đề án đào tạo, phát triển nguồn nhân lực cho lực lượng tác chiến không gian mạng.

- Đầu tư xây dựng cơ sở vật chất, kỹ thuật phục vụ huấn luyện, bồi dưỡng nghiệp vụ và nghiên cứu khoa học về tác chiến không gian mạng; nghiên cứu, xây dựng chế độ, chính sách cho lực lượng tác chiến không gian mạng và các lực lượng tham gia bảo vệ Tổ quốc trên không gian mạng.

10. Tuyên truyền, phổ biến, nâng cao nhận thức và kỹ năng an toàn, an ninh mạng

a) Bộ Thông tin và Truyền thông

- Triển khai Đề án "Tuyên truyền, nâng cao nhận thức và phổ biến kiến thức về an toàn thông tin giai đoạn 2021 - 2025".

- Tăng cường các hoạt động tuyên truyền, nâng cao nhận thức và phổ biến kiến thức, trang bị kỹ năng bảo đảm an toàn thông tin tới toàn thể người sử dụng Internet; triển khai hoạt động trang bị kỹ năng cho các nhóm người yếu thế, dễ bị tổn thương trong xã hội.

- Thực hiện phổ cập các sản phẩm, dịch vụ an toàn thông tin mạng cơ bản cho người sử dụng.

- Xây dựng, hoàn thiện các cơ chế, chính sách và thiết lập các kênh liên hệ, trao đổi để người sử dụng có thể thuận lợi phản ánh, chia sẻ và chung tay bảo đảm an toàn thông tin mạng quốc gia.

- Triển khai các khóa học trực tuyến mở (MOOC) tuyên truyền, phổ biến kỹ năng an toàn thông tin cơ bản cho người dùng.

b) Bộ Công an

- Xây dựng và triển khai Đề án "Tuyên truyền, nâng cao nhận thức và phổ biến kiến thức về an ninh mạng".

- Tổ chức các chiến dịch tuyên truyền, nâng cao nhận thức, kiến thức về bảo đảm an ninh mạng hàng năm, có quy mô lớn, trên phạm vi cả nước, với sự tham gia của các phương tiện truyền thông, báo chí, cơ quan, tổ chức, doanh nghiệp từ trung ương tới địa phương.

- Thiết lập các kênh, mạng xã hội để tuyên truyền, nâng cao nhận thức về bảo đảm an ninh mạng đối với quần chúng nhân dân về âm mưu, phương thức, thủ đoạn, các hành vi xâm phạm an ninh mạng, nâng cao sức đề kháng trước các thông tin xấu độc, thủ đoạn của các loại tội phạm sử dụng công nghệ cao.

- Xây dựng, ban hành Bộ kỹ năng bảo đảm an ninh mạng khi tham gia không gian mạng.

c) Cơ quan, tổ chức, doanh nghiệp

- Cung cấp kịp thời các thông tin chính thống để người dân nắm bắt, cùng phản biện tin giả, thông tin vi phạm pháp luật trên môi trường mạng.

- Trong phạm vi quản lý, tổ chức triển khai các kế hoạch tuyên truyền, phổ biến về thói quen, trách nhiệm, kỹ năng an toàn, an ninh mạng cho cán bộ, công chức, viên chức, người lao động khi tham gia hoạt động trên không gian mạng.

- Các cơ sở giáo dục, đào tạo xây dựng chương trình, kế hoạch học tập, rèn luyện kỹ năng tư duy phản biện cho học sinh, sinh viên về an toàn, an ninh mạng đối với các thông tin sai lệch trên không gian mạng.

- Các doanh nghiệp cung cấp dịch vụ trong và ngoài nước thực hiện tuyên truyền, nâng cao nhận thức, phổ biến kiến thức về an toàn, an ninh mạng; có biện pháp kỹ thuật hạn chế tin giả, tin sai sự thật, xấu, độc trên nền tảng, dịch vụ của mình.

- Các tổ chức truyền thông, báo chí tăng cường thông tin về xu hướng, kiến thức, tình hình, nguy cơ, hậu quả an toàn, an ninh mạng thế giới và Việt Nam.

11. Nâng cao uy tín quốc gia và hợp tác quốc tế

a) Bộ Công an

- Chủ động mở rộng hợp tác quốc tế về bảo đảm an ninh mạng với các nước, đặc biệt là các nước đối tác chiến lược có trình độ khoa học công nghệ tiên tiến, phục vụ sự nghiệp bảo vệ an ninh quốc gia, trật tự an toàn xã hội trong tình hình mới. Chủ động tham gia mạng lưới đổi mới sáng tạo toàn cầu, trong đó nghiên cứu, đổi mới về an ninh mạng.

- Đẩy mạnh thu hút và sử dụng hiệu quả các nguồn lực từ nước ngoài và các đối tác quốc tế cho hoạt động nghiên cứu, ứng dụng, đổi mới sáng tạo, khởi nghiệp, chuyển giao công nghệ về bảo đảm an ninh mạng.

- Rà soát, sửa đổi các quy định luật pháp, cơ chế chính sách hợp tác quốc tế về bảo đảm an ninh mạng cho phù hợp với luật pháp và thông lệ quốc tế. Chủ động tham mưu trong việc tham gia các hiệp định, thỏa thuận quốc tế về an ninh mạng để có được cơ sở pháp lý quốc tế trong việc bảo vệ lợi ích quốc gia, quyền và lợi ích hợp pháp của các doanh nghiệp hoạt động trong lĩnh vực này.

- Triển khai, mở rộng các chương trình, kế hoạch hợp tác nhằm mục tiêu xây dựng, thiết lập vị trí, vai trò của Việt Nam về an ninh mạng tại các địa bàn chiến lược, liên quan trực tiếp tới an ninh quốc gia Việt Nam, góp phần bảo vệ lợi ích, an ninh quốc gia Việt Nam từ xa, từ sớm.

- Tăng cường hợp tác phòng, chống tội phạm qua các kênh quốc tế, như INTERPOL, ASEANAPOL. Cử cán bộ tham gia các diễn đàn, tổ chức quốc tế về phòng, chống tội phạm mạng để nâng cao trình độ, kiến thức và biện pháp kỹ thuật, kinh nghiệm phòng, chống tội phạm mới.

- Tham gia xây dựng luật quốc tế và các tiêu chuẩn, nguyên tắc, các Bộ quy tắc quốc tế, hướng dẫn toàn cầu về an ninh mạng.

- Tham gia vào các tổ chức, diễn đàn quốc tế và khu vực về không gian mạng, an ninh mạng; phối hợp với các quốc gia, nhất là các quốc gia trong khu vực và quốc gia có quan hệ là đối tác chiến lược, đối tác toàn diện của Việt Nam về an ninh mạng.

- Tham gia các Nhóm công tác của Liên hợp quốc, các tổ chức thuộc Liên hợp quốc, các tổ chức quốc tế và các Nhóm chuyên gia về không gian mạng, an ninh mạng.

b) Bộ Thông tin và Truyền thông

- Tăng cường hợp tác song phương với các quốc gia trên thế giới về an toàn thông tin mạng. Tham gia xây dựng luật quốc tế và các tiêu chuẩn, nguyên tắc, quy tắc quốc tế về an toàn thông tin mạng.

- Tham gia vào các tổ chức, diễn đàn quốc tế và khu vực; phối hợp với các quốc gia, nhất là các quốc gia trong khu vực và quốc gia có quan hệ là đối tác chiến lược, đối tác toàn diện của Việt Nam trong việc chia sẻ thông tin, hỗ trợ lẫn nhau phát hiện, xử lý, ứng cứu khi xảy ra tấn công mạng xuyên biên giới. Đẩy mạnh thể hiện vai trò thành viên sáng lập của Diễn đàn GFCE.

- Tham gia các Nhóm công tác kỹ thuật của ITU (SG13, SG17, SG20), Diễn đàn quản trị Internet (IGF), Diễn đàn Chuyên gia không gian mạng toàn cầu (GFCE), Ủy ban kỹ thuật hỗn hợp ISO/IEC về Công nghệ thông tin (JTC1).

- Tiên phong nghiên cứu, tham gia tích cực giải quyết các vấn đề quốc tế mới, khó về chính sách và kỹ thuật liên quan đến an toàn thông tin mạng.

c) Bộ Quốc phòng

- Tăng cường, thúc đẩy hợp tác quốc tế về an toàn thông tin, an ninh mạng theo chức năng, nhiệm vụ được giao nhằm nâng cao hiệu quả phòng, chống chiến tranh thông tin, chiến tranh không gian mạng, bảo vệ chủ quyền quốc gia trên không gian mạng.

- Phối hợp với Bộ Công an, Bộ Thông tin và Truyền thông, Bộ Ngoại giao tham gia hợp tác với các quốc gia về an toàn, an ninh mạng.

d) Bộ Ngoại giao

Phối hợp Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông thúc đẩy hợp tác quốc tế với các quốc gia hàng đầu về an toàn, an ninh mạng, phù hợp với quy định của pháp luật.

12. Đầu tư nguồn lực và bảo đảm kinh phí thực hiện

a) Bố trí đủ nhân lực chuyên trách, chịu trách nhiệm về an toàn, an ninh mạng trong các cơ quan, tổ chức nhà nước.

b) Đầu tư nguồn lực để xây dựng hệ thống kỹ thuật, công cụ và triển khai các hoạt động bảo đảm an toàn, an ninh mạng và trong hoạt động của các cơ quan, tổ chức.

c) Xây dựng cơ chế tiền lương đặc thù cho lực lượng chuyên trách về an toàn thông tin mạng và an ninh mạng trong các cơ quan, tổ chức nhà nước.

d) Ưu tiên bố trí nguồn lực để triển khai các Đề án và xây dựng các hệ thống kỹ thuật bảo đảm an toàn, an ninh mạng quy mô quốc gia.

đ) Bố trí kinh phí chi cho an toàn, an ninh mạng đạt tối thiểu 10% kinh phí chi cho khoa học công nghệ, chuyển đổi số, ứng dụng công nghệ thông tin.

e) Nguồn vốn chi thường xuyên từ ngân sách trung ương được phân bổ để thực hiện các nhiệm vụ thuộc Chiến lược do các cơ quan ở trung ương thực hiện.

g) Ngân sách địa phương bảo đảm kinh phí thực hiện các nhiệm vụ thuộc Chiến lược do các cơ quan thuộc địa phương thực hiện.

h) Ưu tiên nguồn vốn khoa học và công nghệ, nguồn vốn từ các chương trình quốc gia để phát triển công nghệ cao, chương trình phát triển sản phẩm quốc gia để phát triển sản phẩm, dịch vụ, giải pháp nội địa và các nhiệm vụ nghiên cứu, phát triển, chuyển giao công nghệ thuộc Chiến lược.

V. TỔ CHỨC THỰC HIỆN

1. Ban Chỉ đạo An toàn, An ninh mạng quốc gia

a) Giúp Thủ tướng Chính phủ, Trưởng Ban Chỉ đạo An toàn, An ninh mạng quốc gia chỉ đạo sơ kết, tổng kết việc thực hiện Chiến lược này.

b) Đề xuất với Thủ tướng Chính phủ chỉ đạo, điều phối xử lý các vấn đề mới, quan trọng, liên ngành, chưa được quy định hoặc chồng chéo, phức tạp về an toàn, an ninh mạng trong nội dung Chiến lược này, cần sự phối hợp giữa các bộ, ngành, cơ quan chức năng.

2. Bộ Công an

a) Chủ trì, phối hợp hướng dẫn, đôn đốc, kiểm tra các cơ quan, tổ chức, doanh nghiệp triển khai thực hiện các nội dung về an ninh mạng tại Chiến lược; tổ chức sơ kết, tổng kết, tổng hợp, báo cáo Thủ tướng Chính phủ tình hình thực hiện và đề xuất, kiến nghị nhiệm vụ mới cho phù hợp với tình hình thực tiễn đối với các nội dung về an ninh mạng thuộc Chiến lược.

b) Chủ trì, phối hợp với các bộ, ngành, địa phương và tổ chức, doanh nghiệp liên quan thực hiện các nhiệm vụ đã giao Bộ Công an tại phần IV; thực hiện nhiệm vụ tại Mục 1, điểm d Mục 2, Mục 3, các điểm a và d Mục 4, điểm e Mục 5, điểm b Mục 6 phần IV theo chức năng, nhiệm vụ được giao.

c) Xây dựng phương án bảo đảm an ninh chính trị nội bộ, an ninh kinh tế tại các bộ, ngành có cơ sở hạ tầng không gian mạng, hạ tầng số, nền tảng quan trọng phục vụ chuyển đổi số, phát triển kinh tế số, xã hội số theo chức năng, nhiệm vụ được giao.

3. Bộ Thông tin và Truyền thông

a) Chủ trì, phối hợp, hướng dẫn, đôn đốc, kiểm tra các cơ quan, tổ chức, doanh nghiệp tổ chức triển khai thực hiện các nội dung về an toàn thông tin mạng tại Chiến lược này; tổ chức sơ kết, tổng kết, tổng hợp, báo cáo Thủ tướng Chính phủ tình hình thực hiện và đề xuất, kiến nghị nhiệm vụ mới cho phù hợp với tình hình thực tiễn đối với các nội dung về an toàn thông tin mạng thuộc Chiến lược.

b) Chủ trì, phối hợp với các bộ, ngành, địa phương và tổ chức, doanh nghiệp liên quan thực hiện các nhiệm vụ đã giao Bộ Thông tin và Truyền thông tại phần IV; thực hiện nhiệm vụ tại các Mục 1, điểm d Mục 2, Mục 3, các điểm a và d Mục 4, điểm e Mục 5, điểm b Mục 6 phần IV theo chức năng, nhiệm vụ được giao.

4. Bộ Quốc phòng

a) Thực hiện phòng ngừa, ứng phó, xử lý các nguy cơ, thách thức từ không gian mạng theo chức năng, nhiệm vụ được giao.

b) Chủ trì, phối hợp với các bộ, ngành, địa phương và tổ chức, doanh nghiệp liên quan thực hiện các nhiệm vụ đã giao Bộ Quốc phòng tại phần IV; thực hiện nhiệm vụ tại các Mục 1, điểm d Mục 2, Mục 3, các điểm a và d Mục 4, điểm e Mục 5, điểm b Mục 6 phần IV theo chức năng, nhiệm vụ được giao.

5. Bộ Khoa học và Công nghệ

Chủ trì, phối hợp với Bộ Công an, Bộ Thông tin và Truyền thông và các cơ quan, tổ chức, doanh nghiệp liên quan nghiên cứu, thực hiện chuyển giao công nghệ và xây dựng, ban hành các tiêu chuẩn kỹ thuật về an toàn, an ninh mạng.

6. Bộ Nội vụ

Chủ trì, phối hợp với Bộ Công an, Bộ Thông tin và Truyền thông, Bộ Tài chính xây dựng cơ chế tiền lương đặc thù cho lực lượng chuyên trách về an toàn thông tin mạng và an ninh mạng trong các cơ quan, tổ chức nhà nước.

7. Bộ Ngoại giao

Phối hợp với Bộ Quốc phòng, Bộ Công an, Bộ Thông tin và Truyền thông nghiên cứu, xây dựng và trình cấp có thẩm quyền ký kết thỏa thuận hợp tác quốc tế về an toàn, an ninh mạng đối với một số quốc gia hàng đầu về an toàn, an ninh mạng; tăng cường hợp tác song phương với các quốc gia trên thế giới về an toàn, an ninh mạng; triển khai các biện pháp ngoại giao, hợp tác quốc tế về an toàn, an ninh mạng.

8. Bộ Kế hoạch và Đầu tư, Bộ Tài chính ưu tiên bố trí kinh phí từ ngân sách nhà nước để triển khai các nhiệm vụ của Chiến lược theo quy định của pháp luật về đầu tư công, pháp luật về ngân sách nhà nước.

9. Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Uỷ ban nhân dân các tỉnh, thành phố trực thuộc trung ương

a) Chủ trì, phối hợp Bộ Công an, Bộ Thông tin và Truyền thông tổ chức thực hiện các nhiệm vụ được giao tại Chiến lược.

b) Đẩy mạnh hoạt động bảo đảm an toàn, an ninh mạng trong phạm vi quản lý; tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật, hướng dẫn nghiệp vụ của Bộ Công an, Bộ Thông tin và Truyền thông và quy định của pháp luật; ưu tiên sử dụng sản phẩm, giải pháp, dịch vụ an toàn thông tin mạng Make in Viet Nam, an ninh mạng tự chủ. Gắn kết công tác bảo đảm an toàn, an ninh mạng với công tác triển khai chuyển đổi số, ứng dụng công nghệ thông tin, phát triển Chính phủ điện tử hướng tới Chính phủ số, phát triển đô thị thông minh, kinh tế số và xã hội số.

c) Chủ động rà soát, phát hiện và xử lý, hoặc phối hợp với cơ quan chức năng có thẩm quyền xử lý thông tin vi phạm pháp luật trên môi trường mạng thuộc phạm vi quản lý. Tăng cường hoạt động thanh tra, kiểm tra, công bố và xử lý nghiêm các hành vi vi phạm.

d) Chỉ đạo các tập đoàn, tổng công ty, doanh nghiệp thuộc phạm vi quản lý rà soát, đánh giá, có biện pháp tăng cường bảo đảm an toàn, an ninh mạng đối với các hệ thống hạ tầng thông tin, hệ thống điều khiển công nghiệp và các hệ thống thông tin quan trọng khác do doanh nghiệp quản lý, vận hành, khai thác.

đ) Ưu tiên bố trí nguồn lực (nhân lực, kinh phí) và điều kiện để triển khai hoạt động bảo đảm an toàn, an ninh mạng trong hoạt động nội bộ của cơ quan, tổ chức và lĩnh vực quản lý.

e) Kiểm tra, đánh giá và báo cáo hàng năm hoặc đột xuất theo hướng dẫn của Bộ Công an, Bộ Thông tin và Truyền thông về tình hình, kết quả triển khai Chiến lược để tổng hợp, báo cáo Thủ tướng Chính phủ theo quy định về chế độ báo cáo.

10. Ban Cơ yếu Chính phủ

a) Phát triển hạ tầng mật mã quốc gia để bảo vệ thông tin phục vụ lãnh đạo, chỉ đạo, chỉ huy của Đảng, Nhà nước và các lực lượng vũ trang được truyền, lưu giữ trên không gian mạng.

b) Chủ trì, phối hợp với Bộ Thông tin và Truyền thông, các cơ quan liên quan thúc đẩy việc ứng dụng, sử dụng chữ ký số chuyên dùng Chính phủ và bảo mật thông tin trên hệ thống mạng của cơ quan, tổ chức thuộc hệ thống chính trị theo quy định của pháp luật về cơ yếu.

11. Các tập đoàn, tổng công ty, doanh nghiệp nhà nước

Căn cứ nội dung của Chiến lược này, tổ chức triển khai công tác bảo đảm an toàn, an ninh mạng trong hoạt động của doanh nghiệp theo hướng dẫn của Bộ Công an, Bộ Thông tin và Truyền thông.

12. Hiệp hội An ninh mạng quốc gia, Hiệp hội An toàn thông tin Việt Nam

a) Phối hợp chặt chẽ với Bộ Công an, Bộ Thông tin và Truyền thông trong triển khai thực các nhiệm vụ tại Chiến lược.

b) Vận động các hội viên, doanh nghiệp tích cực nghiên cứu, phát triển, sản xuất, cung cấp sản phẩm, dịch vụ, giải pháp an toàn, an ninh mạng chất lượng cao; vận động các cơ quan, tổ chức ưu tiên sử dụng sản phẩm, dịch vụ, giải pháp an toàn thông tin mạng Make in Viet Nam và giải pháp an ninh mạng tự chủ.

13. Các doanh nghiệp viễn thông, Internet, doanh nghiệp chủ quản nền tảng số

a) Chủ động, tích cực phối hợp triển khai công tác bảo đảm an toàn, an ninh mạng trong hoạt động của doanh nghiệp.

b) Tuân thủ các hướng dẫn, yêu cầu của Bộ Công an, Bộ Thông tin và Truyền thông trong hoạt động phát triển hạ tầng số, nền tảng số và bảo vệ dữ liệu số.

c) Định kỳ hàng năm hoặc đột xuất báo cáo Bộ Công an, Bộ Thông tin và Truyền thông tình hình, kết quả triển khai các nhiệm vụ theo hướng dẫn.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký ban hành.

Điều 3. Các Bộ trưởng, Thủ trưởng cơ quan ngang bộ, Thủ trưởng cơ quan thuộc Chính phủ, Chủ tịch Ủy ban nhân dân tỉnh, thành phố trực thuộc trung ương và Thủ trưởng các cơ quan, tổ chức, doanh nghiệp liên quan chịu trách nhiệm thi hành Quyết định này

Nơi nhận:
- Ban Bí thư Trung ương Đảng;
- Thủ tướng, các Phó Thủ tướng Chính phủ;
- Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- HĐND, UBND các tỉnh, thành phố trực thuộc trung ương;
- Văn phòng Trung ương và các Ban của Đảng;
- Văn phòng Tổng Bí thư;
- Văn phòng Chủ tịch nước;
- Hội đồng Dân tộc và các Ủy ban của Quốc hội;
- Văn phòng Quốc hội;
- Tòa án nhân dân tối cao;
- Viện kiểm sát nhân dân tối cao;
- Kiểm toán nhà nước;
- Ủy ban Giám sát tài chính Quốc gia;
- Ngân hàng Chính sách xã hội;
- Ngân hàng Phát triển Việt Nam;
- Ủy ban trung ương Mặt trận Tổ quốc Việt Nam;
- Cơ quan trung ương của các đoàn thể;
- VPCP: BTCN, các PCN, Trợ lý TTg, TGĐ Cổng TTĐT, các Vụ, Cục;
- Lưu: VT, KSTT (2b).110

KT. THỦ TƯỚNG
PHÓ THỦ TƯỚNG

Vũ Đức Đam