

THỦ TƯỚNG CHÍNH PHỦ CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 1875/QĐ-TTg

Hà Nội, ngày 30 tháng 9 năm 2026

QUYẾT ĐỊNH

Ban hành Khung kiến trúc an ninh mạng quốc gia (Phiên bản 1.0)

THỦ TƯỚNG CHÍNH PHỦ

Căn cứ Luật Tổ chức Chính phủ ngày 18 tháng 02 năm 2025;

Căn cứ Luật Tổ chức chính quyền địa phương ngày 16 tháng 6 năm 2025;

Căn cứ Luật An ninh mạng ngày 10 tháng 12 năm 2025;

Căn cứ Luật Bảo vệ dữ liệu cá nhân ngày 26 tháng 6 năm 2025;

Căn cứ Luật Dữ liệu ngày 30 tháng 11 năm 2024;

Căn cứ Luật Giao dịch điện tử ngày 22 tháng 6 năm 2023;

Căn cứ Luật Chuyển đổi số ngày 11 tháng 12 năm 2025;

Căn cứ Nghị định số 331/2026/NĐ-CP ngày 19 tháng 8 năm 2026 của Chính phủ về bảo vệ an ninh mạng đối với hệ thống thông tin;

Căn cứ Nghị quyết số 57-NQ/TW ngày 22 tháng 12 năm 2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia;

Căn cứ Nghị quyết số 11/NQ-CP ngày 14 tháng 01 năm 2026 của Chính phủ sửa đổi, bổ sung, cập nhật Nghị quyết số 71/NQ-CP ngày 01 tháng 4 năm 2025 của Chính phủ sửa đổi, bổ sung cập nhật Chương trình hành động của Chính phủ thực hiện Nghị quyết số 57-NQ/TW ngày 22 tháng 12 năm 2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia;

Căn cứ Quyết định số 1425/QĐ-TTg ngày 29 tháng 7 năm 2026 của Thủ tướng Chính phủ ban hành Khung kiến trúc tổng thể quốc gia số (phiên bản 1.0);

Theo đề nghị của Bộ trưởng Bộ Công an.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Khung kiến trúc an ninh mạng quốc gia (Phiên bản 1.0).

Điều 2. Tổ chức thực hiện

1. Bộ Công an chủ trì, phối hợp với Bộ Khoa học và Công nghệ, Ban Cơ yếu Chính phủ và các bộ, cơ quan liên quan hướng dẫn, đôn đốc, giám sát, đánh giá việc áp dụng Khung kiến trúc an ninh mạng quốc gia trên phạm vi toàn quốc; chủ trì hoạch định, xây dựng hệ thống tiêu chuẩn, quy chuẩn kỹ thuật quốc gia và hướng dẫn kỹ thuật về an ninh mạng; công bố trên Hệ thống quản lý kiến trúc số quốc gia; chủ trì rà soát, đề xuất Thủ tướng Chính phủ xem xét, bổ sung các nền tảng an ninh mạng dùng chung quốc gia vào danh mục nền tảng số dùng chung quốc gia theo quy định.

2. Bộ Khoa học và Công nghệ có trách nhiệm phối hợp với Bộ Công an bảo đảm tính tương thích, liên thông và đồng bộ các tiêu chuẩn kỹ thuật an ninh mạng của các nền tảng, cơ sở dữ liệu dùng chung thuộc Khung kiến trúc tổng thể quốc gia số; chủ trì hướng dẫn phương pháp đánh giá, giám sát mức độ tuân thủ Khung kiến trúc tổng thể quốc gia số theo quy định của pháp luật, trong đó Bộ Công an chủ trì nội dung liên quan đến an ninh mạng theo quy định tại điểm a khoản 3 Điều 2 Quyết định số 1425/QĐ-TTg; tổng hợp, cập nhật thông tin liên quan trên Hệ thống quản lý kiến trúc số quốc gia.

3. Ban Cơ yếu Chính phủ có trách nhiệm quản lý, hướng dẫn tiêu chuẩn mật mã cơ yếu và chữ ký số chuyên dùng công vụ áp dụng trong Khung kiến trúc an ninh mạng quốc gia; triển khai sản phẩm mật mã cơ yếu và hệ thống thông tin cơ yếu để bảo vệ bí mật nhà nước; bảo đảm an ninh mạng theo cấp độ đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ theo quy định tại khoản 3 Điều 34 Nghị định số 331/2026/NĐ-CP.

4. Bộ Quốc phòng có trách nhiệm tham khảo, áp dụng Khung kiến trúc này hoặc xây dựng Khung kiến trúc an ninh mạng chuyên biệt áp dụng đối với các hệ thống thông tin quân sự, cơ yếu thuộc phạm vi quản lý.

5. Bộ Tài chính có trách nhiệm chủ trì, phối hợp với Bộ Công an hướng dẫn cơ chế bố trí, sử dụng kinh phí chi thường xuyên và kinh phí đầu tư phục vụ triển khai Khung kiến trúc an ninh mạng quốc gia, trong đó có kinh phí duy trì hạ tầng phục vụ hoạt động của hệ thống Cảm biến giám sát đặt tại các bộ, ngành, địa phương.

6. Bộ Nội vụ có trách nhiệm hướng dẫn việc sử dụng kết quả nhóm chỉ số an ninh mạng làm một trong các nội dung đánh giá, xếp loại chất lượng hằng năm đối với người đứng đầu cơ quan, tổ chức theo quy định của pháp luật về cán bộ, công chức.

7. Các bộ, cơ quan ngang bộ, Ủy ban nhân dân các tỉnh, thành phố có trách nhiệm:

a) Tham khảo, đối chiếu với các định hướng và yêu cầu tại Khung kiến trúc an ninh mạng quốc gia, trong đó xem xét việc kết nối, chia sẻ dữ liệu giám sát an ninh mạng theo hướng dẫn của Bộ Công an; ưu tiên khai thác, sử dụng các thành phần an ninh mạng dùng chung đã được cung cấp nhằm hạn chế đầu tư trùng lặp; đồng thời tham chiếu các tiêu chuẩn, quy chuẩn kỹ thuật về kết nối và các yêu cầu về bảo đảm an ninh mạng theo cấp độ hệ thống thông tin được đề cập tại Khung kiến trúc an ninh mạng quốc gia;

b) Tham khảo mô hình kiến trúc bốn lớp và các mô hình kiến trúc tham chiếu tại Khung kiến trúc an ninh mạng quốc gia làm cơ sở xây dựng, cập nhật thành phần an ninh mạng trong Khung kiến trúc số của cơ quan, tổ chức mình đối với các hệ thống thông tin nội bộ, mạng dùng riêng phục vụ điều hành, tác nghiệp số; ưu tiên nguồn lực triển khai phân hệ giám sát nhằm chủ động ngăn chặn rủi ro tấn công từ nội bộ.

8. Các tổ chức, doanh nghiệp trực tiếp quản lý, vận hành hệ thống thông tin quan trọng về an ninh quốc gia có trách nhiệm tuân thủ các yêu cầu bắt buộc quy định tại điểm a khoản 7 Điều này; chủ động bố trí nguồn lực đầu tư các thành phần an ninh mạng tại chỗ theo yêu cầu tối thiểu tương ứng với cấp độ hệ thống thông tin; phối hợp với Bộ Công an trong công tác kết nối, giám sát và ứng phó sự cố an ninh mạng.

9. Đề nghị các cơ quan của Đảng, Quốc hội, Văn phòng Chủ tịch nước, Ủy ban Trung ương Mặt trận Tổ quốc Việt Nam, Tòa án nhân dân, Viện kiểm sát nhân dân nghiên cứu, chỉ đạo áp dụng Khung kiến trúc an ninh mạng quốc gia phù hợp với chức năng, nhiệm vụ và đặc thù tổ chức.

10. Kinh phí thực hiện Khung kiến trúc an ninh mạng quốc gia được bảo đảm từ nguồn ngân sách nhà nước theo phân cấp hiện hành, nguồn đầu tư của các doanh nghiệp cung cấp hạ tầng viễn thông, công nghệ thông tin và các nguồn vốn hợp pháp khác theo quy định của pháp luật.

11. Bộ Công an chủ trì rà soát, cập nhật Khung kiến trúc an ninh mạng quốc gia định kỳ hoặc khi cần thiết, trình Thủ tướng Chính phủ xem xét, quyết định; định kỳ hằng năm hoặc khi được yêu cầu, tổng hợp, báo cáo Thủ tướng Chính phủ tình hình triển khai.

Điều 3. Hiệu lực và trách nhiệm thi hành

1. Quyết định này có hiệu lực thi hành kể từ ngày ký ban hành.

2. Các Bộ trưởng, Thủ trưởng cơ quan ngang bộ, Chủ tịch Ủy ban nhân dân các tỉnh, thành phố và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này

Nơi nhận:

- Ban Bí thư Trung ương Đảng;
- Thủ tướng, các Phó Thủ tướng Chính phủ;
- Các bộ, cơ quan ngang bộ;
- UBND các tỉnh, thành phố;
- Văn phòng Trung ương và các Ban của Đảng;
- Văn phòng Tổng Bí thư;
- Văn phòng Chủ tịch nước;
- Hội đồng Dân tộc và các Ủy ban của Quốc hội;
- Văn phòng Quốc hội;
- Ủy ban Trung ương Mặt trận Tổ quốc Việt Nam;
- Cơ quan trung ương của các tổ chức chính trị - xã hội;
- VPCP: BTCN, các PCN, Trợ lý PTTg Hồ Quốc Dũng, các Vụ, Cục, Công báo;
- Lưu: VT, CDS (2)₄₄



**KT. THỦ TƯỚNG
PHÓ THỦ TƯỚNG**

Hồ Quốc Dũng



Phụ lục I

KHUNG KIẾN TRÚC AN NINH MẠNG QUỐC GIA

(Kèm theo Quyết định số 4875/QĐ-TTg

ngày 30 tháng 9 năm 2026 của Thủ tướng Chính phủ)

DANH MỤC TỪ VIẾT TẮT

TT	Từ và thuật ngữ viết tắt	Mô tả
1	AI	Trí tuệ nhân tạo
2	APT - Advanced Persistent Threat	Là thuật ngữ để mô tả một cuộc tấn công kỹ thuật cao, nhằm đánh vào những yếu điểm của hệ thống
3	CDN - Content Delivery Network	Mạng phân phối nội dung
4	CNTT	Công nghệ thông tin
5	CSDL	Cơ sở dữ liệu
6	DMZ	DMZ là một vùng mạng trung lập nằm giữa mạng nội bộ (LAN) và Internet
7	EDR - Endpoint Detection and Response	Phát hiện và ứng phó với mối đe dọa tại điểm cuối
8	IoC - Indicators of Compromise	Dấu vết tấn công hệ thống
9	LGSP - Local Government Service Platform	Nền tảng tích hợp, chia sẻ dữ liệu
10	NCIP	Định danh không gian mạng
11	NDXP	Nền tảng tích hợp, chia sẻ dữ liệu quốc gia
12	OSINT - Open Source Intelligence	Tình báo Nguồn mở
13	SIEM	Hệ thống quản lý sự kiện và thông tin bảo mật
14	SOAR	Điều phối, Tự động hóa và Phản ứng Bảo mật
15	SOP - Standard Operating Procedure	Quy trình thao tác chuẩn
16	TCVN	Tiêu chuẩn Việt Nam
17	TI - Threat Intelligence	Thông tin tình báo về mối đe dọa
18	TSLCD	Mạng truyền số liệu chuyên dùng
19	WAF - Web Application Firewall	Tường lửa ứng dụng web
20	WAN	Mạng diện rộng
21	ASM - Attack Surface Management	Nền tảng phát hiện tài sản và quản lý bề mặt tấn công
22	DDoS - Distributed Denial of Service	Tấn công từ chối dịch vụ phân tán

23	DNS - Domain Name System	Hệ thống phân giải tên miền
24	GenAI - Generative AI	Trí tuệ nhân tạo tạo sinh
25	IDS/IPS	Hệ thống phát hiện/ngăn chặn xâm nhập mạng
26	KPI - Key Performance Indicator	Chỉ số đo lường hiệu quả
27	MFA - Multi-Factor Authentication	Xác thực đa yếu tố
28	OT/ICS	Công nghệ vận hành/Hệ thống điều khiển công nghiệp
29	SDNS - Secure DNS	Hệ thống phân giải tên miền an toàn
30	SOC - Security Operations Center	Trung tâm điều hành, giám sát an ninh mạng
31	TIP - Threat Intelligence Platform	Nền tảng tri thức mối nguy an ninh mạng
32	VNeID	Ứng dụng định danh điện tử quốc gia
33	Zero Trust Architecture	Kiến trúc không tin cậy — xác minh liên tục, không mặc định tin tưởng
34	Big Data Analytics	Phân tích dữ liệu lớn
35	Data Poisoning	Đầu độc dữ liệu huấn luyện trí tuệ nhân tạo
36	Risk Score	Điểm số rủi ro an ninh mạng

I. KHÁI QUÁT CHUNG

Trong kỷ nguyên số, dữ liệu là tài nguyên quốc gia và hạ tầng số là huyết mạch của nền kinh tế. Song hành với quá trình chuyển đổi số quốc gia, Chính phủ đã ban hành Khung Kiến trúc tổng thể quốc gia số (được cập nhật, đồng bộ theo Luật Chuyển đổi số số 148/2025/QH15), xác lập mô hình tổng thể cho quốc gia số Việt Nam.

Hiện nay, chức năng quản lý nhà nước về an toàn thông tin mạng (trước đây thuộc Bộ Thông tin và Truyền thông) đã được chuyển giao và hợp nhất về Bộ Công an; đồng thời, Luật An ninh mạng số 116/2025/QH15 thống nhất sử dụng thuật ngữ “An ninh mạng” bao hàm cả nội hàm an toàn thông tin mạng. Theo đó, Bộ Công an chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về an ninh mạng đối với toàn bộ hệ thống chính trị. Khung kiến trúc này không áp dụng đối với hệ thống thông tin quân sự do Bộ Quốc phòng quản lý và hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ; ranh giới thẩm quyền quản lý về an ninh mạng giữa Bộ Công an và Bộ Quốc phòng thực hiện theo quy định tại khoản 4 Điều 6 Nghị định số 331/2026/NĐ-CP; Bộ Quốc phòng chịu trách nhiệm tham khảo, áp dụng Khung kiến trúc này hoặc xây dựng Khung kiến trúc an ninh mạng chuyên biệt đồng bộ đối với các hệ thống thông tin thuộc phạm vi quản lý. Đối với hệ thống thông tin có xử lý dữ liệu thuộc phạm vi bí mật nhà nước ngoài phạm vi nêu trên, việc kết nối, chia sẻ và trao đổi dữ liệu được thực hiện trên các hạ

tầng, mạng và hệ thống chuyên dùng theo quy định của pháp luật về bảo vệ bí mật nhà nước, an ninh mạng, cơ yếu và các quy định có liên quan, bảo đảm nguyên tắc tách biệt phù hợp với mức độ mật của dữ liệu.

Thực hiện nhiệm vụ cụ thể hóa Khung kiến trúc tổng thể quốc gia số và Chỉ thị 57-CT/TW của Ban Bí thư về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị; Chính phủ giao Bộ Công an xây dựng Khung kiến trúc an ninh mạng quốc gia. Đây là thành phần kiến trúc chạy xuyên suốt, bảo vệ cả 04 lớp của Khung kiến trúc tổng thể quốc gia số (Hạ tầng; Dữ liệu; Ứng dụng; Kênh tương tác).

1. Mục đích

Khung kiến trúc này được ban hành nhằm thiết lập quy hoạch tổng thể cấp quốc gia về công nghệ, dữ liệu và quy trình phòng thủ, cụ thể hóa các thành phần an ninh mạng dùng chung được quy định tại Khung kiến trúc tổng thể quốc gia số, phù hợp với nguyên tắc dùng chung, chia sẻ tài nguyên, tránh đầu tư thừa, trùng lặp quy định tại Điều 6 và Điều 30 Nghị định số 331/2026/NĐ-CP, bao gồm:

- Nền tảng điều hành an ninh mạng quốc gia: Giám sát, điều phối và chỉ huy ứng phó sự cố an ninh mạng thống nhất.
- Nền tảng phòng vệ mạng quốc gia: Hệ thống lá chắn bảo vệ biên giới số và các hệ thống trọng yếu.
- Hạ tầng bảo đảm an ninh, an toàn dữ liệu đầu cuối: bảo vệ thiết bị và người dùng cuối trong các cơ quan, tổ chức.
- Các hệ thống chuyên ngành an ninh mạng thuộc nhóm các nền tảng số dùng chung quốc gia.

Tài liệu này xác định rõ các thành phần an ninh mạng dùng chung trong toàn bộ hệ thống chính trị. Đây là căn cứ để các đơn vị, địa phương xây dựng, triển khai các giải pháp công nghệ thành phần, bảo đảm sự đồng bộ, thống nhất về tiêu chuẩn kết nối và dữ liệu.

2. Mục tiêu chiến lược

- Bảo vệ Hệ thống chính trị và Chủ quyền số: Xây dựng “tám khiên số” vững chắc, thông minh; hình thành hệ thống phòng thủ chủ động, có chiều sâu, bảo vệ toàn vẹn Khung kiến trúc tổng thể quốc gia số trước các nguy cơ tấn công mạng, gián điệp mạng và chiến tranh mạng.

- Triển khai hệ thống phòng thủ hiện đại, sát thực tế: Thiết lập các chuẩn mực công nghệ phòng thủ tiên tiến (như giám sát tự động, phân tích dữ liệu lớn, trí tuệ nhân tạo...) làm định hướng thống nhất. Mục tiêu là tháo gỡ khó khăn cho các đơn vị, địa phương trong việc xác định mô hình đầu tư; bảo đảm chuyển dịch từ việc mua sắm trang thiết bị rời rạc sang đầu tư vào năng lực phòng thủ thực chất, hiệu quả cao, tránh lãng phí nguồn lực do đầu tư công nghệ lạc hậu hoặc không phù hợp.

- Tối ưu hóa nguồn lực quốc gia: Triển khai các Nền tảng dùng chung do Bộ Công an quản lý để bảo đảm an ninh mạng cho hệ thống chính trị; giải quyết triệt để bài toán đầu tư dàn trải, manh mún và thiếu đồng bộ dữ liệu với các thành phần vệ tinh chưa được cung cấp tập trung, căn cứ điều kiện và nguồn lực của từng đơn vị, địa phương, có thể lựa chọn hình thức thuê dịch vụ công nghệ thông tin nhằm bảo đảm an ninh mạng thay cho việc tự đầu tư xây dựng và triển khai, phù hợp với quy định của pháp luật.

3. Phạm vi áp dụng

Khung kiến trúc an ninh mạng quốc gia quy định: (i) các yêu cầu cơ bản về kết nối, chia sẻ dữ liệu giám sát an ninh mạng, không đầu tư trùng lặp với thành phần an ninh mạng dùng chung đã được cung cấp, và các yêu cầu tối thiểu bảo đảm an ninh mạng theo cấp độ hệ thống thông tin; (ii) mô hình kiến trúc tham chiếu để các cơ quan, tổ chức sau xây dựng, cập nhật thành phần an ninh mạng trong Khung kiến trúc số của mình:

- Các bộ, cơ quan ngang bộ.
- Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương.
- Các tổ chức chính trị - xã hội sử dụng ngân sách nhà nước.
- Các tập đoàn, tổng công ty, doanh nghiệp nhà nước và đơn vị sự nghiệp công lập vận hành các hệ thống thông tin quan trọng về an ninh quốc gia.
- Các cơ quan của Đảng, Quốc hội, Văn phòng Chủ tịch nước, Ủy ban Trung ương Mặt trận Tổ quốc Việt Nam, Tòa án nhân dân, Viện kiểm sát nhân dân.

Yêu cầu kỹ thuật cụ thể về thành phần an ninh mạng theo từng cấp độ hệ thống thông tin thực hiện theo Nghị định số 331/2026/NĐ-CP và Tiêu chuẩn quốc gia TCVN 14423:2026 (An ninh mạng - Hệ thống thông tin - Yêu cầu cơ bản), không nhắc lại tại Khung kiến trúc an ninh mạng quốc gia. Trách nhiệm kết nối hạ tầng giám sát an ninh mạng quốc gia quy định tại mục tổ chức triển khai, tiêu mục các bộ, cơ quan ngang bộ, Ủy ban nhân dân cấp tỉnh.

II. NGUYÊN TẮC

Khung Kiến trúc an ninh mạng quốc gia phù hợp với chủ trương, chính sách của Đảng và Nhà nước về phát triển quốc gia số, đồng thời bảo đảm sự thống nhất với các định hướng, chiến lược bảo vệ an ninh mạng quốc gia, giữ gìn trật tự, an toàn xã hội của Bộ Công an; tuân thủ đầy đủ các nguyên tắc cốt lõi, phản ánh chuyển dịch tư duy từ “quản lý hành chính” sang “quản trị phát triển”. Cụ thể như sau:

1. Nguyên tắc quản trị dựa trên kết quả

Mục tiêu cao nhất và thước đo thành công của từng hợp phần trong kiến trúc là tạo ra các kết quả thực chất, có thể định lượng, đo lường và kiểm chứng được.

Các kết quả trọng tâm cần đạt bao gồm: Nâng cao mức độ hài lòng, niềm tin của người dân và doanh nghiệp trong công tác bảo đảm an ninh, an toàn trên không gian mạng.

Mọi quyết định liên quan đến chủ trương đầu tư, thiết kế kỹ thuật và tổ chức vận hành cần được xem xét, thẩm định và đánh giá dựa trên hiệu quả mang lại cho xã hội, quốc gia, thay vì chỉ theo hướng tiếp cận hành chính hoặc hình thức. Áp dụng Khung quản lý rủi ro an ninh mạng để có cơ sở ưu tiên đầu tư vào các hệ thống trọng yếu, tối ưu hóa ngân sách. Khung kiến trúc được rà soát, cập nhật định kỳ để bảo đảm tính mở, linh hoạt và khả năng tích hợp cao.

2. Nguyên tắc lãnh đạo, chỉ đạo, điều hành dựa trên dữ liệu theo thời gian thực

Dữ liệu phải được xác định là tài sản chiến lược, đóng vai trò trung tâm trong mọi quy trình nghiệp vụ bảo đảm an ninh mạng, là nền tảng cho các quyết định chỉ đạo, điều hành; không chỉ giới hạn ở chức năng thống kê, báo cáo sau sự việc.

Lãnh đạo các đơn vị cần từng bước chuyển đổi phương thức chỉ đạo, điều hành sang mô hình ra quyết định dựa trên dữ liệu được phân tích, dự báo, trực quan, cập nhật theo thời gian thực, thay thế phương thức truyền thống vốn chủ yếu dựa trên các báo cáo tổng hợp bằng văn bản giấy, vốn có độ trễ cao, thiếu tính khách quan và không phản ánh đầy đủ bối cảnh thực tiễn.

Đối với các đơn vị, địa phương cần chủ động hạ tầng bảo đảm an ninh mạng, việc cập nhật dữ liệu được cho phép thực hiện theo chu kỳ phù hợp, nhưng vẫn bảo đảm tính kịp thời, chính xác và đầy đủ phục vụ công tác chỉ đạo, điều hành.

Mọi hoạt động thu thập, xử lý, chia sẻ, khai thác dữ liệu cần được thực hiện một cách nghiêm túc, tuân thủ đầy đủ các quy định của pháp luật về an ninh mạng, bảo mật thông tin và bảo vệ dữ liệu cá nhân.

3. Nguyên tắc vận hành thông minh và tự động hóa trên cơ sở ưu tiên ứng dụng trí tuệ nhân tạo (AI First)

Kiến trúc cần được thiết kế với tầm nhìn dài hạn, bảo đảm tích hợp sâu rộng trí tuệ nhân tạo (AI) và các công nghệ tự động hóa vào các quy trình xử lý nghiệp vụ, theo nguyên tắc liên thông, bảo mật, an toàn, hiệu quả, có khả năng mở rộng.

Các hệ thống ứng dụng trí tuệ nhân tạo (AI) được xây dựng và vận hành theo nguyên tắc minh bạch, công bằng, an toàn và có trách nhiệm (AI Trustworthy), bảo đảm không xâm phạm quyền riêng tư, không thiên lệch, có khả năng giải trình, bảo đảm an toàn cho dữ liệu huấn luyện và phòng chống đầu độc dữ liệu (Data Poisoning). Áp dụng cơ chế giám sát rủi ro đặc thù đối với các hệ thống Trợ lý ảo và AI tạo sinh (GenAI) tránh rò rỉ dữ liệu nhạy cảm.

Loại bỏ các quy trình thủ công, đẩy mạnh tự động hóa nhằm: Giải phóng sức lao động cho cán bộ, công chức, viên chức và người lao động; tạo điều kiện tập trung vào các nhiệm vụ có tính phân tích, sáng tạo, yêu cầu tương tác phức tạp và hoạch định chính sách, chiến lược; giảm thiểu các công việc mang tính sự vụ, hành chính thuần túy.

4. Nguyên tắc phân cấp, phân quyền mạnh mẽ

Tập trung phát huy vai trò kiến tạo thể chế, thể hiện qua việc ban hành các tiêu chuẩn, quy chuẩn kỹ thuật, xây dựng và tổ chức vận hành các nền tảng bảo đảm an ninh mạng dùng chung, đồng thời thực hiện chức năng giám sát việc tổ chức thực hiện dựa trên dữ liệu.

Các đơn vị, địa phương cần chủ động, linh hoạt trong thực hiện nhiệm vụ được giao, trên cơ sở khai thác và vận hành hiệu quả các nền tảng bảo đảm an ninh mạng dùng chung trong toàn hệ thống chính trị.

Khai thác các nền tảng số tạo điều kiện giám sát kết quả theo thời gian thực, là cơ sở bảo đảm cho việc điều hành thống nhất, xuyên suốt.

5. Nguyên tắc lấy người dùng làm trung tâm với hệ sinh thái dịch vụ hợp nhất

Bảo đảm khả năng tiếp cận dịch vụ công bằng, bảo vệ công dân, toàn diện, không rào cản cho mọi đối tượng, đặc biệt là người yếu thế; tích hợp đầy đủ các tính năng hỗ trợ như: hướng dẫn bằng giọng nói, ngôn ngữ dân tộc thiểu số, trợ năng cho người khuyết tật.

Bảo đảm mọi người dân đều được thụ hưởng đầy đủ các giải pháp số tiên tiến, bảo đảm an ninh, an toàn trên môi trường số.

Từng bước hình thành thể hệ “Công dân số” – có năng lực vận hành, xử lý, khai thác, bảo đảm an ninh mạng trong môi trường số hiện đại, hiệu quả, đúng quy định. Triển khai cơ chế xác thực đa yếu tố (MFA) thống nhất trên các kênh tương tác nhằm tăng cường bảo đảm an ninh mạng trong quá trình truy cập và sử dụng dịch vụ công.

6. Nguyên tắc bảo đảm an ninh mạng, bảo vệ dữ liệu và quyền riêng tư là yêu cầu tiên quyết, xuyên suốt

An ninh mạng được xác định là yếu tố sống còn, điều kiện tiên quyết và bắt buộc trong toàn bộ quá trình thiết kế, xây dựng, triển khai, vận hành và nâng cấp các thành phần trong mô hình kiến trúc. Thiết kế kiến trúc áp dụng nguyên tắc phòng thủ nhiều lớp gắn liền với mô hình Kiến trúc Không tin cậy (Zero Trust Architecture) - bảo đảm xác minh liên tục, cấp quyền truy cập tối thiểu và không tin tưởng mặc định.

Thực hiện nghiêm túc về bảo đảm an ninh mạng hệ thống thông tin theo cấp độ, bảo đảm triển khai đồng bộ các biện pháp kỹ thuật, tổ chức, nghiệp vụ tương ứng. Mọi hoạt động kết nối, chia sẻ, liên thông dữ liệu cần đi kèm với các phương án: Sao lưu, dự phòng hệ thống; bảo đảm an toàn, toàn vẹn dữ liệu; kế hoạch ứng phó, khắc phục sự cố và phục hồi hệ thống, dữ liệu (bảo đảm hoạt động liên tục và khả năng khôi phục theo quy định).

Tất cả hoạt động liên quan đến dữ liệu, hạ tầng số và an ninh mạng cần tuân thủ các quy định của pháp luật về an ninh mạng, an ninh dữ liệu, bảo vệ dữ liệu cá nhân.

7. Nguyên tắc thúc đẩy phát triển dữ liệu mở, nâng cao tính minh bạch, trách nhiệm giải trình và đổi mới sáng tạo

Ngoại trừ dữ liệu thuộc phạm vi bí mật nhà nước, dữ liệu cá nhân nhạy cảm và dữ liệu có yêu cầu bảo mật theo quy định của pháp luật, các dữ liệu còn lại cần được công khai, chia sẻ dưới dạng dữ liệu mở, phục vụ nhu cầu của cộng đồng, doanh nghiệp, tổ chức nghiên cứu và người dân.

Việc mở dữ liệu cần tuân thủ đầy đủ quy định của pháp luật hiện hành về an ninh dữ liệu, bảo mật thông tin, giao dịch điện tử và các quy định có liên quan.

Việc cung cấp dữ liệu mở nhằm: Nâng cao tính minh bạch và trách nhiệm giải trình trong quản trị nhà nước; tạo điều kiện cho người dân, doanh nghiệp và tổ chức xã hội tham gia giám sát, đánh giá hiệu quả điều hành, qua đó củng cố niềm tin công chúng và hiệu quả thực thi chính sách; thúc đẩy đổi mới sáng tạo, khuyến khích cá nhân, tổ chức khai thác và sử dụng dữ liệu để phát triển sản phẩm, dịch vụ số, nghiên cứu khoa học, khởi nghiệp và đóng góp vào sự phát triển kinh tế - xã hội dựa trên giá trị mà dữ liệu mang lại.

Các nguyên tắc nêu trên có mối quan hệ mật thiết, bổ trợ lẫn nhau, tạo thành một thể thống nhất, tuần hoàn và phát triển bền vững.

Trong đó, bảo đảm an ninh mạng, bảo vệ dữ liệu và quyền riêng tư (Nguyên tắc 6) là nền tảng để các nguyên tắc còn lại có thể được triển khai một cách tin cậy và bền vững. Trên nền tảng an toàn đó, việc lãnh đạo, chỉ đạo, điều hành dựa trên dữ liệu (Nguyên tắc 2) chỉ khả thi khi có hệ thống vận hành thông minh, tự động thu thập dữ liệu (Nguyên tắc 3). Dữ liệu thu thập được cho phép giám sát hiệu quả, từ đó phân cấp, phân quyền mạnh mẽ (Nguyên tắc 4). Hiệu quả của việc phân quyền và toàn bộ mô hình được đo lường bằng kết quả thực chất (Nguyên tắc 1), hướng đến sự hài lòng của người dân và doanh nghiệp thông qua hệ sinh thái hợp nhất, lấy người dùng làm trung tâm (Nguyên tắc 5). Niềm tin của người dùng đối với hệ sinh thái lại được củng cố bởi sự bảo đảm về an ninh mạng (Nguyên tắc 6).

Trên cơ sở đó, việc công khai, chia sẻ, mở dữ liệu (Nguyên tắc 7) không chỉ tăng cường tính minh bạch và trách nhiệm giải trình, mà còn mở rộng tiềm năng đổi mới sáng tạo và khai thác tối đa giá trị dữ liệu, tạo nên vòng tuần hoàn khép kín, tự củng cố và liên tục hoàn thiện.

8. Nguyên tắc thiết kế kiến trúc

Thiết kế Kiến trúc An ninh mạng quốc gia dựa trên các nguyên tắc cốt lõi sau:

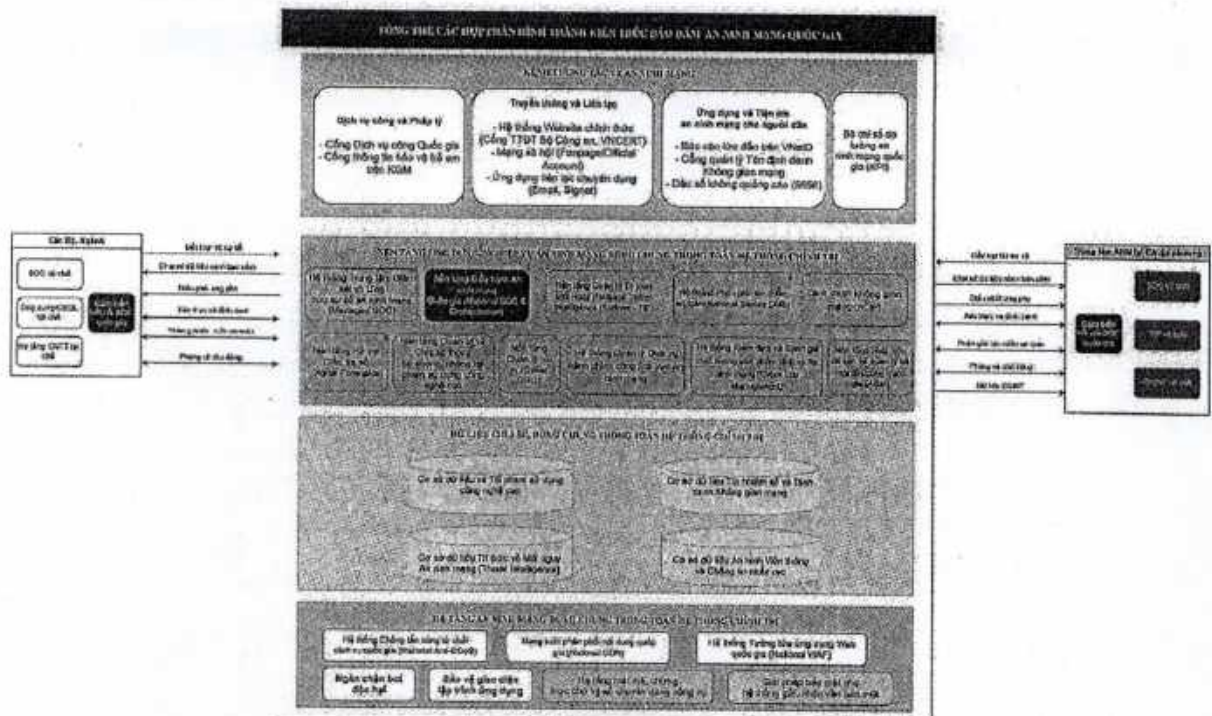
Phòng thủ chiều sâu: Thiết lập nhiều lớp bảo vệ đan xen, bao gồm: hạ tầng mạng, ứng dụng, dữ liệu, người dùng cuối, nhằm bảo đảm rằng khi một lớp bị tấn công, các lớp khác vẫn duy trì khả năng bảo vệ hệ thống, giảm thiểu rủi ro lây lan và mất kiểm soát.

Lấy dữ liệu làm trung tâm: Xác định bảo đảm an ninh dữ liệu là ưu tiên hàng đầu. Tất cả các quyết định điều phối, ứng phó và xử lý tình huống an ninh mạng cần dựa trên phân tích dữ liệu lớn (Big Data Analytics) kết hợp với Trí tuệ nhân tạo (AI), bảo đảm tính chủ động và hiệu quả.

Phòng vệ chủ động: Chuyển dịch từ mô hình phòng thủ bị động sang phòng thủ chủ động, trong đó: Chủ động săn tìm mối nguy (Threat Hunting); tăng cường chia sẻ tri thức và thông tin về mối đe dọa giữa các cấp; ngăn chặn tấn công ngay từ cửa ngõ quốc gia (biên giới số), không để rủi ro lan vào hệ thống trọng yếu.

III. TỔNG THỂ CÁC HỢP PHẦN HÌNH THÀNH KIẾN TRÚC BẢO ĐẢM AN NINH MẠNG QUỐC GIA

Các hợp phần bảo đảm an ninh mạng quốc gia cần được xây dựng nhằm bảo đảm tính thống nhất, đồng bộ và tuân thủ chặt chẽ theo Khung kiến trúc tổng thể quốc gia số. Toàn bộ kiến trúc giải pháp bảo đảm an ninh mạng quốc gia là một tập hợp các thành phần kiến trúc có mối quan hệ hữu cơ, tương hỗ lẫn nhau, bao gồm hai nhóm hợp phần chính:



Hình 1: Tổng thể các hợp phần bảo đảm an ninh mạng quốc gia

1. Kiến trúc An ninh mạng quốc gia (Hợp phần Trụ cột)

Đây là hợp phần đóng vai trò nòng cốt, “xương sống” của hệ thống an ninh mạng quốc gia. Hợp phần này bao gồm các hệ thống, nền tảng công nghệ và cơ sở dữ liệu chuyên ngành do Bộ Công an tổ chức triển khai, quản lý và vận hành.

Phạm vi phục vụ: Cung cấp các dịch vụ, nền tảng dùng chung cho toàn bộ hệ thống chính trị (các bộ, ban, ngành, địa phương) và phục vụ công tác chuyên biệt liên quan an ninh mạng.

Vai trò: Định hình các tiêu chuẩn kỹ thuật, cung cấp dữ liệu tri thức mối nguy, và là trung tâm chỉ huy, điều phối hoạt động ứng cứu sự cố ở quy mô quốc gia.

2. Thành phần bảo đảm an ninh mạng trong Khung kiến trúc số của các cơ quan, tổ chức (Hợp phần Vệ tinh)

Đây là các thành phần an ninh mạng được tích hợp và quy hoạch cụ thể trong Khung kiến trúc số/Kiến trúc Chính phủ số của từng đơn vị, bao gồm:

- Thành phần an ninh mạng trong Khung kiến trúc số của các cơ quan Đảng.
- Thành phần an ninh mạng trong Khung kiến trúc số của Quốc hội.
- Thành phần an ninh mạng trong Khung kiến trúc số của Mặt trận Tổ quốc Việt Nam.
- Thành phần an ninh mạng trong Khung kiến trúc Chính phủ số Việt Nam.
- Thành phần an ninh mạng trong Khung kiến trúc số cấp bộ, cơ quan ngang bộ, (trừ Bộ Công an).
- Thành phần an ninh mạng trong Khung kiến trúc số cấp tỉnh/thành phố trực thuộc trung ương.
- Thành phần an ninh mạng trong Khung kiến trúc số của các tập đoàn, tổng công ty nhà nước và hệ thống thông tin quan trọng thuộc danh mục được ưu tiên bảo vệ trong hệ thống chính trị.

Các thành phần này được xây dựng dựa trên các Mô hình tham chiếu (tại các mục Mô hình kiến trúc tham chiếu cấp tỉnh và cấp bộ nêu dưới đây) để bảo đảm khả năng kết nối, chia sẻ dữ liệu và phối hợp đồng bộ với Kiến trúc An ninh mạng quốc gia.

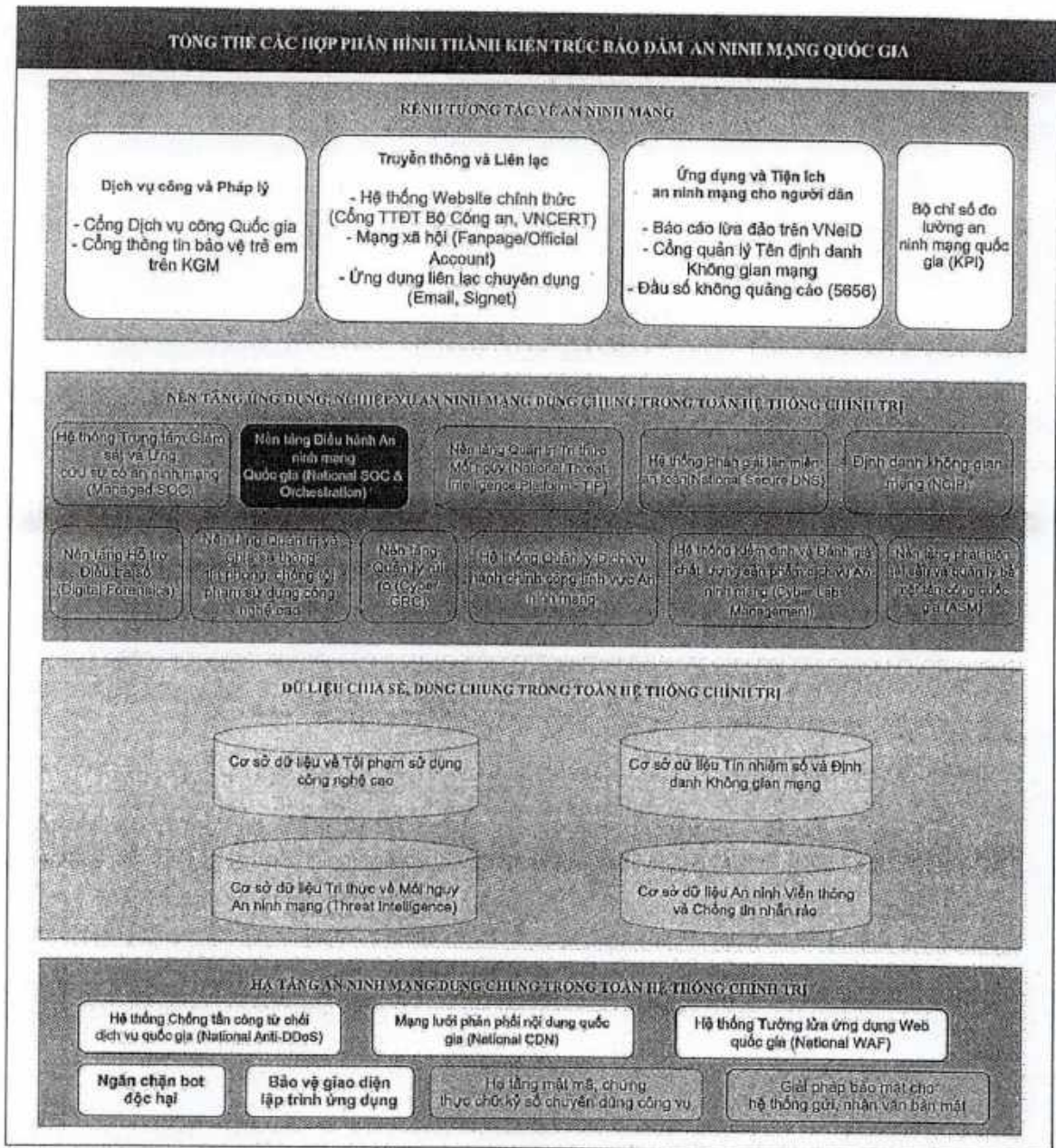
IV. KHUNG KIẾN TRÚC AN NINH MẠNG QUỐC GIA

Kiến trúc An ninh mạng quốc gia được thiết kế dựa trên tư duy phòng thủ chủ động, tích hợp đồng bộ với Khung kiến trúc tổng thể quốc gia số. Hệ thống được cấu trúc thành 04 lớp chức năng liên kết chặt chẽ, hình thành hệ sinh thái an ninh mạng toàn diện: từ hạ tầng giám sát, dữ liệu chiến lược, nền tảng nghiệp vụ đến công tác chỉ huy, điều hành.¹

¹ Lưu ý về Nguyên tắc Kiến trúc (Dữ liệu và Ứng dụng): Sự phân định giữa Lớp 2 (Dữ liệu) và Lớp 3 (Nền tảng) trong kiến trúc này mang tính chất logic hệ thống nhằm làm rõ các tài nguyên dữ liệu cốt lõi cần được quy hoạch, chia sẻ và các công cụ tác nghiệp cần được trang bị. Trong thực tiễn đầu tư và triển khai kỹ thuật:

- Tính tích hợp: CSDL và Nền tảng ứng dụng có thể là các cấu phần gắn liền trong cùng một giải pháp (Ví dụ: CSDL Tri thức mối nguy có thể là một thành phần nội tại của Nền tảng TIP; CSDL OSINT nằm trong Hệ thống khai thác thông tin nguồn mở).

- CSDL nghiệp vụ: Các Nền tảng tại Lớp 3 đều có các CSDL nghiệp vụ riêng để phục vụ vận hành; Lớp 2 chỉ liệt kê các CSDL mang tính chất quốc gia, chuyên ngành dùng chung hoặc phục vụ mục tiêu kết nối, chia sẻ liên ngành.



Hình 2: Kiến trúc an ninh mạng quốc gia²

1. Lớp 1: Hạ tầng an ninh mạng dùng chung trong toàn hệ thống chính trị

Hạ tầng này đóng vai trò là “lá chắn” đầu tiên về vật lý và logic bảo vệ không gian mạng quốc gia. Lớp này được cấu thành từ 3 thành phần cốt lõi của Hệ thống phòng vệ mạng quốc gia (WAF, DDoS, CDN) cụ thể như sau:

² Các thành phần an ninh mạng dùng chung quốc gia nêu tại Mục này, khi ánh xạ vào Khung kiến trúc tổng thể quốc gia số, đều thuộc nhóm “Thành phần an ninh mạng” tại Lớp 1 (Hạ tầng số và an ninh mạng dùng chung) của Khung kiến trúc tổng thể quốc gia số. Việc phân rã tiếp thành 04 lớp dưới đây là cách tổ chức nội bộ theo logic chức năng của Khung kiến trúc an ninh mạng quốc gia, không làm thay đổi vị trí của các thành phần này trong Khung kiến trúc tổng thể quốc gia số.

a) Hệ thống Tường lửa ứng dụng Web quốc gia (National WAF)

Về mặt quản lý, đây là “lá chắn số trực tiếp bảo vệ các Cổng thông tin điện tử, Dịch vụ công trực tuyến và các ứng dụng trọng yếu của Chính phủ và các bộ, ngành. Vai trò chiến lược của nó là bảo đảm “mặt tiền” của quốc gia trên không gian mạng luôn sạch, ngăn chặn các hành vi phá hoại làm thay đổi giao diện (Deface) hoặc đánh cắp dữ liệu công dân, giữ gìn uy tín và hình ảnh của cơ quan nhà nước.

Về mặt kỹ thuật, hệ thống hoạt động ở Lớp 7 (Lớp ứng dụng) trong mô hình OSI. Nó thực hiện kiểm soát chi tiết từng yêu cầu HTTP/HTTPS đi vào các ứng dụng, tự động phát hiện và ngăn chặn các kỹ thuật tấn công phổ biến theo tiêu chuẩn quốc tế (OWASP Top 10) như SQL Injection, XSS. Hệ thống cho phép áp dụng chính sách bảo vệ đồng bộ trên quy mô toàn quốc mà không phụ thuộc vào nền tảng của từng ứng dụng đơn lẻ.

b) Hệ thống Chống tấn công từ chối dịch vụ quốc gia (National Anti-DDoS)

Về vai trò, đây là thành phần bảo đảm “tính sẵn sàng” cho huyết mạch thông tin quốc gia. Nhiệm vụ của nó là ngăn chặn các cuộc tấn công làm tràn ngập băng thông, bảo đảm các hệ thống thông tin quan trọng về an ninh quốc gia luôn hoạt động thông suốt, phục vụ người dân và doanh nghiệp ngay cả trong các tình huống xảy ra xung đột hoặc khủng hoảng an ninh mạng diện rộng.

Về cơ chế vận hành, hệ thống bao gồm các cụm thiết bị làm sạch lưu lượng (Scrubbing Centers) công suất lớn đặt tại các nút mạng viễn thông chủ chốt. Khi phát hiện dấu hiệu tấn công DDoS, hệ thống sẽ tự động điều hướng lưu lượng, tách lọc các truy cập giả mạo hoặc máy tính ma (Botnet) để loại bỏ, chỉ cho phép các truy cập hợp lệ đi qua. Khả năng hấp thụ băng thông lớn giúp hệ thống triệt tiêu các đợt tấn công quy mô lớn mà không làm gián đoạn dịch vụ. Hệ thống lõi quốc gia thiết lập cơ chế phối hợp với các nhà cung cấp dịch vụ mạng viễn thông, bảo đảm không xung đột hạ tầng.

c) Thành phần ngăn chặn bot độc hại

Nhận dạng và phân loại các máy khách tự động truy cập vào hệ thống thông tin của cơ quan, tổ chức; phân biệt bot hợp pháp với bot độc hại; ngăn chặn các hành vi dò tìm mật khẩu, nhồi thông tin đăng nhập và thu thập dữ liệu trái phép quy mô lớn. Thành phần này hoạt động dựa trên phân tích hành vi truy cập qua nhiều phiên, bổ sung cho khả năng phát hiện theo từng yêu cầu của tường lửa ứng dụng web.

d) Thành phần bảo vệ giao diện lập trình ứng dụng (API)

Tự động phát hiện, lập danh mục các giao diện lập trình ứng dụng đang hoạt động; kiểm soát truy cập theo lược đồ API đã công bố; giới hạn tần suất truy cập theo từng điểm cuối; phát hiện bất thường về phân quyền truy cập dữ liệu và dấu hiệu lộ lọt dữ liệu qua API.

Do Khung kiến trúc tổng thể quốc gia số áp dụng nguyên tắc thiết kế API First, phần lớn giao diện lập trình ứng dụng phục vụ liên thông giữa các cơ quan,

tổ chức nằm bên trong mạng, không đi qua biên Internet. Vì vậy, thành phần bảo vệ giao diện lập trình ứng dụng cần có khả năng triển khai cả tại biên Internet và tại các điểm đầu nối liên thông nội bộ.

đ) Mạng lưới phân phối nội dung quốc gia (National CDN)

Xét về khía cạnh phục vụ, hệ thống này giải quyết bài toán về tốc độ và trải nghiệm người dùng, đồng thời gia tăng lớp bảo mật ẩn danh. Nó bảo đảm người dân ở bất kỳ đâu (kể cả vùng sâu, vùng xa hay hải đảo) đều có thể truy cập các dịch vụ công và thông tin tuyên truyền của Đảng, Nhà nước một cách nhanh chóng, ổn định, không bị nghẽn mạng cục bộ.

Về mặt công nghệ, hệ thống bao gồm mạng lưới các máy chủ lưu trữ đệm (Edge Servers) phân tán rộng khắp. Khi người dùng truy cập, dữ liệu sẽ được tải từ máy chủ gần nhất thay vì phải về trung tâm dữ liệu gốc. Đặc biệt, công nghệ CDN góp phần giảm nguy cơ lộ trực tiếp địa chỉ IP thực của các máy chủ nguồn (Origin Server), khiến kẻ tấn công không thể xác định được mục tiêu gốc để thực hiện các hành vi phá hoại trực tiếp.

Trong Khung kiến trúc này, mạng lưới phân phối nội dung quốc gia đóng vai trò hạ tầng chuyển tải của Hệ thống phòng vệ mạng quốc gia: các chức năng bảo vệ (tường lửa ứng dụng web, chống tấn công từ chối dịch vụ, ngăn chặn bot độc hại, bảo vệ giao diện lập trình ứng dụng) được triển khai tại các điểm hiện diện của mạng lưới, gần người sử dụng.

e) Hạ tầng mật mã, chứng thực chữ ký số chuyên dùng công vụ

Theo Khung kiến trúc tổng thể quốc gia số, Hệ thống chứng thực chữ ký số chuyên dùng công vụ do Ban Cơ yếu Chính phủ chủ quản, cung cấp dịch vụ chứng thực chữ ký số để xác thực và bảo đảm tính pháp lý, toàn vẹn cho các văn bản, giao dịch điện tử trong các cơ quan thuộc hệ thống chính trị. Khung kiến trúc an ninh mạng quốc gia kế thừa, dẫn chiếu thành phần này; việc kết nối, chia sẻ và trao đổi dữ liệu thuộc phạm vi bí mật nhà nước thực hiện theo quy định của pháp luật về bảo vệ bí mật nhà nước, an ninh mạng và cơ yếu.

g) Giải pháp bảo mật cho hệ thống gửi, nhận văn bản mật

Đáp ứng yêu cầu liên thông giữa các cơ quan Đảng, Quốc hội, Chính phủ, Mặt trận Tổ quốc Việt Nam và các cơ quan, tổ chức khác theo phạm vi triển khai thực tế; triển khai các giải pháp bảo mật dữ liệu cho phần mềm, ứng dụng (Ban Cơ yếu Chính phủ chủ quản đối với sản phẩm mật mã cơ yếu và hệ thống thông tin cơ yếu).

2. Lớp 2: Dữ liệu chia sẻ dùng chung trong toàn hệ thống chính trị

Dữ liệu được xác định là tài nguyên chiến lược, là đầu vào cốt lõi cho mọi hoạt động nghiệp vụ và chỉ huy. Các cơ sở dữ liệu (CSDL) được quy hoạch tập trung, chuẩn hóa theo các nhóm chuyên biệt. Về phạm vi khai thác, các CSDL này được xác định là tài nguyên dùng chung cho toàn bộ hệ thống chính trị và các cơ quan nhà nước. Các CSDL tại Lớp 2 được bảo vệ bằng các giải pháp mã hóa dữ liệu tại chỗ và mã hóa đường truyền. Đối với các dữ liệu có chứa dữ liệu cá

nhân sẽ được khử định danh thông qua nền tảng khử định danh SDEG(Secure Data Exchange Gateway) khi chia sẻ bảo đảm tuân thủ quy định của luật pháp về dữ liệu và bảo vệ dữ liệu cá nhân.

a) Cơ sở dữ liệu về Tội phạm sử dụng công nghệ cao

Đây là kho dữ liệu tổng hợp từ đấu tranh phòng, chống các loại tội phạm sử dụng công nghệ cao. Từ nguồn thông tin tin cậy tham chiếu quan trọng giúp các tổ chức tài chính, ngân hàng, các nhà cung cấp dịch vụ và người dân có cơ sở đánh giá, nhận thức mức độ rủi ro trước khi thực hiện các giao dịch trên không gian mạng.

Về nội dung kỹ thuật, hệ thống thực hiện lưu trữ hồ sơ định danh (Profiling) chi tiết về đối tượng và phương thức thủ đoạn của các hình thái tội phạm sử dụng công nghệ cao, ví dụ như: các ô nhóm lừa đảo “tuyển cộng tác viên online”, “giả danh cơ quan tư pháp”, hay các đường dây tổ chức đánh bạc nghìn tỷ qua mạng. Dữ liệu bao gồm các “danh sách đen” (Blacklist) được cập nhật liên tục: số tài khoản ngân hàng “rác”, số điện thoại, địa chỉ IP, tên miền (Domain) giả mạo cơ quan nhà nước, các ví điện tử... liên quan đến hoạt động phạm pháp.

b) Cơ sở dữ liệu Tri thức về Môi nguy An ninh mạng (Threat Intelligence)

CSDL này được ví như “bộ não” tri thức của hệ thống phòng thủ quốc gia. Nhiệm vụ của nó là chuyển hóa các dữ liệu thô thành thông tin tình báo có giá trị, giúp chuyển đổi trạng thái phòng thủ từ “bị động” sang “chủ động”. Đặc biệt, nguồn dữ liệu này đóng vai trò là “bộ não” thông minh cho các sản phẩm an ninh mạng chiến lược được triển khai trong hệ thống chính trị (như Tường lửa, EDR...), cung cấp năng lực nhận diện sớm để ngăn chặn các mối đe dọa.

Về mặt cấu trúc dữ liệu, hệ thống chuẩn hóa thông tin theo các tiêu chuẩn quốc tế (như STIX/TAXII). Nội dung bao gồm: Hồ sơ chi tiết về các nhóm tin tặc (APT); Đặc điểm nhận dạng mã độc (ví dụ: mã bả của các dòng Ransomware LockBit, mã độc gián điệp...); Các lỗ hổng bảo mật mới công bố (ví dụ: lỗ hổng Log4Shell, lỗ hổng trong các thiết bị VPN...); Các chỉ dấu xâm phạm (IoC);... Dữ liệu này được phân loại và chia sẻ tự động, phù hợp đối tượng cho các hệ thống SOC có kết nối để cập nhật luật bảo vệ ngay lập tức.

c) Cơ sở dữ liệu Tín nhiệm số

Cơ sở dữ liệu phục vụ đánh giá và công bố mức độ tín nhiệm của các chủ thể, tài nguyên số trên không gian mạng. Nội dung lưu trữ bao gồm: nhãn tín nhiệm và trạng thái xác thực thực chứng của tài khoản có ảnh hưởng xã hội, tổ chức tài chính, trang thông tin điện tử chính thống; danh mục tài nguyên số quan trọng gắn với từng chủ thể cụ thể (địa chỉ IP, tên miền quốc gia, tên định danh cuộc gọi).

Cơ sở dữ liệu là nguồn tham chiếu để hiển thị chỉ dấu tín nhiệm trên trình duyệt, ứng dụng bảo vệ người dùng; phục vụ nhận diện trang thông tin điện tử chính thống, phòng chống giả mạo và lừa đảo trên không gian mạng.

d) Cơ sở dữ liệu An ninh Viễn thông và Chống tin nhắn rác

Đây là công cụ quản lý chuyên ngành phục vụ việc làm sạch môi trường viễn thông và bảo vệ người tiêu dùng. Hệ thống cung cấp cơ sở dữ liệu gốc để ngăn chặn, xử lý hiệu quả vấn nạn tin nhắn rác, cuộc gọi lừa đảo đang gây bức xúc trong xã hội, đồng thời hỗ trợ quản lý chặt chẽ việc sử dụng tên định danh thương mại.

Về cơ chế hoạt động, hệ thống duy trì hai danh sách quan trọng: Danh sách tên định danh hợp lệ (Brandname) và Danh sách thuê bao đăng ký từ chối quảng cáo (DoNotCall). Tên định danh (Brandname) - ví dụ như “VneID”, “BoCongAn”, hay tên các Ngân hàng - sẽ được sử dụng và hiển thị trực tiếp trên điện thoại của người dân khi nhận tin nhắn hoặc cuộc gọi. Điều này giúp người dân dễ dàng nhận biết, phân biệt các cuộc gọi chính thống từ tổ chức, cá nhân đã đăng ký hợp pháp với các cuộc gọi lừa đảo, mạo danh xuất phát từ các số điện thoại rác.

3. Lớp 3: Nền tảng Ứng dụng, nghiệp vụ An ninh mạng dùng chung trong toàn hệ thống chính trị

Lớp này đóng vai trò là “không gian tác nghiệp số”, cung cấp các nền tảng ứng dụng và công cụ chuyên dụng phục vụ trực tiếp cho hoạt động nghiệp vụ của các lực lượng an ninh mạng. Đây là nơi các quy trình nghiệp vụ (như giám sát, điều tra, cấp phép, kiểm định...) được thực thi. Chính thông qua quá trình tác nghiệp và vận hành trên các nền tảng này, các dữ liệu chuyên ngành được sinh ra, xử lý và chuẩn hóa để hình thành nên các Cơ sở dữ liệu tại Lớp 2. Các nền tảng được chia thành 02 nhóm chính:

Nhóm 1: Các Nền tảng Kỹ thuật Phòng vệ và Tác chiến

a) Nền tảng Điều hành An ninh mạng Quốc gia (National SOC & Orchestration)

Về mặt quản lý và chiến lược, đây là thành phần nền tảng số quốc gia trọng yếu được quy định trong Khung kiến trúc tổng thể quốc gia số, dùng chung cho toàn bộ hệ thống chính trị. Nền tảng này đóng vai trò điều hành với chức năng chính là nhận thức tình huống an ninh mạng quốc gia (Situational Awareness). Đây là đầu mối tập trung, tiếp nhận các luồng thông tin, dữ liệu an ninh mạng từ mạng lưới các hệ thống SOC thành phần của các Bộ, ngành và địa phương trên toàn quốc. Từ bức tranh toàn cảnh đó, hệ thống hỗ trợ công tác tham mưu, giúp Lãnh đạo đưa ra các quyết định chỉ huy, điều phối lực lượng ứng cứu sự cố một cách chính xác và kịp thời.

Về góc độ kỹ thuật, hệ thống hoạt động như một “SOC của các SOC”. Nó không đi sâu vào xử lý từng sự kiện nhỏ lẻ của từng đơn vị mà tập trung vào việc tổng hợp dữ liệu, phân tích tương quan để phát hiện các chiến dịch tấn công diện rộng, phức tạp mà các SOC đơn lẻ không thể nhìn thấy. Hệ thống cung cấp cơ chế chỉ huy xuyên suốt, bảo đảm sự phối hợp đồng bộ giữa các lực lượng khi quốc gia đối mặt với các nguy cơ an ninh phi truyền thống trên không gian mạng.

b) Hệ thống Trung tâm Giám sát và Ứng cứu sự cố an ninh mạng (Managed SOC)

Về vai trò, đây là lực lượng trực tiếp, bảo đảm an ninh mạng cho “vùng lõi” của hệ thống. Hệ thống chịu trách nhiệm giám sát liên tục 24/7, phát hiện tức thời và xử lý sự cố tại chỗ cho các hệ thống thông tin quan trọng về an ninh quốc gia. Tập trung bảo vệ các hệ thống có kết nối Internet (Cổng thông tin, Dịch vụ công...). Nhiệm vụ chính là phát hiện các cuộc tấn công từ bên ngoài, ngăn chặn xâm nhập trái phép và các nỗ lực khai thác lỗ hổng từ không gian mạng quốc tế.

c) Nền tảng Quản trị Tri thức Môi nguy (National Threat Intelligence Platform - TIP)

Nền tảng này là công cụ tác nghiệp chuyên sâu dành cho các chuyên gia phân tích an ninh mạng (Threat Hunters), đóng vai trò “nhà máy sản xuất tri thức”. Hệ thống thực hiện quy trình nghiệp vụ khép kín: thu thập dữ liệu thô từ nhiều nguồn (trong nước, quốc tế, Darkweb), chuẩn hóa định dạng (STIX/TAXII), phân tích làm giàu dữ liệu và kiểm chứng độ tin cậy.

Kết quả đầu ra của quá trình tác nghiệp trên TIP chính là các bản tin tình báo và danh sách chỉ dấu xâm phạm (IoC) chất lượng cao được lưu trữ vào CSDL Tri thức môi nguy (Lớp 2). Đồng thời, nền tảng cung cấp cơ chế API để chia sẻ tự động nguồn tri thức này cho các hệ thống giám sát (SOC, EDR, Firewall) trong toàn bộ hệ thống chính trị.

d) Hệ thống Phân giải tên miền an toàn quốc gia (National Secure DNS)

Về vai trò, đây là một hợp phần quan trọng thuộc Nền tảng phòng vệ mạng quốc gia được quy định trong Khung kiến trúc tổng thể quốc gia số. Hệ thống đóng vai trò như một “lớp lọc thô” ở quy mô quốc gia, giúp làm sạch môi trường internet cho người dùng cuối (cán bộ, công chức, người dân) một cách trong suốt mà không yêu cầu họ cài đặt phần mềm phức tạp hay thay đổi thói quen sử dụng; không tự ý can thiệp vào các truy vấn DNS trên mạng internet của thuê bao cá nhân nhằm bảo đảm quyền kết nối.

Về cơ chế kỹ thuật, hệ thống hoạt động dựa trên việc đồng bộ dữ liệu thời gian thực từ đa nguồn tại Lớp 2:

- Chặn lọc: Tiếp nhận dữ liệu chỉ dấu xâm phạm (IoC) từ CSDL Tri thức về Môi nguy An ninh mạng và danh sách các tên miền/URL lừa đảo đã được xác minh từ CSDL về Tội phạm sử dụng công nghệ cao. Khi người dùng truy vấn vào các địa chỉ này, hệ thống tự động ngăn chặn và điều hướng sang trang cảnh báo.

- Định danh tin cậy: Kết nối với Cơ sở dữ liệu Tín nhiệm số để nhận diện các website chính thống. Thông tin này là nguồn tham chiếu để hiển thị các chỉ dấu an toàn (như logo, tích xanh) trên trình duyệt hoặc ứng dụng bảo vệ, giúp người dân yên tâm khi giao dịch.

đ) Định danh không gian mạng (NCIP)

Định danh không gian mạng là thành phần thuộc Nền tảng định danh và xác thực điện tử quy định tại Khung kiến trúc tổng thể quốc gia số, phục vụ định danh và xác thực chủ thể khi tham gia hoạt động trên không gian mạng.

Về cơ chế, người dân được cấp mã định danh không gian mạng (CyberID) dưới dạng mã ẩn danh, sử dụng để đăng ký và xác thực tài khoản số, tài khoản mạng xã hội thay cho việc cung cấp thông tin cá nhân thô; qua đó bảo vệ quyền riêng tư và hạn chế việc chuyển dịch dữ liệu cá nhân ra máy chủ ngoài lãnh thổ. Việc ánh xạ giữa mã định danh không gian mạng với thông tin định danh gốc từ Cơ sở dữ liệu quốc gia về dân cư và ứng dụng định danh điện tử quốc gia được thực hiện trên hạ tầng kỹ thuật tách biệt, có kiểm soát truy cập chặt chẽ, làm cơ sở để cơ quan có thẩm quyền truy nguyên chủ thể vi phạm theo quy định của pháp luật.

Việc xây dựng, vận hành thành phần định danh không gian mạng tuân thủ quy định của pháp luật về bảo vệ dữ liệu cá nhân.

Nhóm 2: Các nền tảng quản trị và nghiệp vụ

e) Nền tảng quản lý rủi ro an ninh mạng (Cyber GRC)

Nền tảng quản lý rủi ro an ninh mạng (Cyber GRC). Là nền tảng số hóa dùng chung quốc gia, thực hiện chức năng hệ thống phần mềm báo cáo quy định tại điểm b khoản 1 Điều 35 Nghị định số 331/2026/NĐ-CP, phục vụ chủ quản hệ thống thông tin gửi báo cáo về quản lý rủi ro an ninh mạng, tuân thủ an ninh mạng theo cấp độ và các nội dung báo cáo khác theo quy định. Nền tảng thay thế phương thức báo cáo giấy thủ công bằng quy trình đánh giá trực tuyến, giúp cơ quan quản lý nhà nước có cái nhìn tổng thể, định lượng về tình hình an ninh mạng của toàn hệ thống chính trị. Các văn bản hướng dẫn về quản lý rủi ro an ninh mạng, chế độ báo cáo theo Nghị định số 331/2026/NĐ-CP sử dụng thống nhất tên gọi Nền tảng quản lý rủi ro an ninh mạng và viết tắt là Cyber GRC khi dẫn chiếu đến nền tảng này.

Về chức năng, hệ thống cho phép các cơ quan, tổ chức thực hiện quy trình tự đánh giá rủi ro và quản lý hồ sơ đề xuất cấp độ hệ thống thông tin. Dựa trên các tiêu chí đầu vào, hệ thống tự động tính toán và đưa ra điểm số rủi ro (Risk Score), từ đó kiến nghị các biện pháp khắc phục cần thiết. Kết quả đánh giá và điểm số rủi ro này sẽ được đồng bộ sang CSDL Tín nhiệm số (Lớp 2) để hình thành hồ sơ tín nhiệm của các hệ thống thông tin.

g) Nền tảng phát hiện tài sản và quản lý bề mặt tấn công quốc gia (ASM)

Nền tảng thực hiện phát hiện, lập danh mục và theo dõi liên tục các tài sản số của cơ quan, tổ chức trong hệ thống chính trị đang hiện diện trên không gian mạng công cộng, bao gồm: tên miền, địa chỉ mạng, cổng dịch vụ, ứng dụng web, giao diện lập trình ứng dụng và chứng thư số đang sử dụng.

Trên cơ sở danh mục tài sản, nền tảng đối chiếu với dữ liệu về lỗ hổng bảo mật đang bị khai thác từ Cơ sở dữ liệu Tri thức mối nguy an ninh mạng, tự động xác định các tài sản có nguy cơ và phát cảnh báo tới đầu mối của chủ quản hệ thống thông tin. Nền tảng cũng phát hiện các tài sản chưa được đăng ký, tài sản không còn chủ quản lý hoặc đã hết hạn hỗ trợ kỹ thuật nhưng vẫn hiện diện trên mạng.

Kết quả từ nền tảng là căn cứ đầu vào cho hoạt động quản lý rủi ro an ninh mạng, xác định cấp độ hệ thống thông tin và kiểm tra, đánh giá an ninh mạng.

h) Hệ thống Quản lý dịch vụ hành chính công lĩnh vực an ninh mạng

Đây là thành phần phục vụ mục tiêu cải cách hành chính và chuyển đổi số của Bộ Công an. Hệ thống đóng vai trò là hệ thống xử lý nghiệp vụ nội bộ, thực hiện số hóa toàn trình các quy trình: từ thẩm định hồ sơ, cấp phép kinh doanh sản phẩm, dịch vụ an ninh mạng đến quản lý chứng chỉ hành nghề.

Hệ thống được thiết kế kết nối, liên thông dữ liệu trực tiếp với Cổng Dịch vụ công Quốc gia. Trong đó, Cổng Dịch vụ công Quốc gia (được mô tả tại Lớp 4) đóng vai trò là đầu mối tương tác thống nhất để người dân và doanh nghiệp nộp hồ sơ và tra cứu kết quả, bảo đảm tính nhất quán và thuận tiện trong giao dịch hành chính. Các dữ liệu về giấy phép kinh doanh và chứng chỉ hành nghề sau khi được xử lý tại đây sẽ là nguồn dữ liệu gốc để tạo lập và cập nhật cho Cơ sở dữ liệu Tín nhiệm số (Lớp 2).

i) Hệ thống Kiểm định và đánh giá chất lượng sản phẩm dịch vụ an ninh mạng (Cyber Lab Management)

Thành phần này đóng vai trò “người gác cổng” về chất lượng kỹ thuật. Nhiệm vụ là bảo đảm mọi thiết bị, phần mềm an ninh mạng trước khi đưa vào sử dụng trong các hệ thống trọng yếu đều phải “sạch”, không chứa mã độc hay “cửa hậu” (backdoor) và đáp ứng các tiêu chuẩn kỹ thuật quốc gia.

Hệ thống quản lý toàn bộ vòng đời kiểm định: từ khâu tiếp nhận mẫu, thực hiện kiểm thử xâm nhập (Pentest), rà soát mã nguồn (Code Review) trong phòng Lab, đến khi cấp chứng nhận hợp chuẩn/hợp quy. Dữ liệu về các sản phẩm đã đạt chuẩn từ hệ thống này sẽ được cập nhật tự động vào CSDL Tín nhiệm số và Định danh An ninh mạng (Lớp 2), phục vụ công tác tra cứu và công bố danh mục sản phẩm tin cậy.

k) Nền tảng Quản trị và Chia sẻ thông tin phòng, chống tội phạm sử dụng công nghệ cao

Đây là nền tảng nghiệp vụ xương sống phục vụ công tác đấu tranh phòng, chống tội phạm sử dụng công nghệ cao của lực lượng chuyên trách. Nền tảng tập trung vào hai nhóm chức năng cốt lõi:

- Tạo lập và Phân tích dữ liệu: Cung cấp bộ công cụ cho các đơn vị nghiệp vụ thực hiện tạo lập, tra cứu, khai thác và phân tích chuyên sâu các dữ liệu về phương thức, thủ đoạn, công cụ, phương tiện phạm tội. Qua đó, giúp nhận diện sớm các xu hướng tội phạm mới và làm giàu cho CSDL về Tội phạm sử dụng công nghệ cao (Lớp 2).

- Kết nối và Cảnh báo cộng đồng: Thiết lập cơ chế kết nối hai chiều (thông qua API bảo mật) để tiếp nhận dữ liệu cảnh báo rủi ro từ Ngân hàng Nhà nước, các tổ chức tài chính, sàn giao dịch. Đồng thời, hệ thống chủ động chia sẻ ngược lại các thông tin về phương thức lừa đảo, tài khoản/trang web độc hại đã được xác

minh. Thông tin này giúp các tổ chức và người dân nâng cao nhận thức, cảnh giác và tự bảo vệ mình khi thực hiện các giao dịch trên không gian mạng.

1) Nền tảng Hỗ trợ điều tra số (Digital Forensics)

Đây là bộ công cụ chuyên dụng phục vụ công tác kỹ thuật hình sự và tố tụng. Vai trò của nền tảng là cung cấp các phương tiện khoa học để chuyển hóa các dữ liệu điện tử vô hình thành các chứng cứ pháp lý hữu hình, có giá trị chứng minh tội phạm trước tòa án.

Về năng lực kỹ thuật, hệ thống bao gồm các công cụ phần cứng và phần mềm có khả năng trích xuất dữ liệu từ ổ cứng, điện thoại, đám mây (ngay cả khi đã bị xóa hoặc mã hóa). Quy trình xử lý bảo đảm tính toàn vẹn của chứng cứ và dữ liệu điện tử đáp ứng yêu cầu của pháp luật tố tụng hình sự.

4. Lớp 4: Kênh Tương tác và đo lường

Đây là lớp giao diện người dùng cuối và lớp trình diễn dữ liệu, nơi kết tinh giá trị của toàn bộ hệ thống để phục vụ hai nhóm đối tượng chính: Lãnh đạo ra quyết định và Xã hội (Tổ chức, người dân).

a) Các Kênh Dịch vụ công và Pháp lý

Đây là cổng giao tiếp chính thống về mặt thủ tục hành chính, bao gồm:

- Các Dịch vụ công lĩnh vực An ninh mạng trên Cổng Dịch vụ công Quốc gia: Là đầu mối thống nhất để người dân, doanh nghiệp nộp hồ sơ xin cấp phép kinh doanh dịch vụ an ninh mạng, nhập khẩu sản phẩm mật mã dân sự và các thủ tục liên quan khác.

- Cổng thông tin bảo vệ trẻ em trên không gian mạng: là nền tảng trực tuyến được xây dựng nhằm hỗ trợ phát hiện, tiếp nhận và xử lý các hành vi xâm hại, vi phạm quyền trẻ em trong môi trường số. Đây là kênh chính thức giúp cá nhân, tổ chức phản ánh, khiếu nại hoặc tố cáo các nội dung, hành vi gây ảnh hưởng tiêu cực đến trẻ em theo đúng quy định của pháp luật.

b) Các Kênh Truyền thông và Liên lạc

Nhóm kênh này bảo đảm dòng chảy thông tin thông suốt giữa cơ quan chức năng và cộng đồng:

- Hệ thống Website chính thức: Bao gồm Website của Bộ Công an về an ninh mạng và Website của Trung tâm VNCERT. Đây là nơi công bố các cảnh báo, văn bản quy phạm pháp luật và tin tức chính thống.

- Các trang Mạng xã hội (Fanpage/Official Account): Các kênh truyền thông trên các nền tảng mạng xã hội phổ biến, giúp lan tỏa thông tin tuyên truyền, cảnh báo phương thức thủ đoạn tội phạm nhanh chóng đến người dân.

- Ứng dụng liên lạc chuyên dụng: Nền tảng liên lạc bảo mật (Signet) phục vụ trao đổi thông tin, chỉ huy, điều hành về an ninh mạng, đặc biệt trong ứng phó, xử lý sự cố an ninh mạng.

c) Hệ sinh thái Ứng dụng và Tiện ích an ninh mạng cho người dân

Nhóm công cụ này trao quyền chủ động cho người dân trong việc tự bảo vệ mình trên không gian mạng:

- Kênh báo cáo lừa đảo trên VNeID: Tích hợp tính năng “Kiến nghị, phản ánh về ANTT” trên ứng dụng định danh điện tử quốc gia, cho phép hàng chục triệu người dân báo cáo nhanh các vụ việc lừa đảo, web độc hại.

- Công quản lý Tên định danh không gian mạng và Đầu số đăng ký không quảng cáo (Đầu số 5656): Hệ thống sử dụng đầu số 5656 (đã được chuyển giao quản lý từ Bộ TT&TT về Bộ Công an). Hệ thống thực hiện hai chức năng chính: tiếp nhận đăng ký từ chối nhận tin nhắn/cuộc gọi quảng cáo (DoNotCall) giúp người dân tránh bị làm phiền; và tiếp nhận hồ sơ đăng ký cấp tên định danh (Brandname) cho các tổ chức, cá nhân.

d) Bộ chỉ số đo lường an ninh mạng quốc gia

Theo Khung kiến trúc tổng thể quốc gia số, Bộ chỉ số giám sát và đo lường kết quả (KPI) bao gồm nhóm chỉ số “Kỹ thuật và an toàn”, trong đó có nội dung về an ninh mạng và bảo vệ dữ liệu; Bộ Công an chủ trì xây dựng nội dung nhóm chỉ số an ninh mạng và an ninh dữ liệu, trình cấp có thẩm quyền ban hành theo quy định.

5. Yêu cầu về khả năng chống chịu của các thành phần dùng chung

Các thành phần an ninh mạng dùng chung quốc gia phục vụ đồng thời nhiều cơ quan, tổ chức nên sự cố của một thành phần có thể ảnh hưởng trên phạm vi rộng. Việc thiết kế, triển khai và vận hành các thành phần này cần đáp ứng các yêu cầu sau:

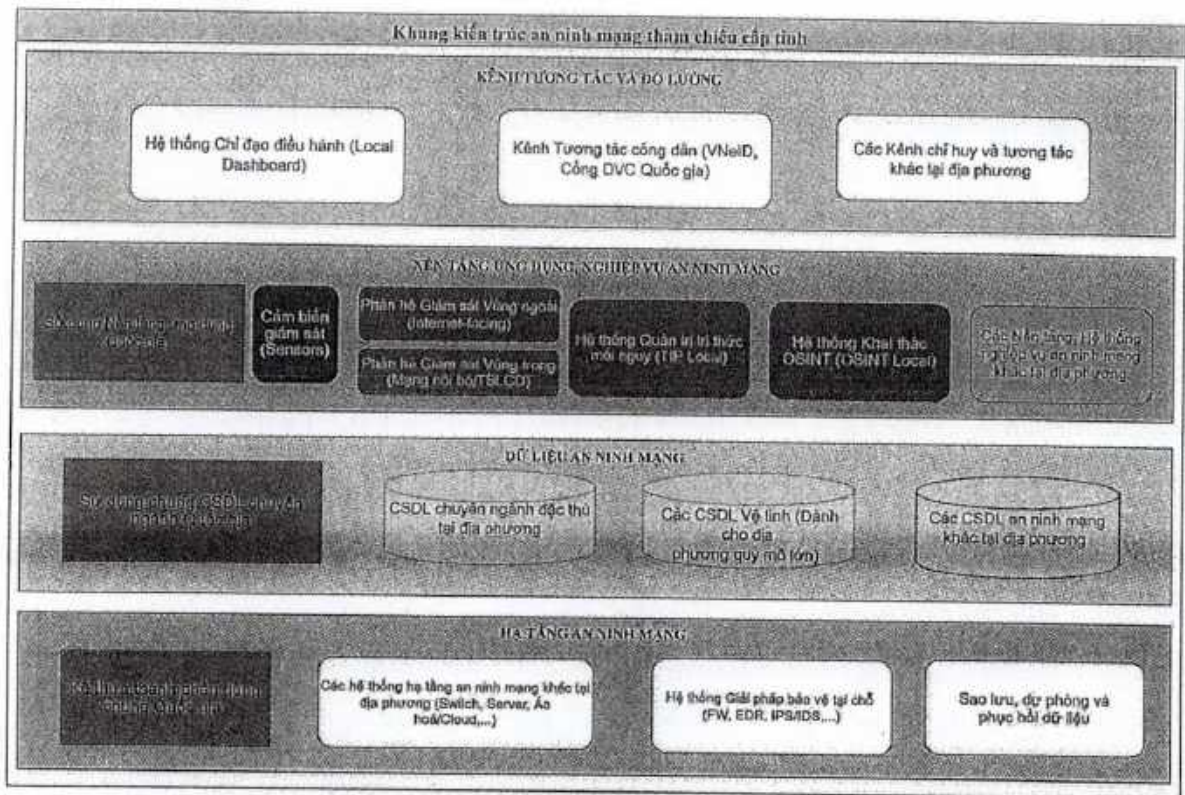
a) Bảo đảm tính sẵn sàng cao, không có điểm hỏng đơn; có phương án dự phòng và phục hồi tương ứng với mức độ ảnh hưởng khi xảy ra sự cố;

b) Xác định rõ chế độ vận hành khi thành phần gặp sự cố hoặc quá tải, bao gồm phương án cho phép lưu lượng đi qua hoặc ngăn chặn, bảo đảm không làm gián đoạn hoạt động cung cấp dịch vụ công thiết yếu;

c) Kho dữ liệu giám sát an ninh mạng quốc gia được bảo vệ theo chế độ đặc biệt: kiểm soát truy cập chặt chẽ theo vai trò, ghi nhật ký toàn bộ hành vi truy cập và định kỳ kiểm tra độc lập việc tuân thủ.

V. KHUNG KIẾN TRÚC AN NINH MẠNG THAM CHIẾU CẤP TỈNH

Mô hình này là khung kiến trúc khái niệm để Ủy ban nhân dân các tỉnh/thành phố trực thuộc trung ương tham chiếu, bổ sung các thành phần an ninh mạng vào Khung kiến trúc số cấp tỉnh. Tại địa phương, mô hình xoay quanh việc hình thành và vận hành Trung tâm an ninh mạng cấp tỉnh, do Công an tỉnh chủ trì quản lý và vận hành.



Hình 3: Kiến trúc an ninh mạng tham chiếu cho địa phương

Mô hình tuân thủ cấu trúc 04 lớp, bảo đảm tính liên thông với Kiến trúc An ninh mạng quốc gia và Kiến trúc tổng thể quốc gia số:

1. Lớp 1: Hạ tầng an ninh mạng (Cấp tỉnh)

Lớp này kết hợp giữa việc kế thừa tài nguyên quốc gia và chủ động triển khai các giải pháp bảo vệ tại chỗ cho hạ tầng số của địa phương:

a) Kế thừa thành phần dùng chung Quốc gia

Hạ tầng mạng cấp tỉnh được bảo vệ bởi các lá chắn từ lớp biên giới quốc gia, bao gồm: Hệ thống Tường lửa ứng dụng Web (WAF) quốc gia, Hệ thống Chống tấn công từ chối dịch vụ (Anti-DDoS) quốc gia và Mạng lưới phân phối nội dung (CDN) quốc gia. Các thành phần này giúp “làm sạch” lưu lượng truy cập trước khi đi vào hệ thống của tỉnh.

b) Hệ thống Giải pháp bảo vệ tại chỗ

Để bảo đảm an ninh chiều sâu, tỉnh triển khai các giải pháp bảo vệ trực tiếp tại Trung tâm dữ liệu và mạng diện rộng (WAN) của tỉnh. Các giải pháp bao gồm: Tường lửa thế hệ mới (NGFW), Hệ thống phát hiện và ngăn chặn xâm nhập (IPS/IDS), và Nền tảng bảo vệ thiết bị đầu cuối (EDR).

Sao lưu, dự phòng và phục hồi dữ liệu: do chủ quản hệ thống thông tin tự đầu tư, triển khai theo yêu cầu tương ứng với cấp độ hệ thống thông tin quy định tại TCVN 14423:2026, trong đó lưu ý áp dụng quy tắc sao lưu 3-2-1 và bảo đảm bản sao đặt cách biệt không bị ảnh hưởng khi hệ thống chính bị tấn công.

Lưu ý triển khai đồng bộ Nền tảng bảo vệ thiết bị đầu cuối thống nhất (Unified EDR) theo tiêu chuẩn của Bộ Công an cho toàn bộ máy trạm và máy chủ của các cơ quan, tổ chức chính trị tại địa phương để bảo đảm khả năng giám sát và phản ứng sự cố đồng bộ.

c) Các hệ thống hạ tầng an ninh mạng khác tại địa phương

Bao gồm các thiết bị, giải pháp hạ tầng đặc thù khác phù hợp với quy mô và yêu cầu thực tế của từng địa phương.

2. Lớp 2: Dữ liệu An ninh mạng (Cấp tỉnh)

Dữ liệu tại lớp này được tổ chức theo nguyên tắc “kết nối chia sẻ” và “đặc thù địa phương”. Các địa phương căn cứ vào tình hình an ninh trật tự và khả năng cân đối nguồn lực, chủ động xem xét đầu tư triển khai CSDL Vệ tinh của địa phương:

a) Sử dụng chung CSDL chuyên ngành quốc gia

Thông qua nền tảng tích hợp, chia sẻ dữ liệu (LGSP/NDXP), các hệ thống của tỉnh được quyền khai thác, tra cứu các CSDL chuyên ngành trong Kiến trúc An ninh mạng quốc gia (như CSDL Tội phạm công nghệ cao, CSDL Tri thức mối nguy, CSDL Tín nhiệm số) để phục vụ công tác quản lý và bảo vệ hệ thống.

b) CSDL chuyên ngành đặc thù tại địa phương

Tỉnh xây dựng và quản lý các CSDL phục vụ yêu cầu riêng biệt, như:

- CSDL Nhật ký an ninh (Log) tập trung: Lưu trữ logs từ toàn bộ hệ thống thông tin của các sở, ban, ngành, UBND xã/phường phục vụ điều tra, truy vết.

- CSDL Sao lưu dự phòng (Backup): Lưu trữ bản sao an toàn của các dữ liệu quan trọng (Đất đai, Hộ tịch, Dữ liệu điều hành...) tách biệt với mạng vận hành để phòng chống mã hóa dữ liệu (Ransomware).

c) Các CSDL Vệ tinh (Dành cho địa phương quy mô lớn)

Đối với các địa phương trọng điểm có quy mô hạ tầng CNTT lớn, để bảo đảm tính chủ động và tốc độ truy xuất cao, có thể xem xét đầu tư triển khai CSDL Tri thức mối nguy vệ tinh và CSDL Tình báo nguồn mở vệ tinh tại chỗ. Các CSDL vệ tinh này được đồng bộ dữ liệu chọn lọc từ CSDL Quốc gia nhưng vận hành độc lập tại địa phương, bảo đảm khả năng hoạt động liên tục ngay cả khi mất kết nối về Trung tâm dữ liệu quốc gia.

d) Các CSDL an ninh mạng khác tại địa phương

Các cơ sở dữ liệu nghiệp vụ khác được xây dựng theo nhu cầu quản lý đặc thù của địa phương.

3. Lớp 3: Nền tảng Ứng dụng, nghiệp vụ an ninh mạng (Cấp tỉnh)

Đây là lớp công cụ tác nghiệp chính của Trung tâm an ninh mạng cấp tỉnh (do Công an tỉnh vận hành).

a) Sử dụng Nền tảng ứng dụng quốc gia

Tỉnh không đầu tư xây dựng mới mà sử dụng lại các nền tảng nghiệp vụ đã được Bộ Công an triển khai thống nhất toàn quốc, bao gồm: Nền tảng quản lý rủi ro an ninh mạng (Cyber GRC), Định danh không gian mạng (NCIP), Nền tảng Hỗ trợ điều tra số... giúp tiết kiệm ngân sách và bảo đảm đồng bộ quy trình.

b) Hệ thống Trung tâm Giám sát an ninh mạng (Provincial SOC)

Hệ thống này được xây dựng tại tỉnh để giám sát 24/7 toàn bộ hệ thống Chính quyền điện tử/Chính quyền số. Kiến trúc hệ thống bao gồm:

- Cảm biến giám sát (Sensors): Được triển khai tại các điểm nút mạng trọng yếu, thực hiện thu thập dữ liệu và kết nối trực tiếp về Nền tảng Điều hành An ninh mạng Quốc gia (Bộ Công an) để chia sẻ thông tin giám sát.

- Phân hệ Giám sát Vùng ngoài (Internet-facing): Áp dụng cho các hệ thống công cộng (Cổng thông tin, Dịch vụ công). Trang bị đầy đủ SIEM (quản lý sự kiện) và SOAR (tự động hóa phản ứng) để xử lý nhanh các cuộc tấn công phổ biến từ Internet.

- Phân hệ Giám sát Vùng trong (Mạng nội bộ/TSLCD): Áp dụng cho mạng truyền số liệu chuyên dùng và mạng nội bộ. Tập trung sử dụng SIEM để phân tích hành vi người dùng, phát hiện rò rỉ dữ liệu và mã độc lây lan trong mạng kín.

c) Các Hệ thống ứng dụng chuyên sâu (Dành cho địa phương quy mô lớn)

Đối với các địa phương đã đầu tư CSDL Vệ tinh (nêu tại Lớp 2 ở trên), có thể triển khai thêm các hệ thống ứng dụng chuyên dụng tương ứng tại chỗ:

- Hệ thống Quản trị tri thức mối nguy (TIP Local): Để tự động hóa việc cập nhật mẫu dấu hiệu tấn công cho các thiết bị bảo mật của tỉnh.

- Hệ thống Khai thác OSINT (OSINT Local): Để chủ động rà quét, nắm bắt thông tin dư luận liên quan đến địa phương một cách nhanh chóng. Các hệ thống này giúp địa phương chủ động phân tích, khai thác và cập nhật dữ liệu cho các kho vệ tinh, giảm sự phụ thuộc hoàn toàn vào năng lực xử lý tập trung của trung ương.

d) Các Nền tảng, Hệ thống nghiệp vụ an ninh mạng khác tại địa phương

Các phần mềm, công cụ hỗ trợ tác nghiệp khác được trang bị theo yêu cầu thực tiễn của địa phương.

4. Lớp 4: Kênh Tương tác và đo lường (Cấp tỉnh)

Lớp này phục vụ công tác chỉ đạo của Tỉnh ủy, Ủy ban nhân dân tỉnh và tương tác với người dân địa phương:

a) Hệ thống Chỉ đạo điều hành (Local Dashboard)

Xây dựng Dashboard giám sát riêng tại chỗ, hiển thị các chỉ số an ninh mạng đặc thù của tỉnh. Hệ thống này hỗ trợ Ban Chỉ đạo An ninh mạng tỉnh nắm bắt tình hình, chỉ đạo các sở, ban, ngành thực hiện ứng cứu sự cố.

b) Kênh Tương tác công dân

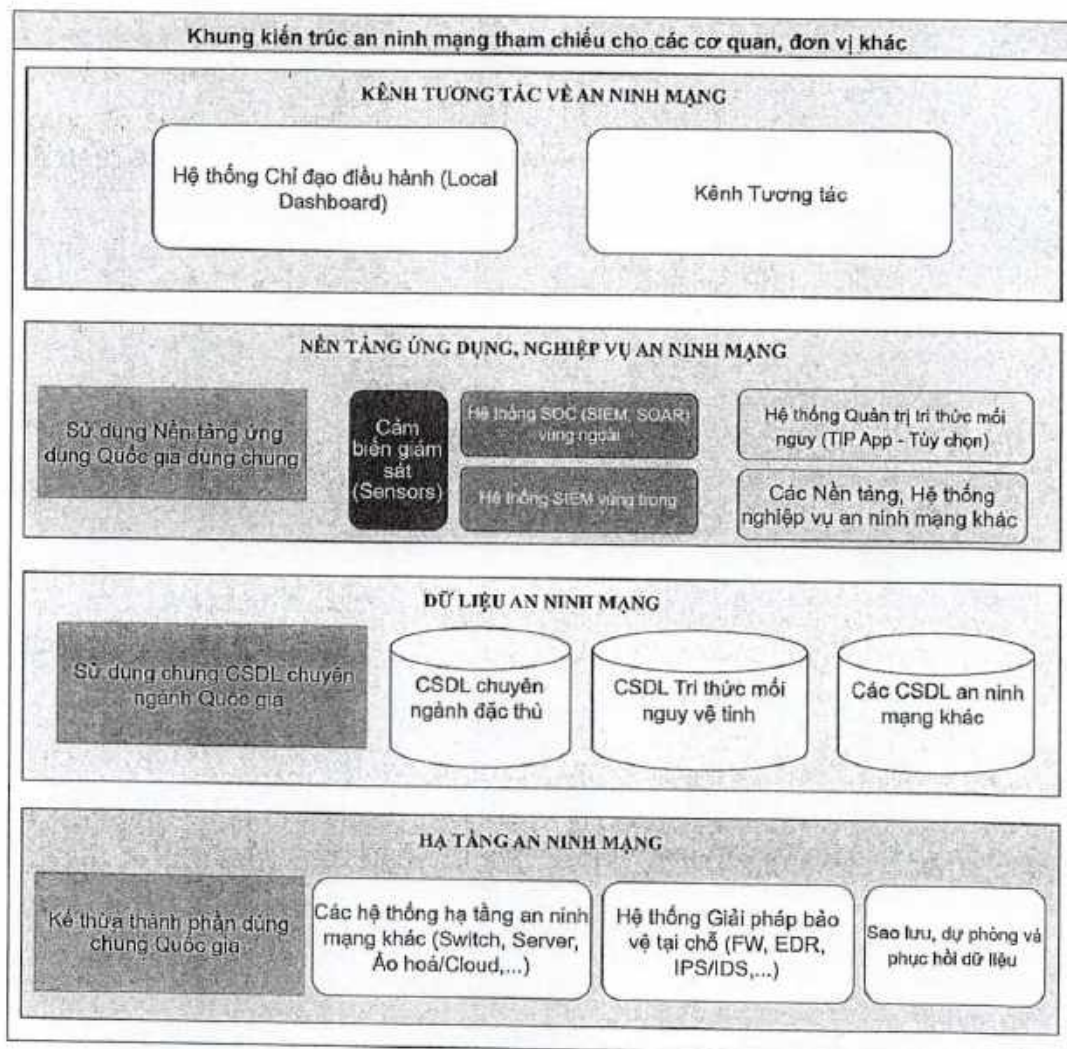
Tuân thủ sử dụng các kênh quốc gia (VNeID, Cổng DVC Quốc gia) làm nòng cốt. Đồng thời, tích hợp các tính năng báo cáo, phản ánh về an ninh mạng vào các Ứng dụng công dân số của tỉnh (như ứng dụng công dân số, thành phố thông minh,...) để tạo sự thuận tiện cho người dân địa phương.

c) Các Kênh chỉ huy và tương tác khác tại địa phương

Các kênh giao tiếp, chỉ đạo khác phù hợp với đặc thù của địa phương.

VI. KHUNG KIẾN TRÚC AN NINH MẠNG THAM CHIẾU CHO CÁC CƠ QUAN, ĐƠN VỊ KHÁC

Mô hình tham chiếu này áp dụng cho các cơ quan khối Đảng, Quốc hội, Mặt trận Tổ quốc, Chính phủ (các bộ, cơ quan ngang bộ) và các tập đoàn, tổng công ty nhà nước quan trọng và các cơ quan, đơn vị khác trong hệ thống chính trị. Mục tiêu là định hướng việc xây dựng thành phần an ninh mạng trong Khung kiến trúc số của từng ngành, lĩnh vực, bảo đảm tính đồng bộ và khả năng liên kết với Kiến trúc An ninh mạng Quốc gia.



Hình 4: Kiến trúc an ninh mạng tham chiếu cho các cơ quan, đơn vị khác

Mô hình tuân thủ cấu trúc 04 lớp, có sự tương đồng với mô hình tham chiếu cấp tỉnh nhưng được điều chỉnh để phù hợp với tính chất quản lý theo ngành dọc và yêu cầu bảo mật đặc thù của khối cơ quan trung ương:

1. Lớp 1: Hạ tầng An ninh mạng

Lớp này kết hợp giữa việc tận dụng năng lực bảo vệ quốc gia và triển khai các giải pháp phòng vệ chiều sâu tại Trung tâm dữ liệu của bộ/ngành:

a) Kế thừa thành phần dùng chung quốc gia

Hạ tầng mạng và các hệ thống Cổng thông tin điện tử, Dịch vụ công của bộ/ngành được bảo vệ bởi các lá chắn từ lớp biên giới quốc gia, bao gồm: Hệ thống Tường lửa ứng dụng Web (WAF) quốc gia, Hệ thống Chống tấn công từ chối dịch vụ (Anti-DDoS) quốc gia và Mạng lưới phân phối nội dung (CDN) quốc gia.

b) Hệ thống Giải pháp bảo vệ tại chỗ

Triển khai các giải pháp bảo vệ chuyên sâu tại Trung tâm dữ liệu, mạng diện rộng (WAN) và các hệ thống thông tin chuyên ngành. Các giải pháp bao gồm: Tường lửa thế hệ mới (NGFW), Hệ thống phát hiện và ngăn chặn xâm nhập (IPS/IDS), Nền tảng bảo vệ thiết bị đầu cuối (EDR).

Nguyên tắc phân vùng (Zoning): Đặc biệt chú trọng việc phân tách vùng mạng (DMZ, Server, Database, Management...) và kiểm soát truy cập nghiêm ngặt giữa các vùng để bảo vệ các CSDL quốc gia chuyên ngành do bộ/ngành quản lý.

Sao lưu, dự phòng và phục hồi dữ liệu: do chủ quản hệ thống thông tin tự đầu tư, triển khai theo yêu cầu tương ứng với cấp độ hệ thống thông tin quy định tại TCVN 14423:2026, trong đó lưu ý áp dụng quy tắc sao lưu 3-2-1 và bảo đảm bản sao đặt cách biệt không bị ảnh hưởng khi hệ thống chính bị tấn công.

c) Các hệ thống hạ tầng an ninh mạng khác

Các thiết bị, giải pháp hạ tầng đặc thù khác phù hợp với quy mô và yêu cầu thực tế của từng bộ, ngành.

2. Lớp 2: Dữ liệu An ninh mạng (Cấp bộ/ngành/tổ chức)

Dữ liệu được tổ chức theo nguyên tắc “kết nối chia sẻ” và phục vụ quản lý chuyên ngành:

a) Sử dụng chung CSDL chuyên ngành quốc gia

Thông qua nền tảng tích hợp, chia sẻ dữ liệu (LGSP/NDXP), các hệ thống của bộ/ngành được quyền khai thác, tra cứu các CSDL chuyên ngành trong Kiến trúc An ninh mạng quốc gia (như CSDL Tội phạm công nghệ cao, CSDL Tri thức mối nguy, CSDL Tín nhiệm số) để phục vụ công tác quản lý và bảo vệ hệ thống.

b) CSDL chuyên ngành đặc thù

Xây dựng và quản lý các CSDL phục vụ yêu cầu riêng biệt của ngành, tiêu biểu:

- CSDL Nhật ký an ninh (Log) tập trung: Lưu trữ logs từ toàn bộ hệ thống thông tin của Bộ/Ngành theo quy định pháp luật.

- CSDL Sao lưu dự phòng (Backup): Bảo đảm khả năng phục hồi dữ liệu nghiệp vụ quan trọng khi xảy ra sự cố.

c) CSDL Tri thức mối nguy vệ tinh (Tùy chọn)

Đối với các bộ, ngành có hệ thống CNTT quy mô lớn và đội ngũ chuyên gia an ninh mạng chuyên trách, có thể cân nhắc triển khai CSDL Tri thức mối nguy (Threat Intelligence) vệ tinh. CSDL này giúp đơn vị chủ động quản lý các mẫu nhận diện tấn công đặc thù của ngành mình, song song với việc đồng bộ dữ liệu từ CSDL quốc gia.

d) Các CSDL an ninh mạng khác

Các cơ sở dữ liệu nghiệp vụ khác được xây dựng theo nhu cầu quản lý đặc thù.

3. Lớp 3: Nền tảng Ứng dụng, nghiệp vụ an ninh mạng (Cấp bộ/ngành/tổ chức)

Lớp này cung cấp công cụ giám sát và tác nghiệp cho đơn vị chuyên trách về CNTT/ANM của bộ/ngành.

a) Sử dụng Nền tảng ứng dụng quốc gia

Sử dụng các nền tảng nghiệp vụ dùng chung quốc gia như: Nền tảng quản lý rủi ro an ninh mạng (Cyber GRC), Định danh không gian mạng (NCIP), Nền tảng Hỗ trợ điều tra số... để bảo đảm tính đồng bộ và hiệu quả.

b) Hệ thống Trung tâm Giám sát an ninh mạng (Ministerial/Agency SOC)

Hệ thống SOC cấp bộ/ngành thực hiện giám sát 24/7 cho các hệ thống thông tin thuộc phạm vi quản lý. Hệ thống này có thể tự triển khai hoặc thuê lại của các đơn vị cung cấp dịch vụ SOC được cấp phép theo quy định. Kiến trúc bao gồm:

- Cảm biến giám sát (Sensors): Kết nối trực tiếp về Nền tảng Điều hành An ninh mạng Quốc gia (Bộ Công an) để chia sẻ thông tin giám sát và sự cố.

- Hệ thống SIEM: Thu thập và phân tích sự kiện an ninh từ cả vùng mạng ngoài và mạng nội bộ.

- Hệ thống SOAR (Tùy chọn): Có thể triển khai nếu quy mô hệ thống lớn, cần tự động hóa quy trình phản ứng. Nếu không, có thể sử dụng cơ chế điều phối tại chỗ thủ công và kết nối với hệ thống điều phối quốc gia.

c) Hệ thống Quản trị tri thức mối nguy (TIP - Tùy chọn)

Đi kèm với CSDL Tri thức mối nguy vệ tinh (nếu có đầu tư), đơn vị có thể triển khai ứng dụng TIP để chủ động thu thập, phân tích và chia sẻ các chỉ dấu xâm phạm (IoC) trong phạm vi nội bộ ngành.

d) Các Nền tảng, Hệ thống nghiệp vụ an ninh mạng khác

Các phần mềm, công cụ hỗ trợ tác nghiệp khác được trang bị theo yêu cầu thực tiễn.

4. Lớp 4: Kênh Tương tác và đo lường (Cấp bộ/ngành/tổ chức)

a) Hệ thống Chi đạo điều hành (Local Dashboard)

Xây dựng Dashboard giám sát riêng, hiển thị tình hình an ninh mạng của toàn ngành, phục vụ lãnh đạo bộ/ngành và Ban Chỉ đạo Chuyển đổi số chỉ đạo điều hành.

b) Kênh Tương tác

Tương tác nội bộ: Sử dụng hệ thống liên lạc chuyên dụng (như Signet, Email công vụ). Yêu cầu sử dụng kênh liên lạc đặc dụng Signet trong ứng phó xử lý sự cố an ninh mạng; hạn chế/tránh sử dụng các kênh email hoặc các ứng dụng OTT thông thường để bảo đảm tính bảo mật.

VII. CÁC THÀNH PHẦN BỒ TRỢ VÀ KHUNG QUẢN TRỊ

Thực hiện chủ trương tại Chỉ thị số 57-CT/TW của Ban Bí thư về tập trung nguồn lực xây dựng nền công nghiệp an ninh mạng tự chủ, tự cường; ưu tiên phát triển các sản phẩm "Make in Vietnam", cần huy động các nguồn lực trong xã hội phát triển năng lực tự chủ, giảm lệ thuộc vào công nghệ nước ngoài trong công tác bảo đảm an ninh mạng.

1. Sản phẩm công nghiệp an ninh trong lĩnh vực an ninh mạng

Các nhóm sản phẩm cốt lõi, nền tảng được ưu tiên làm chủ và sản xuất trong nước bao gồm: giải pháp tường lửa; phòng, chống mã độc; bảo vệ thiết bị đầu cuối; nền tảng điện toán đám mây và hệ điều hành dùng riêng. Đây là các nhóm sản phẩm nắm quyền kiểm soát ở tầng hạ tầng mạng, nhân hệ điều hành và ảo hóa; việc làm chủ các sản phẩm này quyết định khả năng tự chủ của toàn bộ hệ thống phòng thủ quốc gia.

Việc phát triển các nhóm sản phẩm nêu trên thực hiện theo các nhiệm vụ đã được giao tại Quyết định số 808/QĐ-TTg của Thủ tướng Chính phủ về giao nhiệm vụ phát triển công nghệ chiến lược, gồm: "Phát triển nền tảng bảo mật và an ninh mạng cho hạ tầng số quốc gia" và "Xây dựng và phát triển nền tảng điện toán đám mây nội địa phục vụ chuyển đổi số quốc gia, bảo đảm chủ quyền dữ liệu".

2. Khung Quản trị, Pháp lý và Tiêu chuẩn (GRC)

Đây là các yếu tố phi kỹ thuật nhưng đóng vai trò quyết định đến sự thành công của Khung kiến trúc.

a) Hành lang Pháp lý và Tiêu chuẩn

Hệ thống khung pháp lý nền tảng được xác lập dựa trên các văn bản quy phạm pháp luật trọng tâm, bao gồm: Luật An ninh mạng số 116/2023/QH15, Luật Giao dịch điện tử số 20/2023/QH15; cùng các văn bản luật chuyên ngành mang tính chiến lược là Luật Dữ liệu số 60/2024/QH15, Luật Công nghiệp công nghệ

số 71/2025/QH15 và Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15; Luật Trí tuệ nhân tạo số 134/2025/QH15; Luật Chuyển đổi số số 148/2025/QH15.

Bộ tiêu chuẩn áp dụng: TCVN 14423:2026, ISO 27001, ISO 27701.

b) Khung Quản trị rủi ro và Quy trình vận hành

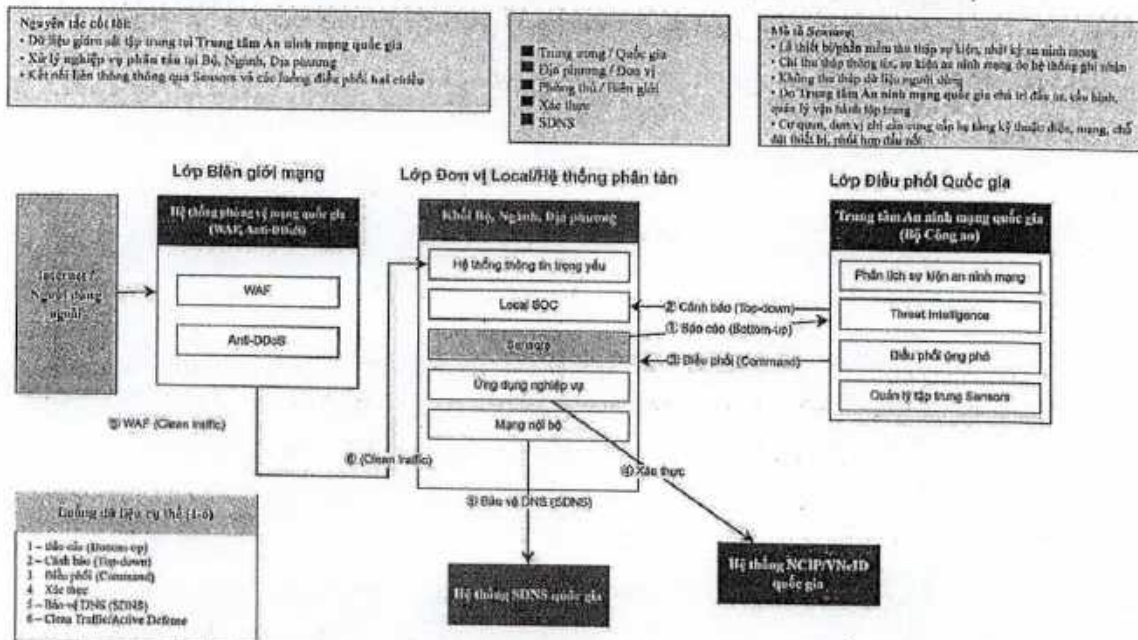
Khung quản lý rủi ro an ninh mạng: Xác định phương pháp luận, tiêu chí đánh giá và cơ chế kiểm soát rủi ro thống nhất. Chuyển dịch tư duy từ “tuân thủ theo mẫu” sang “quản lý dựa trên rủi ro thực tế”, giúp các cơ quan chủ động nhận diện các điểm yếu nhất trong hệ thống của mình.

Quy trình điều phối, ứng phó xử lý sự cố an ninh mạng quốc gia: Quy định chi tiết, cụ thể các bước thực hiện (SOP) từ khi phát hiện, thông báo, khoanh vùng, xử lý đến phục hồi sau sự cố. Quy trình này xác định rõ thẩm quyền chỉ huy của Trung tâm An ninh mạng quốc gia Bộ Công an và trách nhiệm phối hợp của các đơn vị thành viên trong các tình huống khẩn cấp, bảo đảm phản ứng nhanh chóng, đồng bộ.

VIII. MÔ HÌNH LIÊN THÔNG VÀ TÍCH HỢP

Mô hình hoạt động dựa trên nguyên tắc: “Dữ liệu giám sát tập trung - Xử lý nghiệp vụ phân tán”.

Mô hình liên thông và tích hợp – Dữ liệu giám sát tập trung, xử lý nghiệp vụ phân tán



Hình 5: Mô hình liên thông và tích hợp hệ thống an ninh mạng quốc gia

1. Cơ chế kết nối và tích hợp hệ thống

Để kết nối hàng nghìn hệ thống thông tin đơn lẻ thành một mạng lưới phòng thủ quốc gia, Khung kiến trúc sử dụng Cảm biến (Sensors).

Cảm biến (Sensors): Là các thiết bị phần cứng hoặc phần mềm có chức năng thu thập thông tin an ninh mạng cần thiết đặt tại hạ tầng của các cơ quan, đơn vị

trung chuyển về Trung tâm an ninh mạng quốc gia. Các thông tin dữ liệu thu thập chỉ bao gồm các thông tin, sự kiện an ninh mạng do hệ thống ghi nhận, không thu thập các dữ liệu của người dùng trên các hệ thống thông tin.

Các cảm biến này do Trung tâm An ninh mạng quốc gia (Bộ Công an) chủ trì đầu tư, cấu hình và quản lý vận hành tập trung. Điều này bảo đảm tính thống nhất về công nghệ và chất lượng dữ liệu thu thập.

Trách nhiệm của các cơ quan, đơn vị: Các cơ quan, đơn vị không phải đầu tư thiết bị cảm biến giám sát quốc gia. Thay vào đó, có trách nhiệm bố trí mặt bằng, cung cấp hạ tầng kỹ thuật (nguồn điện, kết nối mạng, chỗ đặt thiết bị trên tủ Rack) và phối hợp với cán bộ kỹ thuật của Bộ Công an để đấu nối, tích hợp hệ thống Cảm biến vào hạ tầng mạng nội bộ.

Bộ Công an chủ trì, phối hợp với Bộ Tài chính ban hành quy định về cơ chế tài chính hoặc văn bản hướng dẫn địa phương bố trí nguồn kinh phí chi thường xuyên hàng năm để duy trì hạ tầng phục vụ cho hoạt động của hệ thống Cảm biến (Sensors) đặt tại địa phương.

2. Các luồng dữ liệu nghiệp vụ trọng yếu

Hệ thống vận hành dựa trên 06 luồng dữ liệu chính, tạo thành vòng tròn khép kín từ giám sát đến phản ứng:

Luồng 1 (Báo cáo): Hệ thống giám sát tại chỗ (Local SOC) và các Cảm biến tự động đẩy nhật ký sự kiện, báo cáo sự cố, mẫu mã độc nghi ngờ về trung tâm An ninh mạng quốc gia để phân tích. Cảm biến và Local SOC chỉ gửi các cảnh báo thật sự nghiêm trọng, nhằm hạn chế tình trạng quá nhiều thông tin không cần thiết.

Luồng 2 (Cảnh báo): Sau khi phân tích, Trung ương chia sẻ lại dữ liệu Threat Intelligence (IP Blacklist, Hash mã độc mới) về cho Local SOC. Đơn vị sử dụng dữ liệu này để cập nhật luật chặn lọc cho tường lửa, giúp phát hiện các tấn công mà trước đó họ không biết.

Luồng 3 (Điều phối): Cơ quan chuyên trách tại địa phương chủ động quyết định cô lập, xử lý các sự cố mức độ nhẹ hoặc trung bình. Trong trường hợp tấn công diện rộng, Trung tâm An ninh mạng quốc gia (Bộ Công an) gửi Lệnh điều phối ứng phó xuống các đơn vị, yêu cầu thực hiện các hành động cụ thể (như chặn IP, cách ly máy chủ).

Luồng 4 (Xác thực): Các ứng dụng nghiệp vụ tại địa phương gọi dịch vụ xác thực và định danh điện tử (qua NCIP/VNeID) của Quốc gia để xác minh danh tính người dùng.

Luồng 5 (Bảo vệ truy cập - SDNS): Toàn bộ truy vấn tên miền (DNS Query) từ mạng nội bộ của các cơ quan nhà nước được định tuyến qua hệ thống SDNS Quốc gia. Hệ thống sẽ lọc bỏ các yêu cầu truy cập đến tên miền độc hại trước khi kết nối được thiết lập, ngăn chặn người dùng vô tình truy cập web độc hại, lừa đảo.

Luồng 6 (Làm sạch lưu lượng - Phòng vệ chủ động): Lưu lượng truy cập từ Internet vào các hệ thống quan trọng (Cổng DVC, Email công vụ...) được điều hướng đi qua Hệ thống phòng vệ mạng quốc gia (WAF, Anti-DDoS) tại biên giới mạng. Tại đây, lưu lượng tấn công bị loại bỏ, chỉ có lưu lượng sạch được chuyển về hệ thống đích tại bộ, ngành, địa phương.

IX. TỔ CHỨC TRIỂN KHAI

1. Phân công trách nhiệm

a) Bộ Công an

- Chủ trì đầu tư, quản lý, vận hành các Thành phần dùng chung (Lớp 1, 2, 3) và chủ trì, phối hợp triển khai các kênh tương tác lên các Cổng tương tác dùng chung quốc gia (Lớp 4).

- Đầu tư và tổ chức triển khai hệ thống Cảm biến giám sát tại các bộ, ngành, địa phương.

- Chủ trì thẩm định, đánh giá và kiểm tra sự phù hợp của các thành phần, giải pháp bảo đảm an ninh mạng tại các đơn vị đối với Khung kiến trúc này; chủ trì hướng dẫn phương pháp đánh giá, giám sát mức độ tuân thủ Khung kiến trúc an ninh mạng quốc gia. Kết quả đánh giá mức độ tương thích với Khung kiến trúc được xem xét như một cơ sở kỹ thuật quan trọng trong quá trình thẩm định, kiểm tra điều kiện an ninh mạng theo quy định của Luật An ninh mạng và các văn bản hướng dẫn thi hành.

- Ban hành tiêu chuẩn kỹ thuật, cơ chế kết nối và nền tảng quản trị tập trung đối với hạ tầng bảo đảm an ninh, an toàn dữ liệu đầu cuối; chủ trì xây dựng nội dung nhóm chỉ số an ninh mạng trong Bộ chỉ số giám sát và đo lường kết quả (KPI) của Khung kiến trúc tổng thể quốc gia số.

- Chủ trì hoạch định, xây dựng hệ thống tiêu chuẩn, quy chuẩn kỹ thuật quốc gia và hướng dẫn kỹ thuật về an ninh mạng³, bao gồm quy chuẩn kỹ thuật về kết nối, chia sẻ dữ liệu; ban hành quy chuẩn kỹ thuật quốc gia thuộc thẩm quyền.

- Bảo đảm an ninh mạng đối với hệ thống thông tin trong hệ thống chính trị theo quy định của Luật An ninh mạng, bao gồm cả hệ thống có sử dụng sản phẩm mật mã cơ yếu; việc bảo mật thông tin bằng mật mã cơ yếu do Ban Cơ yếu Chính phủ thực hiện theo phạm vi quy định tại khoản 3 Điều 34 Nghị định số 331/2026/NĐ-CP.

- Chủ trì, phối hợp với Bộ Tài chính ban hành quy định về cơ chế tài chính hoặc văn bản hướng dẫn địa phương bố trí nguồn kinh phí chi thường xuyên hằng năm để duy trì hạ tầng phục vụ hoạt động của hệ thống Cảm biến giám sát.

³ Bảng trên được lập trên cơ sở đối chiếu nội dung Khung kiến trúc an ninh mạng quốc gia với Quyết định số 1425/QĐ-TTg ngày 29/7/2026 của Thủ tướng Chính phủ.

- Ban hành quy định chi tiết về giao thức kết nối hệ thống giám sát, cấu trúc trường dữ liệu giám sát và thông tin sự cố an ninh mạng cần báo cáo, phục vụ thực hiện trách nhiệm vụ báo cáo sự cố quy định tại điểm d khoản 2 Điều 31 Nghị định số 331/2026/NĐ-CP; công bố trên Hệ thống quản lý kiến trúc số quốc gia.

- Đầu tư, quản lý và vận hành Nền tảng phát hiện tài sản và quản lý bề mặt tấn công quốc gia; tổ chức phát hiện, cảnh báo tới chủ quản hệ thống thông tin về tài sản có nguy cơ và lỗ hổng bảo mật đang bị khai thác.

- Xây dựng, quản lý và vận hành Cơ sở dữ liệu Tín nhiệm số; tổ chức đánh giá, công bố mức độ tín nhiệm của chủ thể, tài nguyên số trên không gian mạng.

- Xây dựng, ban hành và thường xuyên rà soát, cập nhật danh mục sản phẩm công nghiệp an ninh, trong đó có các sản phẩm thuộc lĩnh vực an ninh mạng; tổ chức đánh giá, kiểm định làm cơ sở bổ sung vào danh mục các sản phẩm đáp ứng yêu cầu và đưa ra khỏi danh mục các sản phẩm không còn phù hợp; chủ trì huy động các nguồn lực trong xã hội phát triển năng lực tự chủ về công nghệ, giảm lệ thuộc vào công nghệ nước ngoài trong công tác bảo đảm an ninh mạng.

- Đối với các thành phần tại dòng 3 và dòng 10 Phụ lục A, tổ chức rà soát, đề xuất cấp có thẩm quyền xem xét, bổ sung vào danh mục nền tảng số dùng chung quốc gia trước khi ban hành chính thức.

b) Bộ Khoa học và Công nghệ

- Chủ trì, phối hợp Bộ Công an ban hành chi tiết Bộ chỉ số giám sát và đo lường kết quả (KPI), phương pháp đo lường, tiêu chí đánh giá và cơ chế báo cáo theo quy định tại Khung kiến trúc tổng thể quốc gia số.

- Chủ trì hướng dẫn phương pháp đánh giá, giám sát mức độ tuân thủ Khung kiến trúc tổng thể quốc gia số theo quy định của pháp luật, trong đó Bộ Công an chủ trì nội dung liên quan đến an ninh mạng theo quy định tại điểm a khoản 3 Điều 2 Quyết định số 1425/QĐ-TTg.

c) Ban Cơ yếu Chính phủ

Quản lý, hướng dẫn tiêu chuẩn mật mã cơ yếu và chữ ký số chuyên dùng công vụ áp dụng trong Khung kiến trúc an ninh mạng quốc gia; triển khai sản phẩm mật mã cơ yếu và hệ thống thông tin cơ yếu để bảo vệ bí mật nhà nước; bảo đảm an ninh mạng theo cấp độ đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ theo quy định tại khoản 3 Điều 34 Nghị định số 331/2026/NĐ-CP.

d) Bộ Quốc phòng

Tham khảo, áp dụng Khung kiến trúc này hoặc xây dựng Khung kiến trúc an ninh mạng chuyên biệt đồng bộ đối với các hệ thống thông tin thuộc phạm vi quản lý; ranh giới thẩm quyền quản lý về an ninh mạng giữa Bộ Công an và Bộ Quốc phòng thực hiện theo quy định tại khoản 4 Điều 6 Nghị định số 331/2026/NĐ-CP.

đ) Bộ Tài chính

Chủ trì, phối hợp Bộ Công an hướng dẫn cơ chế bố trí, sử dụng kinh phí chi thường xuyên và kinh phí đầu tư phục vụ triển khai Khung kiến trúc an ninh mạng quốc gia, trong đó có kinh phí duy trì hạ tầng phục vụ hoạt động của hệ thống Cảm biến giám sát đặt tại các bộ, ngành, địa phương.

e) Bộ Nội vụ

Hướng dẫn việc sử dụng kết quả nhóm chỉ số an ninh mạng làm một trong các nội dung đánh giá, xếp loại chất lượng hằng năm đối với người đứng đầu cơ quan, tổ chức theo quy định của pháp luật về cán bộ, công chức.

g) Các bộ, ngành, địa phương và các cơ quan, đơn vị liên quan

- Tuân thủ Khung kiến trúc: Không đầu tư trùng lặp các hệ thống mà quốc gia đã cung cấp dùng chung.

- Tập trung nguồn lực: Ưu tiên ngân sách để bảo vệ các lớp ứng dụng và dữ liệu đặc thù; trang bị đồng bộ các sản phẩm chiến lược (EDR, Firewall) tại đơn vị.

- Phối hợp triển khai: Cung cấp hạ tầng kỹ thuật và phối hợp chặt chẽ với Bộ Công an trong việc lắp đặt cảm biến, đấu nối hệ thống và thực hiện quy trình ứng phó sự cố an ninh mạng.

- Đối với hệ thống thông tin từ Cấp độ 3 trở lên và hệ thống thông tin quan trọng về an ninh quốc gia: kết nối, gửi dữ liệu giám sát an ninh mạng về nền tảng SOC quốc gia hoặc Trung tâm An ninh mạng cấp tỉnh theo phân cấp; thực hiện thông báo, báo cáo sự cố an ninh mạng theo quy định tại điểm d khoản 2 Điều 31 Nghị định số 331/2026/NĐ-CP.

- Đối với hạ tầng bảo đảm an ninh, an toàn dữ liệu đầu cuối: chủ động đầu tư, triển khai theo tiêu chuẩn kỹ thuật do Bộ Công an ban hành.

- Không phải đầu tư thiết bị cảm biến giám sát quốc gia; có trách nhiệm bố trí mặt bằng, cung cấp hạ tầng kỹ thuật (nguồn điện, kết nối mạng, chỗ đặt thiết bị...) phục vụ lắp đặt cảm biến.

- Ưu tiên sử dụng các sản phẩm thuộc danh mục sản phẩm công nghiệp an ninh trong lĩnh vực an ninh mạng do Bộ Công an ban hành, đặc biệt là các sản phẩm có khả năng kết nối, kế thừa tri thức từ Cơ sở dữ liệu Tri thức mối nguy an ninh mạng quốc gia.

- Trong ứng phó, xử lý sự cố an ninh mạng, sử dụng kênh liên lạc đặc dụng (Signet); không sử dụng email hoặc các ứng dụng nhắn tin, gọi điện trực tuyến (OTT) khác.

- Đăng ký và duy trì đầu mối tiếp nhận cảnh báo; rà soát, xác nhận danh mục tài sản số do Nền tảng phát hiện tài sản và quản lý bề mặt tấn công quốc gia cung cấp; xử lý các cảnh báo về lỗ hổng bảo mật theo quy định.

h) Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia

Tuân thủ các yêu cầu áp dụng đối với các bộ, cơ quan ngang bộ, Ủy ban nhân dân cấp tỉnh nêu trên; chủ động bố trí nguồn lực đầu tư các thành phần an ninh mạng tại chỗ theo yêu cầu tối thiểu tương ứng với cấp độ hệ thống thông tin; phối hợp với Bộ Công an trong công tác kết nối, giám sát và ứng phó sự cố an ninh mạng.

i) Đề nghị các cơ quan của Đảng, Quốc hội, Văn phòng Chủ tịch nước, Ủy ban Trung ương Mặt trận Tổ quốc Việt Nam, Tòa án nhân dân, Viện kiểm sát nhân dân

Nghiên cứu, áp dụng Khung kiến trúc an ninh mạng quốc gia phù hợp với chức năng, nhiệm vụ và đặc thù tổ chức. a) Giai đoạn 1 (2026 - 2027): Giai đoạn nền tảng.

2. Lộ trình triển khai

a) Giai đoạn 1 (2026 - 2027): Giai đoạn nền tảng.

- Hoàn thiện các Nền tảng lõi tại trung ương
- Ban hành Quy chuẩn kết nối.
- Triển khai thí điểm Cảm biến tại các bộ, ngành trọng yếu.

b) Giai đoạn 2 (2027 - 2028): Kết nối.

- Hoàn thành việc kết nối hệ thống thông tin từ cấp độ 3 trở lên của các bộ, ngành, địa phương vào hệ thống giám sát quốc gia.
- Vận hành chính thức hệ thống Phòng vệ mạng quốc gia và các thành phần dùng chung khác phục vụ các đơn vị.

c) Giai đoạn 3 (2029 - 2030): Thông minh hóa.

- Tự động hóa quy trình ứng phó (SOAR) trên quy mô toàn quốc.
- Hoàn thiện hệ sinh thái dữ liệu an ninh mạng, áp dụng AI sâu rộng trong phòng vệ chủ động.

Điều khoản chuyển tiếp: Căn cứ vào điều kiện thực tiễn, nguồn lực và lộ trình chuyển đổi số của từng ngành, các cơ quan, đơn vị chủ động xây dựng kế hoạch rà soát, đánh giá hệ thống hiện hữu. Ưu tiên bố trí nguồn lực để từng bước nâng cấp, kết nối đáp ứng các tiêu chuẩn kỹ thuật của Khung kiến trúc này. Quá trình triển khai được khuyến khích phấn đấu hoàn thành các mục tiêu kết nối cơ bản trong khoảng thời gian 24 tháng kể từ ngày Quyết định này có hiệu lực, bảo đảm không làm gián đoạn các hoạt động dịch vụ công.



Phụ lục II
BẢNG ANH XA THÀNH PHẦN KHUNG KIẾN TRÚC AN NINH MẠNG
QUỐC GIA VỚI KHUNG KIẾN TRÚC TỔNG THỂ QUỐC GIA SỐ¹
(Kèm theo Quyết định số 1875/QĐ-TTg
ngày 30 tháng 9 năm 2026 của Thủ tướng Chính phủ)

TT	Thành phần trong Khung kiến trúc an ninh mạng quốc gia	Vị trí trong Khung kiến trúc tổng thể quốc gia số	Cơ quan chủ quản	Quan hệ
1	Hệ thống Tường lửa ứng dụng Web quốc gia (National WAF)	Lớp 1 - Thành phần an ninh mạng (Hệ thống phòng vệ mạng quốc gia)	Bộ Công an	Kế thừa
2	Hệ thống Chống tấn công từ chối dịch vụ quốc gia (National Anti-DDoS)	Lớp 1 - Thành phần an ninh mạng (Hệ thống phòng vệ mạng quốc gia)	Bộ Công an	Kế thừa
3	Mạng lưới phân phối nội dung quốc gia (National CDN)	Lớp 1 - Thành phần an ninh mạng (Hệ thống phòng vệ mạng quốc gia - dịch vụ lọc và điều phối lưu lượng thông minh)	Bộ Công an	Kế thừa, chi tiết hóa
4	Hạ tầng bảo đảm an ninh, an toàn dữ liệu đầu cuối	Lớp 1 - Thành phần an ninh mạng (Hệ thống phòng vệ mạng quốc gia)	Chủ quản hệ thống thông tin đầu cuối triển khai; Bộ Công an ban hành tiêu chuẩn, nền tảng quản trị tập trung	Kế thừa, chi tiết hóa đúng chủ thể
5	Hạ tầng mật mã, chứng thực chữ ký số chuyên dùng công vụ	Lớp 1 - Hạ tầng số (Hệ thống chứng thực chữ ký số chuyên dùng công vụ)	Ban Cơ yếu Chính phủ	Kế thừa, dẫn chiếu

¹ Các nhóm sản phẩm, giải pháp an ninh mạng thuộc phạm vi xây dựng, ban hành tiêu chuẩn, quy chuẩn kỹ thuật bao gồm nhưng không giới hạn: hệ thống quản lý sự kiện và thông tin bảo mật (SIEM); nền tảng điều phối, tự động hóa và phản ứng bảo mật (SOAR); nền tảng tri thức mối nguy an ninh mạng (TIP); hệ thống ngăn chặn xâm nhập mạng (NIPS); giải pháp phát hiện và phản ứng tại thiết bị đầu cuối (EDR); giải pháp quản lý truy cập đặc quyền (PAM); thiết bị diode dữ liệu; cổng bảo mật một chiều (USG); cổng bảo mật hai chiều (BSG); nền tảng điện toán đám mây.

6	Giải pháp bảo mật cho hệ thống gửi, nhận văn bản mật	Lớp 1 - Thành phần an ninh mạng	Ban Cơ yếu Chính phủ chủ trì, phối hợp Bộ Công an	Kế thừa
7	Nền tảng Điều hành an ninh mạng quốc gia (National SOC & Orchestration)	Lớp 1 - Thành phần an ninh mạng (Nền tảng điều hành an ninh mạng quốc gia)	Bộ Công an	Kế thừa, chi tiết hóa
8	04 cơ sở dữ liệu chuyên ngành an ninh mạng	Lớp 2 - Dữ liệu và nền tảng lõi (nhóm cơ sở dữ liệu quốc gia, trọng yếu, chuyên ngành)	Bộ Công an	Chi tiết hóa
9	Định danh không gian mạng (NCIP)	Lớp 2 - thành phần thuộc Nền tảng định danh và xác thực điện tử	Bộ Công an	Là thành phần thuộc Nền tảng định danh và xác thực điện tử tại Lớp 2 Khung kiến trúc tổng thể quốc gia số
10	TIP, SDNS, Cyber GRC, Managed SOC, nền tảng hỗ trợ điều tra số (Lớp 3 - Nhóm A)	Chưa có trong Phụ lục II (danh mục nền tảng số dùng chung quốc gia) của Khung kiến trúc tổng thể quốc gia số	Bộ Công an	Đề xuất bổ sung vào danh mục nền tảng số dùng chung quốc gia theo Quyết định số 1132/QĐ-TTg
11	Hệ thống nghiệp vụ chuyên trách của Bộ Công an (Lớp 3 - Nhóm B)	Không thuộc phạm vi thành phần dùng chung quốc gia của Khung kiến trúc tổng thể quốc gia số	Bộ Công an	Thuộc Khung kiến trúc số của Bộ Công an; không phải thành phần dùng chung toàn hệ thống chính trị
12	Kênh tương tác về an ninh mạng và Bộ chỉ số đo lường an ninh mạng (Lớp 4)	Lớp 4 - Kênh tương tác và đo lường hiệu quả (nhóm chỉ số KPI "Kỹ thuật và an toàn")	Bộ Công an, phối hợp Bộ Khoa học và Công nghệ	Chi tiết hóa



Phụ lục III

ĐỀ CƯƠNG KHUNG KIẾN TRÚC AN NINH MẠNG CẤP BỘ, CẤP TỈNH VÀ CỦA CƠ QUAN, TỔ CHỨC

*(Kèm theo Quyết định số 1875/QĐ-TTg
ngày 30 tháng 9 năm 2026 của Thủ tướng Chính phủ)*

Đề cương này hướng dẫn các bộ, cơ quan ngang bộ, Ủy ban nhân dân cấp tỉnh và cơ quan, tổ chức xây dựng, cập nhật thành phần an ninh mạng trong Khung kiến trúc số của mình, bảo đảm hoàn thành trước thời hạn quy định tại khoản 4 Điều 3 Quyết định số 1425/QĐ-TTg (chậm nhất ngày 29 tháng 01 năm 2027) và phù hợp với Khung kiến trúc an ninh mạng quốc gia.

I. Mục đích, phạm vi

Xác định hiện trạng, mục tiêu và lộ trình bảo đảm an ninh mạng của cơ quan, tổ chức, đồng bộ với Khung kiến trúc số của cơ quan, tổ chức mình và với Khung kiến trúc an ninh mạng quốc gia.

Phạm vi: toàn bộ hệ thống thông tin thuộc phạm vi quản lý, không bao gồm hệ thống thông tin quân sự, cơ yếu (áp dụng cơ chế riêng theo quy định).

II. Đánh giá hiện trạng

Danh mục hệ thống thông tin theo cấp độ đã được phê duyệt.

Hiện trạng các thành phần an ninh mạng đã đầu tư (SIEM, SOAR, EDR, tường lửa, IDS/IPS...) và mức độ đáp ứng so với yêu cầu tại Mục I Khung kiến trúc an ninh mạng quốc gia.

Hiện trạng kết nối với các nền tảng dùng chung quốc gia (giám sát, chia sẻ dữ liệu tình báo mỗi nguy...).

Nguồn nhân lực chuyên trách an ninh mạng và năng lực ứng phó sự cố hiện có.

III. Kế thừa thành phần dùng chung quốc gia

Liệt kê các thành phần dùng chung quốc gia được kế thừa, sử dụng lại theo nguyên tắc không đầu tư trùng lặp (đối chiếu Phụ lục A Khung kiến trúc an ninh mạng quốc gia).

Kế hoạch, lộ trình kết nối cảm biến giám sát về nền tảng SOC quốc gia (nếu chưa kết nối).

IV. Thành phần đặc thù cần xây dựng, đầu tư bổ sung

Xác định thành phần tại chỗ cần đầu tư theo yêu cầu tối thiểu tương ứng cấp độ hệ thống thông tin (theo Mục I).

Đối với cơ quan Đảng, Quốc hội, Mặt trận Tổ quốc Việt Nam, Tòa án nhân dân, Viện kiểm sát nhân dân: xác định thành phần đặc thù phù hợp với chức năng, nhiệm vụ và đặc thù tổ chức, trên cơ sở tham chiếu mô hình kiến trúc tại Khung kiến trúc an ninh mạng quốc gia.

Đối với hệ thống điều khiển công nghiệp (OT/ICS) thuộc phạm vi quản lý (nếu có): xác định yêu cầu phân vùng mạng IT/OT và giám sát tương ứng.

V. Tổ chức bảo đảm an ninh mạng

Phân công đơn vị đầu mối chuyên trách an ninh mạng của cơ quan, tổ chức.

Đối với Ủy ban nhân dân cấp tỉnh: xây dựng phương án phối hợp giữa cơ quan chuyên trách về chuyển đổi số và Công an tỉnh trong tổ chức giám sát, phát hiện, cảnh báo và ứng phó sự cố an ninh mạng; bảo đảm kết nối, chia sẻ thông tin và phối hợp xử lý kịp thời, thống nhất, hiệu quả; thực hiện nguyên tắc không đầu tư riêng lẻ, trùng lặp đối với các thành phần, nền tảng, dịch vụ đã được cung cấp tập trung ở cấp Trung ương.

Quy trình ứng phó sự cố nội bộ, kênh liên lạc với Trung tâm an ninh mạng quốc gia.

VI. Lộ trình và nguồn lực

Lộ trình triển khai theo từng giai đoạn, hoàn thành xây dựng, ban hành trước ngày 29 tháng 01 năm 2027.

Dự kiến kinh phí, nguồn vốn và đề xuất hỗ trợ kỹ thuật từ Bộ Công an (nếu có).

VII. Phụ lục kèm theo

Danh mục hệ thống thông tin theo cấp độ.

Bảng tự đánh giá mức độ đáp ứng theo Mục I Khung kiến trúc an ninh mạng quốc gia.