Scientific Quarterly of Supervision and Inspection
Vol. 19, No.73 (16). Autumn 2025
Research Article

Conceptualizing the Proactive Protection Model as a Preventive Security Strategy in Cyberspace

Received: 2025-08-06 **Pp. 35-72** **Accepted:** 2025-11-26

Shirvan Keivani*[1], Mehrdad Norizad[2]

Abstract

Background and Aim: Given the rapid transformation of the digital ecosystem and the growing complexity of threats, traditional and reactive approaches to cybersecurity have lost their effectiveness. The purpose of this study is to conceptualize the proactive (pre-incident) protection model as a preventive security strategy in cyberspace.

Methodology: From the perspective of purpose, this research is applied and was conducted using a qualitative methodology based on Grounded Theory (Strauss & Corbin, 1998). Accordingly, data were collected through in-depth, semi-structured interviews with 15 prominent national experts in the fields of policymaking, cyber defense, law enforcement, and legal affairs. Participants were selected using theoretical sampling, and the interview process continued until theoretical saturation was achieved. Data analysis was carried out in three stages. First, the data were analyzed using open coding, through which initial concepts and primary codes were extracted from the interviews. In the second stage, axial coding was employed to categorize shared concepts and to model the relationships among them around the core phenomenon (proactive protection). Finally, in the selective coding stage, the extracted categories were systematically integrated with the study's paradigmatic model, leading to the comprehensive and coherent formation of the final theory.

Findings: Data analysis resulted in the extraction of a comprehensive paradigmatic model for proactive protection. This model encompasses causal conditions (the necessity of cyber sovereignty), contextual conditions (maturity of indigenous technologies), intervening conditions (legal–ethical challenges), key strategies (active cyber defense, protective safeguarding, and data-driven governance), and strategic consequences (national resilience, sustainable security, and digital ecosystem development).

Conclusion: The findings indicate that proactive protection constitutes a multidimensional strategic framework that transforms security from a passive state into an active, intelligent, and anticipatory process. The realization of this model requires an integrated linkage between advanced technologies, the agile modernization of the legal system, and the enhancement of media literacy as a form of human defensive barrier, thereby transforming cyberspace into a secure and sustainable environment for governance and civic interactions.

Keywords: Proactive Protection, Preventive Security, Cyberspace, Cyber Governance, Grounded Theory.

Citation (APA): Keivani, Shirvan, & Norizad, Mehrdad (2025). Conceptualizing the Proactive Protection Model as a Preventive Security Strategy in Cyberspace, ***Quarterly of Supervision and Inspection***, 19 (73), 35-72.
DOI: https://doi.org/10.22034/si.2026.120954

1- PhD Student, Department of Management, Ur.c., Islamic Azad University, Urmia, Iran. *(Corresponding author)*. Email: shirvan.keivani@iau.ac.ir
2- PhD Student, Department of Management, Ur.c., Islamic Azad University, Urmia, Iran. Email: mehrdad.norizad@gmail.com

فصلنامه علمی نظارت و بازرسی

سال ۱۹، شماره ۷۳ (۱۶)، پاییز ۱۴۰۴

مقاله پژوهشی

تبیین الگوی صیانت پیش‌رویدادی به‌عنوان راهبرد امنیت پیشگیرانه در فضای مجازی

تاریخ دریافت: ۱۴۰۴/۰۵/۱۵ | صص ۷۲-۳۵ | تاریخ پذیرش: ۱۴۰۴/۰۹/۰۵

شیروان کیوانی*[۱]، مهرداد نوری‌زاد[۲]

چکیده

زمینه و هدف: با توجه به تحول پُرشتاب زیست‌بوم دیجیتال و پیچیدگی فزاینده تهدیدات، رویکردهای سنتی و واکنشی در حوزه امنیت سایبری کارآمدی خود را از دست داده‌اند. هدف از انجام این پژوهش، تبیین الگوی صیانت پیش‌رویدادی به‌عنوان راهبرد امنیت پیشگیرانه در فضای مجازی است.

روش‌شناسی: این پژوهش از منظر هدف، کاربردی بوده و با اتخاذ یک روش‌شناسی کیفی مبتنی بر نظریه داده‌بنیاد (استراوس و کوربین، ۱۹۹۸) انجام شده است. در این راستا، داده‌ها از طریق مصاحبه‌های عمیق و نیمه‌ساختاریافته با ۱۵ نفر از نخبگان برجسته در حوزه‌های سیاست‌گذاری، پدافند سایبری، انتظامی و حقوقی کشور گردآوری شدند. مشارکت‌کنندگان با استفاده از روش نمونه‌گیری نظری انتخاب شده و تا رسیدن به اشباع نظری، فرآیند مصاحبه‌ها ادامه یافت. تحلیل داده‌ها در سه مرحله انجام شد. در ابتدا، داده‌ها با استفاده از کدگذاری باز تحلیل شدند، به‌طوری‌که مفاهیم اولیه و کدهای اولیه از دل مصاحبه‌ها استخراج شد. سپس، در مرحله دوم با استفاده از کدگذاری محوری، مفاهیم مشترک دسته‌بندی شدند و روابط میان آن‌ها حول پدیده محوری (صیانت پیش‌رویدادی) شبیه‌سازی شد. در نهایت، در مرحله کدگذاری گزینشی، مقولات استخراج‌شده به‌طور هم‌زمان با مدل پارادایمی تحقیق پیوند داده شدند تا نظریه نهایی تحقیق به‌طور جامع و یکپارچه شکل گیرد.

یافته‌ها: تحلیل داده‌ها به استخراج یک مدل پارادایمی جامع برای «صیانت پیش‌رویدادی» منجر شد. این مدل شامل شرایط علّی (ضرورت حاکمیت سایبری)، شرایط زمینه‌ای (بلوغ فناوری بومی)، شرایط مداخله‌گر (چالش‌های حقوقی-اخلاقی)، راهبردهای کلیدی (پدافند فعال، صیانت حمایتی و حکمرانی داده‌محور) و پیامدهای راهبردی (تاب‌آوری ملی، امنیت پایدار و توسعه زیست‌بوم دیجیتال) است.

نتیجه‌گیری: نتایج نشان می‌دهد که صیانت پیش‌رویدادی یک نظام‌واره راهبردی چندبُعدی است که امنیت را از یک وضعیت انفعالی به یک فرآیند کنشی، هوشمند و پیش‌بینانه تبدیل می‌کند. تحقق این الگو مستلزم پیوندی یکپارچه میان فناوری‌های پیشرفته، چابک‌سازی نظام حقوقی و ارتقای سواد رسانه‌ای به‌عنوان یک سد دفاعی انسانی است تا فضای مجازی به محیطی امن و پایدار برای حکمرانی و تعاملات شهروندی تبدیل شود.

کلیدواژه‌ها: صیانت پیش‌رویدادی، امنیت پیشگیرانه، فضای مجازی، حکمرانی سایبری، نظریه داده‌بنیاد.

استناد (APA): کیوانی، شیروان، و نوری‌زاد، مهرداد (۱۴۰۴). تبیین الگوی صیانت پیش‌رویدادی به‌عنوان راهبرد امنیت پیشگیرانه در فضای مجازی. ***فصلنامه نظارت و بازرسی***، ۱۹(۷۳)، ۷۲-۳۵.

DOI: https://doi.org/10.22034/si.2026.120954

۱- دانشجوی دکتری تخصصی، گروه مدیریت، واحد ارومیه، دانشگاه آزاد اسلامی، ارومیه، ایران. (رایانامه نویسنده مسئول: shirvan.keivani@iau.ac.ir)

۲- دانشجوی دکتری تخصصی، گروه مدیریت، واحد ارومیه، دانشگاه آزاد اسلامی، ارومیه، ایران. (رایانامه: mehrdad.norizad@gmail.com)

مقدمه

تحول شگرف در زیست‌بوم دیجیتال و درهم‌تنیدگی فزاینده زیرساخت‌های حیاتی، خدمات عمومی، اقتصاد دیجیتال و تعاملات اجتماعی با فضای مجازی، مفهوم امنیت را از رویکردهای سنتی واکنشی به سمت الگوهای نوین حکمرانی پیشگیرانه سوق داده است (رافیکا، بالتاسار، آدیویجایا و ریزکی[1]، ۲۰۲۵: ۴). در چنین شرایطی، حکمرانی سایبری دیگر صرفاً یک مسئله فنی یا فناورانه نیست، بلکه به یکی از مؤلفه‌های بنیادین حفظ نظم عمومی، ثبات ملی و امنیت اجتماعی تبدیل شده است؛ امری که نقش نهادهای انتظامی را به‌عنوان متولیان اصلی پیشگیری و صیانت از امنیت عمومی، بیش از پیش برجسته می‌سازد (سعادت سیرت و خانیکی، ۱۴۰۴: ۸).

در جمهوری اسلامی ایران، سازمان انتظامی کشور (فراجا) به‌عنوان بازوی حاکمیتی تأمین امنیت، مأموریتی فراتر از مقابله پسینی با جرم بر عهده دارد و مطابق اسناد بالادستی، پیشگیری هوشمند از جرائم سایبری در رأس اولویت‌های آن قرار گرفته است. در این راستا، معاونت پیشگیری، پلیس فتا (پلیس فضای تولید و تبادل اطلاعات) و دیگر پلیس‌های تخصصی مانند پلیس امنیت اقتصادی، نقش کلیدی در شناسایی و مقابله با تهدیدات سایبری ایفاء می‌کنند. به‌ویژه، نظارت پیش‌رویدادی و واکنش به تهدیدات پیش از وقوع جرم از جمله رویکردهای نوینی است که سازمان‌های انتظامی به‌طور جدی پیگیری می‌کنند. صیانت از فضای مجازی در سطح ملی، به‌ویژه در دوران تحول دیجیتال، فراتر از محدودسازی و کنترل است. این صیانت باید به‌گونه‌ای طراحی شود که بستر امنی برای تعاملات شهروندی فراهم آورد و در عین حال حقوق عمومی را در فضای دیجیتال حفظ کند (ریاضی‌پور، ۱۴۰۳: ۳).

در همین راستا، نظریه‌پردازان امنیت سایبری بر این باورند که پیشگیری از جرائم سایبری باید به‌صورت یکپارچه و سیستمی انجام شود؛ جایی‌که طرح‌های صیانتی به عنوان مکمل پدافند غیرعامل و در هماهنگی با سیاست‌های امنیتی

1- Rafika, Baltasar, Adiwijaya & Rizky

کـلان عمـل کننـد (اکبـری و نـوروزعلی، ۱۴۰۱: ۵). امـا در ایـن میـان، توجـه بـه چالش‌های جـرم‌شناسـی فرهنگـی و احتـرام بـه آزادی‌هـای مشـروع شـهروندان امـری ضـروری اسـت تـا سیاسـت‌هـای جنـایی و امنیتـی در ایـن حـوزه بـه‌طـور مـؤثر پیاده‌سازی شود (رایجیان اصلی، رحیمی‌نژاد و رزم‌آور، ۱۴۰۳: ۱۱۷).

امنیـت ملـی در جهـان معاصـر بـه‌شـدت بـه نظـارت هوشـمند بـر شـبکه‌هـای اجتمـاعی، تحلیـل ترافیـک داده‌هـا و مـدیریت سـامانه‌هـای امنیتـی سـایبری وابسـته اسـت. پـایش پـیش‌رویـدادی فضـای مجـازی، بـه‌ویـژه از طریـق هـوش مصـنوعی و یـادگیری ماشـینی، ابزارهـای قدرتمنـدی را بـرای مقابلـه بـا تهدیـدات نـرم و سـخت فـراهم مـی‌آورد، بـدون آن‌کـه بـه حـریم خصوصـی کـاربران آسـیب وارد کنـد (امـین‌الرعایـا و امـین‌الرعایـا، ۱۴۰۲: ۸۲). طـرح‌هـای راهبـردی بـرای حکمرانـی سـایبری در محـیط بـین‌المللـی، بخشـی از تـلاش دولـت‌هـا بـرای تقویـت حاکمیـت ملـی در ایـن فضـای بـی‌مـرز اسـت کـه بـه‌ویـژه در دوران بحـران‌هـای جهـانی ماننـد پانـدمی‌هـا و تهدیـدات سـایبری جدیـد اهمیـت ویـژه‌ای پیـدا کـرده اسـت (حسـینی، رامـک، انتظـاری و فرخـی، ۱۴۰۳: ۱۳۱). یکـی از ارکـان اصـلی صـیانت پـیش‌رویـدادی، تمرکـز بـر دفـاع سـایبری فعـال اسـت. ایـن رویکـرد، بـرخلاف رویکردهـای منفعـل و واکنشـی، بـه سـازمان‌هـا و نهادهـای انتظـامی اجـازه مـی‌دهـد تـا تهدیـدات سـایبری را پـیش از وقـوع شناسـایی و خنثـی کننـد. تحـول بـه سـمت دفـاع فعـال، بـه‌ویـژه در نهادهـای امنیتـی، یـک تغییـر راهبـردی اسـت کـه در متـون حقـوقی بـین‌المللـی بـه‌عنـوان ضـرورت تـأمین امنیـت بخـش خصوصـی و عمـومی مطرح شده است (موچینگا[1]، ۲۰۲۵: ۳۷۵؛ دزیویس[2]، ۲۰۲۴: ۱۳۸).

تحقـق امنیـت پیشـگیرانه بـه‌ویـژه در حـوزه فضـای مجـازی، بـدون ارتقـای بلـوغ امنیتـی و اسـتفاده از فنـاوری‌هـای نوظهـور ممکـن نیسـت. مـدل‌هـای مفهـومی بلـوغ امنیـت سـایبری در اپراتورهـای بـزرگ مخـابراتی، تأکیـد بـر زیرسـاخت‌هـای فنـی و امنیتی دارند که آسـیب‌پـذیری‌هـا را کـاهش مـی‌دهنـد و بـر اهمیـت آمـوزش در ایـن زمینه تأکیـد دارنـد (بیژنـی، طـالبی و انتظـاری، ۱۴۰۲: ۴۰). در ایـن مسـیر، اسـتفاده

1- Mochinaga
2- Dziwisz

از هوش مصنوعی و یادگیری عمیق در سیستم‌های سایبری-فیزیکی نه‌تنها می‌تواند قابلیت‌های شناسایی حملات فریب‌کارانه را افزایش دهد، بلکه توانمندی شناسایی آنومالی‌های فرآیندی در بسترهای حساس را نیز به‌طور چشم‌گیری بهبود می‌بخشد (گابا، بودیراجا، کومار، مارتا، خورمی، سینگ، سینگ، عسکر و ابوحوش[1]، ۲۰۲۴: ۶۰۲۲؛ کای و کوتسوکوس[2]، ۲۰۲۳: ۷). امنیت پیشگیرانه در فضای مجازی، به‌ویژه در زیرساخت‌های حیاتی، نیازمند شناخت دقیق مؤلفه‌های بومی و الزامات عملیاتی نهادهای انتظامی است. شناسایی ابعاد بومی امنیت فضای مجازی و به‌کارگیری الگوهای راهبردی امن در سامانه‌های کنترل صنعتی، از اقداماتی است که دستگاه‌های اجرایی باید آن را در نظر بگیرند تا از وقوع فجایع و تهدیدات سایبری پیش از آغاز هرگونه فعالیت تخریبی جلوگیری شود (شهیر، حسن‌بیگی، تقی‌پور و ریاضی، ۱۴۰۳: ۷۱؛ غیوری ثالث، مدیری، موحدی صفت و سقایی، ۱۴۰۳: ۱۷۵). تحلیل‌های پیش‌بینانه مبتنی بر هوش مصنوعی، از جمله راه‌کارهای کلیدی در این زمینه است که می‌تواند تهدیدات سایبری مانند حملات باج‌افزاری و نشت داده‌ها را پیش از وقوع شناسایی و مقابله کند (اگو-پرومیس، آسانته، بالیسانه، صالح، آینا، کوره و گاووا[3]، ۲۰۲۵: ۷۲). در کنار این فناوری‌ها، بهره‌گیری از معماری اعتماد صفر، که دسترسی را پیش از هرگونه تأیید از سوی سیستم کنترل می‌کند، امنیت محیط‌های ابری و شبکه‌های نوین را تضمین می‌کند (موثاسامی[4]، ۲۰۲۵: ۲۴). بنابراین عوامل انسانی و روان‌شناختی در راستای تحقق امنیت پیش‌رویدادی نقش حیاتی دارند. آگاهی از تهدیدات سایبری و آمادگی برای تعامل با هوش مصنوعی به‌ویژه در نهادهای انتظامی، از ضروریات سازمان‌های مدرن است تا بتوانند از وقوع تهدیدات و حملات سایبری جلوگیری کنند (لی و پارک[5]، ۲۰۲۳؛ میرزا، جورجاکوپولوس و یاوری[6]، ۲۰۲۳: ۸۲۲).

با وجود تمام تلاش‌های صورت‌گرفته در حوزه‌های فنی و تقنینی، هم‌چنان

1- Gaba, Budhiraja, Kumar, Martha, Khurmi, Singh, Singh, Askar & Abouhawwash
2- Cai & Koutsoukos
3- Egho-Promise, Asante, Balisane, Salih, Aina, Kure & Gavua
4- Muthusamy
5- Lee & Park
6- Mirza, Georgakopoulos & Yavari

یک شکاف عمیق میان «اقدامات واکنشی پس از وقوع جرم» و «سازوکارهای صیانت پیش‌رویدادی» مشاهده می‌شود. اکثر پژوهش‌های موجود یا بر جنبه‌های صرفاً فنی دفاع تمرکز کرده‌اند و یا به تحلیل‌های حقوقی پسینی پرداخته‌اند؛ اما آن‌چه در این میان مغفول مانده، تبیین جامع «صیانت پیش‌رویدادی» به‌عنوان یک راهبرد منسجم است که ابعاد حاکمیتی، پیشگیری وضعی و فناوری‌های پیش‌بینانه را در یک کل واحد ترکیب کند (قربانی و خیامی، ۱۴۰۲: ۲۷). مسئله اصلی این است که چگونه می‌توان بدون آسیب به حقوق شهروندی و با بهره‌گیری از هوش مصنوعی و حکمرانی داده‌محور، پیش از آن‌که تهدیدی به‌وقوع بپیوندد، محیط سایبری را صیانت کرد. این پژوهش در پی آن است تا با پر کردن این خلاء، مدلی تبیینی ارائه دهد که امنیت را از یک وضعیت انفعالی به یک فرایند کنشی و پیشگیرانه تبدیل کند.

پیشینه پژوهش

مطالعه و واکاوی پیشینه‌های پژوهشی در حوزه امنیت سایبری نشان‌دهنده یک چرخش پارادایمیک از «دفاع واکنشی» به سمت «صیانت کنشی و پیشگیرانه» است. با پیچیده‌تر شدن الگوهای نفوذ و بهره‌گیری مهاجمان از ابزارهای هوشمند، ادبیات پژوهش در سال‌های اخیر بر این نکته تمرکز یافته است که صرفِ تکیه بر دیوارهای آتش یا اقدامات قضایی پس از وقوع جرم، دیگر تکاپوی تأمین امنیت ملی و فردی را نمی‌دهد. بررسی مطالعات داخلی و بین‌المللی حکایت از آن دارد که مفهوم «صیانت پیش‌رویدادی» به‌عنوان یک راهبرد نوین، ترکیبی از حکمرانی داده‌محور، پیشگیری اجتماعی و دفاع فعال فناورانه است که هدف آن شناسایی و خنثی‌سازی تهدید در لایه‌های قبل از وقوع[1] می‌باشد. در ادامه، مهم‌ترین پژوهش‌های مرتبط با موضوع پژوهش، مورد بررسی قرار می‌گیرند.

امیرمحمدی، عبدی‌نژاد و شکربیگی (۱۴۰۳) در پژوهشی با عنوان «مطالعه آسیب‌ها و جرائم مرتبط با فضای مجازی و سیاست‌های پیشگیری از آن‌ها در

1- Pre-event

نیروهای مسلح» به بررسی چالش‌های امنیتی در نهادهای نظامی پرداختند. نتایج این پژوهش نشان داد که پیشگیری وضعی (تغییر محیط) و پیشگیری اجتماعی (آموزش) باید به‌صورت هم‌زمان اجرا شوند. پژوهش‌گران تأکید کردند که صیانت پیش‌رویدادی در نیروهای مسلح نه تنها یک انتخاب، بلکه ضرورتی برای جلوگیری از جاسوسی و تخریب زیرساخت‌های دفاعی است.

حسینی و همکاران (۱۴۰۳) در پژوهشی با عنوان «ارائه طرح راهبردی حکمرانی فضای سایبر کشور در محیط بین‌الملل» به تبیین جایگاه ایران در دیپلماسی دیجیتال پرداختند. یافته‌های آن‌ها نشان می‌دهد که صیانت از فضای مجازی بدون داشتن یک مدل حکمرانی منسجم که بتواند تهدیدات فرامرزی را پیش‌بینی و خنثی کند، امکان‌پذیر نیست. آن‌ها بر لزوم ایجاد ائتلاف‌های امنیتی و تقویت قدرت بازدارندگی پیش‌دستانه تأکید ورزیدند.

رایجیان اصلی و همکاران (۱۴۰۳) در پژوهشی با عنوان «سیاست‌گذاری جنایی تقنینی در آینه جرم‌شناسی فرهنگی: با رویکردی انتقادی به چالش‌های صیانت از فضای مجازی» به نقد نگاه‌های صرفاً سخت‌افزاری به امنیت پرداختند. نتیجه این پژوهش حاکی از آن است که اگر صیانت پیش‌رویدادی به‌درستی تبیین نشود و با مقاومت فرهنگی کاربران روبه‌رو شود، خود به عاملی برای تولید جرم تبدیل می‌شود؛ از این‌رو راهبرد پیشگیرانه باید بر مبنای اقناع و حفظ حقوق شهروندی استوار باشد.

غیوری ثالث و همکاران (۱۴۰۳) در پژوهشی با عنوان «ارائه الگوی راهبردی بکارگیری امن سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی کشور» بر امنیت سیستم‌های کنترل متمرکز شدند. آن‌ها نتیجه گرفتند که برای صیانت از نیروگاه‌ها و مراکز حساس، باید از الگوریتم‌های پایش مداوم استفاده کرد که کوچک‌ترین انحراف از عملکرد عادی را قبل از تبدیل شدن به بحران، شناسایی کنند؛ این همان هسته اصلی امنیت پیشگیرانه فنی است.

بیداروند و پورقهرمانی (۱۴۰۳) در پژوهشی با عنوان «نقش پیشگیرانه سواد رسانه‌ای در دوران اپیدمی کوید-۱۹ بر بزه‌کاری سایبری» به بررسی رابطه

آگاهی کاربران و نرخ وقوع جرم پرداختند. یافته‌های آن‌ها ثابت کرد که ارتقای سطح دانش دیجیتال، مانند یک واکسن اجتماعی عمل کرده و با کاهش قربانی‌شدن کاربران، بارِ اقدامات پلیسی و قضایی را به شدت کاهش می‌دهد، که این موضوع لایه‌ای مهم از صیانت پیش‌رویدادی است.

شهیر و همکاران (۱۴۰۳) در پژوهشی با عنوان «ابعاد و مؤلفه‌های بومی امنیت فضای مجازی کشور» به‌دنبال استخراج شاخص‌های اختصاصی برای ایران بودند. آن‌ها به این نتیجه رسیدند که امنیت پیشگیرانه بومی باید شامل مؤلفه‌هایی چون استقلال در ابزارهای رمزنگاری، نظارت هوشمند بر دروازه‌های ورودی ترافیک بین‌الملل و آموزش نیروی انسانی متخصص باشد تا صیانت به معنای واقعی محقق شود.

حسن، حسین، امین، سوتردهر، جنی و محمود[1] (۲۰۲۵) در پژوهشی با عنوان «تقویت دفاع سایبری فعال: چارچوبی نظری برای هوش پیش‌بینانه تهدیدات سایبری مبتنی بر هوش مصنوعی» به بررسی نقش یادگیری ماشین در امنیت پرداختند. آن‌ها نتیجه گرفتند که سامانه‌های صیانتی نوین باید از حالت «واکنشی» به حالت «پیش‌بینانه» تغییر کنند. این سیستم‌ها با تحلیل میلیون‌ها داده در ثانیه، حملات احتمالی آینده را پیش‌بینی کرده و سپر دفاعی را پیش از اصابت تهدید، فعال می‌کنند.

موتوسامی (۲۰۲۵) در پژوهشی با عنوان «بهره‌گیری از معماری‌های اعتماد صفر مبتنی‌بر هوش مصنوعی برای دفاع سایبری فعال» به نقد مدل‌های سنتی قلعه‌مانند پرداخت. او تبیین کرد که در راهبرد صیانت پیش‌رویدادی، هیچ‌کس (حتی مدیر سیستم) نباید مورد اعتماد مطلق باشد. این مدل با احراز هویت مستمر، احتمال نفوذهای داخلی و خارجی را در همان مراحل اولیه به صفر نزدیک می‌کند.

رافیکا و همکاران (۲۰۲۵) در پژوهشی با عنوان «راهبردهای امنیت سایبری برای پیشگیری از حملات باج‌افزاری در اپلیکیشن‌های مبتنی‌بر ابر» بر

1- Hasan, Hossain, Amin, Sutradhar, Jeny & Mahmud

مقابله با باج‌افزارها تمرکز کردند. یافته‌های آن‌ها نشان داد که کلید صیانت در این‌جا، شناسایی «فرایند رمزنگاری غیرمجاز» در همان لحظات شروع است. سیستم‌های پیشگیرانه باید به محض مشاهده اولین تلاش برای رمزنگاری انبوه، دسترسی را متوقف کنند.

موچینگا (۲۰۲۵) در پژوهشی با عنوان «طلوع خورشید در قلمرو سایبری: تغییر راهبردی ژاپن به سمت دفاع سایبری فعال» دکترین جدید ژاپن را بررسی کرد. نتیجه پژوهش نشان می‌دهد که ژاپن با عبور از رویکرد صرفاً دفاعی، به سمت شناسایی منشأ تهدید در خارج از مرزها حرکت کرده است. این مقاله صیانت پیش‌رویدادی را به‌عنوان یک «بازدارندگی فعال» معرفی می‌کند که هزینه حمله را برای مهاجم افزایش می‌دهد.

مانه[1] (۲۰۲۳) در پژوهشی با عنوان «مکانیسم‌های دفاع سایبری فعال برای محیط‌های رایزش ابری» به امنیت داده‌های ذخیره‌شده در ابر پرداختند. نتیجه پژوهش وی نشان داد که به دلیل ماهیت توزیع‌شده ابر، صیانت پیش‌رویدادی تنها از طریق «پایش رفتار محور» ممکن است؛ یعنی هرگونه رفتار غیرعادی کاربر یا سرور باید بلافاصله به عنوان یک تهدید احتمالی مسدود شود تا از نشت اطلاعات جلوگیری شود.

جمع‌بندی پیشینه

مرور پیشینه‌های داخلی و خارجی نشان‌دهنده توافق نظری بر ضرورت عبور از الگوهای واکنشی به سمت راهبردهای کنشی و هوشمند است. تشابه پژوهش حاضر با مطالعات قبلی در تأکید بر نقش کلیدی فناوری‌های پیش‌بینانه و ضرورت حکمرانی منسجم بر فضای مجازی است. با این حال، اکثر پژوهش‌های پیشین به‌صورت تک‌بُعدی یا بر جنبه‌های فنیِ دفاع فعال تمرکز کرده‌اند و یا صرفاً ابعاد حقوقی و تقنینی صیانت را واکاوی کرده‌اند. خلاء اساسی موجود، فقدان یک الگوی جامع و بومی است که بتواند ابعاد متکثر فنی، حقوقی، اجتماعی و حاکمیتی را در قالب یک ساختار واحدِ «صیانت پیش‌رویدادی»

1- Manne

تبیین نماید. بر این اساس، نوآوری و تمایز بنیادین پژوهش حاضر در بهره‌گیری از راهبرد پژوهشی نظریه داده‌بنیاد[1] است. این پژوهش قصد دارد با فرارفتن از نظریات موجود و با تکیه بر تحلیل عمیق تجارب خبرگان و داده‌های کیفی، به جای آزمون الگوهای ترجمه‌ای، به تدوین یک «مدل نظری بومی» دست یابد. این مدل نه‌تنها چگونگی صیانت از فضای مجازی را پیش از وقوع تهدید تبیین می‌کند، بلکه برساختِ یک نظریه زیربنایی برای امنیت پیشگیرانه در زیست‌بوم سایبری کشور هدف قرار داده است.

مبانی نظری پژوهش

تبیین راهبرد صیانت پیش‌رویدادی در وهله نخست مستلزم درک پارادایم «حکمرانی سایبری» به‌عنوان چتری برای امنیت پیشگیرانه است. حکمرانی در فضای مجازی صرفاً به معنای اعمال حاکمیت فنی نیست، بلکه یک ضرورت راهبردی برای ایجاد نظم در زیست‌بوم دیجیتال محسوب می‌شود که بر پایه آن، صیانت از دارایی‌های ملی و معنوی تعریف می‌شود (سامانی‌پور، بزرگمهر، رمضانی‌پور و حقزاد، ۱۴۰۲: ۷). این رویکرد حکمرانی، زیربنای نظری لازم را فراهم می‌آورد تا صیانت از یک اقدام واکنشی و پلیسی، به یک راهبرد پیشینی تبدیل شود که در آن، پیش‌بینی تهدیدات پیش از وقوع، اولویت اصلی نظام سیاست‌گذاری است. در این راستا، صیانت باید به‌گونه‌ای طراحی شود که نه تنها امنیت را تضمین کند، بلکه با حقوق بنیادین شهروندی در تعارض قرار نگیرد و توازنی پویا میان اقتدار حاکمیتی و آزادی‌های فردی برقرار سازد (منصوری‌نیا، ۱۴۰۳: ۴).

در لایه فنی و عملیاتی، صیانت پیش‌رویدادی بر مفهوم «ایمنی‌بخشی به سیستم‌های حیاتی» استوار است (محمدی برزگر، قبادی و حیدرنژاد، ۱۴۰۴: ۵). وارسی و اعتبارسنجی دقیق نیازمندی‌های نرم‌افزار در سیستم‌هایی که وظیفه ایمنی‌بخشی را برعهده دارند، اولین سد دفاعی در برابر نفوذهای مخرب است (مختاری و مدیری، ۱۴۰۱: ۳). این رویکرد نظری تأکید دارد که امنیت

1- Grounded Theory

پیشگیرانه باید از مرحله طراحی و توسعه نرم‌افزار[1] آغاز شود. اگر نیازمندی‌های امنیتی در لایه‌های ابتدایی کدنویسی و معماری سیستم به درستی اعتبارسنجی شوند، بسیاری از آسیب‌پذیری‌هایی که در آینده توسط مهاجمان مورد سوءاستفاده قرار می‌گیرند (وانگ[2]، ۲۰۲۴: ۱۲)، در همان مرحله پیش‌رویدادی شناسایی و حذف خواهند شد که این امر هزینه‌های بازسازی پس از بحران را به شدت کاهش می‌دهد (پاتیل، پاتیل، دسپانده و بنور[3]، ۲۰۲۴: ۳۶۵۱). تحقق صیانت در زیرساخت‌های صنعتی کشور، نیازمند به‌کارگیری هوش مصنوعی در تشخیص ناهنجاری‌های فرآیندی است. بهره‌گیری از تکنیک‌های یادگیری ماشین بدون نظارت[4] برای پایش مداوم کنترل‌کننده‌های منطقی برنامه‌پذیر، امکان شناسایی کوچک‌ترین انحرافات عملکردی را که ناشی از حملات سایبری فریب‌کارانه است، فراهم می‌آورد (ابو بوتنگ و بروس[5]، ۲۰۲۲: ۲۳۱). در این مدل نظری، صیانت پیش‌رویدادی به معنای داشتن یک دیده‌بان هوشمند است که با درک الگوهای عادی رفتار سیستم، هرگونه آنومالی را به‌عنوان یک تهدید بالقوه شناسایی کرده و پیش از آن‌که حمله به فاز تخریب فیزیکی در زیرساخت‌های حیاتی مانند نیروگاه‌ها برسد، واکنش دفاعی را فعال می‌کند. از منظر جرم‌شناسی پیشگیرانه، صیانت پیش‌رویدادی باید با چالش‌های حاکم بر «پیشگیری وضعی» در فضای سایبر مقابله کند. پیشگیری وضعی از طریق دشوار کردن ارتکاب جرم و کاهش جذابیت اهداف مجرمانه عمل می‌کند، اما این رویکرد در فضای مجازی با چالش‌های آسیب‌شناختی متعددی روبه‌رو است که نیازمند بازنگری راهبردی است (امیریان فارسانی، ۱۴۰۲: ۸۳). تبیین این راهبرد در مبانی نظری نشان می‌دهد که بدون شناخت دقیق این چالش‌های ساختاری، صیانت تنها به یک پوسته فیزیکی محدود می‌شود؛ در حالی‌که صیانت پیش‌رویدادی واقعی مستلزم تغییر معماری فضای مجازی به‌گونه‌ای است که فرصت‌های مجرمانه

1- Security by Design
2- Wang
3- Patil, Patil, Despande & Bannore
4- Unsupervised Machine Learning
5- Aboah Boateng & Bruce

پیش از شکل‌گیری، شناسایی و مسدود شوند (کرمانیان، پورقهرمانی و بیگی، ۱۴۰۳: ۱۰).

بخش مهمی از راهبرد امنیت پیشگیرانه، معطوف به شناسایی و مدیریت «انگیزه‌های نوین مجرمانه» نظیر هکتیویسم است. پیشگیری از جرائم سایبری با تأکید بر پدیده هکتیویسم (فعالیت‌های هکری با انگیزه‌های سیاسی-اجتماعی)، نیازمند تبیین مرزهای حقوقی و فقهی میان اعتراض دیجیتال و بزه‌کاری سایبری است (امامی، داودی گرمارودی و پاکزاد، ۱۴۰۲: ۱۲). مبانی نظری این پژوهش استدلال می‌کند که صیانت پیش‌رویدادی باید دارای یک لایه تحلیل محتوایی و انگیزشی باشد تا بتواند با درک ریشه‌های کنش‌گری در فضای مجازی، از تبدیل شدن اعتراضات برخط به حملات مخرب علیه امنیت ملی جلوگیری کرده و راه‌کارهای پیشگیرانه متناسب با هر انگیزه را تدوین کند. در سطح کلان شهری و پدافندی، صیانت پیش‌رویدادی با مفهوم «امنیت دوفضائی» گره خورده است. سنجش شاخص‌های پدافند غیرعامل در کلان‌شهرهایی مانند تهران نشان می‌دهد که تهدیدات مجازی مستقیماً بر امنیت فیزیکی و پایداری خدمات شهری اثرگذارند (سامانی‌پور و همکاران، ۱۴۰۲). بر این اساس، راهبرد صیانت پیش‌رویدادی باید شامل یک مدل جامع برای صیانت از سیستم‌های مدیریت شهری باشد که در آن، پیش‌بینی تهدیدات دوفضایی و مقاوم‌سازی زیرساخت‌های متصل به شبکه، به‌عنوان یک ضرورت برای حفظ نظم عمومی و امنیت شهروندان در برابر بحران‌های احتمالی تعریف شده است.

اثربخشی صیانت پیش‌رویدادی در دستگاه‌های اجرایی، منوط به توسعه ابزارهای سنجش و محاسبه‌گرهای دقیق کاستی‌های امنیتی است (سهراب، ۱۴۰۴). الزامات راهبردی حکم می‌کند که سازمان‌ها برای عبور از امنیت سنتی، به سمت مدل‌های محاسبه‌گر بلوغ و نقص‌های سایبری حرکت کنند تا بتوانند شکاف‌های امنیتی خود را پیش از مهاجمان کشف کنند (رجبی‌زاده و مدیری، ۱۴۰۱). این لایه از مبانی نظری تأکید دارد که صیانت پیش‌رویدادی یک فرآیند ایستا نیست، بلکه نیازمند یک سیستم ارزیابی مستمر است که

نقـاط ضـعف عملیـاتی را در لحظـه شناسـایی کـرده و اقـدامات ترمیمـی را پـیش از وقوع هرگونه نشست یا نفوذ غیرمجاز پیشنهاد دهد.

یکـی از موانـع اصـلی در تحقـق صـیانت پـیش‌رویـدادی، پدیـده روان‌شـناختی-فنـی «خسـتگی از هشـدار» در تـیم‌هـای واکـنش اضـطراری اسـت. زمـانی‌کـه سیسـتم‌هـای امنیتـی انبـوهی از هشـدارهای کـاذب را تولیـد مـی‌کننـد، توانـایی تشـخیص تهدیـد واقعـی کـاهش مـی‌یابـد؛ لـذا اسـتفاده از تکنیـک‌هـای هـوش مصـنوعی بـرای فیلتـر کـردن و اولویـت‌بنـدی هشـدارها، یـک ضـرورت نظـری بـرای حفـظ هوشـیاری در صـیانت پـیش‌رویـدادی اسـت (بـن، سـاموئل، تاکاهاشـی و اینوئـه[1]، ۲۰۲۱: ۱۲). ایـن مفهـوم نشـان مـی‌دهـد کـه صـیانت پـیش‌رویـدادی تنهـا به‌معنای جمع‌آوری داده نیسـت، بلکـه بـه معنـای پـردازش هوشـمندانه داده‌هـا بـرای جلوگیری از اشباع اطلاعـاتی تحلیـل‌گـران و تضـمین واکـنش سـریع بـه تهدیـدات بـا اولویت بالاست (ژانگ و تینگ[2]، ۲۰۲۱: ۱۷).

صـیانت پـیش‌رویـدادی در لایـه اجتمـاعی، پیونـد عمیقـی بـا «حمایـت از گـروه‌هـای آسـیب‌پـذیر» و امنیـت انسـانی دارد. آسـیب‌شناسـی مخـاطرات سـایبری برای اطفال و نوجوانـان نشـان مـی‌دهـد کـه پیشـگیری پـیش‌رویـدادی در ایـن حـوزه بایـد شـامل راه‌کارهـای خنثـی‌سـازی مخـاطرات در محـیط‌هـای آموزشـی و تفریحـی بـرخط باشـد (ولـی‌زاده، ۱۴۰۲: ۵۰). از منظـر نظـری، صـیانت در ایـن‌جـا بـه معنـای ایجاد یک «زیسـت‌بـوم امـن» اسـت کـه در آن، پـیش از آن‌کـه کـودک یـا نوجـوان در معرض محتـوای مجرمانـه یـا بـزه‌کـاری قـرار گیـرد، سـازوکارهای صـیانتی و حمـایتی بـه صـورت خودکـار فعـال شـده و از بـروز آسـیب‌هـای روانـی و اجتمـاعی جلـوگیری کننـد. در نهایـت، تبیـین صـیانت پـیش‌رویـدادی بـه‌عنـوان یـک راهبـرد امنیـت پیشگیرانه، نیازمند اسـتخراج یـک «مـدل بـومی و یکپارچـه» اسـت کـه تمـامی ابعـاد مـذکور را پوشـش دهـد. بـا توجـه بـه ایـن‌کـه مفـاهیم صـیانت و امنیـت در فضـای مجـازی ایـران دارای ویژگـی‌هـای منحصـربه‌فـرد فرهنگـی، سیاسـی و حقـوقی هسـتند، اسـتفاده از روش نظریـه داده‌بنیـاد ضـرورت مـی‌یابـد تـا از دلِ تجـارب و

1- Ban, Samuel, Takahashi & Inoue
2- Zhang & Thing

متون موجود، مقوله‌های اصلی این راهبرد استخراج شوند. این پژوهش بر این مبنا استوار است که صیانت پیش‌رویدادی نه یک ابزار منفرد، بلکه یک «نظام‌واره راهبردی» است که از پایش فنی در لایه کنترل‌کننده‌های منطقی برنامه‌پذیر تا سیاست‌گذاری کلان در لایه حکمرانی را در بر می‌گیرد و هدف غایی آن، تبدیل فضای مجازی از یک محیط ناامن و واکنشی به یک فضای پایدار، قابل پیش‌بینی و صیانت‌شده است.

روش‌شناسی پژوهش

پژوهش حاضر از منظر هدف، در زمره پژوهش‌های کاربردی قرار می‌گیرد و از حیث ماهیت و روش، با اتکاء به رویکرد کیفی و راهبرد نظریه داده‌بنیاد (برگرفته از نظام روش‌شناختی استراوس و کوربین[1]، ۱۹۹۸) به رشته تحریر درآمده است. هدف اصلی این پژوهش، فرارفتن از توصیف‌های سطحی و دست‌یابی به یک الگوی جامع و تبیینی در خصوص «صیانت پیش‌رویدادی به‌عنوان راهبرد امنیت پیشگیرانه» است. این مهم از طریق طی کردن مراحل سه‌گانه کدگذاری باز، محوری و گزینشی و با هدف نظریه‌پردازی بومی در قلمرو حکمرانی فضای مجازی دنبال شده است. جامعه مورد مطالعه در این تحقیق شامل ۱۵ نفر از نخبگان و صاحب‌نظران کلیدی در حوزه‌های سیاست‌گذاری فضای مجازی، پدافند سایبری، انتظامی، حقوق‌دانان فعال در عرصه جرائم نوظهور و مدیران ارشد زیرساخت‌های حیاتی کشور است. جهت گزینش مشارکت‌کنندگان، از روش نمونه‌گیری نظری با رعایت اصل حداکثر تنوع بهره گرفته شد. فرآیند انتخاب به‌گونه‌ای سامان یافت که ابتدا فهرستی از ۳۰ نفر از متخصصانی که دارای تجربه زیسته و دانش عمیق در ابعاد فنی، حاکمیتی و انتظامی صیانت بودند، تدوین شد. در گام نخست، ۳ نفر از خبرگان جهت انجام مصاحبه‌های اکتشافی و ترسیم نقشه اولیه پرسش‌ها برگزیده شدند. در مراحل بعدی، هم‌سو با ظهور مقولات جدید و ضرورت رفع ابهام‌های نظری، سایر مشارکت‌کنندگان به‌صورت هدف‌مند به فرآیند پژوهش فراخوانده

1- Strauss & Corbin

شدند. این روند تا حصول اشباع نظری ادامه یافت؛ به‌گونه‌ای که پس از انجام ۱۵ مصاحبه عمیق، داده‌های جدید منجر به خلق مقوله یا مفهوم نوینی نشد و غنای نظری لازم حاصل شد.

ویژگی‌های مشارکت‌کنندگان در پژوهش در جدول ۱درج شده است. این ویژگی‌ها شامل جنسیت، سن، تحصیلات، حوزه تخصصی، سابقه کاری و سمت کلی ناشناس افراد است که باعث افزایش اعتبار و صحت داده‌ها در روش‌شناسی کیفی می‌شود.

جدول ۱: ویژگی‌های مصاحبه‌شوندگان (منبع: یافته‌های پژوهش)

ردیف	گروه خبرگان	جنسیت	سن	تحصیلات	حوزه تخصصی	سابقه کاری	سمت کلی	کد مصاحبه شونده
۱	مدیران ارشد و سیاست‌گذاران	مرد	۴۸	دکتری	سیاست‌گذاری فضای مجازی	۲۵ سال	مدیر کل	MP1
۲	مدیران ارشد و سیاست‌گذاران	زن	۵۲	دکتری	مدیریت امنیت سایبری	۲۸ سال	مشاور امنیتی	MP2
۳	کارشناسان فنی و مطلع	مرد	۴۴	کارشناسی ارشد	پدافند سایبری	۲۰ سال	کارشناس ارشد	TE1
۴	کارشناسان فنی و مطلع	زن	۳۸	کارشناسی ارشد	امنیت اطلاعات	۱۶ سال	کارشناس فنی	TE2
۵	اساتید دانشگاهی	مرد	۵۶	دکتری	حقوق سایبری	۳۰ سال	استاد دانشگاه	A1
۶	اساتید دانشگاهی	زن	۵۰	دکتری	جرم‌شناسی سایبری	۲۸ سال	استاد دانشگاه	A2
۷	کارشناسان انتظامی	مرد	۴۲	کارشناسی ارشد	امنیت ملی و انتظامی	۱۸ سال	افسر ارشد پلیس	PO1
۸	کارشناسان انتظامی	زن	۳۹	کارشناسی ارشد	حقوق جزا و امنیت فضای مجازی	۱۵ سال	مدیر بخش پلیس فتا	PO2
۹	اساتید دانشگاهی	مرد	۶۰	دکتری	علوم اجتماعی	۳۲ سال	استاد دانشگاه	A3
۱۰	مدیران ارشد و سیاست‌گذاران	مرد	۵۴	دکتری	فناوری اطلاعات و امنیت	۲۲ سال	مشاور عالی امنیتی	MP3
۱۱	کارشناسان فنی و	زن	۴۰	کارشناسی	امنیت شبکه	۱۷	کارشناس	TE3

ردیف	گروه خبرگان	جنسیت	سن	تحصیلات	حوزه تخصصی	سابقه کاری	سمت کلی	کد مصاحبه شونده
	مطلع			ارشد		سال	فنی	
۱۲	اساتید دانشگاهی	مرد	۵۸	دکتری	حقوق و جرم‌شناسی	۳۰ سال	استاد دانشگاه	A4
۱۳	کارشناسان انتظامی	زن	۳۴	کارشناسی ارشد	پدافند سایبری	۱۱ سال	مدیر فنی پلیس فتا	PO3
۱۴	مدیران ارشد و سیاست‌گذاران	مرد	۴۶	دکتری	مدیریت و سیاست‌گذاری امنیت فضای مجازی	۲۰ سال	مدیرکل پدافند سایبری	MP4
۱۵	اساتید دانشگاهی	زن	۵۳	دکتری	حقوق دیجیتال	۲۷ سال	استاد دانشگاه	A5

ابزار اصلی گردآوری داده‌ها در این پژوهش، مصاحبه‌های عمیق و نیمه‌ساختاریافته بود که امکان واکاوی لایه‌های پنهان موضوع را فراهم می‌آورد. فرآیند تحلیل داده‌ها به‌صورت هم‌زمان با گردآوری آن‌ها آغاز شد؛ بدین ترتیب که پس از اتمام هر نشست، محتوای گفت‌وگوها با دقت بازخوانی و مفاهیم اولیه از دلِ عبارات استخراج شدند (کدگذاری باز). در مرحله دوم، بر پایه وجوه اشتراک و تمایز، این مفاهیم در قالب مقولات فرعی دسته‌بندی شده و روابط میان آن‌ها حول پدیده محوری (صیانت پیش‌رویدادی) در قالب یک مدل نظام‌مند شامل شرایط علّی، زمینه‌ای، مداخله‌گر، راهبردها و پیامدها تبیین گشت (کدگذاری محوری). در نهایت، با پیوند دادن تمامی مقولات حول یک خط داستانی منسجم، نظریه نهایی پژوهش پیرامون امنیت پیشگیرانه تدوین شد (کدگذاری گزینشی).

در این پژوهش، جهت حصول اطمینان از استحکام نظریه و ارتقای سطح روایی و پایایی یافته‌ها، معیارهای دقیقی لحاظ شد. برای افزایش قابلیت اعتماد داده‌ها، از راهبرد کثرت‌گرایی در منابع داده‌ای بهره گرفته شد؛ به این معنا که علاوه‌بر مصاحبه‌های عمیق، از یادداشت‌برداری‌های مستمر در میدان، بررسی اسناد راهبردی و پایش نظام‌مند قوانین صیانتی استفاده شد تا تصویری

همه‌جانبه از موضوع ترسیم شود. هم‌چنین، جهت تأیید صحت استنباط‌ها، مقولات استخراج‌شده به تعدادی از مشارکت‌کنندگان بازگردانده شد و نظرات اصلاحی آنان در مدل نهایی اعمال شد (بازبینی توسط اعضاء). افزون بر این، برای تضمین تأییدپذیری، تمامی مراحل کدگذاری و مسیر استخراج نظریه در اختیار داوران و متخصصان روش‌شناسی قرار گرفت و فرآیند تحلیل از منظر دقت و منطق، مورد تأیید قرار گرفت.

یافته‌ها

در این بخش، نتایج حاصل از تحلیل نظام‌مند داده‌های گردآوری شده ارائه می‌شود. داده‌های این پژوهش که از طریق مصاحبه‌های عمیق با خبرگان، پایش میدانی و واکاوی اسناد راهبردی و قوانین حاکمیتی در حوزه فضای مجازی ایران حاصل شده است، مبنای استخراج نظریه قرار گرفتند. فرآیند تحلیل داده‌ها در فاز کیفی، بر مبنای گام‌های سه‌گانه کدگذاری باز، محوری و گزینشی استوار بوده است. یافته‌های مستخرج با بهره‌گیری از رویکرد نظام‌مند «استراوس و کوربین» در قالب یک مدل پارادایمی انتظام یافته‌اند. این مدل، راهبرد صیانت پیش‌رویدادی را در ابعاد پنج‌گانه الگو شامل: شرایط علّی (پیش‌ران‌های صیانت)، شرایط زمینه‌ای (بستر حاکم)، شرایط مداخله‌گر (عوامل تسهیل‌کننده یا بازدارنده)، راهبردها (اقدامات کنشی و پیشگیرانه) و در نهایت پیامدها (دستاوردهای حاصل از صیانت) تبیین می‌کند. در ادامه، جزییات هر یک از این ابعاد بر اساس کدهای استخراج شده ارائه می‌شود.

۱. شرایط علّی (عوامل پیش‌ران)

مشارکت‌کنندگان در فرایند مصاحبه، در پاسخ به پرسش‌های ناظر بر ابعاد مدل پارادایمی، به تبیین و تشریح ضرورت‌های بنیادین تجدیدنظر در ساختار دفاعی و گذار به سمت «صیانت پیش‌رویدادی» پرداختند. از تحلیل عمیق گزاره‌ها و دیدگاه‌های این خبرگان، کدهای اولیه استخراج شد. در مرحله بعد، مفاهیم مشترک و مورد تأکید که نشان‌دهنده محرک‌های اصلی برای اتخاذ راهبرد امنیت پیشگیرانه بودند، در قالب مقولات محوری دسته‌بندی شدند.

توضیحات خبرگان حاکی از آن است که به‌دلیل پیچیدگی روزافزون تهدیدات، دیگر نمی‌توان با رویکردهای سنتی به مقابله با بحران‌های سایبری پرداخت. جزییات مقولات و مفاهیم شناسایی‌شده در رابطه با شرایط علّی در جدول ۲ ارائه شده است. این جدول شامل ۱۵ مفهوم کلیدی در قالب ۴ مقوله اصلی است.

جدول ۲: مقوله‌ها و مفاهیم شناسایی شده مرتبط با شرایط علّی (منبع: یافته‌های پژوهش)

ابعاد پژوهش	مقوله (کد محوری)	مفهوم (کد باز)	کد مصاحبه‌شوندگان	نمونه گفتار مصاحبه‌شونده
شرایط علّی	ضرورت حاکمیت و اقتدار سایبری	افزایش ناهنجاری‌های دیجیتال و تهدیدات نرم؛ مقاومت زیرساخت‌ها در برابر حملات هدف‌مند؛ ضرورت چابک‌سازی نظام دفاعی در سطح کلان ملی؛ لزوم تثبیت حاکمیت بر درگاه‌های تبادل داده.	MP1, MP4, PO1	«یکی از مشکلات اصلی که ما در فضای مجازی داریم، افزایش ناهنجاری‌هاست. این ناهنجاری‌ها می‌تواند تهدیدات بزرگی ایجاد کند که به راحتی قابل کنترل نیستند. برای مقابله با این تهدیدات، باید حاکمیت سایبری کشور تقویت شود.»
	هم‌افزایی راهبردی و ساختاری	همسویی ساختار پدافندی با ماهیت تهدیدات دوفضائی؛ ضرورت تأمین انتظارات شهروندان در حوزه امنیت داده؛ تعهد دستگاه‌های اجرایی به اهداف مشترک صیانتی؛ مشارکت بین‌سازمانی در جهت پیشبرد اسناد راهبردی ملی.	TE2, A1, PO2	«برای مقابله با تهدیدات سایبری، باید ساختار پدافندی کشور به‌طور کامل همسو با ماهیت تهدیدات جدید دوفضائی شود و دستگاه‌های مختلف در این حوزه باید مشارکت داشته باشند».
	نوآوری در فناوری‌های دفاعی	تنوع و پیچیدگی بدافزارهای نوظهور؛ نیاز به خلاقیت و ایده‌پردازی در طراحی سامانه‌های ایمنی‌بخش؛ تحول در ابزارهای پایش به‌واسطه هوش مصنوعی و یادگیری ماشین؛ ضرورت گذار از دفاع منفعل به دفاع فعال.	TE3, MP2, A2	«امروزه بدافزارهایی که منتشر می‌شوند، بسیار پیچیده‌تر از قبل شده‌اند. به همین دلیل، ما به خلاقیت و ایده‌پردازی برای طراحی سامانه‌های دفاعی نیاز داریم که از هوش مصنوعی و یادگیری ماشین برای شناسایی این تهدیدات استفاده کند».
	توانمندسازی و مدیریت منابع	توانمندی در مدیریت هوشمند منابع انسانی و فنی؛ نقش کلیدی سامانه‌های بومی به	MP3, PO3, TE1	«برای مدیریت منابع به‌طور مؤثر، باید از سامانه‌های بومی استفاده کنیم که قدرت تحلیل پیش‌بینانه

ابعاد پژوهش	مقوله (کد محوری)	مفهوم (کد باز)	کد مصاحبه‌شوندگان	نمونه گفتار مصاحبه‌شونده
		عنوان عامل بازدارنده؛ قدرت و توان زیرساخت‌ها در شناسایی پیش‌دستانه نفوذ؛ توان استفاده از تحلیل‌های پیش‌بینانه جهت مدیریت خطر.		بالایی دارند. این سامانه‌ها به ما کمک می‌کنند تا قبل از وقوع هر گونه تهدید، آن را شناسایی کرده و اقدامات پیشگیرانه انجام دهیم».

تحلیل داده‌های جدول ۲ نشان می‌دهد که مهم‌ترین پیش‌ران برای استقرار صیانت پیش‌رویدادی، «ناکافی بودن نظام‌های دفاعی موجود» در برابر تحولات پرشتاب فضای مجازی است. خبرگان بر این باورند که «افزایش بی‌نظمی‌های سایبری» و «تغییر ماهیت حملات از تخریب ساده به جاسوسی و باج‌افزارهای پیچیده»، حاکمیت را ناگزیر به پذیرش الگویی کرده است که در آن، پیشگیری بر درمان مقدم است.

هم‌چنین، «هم‌افزایی نوآوری فنی» به‌عنوان یک شرط علّی برجسته مطرح شد؛ چرا که بدون بهره‌گیری از فناوری‌های نوین نظیر یادگیری ماشین[1]، شناسایی آنومالی‌های فرآیندی در زیرساخت‌های حیاتی ناممکن خواهد بود. در واقع، نیاز به «چابک‌سازی» در پاسخ‌گویی به تهدیدات، محرکی است که دستگاه‌های حاکمیتی را به سمت تدوین راهبردهای صیانت پیش‌رویدادی سوق می‌دهد تا امنیت را از یک وضعیت تصادفی به یک وضعیت پایدار و قابل پیش‌بینی ارتقاء دهند.

۲. شرایط زمینه‌ای (بسترهای حاکم)

شرایط زمینه‌ای بیان‌گر مجموعه ویژگی‌های خاص و بسترهای زیرساختی، قانونی و فرهنگی است که اجرای راهبرد صیانت پیش‌رویدادی در آن فضا صورت می‌گیرد. بر اساس تحلیل داده‌ها، این ابعاد در جدول ۳ ارائه شده است.

1- AI-driven detection

جدول ۳: مقوله‌ها و مفاهیم شناسایی شده مرتبط با شرایط زمینه‌ای

ابعاد پژوهش	مقوله (کد محوری)	مفهوم (کد باز)	کد مصاحبه‌شوندگان	نمونه گفتار مصاحبه‌شونده
شرایط زمینه‌ای	بلوغ فناوری و زیرساخت بومی	سطح آمادگی اپراتورهای مخابراتی؛ میزان استقلال در تجهیزات رمزنگاری؛ پایداری شبکه‌های محلی؛ توانمندی فنی در بومی‌سازی سامانه‌های ایمنی‌بخش.	MP2, TE3, A5	«در حال حاضر، بسیاری از اپراتورهای ما هنوز آمادگی لازم برای مقابله با تهدیدات جدید را ندارند. بومی‌سازی فناوری‌های امنیتی یکی از نیازهای فوری است».
	الزامات قانونی و اسناد بالادستی	انطباق طرح‌های صیانتی با قانون اساسی؛ وجود اسناد راهبردی پدافند سایبری؛ خلاءهای قانونی در جرم‌انگاری پیش‌رویدادی؛ استانداردهای نظارتی در حکمرانی دیجیتال.	MP3, PO2, A4	«یکی از چالش‌های بزرگ ما، عدم انطباق برخی از طرح‌های صیانتی با قانون اساسی است. ما باید اسناد قانونی جدیدی برای شفافیت بیش‌تر در حوزه پیش‌رویدادی داشته باشیم».
	سرمایه اجتماعی و سواد رسانه‌ای	میزان اعتماد کاربران به پلتفرم‌های داخلی؛ سطح آگاهی عمومی از مخاطرات سایبری؛ آمادگی فرهنگی برای پذیرش نظارت‌های صیانتی؛ توانمندی کاربران در تشخیص محتوای مجرمانه.	PO1, A2, MP4	«اگر کاربران به پلتفرم‌های داخلی اعتماد نکنند، هیچ‌گونه نظارت پیشگیرانه‌ای نمی‌تواند موفق باشد. باید آگاهی عمومی از تهدیدات سایبری افزایش یابد».

شرایط زمینه‌ای در این مدل، حکم بستر و اتمسفری را دارد که راهبرد صیانت پیش‌رویدادی در آن متولد و مستقر می‌شود. یافته‌های پژوهش نشان می‌دهد که «بلوغ فناوری» و «اسناد بالادستی» دو ستون اصلی این بستر هستند. بر اساس دیدگاه خبرگان، تا زمانی که زیرساخت‌های بومی و اپراتورهای مخابراتی به سطح مطلوبی از پایداری و خودکفایی نرسند، اجرای صیانت پیش‌رویدادی با اتکاء به ابزارهای خارجی با ریسک نفوذپذیری همراه خواهد بود. هم‌چنین، تأکید بر «سرمایه اجتماعی» نشان‌دهنده این واقعیت است که صیانت پیشگیرانه، صرفاً یک فرآیند سخت‌افزاری نیست؛ بلکه موفقیت آن در گرو آمادگی فرهنگی جامعه و افزایش سواد رسانه‌ای کاربران است تا پایش‌های امنیتی نه به‌عنوان ابزار محدودیت، بلکه به‌عنوان زیرساختِ امنیت عمومی پذیرفته شود.

۳. شرایط مداخله‌گر (عوامل تسهیل‌کننده یا بازدارنده)

عوامل مداخله‌گر شامل متغیرهایی است که خارج از کنترل مستقیم راهبرد بوده اما بر روند تحقق صیانت پیش‌رویدادی اثرگذارند. این عوامل در جدول ۴ تبیین شده‌اند.

جدول ۴: مقوله‌ها و مفاهیم شناسایی‌شده مرتبط با شرایط مداخله‌گر

ابعاد پژوهش	مقوله (کد محوری)	مفهوم (کد باز)	کد مصاحبه‌شوندگان	نمونه گفتار مصاحبه‌شونده
شرایط مداخله‌گر	موانع فنی و فرآیندی	پدیده خستگی ناشی از انبوه هشدارهای کاذب؛ پیچیدگی مدیریت هویت در محیط‌های ابری؛ نفوذناپذیری برخی پروتکل‌های رمزنگاری خارجی؛ باگ‌های ناشناخته در لایه‌های سخت‌افزاری.	PO2, TE1, MP3	«یکی از مشکلاتی که در حین نظارت پیشگیرانه داریم، خستگی ناشی از هشدارهای کاذب است که هم‌زمان تعداد زیادی هشدار بی‌مورد می‌آید. این باعث می‌شود که توجه به تهدیدات واقعی کاهش یابد».
	چالش‌های اخلاقی و حقوقی	تعارض میان نظارت پیشگیرانه و حریم خصوصی؛ فشارهای بین‌المللی و قواعد حقوق عمومی؛ ابهام در مرز میان فعالیت مدنی و بزه‌کاری (هکتیویسم)؛ چالش‌های صیانت از اطفال در محیط‌های رمزگذاری شده.	MP1, A4, PO3	«در بسیاری از موارد، نظارت پیشگیرانه به‌طور مستقیم با حقوق فردی مانند حریم خصوصی در تضاد است. این تضاد بین اخلاق و قوانین حقوق بشر همیشه یک چالش بزرگ بوده است».
	محدودیت‌های ژئوپلیتیک	تحریم‌های فناوری و عدم دسترسی به هوش پیش‌بینانه جهانی؛ تهدیدات ناشی از بازیگران دولتی (حملات هدف‌مند)؛ عدم توازن در همکاری‌های بین‌المللی در حوزه قضایی سایبر.	MP2, TE2, A3	«یکی از موانعی که ما با آن مواجه هستیم، تحریم‌های فناوری است که باعث می‌شود نتوانیم به ابزارهای پیش‌بینانه جهانی دسترسی پیدا کنیم و این محدودیت تأثیر زیادی در اقدامات پیشگیرانه دارد».

عوامل مداخله‌گر در این الگو، نیروهای پیرامونی هستند که می‌توانند سرعت و کیفیت تحقق صیانت را به‌شدت تحت تأثیر قرار دهند. تحلیل یافته‌ها حاکی از آن است که چالش‌های اخلاقی و «تعارض میان نظارت و حریم خصوصی» جدی‌ترین مانع نرم در مسیر صیانت پیش‌رویدادی است. از سوی دیگر، پدیده‌های فنی نظیر «خستگی ناشی از هشدار» هشدار می‌دهند که افزایش حجم داده‌های پایش شده، در صورت عدم مدیریت هوشمند، می‌تواند به ضدِ خود تبدیل شده و کارآمدی تیم‌های دفاعی را مختل کند. هم‌چنین، متغیرهای ژئوپلیتیک و تحریم‌های فناوری، دست‌یابی به ابزارهای هوش تهدید بین‌المللی را دشوار ساخته و ضرورت تمرکز بر ابزارهای بومیِ پیش‌بینانه را به‌عنوان یک راه‌کار مقابله‌ای برجسته می‌کنند.

۴. راهبردهای اجرایی (اقدامات کنشی)

راهبردها شامل مجموعه‌ای از اقدامات هدفمند است که برای مدیریت پدیده محوری و پاسخ به شرایط علّی اتخاذ می‌شوند. این راهبردها در جدول ۵ استخراج شده‌اند.

جدول ۵: مقوله‌ها و مفاهیم شناسایی‌شده مرتبط با راهبردها

ابعاد پژوهش	مقوله (کد محوری)	مفهوم (کد باز)	کد مصاحبه‌شوندگان	نمونه گفتار مصاحبه‌شونده
راهبردها	پدافند فعال و هوشمند	پیاده‌سازی معماری اعتماد صفر؛ استفاده از یادگیری ماشین برای تشخیص آنومالی؛ فعال‌سازی سامانه‌های فریب هوشمند (تله‌گذاری)؛ پایش مداوم رفتار در زیرساخت‌های حیاتی (PLC).	TE2, MP1, PO1	«باید سیستم‌های دفاعی ما به‌گونه‌ای طراحی شوند که بدون دخالت انسانی، خودشان تهدیدات را شناسایی کنند. استفاده از هوش مصنوعی برای تشخیص آنومالی‌ها یکی از این راه‌حل‌هاست».
	صیانت حمایتی و اجتماعی	آموزش‌های پیشگیرانه متمرکز بر گروه‌های آسیب‌پذیر؛ ارتقای سواد رسانه‌ای به عنوان سد دفاع انسانی؛ حمایت حقوقی از کاربران در برابر بزه‌دیدگی؛ تقویت گفتمان صیانت به مثابه حق شهروندی.	A3, PO2, MP4	«ما به‌ویژه باید گروه‌های آسیب‌پذیر را آموزش دهیم و سواد رسانه‌ای‌شان را ارتقاء دهیم تا بتوانند در برابر تهدیدات سایبری مقاوم‌تر شوند. این نیازمند یک گفتمان فرهنگی و اجتماعی است».
	حکمرانی داده‌محور	نظارت هوشمند بر درگاه‌های تبادل داده بین‌المللی؛ استقرار	MP2, A2, TE1	«برای تحقق حکمرانی داده‌محور، باید سیستم‌های نظارتی هوشمند

ابعاد پژوهش	مقوله (کد محوری)	مفهوم (کد باز)	کد مصاحبه‌شوندگان	نمونه گفتار مصاحبه‌شونده
		سیستم‌های اعتبارسنجی نرم‌افزار پیش از بهره‌برداری؛ ارتقای مدل‌های بلوغ امنیت سایبری؛ تدوین پروتکل‌های همکاری مشترک بین دستگاهی.		ایجاد کنیم که بر درگاه‌های تبادل داده بین‌المللی نظارت کنند. هم‌چنین، همکاری میان دستگاه‌های مختلف کشور در این زمینه ضروری است».

راهبردها در مدل پارادایمی، قلب تپنده امنیت پیشگیرانه و کنشی محسوب می‌شوند. یافته‌های استخراج‌شده نشان می‌دهد که صیانت پیش‌رویدادی از طریق یک «مهندسی سه‌گانه» محقق می‌شود: نخست، راهبرد فنی که با تکیه بر «معماری اعتماد صفر» و یادگیری ماشین، کوچک‌ترین ناهنجاری را در زیرساخت‌های حساس (PLC) رصد می‌کند؛ دوم، راهبرد اجتماعی که با تمرکز بر صیانت حمایتی، سپری انسانی در برابر بزه‌کاری سایبری ایجاد می‌کند؛ و سوم، راهبرد حکمرانی که با نظارت هوشمند بر درگاه‌های تبادل داده، به‌دنبال تثبیت اقتدار دیجیتال است. این راهبردهای ترکیبی نشان‌دهنده آن است که صیانت پیش‌رویدادی فراتر از یک لایحه قانونی، یک دکترین دفاعی همه‌جانبه است که در آن «فناوری»، «قانون» و «آموزش» در یک چرخه هم‌افزا قرار می‌گیرند.

۵. پیامدها (خروجی‌های راهبرد)

پیامدها نشان‌دهنده نتایج حاصل از اجرای موفق راهبرد صیانت پیش‌رویدادی هستند که در جدول ۶ ارائه شده‌اند.

جدول ۶: مقوله‌ها و مفاهیم شناسایی‌شده مرتبط با پیامدها

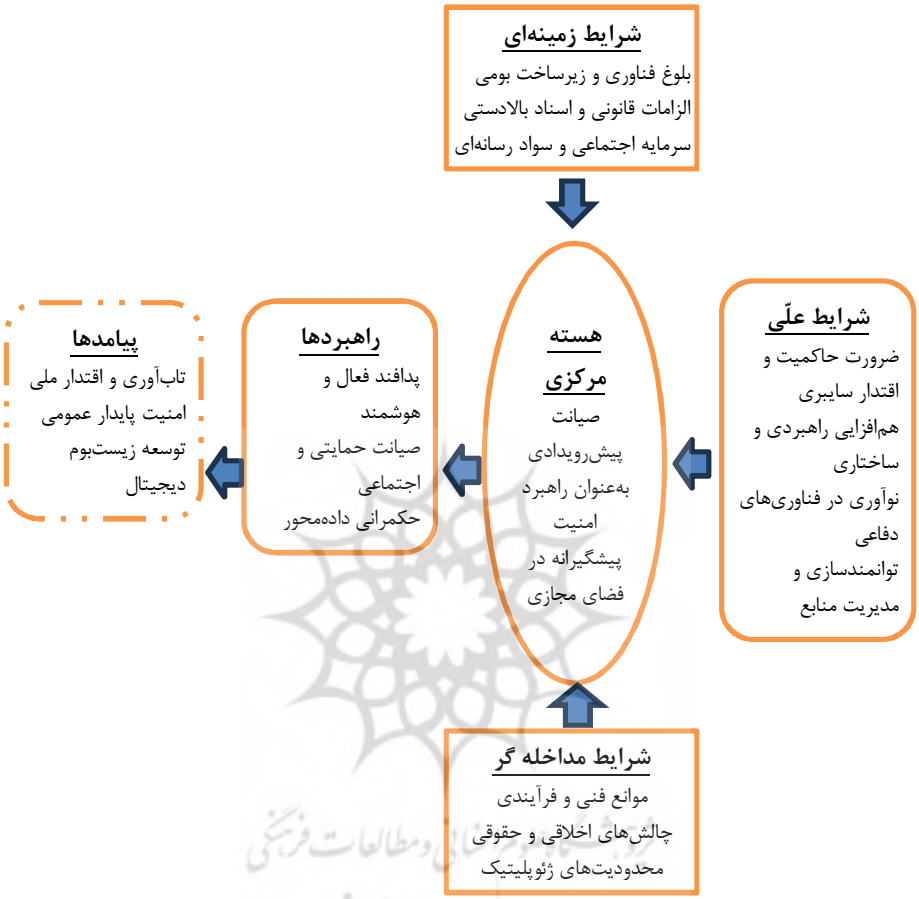
ابعاد پژوهش	مقوله (کد محوری)	مفهوم (کد باز)	کد مصاحبه‌شوندگان	نمونه گفتار مصاحبه‌شونده
پیامدها	تاب‌آوری و اقتدار ملی	افزایش پایداری زیرساخت‌های حیاتی در برابر بحران؛ تثبیت حاکمیت سایبری در محیط بین‌الملل؛ کاهش وابستگی به محصولات امنیتی خارجی؛ ایجاد قدرت بازدارندگی پیش‌دستانه.	MP3, TE1, PO1	«افزایش تاب‌آوری کشور در برابر بحران‌های سایبری و کاهش وابستگی به محصولات امنیتی خارجی می‌تواند به تقویت اقتدار ملی کمک کند. این امر برای تضمین امنیت ملی در سطح جهانی ضروری

ابعاد پژوهش	مقوله (کد محوری)	مفهوم (کد باز)	کد مصاحبه‌شوندگان	نمونه گفتار مصاحبه‌شونده
				است».
	امنیت پایدار عمومی	کاهش نرخ بزه‌دیدگی و جرائم سایبری؛ ایجاد محیط امن برای رشد اطفال و نوجوانان؛ تقویت اعتماد عمومی به خدمات پایه کاربردی؛ کاهش هزینه‌های بازیابی پس از سانحه در سطح کلان.	PO2, MP4, A1	«با بهبود امنیت سایبری، نه‌تنها جرائم سایبری کاهش می‌یابد، بلکه اعتماد عمومی به خدمات دولتی و آنلاین نیز تقویت خواهد شد. این امر می‌تواند به کاهش هزینه‌ها در سطح کلان منجر شود».
	توسعه زیست‌بوم دیجیتال	شکوفایی اقتصاد دیجیتال در بستر امن؛ ارتقای رتبه امنیت سایبری کشور در شاخص‌های جهانی؛ بهبود کیفیت حکمرانی دیجیتال؛ شفافیت در حقوق و تکالیف شهروند مجازی.	TE3, A2, MP2	«ایجاد یک زیست‌بوم دیجیتال امن باعث شکوفایی اقتصاد دیجیتال خواهد شد. اگر امنیت سایبری کشور بهبود یابد، جایگاه ما در شاخص‌های جهانی ارتقا پیدا می‌کند و این موجب رشد پایدار خواهد شد».

پیامدهای استخراج‌شده در این پژوهش، غایت و هدف نهایی استقرار صیانت پیش‌رویدادی را ترسیم می‌کنند. تحلیل نتایج نشان می‌دهد که خروجی غایی این راهبرد، فراتر از امنیت فنی، دست‌یابی به «تاب‌آوری ملی» و «اقتدار سایبری» در محیط بین‌الملل است. با تحقق صیانت پیش‌رویدادی، فضای مجازی از یک محیط تهدیدمحور به یک زیست‌بوم امن برای شکوفایی اقتصاد دیجیتال تبدیل می‌شود. کاهش معنادار نرخ جرائم (به‌ویژه جرائم علیه اطفال) و تقویت اعتماد عمومی به خدمات پایه، پیامدهایی هستند که ثبات اجتماعی را تضمین می‌کنند. در واقع، این پیامدها ثابت می‌کنند که امنیت پیشگیرانه با کاهش هزینه‌های بازیابی و پیشگیری از بحران‌های امنیتی، منجر به پایداری راهبردی نظام حکمرانی در عصر دیجیتال خواهد شد.

با توجه به استخراج نظام‌مند مقوله‌ها و مفاهیم در قالب شرایط علّی، زمینه‌ای، مداخله‌گر، راهبردها و پیامدها، می‌توان گفت که پدیده «صیانت پیش‌رویدادی در فضای مجازی» واجد یک منطق درونی چندسطحی و پویاست که تنها از طریق تحلیل رابطه‌مند اجزای آن قابل فهم است. از این‌رو، به‌منظور نمایش یکپارچه پیوندها، تعاملات و جهت‌گیری‌های علّی میان

مقـولات محـوری و زیرمقولـه‌هـا، اسـتفاده از شـکل ۱ (مـدل پـارادایمی) ضـروری به‌نظر می‌رسد.



شکل ۱: الگوی صیانت پیش‌رویدادی به‌عنوان راهبرد امنیت پیشگیرانه در فضای مجازی

در شکل ۱، الگـوی «صـیانت پـیش‌رویـدادی بـه‌عنـوان راهبـرد امنیـت پیشـگیرانه در فضـای مجـازی» بـا رویکـرد نظریـه داده‌بنیـاد اسـتخراج شـده اسـت. ایـن الگـو بـر اسـاس یافتـه‌هـای کیفـی حاصـل از تحلیـل عمیـق دیـدگاه‌هـای خبرگـان ارائـه شـده اسـت. در ایـن الگـو، شـرایط علّـی، عوامـل پیشـران و ضـرورت‌هـای بنیـادینی هسـتند کـه موجبـات اتخـاذ راهبـرد امنیـت پیشـگیرانه را فـراهم مـی‌آورنـد؛ عـواملی نظیـر

«ضرورت حاکمیت و اقتدار سایبری» و «نوآوری در فناوری‌های دفاعی» که به‌دلیل ناکارآمدی الگوهای سنتی در مواجهه با تهدیدات نوین، از نظر تقدم زمانی و جنبه‌های الزام‌آور بر پدیده اصلی (صیانت پیش‌رویدادی) تأثیر علی داشته‌اند. در لایه بعدی، شرایط زمینه‌ای شامل «بلوغ فناوری و زیرساخت بومی» و «سرمایه اجتماعی»، بستری را توصیف می‌کنند که اجرای راهبرد در آن میسر می‌شود. هم‌زمان، شرایط مداخله‌گر نظیر «محدودیت‌های ژئوپلیتیک» و «چالش‌های اخلاقی و حقوقی»، به عنوان متغیرهای تسهیل‌کننده یا بازدارنده، روند تحقق صیانت را تحت تأثیر قرار می‌دهند.

بخش عملیاتی الگو تحت عنوان راهبردها، مجموعه‌ای از اقدامات کنشی شامل «پدافند فعال و هوشمند»، «صیانت حمایتی» و «حکمرانی داده‌محور» را در بر می‌گیرد که برای مدیریت پدیده‌محوری اتخاذ می‌شوند. نهایتاً، پیامدها بازنمایی‌کننده خروجی‌های راهبردی این الگو هستند که در سه سطح «تاب‌آوری و اقتدار ملی»، «امنیت پایدار عمومی» و «توسعه زیست‌بوم دیجیتال» تبلور یافته و غایت نهایی امنیت پیشگیرانه را در زیست‌بوم فضای مجازی ترسیم می‌کنند.

شرایط زمینه‌ای در این مدل، بیان‌گر بسترهای خاص و زیرساختی از جنس پدیده برای اجرای الگوی صیانت پیش‌رویدادی هستند؛ شرایطی هم‌چون «بلوغ فناوری و زیرساخت بومی»، «الزامات قانونی» و «سرمایه اجتماعی» که می‌بایست برای موفقیت عملیاتی و پذیرش اجتماعی این فرآیندها مورد توجه قرار گیرند. برخلاف شرایط زمینه‌ای، عوامل مداخله‌گر عبارت‌اند از شرایط عام از جنس محیط که بر انتخاب سازوکارهای صیانت مؤثر است و می‌توانند اجرای این راهبردها را تسهیل کرده و یا به‌عنوان بازدارنده (مانند محدودیت‌های ژئوپلیتیک و چالش‌های اخلاقی) عمل کند.

در بُعد اقدامات و راهبردها، کنش‌ها و فعالیت‌های اصلی که می‌توانند در اجرای الگوی صیانت پیش‌رویدادی راه‌گشا باشد، مورد توجه قرار گرفته است؛ اقداماتی نظیر «پدافند فعال و هوشمند»، «صیانت حمایتی» و «حکمرانی داده‌محور». ویژگی مهم این بُعد آن است که مفاهیم و مقوله‌های آن از نوع

فرآیندی نیستند، بلکه از نوع اقدام و دکترین دفاعی هستند که به اجرای پایدار امنیت در فضای مجازی کمک می‌کنند. در بُعد پیامدها، نتایج مورد انتظار از اجرای این الگو در سه سطح «تاب‌آوری و اقتدار ملی»، «امنیت پایدار عمومی» و «توسعه زیست‌بوم دیجیتال» تبیین شده است؛ پیامدهایی که می‌توانند در اثر پیوند ارگانیک میان فناوری، قانون و آموزش عاید حاکمیت و جامعه شود.

در نهایت، با بررسی و کنکاش بر روی ابعاد پنج‌گانه مذکور و با انتزاع بیش‌تر این مقولات در مرحله کدگذاری انتخابی، یک مقوله هسته‌ای به شرح: «تبیین صیانت پیش‌رویدادی به‌عنوان راهبرد امنیت پیشگیرانه در فضای مجازی» ظاهر شد که تمامی مقولات دیگر را پوشش می‌دهد. پس از تهیه الگوی پارادایمی، برای افزایش اعتبار الگو، مدل نهایی در اختیار خبرگانی قرار گرفت که با موضوع امنیت سایبری و روش نظریه داده‌بنیاد آشنایی داشتند تا در مورد فرآیند تدوین و ساختار نهایی نظرات خود را ارائه دهند. بیش‌تر آن‌ها الگو را تأیید کرده و اصلاحات جزیی مدنظر ایشان در یک فرآیند رفت‌وبرگشتی اعمال گردید تا مدل نهایی تثبیت شود.

بحث و نتیجه‌گیری

الگوی استخراج‌شده در این پژوهش نشان می‌دهد که «صیانت پیش‌رویدادی» واجد ماهیتی فراتر از یک بسته اقدامات فنی یا انتظامی است و باید آن‌را به‌مثابه یک الگوی حکمرانی امنیتی چندسطحی در فضای مجازی تحلیل کرد. در این الگو، امنیت سایبری نه به‌عنوان واکنشی به وقوع جرم، بلکه به‌عنوان یک فرآیند کنشی و پیش‌بینانه تعریف می‌شود که هدف آن مدیریت فعال تهدیدات پیش از تبدیل شدن به بحران است. این رویکرد، در تقابل با منطق سنتی امنیت پسینی قرار می‌گیرد و نشان می‌دهد که کارآمدی نظام‌های انتظامی و امنیتی در عصر دیجیتال، بیش از آن‌که به‌شدت واکنش وابسته باشد، به توان پیش‌بینی، پایش هوشمند و مداخله به‌موقع گره خورده است. از منظر نظری، الگوی صیانت پیش‌رویدادی بازتاب‌دهنده یک جابه‌جایی بنیادین در پارادایم امنیت است؛ جابه‌جایی‌ای که در آن تمرکز از «کنترل جرم

واقع‌شده» به «مدیریت ریسک پیشینی» منتقل می‌شود. این تغییر پارادایمی، پیامدهای مهمی برای سیاست‌گذاری انتظامی دارد، زیرا نقش پلیس و نهادهای حافظ نظم عمومی را از یک کنش‌گر واکنشی به یک بازیگر پیش‌دستانه و تحلیل‌محور ارتقاء می‌دهد. در این چارچوب، پلیس دیگر صرفاً مجری قانون پس از وقوع جرم نیست، بلکه به یکی از ارکان کلیدی حکمرانی داده‌محور و پیشگیری هوشمند در فضای مجازی تبدیل می‌شود.

تحلیل روابط میان مقوله‌های الگو نشان می‌دهد که صیانت پیش‌رویدادی تنها در بستر هم‌افزایی میان سطوح مختلف حکمرانی قابل تحقق است. شرایط علّی مانند افزایش تهدیدات دوفضایی و ضرورت اقتدار سایبری، زمانی به راهبردهای مؤثر منجر می‌شوند که در چارچوب شرایط زمینه‌ای مناسب شامل بلوغ زیرساختی، انسجام قانونی و سرمایه اجتماعی عمل کنند. این امر بیان‌گر آن است که امنیت پیشگیرانه در فضای مجازی، پدیده‌ای تک‌علتی یا تک‌نهادی نیست، بلکه محصول تعامل پویا میان سیاست‌گذاری کلان، ظرفیت‌های فناورانه، الزامات حقوقی و کنش‌های انتظامی هدف‌مند است. یکی از دلالت‌های مهم الگوی پژوهش آن است که نقش نهادهای انتظامی، به‌ویژه پلیس‌های تخصصی فعال در حوزه فضای مجازی، در تحقق صیانت پیش‌رویدادی نقشی محوری و غیرقابل جایگزین است. یافته‌ها نشان می‌دهد که پلیس سایبری، پلیس فتا و سایر بخش‌های تخصصی انتظامی، در این الگو صرفاً نقش مجری ندارند، بلکه به‌عنوان حلقه اتصال میان سیاست‌های کلان، فناوری‌های پیش‌بینانه و واقعیت‌های میدانی عمل می‌کنند. این جایگاه، ضرورت بازتعریف مأموریت‌های انتظامی در حوزه سایبر را از تمرکز صرف بر کشف جرم به سمت پیشگیری فعال، پایش مستمر و مدیریت هوشمند تهدیدات برجسته می‌سازد.

از منظر حقوقی و اجتماعی، الگوی صیانت پیش‌رویدادی نشان می‌دهد که پیشگیری مؤثر در فضای مجازی بدون توجه هم‌زمان به حقوق شهروندی، حریم خصوصی و مشروعیت اجتماعی امکان‌پذیر نیست. در این چارچوب، صیانت نه به‌معنای محدودسازی صرف، بلکه به‌مثابه تضمین حق امنیت دیجیتال شهروندان معنا می‌یابد. این تفسیر، به‌ویژه برای نهادهای انتظامی حائز

اهمیت است، زیرا مشروعیت کنش‌های پیشگیرانه پلیس در فضای مجازی، بیش از هر چیز به شفافیت، قانون‌مندی و پذیرش اجتماعی وابسته است. هم‌چنین، الگوی پژوهش نشان می‌دهد که فناوری‌های نوظهور، به‌ویژه هوش مصنوعی و تحلیل‌های پیش‌بینانه، تنها ابزارهای پشتیبان نیستند، بلکه به هسته عقلانی صیانت پیش‌رویدادی تبدیل شده‌اند. این فناوری‌ها امکان عبور از منطق دفاع منفعل و حرکت به سمت دفاع فعال و هوشمند را فراهم می‌کنند، اما در عین حال، بدون هدایت نهادی، انتظامی و حقوقی مناسب، می‌توانند خود به منبع چالش‌های جدید بدل شوند. از این‌رو، الگوی ارائه‌شده بر ضرورت هم‌راستاسازی فناوری با راهبردهای حکمرانی و مأموریت‌های انتظامی تأکید دارد. در نهایت، می‌توان گفت الگوی صیانت پیش‌رویدادی استخراج‌شده در این پژوهش، تصویری نظام‌مند از امنیت پیشگیرانه در فضای مجازی ارائه می‌دهد که در آن، امنیت نه یک وضعیت ایستا، بلکه یک فرآیند پویا، چندبُعدی و آینده‌نگر است. این الگو نشان می‌دهد که تحقق امنیت پایدار در فضای مجازی مستلزم عبور از نگاه‌های بخشی، تقویت نقش پیشگیرانه نهادهای انتظامی و استقرار سازوکارهای حکمرانی داده‌محور است؛ رویکردی که می‌تواند مبنایی نظری و عملی برای بازطراحی سیاست‌های امنیتی و انتظامی کشور در مواجهه با تهدیدات پیچیده سایبری فراهم آورد.

در تبیین شرایط علّی و زمینه‌ای، نتایج پژوهش بر نقش محوری «حاکمیت واحد و هم‌افزایی نهادی» و هم‌چنین «بلوغ فناوری‌های بومی» تأکید می‌ورزد. تفسیر این یافته نشان می‌دهد که بدون وجود یک ساختار فرماندهی منسجم و استقلال در تولید ابزارهای امنیتی، صیانت پیش‌رویدادی در سطح یک ایده نظری باقی خواهد ماند. این بخش از یافته‌ها با نتایج پژوهش حسینی و همکاران (۱۴۰۳) و هم‌چنین برون (۱۴۰۳) که بر لزوم «اقتدار حکمرانی سایبری» و «یکپارچگی ساختاری» برای مقابله با تهدیدات نوین تأکید داشتند، در تراز هم‌سویی کامل قرار دارد. هم‌چنین، تأکید بر بومی‌سازی زیرساخت‌ها در این مدل، با یافته‌های شهیر و همکاران (۱۴۰۳) که امنیت پایدار را در گرو کاهش وابستگی به فناوری‌های بیگانه می‌دانند، قرابت مفهومی دارد.

در سطح راهبردهای عملیاتی، الگوی مستخرج بر دو محور «پدافند هوشمند داده‌محور» و «صیانت حمایتی-آموزشی» استوار است. تفسیر یافته‌ها نشان می‌دهد که بهره‌گیری از هوش مصنوعی و یادگیری ماشین برای پیش‌بینی آنومالی‌ها و رفتارهای بزه‌کارانه قبل از وقوع جرم، هسته سخت صیانت پیش‌رویدادی را تشکیل می‌دهد. این رویکرد پیش‌دستانه با پیشینه‌های بین‌المللی برجسته‌ای نظیر مطالعات رافیکا و همکاران (۲۰۲۵) و سان و همکاران (۲۰۲۳) که بر «استخراج هوش تهدید» و تبدیل امنیت به یک فرآیند پیش‌بینانه تأکید دارند، کاملاً مطابقت دارد. علاوه‌بر این، راهبرد صیانت اجتماعی از طریق ارتقای سواد سایبری کاربران، که در مدل حاضر به‌عنوان یک رکن اساسی شناسایی شد، با نتایج پژوهش بیدارونند و پورقهرمانی (۱۴۰۳) در خصوص نقش «واکسیناسیون اجتماعی» در کاهش نرخ قربانی‌شدن کاربران، هم‌سو است.

تحلیل شرایط مداخله‌گر در این پژوهش، چالش‌های اخلاقی و حقوقی را به‌عنوان متغیرهای محدودکننده صیانت پیش‌رویدادی برجسته ساخت. تفسیر این یافته مبین آن است که در مسیر پیاده‌سازی نظارت‌های پیشگیرانه، همواره بیم نقض حریم خصوصی و حقوق شهروندی وجود دارد؛ از این‌رو صیانت پیش‌رویدادی زمانی مشروعیت و کارآمدی خواهد داشت که در چارچوب «حقوق عمومی سایبری» تعریف و نظام‌مند شود. این دغدغه راهبردی در نتایج پژوهش رایجیان اصلی و همکاران (۱۴۰۳) نیز به‌عنوان یک ضرورت انتقادی مورد بحث قرار گرفته بود که نشان‌دهنده دقت نظر مدل طراحی‌شده در توجه به ملاحظات پیرامونی و چالش‌های اجرایی است. در نهایت، پیامدهای استقرار این الگو، فراتر از امنیت کوتاه‌مدت، به سمت «تاب‌آوری ملی» و «اقتدار بین‌المللی در فضای مجازی» میل می‌کند. تفسیر نهایی یافته‌ها نشان می‌دهد که صیانت پیش‌رویدادی با تغییر موازنه هزینه-فایده به ضرر مهاجمان، منجر به ایجاد یک محیط دیجیتال امن و پایدار برای توسعه اقتصادی و اجتماعی می‌شود. این برون‌داد با پارادایم‌های نوین جهانی همچون «تاب‌آوری سایبری تکاملی» که توسط تزاوارا و واسیلیادیس (۲۰۲۴) تبیین شده است، هم‌خوانی

دارد. به‌طور خلاصه، این مقاله با ارائه یک مدل جامع و چندبُعدی، توانسته است ضمن تجمیع دیدگاه‌های نخبگانی، خلاء موجود در ادبیات پژوهشی پیرامون راهبردهای پیشگیرانه بومی را پوشش داده و نقشه راهی عملیاتی برای سیاست‌گذاران حوزه امنیت فضای مجازی ترسیم کند.

پیشنهادها

بر مبنای یافته‌های حاصل از الگوی پارادایمی صیانت پیش‌رویدادی و با هدف عملیاتی‌سازی نتایج پژوهش در سطوح کلان سیاست‌گذاری و اجرایی، پیشنهادهای زیر ارائه می‌شود:

۱. **پیشنهادهای مبتنی بر شرایط علّی (تقویت پیشران‌های حاکمیتی)**: با توجه به ضرورت هم‌افزایی ساختاری، پیشنهاد می‌شود؛ «ستاد عالی فرماندهی صیانت پیشگیرانه» زیر نظر شورای عالی فضای مجازی تشکیل شود. وظیفه اصلی این ستاد، یکپارچه‌سازی بانک‌های اطلاعاتی تهدیدات و تدوین نظام‌نامه جامع پدافند پیش‌رویدادی برای تمامی دستگاه‌های اجرایی است تا از موازی‌کاری در تشخیص زودهنگام حملات جلوگیری شود.

۲. **پیشنهادهای مبتنی‌بر شرایط زمینه‌ای (توسعه زیرساخت و بومی‌سازی)**: پیشنهاد می‌شود؛ دولت با ارائه تسهیلات ویژه، از شرکت‌های دانش‌بنیان برای تولید سامانه‌های بومی تشخیص نفوذ و تحلیل رفتار مبتنی بر هوش مصنوعی حمایت کند. استقلال در ابزارهای رمزنگاری و زیرساختی، بستر لازم را برای اجرای صیانت پیش‌رویدادی بدون واهمه از کدهای مخفی بیگانه فراهم می‌سازد.

۳. **پیشنهادهای مبتنی‌بر راهبردها (اقدامات عملیاتی و کنشی)**: ضروری است مراکز تحلیل داده‌های عظیم برای رصد فعالیت‌های مشکوک در لایه‌های پنهان شبکه راه‌اندازی شوند. هم‌چنین، اجرای طرح ملی «واکسیناسیون سایبری» از طریق آموزش‌های مستمر سواد رسانه‌ای به کاربران، می‌تواند به‌عنوان یک راهبرد صیانت اجتماعی، نفوذناپذیری

جامعه در برابر حملات مهندسی اجتماعی را تضمین کند.

۴. **پیشنهادهای مبتنی‌بر شرایط مداخله‌گر (مدیریت چالش‌های حقوقی):** به‌منظور صیانت از حقوق شهروندی، پیشنهاد می‌شود؛ «منشور اخلاق و حقوق صیانت پیشگیرانه» تدوین شود. این منشور باید مرزهای دقیق میان نظارت حاکمیتی برای امنیت عمومی و حفظ حریم خصوصی کاربران را شفاف کرده و نظارت قانونی بر فرآیندهای صیانت را تقویت کند تا مشروعیت اجتماعی اقدامات پیشگیرانه حفظ شود.

۵. **پیشنهادهای مبتنی بر پیامدها (پایدارسازی اقتدار سایبری):** پیشنهاد می‌شود؛ «شاخص ملی تاب‌آوری سایبری» به عنوان ابزاری برای ارزیابی سالانه آمادگی دستگاه‌ها تعریف شود. هم‌چنین تقویت دیپلماسی سایبری با کشورهای هم‌سو جهت اشتراک اطلاعات مربوط به تهدیدات نوظهور، می‌تواند پیامد نهایی مدل که همانا اقتدار بین‌المللی و بازدارندگی فعال است را محقق سازد.

با توجه به محدودیت‌های پژوهش مانند پیچیدگی دسترسی به خبرگان امنیتی و ماهیت محرمانه برخی داده‌های زیرساختی، پیشنهاد می‌شود در پژوهش‌های آتی به برازش کمی این مدل در سازمان‌های مختلف پرداخته شود تا پایداری نتایج در ساختارهای متفاوت سازمانی مورد آزمون قرار گیرد.

سپاس‌گزاری

نویسندگان بر خود لازم می‌دانند از تمام نخبگان، همکاران محترم علمی و کلیه مصاحبه‌کنندگان که در فرایند نگارش و تکمیل پژوهش یاری‌گر ما بودند، کمال تشکر و سپاس را داشته باشیم.

منابع

اکبری، عباسعلی، و نوروزعلی، روح‌اله (۱۴۰۱). پیشگیری از جرائم سایبری با نگاهی به طرح صیانت از فضای مجازی. سومین کنفرانس ملی پدافند سایبری. https://civilica.com/doc/1543210

امامی، نسرین، داودی گرمارودی، هما، و پاکزاد، بتول (۱۴۰۲). پیشگیری از جرائم سایبری با تأکید بر هکتیویسم. پژوهش‌های تطبیقی فقه، حقوق و سیاست، ۵ (۲)، ۱۸-۱. https://doi.org/10.61838/csjlp.6.3.4 & https://csjlp.org/index.php/csjlp/article/view/187

امیرمحمدی، محمد، عبدی‌نژاد، صالح، و شکربیگی، علیرضا (۱۴۰۳). مطالعه آسیب‌ها و جرائم مرتبط با فضای مجازی و سیاست‌های پیشگیری از آن‌ها در نیروهای مسلح. پژوهش‌های تطبیقی فقه، حقوق و سیاست، ۶ (۳)، ۲۵-۱. https://doi.org/10.61838/csjlp.6.4.18 & https://csjlp.org/index.php/csjlp/article/view/114

امیریان فارسانی، امین (۱۴۰۲). آسیب‌شناسی چالش‌های حاکم بر پیشگیری وضعی حاکم بر جرائم سایبری. فصلنامه علوم خبری، ۱۲ (۴۶)، ۱۰۵-۷۷. 10.30495/cyberlaw.2023.1979281.1064 & https://journals.iau.ir/article_708037.html

امین‌الرعایا، یاسر، و امین‌الرعایا، حسین (۱۴۰۲). امکان‌سنجی حفظ امنیت ملی از طریق نظارت بر اینترنت و شبکه‌های اجتماعی از منظر قواعد بین‌المللی. فصلنامه مطالعات حقوقی، ۱۵ (۳)، ۹۸-۷۵. DOR: 20.1001.1.25381857.1402.16.61.6.2 & https://journals.ihu.ac.ir/article_208765.html

برون، مهرداد (۱۴۰۳). حکمرانی سایبری؛ مفهوم و ضرورت. اولین کنفرانس ملی حکمرانی و نظام سیاست‌گذاری فرهنگی، تهران. https://civilica.com/doc/2209087

بیدارونـد، مختـار، و پورقهرمـانی، بابـک (۱۴۰۳). نقـش پیشـگیرانه سـواد رسـانه‌ای در دوران اپیـدمی کووید-۱۹ بـر بـزه‌کـاری سـایبری. فصـلنامه مطالعـات حقـوقی فضـای مجـازی، ۳ (۱)، ۲۰-۱. https://sanad.iau.ir/Journal/cyberlaw/Article/1122219

بیژنـی، شـهریار، طـالبی، محمـد، و انتظـاری، محمدحسـن (۱۴۰۲). مـدل مفهـومی بلـوغ امنیـت سـایبری اپراتورهـای بـزرگ مخـابراتی کشـور. فصـلنامه امنیـت ملـی، ۱۳ (۴۸)، ۵۸-۳۵. https://dor.isc.ac/dor/20.1001.1.33292538.1402.13.48.6.2 & https://ns.sndu.ac.ir/article_2509.html

پورمسجدیان، فاطمه، هدایت، مریم سادات، و حدنه، فاطمه (۱۴۰۲). ظرفیت‌های آموزش سواد رسانه در حمایت از حقوق شهروند مجازی. مطالعات فقه و حقوق رسانه، ۵(بهار و تابستان ۱۴۰۲)، ۲۵۰-۲۲۹. doi: 10.22034/5.1.229 & https://journal.refah.ac.ir/article_725482.html

حسینی، محمدرضا، رامک، مهراب، انتظاری، محمدحسن، و فرخی، محمدحسن (۱۴۰۳). ارائه طرح راهبردی حکمرانی فضای سایبر کشور در محیط بین‌الملل. فصلنامه امنیت ملی، ۱۴ (۵۱)، ۱۵۶-۱۱۹. https://journals.sndu.ac.ir/article_2949.html

رایجیان اصلی، مهرداد، رحیمی‌نژاد، اسمعیل، و رزم‌آور، رضا (۱۴۰۳). سیاست‌گذاری جنایی تقنینی در آینه جرم‌شناسی فرهنگی: با رویکردی انتقادی به چالش‌های صیانت از فضای مجازی. پژوهش‌نامه حقوق کیفری، ۱۵ (۱)، ۱۳۵-۱۱۰. https://doi.org/10.22034/jclc.2023.346236.1706 & https://jclc.sdil.ac.ir/article_170718.html

رجبی‌زاده، ایمان، و مدیری، ناصر (۱۴۰۱). الزامات راهبردی و عملیاتی دستگاه‌های اجرایی برای توسعه محاسبه‌گر کاستی‌های امنیت سایبری. فصلنامه سیستم‌های هوشمند، ۲ (۳)، ۱۳-۱. DOR: 20.1001.1.27832570.1400.2.1.1.2 & https://sanad.iau.ir/journal/impcs/Article/683457?jid=683457

ریاضی‌پور، مریم (۱۴۰۳). حقوق عمومی در عصر دیجیتال: چالش‌ها، فرصت‌ها و راه‌کارهای نوین حکمرانی سایبری. نوزدهمین کنفرانس ملی حقوق و علوم اجتماعی، تهران. https://civilica.com/doc/2205432

سامانی‌پور، فرزانه، بزرگمهر، کیا، رمضانی‌پور، مهرداد، و حقزاد، آمنه (۱۴۰۲). سنجش شاخص‌های پدافند غیرعامل متناسب با تهدیدهای دوفضائی کلان‌شهر تهران. امنیت ملی، ۱۴(۵۴)، ۸۰-۴۵. https://ns.sndu.ac.ir/article_3361.html

سعادت سیرت، ناهید، و خانیکی، هادی (۱۴۰۴). شناسایی ساختارهای اطلاعاتی در رسانه‌های اجتماعی و تأثیر آن بر رفتار اشتراک‌گذاری کاربران ایرانی. مطالعات فضای مجازی و رسانه‌های اجتماعی، ۲ (۱)، ۲۰-۱. https://doi.org/10.22083/cssms.2025.526863.1058 & https://cssms.ricac.ac.ir/article_225573.html

سهراب، صمد (۱۴۰۴). بررسی نقش هوش‌مصنوعی به‌عنوان میانجی‌گر در صیانت پیش‌رویدادی پلیس. فصلنامه نظارت و بازرسی، ۱۹(۷۲).

& https://10.22034/si.2025.104974
http://si.jrl.police.ir/article_104974.html

شهیر، احسان، حسن‌بیگی، ابراهیم، تقی‌پور، رضا، و ریاضی، عبدالمجید (۱۴۰۳). ابعاد و مؤلفه‌های بومی امنیت فضای مجازی کشور. فصلنامه راهبرد دفاعی، ۲۲ (۸۵)، ۳۶-۹. https://ssc.sndu.ac.ir/article_3242.html

غیوری ثالث، مجید، مدیری، ناصر، موحدی صفت، محمدرضا، و سقایی، علیرضا (۱۴۰۳). ارائه الگوی راهبردی به‌کارگیری امن سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی کشور. امنیت ملی، ۱۴(۵۱)، ۱۹۸-۱۵۷.
https://dor.isc.ac/dor/20.1001.1.25383329.1403.14.51.6.0 &
https://ns.sndu.ac.ir/article_2950.html

قربانی، علیرضا، و خیامی، عبدالکریم (۱۴۰۲). تحلیل گفتمان طرح حمایت از حقوق کاربران و خدمات پایه کاربردی فضای مجازی. فصلنامه سیاست‌نامه علم و فناوری، ۱۳ (۴)، ۴۲-۲۱. https://dor.isc.ac/dor/20.1001.1.24767220.1402.13.4.2.0
& https://stpl.ristip.sharif.ir/article_23529.html

کرمانیان، پریوش، پورقهرمانی، بابک، و بیگی، جمال (۱۴۰۳). نقش فضای مجازی در پیشگیری اجتماعی از جرائم علیه حیات‌وحش. پژوهش‌های تطبیقی فقه، حقوق و سیاست، ۶ (۴)، ۲۰-۱. https://csjlp.org/article-1-245-fa.html

کریمی کلیمانی، مجتبی (۱۴۰۳). الگوی حکمرانی صنعت امنیت سایبری جمهوری اسلامی ایران. فصلنامه نگرش مدیریت راهبردی، ۲(۳)، ۱۵۲-۱۲۷.
https://dor.isc.ac/dor/20.1001.1.30605865.1403.2.3.5.7 &
https://pmr.sndu.ac.ir/article_3343.html

محمدی برزگر، جعفر، قبادی، عباس، و حیدرنژاد، علیرضا (۱۴۰۴). چالش‌های صیانت پیش‌رویدادی در کارکنان پلیس و ارائه راه‌کارها. فصلنامه نظارت و بازرسی، ۱۹(۷۲). https://10.22034/si.2025.104976 &
http://si.jrl.police.ir/article_104976.html

مختاری، حمیدرضا، و مدیری، ناصر (۱۴۰۱). وارسی و اعتبارسنجی نیازمندی‌های نرم‌افزار در سیستم‌های ایمنی‌بخش. فصلنامه سیستم‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند، ۲ (۴)، ۱۱-۱.
https://dorl.net/dor/20.1001.1.27832570.1400.2.1.5.6 &
https://sanad.iau.ir/journal/impcs/Article/903339

منصوری‌نیا، زینب (۱۴۰۳). تعارض یا تطابق طرح صیانت از فضای مجازی با حقوق شهروندی. نهمین کنفرانس بین‌المللی فقه، حقوق و پژوهش‌های دینی. https://civilica.com/doc/1987654

ولی‌زاده، مریم (۱۴۰۲). امنیت سایبری اطفال و نوجوانان در فضای مجازی؛ آسیب‌شناسی و خنثی‌سازی مخاطرات. پژوهش‌های جرم شناسی کاربردی، ۲(۴)، ۱-۲۴. doi: 10.22034/aqcr.2025.2049110.1047 & https://www.qacr.ir/article_720757.html

Aboah Boateng, E., & Bruce, J. W. (2022). Unsupervised Machine Learning Techniques for Detecting PLC Process Control Anomalies. Journal of Cybersecurity and Privacy, 2(2), 220-244. https://doi.org/10.3390/jcp2020012

Ban, T., Samuel, N., Takahashi, T., & Inoue, D. (2021). Combat security alert fatigue with AI-assisted techniques. Proceedings of the 14th Cyber Security Experimentation and Test Workshop, 9–16. https://doi.org/10.1145/3474718.3474723

Broeders, D. (2021). Private active cyber defense and (international) cyber security—pushing the line? Journal of Cybersecurity, 7(1), tyab010. https://doi.org/10.1093/cybsec/tyab010

Cai, Z., & Koutsoukos, X. (2023). Real-time detection of deception attacks in cyber-physical systems. International Journal of Information Security, 22, 1-16. https://doi.org/10.1007/s10207-023-00677-z

Dziwisz, D. (2024). Legalising Forms of Active Cyber Defense (ACD): The Theory and Practice of Private Cybersecurity Provisioning. Politeja, 21(6), 135-160. https://doi.org/10.12797/Politeja.21.2024.93.06

Egho-Promise, E. I., Asante, G., Balisane, H., Salih, A., Aina, F., Kure, H., & Gavua, E. K. (2025). Leveraging artificial intelligence for predictive cybersecurity: Enhancing threat forecasting and vulnerability management. International Journal of Innovative Research in Advanced Engineering, 12(02), 68–79. https://doi.org/10.26562/ijirae.2025.v1202.01

Eze, E. C., Umeanozie, C. P., & Alozie, C. E. (2025). Enhancing Threat Intelligence for Critical Infrastructure Protection Through Artificial Intelligence: A Proactive Cyber Defence Approach. International Journal of Scientific Research and Modern Technology, 4(5), 20-29. https://doi.org/10.38124/ijsrmt.v4i5.513

Gaba, S., Budhiraja, I., Kumar, V., Martha, S., Khurmi, J., Singh, A., Singh, K. K., Askar, S. S., & Abouhawwash, M. (2024). A systematic analysis of enhancing cyber security using deep learning for cyber physical systems. IEEE Access, 12, 6017–6035. https://doi.org/10.1109/ACCESS.2023.3349022

Hasan, K., Hossain, F., Amin, A., Sutradhar, Y., Jeny, I. J., & Mahmud, S. (2025). Enhancing Proactive Cyber Defense: A Theoretical Framework for AI-Driven

Predictive Cyber Threat Intelligence. Journal of Technologies Information and Communication, 5(1), 33-122. https://doi.org/10.55267/rtic/16176

Islam, S. A. M., et al. (2024). AI-driven Predictive Analytics for Enhancing Cybersecurity in a Post-pandemic World: a Business Strategy Approach. International Journal for Multidisciplinary Research, 6(5), 1-19. https://doi.org/10.36948/ijfmr.2024.v06i05.28493

Lee, J., & Park, J.-H. (2023). AI as "Another I": Journey map of working with artificial intelligence from AI-phobia to AI-preparedness. Organizational Dynamics, 52(3), 100994. https://doi.org/10.1016/j.orgdyn.2023.100994

Manne, T. A. K. (2023). Proactive Cyber Defense Mechanisms for Cloud Computing Environments. Journal of Artificial Intelligence & Cloud Computing, 2(3), 1-5. https://doi.org/10.47363/4ssk7n22

Mirza, I. B., Georgakopoulos, D., & Yavari, A. (2023). Cyber-Physical-Social Awareness Platform for Comprehensive Situation Awareness. Sensors, 23(2), 822. https://doi.org/10.3390/s23020822

Mochinaga, D. (2025). Rising sun in the cyber domain: Japan's strategic shift toward active cyber defense. The Pacific Review, 38(2), 370–395. https://doi.org/10.1080/09512748.2024.2384447

Muthusamy, K. (2025). Harnessing AI-Powered Zero Trust Architectures for Proactive Cyber Defense: A Comprehensive Framework for Future-Ready Network Security Ecosystems. International Journal of AI, BigData, Computational and Management Studies, 6(1), 22-29. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V6I1P103

Patil, R. Y., Patil, Y. H., Despande, H., & Bannore, A. (2024). Proactive cyber defense through a comprehensive forensic layer for cybercrime attribution. International Journal of Information Technology, 16, 3555–3572. https://doi.org/10.1007/s41870-024-01947-2

Rafika, A. S., Baltasar, S., Adiwijaya, A., & Rizky, Z. S. (2025). Cybersecurity strategies for preventing ransomware attacks in cloud-based applications. Journal of Computer Science and Technology Application, 2(2), 1–11. https://doi.org/10.33050/corisinta.v2i2.77

Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives. IEEE Communications Surveys & Tutorials, 25(3), 1748-1774.
https://doi.org/10.1109/COMST.2023.3273282

Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. Journal of Cybersecurity and Privacy, 2(3), 573–586. https://doi.org/10.3390/jcp2030029

Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: a historical and conceptual review. International Journal of Information Security,

23, 1695–1719. https://doi.org/10.1007/s10207-023-00811-x

Wang, R. (2024). AI-Powered Predictive Cybersecurity in Identifying Emerging Threats through Machine Learning. 2024 IEEE 3rd International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA). https://doi.org/10.1109/EEBDA60612.2024.10485789

Zhang, L., & Thing, V. L. L. (2021). Three decades of deception techniques in active cyber defense – Retrospect and outlook. Computers & Security, 106, Article 102288. https://doi.org/10.1016/j.cose.2021.102288