فصلنامه مطالعات دفاعی استراتژیک
سال بیست و دوم، شماره ۹۵، بهار ۱۴۰۳
مقاله نهم، از صفحه ۱۸۹ تا ۲۱۰

مقاله پژوهشی: الگوی پایداری و تداوم عملیاتی شبکه فرماندهی و کنترل در برابر تهدیدات سایبری

ایرج بختیاری[۱]

دریافت مقاله: ۱۴۰۲/۱۰/۰۱ پذیرش مقاله: ۱۴۰۲/۱۲/۰۲

چکیده

امروزه شبکه فرماندهی و کنترل با تهدیدات متنوعی مواجه است، از جمله حوزه‌های تهدید از منظر پدافندغیرعامل؛ تهدیدات سایبری است و در این میان پایداری و تداوم عملیاتی در شرایط تهدید سایبری و درواقع تاب‌آوری سایبری؛ اقدامات و پیش‌بینی‌هایی است که در یک سامانه برای کسب آمادگی جهت مواجه و مقابله با حملات و نفوذ سایبری و تحمل و سازگاری با شرایط بوقوع پیوسته و بازیابی و بازتوانی سریع پس از وقفه های ایجاد شده، بایستی انجام گیرد. بنابراین یک سامانه زمانی پایدار و تاب‌آور است که توانایی مقاومت در برابر حملات یا حوادث سایبری را داشته باشد. هدف اصلی این پژوهش ارایه مدل پایداری و تداوم عملیاتی و تاب آوری سامانه های شبکه فرماندهی و کنترل در برابر تهدیدات سایبری و اهداف فرعی آن تبیین تهدیدات سایبری، آسیب پذیری‌های سایبری، ابعاد و مولفه‌های تاب‌آوری سایبری سامانه‌های شبکه فرماندهی و کنترل است. این پژوهش از نوع کاربردی و از لحاظ روش توصیفی با رویکرد آمیخته می باشد، پژوهشگر در ابتدا با استفاده از تحلیل و دسته بندی روش ها و راهکارهای مطرح شده به اکتشاف الگوی مقتضی می‌پردازد و بمنظور بررسی ارتباط معناداری ابعاد و مولفه‌ها به روش تحلیل عاملی، از نرم‌افزار اسمارت پی.ال.اس استفاده می‌نماید. ضرایب بار عاملی محاسبه شده برای سه بعد فرماندهی و راهبری، کنترل و نظارت، و فرآیند و عملیات به‌ترتیب؛ ۰/۹۲٦، ۰/۹۱۷ و ۰/۹۲۰ می‌باشد که نشان از اهمیت بالای این عوامل در افزایش تاب‌آوری سایبری سامانه‌ها دارد. الگوی تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل در سه بعد فرماندهی و راهبری با چهار مولفه، بعد کنترل و نظارت با چهار مولفه ، بعد فرآیند و عملیات با سه مولفه، در برابر شش عامل تهدید و هفت آسیب پذیری(ضعف) ارایه شده است.

واژگان کلیدی: پایداری سایبری شبکه، تداوم عملیاتی سامانه‌های فرماندهی و کنترل، تهدیدات سایبری، آسیب‌پذیری‌های سایبری.

[۱] عضو هیات علمی دانشگاه پداف ندهوایی خاتم الانبیاء(ص) (نویسنده مسئول) eraj_baktiar@yahoo.com

مقدمه

پایداری و تاب‌آوری سایبری یک رویکرد تدافعی برای حمایت از سازمان‌ها در برابر تهدیدات سایبری است و بکارگیری این روش‌ها، معماری سازمانی سازمان‌های هدف را به نحوی تغییر می‌دهد که بتواند بیشترین انعطاف را در مقابله با حملات و نفوذ سایبری داشته باشد. تاب‌آوری یک فرآیند، توانایی یا پیامد سازگار موفقیت‌آمیز با شرایط تهدیدکننده می‌باشد (Bodeau & etal, 2015). تاب‌آوری سایبری ناظر به توانایی یک سامانه سایبری در ارایه مستمر نتایج مورد نظر به رغم رویدادهای سایبری نامطلوب است. به بیان ساده، سامانه‌های سایبری باید بتوانند حتی در صورت وجود حملات سایبری مخرب به فعالیت ادامه دهند(بت شکن، ۱۳۹۶: ۲).

قابلیت پایداری و تاب‌آوری سایبری شامل تمام مراحلی است که سازمان باید انجام دهد و برای آماده شدن و سازگاری با شرایط در حال تغییر و مقاومت در برابر حوادث و بهبود سریع پس از وقفه‌های ایجاد شده خود را آماده نماید. در این مفهوم یک سازمان زمانی انعطاف پذیر است که توانایی مقاومت در برابر حملات، حوادث یا تهدیدات را داشته باشد.(Conklin & Shoemaker, 2017).

مجموعه‌های نظامی و دفاعی در بکارگیری سامانه‌های مبتنی بر فضای سایبر معمولاً از سایر بخش‌ها، پیشتازترند. چالش بزرگ سامانه‌های فرماندهی و کنترل نوین آن است که فناوری‌های عملیاتی[1] به نحو چشم‌گیری با فناوری‌های اطلاعاتی[2] تلفیق شده و از این رو تهدیدات فراوان و روز افزون فناوری اطلاعاتی به سامانه‌های عملیاتی نیز تعمیم می‌یابد. به علاوه وجود محدودیت-های بکارگیری ابزارهای تشخیص بدافزار در سامانه‌های عملیاتی، موجب افزایش خطرپذیری در سامانه‌های سامانه‌های فرماندهی و کنترل شده است. همچنین سامانه‌های دفاعی سایبر پایه اعم از سامانه‌های فرماندهی و کنترل، با یک تهدید بزرگ‌تر یعنی حساسیت حوزه کاری مواجه است زیرا تمرکز دشمن بر تضعیف توان دفاعی و نظامی کشور هدف می‌باشد(Colbert & Kott, 2016). رشد سریع فناوری‌ها و حرکت به سمت انقلاب صنعتی چهارم و بهره گیری از مزایای فضای سایبر، با وجود به همراه داشتن منافع فراوان برای زندگی بشر، بدلیل بهره گیری فناوری اطلاعات در محیط عملیات، آسیب پذیری های موجود و حملات سایبری به سامانه های فرماندهی و کنترل را افزایش داده است که این امر باعث ایجاد اخلال در عملکرد سامانه‌ها و وقفه در تداوم عملیاتی

1. opration Technology

2. Information Technology

شبکه فرماندهی و کنترل می‌گردد. از آنجائی‌که ایجاد وقفه در عملکرد سامانه و خارج از سرویس نمودن آن در شبکه، به‌واسطه عملی شدن هرگونه تهدید سایبری؛ پایداری و تداوم عملیاتی این سامانه‌ها در شبکه فرماندهی و کنترل، که بایستی بطور ۲٤ ساعته سرپا و پای‌کار باشند و فرآیند رصد و پایش و مراقبت از آسمان کشور را نسبت به هرگونه نفوذ و تهدید با انجام ماموریت طی مراحل؛ کشف، شناسایی، رهگیری و درگیری براساس قوانین و آئین نامه‌های مربوطه انجام دهند را، با اشکال مواجه و امر تصمیم‌سازی و تصمیم‌گیری به موقع و صحیح را تحت تاثیر قرار داده و در نتیجه باعث رکود عملیاتی می‌گردد، دغدغه اصلی این تحقیق که همان پیشگیری و ممانعت از ایجاد وقفه در تداوم امور عملیاتی و یکپارچگی شبکه می‌باشد، شکل گرفت. بنابراین تاکید و توجه به تاب آوری سایبری، به معنی ایجاد تمهیدات مناسب پیش از حمله سایبری، حفظ عملیات اصلی سامانه و پایداری مناسب در زمان حمله سایبری و بازگشت به شرایط اولیه، پس از حمله سایبری یکی از اصلی ترین راهبردها در مواجهه با تهدیدات سایبری می باشد. ایجاد تداوم عملیاتی در سامانه‌های شبکه فرماندهی و کنترل مستلزم در اختیار داشتن سامانه‌های تاب‌آور در مواجهه با رخدادهای روز افزون سایبری و ایجاد معماری مناسب در توسعه این سامانه‌ها است. دستیابی به این مهم نیازمند یک الگوی مناسب است تا اجزاء و موارد مربوط به تاب‌آوری سایبری را برای سامانه‌های فرماندهی و کنترل مشخص نموده و نحوه مواجهه و رفتار مناسب در مقابله با تهدیدات سایبری را جهت استمرار فعالیت سامانه‌ها، تبیین نماید.

دستیابی به شبکه و سامانه‌های تاب‌آور و قابل اطمینان سایبری، مستلزم داشتن نگاه یکپارچه و همچنین وحدت رویه در شناسایی و اقدام مناسب در زمان اجرایی شدن تهدیدات سایبری در سامانه‌های فرماندهی و کنترل در شبکه است که این نکته نشان دهنده اهمیت بهره‌گیری از یک الگوی مناسب در تاب‌آوری سایبری سامانه‌ها در مواجهه با تهدیدات سایبری و درواقع اهمیت موضوع تحقیق می‌باشد. بنابراین مسئله تحقیق، فقدان یک الگوی پایداری و تداوم عملیاتی مناسب در مواجهه با تهدیدات و حملات سایبری به شبکه‌ها و سامانه‌های فرماندهی و کنترل است که از منظر ضرورت تحقیق این مسئله موجب تحمیل هزینه‌های بسیار بالا و بعضاً غیر قابل جبرانی به این سامانه‌ها با توجه به ضعف‌های آن‌ها می‌گردد. همچنین درصورت بروز حمله سایبری، می‌بایست سامانه‌های قربانی، در کمترین زمان ممکن به حالت قبل از حمله برگردند و برای دستیابی به این مهم داشتن یک الگوی مناسب امری ضروری است.

هدف اصلی این پژوهش ارایه مدل تاب‌آوری سایبری شبکه‌های فرماندهی و کنترل و اهداف فرعی آن تبیین تهدیدات سایبری شبکه‌های فرماندهی و کنترل، آسیب پذیری‌های سایبری این سامانه‌ها و تبیین ابعاد، مؤلفه‌ها و شاخص‌های تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل می‌باشد.

مبانی نظری

الف – پیشینه‌شناسی

در راستای بررسی پیشینه‌های مربوط به تاب‌آوری سایبری سامانه‌ها، تعدادی مقاله داخلی و خارجی و سند ارایه شده توسط موسسات پژوهشی و تحقیقاتی، مورد بررسی قرار گرفت که در ادامه به برخی اشاره شده است:

لینکو و همکاران[1] (۲۰۱۳) در پژوهشی تحت عنوان "معیارهای تاب‌آوری برای سامانه‌های سایبری" با توجه به اهمیت ملی و بین المللی اینگونه مسائل بیان می‌دارند که معیارهای تاب‌آوری برای اطلاع از تصمیمات مدیریتی، هنوز در مراحل اولیه توسعه می‌باشند. به همین دلیل، آن‌ها یک چارچوب ماتریسی تاب‌آوری را برای توسعه و سازماندهی معیارهای مؤثر تاب‌آوری برای سامانه‌های سایبری بکار گرفته و یادآوری کرده‌اند که در گزارش سال ۲۰۱۳ هیات علمی دفاعی "سامانه‌های ارتش تاب‌آور و تهدیدات پیشرفته سایبری" دو ویژگی برای معیارها ارایه شده است: (۱) معیارها به اندازه کافی گسترده باشند تا در طیف متنوعی از سامانه استفاده شوند؛ و (۲) به اندازه کافی دقیق باشند تا بتوانند فرآیندها و اجزا سامانه‌های خاص را اندازه‌گیری کنند. محققین پژوهش مذکور، تعاریف چهار ویژگی سامانه از آکادمی ملی علوم[2] را با چهار حوزه جنگ‌آوری متمرکز بر شبکه[3] به منظور ایجاد یک ماتریس کلی از معیارهای تاب‌آوری ترکیب کرده‌اند(گزارش هیات علمی دفاعی آمریکا[4]، ۲۰۱۳).

وی و جی[5](۲۰۱۵)، در مقاله‌ای با عنوان سامانه‌های صنعتی تاب‌آور: مفاهیم، فرمول‌بندی، معیارها و بینش‌ها، ضمن تبیین شاخصه‌های مورد نیاز سامانه‌های صنعتی تاب‌آور، معیارهای

1. Linkov et al.
2. The National Academy of Sciences (NAS)
3. Network-Centric Warfare (NCW)
4. Defense Science Board(DSB)
5. Wei & Ji

ارزیابی تاب‌آوری در مقابل تهدیدات سایبری را در سامانه‌های صنعتی بیان نمـوده‌انـد(Wei & Ji, 2015).

مظفری و همکاران(۱۳۹۹)، در مقاله‌ای با عنوان احصاء شاخص‌های تاب‌آوری برکاهش آسیب پذیری سیستم های کنترل صنعتی در تهدیدات سایبری، بیـان مـی‌دارنـد کـه شـاخص‌هـای حـس تشخیص، اجرای اقدامات کنترلی در عملیات روزمره، توسعه توابع نظـارتی(کنتـرل‌هـای اینترنتـی، بخش قانونی، مدیریت ریسک و امنیت سایبری)، استفاده قوی از بخش ممیزی داخلی و واکنش و ترمیم، برکـاهش آسـیب‌پـذیری سیسـتم‌هـای کنتـرل صـنعتی در برابـر تهدیـدات سـایبری تـاثیر دارد(مظفری و همکاران، ۱۳۹۹).

پژوهشکده امنیت سایبری دانشگاه کارنگی ملون به عنوان یکی از مراکز معتبر در حـوزه ارایـه استانداردها و دستور العمل‌های سایبری در سـال ۲۰۱٦ مجموعـه دسـتور العمـل‌هـای تـاب‌آوری سایبری را در ۱۰ سرفصل کلـی بـا هـدف ارتقـاء امنیـت سـایبری بـه تـاب‌آوری سـایبری ارایـه نمود(بررسی تاب‌آوری سایبری، ۲۰۱٦). همچنین در سال ۲۰۲۱، انیستیتو ملی استاندارد و فناوری آمریکا[1] هم، استاندارد ایجاد تاب‌آوری سایبری در سیستم‌ها و سامانه‌های سایبر پایه را ارایه نمـوده است.(استاندارد تاب‌آوری سایبری سیستم‌ها، ۲۰۲۱)

در پژوهشی توسط امین زاده و همکاران(۱۳۹۹) با عنـوان مـدل افـزایش تـاب آوری سـایبری سامانه ها ی فرماندهی و کنترل صنعتی مبتنی بر بهبود فرآیندها، مدل افزایش تاب آوری سـایبری سامانه های فرماندهی و کنترل صنعتی مبتنی بر مدل یکپارچه سازی، مـدل بلـوغ توانـایی و مـدل بهبود فرآیند ها ، برای سه سطح سامانه های فرماندهی و کنتـرل صـنعتی شـامل سـطح راهبـری ، سطح نظارت و کنترل و سطح عملیات ارائه شده است. در مدل ارائه شده برای بعد رهبـری ، بعـد نظارت و کنترل و بعد عملیات سطح بلوغ یک) اجرایی) ۱۰ مولفه ، برای سطح بلـوغ دو (برنامـه ریزی) ۱۲ مولفه ، برای بلوغ سطح سوم (مدیریت) ۱۲ مولفه ، برای بلوغ سطح چهـارم (انـدازه گیری) ۹ مولفه ، برای بلوغ سطح پنجم (نهادینه) ٦ مولفه در مجموع ٤۹ مولفـه احصـاء و ارایـه شده است . برای تایید مدل ارائه شده با بهره گیری از نرم افزار اسمارت پـی ال اس ، تحلیـل بـار عاملی و آزمون معنی دار بودن مولفه ها انجام و مدل ارائه شـده در سـطح ۹۵ درصـد معنـی داری مورد تایید قرار گرفت.

1. NIST

رستگار (۱۳۹۹)در مقاله‌ای تحت عنوان رویکردهای جدید مدیریت تهدیدات از منظر پدافندغیرعامل، شناخت تخصصی از تهدید و گسترش تهدیدها و ترکیب شدن ان ها با فناوری های نوین، واکاوی و رویکردهای نوین مدیریت یکپارچه تهدیدات[1] و صحنه جنگ تشریح نموده است. تحقیق از نوع کاربردی وروش تحقیق توصیفی ـ تحلیلی بوده و از روش تحلیل سلسله مراتبی برای تحلیل داده ها استفاده کرده است. نتایج نشان داده؛ در مدیریت صحنه جنگ ها و تهدیدات، رویکرد سناریو تأثیر محور و نظامی و گره های اساسی می تواند از سناریوهای برتر در تهاجم کشورها می باشد.

در پژوهشی توسط ربیعی و همکاران(۱۳۹۹) با عنوان معرفی الگویی برای اندازه‌گیری و ارزیابی قدرت سایبری یک سازمان دفاعی در ج.ا.ایران، با هدف شناسایی و الگوسازی مؤلفه‌های ارزیابی قدرت سایبری، برای یک سازمان دفاعی،درنهایت ۵ مؤلفه، ۲٦ شاخص و ۷۸ سنجه برای اندازه‌گیری معرفی گردیده است. الگوی معرفی شده با مطالعه الگوهای ارزیابی سایبری و برنامه-های راهبردی ملی سایبری، مؤلفه‌های قدرت سایبری دفاعی استخراج گردیده، و با استفاده از روش الگوسازی معادلات ساختاری با رویکرد کمترین مربعات جزئی با سنجه‌های تکوینی، کشف و تعیین اعتبار شده است. نتایج سطوح معناداری سنجه‌های تحقیق هر سازه اصلی (ابعاد) و فرعی (مؤلفه‌ها) به میزان بیش از ۹۹٪ را نشان می‌دهد.

می‌توان گفت در پژوهش‌های انجام شده، به مواردی از قبیل اهمیت سامانه‌های مبتنی بر شبکه، پایش و کنترل فرآیندها و ارایه راهکارهای بهبود امنیتی سامانه‌ها، مدیریت و اصلاح انواع مختلف آسیب‌پذیری‌های سامانه‌ها، اشاره شده است. ارایه راهکارهای از پیش تعیین شده، تاکید بر بهبود امنیت سایبری و همچنین روش‌های اندازه‌گیری آن‌ها نیز موضوعی است که در این پژوهش‌ها به آن‌ها اشاره شده است ولی در تحقیقات یاد شده تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل مورد بررسی قرار نگرفته است.چنانکه در پژوهش حاضر، تمرکز اصلی تحقیق بر روی سامانه‌های فرماندهی و کنترل نظامی بوده و مدل تاب‌آوری این سامانه‌ها در مقابله با تهدیدات فضای سایبر ارایه می‌گردد که وجه تمایز اصلی این پژوهش با پژوهش‌های ذکر شده می‌باشد.

[1] UTM(**U**nified **T**hreat **M**anagement)

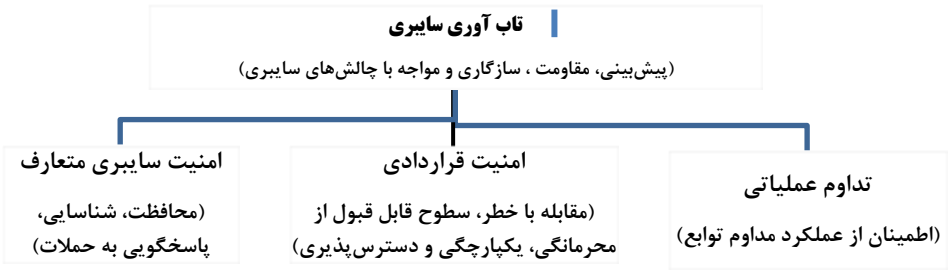
ب– مفهوم شناسی

تاب‌آوری در برابر تهدیدات سایبری را باید در چارچوب سامانه‌های پیچیده‌ای در نظر گرفت که نه تنها فیزیکی و اطلاعاتی بلکه حوزه‌های شناختی و اجتماعی را در برمی‌گیرد. تاب‌آوری سایبری تضمین می‌کند که بازیابی سامانه با در نظر گرفتن سخت افزار، نرم افزار و مؤلفه‌های حساس به هم پیوسته زیرساخت سایبری انجام می‌شود بنابراین تاب آوری سایبری یک پل بین عملکردهای پایدار سامانه و در عین حال اطمینان از اجرای مأموریت است(Kott & Linkov, 2019: 17). 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، نسخه ۱,۱ مدل مدیریت تاب‌آوری تیم واکنش اضطراری رایانه‌ای را منتشر نمود. در سال ۲۰۱۲ برای اولین بار مفهوم تاب‌آوری سایبری توسط ریاست جمهوری آمریکا، در سطح ملی مطرح شد و سپس در اجرای

برنامه کمپین سایبری نیروی هوایی آمریکا، اداره تاب‌آوری سایبری سامانه‌های تسلیحاتی راه‌اندازی شد 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).

تاب‌آوری سایبری

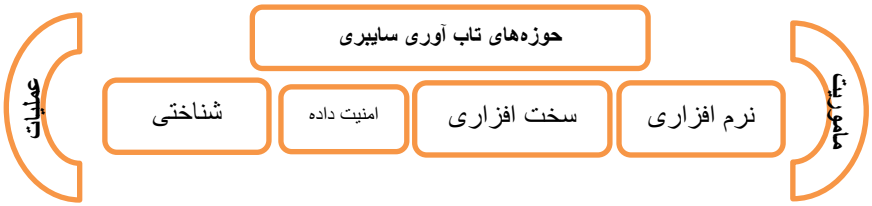
همانگونه که در شکل(۱) نشان داده شده است، تاب‌آوری سایبری بر روی سه پایه امنیت سایبری متعارف، تداوم عملیات و امنیت قراردادی ساخته شده است. در بخش تاب‌آوری سایبری، پیش‌بینی، مقاومت و بازیابی داده‌ها مطرح است. در بخش امنیت سایبری متعارف، کشف و واکنش مناسب به حملات انجام می‌شود. بخش تداوم عملیات، ایمن‌سازی و امنیت داده‌ها مطرح شده است و در بخش امنیت قراردادی، اعتمادسازی و ارایه راه حل مناسب برای خطر و مقابله با آن مطرح است(Bodeau, et al, 2015: 8).



شکل۱: اصول تاب‌آوری سایبری(Bodeau, et al, 2015: 8)

حوزه‌های تاب‌آوری سایبری

تاب‌آوری در برابر تهدیدات سایبری را باید در چارچوب سامانه‌های پیچیده‌ای در نظر گرفت که نه تنها حوزه‌های فیزیکی و اطلاعاتی بلکه حوزه‌های شناختی و اجتماعی را در برمی‌گیرد. تاب‌آوری سایبری تضمین می‌کند که بازیابی سامانه با در نظر گرفتن سخت‌افزار، نرم‌افزار و مؤلفه‌های حساس به هم پیوسته زیرساخت سایبر انجام می‌شود، بنابراین تاب‌آوری سایبری پلی بین عملکردهای پایدار سامانه و در عین حال اطمینان از اجرای مأموریت است.



شکل۲: حوزه‌های تاب‌آوری سایبری(Kott & Linkov, 2019: 18).

دامنه‌های تاب‌آوری در برابر رخدادهای سایبری شامل مؤلفه‌های شناختی، سخت افزار، نرم افزار و امنیت اطلاعات(داده) است که به طور جمعی در پایداری عملکرد سامانه نقش دارند. تاب‌آوری در بسیاری از رشته‌ها ریشه دارد و دیدگاه‌ها و تعاریف زیست محیطی، اجتماعی، روانشناختی، سازمانی و مهندسی را در هم می‌آمیزد. برای مثال مهندسی تاب‌آوری به عنوان "توانایی سامانه‌ها برای پیش‌بینی و سازگاری با شرایط بحرانی" تعریف شده که این مطلب نشان دهنده میزان اهمیت محافظت از سامانه‌ها در مواجهه با حوادث غیرمنتظره می‌باشد(Kott & Linkov, 2019: 17). سه ویژگی اساسی در امنیت فناوری اطلاعات یعنی محرمانگی، یکپارچگی، و قابلیت دسترس بودن همواره مد نظر می‌باشد.

ارکان تاب‌آوری سایبری

تاب‌آوری سایبری نیازمند اصلاح مداوم روندهاست. می‌توان گفت که این روند، چارچوبی است که دارای پنج رکن اصلی: آمادگی و شناسایی، محافظت، کشف، پاسخگویی و بازیابی است و می‌تواند بصورت یک چرخه مداوم تلقی گردد(شکل۳). برای هر یک از این ارکان، رویکردهایی مبتنی بر بهترین راهکارها با هدف به حداقل رساندن خطر سایبری پیشنهاد شده و هر مرحله

نیازمند اقدامات به‌خصوصی است که باید توسط کارکنان فناوری اطلاعات اجرا شوند(سعادتی، ۱٤۰۰: ۱۱۸).

شناسایی دارایی‌ها، سیستم‌ها و داده‌های حیاتی: یک سازمان باید از همه منابعی که از عملکردهای حیاتی آن پشتیبانی می‌کنند، باخبر باشد. محافظت از زیرساخت‌های حیاتی: در این مرحله، سازمان اقدام به طراحی و تولید برنامه‌های امنیتی می‌کند که منجر به محدود شدن یا مقابله با تهدیدات بالقوه می‌شوند. تشخیص رویدادهای عجیب و نشت داده‌ها قبل از بروز حوادث بزرگ: این مرحله نیازمند نظارت مستمر است. واکنش به نواقص یا رخنه‌های امنیتی: این مرحله مستلزم داشتن یک طرح کلی برای واکنش به حوادث است تا سازمان بتواند در صورت مواجهه با حملات سایبری به روال عادی کار خود ادامه دهد. بازیابی همه زیرساخت‌ها، قابلیت‌ها یا سرویس‌های تأثیر پذیرفته از حمله: تمرکز این مرحله، برگرداندن شرایط به حالت عادی است. (فراست، ۱۳۹۹)

سامانه مدیریت یکپارچه تهدیدات یکی از ابزارهای محافظتی در برابر تهدیدات بد افزارهاست.این سامانه در دسته فایروال‌های نسل۳ که به آن‌ها Next-Generation FireWall (NGFW) یا فایروال‌های نسل بعد نیز گفته می‌شود قرار دارند و منظور از یکپارچه بودن آن‌ها این است که در این سامانه‌ها، علاوه بر فایروال، انواع سیستم‌های نظارتی، مدیریت و امنیتی نیز تعبیه شده است.

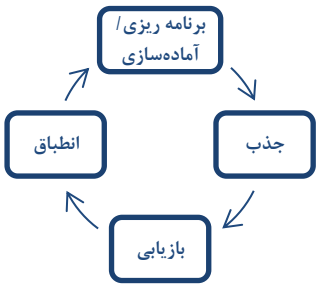
شکل۳: پنج رکن اصلی پایداری و تاب‌آوری سایبری

فرآیند مدیریت اقدامات تاب‌آوری سامانه‌های سایبری

بر اساس نظریه آکادمی بین المللی علوم؛ چهار فاز از چرخه مدیریت رویداد ارایه شده است که هر سامانه بایستی برای ماندگاری و تاب‌آوری سایبری خود، آن‌ها را اعمال کند:

- **برنامه ریزی/ آماده سازی**: پی‌ریزی پایه و اساسی برای حفظ دسترسی به خدمات و فعالیت دارایی‌ها طی یک رویداد مخرب (سوء عمل یا حمله)
- **جذب**: حفظ و نگهداشت فعالیت اکثر دارایی‌های حیاتی و دسترسی به خدمات در حین دفع و جداسازی عامل تخریب.
- **بازیابی**: بازگرداندن کارکرد تمامی دارایی‌ها و دسترسی به خدمات به حالت قبل از رویداد.
- **انطباق**: با استفاده از مدیریت دانش رویداد؛ اصلاح پروتکل، پیکربندی سامانه، آموزش پرسنل، و یا دیگر جنبه‌ها، سامانه‌ها تاب آورتر می‌شوند(Defense Science Board, 2013).

این چهار مرحله به‌صورت شکل زیر ارایه می‌گردند:



شکل ٤: فازهای اقدامات تاب‌آوری سامانه‌های سایبری (DSB, 2013)

مطالعات علمی نشان داده که ۹۷ ٪ از شرکت‌های دارای چارچوب تاب آوری سایبری، مدیران سطح بالایی دارند که به اهمیت داشتن یک چارچوب امنیت سایبری قوی آشنا هستند.(فراست، ۱۳۹۹)

اصول تاب‌آوری سایبری

هفت اصل مهم در تاب‌آوری سایبری وجود دارد که در ادامه مورد بررسی قرار می‌گیرند:

توسعه: سازمان به صورت پویا معماری سایبری خود را بر اساس درس‌های آموخته شده تنظیم می‌کند. این اصل در چارچوب امنیت سایبری بیان می‌گردد.

بازیابی: فرآیندهای تعریف شده باید بصورت مستند در محلی قرار داده شوند که اطمینان حاصل شود که تمام کارکردهای سازمانی به طور کامل در پارامترهای لازم بازسازی می‌شوند.

آزمودن: معماری تاب‌آوری باید قابل اطمینان باشد. این موضوع تابع برنامه‌ریزی و نظارت بوده و مبتنی بر عملکرد کنترل نقادانه در جهت دستیابی به اهداف اعلام شده است.

طراحی/ استقرار: برای تاب‌آوری باید معماری مناسب در نظر گرفته شود به طوری که در صورت بروز یک حمله موفق اطمینان از پایداری سازمان حاصل شود.

رتبه: دارایی‌هایی که سازمان به طور کامل قادر به از دست دادن آنها نیست، انتخاب و ارزیابی شده و یک پاسخ مؤثر برای هر یک از آن‌ها اعمال می‌شود. منابع سازمانی تنها بر تضمین این موارد مهم تمرکز دارند. در مرحله بعد، به دفاع از مابقی دارایی‌های سازمان توجه می‌شود.

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 شناسایی شده باشد.

طبقه‌بندی: برای محافظت از دارایی‌های سازمان، بایستی تمام دارایی‌های سازمان شناسایی، برچسب‌گذاری شده و در یک مبنای منطقی از اشیاء قرار گیرد(سعادتی، ۱٤۰۰: ۱۳۳).

تکنیک‌های ارتقاء تاب‌آوری سایبری

تکنیک‌های تاب‌آوری سایبری راه‌هایی برای دستیابی به یک یا چند هدف میان‌مدت تاب‌آوری سایبری می‌باشند که از عملکردهای ماموریت و منابع سایبری پشتیبانی می‌کنند. تکنیک‌های تاب-آوری سایبری با توجه به معماری یا طراحی ماموریت سازمان انتخاب می‌شوند تا آن‌ها را برای دستیابی به اهداف کمک نمایند. برخی از این تکنیک‌ها در ادامه به صورت مختصر آورده شده است:

۱) پاسخ تطبیقی: بهینه سازی توانایی زیرمجموعه جهت پاسخگویی به موقع و مناسب.
۲) نظارت تحلیلی: نظارت و تشخیص اقدامات و شرایط نامطلوب.
۳) حمایت هماهنگ: اجرای یک راهبرد عمیق دفاعی.
٤) فریب: مخفی کردن دارایی‌های مهم و نمایش دارایی‌های فریبنده.
۵) تنوع: استفاده از ناهمگونی برای به حداقل رساندن خرابی‌ها.
٦) موقعیت‌یابی پویا: کاهش آسیب‌پذیری در مقابل حوادث غیر مترقبه (مانند بلایای طبیعی) از طریق توزیع و متنوع‌سازی شبکه.

۷) عدم تداوم: کاهش آسیب‌پذیری‌هایی از قبیل فساد، اصلاح و یا سازش، از طریق تولید و حفظ منابع برای مدت زمان محدود.

۸) محدودیت خصوصی: ایجاد محدودیت بر اساس ویژگی‌های کاربران، عناصر سیستم و همچنین عوامل محیطی.

۹) تنظیم مجدد: به حداقل رساندن ارتباطات بین سرویس‌های مهم و غیر بحرانی، در راستای کاهش احتمال عدم موفقیت آن دسته از سرویس‌های غیر بحرانی که خدمات مهم را برای ماموریت اصلی تحت تاثیر قرار می‌دهند.

۱۰) افزونگی: ارایه چندین مورد محافظت شده از منابع مهم.

۱۱) تقسیم‌بندی: تفکیک عناصر جداگانه بر اساس حساسیت و اعتماد به نفس.

۱۲) یکپارچگی: مشخص کردن وضعیت سلامت عملکرد کلیه عناصر حیاتی سیستم.

۱۳) غیرقابل پیش بینی بودن: انجام تغییرات بطور تصادفی و غیرمنتظره در راستای کاهش امکان تشخیص فرایندهای محافظی(**Ross & et al, 2018**).

مدل مفهومی پژوهش

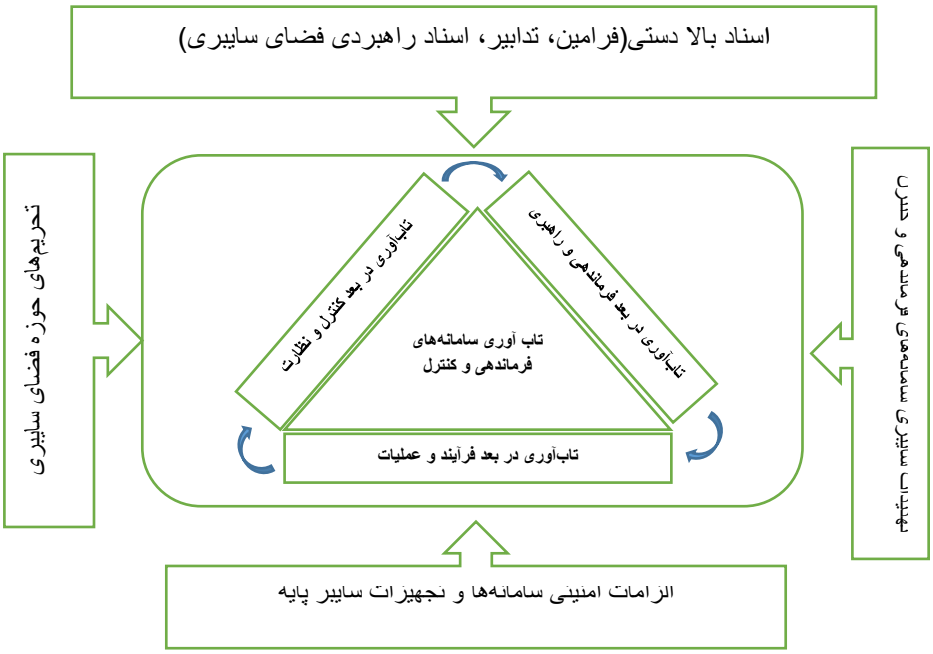
در این پژوهش، پس از مطالعه الزامات مربوط به اسناد بالادستی، تهدیدهای سایبری تجهیزات دفاعی و سامانه‌های فرماندهی و کنترل، محدودیت‌های ناشی از تحریم‌های فناورانه، الزامات امنیتی سامانه‌های سایبرپایه در قالب چارچوب نظری و همچنین بررسی آسیب‌پذیری‌های سامانه‌های سایبرپایه، مدل مفهومی مربوط به الگوی تاب‌آوری سامانه‌های فرماندهی و کنترل، برابر شکل (۵) مشخص گردید. اسناد بالادستی شامل: سند راهبردی امنیت فضای تولید و تبادل اطلاعات، نظام جامع فناوری اطلاعات، اساسنامه شورای عالی فضای مجازی، سیاست‌های کلی برنامه ششم توسعه، بیانیه گام دوم. بعنوان مثال در بند (۳) اهداف کلان سند راهبردی ج. ا. ایران در فضای مجازی؛ دستیابی به قدرت فضای مجازی (سایبری) ج.ا.ا. در تراز جهانی و جایگاه نخست قدرت فضای مجازی (سایبری) در بین کشورهای منطقه و نیل به توان بازدارندگی فضای مجازی (سایبری) مؤثر در سطح بین‌الملل؛ و در بند (۲٤) آن به مصونیت زیرساخت‌ها و ارتقاء حفاظت از منافع ملی در برابر تهدیدات دشمنان در فضای مجازی تاکید شده است.

تهدیدات شامل: تهدیدات معماری و فناوری اطلاعات، تهدیدات شبکه و ارتباطات(خرابکاری صنعتی، نفوذ و کاشت جاسوس افزار)، تهدیدات عملیات و نگهداشت، تهدیدات سازمانی،

تهدیدات محیط فیزیکی، تهدیدات عوامل انسانی(برگرفته از گزارش موسسه تهدیدات امنیت اینترنت؛ ۲۰۱۹).

الزامات امنیتی: امنیت نرم‌افزارهای دفاعی، امنیت سخت‌افزارهای دفاعی، امنیت نیروی انسانی، امنیت شبکه‌های دفاعی، امنیت بسترهای ارتباطی دفاعی، امنیت اطلاعات الکترونیکی.

تحریم‌ها: تحریم‌های حوزه فناوری، تحریم‌های حوزه دفاعی، تحریم‌های مربوط به امکان بروزرسانی سامانه‌ها، عدم اطمینان به امنیت سامانه‌ها ناشی از تحریم‌ها.



شکل۵: چارچوب نظری و مدل مفهومی پژوهش

روش‌شناسی پژوهش

پژوهش حاضر از نظر هدف، کاربردی است و ازلحاظ طرح تحقیق در زمره تحقیقات آینده نگر دسته بندی می‌گردد این پژوهش به این دلیل آینده نگر است که محقق در پی طراحی الگو تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل در جهت مقابله با تهدیدات پیش روی سایبری در آینده می‌باشد. همچنین پژوهش حاضر از لحاظ روش تحقیق در زمره تحقیقات توصیفی/تحلیلی با نگاه اکتشافی دسته بندی می‌گردد. این پژوهش به این دلیل توصیفی/تحلیلی

است که محقق با نگاه راهبردی به توصیف تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل پرداخته و با استفاده از تکنیک‌های راهبردی به تحلیل تهدیدات و آسیب پذیری‌های سایبری در سامانه های فرماندهی و کنترل سایبر پایه پرداخته و بر اساس این دو نگاه با دید اکتشافی، چارچوب اولیه‌ای برای تدوین الگوی تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل ارایه شد. در ادامه با انجام مصاحبه عمیق با خبرگان این حوزه و با بهره‌گیری از روش تحقیق نظریه زمینه‌ای، گویه‌های لازم جهت تدوین شاخص‌های پیاده‌سازی و ارزیابی اقدامات لازم برای اجرای تاب‌آوری سایبری فرماندهی و کنترل احصاء شد. سپس با استفاده از ابزار پرسشنامه، نظر خبرگان و صاحب‌نظران در خصوص میزان اهمیت شاخص‌ها جمع‌آوری و شاخص‌های نهایی الگو مشخص 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 با توزیع آن بین صاحب‌نظران، معیارهای نامفهوم و غیر مرتبط حذف 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 دارای؛ 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. قلمرو موضوعی و مکانی و زمانی این پژوهش سامانه‌های فرماندهی و کنترل بخش دفاعی موجود در کشور در افق ۱۴۰۶ می‌باشد.

تجزیه و تحلیل داده‌ها و یافته‌های تحقیق

الف: تجزیه و تحلیل یافته‌ها

با توجه این که پژوهش حاضر به روش تحقیق نظریه زمینه‌ای انجام شده است، جهت طبقه‌بندی اطلاعات و داده‌های استخراج شده از ادبیات و مبانی نظری و نظرات خبرگان، از روش‌های کدگذاری باز بر مبنای مقولات استخراج شده از مطالعه مقدماتی مبانی نظری تحقیق، کدگذاری محوری و کدگذاری انتخابی استفاده گردید. در کدگذاری باز، مفاهیم درون

اسناد و مدارک و مصاحبه‌ها، بر اساس ارتباط با موضوعات مشابه طبقه‌بندی می‌شوند. نتیجه این مرحله، خلاصه کردن انبوه اطلاعات کسب شده از مصاحبه‌ها و اسناد به درون مفاهیم و دسته‌بندی‌های مشابه است. هدف از کدگذاری محوری ایجاد رابطه بین مقوله‌های تولید شده (در مرحله کدگذاری باز) است. اساس ارتباط دهی در کدگذاری محوری بر بسط و گسترش یکی از مقوله‌ها قرار دارد. کدگذاری انتخابی عبارت است از فرآیند انتخاب دسته‌بندی اصلی، مرتبط کردن نظام‌مند آن‌ها با دیگر دسته‌بندی‌ها، تایید اعتبار این روابط، و تکمیل دسته‌بندی‌هایی که نیاز به اصلاح و توسعه بیشتری دارند. کدگذاری انتخابی بر اساس نتایج کدگذاری باز و کدگذاری محوری، انجام می‌شود.

تشکیل مقوله‌های کلان (مولفه‌ها)

با خوشه‌بندی شناسه‌های همسان و مقوله بندی آن‌ها در چندین مرحله، مقوله‌های کلان (مؤلفه‌ها) مطابق با جدول صفحه بعد استخراج گردید.

جدول۱: استخراج مولفه‌ها از شناسه‌های استخراج شده

شناسه استخراج شده	مقوله کلان (مؤلفه)
شناسایی و اولویت بندی تجهیزات و زیر سامانه‌ها براساس عملکرد، تعیین وظایف و عملکرد تجهیزات و زیرسامانه‌ها، تعیین ارتباط زیر سامانه‌ها و تجهیزات با عملکردها(گزارش موسسه ثبات مالی، ۲۰۱۸)، تعیین سطح دسترسی به زیرسامانه، دسته بندی براساس اطلاعات سامانه‌ها جهت حصول اطمینان و حفظ عملکرد اساسی، اولویت بندی اقدامات پشتیبان عملیات اساسی سامانه(Benz & Chatterjee, 2020)	مدیریت دارایی و تجهیزات سامانه‌های فرماندهی و کنترل
پیاده سازی فرایند مدیریت تغییر در سامانه‌ها، ارزیابی اجرایی شدن الزامات تاب‌آوری در زمان انجام تغییرات در سامانه‌ها(Sharkov,2016)، نظارت بر چرخه حیات سامانه‌ها جهت برنامه ریزی سامانه‌های پشتیبان در مواقع بحرانی(Carias & et al, 2020)، نظارت مستمر بر انجام پیکربندی‌های به موقع برای سامانه‌های فناوری محور نظیر نصب وصله‌ی امنیتی در نرم افزارهای سیستم عامل سامانه‌های عملیاتی(Gourisetti & et al, 2019).	پیکربندی و مدیریت تغییر سامانه های فرماندهی و کنترل
مخفی کردن دارایی‌های مهم و نمایش دارایی‌های فریبنده، استفاده از ناهمگونی برای به حداقل رساندن خرابی‌ها، ارایه چندین مورد محافظت شده از منابع مهم، مشخص کردن وضعیت سلامت عملکرد کلیه عناصر حیاتی سیستم(Ross & et al, 2018).	مدیریت فرایندهای اجرایی غیرعامل
انجام کنترل بر اجرای حفاظت از شبکه و در صورت لزوم، جداسازی شبکه، کنترل برای حفاظت اطلاعات در وضعیت‌های استفاده، کنترل برای حفاظت اطلاعات در زمان وقوع حمله و نشت داده‌ها(Benz & Chatterjee, 2020)، اجرا و کنترل کردن شیوه‌های امنیت سایبری برای	کنترل عملکرد سامانه های فرماندهی و کنترل

منابع انسانی مرتبط با سامانه، تعیین و کنترل سطح دسترسی به سامانه‌ها و دارایی‌ها با ترکیب اصل کمترین قابلیت(Carias & et al, 2020).	
ایجاد فرایند مدیریت ریسک با شناسایی، تحلیل و رفع خطرات، شناسایی حد آستانه ریسک و تمرکز فعالیت‌های مدیریت ریسک با شناسایی حوزه‌های تأثیرپذیر در سامانه(گزارش مرکز امنیت اینترنت، ۲۰۱۹)، تعیین پارامترهای تحمل ریسک برای هر حوزه تأثیرپذیر و تعیین آستانه تاب‌آوری، تجزیه و تحلیل ریسک‌ها و تعیین اقدام مناسب در برابر ریسک(Gourisetti & et al, 2019).	مدیریت ریسک سامانه‌های فرماندهی و کنترل
ایجاد و حفظ روند شناسایی و تجزیه و تحلیل آسیب پذیری نرم افزارها، دسته بندی و اولویت بندی آسیب پذیری‌ها(گزارش مرکز امنیت اینترنت، ۲۰۱۹)، اقدامات لازم برای آسیب‌پذیری‌های شناسایی شده و کاهش اثرپذیری، بررسی علل ریشه‌ای آسیب‌پذیری‌ها و ارزیابی نتایج کاهش آسیب‌پذیری‌ها (Deutscher, 2017).	مدیریت آسیب‌پذیری‌های سامانه‌های فرماندهی و کنترل
ایجاد فرایند شناسایی، تحلیل، پاسخ گویی و یادگیری از حوادث، شناسایی و مستند سازی حوادث و رخدادها شامل رویدادهای سایبری(گزارش موسسه ثبات مالی، ۲۰۱۸)، ثبت رخدادها در پایگاه داده و طبقه بندی، اولویت بندی آنها، ردیابی حوادث، ایجاد سامانه پاسخگویی سریع به حوادث/ حملات سایبری برای هر سامانه(Carias & et al, 2020).	مدیریت رخدادها و حوادث سایبری سامانه‌های فرماندهی و کنترل
توسعه برنامه‌های تداوم خدمات برای خدمات ارزشمند سامانه، تعیین وظیفه نیروی انسانی برای اجرای برنامه‌های تداوم خدمات خاص(گزارش مرکز امنیت اینترنت، ۲۰۱۹)، مستند سازی و دردسترس بودن برنامه‌های پیوستگی خدمات به‌صورت کنترل شده، برنامه ریزی و بررسی برنامه‌های تداوم خدمات و بهبود حاصل شده(Benz & Chatterjee, 2020).	تداوم فعالیت‌های سامانه‌های فرماندهی و کنترل
شناسایی و مدیریت خطرات ناشی از وابستگی‌های خارجی، اعمال الزامات تاب‌آوری به هر سامانه خارجی مرتبط با سرویس‌های اساسی سامانه(Annarelli & Nonino,2020)، نظارت بر عملکرد نهادهای خارجی مرتبط با سامانه، برنامه‌ریزی برای استفاده از خدمات عمومی مرتبط با خدمات حیاتی در زمان بحران(گزارش مرکز امنیت اینترنت، ۲۰۱۹)	وابستگی و ارتباطات خارجی سامانه‌های فرماندهی و کنترل
احصاء نیازمندی های آموزشی سایبری کارکنان مبتنی بر تغییرات فناوری، اجرای مستمر دوره‌ای آموزشی سایبری و به‌روزآوری دانش سایبری کارکنان، ارزیابی اثربخشی دوره‌های آموزشی سایبری در افزایش تاب‌آوری سایبری و ارائه برنامه‌های بهبود آموزش (Armenia & et al, 2021)	آموزش و آگاهی مدیران و کارشناسان فرماندهی و کنترل
راه اندازی سامانه آگاهی وضعیتی تاب‌آوری سایبری، تعیین مسئولیت نظارت بر منابع اطلاعات تهدید شناسایی(Carias & et al, 2020)، اولویت بندی و انتقال اطلاعات تهدید به ذینفعان داخلی، شناسایی، اولویت بندی و انتقال اطلاعات تهدید به ذینفعان خارجی(گزارش مرکز امنیت اینترنت، ۲۰۱۹)	آگاهی وضعیتی تاب‌آوری سامانه‌های فرماندهی و کنترل

تشکیل مقوله‌های محوری (بعدها)

مقوله‌های فوق، مولفه‌های قابل توجه را مشخص نمود و با دسته‌بندی و مقوله‌سازی مجدد از مولفه‌های مرتبط با یکدیگر، مقوله‌های محوری (ابعاد) با نگاه استقرایی طبق جدول ذیل حاصل گردید:

جدول۲: تشکیل ابعاد از مولفه‌های استخراج شده

مقوله کلان (مؤلفه)	مقوله‌های محوری (بُعد)
مدیریت دارایی و تجهیزات سامانه‌های فرماندهی و کنترل	تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل در بعد فرآیند و عملیات
پیکربندی و مدیریت تغییر سامانه‌های فرماندهی و کنترل	
مدیریت فرایندهای اجرایی غیر عامل	
کنترل عملکرد سامانه‌های فرماندهی و کنترل	تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل در بعد کنترل و نظارت
مدیریت ریسک سامانه‌های فرماندهی و کنترل	
مدیریت آسیب‌پذیری‌های سامانه‌های فرماندهی و کنترل	
مدیریت رخدادها و حوادث سایبری سامانه‌های فرماندهی و کنترل	
تداوم فعالیت‌های سامانه‌های فرماندهی و کنترل در مقابله با تهدیدات سایبری	تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل در بعد فرماندهی و راهبری
وابستگی و ارتباطات خارجی سامانه‌های فرماندهی و کنترل	
آموزش و آگاهی مدیران و کارشناسان سامانه‌های فرماندهی و کنترل	
آگاهی وضعیتی تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل	

ب: یافته های تحقیق

بر اساس تجزیه و تحلیل انجام گرفته، نتیجه این پژوهش ارایه الگوی تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل در سه بعد فرماندهی و راهبری با ٤ مولفه اصلی، بعد کنترل و نظارت با ٤ مولفه اصلی و بعد فرآیند و عملیات با ۳ مولفه اصلی است که در یک شکل منسجم ارایه شده است. همچنین در این پژوهش شش عامل تهدید اصلی برای سامانه‌های فرماندهی و کنترل ارایه شده است. آسیب پذیری‌های ذاتی سامانه‌های سایبری فرماندهی و کنترل که بطور نسبی می‌باشند شامل؛ رمزنگاری نامناسب، ضعف در سیستم عامل، پیکربندی ضعیف تجهیزات، ضعف دیواره آتش، اعتبار سنجی نامناسب، دسترسی غیرمجاز به سامانه‌ها، می‌باشند. در این تحقیق

برای آزمون مدل مفهومی از مدل سازی معادلات ساختاری مبتنی بر رویکرد حداقل مربعات جزئی با نرم‌افزار اسمارت پی.ال.اس[1] استفاده شده است. در این روش میزان سهم هر عامل در ایجاد متغیر، مورد بررسی قرار گرفت و برای این کار از تحلیل عاملی تاییدی استفاد شد. در تحلیل عاملی، مقدار بار عاملی کمتر از ۰/۳ نشان دهنده مقیاس ضعیف، بارهای عاملی بین ۰/۳ تا ۰/٦ نشاندهنده مقیاس متوسط و مقادیر بزرگتر از ۰/٦ نیز نشان دهنده متغییر مشاهده‌پذیر با مقیاس قابل اطمینان می‌باشد. در کل مقادیر بارهای عاملی کوچک‌تر از ۰/٤ را می‌توان در مدل حفظ کرد. برای هریک از ابعاد؛ فرآیند و عملیات، کنترل و اتوماسیون و نظارت و راهبری، یک تحلیل عاملی جداگانه محاسبه شده و سهم هریک از گویه‌های مربوط به مولفه‌ها مشخص گردید. در نهایت با استفاده از مدل تحلیل عاملی مرتبه دوم، الگوی نهایی بررسی گردید. نتایج تحلیل بار عاملی در جدول (۳) ارایه شده است.

جدول۳: نتایج تحلیل عاملی تاییدی الگو

بعد	مولفه	بار عاملی
فرایند و عملیات	مدیریت دارایی و تجهیزات سامانه‌های فرماندهی و کنترل	۰/۹۱۲
	پیکربندی و مدیریت تغییر سامانه‌های فرماندهی و کنترل	۰/۹۲۰
	مدیریت فرایندهای اجرایی غیرعامل	۰/۹۲۸
کنترل و نظارت	کنترل عملکرد سامانه‌های فرماندهی و کنترل	۰/۹۲۵
	مدیریت ریسک سامانه‌های فرماندهی و کنترل	۰/۹۱۱
	مدیریت آسیب پذیری‌های سامانه‌های فرماندهی و کنترل	۰/۹۱۹
	مدیریت رخدادها و حوادث سایبری سامانه‌های فرماندهی و کنترل	۰/۹۱۳
فرماندهی و راهبری	تداوم فعالیت‌های سامانه‌های فرماندهی و کنترل در مقابله با تهدیدات سایبری	۰/۹۲۹
	وابستگی و ارتباطات خارجی سامانه‌های فرماندهی و کنترل	۰/۹۳۲
	آموزش و آگاهی فرماندهان، مدیران و کارشناسان سامانه‌های فرماندهی و کنترل	۰/۹۱۹
	آگاهی وضعیتی تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل	۰/۹۲٤

اطلاعات جدول (۳) نشان می‌دهد که تمامی مولفه‌ها، مقادیر بارهای عاملی بزرگ‌تر از ۰/۹ داشته و از اعتبار لازم برخوردار می‌باشند. در الگوی فوق ضرایب مسیرها برای سه بعد فرآیند و عملیات، کنترل و نظارت، و فرماندهی و راهبری، به ترتیب برابر ۰/۹۲۰، ۰/۹۱۷ و ۰/۹۲٦ می‌باشد،

1. SMART PLS 9.98

لذا بعد فرماندهی و راهبری بالاترین تـاثیر و بعـدهای فرآینـد و عملیـات، و کنتـرل و نظـارت بـا اختلاف کمی در جایگاه دوم و سوم قرار دارند.

نتیجه‌گیری و پیشنهادها

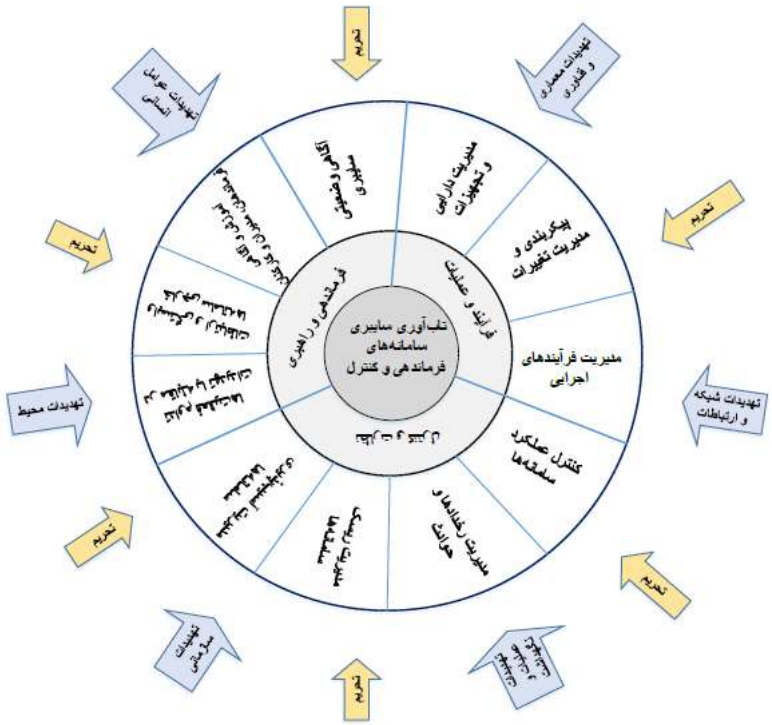
الف) نتیجه‌گیری

براساس مطالعات انجام شده و تایید صاحبنظران، سامانه‌های دفـاعی مشـتمل بـر سـامانه‌هـای فرماندهی و کنترل با شش دسته اصلی تهدید در برگیرنده ویژگی‌های تهدید به شرح جـدول ذیـل مواجه می‌باشند:

جدول٤: تهدیدات سامانه‌های دفاعی و فرماندهی و کنترل

نوع تهدید	زمینه و منشاء اثر تهدید
تهدیدات سازمانی	عدم تعیین سطح اجرایی عملیات، فقدان مدیریت یکپارچـه امنیـت اطلاعـات، تمـایز فرهنگ کاربران، کمبود آموزش کاربران، دوره استهلاک تجهیزات، استانداردهای امنیت فناوری‌اطلاعات و ارتباطات تدارکات
تهدیدات معماری و فناوری	فناوری قدیمی و فرسوده، ناامنی در طراحی سامانه‌ها، قابلیت جدید برای اجزا قدیمی، پروتکل‌ها غیر استاندارد صنعتی، خرابکاری صنعتی، نفوذ و کاشت جاسوس افزارها
تهدیدات شبکه و ارتباطات	محیط عملیاتی نامناسب، دسترسـی از راه دور شـبکه‌ای، وابسـتگی‌هـای سـامانه‌هـای فناوری‌اطلاعات و ارتباطات، ارتباط مستقیم با اینترنت
تهدیدات عوامل انسانی	کمبود آگاهی کاربران، سیاست‌ها و رویه‌های نامناسب، کارمندان ناراضی
تهدیـــدات عملیـــات و نگهداشت	رمزنگاری نامناسـب، عـدم توانمنـدی لازم، عـدم اجـرای مـدیریت تغییـر، عـدم بـه روزرسانی/ پچ کردن، عدم حفاظت از تروجان، مـدیریت نامناسـب دسترسـی سـخت افزار و شبکه
تهدیدات محیط عملیات	امنیت فیزیکی، وابستگی‌ها، افراد نفوذی و وابسته، دسترسی از راه دور

همچنین براساس مطالعات انجام شده و دریافت نظرات خبرگان و کارشناسان حوزه فرماندهی و کنترل و سامانه‌های دفاعی در مراکز و سازمان‌های نظـامی و دفـاعی کشـور، الگـوی تـاب‌آوری سایبری سامانه‌های فرماندهی و کنترل؛ در بعد فرماندهی و راهبری در مقابله با تهدیدات سـایبری با ٤ مولفه اصلی، در بعد کنترل و نظارت با ٤ مولفه اصلی و در بعد فرآیند و عملیات بـا ۳ مولفـه اصلی ، در برابر تحریم‌ها و تهدیدها بشرح شکل (٦) ارایه شده است، از ویژگی‌های این الگـو دو طرفه بودن آن؛ یعنی دربر داشتن جنبه‌های تهاجمی و تدافعی حول محور موضوع پژوهش است.



شکل۶: الگوی پایداری و تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل در مقابل تهدیدها و تحریم‌ها

ب)پیشنهادها

براساس یافته‌ها و نتایج تحقیق و در راستای ارتقاء تاب‌آوری سامانه‌های فرماندهی و کنترل در برابر تهدیدات حوزه سایبر، پیشنهادهای اجرایی زیر ارائه می‌گردد:

۱) نتایج این پژوهش جهت مطالعه و اطلاع رسانی در اختیار سازمان‌های مختلف صنایع دفاعی و در مجموع بخش صنعت قرار گیرد تا از الگوی ارایه شده برای افزایش تاب‌آوری سایبری سامانه‌های فرماندهی و کنترل در دست طراحی و ساخت داخل استفاده نمایند.

۲) در راستای دفع و رفع تهدیدات و آسیب‌پذیری‌های سامانه‌های موجود مورد استفاده، از فرصت‌ها و نقاط قوت موجود و مورد اشاره در این تحقیق بهره‌برداری لازم و موثر بعمل آید.

۳) به‌منظور افزایش توان تاب‌آوری سامانه‌های فرماندهی و کنترل، از منظر تهدید شناسی و پیش بینی راهکارهای مقابله‌ای؛ ویژگی‌های تهدیدها نسبت به هریک از ابعاد و مولفه‌های مرتبط، مد نظر و مورد توجه قرار گیرد.

فهرست منابع:

–امین زاده؛ علی محمد ، محمودزاده؛ ابراهیم، موحدی صفت؛ محمد رضا(۱۳۹۹)*مدل افزایش تاب آوری سایبری سامانه ها ی فرماندهی و کنترل صنعتی مبتنی بر بهبود فرآیندها* ، دوازدهمین کنفرانس ملی فرماندهی و کنترل ایران

–بت شکن، بهمن(۱۳۹٦)، *بررسی مهندسی تاب‌آوری سایبری در فضای سایبری*، سومین اجلاس ملی علوم و مهندسی رایانه و فناوری اطلاعات، دانشگاه اصفهان، دانشکده مهندسی رایانه.

–چمنی؛ مسلم، محمدی؛ اردشیر، بختیاری؛ ایرج(۱۳۹۷) *تحلیل پایداری شبکه فرماندهی و کنترل پدافند هوایی و ارائه راهکار مناسب برای ارتقاء آن*، فصلنامه فرماندهی و کنترل ، شماره ٤

–*راهکارهایی برای تدوین راهبرد تاب آوری سایبری سازمان*، نشریه فراست ، آذر ۱۳۹۹

–*ربیعی؛ بهزاد، علی‌یاری؛ شهرام، مردانی شهربابک، محمد(۱۳۹۹)* معرفی الگویی برای اندازه‌گیری و ارزیابی قدرت سایبری یک سازمان دفاعی در ج.ا.ایران ، *فصلنامه راهبرد دفاعی، شماره ٦۹*

–*رستگار، عبدالمطلب(۱۳۹۹)*،رویکردهای جدید مدیریت تهدیدات از منظر پدافندغیرعامل، *نخستین همایش ملی رویکرد های نوین مدیریت در مطالعات میان رشته‌ای*

–سعادتی، رضا(۱٤۰۰)، *شناسایی و اولویت‌بندی عوامل مؤثر بر تاب‌آوری سایبری ارتش جمهوری اسلامی ایران*، پایان‌نامه کارشناسی ارشد، دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران.

–مظفری و همکاران (۱۳۹۹)، *احصاء شاخص‌های تاب‌آوری برکاهش آسیب پذیری سیستم های کنترل صنعتی در تهدیدات سایبری*، چهارمین کنفرانس بین المللی تحقیقات حوزه اقتصاد و مدیریت.

- Annarelli, A.; Nonino, F.; Palombi, G. Understanding the management of cyber resilient systems. Comput. Ind. Eng. 2020, 149, 106829.
- Armenia, S.; Angelini, M.; Nonino, F.; Palombi, G.; Schlitzer, M.F. A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. Decis. Support Syst. 2021, 147, 113580.
- Benz, M.; Chatterjee, D. Calculated risk? A cybersecurity evaluation tool for SMEs. Bus. Horiz. 2020, 63, 531–540.
- Carias, J.F.; Borges, M.R.S.; Labaka, L.; Arrizabalaga, S.; Hernantes, J. The Order of the Factors DOES Alter the Product: Cyber Resilience Policies' Implementation Order. In Conference on Complex, Intelligent, and Software Intensive Systems; Springer: Burgos, Spain, 2020; pp. 306–315.
- Center for Internet Security (CIS). CIS Controls V 7.1; *Center for Internet Security (CIS)*: East Greenbush, NY, USA, 2019.

- Colbert, E. J. M., & Kott, A. (2016). *Cyber-security of SCADA and Other Industrial Control Systems. Advances in Information Security*, 63. 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 .
- DSB (2013), Defense Science Board. *Task force report: resilient military systems and the advanced cyber threat* .
- Deutscher, S.A.; Bohmayr, W.; Asen, A. *Building a Cyberresilient Organization; BCG Perspectives*: Boston, MA, USA, (2017).
- Financial Stability Institute(FSI), 2018, *Cyber resilience practices, Insights*, no. 21, avalible in fsicmigration@bis.org.
- 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
- Gourisetti, S.N.G.; Mix, S.; Mylrea, M.; Bonebrake, C.; Touhiduzzaman, M. *Secure Design and Development Cybersecurity Capability Maturity Model* (SD2-C2M2). In Proceedings of the Northwest Cybersecurity Symposium 2019, New York, NY, USA, 8 April 2019; ACM Press: New York, NY, USA, 2019; pp. 1–9.
- *Internet Security Threat Report*; Symantec: Sunnyvale, CA, USA, 2019; Volume 24.
- Kott, Alexander; Linkov, Igor; (2019). *Cyber Resilience of Systems and Networks*, springer.
- Linkov, I.; Eisenberg, D. A.; Plourde, K.; Seager T. P. (2013). *Resilience metrics for cyber systems*. Springer Science+Business Media New York (outside the USA) DOI:10.1007/s10669-013-9485-y.
- NIST (2021), National Institute of Standards and Technology. *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*, (SP) 800-160 Volume2, Revision1, Retrieved from https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final
- Ross, R.; Graubart, R.; Bodeau, D. & Mcquaid, R. (2018), Systems Security Engineering: *Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems*, (NIST) National Institute of Standards and Technology.
- Sharkov, G. From cybersecurity to collaborative resiliency. In Proceedings of the 2016 ACM *Workshop on Automated Decision Making for Active Cyber Defense*, Vienna, Austria, 24–28 October 2016; pp. 3–9.