Quarterly Journal Defensive Future Studies
AJA Command and Staff University
http://www.dfsr.ir/
Online ISSN: 2645-7172
Print ISSN: 2588-428x

Maturity pattern of cyber resilience of command and control systems in dealing with future threats

Ali Mohammad Aminzadeh[1]| Rasool Ramazani Dehaghi[2]✉ | Mohammad Sepehri[3]

1. Director of Cyber Defense Center of Information Exchange Security Industries, Tehran, Iran. E-mail: mo.aminzadeh@gmail.com
2. Corresponding Author, Department of cyber, Faculty of Electrical Engineering, University of Khatam Al-Anbia Air Defense, Tehran, Iran. E-mail: sepehrramezany@yahoo.com
3. Department of Management, Faculty of Command and Control, University of Khatam Al-Anbia Air Defense, Tehran, Iran. E-mail: sepehri377@chmail.ir

Article Info

Article type:

Research Article

Article history:

Received

2023-01-02

Received in revised form

2023-06-24

Accepted

2023-07-09

Published online

2023-11-18

Keywords:

Cyber resilience, industrial command and control systems, ability maturity, process improvement.

ABSTRACT

Objective: The main goal of this research is to achieve the maturity pattern of cyber resilience of command and control systems in dealing with future threats.

Methodology: The current research is prospective and applied, and descriptive/analytical with an exploratory approach. The statistical population of the research includes 30 military and cyber experts, and the sample population is considered equal to the statistical population. In order to collect data, interview tools and questionnaires were used, and data analysis was done by factor load analysis using SmartPLS software, and to confirm the model, a significant test was used. The presence of components was used.

Findings: in the final model, for the dimensions of leadership, supervision and operation, there are 10 components in maturity level one, 12 components in maturity level two, 12 components in maturity level three, 9 components in maturity level four and 6 components for the fifth maturity level, and a total of 49 components were calculated and presented.

Conclusion: The cyber maturity model is a method that enables organizations to strengthen their cyber security program, prioritize cyber security actions and investments, and maintain the desired level of security throughout the life cycle of information technology systems. Based on this, in order to reach the maturity of cyber resilience, the three dimensions of leadership, monitoring and control and operation of command and control systems at 5 levels (performed, planned, managed, measured and institutionalized) should be matured.

Cite this article: Ramezany, R., Sepehri, M., & Aminzadeh, A. (2023). Maturity pattern of cyber resilience of command and control systems in dealing with future threats. *Defensive Future Studies*, *8*(30), 39-66.
DOI: 10.22034/dfsr.2023.1986565.1670

© The Author(s)

Publisher: AJA Command and Staff University

فصلنامه علمی آینده‌پژوهی دفاعی
شاپای چاپی: ۲۳۸۸-۲۲۸X شاپای الکترونیکی: ۲۶۴۵-۷۱۷۳ http://www.dfsr.ir/
دانشگاه فرماندهی و ستاد آجا

الگوی بلوغ تاب‌آوری سایبری سامانه فرماندهی و کنترل در مقابله با تهدیدات آینده

علی‌محمد امین‌زاده [۱] | رسول رمضانی دهقی [۲] ✉ | محمد سپهری [۳]

۱. مدیر مرکز دفاع سایبری صنایع امنیت تبادل اطلاعات، تهران، ایران، رایانامه: mo.aminzadeh@gmail.com

۲. نویسنده مسئول، گروه سایبر، دانشکده مهندسی برق، دانشگاه پدافند هوایی خاتم‌الانبیاء (ص)، تهران، ایران، رایانامه: sepehrramezany@yahoo.com

۳. گروه مدیریت، دانشکده فرماندهی و کنترل، دانشگاه پدافند هوایی خاتم‌الانبیاء (ص)، تهران، ایران، رایانامه: sepehri377@chmail.ir

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخ دریافت:
۱۴۰۱/۱۰/۱۲

تاریخ بازنگری:
۱۴۰۲/۰۴/۰۳

تاریخ پذیرش:
۱۴۰۲/۰۴/۱۸

تاریخ انتشار:
۱۴۰۲/۰۸/۲۷

کلیدواژه‌ها:
تاب‌آوری سایبری، سامانه فرماندهی و کنترل، بلوغ توانایی، بهبود فرآیندها

چکیده

هدف: هدف اصلی این پژوهش دستیابی به الگوی بلوغ تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل در مقابله با تهدیدهای آینده است.

روش: پژوهش حاضر از نوع آینده‌نگر و کاربردی و به روش توصیفی/تحلیلی با نگاه اکتشافی است. جامعه آماری پژوهش شامل ۳۰ نفر از خبرگان نظامی و سایبری بوده و جامعه نمونه به‌صورت تمام شمار برابر جامعه آماری در نظر گرفته شده است. جهت جمع‌آوری داده‌ها از ابزارهای مصاحبه و پرسشنامه استفاده گردید و تجزیه‌وتحلیل داده‌ها به روش تحلیل بار عاملی و با استفاده از نرم‌افزار اسمارت پی.ال.اس انجام شده و برای تایید الگو از آزمون معنی‌دار بودن مؤلفه‌ها استفاده شد.

یافته‌ها: الگوی نهایی در مجموع برای سه بعد رهبری، نظارت و عملیات، در سطح بلوغ یک ۱۰ مؤلفه، در سطح بلوغ دو ۱۲ مؤلفه، در بلوغ سطح سوم ۱۲ مؤلفه، در سطح بلوغ چهارم ۹ مؤلفه و برای سطح بلوغ پنجم ۶ مؤلفه و در مجموع ۴۹ مؤلفه احصاء و ارائه گردید.

نتیجه‌گیری: الگوی بلوغ سایبری روشی است که سازمان‌ها را قادر به تقویت برنامه امنیت سایبری، اولویت‌بندی اقدامات و سرمایه‌گذاری‌های امنیت سایبری و حفظ سطح مطلوب امنیت در طول چرخه حیات سیستم‌های فناوری اطلاعات می‌نماید. بر این اساس به‌منظور نیل به بلوغ تاب‌آوری سایبری بایستی سه بعد راهبری، نظارت و کنترل و عملیات سامانه‌های فرماندهی و کنترل در ۵ سطح (انجام‌شده، برنامه‌ریزی‌شده، مدیریت‌شده، اندازه‌گیری شده و نهادینه‌شده) به بلوغ برسد.

استناد: رمضانی، رسول؛ سپهری، محمد؛ و امین زاده، علی محمد. (۱۴۰۲). الگوی بلوغ تاب آوری سایبری سامانه‌های فرماندهی و کنترل در مقابله با تهدیدات آینده. آینده‌پژوهی دفاعی، ۸(۳۰)، ۳۹-۶۶.

DOI: 10.22034/DFSR.2023.1986565.1670

ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

© نویسندگان.

مقدمه

امروزه امنیت سایبری به‌طور گسترده‌ای در سطح جهانی در کانون توجه و اهمیت قرار دارد. بر همین ا ساس عوامل تأثیرگذار در امینت سایبری افزایش یافته و می‌توان عوامل مؤثر بر امنیت سایبر را در یکی از سه وجه ذیل دسته‌بندی نمود: تهدیدات خارجی، تهدیدات داخلی و سیاست‌های اجرایی در به‌کارگیری فناوری‌های نوین (Luiijf, 2016: 75).

بسیاری از سازمان‌ها، انبوهی از تجهیزات الکترونیکی را صرف‌نظر از کاربردهای نظامی و غیرنظامی آن در قالب کامپیوترهای بزرگ و کوچک، ثابت و سیار و یا قطعات کوچک داخل مدارهای پیچیده در ادوات جنگی، جنگنده‌ها، پهپادها، انواع ناوها و ناوچه‌ها، سامانه‌های پدافندی و حتی ماهواره‌ها در کشور استفاده می‌کنند. به علت محدودیت‌های فناورانه، عموم این تجهیزات از کشورهایی تأمین می‌گردند که خود مخرب‌ترین حملات سایبری را در سال‌های اخیر انجام داده‌اند (رمضان‌زاده و همکاران، ۱۴۰۰: ۶۰).

از طرفی نگرانی‌های سازمان‌های دولتی، شرکت‌های بخش خصوصی و مؤسسات 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 ا ستاکس‌نت و ایندا ستروور، بیشترین حملات را به تجهیزات مرتبط با سامانه‌های فرماندهی و کنترل دا شته‌اند و علاوه بر این، حملاتی با م شخ صات بالا به شرکت‌های صنعتی ضربه‌های شدیدی را وارد نموده‌اند. بوئینگ اعلام کرده که توسط بدافزار واناکرای مورد حمله قرارگرفته و چند ماه بعد، همین ویروس کارخانه‌های شرکت تولیدکننده نیمه‌هادی 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 تأثیر گذا شت. در واقع، مهاجمان برای ایجاد اختلال در شرکت‌های صنعتی همیشه به دانش خاصی نیاز ندارند (Luiijf, 2016: 75).

پس از سوء استفاده از آسیب‌پذیری‌ها در زیرساخت‌های فناوری اطلاعات، هکرها می‌توانند به شبکه دسترسی پیدا کنند. 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 شناخته‌شده است. شناسایی آسیب‌پذیری‌های موجود در تجهیزات سامانه‌های فرماندهی و کنترل بسیار مهم است، زیرا این امر به مشاغل اجازه می‌دهد مخاطرات را به‌موقع ارزیابی کرده و اقدامات حفاظتی مناسبی را انجام دهند (Dacey, 2020).

طبق تحقیقات انجام‌شده، 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 سامانه فرماندهی و کنترل برای تخریب و آسیب رساندن به فرایندهای اساسی سامانه، بهره‌برداری نماید (Ross, 2019). از طرفی وجود محدودیت‌های ناشی از تحریم‌های بین‌المللی به‌ویژه در بخش دفاعی/امنیتی کشور و بهره‌گیری سامانه‌های فرماندهی و کنترل از تجهیزات غیر بومی که اغلب ناامن و آسیب‌پذیر می‌باشند و همچنین افزایش تهدیدات سایبری ناشی از توسعه فناوری‌های سایبری که اغلب ناشناخته‌اند، احتمال شکست امنیتی در سامانه‌های فرماندهی و کنترل را افزایش داده و تداوم عملیات را با مخاطره مواجه می‌نمایند. لذا عدم اتخاذ تدابیر لازم فنی و مدیریتی، توسعه زیر ساخت‌ها و پیاده سازی پدافند غیرعامل سایبری و همچنین فرهنگ سازی و آموزش در این زمینه موجب به خطر افتادن امنیت تجهیزات بخش دفاعی/امنیتی کشور خواهد شد (مقدسی لیچاهی و همت، ۱۳۹۷: ۱۱۷).

تاب‌آوری سایبری، به معنی ایجاد تمهیدات مناسب پیش از حمله سایبری، حفظ عملیات اصلی سامانه و پایداری مناسب در زمان حمله و بازگشت به حالت اولیه پس از حمله، یکی از اصلی‌ترین راهبردها در مواجهه با تهدیدات سایبری است. از طرفی تاب‌آوری سایبری زمانی به بلوغ می‌رسد که کل سازمان درگیر اقدامات امنیت سایبری شود، لذا بلوغ تاب‌آوری سایبری روشی است که از طریق اولویت‌بندی، اجرا و مدیریت شیوه‌های امنیت سایبری موجب تقویت برنامه و فرهنگ امنیت سایبری در کل سازمان می‌گردد. برنامه‌های بلوغ تاب‌آوری سایبری از طریق به اشتراک گذاشتن دانش، بهترین شیوه‌ها و مراجع مرتبط در سراسر سازمان موجب تقویت قابلیت‌های امنیت سایبری شده و سازمان را قادر می‌سازد تا به‌طور مؤثر و پیوسته قابلیت‌های امنیت سایبری خود را ارزیابی نماید. با توجه به اینکه برنامه‌های بلوغ تاب‌آوری سایبری نقش مهمی در

کاهش شکست‌های امنیتی سامانه‌های فرماندهی و کنترل دارد، این پژوهش به دنبال ارائه الگوی بلوغ تاب‌آوری سایبری سامانه فرماندهی و کنترل در مواجهه با تهدیدات آینده و روزافزون سایبری است. به این منظور هدف اصلی این پژوهش دستیابی به الگوی بلوغ تاب‌آوری سایبری سامانه فرماندهی و کنترل در مقابله با تهدیدهای آینده بوده و سؤال اصلی پژوهش این است که الگوی بلوغ تاب‌آوری سایبری سامانه فرماندهی و کنترل در مقابله با تهدیدهای آینده کدام است؟

با عنایت به اینکه پس از وقوع یک حمله سایبری، تداوم عملیاتی سامانه فرماندهی و کنترل از اهمیت بالایی برخوردار است، انجام این پژوهش الگوی مناسبی را به‌منظور نیل به بلوغ تاب‌آوری سایبری سامانه فرماندهی و کنترل در اختیار نیروهای عملیاتی 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 الگوی راهبردی مناسب جهت بلوغ 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.

مبانی نظری و پیشینه‌های پژوهش

با پیدایش فضای سایبر و نفوذ فناوری‌های سایبری در روند کنترل سامانه‌ها، مخاطرات سایبری به یکی از مهم‌ترین چالش‌های زیرساخت‌های حیاتی کشورها تبدیل گردید. سامانه‌های جمع‌آوری و کنترل یکپارچه داده‌ها، اغلب بر روی پروتکل‌های پیچیده اجرا می‌شوند اما در شرایط توسعه‌ای جدید، پروتکل‌های کنترل و گزارش آنالوگ در پروتکل‌های دیجیتال جاسازی‌شده و محدودیت‌های مربوط به یکپارچگی و رمزگذاری بر روی پروتکل انتقال در اینترنت، مشکلات را تشدید کرده است. همچنین با قرار دادن سیستم‌عامل جاسازی شده در سیستم‌های کنترل فرآیند، مشکلات جدیدی به وجود آمده است. کنترل‌کننده‌ها به‌طورمعمول از سیستم‌عامل‌های قدیمی استفاده می‌کنند و قادر به پشتیبانی از بخش مرکزی پردازش امنیت[1] نیستند. وصله‌های امنیتی و به‌روزرسانی اعمال نمی‌شود و کاربران نمی‌توانند کنترل‌کننده‌های وصله را بررسی کنند،

1.Security Central Processing Unit

ضمن اینکه خود فرآیند و صله امنیتی می‌تواند باعث خرابی و غیر قابل ا ستفاده شدن سامانه شود.

استفاده از فناوری‌های بی‌سیم در سامانه‌های فرماندهی و کنترل، امکان حملات بیشتر را فراهم آورده است. ابزار و نرم‌افزارهای جدید 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 می‌گیرد و آسیب‌پذیری‌های جدید به‌طور مداوم کشف می شوند. به‌عنوان مثال، تست امنیتی از طریق تزریق اطلاعات نامعتبر، غیر منتظره و یا تصادفی، 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. بهره‌برداری 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 ... انجام شود (Ross, 2018: 11).

همگرایی فناوری اطلاعات و فناوری عملیات

درحالی‌که در اکثر سازمان‌های بزرگ، ممکن است مباحث حوزه فناوری عملیات[1] و فناوری اطلاعات[2] خود را جدا از فناوری اصلی سازمانی بدانند، اما به‌طور فزاینده‌ای هر دو موضوع در امنیت دخالت دارند، چرا که بهره‌گیری از فناوری اطلاعات و فناوری عملیات به‌طور فزاینده‌ای در سراسر سازمان‌ها توسعه و گسترش یافته است. در بسیاری از موارد، متخصصان سایبری، چالش‌های امنیتی شبکه‌های رایانه‌ای را درک می‌کنند و این امر باعث می‌شود که فناوری اطلاعات و فناوری عملیات، همراه با یکدیگر در راستای کاهش خطرات امنیتی گام بردارند. بر همین اساس، هنگام برنامه‌ریزی کلان سازمانی، لازم است موضوع امنیت اطلاعات نه فقط در فرآیندها و فناوری‌های جاری، بلکه در سراسر شرکت (در سطح کلان و در سیاست‌گذاری‌های بهره‌گیری از فناوری‌های نوین) نیز در نظر گرفته شود (Ardagna & etal, 2021: 8).

باوجوداینکه سه ویژگی اساسی در امنیت یعنی محرمانگی، یکپارچگی و قابلیت در دسترس بودن برای امنیت فناوری اطلاعات و امنیت فناوری عملیات در نظر گرفته می‌شوند اما اولویت این سه ویژگی برای هر دو یکسان نیست. در فناوری اطلاعات

1.OT
2.IT

اولویت اول محرمانگی اطلاعات است و یکپارچگی در مرحله دوم و در دسترس بودن در اولویت سوم قرار دارد؛ اما در امنیت فناوری عملیات اولویت‌ها معکوس می شود یعنی در دسترس بودن در اولین اولویت، یکپارچگی در اولویت دوم و محرمانگی در اولویت سوم قرار دارد.

نکته مهم و قابل توجه این است که فناوری اطلاعات در بخش اصلی و میانی فناوری عملیات قرار گرفته است و این هم‌گرایی بین فناوری اطلاعات و فناوری عملیات به همراه گسترش به‌کارگیری انواع سنسورهای هوشمند در سطح عملیاتی، باعث افزایش سطح حملات شده است. در این محیط جدید سطح حملات از سرقت اطلاعات به سطوح پیچیده‌تری نظیر جرائم سایبری تغییر کرده است.

استراتژی دفاع در عمق[1] یک استراتژی امنیت اطلاعات است که با به‌کارگیری سه عنصر اصلی شامل: افراد، تکنولوژی و عملیات، برای ایجاد مانع در برابر نفوذ در لایه‌های مختلف سازمان، توصیه می‌شود. اتخاذ رویکرد دفاع در عمق که به یک رویکرد چند رشته‌ای در تمامی سطوح سامانه نیاز دارد، امکان شناسایی و یا جلوگیری از نقض کامل پروتکل‌های امنیتی را فراهم می‌کند و بخشی از یک استراتژی جامع جهت کاهش خطر است. نکته اساسی در این رویکرد جدید آن است که شبکه آگاهانه‌تر می‌تواند مشکلات امنیت سایبری را در تمامی سطوح سازمان بررسی و شناسایی کند (Elissa, Bennett & Kohno, 2023: 50).

آسیب‌پذیری‌های سامانه فرماندهی و کنترل

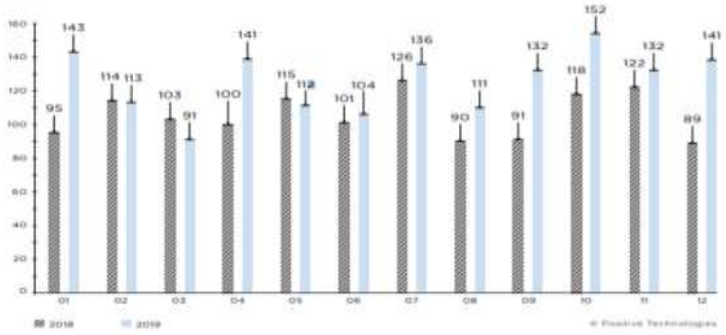
در سال های اخیر علاوه بر آسیب پذیری های نرم‌افزاری، انواع آسیب پذیری های سخت‌افزاری و سفت‌افزاری[2] نیز به شدت مورد توجه کار شناسان امنیت سایبری قرار گرفته است. این آسیب‌پذیری‌ها در پردازنده‌ها و قطعات الکترونیکی به‌طور گسترده وجود دارند و در تجهیزات مخابراتی و نظامی نیز یافت می‌شوند. نمونه بارز این آسیب‌پذیری‌ها، وجود یک نقطه دسترسی مخفی در تراشه‌های ساخت یک شرکت چینی است که در تجهیزات نیروی هوایی آمریکا نیز به کار می‌روند و توسط تیم تحقیقات دانشگاه کمبریج شناسایی شده است. در این بخش سامانه‌های کنترل شامل تجهیزات الکترونیکی و پردازشی متنوعی است که ازجمله مهم‌ترین این تجهیزات،

1.Defense in depth
2. Firmware

عملگرها، سنسورها، سامانه‌های کنترلی قابل برنامه‌ریزی[1] و واحدهای ارتباط از راه دور[2] می‌باشند. مهاجمان با دسترسی به کد نرم‌افزاری و یا سفت‌افزاری این تجهیزات، می‌توانند به‌راحتی به سامانه‌های کنترلی نفوذ کرده و کنترل فرآیند را در دست گیرند.

در پژوهشی که در دانشگاه کارولینای جنوبی انجام شد، به بررسی آسیب‌پذیری کدهای کنترل‌کننده منطقی برنامه‌ریزی‌شده در سامانه‌های فرماندهی و کنترل پرداخته شد، نتایج این پژوهش حاکی از ضعف شدید این ابزارها در حوزه امنیت سایبری بود. یکی از آسیب‌پذیری‌های عنوان شده برای واحد ارتباط از راه دور، تأیید ورودی نامناسب و غیر ایمن این تجهیزات است که منجر به نفوذ مهاجم به سامانه فرماندهی و کنترل می‌گردد. در این مورد خطرات امنیتی ناشی از حملات علیه دستگاه‌های جانبی مانند کنترل‌کننده منطقی برنامه‌ریزی‌شده، مورد توجه قرار گرفت و اقدامات سازگار با فناوری کنترل‌کننده منطقی برنامه‌ریزی‌شده، توسعه یافت (Wei & Ji, 2018: 19).

از لحاظ آماری در سال ۲۰۱۹، بیش از ۱۵۰۰ حمله سایبری بر روی سامانه‌های کنترلی ثبت شد که نشان‌دهنده رشد ۱۹ درصدی نسبت به سال قبل از آن است. در ۸۱ درصد از این حملات، قربانیان، سازمان‌های دولتی، صنعت، بهداشت، علوم، آموزش و امور مالی بوده است.

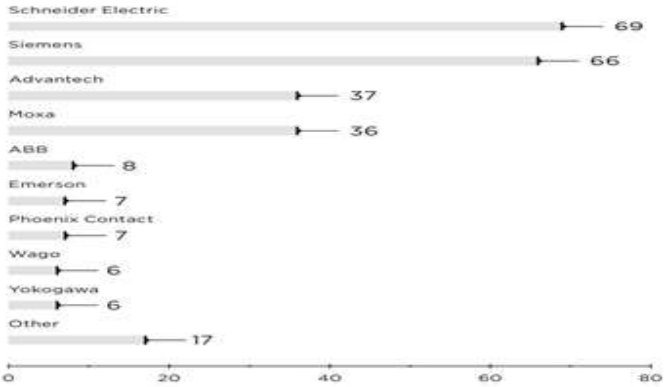


شکل (۱) مقایسه رشد رخدادهای سالیانه

برر سی حملات انجام شده بر روی مح صولات شرکت‌های تولیدکننده ا صلی تجهیزات سامانه‌های کنترلی، بیانگر این نکته ا ست که هرچند تعداد آ سیب‌پذیری‌های موجود در تجهیزات شرکت زیمنس در مقای سه با سنوات گذ شته تقریباً دو برابر شده ا ست ولی

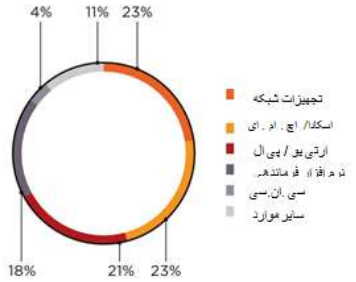
1. PLC
2.RTU

محصولات شرکت اشنایدر بیش‌ترین تعداد آسیب‌پذیری‌ها را به خود اختصاص داده است.



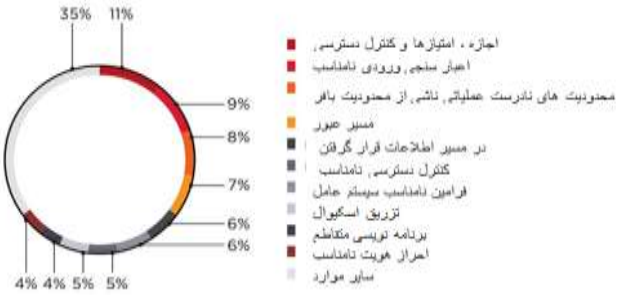
شکل (۲) مقایسه میزان آسیب‌پذیری‌های محصولات تولیدکنندگان تجهیزات سامانه‌های کنترلی

توزیع آسیب‌پذیری‌های سایبری بر اساس نوع مؤلفه سامانه‌های فرماندهی و کنترل به‌طور قابل توجهی تغییریافته است. اکثر این آسیب‌پذیری‌ها در اجزای مختلف سامانه فرماندهی و کنترل قابل مشاهده است. این آسیب‌پذیری‌ها تقریباً به‌طور مساوی بین اسکادا، آر.تی.یو/ پی.ال.سی و تجهیزات شبکه صنعتی توزیع شده‌اند. درصد آسیب‌پذیری در اجزای، آر.تی.یو/ پی.ال.سی نسبت به سال‌های گذشته به‌طور میانگین سالیانه حدود ۷ درصد افزایش یافته است.



شکل (۳) آسیب‌پذیری در انواع مؤلفه سامانه‌های فرماندهی و کنترل

بخش قابل توجهی از آسیب‌پذیری‌های یادشده مربوط به احراز هویت نادرست یا امتیازات بیش‌ازحد بوده و بیش از نیمی از این آسیب‌پذیری‌ها از راه دور قابل بهره‌برداری می‌باشند (Colbert & Kott 2016: 14).



شکل (۴) انواع آسیب‌پذیری در اجزای سامانه‌های فرماندهی و کنترل

ابعاد سامانه‌های فرماندهی و کنترل

سامانه‌های فرماندهی و کنترل در اسناد مختلف به روش‌های متفاوتی سطح‌بندی شده‌اند که در ادامه برخی از این سطح‌بندی‌ها آورده می‌شود.

در رساله دکترایی تحت عنوان الگوی شبکه یکپارچه، کامل، قوی و بروز فرماندهی و کنترل کشور که توسط کریمی در سال ۱۴۰۱ در دانشگاه عالی دفاع ملی انجام شده است، برای سامانه فرماندهی و کنترل پنج بعد شامل: بعد هم‌افزایی و هماهنگی، بعد ارتباطی و اطلاعاتی، بعد فیزیکی، بعد فرآیندها و بعد منابع انسانی در نظر گرفته شده است (کریمی، ۱۴۰۱: ۱۴۷).

در سند حفاظت از زیر ساخت‌های حیاتی که توسط دیسی در سال ۲۰۲۰ ارائه شده است سامانه‌های فرماندهی و کنترل در سه بعد اصلی به‌صورت زیر در نظر گرفته می‌شود:

الف. بعد اول که در بالای ساختار قرار دارد مربوط به نیروهای انسانی یا اپراتورها است که وظیفه پایش، نظارت و پردازش داده‌ها از طریق سنسورها به‌صورت مستقیم و کنترل آن‌ها با استفاده از محرک‌ها را بر عهده دارند.

ب. بعد دوم که سطح میانی آن است مربوط به لایه اتوماسیون است. در این لایه، سامانه فرماندهی و کنترل واقع در مرکز، وظیفه جمع‌آوری بی‌وقفه داده‌ها از فرآیندهای پردازش شده توسط سنسورها، ارائه داده‌های وضعیت و تشخیص به اپراتورها از طریق رابط ماشین و انسان، دریافت دستورات و تنظیمات از اپراتورها و کنترل فرآیندهای کنترل‌شده از طریق سنسورها را بر عهده دارد.

ج. بعد سوم، سطح نهایی است که مرتبط با لایه پردازش یا فرآیند است. در این لایه، فرآیندهای عملیاتی از طریق سنسورها پایش و نظارت می‌گردند و به‌وسیله محرک‌ها کنترل می‌شوند (Dacey, 2020: 8).

در سند مأموریت فرماندهی و کنترل نیروهای ارتش آمریکا که در سال ۲۰۱۹ ارائه گردیده است، سامانه‌های فرماندهی و کنترل به سه سطح تقسیم‌بندی شده‌اند:

الف) برنامه‌های کاربردی کاربر نهایی: شامل سیستم‌های اطلاعاتی خودکار، دستگاه‌های کاربری و نرم‌افزارها که برای کاربران امکان نمایش و انتشار اطلاعات و استفاده از قابلیت‌های شبکه را فراهم می‌آورند.

ب) خدمات و داده‌های اطلاعاتی: هدف اولیه خدمات و داده‌های اطلاعاتی تسهیل تصمیم‌گیری و اجرای به‌موقع و دقیق از طریق پردازش و مدیریت اطلاعات است. خدمات و داده‌ها شامل کلیه خدمات اطلاعاتی، سرورها و استانداردهای داده‌ای است که اطلاعات را جمع‌آوری، پردازش و ذخیره می‌کنند.

ج) مدیریت شبکه انتقال داده: شبکه انتقال شامل تجهیزات و رسانه‌های انتقالی است که اتصال را فراهم کرده و داده‌ها را بین اجزاء مختلف شبکه منتقل می‌کنند (ADP 6-0, 2019: 56).

تاب‌آوری سایبری

مفهوم تاب‌آوری سایبری برای اولین بار در سال ۲۰۱۰ توسط شرکت میتره در قالب چارچوب مهندسی تاب‌آوری سایبری مطرح گردید. در اکتبر ۲۰۱۱ نیز تیم واکنش اضطراری رایانه‌ای دانشگاه کارنگی ملون، نسخه ۱,۱ الگوی مدیریت تاب‌آوری تیم واکنش اضطراری رایانه‌ای را منتشر نموده و در سال ۲۰۱۲ برای اولین بار مفهوم تاب‌آوری سایبری توسط ریاست جمهوری آمریکا، در سطح ملی مطرح شد. پس‌ازآن در اجرای برنامه کمپین سایبری نیروی هوایی آمریکا، اداره تاب‌آوری سایبری سامانه‌های تسلیحاتی راه‌اندازی و مقر آن در هانسکام مستقر گردید. از آن زمان، سازمان‌های دولتی و خصوصی دیگری در تلاش هستند تا مفهوم تاب‌آوری سایبری را توسعه دهند (سعادتی، ۱۴۰۰: ۱۷).

در تاب‌آوری سایبری هفت اصل مهم به شرح ذیل وجود دارد:

توسعه: تنظیم معماری سایبری سازمان به‌صورت پویا بر اساس درس‌های آموخته‌شده قبلی.

بازیابی: قرار دادن فرآیندهای تعریف‌شده در محلی که اطمینان حاصل شود تمام کارکردهای سازمانی به‌طور کامل در پارامترهای لازم بازسازی می‌شوند.

آزمودن: معماری تاب‌آوری باید قابل اطمینان باشد.

طراحی/ استقرار: در نظر گرفتن معماری مناسب برای تاب‌آوری به‌طوری‌که در صورت بروز یک حمله موفق، از پایداری سازمان اطمینان حاصل شود.

رتبه: دارایی‌هایی که از دست دادن آن‌ها به سازمان آسیب غیر قابل جبران می‌زند، انتخاب و ارزیابی‌شده و یک پاسخ مؤثر برای هر یک از آن‌ها پیش‌بینی شود.

ریسک: مدیریت خطر نیاز به آگاهی موقعیتی مناسب دارد، بنابراین ارزیابی ریسک، باید طیف گسترده‌ای از تمام سناریوهای تهدید را شامل شود و مبتنی بر دارایی‌های شناسایی‌شده باشد.

طبقه‌بندی: شناسایی و برچسب‌گذاری کلیه دارایی‌های سازمان به‌منظور محافظت صحیح از سازمان بر یک مبنای منطقی (مهدوی‌پور و آذر، ۱۴۰۱: ۱۰۸).

مدیریت آسیب‌پذیری مهم‌ترین عامل تاب‌آوری سایبری

هدف اصلی مدیریت آسیب‌پذیری دارایی‌ها، شناسایی، تجزیه‌وتحلیل و مدیریت آسیب‌پذیری‌ها در محیط عملیاتی ارائه خدمات حیاتی است. آسیب‌پذیری‌ها یکی از عوامل مهم در نقض عملکرد صحیح تجهیزات و ارائه خدمات حیاتی مربوطه در زمان اختلال می‌باشند. ازآنجایی‌که آسیب‌پذیری‌ها می‌توانند به خطرات عملیاتی منجر شوند، باید مورد شناسایی و مدیریت قرار گیرند تا از وقوع اختلال در محیط عملیاتی خدمات حیاتی جلوگیری شود. یک فرآیند مدیریت آسیب‌پذیری باید قبل از بهره‌برداری از آسیب‌پذیری‌ها، پیاده سازی شود و سامانه را در فرآیند مدیریت ریسک تحلیل و آگاه نماید. دامنه مدیریت آسیب‌پذیری شامل چهار اقدام اصلی به شرح جدول ذیل است (Dacey, 2020: 13):

جدول (۱) ارزیابی و توسعه تاب‌آوری در مقابل تهدیدات سایبری

اقدام اصلی	اقدام فرعی
	تجزیه‌وتحلیل آسیب‌پذیری و ارائه راهبردهای حل‌وفصل مسئله

آماده‌سازی برای تجزیه‌وتحلیل آسیب-پذیری‌ها و فعالیت‌های لازم برای حل‌وفصل آن‌ها	ایجاد مجموعه‌ای از ابزارها و روش‌های ا ستاندارد برای شنا سایی آ سیب‌پذیری در دارایی‌ها
	ایجاد یک مجموعه استاندارد از ابزارها و روش‌ها برای تشخیص کد مخرب در دارایی‌ها
	ایجاد مجموعه‌ای از ابزارها و روش‌های استاندارد برای تشخیص کدهای غیر مجاز در دارایی‌ها
	ایجاد 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 تجزیه‌وتحلیل آسیب‌پذیری‌ها	منابع اطلاعات آسیب‌پذیر شناسایی می‌شود.
	اطلاعات از این منابع در جریان است.
	آسیب‌پذیری‌ها فعالانه کشف می‌شوند.
	آسیب‌پذیری‌ها دسته‌بندی‌شده و اولویت‌بندی می‌شوند.
	آسیب‌پذیری‌ها برای تعیین ارتباط با سازمان تجزیه‌وتحلیل می‌شوند.
	مخزن برای ضبط اطلاعات در مورد آسیب‌پذیری‌ها و حل‌وفصل آن‌ها استفاده می‌شود.
اقدامات لازم برای مدیریت مواجهه آسیب‌پذیری‌های شناسایی‌شده	اقدامات لازم برای مدیریت مواجهه با آسیب‌پذیری‌های شناسایی‌شده انجام می‌شود.
	اثربخشی کاهش آسیب‌پذیری بررسی می‌شود.
	وضعیت آسیب‌پذیری‌های حل‌نشده بررسی می‌شود.
بررسی علل ریشه‌ای آسیب‌پذیری‌ها	علل اصلی آسیب‌پذیری‌ها (از طریق تجزیه‌وتحلیل علل ریشه یا روش‌های دیگر) شناسایی می‌گردند.

الگوی بلوغ توانایی سایبری

الگوی بلوغ توانایی سایبری[1] رو شی ا ست که سازمان‌ها را قادر به تقویت برنامه امنیت سایبری، اولویت‌بندی اقدامات و سرمایه‌گذاری‌های امنیت سایبری و حفظ سطح مطلوب امنیت در طول چرخه حیات سیستم‌های فناوری اطلاعات می‌نماید. این الگو از مجموعه متنوعی از استانداردها، چارچوب‌ها، برنامه‌ها و ابتکارات امنیت سایبری نشات می‌گیرد و شامل مراحلی است که قابلیت اجرایی برای هر سازمانی را دارد. الگوی بلوغ توانایی سایبری روشی مبتنی بر بلوغ سازمان است که برای تاب‌آور نمودن سازمان و سامانه‌ها در مقابل تهدیدات سایبری قابل استفاده است به‌طوری‌که با اجرای کامل الگو در سازمان تاب‌آوری نهادینه می‌شود. نهادینه‌سازی بدان معنی است که شیوه‌های تاب‌آوری سایبری تبدیل به یک بخش عمیق‌تر و پایدارتر از سازمان گردد. هرچه شیوه‌های سایبری

1. Cyber Capability Maturity Model

تاب‌آوری بیشتر نهادینه شوند، مدیران می‌توانند اعتماد بیشتری به قابلیت اطمینان عملی سامانه‌ها دا شته با شند. بلوغ می‌تواند منجر به تطبیق تنگاتنگی بین فعالیت‌های امنیتی سایبری و هدایت‌کنندگان کسب‌وکار سازمان شود. به‌عنوان مثال، در سازمان‌های بالغ‌تر، مدیران نظارت بر حوزه خاص را تأمین می‌کنند و اثربخشی فعالیت‌های امنیتی را ارزیابی می‌کنند. در جدول ۲. مقیاس ارزیابی سطوح بلوغ با ا ستفاده از پنج سطح بلوغ ارائه‌شده است:

جدول (۲) ارزیابی بلوغ تاب‌آوری سایبری

سطوح بلوغ	اقدام
سطح اول (انجام‌شده)	همه شیوه‌هایی که از اهداف در یک دامنه پشتیبانی می‌کنند، به‌صورت اندازه‌گیری شده با پاسخ به سؤالات الگوی ارزیابی و توسعه تاب‌آوری مربوطه انجام می‌شود.
سطح دوم (برنامه‌ریزی‌شده)	یک تمرین خاص در حوزه الگوی ارزیابی و توسعه تاب‌آوری انجام می‌شود و توسط برنامه‌ریزی، ذینفعان و ا ستانداردها و رهنمودهای مربوطه نیز پ شتیبانی می شود. یک فرآیند یا تمرین برنامه‌ریزی‌شده است که: • توسط سازمان از طریق سیاست و یک برنامه مستند ایجادشده باشد. • توسط سهامداران پشتیبانی شود. • توسط استانداردها و دستورالعمل‌های مربوطه پشتیبانی شود.
سطح سوم (مدیریت‌شده)	تمام اقداماتی که در یک دامنه انجام می‌شوند، برنامه‌ریزی‌شده و زیرساخت‌های حاکمیت پایه‌ای برای حمایت از این فرآیند وجود دارد. یک فرآیند یا عمل در صورتی مدیریت‌شده است که: • از کارکنان مناسب و افراد واجد شرایط استفاده شود. • به اندازه کافی تأمین مالی شود. • برنامه مشخص مدیریت ریسک را داشته باشد.
سطح چهارم (اندازه‌گیری شده)	تمام اقداماتی که در یک دامنه انجام، برنامه‌ریزی، مدیریت، نظارت و کنترل می شود در یک فرآیند مشخص اندازه‌گیری می‌شوند و موارد ذیل می‌بایست رعایت شود. • به‌صورت دوره‌ای اثربخشی ارزیابی شود. • به‌طور عینی در مقایسه با شرح و برنامه عملی خودارزیابی انجام پذیرد. • به‌صورت دوره‌ای با مدیریت سطح بالاتر موارد اقدام شده، بررسی شود.
سطح پنجم (نهادینه‌شده)	تمام اقداماتی که در یک دامنه انجام، برنامه‌ریزی، مدیریت و اندازه‌گیری می‌شود و علاقه‌مند به عملکرد تاب‌آوری هستند با هم سازگار می شوند. سطح بلوغ پنجم، فرآیند یا عملی است که: • توسط سازمان و واحدهای عملیاتی درونی سازمان برای استفاده طراحی و تعریف شده است. • اطلاعات پشتیبانی و بهبود سازمان از میان واحدهای مختلف عملیاتی برای بهره‌گیری در کل سازمان جمع‌آوری می‌گردد.

در روش فوق، یک سازمان تنها زمانی می‌تواند به یک سطح بلوغ بالاتر برسد که به تمام سطوح بلوغ پایین‌تر د ست یافته با شد؛ 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 (Colbert & Kott, 2016: 293).

پیشینه پژوهش

در راستای بررسی پیشینه الگوی تاب‌آوری سامانه فرماندهی و کنترل در مقابله با تهدیدهای سایبری، تعدادی از مقالات و ا سناد ارائه شده تو سط مؤ سسات پژوه شی و تحقیقاتی داخلی و خارجی، مورد برر سی و واکاوی قرار گرفت که در ادامه برخی از این پژوهش‌ها آورده شده است:

لانسو 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 به‌عنوان مکمل دفاع سایبری سنتی جهت کمک به اطمینان از انجام کامل مأموریت معرفی می‌نماید (Lansó & etal, 2021).

انیستیتو ملی استاندارد و فناوری آمریکا[1] در سال ۲۰۲۱، استاندارد ایجاد تاب‌آوری سایبری در سیستم‌ها و سامانه‌های سایبر پایه را ارائه نمود (NIST, 2021).

کاریاس و همکاران (۲۰۲۰)، در مقاله‌ای تحت عنوان الگوی پیشرفت تاب‌آوری سایبری، الگویی را برای کمک به شرکت‌ها جهت اجرای استراتژی‌های تدوین‌شده و همچنین اولویت‌بندی سیا ست‌های انعطاف‌پذیری سایبری مبتنی بر یافتن نقاط شروع و تکامل طبیعی سیاست‌ها در طول زمان ارائه می‌دهد (Carías & etal, 2020).

مظفری و همکاران (۲۰۱۹)، در مقاله‌ای تحت عنوان احصاء تأثیر شاخص‌های تاب‌آوری بر کاهش آ سیب‌پذیری سیستم‌های کنترل صنعتی در تهدیدات سایبری، شاخص‌های حس تشخیص، اجرای اقدامات کنترلی در عملیات روزمره، توسعه توابع نظارتی (کنترل‌های 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 ارائه نموده است (مظفری و همکاران، ۲۰۱۹).

1. NIST

پژوهشکده امنیت سایبری دانشگاه کارنگی ملون به‌عنوان یکی از مراکز معتبر در حوزه ارائه استانداردها و دستورالعمل‌های سایبری در سال ۲۰۱۶ به سفارش وزارت امنیت داخلی آمریکا، مجموعه دستورالعمل‌های تاب‌آوری سایبری را در ۱۰ سرفصل کلی با هدف ارتقاء امنیت سایبری به تاب‌آوری سایبری ارائه نمود (DHS, 2016).

بت‌شکن (۱۳۹۶)، 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، سخت‌افزارهای شبکه و سرورها، موجب افزایش تاب‌آوری سایبری سازمان‌ها در مقابل تهدیدات سایبری خواهد شد (بت شکن، ۱۳۹۶: ۲۳).

وی و جی[1] (۲۰۱۵)، در مقاله‌ای با عنوان "سامانه‌های صنعتی تاب‌آور: مفاهیم، فرمول‌بندی، معیارها و بینش‌ها"، ضمن تبیین شاخصه‌های مورد نیاز سامانه‌های صنعتی تاب‌آور، معیارهای ارزیابی تاب‌آوری سایبری در مقابل تهدیدات سایبری را در سامانه‌های صنعتی بیان نموده‌اند (Wei & Ji, 2015).

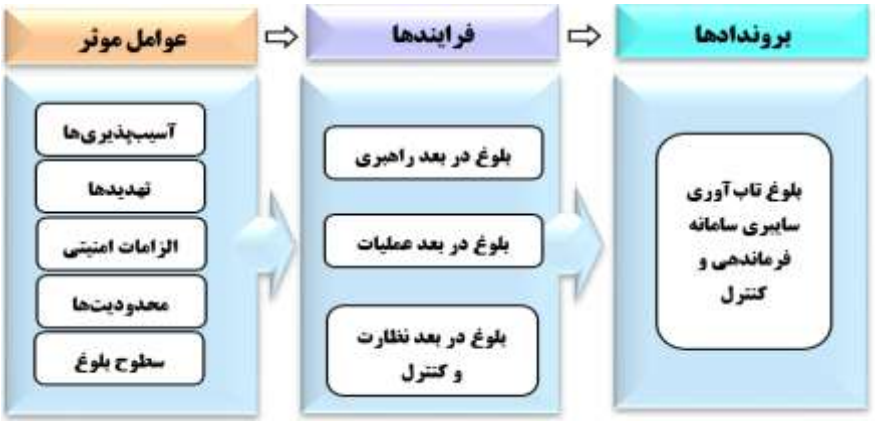
در پژوهش‌های بررسی شده، به مواردی که موجب تاب‌آوری سایبری سامانه می شود از قبیل اهمیت سامانه‌های مبتنی بر شبکه، پایش و کنترل فرآیندها، ارائه راه‌کارهای بهبود امنیتی سامانه‌ها و همچنین مدیریت و اصلاح انواع مختلف آسیب‌پذیری‌های سامانه‌ها، اشاره شده است. ارائه راه‌کارهای از پیش تعیین شده، تأکید بر بهبود امنیت سایبری و همچنین روش‌های اندازه‌گیری آن‌ها نیز موضوع دیگری است که به آن‌ها اشاره شده است. در هیچ‌یک از تحقیقات مورد بررسی، موضوع بلوغ تاب‌آوری سایبری مورد بررسی قرار نگرفته است. الگوی بلوغ تاب‌آوری سایبری، الگویی است که علاوه بر توجه به امنیت و دفاع سایبری در سامانه، در مواجهه با تهدیدات، کل سازمان را در نظر می‌گیرد و اقدامات مورد نیاز را به‌گونه‌ای تدوین می‌نماید که تاب‌آوری سایبری در کل سازمان نهادینه گردد. با توجه به اهمیت نهادینه شدن اقدامات تاب‌آوری سایبری در سامانه‌های فرماندهی و کنترل، در پژوهش حاضر، در پی ارائه الگویی جهت نیل به بلوغ تاب‌آوری

1. Wei & Ji

سایبری سامانه‌های فرماندهی و کنترل در مقابله با تهدیدات آینده هستیم که نکته اصلی متمایزکننده این پژوهش با سایر پژوهش‌های انجام‌شده است.

مدل مفهومی پژوهش

در این پژوهش جهت تدوین الگو از روش نظریه سیستم‌ها شامل اجزاء: عوامل مؤثر، فرایندها و بروندادها (علاقه بند، ۱۴۰۰: ۱۲۴) استفاده شده است. در این راستا ابتدا عوامل مؤثر بر تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل (شامل آسیب‌پذیری‌های سایبری، تهدیدهای سایبری تجهیزات، محدودیت‌های ناشی از تحریم‌های فناورانه، الزامات امنیتی سامانه‌های سایبر پایه و سطوح بلوغ) مورد مطالعه قرار گرفته و بر اساس نتایج حا صله، فرایندها شامل (ابعاد و مؤلفه‌های مرتبط با الگوی بلوغ تاب‌آوری سایبری سامانه فرماندهی و کنترل) استخراج گردید. با توجه به موارد پیش‌گفته، مدل مفهومی تحقیق برابر شکل زیر جمع‌بندی می‌گردد:



شکل (۵) مدل مفهومی پژوهش

روش‌شناسی پژوهش

این پژوهش از نظر روش تحقیق در زمره تحقیقات توصیفی/تحلیلی با دید اکتشافی د سته‌بندی می شود. دلیل تو صیفی/تحلیلی بودن پژوهش حا ضر آن ا ست که محقق به تو صیف بلوغ تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل پرداخته و با ا ستفاده از روش‌های راهبردی به تحلیل سطوح بلوغ تاب‌آوری سایبری در سامانه‌های فرماندهی و کنترل پرداخته است و با نگاه اکتشافی، چارچوب اولیه‌ای برای تدوین الگوی بلوغ

تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل ارائه نموده است. همچنین در این تحقیق محقق در پی طراحی الگوی بلوغ تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل جهت مقابله با تهدیدات آینده ا ست تا در صورت بروز حملات سایبری نوین در آینده، سامانه فرماندهی و کنترل با کمترین آسیب به فعالیت خود ادامه دهد. لذا این پژوهش از نظر طرح تحقیق در زمره تحقیقات آینده‌نگر دسته‌بندی می‌شود.

پژوهش حاضر از لحاظ هدف (نوع تحقیق) در زمره تحقیقات کاربردی دسته‌بندی می‌گردد. این پژوهش به این دلیل 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 چالش‌های ناشی از فقدان امنیت سایبری مناسب در زیرساخت‌ها و فرآیندهای فرماندهی و کنترل می‌گردد. در این تحقیق تهدیدهای سایبری آینده، متغیر مستقل و بلوغ تاب‌آوری سامانه‌های فرماندهی و کنترل متغیر وابسته است.

تجزیه‌وتحلیل یافته‌های پژوهش

برابر اسناد بررسی‌شده برای سامانه‌های فرماندهی و کنترل تعداد ۹ بعد شامل: بعد هم‌افزایی و هماهنگی، ارتباطی و اطلاعاتی، فیزیکی، فرآیندها، منابع انسانی، اتوماسیون، پردازش، برنامه‌های کاربردی و شبکه انتقال داده احصاء گردید. بعدهای یاد شده در یک جمع خبرگی مورد بررسی قرار گرفت و در نهایت برای الگوی بلوغ تاب‌آوری سامانه‌های فرماندهی و کنترل، سه بعد به شرح ذیل انتخاب گردید:

- بعد اول که به تعامل نیروی انسانی و برنامه‌های کاربردی مربوط می‌شود تحت عنوان بعد راهبری
- بعد دوم که به عملکرد اتوما سیون و مدیریت شبکه مربوط می شود تحت عنوان بعد نظارت و کنترل
- بعد سوم که به پردازش داده و اطلاعات مربوط می‌گردد تحت عنوان بعد عملیات.

سطوح بلوغ سازمانی که دربرگیرنده ر شد سازمان در مدیریت آ سیب‌پذیری‌ها ا ست با نظر خبرگان مبتنی بر الگوی یکپارچه بلوغ قابلیت‌های سازمانی با ۵ سطح بلوغ (انجام‌شده، برنامه‌ریزی‌شده، مدیریت‌شده، اندازه‌گیری شده و نهادینه‌شده) در نظر گرفته شد.

با توجه به ابعاد سامانه‌های فرماندهی کنترل و مبتنی بر مطالعات انجام‌شده تعداد ۴۹ مؤلفه اصلی برای تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل مبتنی بر سطوح بلوغ به‌صورت ذیل ارائه شده است.

جدول (۴) الگوی تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل

سطوح بلوغ	بعد راهبری
اول (انجام‌شده)	۱- مدیریت تداوم فعالیت‌های سامانه‌های فرماندهی و کنترل ۲- مدیریت وابستگی و ارتباطات خارجی فرماندهی و کنترل ۳- آموزش و آگاهی مدیران و کارشناسان فرماندهی و کنترل ۴- آگاهی وضعیتی تاب‌آوری فرماندهی و کنترل
دوم (برنامه‌ریزی‌شده)	۱- مستندسازی انجام فعالیت‌های راهبری ۲- تعیین خط‌مشی برای انجام فعالیت‌های راهبری ۳- شناسایی و اطلاع‌رسانی نقش ذینفعان برای فعالیت‌های راهبری ۴- شناسایی و اجرای کردن استانداردها و دستورالعمل‌های راهبری
سوم (مدیریت‌شده)	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 انجام‌شده ۴- کنترل ریسک‌های مربوط به کارایی فعالیت‌های برنامه‌ریزی راهبری
چهارم (اندازه‌گیری شده)	۱- بازنگری دوره‌ای و ارزیابی اثربخشی میزان 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 (نهادینه‌شده)	۱- اتخاذ یک تعریف استاندارد از فعالیت‌های راهبری ۲- مستندسازی و اشتراک‌گذاری پیشرفت فعالیت‌های راهبری
سطوح بلوغ	**بعد نظارت و کنترل**
اول (انجام‌شده)	۱- کنترل بر عملکرد سامانه‌های فرماندهی و کنترل ۲- مدیریت ریسک سامانه‌های فرماندهی و کنترل ۳- مدیریت آسیب‌پذیری‌های سامانه‌های فرماندهی و کنترل ۴- مدیریت رخدادها و حوادث سایبری سامانه‌های فرماندهی و کنترل
دوم (برنامه‌ریزی‌شده)	۱- مستندسازی انجام فعالیت‌های نظارت و کنترل ۲- تعیین خط‌مشی برای انجام فعالیت‌های نظارت و کنترل ۳- شناسایی و اطلاع‌رسانی نقش ذینفعان برای فعالیت‌های نظارت و کنترل ۴- شناسایی و اجرایی کردن استانداردها و دستورالعمل‌های نظارت و کنترل
سوم	۱- نظارت مدیریتی بر کارایی فعالیت‌های نظارت و کنترل ۲- تخصیص کارکنان واجد شرایط برای انجام فعالیت مطابق با برنامه‌ریزی نظارت و کنترل

(مدیریت‌شده)	۳- تعیین بودجه کافی برای انجام فعالیت‌ها مطابق با برنامه‌ریزی انجام‌شده نظارت و کنترل ۴- کنترل ریسک‌های مربوط به کارایی فعالیت‌های برنامه‌ریزی نظارت و کنترل
چهارم (اندازه‌گیری شده)	۱- بازنگری دوره‌ای و ارزیابی اثربخشی میزان‌سنجی فعالیت‌های نظارت و کنترل ۲- بازنگری دوره‌ای فعالیت‌ها جهت اطمینان پیشرفت مناسب نظارت و کنترل ۳- آگاهی‌رسانی به مدیریت سطح بالا از مسائل مربوط به کارایی نظارت و کنترل
پنجم (نهادینه‌شده)	۱- اتخاذ یک تعریف استاندارد از فعالیت‌ها ۲- مستندسازی و اشتراک‌گذاری پیشرفت فعالیت‌ها
سطوح بلوغ	**بعد عملیات**
اول (انجام‌شده)	۱- مدیریت دارایی و تجهیزات سامانه‌های فرماندهی و کنترل ۲- مدیریت تغییر و پیکربندی سامانه‌های فرماندهی و کنترل
دوم (برنامه‌ریزی‌شده)	۱- مستندسازی انجام فعالیت‌های فرآیند و عملیات ۲- تعیین خط‌مشی برای انجام فعالیت‌های فرآیند و عملیات ۳- شناسایی و اطلاع‌رسانی نقش ذینفعان برای فعالیت‌های فرآیند و عملیات ۴- شناسایی و اجرای کردن استانداردها و دستورالعمل‌های فرآیند و عملیات
سوم (مدیریت‌شده)	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 برنامه‌ریزی‌های انجام‌شده ۴- کنترل ریسک‌های مربوط به کارایی فعالیت‌های برنامه‌ریزی فرآیند و عملیات
چهارم (اندازه‌گیری شده)	۱- بازنگری دوره‌ای و ارزیابی اثربخشی میزان‌سنجی فعالیت‌های فرآیند و عملیات ۲- بازنگری دوره‌ای فعالیت‌ها جهت اطمینان پیشرفت مناسب فرآیند و عملیات ۳- آگاهی‌رسانی به مدیریت سطح بالا از مسائل مربوط به کارایی فرآیند و عملیات
پنجم (نهادینه‌شده)	۱- اتخاذ یک تعریف استاندارد از کلیه فعالیت‌های فرآیند و عملیات ۲- مستندسازی و اشتراک‌گذاری پیشرفت فعالیت‌های فرآیند و عملیات

در این تحقیق برای آزمون مدل مفهومی از مدل‌سازی معادلات ساختاری مبتنی بر رویکرد حداقل مربعات جزئی با نرم‌افزار اسمارت پی.ال.اس[1] استفاده شده است. با استفاده از این نرم‌افزار، هم برازش الگو اندازه‌گیری می‌گردد و هم برازش الگوی ساختاری برای سنجش رابطه میان متغیرها با استفاده از ضرایب معناداری انجام می‌شود و همچنین می‌توان اولویت‌بندی مؤلفه‌ها و گویه‌ها را نیز از این طریق مشخص نمود. برای هر یک از ابعاد راهبری، نظارت و کنترل و عملیات یک تحلیل عاملی جداگانه محاسبه شده است و سهم هریک از گویه‌های مربوط به مؤلفه‌ها مشخص شده‌اند. در نهایت با استفاده از الگوی تحلیل عاملی مرتبه دوم، الگوی نهایی بررسی گردید. نتایج

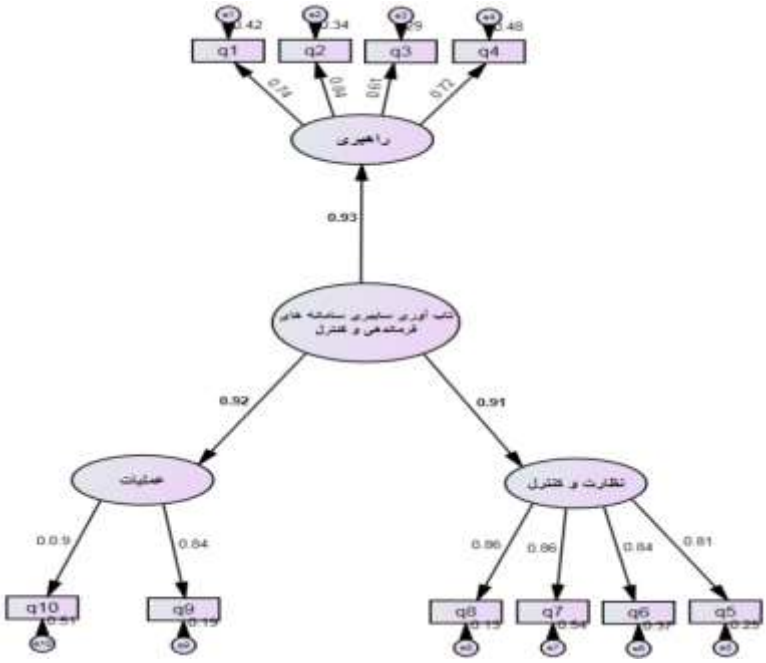
1.SMART PLS 9.98

تحلیل بار عاملی کلیه مؤلفه‌ها در جدول ۴ آورده شـــده و به جهت رعایت اختصـــار در شکل ۷ فقط نتایج سطح بلوغ اول ارائه شده است.

جدول (۴) نتایج تحلیل عاملی تأییدی الگو

بعد	مؤلفه سطح ۱	بار عاملی	مؤلفه سطح ۲	بار عاملی	مؤلفه سطح ۳	بار عاملی	مؤلفه سطح ۴	بار عاملی	مؤلفه سطح ۵	بار عاملی
راهبری	۱	۰/۷۴	۱	۰/۸۵	۱	۰/۸۹	۱	۰/۸۶	۱	۰/۸۸
	۲	۰/۸۴	۲	۰/۷۹	۲	۰/۸۴	۲	۰/۸۹	۲	۰/۸۶
	۳	۰/۶۱	۳	۰/۸۳	۳	۰/۸۷	۳	۰/۸۵	–	–
	۴	۰/۷۲	۴	۰/۸۵	۴	۰/۸۵	–	–	–	–
نظارت و کنترل	۱	۰/۸۱	۱	۰/۸۰	۱	۰/۸۴	۱	۰/۸۱	۱	۰/۸۳
	۲	۰/۸۴	۲	۰/۷۸	۲	۰/۷۹	۲	۰/۸۳	۲	۰/۸۵
	۳	۰/۸۶	۳	۰/۷۸	۳	۰/۸۲	۳	۰/۸۰	–	–
	۴	۰/۸۶	۴	۰/۸۲	۴	۰/۸۳	–	–	–	–
عملیات	۱	۰/۹۰	۱	۰/۸۴	۱	۰/۸۱	۱	۰/۷۹	۱	۰/۸۸
	۲	۰/۸۴	۲	۰/۸۱	۲	۰/۸۵	۲	۰/۸۶	۲	۰/۸۱
	–	–	۳	۰/۸۵	۳	۰/۸۱	۳	۰/۸۶	–	–
	–	–	۴	۰/۸۳	۴	۰/۸۰	–	–	–	–
تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل	بعد راهبری									۰/۹۲۱
	بعد نظارت و کنترل									۰/۹۱۷
	بعد عملیات									۰/۹۲۶

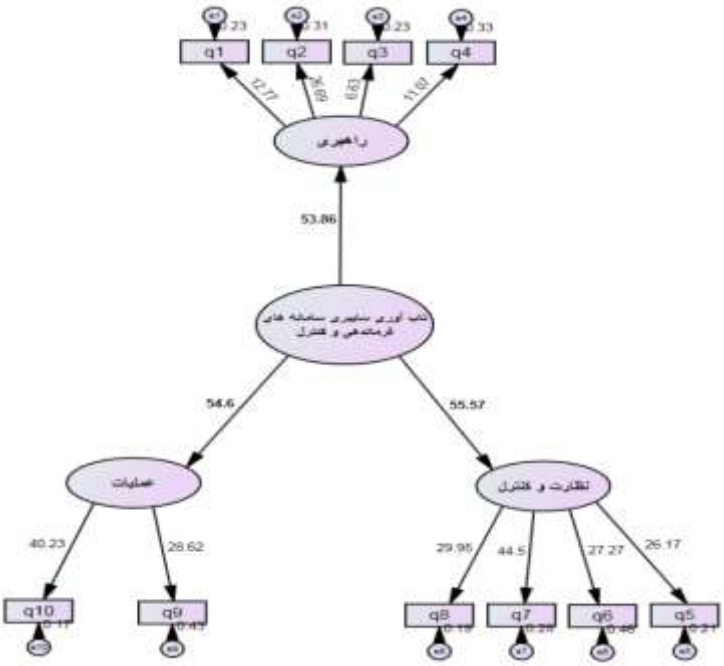
در این روش میزان ســـهم هر گویه یا عامل در ایجاد متغیر مورد بررســـی قرار گرفته و برای این کار از تحلیل عاملی تأییدی ا ستفاده می شود. در تحلیل عاملی تأییدی، مقدار بار عاملی کمتر از ۰/۳ نشان‌دهنده مقیاس ضعیف بوده و باید از الگو حذف شود. بارهای عاملی بین ۰/۳ تا ۰/۶ ن شان می‌دهند که متغیر م شاهده شده مقیاس متو سطی بوده و برای ادامه آنالیز کفایت می‌کند. مقادیر بزرگ‌تر از ۰/۶ نیز نشـــان می‌دهد که متغیر مشـــاهده‌پذیر مقیاس قابل اطمینانی برای محاســـبه اســـت. در کل مقادیر بارهای عاملی بزرگ‌تر از ۰/۴ را می‌توان در الگو حفظ کرد (Baukes, 2017).



شکل (۷) ضرایب تحلیل عاملی الگو

اطلاعات جدول ۵ نشـــان می‌دهد که تمامی مؤلفه‌ها (گویه‌ها) مقادیر بارهای عاملی بزرگ‌تر از ۰/۴ دا شته و از اعتبار لازم برخوردار ه ستند. در الگوی فوق ضرایب م سیرها برای ســـه بعد راهبری، نظارت و کنترل و فرآیند و عملیات ۰/۹۲۱، ۰/۹۱۷ و ۰/۹۲۶ اســـت لذا بعد فرآیند و عملیات بالاترین تأثیر و بعدهای راهبری و نظارت و کنترل با اختلاف کمی در جایگاه دوم و سوم هستند.

آزمون معناداری: نتایج آزمون معناداری در شکل ۸ در ستون مقادیر t نشان داده شده اســت و به دلیل بیشــتر بودن مقادیر t از ۱/۹۶، در ســطح احتمال ۹۵ درصــد معناداری وجود دارد و الگو از اعتبار لازم برخوردار است.



شکل (۸) آزمون معناداری الگو

پارامتر پایایی مرکب[1]: به دلیل اینکه تمام اعداد t از ۰/۶ بیشتر هستند، الگو دارای سطح بالایی از پایداری است.

پارامتر آلفای کرونباخ[2]: بیشتر بودن تمامی اعداد t از ۰/۶، نشانگر پایداری گویه‌ها است.

پارامتر ضریب تعیین[3]: مقادیر استاندارد برای سطوح "قابل ملاحظه"، "متوسط" و "ضعیف" عبارت‌اند از: ۶۷/، ۰/۳۳ و ۰/۱۹ و در الگوی ما، به دلیل بیشتر بودن مقادیر، دارای سطح قابل قبولی است.

همچنین برای برازش الگو، می‌توان از شاخص نیکویی برازش[4] استفاده کرد. این شاخص به‌عنوان معیاری برای سنجش عملکرد الگو بکار می‌رود. این شاخص، مجذور ضرب دو مقدار متوسط اشتراکی[5] و متوسط ضریب تعیین است. مقدار GOF بین صفر و یک در

1.Composite Reiability
2. Cronbech Alpa
3. R.Square
4. GOF
5. Communality

نوسان است. مقدار ۰/۰۱، ۰/۲۵ و ۰/۳۶ به ترتیب به‌عنوان مقادیر ضعیف، متوسط و قوی معرفی شده‌اند.

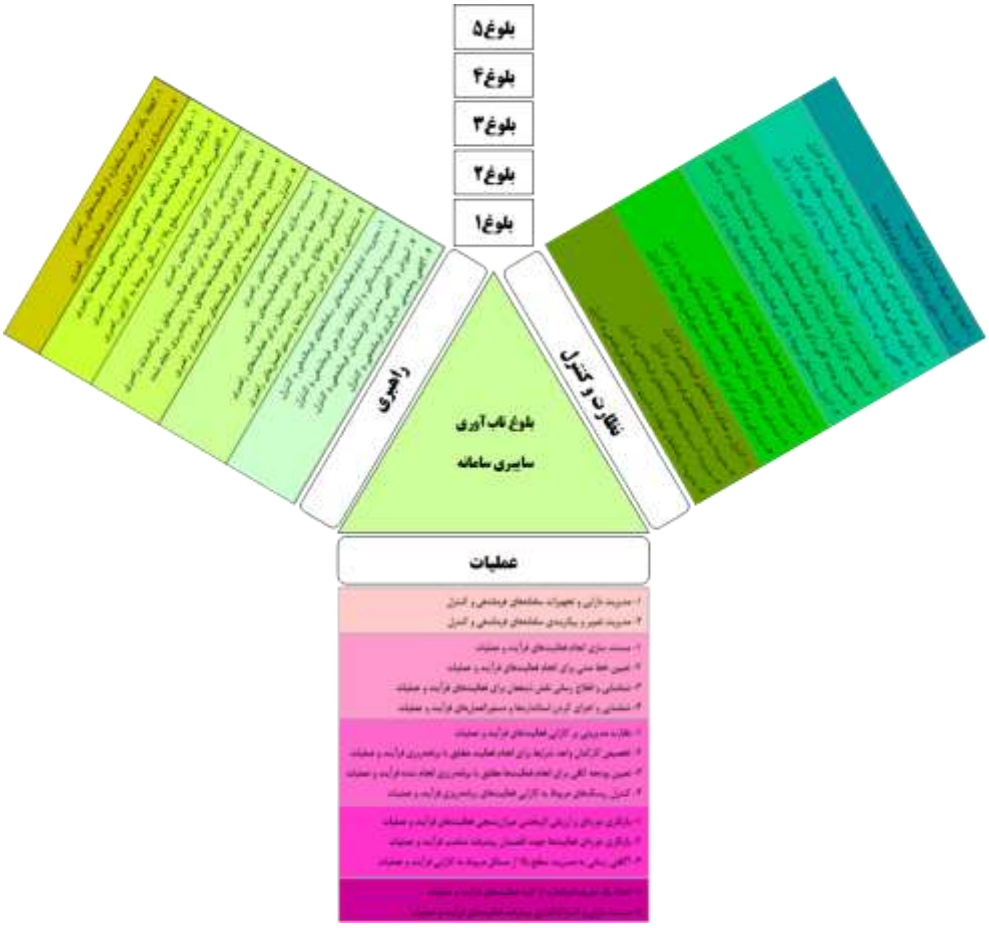
$$GOF=\sqrt{\boldsymbol{Communality} \times \boldsymbol{R^2}}$$

شاخص نیکویی برازش در سه بعد راهبری و نظارت، کنترل و اتوماسیون و فرآیند و عملیات به ترتیب عبارت‌اند از: ۰/۷۹، ۰/۷۸ و ۰/۷۲ و چون همگی بیشتر از ۰/۳۶ هستند، لذا در حد قابل قبول و قوی هستند.

نتیجه‌گیری و پیشنهادها

الگوی بلوغ سایبری روشی است که سازمان‌ها را قادر به تقویت برنامه امنیت سایبری، اولویت‌بندی اقدامات و سرمایه‌گذاری‌های امنیت سایبری و حفظ سطح مطلوب امنیت در طول چرخه حیات سیستم‌های فناوری اطلاعات می‌نماید. با توجه به اینکه تاب‌آوری سایبری زمانی به بلوغ می‌رسد که اقدامات تاب‌آوری در تمامی ارکان سازمان نهادینه شود، لذا در این پژوهش پس از بررسی اسناد و مدارک مختلف و مراجعه به نظر خبرگان، سه بعد راهبری، نظارت و کنترل و عملیات برای سامانه‌های فرماندهی و کنترل انتخاب گردید. همچنین سطوح بلوغ سایبری که مرتبط با رشد سازمان در مدیریت آسیب‌پذیری‌های سایبری است با نظر خبرگان مبتنی بر الگوی بلوغ توانایی سایبری با ۵ سطح بلوغ (انجام شده، برنامه‌ریزی شده، مدیریت شده، اندازه‌گیری شده و نهادینه‌شده) در نظر گرفته شد.

با توجه به بعدهای سامانه‌های فرماندهی کنترل و مبتنی بر مطالعات انجام‌شده، در سطح بلوغ یک (اجرایی) برای بعد رهبری، بعد نظارت و کنترل و بعد عملیات در مجموع ۱۰ مؤلفه، برای سطح بلوغ دو (برنامه‌ریزی) ۱۲ مؤلفه، برای بلوغ سطح سوم (مدیریت) ۱۲ مؤلفه، برای بلوغ سطح چهارم (اندازه‌گیری) ۹ مؤلفه و برای بلوغ سطح پنجم (نهادینه) ۶ مؤلفه و در مجموع ۴۹ مؤلفه، مطابق شکل ۹ ارائه گردید و الگو ارائه شده با بهره‌گیری از نرم‌افزار اسمارت پی.ال.اس، تحلیل بار عاملی و آزمون معنی‌دار بودن مؤلفه‌ها، در سطح ۹۵ درصد معنی‌داری مورد تأیید قرار گرفت.



شکل (۹) الگوی بلوغ تاب‌آوری سایبری سامانه فرماندهی و کنترل

پیشنهادها

پیشنهادهای اجرایی

در را ستای پیاده سازی نتایج این پژوهش و نیل به بلوغ تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل پیشنهاد می‌گردد:

- معاونت ارتباطات و فناوری اطلاعات نیروهای بهره‌بردار از سامانه فرماندهی و کنترل با استفاده از الگوی ارائه شده در این پژوهش نسبت به تدوین دستورالعمل تاب‌آوری سایبری سامانه فرماندهی و کنترل اقدام نموده و با توجه به‌سرعت تغییرات در حوزه سایبری، دستورالعمل مذکور را به‌صورت دوره‌ای به‌روزرسانی نماید.

- یگان‌های بهره‌بردار از سامانه فرماندهی و کنترل با توجه به سطوح بلوغ تاب‌آوری ارائه‌شده در این پژوهش، برنامه‌های آموزشی مورد نیاز جهت کارکنان مربوطه را تدوین و اجرا نماید.

پیشنهادهای پژوهشی

تمرکز این پژوهش بر ارائه یک الگوی بلوغ تاب‌آوری سایبری جهت سامانه‌های فرماندهی و کنترل بوده است، اما لازم است هر کلیه سامانه‌های زیرمجموعه سامانه‌های فرماندهی و کنترل نیز به‌طور ویژه در مقابل حوادث سایبری تاب‌آور شوند. لذا پیشنهاد می‌گردد در حوزه‌های ذیل پژوهش جامعی در خصوص تاب‌آوری در مقابله با تهدیدات و کاهش آسیب‌پذیری‌های سایبری انجام پذیرد.

- تاب‌آوری سامانه‌های ارتباطی در مقابله با تهدیدات سایبری
- تاب‌آوری سامانه‌های موشکی در مقابله با تهدیدات سایبری
- تاب‌آوری سامانه‌های راداری در مقابله با تهدیدات سایبری
- تاب‌آوری سامانه‌های شناسایی سیگنالی در مقابله با تهدیدات سایبری

قدردانی

از خبرگان توانمندی که در طول پژوهش، دانش خویش را سخاوتمندانه در اختیار محققان این پژوهش قرار دادند و استواری پژوهش حاضر بر مشارکت و دانش این بزرگواران قرارگرفته است بسیار سپاسگزاریم.

منابع

- بت‌شکن، بهمن. (۱۳۹۶). *بررسی مهندسی تاب‌آوری در فضای سایبری*، سومین کنفرانس ملی علوم و مهندسی کامپیوتر و فناوری اطلاعات، بابل. دسترسی از طریق: https://civilica.com/doc/676855
- رمضان‌زاده، مجتبی؛ غیوری ثالث، مجید؛ احمدوند، علی‌محمد؛ آقایی، محسن و نظری فرخی، ابراهیم. (۱۴۰۰). بررسی قدرت پدافند سایبری نیروهای مسلح با روش برنامه‌ریزی مبتنی بر سناریو، *فصلنامه علمی پژوهشی آینده‌پژوهی دفاعی*، ۶ (۲۰): ۵۹-۸۱.
- سعادتی، ر ضا. (۱۴۰۰). *شناسایی و اولویت‌بندی عوامل مؤثر بر تاب‌آوری سایبری ارتش جمهوری اسلامی ایران*، پایان‌نامه کارشناسی ارشد، تهران: دافوس آجا.
- علاقه‌بند، علی. (۱۴۰۰). *مبانی نظری و اصول مدیریت آموزشی*، چاپ سی‌ام، تهران: نشر روان.

- کریمی، وحید. (۱۴۰۱). *طراحی الگوی شبکه یکپارچه، کامل، قوی و بروز فرماندهی و کنترل قرارگاه مشترک پدافند هوایی خاتم‌الانبیاء (ص) کشور*، تهران: دانشکده دفاع، دانشگاه عالی دفاع ملی.
- مقدسی لیچاهی، امیرحسین؛ همت، حمید. (۱۳۹۷). ارائه الگوی امنیت در فضای سایبر جمهوری اسلامی ایران با رویکرد آینده‌پژوهانه، *فصلنامه علمی پژوهشی آینده‌پژوهی دفاعی*، ۳ (۱۰): ۱۲۰-۱۰۳.
- مظفری، شهرام؛ پور منصوری، رضوان و پورمنصوری، جمال. (۲۰۱۹). *احصاء شاخص‌های تاب‌آوری بر کاهش آسیب‌پذیری سیستم‌های کنترل صنعتی در تهدیدات سایبری*، چهارمین کنفرانس بین‌المللی تحقیقات مرتبط با اقتصاد و مدیریت، پاریس، فرانسه. دسترسی از طریق: https://www.researchgate.net /343212561
- مهدوی‌پور، مهدی و آذر، داود. (۱۴۰۱). عوامل مؤثر بر امنیت سایبری ارتش جمهوری اسلامی ایران، *فصلنامه علمی پژوهشی علوم و فنون نظامی*، دوره ۱۸، شماره ۶۰، شهریور ۱۴۰۱.
- Ardagna, C; Corbiaux, S; Sfakianakis, A & Douligeris, Christos; (2021). *ENISA THREAT LANDSCAPE 2021*, ISBN: 978-92-9204-536-4 – DOI: 10.2824/324797 – ISSN: 2363-3050
- Baukes, Mike; (2017), Cybersecurity Is Dead, Forbes Technology.
- Carías, Juan F. Arrizabalaga, Saioa; Labaka, Leire & Hernantes, Josune (2020), *Cyber Resilience Progression Model*, Appl. Sci. 2020, 10, 7393; doi:10.3390/app10217393 www.mdpi.com/journal/applsci.
- Colbert, E. J. M. & Kott, A. (2016). *Cybersecurity of SCADA and Other Industrial Control Systems*. Advances in Information Security. doi:10.1007/978-3-319-32125-7
- Conklin, W. A. & Shoemaker, D. (2017). Cyber Resilience: Seven Steps for Institutional Survival. *EDPACS*, 55(2), 14-22.
- Dacey, R.F. (2020). *Critical infrastructure protection: Challenges and efforts to secure control systems*. U.S. GAO.
- Elissa M. Redmiles, Mia M. Bennett, Tadayoshi Kohno, (2023). "Power in Computer Security and Privacy: A Critical Lens", *IEEE Security & Privacy*, vol.21, no.2, pp.48-52, 2023.
- DHS (2016). Department of Homeland Security, *Cyber Resilience Review, Carnegie Mellon University's Software Engineering Institute for managing operational resilience*. Retrieved from http://www.cert.org/resilience/rmm.html
- Lansó, Thomas H. Hedgecock, Daniel A. & Pendergrass, J. Aaron (2021). The State of Cyber Resilience: Now and in the Future, *Johns Hopkins APL*

Technical Digest, Volume 35, Number 4 (2021), www.jhuapl.edu/techdigest

- Luiijf, E. (2016). Threats in Industrial Control Systems Cybersecurity of SCADA and Other Industrial Control Systems, Springer.
- NIST (2021). *National Institute of Standards and Technology, Developing Cyber Resilient Systems*: A Systems Security Engineering Approach, (SP) 800-160 Volume 2, Revision 1, Retrieved from https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final
- Ross, R; (2018). *Systems Security Engineering Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems*- SP 800-160 Vol. 2 (Draft), March 2018.
- Ross, R; (2019). *Developing Cyber Resilient Systems*: A Systems Security Engineering Approach - SP 800-160 Vol. 2- Rev. 1, November 2019
- Wei, D. & Ji, K. (2018). *Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights*. Paper presented at the Resilient Control Systems (ISRCS), 3rd International Symposium.