

Giải pháp chủ động phòng ngừa, ứng phó các nguy cơ an ninh phi truyền thống, trọng tâm đảm bảo an ninh mạng, an ninh thông tin trong bối cảnh thế giới đại chuyển đổi dưới tác động của cuộc Cách mạng công nghiệp lần thứ tư

PGS, TS NGUYỄN VĂN THÀNH

Hội đồng Lý luận Trung ương

Nhận ngày 7 tháng 11 năm 2022; chấp nhận đăng tháng 12 năm 2022.

Tóm tắt: Trong bối cảnh thế giới đại chuyển động dưới ảnh hưởng của cuộc Cách mạng công nghiệp 4.0, các vấn đề an ninh phi truyền thống đã trở thành những yếu tố bất ổn, ảnh hưởng đến an ninh quốc gia, đồng thời, đặt ra những thách thức mới đối với hòa bình, ổn định khu vực và quốc tế. Theo thống kê của Liên hợp quốc, an ninh phi truyền thống đang đối mặt với hàng chục mối đe dọa. Trong đó, có những vấn đề cần được đặc biệt quan tâm như khủng bố, ma túy, tin tặc, thảm họa môi trường, dịch bệnh, mua bán người, di cư trái phép, đặc biệt là vi phạm chủ quyền không gian mạng, an ninh không gian mạng, tội phạm công nghệ cao... cần có các giải pháp hữu hiệu để chủ động phòng ngừa, ứng phó. Trên tinh thần đó, các giải pháp được tác giả nhấn mạnh bao gồm về nguồn nhân lực, vật lực, chính sách, đặc biệt là giải pháp công nghệ.

Từ khóa: cuộc cách mạng công nghiệp 4.0; an ninh phi truyền thống; không gian mạng; an ninh mạng.

Abstract: In the context of a fast-moving world under the influence of the 4.0 industrial revolution, non-traditional security issues have become destabilizing factors affecting national security, and also pose new challenges to regional and international peace and stability. United Nation statistics show non-traditional security is facing dozens of threats. In particular, there are issues that need special attention and effective solutions to proactively prevent and respond such as terrorism, drugs, hackers, environmental disasters, epidemics, human trafficking, illegal migration, especially violations of cyber sovereignty, cyber security, high-tech crime, etc. In this article, the solutions emphasized by the author include human resources, material resources, policies, especially technological solutions.

Keywords: industrial revolution 4.0; Non-traditional security; cyberspace; network security.

1. Tác động của cuộc Cách mạng công nghiệp lần thứ tư

Lịch sử loài người đã và đang trải qua các cuộc cách mạng công nghiệp (CMCN): CMCN lần thứ nhất vào năm 1784, khởi nguồn từ nước Scotland, đặc trưng là cơ khí hóa với máy chạy bằng thủy lực và phát minh ra động cơ hơi nước (phát minh này của James Watt công bố năm 1775) - Kỷ nguyên sản xuất cơ khí. Loài người chuyển từ văn minh nông nghiệp sang văn minh công nghiệp. CMCN lần thứ

hai: từ năm 1871 - 1914 đặc trưng là động cơ điện, vận tải, hóa học, sản xuất thép và sản xuất trên cơ sở điện cơ khí và sang giai đoạn tự động hóa và khởi nguồn từ Mỹ. CMCN lần thứ ba: từ năm 1969, với sự ra đời của công nghệ thông tin (CNTT), sử dụng điện tử và CNTT để tự động hóa sản xuất, được xúc tác bởi chất bán dẫn, siêu máy tính, laptop (1970 và 1980), Internet (thập niên 1990), trung tâm và khởi nguồn từ Mỹ. Cuộc Cách mạng công nghiệp lần thứ tư (The Fourth Industrial Revolution - FIR) bắt đầu

từ dự án trong chiến lược CNC của chính phủ Đức, thuật ngữ được sử dụng lần đầu vào năm 2011 tại Hội chợ Hannover; chính thức nhận diện khái niệm, nội hàm tại Diễn đàn Kinh tế Thế giới (WEF) lần thứ 46, ngày 20.01.2016.

Cuộc Cách mạng công nghiệp lần thứ tư được nhận diện ở những đặc điểm, đặc trưng sau:

Sự đột phá của khoa học công nghệ dựa trên nền tảng công nghệ số tích hợp công nghệ “thông minh” để tối ưu hóa quy trình, phương thức sản xuất. Điểm “đòn bẩy” là: AI (trí tuệ nhân tạo); công nghệ (CN) in 3D, CN sinh học, CN vật liệu mới, CN tự động hóa, Robot, công nghệ kết nối vạn vật (IoT) và Internet các dịch vụ (IoS). Đặc trưng của CM 4.0 là các hệ thống sản xuất thực-ảo (Cyber-Physical Systems-CPS), lần đầu tiên được TS Jame Truchat, Giám đốc điều hành của National Instrument đưa ra vào năm 2006, trong đó, thiết bị thông minh làm việc với nhau qua mạng không dây hoặc qua “đám mây”.

Quy mô tốc độ phát triển chưa từng có trong lịch sử, tốc độ phát triển cấp số nhân, tác động to lớn về kinh tế và môi trường sinh thái. Tiêu chí tốc độ lan truyền của công nghệ được sử dụng đạt ngưỡng 50 triệu người (điện thoại 75 năm, radio cần 38 năm, tivi cần 13 năm, Internet chỉ cần 4 năm, Facebook cần 3,5 năm). Về kinh tế tác động đến tiêu dùng, sản xuất, năng xuất và giá cả. Bản đồ kinh tế thế giới, bản đồ sức mạnh của các doanh nghiệp cũng đang được vẽ lại. Ví dụ: công nghệ in 3D trị giá 3,1 tỷ USD/năm tăng 35% so với năm 2012; tăng trung bình 32% đạt 21 tỷ USD vào năm 2020.

Tác động của công nghệ mới nổi của CMCN 4.0 đến các mặt của đời sống xã hội. Công nghệ số IoT (kết nối vạn vật) thông qua hệ thống các công nghệ kết nối và các nền tảng khác nhau. Là một phân tích hợp của Internet tương lai bao gồm các phát triển của Internet và mạng hiện tại và tiến hóa với cơ sở hạ tầng mạng động toàn cầu dựa trên giao thức liên kết và tương tác “vạn vật” hữu hình và ảo sử dụng các giao diện thông minh Smart được tích hợp vào mạng thông tin một cách thông suốt. Viễn cảnh IoT: (i) IoE : Internet năng lượng; (ii) IoS : Internet dịch vụ; (iii) IoM: Internet Truyền thông; (iv) IoP: Internet con người, (v) Io : Internet vạn vật. IoT sẽ thay đổi cả phương thức hoạt động của một nền kinh tế tạo

mô hình kinh doanh mới. IoT sẽ thay đổi cả phương thức hoạt động của một nền kinh tế tạo mô hình sản xuất - kinh doanh mới. Các siêu kết nối thông qua IoT và điện toán đám mây sẽ cho phép truyền thông tin và giao tiếp phổ quát toàn cầu và gần như tức thời, xuất hiện những cách thức cung cấp hàng hóa dịch vụ trước đây là điều không tưởng.

Trí tuệ nhân tạo AI (Artificial Intelligence): Là hệ thống máy tính thể hiện hành vi đòi hỏi trí thông minh (Smart). Phân loại: (i) Hệ thống có tư duy như con người (mạng lưới thần kinh và kiến trúc nhận thức); (ii) Hệ thống hành động như con người (suy luận tự động); (iii) Hệ thống tư duy hợp lý (suy luận, tối ưu hóa); (iv) Hệ thống hành động hợp lý (phần mềm thông minh, Robot đạt mục tiêu thông qua nhận thức xây dựng kế hoạch; giao tiếp, quyết định và hành động). Thiết bị 4 rộng khắp: (i) cảm biến mọi nơi, (ii) kết nối mọi nơi; (iii) dữ liệu mọi nơi, (iv) dịch vụ mọi nơi

2. An ninh phi truyền thống: đặc điểm và những nguy cơ thách thức

- Quan niệm an ninh phi truyền thống

An ninh phi truyền thống (ANPTT) là khái niệm tương đối mới trong khoa học nghiên cứu về lĩnh vực an ninh. GS Mely Caballero Anthony, Tổng Thư ký Liên minh các cơ sở nghiên cứu về ANPTT ở châu Á (NTS-Asia) cho rằng, theo nghĩa rộng, ANPTT “đề cập đến sự chuyển hướng khỏi trọng tâm quân sự, nhà nước của các mô hình an ninh truyền thống.” NTS-Asia định nghĩa: “Các vấn đề an ninh phi truyền thống là các thách thức đối với sự tồn vong và thịnh vượng của con người và các nhà nước, xuất hiện chủ yếu trong các nguồn phi quân sự, chẳng hạn như biến đổi khí hậu, nguồn tài nguyên cạn kiệt, bệnh truyền nhiễm, thiên tai, di cư trái phép, tình trạng thiếu lương thực, đưa người di cư trái phép, buôn bán ma túy trái pháp luật và tội phạm xuyên quốc gia. Những mối nguy hiểm này thường xuyên quốc gia về phạm vi, bất chấp các biện pháp khắc phục đơn phương và đòi hỏi sự ứng phó toàn diện - chính trị, kinh tế, xã hội, cũng như sử dụng lực lượng quân sự nhân đạo”.

Tại Hội nghị Thượng đỉnh lần thứ 6 giữa các nước thuộc Hiệp hội các quốc gia Đông Nam Á (ASEAN) và Trung Quốc ngày 01.11.2002, cụm từ

“an ninh phi truyền thống” chính thức xuất hiện trong “Tuyên bố chung ASEAN - Trung Quốc về hợp tác trên lĩnh vực an ninh phi truyền thống” và thống nhất trong nhận thức rằng: “các vấn đề an ninh phi truyền thống như buôn bán ma túy bất hợp pháp, mua bán người bao gồm mua bán phụ nữ và trẻ em, cướp biển, khủng bố, buôn lậu vũ khí, rửa tiền, tội phạm kinh tế quốc tế và tội phạm mạng, đã trở thành những yếu tố bất ổn quan trọng, ảnh hưởng đến an ninh khu vực, quốc tế và đang đặt ra những thách thức mới đối với hòa bình, ổn định của khu vực và quốc tế”.

Trong từng lĩnh vực cụ thể, giữa các vấn đề an ninh truyền thống và an ninh phi truyền thống có sự tác động, đan xen lẫn nhau. Tuy nhiên, cần nhận thức rõ về sự khác nhau trên một số phương diện chính giữa an ninh truyền thống và an ninh phi truyền thống như sau: An ninh truyền thống nhấn mạnh đến bảo đảm an ninh quốc gia bằng sử dụng biện pháp quân sự là chủ yếu, các biện pháp chính trị, ngoại giao chỉ mang tính chất hỗ trợ; thì biện pháp đảm bảo an ninh phi truyền thống đa dạng hơn và chủ yếu mang tính chất phi quân sự, với hợp tác, phối hợp hành động; thúc đẩy phát triển kinh tế, tiến bộ và công bằng xã hội, thực hiện an sinh xã hội...

An ninh truyền thống lấy chủ quyền quốc gia làm trung tâm, nhấn mạnh đến các mối đe dọa có nguồn gốc từ bên ngoài; An ninh phi truyền thống lấy con người làm trung tâm, nhấn mạnh đến việc bảo đảm cho mỗi cá nhân trong cộng đồng được hưởng các quyền cơ bản và điều kiện thuận lợi để phát triển năng lực của mình. Vì vậy, nguy cơ An ninh phi truyền thống có thể đến từ cả bên ngoài lẫn bên trong, trong đó nhấn mạnh những mối đe dọa từ bên trong mỗi quốc gia.

An ninh phi truyền thống là sự mở rộng trong nội hàm và ngoại diên của khái niệm An ninh truyền thống và khái niệm an ninh quốc gia, an ninh truyền thống. Thực tế những vấn đề an ninh phi truyền thống đã diễn biến hoặc phát sinh từ lâu nhưng hiện nay lại có những đặc điểm mới và được coi là một loại uy hiếp an ninh mới như chủ nghĩa khủng bố, di dân phi pháp, thiếu hụt tài nguyên nước, môi trường sinh thái, buôn lậu ma túy... đang toàn cầu hóa, mạng lưới hóa với phương thức, thủ đoạn hoạt động, hậu

quả có nhiều khác biệt so với trước đây.

An ninh phi truyền thống và an ninh truyền thống trong một điều kiện nhất định có thể chuyển hóa lẫn nhau, diễn hình như các vấn đề dân tộc thiểu số, xung đột tôn giáo, khủng hoảng kinh tế... trong nội bộ một nước có thể vượt qua biên giới quốc gia và lan tỏa ra bên ngoài, trở thành vấn đề xuyên quốc gia, mang tính toàn cầu, ảnh hưởng đến sự ổn định và an ninh của nước khác, khu vực khác... Ngoài ra, an ninh phi truyền thống và an ninh truyền thống cùng tác động, ảnh hưởng đến việc xây dựng chiến lược và chính sách an ninh của mỗi quốc gia nhằm ứng phó với những uy hiếp và thách thức mà an ninh truyền thống và an ninh phi truyền thống cấu thành.

- Đặc điểm của an ninh phi truyền thống:

An ninh phi truyền thống có một số đặc điểm: (i) An ninh phi truyền thống mang tính xuyên quốc gia rõ nét. (ii) An ninh phi truyền thống mang tính phi chính phủ, (iii) An ninh phi truyền thống có sự chồng lấn tương đối giữa thách thức an ninh truyền thống và an ninh phi truyền thống; (iv) An ninh phi truyền thống mang tính toàn cầu; (v) An ninh phi truyền thống có tính chất bạo lực và tính chất phi bạo lực. Tính chất bạo lực trong ANPTT có đặc trưng phi quân sự như chủ nghĩa khủng bố, buôn lậu ma túy, tội phạm có tổ chức xuyên quốc gia..tính chất phi bạo lực như các vấn đề ô nhiễm môi trường, sinh thái xấu đi, khủng hoảng tài chính - tiền tệ, bệnh dịch hoành hành, lũ lụt, thiên tai, cạn kiệt tài nguyên...

- Các mối đe dọa của an ninh phi truyền thống

Theo quan điểm của Liên hợp quốc, An ninh phi truyền thống gồm 10 mối đe dọa: (1) khủng bố, (2) ma túy, (3) hải tặc, (4) rửa tiền, (6) tin tặc, (7) thảm họa môi trường, (8) dịch bệnh, (9) mua bán người, (9) di cư trái phép và (10) cực đoan dân tộc, tôn giáo). Sau đó được sử dụng rộng rãi, phổ biến trên nhiều diễn đàn quốc tế thảo luận về các vấn đề chính trị, an ninh, quốc phòng, kinh tế, xã hội; trong chiến lược quốc phòng, an ninh của nhiều quốc gia - dân tộc, cũng như trong hợp tác an ninh của nhiều khu vực và thế giới.

Dự báo nguy cơ rủi ro hàng đầu đe dọa trong thời gian tới là: (1) Các sự kiện thời tiết cực đoan (ví dụ như lũ lụt, bão, v.v.); (2) Thất bại của giảm thiểu và thích ứng với biến đổi khí hậu, nước biển dâng; (3)

Thảm họa thiên nhiên lớn (ví dụ như động đất, sóng thần, phun trào núi lửa, bão địa từ); (4) Mất đa dạng sinh học lớn và sụp đổ hệ sinh thái; (5) Thiệt hại và thảm họa môi trường sinh thái do con người gây ra; (6) Thất bại của giảm thiểu và thích ứng với biến đổi khí hậu; (7) Vũ khí hủy diệt hàng loạt; (8) Các sự kiện thời tiết cực đoan (ví dụ như lũ lụt, bão, v.v.); (9) khủng hoảng tài nguyên nước, năng lượng; (10) An ninh con người (liên quan đến nhân quyền) do sự phát triển của AI (Artificial Intelligence) Trí tuệ nhân tạo.

Tính chất nguy hiểm của các mối đe dọa an ninh phi truyền thống không chỉ biểu hiện ở mức độ hủy hoại, sự tàn phá của nó đối với cuộc sống của con người, mà còn đặt ra nhiều thách thức đối với sự ổn định xã hội, sự tồn vong của cả cộng đồng, hiệu quả thực tế của hợp tác và hội nhập toàn cầu; thậm chí còn làm nảy sinh các vấn đề về an ninh quân sự. Các thảm họa thiên nhiên, động đất, sóng thần, bão lụt, dịch bệnh, cạn kiệt tài nguyên thiên nhiên... ngày càng thách thức các thành tựu của khoa học, kỹ thuật hiện đại và khả năng, nỗ lực của con người. Khủng bố, tội phạm xuyên quốc gia, tội phạm công nghệ cao, những vấn đề tài chính, an ninh năng lượng, an ninh lương thực... đang thử thách nghiêm ngặt năng lực điều hành của các chính phủ, sự vững chắc của các thể chế chính trị và các nền kinh tế, kể cả nền kinh tế giàu mạnh nhất, cũng như tính khả thi, bền vững của các liên kết quốc tế.

Nội hàm của vấn đề ANPTT mang tính chất “động” và cùng với thời gian, có thể tiếp tục được mở rộng hơn, không phải ngẫu nhiên mà cách đặt vấn đề về an ninh phi truyền thống của các quốc gia, khu vực và cộng đồng có những điểm khác nhau nhất định. Việc xác định những vấn đề cụ thể nào đó trong nội hàm của vấn đề an ninh phi truyền thống chỉ mang ý nghĩa tương đối, nhằm phục vụ cho việc hoạch định, xây dựng chính sách, chiến lược an ninh của đất nước và những cam kết an ninh song phương, đa phương trong hợp tác, liên kết quốc tế, mặt khác là để so sánh sự khác biệt với vấn đề an ninh truyền thống của từng quốc gia cũng như từng khu vực và trên toàn thế giới.

3. Nhận thức về chủ quyền không gian mạng, an ninh mạng

Khái niệm về chủ quyền xuất hiện từ năm 1648

khi hệ thống Westphalia ra đời, theo đó cho rằng, các nhà nước có chủ quyền đối với các lãnh thổ và vấn đề nội bộ của quốc gia mình mà các quốc gia khác không có quyền can thiệp. Nguyên tắc chủ quyền gắn chặt với luật pháp quốc tế và có liên quan tới sự bình đẳng, do đó, mỗi quốc gia bình đẳng với nhau theo luật pháp quốc tế và không có quyền áp đặt lên bất kỳ quốc gia nào.

Về quan niệm an ninh mạng, không gian mạng, Luật an ninh mạng năm 2019 quy định tại Điều 2 như sau:

(1) An ninh mạng là sự bảo đảm hoạt động trên không gian mạng 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.

(2) Bảo vệ an ninh mạng là phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh mạng.

(3) Không gian mạng là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian.

(4) Không gian mạng quốc gia là không gian mạng do Chính phủ xác lập, quản lý và kiểm soát.

Về bản chất vật lý, kỹ thuật, “không gian mạng” có cấu trúc ba lớp: Hạ tầng truyền dẫn vật lý bao gồm các thiết bị phần cứng công nghệ thông tin kết nối một cách hợp lý với nhau, tạo ra các loại mạng; hạ tầng dịch vụ lõi và các dịch vụ tạo ra các giao thức để lưu trữ, xử lý, trao đổi thông tin, chủ yếu bao gồm các quy định chuẩn, hệ điều hành, các công nghệ nền tảng như công nghệ phần mềm, công nghệ mạng, giao diện, phương thức giao tiếp, giao thức, truyền dẫn xử lý thông tin, điều khiển... phần mềm ứng dụng với việc tạo các thư viện và dịch vụ dùng chung; hệ thống ứng dụng công nghệ thông tin và cơ sở dữ liệu, các phần mềm ứng dụng để thông tin dưới dạng số được tạo ra, lưu trữ, xử lý trao đổi nhằm phục vụ nhu cầu cuộc sống và tác động đến nhận thức của con người.

Về tính chất xã hội, “không gian mạng” là môi trường xã hội đặc biệt của con người hội tụ đủ 06 thành tố: (1) chính sách, pháp luật; (2) năng lực công nghệ; (3) nội dung thông tin; (4) nguồn nhân lực; (5)

cơ cấu tổ chức bộ máy; (6) ý thức của con người trên không gian mạng, tạo ra môi trường xã hội đặc biệt của con người.

Trong đó, chính sách, pháp luật là những quy định, quy tắc ứng xử điều chỉnh hành vi và các mối quan hệ giữa cá nhân, tổ chức, cơ quan quản lý nhà nước, các quốc gia, các tổ chức quốc tế khi tham gia vào không gian mạng. Nó tạo hành lang pháp lý đảm bảo cho sự hoạt động an toàn và hiệu quả của không gian mạng, mở đường cho công nghệ phát triển.

Năng lực công nghệ là công nghệ đã được ứng dụng và khả năng nghiên cứu, phát triển công nghệ mới cho hạ tầng công nghệ thông tin, phần mềm, dịch vụ... cấu thành nên không gian mạng, bao gồm các loại công nghệ nền tảng như công nghệ mạng, công nghệ điện tử, bán dẫn, vi xử lý, công nghệ phần mềm... Bên cạnh đó, còn có các quy định chuẩn công nghệ, các quy trình phương thức giao tiếp, giao diện giữa các tầng kiến trúc của một công nghệ nào đó...

Từ góc độ lý thuyết, từ năm 1994, một số học giả quốc tế đã đề cập đến mối quan hệ giữa “không gian mạng” và “chủ quyền quốc gia” hay sự liên quan trong việc áp dụng các lý thuyết trong quan hệ quốc tế đối với Internet. Sự phát triển nhanh chóng của khoa học - công nghệ và Internet đi kèm với sự nổi lên của các vấn đề an toàn, an ninh thông tin, an ninh mạng, do thám mạng, nguy cơ xung đột, chiến tranh mạng giữa các quốc gia trong quan hệ quốc tế... Những vấn đề này đặt ra yêu cầu về quản lý, bảo vệ lãnh thổ, lợi ích quốc gia - dân tộc trên không gian mạng hay còn được hiểu chung trong thuật ngữ “chủ quyền không gian mạng”. Có nhiều ý kiến cho rằng, chủ quyền quốc gia tồn tại trong không gian mạng vì có sự tồn tại của các kết cấu hạ tầng thiết yếu để không gian mạng hình thành và chủ quyền không gian mạng có thể được coi là sự nối dài về quy tắc lãnh thổ trong chủ quyền.

Từ góc độ thực tiễn, ở cấp độ toàn cầu, Tuyên bố năm 2003 về các nguyên tắc của Hội nghị thượng đỉnh thế giới về xã hội thông tin (WSIS) nêu rõ thẩm quyền chính sách đối với các vấn đề chính sách công liên quan đến Internet là quyền chủ quyền của các quốc gia. Báo cáo của Nhóm chuyên gia chính phủ Liên hợp quốc (UNGGE) năm 2013 và năm 2015 nhấn mạnh, chủ quyền của nhà nước và các chuẩn

mực, luật lệ quốc tế bắt nguồn từ chủ quyền áp dụng cho việc nhà nước tiến hành các hoạt động liên quan đến công nghệ thông tin - truyền thông; nguyên tắc chủ quyền là cơ sở để tăng cường bảo mật trong việc sử dụng công nghệ thông tin - truyền thông của các quốc gia.

Về chủ quyền không gian mạng ở Việt Nam, dưới góc độ lý luận, từ năm 2014, Đảng và Nhà nước Việt Nam đã có nhiều văn bản đề cập đến vấn đề “bảo đảm chủ quyền, an ninh quốc gia” trên cơ sở nội dung về các nguy cơ, biện pháp bảo đảm an toàn, an ninh, bảo vệ bí mật quốc gia trong không gian mạng, như Văn kiện Đại hội XIII của Đảng, Nghị quyết số 29-NQ/TW, ngày 25.7.2018, của Bộ Chính trị khóa XII, “Về Chiến lược bảo vệ Tổ quốc trên không gian mạng”; Nghị quyết số 30-NQ/TW, ngày 25.7.2018, của Bộ Chính trị, “Về Chiến lược an ninh mạng quốc gia”... Có thể thấy, các nghị quyết, chỉ thị của Đảng, cũng như các văn bản quy phạm pháp luật của Nhà nước đều thống nhất quan điểm chỉ đạo về bảo đảm an toàn, an ninh thông tin và bảo vệ chủ quyền quốc gia trên không gian mạng.

4. Thách thức an ninh không gian mạng hiện nay

Hiện nay, tình hình an ninh trên không gian mạng, tội phạm công nghệ cao trên thế giới và ở Việt Nam diễn biến phức tạp. Ví dụ an ninh hàng không: Trong những năm gần đây, số vụ tấn công mạng nhằm vào các hệ thống thông tin lĩnh vực hàng không có xu hướng gia tăng cả về tần suất, quy mô và mức độ phức tạp. Theo Cơ quan An toàn hàng không châu Âu (EASA), trung bình mỗi tháng có khoảng 1.000 sự cố an ninh mạng trong lĩnh vực hàng không trên toàn thế giới. Theo báo cáo kết quả khảo sát của công ty an ninh mạng Immuniweb năm 2020, có đến 97% trong số 100 sân bay hàng đầu thế giới chưa đạt yêu cầu kiểm tra về an ninh mạng, tồn tại những điểm yếu bảo mật có thể bị khai thác và tấn công mạng. Từ năm 2019 đến 2020, số vụ tấn công mạng nhằm vào các hãng hàng không tăng 530%, trong đó chỉ tính riêng năm 2020 xảy ra 755 vụ tấn công mạng vào các hãng hàng không, 150 vụ nhằm vào các cảng hàng không; chủ yếu nhằm đánh cắp thông tin cá nhân, tin dụng để lừa đảo, tống tiền, chiếm đoạt tài sản. Điển hình như:

(1) Tháng 01.2016, nhóm tin tặc “Babylon APT” đăng quảng cáo trên thị trường chợ đen trực tuyến, rao bán thông tin về các lỗ hổng bảo mật trong hệ thống mạng của một loạt các hãng hàng không lớn trên thế giới như Delta Airlines, United Airlines, Japan Airlines...;

(2) Đầu tháng 8.2016, hệ thống mạng máy tính của hãng Hàng không Delta của Mỹ đã “gặp sự cố mạng nghiêm trọng”, hệ thống hiển thị thông tin chuyến bay của Hãng bị rối loạn, hãng phải thực hiện thủ công các thủ tục cho hành khách, gây đình trệ gần 3.000 chuyến bay, buộc Delta Airlines phải hủy bỏ hơn 740 chuyến bay của Hãng trên toàn thế giới, gây thiệt hại vật chất ước tính gần 100 triệu USD trong 03 ngày gián đoạn dịch vụ;

(3) Tháng 9.2019, hãng sản xuất máy bay Airbus xác nhận nhiều lần bị tấn công mạng, xâm nhập trái phép hệ thống mạng;

(4) Tháng 11.2020, hãng sản xuất máy bay Embraer của Brazil bị mã hóa, đòi tiền chuộc;

(5) Tháng 02.2021, tin tặc tấn công Công ty Viễn thông hàng không quốc tế (SITA) đánh cắp dữ liệu cá nhân khách hàng...

Nguy hiểm hơn, một số nhóm tin tặc được sự hậu thuẫn của chính phủ các nước tiến hành tấn công mạng nhằm vào các hãng hàng không, cảng hàng không của các nước nhằm mục đích phá hoại, tác động đến chính trị, ngoại giao, kinh tế. Gần đây nhất là vụ tấn công mạng nhằm vào hệ thống thông tin Cơ quan Vận tải hàng không Liên bang Nga (Rosaviasia) hồi tháng 3.2022 và xóa hơn 65 Terabyte dữ liệu và khiến trang web của Rosaviasia không thể truy cập được trong một thời gian.

Tổng quan, những nguy cơ thách thức an ninh không gian mạng bao gồm:

Thứ nhất, sử dụng không gian mạng để tấn công nhằm phá hoại, gây đình trệ hệ thống hạ tầng công nghệ thông tin, hoạt động của cơ quan, tổ chức và cá nhân. Mục tiêu tấn công là các hệ thống thông tin quan trọng như Chính phủ điện tử; hệ thống điều khiển giao thông đường bộ, đường hàng không, cung cấp điện, nước, điều khiển nông nghiệp công nghệ cao; các sân bay, nhà ga, bến cảng, ngân hàng...

Theo Báo cáo chỉ số an toàn thông tin toàn cầu

2017 của Liên minh viễn thông quốc tế (ITU) thuộc Liên hợp quốc, Việt Nam xếp hạng 120/193 quốc gia trên thế giới, 10/11 quốc gia Đông Nam Á, 23/29 quốc gia khu vực Châu Á - Thái Bình Dương về năng lực bảo đảm an toàn thông tin mạng. (Kết quả này được đưa ra dựa trên việc xác định vị trí những địa chỉ IP khởi động các cuộc tấn công. Trong một số trường hợp, các địa chỉ IP được tin tặc sử dụng có thể là địa chỉ các proxy để ẩn đi vị trí thực sự của chúng).

Thứ hai, tấn công vào cơ sở dữ liệu các cơ quan, tổ chức, tập đoàn kinh tế lớn nhằm thu thập, trộm cắp thông tin, dữ liệu, Tháng 7.2016, trang web của Vietnam Airline cũng bị hacker tấn công và hậu quả là rất nhiều thông tin cá nhân của khách hàng đã bị lộ; trong các ngày 08,09,10.3.2017, tin tặc đã tấn công, thay đổi giao diện website Cảng hàng không quốc tế Tân Sơn Nhất, Đà Nẵng, Phú Quốc, Rạch Giá.

Thứ ba, tấn công nhằm chiếm quyền điều khiển máy tính, thiết bị số, truy cập bất hợp pháp vào hệ thống công nghệ thông tin của các cơ quan, tổ chức, doanh nghiệp chiếm quyền điều khiển từ xa, thay đổi giao diện Website hoặc cơ sở dữ liệu... nhằm mục đích tống tiền hoặc hạ uy tín của các đơn vị này. Hệ thống mạng thông tin của ngành hàng không tại nước ta cũng đã và đang là mục tiêu hàng đầu của tấn công, khủng bố mạng.

Thứ tư, lợi dụng kết nối Internet để thực hiện tội phạm, nổi lên là lừa đảo chiếm đoạt tài sản thông qua hoạt động kinh doanh đa cấp, thương mại điện tử; gian lận, trộm cắp trong hoạt động thanh toán thẻ và thanh toán điện tử; trộm cắp, mua bán thông tin thẻ tín dụng nhằm chiếm đoạt tài sản; đánh bạc và tổ chức đánh bạc thông qua mạng Internet; trộm cắp tài khoản người dùng mạng xã hội để lừa đảo chiếm đoạt tài sản; truyền bá, phát tán ấn phẩm đồi trụy, tổ chức môi giới mại dâm, phát tán ảnh đồi trụy, hình ảnh riêng tư để làm nhục người khác.

Thứ năm, tội phạm sử dụng công nghệ cao đang ngày càng gây ra những thiệt hại lớn đối với sự phát triển của mỗi quốc gia và trên toàn thế giới. Theo dự báo của trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT), xu hướng khai thác và tấn công từ các thiết bị IOT như camera, smart TV là một trong 5 xu hướng tấn công mạng.

5. Giải pháp chủ động đảm bảo an ninh mạng trong bối cảnh hiện nay

5.1 Nhóm giải pháp chung:

Một là, hoàn thiện, nâng cao năng lực bảo đảm an toàn, an ninh mạng và thông tin mạng quốc gia cho các cơ quan, ban, ngành, địa phương; các công trình hạ tầng trọng yếu có kết nối mạng, các tập đoàn kinh tế quan trọng

Hoàn thiện hệ thống hạ tầng thông tin, thiết bị công nghệ thông tin bảo đảm an toàn, an ninh mạng và thông tin mạng quốc gia cho các cơ quan trung ương và địa phương; các công trình hạ tầng trọng yếu, các tập đoàn kinh tế quan trọng có kết nối mạng. Các hệ thống thông tin quan trọng quốc gia được xác định, áp dụng các biện pháp bảo vệ tương xứng, liên tục từ giai đoạn thiết kế, xây dựng, phát triển, vận hành và sử dụng. (2) Tập trung được nguồn lực toàn xã hội trong bảo đảm an toàn, an ninh mạng và thông tin mạng quốc gia. (3) Nhà nước bảo đảm kinh phí cho công tác an toàn, an ninh mạng và thông tin mạng quốc gia.

Hai là, xây dựng môi trường không gian mạng lành mạnh: Nhận thức, năng lực bảo đảm an toàn, an ninh mạng và thông tin mạng quốc gia của toàn xã hội được nâng cao. Người sử dụng có kiến thức cơ bản về bảo mật trong môi trường mạng; thường xuyên được cập nhật về tình hình, mức độ rủi ro mất an toàn thông tin để có thể tự phòng ngừa hiệu quả. Hệ thống mạng thông tin bảo đảm các tiêu chuẩn về bảo mật.

Các doanh nghiệp công nghệ thông tin trong nước lớn mạnh, làm chủ thị trường, không bị lệ thuộc vào sản phẩm của nước ngoài. Các loại hình báo chí chính thống giữ vai trò chủ đạo, định hướng dư luận để đủ sức đề kháng đối với các thông tin xấu, độc trên không gian mạng.

Huy động sức mạnh của cả hệ thống chính trị và toàn dân trong đấu tranh phản bác, vô hiệu hoá các thông tin xấu, luận điệu phản tuyên truyền trên không gian mạng.

Ba là, xây dựng lực lượng chuyên trách đủ năng lực, chủ động đối phó với mọi nguy cơ xảy ra trên không gian mạng: Lực lượng chuyên trách bảo đảm an ninh thông tin, an ninh không gian mạng quốc gia trực thuộc Bộ Công an; lực lượng thực hiện nhiệm vụ quốc phòng trên không gian mạng trực thuộc Bộ

Quốc phòng; lực lượng bảo đảm an toàn thông tin trực thuộc Bộ Thông tin và Truyền thông đủ năng lực, sẵn sàng, chủ động đối phó với mọi nguy cơ xảy ra trên không gian mạng.

Bốn là, quan hệ hợp tác quốc tế trên lĩnh vực bảo đảm an toàn, an ninh thông tin, an ninh mạng được mở rộng và tăng cường: (1) Mở rộng quan hệ hợp tác quốc tế với các nước trên thế giới về bảo đảm an toàn, an ninh mạng và thông tin mạng quốc gia, tranh thủ sự ủng hộ của cộng đồng quốc tế đấu tranh phản bác luận điệu sai trái của các thế lực thù địch chống Việt Nam. (2) Tham gia các công ước, thỏa thuận quốc tế về bảo đảm an toàn, an ninh mạng và thông tin mạng quốc gia, phòng, chống tội phạm mạng phù hợp với chủ trương, đường lối, chính sách, pháp luật của Đảng, Nhà nước. (3) Triển khai có hiệu quả, thiết thực các Nghị định thư, thỏa thuận hợp tác về phòng chống tội phạm mạng đã ký kết với các nước.

5.2 Nhóm giải pháp cụ thể khác:

Mã hóa dữ liệu: Đối với những thông tin quan trọng, mật thiết, người dùng nên mã hóa trước khi gửi đi. Mục đích của việc mã hóa thông tin là tránh khỏi sự nhòm ngó, tấn công của tin tặc.

Cập nhật phần mềm: Một trong những giải pháp tránh mất thông tin hiệu quả là cài đặt phần mềm. Người dùng nên cài đặt và cập nhật thường xuyên phần mềm diệt virus, phần mềm cảnh báo tấn công, phần mềm giám sát hệ thống...

Cài đặt phần mềm diệt virus: Cài đặt phần mềm chống virus xâm nhập cũng là một giải pháp được các chuyên gia khuyến cáo. Lưu ý, người dùng nên quét virus trước khi tải phần mềm về máy. Một số công cụ online giúp kiểm tra mã độc online như: virus total, 6scan security, sitecheck.

Sử dụng phần mềm có nguồn gốc rõ ràng: Đảm bảo rằng mọi phần mềm, ứng dụng trên thiết bị của người dùng có nguồn gốc rõ ràng sẽ giúp hạn chế nguy cơ làm mất an toàn thông tin.

Kiểm soát quyền trên thiết bị: Hãy phân chia quyền thật rõ ràng cho các thành viên, người thân trên thiết bị mà người dùng sở hữu.

Tắt các kết nối Wifi, Bluetooth, NFC khi không sử dụng: Hãy nhớ sau khi vào mạng, người dùng phải tắt các kết nối Wifi, bluetooth, NFC để tránh nguy cơ bị rò rỉ mật khẩu, tài liệu và thông tin cá nhân./.