Military Science and Tactics
AJA Command and Staff University
https://www.qjmst.ir/
Online ISSN: 4520-2676
Print ISSN: 2008-191x

# Cyber Resilience Model of Defense Systems and Products

**Rasool Ramezani Dehaghi [1]✉ | Ali Mohammad Aminzadeh[2]**

1. Ph.D. in Strategic Management of Cyber Space, Assistant Professor of Khatam Al-Anbia Air Defense University, Tehran, Iran.
   E-mail: mo.aminzadeh@gmail.com
2. Ph.D. in Strategic Management of Cyber Space, Director of Cyber Defense Center of Information Exchange Security Industries, Tehran, Iran.
   E-mail: Sepehrramezany@yahoo.com

**Article Info**

**Article type:**
Research Article

**Article history:**
Received 18 March 2023
Received in revised form 1 July 2023
Accepted 16 July 2023
Published online 4 September 2023

**Keywords**:
*Maintenance of defense items, maintenance and repairs of weapons, grassroots unit, maintenance and repairs strategy, sustainable resistance network, pathology.*

**ABSTRACT**

**Objective:** The main goal of this research is to present the model of cyber resilience of defense systems and its sub-goals are to explain the cyber threats of defense systems, and to explain the dimensions, components and indicators of cyber resilience of defense systems.

**Method:** The current research is categorized as descriptive/analytical research with an exploratory perspective. Data collection was done using the grounded theory method and interview tool, and the questionnaire tool was used to determine the importance of the indicators and select the final indicators. In order to check the significance of the relationship between dimensions, components and indicators, factor analysis method and Smart P.L.S. software was used. The statistical population of the research includes 30 experts in this field and the sample population is considered as a whole number.

**Findings:** The cyber resilience model of defense systems was presented in the dimensions of supervision and leadership with 4 components and 21 indicators, control dimension with 4 components and 16 indicators, process and operation dimension with 3 main components and 17 indicators. The factor loading coefficients for the three mentioned dimensions were obtained as 0.921, 0.917 and 0.926, respectively, which is a sign of the high importance of these factors in increasing cyber resilience.

**Conclusion:** Cyber resilience of defense systems includes measures that defense organizations must take to resist cyber incidents and recover quickly after interruptions. Therefore, in order to be able to resist attacks, incidents or cyber threats, defense systems must be resilient in the three dimensions of supervision and leadership, control and automation, as well as the dimension of process and operations.

**Cite this article:** Ramezani Dehaghi, R., & Aminzadeh, A. M. (2023). Cyber resilience model of defense systems. Military Science and Tactics, 19(64), 81-96.
doi: 10.22034/qjmst.2023.551755.1693


**Publisher:** Command and Staff University
DOI: 10.22034/QJMST.2023.551755.1693

فصلنامه علمی علوم و فنون نظامی
شاپای چاپی: ۱۹۱۸-۲۰۰۸ شاپای الکترونیکی: ۴۵۳۰-۲۶۷۶ https://www.qjmst.ir/ دانشگاه فرماندهی و ستاد آجا

# الگوی تاب‌آوری سایبری سامانه‌ها و محصولات دفاعی

رسول رمضانی‌دهقی[1]✉ | علی‌محمد امین‌زاده [2]

۱. دکترای مدیریت راهبردی فضای سایبر، استادیار دانشگاه پدافند هوایی خاتم الانبیاء(ص)، تهران، ایران.
رایانامه: Sepehrramezany@yahoo.com

۲. دکتری مدیریت راهبردی فضای سایبر، مدیر مرکز دفاع سایبری صنایع امنیت تبادل اطلاعات، تهران، ایران.
رایانامه: mo.aminzadeh@gmail.com

اطلاعات مقاله

**نوع مقاله:**
**مقاله پژوهشی**
مقالهٔ پژوهشی

**تاریخ دریافت:**
۱۴۰۱/۱۲/۲۷

**تاریخ بازنگری:**
۱۴۰۲/۰۴/۱۰

**تاریخ پذیرش:**
۱۴۰۲/۰۴/۲۵

**تاریخ انتشار:**
۱۴۰۲/۰۶/۱۳

**کلیدواژه‌ها:**
*تاب‌آوری سایبری، سامانه‌های دفاعی، تهدیدات سایبری، آسیب‌پذیری‌های سایبری.*

چکیده

**هدف:** هدف اصلی این پژوهش ارایه الگوی تاب‌آوری سایبری سامانه‌های دفاعی و اهداف فرعی آن تبیین تهدیدات سایبری سامانه‌های دفاعی، تبیین ابعاد، مؤلفه‌ها و شاخص‌های تاب‌آوری سایبری سامانه‌های دفاعی است.

**روش:** پژوهش حاضر در زمره تحقیقات توصیفی/تحلیلی با نگاه اکتشافی دسته‌بندی می‌گردد. جمع‌آوری داده‌ها در این پژوهش با بهره‌گیری از روش نظریه زمینه‌ای و ابزار مصاحبه عمیق انجام شده و از ابزار پرسشنامه جهت تعیین میزان اهمیت شاخص‌ها و انتخاب شاخص‌های نهایی استفاده گردید. به منظور بررسی معنی‌دار بودن ارتباط ابعاد، مولفه‌ها و شاخص‌ها، از روش تحلیل بارعاملی و نرم‌افزار اسمارت پی. ال. اس استفاده شد. جامعه آماری پژوهش شامل تعداد ۳۰ نفر از خبرگان و صاحب‌نظران این حوزه و جامعه نمونه به صورت تمام شمار در نظر گرفته شده است.

**یافته‌ها:** الگوی تاب‌آوری سایبری سامانه‌های دفاعی در بعدهای نظارت و راهبری با ۴ مولفه اصلی و ۲۱ شاخص، بعد کنترل با ۴ مولفه اصلی و ۱۶ شاخص، بعد فرآیند و عملیات با ۳ مولفه اصلی و ۱۷ شاخص ارایه گردید. ضرایب بار عاملی برای سه بعدهای یاد شده به ترتیب برابر ۰/۹۲۱، ۰/۹۱۷ و ۰/۹۲۶ به‌دست آمد که نشانه اهمیت بالای این عوامل در افزایش تاب‌آوری سایبری است.

**نتیجه‌گیری:** تاب‌آوری سایبری سامانه‌های دفاعی شامل اقداماتی است که سازمان‌های دفاعی باید برای مقاومت در برابر رخدادهای سایبری و بهبود سریع پس از وقفه‌های ایجاد شده انجام دهند. براین اساس به منظور توانایی مقاومت در برابر حملات، حوادث یا تهدیدات سایبری، سامانه‌های دفاعی بایستی در سه بعد راهبری و نظارت، کنترل و اتوماسیون و همچنین بعد فرآیند و عملیات تاب‌آور شوند.

**استناد:** رمضانی دهقی، رسول و امین زاده، علی محمد. (۱۴۰۲). الگوی تاب آوری سایبری سامانه ها و محصولات دفاعی. علوم و فنون نظامی، ۱۹(۶۴)، ۹۶-۸۱. doi: 10.22034/qjmst.2023.551755.1693

**ناشر:** دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

**مقدمه**

تاب‌آوری یک فرآیند، توانایی و یا پیامد سازگار موفقیت‌آمیز با شرایط تهدیدکننده است (Bodeau & etal, 2015). تاب‌آوری سایبری ناظر به توانایی یک سامانه سایبری در ارایه مستمر نتایج مورد انتظار به رغم رویدادهای سایبری نامطلوب است. به بیان ساده، سامانه‌های سایبری باید بتوانند حتی در صورت وجود حملات سایبری مخرب به فعالیت خود ادامه دهند (بت شکن، ۱۳۹۶: ۲).

تاب‌آوری سایبری یک رویکرد نوظهور برای حمایت از سازمان‌ها در برابر تهدیدات سایبری است و بکارگیری این رویکردها، معماری سایبری سازمان‌های هدف را به نحوی تغییر می‌دهد که بتوانند بیش‌ترین انعطاف را در مقابله با حملات سایبری داشته باشند. تاب‌آوری سایبری شامل تمام مراحلی است که سازمان باید انجام دهد تا برای سازگاری با شرایط در حال تغییر، مقاومت در برابر حوادث و بهبود سریع پس از وقفه‌های ایجاد شده، خود را آماده نماید. در این مفهوم، یک سازمان زمانی انعطاف‌پذیر است که توانایی مقاومت در برابر حملات، حوادث یا تهدیدات را داشته باشد (Conklin & Shoemaker, 2017).

اغلب، بکارگیری سامانه‌های سایبرپایه در مجموعه‌های نظامی و دفاعی، از سایربخش ها پیشروتر است. چالش بزرگ سامانه‌های دفاعی نوین آن است که فناوری‌های عملیاتی[1] به نحو چشم‌گیری با فناوری‌های اطلاعاتی[2] تلفیق شده است، از این رو تهدیدات فراوان و روزافزون فناوری اطلاعاتی، به سامانه‌های عملیاتی نیز تعمیم یافته است. به علاوه، وجود محدودیت‌های متعدد در بکارگیری ابزارهای تشخیص بدافزار در سامانه های عملیاتی، موجب افزایش خطرپذیری در سامانه‌های دفاعی شده است. همچنین سامانه‌های دفاعی سایبر پایه، با یک تهدید بزرگ‌تر، یعنی حساسیت حوزه کاری مواجه می‌باشند زیرا تمرکز دشمن بر تضعیف توان دفاعی و نظامی کشور است (Colbert & Kott, 2016).

ایجاد تداوم عملیاتی در سامانه‌های دفاعی مستلزم در اختیار داشتن سامانه‌های تاب‌آور در مواجهه با رخدادهای روز افزون سایبری و ایجاد معماری مناسب در توسعه سامانه‌های دفاعی است. دستیابی به این مهم نیازمند یک الگوی مناسب است تا اجزاء و موارد مربوط به تاب‌آوری سایبری را برای سامانه‌ها و محصولات دفاعی مشخص نموده و نحوه مواجهه و رفتار مناسب در مقابله با تهدیدات سایبری را جهت استمرار فعالیت سامانه‌ها، تعیین نماید.

---

[1] Opration Technology

[2] Information Technology

دستیابی به سامانه‌های دفاعی تاب‌آور سایبری، مستلزم داشتن نگاه یکپارچه و همچنین وحدت رویه در شناسایی و اقدام مناسب در زمان اجرایی شدن تهدیدات سایبری در سامانه‌های دفاعی است که این نکته نشان دهنده اهمیت بهره‌گیری از یک الگوی مناسب در تاب‌آوری سایبری سامانه‌های دفاعی در مواجهه با تهدیدات سایبری می‌باشد. فقدان یک الگوی مناسب در مواجهه با حملات سایبری به سامانه‌های دفاعی، موجب تحمیل هزینه‌های بسیار بالا و در برخی موارد، غیر قابل جبران، به سیستم دفاعی کشور می‌گردد. همچنین در صورت بروز حمله سایبری، می‌بایست سامانه‌های دفاعی مورد حمله، 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 الگوی تاب‌آوری سایبری سامانه‌های دفاعی بوده و اهداف فرعی آن بررسی تهدیدات سایبری سامانه‌های دفاعی، تبیین آسیب‌پذیری‌های سایبری سامانه‌های دفاعی و در نهایت ارایه ابعاد، مؤلفه‌ها و شاخص‌های الگوی تاب‌آوری سایبری سامانه‌های دفاعی می‌باشد.

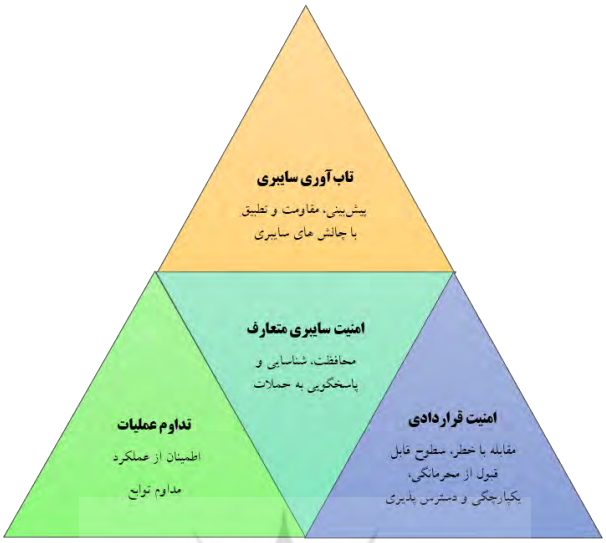
## مبانی نظری و پیشینه‌های پژوهش

### مبانی نظری

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 مدل 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. سپس 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).

### مبانی تاب‌آوری سایبری

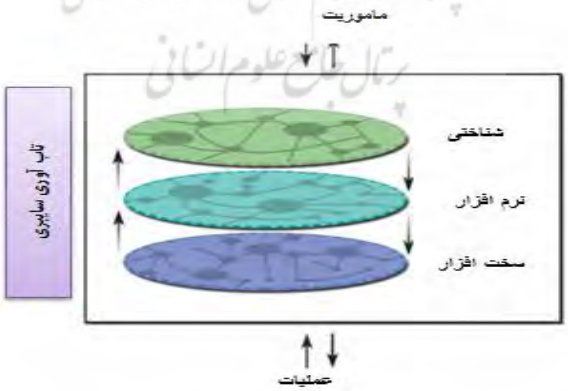
همانگونه که در شکل ۱ نشان داده شده است، تاب‌آوری سایبری بر روی سه پایه امنیت سایبری متعارف، تداوم عملیات و امنیت قراردادی، ساخته شده است. بر اساس این مدل: دربخش امنیت سایبری متعارف، کشف حملات و واکنش مناسب به آن‌ها، انجام می‌شود.بخش تداوم عملیات، ایمن‌سازی و امنیت داده‌ها را تامین می‌کند.بخش امنیت قراردادی،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




**شکل (۱) مبانی 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 فیزیکی و اطلاعاتی بلکه حوزه‌های شناختی و اجتماعی را در بر می‌گیرند. تاب‌آوری سایبری تضمین می‌کند که بازیابی سامانه، با در نظر گرفتن زیرساخت‌های سایبری (سخت‌افزار، نرم‌افزار) و مؤلفه‌های حساس به هم پیوسته، در اسرع وقت انجام می‌شود. بنابراین تاب‌آوری سایبری یک پل بین پایداری عملکردهای سامانه و اطمینان از اجرای ماموریت است.




**شکل (۲) حوزه‌های تاب‌آوری سایبری (Kott & Linkov, 2019: 18).**

حوزه‌های تاب‌آوری در برابر رخدادهای سایبری شامل مولفه‌های شناختی، سخت افزار و نرم افزار 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، روان شناختی، سازمانی و مهندسی را در هم می‌آمیزد. برای مثال مهندسی تاب‌آوری به عنوان "توانایی سامانه‌ها برای پیش‌بینی و سازگاری با شرایط بحرانی" تعریف شده است. که این مطلب نشان دهنده میزان اهمیت محافظت از سامانه‌ها در مواجهه با حوادث غیرمنتظره است (Kott & Linkov, 2019: 17).

## پنج رکن اصلی تاب‌آوری سایبری

تاب‌آوری سایبری نیازمند اصلاح مداوم است. می‌توان این‌گونه گفت که این روند، چارچوبی است که دارای پنج رکن اصلی: آمادگی و شناسایی، محافظت، کشف، پاسخگویی و بازیابی است. برای هر یک از این ارکان، رویکردهایی مبتنی بر بهترین راه‌کارها با هدف به حداقل رساندن خطر سایبری پیشنهاد شده و هر رکن، نیازمند اقدامات به‌خصوصی است که باید توسط کارکنان فناوری اطلاعات اجرا شوند (سعادتی، ۱۴۰۰: ۱۱۸).

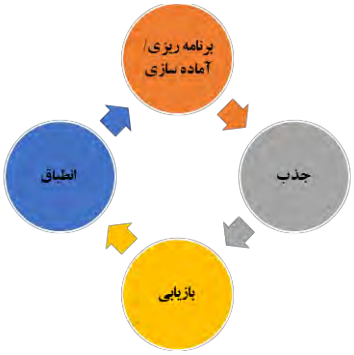

**شکل (۳) پنج رکن اصلی تاب‌آوری سایبری**

## معیارهای تاب‌آوری برای سامانه‌های سایبری

آکادمی بین المللی علوم آمریکا، چهار فاز را در چرخه مدیریت رویداد، ارایه کرده که هر سامانه می‌بایست برای ماندگاری تاب‌آوری خود، آن‌ها را اعمال نماید.

- **برنامه‌ریزی آماده‌سازی** قراردادن پایه و اساسی برای حفظ دسترسی به خدمات و فعالیت سامانه‌ها طی یک رویداد مخرب (سوء عمل یا حمله)
- **جذب:** حفظ و نگهداشت فعالیت اکثر سامانه‌های حیاتی و دسترسی به خدمات در حین دفع و جداسازی عامل تخریب.
- **بازیابی:** بازگرداندن کارکرد تمامی سامانه‌ها و دسترسی به خدمات به حالت قبل از رویداد.
- **انطباق:** با کسب دانش از رویدادها، اصلاح پروتکل، تصحیح پیکربندی، آموزش پرسنل، و... ، سامانه‌ها تاب‌آورتر می‌شوند (DSB, 2013).

این چهار مرحله به‌صورت شکل زیر ارایه می‌گردند:




**شکل (۴) معیارهای تاب‌آوری برای سامانه‌های سایبری (DSB, 2013).**

## اصول تاب‌آوری سایبری

در تاب‌آوری سایبری هفت اصل مهم 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 بر اساس چارچوب امنیت سایبری بیان می‌گردد.

بازیابی: فرآیندهای تعریف شده باید مستند و در محلی قرار داده شوند که اطمینان حاصل شود 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، از پایداری سازمان اطمینان حاصل شود.

رتبه: دارایی‌هایی که از دست دادن آن‌ها به سازمان آسیب غیر قابل جبران می‌زند، انتخاب و ارزیابی شده و یک پاسخ موثر برای هر یک از آن‌ها پیش‌بینی می‌شود. منابع سازمان تنها به تضمین این موارد مهم متمرکز می‌شوند. در مرحله بعد، به دفاع از بقیه دارایی‌های سازمان توجه می‌گردد.

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 سازمان، بایستی تمام دارایی‌های سازمان شناسایی و برچسب‌گذاری شده و در یک مبنای منطقی از اشیاء قرار گیرند (سعادتی، ۱۴۰۰: ۱۳۳).

## تکنیک‌های ارتقاء تاب‌آوری سایبری

تکنیک‌های تاب‌آوری سایبری، روش‌هایی هستند که با پشتیبانی از عملکرد منابع سایبری، یک یا چند هدف میان‌مدت را در تاب‌آوری سایبری سازمان محقق می‌نمایند. این تکنیک‌ها با توجه به معماری یا طراحی ماموریت سازمان انتخاب می‌شوند تا آن‌ها را برای دستیابی به اهداف سازمان کمک نمایند. برخی از این تکنیک‌ها در ادامه به صورت مختصر آورده شده است.

۱) پاسخ تطبیقی: بهینه‌سازی توانایی زیرمجموعه جهت پاسخگویی به‌موقع و مناسب.
۲) نظارت تحلیلی: نظارت و تشخیص اقدامات و شرایط نامطلوب.
۳) حمایت هماهنگ: اجرای یک راهبرد عمیق دفاعی.
۴) فریب: مخفی کردن دارایی‌های مهم و نمایش دارایی‌های فریبنده.
۵) تنوع: استفاده از ناهمگونی برای به حداقل رساندن خرابی‌ها.
۶) 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 پیش‌بینی بودن: انجام تغییرات را به‌طور تصادفی و غیر منتظره در راستای کاهش امکان تشخیص فرایندهای محافظتی (Ross & et al, 2018).

## پیشینه پژوهش

در راستای بررسی پیشینه الگوی تاب‌آوری سایبری سامانه‌ها و سیستم‌ها، تعداد ۱۸ مقاله داخلی و خارجی و ۵ سند ارایه شده توسط موسسات پژوهشی و تحقیقاتی، مورد بررسی و واکاوی قرار گرفت که در ادامه برخی از این پژوهش‌ها آورده شده است:

لینکو و همکاران[1] (۲۰۱۳) در پژوهشی تحت عنوان "معیارهای تاب‌آوری برای سامانه‌های سایبری" یک چارچوب ماتریسی تاب‌آوری را برای توسعه و سازماندهی معیارهای موثر تاب‌آوری برای سامانه‌های سایبری ارایه نمودند. همچنین آن‌ها در گزارش سال ۲۰۱۳ هیئت علمی دفاعی آمریکا[2] تحت عنوان "سامانه‌های ارتش تاب‌آور و تهدیدات پیشرفته سایبری" بر دو ویژگی برای معیارهای تاب‌آوری سایبری تاکید نمودند: (۱) معیارها به اندازه کافی گسترده باشند تا در طیف متنوعی از سامانه استفاده شوند؛ (۲) معیارها به اندازه کافی دقیق باشند تا بتوانند فرآیندها و اجزای سامانه‌های خاص را اندازه‌گیری کنند (Linkov & etal, 2013).

وی و جی[3](۲۰۱۵)، در مقاله‌ای با عنوان "سامانه‌های صنعتی تاب‌آور: مفاهیم، فرمول‌بندی، معیارها و بینش‌ها"، ضمن تبیین شاخصه‌های مورد نیاز سامانه‌های صنعتی تاب‌آور، معیارهای ارزیابی تاب‌آوری در مقابل تهدیدات سایبری را در سامانه‌های صنعتی بیان نموده‌اند (Wei & Ji, 2015).

مظفری و همکاران(۲۰۱۹)، در مقاله‌ای تحت عنوان "احصاء شاخص‌های تاب‌آوری برکاهش آسیب‌پذیری سیستم‌های کنترل صنعتی در تهدیدات سایبری"، بیان می‌دارند که شاخص‌های حس تشـــخیص، اجرای اقدامات کنترلی در عملیات روزمره، توســـعه توابع نظارتی (کنترل‌های اینترنتی،بخش قانونی، مدیریت ریسک و امنیت سایبری)، استفاده قوی ازبخش ممیزی داخلی و واکنش و ترمیم، بر کاهش آسیب‌پذیری سیستم‌های کنترل صنعتی در برابر تهدیدات سایبری تاثیر دارد (مظفری و همکاران، ۲۰۱۹).

پژوهشکده امنیت سایبری دانشگاه کارنگی ملون به عنوان یکی از مراکز معتبر در حوزه ارایه استانداردها و دستور العمل‌های سایبری در سال ۲۰۱۶ به سفارش وزارت امنیت داخلی آمریکا، مجموعه دســـتور العمل‌های تاب‌آوری ســـایبری را در ۱۰ ســـرفصـــل کلی با هدف ارتقاء امنیت سایبری به تاب‌آوری سایبری ارایه نمود (DHS, 2016).

انیستیتو ملی استاندارد و فناوری آمریکا[4] در سال ۲۰۲۱، استاندارد ایجاد تاب‌آوری سایبری در سیستم‌ها و سامانه‌های سایبر پایه را ارایه نمود (NIST, 2021).

در پژوهش‌های انجام شده فوق، به مواردی از قبیل اهمیت سامانه‌های مبتنی بر شبکه، پایش و کنترل فرآیندها، ارایه راه‌کارهای بهبود امنیتی سامانه‌ها و همچنین مدیریت و اصلاح انواع مختلف آسیب‌پذیری‌های سامانه‌ها، اشاره شده است. ارایه راه‌کارهای از پیش تعیین شده، تاکید

---

[1] Linkov et al.

[2] Defense Science Board(Dsb)

[3] Wei & Ji

[4] Nist

بر بهبود امنیت سایبری و همچنین روش‌های اندازه‌گیری آن‌ها نیز موضوع دیگری است که به آن‌ها اشاره شده است ولی در تحقیقات یاد شده، تاب‌آوری سامانه‌ها و محصولات دفاعی مورد بررسی قرار نگرفته است. در پژوهش حاضر، تمرکز اصلی تحقیق بر روی سامانه‌ها و محصولات خاص دفاعی و نظامی بوده و الگوی تاب‌آوری سامانه‌ها و محصولات دفاعی در مقابله با تهدیدات فضای سایبر ارایه گردیده است که نکته اصلی متمایز کننده این پژوهش با سایر پژوهش‌های انجام شده است.

## مدل مفهومی پژوهش

در این پژوهش جهت تدوین الگو از روش نظریه سیستم‌ها شامل اجزاء: عوامل موثر، فرایندها و بروندادها (علاقه بند، ۱۴۰۰: ۱۲۴) استفاده شده است. در این راستا ابتدا عوامل موثر بر تاب‌آوری سایبری سامانه‌های دفاعی (شامل الزامات مندرج در اسناد بالادستی، تهدیدهای سایبری تجهیزات و سامانه‌های دفاعی، محدودیت‌های ناشی از تحریم‌های فناورانه، الزامات امنیتی سامانه‌های سایبر پایه و آسیب‌پذیری‌های سامانه‌های سایبر پایه) مورد مطالعه قرار گرفته و بر اساس نتایج حاصله، فرایندها شامل (ابعاد، مولفه‌ها و شاخص‌های مرتبط با الگوی تاب‌آوری سامانه‌های دفاعی) استخراج گردید. با توجه به موارد پیش گفته، مدل مفهومی تحقیق برابر شکل زیر جمع‌بندی می‌گردد:


**شکل (۵) مدل مفهومی پژوهش**

## روش‌شناسی پژوهش

پژوهش حاضر از لحاظ طرح تحقیق در زمره تحقیقات آینده‌نگر دسته‌بندی می‌گردد. این پژوهش به این دلیل آینده‌نگر است که محقق در پی طراحی الگوی تاب‌آوری سایبری سامانه‌های دفاعی در جهت مقابله با تهدیدات سایبری آتی پیش روی سامانه‌های دفاعی می‌باشد. همچنین پژوهش حاضر از لحاظ روش تحقیق در زمره تحقیقات توصیفی/تحلیلی با نگاه اکتشافی دسته‌بندی می‌گردد. این پژوهش به این دلیل توصیفی/تحلیلی است که محقق با نگاه راهبردی به توصیف تاب‌آوری سایبری سامانه‌های دفاعی پرداخته و با استفاده از روش‌های راهبردی به تحلیل تهدیدات و آسیب‌پذیری‌های سایبری در سامانه‌های دفاعی سایبر پایه پرداخته است و بر اساس این دو نگاه با دید اکتشافی، چارچوب اولیه‌ای برای تدوین الگوی تاب‌آوری سایبری سامانه‌های دفاعی ارایه نموده است.

در راستای احصای گویه‌های لازم جهت تدوین شاخص‌های پیاده‌سازی و ارزیابی اقدامات لازم برای اجرای تاب‌آوری سایبری دفاعی، از روش تحقیق نظریه زمینه‌ای و ابزار مصاحبه عمیق با خبرگان این حوزه استفاده گردید. سپس با استفاده از ابزار پرسشنامه، نظر خبرگان و صاحب‌نظران در خصوص میزان اهمیت شاخص‌ها جمع‌آوری و شاخص‌های نهایی الگو تعیین شد.

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 تحقیق، 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 است (که دارای شرایط: مدرک کارشناشی ارشد و بالاتر، آشنایی با مباحث سایبری و دارا بودن جایگاه شغلی راهبردی می‌باشند) و جامعه نمونه به صورت تمام شمار برابر با جامعه آماری در نظر گرفته شد. قلمرو مکانی پژوهش حاضر کشور جمهوری اسلامی ایران و قلمرو زمانی آن افق ۱۴۰۴ می‌باشد.

## تجزیه و تحلیل داده‌ها

با توجه به این که پژوهش حاضر به روش تحقیق نظریه زمینه‌ای انجام شده است، جهت طبقه‌بندی اطلاعات 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 که در جدول شماره ۱ قابل مشاهده 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 که خروجی این مرحله در جدول شماره ۲ آورده شده است. کدگذاری انتخابی عبارت است از فرآیند انتخاب دسته‌بندی اصلی، مرتبط کردن نظام‌مند آن‌ها با دسته‌بندی‌های دیگر، 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 مقوله‌سازی از آن‌ها در چندین مرحله، مقوله‌های کلان (مؤلفه‌ها) مطابق با جدول ذیل استخراج گردید.

**جدول (۱) استخراج مولفه‌ها از شناسه‌های استخراج شده**

| شناسه استخراج شده | مقوله کلان (مولفه) |
|---|---|
| شناسایی و اولویت‌بندی تجهیزات و زیر سامانه‌ها براساس عملکرد، تعیین وظایف و عملکرد تجهزات و زیر سامانه‌ها، تعیین ارتباط زیر سامانه‌ها و تجهیزات با عملکردها (گزارش موسسه ثبات مالی، ۲۰۱۸)، تعیین سطح دسترسی به زیر سامانه، دسته‌بندی براساس اطلاعات سامانه‌ها جهت حصول اطمینان و حفظ عملکرد اساسی، اولویت‌بندی اقدامات پشتیبان عملیات اساسی سامانه (Benz & Chatterjee, 2020) | مدیریت دارایی و تجهیزات سامانه‌های دفاعی |
| پیاده‌سازی فرایند مدیریت تغییر در سامانه‌ها، ارزیابی اجرایی شدن الزامات تاب‌آوری در زمان انجام تغییرات در سامانه‌ها (Sharkov,2016)، نظارت بر چرخه زندگی سامانه‌ها در جهت برنامه‌ریزی سامانه‌های پشتیبان در مواقع بحرانی (Carias & et al, 2020)، نظارت مستمر بر انجام پیکربندی‌های به موقع برای سامانه‌های فناوری محور نظیر نصب وصله‌های امنیتی در نرم افزارهای سیستم عامل سامانه‌های عملیاتی (Gourisetti & et al, 2019). | پیکربندی و مدیریت تغییر سامانه‌های دفاعی |
| 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 غیر عامل |
| انجام کنترل برای اجرای حفاظت از شبکه و در صورت لزوم، جداسازی شبکه، کنترل برای حفاظت اطلاعات در وضعیت‌های مورد استفاده، کنترل برای حفاظت اطلاعات در زمان وقوع حمله و نشت داده‌ها (Benz & Chatterjee, 2020)، اجرا و کنترل شیوه‌های امنیت سایبری برای منابع انسانی مرتبط با سامانه، تعیین و کنترل سطح دسترسی به سامانه‌ها و دارایی‌ها با ترکیب اصل کم‌ترین قابلیت (Carias & et al, 2020). | کنترل عملکرد سامانه‌های دفاعی |
| ایجاد فرایند مدیریت ریسک با شناسایی، تحلیل و رفع خطرات، شناسایی حد آستانه ریسک و تمرکز فعالیت‌های مدیریت ریسک با شناسایی حوزه‌های تاثیرپذیر در سامانه (گزارش مرکز امنیت اینترنت، ۲۰۱۹)، تعیین پارامترهای تحمل ریسک برای هر حوزه تاثیرپذیر و تعیین آستانه تحمل‌پذیری تجزیه و تحلیل ریسک‌ها و تعیین اقدام مناسب در برابر آن (Gourisetti & et al, 2019). | مدیریت ریسک سامانه‌های دفاعی |

| شناسه استخراج شده | مقوله کلان (مولفه) |
|---|---|
| ایجاد و حفظ روند شناسایی و تجزیه و تحلیل آسیب‌پذیری نرم افزارها، دسته‌بندی و اولویت‌بندی آسیب‌پذیری‌ها (گزارش مرکز امنیت اینترنت، ۲۰۱۹)، اقدامات لازم برای مواجهه آسیب‌پذیری‌های شناسایی شده و کاهش اثرپذیری، بررسی علل ریشه‌ای آسیب‌پذیری‌ها و ارزیابی نتایج کاهش آسیب‌پذیری‌ها (Deutscher, 2017). | مدیریت آسیب‌پذیری‌های سامانه‌های دفاعی |
| ایجاد فرایند شناسایی، تحلیل، پاسخ‌گویی و یادگیری از حوادث، شناسایی و مستندسازی حوادث و رخدادها شامل رویدادهای سایبری (گزارش موسسه ثبات مالی، ۲۰۱۸)، ثبت رخدادها در پایگاه داده و طبقه‌بندی و اولویت‌بندی آن‌ها، ردیابی حوادث، ایجاد سامانه پاسخ‌گویی سریع به حوادث/ حملات سایبری برای هر سامانه (Carias & et al, 2020). | مدیریت رخدادها و حوادث سایبری سامانه‌های دفاعی |
| توسعه برنامه‌های تداوم خدمات برای خدمات ارزشمند سامانه، تعیین وظیفه نیروی انسانی برای اجرای برنامه‌های تداوم خدمات خاص (گزارش مرکز امنیت اینترنت، ۲۰۱۹)، مستندسازی و در دسترس بودن برنامه‌های پیوستگی خدمات به صورت کنترل شده، برنامه‌ریزی و بررسی برنامه‌های تداوم خدمات و بهبود حاصل شده (Benz & Chatterjee, 2020). | تداوم فعالیت‌های سامانه‌های دفاعی |
| 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 دفاعی |
| احصای نیازمندی‌های 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 ارایه برنامه‌های بهبود آموزشی (Armenia & et al, 2021) | آموزش و آگاهی مدیران و کارشناسان دفاعی |
| راه‌اندازی سامانه آگاهی وضعیتی تاب‌آوری سایبری، تعیین مسئولیت نظارت بر منابع اطلاعات تهدید شناسایی (Carias & et al, 2020)، اولویت‌بندی و انتقال اطلاعات تهدید به ذینفعان داخلی، شناسایی، اولویت‌بندی و انتقال اطلاعات تهدید به ذینفعان خارجی (گزارش مرکز امنیت اینترنت، ۲۰۱۹) | آگاهی وضعیتی تاب‌آوری سامانه‌های دفاعی |

**تشکیل مقوله‌های محوری (بعدها)**

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

**جدول (۲) تشکیل ابعاد از مولفه‌های استخراج شده**

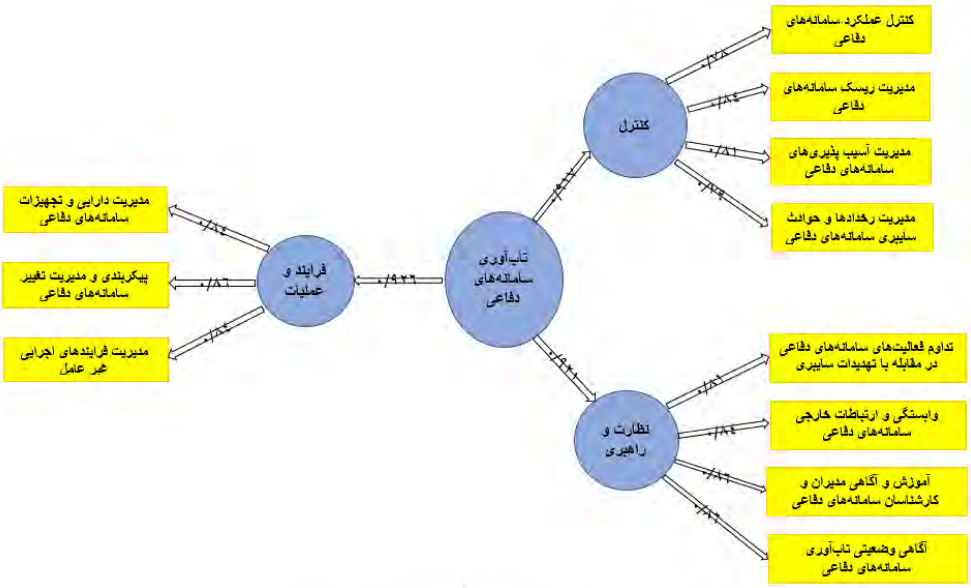
| مقوله کلان (مولفه) | مقوله‌های محوری (بُعد) |
|---|---|
| مدیریت دارایی و تجهیزات سامانه‌های دفاعی | تاب‌آوری سایبری سامانه‌های دفاعی در بعد فرآیند و عملیات |
| پیکربندی و مدیریت تغییر سامانه‌های دفاعی | |
| مدیریت فرایندهای اجرایی غیر عامل | |
| کنترل عملکرد سامانه‌های دفاعی | تاب‌آوری سایبری سامانه‌های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

## یافته‌های تحقیق

نتیجه اصلی این پژوهش ارایه الگوی تاب‌آوری سایبری سامانه‌های دفاعی در سه بعد نظارت و راهبری با ۴ مولفه اصلی و ۲۱ شاخص، بعد کنترل و اتوماسیون با ۴ مولفه اصلی و ۱۶ شاخص و بعد فرآیند و عملیات با ۳ مولفه اصلی و ۱۷ شاخص است که در یک شکل منسجم ارایه شده است. همچنین در این پژوهش ۶ عامل تهدید اصلی که در بر گیرنده ۲۸ تهدید فرعی برای سامانه‌های دفاعی می‌باشد ارایه شده است.

در این تحقیق برای آزمون مدل مفهومی از مدل‌سازی معادلات ساختاری مبتنی بر رویکرد حداقل مربعات جزیی با نرم‌افزار اسمارت پی. ال. اس[1] استفاده شده است. در این روش میزان سهم هر عامل در ایجاد متغیر، مورد بررسی قرار می‌گیرد و برای این کار از تحلیل عاملی تاییدی استفاد می‌شود. در تحلیل عاملی، مقدار بار عاملی کمتر از ۰/۳ نشان دهنده مقیاس ضعیف، بارهای عاملی بین ۰/۳ تا ۰/۶ نشان دهنده مقیاس متوسط و مقادیر بزرگتر از ۰/۶ نیز نشان دهنده متغیر مشاهده پذیر با مقیاس قابل اطمینان می‌باشد. در کل مقادیر بارهای عاملی کوچک‌تر از ۰/۴ 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 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 ۶ ارایه شده است.

[1] Smart Pls 9.98

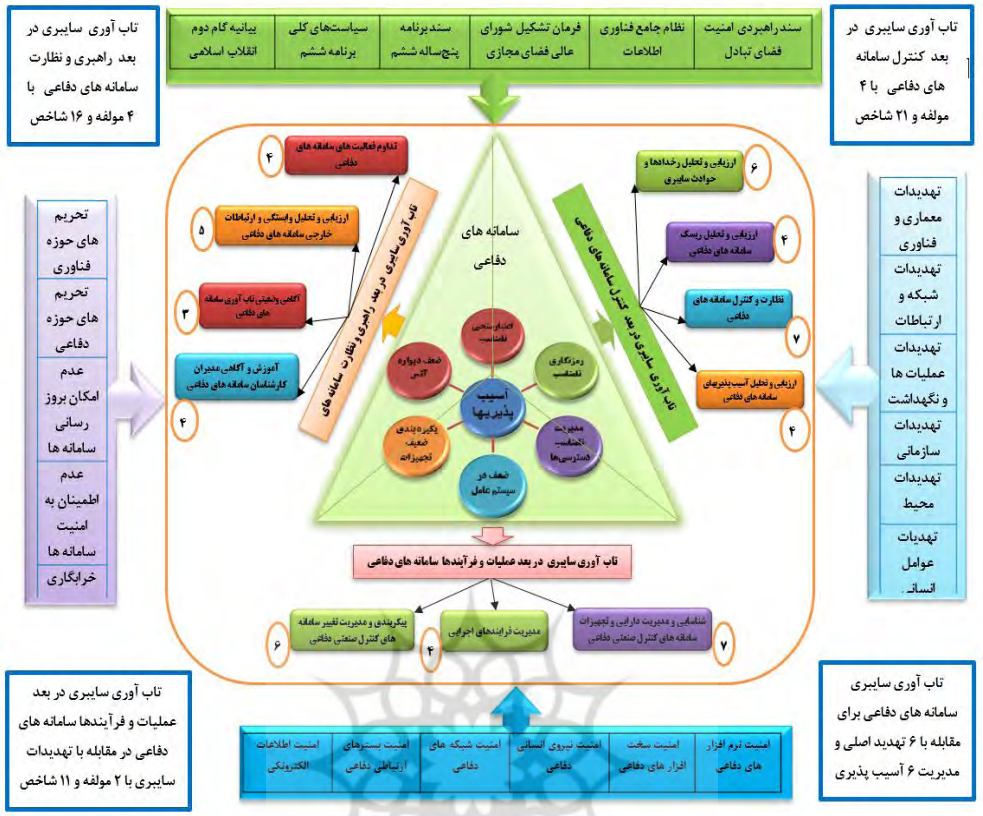



**شکل (۶) نتایج تحلیل عاملی الگو**

همان‌گونه که در شکل فوق مشاهده می‌شود تمامی مولفه‌ها، مقادیر بارهای عاملی بزرگ‌تر از ۰/۷ داشته و از اعتبار لازم برخوردار می‌باشند. در الگوی فوق ضرایب مسیرها برای سه بعد فرآیند و عملیات، کنترل و اتوماسیون و نظارت و راهبری، به ترتیب برابر ۰/۹۲۶، ۰/۹۱۷ و ۰/۹۲۱ می‌باشد، لذا بعد فرآیند و عملیات، بالاترین تاثیر و بعدهای نظارت و راهبری و کنترل و اتوماسیون با اختلاف کمی در جایگاه دوم و سوم قرار دارند.

## نتیجه‌گیری و پیشنهاد

براساس مطالعات انجام شده و دریافت نظر خبرگان و کارشناسان حوزه سامانه‌های دفاعی در سازمان‌های صنایع دفاعی کشور، الگوی تاب‌آوری سایبری سامانه‌های دفاعی در بعد راهبری و نظارت در مقابله با تهدیدات سایبری با ۴ مولفه اصلی و ۲۱ شاخص، در بعد کنترل و اتوماسیون با ۴ مولفه اصلی و ۱۶ شاخص و در بعد فرآیند و عملیات با ۳ مولفه اصلی و ۱۷ شاخص، برابر شکل ۷ ارایه شده است.




**شکل (۷) الگوی تاب‌آوری سایبری سامانه‌های دفاعی**

سامانه‌های دفاعی با شش دسته تهدید اصلی که در برگیرنده ۲۸ تهدید می‌باشد به شرح جدول ذیل مواجه می‌باشند.

**جدول (۳) تهدیدهای سامانه‌های دفاعی (گزارش موسسه تهدیدهای امنیت اینترنت، ۲۰۱۹)**

| عامل اصلی | تهدیدهای سامانه‌ها |
|---|---|
| تهدیدهای سازمانی | عدم تعیین سطح اجرایی عملیات، فقدان مدیریت یکپارچه امنیت اطلاعات، تمایز فرهنگ کاربران، کمبود آموزش کاربران، دوره استهلاک تجهیزات، استانداردهای امنیت فناوری‌اطلاعات و ارتباطات |
| تهدیدهای معماری و فناوری | فناوری قدیمی و فرسوده، ناامنی در طراحی سامانه‌ها، قابلیت جدید برای اجزای قدیمی، پروتکل‌های غیر استاندارد صنعتی |
| شبکه و ارتباطات | محیط عملیاتی نامناسب، دسترسی از راه دور به شبکه، وابستگی‌های سامانه‌های فناوری اطلاعات و ارتباطات، ارتباط مستقیم با اینترنت |
| عوامل انسانی | کمبود آگاهی کاربر، سیاست‌ها و رویه‌های نامناسب، کارمند ناراضی |
| عملیات‌ها و نگهداشت | رمزنگاری نامناسب، عدم توانمندی لازم، عدم اجرای مدیریت تغییر، عدم به‌روزرسانی/ پچ کردن، عدم حفاظت در مقابل تروجان، مدیریت نامناسب دسترسی سخت‌افزار و شبکه |
| محیط عملیات | امنیت فیزیکی، وابستگی‌ها، افراد شخص ثالث، دسترسی از راه دور |

ابعاد، مؤلفه‌ها و شاخص‌های تاب‌آوری سایبری سامانه‌های دفاعی در سه بعد اصلی، ۱۱ مولفه (جدول شماره ۲) و ۵۴ شاخص به شرح ذیل می‌باشد.

**جدول (۴) شاخص‌های تاب‌آوری سایبری سامانه‌های دفاعی**

| ردیف | شاخص‌های تاب‌آوری سایبری سامانه‌های دفاعی |
|---|---|
| ۱ | شناسایی و اولویت‌بندی تجهیزات و زیر سامانه‌ها براساس عملکرد |
| ۲ | تعیین وظایف و عملکرد تجهزات و زیر سامانه‌ها |
| ۳ | تعیین ارتباط زیر سامانه‌ها و تجهیزات با عملکردها |
| ۴ | تعیین سطح دسترسی به زیر سامانه |
| ۵ | دسته‌بندی بر اساس اطلاعات سامانه‌ها جهت حصول اطمینان و حفظ عملکرد اساسی |
| ۶ | اولویت‌بندی اقدامات پشتیبان عملیات اساسی سامانه |
| ۷ | تعیین و اولویت‌بندی اهداف کنترل برای زیر سامانه‌های مورد نیاز |
| ۸ | انجام کنترل برای اجرای حفاظت از شبکه و در صورت لزوم جداسازی شبکه |
| ۹ | کنترل برای حفاظت اطلاعات در وضعیت‌های مورد استفاده |
| ۱۰ | کنترل برای حفاظت اطلاعات در زمان وقوع حمله و نشت داده‌ها |
| ۱۱ | اجرا و کنترل شیوه‌های امنیت سایبری برای منابع انسانی مرتبط با سامانه |
| ۱۲ | تعیین و کنترل سطح دسترسی به سامانه‌ها و دارایی‌ها با ترکیب اصل کم‌ترین قابلیت |
| ۱۳ | تجزیه و تحلیل و رهگیری طرح‌های کنترل برای شناسایی شکاف‌های بازدارنده اهداف کنترل |
| ۱۴ | مخفی کردن دارایی‌های مهم و نمایش دارایی‌های فریبنده (فریب). |
| ۱۵ | استفاده از ناهمگونی برای به حداقل رساندن خرابی‌ها (تنوع). |
| ۱۶ | ارایه چندین مورد محافظت شده از منابع مهم (افزونگی). |
| ۱۷ | مشخص کردن وضعیت سلامت عملکرد کلیه عناصر حیاتی سیستم (یکپارچگی). |
| ۱۸ | ایجاد فرایند مدیریت ریسک با شناسایی، تحلیل و رفع خطرها |
| ۱۹ | شناسایی حد آستانه ریسک و تمرکز فعالیت‌های مدیریت ریسک |
| ۲۰ | تعیین پارامترهای تحمل ریسک برای هر حوزه تاثیرپذیر و تعیین آستانه تحمل‌پذیری |
| ۲۱ | تجریه و تحلیل ریسک‌ها و تعیین اقدام مناسب در برابر ریسک (پذیرش، انتقال، کاهش) |
| ۲۲ | ایجاد و حفظ روند شناسایی و تجزیه و تحلیل آسیب‌پذیری‌های نرم‌افزارها |
| ۲۳ | دسته‌بندی و اولویت‌بندی آسیب‌پذیری‌ها |
| ۲۴ | اقدامات لازم برای مواجهه با آسیب‌پذیری‌های شناسایی شده و کاهش اثرپذیری |
| ۲۵ | بررسی علل ریشه‌ای آسیب‌پذیری‌ها و ارزیابی نتایج کاهش آسیب‌پذیری‌ها |
| ۲۶ | ایجاد فرایند شناسایی، تحلیل، پاسخ گویی و یادگیری از حوادث |
| ۲۷ | شناسایی و مستندسازی حوادث و رخدادها شامل رویدادهای سایبری |
| ۲۸ | ثبت رخدادها در پایگاه داده و طبقه‌بندی، اولویت‌بندی و ردیابی حوادث |
| ۲۹ | ایجاد سامانه پاسخ‌گویی سریع به حوادث / حملات سایبری برای هر سامانه |
| ۳۰ | بررسی علت ریشه‌ای حوادث، رهگیری و تجزیه و تحلیل حوادث |
| ۳۱ | ایجاد روش ارتباطی بین فرآیند مدیریت رخدادها و سایر فرایندهای مرتبط |
| ۳۲ | توسعه برنامه‌های تداوم خدمات برای خدمات ارزشمند سامانه |
| ۳۳ | تعیین وظیفه نیروی انسانی برای اجرای برنامه‌های تداوم خدمات خاص |

| ردیف | شاخص‌های تاب‌آوری سایبری سامانه‌های دفاعی |
|---|---|
| ۳۴ | مستندسازی و در دسترس بودن برنامه‌های پیوستگی خدمات به صورت کنترل شده |
| ۳۵ | برنامه‌ریزی و بررسی برنامه‌های تداوم خدمات و بهبود حاصل شده |
| ۳۶ | شناسایی و مدیریت خطرات ناشی از وابستگی‌های خارجی |
| ۳۷ | اعمال الزامات تاب‌آوری به هر سامانه خارجی مرتبط با سرویس‌های اساسی سامانه |
| ۳۸ | نظارت بر عملکرد نهادهای خارجی مرتبط با سامانه |
| ۳۹ | برنامه‌ریزی برای استفاده از خدمات عمومی مرتبط با خدمات حیاتی در زمان بحران |
| ۴۰ | مستندسازی ارایه دهندگان زیرساخت خدمات حیاتی (خدمات مخابراتی منابع انرژی ) |
| ۴۱ | پیاده‌سازی فرایند مدیریت تغییر در سامانه‌ها |
| ۴۲ | ارزیابی اجرایی شدن الزامات تاب‌آوری در زمان انجام تغییرات در سامانه‌ها |
| ۴۳ | نظارت بر چرخه سامانه‌ها در جهت برنامه‌ریزی سامانه‌های پشتیبان در مواقع بحرانی |
| ۴۴ | نظارت مستمر بر انجام پیکربندی‌های به‌موقع برای سامانه‌های فناوری محور، نظیر نصب وصله‌های امنیتی در نرم افزارهای سیستم عامل سامانه‌های عملیاتی |
| ۴۵ | تدوین الزامات یکپارچگی تعیین کارکنان مجاز به انجام تغییر در دارایی‌های اطلاعاتی |
| ۴۶ | اجرای سامانه تعمیر و نگهداری پیش‌دستانه برای اطمینان از انجام به موقع تعمیر و نگهداری تجهیزات و سامانه‌ها |
| ۴۷ | نظارت و ارزیابی مستمر بر تعمیر و نگهداری‌های از راه دور |
| ۴۸ | احصای نیازمندی‌های آموزشی سایبری کارکنان مبتنی بر تغییرات فناوری |
| ۴۹ | اجرای مستمر دوره‌ای آموزشی سایبری و به‌روزآوری دانش سایبری کارکنان |
| ۵۰ | ارزیابی اثربخشی دوره‌های آموزشی سایبری در افزایش تاب‌آوری سایبری |
| ۵۱ | راه‌اندازی سامانه آگاهی وضعیتی تاب‌آوری سایبری |
| ۵۲ | تعیین مسئولیت نظارت بر منابع اطلاعات تهدید |
| ۵۳ | شناسایی، اولویت‌بندی و انتقال اطلاعات تهدید به ذینفعان داخلی |
| ۵۴ | شناسایی، اولویت‌بندی و انتقال اطلاعات تهدید به ذینفعان خارجی |

## پیشنهادها

### پیشنهادهای اجرایی

در راستای پیاده‌سازی نتایج این پژوهش و ارتقای تاب‌آوری سایبری سامانه‌های دفاعی پیشنهاد می‌گردد:

- معاونت ارتباطات و فناوری اطلاعات آجا با بهره‌گیری از دسته‌بندی تهدیدهای سایبری ارایه شده در این پژوهش نسبت به تدوین دستور العمل‌های امنیت سایبری اقدام نموده و با توجه به سرعت تغییرات در حوزه سایبری، دستور العمل‌های مذکور را به صورت دوره‌ای به‌روز رسانی نماید.
- معاونت‌های ارتباطات و فناوری اطلاعات نیروهای چهارگانه آجا با بهره‌گیری از الگوی ارایه شده در این پژوهش، دستور العمل تاب‌آوری سایبری جهت هر یک از سامانه‌های دفاعی را تدوین و در اختیار کاربران این سامانه‌ها قرار دهند.

- نیروهای چهارگانه آجا بر مبنای الگوی ارایه شده در این پژوهش، در قرارداد ساخت محصولات نوین دفاعی، نسبت به سنجش و ارزیابی تاب‌آوری سایبری محصولات دفاعی اقدام نمایند.

**پیشنهادهای پژوهشی**

تمرکز این پژوهش بر ارایه یک الگو جهت سامانه‌های دفاعی بوده است، اما لازم است هر یک از سامانه‌های دفاعی و نظامی کشور به‌طور ویژه در مقابل حوادث سایبری تاب‌آور شوند و پیشنهاد می‌گردد در حوزه‌های دفاعی ذیل پژوهش جامعی در خصوص تاب‌آوری در مقابله با تهدیدات و کاهش آسیب‌پذیری‌های سایبری انجام پذیرد.

- تاب‌آوری سامانه‌های موشکی در مقابله با تهدیدات سایبری
- تاب‌آوری سامانه‌های دریانوردی دفاعی در مقابله با تهدیدات سایبری
- تاب‌آوری سامانه‌های هوایی دفاعی در مقابله با تهدیدات سایبری
- تاب‌آوری سامانه‌های جنگ‌افزاری سایبر پایه در مقابله با تهدیدات سایبری

## قدردانی

از خبرگان توانمندی که در طول پژوهش، به محققان کمک کردند سپاس‌گزاریم.

## منابع


- بت شکن، بهمن. (۱۳۹۶). بررسی مهندسی تاب‌آوری سایبری در فضای سایبری، *سومین اجلاس ملی علوم و مهندسی رایانه و فناوری اطلاعات*، اصفهان: دانشگاه اصفهان، دانشکده مهندسی رایانه.
- سعادتی، رضا. (۱۴۰۰). *شناسایی و اولویت‌بندی عوامل موثر بر تاب‌آوری سایبری ارتش جمهوری اسلامی ایران*، پایان‌نامه کارشناسی ارشد، تهران: دافوس آجا.
- علاقه بند، علی. (۱۴۰۰). *مبانی نظری و اصول مدیریت آموزشی*، چاپ سی‌ام، تهران: نشر روان.
- مظفری، شهرام. ، پورمنصوری، رضوان. و پورمنصوری، جمال. (۲۰۱۹). احصاء شاخص‌های تاب‌آوری بر کاهش آسیب‌پذیری سیستم‌های کنترل صنعتی در تهدیدات سایبری، *چهارمین کنفرانس بین المللی تحقیقات حوزه اقتصاد و مدیریت*، فرانسه: پاریس.
- Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient systems. Computers & industrial engineering, 149, 106-829.
- Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, 147, 113-580.
- Benz, M., Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Bus. Horiz*. 2020, 63, 531–540.
- Bodeau, D., Graubart, R., Heinbockel, W. & Laderman, E. (2015). *Cyber Resiliency Engineering Aid Guidance on Applying Cyber Resiliency Techniques*, The MITRE Corporation.

- Carias, J. F., Borges, M. R. S., Labaka, L., Arrizabalaga, S., Hernantes, J. (2020). 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), (2019). *CIS Controls*, V 7. 1 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*, USA.
- Deutscher, S. A., Bohmayr, W., Asen, A. (2017). *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.
- Pinckard, J., Rattigan, M., & Vrtis, R. (2016). Mapping of the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT) to the Cyber Resilience Review (CRR).
- Gourisetti, S. N. G., Mix, S., Mylrea, M., Bonebrake, C., Touhiduzzaman, M. (2019). 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; pp. 1–9.
- *Internet Security Threat Report*; Symantec: Sunnyvale, CA, USA, (2019). Volume 24.
- Kott, A., Linkov, I. (2019). *Cyber Resilience of Systems and Networks*, Springer Science+Business Media New York.
- 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 Volume 2, Revision 1, 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. (2016). 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.
- Wei, D., & Ji, K. (2015). Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights. *3rd International Symposium on Resilient Control Systems (ISRCS)*, 2015.