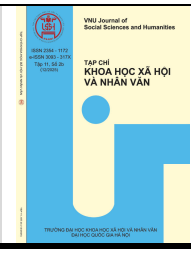
Tạp chí Khoa học Xã hội và Nhân văn
Tập 11, Số 2b (2025) 286-299

ISSN: 2354-1172
e-ISSN: 3093-317X



Hợp tác Hàn Quốc - Đông Nam Á trong lĩnh vực an ninh mạng

Dương Quỳnh Thu*

Tóm tắt: Sự cố rò rỉ dữ liệu SK Telecom vào tháng 04 năm 2025 đặt ra nhu cầu cấp bách phải tăng cường các biện pháp an ninh mạng trước các mối đe doạ toàn cầu ngày càng tinh vi. Nghiên cứu này sẽ cung cấp cái nhìn toàn diện về chiến lược an ninh mạng của Hàn Quốc, từ hệ thống chính sách quốc gia thúc đẩy phối hợp công – tư đến vai trò nòng cốt của các giải pháp công nghệ như AhnLab V3. Qua việc đánh giá thực trạng và các chiến lược hợp tác tại Đông Á, bài viết làm rõ xu hướng tương lai của Hàn Quốc trong việc định hình một hệ sinh thái số tự cường và chủ động. Từ đó, nghiên cứu gợi mở các hướng hợp tác chiến lược, đặc biệt là với Việt Nam, nhằm tăng cường năng lực quản lý, đảm bảo an ninh mạng chung trong khu vực Đông Nam Á.

Từ khóa: hợp tác an ninh mạng; ASEAN; hợp tác Hàn Quốc – Việt Nam; phòng thủ chủ động.

Ngày nhận: 26/10/2025; ngày chỉnh sửa: 05/12/2025; ngày chấp nhận đăng: 31/12/2025

DOI: https://doi.org/10.33100/vjossh.2025.11.2b.7

1. Đặt vấn đề

Trong bối cảnh toàn cầu hiện nay, an ninh mạng đang trở thành một ưu tiên hàng đầu khi thế giới ngày càng số hóa và các tài sản kỹ thuật số không còn bị giới hạn bởi biên giới địa lý. Các mối đe dọa mạng đang không ngừng phát triển cả về mức độ tinh vi và tần suất, đòi hỏi các quốc gia phải liên tục đổi mới và đẩy mạnh hợp tác quốc tế. Hàn Quốc, một quốc gia hàng đầu thế giới về tiến bộ công nghệ, gần đây đã bị ảnh hưởng bởi một sự cố an ninh mạng[1] làm nổi bật tính chất dai dẳng và không ngừng phát triển của các mối đe dọa không gian mạng.

Trong thời đại Cách mạng Công nghiệp 4.0 hiện nay, dữ liệu đã trở thành một tài sản chiến lược, là động lực chính thúc đẩy tăng trưởng kinh tế, đổi mới và an ninh quốc gia. Tính chất nghiêm trọng của các sự cố mạng gần đây khẳng định rằng bảo mật dữ liệu là mắt xích không thể tách rời của an ninh quốc gia. Việc đảm bảo an toàn thông tin không chỉ bảo vệ quyền lợi cá nhân mà còn duy trì sự vận hành thông suốt của các hạ tầng chiến lược, đồng thời giữ vững niềm tin số trong cộng đồng. Năm 2023, trong phiên họp thứ hai của Ban chỉ đạo An toàn, An ninh mạng quốc gia, với vai trò Trưởng Ban chỉ đạo, Thủ tướng Phạm Minh Chính đã nhấn mạnh, an ninh mạng và an toàn thông tin phải là nhiệm vụ quan trọng, thường xuyên và lâu dài để duy trì một môi trường trực tuyến an toàn, lành mạnh và đáng tin

* Trường Đại học Khoa học Xã hội và Nhân văn, ĐHQG Hà Nội; email: quynhthu14@gmail.com

[1] Sự cố lộ thông tin khách hàng của công ty viễn thông lớn nhất Hàn Quốc.

cậy cho các cơ quan chính phủ, tổ chức, doanh nghiệp và công dân, song song với phát triển kinh tế - xã hội (Báo Nhân Dân 2023). Bảo vệ dữ liệu không chỉ giới hạn ở việc ngăn chặn rò rỉ thông tin cá nhân mà còn bao gồm việc đảm bảo tính toàn vẹn, bảo mật và khả năng truy cập của dữ liệu trong các hệ thống phức tạp như điện toán đám mây và Internet vạn vật (IoT) - nơi các mối đe dọa ngày càng gia tăng do sự hạn chế về tài nguyên và sự hội tụ công nghệ.

Bài nghiên cứu này sẽ đề cập tới sự cần thiết của hợp tác quốc tế trong an ninh mạng, các chiến lược hợp tác khu vực và quốc tế đang phát triển trong lĩnh vực an ninh thông tin mạng. Thông qua việc tổng hợp các yếu tố thể hiện năng lực quốc gia trong lĩnh vực an ninh mạng của Hàn Quốc, nghiên cứu đề xuất một vài hàm ý hợp tác trong lĩnh vực an ninh mạng quốc tế giữa Việt Nam và Hàn Quốc nói riêng cũng như các quốc gia trong khu vực Đông Á nói chung. Nghiên cứu này được thực hiện dựa trên phương pháp tổng hợp tài liệu và phân tích chính sách nhằm cung cấp một cái nhìn toàn diện về lập trường an ninh mạng của Hàn Quốc. Đồng thời đây cũng là những gợi mở ra hướng hợp tác chiến lược giữa Hàn Quốc với các quốc gia Đông Nam Á, đặc biệt là Việt Nam.

Các nguồn tư liệu chính được phân tích tập trung vào giai đoạn 2018-2025; đây cũng chính là phạm vi thời gian của nghiên cứu này. Theo đó các nguồn tư liệu được khai thác bao gồm các văn bản pháp lý, chiến lược quốc gia của Hàn Quốc (như Quy định quản lý an ninh mạng quốc gia, Đạo luật bảo vệ thông tin cá nhân) và các báo cáo, bài báo khoa học chuyên sâu về an ninh mạng khu vực. Khung phân tích được áp dụng xoay quanh các trụ cột chính như đánh giá khung pháp lý và phương thức quản trị của Hàn Quốc, phân tích các chương trình hợp tác khu vực và song phương, đồng thời so sánh những điểm thuận lợi, thách thức và triển vọng hợp tác giữa Hàn Quốc và các đối tác Đông Nam Á.

2. Các mối đe doạ an ninh mạng đã từng xảy ra và lựa chọn đối tác hợp tác

2.1. Các sự cố tấn công mạng tại một vài quốc gia trong khu vực

Trong hai năm gần đây (2024-2025), khu vực Đông Á và đặc biệt là Đông Nam Á đối mặt với sự gia tăng đáng kể các cuộc tấn công mạng. Ransomware và các chiến dịch gián điệp mạng do nhà nước bảo trợ là những mối đe dọa phổ biến nhất, chủ yếu hướng tới các lĩnh vực sản xuất, chính phủ và hạ tầng quan trọng. Các yếu tố địa chính trị và sự phát triển của trí tuệ nhân tạo (AI) đã thúc đẩy mức độ tinh vi và số lượng cuộc tấn công, điều này khiến khu vực này trở thành điểm nóng về rủi ro mạng toàn cầu (Lavrova 2025).

Theo tổng hợp của Tạp chí Thông tin & Truyền thông, cơ quan ngôn luận của Bộ Thông tin và Truyền thông, số lượng các cuộc tấn công mạng ở Nhật Bản đang gia tăng. Đặc biệt là xung quanh Thế vận hội Tokyo 2020 (diễn ra vào 2021). Các cuộc tấn công này thường mang tính chất thăm dò, gây rối hoặc đánh cắp dữ liệu liên quan đến công tác tổ chức sự kiện. Số trường hợp truy cập trái phép và các cuộc tấn công mạng tăng vọt tại Nhật Bản đã được Cơ quan Cảnh sát Quốc gia (NPA) xác nhận trong các báo cáo chính thức của họ năm 2022. Những vụ việc này cho thấy an ninh mạng là một vấn đề toàn cầu, không phân biệt các nền kinh tế số phát triển hay đang phát triển. Điều này tạo ra một nhu cầu tất yếu về hợp tác giữa các quốc gia để cùng triển khai các biện pháp đối phó với các mối đe doạ chung.

Tháng 4 năm 2025, SK Telecom (SKT), nhà mạng viễn thông di động lớn nhất Hàn

Quốc, đã công bố một vụ rò rỉ dữ liệu lớn làm lộ thông tin người dùng liên quan đến thẻ SIM[2], bao gồm hồ sơ nhận dạng thuê bao di động quốc tế (IMSI[3]) và khóa xác thực USIM của khoảng 27 triệu thuê bao (The Korea Harald 2025). Kết quả điều tra cho thấy phần mềm độc hại đã nằm ẩn trong hệ thống từ tháng 6 năm 2022 mà không bị phát hiện trên mạng của SKT trong gần ba năm. Sự cố này đã dẫn đến việc 640.000 khách hàng rời bỏ mạng viễn thông SKT tính đến hết tháng 6 năm 2025 (Hankookilbo 2025), trở thành một trong những vụ vi phạm an ninh viễn thông lớn nhất của Hàn Quốc và gây ra mối lo ngại rộng rãi về các lỗ hổng nghiêm trọng trong cơ sở hạ tầng viễn thông. Trước đó, năm 2013, Hàn Quốc đã phải xử lý một cuộc tấn công mạng vào hệ thống ngân hàng, truyền hình. Cuộc tấn công đã gây tê liệt hệ thống của nhiều ngân hàng lớn cũng như các cơ quan truyền hình – tiêu biểu là đài truyền hình YTN của Hàn Quốc, làm ảnh hưởng nghiêm trọng tới hoạt động kinh tế xã hội (Boannews 2013). Tình hình này đã trở thành tiền đề để Hàn Quốc nỗ lực vươn lên trở thành một quốc gia có vai trò tiên phong trong việc ứng phó các cuộc tấn công quy mô lớn.

Tương tự, Singapore được biết đến là một trung tâm về tài chính và có tiềm lực công nghệ mạnh mẽ trong khu vực Đông Nam Á (Tạp chí Thông tin Truyền thông 2025). Tuy nhiên, theo các công bố thường xuyên của Cơ quan An ninh mạng Singapore (CSA) cho thấy tình hình an ninh mạng của quốc gia phải đối mặt với các đe dọa liên quan đến lĩnh vực tài chính, thương mại điện tử và dịch vụ công. Các vụ việc lớn như vụ tấn công vào SingHealth (2018), nơi dữ liệu cá nhân của hàng triệu bệnh nhân bị đánh cắp, thể hiện điểm yếu trong bảo mật dữ liệu.

Việt Nam cũng là một nạn nhân của các nhóm tấn công mạng. Đáng nói, các cuộc tấn công mạng diễn ra tại Việt Nam không chỉ nhằm vào các tổ chức tư nhân mà một lượng lớn đang hướng trực tiếp tới các cơ quan chức năng, hệ thống thông tin quan trọng như các tên miền mang tên .gov.vn (Tạp chí Khoa học & Công nghệ Việt Nam 2024). Theo Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05), số vụ tấn công mạng tăng 9,5% vào năm 2023 so với năm 2022. Trong số 554 trang web bị tấn công vào năm 2023, 212 địa chỉ web đến từ các văn phòng chính phủ Việt Nam, làm tăng thêm lo ngại về các cuộc tấn công quy mô lớn vào các cơ sở dữ liệu quốc gia mật. An ninh mạng đã trở nên phức tạp để giải quyết, vì nó có thể tạo ra nhiều tác động tiêu cực khác nhau, từ bất ổn xã hội đến nguy cơ đối với bộ máy chính phủ mong manh của Việt Nam. Sự phức tạp này đòi hỏi những nỗ lực phối hợp chặt chẽ của nhiều bên để bảo vệ an ninh quốc gia (Trịnh Viết Dũng 2024).

Như vậy, có thể thấy, trong bối cảnh địa chính trị phức tạp và sự phát triển nhanh chóng của công nghệ, các quốc gia Đông Á, đặc biệt là Đông Nam Á, đang phải đối mặt với làn sóng tấn công mạng ngày càng gia tăng và tinh vi. Các cuộc tấn công này không chỉ nhắm vào các tổ chức tư nhân mà còn tập trung vào hạ tầng trọng yếu của chính phủ, gây ra những thiệt hại kinh tế và xã hội nghiêm trọng. Từ những sự cố rò rỉ dữ liệu thẻ SIM ở Hàn Quốc, các cuộc tấn công vào hạ tầng tài chính của Singapore, đến các vụ tấn công vào hệ thống của chính phủ Việt Nam, tất cả đều cho thấy một thực trạng chung: an ninh mạng đã trở thành một mối đe dọa thường trực, đòi hỏi các quốc gia phải có những nỗ lực phối hợp và chủ động

[2] Subscriber Identity Module (SIM). Bản chất bảo mật của thẻ SIM đảm bảo dữ liệu người dùng được bảo vệ, ngay cả khi thẻ bị tháo khỏi thiết bị. Mã hóa tiên tiến và phần cứng chống giả mạo, điều này khiến những cá nhân không được phép khó có thể truy cập vào dữ liệu được lưu trữ trên thẻ SIM.

[3] International Mobile Subscriber Identity: Một số duy nhất dùng để xác định thuê bao trong mạng.

để bảo vệ không gian kỹ thuật số của mình, từ đó thúc đẩy nhu cầu hợp tác khu vực.

2.2. Hàn Quốc: Đối tác phù hợp cho hợp tác an ninh mạng

Thomas (2009) đã từng nhận định về những cuộc tấn công mạng nêu trên không chỉ diễn ra ở một quốc gia nhất định mà nhiều quốc gia khác trong khu vực Đông Á đều đang phải đối mặt với các cuộc tấn công mạng từ bên ngoài biên giới quốc gia. Và nhận định này một lần nữa được khẳng định tính thời sự trong các báo cáo GCI (Global Cybersecurity Index) của ITU[4] được công bố vào năm 2024. Theo đó ITU "nhấn mạnh các cuộc tấn công bằng phần mềm tống tiền nhắm vào dịch vụ chính phủ và các lỗ hổng ảnh hưởng tới ngành công nghiệp chủ chốt" (ITU 2024: 17).

Mặc dù cả Nhật Bản và Singapore đều là những cường quốc trong lĩnh vực công nghệ thông tin, trọng tâm chiến lược của hai quốc gia có sự phân hoá rõ rệt theo các ưu tiên quốc gia. Theo báo cáo so sánh của ASPI (2024) và ITU (2024) các chiến lược an ninh mạng của Nhật Bản thường nhấn mạnh vào việc bảo vệ hạ tầng trọng yếu (Critical Infrastructure Protection - CIP), an ninh chuỗi cung ứng, và phòng chống tội phạm mạng. Trong khi đó, Singapore tập trung vào việc xây dựng một hệ sinh thái an ninh mạng vững mạnh để hỗ trợ nền kinh tế số và vị thế là trung tâm công nghệ. Chiến lược của Singapore chú trọng vào quy định, quản trị, hợp tác quốc tế trong lĩnh vực phòng chống tội phạm mạng và bảo vệ dữ liệu.

Do thực trạng địa chính trị phức tạp, Hàn Quốc đã chuyển từ các chiến lược thụ động đối ứng sang các chiến lược chủ động và toàn diện. Dựa trên các thông tin tổng hợp từ trung tâm thông tin quy định pháp luật Quốc gia Hàn Quốc (국가법령정보센터) và thư viện quốc hội Hàn Quốc có thể thấy Hàn Quốc đã xây dựng khung pháp lý và quản trị tổng thể từ nhiều luật chuyên biệt như:

Quy định Quản lý An ninh mạng Quốc gia [국가사이버안보 관리규정] phác thảo một hệ thống ứng phó toàn quốc chống lại các cuộc tấn công mạng.

Luật Bảo vệ Cơ sở Hạ tầng Thông tin Quan trọng [중요정보통신기반시설 보호법] (ban hành năm 2002) thiết lập khuôn khổ quốc gia để bảo vệ hạ tầng thông quốc gia.

Sau các cuộc tấn công mạng vào Công ty điện hạt nhân và thủy điện Hàn Quốc (KHNP-Korea Hydro & Nuclear Power), Đạo luật về các biện pháp bảo vệ cơ sở hạt nhân [원자력시설등의 방호 및 방사능방재대책법] v.v… đã được ban hành để tăng cường hệ thống bảo vệ cơ sở hạt nhân.

Luật phát triển ngành an ninh mạng [정보보호산업 진흥법]mới được ban hành vào tháng 9 năm 2024 nhằm thúc đẩy sự phát triển của ngành công nghiệp an ninh mạng Hàn Quốc.

Luật bảo vệ thông tin cá nhân [개인정보 보호법] (ban hành đầu tiên năm 2011 và liên tục được chỉnh sửa, thông qua quốc hội vào các năm 2023, 2024) quy định các biện pháp bảo mật thông tin cá nhân.

Chính phủ Hàn Quốc đã thúc đẩy việc hoàn thiện hành lang pháp lý liên quan tới công nghệ thông tin và truyền thông có thể kể đến như Đạo luật phát triển Điện toán đám mây và Bảo vệ người dùng [클라우드컴퓨팅 발전 및 이용자 보호 법] năm 2015, Chiến lược Kỹ thuật số Quốc gia [대한민국 디지털 전략] năm 2022, 2024.

Bên cạnh đó, chính phủ Hàn Quốc còn xây dựng một cấu trúc quản trị với sự tham gia của nhiều cơ quan tổ chức chính phủ như: Văn phòng An ninh Quốc gia, Cơ quan Tình báo Quốc gia, Bộ Khoa học và Công nghệ Thông tin, Bộ Nội vụ và các tổ chức công chuyên biệt như: Trung tâm An ninh

[4] ITU- International Telecommunication Union – Liên minh Viễn thông Quốc tế

mạng quốc gia[5] (NCSC), Cơ quan Internet và An ninh Hàn Quốc[6] (KISA). Sự tức thời trong việc ban hành các quy định pháp luật liên quan của chính phủ Hàn Quốc đã trở thành một nền tảng vững chắc cho các nghiên cứu phát triển về an ninh mạng tại Hàn Quốc. Các trường đại học hàng đầu của Hàn Quốc với các chương trình an ninh mạng mạnh mẽ bao gồm Viện Khoa học và Công nghệ Tiên tiến Hàn Quốc (KAIST), Đại học Quốc gia Seoul (SNU), Đại học Khoa học và Công nghệ Pohang (POSTECH), Đại học Sungkyunkwan (SKKU) và Đại học Hanyang. Các viện nghiên cứu nổi bật như Viện Nghiên cứu An ninh Quốc gia (NSRI) tập trung vào các hệ thống an ninh quốc gia và công nghệ an toàn mạng. Trường An ninh mạng (SCS) và Khoa Phòng thủ mạng của Đại học Hàn Quốc (Korea University), được Bộ Quốc phòng hỗ trợ, đào tạo các sĩ quan an ninh mạng hàng đầu. Thông qua việc xây dựng khung pháp lý vững chắc và khởi xướng các chính sách chiến lược, chính phủ Hàn Quốc đã tạo ra một môi trường thuận lợi, thúc đẩy sự đổi mới và phát triển của các doanh nghiệp công nghệ thông tin và truyền thông (ICT) trong nước. Các nỗ lực này không chỉ nhằm mục đích bảo vệ cơ sở hạ tầng quốc gia mà còn giúp định hình các hướng nghiên cứu mới nổi, đảm bảo Hàn Quốc luôn đi đầu trong cuộc chiến chống lại các mối đe dọa từ an ninh mạng.

Các doanh nghiệp của Hàn Quốc được tạo điều kiện để phát triển, trong đó tiêu biểu là AhnLab. Theo thông tin tổng hợp từ trang chủ của Ahnlab, bắt đầu từ phần mềm diệt virus V3 trên một đĩa mềm duy nhất, công ty AhnLab đã phát triển thành một nền tảng bảo mật toàn diện, bảo vệ các điểm cuối, mạng, đám mây và hệ thống công nghiệp. Theo Sách trắng về an ninh mạng Hàn Quốc do MSIT[7] và KISA[8] phối hợp công bố năm 2023 và 2024, AhnLab đã nhận được sự công nhận rộng rãi trên toàn cầu, liên tục đạt được các chứng nhận và giải thưởng từ các tổ chức kiểm định uy tín. Chính phủ Hàn Quốc đánh giá cao vai trò của AhnLab trong việc củng cố an ninh mạng quốc gia. AhnLab Security Intelligence Center (ASEC) và Trung tâm An ninh mạng Quốc gia (NCSC) của Hàn Quốc đã hợp tác chặt chẽ trong việc phát hiện và phân tích các lỗ hổng bảo mật nghiêm trọng, như lỗ hổng zero-day của Internet Explorer, và thông báo chúng cho các nhà cung cấp phần mềm để khắc phục. Sự hợp tác này không chỉ thể hiện sự tin tưởng của chính phủ vào chuyên môn của AhnLab cũng như vai trò của hãng trong việc bảo vệ cơ sở hạ tầng kỹ thuật số của Hàn Quốc (Chosun 2022).

Trong giai đoạn 2024-2025 các xu hướng bao gồm sự gia tăng của tấn công dựa trên Trí tuệ nhân tạo (AI), trong đó các tác nhân độc hại sử dụng AI để tạo ra mã độc khó phát hiện, công nghệ deepfake[9] và các chiến dịch lừa đảo tinh vi. Mô hình Ransomware-as-a-Service[10] (RaaS) và các cuộc tấn công ransomware[11] nói chung vẫn là mối đe dọa nghiêm trọng, gây thiệt hại lớn về tài chính và dữ liệu. Ngoài ra, tấn công không cần file

[5] NCSC - National Cybersecurity Center – được thành lập năm 2004".

[6] Kisa - Korea Internet & Security Agency – được thành lập năm 1996.

[7] Ministry of Science and ICT – Bộ Khoa học và Công nghệ thông tin Hàn Quốc.

[8] Korea Internet & Secủity Agency – Cơ quan Internet và An ninh mạng Hàn Quốc.

[9] Deepfake là công nghệ mô phỏng hình ảnh khuôn mặt con người, được đặt tên theo cụm từ được kết hợp giữa "deep learning" (máy học) và "fake" (giả).

[10] Một nhóm tội phạm sẽ xây dựng mã độc và bán các mã độc cho một nhóm khác để sử dụng những mã độc ransomware này và xâm nhập vào một DN hoặc tổ chức dễ bị tấn công.

[11] Ransomware là phần mềm độc hại mã hóa các tệp khi lọt vào thiết bị cần tấn công hoặc ngăn chủ thiết bị sử dụng máy tính cho đến khi chủ thiết bị trả tiền (tiền chuộc) để được mở khóa thiết bị của mình.

(Fileless Malware[12]), chạy trực tiếp trên bộ nhớ hệ thống, đang trở nên phổ biến hơn, gây khó khăn cho việc phát hiện và xử lý. Cùng với đó, an ninh đám mây và bảo mật IoT (Internet of Things – Internet vạn vật) trở thành những lĩnh vực trọng tâm do sự phụ thuộc ngày càng tăng vào các nền tảng đám mây và số lượng thiết bị IoT được kết nối bùng nổ, tạo ra bề mặt tấn công rộng lớn hơn (ITU 2024).

Có thể thấy, Hàn Quốc là một đối tác hợp tác an ninh mạng đầy triển vọng. Với khung pháp lý toàn diện, liên tục được cập nhật và một hệ thống quản trị chặt chẽ, Hàn Quốc đã thể hiện sự chủ động trong việc đối phó với các mối đe dọa mạng. Sự kết hợp giữa các cơ quan chính phủ chuyên biệt, các viện nghiên cứu hàng đầu và các doanh nghiệp công nghệ lớn như AhnLab đã tạo nên một hệ sinh thái an ninh mạng mạnh mẽ và có khả năng ứng phó tức thời. Điều này cho thấy Hàn Quốc không chỉ có năng lực kỹ thuật mà còn có một chiến lược dài hạn, giúp quốc gia này trở thành một đối tác đáng tin cậy trong cuộc chiến chống lại các mối đe dọa an ninh mạng xuyên biên giới ngày càng phức tạp.

3. Các chương trình hợp tác trong lĩnh vực an ninh mạng của Hàn Quốc

Trước những cuộc tấn công vào mạng lưới an ninh thông tin quốc gia, các nước đều phải nâng cao năng lực phòng thủ, chống lại các hoạt động mạng độc hại sau khi bị tấn công. Tuy nhiên, thay vì phương thức phòng thủ thụ động, Mỹ đã tiên phong thay đổi mô hình sang hướng tăng cường khả năng phòng thủ chủ động vào năm 2018. Để phòng thủ chủ động, các quốc gia cần thu thập thông tin chi tiết về các hành vi của đối thủ trong không gian mạng trước khi tác động của chúng đến các mục tiêu dự định. Những thông tin chi tiết này chủ yếu được nhúng trong các cơ sở hạ tầng vật lý mà đối thủ khai thác cho các hoạt động mạng độc hại - các cơ sở chủ yếu nằm ở các vùng lãnh thổ nước ngoài. Đó là lý do tại sao hợp tác với các đồng minh và đối tác là rất quan trọng đối với phòng thủ mạng chủ động. Trước bối cảnh này, Hàn Quốc và Hoa Kỳ đã rất nỗ lực hợp tác trong nâng cao năng lực phòng thủ một cách chủ động (Park and Kim 2025).

Cùng quan điểm Hàn Quốc cần phải nâng cao năng lực quốc gia trong an ninh mạng, Kim (2025: 10) lập luận rằng, bên cạnh những mối an ninh truyền thống như kinh tế, chính trị thì hiện nay, Hàn Quốc đang phải đối mặt với các mối đe dọa phi truyền thống trên mạng, đặc biệt "khi các tác nhân thù địch phá vỡ phòng tuyến kỹ thuật số". Theo đó, Hàn Quốc nói riêng và nhiều quốc gia khác nói chung bắt buộc phải hợp tác cùng các quốc gia khác để tạo ra các "rào cản" phòng thủ tấn công mạng cũng như chủ động tìm kiếm và loại trừ các nguy cơ tấn công trên mạng.

Chiến lược An ninh mạng Quốc gia năm 2024 của Hàn Quốc thể hiện một tầm nhìn hướng tới trở thành "một quốc gia trụ cột toàn cầu thực hiện vai trò và trách nhiệm quốc tế của mình trong khi bảo vệ các giá trị tự do, nhân quyền và pháp quyền trong không gian mạng" (Kim 2024: 3). Chiến lược này nhấn mạnh tầm quan trọng của việc xác định các tác nhân đe dọa mạng, xây dựng khả năng tấn công để chống lại các hoạt động mạng độc hại và tăng cường khả năng tự cường quốc gia. Hàn Quốc cam kết sẽ đóng góp cho cộng đồng quốc tế, thúc

[12] Một dạng phần mềm độc hại có khả năng hoạt động mà không cần lưu trữ dưới dạng file trên hệ thống. Không giống như virus truyền thống, fileless malware không để lại dấu vết trên ổ cứng, khiến cho các phần mềm diệt virus thông thường khó lòng phát hiện ra sự hiện diện của phần mềm này. Khi xâm nhập, phần mềm này có thể đánh cắp các thông tin nhạy cảm như mật khẩu, thông tin tài khoản, thông tin tài khoản ngân hàng, điều khiển hệ thống từ xa, tạo lỗ hổng để xâm nhập vào hệ thống về sau.

đẩy hợp tác và cùng nhau ứng phó với các tác nhân độc hại. Để đạt được điều này, Hàn Quốc đặt mục tiêu đa dạng hóa các kênh và đối tác hợp tác quốc tế, tích cực thúc đẩy xây dựng năng lực mạng và cung cấp hỗ trợ cho các quốc gia khác (Kim 2024).

Hàn Quốc thể hiện sự tích cực trong hợp tác an ninh mạng với nhiều tổ chức, hiệp hội, quốc gia khu vực trên thế giới. Trong đó việc hợp tác với các quốc gia Đông Á và đặc biệt là khu vực Đông Nam Á là một phần quan trọng trong chiến lược ngoại giao an ninh mạng và an ninh quốc gia Hàn Quốc. Thông qua "Hội nghị cấp Bộ trưởng ASEAN – ROK về An ninh mạng (AMCC)" hay "Đối thoại cam kết hỗ trợ chiến lược an ninh mạng toàn diện của ASEAN – ROK", Bộ trưởng phụ trách an ninh mạng của Hàn Quốc và các nước ASEAN thảo luận, phối hợp chính sách, tăng cường hợp tác. Các cuộc đối thoại này đã giúp các bên chia sẻ thông tin, kinh nghiệm và cùng xây dựng năng lực đối phó với các thách thức an ninh mạng trong khu vực. Bên cạnh những chương trình hội đàm cấp cao chuyên sâu về an ninh mạng, Hàn Quốc cũng tham gia vào Diễn đàn an ninh khu vực ASEAN (ARF) để thúc đẩy các nguyên tắc và chuẩn mực về hành vi có trách nhiệm của nhà nước trong không gian mạng (Kim 2022).

Hàn Quốc cũng thường xuyên cung cấp các chương trình đào tạo chuyên sâu, hội thảo và các khoá huấn luyện cho các chuyên gia an ninh mạng từ các nước ASEAN nhằm nâng cao năng lực kỹ thuật và quản lý. Điển hình có thể kể đến cuộc thi ASEAN Cyber Shield (ACS). Đây là một cuộc thi an ninh mạng hàng năm được khởi xướng vào năm 2023 được tổ chức bởi Quỹ Hợp tác ASEAN-Hàn Quốc (Asean – Korean Cooperation Fund- AKCF). ACS đóng vai trò là một nền tảng đào tạo thực hành cho các chuyên gia an ninh mạng. Ngoài ra đây cũng là cuộc thi theo hình thức Capture The Flag (CTF), nơi các đội thi sẽ giải các bài toán liên quan đến an ninh mạng, bao gồm cả tấn công và phòng thủ. Các bài toán thường được xây dựng dựa trên các kịch bản thực tế, phản ánh các lĩnh vực dễ bị tổn thương và các công nghệ mới nhất, như AI và blockchain. Mục tiêu của cuộc thi là phát hiện và bồi dưỡng tài năng an ninh mạng trong khu vực. Cuộc thi cung cấp một nền tảng để các tài năng thể hiện kỹ năng, thúc đẩy sự sáng tạo và hợp tác trong lĩnh vực an ninh mạng tại ASEAN (AKCF 2023).

Hàn Quốc đã thể hiện vai trò tích cực trong việc hỗ trợ các nước đang phát triển nâng cao năng lực an ninh mạng. Thông qua các chương trình đào tạo, viện trợ phát triển chính thức (ODA), và các trung tâm đào tạo như Asia-Pacific Cybercrime (APC) Capacity-Building Hub, Hàn Quốc giúp các quốc gia đối tác tăng cường khả năng chống tội phạm mạng và xây dựng nguồn nhân lực (KOICA 2023). Mặc dù có những khác biệt về chính sách, các nước trong khu vực đều có chung nhu cầu hợp tác để chống lại tội phạm mạng, đặc biệt là các mối đe dọa xuyên quốc gia. Các nền tảng như Diễn đàn khu vực ASEAN (ARF) và Hội nghị thượng đỉnh Đông Á (EAS) là cơ chế để các quốc gia cùng nhau chia sẻ thông tin và kinh nghiệm. Các công ty Hàn Quốc có thể phát huy lợi thế về công nghệ và kinh nghiệm để hợp tác với các quốc gia này trong việc xây dựng cơ sở hạ tầng an toàn, phát triển các giải pháp bảo mật, và đào tạo nguồn nhân lực an ninh mạng. Các tổ chức và diễn đàn khu vực như ASEAN đã thiết lập các Chiến lược Hợp tác An ninh Mạng (ASEAN's Cybersecurity Cooperation Strategy) và các cơ chế như ASEAN CERT [13] để chia sẻ thông tin về các mối đe dọa. Việc Hàn Quốc nâng tầm quan hệ với ASEAN lên Đối tác

[13] ASEAN CERT viết tắt của ASEAN Computer Emergency Resopnse Team – Nhóm ứng cứu khẩn cấp máy tính ASEAN. ASEAN CERT đóng vai trò quan trọng trong việc hỗ trợ triển khai khung Thoả thuận An ninh mạng ASEAN, góp phần xây dựng một không gian mạng an toàn và bền vững trong khu vực.

chiến lược toàn diện (CSP) là một bước đệm quan trọng để đẩy mạnh hợp tác trong lĩnh vực an ninh mạng. Điều này không chỉ giúp tăng cường an ninh mạng cho khu vực mà còn thúc đẩy mối quan hệ kinh tế song phương giữa Hàn Quốc và khu vực Đông Nam Á (ASEAN Secretariat 2021).

Các hoạt động của cơ quan KISA cũng đóng một vai trò quan trọng trong hợp tác an ninh mạng quốc tế của Hàn Quốc. Trung tâm Điều phối Ứng cứu Khẩn cấp Máy tính Hàn Quốc (KrCERT/CC-KOREA Computer Emergency Response Team Coordination Center) trực thuộc KISA, hoạt động như một nhóm ứng phó sự cố an ninh mạng quốc gia (National CSIRT) và là điểm liên lạc trung tâm cho Hàn Quốc trong việc xử lý các sự cố an ninh mạng quốc tế. KrCERT/CC hợp tác với Cơ quan Tình báo Quốc gia (NIS) và khu vực tư nhân trong nước, cũng như với các nhóm ứng phó sự cố an ninh mạng quốc gia khác và các nhà cung cấp an ninh mạng toàn cầu. KrCERT/CC là thành viên của Hiệp hội các tổ chức ứng cứu khẩn cấp sự cố máy tính - mạng của các quốc gia thuộc khu vực châu Á - Thái Bình Dương [14] (APCERT 2024; KISA & MIST 2023).

Quan hệ đối tác giữa Hàn Quốc và Việt Nam đã được nâng cấp lên thành Đối tác Chiến lược Toàn diện vào năm 2022 (Cổng Thông tin điện tử Chính phủ 2022). Hợp tác song phương hai nước đang mở rộng sang các lĩnh vực tăng trưởng trong tương lai, bao gồm các ngành công nghiệp tiên tiến, khoa học và công nghệ, thông tin và truyền thông, và tăng trưởng xanh. Ở cấp cơ quan chính phủ, năm 2019 Bộ Khoa học và Công nghệ thông tin Hàn Quốc đã ký kết biên bản ghi nhớ hợp tác với Bộ Thông tin và Truyền thông Việt Nam. Theo đó, Hàn Quốc và Việt Nam sẽ cùng triển khai các hoạt động hợp tác rộng lớn về công nghiệp công nghệ thông tin và truyền thông, trong đó có an ninh mạng. Ngoài ra, Cục an toàn thông tin thuộc Bộ Thông tin và Truyền thông Việt Nam và KISA Hàn Quốc cũng đã ký biên bản ghi nhớ hợp tác, thoả thuận về việc tập trung cụ thể vào hợp tác an ninh mạng, bao gồm chia sẻ thông tin về các mối đe doạ, xây dựng năng lực và hỗ trợ kỹ thuật (Bộ Khoa học và Công nghệ 2020).

Từ việc hợp tác với cường quốc như Hoa Kỳ để chuyển đổi sang mô hình phòng thủ chủ động, cho đến các sáng kiến cấp khu vực với ASEAN, Hàn Quốc đã khẳng định vai trò là một đối tác đáng tin cậy. Các cơ chế hợp tác từ hội nghị cấp bộ trưởng, đối thoại chiến lược, đến các chương trình đào tạo kỹ thuật như cuộc thi ACS và sự tham gia của các tổ chức chuyên biệt như KISA, đều minh chứng cho một cam kết mạnh mẽ của Hàn Quốc. Đặc biệt, việc nâng cấp quan hệ với Việt Nam lên đối tác chiến lược toàn diện và các biên bản ghi nhớ giữa các cơ quan chính phủ đã tạo ra một khuôn khổ vững chắc, mở rộng hợp tác sang các lĩnh vực tiên tiến, bao gồm cả an ninh mạng. Những nỗ lực này không chỉ nâng cao năng lực phòng thủ cho hai quốc gia Việt Nam – Hàn Quốc mà còn góp phần xây dựng một không gian mạng an toàn và ổn định hơn cho toàn khu vực.

4. Yếu tố ảnh hưởng tới hợp tác trong lĩnh vực an ninh mạng giữa Hàn Quốc và đối tác

Hệ thống pháp lý là nền tảng chi phối mọi hoạt động hợp tác an ninh mạng quốc tế. Các quốc gia trong khu vực, bao gồm Hàn Quốc và các nước Đông Nam Á như Việt Nam, Singapore, Thái Lan, đều đã ban hành hoặc sửa đổi các luật để tăng cường bảo vệ dữ liệu cá nhân và an ninh của các hệ thống thông tin, cơ sở hạ tầng quan trọng. Các luật này đều có các quy định về chống

[14] APCERT – Asia Pacific Computer Security Incident Response Teams

tội phạm mạng và bảo vệ thông tin công dân. Tất cả các nước đều nhận thức được sự gia tăng của các mối đe dọa mạng như ransomware, gián điệp mạng và các cuộc tấn công có chủ đích từ các nhóm tội phạm hoặc được nhà nước bảo trợ. Điểm chung trong khung pháp lý của các quốc gia kể trên đều hướng đến việc phòng ngừa, phát hiện và ứng phó với các mối đe dọa này. Tuy nhiên, vẫn tồn tại sự khác biệt trong cách tiếp cận lập pháp giữa Hàn Quốc và các quốc gia Đông Nam Á có thể khái quát thành hai mô hình chính.

Mô hình pháp lý "Đơn nhất – Toàn diện" là lựa chọn của nhiều quốc gia Đông Nam Á, phản ánh nhu cầu cấp bách trong bối cảnh số hoá bùng nổ (Lim and Alfred 2024). Có thể kể tên một vài văn bản luật tại một số quốc gia trong khu vực Đông Nam Á như sau: Trong cùng năm 2018, Việt Nam ban hành Luật An ninh mạng, Singapore thông qua Đạo luật An ninh mạng (Cybersecurity Act). Bên cạnh Đạo luật An ninh mạng được ban hành vào năm 2019, Thái Lan cũng đã thông qua Đạo luật bảo vệ dữ liệu cá nhân – Personal Data Protection Act. Trong hai năm 2023, 2024, Malaysia và Brunei đã thông qua Đạo luật An ninh mạng. Cũng là một quốc gia trong khu vực Đông Nam Á, Philippines đã thông qua Đạo luật phòng chống tội phạm mạng – Cybercrime Prevention Act từ 2012… (Brock 2024). Qua tổng hợp, có thể thấy các hành lang pháp lý của Việt Nam, Singapore hay Malaysia, Brunei thường được xây dựng nhằm mục tiêu kép: quản lý hạ tầng thông tin quan trọng và tập trung hoá thẩm quyền quản lý về an ninh mạng vào một cơ quan chủ đạo nhằm đảm bảo sự thống nhất và tập trung trong quản lý (KISA & MIST 2023). Tuy nhiên, khi đặt lên cán cân so sánh có thể thấy, các quy định về dữ liệu ở Đông Nam Á còn có sự khác biệt lớn giữa các quốc gia. Chẳng hạn, Việt Nam nhấn mạnh vào an ninh quốc gia, trong khi Philippines lại ưu tiên quy trình kinh doanh và cho phép truyền dữ liệu xuyên biên giới tự do hơn (CSIS 2023). Sự thiếu hài hòa trong các quy định này làm phức tạp hóa các nỗ lực hợp tác khu vực.

Ngược lại, Hàn Quốc sở hữu một hệ thống luật an ninh mạng và bảo vệ thông tin cá nhân đã được thiết lập từ lâu và có cấu trúc phức tạp có thể được coi là mô hình "Đa luật – Nhiều trụ cột". Thay vì một đạo luật bao trùm, Hàn Quốc quản lý an ninh mạng thông qua các luật riêng biệt theo chức năng và ngành dọc, điển hình như "Đạo luật bảo vệ thông tin cá nhân" hay các quy định an ninh đặc thù cho ngành tài chính (Shin 2021). Mới đây, Hàn Quốc cũng đã sửa đổi các quy định để có các biện pháp phòng thủ mạng chủ động hơn (MSIT & NIS 2024). Sự khác biệt căn bản giữa mô hình tập trung quyền lực (Đông Nam Á) và phân tách chức năng (Hàn Quốc) tạo ra thách thức trong việc đồng bộ hoá các tiêu chuẩn kỹ thuật và quy trình báo cáo, chia sẻ thông tin khi hai bên tiến hành hợp tác chiến lược đòi hỏi các đối tác phải tìm kiếm giải pháp tương thích linh hoạt.

Mặc dù tồn tại sự khác biệt về pháp lý, hợp tác Hàn Quốc – Đông Nam Á vẫn được thúc đẩy bởi nhiều yếu tố cấu trúc thuận lợi. Đầu tiên, thế mạnh công nghệ và kinh nghiệm của Hàn Quốc là không thể phủ nhận. Với năng lực công nghệ hàng đầu và kinh nghiệm thực chiến quý báu trong việc đối phó với các cuộc tấn công quy mô lớn, Hàn Quốc đáp ứng trực tiếp nhu cầu cấp bách của ASEAN về chuyển giao công nghệ và xây dựng năng lực phòng thủ. Cách tiếp cận "phát triển" của Hàn Quốc, cùng với năng lực công nghệ và sự hiện diện kinh tế mạnh mẽ trong khu vực tạo ra động lực kinh tế và cơ hội xây dựng năng lực đáng kể. Thứ hai, môi trường chính sách tạo ra cơ sở chính sách vững chắc và nguồn tài trợ ổn định cho các chương trình hợp tác khu vực như ASEAN Cyber Shield (AKCF 2023).

Cuối cùng, các nước Đông Nam Á có nền kinh tế số đang phát triển mạnh mẽ, thu hút đầu tư lớn từ các tập đoàn công nghệ Hàn Quốc cũng đang phải đối mặt với các lỗ hổng an ninh mạng. Nhu cầu bảo vệ các khoản đầu tư và cơ sở hạ tầng số này tạo ra động lực kinh tế mạnh mẽ cho việc hợp tác, hình thành nhu cầu mang tính ràng buộc lẫn nhau để bảo vệ chuỗi cung ứng kỹ thuật số chung (Bimantara 2021; Rahman 2025).

Bên cạnh những yếu tố thuận lợi, vẫn tồn tại những khó khăn ảnh hưởng tới việc thúc đẩy hợp tác Hàn Quốc và khu vực Đông Nam Á trong lĩnh vực an ninh mạng.

Thứ nhất là sự khác biệt về mục tiêu trong hệ thống luật định. Sự khác biệt về mục tiêu cốt lõi của luật an ninh mạng (ưu tiên an ninh quốc gia so với quyền riêng tư cá nhân) tạo ra một trở ngại lớn đặc biệt làm tăng chi phí vận hành cho các doanh nghiệp công nghệ quốc tế (Lewis 2023: 4-5). Sự khác biệt này được thể hiện rõ qua yêu cầu lưu trữ dữ liệu tại chỗ được quy định tại Điều 26 Nghị định 53/2022/NĐCP của Việt Nam, nhằm đảm bảo chủ quyền số và an ninh quốc gia. Ngược lại, khung pháp lý của Hàn Quốc – điển hình là Luật Bảo vệ thông tin cá nhân [개인정보 보호법] chú trọng tới quyền tự quyết chia sẻ thông tin cá nhân và thúc đẩy lưỡng dữ liệu tự do để phát triển kinh tế số.

Thứ hai là thiếu sự đồng bộ trong quy định. Sự đa dạng về quy định giữa các quốc gia Đông Nam Á khiến việc thiết lập một khung hợp tác chung trở nên phức tạp. Sự thiếu đồng bộ này được minh chứng qua khoảng cách lớn trong chỉ số An ninh mạng toàn cầu của ITU. Trong khi Singapore thường xuyên nằm trong nhóm dẫn đầu về hạ tầng và luật định, các quốc gia như Việt Nam hay Malaysia lại đang ở các giai đoạn hoàn thiện pháp lý khác nhau với ưu tiên riêng biệt về kiểm soát nội dung và hạ tầng. Theo báo cáo của ERIA15 (2023), việc thiếu một khung quản trị dữ liệu chung là rào cản khiến Hàn Quốc phải duy trì phương pháp tiếp cận hợp tác song phương thay vì phương pháp đa phương.

Những khó khăn tiếp theo có thể kể đến là khoảng cách về năng lực kỹ thuật, cơ sở hạ tầng, sự thiếu hụt nhân lực chuyên môn và các yếu tố địa chính trị phức tạp. Mô hình 5 cấp độ mới của GCI là một minh chứng cho thấy tồn tại sự khác biệt về mức độ phát triển an ninh mạng giữa các quốc gia trong khu vực Đông Á (ITU 2024: 26). "Khoảng cách kỹ thuật số" tồn tại trên khắp Đông Á, với các mức độ tiến bộ công nghệ và cơ sở hạ tầng khác nhau giữa các quốc gia như Nhật Bản, Hàn Quốc và Singapore so với Brunei, Campuchia, Lào, Myanmar và Việt Nam (Thomas 2009). Trong khi Hàn Quốc là một trong những quốc gia tiên tiến nhất về công nghệ số, nhiều nước Đông Nam Á, đặc biệt là các quốc gia đang phát triển, vẫn phải đối mặt với cơ sở hạ tầng cũ kỹ và mức độ nhận thức về an ninh mạng còn hạn chế. Sự chênh lệch này khiến việc chia sẻ các giải pháp kỹ thuật phức tạp hoặc thiết lập các tiêu chuẩn đồng nhất trở nên khó khăn.

Khu vực Đông Nam Á đang đối mặt với tình trạng thiếu hụt trầm trọng các chuyên gia an ninh mạng có tay nghề cao. Đặc biệt, sự thiếu hụt chuyên gia an ninh mạng đang làm gia tăng khoảng cách kỹ thuật số và trở thành một rào cản lớn đối với an ninh mạng và tăng trưởng kỹ thuật số, đặc biệt đối với các quốc gia đang phát triển nói chung và với khu vực Đông Á nói riêng (WorldBank 2023: 4).

Mặc dù Hàn Quốc có thể cung cấp các chương trình đào tạo, nhưng việc đáp ứng nhu cầu khổng lồ về nhân lực cho toàn khu vực là một thách thức lớn. Ngoài ra, khu vực Đông Á và Đông Nam Á là nơi chịu ảnh

[15] Economic Research Institute for ASEAN and East Asia – Viên nghiên cứu kinh tế Đông Nam Á và Đông Á.

hưởng của các cường quốc lớn như Trung Quốc và Mỹ. Sự cạnh tranh địa chính trị này có thể tác động đến việc lựa chọn công nghệ (ví dụ: công nghệ 5G từ các nhà cung cấp như Huawei) và các liên minh an ninh mạng, gây ra sự phân mảnh và làm phức tạp hóa nỗ lực hợp tác chung. Tóm lại, những khó khăn này đòi hỏi các quốc gia phải có một chiến lược hợp tác linh hoạt và phù hợp, không chỉ ở cấp độ khu vực mà còn ở cấp độ song phương.

5. Kết luận và kiến nghị

5.1. Kết luận

Trong bối cảnh các mối đe dọa an ninh mạng ngày càng gia tăng về cả tần suất và mức độ tinh vi, hợp tác quốc tế đã trở thành yếu tố then chốt để bảo vệ không gian kỹ thuật số, được minh chứng qua các nỗ lực toàn cầu như Công ước Hà Nội (tổ chức tại Việt Nam vào tháng 11 năm 2025). Nghiên cứu đã rút ra bốn luận điểm chính về bối cảnh hợp tác an ninh mạng Hàn Quốc – Đông Nam Á.

Thứ nhất, các cuộc tấn công mạng (như ransomware và gián điệp mạng) có tính chất xuyên biên giới và tác động đến mọi cấp độ phát triển số hoá, những rủi ro chung và nhu cầu hợp tác giữa các quốc gia.

Thứ hai, tồn tại sự khác biệt cấu trúc pháp lý giữa mô hình "Đơn nhất – Toàn diện" của Đông Nam Á (ưu tiên an ninh quốc gia, tập trung quyền lực) và mô hình "Đa luật – Nhiều trụ cột" của Hàn Quốc (chuyên ngành, phân tán chức năng), tạo ra cả thách thức trong đồng bộ hoá lẫn cơ hội học hỏi kinh nghiệm xây dựng chính sách.

Thứ ba, động lực hợp tác mạnh mẽ được tạo ra bởi thế mạnh công nghệ và cách tiếp cận "phát triển" của Hàn Quốc cùng với nhu cầu xây dựng năng lực cấp thiết của Đông Nam Á và nhu cầu bảo vệ các khoản đầu tư kinh tế số chung.

Cuối cùng, thách thức lớn nhất đối với sự hợp tác là "khoảng cách kỹ thuật số" và tình trạng thiếu hụt trầm trọng chuyên gia an ninh mạng trong khu vực. Đây sẽ là rào cản đối với nỗ lực thiết lập các tiêu chuẩn và giao thức chung.

Lập trường an ninh mạng mạnh mẽ của Hàn Quốc được xây dựng dựa trên sự hiệp đồng giữa đổi mới tiên phong trong nước (như AhnLab V3) và một chiến lược quốc gia chủ động, định hình Hàn Quốc trở thành một hình mẫu về khả năng phục hồi mạng trong thế kỷ XXI.

5.2. Kiến nghị chính sách trọng tâm cho hợp tác Việt Nam – Hàn Quốc

Trên cơ sở các luận điểm nêu trên, đặt trong bối cảnh Việt Nam – Hàn Quốc là đối tác chiến lược toàn diện của nhau, sự hợp tác an ninh mạng giữa Việt Nam và Hàn Quốc cần tập trung vào các lĩnh vực mang tính thực tiễn cao:

Đầu tiên, cần tập trung vào việc chia sẻ kinh nghiệm xây dựng chính sách, quy định và tiêu chuẩn kỹ thuật thay vì chỉ chia sẻ văn bản luật. Hàn Quốc có thể hỗ trợ Việt Nam bằng cách chuyển giao kinh nghiệm thực thi và các hệ thống thiết chế (cách vận hành của NIS, KISA, KrCERT/CC) đã được kiểm chứng qua thực tiễn, thay vì chỉ dựa trên một đạo luật thống nhất. Hợp tác nên ưu tiên xây dựng tiêu chuẩn kỹ thuật và quy trình vận hành Trung tâm ứng cứu khẩn cấp máy tính (CERT/CC), đặc biệt tập trung vào bảo vệ hạ tầng thông tin quan trọng trong các lĩnh vực viễn thông, tài chính – ngân hàng và cơ sở dữ liệu chính phủ. Việc này không chỉ giúp Việt Nam củng cố hành lang pháp lý (như Luật An ninh mạng 2018) mà còn tạo ra một môi trường đầu tư rõ ràng và đáng tin cậy.

Tiếp theo, để đối phó với các mối đe doạ tinh vi như APT và ransomware, cần đẩy mạnh nghiên cứu và phát triển (R&D) cũng như các giải pháp phòng thủ nâng cao có mục tiêu. Hàn Quốc có thể tăng cường đào tạo chuyên sâu về phòng thủ nâng cao và triển khai các dự án thí điểm về phòng thủ nâng cao cho các hệ thống dữ liệu chính phủ điện tử tại một hoặc hai địa phương/ngành trọng điểm của Việt Nam để chứng minh tính hiệu quả. Ngoài ra, việc thiết lập các phòng nghiên cứu chung và tổ chức cuộc thi Hackathon chuyên biệt về Trí tuệ nhân tạo trong an ninh mạng sẽ giúp hai quốc gia cùng đối phó với các mối đe doạ mới do AI điều khiển và xây dựng năng lực trong lĩnh vực công nghệ mũi nhọn này.

Cuối cùng, giải quyết bài toán thiếu hụt nhân lực là ưu tiên hàng đầu. Việt Nam rất cần sự hỗ trợ từ Hàn Quốc trong việc xây dựng nguồn chất lượng cao dài hạn thông qua việc mở rộng chương trình học bổng, trao đổi giảng viên/chuyên gia để hỗ trợ thành lập các trung đào tạo về an ninh mạng tại các trường đại học tại Việt Nam. Những nỗ lực này sẽ góp phần tạo ra một thế hệ chuyên gia an ninh mạng tài năng, sẵn sàng bảo vệ không gian kỹ thuật số của Việt Nam trong tương lai và giảm bớt khoảng cách kỹ thuật số hiện có trong khu vực Đông Á.

* Kết quả nghiên cứu thuộc Dự án "Hàn Quốc học tại miền Bắc Việt Nam: chia sẻ và phát triển" trong Chương trình Hạt giống Hàn Quốc học do Viện nghiên cứu Hàn Quốc học trung ương tài trợ. Mã số AKS-2022-INC-22500XX.

Tài liệu trích dẫn

ASEAN – Korea Cooperation Fund (AKCF). 2023. *ASEAN Cyber Shield: Building a Resilient Cyber Ecosystem in ASEAN*. Jakarta: AKCF.

ASEAN Secretariat. 2021. *ASEAN Cybersecurity Cooperation Strategy 2021-2025*. Jakarta: ASEAN Secretariat.

Asia Pacific Computer Emergency Response Team (APCERT). 2024. *APCERT Annual Report 2023*. Tokyo:APCERT.

Australian Strategic Policy Institute (ASPI). 2024. *Cyber Maturity in the Indo-Pacific 2024*. Canberra:ASPI.

Azza Bimantara. 2021. "The Normative Enactment of International Cybersecurity Capacity Building Assistance: A Comparative Analysis on Japanese and South Korean Practices". Master thesis, University of Muhammadiyah Malang, Indonesia.

Báo Nhân Dân. 2023. "Thủ tướng chủ trì họp Ban chỉ đạo an toàn, An ninh mạng quốc gia lần thứ 2". Truy cập ngày 23 tháng 6 năm 2025. https://nhandan.vn/anh-thu-tuong-chu-tri-hop-ban-chi-dao-an-toan-an-ninh-mang-quoc-gia-lan-thu-hai-post769267.html

Bộ Khoa học và Công nghệ. 2020. "Việt Nam và Hàn Quốc đẩy mạnh hợp tác trong lĩnh vực ICT". Truy cập ngày 23 tháng 6 năm 2025. https://mst.gov.vn/viet-nam-han-quoc-tang-cuong-hop-tac-trong-linh-vuc-ict-197140722.htm

Boannews. 2013. "6.25 사이버 공격 배후는 '다크서울'". (Kẻ đứng sau cuộc tấn công mạng 25/6 là 'Dark Seoul'). Truy cập ngày 23 tháng 6 năm 2025. https://www.boannews.com/media/view.asp?idx=36706&kind=1

Center for Strategic and International Studies (CSIS). 2023. *Cloud Computing in Southeast Asia and Digital Competition*. Washington, DC

Chính phủ. 2022. "Nghị định Quy định chi tiết một số điều của Luật An ninh mạng". Văn bản chính phủ. Truy cập 29 tháng 6 năm 2025. https://vanban.chinhphu.vn/?pageid=27160&docid=206381

Chosun. 2022. " 사이버안보, 민-관-군 협력 대응 국정원이 만든 사이버안보협력센터 가보니". (An ninh mạng, phản ứng hợp tác Công – Tư – Quân đội: Chuyến thăm Trung tâm Hợp tác An ninh mạng do Viện Tình báo Quốc gia thành lập). Truy cập 29 tháng 6 năm 2025. https://biz.chosun.com/it-science/ict/2022/12/22/TUF3TASXXZELNBDYJGQ3UP7NBE/

Cổng thông tin điện tử chiến lược quốc gia -thư viện quốc hội Hàn Quốc. 2025. "Chiến lược kỹ thuật số quốc gia". Truy cập 23 tháng 6 năm 2025. https://nsp.nanet.go.kr/plan/subject/detail.do?nationalPlanControlNo=PLAN0000040705

Cổng Thông tin điện tử Chính phủ. 2022. "Tuyên bố chung về quan hệ Đối tác chiến lược toàn diện giữa nước Cộng hòa xã hội chủ nghĩa Việt Nam và Đại dân quốc Hàn Quốc" Truy cập ngày 23 tháng 6 năm 2025. https://baochinhphu.vn/tuyen-bo-chung-ve-quan-he-doi-tac-chien-luoc-toan-dien-giua-viet-nam-va-han-quoc-102221205164010363.htm

Lavrova, Darya. 2025. *Cybersecurity threatscape in Southeast Asia*. Report of PT Cyber Analytics.

Economic Research Institute for ASEAN and East Asia (ERIA). 2023. *ASEAN Digital Community 2045*. Jakarta

Felix Kim. 2025. "Seoul mobilizes national cyber defenses amid surge in AI-driven attacks". Presented at Indo-Pacific Defense FORUM.

Homepage của công ty Ahnlab – Hàn Quốc. Truy cập ngày 29 tháng 6 năm 2025 https://www.ahnlab.com/en/overseas/company/about

International Telecommunication Union (ITU). 2024. *Global Cybersecurity Index 2024*. Geneva.

James A.Lewis. 2023. "Cloud Computing in Southeast Asia and Digital Competition with China", *CSIS*. Truy cập ngày 29 tháng 6 năm 2025. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-08/230807_Lewis_Cloud_SEAsia.pdf?VersionId=d6O9MUjrkssGTGVKCmqcpJL7T8ISRei1

Julia Brock. 2024. "ASEAN's cyber Initiatives: A select list". *Center for strategic & International Studies.*

Kim Seunghwan. 2025. "Fortifying South Korea's Nontraditional Security Addressing Cybersicurity and Economic Vulnerabilities", *Kenney papers on Indo -Pacific Security studies.* No11. 2025, Air University Press.

So Jeong, Kim. 2024. "ROK's New National Cybersecurity Strategy and Its Implication", *INSS Issue Brief Vol 106, No 3.*

KISA & MSIT. 2023. *National Cyberscecurity White Paper*. Korea.

KISA & MSIT. 2024. *National Cyberscecurity White Paper*. Korea.

Korea International Cooperation Agency (KOICA). 2023. *KOICA Annual report 2022: Partnering for a Better Future*. Seongnam. Korea.

Korea Internet & Security Agency (KISA). 2023. *KrCERT/CC: National Cybersecurity Incident Response Operations*. Korea: Naju.

Lim, Chong Kin and David N. Alfred. 2024. *Data Protection and Cybersecurity Regulation in Southeast Asia*. Singapore: Drew & Napier LLC.

M.Faizal bin Abdul Rahman. 2025. "Geopolitical Challenges to the Cybersecurity Goals of the ASEAN 2045 Vision". Truy cập ngày 29 tháng 6 năm 2025. https://moderndiplomacy.eu/2025/06/15/geopolitical-challenges-to-the-cybersecurity-goals-of-the-asean-2045-vision/

Ministry of Science and ICT (MSIT) and National Intelligence Service (NIS). 2024. *2024 National Cybersecurity White Paper*. Seoul

National Policy Agency. 2022. *Police Agency of Japan (NPA)*. Tokyo: National Policy Agency

Nicholas Thomas. 2009. "Cyber Security in East Asia: Governing Anarchy", *Asian Security*, 5:1, 3-23.

Park Joohui and Kim Donghee . 2025. "South Korea's Proactive Cyber Defense and Strategy Cooperation with the United States. Forging Forward". Presented in Center for Strategic and International Studies.

Shin Yong Joong. 2021. *Data Protection Law in South Korea*. Cham, Switzerland: Springer Nature. https://doi.org/10.4258/hir.2021.27.1.1

Tạp chí Khoa học & Công nghệ. 2023."Tấn công mạng vào Nhật Bản tăng vọt khi tin tặc "nắm thóp" lỗ hổng của các đơn vị". Truy cập ngày 23 tháng 7 năm 2025. https://ictvietnam.vn/tan-cong-mang-vao-nhat-ban-tang-vot-khi-tin-tac-nam-thop-lo-hong-cua-cac-don-vi-55409.html

Tạp chí Khoa học & Công nghệ Việt Nam. 2024. "Các cuộc tấn công mạng ngày càng tinh vi và phức tạp hơn". Truy cập ngày 28 tháng 6 năm 2025.https://ictvietnam.vn/print/67939.html

Tạp chí Thông tin Truyền thông. 2025. "Việt Nam là trung tâm công nghệ đang nổi lên tại Đông Nam Á". Truy cập ngày 29 tháng 6 năm 2025. https://ictvietnam.vn/viet-nam-la-trung-tam-cong-nghe-dang-noi-len-tai-dong-nam-a-69025.html.

The Korea Harald. 2025. “Nearly 27 million mobile fingerprints leaked in SK Telecom data breach”. Truy cập 23 tháng 6 năm 2025. https://www.koreaherald.com/article/10490627

The World Bank. 2023. “ ‘Hacking’ The CyberSecurity skills gap in developing countries”. *Pratitioner note*. Washington, DC: World Bank Group.

Trịnh Viết Dũng. 2024. “Vietnam’s struggle with cyber security”, *East Asia forum*. https://doi.org/10.59425/eabc.1710972000.

국가법령정보센터.2025. (Trung tâm thông tin quy định pháp luật quốc gia Hàn Quốc). Truy cập ngày 23 tháng 6 năm 2025. . https://www.law.go.kr/

국토교통부. 2016. 국가전략 프로젝트로. ”세계 선도형 스마트 시티 구축사업’선정.한국. 국토부-국가전략-프로젝트로-세계-선도형-스마트시/ (Bộ Giao thông, Đất đai và Hạ tầng Hàn Quốc. 2016. “Dự án chiến lược quốc gia. Lựa chọn “dự án xây dựng thành phố thông minh bậc nhất toàn cầu”). Truy cập 29 tháng 6 năm 2025. https://smartcity.go.kr/2016/08/10/

김성규. 2022. “국방 사이버 분야 국제협력 방안 연구”. *국외 장기훈련 결과보고서.* (Kim Seung Gyu. 2022. “Nghiên cứu đề xuất hợp tác quốc tế trong lĩnh vực an ninh mạng”. Báo cáo tại hội thảo tập huấn nước ngoài, Bộ Quốc phòng Hàn Quốc)

한국일보. 2025.“두 달 가입자 50 만 잃은 SKT, ‘위약금 면제’여파는?”. (Nhật báo Hàn Quốc. “Mất nửa triệu thuê bao sau 2 tháng, SKT lao đao vì chính sách miễn phí huỷ hợp đồng”). Truy cập ngày 23 tháng 07 năm 2025. https://www.hankookilbo.com/News/Read/A20250621122400050 01?did=NA