Warfare Study Quarterly
https://www.qjws.ir/
Online ISSN: 2717-1760
Print ISSN: 2717-1760

Identifying and prioritizing predictive indicators in cyber resilience evaluation

Hamed Rafiani[1] | Davod Azar[2]✉ | Nima Farzamnia[3]

1. Department of Information Science, Faculty of Management, University of Tehran, Tehran, Iran. E-mail: rafiani.hamed@casu.ac.ir
2. Corresponding Author, Department of Information Science, Faculty of Management, University of Tehran, Tehran, Iran. E-mail: davodazar@yahoo.com
3. Department of Information Science, Faculty of Management, University of Tehran, Tehran, Iran. E-mail: nf@casu.ac.ir

Article Info

Article type:
Research Article

Article history:
Received
26 October 2024
Received in revised form
02 December 2024
Accepted
10 December 2024
Published online
20 December 2024

Keywords:
Cyber, cyberspace, assessment, resilience, prediction, evaluate.

ABSTRACT

Purpose: The primary objective of this research is to identify and prioritize predictive indicators for assessing cybersecurity resilience.

Methodology: This research employed a descriptive method with an applied approach and a mixed research design. Data was collected through a review of relevant literature and interviews with nine cybersecurity experts. Based on this data, a questionnaire was developed. The questionnaire's face and content validity were confirmed, and its reliability was verified with a Cronbach's alpha of 0.83. A sample of 100 cybersecurity commanders, managers, and experts was selected to distribute the questionnaire. Data was analyzed using SPSS and statistical methods.

Findings: After reviewing literature and conducting interviews with experts, three dimensions and eight components for assessing cybersecurity resilience with a focus on predicting cyberattacks were identified.

Conclusion: By identifying and prioritizing indicators and components for assessing cybersecurity resilience with a focus on predicting cyberattacks, it was concluded that machine learning algorithms can be used to detect anomalies, intrusion detection and response systems can leverage artificial intelligence, neural networks can be used to detect anomalies and identify cyber threats, cybersecurity regulations and guidelines, regular data backups, a cybersecurity risk management team, cybersecurity command and control centers, and regular execution of hypothetical attack scenarios can be beneficial.

Cite this article: Rafiani, H. , azar, D. and farzamnia, N. (2024). Identifying and prioritizing predictive indicators in cyber resilience evaluation. War Studies, 6(22), 25- 44.

DOI: 10.22034/qjws.2024.2037229.1247

Publisher: Command and Staff University

فصلنامه علمی مطالعات جنگ
https://www.qjws.ir/
شاپای چاپی: ۲۳۷۷-۱۷۴۰ شاپای الکترونیکی: ۲۷۱۷-۱۷۴۰
دانشگاه فرماندهی و ستاد آجا

شناسایی و اولویت‌بندی شاخص‌های پیش‌بینی در ارزیابی تاب‌آوری سایبری

حامد رفیعانی[۱] | داود آذر[۲] ✉ | نیما فرزام‌نیا [۳]

۱. گروه مطالعات علم و فناوری، دانشکده فرماندهی و ستاد، دانشگاه فرماندهی و ستاد، تهران، ایران، رایانامه: rafiani.hamed@casu.ac.ir

۲. نویسنده مسئول، گروه مطالعات علم و فناوری، دانشکده فرماندهی و ستاد، دانشگاه فرماندهی و ستاد، تهران، ایران، رایانامه: davodazar@yahoo.com

۳. گروه مطالعات علم و فناوری، دانشکده فرماندهی و ستاد، دانشگاه فرماندهی و ستاد، تهران، ایران، رایانامه: nf@casu.ac.ir

اطلاعات مقاله

نوع مقاله:
پژوهشی

تاریخ دریافت:
۱۴۰۳/۰۸/۰۵

تاریخ بازنگری:
۱۴۰۳/۰۹/۱۲

تاریخ پذیرش:
۱۴۰۳/۰۹/۲۰

تاریخ انتشار:
۱۴۰۳/۰۹/۳۰

کلیدواژه‌ها:
سایبر، فضای سایبری، ارزیابی، تاب‌آوری، پیش‌بینی.

چکیده

هدف: هدف از این پژوهش شناسایی و اولویت‌بندی شاخص‌های پیش‌بینی در ارزیابی تاب‌آوری سایبری است.

روش: پژوهش حاضر با روش توصیفی صورت پذیرفته و از نوع کاربردی و رویکرد تحقیق نیز آمیخته است. داده‌های موردنظر به‌صورت مطالعه اسناد و مدارک معتبر و مصاحبه با ۹ نفر از صاحب‌نظران حوزهٔ تحقیق، جمع‌آوری و بر اساس آن‌ها نیز پرسشنامه تدوین شده است. روایی پرسشنامه به روش ظاهری/محتوایی و پایایی آن با ضریب آلفای کرون باخ ۰/۸۳ تأیید شد و بین حجم نمونه که تعداد ۱۰۰ نفر از فرماندهان، رؤسا و مدیران و کارشناسان سایبری و نیز افسران عملیاتی در سطح اجرایی و ستادی تقسیم شد که با خصوصیات و ویژگی‌های مأموریت‌های سایبری آشنایی داشته‌اند. داده‌های پژوهش با استفاده از نرم‌افزار SPSS و روش‌های آماری مورد تجزیه‌وتحلیل قرار گرفتند.

یافته‌ها: در این تحقیق، پس از مطالعهٔ منابع و مصاحبه با صاحب‌نظران ۳ بُعد و ۸ مؤلفه برای ارزیابی تاب‌آوری سایبری با پیش‌بینی حملات سایبری احصاء شد.

نتیجه‌گیری: با شناسایی و اولویت‌بندی شاخص‌ها و مؤلفه‌های ارزیابی تاب‌آوری سایبری با رویکرد پیش‌بینی حملات سایبری این‌گونه نتیجه‌گیری شد که از الگوریتم‌های یادگیری ماشین برای تشخیص الگوهای غیرعادی، سیستم‌های تشخیص نفوذ و پاسخ به نفوذ با بهره‌گیری از هوش مصنوعی، شبکه‌های عصبی برای تشخیص الگوهای غیرعادی و شناسایی تهدیدات سایبری، بخشنامه‌ها و آیین‌نامه‌های سایبری، پشتیبان‌گیری منظم از داده‌ها، وجود تیم مدیریت ریسک سایبری، ایجاد مراکز فرماندهی و کنترل سایبری و اجرای منظم سناریوهای حملات فرضی بهره برد.

استناد: رفیعانی، حامد؛ آذر، داود و فرزام‌نیا، نیما. (۱۴۰۳). شناسایی و اولویت‌بندی شاخص‌های پیش‌بینی در ارزیابی تاب‌آوری سایبری. فصلنامه مطالعات جنگ، ۶(۲۲)، ۲۵- ۴۴.

DOI: 10.22034/qjws.2024.2037229.1247

ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

مقدمه

در دهه‌های اخیر، با پیشرفت فراگیر فناوری اطلاعات و ارتباطات، جوامع جهانی با چالش‌ها و تهدیدهای بی‌شمار در زمینه سایبری روبه‌رو شده‌اند. حمله‌های سایبری که ممکن است از نقض حریم خصوصی تا تخریب سامانه‌های اطلاعاتی یک سازمان را شامل شود، این روند را به چالشی پیچیده تبدیل کرده‌اند. در این شرایط، تاب‌آوری سایبری به‌عنوان مفهومی اساسی در حفظ امنیت دیجیتال و استمرار فعالیت‌ها نقش بسزایی ایفا می‌کند. (رفیعانی، ۱۳۹۶: ۸). امروزه اهمیت تاب‌آوری سایبری نه‌تنها در امنیت اطلاعات بلکه در پایداری و ادامه فعالیت‌های تجاری نیز بیش‌ازپیش حائز اهمیت است. تاب‌آوری سایبری از دیدگاهی به‌عنوان یک راهبرد فراتر از محافل فنّاورانه، به مدیران امنیت و مدیران عالی سازمان‌ها چالش‌های جدیدی را ارائه می‌دهد. تاب‌آوری سایبری به‌عنوان یک ستون اساسی در ساختار امنیت دیجیتال مطرح می‌شود (ولوی، ۱۳۹۷: ۲۴). این مفهوم که به‌اصطلاح به معنای توانایی سازمان‌ها برای مقابله با تهدیدهای سایبری، بازیابی سریع از حملات و حفظ استمرار فعالیت‌هاست، به‌ویژه در مقابله با حمله‌های پیچیده و پیشرفته نظیر نفوذهای مداوم و حملات ناشناخته، اهمیت خاصی پیداکرده است (ولوی، ۱۳۹۷: ۲۵). تاب‌آوری سایبری به معنای توانمندی سازمان در مقابله با حملات سایبری، بازیابی سریع از خسارات و ادامه فعالیت‌ها در شرایط پساحمله است. این تعریف ابعاد گسترده‌ای از تاب‌آوری را شامل می‌شود. خسارت ناشی از حملات سایبری ممکن است به یک سازمان آسیب جبران‌ناپذیر وارد کند، اما با انجام ارزیابی تاب‌آوری سایبری، سازمان می‌تواند بهترین راهکارهای سایبری را شناسایی کرده و مقاومت خود را در برابر این تهدیدات افزایش دهد. ارزیابی تاب‌آوری سایبری، میزان امنیت اطلاعات در سازمان را ارتقاء می‌دهد (فردریک بیجورک، ۲۰۲۲: ۱۶).

صحنهٔ نبرد سایبری در حملات منع خدمت‌رسانی توزیع‌شده دارای دو بازیگر مهاجم و مدافع (قربانی) است که مهاجم با گسیل بسته‌های پی‌درپی و تغییر روش‌های خود درصدد قطع یا کاهش خدمت‌رسانی قربانی است و قربانی با انجام انواع تمهیدات امنیتی درصدد دفاع بوده و اصرار بر خدمت‌رسانی به ذینفعان خود دارد. ارزیابی این صحنه از منظر یک ناظر می‌تواند دارای ابهام باشد به‌طوری‌که قادر باشد ادامهٔ این صحنه را پیش‌بینی کند (اکبری، ۱۳۹۸: ۱۱). درصورتی‌که حمله سایبری از قدرت زیادی برخوردار باشد و موجب هرگونه اختلال در سامانه‌ها گردد نیاز به ترمیم سریع و حاضر به کاری سامانه‌ها نمود پیدا خواهد کرد که این موارد

زنجیروار به دنبال هم باعث می‌شود یک مجموعه از تاب‌آوری سایبری برخوردار شود (آذر، قدرت سایبری، ۱۴۰۱).

امروزه سایبر به‌عنوان یک عرصه قدرت در کلیه ارتش‌های جهان مطرح‌شده است و با توجه به گستردگی آن در تمامی بخش‌ها ازنظر امنیتی یکی از مهم‌ترین بخش‌ها به شمار می‌رود. نیروهای مسلح ایران نیز از این امر دور نبوده و در سال‌های اخیر به فضای سایبر اهمیت بسیاری نشان داده‌اند. ارتش جمهوری اسلامی ایران به‌عنوان بخشی از نیروی مسلح به مسئله سایبر توجه ویژه داشته و از این فضا به‌خوبی استفاده می‌کند. با موارد مطروحه احتمال هرگونه نفوذ و یا حمله به ارتش از طریق فضای سایبری وجود خواهد داشت که میزان تاب‌آوری سامانه‌ها و تجهیزات در مواجهه با این تهدیدات از اهمیت بالایی برخوردار است. ازاین‌رو سؤال اصلی این مقاله این است که شناسایی و اولویت‌بندی شاخص‌های پیش‌بینی در ارزیابی تاب‌آوری سایبری چگونه است؟

این مقاله برای گذر از مسائل موجود در حوزهٔ نحوه پیش‌بینی حملات سایبری به دنبال کشف راه‌حل‌های بدیع و اعتبارسنجی آن‌ها در مقام عمل بوده و در یک فرایند علمی سعی در پاسخگویی به آن را دارد و در صورت غفلت از چنین فناوری‌هایی میدان عمل نیروهای نظامی و به‌خصوص ارتش مزیت‌های رقابتی خود را از دست داده و مشکلات و نارسایی‌هایی در خصوص فضای سایبر ظهور خواهد کرد.

مبانی نظری و پیشینه‌های پژوهش

مبانی نظری

سایبر

واژهٔ سایبر از لغت یونانی کایبرنتس به معنی سکان‌دار یا راهنما مشتق شده است. در واقع به هر آنچه مرتبط با فعالیت‌های رایانه‌ای و مجازی باشد، اطلاق می‌گردد. به‌عبارتی‌دیگر، به دامنهٔ جهانی در محیط اطلاعاتی گفته می‌شود که متشکل از شبکه‌های وابسته به زیرساخت‌های فناوری اطلاعات از جمله اینترنت، شبکه‌های ارتباطی، دستگاه‌های رایانه‌ای و کنترل‌کننده‌ها و پردازشگرهای جاسازی‌شده است. (قاسمی و همکاران، ۱۴۰۱: ۱۲)

امنیت سایبری

به اقدامات انجام‌شده در فضای سایبری محافظت‌شده برای جلوگیری از دسترسی غیرمجاز، بهره‌برداری یا آسیب به رایانه‌ها، سیستم‌های ارتباطات الکترونیکی و سایر فناوری‌های

اطلاعاتی، از جمله فناوری اطلاعات پلتفرم و همچنین اطلاعات موجود در آن برای اطمینان از در دسترس بودن، یکپارچگی، احراز هویت، محرمانه بودن و عدم انکار گفته می‌شود (وزارت دفاع ایالات‌متحده ۲۰۲۱: ۵۵).

فضای سایبر

فضای سایبر حوزه‌ای سراسری در محیط اطلاعاتی است که دربرگیرندهٔ شبکه‌های به‌هم‌پیوسته زیرساخت‌های فناوری اطلاعات است و اطلاعات موجود در آن شامل اینترنت، شبکه‌های مخابراتی، سامانه‌های رایانه‌ای و پردازنده‌ها و کنترل‌کننده‌های تعبیه‌شده در آن‌ها می‌شود. (اف ام ۳-۱۲ ارتش آمریکا، ۲۰۱۷: ۲)

پیش‌بینی سایبری

حس تشخیص، توانایی سازمان‌ها برای پیش‌بینی و تشخیص تهدیدات سایبری است. سازمان‌ها به استفاده از هوش تهدید سایبری و دفاع فعال برای پیش‌بینی تهدیدات یا حملات پیش رو نیاز دارند. قبل از موفق شدن حملات، آن‌ها به دانستن آنچه اتفاق می‌افتد، نیاز دارند و همچنین آن‌ها نیاز به تجزیه‌وتحلیل‌های پیچیده برای دستیابی زودهنگام به هشدارهای سایبری دارند. باتوجه‌به ماهیت فضای سایبر که امکان پیش‌بینی بسیط و خطی از تهدیدات آینده را تقریباً غیرممکن کرده، احتمال غافلگیری کنشگران منفعل و محافظه‌کار در مقابل تهدیدات آتی بسیار بالا ارزیابی می‌شود. در این شرایط، مقابله با تهدیدات پیشرو و استفاده از فرصت‌های احتمالی، نیازمند ایجاد آمادگی نرم‌افزاری و سخت‌افزاری برای مقابله با چالش‌های آتی است (ولوی، ۱۳۹۷: ۲۷).

چیزی که در سیستم‌های خودمختار توصیف می‌شود، احتمالات است و ناظران انسانی نمی‌توانند همهٔ رویدادها و حوادث را با فعال‌شدن سیستم، پیش‌بینی کنند. داده‌های ارائه‌شده به یک سیستم، در رفتار آن سیستم تأثیر زیادی دارد و به همین دلیل است که همیشه در حال تولید داده‌ها و اطلاعات جدید در فضای سایبری هستیم؛ لذا نمی‌توان پیش‌بینی آینده را در خصوص ورودی‌های سیستم انجام داد و اقدامات لازم را برای همه ترکیبات احتمالی داده‌ها آماده یا پیش‌بینی کرد.

به‌طورکلی، پیش‌بینی رفتار دقیق سیستم‌هایی که از یادگیری ماشین استفاده می‌کنند، بسیار دشوار است. علاوه بر این، وقتی به خودمختاری به معنای قوی‌تر و هوش مصنوعی فکر می‌کنیم

مانند اینکه بتوانیم به‌طور کامل یک متخصص انسانی را در سیستم جایگزین کنیم، باید تصدیق کنیم که چنین سیستم‌هایی تاکنون وجود نداشته و به‌احتمال‌زیاد دستیابی به سیستم‌های دفاع یا حملات خودگردان سایبری کاملاً مستقل از متخصص انسانی، دشوار است. برای سطح پایین‌تری از خودمختاری، مشاهده می‌کنیم با وجود اینکه همواره ابزارها با بهره‌گیری از هوش مصنوعی در حال تغییر و پیشرفت هستند، هنوز برای استفادهٔ گسترده به کیفیت و بلوغ نرسیده‌اند (تامت‌تانل، ۲۰۲۱: ۳۷-۳۹).

انتظار می‌رود که تاب‌آوری سایبری با افزایش غیرخطی هوش ماشینی در طول زمان، پیچیده‌تر شود. همچنین محاسبات کوانتومی و روش‌های یادگیری ماشین می‌توانند تأثیرات بزرگ‌تری داشته باشند. برای مثال، قابلیت‌های یادگیری ماشینی می‌توانند اقدامات دشمن را زودتر پیش‌بینی کنند تا اقدامات پیشگیرانه نیمه یا کاملاً خودکار را انجام دهند (توماس لانسو، ۲۰۲۱: ۳۳۲).

ساده‌ترین و رایج‌ترین فناوری هوش مصنوعی که در پدافند سایبری استفاده می‌شود، تشخیص بیرونی یا ناهنجاری است. ازآنجاکه تجزیه‌وتحلیل علل، تلاش زیادی می‌طلبد، مشکلی که اغلب رخ می‌دهد این است که در صورت تشخیص حملهٔ بیرونی عکس‌العمل صحیح قابل‌تشخیص نیست (پییر پارند و همکاران، ۲۰۱۸: ۴-۲).

یکی از این سیستم‌های تشخیص نفوذهای نصب‌شده، ممکن است میلیون‌ها هشدار در روز ایجاد کند. تحلیلگر انسانی قادر است تعداد کمی از هشدارها را بررسی کند. تحقیقات فعلی نشان می‌دهد سیستمی که از یک منبع انسانی بهره می‌جوید، نیاز به به‌روز کردن منظم دارد؛ بنابراین سیستم یادگیری به‌طور بالقوه حجم کار تحلیلگر را کاهش می‌دهد. با توجه به پیچیدگی‌هایی که وجود دارد، چنین سیستم‌های یادگیری به علت تحقیقاتی بودن و عملیاتی نشدن، به‌طور گسترده و کاربردی در سیستم‌های دفاع سایبری استفاده نمی‌شوند. تحقیقات نشان می‌دهد که برای این کار خاص، سیستم‌های یادگیری مبتنی بر درخت تصمیم‌گیری بهتر از شبکه‌های عصبی عمل می‌کنند (جیوانی آپروزس و همکاران، ۲۰۱۸: ۳۷۷-۳۷۱).

هوش مصنوعی با استفاده از الگوریتم‌های پیشرفتهٔ یادگیری ماشین و تحلیل داده‌های بزرگ، می‌تواند الگوهای پیچیده تهدیدات سایبری را شناسایی کرده و حملات احتمالی را پیش‌بینی کند. این تکنیک‌ها شامل تحلیل رفتارهای غیرعادی، شناسایی ناهنجاری‌ها و پیش‌بینی نقاط ضعف بالقوه در سیستم‌های امنیتی هستند. در این فرایند چالش‌هایی مانند نیاز به داده‌های باکیفیت، پیچیدگی الگوریتم‌ها و مسائل مربوط به حفظ حریم خصوصی و امنیت داده‌ها وجود

دارد اما محققان به این نتیجه رسیده‌اند که با غلبه بر این چالش‌ها، هوش مصنوعی می‌تواند به‌طور قابل‌توجهی قابلیت پیش‌بینی و واکنش سریع‌تر به تهدیدات سایبری را بهبود بخشد و درنتیجه تاب‌آوری سایبری سازمان‌ها را افزایش دهد (جان دا، ۲۰۲۱: ۱۸-۱۱).

در حوزه تاب‌آوری سایبری، استفاده از مدل‌های پیش‌بینی مبتنی بر پایگاه داده نقشی محوری در شناسایی تهدیدات و آسیب‌پذیری‌های احتمالی پیش از بهره‌برداری از آن‌ها ایفا می‌کند. با بهره‌گیری از مقادیر عظیم داده‌های تاریخی، این مدل‌ها قادر به تشخیص الگوها و ناهنجاری‌هایی هستند که ممکن است نشان‌دهندهٔ یک حمله سایبری قریب‌الوقوع باشند. این رویکرد مبتنی بر داده به سازمان‌ها اجازه می‌دهد که به‌طور مؤثرتری ریسک‌ها را پیش‌بینی و کاهش دهند و اطمینان حاصل کنند که استراتژی‌های امنیت سایبری آن‌ها به‌صورت پیش‌دستانه عمل می‌کند. علاوه بر این، ادغام تحلیل‌های پیشرفته و الگوریتم‌های یادگیری ماشین دقت و قابلیت اطمینان این مدل‌های پیش‌بینی را بهبود می‌بخشد و یک چارچوب قوی برای نظارت مداوم و دفاع در برابر تهدیدات سایبری فراهم می‌آورد (تامپسون، ۲۰۲۱: ۵۶-۵۹).

سیستم‌های خودگردان با استفاده از الگوریتم‌های هوش مصنوعی و یادگیری ماشین قادر به شناسایی الگوها و تهدیدات ناشناخته هستند که می‌توانند پیش از وقوع حملات، اقدامات پیشگیرانه انجام دهند. تکنیک‌های مختلفی مانند تحلیل پیش‌بینی، یادگیری نظارت‌شده و یادگیری تقویتی وجود دارد که به سیستم‌های خودگردان اجازه می‌دهد به‌طور مداوم محیط سایبری را پایش کرده و بهبود یابند. نتیجه حاکی از آن است که سیستم‌های خودگردان با ارائه پیش‌بینی‌های دقیق و واکنش‌های سریع، می‌توانند به‌طور قابل‌توجهی تاب‌آوری سایبری سازمان‌ها را افزایش دهند و از خسارات ناشی از حملات سایبری جلوگیری کنند (آدامز، ۲۰۲۱: ۲۱-۳۷).

پیشینه‌های پژوهش

سعادتی، رضا (۱۴۰۱) در تحقیق خود با عنوان «شناسایی و اولویت‌بندی عوامل مؤثر بر تاب‌آوری سایبری ارتش جمهوری اسلامی ایران» عوامل مؤثر بر تاب‌آوری سایبری را شناسایی کرده و به این نتیجه رسیده است که پیش‌بینی نوع حمله، تشخیص به‌موقع، آموزش مستمر کارکنان، عملکرد کارکنان مراکز امنیت و دفاع سایبری، بسترهای ارتباط جایگزین، زیرمؤلفه‌های پشتیبان‌گیری صحیح و قابل‌اطمینان، مدیریت نیروی انسانی، ارتقای فرهنگ سایبری، رمزگذاری داده‌ها، مدیریت وصله‌ها، تجهیزات امنیتی بومی، رعایت فن افزونگی،

مسدود کردن پورت‌ها، حفظ یکپارچگی داده‌ها و ایجاد ساختار ابری از عوامل مؤثر بر تاب‌آوری سایبری هستند.

کشاورز، رضا (۱۴۰۰) در تحقیق خود با عنوان «ارائهٔ مدل پیشنهادی CERT سازمان‌های دفاعی به‌منظور کاهش تهدیدات سایبری» به تبیین مفاهیم، مدل‌ها، سرویس‌ها و خدمات و دیگر مؤلفه‌ها و موارد اثرگذار در CERT موردبررسی قرارگرفته و نتایج مقاله بیانگر موارد ذیل است:

جهت جلوگیری از نفوذ و حمله سایبری در سطح و واکنش به‌موقع به آن موارد زیر بایستی موردتوجه قرار گیرد:

الف- پیش‌بینی نسبت به حملات احتمالی و دفع آن پیش از وقوع،

ب- ارتقاء زیرساخت سایبری و افزایش امنیت شبکه،

ج- جلب نظر فرماندهان و تصمیم‌گیران در خصوص اهمیت، ضرورت و نیاز به راه‌اندازی **CERT** خصوصاً در مراکز نظامی.

قاسمی، محمد (۱۴۰۱) در تحقیق خود با عنوان «چگونگی ارزیابی قدرت سایبری ارتش جمهوری اسلامی ایران» به این نتیجه رسید که با بررسی حوزهٔ آفند سایبری، پدافند سایبری و تاب‌آوری سایبری می‌توان قدرت سایبری را مورد تجزیه‌وتحلیل قرار داد و از نتایج هر بخش می‌توان به مواردی همچون دانش نیروی انسانی، رصد مستمر فناوری‌های نوین، یکپارچه‌سازی و ادغام اطلاعات سایبری، مهارت و تخصص نیروی انسانی، هدایت و کنترل، مبهم‌سازی حمله، استفاده از فناوری‌های جدید، متناسب با تهدید بودن تجهیزات، فرهنگ‌سازی سایبری، طراحی اهداف جعلی، فرماندهی یکپارچه هوشمند بحران، استفاده از هوش مصنوعی، توسعهٔ هم‌زمان در سه حوزهٔ تمهیدات انسانی فنی و فرایندها اشاره کرد (قاسمی، ۱۴۰۱).

علی‌محمدی، سجاد و همکاران (۱۴۰۳) در تحقیق خود با عنوان «ارائه سیستم تشخیص نفوذ در اینترنت اشیاء صنعتی با استفاده از الگوریتم گرگ خاکستری»، اهمیت استفاده از الگوریتم‌های پیشرفته در بهبود عملکرد سیستم‌های **IDS** را موردبررسی قرار داده‌اند و تأثیر آن‌ها بر دقت و کارایی شناسایی تهدیدات نشان داده شده است. به‌ویژه سیستم‌های **IDS** می‌توانند با استفاده از روش‌هایی مانند الگوریتم گرگ خاکستری به بهینه‌سازی فرایند استخراج ویژگی‌ها و کاهش نرخ خطا بپردازند (منبع مقاله). نتایج این تحقیق نشان می‌دهد که به‌کارگیری این تکنیک‌ها می‌تواند باعث افزایش دقت در شناسایی حملات و در نتیجه بهبود تاب‌آوری سایبری سیستم‌ها شود. به‌طور خاص، با توسعهٔ سیستم‌های **IDS** مبتنی بر

یادگیری ماشین، سامانه‌ها قادر خواهند بود تا ضمن شناسایی سریع و مؤثر تهدیدات، بهبود عملکرد و کاهش زمان پاسخ به حملات را نیز به همراه داشته باشند. این امر در نهایت به تسهیل بازگشت به حالت عادی و کاهش خسارات ناشی از حملات سایبری منجر خواهد شد (علی‌محمدی، سجاد؛ فتحی، محمد. ۱۴۰۳).

روش‌شناسی پژوهش

پژوهش حاضر در پی شناسایی و اولویت‌بندی شاخص‌های پیش‌بینی ارزیابی تاب‌آوری سایبری با استفاده از روش توصیفی است و نوع آن کاربردی و رویکرد آن نیز آمیخته است. برای جمع‌آوری داده‌ها از دو روش مطالعات کتابخانه‌ای (مطالعه اسناد و مدارک) و میدانی (پرسشنامه) استفاده‌شده و تجزیه‌وتحلیل آن نیز به‌صورت آمیخته صورت پذیرفته است. جامعهٔ آماری در این تحقیق ۱۳۵ نفر از فرماندهان، رؤسا و کارشناسان سایبری در ارتش جمهوری اسلامی ایران در نظر گرفته شده که با خصوصیات و ویژگی‌های مأموریت سایبری آشنایی داشته و دارای مدرک کارشناسی ارشد و بالاتر هستند. حجم نمونه بر اساس فرمول کوکران تعداد ۱۰۰ نفر محاسبه شده که به‌صورت جدول زیر، پرسشنامه بین ایشان توزیع گردیده است.

جدول (۱) جامعه آماری تحقیق

طبقات جامعه آماری	جامعه آماری (N)	جامعه نمونه (n)
کارکنان ستادی	۵۵	۴۰
کارکنان آموزشی	۳۵	۲۶
کارکنان اجرایی	۴۵	۳۴
مجموع	۱۳۵	۱۰۰

در این تحقیق در ابتدا با تجزیه‌وتحلیل کیفی اسناد و مدارک و منابع موردمطالعه و مصاحبه‌های انجام‌شده با خبرگان، مؤلفه‌های پژوهش استخراج و بر این اساس پرسشنامه تهیه شد و در بین نمونه آماری توزیع گردید و نتایج حاصل از آن با استفاده از نرم‌افزار SPSS و روش‌های آماری مورد تجزیه‌وتحلیل کمّی قرار گرفت و درنهایت با در نظر گرفتن نتایج در تجزیه‌وتحلیل‌های کیفی و کمی، تجزیه‌وتحلیل آمیخته به انجام رسید.

به‌منظور بررسی روایی اسناد و مدارک، از اسناد بالادستی و مدارک معتبر به‌روز و مرتبط با موضوع که کاربردی هستند، در جریان پژوهش استفاده شده است.

جهت بررسی روایی مصاحبه پژوهش، صاحب‌نظران انتخاب‌شده از متخصصین آگاه در حوزهٔ سایبری هستند که به موضوع تحقیق آشنایی کامل دارند؛ سؤال‌ها به‌گونه‌ای طراحی شده‌اند که تمام ابعاد موضوع را پوشش دهند و محقق را در دستیابی به اهداف تحقیق یاری رسانند. در زمینهٔ بررسی روایی پرسش‌نامه، پس از تهیه پرسش‌نامه مورد قضاوت افراد مطلع و آگاه و صاحب‌نظر در موضوع تحقیق قرار گرفت و نظرات و نکات موردنظر آنان در پرسش‌نامه اعمال شد.

پایایی مصاحبه پژوهش از روش دلفی و با ارائه سؤالات مصاحبه به گروهی از صاحب‌نظران و اخذ نظر آنان در زمان‌های متفاوت و مقایسهٔ پاسخ‌های ارائه‌شده به‌منظور سنجش روایی سؤالات مصاحبه استفاده شد. برای سنجش پایایی اسناد و مدارک نیز از اسناد و مدارک معتبر موجود در کتابخانه‌ها و مقاله‌های علمی از سایت‌های اینترنتی معتبر استفاده شد. همچنین با استفاده از منابع متعدد پر ارجاع بر میزان اعتبار منابع افزوده شد و برای اطمینان از اعتبار منابع، نظرات متخصصین موضوع و اساتید محترم مورداستفاده قرار گرفت.

پایایی پرسش‌نامه تحقیق نیز با توجه به اینکه اطلاعات کمی با استفاده از طیف لیکرت جمع‌آوری شده‌اند؛ بنابراین از آلفای کرونباخ برای بررسی پایایی پرسش‌نامه استفاده شد و نتیجه آن برابر جدول زیر به‌دست آمد که نشان می‌دهد پرسش‌نامه از پایایی لازم برخوردار است.

جدول (۲) محاسبه پایایی

پایایی پرسش‌نامه		
بعد	تعداد سؤالات	آلفای کرونباخ
سؤالات پیش‌بینی سایبری	۸	۰.۸۳۱

تجزیه‌وتحلیل داده‌ها

در تجزیه‌وتحلیل کیفی بر اساس تلخیص اطلاعات از اسناد و مدارک، صاحب‌نظران و پردازش اطلاعات جمع‌آوری‌شده، مؤلفه‌های پیش‌بینی در ارزیابی تاب‌آوری سایبری به شرح زیر شناسایی شد.

- استفاده از هوش مصنوعی در پیش‌بینی حملات سایبری،
- به‌روز کردن بانک اطلاعاتی،
- استفاده از سیستم خودگردان.

بر همین اساس مؤلفه‌ها و شاخص‌های احصاء شده در جدول زیر آورده شده است:

جدول (۳) مؤلفه‌ها و شاخص‌های حاصل از فرایند تجزیه‌وتحلیل کیفی

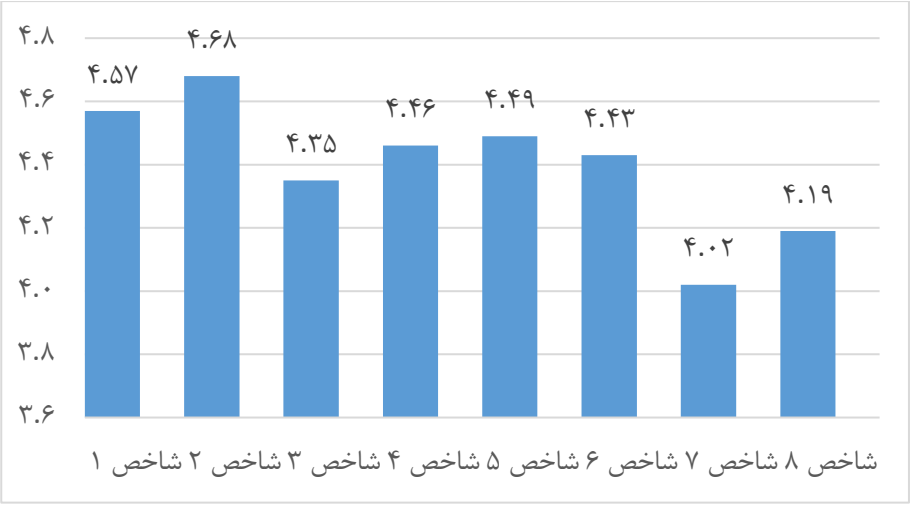
ردیف	مؤلفه	شاخص‌ها
۱	استفاده از هوش مصنوعی	نحوهٔ استفاده از الگوریتم‌های یادگیری ماشین، نحوهٔ استفاده از سیستم‌های تشخیص نفوذ و پاسخ به نفوذ، نحوهٔ استفاده از شبکه‌های عصبی برای تشخیص الگوهای غیرعادی
۲	به‌روز کردن بانک اطلاعاتی	وجود بخشنامه‌ها، دستورالعمل‌ها و آیین‌نامه‌های سایبری رده‌بالا، نحوهٔ پشتیبان‌گیری از داده‌ها
۳	استفاده از سیستم خودگردان	وجود تیم مدیریت ریسک سایبری، نحوهٔ ایجاد مراکز فرماندهی و کنترل سایبری، اجرای منظم سناریوهای حملات فرضی

نتیجه به‌دست‌آمده از تجزیه‌وتحلیل پاسخ جامعهٔ نمونه به پرسشنامه که شامل ۸ سؤال بود، به شرح زیر است:

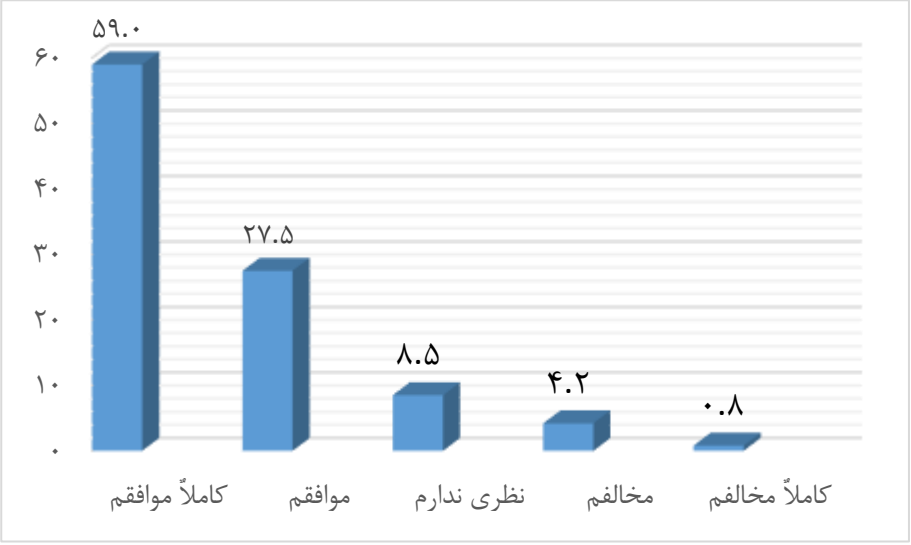
جدول (۴) فراوانی سؤالات پرسشنامه

مؤلفه	شاخص‌ها	کاملاً موافقم	موافقم	نظری ندارم	مخالفم	کاملاً مخالفم	میانگین

استفاده از هوش مصنوعی	با استفاده از الگوریتم‌های یادگیری ماشین برای تشخیص الگوهای غیرعادی و شناسایی تهدیدات سایبری، می‌توان تاب‌آوری سایبری را ارزیابی کرد.	۶۸	۲۳	۷	۲	۰	۴/۵۷
	با استفاده از سیستم‌های تشخیص نفوذ و پاسخ به نفوذ که از هوش مصنوعی بهره می‌گیرند، می‌توان تاب‌آوری سایبری را ارزیابی نمود.	۷۶	۱۸	۴	۲	۰	۴/۶۸
	با استفاده از شبکه‌های عصبی برای تشخیص الگوهای غیرعادی، می‌توان تاب‌آوری سایبری را ارزیابی کرد.	۶۱	۲۱	۱۰	۸	۰	۴/۳۵
به‌روز کردن بانک اطلاعاتی	با استفاده از بخشنامه‌ها، دستورالعمل‌ها و آیین‌نامه‌های سایبری رده‌بالا، می‌توان تاب‌آوری سایبری را ارزیابی کرد.	۵۹	۳۱	۷	۳	۰	۴/۴۶
	با پشتیبان‌گیری منظم می‌توان تاب‌آوری سایبری را ارزیابی کرد.	۶۸	۱۹	۸	۴	۱	۴/۴۹
استفاده از سیستم خودگردان	با استفاده از تیم مدیریت ریسک سایبری، می‌توان تاب‌آوری سایبری را ارزیابی کرد.	۵۹	۲۸	۱۰	۳	۰	۴/۴۳
	با ایجاد مراکز فرماندهی و کنترل سایبری، می‌توان تاب‌آوری سایبری را ارزیابی کرد.	۳۸	۴۱	۱۰	۷	۴	۴/۰۲
	با اجرای منظم سناریوهای حملات فرضی به‌منظور بررسی واکنش سیستم خودگردان، می‌توان تاب‌آوری سایبری را ارزیابی کرد.	۴۳	۳۹	۱۳	۴	۱	۴/۱۹
میانگین		۵۹	۲۷/۵	۸/۵	۴/۲	۰/۸	۴/۴
فراوانی		۴۷۲	۲۲۰	۶۹	۳۳	۶	
درصد فراوانی		۴۷/۲	۲۲	۶/۹	۳/۳	۶/۰	



نمودار (۱) میانگین پاسخ‌گویی به شاخص‌ها



نمودار (۲) درصد فراوانی میانگین مؤلفه‌های پیش‌بینی در ارزیابی تاب‌آوری سایبری

نتایج در جدول و نمودارهای بالا نشان‌دهندهٔ آن است که به‌طور متوسط از تعداد ۱۰۰ نفر نمونهٔ آماری، تعداد ۵۹ نفر (۵۹ درصد) گزینهٔ کاملاً موافقم، تعداد ۲۷/۵ نفر (۲۷/۵ درصد) گزینهٔ موافقم، تعداد ۸/۵ نفر (۸/۵ درصد) گزینهٔ نظری ندارم، تعداد ۴/۲ نفر (۴/۲ درصد)

گزینهٔ مخالفم و تعداد ۰/۸ نفر (۰/۸ درصد) گزینهٔ کاملاً مخالفم را انتخاب کرده‌اند. میانگین پاسخ‌های پاسخ‌دهندگان به این شاخص‌ها برابر با ۴/۴ است.

تجزیه‌وتحلیل استنباطی

الف) آزمون فرضیه

گام اول- تعریف فرضیه‌های پژوهشی H_0 و H_1 (فرض‌ها)

در این پژوهش، بررسی تصادفی نبودن پاسخ‌های نمونه آماری با آزمون کای- مربع (خی دو) انجام شده است؛ زیرا این آزمون برای بررسی دو متغیر که حداقل یکی از آن‌ها کیفی است، استفاده می‌شود و در آن فراوانی‌های مشاهده شده با فراوانی‌های مورد انتظار استقلال دو متغیر مقایسه می‌شوند. در ادامه تصادفی نبودن پاسخ‌های نمونهٔ آماری فرضیه‌های تحقیق را مورد آزمون قرار می‌دهیم.

فرضیه اول

گام اول- تعریف فرضیه‌های پژوهشی H_0 و H_1 (فرض‌ها)

نقیض ادعا (H_0): به نظر می‌رسد با استفاده از هوش مصنوعی نمی‌توان ارزیابی لازم را برای پیش‌بینی حملات سایبری در حوزهٔ تاب‌آوری سایبری انجام داد.

ادعا (H_1): به نظر می‌رسد با استفاده از هوش مصنوعی می‌توان ارزیابی لازم را برای پیش‌بینی حملات سایبری در حوزهٔ تاب‌آوری سایبری انجام داد.

گام دوم- آمارهٔ آزمون

آزمون استقلال خی - دو فرضیه اول در سطح اطمینان ۹۵٪ انجام شده است. برای این منظور از نرم‌افزار SPSS استفاده شده است که نتیجه آن به شرح زیر است:

در فرمول کای مربع داریم:

$$\chi^2 = \sum_{i=1}^{k} \frac{(fo_i - fe_i)^2}{fe_i}$$

که در آن Fo_i و Fe_i به ترتیب فراوانی‌های مشاهده شده و مورد انتظار در سلول‌های جدول توافقی هستند.

درصورتی‌که مقدار *P*-Value کمتر از ۰/۰۰۵ باشد، H_0 رد و ادعای ما ثابت شده و در غیر این صورت نقیض ادعا مورد تأیید است. با در نظر گرفتن سطح اطمینان ۹۵٪، داده‌ها بررسی شد که نتایج آن در جدول (۵) ارائه شده است، که نشان دهندهٔ تائید ادعا است. در گام بعدی برای بررسی بیشتر برابر روش فرضیه آماری مقدار بحرانی نیز موردبررسی قرار می‌گیرد.

جدول (۵) نتایج آزمون کای مربع فرضیه اول

کای مربع	۹۵/۱۵
درجه آزادی	۶
P-Value	۰/۰۰۱

گام سوم- قضاوت و استنتاج

با توجه به نتیجهٔ مشاهده شده در جدول (۵) نتیجه می‌گیریم، برای فرضیه اول با درجه آزادی ۶ و مقدار سطح خطا ۰/۰۵ مقدار بحرانی برابر فرمول زیر محاسبه می‌شود:

$$\boldsymbol{a = 0.05}, \quad \boldsymbol{df = 6}, \quad \boldsymbol{\chi^2_{\underset{05,6}{0}} = 12.5916}$$

مقدار بحرانی از جدول کای مربع استخراج شد که مطابق فرمول یک برابر ۱۲.۵۹۱۶ به‌دست‌آمده است.

گام چهارم- نتیجه‌گیری

ازآنجاکه آمارهٔ آزمون در ناحیه قرار دارد، پس می‌توان گفت که در سطح اطمینان ۹۵ درصد بین هوش مصنوعی و تاب‌آوری سایبری ارتباط معنی‌داری وجود دارد.

فرضیه دوم

گام اول- تعریف فرضیه‌های پژوهشی H_0 و H_1 (فرض‌ها)

نقیض ادعا (H_0): به نظر می‌رسد با نحوهٔ به‌روز کردن بانک اطلاعاتی نمی‌توان ارزیابی لازم را برای پیش‌بینی حملات سایبری در حوزهٔ تاب‌آوری سایبری انجام داد.

ادعا (H_1): به نظر می‌رسد با نحوهٔ به‌روز کردن بانک اطلاعاتی می‌توان ارزیابی لازم را برای پیش‌بینی حملات سایبری در حوزهٔ تاب‌آوری سایبری انجام داد.

گام دوم- آمارهٔ آزمون

برای فرضیه دوم پژوهش، با در نظر گرفتن سطح اطمینان ۹۵٪ داده‌ها بررسی شد که نتایج آن در جدول (۶) ارائه شده است و نشان‌دهندهٔ تأیید ادعا است. در گام بعدی برای بررسی بیشتر برابر روش فرضیه آماری مقدار بحرانی نیز موردبررسی قرار می‌گیرد.

جدول (۶) نتایج آزمون کای مربع فرضیه دوم

کای مربع	۱۳۷/۷۳
درجه آزادی	۹
P-Value	۰/۰۰۱

گام سوم- قضاوت و استنتاج

با توجه به نتیجه مشاهده شده در جدول (۶) نتیجه می‌گیریم که برای فرضیهٔ اول با درجه آزادی ۹ و مقدار سطح خطا ۰/۰۵ مقدار بحرانی برابر فرمول زیر محاسبه می‌شود:

$$a = 0.05\,, \qquad df = 9, \qquad \chi^2_{\underline{0}\,\underline{6}}{}_{05,6} = 14.5616$$

مقدار بحرانی از جدول کای مربع استخراج شد که مطابق فرمول یک برابر ۱۴.۵۶۱۶ به‌دست‌آمده است.

گام چهارم- نتیجه‌گیری

ازآنجاکه آمارهٔ آزمون در ناحیه قرار دارد پس می‌توان گفت که در سطح اطمینان ۹۵ درصد بین به‌روز کردن بانک اطلاعاتی و تاب‌آوری سایبری ارتباط معنی‌داری وجود دارد.

فرضیه سوم

گام اول- تعریف فرضیه‌های پژوهشی H_0 و H_1 (فرض‌ها)

نقیض ادعا (H_0): به نظر می‌رسد با استفاده از سیستم‌های خودگردان نمی‌توان ارزیابی لازم را برای پیش‌بینی حملات سایبری در حوزهٔ تاب‌آوری سایبری انجام داد.

ادعا (H_1): به نظر می‌رسد با استفاده از سیستم‌های خودگردان می‌توان ارزیابی لازم را برای پیش‌بینی حملات سایبری در حوزهٔ تاب‌آوری سایبری انجام داد.

گام دوم- آمارهٔ آزمون

برای فرضیهٔ سوم پژوهش، با در نظر گرفتن سطح اطمینان ۹۵٪ داده‌ها بررسی شد که نتایج آن در جدول (۷) آمده است که با توجه به مقدار *P*-Value=0.001، نشان دهندهٔ تأیید ادعا است. در گام بعدی برای بررسی بیشتر برابر روش فرضیهٔ آماری مقدار بحرانی نیز موردبررسی قرار می‌گیرد.

جدول (۷) نتایج آزمون کای مربع فرضیه سوم

کای مربع	۳۶/۰۰
درجه آزادی	۸
P-Value	۰/۰۰۱

گام سوم- قضاوت و استنتاج

با توجه به نتیجهٔ مشاهده شده در جدول (۷) نتیجه می‌گیریم که برای فرضیهٔ اول با درجه آزادی ۸ و مقدار سطح خطا ۰/۰۵ مقدار بحرانی برابر فرمول زیر محاسبه می‌شود.

$$a = 0.05\,, \qquad df = 8, \qquad \chi^2_{\underset{05,6}{0}} = 15.5073$$

مقدار بحرانی از جدول کای مربع استخراج شد که مطابق فرمول یک برابر ۱۵.۵۰۷۳ به‌دست‌آمده است.

گام چهارم- نتیجه‌گیری

ازآنجاکه آمارهٔ آزمون در ناحیه قرار دارد پس می‌توان گفت که در سطح اطمینان ۹۵ درصد بین استفاده از سیستم‌های خودگردان و تاب‌آوری سایبری ارتباط معنی‌داری وجود دارد.

نتیجه‌گیری و پیشنهادها

با توجه به شاخص‌های مستخرج از مصاحبهٔ اکتشافی با صاحب‌نظران و مطالعهٔ اسناد و مدارک و همچنین پاسخ‌های دریافت شده از پرسشنامه، فرضیه‌های این تحقیق در فرایند آمار استنباطی و با استفاده از آزمون کای مربع مورد تأیید قرار گرفته و در پایان هشت شاخص در بُعد پیش‌بینی در ارزیابی تاب‌آوری سایبری به دست آمد؛ لذا نتیجه می‌گیریم که می‌توان از ارزیابی تاب‌آوری سایبری با پیش‌بینی حملات سایبری بهره برد و همچنین مبتنی بر داده‌های جمع‌آوری‌شده، اولویت شاخص‌های بُعد پیش‌بینی در ارزیابی تاب‌آوری سایبری به‌این‌ترتیب است:

۱. با استفاده از سیستم‌های تشخیص نفوذ و پاسخ به نفوذ که از هوش مصنوعی بهره می‌گیرند، می‌توان تاب‌آوری سایبری را ارزیابی کرد؛
۲. با استفاده از الگوریتم‌های یادگیری ماشین برای تشخیص الگوهای غیرعادی و شناسایی تهدیدات سایبری، می‌توان تاب‌آوری سایبری را ارزیابی کرد؛
۳. با پشتیبان‌گیری منظم می‌توان تاب‌آوری سایبری را ارزیابی کرد؛
۴. با استفاده از بخشنامه‌ها، دستورالعمل‌ها و آیین‌نامه‌های سایبری رده‌بالا، می‌توان تاب‌آوری سایبری را ارزیابی کرد؛
۵. با استفاده از تیم مدیریت ریسک سایبری، می‌توان تاب‌آوری سایبری را ارزیابی کرد؛
۶. با استفاده از شبکه‌های عصبی برای تشخیص الگوهای غیرعادی، می‌توان تاب‌آوری سایبری را ارزیابی کرد؛
۷. با اجرای منظم سناریوهای حملات فرضی به‌منظور بررسی واکنش سیستم خودگردان، می‌توان تاب‌آوری سایبری را ارزیابی کرد؛
۸. با ایجاد مراکز فرماندهی و کنترل سایبری، می‌توان تاب‌آوری سایبری را ارزیابی کرد.

قدردانی

از تمام استادان و بزرگوارانی که در انجام این پژوهش ما را یاری کردند، سپاسگزاریم.

منابع

- آذر، داود و ملکی، علیرضا (۱۳۹۸)، جنگ سایبر و راه‌های مقابله با حملات سایبری، انتشارات دافوس، چاپ اول.
- رشیدی، علی جبار؛ داداش تبار احمدی، کوروش و نظرپور، بهزاد (۱۳۹۶). آگاهی وضعیتی سایبری، دانشگاه صنعتی مالک اشتر، چاپ اول، پاییز، ص ۱۸.
- رفیعانی، حامد و برومندنیا، علی (۱۳۹۶)، تأثیر الگوریتم‌های تکاملی در مسیریابی شبکه‌های Vanet و نقش آن در امنیت ارسال پیام، اولین همایش پیشرفت فناوری اطلاعات، آبان.
- سجادی اصیل، وحید و آذر، داود (۱۳۹۹)، عملیات سایبری در طرح‌ها و برنامه‌های وزارت دفاع آمریکا، *انتشارات دافوس*، تهران، ۴۱-۴۵.
- سند جامع سایبری نیروهای مسلح (۱۳۹۹)، تدوین‌کننده معاونت علوم تحقیقات و فناوری ستاد کل نیروهای مسلح، *اداره علوم سایبری و هوش مصنوعی*، اسفندماه.

- سند جامع سایبری نیروهای مسلح (۱۳۹۹)، تدوین‌کننده معاونت علوم تحقیقات و فناوری ستاد کل نیروهای مسلح، اداره علوم سایبری و هوش مصنوعی، اسفندماه.
- علی محمدی، سجاد و فتحی، محمد. (۲۰۲۴). ارائه سیستم تشخیص نفوذ در اینترنت اشیاء صنعتی با استفاده از الگوریتم گرگ خاکستری. فصلنامه فناوری اطلاعات و ارتباطات ایران، ۶۱ (۱۶)، ۲۲۸-۲۱۸.
- قاسمی، محمد. (۱۴۰۱)، قدرت سایبری، انتشارات دافوس، چاپ اول.
- ولوی، محمدرضا؛ حسنی اصل، حمیدرضا؛ نیک‌نفس، علی و دلگیر، علی. (۱۳۹۹). احصاء، ارزیابی و تحلیل شکاف ابعاد نظام رصد، پایش و هشداردهی سایبری از منظر امنیت ملی. امنیت ملی، ۱۰(۳۷)، ۲۲۴-۱۸۹. doi: dor:20.1001.1.33292538.1399.10.37.6.9.

- D. Bodeau, et al, (2015) "Cyber Resiliency Engineering Aid- the Updated cyber Resiliency Engineering Framwork and Guidance on Applying Cyber Resiliency Techniques".
- Tammet, Tanel, Autonomous Cyber Defence Capabilities, Autonomous Cyber Capabilities under International Law, NATO CCDCOE Publications, Chapter 3, 2021, PP 37-39.
- Giovanni Apruzzese and others, 'On the Effectiveness of Machine and Deep Learning for Cyber Security' in Tomáš Minárik, Raik Jakschis and Lauri Lindström (eds), 10th International Conference on Cyber Conflict, CyCon X: Maximising Effects (NATO CCDCOE 2018).PP 371-377.
- L Llansó, Thomas H, Hedgecock, Daniel A, and Pendergrass, J. Aaron, The State of Cyber Resilience: Now and in the Future, Johns Hopkins APL Technical Digest, Volume 35, Number 4, 2021, P 332.
- Jennifer Adams, Michael Stevens "Autonomous Systems for Cyber Resilience: Techniques and Applications" Journal of Cybersecurity and Autonomous Systems, 2021, PP 22-24.
- Parend, Pierre, and others, Foundations and Applications of Artificial Intelligence for Zero-Day and Multi-Step Attack Detection, 4 EURASIP Journal on Information Security, 2018, PP 2-4.
- John Doe, Jane Smith "Artificial Intelligence in Enhancing Cybersecurity Resilience: Techniques and Challenges" Journal of Cybersecurity Research, 2021.
- Parend, Pierre, and others, Foundations and Applications of Artificial Intelligence for Zero-Day and Multi-Step Attack Detection, 4 EURASIP Journal on Information Security, 2018, PP 2-4.
- Sarah Thompson, David White "Database-Driven Predictive Models for Cyber Resilience" International Journal of Cyber Security and Digital Forensics,2021.