

BỘ CÔNG AN

ĐỀ ÁN
NGÀY AN NINH MẠNG VIỆT NAM

Hà Nội - 2023

MỤC LỤC

I. SỰ CẦN THIẾT	1
II. CƠ SỞ CHÍNH TRỊ VÀ CƠ SỞ PHÁP LÝ.....	7
III. MỤC ĐÍCH, YÊU CẦU.....	10
IV. NỘI DUNG ĐỀ ÁN	11
1. Lựa chọn Ngày An ninh mạng Việt Nam	11
2. Các hoạt động Ngày An ninh mạng Việt Nam	11
3. Công tác thông tin, tuyên truyền về Ngày An ninh mạng Việt Nam	12
V. TỔ CHỨC THỰC HIỆN.....	13
V. KINH PHÍ THỰC HIỆN.....	13

I. SỰ CẦN THIẾT

1. Ngày An ninh mạng Việt Nam sẽ góp phần tăng cường công tác bảo đảm an ninh mạng, góp phần quan trọng phát triển kinh tế, xã hội của đất nước trong thời đại Cách mạng công nghiệp lần thứ tư, chuyển đổi số

Không gian mạng với nền tảng là khoa học, đổi mới, sáng tạo đang phát triển nhanh, đột phá, tác động sâu rộng trên nhiều lĩnh vực của đời sống xã hội, trở thành nhân tố quyết định đối với năng lực cạnh tranh của mỗi quốc gia. Cách mạng công nghiệp lần thứ tư là cuộc cách mạng của khoa học công nghệ, với sự phát triển của Internet kết nối vạn vật, các công nghệ xử lý dữ liệu lớn, dữ liệu nhanh và máy tính lượng tử, ứng dụng trí tuệ nhân tạo, các hệ thống kết nối thực ảo mang lại sự sáng tạo, đột phá, có thể làm thay đổi phương thức sản xuất của con người. Công nghệ là nền tảng cho sự phát triển, đổi mới và hội nhập quốc tế, giúp đất nước phát triển lên một tầm cao mới. Quá trình xây dựng, phát triển luôn gắn với quá trình bảo đảm an toàn, an ninh mạng, với các nhiệm vụ trọng tâm, trụ cột là xác định, bảo vệ chủ quyền, lợi ích quốc gia trên không gian mạng, bảo đảm trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân. Bảo vệ để phát triển trở thành bài toán cho mô hình, phương thức quản lý mới của mỗi quốc gia trong thời đại không gian mạng, với những thời cơ sau:

Một là, mở rộng phạm vi chủ quyền và lợi ích quốc gia trên không gian mạng. Đảng và Nhà nước hiện nay đang tập trung thúc đẩy phát triển kinh tế, xã hội trên không gian mạng, coi đây là ưu tiên chiến lược của quốc gia. Đại dịch Covid-19 tác động sâu sắc đến trật tự, cấu trúc kinh tế, phương thức quản trị quốc gia và cách thức hoạt động của đời sống xã hội nhưng cũng đồng thời mở ra cơ hội mới cho quốc gia xây dựng mô hình phát triển mới, gắn với khoa học công nghệ. Cơ sở hạ tầng không gian mạng, cơ sở dữ liệu quốc gia, dữ liệu cá nhân, quyền quản lý và kiểm soát không gian mạng là những trụ cột cho quá trình xây dựng và phát triển mô hình quản trị mới của quốc gia. Những trụ cột này gắn liền và không thể tách rời với công tác bảo đảm an toàn, an ninh mạng, làm căn cơ nền tảng cho xác định chủ quyền quốc gia trên không gian mạng, lãnh thổ mạng, biên giới mạng, cửa khẩu mạng, lợi ích quốc gia trên không gian mạng, phát triển xã hội số.

Hai là, hình thành Thế trận An ninh nhân dân trên không gian mạng. Việt Nam là một trong những quốc gia có số lượng người sử dụng Internet lớn nhất thế giới. Tính tới thời điểm tháng 01/2024, nước ta có gần 79 triệu người sử dụng Internet, tương đương hơn 73% dân số tham gia hoạt động trên không gian mạng. Sự tham gia đông đảo của quần chúng nhân dân trên không gian mạng là nguồn lực lớn cho đất nước trong phát triển kinh tế, xã hội. Quy mô hoạt động kinh tế trên không gian mạng ngày một lớn, từ 3 tỷ USD năm 2015 lên 14 tỷ USD năm 2020 và dự kiến đạt 52 tỷ USD vào năm 2025. Hiện nay, quá trình chuyển đổi số

đang diễn ra mạnh mẽ, các phương thức sản xuất dần được số hóa. Quyền và lợi ích hợp pháp của tổ chức cá nhân gắn liền với quá trình hình thành và phát triển của không gian mạng, trở thành nhiệm vụ trọng yếu của công tác bảo đảm an toàn, an ninh mạng. Nhiệm vụ quan trọng của công tác bảo đảm an ninh mạng là phải xây dựng, hình thành được Thế trận An ninh nhân dân trên không gian mạng trên cơ sở sự tham gia đồng đảo của quần chúng nhân dân.

Ba là, hoàn thiện mô hình quản trị quốc gia về không gian mạng, nâng cao thế và lực của quốc gia. Quản lý, phát triển không gian mạng trở thành động lực, trụ cột cho phát triển kinh tế xã hội đã được Đảng, Nhà nước quan tâm, chỉ đạo nhằm đạt mục tiêu bảo đảm chủ quyền, lợi ích, an ninh quốc gia, bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia, nâng cao năng lực tự chủ, làm chủ, chiếm lĩnh thị trường, xây dựng, phát triển nền công nghiệp an ninh mạng, ngành nghề về sản phẩm, dịch vụ an ninh mạng, đào tạo nguồn nhân lực chất lượng cao, đẩy mạnh ứng dụng, phát triển khoa học, công nghệ và đổi mới sáng tạo, nghiên cứu nắm bắt, nâng cao năng lực tiếp cận và chủ động đón nhận cơ hội do không gian mạng mang lại, được thể hiện qua Nghị quyết 52-NQ/TW ngày 27-9-2019 của Bộ Chính trị về chủ trương, chính sách chủ động tham gia cuộc Cách mạng công nghiệp lần thứ tư, Nghị quyết 30-NQ/TW ngày 25-7-2018 của Bộ Chính trị về Chiến lược An ninh mạng quốc gia.

Bốn là, huy động lực lượng có trình độ khoa học công nghệ cao vào sự nghiệp phát triển kinh tế, xã hội. Phát triển nhanh và bền vững dựa chủ yếu vào khoa học công nghệ, đổi mới sáng tạo là một trong những quan điểm của Đảng, Nhà nước được thể hiện trong Chiến lược phát triển kinh tế - xã hội 10 năm 2021 - 2030. Căn bản của sự phát triển nhanh và bền vững là nguồn nhân lực. Con người yếu tố trung tâm của các cuộc cách mạng khoa học công nghệ và sự “nhảy vọt thần kỳ” của một số quốc gia. Nguồn nhân lực về an toàn, an ninh mạng là nguồn nhân lực chất lượng cao, có trình độ về khoa học công nghệ, có thể được sử dụng vào mục tiêu kép là “vừa bảo vệ vừa phát triển”, đồng thời thực hiện các nhiệm vụ phát triển kinh tế xã hội. Trong kỷ nguyên các hoạt động kinh tế gắn liền với yếu tố kỹ thuật, công nghệ, an ninh mạng, yêu cầu bảo vệ chủ quyền, lợi ích, an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân trên không gian mạng giữ vai trò quan trọng, có quan hệ mật thiết với quá trình phát triển kinh tế, xã hội của đất nước.

Bốn là, góp phần thực hiện thắng lợi công cuộc chuyển đổi số quốc gia. Ngày 27 tháng 9 năm 2019, Bộ Chính trị đã ban hành Nghị quyết số 52-NQ/TW về một số chủ trương, chính sách chủ động tham gia cuộc Cách mạng công nghiệp lần thứ tư, trong đó nhấn mạnh yêu cầu cấp bách để đẩy nhanh quá trình chuyển đổi số. Chính phủ cũng đã ban hành Chương trình hành động của Chính phủ thực hiện Nghị quyết số 52-NQ/TW ngày 27 tháng 9 năm 2019 của Bộ

Chính trị. Trên cơ sở đó, ngày 03 tháng 6 năm 2020, Thủ tướng Chính phủ đã ban hành Quyết định số 749/QĐ-TTg phê duyệt “Chương trình Chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030”. Đại hội đại biểu toàn quốc lần thứ XIII của Đảng đề cao ý chí, khát vọng phát triển đất nước, đề đến năm 2025 đưa nước ta trở thành nước có công nghiệp theo hướng hiện đại, vượt mức thu nhập trung bình thấp; đến năm 2030, nước ta trở thành nước có công nghiệp hiện đại, thu nhập trung bình cao và đến năm 2045, nước ta trở thành nước phát triển, có thu nhập cao. Trong đó, chủ trương đẩy mạnh chuyển đổi số, phát triển kinh tế số là một trong những biểu hiện cụ thể thể hiện ý chí, khát vọng phát triển đất nước đó. Đây chính là mục tiêu, ý nghĩa của việc đẩy mạnh chuyển đổi số, phát triển kinh tế số ở nước ta; là lý do để Đại hội XIII của Đảng đặc biệt nhấn mạnh chủ trương chuyển đổi số, phát triển kinh tế số trong các văn kiện Đại hội. Nội dung về chuyển đổi số, phát triển kinh tế số được đề cập đến nhiều lần trong các văn kiện Đại hội XIII; được đưa vào Báo cáo chính trị thành một trong những nhiệm vụ trọng tâm và các đột phá chiến lược trong nhiệm kỳ Đại hội XIII. Báo cáo chiến lược phát triển kinh tế - xã hội 10 năm 2021 - 2030 xác định “phải đổi mới tư duy phát triển, thay đổi cách làm việc, cách sống, đẩy mạnh cải cách thể chế, ứng dụng tiến bộ khoa học - công nghệ và đổi mới sáng tạo; thực hiện quyết liệt chuyển đổi số, xây dựng nền kinh tế số, xã hội số”. Báo cáo chính trị đề ra 12 định hướng phát triển đất nước trong giai đoạn 2021-2030; một trong những định hướng đó xác định phải đẩy mạnh chuyển đổi số quốc gia, phát triển kinh tế số trên nền tảng khoa học - công nghệ và đổi mới sáng tạo. Chiến lược phát triển kinh tế - xã hội 10 năm 2021 - 2030 đưa ra 5 quan điểm phát triển; trong đó, có 2 quan điểm nhấn mạnh về chuyển đổi số, phát triển kinh tế số. Muốn thực hiện thành công chuyển đổi số, vai trò, sứ mệnh của không gian mạng là yếu tố cốt lõi

2. Ngày An ninh mạng Việt Nam sẽ góp phần chủ động ứng phó với nguy cơ, thách thức từ không gian mạng, bảo đảm quá trình phát triển kinh tế, xã hội của đất nước hiệu quả, bền vững

Đại hội Đảng toàn quốc lần thứ XIII đã xác định: “An ninh mạng ngày càng tác động mạnh, nhiều mặt, đe dọa nghiêm trọng đến sự phát triển ổn định, bền vững của thế giới, khu vực và đất nước ta. Thực tiễn thời gian qua cho thấy, không gian mạng đã và đang làm thay đổi phương thức hoạt động, tổ chức cách thức tiến hành chiến tranh, can dự/can thiệp của các nước; cũng như nhiều khía cạnh khác của hoạt động an ninh, quân sự, tình báo, tội phạm. Tác chiến mạng đã trở thành một loại hình tác chiến hiện đại; an ninh mạng là ưu tiên hàng đầu trong chiến lược an ninh quốc gia của nhiều nước trên thế giới; thậm chí đã được sử dụng là lực lượng, chiến thuật tiên phong, mở đường cho hoạt động quân sự

truyền thông; là vũ khí quan trọng để tiến hành âm mưu, ý đồ “cách mạng màu”, “cách mạng đường phố”.

Nghị quyết số 30-NQ/TW ngày 25 tháng 7 năm 2018 của Bộ Chính trị về Chiến lược An ninh mạng quốc gia đã khẳng định, nhiệm vụ của công tác bảo vệ an ninh mạng là bảo vệ vững chắc an ninh quốc gia, trật tự an toàn xã hội trên không gian mạng; phòng ngừa, phát hiện, ngăn chặn, xử lý hiệu quả các hành vi xâm phạm an ninh mạng quốc gia, góp phần bảo vệ vững chắc chủ quyền, lợi ích quốc gia; xây dựng không gian mạng an toàn, lành mạnh, trở thành nguồn lực mạnh mẽ cho xây dựng, phát triển và bảo vệ Tổ quốc.

Thực tiễn công tác bảo vệ an ninh mạng thời gian qua đã cho thấy, không gian mạng đang đặt ra nhiều nguy cơ, thách thức đối với an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân. Cụ thể:

Thách thức về bảo vệ nền tảng tư tưởng của Đảng, Nhà nước trên không gian mạng: Không gian mạng trở thành môi trường thực hiện các hoạt động xuyên tạc, tấn công vào hệ thống lý luận, nền tảng tư tưởng của Đảng, phủ nhận vai trò lãnh đạo của Đảng, con đường đi lên chủ nghĩa xã hội của nước ta, tổ chức các chiến dịch xuyên tạc, bôi xấu đất nước. Hoạt động tán phát tin giả, sai sự thật, thông tin xấu độc, kích động hận thù tiếp tục diễn biến phức tạp và sẽ còn tồn tại, gắn liền với sự phát triển của không gian mạng. Các đối tượng triệt để sử dụng các tiện ích như mạng xã hội, website, blog để tuyên truyền phá hoại tư tưởng, đưa thông tin trái ngược với thuần phong mỹ tục, làm thay đổi nhận thức, suy nghĩ và lối sống của một bộ phận quần chúng nhân dân, cổ vũ lối sống không đúng chuẩn mực, kêu gọi tham gia các phong trào, tổ chức vi phạm pháp luật, thúc đẩy hình thành các luồng tư tưởng cực đoan, kích động các hoạt động khủng bố, bạo lực.

Thách thức về bảo vệ chủ quyền không gian mạng quốc gia: Nhiều quốc gia trên thế giới đã ban hành các văn bản quy định về chủ quyền không gian mạng quốc gia, quy định về Chủ quyền lãnh thổ mạng, Quyền kiểm soát hoạt động mạng trên lãnh thổ mạng quốc gia, Quyền tài phán, Quyền pháp lý theo quốc kỳ và hồ sơ đăng ký tại quốc gia, Quyền miễn trừ quốc gia. Trong khi đó, nước ta chưa có văn bản quy định về vấn đề này. Điều này đặt ra nhiều thách thức trong công tác bảo vệ chủ quyền, lợi ích, an ninh quốc gia trên không gian mạng.

Thách thức về tấn công mạng: Hoạt động tấn công mạng nhằm vào hệ thống thông tin trong nước và cơ sở hạ tầng thông tin trọng yếu quốc gia diễn biến phức tạp, với phương thức, thủ đoạn mới, tinh vi, nguy hiểm, nhiều vụ gây nhiều hậu quả đặc biệt nghiêm trọng. Tấn công mạng vào hệ thống thông tin của tổ chức, doanh nghiệp nhằm phá hoại, chiếm đoạt dữ liệu ngày càng phổ biến và gây hậu quả nghiêm trọng. Tình trạng lộ, mất bí mật nhà nước, thông tin quan

trọng, nhạy cảm vẫn tiếp diễn, nguyên nhân chủ yếu vẫn do yếu tố con người, nhận thức và kiến thức về bảo đảm an ninh mạng còn hạn chế, hệ thống thông tin của ta còn bộc lộ nhiều sơ hở, không được quan tâm đầu tư đúng mức.

Thách thức về tội phạm mạng: Các loại tội phạm mạng, tội phạm sử dụng công nghệ cao diễn biến phức tạp, gây nhiều hậu quả, thiệt hại đối với quyền và lợi ích hợp pháp của tổ chức, cá nhân. Hoạt động đánh bạc, tổ chức đánh bạc, lừa đảo chiếm đoạt tài sản qua mạng, “tín dụng đen”, tội phạm trong lĩnh vực thanh toán điện tử, thương mại điện tử, tiền ảo, đầu tư đa cấp trái pháp luật, tội phạm mạng có yếu tố nước ngoài, xuyên quốc gia tiếp tục diễn biến nguy hiểm, xảy ra tại hầu hết các địa phương với nhiều thủ đoạn tinh vi, thiệt hại ước tính hàng nghìn tỷ đồng mỗi năm, ảnh hưởng nghiêm trọng đến trật tự an toàn xã hội, gây tâm lý lo lắng, bất an trong quần chúng nhân dân.

Thách thức về bảo vệ an ninh mạng đối với dữ liệu quốc gia: Dữ liệu công dân, dữ liệu phát triển kinh tế trên phạm vi quốc gia đang bị thu thập, sử dụng, lưu trữ chưa đúng quy định, đặt ra nguy cơ mất tự chủ về dữ liệu. Trong khi đó, chính sách, pháp luật về bảo vệ dữ liệu nói chung và dữ liệu cá nhân nói riêng đang trong quá trình xây dựng, hoàn thiện; còn tồn tại sự chưa bình đẳng giữa doanh nghiệp trong và ngoài nước trong kinh doanh dữ liệu; an ninh con người, quyền con người, an ninh kinh tế, an ninh quốc gia có thể bị đe dọa khi dữ liệu bị sử dụng không đúng mục đích.

Thách thức về nhận thức, kiến thức về không gian mạng còn hạn chế: Nhận thức, kiến thức bảo đảm an ninh mạng của quần chúng nhân dân về tính hai mặt của không gian mạng chưa theo kịp sự phát triển của khoa học công nghệ. Còn xảy ra tình trạng thiên về mặt tích cực mà coi nhẹ mặt tiêu cực. Việc tham gia không gian mạng an toàn chưa được chú trọng. Ý thức, nhận thức về an ninh mạng của cán bộ quản trị, người sử dụng còn kém dẫn tới tình trạng lộ, mất bí mật nhà nước, bí mật cá nhân, công khai thông tin nhạy cảm, quan trọng dễ bị tội phạm mạng lợi dụng, sử dụng. Trách nhiệm bảo vệ an ninh mạng chưa gắn với trách nhiệm của người đứng đầu cơ quan, tổ chức, doanh nghiệp. An ninh mạng chưa được triển khai đồng bộ với quá trình ứng dụng công nghệ thông tin, xây dựng hệ thống thông tin. Công tác tuyên truyền về an ninh mạng chưa được chú ý đúng mức, nhiều thủ đoạn phạm tội chưa được cập nhật, phổ biến rộng rãi tới quần chúng nhân dân.

Thách thức về khả năng làm chủ công nghệ, sản phẩm bảo đảm an toàn, an ninh mạng: Công nghiệp an ninh mạng chưa được hình thành và phát triển mặc dù Đảng và Nhà nước đã quan tâm, chỉ đạo xây dựng và phát triển công nghiệp an ninh mạng. Việc đầu tư nghiên cứu, chế tạo các sản phẩm, dịch vụ an ninh mạng, làm chủ công nghệ chưa được chú trọng, chưa có hàm lượng công nghệ cao. Công nghiệp an ninh mạng chưa được quy định trong các văn bản quy

phạm pháp luật, sự huy động các tổ chức, cá nhân tham gia chưa nhiều; chưa tạo được cơ chế và môi trường để nghiên cứu, xây dựng, phát triển, chế tạo các sản phẩm công nghiệp an ninh mạng cả chuyên sâu và lưỡng dụng. Khả năng làm chủ, tự chủ các thiết bị, sản phẩm, dịch vụ xây dựng hạ tầng không gian mạng quốc gia chưa cao. Hầu hết các sản phẩm có ứng dụng công nghệ đều phải nhập từ nước ngoài, chưa hình thành được công nghiệp an ninh mạng. Các doanh nghiệp công nghệ thông tin vẫn còn có quy mô nhỏ, giá trị chưa cao, chủ yếu tập trung vào các sản phẩm, dịch vụ phần mềm, nội dung số, dịch vụ công nghệ thông tin. Doanh nghiệp sản xuất phần cứng, điện tử chưa nhiều, doanh thu chủ yếu đến từ các thiết bị, sản phẩm doanh nghiệp nước ngoài đặt nhà máy lắp ráp tại Việt Nam. Doanh nghiệp kinh doanh phần mềm, dịch vụ công nghệ thông tin có bước phát triển mạnh, có khả năng cạnh tranh với các doanh nghiệp nước ngoài, một số sản phẩm phần mềm đóng gói thương hiệu Việt chiếm lĩnh thị trường trong nước, tuy nhiên phần lớn các doanh nghiệp hoạt động theo hướng gia công sản phẩm.

Thách thức về nguồn nhân lực bảo đảm an toàn, an ninh mạng: Nguồn nhân lực công nghệ cao chưa đáp ứng được yêu cầu, chưa có nhiều đội ngũ chuyên gia nổi tiếng thế giới, có khả năng sáng tạo, phát minh, sáng kiến, tự chủ về công nghệ. Nguồn nhân lực công nghệ thông tin nước ta năm 2020 ước tính khoảng 1 triệu người, nhưng đa phần là nhân lực gia công sản phẩm hoặc lắp ráp linh kiện điện tử, trong đó có khoảng hơn 700 người là lao động trong ngành công nghiệp phần cứng, điện tử; 130 nghìn người làm trong ngành phần mềm; khoảng 138 nghìn người làm trong ngành dịch vụ và nội dung số. Thiếu nguồn nhân lực trên các lĩnh vực công nghệ chuyên sâu, như: trí tuệ nhân tạo, điện toán đám mây, học máy, học sâu.

Thách thức về chiến tranh mạng, nhiệm vụ quốc phòng trên không gian mạng: Không gian mạng được ứng dụng sâu rộng vào hoạt động quân sự, nâng cao năng lực tác chiến của lực lượng vũ trang. Chiến tranh thông tin, chiến tranh mạng có thể xảy ra vào bất cứ lúc nào và không giới hạn về không gian, thời gian.

Để giữ vững an ninh quốc gia, bảo đảm trật tự an toàn xã hội trước những yêu cầu, thách thức của tình hình mới đòi hỏi bên cạnh những giải pháp cấp bách, trước mắt, cần phải có định hướng, chủ trương, giải pháp cơ bản, chiến lược lâu dài nhằm từng bước nâng cao tiềm lực, khả năng và sức mạnh trong đảm bảo an ninh mạng, góp phần bảo vệ vững chắc độc lập, chủ quyền, an ninh quốc gia và phát triển đất nước, từng bước đưa nước ta trở thành quốc gia có môi trường không gian mạng lành mạnh, có khả năng chủ động ứng phó hiệu quả với các mối đe dọa trên không gian mạng, không để bị động, bất ngờ trong mọi tình huống.

II. CƠ SỞ CHÍNH TRỊ VÀ CƠ SỞ PHÁP LÝ

1. Cơ sở chính trị

- Nghị quyết Đại hội đại biểu toàn quốc lần thứ XIII của Đảng đã khẳng định: “An ninh mạng ngày càng tác động mạnh, nhiều mặt, đe dọa nghiêm trọng đến sự phát triển ổn định, bền vững của thế giới, khu vực và đất nước ta. Thực tiễn thời gian qua cho thấy, không gian mạng đã và đang làm thay đổi phương thức hoạt động, tổ chức cách thức tiến hành chiến tranh, can dự/can thiệp của các nước; cũng như nhiều khía cạnh khác của hoạt động an ninh, quân sự, tình báo, tội phạm. Tác chiến mạng đã trở thành một loại hình tác chiến hiện đại; an ninh mạng là ưu tiên hàng đầu trong chiến lược an ninh quốc gia của nhiều nước trên thế giới; thậm chí đã được sử dụng là lực lượng, chiến thuật tiên phong, mở đường cho hoạt động quân sự truyền thống; là vũ khí quan trọng để tiến hành âm mưu, ý đồ “cách mạng màu”, “cách mạng đường phố”. Đây là căn cứ quan trọng để thúc đẩy.

- Nghị quyết số 30-NQ/TW ngày 25 tháng 7 năm 2018 của Bộ Chính trị về Chiến lược An ninh mạng quốc gia đã xác định:

+ An ninh mạng có vị trí đặc biệt quan trọng, là nhiệm vụ trọng yếu thường xuyên, vừa cấp bách, vừa lâu dài của cả hệ thống chính trị, của toàn dân, của các cấp, các ngành dưới sự lãnh đạo của Đảng, sự quản lý thống nhất của Nhà nước, trong đó lực lượng Công an nhân dân, Quân đội nhân dân giữ vai trò nòng cốt

+ Huy động và phát huy sức mạnh tổng hợp của hệ thống chính trị và của toàn xã hội trong công tác bảo đảm an ninh mạng. Kết hợp chặt chẽ giữa nhiệm vụ phát triển kinh tế, văn hóa, xã hội, khoa học - công nghệ, đối ngoại với nhiệm vụ bảo đảm an ninh quốc gia, trật tự an toàn xã hội trên không gian mạng. Chú trọng công tác tuyên truyền, vận động nâng cao nhận thức và kiến thức về bảo vệ an ninh mạng cho toàn xã hội, từng bước xây dựng thế trận an ninh nhân dân gắn với thế trận quốc phòng toàn dân vững chắc trên không gian mạng.

+ Tăng cường hiệu lực, hiệu quả quản lý nhà nước về an ninh mạng; quản lý chặt chẽ hoạt động cung cấp, sử dụng dịch vụ viễn thông, Internet tại Việt Nam; nâng cao hiệu quả quan hệ phối hợp giữa các ngành chức năng trong quản lý nhà nước về an ninh mạng; đề cao trách nhiệm của người đứng đầu các cơ quan, tổ chức, đơn vị trong công tác bảo vệ an ninh mạng trong phạm vi địa bàn, lĩnh vực được giao phụ trách. Không để bị động, bất ngờ trong mọi tình huống.

+ Đầu tư cho bảo vệ an ninh mạng là đầu tư cho phát triển và bảo vệ đất nước, ưu tiên đầu tư cho an ninh mạng; ứng dụng công nghệ thông tin trong các lĩnh vực phải gắn với đầu tư cho bảo vệ an ninh mạng, bảo đảm theo kịp sự phát triển của khoa học - công nghệ của thời đại. Lấy con người, trí tuệ con người

làm trung tâm, là nhân tố quyết định, đồng thời tranh thủ tối đa những thành tựu của khoa học – công nghệ; không để bị tụt hậu về con người và công nghệ.

+ Xây dựng lực lượng chuyên trách bảo vệ an ninh mạng chính quy, tinh nhuệ, hiện đại, ngang tầm khu vực và quốc tế; nắm chắc tình hình, chủ động phòng ngừa, đấu tranh, xử lý kịp thời hiệu quả các nguy cơ đe dọa và tình huống nguy hiểm về an ninh mạng, bảo vệ vững chắc chủ quyền, lợi ích, an ninh quốc gia trên không gian mạng.

+ Huy động, phát huy hiệu quả các nguồn lực trong nước đi đôi với tăng cường, mở rộng hợp tác quốc tế trong bảo đảm an toàn, an ninh thông tin và an ninh mạng; phát huy mạnh mẽ sức sáng tạo, tinh thần yêu nước, tự hào dân tộc, độc lập, tự chủ, tự cường xây dựng và phát triển công nghiệp an ninh mạng.

- Nghị quyết số 52/NQ-TW ngày 27/9/2019 của Bộ Chính trị về một số chủ trương, chính sách chủ động tham gia cuộc Cách mạng công nghiệp lần thứ tư, trong đó nhấn mạnh yêu cầu cấp bách về bảo đảm an ninh mạng, trong đó khẳng định việc bảo đảm an ninh mạng còn nhiều thách thức; hoàn thiện pháp luật, chính sách về an ninh mạng; đầu tư nâng cấp hạ tầng kỹ thuật bảo đảm an ninh mạng; thực hiện lộ trình phổ cập kxy ăng số, kỹ năng bảo đảm an toàn, an ninh mạng đạt trình độ cơ bản của người dân; tập trung phát triển lĩnh vực an ninh mạng thành ngành nghề ưu tiên, có mức độ sẵn sàng cao.

- Quyết định 964/QĐ-TTg ngày 10 tháng 8 năm 2022 của Thủ tướng Chính phủ 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 năm 2030 đã khẳng định:

+ Xác định tầm nhìn chiến lược về không gian mạng. Không gian mạng mang tới cả cơ hội và thách thức. Phải 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.

+ Bảo đảm an toàn, an ninh mạng là yêu cầu tất yếu khách quan, là nhiệm vụ có ý nghĩa chiến lược đặc biệt quan trọng, vừa cấp bách vừa lâu dài của cả hệ thống chính trị và toàn xã hội, gắn chặt với quá trình ứng dụng, sử dụng thành tựu của không gian mạng vào đời sống xã hội. Chủ động ứng phó từ sớm, từ xa, nguy cơ, thách thức, hoạt động gây tổn hại tới chủ quyền, lợi ích, an ninh quốc gia trên không gian mạng. Nhận thức đúng đắn về không gian mạng, lấy con người làm trung tâm trong ứng phó với các thách thức từ không gian mạng, coi đó là giải pháp đột phá để nâng cao năng lực bảo đảm an toàn, an ninh mạng quốc gia.

+ Phát huy tối đa các nguồn lực, bảo đảm đủ nguồn lực cho việc chủ động ứng phó với các thách thức từ không gian mạng, 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.

- Quyết định số 77/QĐ-TTg ngày 30/11/2022 của Thủ tướng Chính phủ phê duyệt Đề án “Xây dựng Thế trận An ninh nhân dân trên không gian mạng”, đã xác định xây dựng, triển khai đồng bộ, thống nhất Thế trận An ninh nhân dân trên không gian mạng trên phạm vi cả nước nhằm huy động quần chúng nhân dân và lực lượng chức năng tham gia chủ động phòng ngừa, chủ động đấu tranh bảo vệ vững chắc chủ quyền, lợi ích, an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân, gắn với xây dựng lực lượng Công an nhân dân cách mạng, chính quy, tinh nhuệ, hiện đại.

- Quyết định số 49/QĐ-TTg ngày 15/7/2022 của Thủ tướng Chính phủ phê duyệt Đề án “Đào tạo nguồn nhân lực an ninh mạng đến năm 2025, tầm nhìn đến năm 2030” đã xác định đào tạo, phát triển đội ngũ nhân lực an ninh mạng là nội dung quan trọng để hiện thực hóa tầm nhìn đưa Việt Nam trở thành cường quốc về an ninh mạng, góp phần triển khai thành công Chương trình chuyển đổi số quốc gia, phát triển Chính phủ điện tử hướng tới Chính phủ số, nền kinh tế - xã hội số và nâng cao uy tín, xếp hạng quốc tế của Việt Nam về an ninh mạng.

- Chỉ thị số 01/CT-TTg ngày 18 tháng 02 năm 2021 của Thủ tướng Chính phủ đã chỉ đạo tăng cường tuyên truyền, phổ biến chủ trương, chính sách, pháp luật, chế tài xử lý và phương thức, thủ đoạn sử dụng không gian mạng vi phạm pháp luật; nghiên cứu, đề xuất, kiện toàn mô hình tổ chức của lực lượng bảo vệ an toàn, an ninh mạng, lực lượng tham gia bảo vệ an toàn, an ninh mạng bảo đảm tập trung, thống nhất, đáp ứng yêu cầu, nhiệm vụ trong tình hình mới.

2. Căn cứ pháp lý

- Luật An ninh mạng được ban hành năm 2018 đã khẳng định Đảng và Nhà nước ưu tiên bảo vệ an ninh mạng trong quốc phòng, an ninh, phát triển kinh tế - xã hội, khoa học, công nghệ và đối ngoại; xây dựng không gian mạng lành mạnh, không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; ưu tiên nguồn lực xây dựng lực lượng chuyên trách bảo vệ an ninh mạng; nâng cao năng lực cho lực lượng bảo vệ an ninh mạng và tổ chức, cá nhân tham gia bảo vệ an ninh mạng; ưu tiên đầu tư cho nghiên cứu, phát triển khoa học, công nghệ để bảo vệ an ninh mạng; khuyến khích, tạo điều kiện để tổ chức, cá nhân tham gia bảo vệ an ninh mạng, xử lý các nguy cơ đe dọa an ninh mạng; nghiên cứu, phát triển công nghệ, sản phẩm, dịch vụ, ứng dụng nhằm bảo vệ an ninh mạng; phối hợp với cơ quan chức năng trong bảo vệ an ninh mạng; tăng cường hợp tác quốc tế về an ninh mạng.

- Thời gian qua, Chính phủ đã ban hành Nghị định số 04/2019/NĐ-CP ngày 27 tháng 12 năm 2019 của Chính phủ quy định chi tiết trình tự, thủ tục áp dụng một số biện pháp bảo vệ an ninh mạng, Nghị định số 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022 quy định chi tiết một số điều của Luật An ninh mạng, Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân; đồng thời, chỉ đạo xây dựng các văn bản pháp luật về an ninh mạng, gồm: dự thảo Nghị định xử phạt vi phạm hành chính trong lĩnh vực an ninh mạng, dự thảo Nghị định quy định về kinh doanh sản phẩm, dịch vụ an ninh mạng, dự án xây dựng Luật Bảo vệ dữ liệu cá nhân.

3. Như vậy, để triển khai các văn bản chỉ đạo, văn bản pháp luật nêu trên cần có sự chỉ đạo tập trung, thống nhất, đồng bộ của Đảng, Nhà nước từ Trung ương tới địa phương; đồng thời, có sự đồng bộ về nhận thức, sự chung tay của quần chúng nhân dân. Do đó, việc đề xuất thành lập ngày An ninh mạng Việt Nam là vô cùng cần thiết, không chỉ đáp ứng yêu cầu bảo vệ, mà còn đáp ứng yêu cầu phát triển.

III. MỤC ĐÍCH, YÊU CẦU

1. Triển khai thực hiện có hiệu quả công tác bảo đảm an ninh mạng theo các văn bản chỉ đạo, văn bản pháp luật của Đảng, Nhà nước, nâng cao năng lực, hiệu quả thực tiễn của công tác bảo đảm an ninh mạng.

2. Nâng cao nhận thức của người dân toàn xã hội về vai trò, ý nghĩa, trách nhiệm và nghĩa vụ của công tác bảo đảm an ninh mạng. Theo đó, công tác bảo đảm an ninh mạng sẽ chỉ thực sự thành công nếu mọi người dân đều nhận thức rõ lợi ích, trách nhiệm, quyền và trách nhiệm mà không gian mạng mang lại cho cuộc sống. Đây là việc cần làm ngay, vì công tác bảo đảm an ninh mạng phụ thuộc vào mỗi cá nhân.

3. Thúc đẩy sự tham gia vào cuộc của cả hệ thống chính trị, hành động đồng bộ ở các cấp và sự tham gia của toàn dân vào công tác bảo đảm an ninh mạng. Đây chính là yếu tố bảo đảm sự thành công của công tác bảo đảm an ninh mạng. Bởi lẽ, trong bối cảnh Cách mạng công nghiệp lần thứ tư, công nghệ số, chuyển đổi số diễn ra mạnh mẽ như hiện nay, công tác phòng ngừa, chủ động phòng ngừa tới từ tổ chức, cá nhân từ Trung ương tới địa phương, trên quy mô rộng khắp, toàn quốc mới là yếu tố bảo đảm sự thành công của công tác bảo đảm an ninh mạng.

4. Đẩy nhanh tiến độ triển khai các nhiệm vụ bảo đảm an ninh mạng quốc gia. Ngày An ninh mạng Việt Nam không chỉ mang ý nghĩa chào mừng, tôn vinh, khen thưởng các tổ chức, cá nhân đã tham gia vào công tác bảo đảm an ninh mạng, mà còn là dấu mốc để đánh giá công tác bảo đảm an ninh mạng hằng năm.

IV. NỘI DUNG ĐỀ ÁN

1. Lựa chọn Ngày An ninh mạng Việt Nam

Lấy ngày 06 tháng 8 hằng năm là Ngày An ninh mạng Việt Nam, là dấu mốc để đánh giá công tác bảo đảm an ninh mạng hằng năm, đồng thời là thời điểm để chào mừng, tôn vinh, khen thưởng các tổ chức, cá nhân đã tham gia vào công tác bảo đảm an ninh mạng.

Việc lấy ngày 06 tháng 8 còn có ý nghĩa kỷ niệm ngày thành lập của lực lượng An ninh mạng Việt Nam (ngày thành lập Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an).

2. Các hoạt động Ngày An ninh mạng Việt Nam

2.1. Lễ công bố Ngày An ninh mạng Việt Nam

Sau khi có Quyết định phê duyệt của Thủ tướng Chính phủ về Ngày An ninh mạng Việt Nam, Bộ Công an phối hợp với các bộ, ngành, địa phương liên quan tổ chức Lễ giới thiệu và công bố về Ngày An ninh mạng Việt Nam để công bố rộng rãi tới các tổ chức, cá nhân, phát động các hoạt động về bảo đảm an ninh mạng hằng năm trên cả nước, đồng thời công bố logo, hình ảnh biểu trưng, bộ nhận diện của Ngày An ninh mạng Việt Nam bảo đảm thiết thực, hiệu quả, tiết kiệm.

2.2. Các hoạt động hằng năm tại Trung ương

Tổ chức tuần lễ An ninh mạng Việt Nam, trong đó có các sự kiện sau:

a) Tổ chức Ngày An ninh mạng Việt Nam

- Đơn vị chủ trì: Bộ Công an

- Đơn vị phối hợp: Văn phòng Chính phủ, Bộ Thông tin và Truyền thông, Bộ Quốc phòng, Bộ Văn hóa, Thể thao và Du lịch, Bộ Khoa học và Công nghệ, Ủy ban nhân dân thành phố Hà Nội, Trung ương Đoàn TNCS Hồ Chí Minh, Hiệp hội An ninh mạng quốc gia (NCA), Hiệp hội An toàn thông tin (VNISA), Hội Truyền thông số Việt Nam (VDCA), Phần mềm và Dịch vụ công nghệ thông tin Việt Nam (VINASA), các doanh nghiệp,...

- Thời gian: Tuần lễ diễn ra Ngày An ninh mạng Việt Nam.

- Hoạt động chính: Tổ chức Hội nghị đánh giá kết quả thực hiện công tác bảo đảm an ninh mạng theo từng năm; các diễn đàn, hội nghị chuyên đề về an ninh mạng theo các lĩnh vực trọng tâm; tạo sự kiện gắn kết cộng đồng người làm công tác bảo đảm an ninh mạng và người tham gia; hoạt động vinh danh các tổ chức, cá nhân có đóng góp cho sự nghiệp bảo đảm an ninh mạng.

b) Tổ chức Triển lãm về An ninh mạng

- Đơn vị chủ trì: Bộ Công an.

- Đơn vị phối hợp: Văn phòng Chính phủ, Bộ Thông tin và Truyền thông, Bộ Quốc phòng, Bộ Văn hóa Thể thao và Du lịch, Bộ Khoa học và Công nghệ, Ủy ban nhân dân thành phố Hà Nội, Trung ương Đoàn TNCS Hồ Chí Minh, Các hội, hiệp hội (VINASA, VDCA...),...

- Thời gian: Tuần lễ diễn ra Ngày An ninh mạng Việt Nam.

- Hoạt động chính: Triển lãm giới thiệu các thành tựu, mô hình, sản phẩm, dịch vụ, công nghệ về an ninh mạng của các doanh nghiệp, cơ quan nhà nước, tổ chức, cá nhân trong và ngoài nước; giới thiệu các sản phẩm, dịch vụ, công nghệ của Việt Nam.

c) Tổ chức các giải thưởng về an ninh mạng tôn vinh doanh nghiệp Việt Nam

Bộ Công an với vai trò điều phối các bên để tổ chức trao giải của các giải thưởng An ninh mạng (sản phẩm, dịch vụ, chuyên gia) vào Tuần lễ Ngày An ninh mạng Việt Nam, góp phần làm tăng hiệu ứng truyền thông, quảng bá hình ảnh an ninh mạng đến mọi thành phần trong xã hội.

2.2. Các hoạt động hằng năm tại địa phương

Tổ chức Ngày An ninh mạng Việt Nam tại các tỉnh, thành phố trong cả nước tùy theo tình hình thực tế của địa phương. Các tỉnh, thành phố dựa trên kế hoạch chung, căn cứ vào tình hình thực tế của địa phương để xây dựng kế hoạch triển khai cụ thể.

- Thời gian: Tuần lễ diễn ra Ngày An ninh mạng Việt Nam.

- Hoạt động chính: Trong Tuần lễ An ninh mạng Việt Nam có thể tổ chức nhiều hoạt động trên địa bàn tỉnh: Hội thảo chuyên đề, nói chuyện, tọa đàm; Tổ chức Giải thưởng An ninh mạng cấp tỉnh (do UBND cấp tỉnh chủ trì triển khai); Tổ chức triển lãm về thành tựu bảo đảm an ninh mạng trên địa bàn tỉnh.

3. Công tác thông tin, tuyên truyền về Ngày An ninh mạng Việt Nam

3.1. Đài Truyền hình Việt Nam, Đài Tiếng nói Việt Nam, Thông tấn xã Việt Nam

Xây dựng kế hoạch tuyên truyền trên các kênh về an ninh mạng và Ngày An ninh mạng Việt Nam.

3.2. Các cơ quan thông tấn, báo chí ở trung ương và địa phương

- Đẩy mạnh việc tuyên truyền, quảng bá về Ngày An ninh mạng Việt Nam;

- Xây dựng các chương trình giới thiệu và tuyên dương các cơ quan, tổ chức, doanh nghiệp điển hình đã đi đầu trong công tác bảo đảm an ninh mạng.

- Tổ chức truyền thông đối ngoại, quảng bá Ngày An ninh mạng Việt Nam đến cộng đồng người Việt Nam ở nước ngoài và người nước ngoài trên các

phương tiện truyền thông đại chúng trong và ngoài nước, phương tiện truyền thông mới, trên các nền tảng mạng xã hội và lòng ghép tại các sự kiện quốc tế diễn ra ở Việt Nam, các sự kiện Việt Nam ở nước ngoài.

V. TỔ CHỨC THỰC HIỆN

1. Bộ Công an

Chủ trì, phối hợp với Bộ Văn hóa, Thể thao và Du lịch, Bộ Thông tin và Truyền thông, Bộ Quốc phòng, Bộ Khoa học và Công nghệ, các bộ, ngành liên quan và Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương xây dựng kế hoạch triển khai cụ thể; hướng dẫn, chỉ đạo tổ chức thực hiện các hoạt động truyền thông Ngày An ninh mạng Việt Nam hằng năm bảo đảm thiết thực, hiệu quả, tiết kiệm.

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

Căn cứ kế hoạch, hướng dẫn của Bộ Công an và điều kiện thực tế của từng bộ, ngành, địa phương để tổ chức thực hiện các hoạt động phù hợp truyền thông Ngày An ninh mạng Việt Nam hằng năm tại bộ, ngành, địa phương.

3. Đài Truyền hình Việt Nam, Đài Tiếng nói Việt Nam, Thông tấn xã Việt Nam

Xây dựng kế hoạch tuyên truyền trên các kênh về an ninh mạng và Ngày An ninh mạng Việt Nam.

4. Hiệp hội An ninh mạng quốc gia

Chỉ đạo các tổ chức thành viên trực thuộc tham gia và tổ chức các hoạt động truyền thông Ngày An ninh mạng Việt Nam hằng năm.

5. Các cơ quan thông tấn, báo chí ở trung ương và địa phương

Thực hiện đẩy mạnh việc tuyên truyền, quảng bá về Ngày An ninh mạng Việt Nam; xây dựng các chương trình giới thiệu và tuyên dương các cơ quan, tổ chức, doanh nghiệp điển hình đã đi đầu trong công tác bảo đảm an ninh mạng.

V. KINH PHÍ THỰC HIỆN

Kinh phí tổ chức Ngày An ninh mạng Việt Nam hằng năm bao gồm: Ngân sách nhà nước (ngân sách Ban Chỉ đạo An toàn, An ninh mạng quốc gia, Tiểu ban An toàn, An ninh mạng tại địa phương); nguồn đầu tư của doanh nghiệp, khu vực tư nhân, cộng đồng và các nguồn kinh phí hợp pháp khác.

Các bộ, ngành, địa phương căn cứ nhiệm vụ được giao bố trí nguồn lực để tổ chức thực hiện các hoạt động phù hợp truyền thông Ngày An ninh mạng Việt Nam hằng năm tại bộ, ngành, địa phương./.