An ninh mạng và truyền thông an ninh mạng: Tổng quan nghiên cứu quốc tế và tiếp cận liên ngành tại Việt Nam

Cybersecurity and cybersecurity communication: A review of international research and an interdisciplinary approach in Vietnam

ThS. TRẦN XUÂN QUỲNH
Học viện Phụ nữ Việt Nam; Email: xuanquynh@vwa.edu.vn

Ngày nhận bài: 26/02/2026 Ngày phản biện: 27/02/2026 Ngày duyệt đăng: 20/3/2026
Chủ đề của bài viết thuộc lĩnh vực: Báo chí, truyền thông

Tóm tắt: *Bài viết hệ thống các nghiên cứu quốc tế và trong nước về an ninh mạng nhằm làm rõ các xu hướng nghiên cứu về an ninh mạng và truyền thông an ninh mạng. Kết quả nghiên cứu các công trình quốc tế chỉ ra sự chuyển dịch từ tiếp cận kỹ thuật/quân sự sang tiếp cận lấy con người và tâm lý hành vi trên không gian mạng làm trung tâm, trong khi đó, các nghiên cứu tại Việt Nam hiện vẫn tập trung trọng tâm vào bình diện pháp lý và quản trị nhà nước. Điều này thúc đẩy tác giả đưa ra các hướng tiếp cận liên ngành thiết yếu kết nối giữa quản trị nhà nước và hành vi người dùng, góp phần xây dựng chiến lược an ninh mạng quốc gia toàn diện.*
Từ khóa: *An ninh mạng; truyền thông an ninh mạng; hành vi người dùng; quản trị nhà nước; tiếp cận liên ngành.*

Abstract: *This article systematizes both international and domestic studies on cybersecurity to clarify major research trends in cybersecurity and cybersecurity communication. The findings indicate a shift in international research from technical and military approaches to human-centered perspectives focusing on user behavior and psychology in cyberspace, whereas studies in Vietnam remain primarily focused on legal frameworks and state governance. This gap motivates the author to propose essential interdisciplinary approaches that connect state governance with user behavior, contributing to the development of a comprehensive national cybersecurity strategy.*
Keywords: *Cybersecurity; cybersecurity communication; user behavior; state governance; interdisciplinary approach.*

1. Đặt vấn đề

Trên thế giới, nghiên cứu về an ninh mạng đã phát triển trong hai thập niên qua với sự tham gia của như an ninh học, luật học, khoa học máy tính, truyền thông và tâm lý học. Tại Việt Nam, hội nhập quốc tế và chuyển đổi số, an ninh mạng ngày càng thu hút sự quan tâm của giới nghiên cứu và hoạch định chính sách, sau khi Luật An ninh mạng năm 2018 được ban hành và Luật An ninh mạng năm 2025 (số 116/2025/QH15) được thông qua. Tuy nhiên, các công trình nghiên cứu phân tán, thiếu hệ thống và chưa làm rõ đầy đủ vai trò của truyền thông yếu tố con người trong bảo đảm an ninh mạng. Xuất phát từ thực tiễn đó, bài viết tiến hành điểm luận các công trình tiêu biểu về an ninh mạng và truyền thông an ninh mạng ở cả bình diện quốc tế và trong nước, nhằm xác định các khoảng trống nghiên cứu và gợi mở hướng tiếp cận liên ngành cho nghiên cứu an ninh mạng tại Việt Nam trong thời gian tới.

2. Phương pháp nghiên cứu

Bài báo sử dụng phương pháp tổng quan tài liệu, tài liệu được thu thập từ các cơ sở dữ liệu khoa học quốc tế (Web of Science, Scopus, Google Scholar, ITU…) và trong nước (V-CitationGate, tạp chí chuyên ngành…), giai đoạn 2009 - 2025 nhằm đảm bảo tính cập nhật. Các công trình được phân tích, phân loại theo các hướng tiếp cận chủ đạo ở trong và ngoài nước, đồng thời so sánh để nhận diện sự tương đồng, khác biệt và các khoảng trống nghiên cứu. Xây dựng một cái nhìn hệ thống về sự phát triển của nghiên cứu an ninh mạng và truyền thông an ninh mạng, đề xuất hướng nghiên cứu tiếp theo.

3. Kết quả nghiên cứu và thảo luận

3.1. Các hướng nghiên cứu về an ninh mạng và truyền thông an ninh mạng trên thế giới

Thứ nhất, hướng nghiên cứu về mối tương quan giữa an ninh mạng và an ninh quốc gia. Ở giai đoạn đầu, không gian mạng được ví như một "chiến trường mới" và thành tố cấu thành của sức mạnh quốc gia. Các công trình nền tảng như cuốn sách "Chiến trường không gian mạng: Những góc nhìn về tác chiến mạng" (tựa gốc: The Virtual Battlefield: Perspectives on Cyber Warfare) của Czosseck và Geers (2009) nền móng cho việc hình thành lý thuyết về chiến tranh mạng, giám sát thông tin, đánh giá tác động kinh tế - xã hội và xây dựng năng lực phòng thủ chủ động.

Cùng năm, tuyển tập "Sức mạnh không gian mạng và An ninh quốc gia" (tựa gốc: Cyberpower and National Security) do Kramer và Starr (2009) biên tập đã hệ thống hóa mối liên hệ giữa sức mạnh không gian mạng và an ninh quốc gia, nhấn mạnh vai trò của thể chế, chính sách và hạ tầng trong chiến lược an ninh quốc gia của các cường quốc.

Dòng nghiên cứu này tiếp tục được phát triển trong thập niên 2010, khi các học giả như Clarke và Knake (2010) hay Richards (2014) phân tích sâu bản chất của chiến tranh mạng, các kịch bản xung đột và khả năng tác chiến của các quốc gia lớn như Mỹ, Nga và Trung Quốc. Những nghiên cứu này cho thấy an ninh mạng gắn chặt với chiến lược, địa chính trị và cạnh tranh quyền lực toàn cầu. Valeriano và Maness (2014), trong tác phẩm "Đối sánh giữa Chiến tranh mạng và Thực tiễn không gian mạng: Xung đột mạng trong hệ thống quốc tế" (tựa gốc: Cyber War versus Cyber Realities: Cyber Conflict in the International System), chỉ ra rằng xung đột mạng trên thực tế thường bị giới hạn về cường độ và mục tiêu, đồng thời nhấn mạnh vai trò của chuẩn mực, quy tắc và sự tương tác giữa các chủ thể nhà nước và phi nhà nước trong hệ thống quốc tế.

Thứ hai, hướng nghiên cứu về chính sách an ninh mạng và quản trị an ninh mạng. Nghiên cứu của Hashim (2011) về Chính sách An ninh mạng Quốc gia của Malaysia cho thấy tiếp cận tích hợp, đa ngành và đa chủ thể là điều kiện then chốt để bảo vệ hạ tầng thông tin quan trọng. Các nghiên cứu so sánh như của Min, Chai và Han (2015) cũng khẳng định xu hướng gia tăng vai trò của nhà nước và quan hệ đối tác công - tư trong chiến lược an ninh mạng tại Mỹ, EU và Nhật Bản. Gần đây hơn, Cheung (2018) đã phân tích sự trỗi dậy của Trung Quốc như một cường quốc công nghiệp an ninh mạng, nhấn mạnh mối quan hệ chặt chẽ giữa an ninh quốc gia, phát triển công nghệ và can thiệp của nhà nước. Ở cấp độ thực thi, các nghiên cứu thực nghiệm như của Hatcher, Meares và Heslen (2020) hay Carrapico và Farrand (2020) cho thấy dù chính sách an ninh mạng ngày càng hoàn thiện, nhưng vẫn tồn tại khoảng cách đáng kể giữa thiết kế chính sách và thực hành quản trị.

Thứ ba, hướng nghiên cứu về tội phạm mạng và tư pháp hình sự. Các công trình nghiên cứu của Easttom và Taylor (2011), Moore (2011) và Yar (2013) đã góp phần hệ thống hóa các dạng thức tội phạm mạng, những thách thức pháp lý đặt ra trong quá trình thu thập, bảo quản và sử dụng chứng cứ điện tử có tính chất ngày càng phức tạp và phạm vi hoạt động xuyên quốc gia của các hành vi phạm tội trong môi trường số (Day, 2014).

Thứ tư, hướng nghiên cứu về yếu tố con người và truyền thông. Hành vi của người dùng giữ vai trò then chốt trong toàn bộ hệ thống bảo mật nhằm bảo đảm an ninh mạng. Kumaraguru và cộng sự (2009) cho thấy các chương trình đào tạo sáng tạo, lặp lại và gắn với bối cảnh thực tế có thể cải thiện đáng kể khả năng nhận diện lừa đảo mà không gây phản tác dụng. Các nghiên cứu của Johnston và Warkentin (2010), cũng như Bulgurcu, Cavusoglu và Benbasat (2010), đã cho thấy trung gian của nhận thức an ninh, thái độ và động cơ cá nhân đối với hành vi tuân thủ chính sách bảo mật.

Các nghiên cứu sau đó tiếp tục mở rộng phân tích theo hướng đi sâu vào những giới hạn về nhận thức và tâm lý của người sử dụng. Albrechtsen và Hovden (2010) chỉ ra rằng các chương trình đào tạo theo hướng tương tác, gắn với tình huống thực tế, thường mang lại hiệu quả cao hơn so với hình thức truyền đạt một chiều. Trong khi đó, Caputo và cộng sự (2014) cho thấy các chương trình mô phỏng tấn công phishing chỉ phát huy tác dụng khi được thiết kế một cách hấp dẫn, minh bạch, tránh tạo cảm giác "giăng bẫy" khiến người tham gia nảy sinh tâm lý phòng vệ tiêu cực. Stanton và cộng sự (2016) đưa ra khái niệm "security fatigue" để chỉ trạng thái mệt mỏi, quá tải khi người dùng phải liên tục tiếp nhận các cảnh báo và yêu cầu bảo mật. Theo các tác giả, tình trạng này có thể làm giảm khả năng xử lý thông tin và ảnh hưởng tiêu cực đến chất lượng quyết định trong môi trường số. Ở một hướng tiếp cận khác, Vishwanath và cộng sự (2016) nhận thấy một số cá nhân dễ trở thành nạn nhân của lừa đảo trực tuyến. Mô hình này nhấn mạnh vai trò của thói quen xử lý thông tin và mức độ hoài nghi của người dùng khi tiếp nhận thông điệp.

Những nghiên cứu gần đây mở rộng trọng tâm sang thiết kế cảnh báo và truyền thông đại chúng về an ninh mạng. Acar và cộng sự (2017) cho thấy việc xử lý triệt để nguyên nhân của các cảnh báo sai có thể nâng cao đáng kể hiệu quả bảo mật. Trong khi đó, Bada, Sasse và Nurse (2019) chỉ ra rằng nhiều chiến dịch nâng cao nhận thức không đạt kết quả như kỳ vọng do chưa thực sự coi trọng việc tiếp cận người dùng theo hướng coi họ là trung tâm.

Ở lĩnh vực mạng xã hội, Ozkaya (2020) và Saleem (2021) nhấn mạnh mối liên hệ chặt chẽ giữa hành vi sử dụng nền tảng số, vấn đề quyền riêng tư với rủi ro an ninh mạng. Tổng quan hệ thống của Desolda và cộng sự (2022) khẳng định vai trò quyết định của yếu tố con người đối với thành công hay thất bại của các biện pháp bảo mật, đề xuất tăng cường nghiên cứu liên ngành và cá nhân hóa các giải pháp an ninh mạng.

3.2. Các công trình nghiên cứu trong nước về an ninh mạng và truyền thông an ninh mạng

Các công trình nghiên cứu trong nước về an ninh mạng cho thấy sự hình thành và phát triển của một diễn ngôn học thuật gắn chặt với yêu cầu bảo vệ an ninh quốc gia, quản trị nhà nước và ổn định chính trị - xã hội. Có thể phân loại các nghiên cứu thành ba nhóm chính: (i) an ninh mạng trong quan hệ với an ninh quốc gia; (ii) pháp luật an ninh mạng và đấu tranh phòng, chống tội phạm mạng; và (iii) an toàn

thông tin, quản trị rủi ro và nâng cao nhận thức xã hội.

Thứ nhất, hướng nghiên cứu về an ninh mạng trong quan hệ với an ninh quốc gia là hướng tiếp cận sớm và chiếm ưu thế trong học thuật Việt Nam

Các công trình thuộc nhóm này coi không gian mạng là một bộ phận cấu thành của chủ quyền quốc gia và là "mặt trận mới" trong bảo vệ an ninh quốc gia. Luận văn của Bùi Thanh Hà (2014) là một trong những nghiên cứu sớm tiếp cận an ninh mạng dưới góc độ hợp tác quốc tế, nhấn mạnh tính toàn cầu của các mối đe dọa an toàn mạng và khẳng định hợp tác quốc tế là yêu cầu tất yếu do không quốc gia nào có thể đơn phương ứng phó với các cuộc tấn công mạng xuyên biên giới.

Các nghiên cứu tiếp theo có xu hướng làm sâu sắc hơn nội hàm an ninh mạng trong mối quan hệ với tình báo, chiến tranh và cạnh tranh quyền lực. Công trình chuyên khảo của Phạm Bình (2015) mở rộng phạm vi phân tích sang lĩnh vực tình báo điện tử, tình báo mạng, nguy cơ đe dọa an ninh thông tin quốc gia và sự gia tăng của tội phạm công nghệ cao. Các bài viết trên Tạp chí An toàn thông tin của Nguyễn Thị Thu Thủy (2018) và Vũ Mạnh Hùng (2018) tiếp tục củng cố cách tiếp cận này thông qua việc dự báo xu hướng phát triển không gian mạng và làm rõ yêu cầu bảo đảm an toàn, an ninh thông tin trong nhiều môi trường khác nhau.

Từ năm 2020 trở đi, diễn ngôn an ninh mạng có sự gắn kết chặt chẽ với bối cảnh quốc tế và đường lối chính trị của Việt Nam. Nguyễn Việt Lâm (2020) coi không gian mạng là "chiến trường mới" và sự gia tăng tranh chấp về chủ quyền dữ liệu. Các nghiên cứu của Hoàng Thị Quyên (2020), Cao Anh Dũng (2021) và Nguyễn Việt Lâm (2021) tiếp tục khẳng định vai trò trung tâm của Luật An ninh mạng và định hướng Đại hội XIII của Đảng trong bảo vệ chủ quyền quốc gia trên không gian mạng.

Thứ hai, hướng nghiên cứu tập trung vào pháp luật an ninh mạng và đấu tranh phòng, chống tội phạm mạng, phát triển mạnh mẽ sau khi Luật An ninh mạng 2018 có hiệu lực

Các nghiên cứu của Nguyễn Thị Ngọc Hoa và Bùi Thị Long (2020) hay Nguyễn Minh Chính (2021) đã đánh giá khung pháp lý hiện hành, chỉ ra những tiến bộ quan trọng trong việc thiết lập hành lang pháp lý bảo vệ không gian mạng, đồng thời chỉ rõ những hạn chế trong thi hành, phối hợp liên ngành và hợp tác quốc tế. Ở cấp độ chuyên sâu hơn, các luận án tiến sĩ của Nguyễn Tiến Phương (2021), Nguyễn Quý Khuyến (2022) và Bùi Thị Long (2022) đã cung cấp bằng chứng thực nghiệm về những khó khăn trong điều tra, thu thập chứng cứ điện tử và áp dụng pháp luật hình sự đối với tội phạm mạng.

Thứ ba, hướng nghiên cứu về an toàn thông tin, quản trị rủi ro và nâng cao nhận thức xã hội

Các nghiên cứu của Lê Văn Thắng (2020), Nguyễn Văn Phương và Trần Văn Diễn (2020) đã chỉ ra khoảng cách lớn giữa mức độ tham gia không gian mạng và nhận thức an ninh mạng của người dùng Việt Nam. Các nghiên cứu về giáo dục và truyền thông như của Nguyễn Thị Hà và cộng sự (2021), Vũ Trọng Lâm (2022) và Dương Thị Thu Hương và Nguyễn Thế Duy Long (2024) nhấn mạnh vai trò của tuyên truyền, giáo dục kỹ năng số và xây dựng văn hóa ứng xử trên không gian mạng.

Luận án của Trần Văn Diễn (2024) đánh dấu bước tiến lý luận quan trọng khi vận dụng các lý thuyết hành vi hiện đại để phân tích tác động của truyền thông và chính sách đến hành vi bảo vệ an ninh mạng của nhân viên.

Từ tổng quan các công trình nghiên cứu trong và ngoài nước, có thể thấy hướng nghiên cứu về truyền thông an ninh mạng tại Việt Nam cần được định hình theo cách tiếp cận liên ngành, lấy con người làm trung tâm thay vì chỉ dừng lại ở bình diện pháp lý và quản trị nhà nước. Trước hết, cần chuyển dịch từ tư duy "bảo đảm an ninh bằng công cụ kỹ thuật và pháp luật" sang tư duy "quản trị an ninh thông qua thay đổi nhận thức và hành vi", trong đó truyền thông giữ vai trò cầu nối giữa chính sách và thực tiễn xã hội. Điều này đòi hỏi các nghiên cứu phải tập trung làm rõ cơ chế tiếp nhận thông tin, quá trình hình thành nhận thức rủi ro và các yếu tố tâm lý - xã hội chi phối hành vi của người dùng trên không gian mạng.

4. Kết luận

Bài viết đã hệ thống hóa một cách có chọn lọc các công trình nghiên cứu tiêu biểu trong và ngoài nước về an ninh mạng và truyền thông an ninh mạng, qua đó làm rõ các khuynh hướng phát triển chủ đạo của lĩnh vực này. Kết quả nghiên cứu cho thấy, trên bình diện quốc tế, nghiên cứu an ninh mạng đã có sự chuyển dịch rõ rệt từ cách tiếp cận thiên về kỹ thuật và quân sự sang cách tiếp cận tích hợp, nhấn mạnh vai trò của yếu tố con người, hành vi và truyền thông trong bảo đảm an ninh. Và khẳng định rằng truyền thông an ninh mạng cần được nhìn nhận như một trụ cột quan trọng trong chiến lược an ninh mạng quốc gia. Đây cũng là hướng nghiên cứu tiềm năng, đòi hỏi sự tiếp tục đầu tư cả về lý luận và thực nghiệm trong bối cảnh chuyển đổi số ngày càng sâu rộng tại Việt Nam./.

TÀI LIỆU THAM KHẢO

1. Acar, E., Fahl, S., & Mazurek, M. L. (2017). Where the wild warnings are: Root causes of Chrome HTTPS certificate errors. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 1407 - 1420.

2. Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection: An intervention study. *Computers & Security,* 29(4), 432 - 445.

3. Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *In*

International Conference on Cyber Security for Sustainable Society (pp. 118 - 131). Springer.

4. Bùi Thanh Hà. (2014). *Hợp tác quốc tế trong lĩnh vực an toàn mạng tại Bộ Thông tin và Truyền thông* (Luận văn thạc sĩ). Đại học Quốc gia Hà Nội.

5. Bùi Thị Long. (2022). *Thực hiện pháp luật về an ninh mạng ở Việt Nam* (Luận án tiến sĩ). Học viện Chính trị Quốc gia Hồ Chí Minh.

6. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly,* 34(3), 523 - 548.

7. Cao Anh Dũng. (2021). Bảo vệ an ninh quốc gia trên không gian mạng trong bối cảnh Cuộc cách mạng công nghiệp lần thứ tư theo định hướng Đại hội XIII của Đảng. *Tạp chí Cộng sản điện tử.*

8. Caputo, D. D., Pfleeger, S. P., Freeman, J. H., & Johnson, M. E. (2014). Going spear-phishing: Exploring embedded training and awareness. *IEEE Security & Privacy,* 12(1), 28 - 38.

9. Carrapico, H., & Farrand, B. (2020). Discursive continuity and change in the time of Covid-19: The case of EU cybersecurity policy. *Journal of European Integration,* 42(8), 1111 - 1126.

10. Cheung, T. M. (2018). The rise of China as a cybersecurity industrial power: Balancing national security, geopolitical, and development priorities. *Journal of Cyber Policy*, 3(2), 208 - 229.

11. Clarke, R. A., & Knake, R. K. (2010). Cyber war: The next threat to national security and what to do about it. *HarperCollins.*

12. Czosseck, C., & Geers, K. (Eds.). (2009). The virtual battlefield: Perspectives on cyber warfare (Vol. 3). *IOS Press*.

13. Day, P. (2014). Cyber attack: The truth about digital crime, cyber warfare and government snooping. *CreateSpace Independent Publishing Platform*.

14. Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2022). Human factors in phishing attacks: A systematic literature review. *ACM Computing Surveys,* 54(8), 1 - 35.

15. Dương Thị Thu Hương, Nguyễn Thế Duy Long. (2024). Những nguy cơ mất an toàn trong việc sử dụng mạng xã hội trên không gian mạng của sinh viên hiện nay, *Tạp chí Lý luận Chính trị và Truyền thông*.

16. Easttom, C., & Taylor, J. (2011). Computer crime, investigation, and the law. *Course Technology.*

17. Hashim, M. S. B. (2011). Malaysia's national cyber security policy: The country's cyber defence initiatives. *Proceedings of the Second Worldwide Cybersecurity Summit*, 1 - 7.

18. Hatcher, W., Meares, W. L., & Heslen, J. (2020). The cybersecurity of municipalities in the United States: An exploratory survey of policies and practices. *Journal of Cyber Policy,* 5(2), 302 - 325.

19. Hoàng Thị Quyên. (2020). Bảo vệ chủ quyền quốc gia trên không gian mạng trong thời đại công nghệ số. *Tạp chí Lý luận chính trị*, số 10/2020

20. Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly,* 34(3), 549 - 566.

21. Kramer, F. D., Starr, S. H., & Wentz, L. K. (Eds.). (2009). Cyberpower and national security. *Potomac Books*.

22. Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L. F., Hong, J. I., Blair, M. A., & Pham, T. (2009). School of phish: A real-world evaluation of anti-phishing training. *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS 2009),* 1 - 12.

23. Lê Văn Thắng. (2020). An ninh thông tin ở Việt Nam trong điều kiện hiện nay - Vấn đề đặt ra và giải pháp. *Tạp chí Tuyên giáo điện tử.*

24. Luật An ninh mạng (số 24/2018/QH14). Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam

25. Luật An ninh mạng (số 116/2025/QH15). Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam;

26. Min, K. S., Chai, S. W., & Han, M. (2015). An international comparative study on cyber security strategy. *International Journal of Security and Its Applications*, 9(2), 77 - 88.

27. Moore, R. (2011). Cybercrime: Investigating high-technology computer crime (2nd ed.). *Routledge.*

28. Nguyễn Minh Chính. (2021). Hoàn thiện pháp luật về an ninh mạng trong tình hình hiện nay. *Tạp chí Cộng sản điện tử.*

29. Nguyễn Quý Khuyến. (2022). *Tội phạm trong lĩnh vực công nghệ thông tin và mạng viễn thông theo pháp luật hình sự Việt Nam* (Luận án tiến sĩ). Học viện Cảnh sát nhân dân.

30. Nguyễn Thị Hà, Lê Thanh Bình, Nguyễn Văn Phương. (2021). Một số giải pháp nâng cao hiệu quả tuyên truyền, phổ biến pháp luật về an toàn thông tin và kỹ năng sử dụng mạng xã hội cho học sinh, sinh viên hiện nay. *Tạp chí Công Thương*.

31. Nguyễn Thị Ngọc Hoa, Bùi Thị Long. (2020). Nhìn lại một năm thực hiện pháp luật về an ninh mạng. *Tạp chí Lý luận chính trị*, số 4/2020.

32. Nguyễn Thị Thu Thủy. (2018). Dự báo về An toàn mạng năm 2018. *Tạp chí An toàn thông tin*.

33. Nguyễn Tiến Phương. (2021). *Áp dụng pháp luật trong điều tra tội phạm sử dụng không gian mạng xâm phạm an ninh quốc gia của Cơ quan An ninh điều tra, Bộ Công an Việt Nam* (Luận án tiến sĩ). Học viện Chính trị Quốc gia Hồ Chí Minh.

34. Nguyễn Văn Phương, Trần Văn Diễn. (2020). Rủi ro và thách thức an ninh mạng trong lĩnh vực ngân hàng tại Việt Nam. *Tạp chí khoa học Đại học Mở thành phố Hồ Chí Minh*.

35. Nguyễn Việt Lâm. (2020). Hợp tác và đấu tranh về an ninh mạng trong quan hệ quốc tế: Cơ hội, thách thức về đề xuất chính sách đối với Việt Nam. *Tạp chí Cộng sản điện tử.*

36. Nguyễn Việt Lâm. (2021). Trung Quốc với chủ quyền không gian mạng. *Tạp chí Lý luận chính trị.*

37. Ozkaya, E. (2020). *Cyber security challenges in social media* [Doctoral dissertation, Charles Sturt University]. CSU Research Output.

38. Phạm Bình. (2015). *Tình báo điện tử không gian*. Nhà xuất bản Công an nhân dân.

39. Richards, J. (2014). Cyber war: The anatomy of a global security threat. *Palgrave Macmillan.*

40. Saleem, A. N. (2021). *Cybersecurity issues in social media* (Master's thesis, Near East University). Near East University Institutional Repository.

41. Stanton, B., Theofanos, M., Prettyman, S. S., & Furman, S. (2016). Security fatigue. *IT Professional,* 18(5), 26 - 32.

42. Trần Văn Diễn. (2024). *Khai phóng tiềm năng truyền thông chính phủ và chính sách an ninh mạng trong tổ chức: Vai trò của các yếu tố ảnh hưởng đến hành vi bảo vệ an ninh mạng của nhân viên* (Luận án tiến sĩ). Trường Đại học Quốc tế - Đại học Quốc gia TP.HCM.

43. Valeriano, B., & Maness, R. C. (2015). Cyber war versus cyber realities: Cyber conflict in the international system. *Oxford University Press*.

44. Vishwanath, A., Harrison, B., & Ng, Y. J. (2016). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, 43(4), 594 - 621.

45. Vũ Mạnh Hùng. (2018). Một số vấn đề an toàn, an ninh thông tin mạng trên thế giới. *Tạp chí An toàn thông tin*.