BẢO ĐẢM AN NINH, AN TOÀN THÔNG TIN MẠNG Ở VIỆT NAM

PGS, TS.Trần Đăng Bộ[1], Đại tá, TS.Đàm Trọng Tùng[2]

[1]Trường Đại học Thành Đô;

Email:trandangbo@yahoo.com.vn.

[2]Học viện Kỹ thuật quân sự.

TÓM TẮT

Trong kỷ nguyên số, thông tin và hệ thống thông tin là một trong những yếu tố quyết định sự phát triển bền vững của quốc gia, vùng lãnh thổ. Theo đó, việc đảm bảo an ninh mạng và an toàn thông tin mạng cho quốc gia, vùng lãnh thổ phát triển bền vững là nhu cầu cần thiết, cấp bách. Mạng và không gian mạng không chỉ mở ra cơ hội để con người khai mở tri thức, mà cùng với quá trình đó đã làm phát sinh không ít vấn đề phức tạp như: Chiến tranh mạng, tội phạm mạng, tấn công mạng, khủng bố mạng, gián điệp mạng… Đây là những nguy cơ đe dọa an ninh, an toàn thông tin mạng, trực tiếp ảnh hưởng đến sự phát triển bền vững của mọi quốc gia, vùng lãnh thổ, trong đó có Việt Nam. Vậy thực tiễn an ninh, an toàn thông tin mạng ở Việt Nam hiện nay thế nào? Cần giải pháp gì để tăng cường bảo đảm an ninh, an toàn thông tin mạng? Bài viết sẽ góp phần làm rõ những nội dung này.

Từ khóa: *An ninh mạng*; *An toàn thông tin mạng*; *Hệ thống thông tin*; *Không gian mạng.*

ABSTRACT

In the digital era, information and information systems are among the decisive factors for the sustainable development of a nation or region. Accordingly, ensuring cybersecurity and network information safety for the sustainable development of a nation or region is a necessary and urgent need. Networks and cyberspace not only open opportunities for human knowledge expansion but also give rise to numerous complex issues such as cyber warfare, cybercrime, cyber attacks, cyber terrorism, cyber espionage, etc. These are risks that threaten the security and safety of network information, directly affecting the sustainable development of all nations and regions, including Vietnam. So, what is the current state of network information security and safety in Vietnam? What solutions are needed to enhance the assurance of network information security and safety? This article will contribute to clarifying these contents.

Keywords: *Cybersecurity; Network Information Safety; Information Systems; Cyberspace.*

1. GIỚI THIỆU

Sự kết nối và tương tác thông qua không gian mạng, nhất là mạng internet đã tạo ra khả năng mới chưa từng có trong lịch sử nhân loại, làm thay đổi vai trò của con người đối với sự phát triển của xã hội. Ngoài lợi ích đối với việc xây dựng xã hội thông tin và phát triển kinh tế tri thức, xã hội số, kinh tế số mà mạng và không gian mạng đem lại, thì chiến tranh mạng, tội phạm mạng, tấn công mạng, khủng bố mạng, gián điệp mạng và nhiều vấn đề phức tạp khác trên môi trường mạng và không gian mạng là những nguy cơ không chỉ đe dọa an ninh, an toàn thông tin mạng, mà còn trực tiếp đe doạ quốc phòng, an ninh

quốc gia của mọi quốc gia, dân tộc, trong đó có Việt Nam. Do nhận thức rõ ý nghĩa, tầm quan trọng của an ninh, an toàn thông tin mạng, tại Hội nghị Trung ương 6 khóa XIII Đảng ta khẳng định: "bảo đảm an ninh, an toàn thông tin mạng là then chốt, ưu tiên đầu tư phát triển nhanh, đi trước một bước"[1]. Cụm từ *an ninh, an toàn thông tin mạng* sử dụng trong bài viết là cụm từ viết tắt được hình thành trên cơ sở ghép hai thuật ngữ: *An ninh mạng* và *An toàn thông tin mạng*; và được viết tắt là *an ninh, an toàn thông tin mạng*.

Nội dung bài viết nhằm làm rõ thêm một số vấn đề về mạng và không gian mạng, về an ninh, an toàn thông tin mạng, nhất là thực tiễn an ninh, an toàn thông tin mạng ở Việt Nam thời gian gần đây, từ đó rút ra một số vấn đề cần sớm giải quyết để bảo đảm tốt hơn an ninh, an toàn thông tin mạng. Những vấn đề lý luận và thực tiễn về an ninh, an toàn thông tin mạng sẽ góp phần nâng cao nhận thức, trách nhiệm của các cơ quan, tổ chức, cá nhân quản lý, vận hành, sử dụng mạng và không gian mạng, nhất là lực lượng chuyên trách bảo đảm an toàn, an ninh mạng. Theo đó, bảo đảm an toàn, an ninh mạng là trách nhiệm của các cơ quan, tổ chức, cá nhân Việt Nam và các tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến bảo đảm an toàn, an ninh mạng tại Việt Nam. Bảo đảm an toàn, an ninh mạng phải tuân thủ Hiến pháp, pháp luật Việt Nam và quy định của luật pháp quốc tế; Đặt dưới sự lãnh đạo của Đảng, sự quản lý thống nhất của Nhà nước, huy động sức mạnh tổng hợp của hệ thống chính trị và toàn dân tộc, phát huy vai trò nòng cốt của lực lượng chuyên trách bảo đảm an toàn, an ninh mạng.

2. PHƯƠNG PHÁP NGHIÊN CỨU

Để thực hiện bài viết này, tác giả sử dụng các phương pháp thu thập và phân tích dữ liệu. Các dữ liệu của bài viết được hệ thống hóa, phân tích, tổng hợp nhằm đánh giá trung thực, khách quan thực tiễn an ninh, an toàn thông tin mạng ở Việt Nam giai đoạn 2018-2022; đồng thời đề xuất giải pháp tăng cường bảo đảm an ninh, an toàn thông tin mạng thời gian tới. Số liệu phục vụ nghiên cứu được thu thập liên quan đến đánh giá thực tiễn an ninh, an toàn thông tin mạng gồm: Một số báo cáo và công trình nghiên cứu liên quan đã công bố; Văn kiện của Đảng và văn bản quy phạm pháp luật về an ninh, an toàn thông tin mạng, về tăng cường bảo đảm an ninh, an toàn thông tin mạng, trực tiếp là các văn bản quy phạm pháp luật của Chính phủ, các bộ, ngành về an ninh, an toàn thông tin mạng ở Việt Nam.

3. KẾT QUẢ NGHIÊN CỨU

3.1. Một số vấn đề về mạng, không gian mạng và an ninh, an toàn thông tin mạng ở Việt Nam

Sự phát triển của khoa học và công nghệ trong kỷ nguyên số đã tạo ra một không gian phát triển mới, có ý nghĩa chiến lược, đó là mạng và không gian mạng. Hiện nay, tuy mỗi quốc gia, vùng lãnh thổ có quan niệm riêng về mạng và không gian mạng, nhưng nội hàm của các quan niệm này không nhiều khác biệt. Trong đó, nhiều quốc gia, vùng lãnh thổ có quan niệm tương đồng với quan niệm của Việt Nam về mạng và không gian mạng. Đó là, theo *Luật An toàn thông tin mạng năm 2015* và *Luật An ninh mạng năm 2018* của Việt Nam thì: *Mạng* là môi trường, trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính; *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. Với các quan niệm này, nội hàm của quan niệm không gian mạng rộng hơn và bao quát nội hàm của quan niệm mạng. Với những đặc tính như vậy, không gian mạng trở thành một bộ phận cấu thành của xã hội, có ảnh hưởng tới mọi mặt đời sống xã hội, đem lại nhiều cơ hội mới để các quốc gia xây dựng và phát triển. Vì thế ngày nay, mạng và không gian mạng đã trở thành môi trường chủ yếu, không thể thiếu trong triển khai chiến lược quan hệ đối ngoại, củng cố, duy trì các hoạt động của mọi quốc gia, dân tộc mang lại lợi ích to lớn, đóng góp quan trọng vào đổi mới tư duy và phát triển trên mọi lĩnh vực.

Thực tiễn cho thấy, mạng và không gian mạng đã mở ra cơ hội để con người khai mở tri thức, đồng thời làm phát sinh không ít vấn đề phức tạp. Những vấn đề phức tạp này đặt ra yêu cầu phải đảm bảo an ninh, an toàn thông tin mạng. Theo *Luật An ninh mạng năm 2018*: *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; theo *Luật An toàn thông tin mạng năm 2015*: *An toàn thông tin mạng* là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

Khi con người phụ thuộc ngày càng nhiều vào mạng và không gian mạng, nhất là sử dụng mạng internet, các thiết bị kết nối mạng và công nghệ mạng, thì vấn đề kiểm soát và làm chủ không gian mạng nhằm bảo đảm an ninh, an toàn thông tin mạng cho tăng trưởng và phát triển bền vững là nhiệm vụ quan trọng, cấp bách đối với mọi quốc gia, vùng lãnh thổ không phân biệt chế độ chính trị và trình độ phát triển. Như Chủ tịch Interpol tại Interpol World 2017 cảnh báo: Cùng với những lợi ích từ quá trình toàn cầu hóa, cách mạng công nghệ và không gian mạng xuyên biên giới, thế giới còn phải đối mặt với những mối đe dọa tội phạm và khủng bố do các đối tượng xấu lợi dụng sự thuận tiện, linh hoạt và khả năng ẩn danh mà công nghệ cao mang tới cho người sử dụng. Mạng và không gian mạng có vai trò quan trọng như vậy nên an ninh, an toàn thông tin mạng được xác định "là trụ cột quan trọng, xuyên suốt để tạo lập niềm tin số và bảo vệ sự phát triển thịnh vượng của đất nước trong kỷ nguyên số nhằm thực hiện thành công chuyển đổi số quốc gia, một trong những nhiệm vụ trọng tâm và đột phá chiến lược" [2]. Với ý nghĩa như vậy mà "bảo đảm an ninh, an toàn thông tin mạng mạng là then chốt, ưu tiên đầu tư phát triển nhanh, đi trước một bước"[1].

3.2. Thực tiễn an ninh, an toàn thông tin mạng ở Việt Nam giai đoạn 2018-2022 và 6 tháng đầu năm 2023

Việt Nam là quốc gia có sự phát triển internet nhanh. Nếu tháng 6/2021, số người dùng Internet ở Việt Nam là gần 70 triệu người, chiếm gần 70% dân số [3]; thì đến tháng 01/2023 có 77,93 triệu người dùng Internet, chiếm 79,1% tổng dân số, trong khi năm 2022, thế giới có 63% dân số sử dụng Internet. Với số lượng người Việt Nam dùng Internet lớn cùng với sự gia tăng và phổ biến của mạng xã hội, các hệ thống như website, ứng dụng hoặc email của các cơ quan, tổ chức, cá nhân và doanh nghiệp ở Việt Nam trở thành mục tiêu hấp dẫn cho các cuộc tấn công mạng và vi phạm bảo mật. Điều này đồng nghĩa với việc gia tăng khả năng rủi ro, khiến thách thức về an ninh, an toàn thông tin mạng gia tăng với tính chất, quy mô và mức độ ngày càng nghiêm trọng hơn. Theo đó, việc đảm bảo an ninh, an toàn thông tin mạng là thách thức không nhỏ

đối với các cơ quan, tổ chức, cá nhân và doanh nghiệp trong kỷ nguyên số. Vậy, thực tiễn an ninh, an toàn thông tin mạng và bảo đảm an ninh, an toàn thông tin mạng ở Việt Nam thời gian qua như thế nào?

Số liệu thống kê cho thấy, trung bình mỗi năm Việt Nam phát hiện trên 850.000 tài liệu chiến tranh tâm lý, phản động, ân xá quốc tế, tài liệu tuyên truyền tà đạo trái phép; gần 750.000 tài liệu tuyên truyền chống Đảng, Nhà nước được tán phát vào Việt Nam qua đường bưu chính [3]. Riêng giai đoạn 2010-2019 có 53.744 lượt cổng thông tin, trang tin điện tử có tên miền .vn bị tấn công, trong đó có 2.393 lượt cổng thông tin, trang tin điện tử của cơ quan Đảng, Nhà nước ".gov.vn", xuất hiện nhiều cuộc tấn công mang màu sắc chính trị, gây hậu quả nghiêm trọng [4]. Cụ thể thực tiễn an ninh, an toàn thông tin mạng trong giai đoạn 2018-2022 và 6 tháng đầu năm 2023 như sau:

Trong năm 2018 xảy ra một số cuộc tấn công mạng có chủ đích, đánh cắp thông tin bí mật nhà nước, gây hậu quả nghiêm trọng ở một số lĩnh vực. Trong đó tháng 3/2018, Facebook làm lộ dữ liệu cá nhân để một nhà phát triển bán lại cho Công ty Cambridge Analityca, dẫn tới 87 triệu dữ liệu thông tin người dùng bị lộ, trong đó có 427.466 tài khoản của người dùng Việt Nam [5]. Vì vậy, trong Báo cáo chỉ số an toàn, an ninh thông tin toàn cầu (GCI) của Liên minh Viễn thông Quốc tế (ITU), xếp hạng của Việt Nam ở mức thấp. Trong bảng xếp hạng GCI năm 2017 và 2018 tiến hành tháng 3/2019, Việt Nam xếp thứ 50/194 quốc gia, vùng lãnh thổ, thứ 5/11 trong ASEAN [6]. Theo số liệu thống kê của Kaspersky: Việt Nam thường xuyên nằm trong top 3 quốc gia bị tấn công mạng nhiều nhất năm 2018.

Năm 2019, hoạt động gián điệp mạng, tình trạng lộ bí mật nhà nước trên không gian mạng diễn biến phức tạp. Bằng chứng là: "phát hiện hàng trăm trang web tên miền quốc gia bị tấn công; 127 trang và 349 cổng thông tin điện tử của nhiều cơ quan, đơn vị tồn tại các lỗ hổng bảo mật nghiêm trọng; 40 vụ lộ bí mật nhà nước qua intơnét với 241 đầu tài liệu"[7]; riêng Bộ Công an khởi tố 10 vụ với 116 bị can; bắt giữ và bàn giao cảnh sát các nước 555 đối tượng; phối hợp xử phạt hành chính và trục xuất 254 đối tượng phạm tội trên không gian mạng [7]. Báo cáo của Microsoft (ngày 24/6/2020) về các mối đe doạ bảo mật cho biết, năm 2019 Việt Nam là quốc gia có tỷ lệ gặp phải mã độc tống tiền cao nhất Châu Á Thái Bình Dương. Đặc biệt, để thu thập, chiếm đoạt thông tin, tài liệu bí mật nhà nước, tin tặc không ngừng gia tăng hoạt động tấn công mạng vào hệ thống thông tin quan trọng quốc gia, hệ thống thông tin an ninh quốc gia, nhất là các cơ quan trọng yếu, các tập đoàn kinh tế lớn. Báo cáo đánh giá an ninh mạng năm 2019 của Tập đoàn công nghệ Bkav cho thấy: Chỉ tính riêng thiệt hại do virus máy tính gây ra đối với người dùng Việt Nam đã lên tới 20.892 tỷ đồng (tương đương 902 triệu USD), hơn 1,8 triệu máy tính bị mất dữ liệu do sự lan tràn của các loại mã độc mã hóa dữ liệu tống tiền, trong đó có nhiều máy chủ chứa dữ liệu của các cơ quan, gây đình trệ hoạt động của nhiều cơ quan, doanh nghiệp. Theo dữ liệu từ Kaspersky: Số vụ tấn công trực tuyến ở Việt Nam năm 2019 giảm hơn 30% so với năm 2018 với 75.004.388 vụ, xếp thứ 17 toàn cầu; 371.979.051 vụ tấn công ngoại tuyến, giảm hơn 10% so với năm 2018, xếp thứ 6 thế giới; sự cố gây ra do nguồn đe dọa mạng năm 2019 giảm 49,75% so với năm 2018 (từ 5.335.619 còn 2.681.360 sự cố), xếp thứ 30 thế giới.

Trong năm 2020, đại dịch Covid-19 diễn biến phức tạp, khó lường phải

thực hiện giãn cách xã hội, nhiều hoạt động trong đời sống xã hội được thực hiện trên không gian mạng, nên các nhóm tin tặc hoạt động rất tích cực trên không gian mạng; do đó **phương thức, thủ đoạn, quy mô lừa đảo trực tuyến tăng cao.** Cụ thể: Hoạt động lừa đảo trực tuyến - một hình thức tấn công mạng phổ biến gia tăng, nhất là các nhóm tin tặc sử dụng mạng viễn thông, mạng xã hội để lừa đảo. Đặc biệt, khi nhiều sản phẩm, phần mềm, ứng dụng phổ biến được công bố điểm yếu và lỗ hổng bảo mật nguy hiểm, thì các nhóm tin tặc đã lợi dụng những điểm yếu và lỗ hổng bảo mật này để tiến hành nhiều chiến dịch tấn công mạng với những quy mô khác nhau. Trong đó, Việt Nam không là ngoại lệ khi phát hiện và ngăn chặn hàng loạt chiến dịch tấn công mạng qui mô lớn, có chủ đích với hậu quả ngày càng nghiêm trọng hơn.

Năm 2020, riêng Bộ Công an đã điều tra, đề nghị xử lý hình sự 81 đối tượng, xử phạt vi phạm hành chính 353 trường hợp có hành vi tán phát thông tin sai sự thật trên không gian mạng [7]. Theo Kaspersky: Đã phát hiện 64,354,130 các mối đe dọa mạng khác nhau; trong đó, số lượng mối đe dọa trực tuyến và ngoại tuyến giảm 14,2% và 27,8% so với năm 2019; Tỷ lệ người dùng bị ảnh hưởng bởi mối đe dọa mạng là 39,1% tương ứng vị trí thứ 19 toàn cầu, giảm 2 bậc so với năm 2019; ngoài ra, 64,6% người dùng bị ảnh hưởng bởi mối đe dọa ngoại tuyến, tương ứng với vị trí thứ 8 trên thế giới về các mối nguy hiểm liên quan đến phần mềm độc hại phát tán qua USB, CD và DVD và các phương thức ngoại tuyến khác, giảm 2 bậc so với năm 2019. Tháng 6/2021, ITU công bố GCI năm 2020; trong đó, Việt Nam vươn lên thứ 25/194 quốc gia, vùng lãnh thổ, đứng thứ 7 trong khu vực châu Á - Thái Bình Dương và thứ 4 trong ASEAN [8].

Với nỗ lực không ngừng của Chính phủ Việt Nam trong việc bảo đảm an ninh, an toàn thông tin mạng, mà trong năm 2021 số lượng các cuộc tấn công mạng giảm. Tuy nhiên, lợi dụng việc các cơ quan, tổ chức, cá nhân chuyển sang hình thức làm việc từ xa, trực tuyến là phổ biến, nên năm 2021 là năm có nhiều cuộc tấn công mạng lớn, xảy ra nhiều vụ rò rỉ thông tin, dữ liệu cá nhân người Việt Nam; điển hình là: Chiều ngày 13/5/2021, 17GB dữ liệu thông tin cá nhân của 9.667 người dùng Việt Nam trong 5 tập hợp file bị tài khoản Ox1337xO đăng tải lên diễn dàn RaidForum; Ngày 04/8/2021 một tài khoản có tên @lovebkav@protonmail.com@ đăng bán công khai thông tin về mã nguồn được cho là của phần mềm BKAV; Ngày 08/8/2021, một tài khoản có tên chunxong tiếp tục đưa tin nhắn trên nền tảng chat nội bộ của Bkav để khẳng định mình sở hữu dữ liệu mới và rao bán gói dữ liệu của Bkav với giá 290.000 USD, tương đương 6.6 tỷ đồng; tháng 8/2021, trên diễn đàn Raidforums, tài khoản có tên xiaolin1983 đăng bán dữ liệu thông tin cá nhân, gồm tên cha mẹ và công việc của hơn 300.000 sinh viên của 10 trường Đại học tại Việt Nam [8].

Cùng năm 2021, Kaspersky phát hiện và chặn 63.482.728 vụ tấn công mạng khác nhau lây lan qua Internet trên máy tính người dùng thuộc Kaspersky tại Việt Nam. Đây là con số thấp nhất giai đoạn 2017-2021, giảm 871.402 vụ so với năm 2020. Số liệu từ Kaspersky còn cho thấy, số lượng các mối đe dọa ngoại tuyến ở Việt Nam năm 2021 giảm so với các năm trong giai đoạn 2017-2021 với 162.913.157 mối đe dọa liên quan đến phần mềm độc hại phát tán qua USB, CD, DVD và các phương thức

ngoại tuyến khác. So với năm 2020, giảm 38,3% và 56,7% người dùng Việt Nam bị tấn công bởi phần mềm độc hại lây lan, xếp thứ 31 trên toàn cầu và giảm 23 bậc. Kết quả từ Chương trình đánh giá an ninh mạng dành cho người sử dụng cá nhân, do Tập đoàn Bkav thực hiện tháng 12/2021 cho thấy: Thiệt hại do virus máy tính gây ra đối với người dùng Việt Nam tiếp tục ở mức rất cao, khoảng 24.400 tỷ đồng. Năm 2021 có 70,7 triệu lượt máy tính bị nhiễm virus; trong đó số lượt máy tính bị virus mã hoá dữ liệu tấn công lên tới hơn 2,5 triệu lượt, cao gấp 4,5 lần so với năm 2020. Đến tháng 12/2021 Việt Nam là quốc gia có tỷ lệ nhiễm mã độc và hứng chịu các cuộc tấn công mạng thuộc nhóm cao trên thế giới; xếp thứ 25/194 quốc gia, vùng lãnh thổ, thứ 7 khu vực châu Á - Thái Bình Dương, thứ 4 trong ASEAN về an ninh, an toàn thông tin mạng.

Năm 2022, Kaspersky phát hiện và chặn 41,989,163 mối đe dọa mạng khác nhau từ Internet, so với năm 2021, con số này giảm 34%; Về các nguy cơ liên quan đến phần mềm độc hại phát tán qua USB, CD, DVD và các phương thức ngoại tuyến khác giảm đáng kể, với tổng số 121,542,272 vụ, giảm 25,39% so với năm 2021. Sáu tháng đầu năm 2022, Bộ Công an phát hiện, xử lý 840 chuyên án, vụ việc liên quan tội phạm lừa đảo, chiếm đoạt tài sản qua mạng, tăng 42% so với 6 tháng cuối năm 2021[9]. Kaspersky cho biết: Năm 2022 là năm thứ 5 liên tiếp Việt Nam chứng kiến sự sụt giảm về số lượng các vụ tấn công mạng. Đáng chú ý, số lượng các mối đe dọa từ Internet và các mối đe dọa ngoại tuyến ở mức thấp nhất trong vòng nửa thập kỷ qua.

Theo Bộ Thông tin và Truyền thông: Sáu tháng đầu năm 2023 ghi nhận, cảnh báo và hướng dẫn xử lý 6.362 cuộc tấn công mạng gây ra sự cố vào các hệ thống thông tin tại Việt Nam giảm 4,2% so với 6 tháng đầu năm 2022 với 6.641 cuộc; đã điều phối ngăn chặn 1.530 trang web/blog vi phạm pháp luật (559 trang lừa đảo trực tuyến chiếm 36,5%); bảo vệ hơn 2,7 triệu người dân không truy cập vào các website lừa đảo trực tuyến, vi phạm pháp luật trên không gian mạng; song lừa đảo trực tuyến 6 tháng đầu năm 2023 tăng gần 65% so với cùng kỳ năm 2022 [10]. Tuy nhiên, nhờ công tác tổ chức kiểm tra, đánh giá, giám sát, bảo đảm an toàn, an ninh mạng cho các hệ thống thông tin phục vụ chính phủ điện tử, chuyển đổi số tiếp tục được đẩy mạnh mà số lượng các cuộc tấn công mạng trong tháng 7/2023 đã giảm nhiều.

3.3. Một số vấn đề đặt ra từ thực tiễn an ninh, an toàn thông tin mạng

Thực tiễn an ninh, an toàn thông tin mạng giai đoạn 2018-2022 và 6 tháng đầu năm 2023 đang đặt ra một số vấn đề cần sớm giải quyết để bảo đảm tốt hơn an ninh, an toàn thông tin mạng trong thời gian tới như:

Một là, *nguy cơ đe dọa an ninh, an toàn thông tin mạng trong quá trình chuyển đổi số quốc gia ngày càng gia tăng, khó kiểm soát*. Cùng với sự phát triển của các thiết bị thông minh, kết nối mạng và các hoạt động trên không gian mạng đặt ra nhiều khó khăn, thách thức mới đối với công tác quản lý an ninh, an toàn thông tin mạng; trong đó các nguy cơ đe dọa an ninh, an toàn thông tin mạng sẽ gia tăng đột biến, khó dự lường, khó kiểm soát hơn. Tin tặc, nhất là các thế lực thù địch lợi dụng mạng và không gian mạng để tuyên truyền xuyên tạc, chống phá nhằm chia rẽ khối đại đoàn kết toàn dân tộc, làm suy giảm niềm tin của cán bộ, đảng viên và nhân dân đối với Đảng, Nhà nước và chế độ chính trị ở nước ta. Hàng loạt chiến dịch tuyên truyền phá hoại nền tảng tư tưởng của Đảng, chia rẽ nội bộ, kích động bạo loạn, gây rối an ninh, trật tự, an toàn xã

hội đã và đang diễn ra ngày càng phức tạp. Đó cũng là những nguy cơ đe dọa an ninh, an toàn thông tin mạng sẽ xuất hiện ngày càng gia tăng, rất khó kiểm soát trong quá trình chuyển đổi số quốc gia.

Hai là, *hệ thống văn bản quy phạm pháp luật về quản lý an ninh, an toàn thông tin mạng còn bất cập, chưa bắt kịp thực tiễn tình hình*. Thực tiễn những năm gần đây cho thấy, các vụ tấn công mạng, tội phạm mạng gia tăng cả số lượng và quy mô, trong khi hệ thống văn bản quy phạm pháp luật về quản lý an ninh, an toàn thông tin mạng còn nhiều bất cập, chưa bắt kịp với sự phát triển của các loại thiết bị thông minh, kết nối mạng và công nghệ được sử dụng trên không gian mạng. Quản lý nhà nước về an ninh, an toàn thông tin mạng còn sơ hở, chưa theo kịp tốc độ phát triển của khoa học, công nghệ và hội nhập quốc tế. Về điều này, Đại hội XIII của Đảng đánh giá: "Công tác quản lý, bảo đảm an toàn thông tin, an ninh mạng còn hạn chế".

Ba là, *thiếu cơ sở pháp lý và cơ chế hợp tác quốc tế về bảo đảm an ninh, an toàn thông tin mạng*. Cũng như các mối đe dọa an ninh phi truyền thống khác, các mối đe dọa an ninh, an toàn thông tin mạng mang tính xuyên quốc gia, không có giới hạn về không gian và thời gian. Vì vậy, để giải quyết vấn đề này, đòi hỏi phải có cơ chế hợp tác quốc tế. Mặc dù các quốc gia, dân tộc đều nhận thức rõ rủi ro trên không gian mạng và sự cần thiết phải bảo đảm an ninh, an toàn thông tin mạng, nhưng cho đến nay mới chỉ có các thỏa thuận giữa một số quốc gia liên quan đến bảo đảm an ninh, an toàn thông tin mạng trong một số lĩnh vực, mà chưa có các quy chuẩn thống nhất mang tính quốc tế, nhất là chưa thiết lập được các nguyên tắc pháp lý mang tính quốc tế để ứng phó với các mối đe dọa an ninh, an toàn thông tin mạng - một loại hình mới về các mối đe dọa an ninh phi truyền thống.

Bốn là, *phối hợp, hợp tác giữa các cơ quan, tổ chức, cá nhân trong bảo đảm an ninh, an toàn thông tin mạng chưa chặt chẽ, thiếu chuyên nghiệp*. Bảo đảm an ninh, an toàn thông tin mạng, nhất là an ninh, an toàn thông tin mạng cho hệ thống thông tin quan trọng về quốc phòng, an ninh và phòng, chống tội phạm mạng, tấn công mạng, khủng bố mạng, gián điệp mạng và các nguy cơ đe dọa an ninh, an toàn thông tin mạng khác, không chỉ là nhiệm vụ của các lực lượng chuyên trách, mà còn là trách nhiệm của các cơ quan, tổ chức, cá nhân Việt Nam và các tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến bảo đảm an toàn, an ninh mạng tại Việt Nam. Tuy nhiên, sự phối hợp, hợp tác bảo đảm an ninh, an toàn thông tin mạng giữa các lực lượng này chưa thường xuyên chặt chẽ, thiếu tính chuyên nghiệp và tính hiện đại, thậm chí chưa đáp ứng yêu cầu bảo đảm an ninh, an toàn thông tin mạng trước sự phát triển mạnh mẽ, khó đoán định của cách mạng 4.0.

Năm là, *các nguồn lực, nhất là nguồn nhân lực bảo đảm an ninh, an toàn thông tin mạng đòi hỏi ngày càng cao theo hướng hiện đại*. Trong khi các nguồn lực bảo đảm an ninh, an toàn thông tin mạng đòi hỏi ngày càng cao theo hướng hiện đại, nhưng thực lực của các nguồn lực, nhất là nguồn nhân lực cũng như công nghệ, cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế còn hạn chế, bất cập. Thật vậy, cùng với sự phát triển với nhiều đột biến của cách mạng 4.0, thì tội phạm mạng sử dụng công nghệ cao cũng có xu hướng gia tăng với nhiều phương thức, thủ đoạn mới, tinh vi, nguy hiểm, làm ảnh hưởng trực tiếp đến nhiều lĩnh vực đời sống xã hội, gây khó khăn cho việc triển khai công tác bảo đảm an ninh, an

toàn thông tin mạng. Thực tế là, Việt Nam đang có những giới hạn về nguồn lực, nhất là nguồn nhân lực và cơ sở hạ tầng không gian mạng quốc gia, bao gồm hệ thống cơ sở vật chất, kỹ thuật để tạo lập, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên không gian mạng quốc gia chưa đáp ứng yêu cầu bảo đảm an ninh, an toàn thông tin mạng trong điều kiện hiện nay.

3.4. Một số giải pháp tăng cường bảo đảm an ninh, an toàn thông tin mạng

Sự phát triển nhanh của cách mạng 4.0 và thực tiễn phát triển của hệ thống thông tin tiếp tục đặt ra nhiều khó khăn, thách thức mới trong công tác bảo đảm an ninh, an toàn thông tin mạng, đặc biệt là hệ thống thông tin quan trọng quốc gia vì hệ thống thông tin này nếu bị xâm phạm, phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới quốc phòng, an ninh quốc gia. Để tăng cường bảo đảm an ninh, an toàn thông tin mạng, nhất là khả năng phòng, chống các nguy cơ tấn công, xâm nhập hệ thống công nghệ thông tin, bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin, đồng thời ngăn chặn, khắc phục kịp thời và hạn chế hậu quả từ các sự cố an ninh, an toàn thông tin mạng cần tiến hành một số giải pháp sau:

Thứ nhất, *quán triệt và tổ chức thực hiện có hiệu quả chủ trương, chính sách của Đảng, pháp luật của Nhà nước về bảo đảm an ninh, an toàn thông tin mạng*. Chủ trương, chính sách của Đảng, pháp luật của Nhà nước là định hướng chính trị và pháp lý để các chủ thể, trong đó có lực lượng chuyên trách thực hiện chức năng, nhiệm vụ bảo đảm an ninh, an toàn thông tin mạng. Trong đó có: Nghị quyết số 29-NQ/TW ngày 25/7/2018 về *Chiến lược bảo vệ Tổ quốc trên không gian mạng*; Nghị quyết số 30-NQ/TW ngày 25/7/2018 về *Chiến lược an ninh mạng quốc gia*; Nghị quyết số 52-NQ/TW ngày 27/9/2019 *Về một số chủ trương, chính sách chủ động tham gia cuộc cách mạng công nghiệp lần thứ tư*; Luật Cơ yếu số 05/2011/QH13; Luật An toàn thông tin mạng số 86/2015/QH13; Luật An ninh mạng số 24/2018/QH14; Luật Bảo vệ bí mật nhà nước số 29/2018/QH14… và các văn bản quy phạm pháp luật hướng dẫn thi hành về công tác bảo đảm an ninh, an toàn thông tin mạng.

Chỉ có trên cơ sở tiếp tục quán triệt sâu sắc và thực hiện nghiêm túc, có hiệu quả các văn bản trên đây không chỉ góp phần nâng cao nhận thức của các chủ thể trong hệ thống chính trị về vị trí, vai trò và tầm quan trọng của công tác bảo đảm an ninh, an toàn thông tin mạng cũng như tính chất nguy hiểm từ những âm mưu, hoạt động chống phá của các thế lực thù địch và các loại tội phạm trên không gian mạng, mà còn tạo nền tảng chính trị tinh thần để các chủ thể bảo đảm an ninh, an toàn thông tin mạng mới có thể vượt qua được những khó khăn, thách thức mới trong công tác quản lý an ninh, an toàn thông tin mạng. Trong đó, vấn đề cốt lõi là làm cho các chủ thể bảo đảm an ninh, an toàn thông tin mạng đều nhận thức sâu sắc rằng: Bảo đảm an ninh, an toàn thông tin mạng là góp phần bảo vệ chủ quyền quốc gia trên không gian mạng; Một bộ phận trọng yếu của cuộc đấu tranh bảo vệ an ninh quốc gia và giữ gìn trật tự, an toàn xã hội; Một nhiệm vụ chiến lược, cấp bách, thường xuyên, lâu dài của cả hệ thống chính trị và toàn dân dưới sự lãnh đạo của Đảng, sự quản lý tập trung của Nhà nước.

Thứ hai, *rà soát, bổ sung, hoàn thiện và ban hành mới văn bản quy phạm pháp luật về bảo đảm an ninh, an toàn thông tin mạng*. Việc rà soát, bổ sung, hoàn thiện và ban hành mới hệ thống văn bản quy phạm pháp luật về bảo đảm an ninh, an toàn thông tin mạng cần tiến hành theo hướng xác định rõ trách

nhiệm của các chủ thể trong bảo đảm an ninh, an toàn thông tin mạng. Thực tiễn công tác bảo đảm an ninh, an toàn thông tin mạng thời gian qua cho thấy, hệ thống văn bản quy phạm pháp luật về bảo đảm an ninh, an toàn thông tin mạng đã bộc lộ không ít hạn chế, bất cập, thiếu đồng bộ và hiệu lực thi hành chưa cao, chưa đáp ứng yêu cầu bảo đảm an ninh, an toàn thông tin mạng trong bối cảnh nền kinh tế thị trường định hướng xã hội chủ nghĩa và hội nhập quốc tế ngày càng sâu rộng. Theo đó là công tác quản lý nhà nước về bảo đảm an ninh, an toàn thông tin mạng còn sơ hở, chưa theo kịp tốc độ phát triển và ứng dụng công nghệ thông tin, đặc biệt là các thế lực thù địch và tội phạm mạng, nhất là tội phạm công nghệ cao, không ngừng gia tăng hoạt động chống phá. Trước bối cảnh tình hình như vậy, xuất phát từ mục tiêu, quan điểm chỉ đạo và định hướng của Đảng, Nhà nước về bảo đảm an ninh, an toàn thông tin mạng; để bổ sung, hoàn thiện cơ sở pháp lý về bảo đảm an ninh, an toàn thông tin mạng, nên việc tiếp tục rà soát, bổ sung, hoàn thiện và ban hành mới hệ thống văn bản quy phạm pháp luật về bảo đảm an ninh, an toàn thông tin mạng theo hướng vừa xác định rõ trách nhiệm của các chủ thể trong hệ thống chính trị; đồng thời quy định rõ các tiêu chuẩn, quy chuẩn an ninh, an toàn thông tin mạng và quy trình thẩm định phương án, biện pháp bảo vệ an ninh, an toàn thông tin mạng đối với các hệ thống thông tin quốc gia quan trọng, đặc biệt là hệ thống thông tin quan trọng về an ninh quốc gia là yêu cầu khách quan và cần thiết.

Thứ ba, *tăng cường năng lực, nâng cao hiệu quả quản lý nhà nước về bảo đảm an ninh, an toàn thông tin mạng theo hướng mở rộng hợp tác quốc tế***.** Theo đó, cần sớm kiện toàn tổ chức bộ máy chuyên trách quản lý nhà nước về an ninh, an toàn thông tin mạng quốc gia, đặc biệt là hệ thống đơn vị chuyên trách về bảo đảm an ninh, an toàn thông tin, công nghệ thông tin gắn với hiện thực hoá Nghị quyết số 18-NQ/TW Hội nghị Trung ương 6 khóa XII về *Một số vấn đề về tiếp tục đổi mới, sắp xếp tổ chức bộ máy của hệ thống chính trị tinh gọn, hoạt động hiệu lực, hiệu quả*. Bố trí cán bộ quản lý, cán bộ kỹ thuật phù hợp chịu trách nhiệm đảm bảo an ninh, an toàn thông tin mạng cho các hệ thống thông tin, nhất là hệ thống thông tin quan trọng quốc gia. Mặt khác, cần nâng cao năng lực hợp tác quốc tế trong phòng ngừa, phát hiện, đấu tranh có hiệu quả với mọi âm mưu, hoạt động phạm tội trên không gian mạng của các chủ thể mà nòng cốt là các chủ thể chủ quản hệ thống thông tin mạng bao gồm cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin. Kiện toàn tổ chức, bộ máy đảm bảo các điều kiện, nâng cao năng lực hợp tác quốc tế cho cơ quan chuyên trách về công nghệ thông tin và an ninh, an toàn thông tin mạng. Xử lý nghiêm mọi hành vi gây mất an ninh, an toàn thông tin mạng, làm lộ, lọt bí mật nhà nước.

Thứ tư, *xây dựng, hoàn thiện cơ chế phối hợp giữa Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông, Ban Tuyên giáo Trung ương và các bộ, ban, ngành, địa phương trong bảo đảm an ninh, an toàn thông tin mạng*. Tổ chức phổ biến, tập huấn để nâng cao nhận thức và năng lực bảo đảm an ninh, an toàn thông tin mạng cho các cơ quan, tổ chức, cá nhân, trước hết là cán bộ lãnh đạo, cán bộ chuyên trách quản lý và vận hành hệ thống thông tin quan trọng về an ninh quốc gia. Nghiên cứu xây dựng mô hình hợp tác công - tư trong bảo đảm an ninh, an toàn thông tin mạng, trong phòng, chống tội phạm trên không gian mạng ở Việt Nam, tạo cơ chế phối hợp chặt chẽ giữa các cơ quan

nhà nước với các tổ chức và doanh nghiệp nhằm khai thác tối đa nguồn lực xã hội nhằm bảo đảm an ninh, an toàn thông tin mạng. Tăng cường tuyên truyền, phổ biến, nâng cao nhận thức, cảnh giác của người dân trong phòng ngừa tội phạm và vi phạm pháp luật về an ninh, an toàn thông tin mạng.

Thứ năm*, đẩy mạnh phát triển nguồn nhân lực bảo đảm an ninh, an toàn thông tin mạng, nhất là lực lượng chuyên trách có số lượng đáp ứng yêu cầu, chất lượng ngày càng cao, cơ cấu phù hợp*. Đảng, Nhà nước Việt Nam luôn khẳng định con người là trung tâm của sự phát triển, của công cuộc xây dựng và bảo vệ Tổ quốc; Phát triển nguồn nhân lực là một trong ba khâu đột phá làm nền tảng phát triển bền vững và tăng lợi thế cạnh tranh quốc gia; Phát triển nguồn nhân lực là then chốt để bảo đảm an ninh, an toàn thông tin mạng. Vì vậy, để phát triển nguồn nhân lực an ninh, an toàn thông tin mạng, cần căn cứ vào Quyết định số 146/QĐ-TTg ngày 28/01/2022 của Thủ tướng Chính phủ Phê duyệt Đề án "*Nâng cao nhận thức, phổ cập kỹ năng và phát triển nguồn nhân lực chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030*" gắn với hiện thực hóa Nghị quyết số 36-NQ/TW ngày 01/7/2014 của Bộ Chính trị về *Đẩy mạnh ứng dụng, phát triển công nghệ thông tin đáp ứng yêu cầu phát triển bền vững và hội nhập quốc tế*, trong đó có mục tiêu phát triển nguồn nhân lực công nghệ thông tin đạt chuẩn quốc tế, bảo đảm đáp ứng nhu cầu trong nước về số lượng và chất lượng, có khả năng cung cấp nguồn nhân lực công nghệ thông tin chất lượng cao. Việc phát triển nguồn nhân lực an ninh, an toàn thông tin mạng phải có tầm nhìn chiến lược phát triển tổng thể và dài hạn; đồng thời, trong mỗi thời kỳ nhất định, cần xây dựng những định hướng cụ thể, để từ đó đánh giá thời cơ, thách thức, những khó khăn, hạn chế và nguyên nhân… để đề ra mục tiêu và giải pháp phát triển nguồn nhân lực này cho thích hợp với giai đoạn đó, phù hợp với bối cảnh kinh tế, xã hội trong nước và quốc tế. Về ngắn hạn, cần lập kế hoạch đào tạo bồi dưỡng nghiệp vụ cho đội ngũ chuyên trách về an ninh, an toàn thông tin mạng; đồng thời đào tạo, phổ biến kiến thức, kỹ năng cho người sử dụng mạng và không gian mạng về phòng, chống các nguy cơ mất an ninh, an toàn thông tin mạng khi sử dụng mạng internet hay kết nối di động.

Thứ sáu, *áp dụng các giải pháp đảm bảo an ninh, an toàn thông tin mạng, chống virus và mã độc hại cho các hệ thống thông tin và các máy tính cá nhân có kết nối mạng internet.* Đối với các hệ thống thông tin quan trọng, nhất là hệ thống thông tin quan trọng quốc gia, các cổng thông tin điện tử, hay các trang thông tin điện tử quan trọng khác phải áp dụng chính sách ghi lưu tập trung biên bản hoạt động cần thiết để phục vụ công tác điều tra và khắc phục sự cố mạng với thời hạn lưu giữ theo hướng dẫn của Bộ Thông tin và Truyền thông, nhưng tối thiểu không ít hơn 3 tháng. Các cơ quan, đơn vị có trang thông tin điện tử, cổng thông tin điện tử phải thực hiện chế độ trực thường xuyên theo dõi hoạt động của trang thông tin điện tử, cổng thông tin điện tử, phát hiện kịp thời và có giải pháp xử lý khi bị thay đổi thông tin, bị đăng tải thông tin lạ. Tổ chức quản lý chặt chẽ các tài khoản của các hệ thống thông tin, thường xuyên tổ chức kiểm tra các tài khoản của hệ thống thông tin nhằm tránh tình trạng truy cập trái phép vào hệ thống.

4. KẾT LUẬN

Thực tiễn an ninh, an toàn thông tin mạng ở Việt Nam thời gian qua đang đặt ra một số vấn đề cần sớm giải quyết. Để bảo đảm an ninh, an toàn thông tin mạng, nhất là hệ thống thông tin trọng

yếu về quốc phòng, an ninh cần tiến hành đồng bộ, đồng thời, có trọng tâm, trọng điểm 6 giải pháp sau: *i) Quán triệt và tổ chức thực hiện* có hiệu quả chủ trương, chính sách của Đảng, pháp luật của Nhà nước về bảo đảm an ninh, an toàn thông tin mạng; *ii) Rà soát, bổ sung, hoàn thiện* và ban hành mới văn bản quy phạm pháp luật về bảo đảm an ninh, an toàn thông tin mạng; *iii) Tăng cường năng lực*, nâng cao hiệu quả quản lý nhà nước về bảo đảm an ninh, an toàn thông tin mạng theo hướng mở rộng hợp tác quốc tế; *iv) Xây dựng, hoàn thiện* cơ chế phối hợp giữa Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông, Ban Tuyên giáo Trung ương và các bộ, ban, ngành, địa phương trong bảo đảm an ninh, an toàn thông tin mạng; *v) Đẩy mạnh phát triển* nguồn nhân lực bảo đảm an ninh, an toàn thông tin mạng, nhất là lực lượng chuyên trách có số lượng đáp ứng yêu cầu, chất lượng ngày càng cao, cơ cấu phù hợp; *vi) Áp dụng* các giải pháp đảm bảo an ninh, an toàn thông tin mạng, chống virus và mã độc hại cho các hệ thống thông tin và các máy tính cá nhân có kết nối mạng internet. Đó không chỉ là nhiệm vụ của lực lượng chuyên trách, mà còn là trách nhiệm của các cơ quan, tổ chức, cá nhân trong hệ thống chính trị Việt Nam và các tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến bảo đảm an toàn, an ninh mạng tại Việt Nam.

TÀI LIỆU TRÍCH DẪN

[1]. Ban chấp hành Trung ương (2022), *Nghị quyết số 29-NQ/TW ngày 17/11/2022 Hội nghị 6 khóa XIII về tiếp tục đẩy mạnh công nghiệp hóa, hiện đại hóa đất nước đến năm 2030, tầm nhìn đến năm 2045*.

[2]. Thủ tướng Chính phủ (2022), *Chỉ thị số 18/CT-TTg ngày 13/10/2022 Về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam*.

[3]. Thu Thanh (2021), *Bảo đảm chủ quyền quốc gia trên không gian mạng*, Tạp chí Cộng sản, số tháng 12/2021.

[4]. Lê Văn Thắng (2019), *An ninh thông tin của Việt Nam trong điều kiện hiện nay: Thực trạng, vấn đề đặt ra và giải pháp*, Đề tài khoa học cấp Nhà nước, Hà Nội.

[5]. Bộ Công an (2018), Báo cáo số 403/BC-A68-P1 ngày 13/3/2018: *Báo cáo sơ kết 04 năm thực hiện Chỉ thị số 28-CT/TW của Ban bí thư về tăng cường công tác bảo đảm an ninh, an toàn thông tin mạng trong tình hình mới*.

[6]. Thủ tướng Chính phủ (2019), Chỉ thị số 14/CT-TTg ngày 07/6/2019 *Về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam*.

[7]. Tô Lâm (2020), *Bảo đảm an ninh mạng trong tình hình mới*, Tạp chí Cộng sản, số tháng 08/2020.

[8]. PV (2022), *10 sự kiện nổi bật trong lĩnh vực bảo mật và an toàn thông tin năm 2021 tại Việt Nam*, Tạp chí An toàn thông tin, số tháng 01/2022.

[9]. Nguyễn Ngọc Cương (2022), *Tình hình an ninh mạng và xu hướng tội phạm mạng tại Việt Nam giai đoạn 2022-2023*, Tạp chí An toàn thông tin, số tháng 10/2022.

[10].T.Đào (2023), *Lừa đảo trực tuyến tăng gần 65% trong 6 tháng đầu năm*, Kinh tế Sài Gòn Online, https://thesaigontimes.vn/lua-dao-truc-tuyen-tang-gan-65-trong-6-thang-dau-nam/, ngày 12/07/2023./.