فصلنامه علمی - پژوهشی فرماندهی و کنترل، سال هفتم، شماره دو، تابستان ۱۴۰۲

ارایه الگوی تاب‌آوری سامانه‌های فرماندهی و کنترل در مقابل تهدیدهای سایبری

دکتر علی محمد امین زاده[1*]، دکتر رسول رمضانی دهقی[2]

تاریخ دریافت: ۱۴۰۰/۰۳/۰۹ تاریخ پذیرش: ۱۴۰۱/۰۹/۲۶

چکیده

رشد سریع فناوری‌ها و حرکت به سمت انقلاب صنعتی چهارم و بهره‌گیری از مزایای فضای سایبر، با وجود مزایای فراوانی که برای جامعه نوین به همراه داشته است، اما موجب افزایش آسیب‌پذیری‌های موجود و بروز حملات سایبری به سامانه‌های فرماندهی و کنترل شده است. حفظ عملیات اصلی سامانه و پایداری مناسب در زمان حمله سایبری و بازگشت به حالت اولیه پس از حمله سایبری، یکی از اصلی‌ترین راهبردها در مواجهه با تهدیدات سایبری می‌باشد. ارایه الگوی تاب آوری سامانه های فرماندهی و کنترل در مقابل تهدیدهای سایبری مبتنی بر مدل یکپارچه سازی مدل بلوغ توانایی و مدل بهبود فرآیندها، برای سه سطح راهبری، کنترل و عملیات سامانه‌های فرماندهی و کنترل هدف اصلی این پژوهش می‌باشد. پژوهش حاضر از لحاظ نوع تحقیق در زمره تحقیقات بنیادی و کاربردی دسته بندی میگردد و با بررسی مبانی علمی یک الگوی جدید برای شناسایی و مدیریت آسیب پذیریها و مواجهه با رخدادهای سایبری ارایه می‌نماید. نتیجه اصلی این پژوهش ارائه الگوی تاب آوری سامانه‌های فرماندهی و کنترل در مقابل تهدیدهای سایبری در سه بعد رهبری، بعد نظارت و کنترل و بعد عملیات مبتنی بر مدل بلوغ ۵ سطحی می‌باشد. در الگوی ارائه شده در سطح بلوغ یک (اجرایی) ۱۰ مولفه ، در سطح بلوغ دو (برنامه‌ریزی) ۱۲ مولفه، درسطح بلوغ سه (مدیریت) ۱۲ مولفه، درسطح بلوغ چهار (اندازه گیری) ۹ مولفه و در بلوغ سطح پنج (نهادینه) ٦ مولفه و در مجموع ٤٩ مولفه احصاء و ارایه شده است.

برای تایید الگوی ارایه شده پس از انجام مصاحبه با خبرگان حوزه فرماندهی و کنترل با بهره‌گیری از نرم‌افزار اسمارت پی.ال.اس، تحلیل بار عاملی و آزمون معنی‌دار بودن مولفه‌ها انجام و الگوی ارایه شده در سطح ۹۵ درصد معنی‌داری مورد تایید قرار گرفته است.

واژگان کلیدی: تاب‌آوری سایبری، سامانه‌های فرماندهی و کنترل، بلوغ توانایی، بهبود فرآیندها.

۱. دکترای مدیریت راهبردی دانشگاه عالی دفاع ملی mo.aminzadeh@gmail.com (نویسنده مسئول)

۲. دکترای مدیریت راهبردی، عضو هیئت علمی دانشگاه پدافند هوایی خاتم الانبیاء(ص) sepehrramezany@yahoo.com

۱. کلیات

۱.۱. مقدمه

امروزه امنیت سایبری به طور گسترده‌ای در سطح جهانی در کانون توجه و اهمیت قرار دارد. بر همین اساس عوامل تاثیر گذار در امینت سایبری افزایش پیدا کرده و می‌توان عوامل موثر بر امنیت سایبر را در یکی از از سه وجه ذیل دسته‌بندی نمود: تهدیدات خارجی، تهدیدات داخلی و سیاست‌های اجرایی در بکارگیری فناوری‌های نوین.

از طرفی نگرانی‌های سازمان‌های دولتی، شرکت‌های بخش خصوصی و موسسات علمی از تهدیدات خارجی ناشی از دسترسی به اطلاعات حساس، خرابکاری اینترنتی و حملات انکار سرویس توسط طیف هکرها، جنایتکاران، تروریست‌ها و بازیگران دولتی رو به افزایش است. سال‌های ۲۰۱۹ و ۲۰۲۰ سرشار از حوادث سایبری بود. مطابق با جزئیات منتشر شده در تریتون در خصوص حملات سایبری، بدافزارهایی نظیر استاکس‌نت و ایندااسترووور، بیشترین حملات را به تجهیزات سامانه‌های فرماندهی و کنترل را داشته‌اند و علاوه بر این، حملاتی با مشخصات بالا به شرکت‌های صنعتی ضربه‌های شدیدی را وارد نموده‌اند. بوئینگ اعلام کرده که توسط بدافزار واناکرای مورد حمله قرار گرفته و چند ماه بعد، همین ویروس کارخانه‌های شرکت تولیدی نیمه هادی تایوان را به خاموشی کشاند. اگرچه این حملات زیرساخت‌های فناوری اطلاعات را مورد هدف قرار دادند، اما پیامدهای آن‌ها بر فناوری عملیاتی مورد استفاده برای تولید نیز تاثیر گذاشت. در واقع، مهاجمان برای ایجاد اختلال در شرکت‌های صنعتی همیشه به دانش خاصی نیاز ندارند [۵].

پس از سوء استفاده از آسیب‌پذیری‌ها در زیرساخت‌های فناوری اطلاعات، هکرها می‌توانند به شبکه دسترسی پیدا کنند. طبق تحقیقات انجام شده، یک مهاجم داخلی که از قبل بر روی سامانه اطلاعاتی شرکت دسترسی داشته است، در اغلب موارد قادر خواهد بود به شبکه نفوذ کند. مهاجمین از روش‌های گوناگونی برای انجام اقدامات مخرب بر روی اجزای مختلف سامانه‌های فرماندهی و کنترل بهره می‌گیرند که متداول‌ترین آن روش‌ها سوء استفاده از آسیب‌پذیری‌های شناخته شده است. شناسایی آسیب‌پذیری‌های موجود در تجهیزات سامانه‌های فرماندهی و کنترل بسیار مهم است، زیرا این امر به مشاغل اجازه می‌دهد مخاطرات را به موقع ارزیابی کرده و اقدامات حفاظتی مناسبی را انجام دهند [٦].

۲.۱. بیان مسئله

یک مهاجم داخلی که از قبل به سامانه اطلاعاتی یک سازمان دسترسی داشته باشد، در ۸۲ درصد موارد می‌تواند به شبکه نفوذ کرده و از آسیب‌پذیری‌های موجود در سامانه‌های فرماندهی و کنترل برای تخریب و آسیب رساندن به فرایندهای اساسی سامانه، بهره‌برداری نماید [٤]. وجود محدودیت‌های ناشی از تحریم‌های بین المللی به ویژه در بخش دفاعی/امنیتی کشور و وابستگی به سامانه‌های فرماندهی و کنترل غیر بومی که اغلب ناامن و آسیب‌پذیر می‌باشند از یک طرف و افزایش تهدیدات سایبری ناشی از توسعه فناوری‌های سایبری که اغلب ناشناخته می‌باشند از طرف دیگر، احتمال شکست امنیتی در سامانه‌های فرماندهی و کنترل را افزایش داده و تداوم عملیات دفاعی و نظامی را با مخاطره مواجه نموده است. با توجه به اینکه بهبود فرایندهای امنیت سایبری نقش مهمی در کاهش شکست‌های امنیتی سامانه‌های فرماندهی و کنترل دارد، این پژوهش با ارایه الگوی افزایش تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل در مقابل تهدیدهای سایبری مبتنی بر بهبود فرایندها به دنبال ارایه پاسخی مناسب جهت افزایش تاب‌آوری سامانه‌های فرماندهی و کنترل در مواجهه با تهدیدات روزافزون سایبری می‌باشد. به این منظور هدف اصلی این پژوهش دستیابی به الگوی تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل در مقابل تهدیدهای سایبری بوده و سوال اصلی پژوهش این است که الگوی تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل در مقابل تهدیدهای سایبری کدام است؟

۳.۱. اهمیت و ضرورت تحقیق

با عنایت به اینکه پس از وقوع یک حمله سایبری، تداوم عملیاتی سامانه‌های فرماندهی و کنترل از اهمیت بالایی برخوردار است، انجام این پژوهش الگوی مناسبی را به منظور ارتقاء تاب‌آوری سامانه‌های فرماندهی و کنترل در اختیار سازمان‌های دفاعی قرار می‌دهد تا علاوه بر ادامه فعالیت‌های

اساسی، در کمترین زمان ممکن نسبت به بازگشت به حالت پیش از حمله سایبری احتمالی، اقدام نمایند.

فقدان یک مدل راهبری مناسب جهت تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل، ضمن کاهش تداوم عملیاتی سامانه‌های فرماندهی و کنترل در مواجهه با تهدیدهای سایبری نوین، موجب تحمیل هزینه‌های هنگفت به سیستم جهت بازگشت به وضعیت پیش از حمله خواهد شد.

٤.١. پیشینه پژوهش

للانسو و همکاران (۲۰۲۱)، در مقاله‌ای تحت عنوان وضعیت تاب‌آوری سایبری: اکنون و در آینده، به بررسی وضعیت سایبری در حال حاضر پرداخته و تکنیک‌های انعطاف‌پذیری سایبری را به عنوان مکمل دفاع سایبری سنتی جهت کمک به اطمینان از انجام کامل ماموریت معرفی می‌نماید [١٤].

کاریاس و همکاران (۲۰۲۰)، در مقاله‌ای تحت عنوان مدل پیشرفت تاب‌آوری سایبری، مدلی را برای کمک به شرکت‌ها جهت اجرای استراتژی‌های تدوین شده و همچنین اولویت‌بندی سیاست‌های انعطاف‌پذیری سایبری مبتنی بر یافتن نقاط شروع و تکامل طبیعی سیاست‌ها در طول زمان ارایه می‌دهد [۱۳].

مظفری و همکاران (۲۰۱۹)، در مقاله‌ای تحت عنوان احصاء شاخص‌های تاب‌آوری برکاهش آسیب‌پذیری سیستم های کنترل صنعتی در تهدیدات سایبری، شاخص‌های حس تشخیص، اجرای اقدامات کنترلی در عملیات روزمره، توسعه توابع نظارتی(کنترل های اینترنتی، بخش قانونی، مدیریت ریسک و امنیت سایبری)، استفاده قوی از بخش ممیزی داخلی و واکنش و ترمیم، را جهت کاهش آسیب‌پذیری سیستم‌های کنترل صنعتی در مقابل تهدیدات سایبری احصاء نموده است [۲].

بت‌شکن (۱۳۹٦)، در مقاله‌ای تحت عنوان بررسی مهندسی تاب‌آوری در فضای سایبری، بیان می‌دارد که اقداماتی از قبیل اعمال کنترل‌های تکنیکی و تنظیمات شبکه، استفاده از دستگاه و رایانه‌های اختصاصی و منفرد با امنیت بیشتر و همچنین داشتن شبکه با دسترسی اختصاصی برای انجام تنظیمات ابزارها، سخت افزارهای شبکه و سرورها، موجب افزایش تاب‌آوری سایبری سازمان‌ها در مقابل تهدیدات سایبری خواهد شد [۱].

۲. مبانی نظری تحقیق

۱.۲. سامانه فرماندهی و کنترل

فرماندهی و کنترل شامل برنامه‌ریزی، هدایت، هماهنگی و کنترل عملیات، مبتنی بر اجرای موثر سناریوی عملیاتی می‌باشد. در راستا، تکامل فناوری اطلاعات به نحو فزاینده‌ای به نیروهای نظامی اجازه خواهد داد که اشکال سنتی عملیات اطلاعاتی را با منابع پیچیده اطلاعاتی، نظارت و تجسس در قالب یک حرکت اطلاعاتی، هماهنگ نمایند. توسعه یک مفهوم با عنوان شبکه اطلاعات جهانی، محیط شبکه‌ای لازم برای دستیابی به این هدف را فراهم می‌سازد. این شبکه در سراسر جهان گسترده شده، پایانه‌های اطلاعاتی و افراد را به یکدیگر مرتبط ساخته، پردازش‌ها را یکپارچه نموده و اطلاعات مورد نیاز جنگجویان، تصمیم‌سازان و پرسنل پشتیبانی کننده را فراهم نموده و قدرت رزم را افزایش می‌دهد و به موفقیت عملیات نظامی کمک می‌کند [۳].

فرماندهی و کنترل مؤثرترین اقدام به‌ویژه در زمانی است که برتری تصمیم‌گیری مد نظر است. برتری تصمیم‌گیری از برتری اطلاعاتی ناشی می‌شود بنابراین یک فرمانده باید آخرین تحولات صحنه نبرد را مد نظر داشته باشد و دستورات لازم را برای مقابله با متغیرهای پیش‌بینی نشده صادر کرده و برای نیروهای عملیاتی ارسال و بر فرآیند عملیات اشراف کامل داشته باشد. با این وجود، ارسال کلیه داده‌های جمع‌آوری شده از تمامی حساسه‌ها به راس هرم تصمیم‌گیری، سامانه فرماندهی و کنترل را در هر لحظه با حجم انبوهی از داده‌ها و اطلاعات مختلف مواجه می‌نماید که این امر موجب کاهش تمرکز و قدرت پردازش و تصمیم‌گیری خواهد شد. لذا به طور معمول برای سامانه‌های فرماندهی و کنترل، سه سطح اصلی به صورت زیر در نظر گرفته می‌شود:

الف. سطح اول که در بالای ساختار قرار دارد مربوط به نیروهای انسانی یا اپراتورها هستند که وظیفه پایش، نظارت و پردازش داده‌ها از طریق سنسورها به صورت مستقیم و کنترل آن‌ها با استفاده از محرک‌ها را برعهده دارند.

ب. سطح دوم که سطح میانی آن است مربوط به لایه اتوماسیون می‌باشد. در این لایه، سامانه فرماندهی و کنترل واقع در مرکز، وظیفه جمع‌آوری بی‌وقفه داده‌ها از فرآیندهای پردازش شده

توسط سنسورها، ارایه داده‌های وضعیت و تشخیص به اپراتورها از طریق رابط ماشین و انسان، دریافت دستورات و تنظیمات از اپراتورها و کنترل فرآیندهای کنترل شده از طریق سنسورها را برعهده دارد.

ج. سطح سوم، سطح نهایی است که مرتبط با لایه پردازش یا فرآیند است. در این لایه، فرآیندها از طریق حساسه‌های مختلف پایش و نظارت شده و به وسیله محرک‌ها کنترل می‌شوند [۱۲].

۲.۲. آسیب‌پذیری‌های سامانه‌های فرماندهی و کنترل

در طی سال‌های گذشته آسیب‌پذیری‌های سامانه‌های فرماندهی و کنترل با تغییر فناوری به طور دایم در حال تغییر بوده و به عوامل مختلفی وابستگی داشته است. یکی از مهم‌ترین این عوامل، مشکلات ناشی از مهاجرت این سامانه‌ها به شبکه‌های انتقال/اینترنت می‌باشد. سامانه‌های جمع‌آوری و کنترل یکپارچه داده‌ها[۳] و کنترل توزیع[۴] شده، اغلب بر روی پروتکل‌های پیچیده اجرا می‌شوند اما در شرایط توسعه‌ای جدید، پروتکل‌های کنترل و گزارش آنالوگ در پروتکل‌های دیجیتال جاسازی شده و محدودیت‌های یکپارچگی، رمزگذاری برروی پروتکل انتقال/ اینترنت مشکلات را تشدید کرده است.

از طرفی استفاده از فناوری‌های بی‌سیم امکان حملات بیشتر به سامانه‌های فرماندهی و کنترل را فراهم آورده است. ابزارها و نرم‌افزارهای جدیدی برای حمله و سرقت اطلاعات در هر فرستنده رادیویی ظهور یافته و قالب جدیدی برای شکل دادن به اطلاعات مربوط به نرم‌افزار بسته‌های رادیویی شکل گرفته و آسیب‌پذیری‌های جدیدی به طور مداوم کشف می‌شوند. به عنوان مثال، تست امنیتی از طریق تزریق اطلاعات نامعتبر، غیر منتظره و یا تصادفی (مانند فازینگ[۵]) ده‌ها آسیب‌پذیری را در سامانه‌های زیربنایی بحرانی کشف کرده است. اکثر این سامانه‌ها برای انجام کارهای درست با داده‌های معمول طراحی شده‌اند و برنامه‌ریزی دفاعی کمی دارند. بهره برداری می‌تواند از طریق دسترسی فیزیکی به شبکه‌ها و یا از طریق تکنیک‌هایی مانند وارد کردن رمز عبور بی‌قاعده، هک دستگاه‌های متصل به اینترنت، فیشینگ و ... اجرا شود [۸].

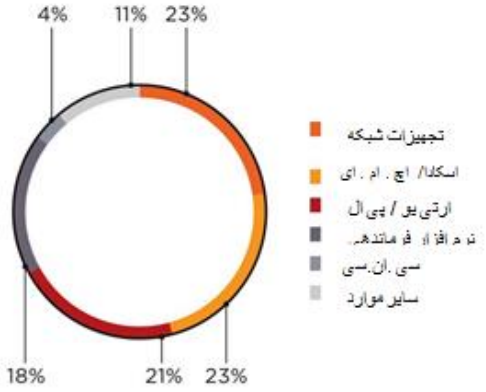
در سال‌های اخیر علاوه بر آسیب‌پذیری‌های نرم‌افزاری، انواع آسیب‌پذیری‌های سخت‌افزاری و سفت‌افزاری نیز به شدت بر روی امنیت سامانه‌های فرماندهی و کنترل تاثیر داشته است. این آسیب‌پذیری‌ها در پردازنده‌ها و قطعات الکترونیکی به طور گسترده وجود دارند و حتی در سطوح مخابرانی و یا نظامی نیز یافت می‌شوند. نمونه بارزی از این آسیب‌پذیری‌ها، وجود یک نقطه دسترسی مخفی در تراشه‌های ساخت یک شرکت چینی است که در تجهیزات نیروی هوایی آمریکا کاربرد داشته و توسط تیم تحقیقات دانشگاه کمبریج شناسایی گردید. سامانه‌های کنترل و فرماندهی در این بخش شامل تجهیزات الکترونیکی و پردازشی متنوعی است که از جمله مهم‌ترین این تجهیزات، عملگرها، حساسه‌ها، سامانه‌های کنترلی قابل برنامه‌ریزی[۶] و واحدهای ارتباط از راه دور[۷] است. مهاجمان با دسترسی به کد نرم‌افزاری و یا سفت‌افزاری این تجهیزات، می‌توانند به راحتی به سامانه‌های کنترل و فرماندهی نفوذ کرده و کنترل سامانه را در دست گیرند.

یکی از آخرین پژوهش‌های انجام شده در این خصوص که در دانشگاه کارولینای جنوبی انجام شده است، به آسیب‌پذیری کدهای کنترل کننده‌های منطقی برنامه‌ریزی شده[۸] اختصاص دارد و حاکی از ضعف شدید این ابزارها در حوزه امنیت سایبری است. از جمله آسیب‌پذیری‌های عنوان شده در این خصوص به واحدهای ارتباط از راه دور[۹] سامانه مربوط می‌شود که از طریق تایید ورودی نامناسب و غیر ایمن این تجهیزات منجر به نفوذ مهاجم به سامانه فرماندهی و کنترل می‌گردد [۷].

بررسی آماری آسیب‌پذیری‌های سایبری سامانه‌های فرماندهی و کنترل نیز حایز اهمیت بالایی است. همانگونه که در (شکل ۱) مشاهده می‌شود در سال‌های اخیر توزیع آسیب‌پذیری‌های سایبری بر اساس نوع مؤلفه سامانه‌های فرماندهی و کنترل به طور قابل توجهی تغییر یافته است. اکثر این آسیب‌پذیری‌ها تقریبا به طور مساوی بین حساسه‌ها، نرم‌افزارها، آر.تی.یو/ پی.ال.سی

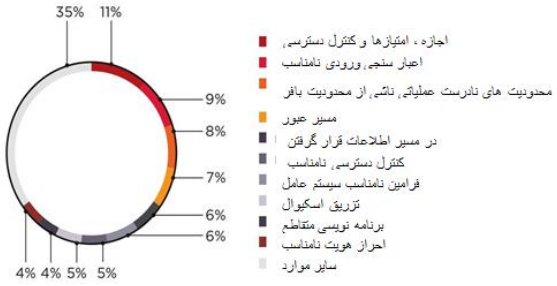
۳. SCADA
۴. DCS
۵. fuzzing
۶. PLC
۷. RTU
۸. PLC
۹. RTU

و تجهیزات شبکه توزیع شده‌اند.



شکل ۱. آسیب‌پذیری در انواع مؤلفه سامانه‌های فرماندهی و کنترل.

(شکل ۲) توزیع آسیب‌پذیری‌های مهم اجزای مختلف سامانه‌های فرماندهی کنترل را نشان می‌دهد که بخش قابل توجهی از این آسیب‌پذیری‌ها مربوط به احراز هویت نادرست یا امتیازات بیش از حد است. نکته قابل توجه آن است که بیش از نیمی از این آسیب‌پذیری‌ها (٦٤٪) از راه دور قابل استفاده می‌باشند [۹].



شکل ۲. انواع آسیب‌پذیری در اجزای سامانه‌های فرماندهی و کنترل.

۳.۲. مدیریت آسیب‌پذیری مهم‌ترین عامل در افزایش تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل

هدف اصلی مدیریت آسیب‌پذیری دارایی‌ها، شناسایی، تجزیه و تحلیل و مدیریت آسیب‌پذیری‌ها در محیط عملیاتی ارایه خدمات حیاتی می‌باشد. آسیب‌پذیری یکی از حساسیت‌های مهم در عملکرد صحیح تجهیزات و ارایه خدمات حیاتی مربوطه در زمان اختلال می‌باشد. از آنجایی که آسیب‌پذیری‌ها می‌توانند به خطرات عملیاتی منجر شوند، باید شناسایی و مدیریت شوند تا از وقوع اختلال در محیط عملیاتی خدمات حیاتی جلوگیری شود. یک فرآیند مدیریت آسیب‌پذیری باید قبل از بهره‌برداری از آسیب‌پذیری‌ها شناسایی و تحلیل شود و سامانه را در فرآیند مدیریت ریسک تحلیل و آگاه نماید. دامنه مدیریت آسیب‌پذیری شامل چهار اقدام اصلی به شرح (جدول ۱) می‌باشد [٦]:

جدول ۱. ارزیابی و توسعه تاب‌آوری در مقابل تهدیدات سایبری.

اقدام اصلی	اقدام فرعی
آماده سازی برای تجزیه و تحلیل آسیب پذیری‌ها و فعالیت‌های لازم برای حل و فصل آن‌ها	تجزیه و تحلیل آسیب‌پذیری و ارایه راهبردهای حل و فصل مسئله
	وجود مجموعه‌ای از ابزارها و روش‌های استاندارد برای شناسایی آسیب‌پذیری
	وجود یک مجموعه استاندارد از ابزارها و روش‌ها برای تشخیص کد مخرب
	وجود مجموعه‌ای از ابزارها و روش‌های استاندارد برای تشخیص کدهای غیر مجاز
	وجود یک مجموعه استاندارد از ابزارها و روش‌ها برای نظارت بر دارایی‌ها برای پرسنل غیر مجاز، اتصالات، دستگاه‌ها و نرم‌افزار
ایجاد و حفظ روند شناسایی و تجزیه و تحلیل آسیب پذیری‌ها	شناسایی منابع اطلاعات آسیب‌پذیر
	اطلاعات از این منابع در جریان است.
	آسیب‌پذیری‌ها فعالانه کشف می‌شوند.
	دسته بندی و اولویت‌بندی آسیب‌پذیری‌ها
	تجزیه و تحلیل آسیب‌پذیری‌ها برای تعیین ارتباط با سازمان
	استفاده از مخزن برای ضبط اطلاعات در مورد آسیب‌پذیری‌ها و حل و فصل آن‌ها
شناسایی اقدامات لازم جهت مدیریت مواجهه با آسیب پذیری‌ها	اقدامات در خصوص مدیریت مواجهه با آسیب‌پذیری‌های شناسایی شده
	اثربخشی کاهش آسیب‌پذیری بررسی شده است.
	وضعیت آسیب‌پذیری‌های حل نشده تحت نظارت است.
بررسی علل ریشه‌ای آسیب پذیری‌ها	علل اصلی آسیب‌پذیری‌ها (از طریق تجزیه و تحلیل علل ریشه یا روش‌های دیگر) شناسایی شده و مورد توجه قرار می‌گیرند.

٤.۲. مدل یکپارچه سازی بلوغ توانایی

مدل یکپارچه سازی بلوغ توانایی[10] روشی مبتنی بر بلوغ سازمان است که برای تاب‌آور نمودن سازمان و سامانه‌ها در مقابل تهدیدات سایبری قابل استفاده می‌باشد به طوری که با اجرای کامل مدل در سازمان تاب‌آوری نهادینه می‌شود. نهادینه سازی بدان معنی است که شیوه‌های تاب‌آوری سایبری تبدیل به یک بخش عمیق‌تر و پایدارتر از سازمان گردد. هرچه شیوه‌های سایبری تاب‌آوری بیشتر نهادینه شوند، مدیران می‌توانند اعتماد بیشتری نسبت به پیش‌بینی و قابلیت اطمینان عملی داشته باشند. این شیوه‌ها در طول زمان باعث اختلال یا استرس بیشتر به سازمان نیز می‌شوند. بلوغ نیز می‌تواند منجر به تطبیق تنگاتنگی بین فعالیت‌های امنیتی سایبری و هدایت کنندگان کسب و کار سازمان شود. به عنوان مثال، در سازمان‌های بالغ‌تر، مدیران نظارت بر حوزه خاص را تأمین می‌کنند و اثربخشی فعالیت‌های امنیتی را ارزیابی می‌کنند. در (جدول ۲) مقیاس ارزیابی سطح بلوغ با استفاده از پنج سطح بلوغ ارایه شده است.

جدول ۲. ارزیابی بلوغ تاب‌آوری سایبری.

سطوح بلوغ	اقدام
اول (انجام شده)	همه شیوه‌هایی که از اهداف در یک دامنه پشتیبانی می‌کنند، به صورت اندازه‌گیری شده با پاسخ به سوالات مدل ارزیابی و توسعه تاب‌آوری مربوطه انجام می‌شود.
دوم (برنامه‌ریزی شده)	یک تمرین خاص در حوزه مدل ارزیابی و توسعه تاب‌آوری انجام می‌شود و توسط برنامه‌ریزی، ذینفعان و استانداردها و رهنمودهای مربوطه نیز پشتیبانی می‌شود. یک فرآیند یا تمرین برنامه‌ریزی شده است که: • توسط سازمان از طریق سیاست و یک برنامه مستند ایجاد شده باشد. • توسط سهامداران پشتیبانی شود • توسط استانداردها و دستورالعمل های مربوطه پشتیبانی شود.
سوم (مدیریت شده)	تمام اقدامات در یک دامنه انجام می‌شود، برنامه‌ریزی شده، و زیرساخت‌های حاکمیت پایه‌ای برای حمایت از این فرآیند وجود دارد. یک فرآیند یا عمل در صورتی مدیریت‌شده است که: • توسط سازمان مدیریت شود • از کارکنان مناسب و افراد واجد شرایط استفاده شود. • به اندازه کافی تامین مالی شود. • برنامه مشخص مدیریت ریسک را داشته باشد.
چهارم (اندازه‌گیری شده)	تمام اقداماتی که در یک دامنه انجام، برنامه‌ریزی، مدیریت، نظارت و کنترل می‌شود در یک فرآیند مشخص اندازه‌گیری می‌شود و موارد ذیل می‌بایست رعایت شود. • به صورت دوره‌ای اثربخشی ارزیابی شود. • به طور عینی در مقایسه با شرح و برنامه عملی خود ارزیابی انجام پذیرد. • به صورت دوره‌ای با مدیریت سطح بالاتر موارد اقدام شده، بررسی شود.
پنجم (نهادینه شده)	تمام اقدامات در یک دامنه انجام، برنامه‌ریزی، مدیریت، اندازه‌گیری و سازگاری در همه حوزه‌های انتخابی در یک سازمان علاقه‌مند به عملکرد تاب‌آوری هستند انجام می‌شود. سطح بلوغ پنجم ، فرآیند یا عملی است که: • توسط سازمان و واحدهای عملیاتی درونی سازمان برای استفاده طراحی و تعریف شده است • اطلاعات پشتیبانی شده و بهبود یافته از میان واحدهای عملیاتی برای به انتفاع کلی سازمان جمع آوری شده است.

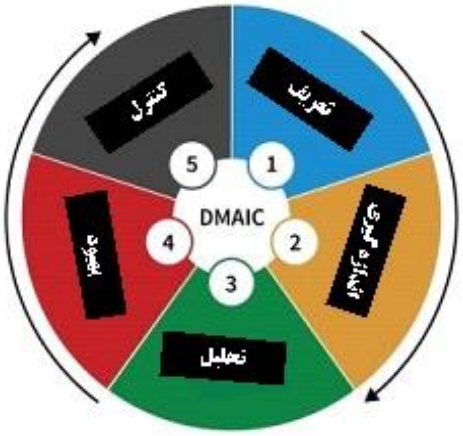
در روش فوق، یک سازمان تنها زمانی می‌تواند به یک سطح بلوغ بالاتری برسد که به تمام سطوح بلوغ پایین‌تر دست یافته باشد. به عبارت دیگر، یک سازمان که تمام اقدامات سایبری در سطح بلوغ یک را در یک دامنه انجام نمی‌دهد، نمی‌تواند به سطح بلوغ دوم در آن دامنه دسترسی پیدا کند، حتی اگر تمام الزامات در سطح بلوغ دوم را رعایت کند [۹].

۵.۲. مدل بهبود فرآیندها[11]

یکی از بهترین راه‌های بهبود و پیشرفت در فرایندهای کسب و کار و تجارت، استفاده از مدل بهبود فرآیندها می‌باشد. این مدل بهبود یک رویکرد بسیار موثر مبتنی بر داده، ۵ مرحله‌ای و یکی از مولفه‌های بسیار مفید برای بهبود کسب و کار است که مراحل ۵ گانه آن به شرح (شکل ۳) و (جدول ۳) می‌باشد [۱۰].

۱۰. Capability Maturity Model Integration

۱۱. DMAIC



شکل ۳. مدل بهبود فرآیندها.

جدول ۳. مدل بهبود فرآیندها.

مرحله	اقدام
تعریف کردن[۱۲]	اولین مرحله از این چرخه، بهبود کسب و کار است. در این بخش اهداف پروژه برای مشتریان داخلی و خارجی تعریف می‌شود. این بخش روی انتخاب متمرکز می‌شود که بسیار در درک پروژه و اینکه کدام معیارهای موقعیت و تعریف در بهبود پروژه تاثیرگذار است. اینکه آیا این تعریف و تعیین اهداف کسب و کار را به هدف می‌رساند.
اندازه گیری[۱۳]	در این بخش فرم‌های اندازه‌گیری تایید و اندازه‌گیری می‌شود، همانند استفاده از نظرسنجی مشتری برای تعیین کمبودها. مرحله اندازه‌گیری مجموعه‌ای از داده‌ها را از تعداد زیادی از منابع برای تعیین انواع معیارها و نقص‌ها جمع‌آوری می‌کند.
تجزیه و تحلیل[۱۴]	در این مرحله تمرکز بر جداسازی علل مهم بوده و مورد بررسی قرار می‌گیرد. در حالت ایده‌آل باید سه دلیل وجود داشته باشد و کنترل شود. البته وجود بیش از ۳ دلیل و علت به این معنی نیست که نمی‌شود علل مهم را تجزیه و تحلیل کرد و یا اینکه بیش از اندازه هدف بلند پروازانه داشت. در حقیقت این مرحله هرگونه شکاف بین عملکرد و هدف و اولویت در بهبود را شناسایی می‌کند.
بهبود[۱۵]	هدف از مرحله بهبود این است که با از بین بردن یا کنترل عملی می‌خواهیم به مطلوب مورد نظر دست یابیم. در اینجا با استفاده از تکنولوژی و نظم و انضباط، تیم طراحی راه‌های نوآورانه ارایه می‌دهد تا مشکلات را حل و یا از ایجاد مشکلات جلوگیری کند.
کنترل[۱۶]	اطمینان حاصل شود که تغییرات نتایج پایداری دارد. بهترین کنترل‌ها نظیر طراحی فرایند یا تغییرات غیر قابل برگشت نظیر طراحی فرایند، تغییرات در محصول است. اما معمولا روش‌های تنظیم، تنظیم فرایند، سایر بخش‌هایی که نیاز به نظارت و عملیات روزانه دارند. این چرخه و فرایند انجام می‌شود تا اطمینان حاصل شود که بهترین نتیجه ممکن به دست می‌آید.

۳. روش‌شناسی تحقیق

پژوهش حاضر از لحاظ هدف(نوع تحقیق) در زمره تحقیقات بنیادی و کاربردی دسته‌بندی می‌گردد این پژوهش به این دلیل بنیادی است که با بررسی مبانی علمی یک الگوی جدید برای شناسایی و مدیریت آسیب‌پذیری‌ها و تهدیدات سایبری ارایه می‌کند و از این منظر کاربردی است که یافته‌های آن به سازمان‌ها و نهادهای کشور در برابر هجمه‌های احتمالی نظام سلطه کمک خواهد نمود و باعث ارتقاء، توانمندی و افزایش مهارت‌های راهبردی متولیان در برآورد تهدیدات و فرصت‌های ناشی از عدم ایجاد امنیت سایبری مناسب در زیر ساخت‌ها و فرآیندهای فرماندهی و کنترل می‌گردد. این پژوهش از لحاظ طرح تحقیق در زمره تحقیقات آینده‌نگر دسته‌بندی می‌گردد و به این دلیل آینده‌نگر است که محقق به شناسایی تهدیدات آتی سامانه‌های فرماندهی و کنترل مبتنی بر فضای سایبر پرداخته است. تحقیق حاضر از لحاظ روش در زمره تحقیقات توصیفی/تحلیلی با نگاه اکتشافی دسته‌بندی می‌گردد زیرا محقق با نگاه راهبردی به توصیف چالش‌های ناشی از عدم رعایت امنیت فضای سایبر در حوزه فرماندهی و کنترل پرداخته است و در نهایت الگوی پیشنهادی را ارایه نموده است.

ابزار گردآوری اطلاعات در این پژوهش، پرسشنامه است. در این تحقیق ابتدا با انجام مطالعات کتابخانه‌ای و بررسی تحقیقات صورت گرفته در داخل و خارج از کشور، شاخص‌های مرتبط

۱۲. Define
۱۳. Measure
۱۴. Analyze
۱۵. Improve
۱۶. Control

با تاب‌آوری سایبری و فرایندهایامنیت سایبری مورد تحلیل و بررسی قرار گرفت. سپس طی دو مرحله با استفاده از پرسشنامه، نظر خبرگان و صاحب‌نظران در خصوص میزان اهمیت هر یک از شاخص‌های احصاء شده جمع‌آوری گردید.

در این تحقیق برای سنجش روایی پرسشنامه از روایی محتوا، استفاده شده است. روایی محتوا اطمینان می‌دهد که ابزار مورد نظر به تعداد کافی، پرسش مناسب برای اندازه‌گیری مفهوم مورد سنجش را دارد. هر قدر این عناصر، مقیاس گسترده‌تر و قلمرو مفهوم مورد سنجش را بیشتر در برگیرند، روایی محتوا بیشتر خواهد بود. در این تحقیق، سوال‌های پرسشنامه متناسب با مبانی نظری طراحی شده و سپس با توزیع آن بین صاحب‌نظران مرتبط با موضوع، معیارهای نامفهوم و غیر مرتبط تعدیل یا حذف شد و با پیشنهادهای ارایه شده، معیارهایی نیز اضافه شده و پرسشنامه اصلی بعد از این مرحله تدوین و توزیع گردید. جامعه آماری پژوهش شامل تعداد ۳۰ نفر از خبرگان و صاحبنظران، مدیران و فرماندهان نظامی(که دارای شرایط: داشتن مدرک کارشناشی ارشد و بالاتر، آشنایی با مباحث سایبری و فرماندهی و کنترل و دارا بودن جایگاه مسئولیتی راهبردی) می‌باشد و جامعه نمونه به صورت تمام شمار برابر با جامعه آماری در نظر گرفته شد.

٤. یافته‌ها و تجزیه و تحلیل داده‌ها

در این پژوهش در پی ارایه الگوی تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل در مقابل تهدیدهای سایبری می‌باشیم. در الگوی پیشنهادی برای مدیریت آسیب‌پذیری‌ها در تاب‌آوری سایبری سه محور اصلی در نظر گرفته شده است:

سطوح سامانه‌های فرماندهی و کنترل (راهبری، نظارت و کنترل، عملیات) معادل سه سطح مدیریت سازمانی (راهبردی، میانی، عملیاتی) است. نظارت و راهبری سامانه وابستگی بیشتر به نیروی انسانی خبره و تصمیم‌گیر دارد. سطح کنترل بیشتر وابسته به ابزارهای کنترلی نظیر سامانه‌های فناوری عملیات، اسکادا[17] و سامانه‌های قابل برنامه‌ریزی[18] است و سطح عملیات در برگیرنده تجهیزات و حساسه‌ها[19] و عملگرها[20] می‌باشد.

سطوح بلوغ سازمانی که در برگیرند رشد سازمان در مدیریت آسیب پذیری‌ها با ۵ سطح بلوغ (انجام شده، برنامه‌ریزی شده، مدیریت شده، اندازه‌گیری شده، نهادینه شده) است مبتنی بر مدل یکپارچه بلوغ قابلیت‌های سازمانی در نظر گرفته شده است.

فرآیند اجرای مدیریت آسیب‌پذیری‌های سامانه‌های فرماندهی و کنترل بر پایه مدل پنج مرحله‌ای بهبود فرآیندها (شناخت، اندازه‌گیری، تحلیل، اجرا، کنترل) برای فرآیند پیاده‌سازی در نظر گرفته می‌شود.

بر اساس الگوی ارایه شده ٤٩ مولفه اصلی برای تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل مبتنی بر بهبود فرآیندها به صورت ذیل ارایه شده است (جدول ٤).

جدول ٤. الگوی تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل.

سطوح سامانه‌های فرماندهی و کنترل	راهبری
اول (انجام شده)	۱- مدیریت تداوم فعالیت‌های سامانه‌های فرماندهی و کنترل ۲- مدیریت وابستگی و ارتباطات خارجی فرماندهی و کنترل ۳- آموزش و آگاهی مدیران کارشناسان فرماندهی و کنترل ٤- آگاهی وضعیتی تاب‌آوری فرماندهی و کنترل
دوم (برنامه‌ریزی شده)	۱- مستند سازی انجام فعالیت‌های راهبری ۲- تعیین خط مشی برای انجام فعالیت‌های راهبری ۳- شناسایی و اطلاع رسانی نقش ذینفعان برای فعالیت‌های راهبری ٤- شناسایی و اجرای کردن استانداردها و دستورالعمل‌های راهبری
سوم (مدیریت شده)	۱- نظارت مدیریتی بر کارایی فعالیت‌های راهبری ۲- تخصیص کارکنان واجد شرایط برای انجام فعالیت مطابق با برنامه‌ریزی راهبری ۳- تعیین بودجه کافی برای انجام فعالیت‌ها مطابق با برنامه‌ریزی انجام شده ٤- کنترل ریسک‌های مربوط به کارایی فعالیت-های برنامه‌ریزی راهبری
چهارم	۱- بازنگری دوره‌ای و ارزیابی اثر بخشی میزان-

۱۷. SCADA
۱۸. PLC
۱۹. sensors
۲۰. Actuators

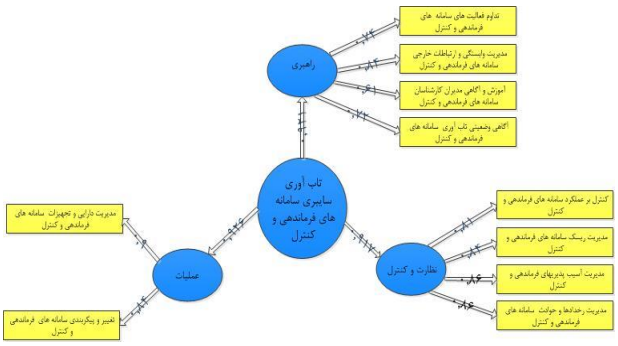
(اندازه‌گیری شده)	سنجی فعالیت‌ها راهبری ۲- بازنگری دوره‌ای فعالیت‌ها جهت اطمینان پیشرفت مناسب راهبری ۳- آگاهی‌رسانی به مدیریت سطح بالا از مسائل مربوط به کارایی راهبری
پنجم (نهادینه شده)	۱- اتخاذ یک تعریف استاندارد از فعالیت‌های راهبری مستندسازی و اشتراک‌گذاری پیشرفت فعالیت-های راهبری
سطوح سیستم‌های فرماندهی و کنترل	**نظارت و کنترل**
اول (انجام شده)	۱- کنترل بر عملکرد سامانه‌های فرماندهی و کنترل ۲- مدیریت ریسک سامانه‌های فرماندهی و کنترل ۳- مدیریت آسیب‌پذیری‌های سامانه‌های فرماندهی و کنترل ٤- مدیریت رخدادها و حوادث سایبری سامانه-های فرماندهی و کنترل
دوم (برنامه‌ریزی شده)	۱- مستند سازی انجام فعالیت‌های نظارت و کنترل ۲- تعیین خط مشی برای انجام فعالیت‌های نظارت و کنترل ۳- شناسایی و اطلاع رسانی نقش ذینفعان برای فعالیت‌های نظارت و کنترل ٤- شناسایی و اجرایی کردن استانداردها و دستورالعمل‌های نظارت و کنترل
سوم (مدیریت شده)	۱- نظارت مدیریتی بر کارایی فعالیت‌های نظارت و کنترل ۲- تخصیص کارکنان واجد شرایط برای انجام فعالیت مطابق با برنامه‌ریزی نظارت و کنترل ۳- تعیین بودجه کافی برای انجام فعالیت‌ها مطابق با برنامه‌ریزی انجام شده نظارت و کنترل ٤- کنترل ریسک‌های مربوط به کارایی فعالیت-های برنامه‌ریزی نظارت و کنترل
چهارم (اندازه‌گیری شده)	۱- بازنگری دوره‌ای و ارزیابی اثربخشی میزان-سنجی فعالیت‌های نظارت و کنترل ۲- بازنگری دوره‌ایی فعالیت‌ها جهت اطمینان پیشرفت مناسب نظارت و کنترل ۳- آگاهی رسانی به مدیریت سطح بالا از مسائل مربوط به کارایی نظارت و کنترل
پنجم (نهادینه شده)	۱- اتخاذ یک تعریف استاندارد از فعالیت‌ها ۲- مستند سازی و اشتراک‌گذاری پیشرفت فعالیت‌ها
سطوح سیستم‌های فرماندهی و کنترل	**فرآیند و عملیات**
اول (انجام شده)	۱- مدیریت دارایی و تجهیزات سامانه‌های فرماندهی و کنترل ۲- مدیریت تغییر و پیکربندی سامانه‌های فرماندهی و کنترل ۳- تاب‌آوری فرماندهی و کنترل
دوم (برنامه‌ریزی شده)	۱- مستند سازی انجام فعالیت‌های فرآیند و عملیات ۲- تعیین خط مشی برای انجام فعالیت‌های فرآیند و عملیات ۳- شناسایی و اطلاع رسانی نقش ذینفعان برای فعالیت‌های فرآیند و عملیات ٤- شناسایی و اجرای کردن استانداردها و دستورالعمل‌های فرآیند و عملیات
سوم (مدیریت شده)	۱- نظارت مدیریتی بر کارایی فعالیت‌های فرآیند و عملیات ۲- تخصیص کارکنان واجد شرایط برای انجام فعالیت مطابق با برنامه‌ریزی فرآیند و عملیات ۳- تعیین بودجه کافی برای انجام فعالیت‌ها مطابق با برنامه‌ریزی انجام شده فرآیند و عملیات ٤- کنترل ریسک‌های مربوط به کارایی فعالیت-های برنامه‌ریزی فرآیند و عملیات
چهارم (اندازه‌گیری شده)	۱- بازنگری دوره‌ای و ارزیابی اثربخشی میزان-سنجی فعالیت‌های فرآیند و عملیات ۲- بازنگری دوره‌ای فعالیت‌ها جهت اطمینان پیشرفت مناسب فرآیند و عملیات ۳- آگاهی رسانی به مدیریت سطح بالا از مسائل مربوط به کارایی فرآیند و عملیات
پنجم (نهادینه شده)	۱- اتخاذ یک تعریف استاندارد از کلیه فعالیت‌های فرآیند و عملیات ۲- مستند سازی و اشتراک‌گذاری پیشرفت فعالیت‌های فرآیند و عملیات

در این تحقیق برای آزمون مدل مفهومی از مدل سازی معادلات ساختاری مبتنی بر رویکرد حداقل مربعات جزئی با

نرم‌افزار اسمارت پی.ال.اس[۲۱] استفاده شده است. با استفاده از این نرم‌افزار، هم برازش مدل اندازه‌گیری می‌گردد و هم برازش مدل ساختاری برای سنجش رابطه میان متغیرها با استفاده از ضرایب معناداری انجام می‌شود و همچنین می‌توان اولویت‌بندی مولفه‌ها و گویه‌ها را نیز از این طریق مشخص نمود.

در این روش میزان سهم هر گویه یا عامل در ایجاد متغیر مورد بررسی قرار گرفته و برای این کار از تحلیل عاملی تاییدی استفاد می‌شود. در تحلیل عاملی، مقدار بار عاملی کمتر از ۰/۳ نشان دهنده مقیاس ضعیف بوده و باید از مدل حذف شود. بارهای عاملی بین ۰/۳ تا ۰/٦ نشان می‌دهند که متغیر مشاهده شده مقیاس متوسطی بوده و برای ادامه آنالیز کفایت می‌کند. مقادیر بزرگتر از ۰/٦ نیز نشان می‌دهد که متغییر مشاهده‌پذیر مقیاس قابل اطمینانی برای محاسبه می‌باشد. در کل مقادیر بارهای عاملی بزرگ‌تر از ۰/٤ را می‌توان در مدل حفظ کرد [۱۱].

برای هریک از ابعاد راهبری، نظارت و کنترل و فرآیند و عملیات یک تحلیل عاملی جداگانه محاسبه شده است و سهم هریک از گویه‌های مربوط به مولفه‌ها مشخص شده است. در نهایت با استفاده از مدل تحلیل عاملی مرتبه دوم، الگوی نهایی بررسی گردید. نتایج تحلیل بار عاملی در (شکل ٤) و جدول ۵ ارایه شده است .



شکل٤. ضرایب تحلیل عاملی مدل.

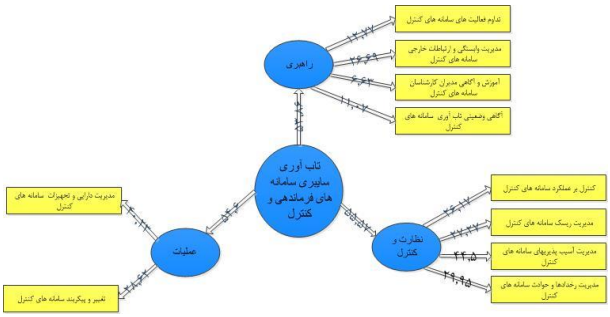
جدول ۵ – نتایج تحلیل عاملی تاییدی الگو.

بعد	مولفه	بار عاملی
راهبری	مدیریت تداوم فعالیت‌های سامانه‌های فرماندهی و کنترل	۰.۷٤
	مدیریت وابستگی و ارتباطات خارجی فرماندهی و کنترل	۰.۸٤
	آموزش و آگاهی مدیران کارشناسان فرماندهی و کنترل	۰.٦۱
	آگاهی وضعیتی تاب‌آوری فرماندهی و کنترل	۰.۷۲
نظارت و کنترل	کنترل بر عملکرد سامانه‌های فرماندهی و کنترل	۰.۸۱
	مدیریت ریسک سامانه‌های فرماندهی و کنترل	۰.۸٤
	مدیریت آسیب‌پذیری‌های سامانه‌های فرماندهی و کنترل	۰.۸٦
	مدیریت رخدادها و حوادث سایبری سامانه‌های فرماندهی و کنترل	۰.۸٦
فرآیند و عملیات	مدیریت دارایی و تجهیزات سامانه های فرماندهی و کنترل	۰.۹
	مدیریت تغییر پیکربندی سامانه‌های فرماندهی و کنترل	۰.۸٤
تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل	راهبری	۰.۹۲۱
	نظارت و کنترل	۰.۹۱۷
	فرآیند و عملیات	۰.۹۲٦

اطلاعات (جدول ۵) نشان می‌دهد که تمامی مولفه‌ها (گویه-ها) مقادیر بارهای عاملی بزرگ‌تر از ۰/٤ داشته و از اعتبار لازم برخوردار هستند. در الگوی فوق ضرایب مسیرها برای سه بعد راهبری، نظارت و کنترل و فرآیند و عملیات ۰/۹۲۱ ، ۰/۹۱۷ و ۰/۹۲٦ می‌باشد، لذا بعد فرآیند و عملیات بالاترین تاثیر و بعدهای راهبری و نظارت و کنترل با اختلاف کمی در جایگاه دوم و سوم می‌باشند.

آزمون معناداری: نتایج آزمون معناداری در (شکل ۵) بر اساس مقادیر ***t*** نشان داده شده است و به دلیل بیشتر بودن مقادیر ***t*** از ۱/۹٦، الگوی ارایه شده در سطح احتمال ۹۵ درصد معناداری قرار داشته و از اعتبار لازم برخوردار است.

۲۱. SMART PLS ۹.۹۸



شکل۵. آزمون معناداری الگو.

پارامتر پایایی مرکب[۲۲]: به دلیل اینکه تمام اعداد t از ۰/٦ بیشتر هستند، الگوی دارای سطح بالایی از پایداری است.

پارامتر آلفای کرونباخ[۲۳]: بیشتر بودن تمامی اعداد t از ۰/٦، نشانگر پایداری گویه‌ها می‌باشد.

پارامتر ضریب تعیین[۲٤]: مقادیر استاندارد برای سطوح "قابل ملاحظه"، "متوسط" و "ضعیف" عبارتند از: ٦۷/ ، ۰/۳۳ و ۰/۱۹ و در الگوی ما، به دلیل بیشتر بودن مقادیر، دارای سطح قابل قبولی است.

همچنین برای برازش الگو، از شاخص نیکویی برازش[۲۵] استفاده شده است. این شاخص به عنوان معیاری برای سنجش عملکرد الگو بکار می‌رود. این شاخص، مجذور ضرب دو مقدار متوسط اشتراکی[۲٦] و متوسط ضریب تعیین است. مقدار ***GOF*** بین صفر و یک در نوسان است. مقدار ۰/۰۱، ۰/۲۵ و ۰/۳٦ به ترتیب به عنوان مقادیر ضعیف، متوسط و قوی معرفی شده‌اند.

$$GOF=\sqrt{Communality \times R^2}$$

شاخص نیکویی برازش در سه بعد راهبری و نظارت، نظارت و کنترل و فرآیند و عملیات به ترتیب عبارت‌اند از: ۰/۷۹، ۰/۷۸ و ۰/۷۲ و چون همگی بیشتر از ۰/۳٦ هستند، لذا در حد قابل قبول و قوی می‌باشند.

۵. نتیجه‌گیری

تحولات نوین سایبری موجب نفوذ فناوری‌های گوناگون سایبری در بخش‌های مختلف از جمله سامانه‌های فرماندهی و کنترل گردیده است. فناوری‌های سایبری در کنار فرصت‌ها و امکانات مختلفی که در اختیار سامانه‌های فرماندهی و کنترل قرار می‌دهند موجب بروز تهدیدهای نوینی بر روی این سامانه‌ها گردیده است که تداوم عملیاتی این سامانه‌ها را با مخاطره مواجه می‌نماید. از این جهت بهره‌گیری از یک الگوی مناسب جهت تاب آوری سایبری در مقابله تهدیدهای سایبری بیش از هر زمان دیگری ضروری است. تاب‌آوری سایبری، به معنی ایجاد تمهیدات مناسب پیش از حمله سایبری، حفظ عملیات اصلی سامانه و پایداری مناسب در زمان حمله سایبری و بازگشت به حالت اولیه پس از حمله سایبری، یکی از اصلی‌ترین راهبردها در مواجهه با تهدیدات سایبری است.

در این پژوهش الگوی تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل در مقابل تهدیدهای سایبری مبتنی بر یکپارچه سازی مدل بلوغ توانایی و مدل بهبود فرآیندها، برای سه سطح راهبری، کنترل و عملیات سامانه‌های فرماندهی و کنترل مطابق (شکل ٦) ارایه گردیده است.

در این الگو، در سطح بلوغ یک (اجرایی) برای ابعاد رهبری، نظارت و کنترل و عملیات تعداد ۱۰ مولفه ارایه شده است. البته براساس ضرایب به دست آمده بعد فرآیند و عملیات نسبت به بعدهای راهبری و نظارت و کنترل دارای تاثیر بیشتری می‌باشد، در سطح بلوغ دو (برنامه‌ریزی) تعداد ۱۲ مولفه، در سطح بلوغ سوم (مدیریت) تعداد ۱۲ مولفه، در سطح بلوغ چهارم (اندازه گیری) تعداد ۹ مولفه و در سطح بلوغ پنجم (نهادینه) تعداد ٦ مولفه، و در مجموع تعداد ٤۹ مولفه، ارایه گردید.

الگوی ارایه شده با بهره‌گیری از نرم‌افزار اسمارت پی.ال.اس، تحلیل بار عاملی و آزمون معنی‌دار بودن مولفه‌ها، در سطح ۹۵ درصد معنی‌داری، مورد تایید قرار گرفت.

۲۲. Composite Reiability
۲۳. Cronbech Alpa
۲۴. R.Square
۲۵. GOF
۲٦. Communality

شکل ٦. الگوی تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل در مقابل تهدیدهای سایبری.

٦. مراجع

[١] بت شکن، بهمن(١٣٩٦)، بررسی مهندسی تاب آوری در فضای سایبری، سومین کنفرانس ملی علوم و مهندسی کامپیوتر و فناوری اطلاعات، بابل، دسترسی از طریق: https://civilica.com/doc/٦٧٦٨٥٥

[٢] مظفری، شهرام، پورمنصوری، رضوان، پورمنصوری، جمال(٢٠١٩)، احصاء شاخص‌های تاب‌آوری برکاهش آسیب پذیری سیستم‌های کنترل صنعتی در تهدیدات سایبری، چهارمین کنفرانس بین المللی تحقیقات مرتبط با اقتصاد و مدیریت، پاریس، فرانس، دسترسی از طریق: https://www.researchgate.net /٣٤٣٢١٢٥٦١

[٣] مؤسسه آموزشی و تحقیقاتی صنایع دفاعی (١٣٩٢)، "نگاهی به آینده سامانه‌های فرماندهی و کنترل".

[٤] Developing Cyber Resilient Systems (٢٠١٩), A Systems Security Engineering Approach - SP ٨٠٠-١٦٠ Vol. ٢.

[٥] Luiijf, E. (٢٠١٦), "Threats in Industrial Control Systems Cyber-security of SCADA and Other Industrial Control Systems" (pp. ٦٩-٩٣), Springer.

[٦] U.S.GAO.٢٠٠٤. (٢٠١٤), Critical infrastructure protection: Challenges and efforts to secure control systems. U.S. GAO.

[٧] Wei, D., & Ji, K. (٢٠١٠), Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights. Paper presented at the Resilient Control Systems (ISRCS), ٢٠١٠ ٣rd International Symposium.

[٨] Systems Security Engineering Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems, (٢٠١٨).

[٩] Colbert, E. J. M., & Kott, A. (٢٠١٦). Cyber-security of SCADA and Other Industrial Control Systems. Advances in Information Security, ٦٣. doi:١٠,١٠٠٧/٩٧٨-٣-٣١٩-٣٢١٢٥-٧.

[١٠] Conklin, W. A., & Shoemaker, D. (٢٠١٧). Cyber-Resilience: Seven Steps for Institutional Survival. EDPACS, ٥٥(٢), ١٤-٢٢.

[١١] Council, E., Forbes Technology. Cybersecurity Is Dead. Forbes.

[١٢] Davis, Z. (٢٠١٥), Definition of computer security. Encyclopedia. Retrieved ٦.

[١٣] Carías, Juan F.; Arrizabalaga, Saioa; Labaka, Leire; Hernantes, Josune (٢٠٢٠), Cyber Resilience Progression Model, Appl. Sci. ٢٠٢٠, ١٠, ٧٣٩٣; doi:١٠,٣٣٩٠/app١٠٢١٧٣٩٣ www.mdpi.com/journal/applsci.

[١٤] Llansó, Thomas H., Hedgecock, Daniel A., Pendergrass, J. Aaron (٢٠٢١), "The State of Cyber Resilience: Now and in the Future", Johns Hopkins APL Technical Digest, Volume ٣٥, www.jhuapl.edu/techdigest.