امنیت الکترونیک

فصل‌نامهٔ اختصاصی صنعت تجهیزات ایمنی و حفاظت

سال هفتم | شماره نهم |زمستان ۱۴۰۴| ۶۵۰ هزار تومان

در این شماره می‌خوانیم:


هزاربین
آتن
آزمایشگاه تجهیزات نظارت تصویری
سیمنا
سامانه یکپارچه مدیریت و نظارت ایکس-ری
Automation
IP
سامانه
میهن
سامانه مدیریت یکپارچه هشدار نفوذ
رخ پایش®
نگهبان هوشمند
امن پایش®
AmnPaayesh
هوبان
سامانه‌ی
اتوماسیون
پارکینگ
فرجا

بسم الله الرحمن الرحیم

امنیت الکترونیک

صاحب امتیاز و مدیرمسئول: محمد قلم‌چی
سردبیر: سارا قلم‌چی

هیئت تحریریه (به‌ترتیب حروف الفبا): مونا احمدی
محمد قلم‌چی
محمود سعیدی

ویراستار: محمود سعیدی
صفحه‌آرایی و طراحی: سارا قلم‌چی
طرح روی جلد: زهرا سنجابی

مشخصات نشر: تهران، مجتمع چاپ ایران‌کهن

نشانی دبیرخانه: تهران- اقدسیه- بلوار ارتش- اراج- شانزده‌متری ولیعصر- نبش خیابان پروین- پلاک ۲- واحد ۴
تلفن: ۲۲۹۶۷۷۶۳-۰۲۱
نمابر: ۲۲۹۶۷۷۶۹-۰۲۱
نشانی اینترنتی: www.electronicsecurity.ir
پست الکترونیک: info@electronicsecurity.ir

فهرست

سرمقاله

نتایج ناگوار بی‌توجهی به آسیب‌شناسی زیست‌بوم نظارت‌تصویری کشور

نویسنده: محمد قلم‌چی

مدیرعامل مؤسسه دانش‌بنیان
خدمات مدیریت و فناوری رشد قلم‌چی

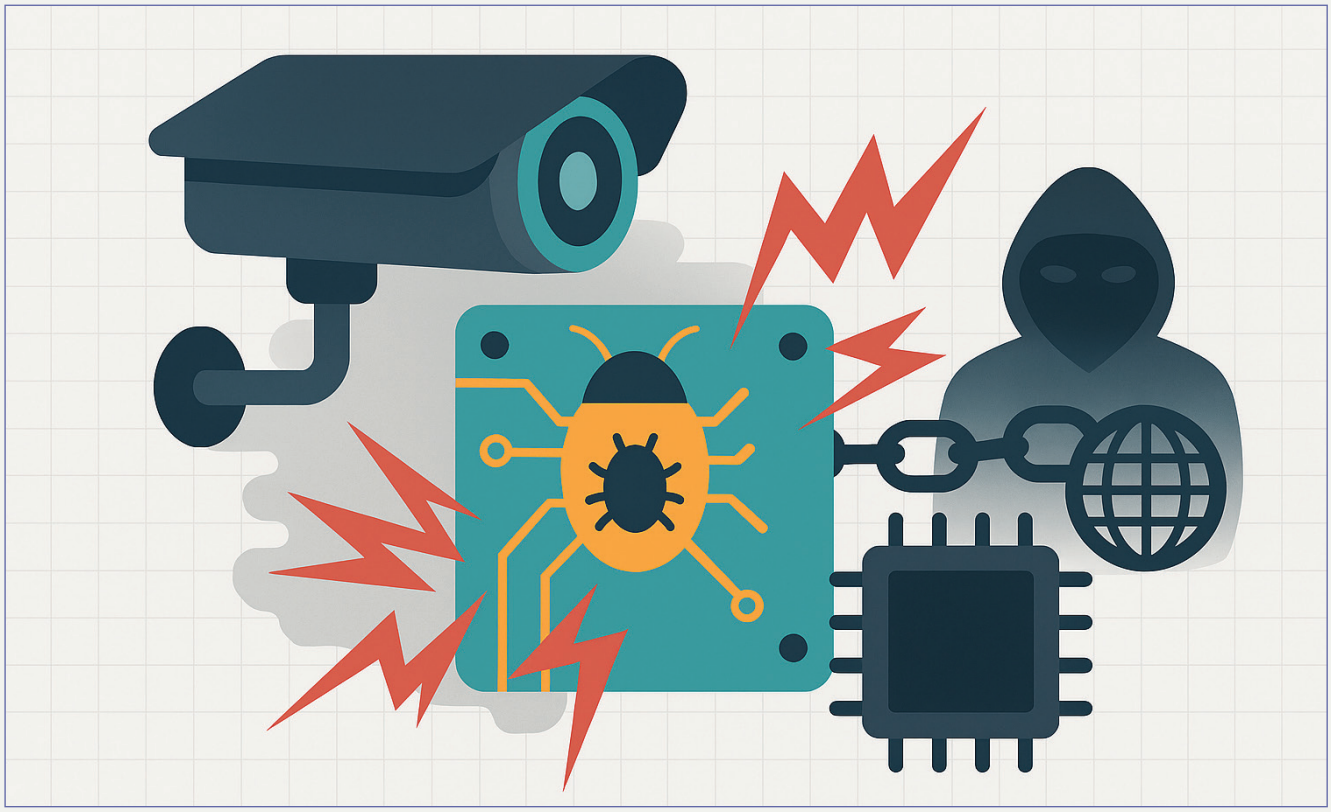
فایننشال‌تایمز مدعی شده اسرائیل با هک دوربین‌های ترافیکی، بیت رهبری را زیر نظر داشته است. فایننشال‌تایمز با گفتگو با بیش از ۱۲ مقام فعلی و سابق اطلاعاتی اسرائیل در گزارشی از جزئیات این عملیات پرده برداشته است. بنابر این گزارش، اسرائیل با هک دوربین‌های کنترل ترافیک تهران محافظان رهبری را زیر نظر گرفته بود و سازمان سیا نیز یک منبع انسانی در ایران داشت. درصورت صحت این گزارش، ضعف امنیتی دوربین‌های مداربسته سازمان کنترل ترافیک شهرداری تهران، در موفقیت ترور رهبر معظم انقلاب، نقش داشته است. این در حالی است که در مستند پخش شده از تلویزیون اسرائیل، در جنگ ۱۲ روزه که چند ماه قبل با ترور فرماندهان ارشد کشور ایران عزیزمان شروع شد، متجاوز مدعی شده است که کنترل بخش عمده‌ای از دوربین‌های مداربسته کشور، از جمله دوربین‌های نظارت شهری و کنترل ترافیک تهران را در ایام جنگ در دست داشته است. این اخبار هیچگاه از طرف ایران تایید نشدند، ولی با نبود استانداردها و راهکارهای امنیت سایبری تخصصی نظارت تصویری، خیلی هم دور از ذهن نیستند.

خبرهایی نیز منتشر شده است که ادعای نفوذ سرویس‌های اطلاعاتی اسرائیل به سامانه‌های نظارت‌تصویری یک طرفه نبوده است و این کشور مدعی فناوری‌های نفوذ، نتوانسته امنیت سایبری سامانه‌های نظارت تصویری خود را تامین نماید. گروه هکری محور مقاومت اسلامی سایبری «Cyber Islamic resistance-Axis» اعلام کرد که در عملیاتی در جبهه جنوبی، موفق به نفوذ و کنترل بیش از ۱۲۰ دوربین و سرور اینترنتی متعلق به رژیم صهیونیستی شده است. همچنین گروه موسوم به «راچل هانتر» اعلام کرده است که موفق به نفوذ به سامانه‌های نظارتی و دوربین‌های مداربسته اماکن مذهبی حساس در اورشلیم شده و به سورهای ذخیره‌سازی ویدئو و داده‌های تشخیص چهره دسترسی پیدا کرده است. اخبار نفوذ به سامانه‌های نظارت تصویری هیچگاه به صورت کامل تایید نشده‌اند، این تنها برخی از اخباری است که نشان می‌دهد هر دو طرف توانایی تامین کامل امنیت سایبری سامانه‌های نظارت تصویری خود، خصوصاً دوربین‌های مداربسته شهری را ندارند.

در سرمقاله تابستان امسال، استاندارد، آزمایش و انطباق‌پذیری سامانه‌های نظارت تصویری، به عنوان مولفه‌های تحقق کارآمدی نظارت تصویری معرفی شد، ولی در شرایط افزایش تهدیدات در کشور، مافیای نظارت تصویری که منافع خود را در کارشکنی تصویب استانداردهای امنیت سایبری نظارت تصویری و همچنین جلوگیری از انطباق‌سنجی سامانه‌های نظارت تصویری می‌بینند، نهایت تلاش خود را برای رسیدن به منافع خود که نتیجه‌ای جز کاهش امنیت سایبری سامانه‌های نظارت تصویری کشور به همراه نداشته است، به کار بسته‌اند. طبق تحلیل‌ها، مافیای نظارت تصویری شامل سه دسته هستند. دسته اول، مشاورین فاسد و کم سواد سامانه‌های نظارت تصویری و ITS هستند. استانداردی که موجب عدم نیاز به اسناد بی‌ارزش و کپی شده می‌شود و به عنوان نقشه‌راه مورد استفاده قرار می‌گیرد، موجب می‌شود اسناد کم‌ارزشی که یکبار بدست آورده‌اند را نتوانند به قیمت گزاف به سازمان‌های مختلف و شهرداری‌های سراسر کشور به قیمت‌های میلیاردی بفروش رسانند. از سوی دیگر نتایج آزمایشگاهی موجب جلوگیری از انتخاب تجهیزات ناکارآمد شده و ریسک برملا شدن دست ایشان در تبانی با فروشندگان محصولات بی‌کیفیت را بالا می‌برد. انطباق‌پذیری ادواری نیز واقعیت پروژه‌های انجام شده را برملا می‌کند. دسته دوم، فروشندگان اجناس بی‌کیفیت نظارت تصویری هستند. فروشندگانی که اکثراً تولید را هم بدنام کرده‌اند، از افشای کیفیت واقعی تجهیزاتی که بعضاً به ۲۰ برابر قیمت در پروژه‌های اکثراً دولتی می‌فروشند، در بیم هستند. دسته سوم دلالان فاقد دانش، تخصص و ریاکاری هستند که با ادعای ارتباط با نهادهای انتظامی و امنیتی، خود را به تصمیم‌گیران، کارگروه‌ها و بعضاً اتحادیه‌های غیرقانونی نزدیک نموده‌اند، لکن در اصل دلال فروش تجهیزات و اجرای پروژه‌ها در کشور هستند و به دلیل کاهش تاثیرشان و به طبع آن درآمد نامشروعی که از فروشندگان دریافت می‌کنند از تصویب استاندارد و انجام انطباق‌سنجی سامانه‌های نظارت تصویری بسیار ناخشنودند و تمامی تلاش خود را برای کارشکنی در کار آزمایشگاه‌های تخصصی بکار بسته‌اند. سطح نازل دانش و عدم حداقل تخصص ایشان از سرقت داده و کپی‌برداری غیرمجازی که از اولین پرتال تخصصی انطباق‌سنجی سامانه‌های نظارت تصویری در ایران انجام داده‌اند، مشخص است.

پروتکل‌های اختصاصی و کمتر شناخته شده، سفت‌افزارهای مستعد نفوذ، حجم بالای تبادل داده نسبت به سایر تجهیزات ICT، ضعف بالا در رمزنگاری کامل داده حتی در راهکارهای رده بالا، موجب نیاز گسترده جهانی به محصول تخصصی تامین امنیت سایبری راهکارهای نظارت تصویری شده است. ایران اولین کشور جهان است که به محصولی تخصصی برای تامین امنیت فعال و پیشگیرانه شبکه نظارت تصویری دست یافته است. موسسه دانش‌بنیان خدمات مدیریت و فناوری رشد قلم‌چی، از سال ۱۳۹۲ محصول تخصصی امنیت سایبری نظارت تصویری را برای اولین بار در جهان تولید کرده و در حال توسعه آن است و منتظر رونمایی رسمی پس از بهره‌برداری گسترده در سطح ملی است. چنین محصولاتی برای تاثیرگذاری در حکمرانی سایبری کشور نیازمند عظم جدی مسئولان است.

سوال بزرگ اینجاست که آیا تلاش برای ترور رهبر عالی‌قدر یک کشور نباید موجب اقدامی موثر در آن کشور برای جلوگیری از روش‌های نفوذ و جمع‌آوری اطلاعات دشمن شود؟ وقتی بارها هشدارهای لازم، سال‌ها و تکرار آن ماه‌ها قبل از حادثه داده شده است، وقتی دشمن خود بارها اعتراف کرده که ترور را در برنامه خود دارد و سابقه ترور فرماندهان کشور را نیز در کارنامه خود داشت، چرا روش‌های جمع‌آوری اطلاعات دشمن مسدود نشد؟ چرا با مافیای نظارت تصویری برخورد مناسب صورت نمی‌پذیرد؟ آیا کسانی در این میان منافعی دارند که حتی به قیمت ترور رهبرشان حاضر نیستند دست از آن منافع بکشند؟



تروجان‌های سخت‌افزاری در سامانه‌های نظارت تصویری:

انواع، اجزا و روش‌های فعال‌سازی

نویسنده: محمود سعیدی

تروجان‌های سخت‌افزاری به‌عنوان یکی از مهم‌ترین تهدیدات در حوزه امنیت سایبری و زنجیره تأمین سخت‌افزار، نقش پررنگی در به خطر انداختن امنیت سامانه‌های حیاتی دارند. این تروجان‌ها به‌صورت تغییرات عمدی و پنهان در طراحی یا ساخت تراشه‌ها اعمال می‌شوند و می‌توانند عملکرد یک سامانه را مختل کرده یا اطلاعات حساس را به خارج از سامانه منتقل کنند. در سامانه‌های نظارت تصویری که در زیرساخت‌های حیاتی، امنیت شهری و مراکز حساس استفاده می‌شوند، وجود تروجان‌های سخت‌افزاری می‌تواند منجر به تهدیدات جدی از جمله افشای اطلاعات، از کار افتادن سامانه یا ایجاد نقاط کور امنیتی شود. این مقاله به معرفی تروجان‌های سخت‌افزاری، انواع و روش‌های فعال‌سازی آنها در سامانه‌های نظارت تصویری می‌پردازد.

با افزایش پیچیدگی سامانه‌های نظارت تصویری و ادغام فناوری‌های پیشرفته مانند هوش مصنوعی و شبکه‌های پرسرعت، سطح حملات امنیتی نیز گسترش یافته است. یکی از مهم‌ترین تهدیدات نوظهور در این حوزه، تروجان‌های سخت‌افزاری[1] هستند که برخلاف بدافزارهای نرم‌افزاری، در سطح تراشه و سخت‌افزار تعبیه می‌شوند. این نوع تروجان‌ها می‌توانند در مراحل مختلف زنجیره تأمین، از طراحی تا تولید وارد سامانه شوند و عملکرد آن را تحت کنترل مهاجم قرار دهند. تروجان سخت‌افزاری یک تغییر مخرب در طراحی یا ساختار یک تراشه یا قطعه سخت‌افزاری است که می‌تواند عملکرد سامانه را مختل کند، داده‌ها را به بیرون منتقل کرده یا حتی کل سامانه را از کار بیندازد. این تهدید در سطح سخت‌افزار ایجاد شده و معمولاً به‌گونه‌ای طراحی می‌شود که در حالت عادی، شناسایی آن دشوار باشد [۱].
ویژگی پنهان‌کاری و غیرقابل‌مشاهده بودن این تروجان‌ها باعث می‌شود که تشخیص آن‌ها به‌وسیله روش‌های سنتی بسیار دشوار باشد [۲]. یک تروجان سخت‌افزاری ممکن است تنها تحت شرایط خاص فعال شود یا به‌صورت تدریجی عملکرد سامانه را مختل کند. این ویژگی‌ها باعث می‌شود که این نوع تهدید برای سامانه‌هایی مانند دوربین‌های نظارتی، دستگاه‌های ضبط و واحدهای پردازشی که در محیط‌های امنیتی استفاده می‌شوند، بسیار خطرناک باشد [۳]. اهمیت موضوع زمانی بیشتر می‌شود که بدانیم بسیاری از تراشه‌های به‌کاررفته در تجهیزات نظارتی از طریق زنجیره تأمین بین‌المللی تأمین می‌شوند و کنترل کامل بر تمامی مراحل تولید امکان‌پذیر نیست. بنابراین، تروجان‌های سخت‌افزاری می‌توانند بدون شناسایی وارد سیستم شوند و حتی در طولانی‌مدت باقی بمانند [۴].

انواع تروجان‌های سخت‌افزاری در سامانه‌های نظارت تصویری

تروجان‌های سخت‌افزاری باعث ایجاد رفتارهای غیرمجاز، نقض امنیت یا اختلال در عملکرد می‌شوند. این تروجان‌ها می‌توانند در مراحل مختلف چرخه عمر سخت‌افزار، از طراحی اولیه تا تولید و توزیع، اضافه شوند و به‌دلیل ماهیت فیزیکی‌شان، شناسایی و حذف آن‌ها بسیار دشوار است. تروجان‌های سخت‌افزاری می‌توانند بر مبنای اهداف مهاجم، محرمانگی داده‌ها را نقض کنند یا حتی باعث خرابی کامل سامانه نظارت تصویری شوند.
تروجان‌های سخت‌افزاری را می‌توان به چهار گروه اصلی تقسیم کرد:

الف) تروجان‌های عملکردی[2]
ب) تروجان‌های اطلاعاتی[3]
ج) تروجان‌های تخریبی[4]
د) تروجان‌های کاهش قابلیت اطمینان[5]

۱. تروجان‌های عملکردی

تروجان‌های عملکردی نوعی از تروجان‌های سخت‌افزاری یا نرم‌افزاری هستند که به گونه‌ای طراحی می‌شوند تا عملکرد سامانه هدف را به طور مخفیانه تغییر دهند یا اختلال ایجاد کنند بدون آنکه به راحتی قابل شناسایی باشند. این تروجان‌ها معمولاً در بخش‌هایی از سامانه تعبیه می‌شوند که فعالیت عادی را انجام می‌دهند اما تحت شرایط خاص، رفتار غیرمنتظره و مخرب از خود نشان می‌دهند [۵]. به عنوان مثال، تروجان‌های عملکردی ممکن است منطق یک مدار را تغییر دهند تا در هنگام بروز یک ورودی خاص، داده‌ها به صورت نادرست پردازش شوند یا سیگنال‌های کنترلی را دستکاری کنند. شناسایی و مقابله با این نوع از تروجان‌ها به دلیل پنهان‌کاری بالا در آنها بسیار دشوار است.
یکی از ویژگی‌های مهم تروجان‌های عملکردی، فعال‌سازی در شرایط خاص و نه به صورت همیشگی است. به این معنی که این تروجان‌ها معمولاً تنها زمانی که یک الگوی خاص از ورودی‌ها یا وضعیت‌های سیستمی رخ می‌دهد، فعال می‌شوند و عملکرد سیستم را تحت تاثیر قرار می‌دهند [۶]. این رفتار شرطی باعث می‌شود که آزمون‌های استاندارد و بازبینی‌های معمول نتوانند آن‌ها را شناسایی کنند زیرا در طول زمان آزمون، رفتار سامانه طبیعی به نظر می‌رسد و تروجان خاموش باقی می‌ماند. بنابراین، این تروجان‌ها به طور هوشمندانه در طراحی و تولید سامانه‌ها جاسازی می‌شوند.
از دیدگاه امنیت سایبری، تروجان‌های عملکردی تهدید جدی برای یکپارچگی و قابلیت اعتماد سیستم‌ها به ویژه در حوزه‌های حیاتی مانند نظامی، پزشکی و صنایع حیاتی هستند [۷].
مقابله با این نوع تروجان‌ها نیازمند روش‌های پیشرفته تحلیل و اعتبارسنجی سخت‌افزاری، شناسایی رفتارهای غیرمعمول و استفاده از تکنیک‌های یادگیری ماشین برای تشخیص ناهنجاری‌ها است. در نتیجه، پژوهش‌های گسترده‌ای در زمینه طراحی روش‌های تشخیص زودهنگام و حذف تروجان‌های عملکردی با هدف افزایش امنیت سامانه‌ها در حال انجام است.

۲. تروجان‌های اطلاعاتی

تروجان‌های اطلاعاتی نوعی بدافزار یا قطعه مخرب سخت‌افزاری یا نرم‌افزاری هستند که به منظور سرقت، دستکاری یا افشای غیرمجاز اطلاعات حساس در سامانه‌های کامپیوتری طراحی می‌شوند. این تروجان‌ها معمولاً به صورت پنهان و غیرقابل تشخیص وارد سامانه می‌شوند و با جمع‌آوری داده‌ها مانند رمزهای عبور، کلیدهای رمزنگاری یا اطلاعات شخصی کاربران، تهدیدی جدی برای حریم خصوصی و امنیت داده‌ها به شمار می‌روند [۸].
یکی از روش‌های رایج فعالیت تروجان‌های اطلاعاتی، جاسوسی پنهان از ترافیک داده‌ها و استخراج اطلاعات کلیدی در شبکه‌ها یا سامانه‌های هدف است.
این نوع تروجان‌ها ممکن است در سخت‌افزارهای شبکه، سامانه‌های کنترل صنعتی یا حتی در تراشه‌های الکترونیکی تعبیه شوند تا به طور مداوم اطلاعات مهم را رهگیری کنند [۳]. به دلیل ماهیت پنهان این تروجان‌ها، شناسایی آن‌ها نیازمند استفاده از تکنیک‌های پیشرفته تحلیل رفتاری و بررسی دقیق جریان داده‌ها است که معمولاً توسط ابزارهای امنیتی سنتی قابل شناسایی نیستند.
از سوی دیگر، تروجان‌های اطلاعاتی می‌توانند به صورت نرم‌افزاری در قالب برنامه‌های مخرب یا افزونه‌های مرورگر نیز ظاهر شوند که پس از نصب توسط کاربر، داده‌های خصوصی را جمع‌آوری و به سرورهای مهاجم ارسال می‌کنند
مقابله با این تهدیدات مستلزم به‌کارگیری راهکارهای امنیتی چندلایه شامل رمزنگاری داده‌ها، تحلیل رفتاری برنامه‌ها و آموزش کاربران برای شناسایی و اجتناب از دانلود نرم‌افزارهای مخرب است [۹].
همچنین بررسی صحت سخت‌افزار و نرم‌افزار به منظور شناسایی هر گونه تغییر غیرمجاز یا افزوده شدن تروجان‌های اطلاعاتی اهمیت بالایی دارد

۳. تروجان‌های تخریبی

تروجان‌های تخریبی نوعی بدافزار یا قطعه مخرب سخت‌افزاری هستند که هدف اصلی آن‌ها ایجاد خسارت فیزیکی یا منطقی به سامانه‌های هدف است. برخلاف تروجان‌های اطلاعاتی یا عملکردی که بیشتر به سرقت یا تغییر اطلاعات می‌پردازند، تروجان‌های تخریبی با هدف از کار انداختن سامانه، نابودی داده‌ها، یا آسیب‌رساندن به اجزای سخت‌افزاری طراحی می‌شوند [۱۰]. این نوع تروجان‌ها می‌توانند در لایه‌های مختلف سامانه‌های الکترونیکی و کامپیوتری جایگذاری شوند و در زمان یا شرایط خاصی فعال شوند تا حداکثر تخریب را ایجاد کنند.

یکی از مهم‌ترین ویژگی‌های تروجان‌های تخریبی، توانایی آن‌ها در ایجاد خرابی‌های جدی و گاهی جبران‌ناپذیر است. به عنوان مثال، در سخت‌افزارهای صنعتی یا سامانه‌های کنترلی حیاتی، فعال شدن این تروجان‌ها می‌تواند باعث از کار افتادن ماشین‌آلات، ایجاد حوادث ایمنی یا نابودی اطلاعات حساس شود [۱۱]. همچنین این تروجان‌ها ممکن است به گونه‌ای طراحی شوند که پس از مدتی غیرفعال باقی بمانند و سپس به صورت ناگهانی فعال شده و خسارت عمده‌ای به سامانه وارد کنند که این موضوع تشخیص آن‌ها را بسیار دشوار می‌کند.

مقابله با تروجان‌های تخریبی نیازمند استراتژی‌های جامع امنیتی است که علاوه بر شناسایی و حذف آن‌ها، تمرکز ویژه‌ای بر روی نظارت مستمر و آنالیز رفتار سیستم‌ها داشته باشد. استفاده از روش‌های آنالیز رفتاری و تکنیک‌های یادگیری ماشین برای تشخیص الگوهای غیرعادی می‌تواند در شناسایی زودهنگام این تروجان‌ها موثر باشد [۱۲]. همچنین، طراحی سامانه‌های مقاوم و استفاده از معماری‌های امن در سخت‌افزار و نرم‌افزار از جمله راهکارهای پیشگیری در برابر حملات تخریبی محسوب می‌شوند.

۴. تروجان‌های کاهش قابلیت اطمینان

تروجان‌های کاهش قابلیت اطمینان نوعی از تروجان‌های سخت‌افزاری هستند که هدف اصلی آن‌ها کاهش تدریجی و پنهان قابلیت اطمینان و عمر مفید سیستم‌های هدف می‌باشد. برخلاف تروجان‌های تخریبی که به طور ناگهانی خسارت وارد می‌کنند، این تروجان‌ها به گونه‌ای طراحی شده‌اند که در طول زمان باعث کاهش عملکرد و افزایش نرخ خرابی قطعات سخت‌افزاری شوند. این نوع تروجان‌ها معمولاً به صورت تغییرات جزئی و پنهان در مدارهای الکترونیکی اعمال می‌شوند که به مرور زمان باعث افزایش خطا و ناپایداری سامانه می‌شوند.

از آنجا که تروجان‌های کاهش قابلیت اطمینان به صورت مخفی و تدریجی عمل می‌کنند، تشخیص آن‌ها بسیار دشوار است و معمولاً تا زمانی که آسیب‌های قابل توجهی ایجاد نکنند، شناسایی نمی‌شوند [۱۳]. این تروجان‌ها می‌توانند باعث افزایش مصرف انرژی، بروز خطاهای مکرر یا کاهش سرعت عملکرد سامانه شوند که در نهایت به کاهش عمر مفید قطعات منجر می‌شود. به همین دلیل، چنین تروجان‌هایی تهدیدی جدی برای صنایع حساس به قابلیت اطمینان مانند هوافضا، نظامی و پزشکی محسوب می‌شوند.

برای مقابله با تروجان‌های کاهش قابلیت اطمینان، روش‌های مختلفی از جمله تحلیل عمیق ساختار سخت‌افزار، آزمون‌های استرس طولانی‌مدت و روش‌های مبتنی بر یادگیری ماشین برای شناسایی تغییرات غیرطبیعی در رفتار قطعات ارائه شده است [۱۴]. این رویکردها به شناسایی زودهنگام و پیشگیری از بروز خسارات جدی کمک می‌کنند. همچنین، افزایش آگاهی تولیدکنندگان و به‌کارگیری استانداردهای کنترل کیفیت سخت‌افزاری می‌تواند در کاهش خطرات ناشی از این تروجان‌ها موثر باشد.

اجزای تشکیل‌دهنده تروجان‌های سخت‌افزاری

تروجان‌های سخت‌افزاری به عنوان یکی از تهدیدهای مهم امنیتی در حوزه سخت‌افزار، شامل بخش‌ها و اجزای مختلفی هستند که هر یک در ایجاد، فعال‌سازی و اثرگذاری این نوع بدافزار نقش دارند. به طور کلی، این بخش‌ها را می‌توان به سه گروه اصلی ذیل تقسیم کرد:

الف) بخش محرک یا فعال‌ساز[۶]

ب) بخش بار یا موثر[۷]

ج) بخش منطقی[۸]

۱. بخش محرک یا فعال‌ساز در تروجان‌های سخت‌افزاری

بخش محرک مسئول فعال‌سازی تروجان‌های سخت‌افزاری است و معمولاً به‌گونه‌ای طراحی می‌شود که در شرایط خاص و غیرمعمول فعال گردد تا احتمال کشف آن در مراحل آزمون و اعتبارسنجی به حداقل برسد. محرک‌ها می‌توانند بر اساس رویدادهای نادر، شمارنده‌های خاص، الگوهای ورودی یا حتی ترکیبی از این موارد طراحی شوند. این ویژگی باعث می‌شود که تروجان در شرایط عادی خاموش و غیرقابل تشخیص باقی بماند.

یکی از روش‌های متداول در طراحی محرک، استفاده از شمارنده‌های داخلی است که تنها پس از گذشت تعداد زیادی چرخه کلاک، تروجان را فعال می‌کنند. به این ترتیب، در آزمایش‌های کوتاه‌مدت سخت‌افزاری، تروجان فعال نمی‌شود و شناسایی آن بسیار دشوار خواهد بود [۱۵].

نوع دیگر محرک‌ها بر اساس الگوهای خاص ورودی عمل می‌کنند. در این روش، تروجان تنها زمانی فعال می‌شود که ترکیب خاصی از بیت‌های ورودی به مدار اعمال شود. این شیوه به مهاجم اجازه می‌دهد که فعال‌سازی را در شرایطی کنترل‌شده انجام دهد و در عین حال از شناسایی تصادفی آن جلوگیری کند [۳].

۲. بخش بار یا موثر در تروجان‌های سخت‌افزاری

بخش بار یا مؤثر، وظیفه انجام عملیات مخرب را بر عهده دارد. این بخش پس از فعال شدن محرک، عملکرد عادی سامانه را تغییر می‌دهد یا داده‌های حساسی را افشا می‌کند. بار می‌تواند در سطوح مختلفی اعم از تغییر در خروجی‌ها، ایجاد تأخیر در پردازش، افشای کلیدهای رمزنگاری یا حتی تخریب فیزیکی بخشی از مدار عمل کند [۱۶].

یکی از شایع‌ترین حملات بار، نشت اطلاعات[۹] است. در این حالت، تروجان داده‌های حساس مانند

کلید رمزنگاری را از طریق کانال‌های جانبی[10] نظیر توان مصرفی یا سیگنال‌های الکترومغناطیسی منتقل می‌کند. این نوع بار به‌ویژه در تراشه‌های رمزنگاری اهمیت زیادی دارد، زیرا می‌تواند امنیت کل سامانه را به خطر بیندازد [۳].
همچنین بار می‌تواند به شکل ایجاد اختلال در عملکرد[11] عمل کند. به عنوان مثال، در تراشه‌های پردازشی، تروجان می‌تواند با تزریق خطا یا ایجاد تأخیرهای عمدی، کارایی سیستم را مختل کند. این نوع حمله در سامانه‌های حیاتی مانند تجهیزات نظامی یا هوافضا می‌تواند خسارات جبران‌ناپذیری ایجاد کند [۱۷].

۳. بخش منطقی یا ساختاری در تروجان‌های سخت‌افزاری

بخش منطقی شامل سازوکار پیاده‌سازی تروجان در طراحی سخت‌افزار است. این بخش تعیین می‌کند که تروجان در کدام سطوح از چرخه طراحی شامل لایه فیزیکی[12]، سطح گیت[13]، سطح انتقال ثبات[14] یا حتی مرحله ساخت وارد سامانه می‌شود [۱۸]. انتخاب سطح درج تروجان بر میزان پنهان‌کاری، پیچیدگی و قابلیت شناسایی آن تأثیر مستقیم دارد.
در سطح انتقال ثبات، تروجان‌ها معمولا به صورت ماژول‌های کوچک و پنهان وارد کد طراحی می‌شوند. این روش ساده‌تر است اما احتمال کشف آن توسط تحلیل کد منبع بالاتر است. در سطح گیت، تروجان‌ها با افزودن یا تغییر گیت‌ها پیاده‌سازی می‌شوند و تشخیص آنها دشوارتر است [۳].
در سطح فیزیکی، تروجان می‌تواند از طریق تغییرات جزئی در مسیرهای سیم‌کشی یا تغییر ابعاد ترانزیستورها اضافه شود. این روش بسیار پنهان‌کارانه است و تنها با ابزارهای بسیار پیشرفته مانند میکروسکوپ الکترونی عبوری[15] با مقایسه تصویر لایه‌ای قابل کشف است [۴].

روش‌های فعال‌سازی تروجان‌های سخت‌افزاری

تروجان‌ها به عنوان یکی از انواع بدافزارها، به صورت مخفیانه و با اهداف مخرب وارد سامانه‌های کامپیوتری می‌شوند. روش‌های فعال‌سازی تروجان‌ها به شکل‌های مختلفی صورت می‌پذیرد که بسته به نوع تروجان و هدف مهاجم می‌تواند متفاوت باشد. در ادامه، سه روش اصلی فعال‌سازی تروجان‌ها شرح داده می‌شود.

الف) فعال‌سازی تروجان از طریق اجرای مستقیم فایل مخرب توسط کاربر
ب) فعال‌سازی تروجان از طریق بهره‌برداری از آسیب‌پذیری‌های نرم‌افزاری
ج) فعال‌سازی تروجان از طریق اسکریپت‌هایا برنامه‌های زمان‌بندی‌شده

۱. فعال‌سازی تروجان از طریق اجرای مستقیم فایل مخرب توسط کاربر

تروجان‌ها یکی از مهم‌ترین تهدیدات در حوزه بدافزارها هستند که با روش‌های مختلف فعال می‌شوند. یکی از ساده‌ترین و در عین حال رایج‌ترین روش‌های فعال‌سازی آن‌ها، اجرای مستقیم فایل مخرب توسط کاربر است. در این حالت، مهاجم فایل آلوده را در قالب یک نرم‌افزار یا مستند عادی (مانند فایل نصبی، فایل PDF یا حتی یک بازی کوچک) به کاربر ارائه می‌دهد. هنگامی‌که کاربر به صورت دستی فایل را اجرا می‌کند، کد مخرب موجود در آن فعال شده و فرایند آلوده‌سازی آغاز می‌شود. این روش به شدت بر فریب مهندسی اجتماعی متکی است، زیرا مهاجم باید کاربر را قانع کند که فایل موردنظر بی‌خطر یا حتی مفید است [۱۹].
مهاجمان برای افزایش احتمال اجرای دستی فایل‌های مخرب، معمولاً از تکنیک‌های متنوعی بهره می‌گیرند. برای مثال، آن‌ها ممکن است فایل تروجان را در قالب ضمیمه ایمیل‌های فیشینگ، لینک‌های جعلی در شبکه‌های اجتماعی یا بسته‌های نرم‌افزاری کرک شده منتشر کنند. بسیاری از کاربران به دلیل کنجکاوی یا نیاز به دسترسی به نرم‌افزارهای رایگان، این فایل‌ها را بدون بررسی امنیتی اجرا می‌کنند. پس از اجرا، تروجان می‌تواند به نصب بک‌دور، سرقت اطلاعات یا حتی دانلود بدافزارهای دیگر اقدام کند [۲۰].
علاوه بر این، برخی تروجان‌ها از نام‌ها و آیکون‌های جعلی برای فریب کاربر استفاده می‌کنند؛ مثلا ممکن است یک فایل مخرب با نامی شبیه به "setup.exe" یا "document.pdf.exe" ارائه شود تا کاربر تصور کند با یک فایل سالم مواجه است. به محض اجرای فایل، بدافزار در سامانه مستقر می‌شود و اغلب به صورت پنهانی در حافظه یا رجیستری باقی می‌ماند تا در دفعات بعد نیز فعال گردد. بنابراین، آگاهی کاربران از این روش ساده اما خطرناک فعال‌سازی، اهمیت زیادی در پیشگیری دارد [۲۱].

۲. فعال‌سازی تروجان از طریق بهره‌برداری از آسیب‌پذیری‌های نرم‌افزاری

یکی از روش‌های پیشرفته و خطرناک فعال‌سازی تروجان‌ها، بهره‌برداری از آسیب‌پذیری‌های نرم‌افزاری است. در این روش، برخلاف اجرای دستی توسط کاربر، مهاجم از حفره‌های امنیتی موجود در سیستم‌عامل یا نرم‌افزارهای کاربردی سوءاستفاده می‌کند تا کد مخرب را به صورت خودکار اجرا کند. این آسیب‌پذیری‌ها معمولاً ناشی از نقص در مدیریت حافظه، اعتبارسنجی ورودی‌ها یا ضعف در ماژول‌های امنیتی نرم‌افزار هستند. به‌عنوان مثال، آسیب‌پذیری‌های نوع سرریز بافر[16] یا اجرای کد از راه دور[17] به مهاجم اجازه می‌دهند که بدون نیاز به دخالت کاربر، کد تروجان را در سامانه قربانی فعال کند [۱۹].
یکی از شناخته‌شده‌ترین نمونه‌های سوءاستفاده از آسیب‌پذیری برای فعال‌سازی خودکار بدافزارها، سوءاستفاده از حفره امنیتی در پروتکل SMB ویندوز بود که منجر به شیوع بدافزارهایی مانند WannaCry شد. این باج‌افزار با استفاده از اکسپلویت معروف EternalBlue بدون نیاز به اجرای مستقیم توسط کاربر، در سامانه‌ها فعال شد و به سرعت در سطح جهانی گسترش یافت. همین مکانیزم در بسیاری از تروجان‌ها نیز به کار می‌رود؛ یعنی کد مخرب پس از بهره‌برداری از یک آسیب‌پذیری، روی سامانه هدف اجرا و به‌طور خودکار در شبکه پخش می‌شود [۲۰].
از آنجا که کاربران معمولاً متوجه فرایند بهره‌برداری نمی‌شوند، شناسایی این نوع حملات دشوارتر از روش‌های سنتی است. مهاجمان با استفاده از کیت‌های اکسپلویت[18] یا حتی صفحات وب آلوده، می‌توانند سامانه‌های دارای نرم‌افزارهای به‌روز نشده را هدف قرار

دهند و تروجان‌ها را فعال کنند. به همین دلیل، به‌روزرسانی منظم سیستم‌عامل و نرم‌افزارها، نصب وصله‌های امنیتی و استفاده از ابزارهای شناسایی نفوذ از مهم‌ترین راهکارهای پیشگیری در برابر این نوع تهدیدها محسوب می‌شود [۲۱].

۳. فعال‌سازی تروجان از طریق اسکریپت‌ها یا برنامه‌های زمان‌بندی‌شده

یکی دیگر از روش‌های رایج فعال‌سازی تروجان‌ها، استفاده از اسکریپت‌ها یا برنامه‌های زمان‌بندی‌شده در سیستم عامل است. مهاجمان پس از نصب تروجان، معمولاً یک اسکریپت مخرب را در سامانه قربانی قرار می‌دهند که به طور خودکار و طبق زمان‌بندی مشخص اجرا می‌شود. در سیستم‌های ویندوز، این کار اغلب از طریق Task Scheduler انجام می‌شود و در سیستم‌های مبتنی بر یونیکس/لینوکس از Cron jobs استفاده می‌شود. این روش به بدافزار اجازه می‌دهد که حتی پس از راه‌اندازی مجدد سامانه نیز فعال باقی بماند و مجدداً اجرا شود [۱۹].

اسکریپت‌ها علاوه بر اجرای خودکار تروجان، می‌توانند وظایف دیگری همچون برقراری ارتباط با سرور فرمان و کنترل[19]، دانلود نسخه‌های جدید بدافزار یا جمع‌آوری اطلاعات سیستم را نیز انجام دهند. به عنوان مثال، برخی تروجان‌های بانکی از اسکریپت‌های زمان‌بندی‌شده برای به‌روزرسانی خود و حفظ ماندگاری در سامانه قربانی استفاده کرده‌اند. این اسکریپت‌ها به گونه‌ای طراحی می‌شوند که در پس‌زمینه و به شکل مخفیانه عمل کنند و کاربر هیچ‌گونه اخطار یا نشانه‌ای از فعالیت آن‌ها مشاهده نکند [۲۰].

افزون بر این، مهاجمان برای مخفی‌سازی بهتر فعالیت‌های خود، گاهی نام اسکریپت‌ها یا وظایف زمان‌بندی‌شده را مشابه فرایندهای عادی سامانه انتخاب می‌کنند تا در صورت بررسی سطحی توسط کاربر یا مدیر سامانه، مورد توجه قرار نگیرد. چنین رویکردی باعث می‌شود که تروجان بتواند در بلندمدت بدون شناسایی اجرا شود. به همین دلیل، بررسی مداوم وظایف زمان‌بندی‌شده، استفاده از آنتی‌ویروس‌های به‌روز و پایش رفتار سامانه از مهم‌ترین اقدامات دفاعی در برابر این روش فعال‌سازی محسوب می‌شود [۲۱].

جمع‌بندی و نتیجه‌گیری

تروجان‌های سخت‌افزاری به‌عنوان یکی از پیچیده‌ترین و خطرناک‌ترین تهدیدات در حوزه امنیت سایبری، به‌ویژه در سامانه‌های نظارت تصویری، اهمیت ویژه‌ای دارند. این تهدیدات به دلیل ماهیت پنهان‌کارانه، قابلیت فعال‌سازی تحت شرایط خاص و دشواری شناسایی در مراحل طراحی و تولید می‌توانند پیامدهای جدی برای امنیت زیرساخت‌های حیاتی به همراه داشته باشند. همان‌گونه که در این مقاله نشان داده شد، تروجان‌ها با اهداف مختلفی از جمله ایجاد اختلال در عملکرد، سرقت اطلاعات، تخریب مستقیم و یا کاهش تدریجی قابلیت اطمینان سامانه، طراحی و پیاده‌سازی می‌شوند. با توجه به تحلیل اجزای تشکیل‌دهنده تروجان‌ها شامل بخش محرک، بار و منطق ساختاری می‌توان نتیجه گرفت که هر یک از این اجزا نقش مهمی در افزایش پنهان‌کاری و کارایی حملات دارند. علاوه بر این، روش‌های فعال‌سازی مختلف از جمله اجرای مستقیم فایل‌ها توسط کاربر، سوءاستفاده از آسیب‌پذیری‌های نرم‌افزاری و بهره‌گیری از اسکریپت‌ها یا برنامه‌های زمان‌بندی‌شده بیانگر تنوع راهکارهای مهاجمان برای استقرار این تهدیدات است.

با توجه به این واقعیت که سامانه‌های نظارت تصویری در مراکز حساس و حیاتی مورد استفاده قرار می‌گیرند، پیامدهای ناشی از تروجان‌های سخت‌افزاری می‌تواند امنیت ملی، حریم خصوصی شهروندان و پایداری خدمات حیاتی را تحت تأثیر قرار دهد.

بنابراین، ضرورت دارد که راهبردهای پیشگیرانه از جمله استفاده از زنجیره تأمین قابل اعتماد، به‌کارگیری آزمون‌ها و تحلیل‌های پیشرفته سخت‌افزاری، نظارت مستمر بر رفتار سامانه و بهره‌گیری از فناوری‌های نوین مانند یادگیری ماشین در شناسایی ناهنجاری‌ها مورد توجه ویژه قرار گیرد. در نهایت، می‌توان نتیجه گرفت که مقابله با تروجان‌های سخت‌افزاری در سامانه‌های نظارت تصویری تنها با رویکردی چندلایه، شامل جنبه‌های فنی، مدیریتی و راهبردی امکان‌پذیر است. این موضوع نیازمند همکاری گسترده میان محققان، تولیدکنندگان، نهادهای امنیتی و سیاست‌گذاران است تا بتوان با ایجاد چارچوب‌های استاندارد و راهکارهای عملی، از تهدیدات پیچیده در این حوزه پیشگیری و مقابله کرد.

1. Hardware Trojans
2. Functional Trojans
3. Information Leakage Trojans
4. Destructive Trojans
5. Reliability Reduction Trojans
6. Trigger Part
7. Payload / Malicious Effect Part
8. Insertion / Logic Part
9. Information Leakage
10. Side Channels
11. Denial of Service (DoS)
12. Layout level
13. Gate level
14. Register Transfer Level (RTL)
15. Transmission Electron Microscope (TEM)
16. Buffer overflow
17. Remote Code Execution (RCE)
18. Exploite Kits
19. Command and Control Server

منابع

[1] M. Tehranipoor, F. Koushanfar, "A survey of hardware Trojan taxonomy and detection", IEEE Design & Test of Computers, 25-10 ,(1)27 ,2010.

[2] S. Bhunia, M. Tehranipoor, "Hardware Security: A Hands-on Learning Approach. Morgan Kaufmann", 2018.

[3] D. Forte, S. Bhunia, M. Tehranipoor, "Hardware Trojan attacks: Threat analysis and countermeasures", 2017. Proceedings of the IEEE, -1930 ,(10)105 1952.

[4] A. Waksman, S. Sethumadhavan, "Silencing hardware backdoors", IEEE Symposium on Security and Privacy, 2011.

[5] F. Koushanfar, M. Potkonjak, "Hardware trojan detection and prevention: Challenges and solutions", IEEE Design & Test of Computers, 19-10 ,(1)27 ,2010.

[6] J. Rajendran, R. Pino, S. Chatterjee, S. Kim, R. Karri, "Design and analysis of ring oscillator based tunable sensors for hardware Trojan detection", IEEE Transactions on Information Forensics and Security, 1426-1415 ,(7)11 ,2016.

[7] Y. Zhang, M. Tehranipoor, D. Forte, "Hardware trojan detection: A survey",

2019, IEEE Design & Test, 24-8 ,(3)36.
[8] A. Alrawashdeh, C. Purdy, "An enhanced malware detection approach using machine learning", Proceedings of the 7th International Conference on Cyber Warfare and Security, -312 ,2013 319.
[9] M. Farooq, M. Aamir, "Malware detection techniques and research challenges: A review", International Journal of Advanced Computer Science and Applications, 9-1 ,(6)11 ,2020.
[10] Y. Xiao, Z. Han, J. Xie, "Hardware Trojan attacks: A survey and taxonomy", IEEE Access, 141743-141730 ,7 ,2019.
[11] J. Gao, Y. Yang, W. Shi, W, "Detection and mitigation of destructive hardware Trojans in integrated circuits", IEEE Transactions on Information Forensics and Security, ,(11)12 ,2017 2639-2626.
[12] L. Wang, J. Zhang, H. Li, "Machine learning-based detection of hardware Trojans: Current challenges and future directions", Journal of Hardware and Systems Security, 135-123 ,(2)5 ,2021.
[13] J. Wang, H. Zhang, Y. Li, "Detection of reliability degradation hardware Trojans using aging analysis" IEEE Transactions on Very Large-Scale Integration (VLSI) Systems, ,(4)26 ,2018 774-763.
[14] H. Salmani, M. B. Tahoori, F. Koushanfar, "Hardware Trojan detection using machine learning: Challenges and opportunities" IEEE Transactions on Information Forensics and Security, 102-88 ,15 ,2020.
[15] J. Zhang, M. Tehranipoor, "Case study: Detecting hardware Trojans", in third-party digital IP cores. IEEE HOST, 2011.
[16] R. Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, "Trustworthy hardware: Identifying and classifying hardware Trojans. Springer, 2010.
[17] X. Lyu, P. Mishra, "Scalable activation of rare triggers in hardware Trojans", IEEE VLSI Test Symposium, 2012.
[18] M. Tehranipoor, C. Wang, "Introduction to hardware security and trust", Springer, 2012.
[19] W. Stallings, "Computer Security: Principles and Practice", 4th ed. Pearson, 2020.
[20] Symantec, "Internet Security Threat Report", vol 27, Symantec Corporation, 2022.
[21] Kaspersky Lab, "Trojan Malware Definition", 2021. [Online], Available: https://www.kaspersky.com.

تحلیل تخصصی استانداردهای IEC62676 و چرایی عدم کارایی در امنیت سایبری سامانه‌های نظارت تصویری

نویسنده: محمدقلم‌چی

متخصصان نظارت تصویری که علم کافی در حوزهٔ ویدئو دیجیتال و همچنین تجربه و تسلط کافی را در تمامی اجزای نظارت تصویری داشته باشند، در سطح جهانی کمیابند. از سوی دیگر، متخصصان امنیت سایبری نیز هریک تخصص ویژهٔ خود را دارند و به ندرت دانش و تجربه در حوزه داده‌های عظیم ویدئویی دارند. خانوادهٔ IEC62676 (معروف به EN/IEC 62676 در برخی کشورها) مجموعه‌ای از استانداردهای بین‌المللی برای «سامانه‌های نظارت تصویری برای کاربردهای امنیتی» است که عمدتاً روی سازگاری، مشخصات رابط‌ها، مشخصات داده/کیفیت تصویر و راهنمای کاربرد تمرکز دارد. به‌رغم ارزشِ فنی این مجموعه استاندارد در تضمین عملکردِ تصویری و بین‌عملکردپذیری، در متن و حوزهٔ کاربردِ بخش‌های

اصلی آن الزاماتِ امنیت سایبری (مثل مدیریت هویت دستگاه، رمزنگاری، به‌روزرسانی امن، مدیریت آسیب‌پذیری، زنجیرهٔ تامین نرم‌افزاری، پاسخ به حادثه و غیره) به‌صورت جامع یا تکمیلی مطرح نشده‌اند؛ یا صراحتاً از محدوده خارج شده‌اند. در این مقاله ابتدا هر یک از پنج بخشِ اصلی این استانداردها را خلاصه می‌کنیم، سپس نشان می‌دهیم چرا اجرای صرفِ IEC62676 اسکلتِ «امنیت سایبری» را تضمین نمی‌کند و در نهایت دلایل و چارچوب پیشنهادی برای تدوین یک استاندارد تخصصی سایبری برای سامانه‌های نظارت تصویری را ارائه می‌دهیم. منابع رسمی و راهنمایی‌های ملی/اروپایی که جایگزین یا مکملِ الزامات سایبری اند نیز مرور می‌شوند [۱][۲].

مروری بر فهرست کوتاهِ بخش‌های مربوط

الف) Part 1

System requirements

حداقل عملکردیِ سیستم، بلوک‌های عملکردی و نیازمندی‌های عملکردی و مدیریتی را تعریف می‌کند؛ اما طراحی، نصب، عملیات یا جنبه‌های کامل نگهداری را در گسترهٔ خود قرار نمی‌دهد.

ب) Part 2

Video transmission protocols

سازوکارهای انتقال و پروفایل‌های بین‌عملکردپذیری شبکه‌ای و پیاده‌سازی‌های مبتنی بر HTTP/ REST/Web services و پروفایل‌های VMS/VSaaS را شرح می‌دهد.

پ) Part 3

Analog & digital video interfaces

مشخصات فیزیکی، الکتریکی و پروتکل‌های رابطِ ویدئویی را تعریف می‌کند.

ت) Part 4

Application guidelines

راهنمایی‌های طراحی، انتخاب، نصب، راه‌اندازی و تست سیستم را ارائه می‌دهد (نسخهٔ جدید در سال ۲۰۲۵ به‌روزرسانی و منتشر شده است).

ث) Part 5

Data specifications & image quality

متدولوژی‌ها و معیارهای اندازه‌گیری کیفیت تصویر و مشخصات دادهٔ دوربین‌ها (و زیربخش‌های محیطی برای تست) را تعریف می‌کند.

نکتهٔ کلیدی:

مجموعه IEC62676 روی «عملکرد تصویری» و «بین‌عملکردپذیری[۱]» متمرکز است و در چند مورد صراحتاً برخی حوزه‌ها مثل «قابلیت در دسترس بودن سیستم، حریم خصوصی، محدودیت‌های قانونی یا امنیت سایبری» را خارج از محدوده اعلام کرده یا در سطحی کلی به آن اشاره کرده است[۳].

چرا اجرای IEC62676 به‌تنهایی امنیت سایبری را تأمین نمی‌کند؟

در ادامه، دلایلِ فنی و ساختاری که نشان می‌دهد چرا استاندارد ۶۲۶۷۶ به‌تنهایی برای امنیت سایبری کافی نیست، همراه با سند مرجع و استدلال ارائه شده است.

تعریف حوزه و «خارج بودنِ» صریحِ سایبری از دامنهٔ بسیاری از بخش‌ها

متن برخی بخش‌ها به‌وضوح اعلام می‌کند که نیازمندی‌های امنیت سایبری، حریم خصوصی و برخی الزامات عملیاتی خارج از حوزهٔ این بخش‌ها است یا «جزئیات دقیق» آنها پوشش داده نمی‌شود. بنابراین سیستم‌هایی که فقط از این استانداردها پیروی کنند ممکن است فاقد الزامات حیاتیِ امنیتی باشند.

تمرکز بر عملکرد و بین‌عملکردپذیری، نه بر قواعدِ محافظتی قابل اندازه‌گیری

۶۲۶۷۶ در درجهٔ اول پارامترهای عملکردی (مثلاً نرخ فریم، کیفیت تصویر، تاخیر، پروتکل‌های تبادل) و توصیف رابط‌ها را مشخص می‌کند. اما امنیت سایبری نیازمند الزامات عملیاتی و فنی قابل‌ارزیابی (مثلاً قوی‌بودن الگوریتم‌های رمزنگاری، مکانیزم احراز هویت، مدیریت کلیدها، روش‌های به‌روزرسانی امن و مقابله با حملات تزریق) است که در این استانداردها به‌صورت «نیازمندی‌های فنی امنیتی» قابل تست و سنجش تعریف نشده‌اند.

(مقایسه: استانداردهای سایبری معمولاً مجموعه‌ای از کنترل‌های فنی، فرایندی و مدیریتی قابل آزمون ارائه می‌دهند؛ در صورتیکه ۶۲۶۷۶ عمدتاً معیارهای عملکردی تصویری ارائه می‌دهد).

نبود الزامات توسعهٔ امن (Secure SDLC) و مدیریت آسیب‌پذیری

امنیت یک دوربین یا سامانه نظارت تصویری از مرحلهٔ طراحی نرم‌افزار/فریم‌ور تا انتشار و به‌روزرسانی و پاسخ به آسیب‌پذیری پیوستگی لازم را می‌طلبد (مثلاً امضای فریم‌ور، سیاست به‌روزرسانی، برنامهٔ افشای آسیب‌پذیری و مدیریت وصله). متن‌های IEC62676 این حلقهٔ حیاتی را به‌صورت قاعده‌مند پوشش نمی‌دهند. بنابراین حتی اگر دستگاه مطابق ۶۲۶۷۶ از منظر کیفیت تصویر یا APIها باشد، ممکن است با یک آسیب‌پذیری ساده مثل حساب پیش‌فرض یا به‌روزرسانی‌نشده، به یک بردهٔ باتنت یا دروازهٔ نفوذ تبدیل شود. (مفاهیم مشابه و توصیه‌های عملی را نهادهای سایبری ملی پیشنهاد داده‌اند).

فقدان الزامات رمزنگاری/ کنترل دسترسی در سطوح تجویزی

۶۲۶۷۶ پروتکل‌ها و فرمت‌ها را شرح می‌دهد اما الزام قاطع به استفاده از پروتکل‌های رمزنگاری معتبر (مثلاً TLS با مدیریت صحیح نسخه/ سازگاری/پروفایل) یا الزامات سخت‌گیرانهٔ کنترل دسترسی و مدیریت کلیدها را که برای حفاظت از ویدئو در انتقال و ذخیره‌سازی لازم است را در بسیاری موارد ارائه نمی‌کند و در موارد بسیار کمی که ارائه شده، در سطحی عمومی است که برای پیاده‌سازی مقاوم کافی نیست. اسناد ملی/ آژانس‌ها مانند ANSSI یا NCSC توصیه‌های دقیق‌تری برای تنظیم TLS، مدیریت رمزها و بخش‌بندی شبکه دارند [۴].

عدم پوشش خطرات زنجیرهٔ تامین و سخت‌افزار/فرم‌ور تأمین‌شده

دوربین‌ها و سیستم‌های VMS ترکیبی از اجزای سخت‌افزاری، کتابخانه‌های متن‌باز، فرم‌ورهای تولیدکنندگان متعدد و سرویس‌های ابری‌اند؛ ریسک‌های زنجیرهٔ تأمین نیاز به الزامات کنترل شده و قابل‌تفکیک دارد (SBOM، بررسی امضای باینری، مدیریت وابستگی‌ها) _ در ۶۲۶۷۶ این موارد به‌عنوان الزام عملیاتی استاندارد بیان نشده‌اند. استانداردهای سایبری جدید (مثلا645 EN303 و راهنمای آن) روی این موضوعات تمرکز کرده یا الزامات پایه‌ای ارائه داده‌اند اما آنها هم برای حوزهٔ نظارت تصویری به‌لحاظ ویژگی‌محور (مثلا سازوکارهای chain-of-evidence کفایت نمی‌کنند [۵].

جنبه‌های قانونی، حریم خصوصی و شواهد قانونی (chain of custody)

۶۲۶۷۶ در بخش‌هایی راهنمایی کاربردی برای ضبط و کیفیت تصویر می‌دهد اما موضوعاتی مانند محافظت از حریم خصوصی، دورهٔ نگهداری حداقلی/حداکثری ویدئو، ثبت دسترسی‌ها (audit trail) با ضمانت عدم تغییر (tamper-evident logging) و فرایندهای ادلهٔ قضایی را به‌صورت الزامی سایبری ـ حقوقی پوشش نمی‌دهد؛ در حالی که بسیاری از ریسک‌های واقعی سامانه‌ها از این خلاها ناشی می‌شود و برای اعتماد عمومی و پذیرش قانونی ضروری است. نهادهای حفاظت از داده کشورها (مثلا CNIL، ICO، EDPS) راهنمایی‌هایی دربارهٔ حقوق دادهها ارائه کرده‌اند اما جای یک استانداردِ فنیِ سایبری–حقوقی تخصصی خالی است [۶].

وضعیت بین‌المللی، کشورهایی که استاندارد یا دستورالعمل ویژهٔ امنیت سایبری سامانه‌های نظارت تصویری صادر کرده‌اند

در قرن جدید، نفوذ به سامانه‌های نظارت تصویری و یا نفوذ از طریق سامانه‌های نظارت تصویری و همچنین جعل عمیق ویدئوی دیجیتال فجایع متعددی در سراسر جهان به بارآورد و بزرگترین نفوذ سایبری جهان که موجب قطعی نیمی از اینترنت جهانی شد، از طریق سامانه‌های نظارت تصویری صورت گرفت. این مهم تا آنجا پیش رفت که سه سازمان جهانی مرتبط با استاندارد از جمله سازمان جهانی استاندارد (ISO)، نام سال ۲۰۱۹ را «استانداردهای ویدئویی، سازنده صحنه جهانی» نامگذاری نمود. به همین دلیل اکثر کشورهای جهان در حال تدوین استانداردهای امنیت سایبری ویژهٔ سامانه‌های نظارت تصویری هستند. در ایران در همین سال، موسسهٔ دانش‌بنیان خدمات مدیریت و فناوری رشد قلم‌چی، پیشنهاد تالیف استاندارد امنیت (سایبری) سامانه‌های نظارت تصویری را به سازمان فناوری اطلاعات ارایه داد.

سازمان فناوری اطلاعات ایران در سال ۱۴۰۰ نسبت به تالیف این استاندارد اقدام و به سازمان ملی استاندارد پیشنهاد داد که مورد تصویب قرار گرفت، لکن در روند تصویب دچار کارشکنی‌هایی شد که امید است دستور معاون اول ریاست جمهوری اسلامی ایران موجب تسریع در تصویب این استاندارد گردد.

کشورهایی که هم اکنون استاندارد مصوب امنیت سایبری دارند

کشورهای تایوان و ویتنام برای حوزهٔ امنیت سایبری سامانه نظارت تصویری، استاندارد ملی مصوب دارند، لکن با مشاهده متن آن متوجه می‌شویم این استانداردها بیشتر فهرستی از نیازها هستند که قرار است در شماره‌های بعدی تکمیل گردند.

تایوان

استاندارد ملی تحت عنوان «TAICS TS-0014 Video Surveillance System Cybersecurity Standard – Part 1» و «Part2» برای سامانه‌های نظارت تصویری (دوربین‌های IP، NVR/DVR، ذخیره‌سازی شبکه) توسط Taiwan Association of Information and Communication Standards(TAICS) تدوین و منتشر شده است.

ویتنام

مقررات ملی «QCVN 135:2024/BTTTT – National Technical Regulation on Surveillance Cameras Using Internet Protocol (Basic Cybersecurity Requirements)» توسط وزارت اطلاعات و ارتباطات این کشور تصویب شده، که الزام می‌کند از تاریخ مشخصی همهٔ دوربین‌های تحت شبکه وارداتی یا تولید داخلی مطابق الزام‌های امنیت سایبری باشند.

کشورهایی که هنوز استاندارد مصوب نکرده‌اند، اما دستورالعمل‌هایی در این حوزه دارند

در بسیاری از کشورها هنوز استاندارد ملی مصوب نشده و به‌جای یک «استاندارد فنی تخصصیِ سایبری برای سامانه‌های نظارت تصویری» ترکیبی از اقدامات زیر وجود دارد: راهنمایی‌های دولتی، دستورالعمل‌های حفاظت از داده، مقررات محصول (قوانین IoT)، و استانداردهای عمومیِ سایبری یا IoT که به سیستم‌های نظارتی قابل تعمیم‌اند. کشورها و سازمان‌های متولی شاخص در آن‌ها به شرح ذیل است:

انگلستان (NCSC/ Home Office/ ICO/ NPSA)

مرکز ملی امنیت سایبری (NCSC) مستنداتی با عنوان راهنمایی‌هایی برای «دوربین‌های هوشمند» و مدیریت داده‌های ویدئویی منتشر کرده است. همچنین «Surveillance Camera Code of Practice» و اسناد حاکمیتی در انگلستان (GOV.UK) برای مدیریت و امنیت داده وجود دارد که ترکیبِ راهکار فنی و حریم خصوصی (راهنمایی‌های عملی برای پیکربندی امن، مدیریت دسترسی، ثبت رخداد و غیره) را توصیه می‌کند.

فرانسه (ANSSI و CNIL)

آژانس ملی امنیت سیستم‌های اطلاعاتی (ANSSI) راهنمایی‌ها و توصیه‌های فنی [۷] برای امن‌سازی سیستم‌های کنترل دسترسی و ویدئو منتشر کرده و CNIL نیز روی مسائل حریم خصوصی و قوانین ویدئوکاربری تمرکز دارد. این اسناد شامل توصیه‌هایی برای رمزنگاری TLS، مدیریت آسیب‌پذیری و الزامات دسترسی است.

آلمان (BSI) [۸]

آلمان رهنمودها و برچسب (IT Security Label) و توصیه‌هایی دربارهٔ دوربین‌ها و دستگاه‌های IoT دارد. شایان ذکر است BSI و مجامع آلمانی معمولا تحلیل‌های فنی و توصیه‌های سخت‌گیرانه ارائه می‌دهند.

استرالیا (ACSC / ASD)

مرکز سایبری استرالیا (ACSC / ASD) راهنمایی‌های عملی برای استقرار امنِ سامانه‌ها [۹] (شامل سامانه‌های نظارتی) تالیف، تصویب و منتشر نموده است؛ همچنین آموزش‌ها و چارچوب‌های Security-by-Design برای سازندگان دستگاه‌های IoT در این کشور وجود دارد که مناسبِ اعمال روی دوربین‌ها نیز هست و تا حدی امنیت سایبری سامانه‌های نظارت تصویری را تامین می‌نماید.

ایالات متحده (NIST / CISA)

موسسهٔ ملی استاندارد و تکنولوژی آمریکا (NIST) و همچنین قوانین در برخی ایالت‌های امریکا (به عنوان نمونه California SB-327) توصیه‌هایی در حوزه پردازش ویدئو و اخذ خروجی[۲] تالیف، مصوب و منتشر کرده‌اند. همچنین CISA[۳] هشدارها و راهنماهایی در حوزه امنیت سایبری نظارت تصویری منتشر نموده است. در سطح قانون‌گذاری، ایالت‌ها (مثلا کالیفرنیا) قوانینی برای «امنیت دستگاه‌های متصل» وضع کرده‌اند که شامل دوربین‌ها نیز می‌شود.

اروپا (ETSI / ENSIA)

ETSI[۴] دستورالعمل‌های EDPS[۶] / GDPR و همچنین استاندارد EN303 645 (یک استاندارد پایه برای امنیت دستگاه‌های مبتنی بر فناوری IoT) منتشر کرده که اصول پایه‌ای امنیت سایبری مانند «بدون رمز پیش‌فرض»، «سیاست افشای آسیب‌پذیری» و «به‌روزرسانی نرم‌افزاری» را اجباری می‌کند؛ این استاندارد برای حوزهٔ نظارت تصویری پایهٔ خوبی است اما عمومیت آن در سامانه‌های نظارت تصویری، نیاز به درج ملاحظات تخصصی سامانه‌های نظارتی دارد. ENISA[۷] و EDPS نیز ملاحظات امنیت و حریم خصوصی را منتشر کرده‌اند.

جمع‌بندی

دو کشور تایوان و ویتنام بخشی از استاندارد امنیت سایبری سامانه‌های نظارت تصویری را تالیف و مصوب کرده‌اند، چند کشور راهنمایی‌های فنی و قانونی (و بعضاً الزامات محصول/برچسب) منتشر کرده‌اند، اما هنوز یک استاندارد بین‌المللیِ فنیِ واحد و تخصصی که الزاماتِ قابل‌سنجشِ سایبری مخصوص سامانه‌های نظارت تصویری (شامل حفظ زنجیرهٔ ادله، ثبت tamper-evident، ویژگی‌های فارنزیک و نیازمندی‌های SOC/VMS مخصوص) را تعریف کند، وجود ندارد.

نبود استانداردهای تخصصی امنیت سایبری نظارت تصویری ایران را دچار چه چالش‌هایی کرده است؟

عدم توجه به اهمیت امنیت سایبری در سامانه‌های نظارت تصویری در ایران موجب رخدادهای نگران کننده مهمی که بعضاً امنیت ملی را نشانه گرفته‌اند، شده است. از حادثه‌های لو رفتن تصاویر زندان‌ها گرفته تا نفوذ و از کارافتادن دوربین‌های نظارت تصویری شهرداری‌ها که در اخبار عمومی منعکس شده‌اند. شواهد متعددی وجود دارد که در جنگ ۱۲ روزه و ترورهای مختلف دیگر، حجم قابل توجهی از داده‌های تروریست‌ها از نفوذ به سامانه‌های نظارت تصویری بدست آمده است. عدم توجه به امنیت سایبری سامانه‌های نظارت تصویری، دوربین ها را تبدیل به ابزار جاسوسی دزدان، مهاجمین، خرابکاران و دشمن خواهد کرد.

۱. حملات و مشکلاتی که در IEC62676 پوشش داده نشده‌اند

در یک سامانه‌ای که صرفاً مطابق IEC62676 پیاده‌سازی شود (و الزامات امنیت سایبری در آن لحاظ نشود)، موارد و مشکلات زیر رخ می‌دهد:

۱-۱. حملات به هویت و دسترسی (بدون مدیریت هویت امن)

عدم مدیریت امن هویت موجب می‌شود مهاجم امکان استفاده از رمزهای پیش‌فرض کارخانه (Admin/Admin) را داشته باشد. عدم الزام سیاست‌های پیچیدگی و تغییر رمز، نفوذ مهاجم را تسهیل و تسریع می‌کند. عدم وجود احراز هویت چندعاملی و امکان دور زدن پنل‌های دسترسی با پروتکل‌های پشتیبان (RTSP) موجب می‌شود مهاجم بتواند به راحتی وارد

سامانه نظارت تصویری شود و کنترل سامانه را در دست گیرد.

۱-۲. شنود و سرقت تصویر (عدم الزام رمزنگاری TLS/RTSP/SRTP)

ویدئو اغلب بدون رمزنگاری منتقل می‌شود، لذا مهاجم روی شبکه به سادگی می‌تواند تصویر زنده را مشاهده کند، تصویر را ضبط و منتشر نماید و اطلاعات موقعیتی و حرکتی را استخراج کند. عدم رمزنگاری به مهاجم امکان نفوذ و خرابکاری از روش‌های مختلفی از جمله رهگیری حفاظتی، شناسایی عادات رفت‌وآمد و برنامه‌ریزی جرم هدفمند را می‌دهد.

۱-۳. حملات تغییر تصویر[8]

بدون مکانیزم‌های یکپارچگی[9]، مهاجم می‌تواند تصویر زنده را تاخیر دهد[10]، جایگزین کند[11] و یا ویرایش کند[12] لذا سامانهٔ نظارت تصویری ممکن است چیزی را نشان دهد که واقعی نیست.

۱-۴. تبدیل شدن دوربین‌ها به عضو بات‌نت[13]

فرم‌ورهای دوربین معمولاً بدون امضا، قدیمی و بدون مدیریت وصله امنیتی هستند. مخاطره آن وجود دارد که مهاجم از آسیب‌پذیری‌های شناخته‌شده استفاده کند و دوربین را در بات‌نت‌ها (مانند Mirai) عضو نماید. به بیان دیگر، این آسیب‌پذیری موجب می‌شود تجهیزات نظارت تصویری تبدیل به ابزار مهاجم در داخل شبکهٔ سازمان شوند. یکی از پیامدهای این مخاطره، حمله DDoS از همان شبکه امنیتی است که باید امن‌ترین شبکه سازمان باشد.

۱-۵. نفوذ از طریق دوربین به شبکه داخلی

چون تقسیم‌بندی شبکه[14] در استاندارد ۶۲۶۷۶ مطرح نشده، مهاجم از طریق دوربین‌های سازمان می‌تواند به سوئیچ دسترسی پیداکند، از سوئیچ به سرور دسترسی خواهد یافت و از آن طریق می‌تواند داده‌های سازمان را سرقت کند یا باج‌گیری (رنسوم‌ویر) نماید.

۱-۶. از بین رفتن ارزش قانونی ویدئو (عدم وجود Chain-of-Custody)

در استاندارد ۶۲۶۷۶ لاگ تغییرات، دسترسی‌ها و زمان‌بندی‌ها الزامی نیست، لاگ‌ها ضددستکاری نیستند و هش یا امضای دیجیتال ذخیره‌سازی تصویر تعریف نشده است. عدم توجه به این موارد در استاندارد فوق موجب می‌شود ویدئوی ضبط‌شده در مراجع رسمی همچون دادگاه قابل استناد نباشد. به بیان دیگر استاندارد فوق موجب نمی‌شود تصویری که توسط سامانه نظارت تصویری که الزامات IEC62676 را برآورده کرده است به عنوان سند در دادگاه مطرح شود و این داده ویدئویی قابل استناد نبوده، از نگاه قاضی در سطح شواهد و قرائن باقی خواهند ماند

۲. نمونه‌های واقعی نفوذ در نتیجه فقدان استاندارد امنیت سایبری نظارت تصویری

نمونه‌های واقعی نفوذ که مرتبط با عدم وجود استاندارد امنیت سایبری نظارت تصویری بوده‌اند در جدول ذیل آمده است.

1. Interoperability
2. Digital Video Export Profile
3. Cybersecurity and Infrastructure Security Agency
4. European Telecommunications Standards Institute
5. General Data Protection Regulation
6. European Data Protection Supervisor
7. The European Union Agency for Cybersecurity
8. Video Tampering
9. Integrity Protection
10. Delay Attack
11. Replay/Fake Feed
12. Deep Fake Injection
13. Botnet Infection
14. Segmentation

منابع

[1] International Electrotechnical Commission (IEC), IEC 1-1-62676: Video surveillance systems for use in security applications – Part 1-1: System requirements – General, IEC, Geneva, Switzerland, 2013.

[2] International Electrotechnical Commission (IEC), IEC 2-2-62676: Video surveillance systems for use in security applications – Part 2-2: Video transmission protocols, IEC, Geneva, Switzerland, 2012.

[3] Swedish Standards Institute (SIS), Larmsystem – System för videoövervakning (VSS) – Del 11-2: Protokoll för videoöverföring – Interoperabilitetsprofiler för VMS och VSaaS, SS-EN IEC 11-2-62676, ed. 1, Stockholm, Sweden, 2025.

[4] Agence nationale de la sécurité des systèmes d'information (ANSSI), Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et vidéoprotection, version 2.1, ANSSI, France, Oct. 2023 ,10 (updated) – PDF available at cyber.gouv.fr.

سال	کشور/ سازمان	شرح نفوذ	ارتباط با خلأ IEC62676
۲۰۱۶	جهانی	باتنت Mirai، ده‌ها هزار دوربین را آلوده و از آنها برای حملات DDoS استفاده کرد	نبود مدیریت وصله و رمزهای پیش‌فرض
۲۰۲۱	آمریکا	نفوذ به سامانه‌های شرکت Verkada و دسترسی به ۱۵۰،۰۰۰ دوربین در زندان‌ها و شرکت‌ها	نبود MFA و مدیریت دسترسی متمرکز
۲۰۲۲	انگلستان	افشای تصاویر اتاق‌های اورژانس توسط نفوذگر در شبکه بیمارستان	نبود رمزنگاری RTSP و عدم جداسازی شبکه
۲۰۲۳	خاورمیانه	دسترسی مهاجم به دوربین‌های شهری و ایجاد فید جعلی	نبود حفاظت صحت تصویر و امضای دیجیتال

نتیجه‌گیری

IEC62676 مجموعه‌ای ارزشمند برای تضمینِ کیفیتِ عملکردی و بین‌عملکردپذیریِ سامانه‌های نظارت تصویری است، اما این استانداردها به‌خودی‌خود ضمانت‌کنندهٔ امنیت سایبریِ جامع نیستند؛ زیرا دامنهٔ کاربرد آن‌ها غالباً «عملکرد تصویری» است نه «حفاظت از سامانه در برابر تهدیدات سایبری».

برای مواجههٔ مؤثر با تهدیدات روز افزون سایبری از جمله باتنت‌ها، افشای تصاویر، تغییر شواهد، حملات زنجیرهٔ تامین و غیره، لازم است استانداردِ تخصصیِ سایبری برای نظارت تصویری تدوین شده توسط سازمان فناوری اطلاعات ایران (که کنترل‌های فنی و فرایندی مربوطه را به‌صورت قابل‌سنجش و آزمون‌پذیر تعریف نموده) ، به قید فوریت تصویب و ابلاغ گردد.

هر روز تاخیر در تامین امنیت سایبری سامانه‌های نظارت تصویری کشور، می‌تواند موجب بروز فجایع غیرقابل جبرانی برای کشور شود.

[5] European Telecommunications Standards Institute (ETSI), Cyber Security for Consumer Internet of Things: Baseline Requirements, ETSI EN 645 303 V3.1.3, Sept. 2024.

[6] Information Commissioner's Office (ICO), Video surveillance (including guidance for organisations using CCTV), UK Government, London, UK. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/video-surveillance.

[7] Agence nationale de la sécurité des systèmes d'information (ANSSI), Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection, ANSSI, France, version 2023 ,2.1. [Online]. Available: https://cyber.gouv.fr/sites/default/files/document/Recommandations20%sur20%la20%s%C%3A9curisation20%des20%syst%C%3A8mes20%de20%contr%C%3B41e20%d27%acc%C%3A8s20%physique20%et20%vid%C%3A9oprotection20%-20%v2.1.pdf.

[8] Bundesamt für Sicherheit in der Informationstechnik (BSI), Guidelines and recommendations on information security, Germany. [Online]. Available: https://www.bsi.bund.de.

[9] Australian Cyber Security Centre (ACSC), Cyber security guidelines, Information Security Manual (ISM), Australian Signals Directorate (ASD), Commonwealth of Australia. [Online]. Available:https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism/cybersecurity-guidelines

امنیت الکترونیک موزه

بازرسی ادواری انطباق‌سنجی با استاندارد ایرانی امنیت الکترونیک موزه‌ها، راه پایان قطعی سرقت از موزه‌ها

نویسنده: محمدقلم‌چی

پنج سرقت دیگر از موزه‌های فرانسه پس از لوور فقط در یک ماه، آماری نگران کننده است. در سال‌های اخیر، موزه‌ها به‌عنوان یکی از حساس‌ترین نهادهای فرهنگی و میراثی مورد نظر مجرمان، گروه‌های سرقت سازمان‌یافته و حتی عملیات دولتی-غیردولتی قرار گرفته‌اند. خبر سرقت از موزه لوور[1] و سپس موزه‌های دیگر فرانسه، نشان می‌دهد که حتی مراکز بزرگ با شهرت بین‌المللی نیز در مقابل تهدیدات الکترونیک و فیزیکی آسیب‌پذیر هستند. به‌عنوان مثال، از ابتدای سپتامبر، ششمین سرقت از موزه‌های فرانسه صورت گرفته است.

در ایران ، استانداردی ملی با عنوان «استاندارد امنیت الکترونیک موزه‌های ایران» تدوین شده است که هدف آن ارتقای سطح حفاظت از میراث فرهنگی در فضای الکترونیکی، نظارت تصویری و امنیتی است. اگرچه این استانداردها در داخل کشور طراحی شده‌اند، ولی هنوز به‌صورت گسترده به عنوان مرجع اجرایی در سطح بین‌المللی پذیرفته نشده‌اند یا به اجرا درنیامده‌اند.

این نوشتار، از نگاه پدر دانش امنیت الکترونیک ایران که رئیس تالیف این استاندارد بوده، نخست خلاصه‌ای از آنچه در استاندارد ملی ایران تدوین شده را بررسی می‌کند و سپس تحلیل می‌کند که در صورت عدم اجرای فوری و بین‌المللی این استاندارد، چه مشکلات جدیدی ممکن است برای موزه‌ها در سطح جهان به‌وجود آید.

موزه‌ها به‌عنوان مراکز نگهداری میراث فرهنگی و هنری، در سال‌های اخیر با تهدیدات گوناگون فیزیکی و الکترونیکی مواجه شده‌اند. نمونه‌هایی چون سرقت از موزه لوور و دیگر مراکز فرهنگی در فرانسه، ضرورت بازبینی و ارتقای استانداردهای امنیتی را نشان می‌دهند. این مقاله با بررسی تفصیلی استاندارد ملی امنیت الکترونیک موزه‌های ایران، تحلیل نمونه‌های موردی، و شناسایی ریسک‌های کلیدی، نشان می‌دهد که اگر این استاندارد در سطح بین‌المللی و با فوریت اجرا نگردد، چه پیامدهای خطرناکی ممکن است به‌وجود آید. در پایان نیز توصیه‌های فنی برای موزه‌ها ارائه می‌گردد.

موزه‌ها نه تنها محل نمایش آثار فرهنگی بلکه ذخیره‌کننده هویت ملی و جهانی هستند. در نتیجه، امنیت آنها یکی از مؤلفه‌های کلیدی حفظ میراث بشری است. در عصر کنونی، تهدیدها ترکیبی از سرقت فیزیکی، نفوذ سایبری، دستکاری داده‌های ضبط‌شده و حتی حملات سازمان‌یافته هستند. هرچند کشورهایی چون

فرانسه موزه‌های بزرگ دارند، ولی این نیز مانع وقوع سرقت نشده است. در ایران نیز استانداردی تحت عنوان «استاندارد ملی امنیت الکترونیک موزه‌های ایران» تدوین گردیده که می‌تواند الگویی برای جهان باشد. اگر این استاندارد به‌صورت بین‌المللی اجرا نشود، موزه‌ها در سطح جهان با ریسک‌های جدی مواجه خواهند شد.

مروری بر مفاد استاندارد ملی امنیت الکترونیک موزه‌های ایران [۱]

طبق منابع موجود، این استاندارد با همکاری سازمان ملی استاندارد ایران و سازمان میراث فرهنگی، صنایع دستی و گردشگری و با مشارکت کارشناسان، به ریاست دکتر محمد قلم‌چی در سال ۱۳۹۱ تالیف شده است. بخش‌های کلیدی آن را می‌توان به شرح ذیل خلاصه کرد:

این استاندارد نه صرفاً ترجمه‌ای از یک استاندارد خاص بلکه تألیفی براساس مطالعه استانداردهای موجود جهانی و در نظر گرفتن ویژگی‌های موزه‌های داخلی و شرایط اقلیمی و محیطی ایران است. بنابراین، استاندارد ایران تلاش کرده است ترکیبی از الزامات فنی، سازمانی، آموزشی و نگهداری را پوشش دهد.

نمونه‌های موردی سرقت از موزه‌ها

تنها در سپتامبر سال ۲۰۲۵، چندین سرقت از موزه‌های مطرح جهان گزارش شده است. به عنوان مثال، به گزارش اشوسیتد پرس، در موزه Egyptian Museum واقع در شهر قاهره، در ۹ سپتامبر ۲۰۲۵ دست‌بند طلای ۳۰۰۰ ساله مربوط به فرعون (Amenemope) از آزمایشگاه مرمت ناپدید شد و بعداً گزارش شد که ذوب و فروخته شده است؛ مظنونان دستگیر شدند. همچنین در Royal Albert Memorial Museum (RAMM)، اگزر (Exeter) در کشور انگلستان، مورخ ۱۰ سپتامبر ۲۰۲۵ ورود با زور و سرقت چندین شئ (حدود ۱۷ ساعت مچی عتیقه و سلاح) کشف شده و موزه موقتاً تعطیل و گزارش پلیس منتشر شد، اما بیشترین سرقت‌ها در فرانسه گزارش شده است.

۱. سرقت از موزه لوور

سرقت از موزه لوور پیش‌بینی‌شده بوده و استاندارد ایران می‌توانست از وقوع آن جلوگیری کند. اگر سیستم‌های نظارت، هشدار و تحلیل رخداد به شیوه استاندارد ایران به‌کار گرفته شده بودند، ممکن بود کشف اولیه سرقت سریع‌تر صورت گیرد یا مهاجمین منصرف شوند.

۲. سرقت‌های ادامه‌دار در موزه‌های فرانسه

در خبرها آمده است که موج سرقت از موزه‌های فرانسه ادامه دارد. این افزایش تعداد سرقت‌ها نشان می‌دهد که تهدیدات به سادگی محدود به یک موزه نبوده، بلکه دارای الگو و احتمال سرایت است. این

جدول ۱. بخش‌های کلیدی استاندارد ملی امنیت الکترونیک موزه‌های ایران

بخش / عنوان	توضیح کلی
طراحی و ساختار سیستم امنیت الکترونیک	شامل تحلیل مخاطره، جانمایی تجهیزات، معماری شبکه، حفاظت فیزیکی از سامانه‌ها
سامانه نظارت تصویری (CCTV) و هوشمندسازی	الزام به نصب دوربین‌های با کیفیت، پوشش همه فضاهای حساس، ذخیره‌سازی امن تصاویر، نگهداری لاگ‌ها
سامانه کنترل دسترسی و هشدار	کنترل ورود/خروج افراد، تعریف سطوح دسترسی، سامانه‌های هشدار به زمان واقعی، پایش رخداد
سامانه اعلان و اطفای حریق، حفاظت زیرساخت‌ها	بخشی از استاندارد بر حفاظت از زیرساخت‌ها و تجهیزات حساس تأکید دارد.
امنیت شبکه و فناوری اطلاعات	حفاظت از سرورها، سوئیچ‌ها، سیستم‌های ذخیره‌سازی، سامانه‌های BMS (سیستم مدیریت ساختمان) و امنیت سایبری
بهره‌برداری، نگهداری و آموزش پرسنل	استاندارد تأکید دارد که فناوری به‌تنهایی کافی نیست؛ بهره‌برداری صحیح، نگهداری منظم، آموزش کارکنان از مؤلفه‌های مهمند
مستندسازی، ارزیابی و بازبینی دوره‌ای	تعریف شاخص‌ها، گزارش رخداد، پاسخ به بحران، ممیزی داخلی برای سنجش کارایی سیستم امنیتی (مستندسازی دقیق ضمن استاندارد مطرح شده است)

موارد نمایانگر این هستند که حتی مراکز معتبر با نقص‌های امنیتی مواجه‌اند.

تحلیل ریسک

در جدول ۲ ماتریس ریسک برای موزه‌ها ارائه شده است.

بررسی کلیدی:

الف) احتمال وقوع سرقت فیزیکی آثار با ارزش بسیار بالا است، زیرا مهاجمان انگیزه و امکان دارند.

ب) شدت پیامد سرقت فیزیکی آثار با ارزش بسیار بالا است، زیرا اثر اقتصادی، فرهنگی و برندینگ دارد.

پ) عدم کشف و پاسخ به موقع یکی از مهم‌ترین ضعف‌ها است. این نقطه‌ای است که استاندارد ایران تلاش دارد آن را پوشش دهد.

ت) نفوذ سایبری نیز رو به افزایش است چرا که بسیاری از سامانه‌های موزه‌ها به شبکه متصل‌شده‌اند اما ممکن است حفاظت مناسبی نداشته باشند.

ث) پیامد از بین رفتن اعتماد عمومی کمتر فوری دیده می‌شود ولی اثرات بلندمدت آن می‌تواند به تعطیلی یا کاهش مشارکت بین‌المللی منجر شود.

ج) خسارت معنوی ممکن است قابل جبران نباشد، پس باید در اولویت باشد.

اگر استاندارد اجرا نشود؛ پیامدهای موردی:

اگر اجرای استاندارد ملی امنیت الکترونیک موزه‌های ایران به فوریت بین‌المللی نشود، موارد ذیل می‌تواند به‌وقوع بپیوندد:

الف) مهاجمان مدل‌های موفق از حمله به موزه‌ها را بازتولید کرده و با سرعت بیشتری عمل می‌کنند.

ب) موزه‌ها ممکن است دچار «حمله دوم» یا «حمله تکراری» شوند، چون پس از یک سرقت مراتب ضعف آنان برملا می‌شود.

پ) سامانه‌های نظارت و پاسخ ضعیف می‌شود، یعنی حتی اگر ورود تشخیص داده شود، پاسخ به زمان واقعی نیست و فرصت بازیابی کاهش می‌یابد.

ت) هزینه‌های محافظت بسیار افزایش پیدا می‌کند؛ موزه‌ها مجبور به سرمایه‌گذاری‌های اضطراری در امنیت می‌شوند که می‌توانست از ابتدا با استراتژی استاندارد کاهش یابد.

ث) آثار به بازار سیاه منتقل شده یا نگهداری مناسبی نداشته باشند؛ بدین ترتیب میراث فرهنگی تخریب شده یا گم می‌شود.

ج) در سطح بین‌المللی، موزه‌ها دیگر نمی‌توانند اعتماد شرکای بین‌المللی را کسب کنند؛ قراردادهای امانت، نمایشگاه‌های مشترک، تبادل آثار کاهش می‌یابد.

چ) زیرساخت‌های فناوری موزه‌ها مانند دوربین‌ها، ذخیره‌سازها و شبکه‌ها مهاجم‌پذیر می‌شوند و ممکن است علاوه بر سرقت، داده‌ها پاک شود یا سامانه‌ها مختل گردند.

ح) رخدادهای بحران (مثلاً بلایای طبیعی، جنگ، حملات تروریستی) هنگامی که سامانه امنیت الکترونیکی ضعفی دارد، تأثیر آن

جدول ۲. ماتریس کلیدی ریسک برای موزه‌ها

ریسک	احتمال وقوع	شدت پیامد	توضیح
سرقت فیزیکی آثار با ارزش	زیاد	بسیار بالا	سرقت مستقیم و خروج آثار یا تخریب آنها
نفوذ سایبری به سامانه‌های امنیتی	متوسط	بالا	نفوذ به سامانه نظارت، کنترل دسترسی یا ضبط تصویر
عدم کشف به‌موقع رخداد (تاخیر یا عدم پاسخ)	زیاد	بالا	نقص در تحلیل یا پاسخ سبب افزایش خسارت می‌شود
تخریب یا دستکاری زیرساخت‌های امنیتی	متوسط	متوسط	حمله به تجهیزات، قطع برق، از کار انداختن سیستم‌ها
از بین رفتن اعتماد عمومی و شرکای بین‌المللی	کم	متوسط	وقتی موزه امنیت ندارد، قراردادها و بازدیدها کاهش می‌یابد
آسیب به میراث فرهنگی و معنوی	کم	بسیار بالا	خسارت فرهنگی و معنوی جبران‌ناپذیر است.

به‌مراتب بیشتر می‌شود.

بازرسی استاندارد، کلید تحقق امنیت موزه‌ها

بازرسی استاندارد بصورت ادواری در موزه‌ها از اهمیت ویژه برخوردار است. همانند سپتام، تداوم فعالیت موزه‌ها نیاز است به رعایت استاندارد ملی امنیت الکترونیک منوط شود. در این بازرسی‌ها، موارد ذیل باید لحاظ گردد:

۱. ارزیابی اولیه و طراحی امنیتی

الف) انجام «تحلیل مخاطره» ویژه موزه (ارزش آثار، زمینه فرهنگی، میزان بازدید، دسترسی عمومی)؛

ب) تنظیم معماری سامانه امنیت الکترونیک شامل نظارت تصویری، کنترل دسترسی، سامانه اعلان و اطفای حریق، شبکه و سرورها؛

پ) جانمایی دوربین‌ها و تجهیزات بر اساس استاندارد: پوشش همه نقاط حساس، نقاط کور صفر یا حداقل.

۲. سامانه نظارت تصویری امن و ضبط با کیفیت

الف) دوربین‌های با وضوح مناسب، پوشش ۲۴×۷، امکان بزرگ‌نمایی و شناسایی چهره؛

ب) ذخیره‌سازی امن تصاویر، نگهداری لاگ‌ها، دسترسی محدود برای تحلیل رخداد؛

پ) ترکیب با تحلیل هوشمند (مثلاً تشخیص حرکت، رفتار مشکوک، خروج غیرمجاز) برای هشدار به زمان واقعی.

۳. کنترل دسترسی و هشدار

الف) تعیین سطوح دسترسی دقیق برای کارکنان، پیمانکاران و بازدیدکنندگان؛

ب) استفاده از کارت‌های هوشمند یا بیومتریک در محل‌های حساس؛

پ) سامانه هشدار که وقتی رویداد غیرمجاز رخ دهد، فوراً تیم واکنش را مطلع کند.

۴. امنیت شبکه و فناوری اطلاعات

الف) تفکیک شبکه‌های امنیتی از شبکه‌های عمومی و استفاده از VLAN و دیواره آتش[2]؛

ب) رمزنگاری ارتباط بین تجهیزات و سرورها، به‌روزرسانی منظم سیستم‌ها و پایش logs شبکه؛

پ) پشتیبان‌گیری دوره‌ای از داده‌ها و برنامه بازگردانی در صورت حمله.

۵. نگهداری، آموزش و مستندسازی

الف) برنامه نگهداری منظم برای تجهیزات امنیتی: تست هشدارها، تغییر پیکربندی‌ها و بررسی به‌روزرسانی‌ها؛

ب) آموزش پرسنل موزه در زمینه امنیت الکترونیک، تحلیل رخداد، دکمه کنترلی و پاسخ به بحران؛

پ) مستندسازی دقیق: شناسایی رخدادها، گزارش‌ها، بازبینی انطباق با استاندارد و ممیزی دوره‌ای.

۶. پاسخ به بحران و بازیابی

الف) طراحی برنامه واکنش به بحران (سرقت، تخریب، حمله سایبری، بلایای طبیعی)؛

ب) تمرین سناریوها با پرسنل، ارزیابی زمان پاسخ، کاهش زمان خاموشی[3]؛

پ) هم‌افزایی با پلیس، نهادهای بین‌المللی، بیمه‌های آثار فرهنگی.

نتیجه‌گیری

موزه‌ها در سطح جهان، علی‌رغم برخورداری از نیروی انسانی متخصص و بودجه، هنوز در معرض تهدیدات جدی قرار دارند. نمونه‌های سرقت از موزه‌هایی مانند موزه لوور و دیگر مراکز فرانسه، گویای این واقعیت‌اند. استاندارد ملی امنیت الکترونیک موزه‌های ایران، مجموعه‌ای جامع از الزامات فنی، سازمانی و عملیاتی ارائه کرده است که اگر به‌فوریت و در سطح بین‌المللی اجرا شود، می‌تواند نقش مؤثری در کاهش این تهدیدات ایفا کند. در مقابل، تاخیر یا عدم اجرا به معنای پذیرش ریسک‌های بالاتر، خسارات مادی و معنوی بیشتر و تضعیف جایگاه موزه‌هاست.

از این رو، توصیه می‌شود موزه‌های بین‌المللی، سازمان‌های مرتبط با میراث فرهنگی و نهادهای استانداردسازی، این سند را جدّی گرفته و آن را به‌عنوان بخشی از چارچوب حفاظتی خویش پذیرفته و اجرا نمایند. استانداردسازی امنیت الکترونیک در تمامی طول عمر موزه اهمیت دارد، لذا توصیه می‌شود به منظور کاهش امکان سرقت و سایر مخاطرات، تداوم فعالیت موزه‌ها، به نتایج بازرسی ادواری سامانه‌های امنیت الکترونیک این اماکن وابسته شود.

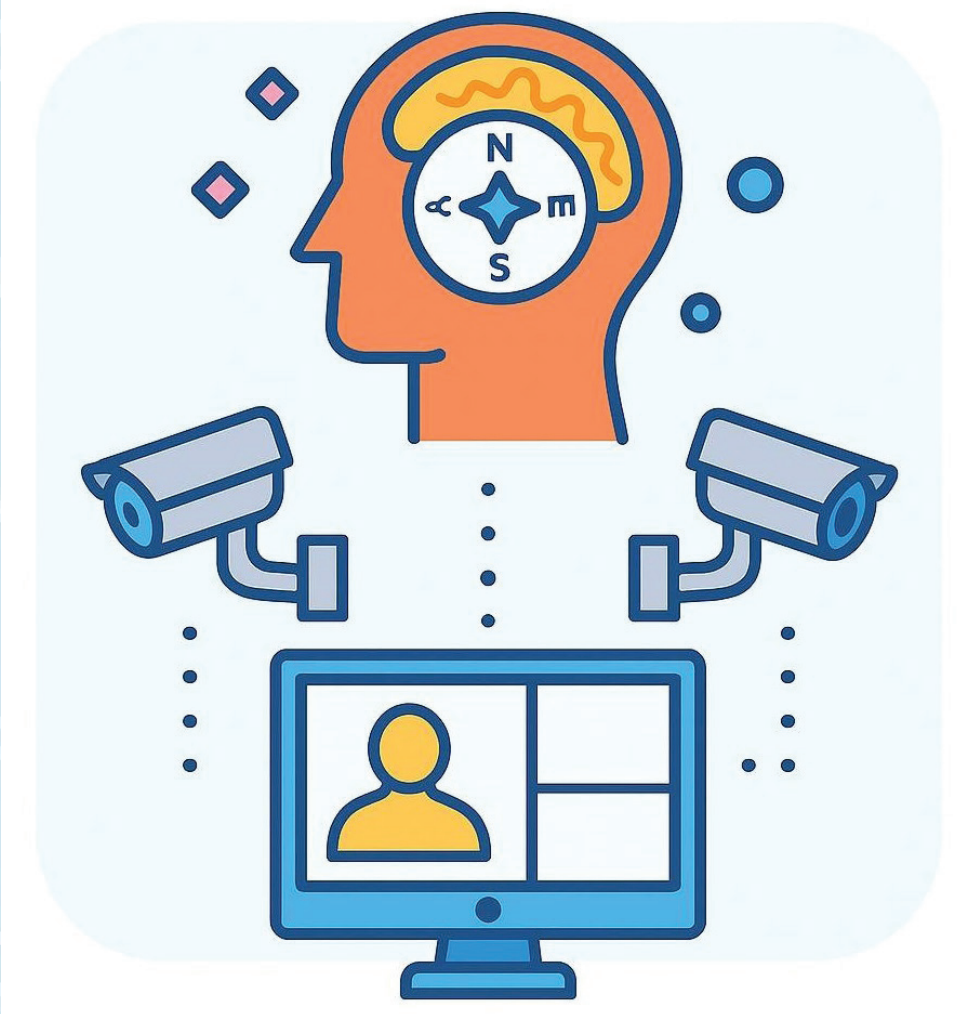
1. Musée du Louvre
2. Firewall
3. Downtime

منبع

۱. استاندارد ملی ایران شماره ۱۴۲۷۹: «الزامات حفاظت الکترونیکی موزه‌ها»، سازمان ملی استاندارد ایران، ۱۳۹۱.

هوش مکانی در سامانه‌های نظارت تصویری

نویسنده: محمود سعیدی



با گسترش روزافزون سامانه‌های نظارت تصویری در محیط‌های شهری، صنعتی و امنیتی، نیاز به تحلیل هوشمند داده‌های مکانی و تصویری بیش از پیش احساس می‌شود. در این میان، هوش مکانی[1] به‌عنوان یکی از زیرشاخه‌های کلیدی هوش مصنوعی، توانایی درک روابط مکانی میان اشیاء، رویدادها و مکان‌ها را فراهم می‌سازد و موجب ارتقای قابلیت‌های تحلیلی سامانه‌های نظارتی می‌شود. در واقع، هوش مکانی به توانایی درک، تحلیل و تفسیر روابط مکانی میان اشیاء و محیط اطراف اشاره دارد. این فناوری با ترکیب داده‌های مکانی، زمانی و تصویری، امکان تحلیل موقعیت‌محور را برای تشخیص دقیق‌تر رخدادها و تصمیم‌گیری در زمان واقعی فراهم می‌کند. چنین رویکردی در حوزه‌هایی مانند مدیریت ترافیک، امنیت شهری و نظارت بر زیرساخت‌های حیاتی نقش مهمی ایفا می‌کند.

از منظر فنی، پیاده‌سازی هوش مکانی در سامانه‌های نظارت تصویری مستلزم ادغام الگوریتم‌های بینایی

ماشین[۲]، یادگیری عمیق[۳] و تحلیل داده‌های مکانی است. مدل‌های شبکه‌های عصبی پیچشی[۴]، در کنار شبکه‌های عصبی گرافی[۵] می‌توانند روابط مکانی- زمانی را میان اشیاء استخراج کرده و الگوهای رفتاری غیرعادی را شناسایی کنند. علاوه بر این، ترکیب داده‌های تصویری با سامانه‌های اطلاعات جغرافیایی[۶] و حسگرهای اینترنت اشیاء[۷] منجر به ایجاد دیدی چندبعدی از محیط می‌شود که به‌صورت بلادرنگ، موقعیت، جهت حرکت و تعامل اشیاء را تحلیل می‌کند.

با وجود این پیشرفت‌ها، چالش‌هایی همچون حجم عظیم داده‌های مکانی- تصویری، نیاز به توان پردازشی بالا و نگرانی‌های مربوط به حفظ حریم خصوصی و امنیت داده‌ها همچنان پابرجاست. برای غلبه بر این چالش‌ها، پژوهش‌های آینده باید بر توسعه معماری‌های پردازش لبه‌ای، فشرده‌سازی هوشمند داده‌های مکانی و الگوریتم‌های یادگیری مقاوم به نویز متمرکز شوند. در مجموع، تلفیق هوش مکانی با سامانه‌های نظارت تصویری می‌تواند گامی مؤثر در جهت تحقق محیط‌های هوشمند، خودآگاه و ایمن شهری باشد.

در این مقاله، با تحلیل ساختار مفهومی و چالش‌های فنی پیاده‌سازی هوش مکانی در سامانه‌های نظارت تصویری، تصویری جامع از وضعیت موجود و مسیرهای آینده این حوزه ارائه می‌شود.

با افزایش پیچیدگی محیط‌های شهری و رشد نیاز به امنیت و پایش بلادرنگ، سامانه‌های نظارت تصویری به یکی از مؤلفه‌های کلیدی در زیرساخت‌های هوشمند شهری تبدیل شده‌اند. این سامانه‌ها در ابتدا تنها برای ثبت و ذخیره تصاویر طراحی می‌شدند اما با گسترش فناوری‌های هوش مصنوعی، اکنون قادر به تحلیل خودکار و تشخیص رویدادهای خاص در زمان واقعی هستند. هوش مکانی به عنوان یکی از نوآوری‌های مهم در حوزه‌ی هوش مصنوعی، نقش تعیین‌کننده‌ای در افزایش دقت، سرعت و کارایی سامانه‌های نظارتی ایفا می‌کند.

هوش مکانی به عنوان زیرمجموعه‌ای از هوش مصنوعی، با تمرکز بر تحلیل روابط مکانی بین اشیاء (موقعیت، فاصله، مسیر حرکت و تغییرات فضایی)، نقشی کلیدی در ارتقای دقت و کارایی سامانه‌های نظارت تصویری ایفا می‌کند. هوش مکانی را می‌توان توانایی سامانه در درک روابط فضایی میان اشیاء، مکان‌ها و رویدادها دانست، به‌گونه‌ای که بتواند محیط پیرامون خود را نه صرفاً به‌صورت تصویری، بلکه به‌صورت موقعیت‌محور[۸] تحلیل کند [۱]. برخلاف روش‌های سنتی پردازش تصویر که تنها به شناسایی اشیاء در فریم‌های جداگانه می‌پردازند، هوش مکانی روابط میان عناصر محیطی را بر اساس داده‌های مکانی و زمانی استخراج کرده و الگوهای رفتاری یا حرکتی را تفسیر می‌کند [۲]. این قابلیت، زیربنای تصمیم‌گیری‌های هوشمند در کاربردهایی نظیر مدیریت ترافیک، کنترل مرزها، پایش تأسیسات حیاتی و حتی تحلیل ازدحام جمعیت است [۳].

با وجود پیشرفت‌های قابل توجه در یادگیری عمیق و بینایی ماشین، چالش‌هایی نظیر حجم عظیم داده‌های ویدئویی، نیاز به توان پردازشی بالا، عدم وجود استانداردهای داده مکانی و نگرانی‌های حریم خصوصی، پیاده‌سازی کامل هوش مکانی را با محدودیت‌هایی روبه‌رو کرده است [۴]. برای غلبه بر این موانع، پژوهش‌های اخیر بر استفاده از معماری‌های پردازش لبه‌ای[۹] و سامانه‌های توزیع‌شده برای تحلیل داده‌های مکانی در محل تمرکز یافته‌اند [۵]. همچنین، ترکیب داده‌های سامانه‌های اطلاعات جغرافیایی با تصاویر ویدئویی و اطلاعات حسگرهای اینترنت اشیاء، بستری مناسب برای شکل‌گیری نظارت تصویری موقعیت‌محور[۱۰] فراهم ساخته است [۶].

مفهوم هوش مکانی

هوش مکانی یکی از شاخه‌های مهم هوش انسانی و مصنوعی است که به توانایی درک، تحلیل و تفسیر روابط فضایی میان اشیاء، مکان‌ها و الگوهای محیطی اشاره دارد. این نوع از هوش، نقش اساسی در فعالیت‌هایی نظیر ناوبری، طراحی معماری، تحلیل داده‌های جغرافیایی و حتی در سامانه‌های نظارت تصویری ایفا می‌کند.

در حوزه علوم شناختی، هوش مکانی به‌عنوان توانایی ذهنی برای تصور، تجسم و دست‌کاری تصاویر فضایی تعریف می‌شود. این مفهوم در نظریه "هوش‌های چندگانه" گاردنر مطرح شد که در آن، هوش مکانی به‌عنوان یکی از انواع مستقل هوش انسانی معرفی گردید [۷].

در حوزه فناوری و به‌ویژه در هوش مصنوعی، هوش مکانی به قابلیت سامانه‌ها برای درک محیط پیرامونی و استنتاج روابط فضایی از داده‌های حسی اشاره دارد. در سامانه‌های هوشمند نظارت تصویری، این نوع از هوش می‌تواند برای تشخیص موقعیت اشیاء، ردیابی حرکت، و تحلیل الگوهای رفتاری در فضاهای فیزیکی به کار رود [۸]. به عنوان مثال، در یک شبکه نظارت شهری، هوش مکانی به سامانه اجازه می‌دهد تا محل وقوع رویدادها را در نقشه به‌صورت خودکار تشخیص دهد و داده‌های ویدئویی را با موقعیت‌های جغرافیایی مرتبط سازد. چنین قابلیتی موجب ارتقای آگاهی موقعیتی و تسریع در تصمیم‌گیری‌های امنیتی می‌شود [۹].

از منظر سامانه‌های اطلاعات مکانی، هوش مکانی مفهومی فراتر از نقشه‌سازی صرف است و شامل فرایندهای شناختی و محاسباتی برای استنتاج الگوهای فضایی، پیش‌بینی تغییرات محیطی و بهینه‌سازی تصمیم‌ها بر اساس داده‌های مکانی است. به‌کارگیری الگوریتم‌های یادگیری ماشین در پردازش داده‌های مکانی، موجب شکل‌گیری شاخه‌ای جدید به نام هوش مکانی مصنوعی شده است که در کاربردهایی مانند شهر هوشمند، کشاورزی دقیق و مدیریت بحران مورد استفاده قرار می‌گیرد [۱۰]. این رویکرد، ترکیبی از تحلیل داده‌های مکانی، بینایی ماشین و مدل‌سازی پیش‌بینانه است که درک سیستماتیکی از "کجا" و "چرا" در داده‌ها فراهم می‌آورد.

به طور کلی، هوش مکانی با فراهم آوردن درک عمیق از ساختار فضایی محیط، زمینه‌ساز نسل

جدیدی از سامانه‌های نظارت تصویری است که نه‌تنها قادر به تشخیص رخدادها بلکه قادر به درک معنای فضایی و رفتاری آن‌ها نیز خواهند بود. چنین تحولی می‌تواند نقش مهمی در ایجاد شهرهای هوشمند، کاهش جرایم، بهبود واکنش اضطراری و ارتقای بهره‌وری سیستم‌های امنیتی ایفا کند [۱۱] [۵].

مروری بر پژوهش‌های پیشین

پژوهش‌های مرتبط با هوش مکانی در سامانه‌های نظارت تصویری طی دهه اخیر رشد قابل‌توجهی داشته است. در مراحل اولیه، تمرکز اصلی تحقیقات بر تشخیص اشیاء و رویدادها با استفاده از الگوریتم‌های کلاسیک بینایی ماشین بود، بدون آنکه ارتباط فضایی میان اشیاء یا محیط مورد توجه قرار گیرد [۱۲]. با ظهور یادگیری عمیق به‌خصوص شبکه‌های عصبی پیچشی عمیق، امکان استخراج ویژگی‌های مکانی از تصاویر فراهم شد، اما این ویژگی‌ها اغلب ایستا و فریم‌محور بودند و توان تحلیل روابط فضایی پویا را نداشتند [۱۱]. در نتیجه، نسل جدیدی از رویکردها با محوریت یادگیری مکانی–زمانی شکل گرفت که هدف آن درک ارتباط میان موقعیت، حرکت و تعامل اشیاء در ویدئوها بود [۲].

در برخی از پژوهش‌های انجام شده، مفهوم هوش مکانی به‌عنوان توانایی شناخت روابط فضایی در داده‌ها مطرح و زیربنای تحلیل‌های مبتنی بر موقعیت در نظر گرفته شده است [۱]. این مفهوم بعدها در حوزه‌ی نظارت تصویری به‌کار گرفته شد تا سامانه‌ها بتوانند فراتر از تشخیص، به درک موقعیت‌محور محیط برسند. در همین راستا، با تلفیق حسگرهای اینترنت اشیاء و سامانه‌های اطلاعات جغرافیایی، چارچوبی برای نظارت مکانی بلادرنگ ارائه شده است که قادر به شناسایی تغییرات محیطی و حرکتی در سطح شهری است. نتایج پژوهش‌ها نشان داد که ترکیب داده‌های مکانی و تصویری می‌تواند دقت تشخیص رخدادها را تا ۳۵٪ افزایش دهد [۳].

در حوزه مدل‌سازی هوشمند، استفاده از شبکه‌های عصبی گرافی برای استخراج ساختارهای مکانی–زمانی پیشنهاد شده است. این روش امکان تحلیل روابط میان اشیاء و مسیرهای حرکتی را فراهم می‌سازد و به‌ویژه در شناسایی رفتارهای غیرعادی یا تهدیدهای امنیتی عملکرد مناسبی دارد [۲]. در پژوهش مشابه دیگری، مفهوم هوش مکانی–زمینه‌ای[11] ارائه شده است که بهره‌گیری از داده‌های چندمنبعی (تصویری، مکانی و زمانی)، محیط پیرامون دوربین‌ها را در قالب یک نقشه هوشمند بازنمایی می‌کند. این رویکرد، پایه‌ای برای توسعه سامانه‌های خودآگاه در حوزه‌ی شهر هوشمند به‌شمار می‌رود [۶].

برخی مطالعات به بررسی چالش‌ها و ملاحظات اجرایی در پیاده‌سازی هوش مکانی پرداخته‌اند. در یکی از پژوهش‌ها، به مشکلاتی مانند نیاز به پردازش حجم عظیم داده‌های ویدئویی، پیچیدگی هم‌زمان‌سازی داده‌های مکانی و تصویری، و نگرانی‌های مربوط به حفظ حریم خصوصی اشاره شده است. در این پژوهش، تأکید شده است که استفاده از پردازش لبه‌ای و تحلیل توزیع‌شده می‌تواند بخشی از این چالش‌ها را کاهش دهد [۴]. همچنین در پژوهش دیگری پیشنهاد شده است که طراحی سامانه‌های نظارتی باید به سمت معماری‌های آگاه از مکان[12] حرکت کند تا بتواند تصمیم‌گیری‌های محلی و بلادرنگ را ممکن سازد [۵] . مرور بر مطالعات پیشین نشان می‌دهد که تمرکز فعلی پژوهش‌ها از تشخیص صرف اشیاء به سمت درک هوشمند از مکان و موقعیت تغییر یافته است. با وجود این، هنوز خلأهایی در زمینه‌ی استانداردسازی داده‌های مکانی–تصویری، هم‌افزایی میان سامانه‌های اطلاعات جغرافیایی و هوش مصنوعی و حفظ امنیت داده‌های مکانی وجود دارد که نیازمند پژوهش‌های میان‌رشته‌ای بیشتر است [۵] [۱۱].

چالش‌های پیاده‌سازی هوش مکانی در سامانه‌های نظارت تصویری

با وجود پیشرفت‌های قابل‌توجه در حوزه‌ی هوش مصنوعی و یادگیری عمیق، پیاده‌سازی هوش مکانی در سامانه‌های نظارت تصویری همچنان با چالش‌های فنی، سازمانی و اخلاقی متعددی مواجه است. این چالش‌ها عمدتاً ناشی از ماهیت پیچیده داده‌های مکانی–تصویری، الزامات پردازشی سنگین و ملاحظات امنیتی و حریم خصوصی هستند [۱۱]. در این بخش، مهم‌ترین موانع پیش روی توسعه و استقرار هوش مکانی در سامانه‌های نظارتی مورد بررسی قرار می‌گیرد. چالش‌های ارائه شده در این بخش، نشان می‌دهد که پیاده‌سازی هوش مکانی در سامانه‌های نظارت تصویری، فراتر از یک مساله فنی صرف است و نیازمند همکاری میان حوزه‌های هوش مصنوعی، ژئوانفورماتیک، امنیت سایبری و حقوق داده است. غلبه بر این موانع می‌تواند راه را برای توسعه سامانه‌های نظارت هوشمند، خودآگاه و اخلاق‌مدار هموار سازد.

۱. حجم عظیم و پیچیدگی داده‌های مکانی–تصویری

یکی از چالش‌های اصلی در پیاده‌سازی هوش مکانی، مدیریت حجم بسیار زیاد داده‌های تولیدشده توسط دوربین‌ها و حسگرهای محیطی است. هر سامانه نظارت شهری می‌تواند روزانه چندین ترابایت داده ویدئویی و مکانی تولید کند که پردازش، انتقال و ذخیره‌سازی آن نیازمند زیرساخت‌های قوی و هزینه‌بر است. علاوه بر حجم، داده‌های مکانی دارای ناهمگونی ذاتی‌اند؛ به‌گونه‌ای که داده‌های تصویری، سامانه موقعیت‌یابی جهانی[13]، نقشه‌های سامانه‌های اطلاعات جغرافیایی باید در قالب یک چارچوب تحلیلی یکپارچه شوند. این هم‌ترازی داده‌ها مستلزم طراحی مدل‌های هم‌زمان‌سازی مکانی–زمانی و الگوریتم‌های فشرده‌سازی هوشمند است که همچنان از چالش‌های بازپژوهی محسوب می‌شود.

۲. توان پردازشی بالا و زمان پاسخ بلادرنگ

تحلیل داده‌های مکانی در کنار ویدئوهای زنده مستلزم اجرای هم‌زمان عملیات محاسباتی سنگین شامل تشخیص اشیاء، تحلیل موقعیت، ردیابی حرکتی و مدل‌سازی روابط فضایی است. این موضوع به‌ویژه در کاربردهای حیاتی مانند نظارت مرزی یا کنترل ترافیک، نیازمند پاسخ بلادرنگ و تأخیر بسیار پایین است. با این حال، محدودیت توان پردازشی در گره‌های شبکه، به‌خصوص در نقاط لبه‌ای[14]، مانعی جدی محسوب می‌شود. راهکارهایی مانند پردازش لبه‌ای توزیع‌شده[15] و یادگیری فدره‌ای[16] می‌توانند بخشی از این چالش را کاهش دهند [۵]. اما هنوز مسائلی چون هماهنگی گره‌ها، به‌روزرسانی مدل‌ها و اطمینان از امنیت انتقال داده پابرجاست.

۳. چالش‌های حریم خصوصی و امنیت داده‌ها

استفاده از هوش مکانی مستلزم جمع‌آوری

و تحلیل اطلاعات حساس از موقعیت‌های جغرافیایی، رفتار افراد و تعاملات فضایی آن‌هاست که نگرانی‌های جدی در زمینه‌ی حریم خصوصی ایجاد می‌کند. در بسیاری از کشورها، چارچوب‌های قانونی مشخصی برای حفاظت از داده‌های مکانی افراد وجود ندارد و همین امر خطر سوءاستفاده از داده‌های نظارتی را افزایش می‌دهد. علاوه بر این، سامانه‌های مبتنی بر هوش مکانی خود می‌توانند هدف حملات سایبری قرار گیرند، به‌ویژه زمانی که داده‌های مکانی از طریق شبکه‌های بی‌سیم یا سامانه‌های ابری منتقل می‌شوند. پژوهش‌ها نشان می‌دهند که استفاده از رمزنگاری هم‌ریخت[17] و ناشناس‌سازی مکانی[18] می‌تواند تا حد زیادی از افشای داده‌ها جلوگیری کند [۶].

۴.چالش‌های استانداردسازی و یکپارچگی میان‌سیستمی

نبود استانداردهای مشخص برای تبادل داده‌های مکانی–تصویری از دیگر موانع مهم پیاده‌سازی هوش مکانی در سامانه‌های نظارتی است. بسیاری از سازمان‌ها از قالب‌ها و پروتکل‌های متفاوتی برای ذخیره و انتقال داده استفاده می‌کنند که مانع یکپارچگی میان سامانه‌ها می‌شود. در همین راستا، نهادهای بین‌المللی مانند کنسرسیوم باز جغرافیایی[19] (یک سازمان بین‌المللی است که به تدوین و ترویج استانداردهای باز برای داده‌ها و خدمات مکانی و جغرافیایی می‌پردازد) در حال تدوین استانداردهایی برای تبادل داده‌های مکانی در سامانه‌های هوشمند هستند، اما هنوز در مرحله‌ی اولیه توسعه قرار دارند. نبود این استانداردها نه‌تنها هم‌افزایی میان سامانه‌های نظارتی را دشوار می‌سازد، بلکه باعث کاهش قابلیت همکاری[20] و بهره‌وری اطلاعات مکانی می‌شود.

۵. محدودیت‌های داده‌های آموزشی و تعمیم‌پذیری مدل‌ها

الگوریتم‌های یادگیری عمیق که در قلب هوش مکانی قرار دارند، نیازمند حجم بالایی از داده‌های آموزشی مکانی–زمانی دقیق و برچسب‌خورده هستند. با این حال، دسترسی به چنین داده‌هایی در حوزه‌های امنیتی و نظارتی بسیار محدود است. علاوه بر این، مدل‌های آموزش‌دیده در یک محیط خاص معمولاً در محیط‌های دیگر عملکرد مطلوبی ندارند، زیرا روابط فضایی و الگوهای رفتاری از مکانی به مکان دیگر متفاوت است. بنابراین توسعه مدل‌های تعمیم‌پذیر و مستقل از مکان[21] از اولویت‌های اصلی تحقیقات آینده محسوب می‌شود.

کاربردها و مزایای هوش مکانی در سامانه نظارت تصویری

هوش مکانی با فراهم‌کردن توانایی درک و تحلیل روابط مکانی میان اشیاء، رویدادها و محیط، موجب تحول اساسی در عملکرد سامانه‌های نظارت تصویری شده است. در مقایسه با سامانه‌های سنتی که صرفاً به ثبت تصاویر و تشخیص اشیاء محدود می‌شوند، سامانه‌های مبتنی بر هوش مکانی قادرند تحلیل موقعیت‌محور انجام دهند و از سطح شناسایی ساده فراتر روند. در این بخش، کاربردهای اصلی و مزایای کلیدی هوش مکانی در حوزه‌های امنیتی، شهری و صنعتی مورد بررسی قرار می‌گیرد.

۱.نظارت شهری و مدیریت ترافیک هوشمند

یکی از مهم‌ترین کاربردهای هوش مکانی، در سامانه‌های نظارت شهری و کنترل هوشمند ترافیک است. این سامانه‌ها با بهره‌گیری از تحلیل مکانی–زمانی، می‌توانند الگوهای حرکتی وسایل نقلیه و عابران را شناسایی کرده و در صورت بروز رفتارهای غیرعادی مانند توقف غیرمجاز یا ازدحام ناگهانی هشدار صادر کنند. ترکیب داده‌های تصویری با سامانه‌های اطلاعات جغرافیایی، امکان تحلیل ترافیک در سطح شبکه شهری را فراهم می‌سازد و تصمیم‌گیری هوشمند در زمینه‌ی مدیریت مسیرها، کنترل چراغ‌های راهنمایی و پیش‌بینی تراکم را ممکن می‌سازد. همچنین استفاده از مدل‌های یادگیری مکانی–زمانی در نظارت ترافیکی موجب افزایش دقت تشخیص ازدحام در مقایسه با روش‌های سنتی شده است.

۲. امنیت محیطی و کنترل مرزی

در حوزه‌ی امنیت محیطی، هوش مکانی نقش کلیدی در درک موقعیت و رفتارهای غیرعادی در محیط‌های باز یا مرزی دارد. به کمک مدل‌های گراف‌محور و تحلیل روابط مکانی، سامانه‌های نظارتی می‌توانند الگوهای نفوذ، عبور از مرز یا حرکات مشکوک را در محیط‌های وسیع تشخیص دهند. همچنین، با استفاده از داده‌های مکانی از حسگرهای زمینی، پهپادها و دوربین‌های حرارتی، امکان تحلیل چندمنبعی از تهدیدات فراهم می‌شود. این ترکیب داده‌ها، دقت تشخیص تهدید را به‌طور چشمگیری افزایش داده و از هشدارهای کاذب می‌کاهد. افزون بر این، در حوزه‌ی امنیت زیرساخت‌های حیاتی مانند نیروگاه‌ها یا فرودگاه‌ها، تحلیل مکانی به سامانه‌ها کمک می‌کند تا مسیرهای احتمالی نفوذ و مناطق آسیب‌پذیر را شناسایی کنند.

۳.تحلیل رفتاری و تشخیص الگوهای مکانی–زمانی

یکی دیگر از کاربردهای مهم هوش مکانی تحلیل رفتار افراد و اشیاء در مکان و زمان است. این نوع تحلیل با استفاده از مدل‌های یادگیری عمیق به‌خصوص شبکه‌های CNN و GNN قادر است الگوهای رفتاری را بر اساس موقعیت، مسیر و تعامل با سایر عناصر محیط شناسایی کند [۱۱]. به عنوان مثال، در محیط‌های عمومی نظیر ایستگاه‌ها یا مراکز خرید، سامانه می‌تواند رفتارهای غیرعادی مانند توقف طولانی، مسیرهای تکراری یا حرکت ناگهانی گروهی از افراد را شناسایی کرده و هشدار امنیتی صادر کند. علاوه بر کاربردهای امنیتی، این قابلیت در تحلیل رفتار مشتریان و بهینه‌سازی طراحی فضاهای شهری نیز قابل استفاده است.

۴. پایش محیطی و مدیریت بحران

هوش مکانی همچنین در حوزه‌های زیست‌محیطی و مدیریت بحران کاربرد فراوان دارد. با استفاده از تصاویر ماهواره‌ای و داده‌های ویدئویی زمینی، می‌توان تغییرات مکانی در محیط‌های طبیعی مانند جنگل‌ها، رودخانه‌ها یا مناطق پرخطر را شناسایی و مدل‌سازی کرد. در زمان بروز بحران‌هایی مانند آتش‌سوزی، سیل یا زلزله، سامانه‌های نظارتی مکانی می‌توانند

مسیر گسترش حادثه را به‌صورت بلادرنگ پیش‌بینی کرده و اطلاعات حیاتی را برای تیم‌های امداد ارسال کنند. بر اساس نتایج پژوهش‌های اخیر، استفاده از الگوریتم‌های هوش مکانی در مدیریت بحران موجب کاهش میانگین زمان واکنش اضطراری تا ۳۰٪ شده است [۶].

۵. مزایای کلیدی پیاده‌سازی هوش مکانی

به‌طور کلی، پیاده‌سازی هوش مکانی در سامانه‌های نظارت تصویری منجر به افزایش دقت، کاهش هشدارهای کاذب، بهبود درک موقعیتی و تصمیم‌گیری سریع‌تر می‌شود. این فناوری با ایجاد قابلیت‌های خودیادگیر و موقعیت‌محور، موجب بهبود پایداری سامانه‌ها در محیط‌های پویا می‌گردد. افزون بر آن، هوش مکانی بستری برای توسعه سامانه‌های خودآگاه فراهم می‌کند که قادر به تفسیر و واکنش مستقل در شرایط مختلف هستند. چنین قابلیتی، گامی مهم در مسیر تحقق شهرهای هوشمند، امنیت پایدار و مدیریت هوشمند منابع محسوب می‌شود.

نتیجه‌گیری

هوش مکانی به‌عنوان یکی از ارکان نوظهور در توسعه سامانه‌های نظارت تصویری، زمینه‌ساز گذار از نظارت سنتی مبتنی بر مشاهده به نظارت هوشمند مبتنی بر درک موقعیت و روابط مکانی است. تلفیق این رویکرد با فناوری‌هایی همچون بینایی ماشین، یادگیری عمیق، اینترنت اشیاء و سامانه‌های اطلاعات جغرافیایی، امکان تحلیل چندبعدی محیط را فراهم می‌سازد و موجب ارتقای چشمگیر درک موقعیتی، دقت تصمیم‌گیری و واکنش بلادرنگ در سامانه‌های نظارت تصویری می‌شود.

یافته‌های این پژوهش نشان می‌دهد که هوش مکانی نه‌تنها به بهبود قابلیت‌های فنی سامانه‌های نظارت تصویری مانند ردیابی اشیاء و تشخیص رفتارهای غیرعادی، منجر می‌شود بلکه بستر لازم برای توسعه سامانه‌های خودآگاه و پیش‌بین را نیز فراهم می‌کند. این تحول می‌تواند نقش تعیین‌کننده‌ای در امنیت شهری، مدیریت بحران، کنترل ترافیک و پایش زیرساخت‌های حیاتی ایفا کند.با این حال، پیاده‌سازی کامل هوش مکانی مستلزم غلبه بر چالش‌هایی همچون حجم عظیم داده‌های مکانی–تصویری، نیاز به توان پردازشی بالا، کمبود استانداردهای تبادل داده و نگرانی‌های حریم خصوصی است. رویکردهایی مانند پردازش لبه‌ای، یادگیری فدره‌ای، رمزنگاری هم‌ریخت و توسعه استانداردهای باز مکانی، می‌توانند مسیر پیشرفت این حوزه را هموار سازند. در مجموع، هوش مکانی چشم‌اندازی نو برای آینده سامانه‌های نظارت تصویری ترسیم می‌کند؛ سامانه‌هایی که فراتر از ثبت و تشخیص، قادر به درک زمینه، پیش‌بینی رخداد و تصمیم‌گیری هوشمند در زمان واقعی هستند تداوم پژوهش‌های میان‌رشته‌ای در زمینه‌ی تلفیق داده‌های مکانی، تصویری و زمانی می‌تواند گامی مؤثر در جهت تحقق نسل آینده‌ی سامانه‌های نظارتی موقعیت‌محور، هوشمند و پایدار باشد.

1. Spatial Intelligence
2. Machine Vision
3. Deep Learning (DL)
4. Convolutional Neural Networks (CNN)
5. Graph Neural Networks (GNN)
6. Geographic Information Systems (GIS)
7. Internet of Things (IoT)
8. Geo-Contextual
9. Edge AI
10. Geo-Contextual Surveillance
11. Geo-Contextual Intelligence
12.Spatially-Aware Architectures
13. Global Positioning System (GPS)
14. Edge Devices
15. Distributed Edge Computing
16. Federated Learning
17. Homomorphic Encryption
18. Spatial Anonymization
19. Open Geospatial Consortium (OGC)
20. Interoperability
21. Location-independent Models

منابع

[1] M. F. Goodchild, "Spatial intelligence and the future of geographic information science", International Journal of Geographical Information Science, 230–213 ,(2)34 ,2020.

[2] Q. Zhang, T. Wang, H. Liu, "Graph-based spatiotemporal learning for abnormal event detection in video surveillance", Pattern Recognition Letters, 121–112 ,168 ,2023.

[3] J. Wang, L. Zhao, D. Xu, "IoT-driven spatial intelligence for real-time video monitoring", IEEE Internet of Things Journal, –8324 ,(10)8 ,2021 8335.

[4] R. Alshammari, A. Murray, "Challenges in implementing spatial AI for surveillance applications", Computers & Security, ,112 ,2022 102515

[5] D. Santos, J. Rodrigues, P. Costa, "Spatially aware AI systems for urban safety and intelligent monitoring". Expert Systems with Applications, 122017 ,243 ,2024.

[6] L. Huang, Y. Sun, Z. Guo, "Geo-contextual intelligence in surveillance systems: From sensors to spatial cognition", ISPRS International Journal of Geo-Information, ,2023 159–145 ,(2)12.

[7] H. Gardner, "Frames of Mind: The Theory of Multiple Intelligences", Basic Books, 1983.

[8] Goodchild, M. F. (2018). "Reconsidering the idea of spatial intelligence." International Journal of Geographical Information Science, 1954–1943 ,(10)32.

[9] Li, S., Dragicevic, S., Castro, F. A., & Sester, M. (2021). "Spatial artificial intelligence for geospatial data analysis: Recent developments and future directions." ISPRS Journal of Photogrammetry and Remote Sensing, 179–163 ,178

[10] Jiang, B., Yin, J., & Sandberg, M. (2020). "Geospatial intelligence and spatial data science: A new paradigm." Computers, Environment and Urban Systems, 101528 ,83

[11] J. Chen, H. Zhang, S. Liu, "Spatial intelligence in visual surveillance: A review", IEEE Transactions on Intelligent Systems, –512 ,(4)37 ,2022 528.

[12] Li, X., & Fan, Y. (2021). Integrating spatial cognition and video analytics for smart surveillance. Sensors, ,(14)21 4823.

فصلنامه امنیت الکترونیک در پایگاه سیویلیکا نمایه شد

فصلنامه امنیت الکترونیک تحت حمایت سیویلیکا قرار گرفت و مقالات هر شماره از آن در پایگاه سیویلیکا نمایه‌سازی و منتشر می‌شود.

آدرس فصلنامه در پایگاه سیویلیکا:
https://civilica.com/l/177742/

فصلنامه امنیت الکترونیک در سیویلیکا به شرح ذیل معرفی شده است:

نشریه امنیت الکترونیک به بسط و توسعه دانش امنیت الکترونیک در کشور و اطلاع رسانی اخبار آن می پردازد.
این نشریه با هدف انعکاس دستاوردهای علمی پژوهشگران، به صورت فصلنامه در محورهای زیر مبادرت به انتشار مقالات علمی، ترویجی و پژوهشی می نماید:

- امنیت تجهیزات الکترونیکی
- امنیت سایبری
- مکاترونیک
- الکترومغناطیس
- بیوالکترومغناطیس
- ژئوالکترومغناطیس
- سایبرالکترومغناطیس
- ماهواره
- میکروالکترونیک
- اپتیک و لیزر
- آکوستیک
- هوش مصنوعی
- تحلیل ویدئو
- امنیت شبکه و سامانه ها

The Electronic Security Journal is dedicated to the expansion and development of electronic security knowledge in the country and to reporting news related to this field.
This journal, with the aim of reflecting the scientific achievements of researchers, publishes scientific, promotional, and research articles on a quarterly basis in the following areas:

- Electronic Equipment Security
- Cybersecurity
- Mechatronics
- Electromagnetic
- Bioelectromagnetics
- Geoelectromagnetics
- Cyber Electromagnetics
- Satellite
- Microelectronics
- Optics and Laser
- Acoustics
- Artificial Intelligence (AI)
- Video Analytics
- Network and Systems Security

مجله معتبر در حال پذیرش مقاله

آخرین شماره نمایه شده: ۱۴۰۴/۱۰/۱۷

ارسال مقاله به مجله

Sponsored and Indexed by

CIVILICA

We Respect the Science

این ژورنال تحت حمایت سیویلیکا می باشد و مقالات هر شماره آن پس از انتشار در پایگاه سیویلیکا نمایه سازی و منتشر می شود
مقالات نمایه شده درنظام رتبه بندی دانشگاهها و پژوهشگاههامورد تحلیل قرار میگیرد.

اطلاعات مجله

Electronic security Journal

صاحب امتیاز: محمد قلمچی

تاریخ ثبت: ۱۶ مهر ۱۴۰۴

مشاهده: ۱,۲۸۰

دریافت: ۶

زبان ژورنال: فارسی

ترتیب انتشار: فصلی

سال شروع انتشار: ۱۴۰۱

کداختصاصی ژورنال: JR_ELECT

موضوعات تحت پوشش فصلنامه امنیت الکترونیک

مهندسی برق و الکترونیک

تحلیل جامعه‌شناختی مقاومت اصناف و کسب‌وکارها در برابر سامانه پایش تطابق سنجی امنیت الکترونیک (سپتام)

نویسنده: مونا احمدی

مقاله حاضر با هدف تحلیل جامعه‌شناختی مقاومت اصناف و کسب‌وکارها در برابر «سامانه پایش تطابق سنجی امنیت الکترونیک (سپتام)» ارائه شده است. با اتکا به نظریه‌های کنش جمعی، سرمایه اجتماعی و سازه‌انگاری، این پژوهش نشان می‌دهد که مقاومت مذکور ریشه در سه دسته عوامل فرهنگی-اجتماعی (شکاف دانش و احساس تهدید حریم خصوصی)، ساختاری-نهادی (ضعف در اطلاع‌رسانی و اجبار بدون توضیح) و تحلیل قدرت (تقابل با شبکه‌های ذی‌نفع و بازتوزیع قدرت) دارد. این مطالعه نتیجه می‌گیرد که نادیده گرفتن زمینه اجتماعی اصناف، سامانه‌های نظارتی را با چالش مشروعیت و مقبولیت عمومی مواجه می‌سازد.

استقرار فناوری‌های نظارتی جدید در هر جامعه‌ای، به‌ویژه در بافت‌های اقتصادی–اجتماعی، همواره با چالش‌های پذیرش و اشکال مختلف مقاومت مواجه است [۱]. در ایران، نمونهٔ عینی این چالش را می‌توان در راه‌اندازی «سامانه سپتام» مشاهده کرد؛ طرحی ملی که با هدف استانداردسازی و یکپارچه‌سازی سامانه‌های نظارت تصویری در اماکن عمومی و خصوصی کلید خورد [۲]. اگرچه اهداف رسمی این سامانه، مشتمل بر ارتقای امنیت عمومی، ایجاد شفافیت اقتصادی و ساماندهی امور اصناف اعلام شد، اما در مرحلهٔ اجرا، بخش قابل‌توجهی از جامعهٔ اصناف در برابر آن موضع‌گیری کردند و مقاومت نشان دادند [۳].

این مقاله با اتکا بر یک رویکرد جامعه‌شناختی و با به‌کارگیری چارچوب نظریهٔ «کنش جمعی» و مفهوم «سرمایهٔ اجتماعی»، در پی تحلیل ریشه‌های این مقاومت است [۴]. پرسش محوری مقاله این است: با فرض اینکه اصناف خود از ذی‌نفعان اصلی برقراری نظم و امنیت به شمار می‌روند، چه دلایلی موجب شده است تا در برابر سیاستی که مدعی تحقق همین اهداف است، مقاومت کنند [۵]. فرضیهٔ پژوهش حاضر این است که این مقاومت را نمی‌توان صرفاً به عنوان واکنشی اقتصادی به «بهای» اجرای طرح تقلیل داد. بلکه این کنش جمعی، پاسخی است به «چگونگی» و «علت» اجرای طرح، که درک شده است به منزلهٔ تهدیدی برای «سرمایهٔ اجتماعی» (شبکه‌های اعتماد و روابط) و «اختیار عمل سنتی آنان» [۶].

چارچوب نظری

جامعه‌شناسی مقاومت در برابر فناوری‌های نظارتی، به عنوان حوزه‌ای انتقادی، به بررسی اشکال، زمینه‌ها و پیامدهای واکنش‌های جمعی و فردی در برابر نظام‌های نوین کنترل و حکمرانی تکنولوژیک می‌پردازد.
این رویکرد، مقاومت را نه یک مانع، بلکه یک پدیده اجتماعی کلیدی برای فهم تقابل میان تحولات فنی، بازسازی قدرت و دگرگونی اعتماد در بافت‌های اجتماعی جدید می‌داند.

نظریه‌ی کنش جمعی

بر اساس بنیان‌های نظریه کنش جمعی، که «رابرت پاتنام»، از چهره‌های شاخص آن است، افراد و گروه‌ها عموماً بر مبنای محاسبه عقلانی هزینه‌ها و فواید اقدام به کنش می‌کنند [۷].
در این چارچوب، مقاومت اصناف در برابر سامانه سپتام را می‌توان شکلی از «کنش جمعی» در واکنش به «کنش» حکمرانی دولتی تفسیر کرد [۸].
این مقاومت عمدتاً در شرایطی ظهور می‌یابد که هزینه‌های محاسبه‌شده تطبیق با سامانه شامل هزینه‌های مالی، زمانی و مهم‌تر از آن، هزینه‌های ناشی از کاهش استقلال عمل از منافع ادراک‌شده آن، همچون امنیت بالاتر یا مشروعیت حقوقی، پیشی گیرد [۹].
این تحلیل را می‌توان با مفهوم «سرمایه اجتماعی» تکمیل کرد. به باور پژوهشگرانی مانند مانکور اولسون، سرمایه اجتماعی بر پایه شبکه‌های روابط اجتماعی، هنجارهای اعتماد و عمل متقابل شکل می‌گیرد و بسترساز همکاری است.
پیاده‌سازی سامانه متمرکزی مانند سپتام، با ایجاد یک شبکه نظارتی رسمی و الزام‌آور، عملاً در تقابل با شبکه‌های سنتی اعتماد و همکاری درون‌صنفی (نظیر شبکه‌های خویشاوندی، صنفی و محلی) قرار گرفته است [۱۰].
بنابراین، مقاومت صورت‌گرفته را می‌توان پاسخی در جهت حفاظت از این سرمایه اجتماعی سنتی تفسیر کرد که معیارهای اعتبار و کنش در آن، پیش از این توسط منطق درونی جامعه اصناف تعریف می‌شد [۱۱].
به عبارت دیگر، تهدید احساس‌شده علیه این سرمایه اجتماعی، هزینه محاسبه‌شده کنش جمعی مقاومت را افزایش داد [۱۲].

سازه‌انگاری و هویت‌سازی

از منظر نظریه سازه‌انگاری در روابط بین‌الملل و جامعه‌شناسی سیاسی که بر ساخته‌شدگی اجتماعی واقعیت‌ها تأکید دارد، هویت‌ها و منافع کنشگران اموری ثابت و از پیش‌تعیین‌شده نیستند، بلکه در فرایند تعامل و به‌ویژه از طریق گفتمان‌ها ساخته و بازتولید می‌شوند [۱۳]. در مورد سامانه سپتام، یک تقابل گفتمانی کلیدی شکل گرفت: گفتمان رسمی حاکمیتی با برجسته‌سازی مفاهیمی چون «امنیت عمومی»، «شفافیت» و «قانونمندی» مطرح بود. در حالی که گفتمان مقاومت در میان برخی اصناف، بر مفاهیم "تحمیل"، "تعدی به حریم" و "فشار اقتصادی" متمرکز بود. این تقابل صرفاً یک اختلاف نظر در روش نبود، بلکه نبرد بر سر معناسازی و تعریف «وضعیت مطلوب» محسوب می‌شد. بر این اساس، مقاومت را می‌توان کنشی در جهت حفاظت از هویت جمعی موجود اصناف در برابر بازتعریف تحمیلی آن توسط یک گفتمان تکنوکراتیک دانست. این منازعه گفتمانی، مشروعیت طرح را به چالش کشید و زمینه را برای بسیج جمعی فراهم آورد [۱۴].

اقتصاد سیاسی فناوری

استقرار هر فناوری نوین را باید در چارچوب اقتصاد سیاسی مورد تحلیل قرار داد، چرا که دگرگونی‌های تکنولوژیک همواره با تحول در روابط قدرت و جابجایی منابع مادی و نمادین همراه هستند [۱۵]. راه‌اندازی سامانه سپتام را نیز می‌توان در این چارچوب تفسیر کرد. این طرح نه تنها ابزاری نظارتی، که عاملی برای شکل‌دهی به شبکه‌ای جدید از ذی‌نفعان رسمی (نظیر کارشناسان معتمد سامانه، آزمایشگاه‌ها و پیمانکاران تأییدشده) محسوب می‌شود. در مقابل، این تغییر بالقوه می‌تواند منافع اقتصادی شبکه‌های پیشین و غیررسمی فعال در حوزه نصب، نگهداری و فروش تجهیزات نظارتی را به چالش بکشد و به بازتنظیم بازار این خدمات منجر شود. بنابراین، مقاومت در برابر سپتام گواه بر بازتوزیع قدرت اقتصادی و امتیازات مرتبط با آن است [۱۶].

تحلیل یافته‌ها

مقاومت اصناف در برابر سامانه سپتام، پدیده‌ای چندبُعدی و برآمده از درهم‌تنیدگی عوامل مختلفی است که به بررسی آنها می‌پردازیم.

الف) عوامل فرهنگی-اجتماعی و بی‌اعتمادی

مقاومت اصناف در برابر استقرار سامانه‌هایی مانند «سپتام» را می‌توان در چارچوب عوامل فرهنگی-اجتماعی و مقوله بی‌اعتمادی ساختاری تحلیل کرد. یکی از محوری‌ترین دلایل این مقاومت، وجود شکاف دانش و ضعف فرهنگ‌سازی هدفمند است [۱۷]. برای بخش قابل‌توجهی از جامعه اصناف، کارکرد واقعی، مزایای اقتصادی-امنیتی و ضرورت این سامانه به‌درستی تبیین نشده است. درنتیجه، این ابزار نه به‌عنوان یک مکانیسم بهبوددهنده، بلکه در ذهنیت آنان به ابزاری بوروکراتیک تقلیل یافته است که صرفاً بر پیچیدگی‌های اداری و هزینه‌های مالی می‌افزاید [۱۸]. این نگرش، عمدتاً ریشه در ضعف فرایند اطلاع‌رسانی، فرهنگ‌سازی شفاف و فراگیر از سوی نهادهای متولی دارد که به‌جای ایجاد باور و مشارکت، به دامنه بی‌اعتمادی دامن می‌زند [۱۹].

ب) احساس تهدید حریم خصوصی و استقلال کسب‌وکار

تمرکز داده‌های تصویری در یک سامانه ملی، این نگرانی را ایجاد می‌کند که حریم خصوصی مشاغل در خطر قرار گیرد و داده‌ها ممکن است فراتر از هدف اصلی (امنیت) مورد استفاده قرار گیرند [۲۰]. این احساس که «چشم دولت» به داخل کسب‌وکارشان نفوذ کرده، یک عامل فرهنگی قدرتمند در ایجاد مقاومت است [۲۱].

ج) عوامل ساختاری-نهادی و شیوه اجرا

راهبرد دستوری و آمرانه در ابلاغ الزامات سامانه سپتام، بدون تبیین منطق و فراهم‌آوردن سازوکارهای تسهیل‌گر، نقش بسزایی در تقویت مقاومت اصناف ایفا می‌کند [۲۲]. رویکردی که در آن مجریان، به جای گفتمان و ایجاد بسترهای حمایتی (نظیر تسهیلات مالی کم‌بهره یا دوره‌های توانمندسازی)، صرفاً به ابلاغ دستور و تکلیف می‌پردازند. چنین روندی این احساس را در جامعه هدف ایجاد می‌کند

که تصمیمی یک‌سویه بر آنان تحمیل شده است، نه اینکه با آنان مشورت شده باشد. این دریافت، واکنش‌های منفی و مقاومت فعال را به پاسخی طبیعی و قابل‌انتظار بدل می‌سازد [۲۳].

یکی دیگر از کانون‌های مقاومت، عدم شفافیت مالی و ابهام در مدل درآمدی سامانه است [۲۴]. برای اصناف این پرسش اساسی بی‌پاسخ مانده است که عواید حاصل از هزینه‌های پرداختی، دقیقاً به چه مقاصدی تخصیص می‌یابد و ذی‌نفعان اصلی این فرایند چه اشخاص یا نهادهایی هستند [۲۵]. این ابهام در تخصیص منابع و انباشت درآمدها، نه‌تنها معیاری برای ارزیابی عادلانه‌بودن هزینه‌ها در اختیار آنان نمی‌گذارد، بلکه به‌عنوان بستری برای گسترش شایعات و تعمیق بی‌اعتمادی عمل می‌کند. در واقع، فقدان شفافیت، فضای لازم برای شکل‌گیری تفسیرهای منفی و بدبینانه را به‌طور کامل فراهم می‌سازد.

نتیجه‌گیری

مقاومت اصناف در برابر سامانه سپتام را باید پدیده‌ای چندوجهی و پیچیده تلقی کرد که برآمده از درهم‌تنیدگی عوامل گوناگون است. این عوامل در سطوح فرهنگی–اجتماعی از جمله بی‌اعتمادی تاریخی و شکاف دانش، ساختاری نظیر رویکرد آمرانه و ضعف در اطلاع‌رسانی و همچنین در عرصه رقابت گروه‌های ذی‌نفع قابل ردیابی هستند.

از نگاه جامعه‌شناختی، موفقیت یک فناوری نظارتی در گرو عبور از چالش اجتماعی پذیرش آن است. بر این اساس، عامل تعیین‌کننده در شکست طرح‌های مذکور، غفلت از این بستر اجتماعی و نه لزوماً مشکلات فنی ارزیابی می‌شود. هنگامی که ذی‌نفعان کلیدی یک طرح (یعنی اصناف) نه به عنوان شرکای فعال و دارای اراده، بلکه در جایگاه اجراکنندگان بی چون و چرای حکمرانی تصور شوند، شکل‌گیری مقاومت پیامدی اجتناب‌ناپذیر خواهد بود. این مطالعه نشان می‌دهد که مشروعیت، پیش‌شرط کارآمدی است. هیچ سامانه نظارتی، صرف نظر از میزان پیچیدگی و پیشرفت فنی آن، بدون کسب مقبولیت اجتماعی و جلب اعتماد فعالانه ذی‌نفعان، محکوم به ناکامی است.

منابع

[1] M. Foucault, Discipline and Punish: The Birth of the Prison. Paris, France: Gallimard, 1977.

[۲] روزنامه ایران، «طرح سپتام تصویب شد»، ۱۴۰۰.

[۳] روزنامه دنیای اقتصاد، «واکنش اصناف به الزامات سپتام»، ۱۴۰۱.

[4] M. S. Granovetter, "ش pp. –1360 1973 ,1380.

[5] A. Giddens, The Constitution of Society: Outline of the Theory of Structuration. Berkeley, CA, USA: University of California Press, 1984.

[6] P. Bourdieu, "The forms of capital," in Handbook of Theory and Research for the Sociology of Education, J. G. Richardson, Ed. Westport, CT, USA: Greenwood Press, 1986, pp. 258–241.

[7] R. D. Putnam, Making Democracy Work: Civic Traditions in Modern Italy. Princeton, NJ, USA: Princeton University Press, 1993.

[8] C. Tilly, From Mobilization to Revolution. Reading, MA, USA: Addison-Wesley, 1978.

[9] E. Ostrom, Governing the Commons: The Evolution of Institutions for Collective Action. Cambridge, UK: Cambridge University Press, 1990.

[10] M. Olson, The Logic of Collective Action: Public Goods and the Theory of Groups. Cambridge, MA, USA: Harvard University Press, 1965.

[11] J. S. Coleman, "Social capital in the creation of human capital," American Journal of Sociology, vol. 94, pp. S95–S1988 ,120.

[12] F. Fukuyama, Trust: The Social Virtues and the Creation of Prosperity. New York, NY, USA: Free Press, 1995.

[13] A. Wendt, "Anarchy is what states make of it: The social construction of power politics," International Organization, vol. 46, no. 2, pp. –391 1992 ,425.

[14] R. Freeman, "Resistance in the age of digital surveillance," Surveillance & Society, vol. 18, no. 2020 ,1.

[15] G. T. Marx, "What's new about the 'new surveillance'? Classifying for change and continuity," Knowledge, Technology & Policy, vol. 15, no. 3, pp. 2002 ,29–9.

[16] S. Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York, NY, USA: PublicAffairs, 2019.

[17] J. C. Scott, Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed. New Haven, CT, USA: Yale University Press, 1998.

[18] J. Habermas, The Theory of Communicative Action, vol. 1. Boston, MA, USA: Beacon Press, 1981.

[۱۹] انجمن دفاع از حقوق شهروندی، «نگرانی‌های حریم خصوصی در سپتام»، ۱۴۰۲.

[20] D. Lyon, Surveillance Society: Monitoring Everyday Life. Buckingham, UK: Open University Press, 2001.

[۲۱] پژوهشکده مطالعات فرهنگی و اجتماعی، «تحلیل شیوه اجرای سپتام»، ۱۴۰۲.

[22] M. S. Archer, Realist Social Theory: The Morphogenetic Approach. Cambridge, UK: Cambridge University Press, 1995.

[۲۳] پایگاه خبری اقتصاد ایران، «شفافیت در درآمدهای سپتام»، ۱۴۰۲.

[24] B. Rothstein, "Institutions, social trust, and capital," Political Studies, vol. 48, no. 1, pp. 2000 ,20–1.

[25] M. E. Warren, Democracy and Trust. Cambridge, UK: Cambridge University Press, 1999.

سپتام

سامانه پایش تصویری اماکن

توسعه خدمات سپتام

رشد تولیدات تجهیزات نظارت تصویری و رونق عرضه در بازار کشور مطابق با استانداردهای جهانی را به همراه دارد.

saptam.ir

+۹۸ ۲۱-۲۲۹۴۸۸۶۸

+۹۸ ۲۱-۲۲۹۶۷۷۶۹

www.electronicsecurity.ir

info@electronicsecurity.ir