Vấn đề an ninh mạng tại các cơ quan báo mạng điện tử ở Việt Nam hiện nay

PGS, TS. PHẠM THỊ THANH TỊNH
Học viện Báo chí và Tuyên truyền; Email: thanhtinh.ajc@gmail.com

Nhận ngày 2 tháng 8 năm 2023; chấp nhận đăng tháng 9 năm 2023.

Tóm tắt: *Đối với báo chí trong thời đại số, đi cùng với cơ hội phát triển cũng có nhiều nguy cơ, thách thức xảy ra, một trong số đó là nguy cơ đối với vấn đề an ninh mạng. An ninh mạng ở cơ quan báo mạng điện tử là sự bảo vệ thông tin và hệ thống thông tin 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. Các cơ quan báo chí là phương tiện quản lý của Đảng và Nhà nước sẽ là mục tiêu mà các thế lực thù địch thực hiện các hành vi tấn công mạng nhằm phá hoại hệ thống, lấy cắp dữ liệu, thay đổi nội dung, giao diện. Do vậy, công tác bảo đảm an mạng là hoạt động hết sức quan trọng và cần được triển khai một cách đồng bộ và toàn diện.*
Từ khóa: *an ninh mạng, an ninh thông tin, tấn công mạng, không gian mạng.*

Abstract: *In the digital age, electronic news agencies face both opportunities and challenges, including the risk of cybersecurity threats. Ensuring cybersecurity in electronic news agencies involves protecting information and information systems against unauthorized access, use, disclosure, disruption, modification, or destruction to maintain the integrity, confidentiality, and availability of information. Cyber adversaries target news agencies, attempting to undermine their systems, steal data, manipulate content, or disrupt operations. Thus, ensuring cybersecurity is of utmost importance and needs to be implemented comprehensively and consistently.*
Keywords: *Cybersecurity, information security, cyberattacks, cyberspace.*

Cuộc tấn công mạng xảy ra khi có sự truy cập trái phép vào hệ thống máy tính có kết nối của một tổ chức khiến cho các dữ liệu bảo mật bị đánh cắp, xoá, thay đổi. Tội phạm công nghệ cao khi tấn công mạng và các tổ chức khác thường sử dụng nhiều phương thức, thủ đoạn khác nhau và luôn thay đổi các hình thức công nghệ mới. Các sự kiện tấn công mạng diễn ra khắp nơi trên thế giới cũng như ở Việt Nam, trên mọi lĩnh vực trong đó có lĩnh vực báo chí- nơi rất chú trọng đến các vấn đề an ninh mạng. Do vậy, cũng như bảo mật tài sản vật lý, các cơ quan báo chí cần vận dụng và nâng cấp các biện pháp an ninh mạng, bắt kịp những công nghệ và công cụ tấn công kỹ thuật số mới và không ngừng biến hóa nhằm bảo mật tài sản kỹ thuật số và bảo vệ hệ thống không bị truy cập ngoài ý muốn.

Theo khoản 1 Điều 2 Luật An ninh mạng 2018 định nghĩa an ninh mạng như sau:

"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"[1].

Theo trang Web Amazon.com "An ninh mạng là phương pháp bảo vệ an toàn cho máy tính, mạng, ứng dụng phần mềm, hệ thống quan trọng và dữ liệu khỏi các mối đe dọa kỹ thuật số tiềm ẩn. Các tổ chức chịu trách nhiệm bảo mật dữ liệu để duy trì lòng tin của khách hàng cũng như đáp ứng việc tuân thủ quy định. Họ sử dụng các biện pháp và công cụ an ninh mạng để bảo vệ dữ liệu nhạy

cảm khỏi bị truy cập trái phép cũng như ngăn chặn gián đoạn trong hoạt động kinh doanh gây ra bởi hoạt động mạng ngoài ý muốn. Các tổ chức triển khai an ninh mạng bằng cách hợp lý hóa công tác phòng vệ kỹ thuật số giữa con người, quy trình và công nghệ[2].

An ninh mạng trên báo mạng điện tử là các hoạt động bảo vệ các dữ liệu trên không gian mạng đảm bảo ngăn ngừa sự xâm phạm nhằm thay đổi, bổ sung nội dung, giao diện trên các trang báo mạng điện tử.

Thực trạng an ninh mạng tại các cơ quan báo mạng điện tử hiện nay

Hiện nay, các cơ quan báo chí ở nước ta đã ứng dụng nhiều thành tựu công nghệ và đang trong quá trình chuyển đổi số mạnh mẽ, tuy nhiên công tác đảm bảo an ninh và khả năng đảm bảo trên môi trường số đang có nhiều hạn chế. Cho nên nhiều cơ quan báo chí đã bị mất an ninh thông tin trên không gian mạng. *Theo thống kê năm 2020, đã có 156 cuộc tấn công của 8 nhóm tin tặc nhằm vào các tổ chức tại Việt Nam, trong đó mục tiêu đối tượng là các cơ quan báo chí và truyền thông, chiếm 21% số cuộc tấn công. Thực tế kiểm tra tại một cơ quan báo chí quan trọng của Nhà nước, kết quả cho thấy tại hầu hết các cơ quan báo chí, truyền thông, công tác bảo đảm an toàn thông tin vẫn chưa theo kịp được tốc độ chuyển đổi số, từ đó tồn tại nhiều nguy cơ bị tin tặc tấn công. Việc quản lý kết nối máy tính cá nhân, máy tính nghiệp vụ chưa chặt chẽ. Các máy tính cá nhân có thể kết nối vào hệ thống mạng nội bộ của cơ quan sau đó kết nối vào Internet và ngược lại. Sử dụng USB không an toàn. Số lượng máy tính cá nhân nhiễm mã độc chiếm khoảng 7.5%. Số lượng máy tính sử dụng phần mềm crack bản quyền chiếm hơn 24%. Khoảng 3.5% số máy có truy vấn đến tên miền độc hại hoặc các máy chủ điều khiển từ xa. Các máy chủ dịch vụ không được cập nhật thường xuyên, có gần 90% số máy chủ có lỗ hổng bảo mật, trong đó có những lỗ hổng bảo mật nghiêm trọng cho phép hacker leo thang đặc quyền và chiếm quyền điều khiển hệ thống*[3].

Sản phẩm báo chí là công cụ truyền bá thông tin cho một tổ chức, chính phủ nhằm mục tiêu quản lý xã hội của mỗi quốc gia. Nếu một cơ quan báo chí bị tin tặc tấn công sẽ dẫn đến tốc độ truy cập bị chậm hoặc toàn bộ cơ sở dữ liệu sẽ bị đánh cắp, nội dung trên trang báo bị thay đổi Các dữ liệu khi bị đánh cắp sẽ bị lợi dụng để khai thác bóp mép sự thật hoặc vào các mục đích đen tối khác dẫn đến sự mất niềm tin của công chúng, nếu là những thông tin bị thay đổi, chỉnh sửa theo hướng sai lệch theo đường lối chính sách của Đảng và Nhà nước thì dư luận xã hội bị đảo lộn, tác động xấu tới sự phát triển mọi mặt của quốc gia.

Thực tế một số báo mạng điện tử ở nước ta như *VietnamNet*, *VOV, Pháp luật TP.HCM, Sài Gòn giải phóng, Thanh Niên* đã bị hacker tấn công có chủ đích, gây gián đoạn truy cập.

Trường hợp mất an ninh mạng trên quy mô lớn với báo mạng điện tử nước ta xảy ra ở báo VietnamNet. Các đối tượng đã sử dụng cách thức tấn công DDos - tức là cho một lượng lớn truy cập ồ ạt cùng một thời điểm, làm tràn băng thông, khiến người đọc không thể truy cập vào trang web. Các máy tính này đã đồng loạt thực hiện truy cập vào tên miền Vietnamnet.vn dẫn đến hiện tượng đường truyền mạng bị quá tải. Vào thời điểm này khi độc giả truy cập vào báo VietNamNet bị báo lỗi không tìm thấy máy chủ. Hậu quả là hàng chục ngàn máy tính bị nhiễm virus và chiếm quyền điều khiển.

Ngày 12/6/2021, Báo điện tử VOV (Đài Tiếng nói Việt Nam) đăng tải hai bài viết liên quan đến bà Nguyễn Phương Hằng (vợ ông Huỳnh Uy Dũng, chủ khu du lịch Đại Nam) gồm: Bà Phương Hằng với các livestream lệch chuẩn: Đã đến lúc cần xử lý nghiêm và Không thể cho mình quyền xúc phạm bất kỳ ai trên mạng. Loạt bài viết đăng tải ý kiến khách quan của các chuyên gia là chính khách, luật sư, nhà báo... và không quy chụp hay phán xét chủ quan từ tòa soạn[4]. Tuy nhiên, sau khi loạt bài viết được đăng tải, một số đối tượng đã có hành vi kích động, tạo các tài khoản ảo để tấn công nhiều nền tảng của Báo Điện tử VOV.

Ngày 13/6/2021, hệ thống mạng của báo này đã bị tin tặc tấn công với hình thức DDos, đây phương thức tấn công mà các hacker hay sử dụng, và đã ra

gây hậu quả làm sụp đổ cả một hệ thống máy chủ trực tuyến. Một tài khoản đã tìm được một lỗ hổng nghiêm trọng từ trang quản trị admin của VOV, qua đó truy cập toàn bộ tên đăng nhập theo mật khẩu nội bộ của VOV. Ngoài ra trang web, fanpage, hệ thống quản trị nội dung, Google Map... của báo VOV cũng đồng loạt bị tấn công.

Trường hợp tấn công mạng đối với báo *Pháp luật TP.HCM* vào sáng 15/6/2021, Báo có bài phân tích và lên án vụ tấn công VOV. Đến 15h cùng ngày bộ phận kỹ thuật báo có dấu hiệu Báo bị tấn công bằng DDos, mạng chập chờn, website xảy ra tình trạng không truy cập được, các đánh giá 1 sao bắt đầu xuất hiện trên Google Map dù bộ phận kỹ thuật đã tắt trên hệ thống Google. Cuộc tấn công chính thức được chia làm 3 đợt.

Từ 15:50 tới 17:20 cùng ngày: Báo bị mất truy cập hoàn toàn, những lúc khác rất chập chờn và chức năng hiển thị trang bìa của PLO bị ảnh hưởng (bài chỉ hiển thị lên trang trong); từ 17:35 tới 18:20: Có lúc mất truy cập hoàn toàn, tuy nhiên đã có sự chống đỡ và tắt các chức năng API của website nên xử lý việc mất truy cập nhanh hơn và không ảnh hưởng nhiều tới việc gián đoạn ở lần này. Dù vậy, hệ thống vẫn có đôi lúc chậm khiến tình trạng hiển thị từ khi xuất bản bản tin lên website hiển thị chậm đi; từ 18:25 tới 19:10: Cường độ tấn công khá dồn dập, truy dấu vết cho thấy hacker tấn công từ nhiều máy chủ ở nước ngoài liên tục ra các yêu cầu truy cập vượt quá khả năng đáp ứng của băng thông. Cuộc tấn công yếu dần rồi dừng hẳn sau 22:00.

Điều này cũng cho thấy nguy cơ rủi ro, mất an toàn an ninh, bị tấn công là rất lớn trên môi trường mạng, đặc biệt là với những trang báo điện tử có lượng người dùng lớn. Như vậy, không chỉ cơ sở dữ liệu máy tính của tổ chức, doanh nghiệp bị tấn công để đánh cắp thông tin khách hàng mà các cơ quan báo chí cũng là đối tượng mà các hacker hướng tới xâm nhập với các chủ đích khác nhau. Do vậy, mỗi cơ quan báo chí hoạt động trên môi trường số cần có các giải pháp bảo đảm an ninh mạng để kẻ xấu không thể đánh cắp, thao túng thông tin trên các web của mình.

Một số giải pháp đảm bảo an ninh mạng tại cơ quan báo mạng điện tử ở Việt Nam hiện nay

Theo Cục An toàn thông tin (Bộ Thông tin và Truyền Thông) khi xảy ra sự cố tấn công mạng, các cơ quan báo chí cần thực hiện theo quy trình gồm 5 bước: Phát hiện, báo cáo sự cố; xác định hình thức tấn công, mức độ khẩn cấp; ứng cứu sự cố, khôi phục hệ thống; điều phối, ứng cứu sự cố; kết thúc xử lý sự cố, với thời gian cụ thể cho mỗi bước. Tại mỗi bước đều có hướng dẫn cụ thể rõ ràng về nhiệm vụ của đơn vị vận hành (doanh nghiệp, tổ chức được cơ quan báo chí giao nhiệm vụ vận hành hệ thống thông tin bị tấn công mạng), bộ phận ứng cứu sự cố tại chỗ (bộ phận do cơ quan báo chí - chủ quản hệ thống thông tin thành lập và giao nhiệm vụ ứng cứu, xử lý sự cố tấn công mạng) và Cục An toàn thông tin[5].

Theo lãnh đạo một cơ quan báo chí, khi bị tấn công cơ quan cần có một số cách ứng phó ngay lập tức như báo với nhà cung cấp để bảo đảm băng thông, báo với Bộ TT&TT để phối hợp hỗ trợ khi xảy ra sự cố; rà soát các lỗ hổng bảo mật; tắt một số tính năng trên mạng xã hội, tắt bình luận là những công cụ có thể bị lợi dụng tấn công, tăng cường thêm đội ngũ nhân sự kỹ thuật để phối hợp với các bên liên quan bảo vệ hệ thống[6].

Theo trang vneconomy.vn cách chống tấn công mạng bằng DDos trên các website là: Đầu tư vào phần cứng mạng tốt; thuê một dịch vụ giảm thiểu được Ddos; loại bỏ lỗ hổng trang web; sử dụng tường lửa ứng dụng web và CDN (mạng phân phối nội dung có thể cân bằng lưu lượng trên trang web); tăng dung lượng băng thông Internet và dung lượng server; liên tục sao lưu website để có thể khôi phục lại sau khi bị tấn công. Ngoài ra, không được bỏ qua bất kỳ request nào đáng ngờ được gửi cho website[7].

Hiện nay các cơ quan báo chí đã rất quan tâm đến nội dung và hình thức thông tin để chuyển đến cho công chúng. Tuy nhiên các vấn đề phát sinh mới trong quá trình phát triển cũng cần được chú trọng, đặc biệt trong thời đại kỹ thuật số hiện nay việc đảm bảo an ninh thông tin trên môi trường số là một nhiệm vụ quan trọng. Do đó, cần có những

giải pháp triển khai đồng bộ từ cán bộ lãnh đạo cấp trên, lãnh đạo cơ quan báo chí, người trực tiếp làm báo và công chúng tiếp nhận.

Tăng cường sự lãnh đạo của Đảng, nâng cao hiệu quả quản lý nhà nước về an ninh thông tin mạng.

An ninh thông tin là một nội dung của an ninh quốc gia, do vậy hoàn thiện môi trường pháp lý cho việc chia sẻ dữ liệu số xuyên biên giới an toàn, tin cậy là điều rất cần thiết trong điều kiện hiện nay. Cần hơn nữa vai trò lãnh đạo của Đảng và Nhà nước trong việc tiếp tục nghiên cứu xây dựng và hoàn thiện luật về chống thông tin giả, thông tin xấu, độc hại; chặn lọc thông tin xuyên tạc, sai sự thật trên không gian mạng; xây dựng bộ quy tắc ứng xử trên không gian mạng.

Chính phủ cần tăng cường đầu tư cơ sở hạ tầng hiện đại, băng thông đủ rộng để vượt qua các cuộc tấn công gây nghẽn mạng, có hệ thống máy lưu trữ dự phòng để chuyển hướng dữ liệu trước các cuộc tấn công và phục hồi sau tấn công mạng; Xây dựng, triển khai thực hiện các giải pháp kỹ thuật chuyên biệt nhằm kiểm tra, phát hiện các nguy cơ gây mất an ninh thông tin. Tổ chức diễn tập hàng năm về phòng, chống tấn công mạng cấp quốc gia với sự tham gia của các bộ, ban ngành và các cơ quan báo chí

Nhà nước cần tập trung nguồn lực để xây dựng công nghiệp an ninh thông tin, kết hợp cả trong lĩnh vực dân sự với bảo đảm an ninh, quốc phòng; đối tác công tư; cần có cơ chế khuyến khích nghiên cứu, phát triển, sử dụng các phần mềm, dịch vụ thông tin riêng của Việt Nam, đáp ứng yêu cầu bảo mật thông tin, sự an toàn của bí mật nhà nước, giám sát an ninh mạng; khuyến khích, hình thành các doanh nghiệp có năng lực tự sản xuất, cung cấp dịch vụ, các trang thiết bị, giải pháp gắn với bảo vệ an ninh mạng, tăng tỷ lệ nội địa hóa các sản phẩm công nghệ thông tin.

Nâng cao nhận thức vấn đề an ninh mạng đối với người làm báo và công chúng

Trước hết, nâng cao nhận thức của đội ngũ lãnh đạo, quản lý về vấn đề an ninh mạng tại các cơ quan báo mạng điện tử. Đây là điều kiện tiên quyết đối với việc đảm bảo an ninh mạng, cụ thể cần thực hiện tốt: quán triệt và triển khai thực hiện nghiêm túc các chỉ thị, nghị quyết của Đảng, Nhà nước, Bộ TT&TT về công tác báo chí; thường xuyên đổi mới nội dung, hình thức, phương pháp tuyên truyền, giáo dục; lãnh đạo, các cơ quan báo chí cần nâng cao năng lực lãnh đạo, chỉ đạo tập trung, thống nhất trong thực hiện công tác bảo đảm an ninh mạng tại cơ quan báo mạng điện tử, điều này góp phần giúp các chủ thể nhận thức rõ vị trí, ý nghĩa tầm quan trọng của công tác an ninh mạng tại cơ quan báo mạng điện tử

An ninh quốc gia là lợi ích quốc gia trên không gian mạng nhằm đảm bảo sự an toàn, vững mạnh của một đất nước do vậy cần sử dụng đồng bộ các biện pháp toàn diện. Pháp luật cần xử lý nghiêm khắc các trường hợp tiếp tay cho các hành vi tấn công mạng trên mọi lĩnh vực. Phối hợp đồng bộ giữa các cơ quan có liên quan để hỗ trợ và bảo vệ an toàn an ninh mạng cho các cơ quan báo chí, bảo vệ an toàn cho những người làm báo chân chính. Nâng cao nhận thức của mọi tầng lớp nhân dân, tạo dựng một môi trường an toàn, lành mạnh giúp các cơ quan báo chí thực hiện tốt nhiệm vụ, chức năng của mình trong điều kiện hiện nay là điều cần thiết.

Khoa học, công nghệ luôn phát triển, các hacker thường ứng dụng công nghệ mới một cách tinh vi nhằm qua được kẽ hở về an ninh mạng của các tổ chức. Do đó, các cơ quan báo mạng điện tử cần tổ chức chuyên mục riêng về an ninh mạng trên báo; thường xuyên có những lớp đào tạo, giáo dục, bồi dưỡng, nâng cao ý thức của người làm báo, huấn luyện những người làm báo chuyên trách các kỹ năng phòng chống tấn công mạng. Điều này sẽ giúp cho thông tin trên báo chí tuyên truyền đúng hướng, giảm thiểu sự việc các trang báo bị tấn công mạng. Qua quá trình tiếp nhận thông tin đúng hướng, công chúng sẽ có sự lựa chọn đúng đắn trong quá trình lựa chọn thông tin, có khả năng ứng xử với những thông tin độc hại, tin giả, biết nhận diện phân biệt các trang web để tiếp nhận thông tin hàng ngày. Từ đó, sẽ nâng cao ý thức, bản lĩnh chính trị của mỗi người trước sự biến động trên thị trường tin tức hiện nay.

Đối với công nghệ bảo vệ an ninh mạng tại cơ quan báo mạng điện tử

Để vấn đề bảo mật được tốt, điều cần thiết là các cơ quan báo chí thiết lập các hệ thống mạng mạng nội bộ và sử dụng các biện pháp trao đổi dữ liệu an toàn qua CDROM, các hệ thống truyền 1 chiều...

Các máy tính, Laptop của cán bộ, phóng viên cần được cài đặt đầy đủ các phần mềm diệt vi-rút có bản quyền, cập nhật đầy đủ. Các tài liệu quan trọng có thể tạm sử dụng mã hóa bằng mật khẩu và gửi mật khẩu qua tin nhắn SMS, không nên lạm dụng gửi qua các hệ thống email Thường xuyên cập nhật hệ thống, bảo đảm vá các lỗ hổng bảo mật kịp thời, không để tin tặc khai thác. Hạn chế sử dụng các thiết bị lưu trữ ngoài. Khi cần thiết phải sử dụng ổ đĩa CD/DVD để sao lưu dữ liệu, nếu sử dụng USB thường sẽ có nhiều mã động tự động lây lan trong hệ thống mạng.

Các cơ quan báo mạng điện tử cần triển khai các giải pháp giám sát mạng tập trung để phát hiện và đưa ra cảnh báo về nguy cơ mất an toàn thông tin sớm nhất. Để thực hiện các yêu cầu trên không thể thiếu đội ngũ chuyên gia bảo mật để bảo vệ phần mềm và hệ thống an ninh mạng của cơ quan báo chí.

Ngoài ra để thực hiện tốt vấn đề an ninh mạng, cơ quan báo mạng điện tử cần thực hiện tốt một số nội dung: nghiên cứu lại tổng thể nhiệm vụ các phòng, ban trong toàn bộ các tờ báo mạng điện tử, xác định vị trí, tầm quan trọng của các thông điệp về bảo vệ an ninh quốc gia và vai trò, thẩm quyền rõ ràng của từng bộ phận tham gia; coi trọng công tác tuyển chọn nhân lực đầu vào có sự chuẩn hóa ngay đối với những kỹ năng chuyên môn định hướng tới; thường xuyên tập huấn, nâng cao trình độ tổ chức sản xuất cho đội ngũ phóng viên, biên tập viên, đặc biệt là tại các cơ sở đào tạo báo chí truyền thông chuyên nghiệp; đổi mới quy trình tổ chức sản xuất hiện tại, ban hành văn bản chuẩn hóa quy trình.

Thời gian quan, nước ta đã áp dụng kỹ thuật, công nghệ số trên mọi lĩnh vực, bước đầu đã có những thành công nhất định. Hệ thống thông tin đã có sự phát triển mạnh mẽ phục vụ cho sự phát triển trên mọi lĩnh vực, đặc biệt là giúp cho sự lãnh đạo của Đảng, quản lý của Nhà nước trong quá trình thông tin tuyên truyền đến với người dân, đảm bảo an ninh cho đất nước. Tuy nhiên, các thế lực thù địch luôn tìm cách phá hoại chúng ta, trong lĩnh vực thông tin, chúng cố tính bôi xấu, phát tán thông tin độc hại nhằm tạo dư luận gây ảnh hưởng đến hệ thống chính sách, pháp luật của Việt Nam. Chúng luôn rình rập tấn công mạng vào hệ thống thông tin quan trọng về an ninh quốc gia. Nguy cơ mất an ninh mạng trên các trang báo hay website điện tử có thể xảy ra bất kỳ lúc nào. Bên cạnh sự đối mặt với việc tấn công vào cơ sở hạ tầng dữ liệu, nguy cơ lớn nhất đối với các cơ quan báo mạng điện tử là nội dung thông tin tuyên truyền trong không gian mạng bị thay đổi, xóa bỏ, trang web bị đánh sập không hoạt động được. Do đó, các cơ quan báo chí cần trang bị tốt hệ thống an ninh mạng, chủ động các phương án, hệ thống kỹ thuật và lên kế hoạch ứng phó kịp thời khi có các vụ tấn công mạng xảy ra.

Sự phát triển của công nghệ, quá trình chuyển đổi số diễn ra nhanh chóng, thông tin dần trở thành yếu tố trung tâm của sự phát triển. Các tổ chức báo chí và truyền thông đang trở thành những mục tiêu tấn công chủ yếu của tội phạm mạng, nên việc tăng cường bảo đảm an ninh mạng cho các cơ quan báo chí là hết sức cần thiết trong điều kiện hiện nay./.

(1) https://thuvienphapluat.vn/phap-luat/an-ninh-mang-la-gi-nguyen-tac-bao-ve-an-ninh-mang-dua-tren-nguyen-tac-nao-bao-ve-an-ninh-mang-bao-g-668970-4933.html

(2) https://aws.amazon.com/vi/what-is/cybersecurity/

(3) https://dangcongsan.vn/bao-ve-nen-tang-tu-tuong-cua-dang/tang-cuong-cac-giai-phap-cong-nghe-trong-viec-bao-dam-an-ninh-an-toan-thong-tin-cho-he-thong-bao-chi-596842.html

(4) https://vietnamnet.vn/bo-cong-an-dang-dieu-tra-nhom-doi-tuong-tan-cong-mang-bao-dien-tu-vov-745709.html#inner-article

(5) https://laodong.vn/xa-hoi/5-buoc-can-thuc-hien-khi-co-quan-bao-chi-bi-tan-cong-mang-925124.ldo

(6) https://vietnamnet.vn/bao-dien-tu-bi-tan-cong-se-duoc-khan-cap-ung-cuu-746453.html

(7) https://vneconomy.vn/them-nhieu-bao-dien-tu-bi-tan-cong-tu-choi-dich-vu-truy-cap-bi-gian-doan.htm.