AJA Command and Staff University

Warfare Study Quarterly

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

Identifying Cyber Range Components in a Cyber Wargaming System

Mohammad Ghasemi Tadavani[1] | Ali Sedighi[2]✉ | Hamid Bigdeli[3]

1. Faculty of Command and Staff University, Tehran, Iran. **E-mail**: m.ghasemi@casu.ac.ir
2. Graduated from Command and Staff University, Tehran, Iran. **E-mail**: ali.sedighi496@gmail.com
3. Faculty of Command and Staff University, Tehran, Iran. E-mail: H.bigdeli@casu.ac.ir

Article Info

Article type:

Research Article

Article history:

Received

29 November 2025

Received in revised form

14 February 2026

Accepted

10 March 2026

Published online

19 February 2026

Keywords:

Cyber Range, Cyber Wargaming, Cyber Security

ABSTRACT

Objective: The objective of this research is to identify the components of cyber range in the cyber warfare game system, such that a comprehensive and effective educational environment is created, and the level of cybersecurity in organizations, especially the cyber warfare game system of the Army of the Islamic Republic of Iran, can be enhanced.

Method: The research method in this study is mixed, including qualitative and quantitative analysis. Qualitative data is extracted and analyzed from interviews and documents using content analysis and MAXQDA software. Quantitative data is statistically analyzed using questionnaires and SPSS software. Cronbach's alpha coefficient was used to increase the reliability of measurement tools. The research process includes categorization, refinement, and descriptive and inferential analysis of data to ultimately achieve results aligned with the research objectives and provide a framework for developing new cyber range educational models.

Findings: The findings of this research showed that each of the dimensions of required infrastructure, scenario and content, human resources, and evaluation and analysis are the most important components and indicators of cyber range in the cyber warfare game system.

Results: The results show that the use of cyber ranges not only provides practical training in directly confronting security threats, but also strengthens the cooperation and interaction of team members and helps improve defensive strategies. This can have a significant impact on increasing the resilience and security of cyberspace.

Cite this article: Ghasemi Tadavani, M. Sedighi, A. & Bigdeli, H. (2026). Identifying Cyber Range Components in a Cyber Wargaming System. *Warfare Study Quarterly*, 7 (27), 79-109.

DOI: http//doi.org/10.22034/qjws.2026.2083464.1331

 Publisher: Command and Staff University

DOI: 10.22034/qjws.2026.2083464.1331

فصلنامه علمی مطالعات جنگ
شاپای چاپی: ۱۷۶۰-۲۷۱۷ شاپای الکترونیکی: ۱۷۶۰-۲۷۱۷ https://www.qjws.ir/ دانشگاه فرماندهی و ستاد آجا

شناسایی مولفه‌های سایبر رنج در سامانه بازی جنگ سایبری

محمد قاسمی تادوانی[۱] | علی صدیقی[۲]✉ | حمید بیگدلی[۳]

۱. عضو هیئت علمی دانشگاه فرماندهی و ستاد آجا، تهران، ایران، رایانامه: m.ghasemi@casu.ac.ir
۲. نویسنده مسئول، کارشناس ارشد مدیریت دفاعی، تهران، ایران، رایانامه: ali.sedighi496@gmail.com
۳. دانشیار دانشگاه فرماندهی و ستاد آجا، تهران، ایران، رایانامه: H.bigdeli@casu.ac.ir

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی
تاریخ دریافت:
۱۴۰۴/۰۹/۰۸
تاریخ بازنگری:
۱۴۰۴/۱۱/۲۵
تاریخ پذیرش:
۱۴۰۴/۱۲/۱۰
تاریخ انتشار:
۱۴۰۴/۱۲/۲۸
کلیدواژه‌ها:
سایبر رنج، بازی جنگ سایبری، امنیت سایبری

چکیده

هدف: هدف از انجام این پژوهش، شناسایی مولفه‌های سایبر رنج در سامانه بازی جنگ سایبری است به گونه‌ای که محیط آموزشی جامع و مؤثری ایجاد شود و بتواند سطح امنیت سایبری در سازمان‌ها، به ویژه سامانه بازی جنگ سایبری، ارتقاء یابد.

روش: روش تحقیق در این پژوهش تلفیقی و شامل تحلیل کیفی و کمی است. داده‌های کیفی با استفاده از روش تحلیل محتوا و نرم‌افزار MAXQDA از مصاحبه‌ها و اسناد استخراج شده و تجزیه و تحلیل شده‌اند. داده‌های کمی نیز با استفاده از پرسش‌نامه و نرم‌افزار SPSS تحلیل آماری شده‌اند. برای افزایش قابلیت اعتماد ابزارهای سنجش، از ضریب آلفای کرونباخ استفاده شده است. فرایند تحقیق شامل دسته‌بندی، پالایش، و تحلیل توصیفی و استنباطی داده‌ها است.

یافته‌ها: یافته‌های این تحقیق نشان می‌دهد که هریک از ابعاد زیرساخت‌های مورد نیاز، سناریو و محتوا، نیروی انسانی، ارزیابی و تحلیل، مهم‌ترین مولفه‌ها و شاخص‌های سایبر رنج در سامانه بازی جنگ سایبری هستند.

نتایج: نتایج نشان می‌دهد بکارگیری سایبر رنج‌ها، نه‌تنها امکان آموزش عملی در مواجهه مستقیم با تهدیدات امنیتی را فراهم می‌کند، بلکه همکاری و تعامل اعضای تیم‌ها را تقویت کرده و به بهبود راهکارهای دفاعی کمک می‌کند. این امر می‌تواند تاثیر چشم‌گیری در افزایش تاب‌آوری و امنیت فضای سایبری داشته باشد.

استناد: قاسمی تادوانی، محمد؛ صدیقی، علی؛ و بیگدلی، حمید (۱۴۰۵). شناسایی مولفه‌های سایبر رنج در سامانه بازی جنگ سایبری. *فصلنامه مطالعات جنگ*، ۷ (۲۷)، ۱۰۹-۷۹.

DOI: http//doi.org/10.22034/qjws.2026.2083464.1331

ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

DOI:10.22034/qjws.2026.2083464.1331

مقدمه

امروزه، با توجه به گسترش بی‌وقفه فناوری اطلاعات و ارتباطات، امنیت سایبری به عنوان یکی از زیرساخت‌های حیاتی و غیرقابل چشم‌پوشی برای سازمان‌ها، نهادها مطرح می‌شود. با پیچیده‌تر شدن ساختار حملات سایبری و ظهور تهدیدات امنیتی جدید، سازمان‌ها نیازمند اتخاذ رویکردی جامع و هوشمندانه در زمینه امنیت سایبری هستند تا بتوانند از اطلاعات و دارایی‌های دیجیتال خود در برابر این تهدیدات محافظت نمایند و از بروز خسارات جبران‌ناپذیر جلوگیری کنند (دویر موگ، و همکاران، ۲۰۲۳).

در این میان، مفهوم سایبر رنج[1]، به عنوان یک راهکار مؤثر و کارآمد برای آموزش و تمرین در زمینه امنیت سایبری به سرعت در حال توسعه و فراگیر شدن است. سایبر رنج، محیطی شبیه‌سازی شده و پویا را فراهم می‌آورد که کاربران در آن قادرند طیف گسترده‌ای از شبکه‌ها، سرورها و سیستم‌های رایانه‌ای را به صورت مجازی تجربه نمایند (گلاس ویلبرت، و همکاران، ۲۰۲۳).

از سوی دیگر، بازی جنگ سایبری[2] به عنوان یک ابزار استراتژیک در مواجهه با تهدیدات سایبری و تقویت آمادگی نیروهای نظامی و امنیتی، اهمیت فزاینده‌ای یافته است. در واقع، بازی جنگ سایبری به گونه‌ای طراحی شده است که سناریوهای تهدیدات جنگ سایبری را شبیه‌سازی کند و به کارشناسان و تصمیم‌گیرندگان این امکان را می‌دهد تا با تحلیل رفتارها و واکنش‌ها در شرایط مختلف، استراتژی‌های مؤثرتری را توسعه دهند (بوران و همکاران، ۲۰۱۹).

مسئله قابل توجه این است که، با ظهور عرصه سایبری و شکل‌گیری تهدیدهای نوین در این حوزه، سازمان‌های نظامی و نهادهای غیرنظامی به‌طور فزاینده‌ای به فعالیت در زمینه شبیه‌سازی و سنجش قابلیت‌های سایبری روی آورده و بازی‌های جنگ سایبری را به‌عنوان ابزاری کلیدی برای ارزیابی وضعیت امنیت سایبری و آزمون راهبردهای تاکتیکی و عملیاتی خود به‌کار می‌گیرند. در این چارچوب، مفهوم سایبر رنج، به‌عنوان مجموعه‌ای از فناوری‌ها، ابزارها و محیط‌های شبیه‌سازی که سناریوهای متنوع حمله و دفاع را بازتولید می‌کنند، نقشی محوری ایفا می‌نماید (لاتس و همکاران، ۲۰۲۳).

---

[1] Cyber range
[2] Cyber Wargaming

با توجه به پژوهش انجام شـــده و بررســـی جامع مولفه‌های مختلف مؤثر بر ســـایبر رنج، محقق چهار بعد را که دارای بیشترین تاثیر در شناسایی مولفه‌های سایبر رنج در سامانه بازی جنگ سایبری هستند، انتخاب کرده است:

زیرســـاخت‌های مورد نیاز اســـت که شـــامل نرم‌افزارهای اختصـــاصـــی، ســـخت‌افزارهای اختصاصی، زیرساخت شبکه سخت‌افزاری و نرم‌افزاری، واقعیت مجازی و واقعیت افزوده، اســـت که هم قابلیت ایجاد تجارب غوطه‌ورکننده و هم قابلیت کنترل و مدیریت ایمن محیط‌های شـــبیه‌ســـازی را فراهم می‌آورند. این بخش زیربنای فنی لازم برای اجرای سناریوهای پیچیده و مقیاس‌پذیر را تضمین می‌کند (دایر و همکاران، ۲۰۲۳).

سناریو و محتوا شامل فرایندهای طراحی و اجرا برای سناریوی حمله و سناریوی دفاع، و نیز سامانه‌های تولید خودکار سناریو است که کیفیت، تنوع و واقع‌نمایی تجربیات آزمون را تعیین می‌کننـد و بـه ارزیـابی توانمنـدی‌هـای فنی و انســـانی در شـــرایط متنوع و چالش‌برانگیز کمک می‌نمایند (گلاس و همکاران، ۲۰۲۳).

نیروی انســـانی به عنوان بعدی حیاتی متشـــکل از تعیین دقیق نقش‌ها و مســـئولیت‌ها، پیاده‌ســـازی ســـامانه‌های احراز هویت چندعاملی، مکانیزم‌های ردیابی و تحلیل فعالیت کاربران، و برنامه‌های آموزش و ارتقای مهارت است که تضـمین می‌کند بازیگران انسـانی در فرآیندهای شـبیه‌سـازی و دفاعی توانمند، پاسـخگو و قابل اتکا باشـند. این بعد به ویژه در کاهش خطاهای انســـانی و افزایش اثربخشـــی عملیات ســـایبری نقش محوری دارد (گلاس و همکاران، ۲۰۲۳).

در نهایت، ارزیابی و تحلیل شـــامل ســـامانه‌های امتیازدهی، ابزارهای تحلیل رفتاری و مکانیســـم‌های گزارش‌دهی و ارتقا اســـت که امکان ســـنجش عملکرد، اســـتخراج الگوهای تهدید، و بهینه‌سازی مستمر فرایندها را فراهم می‌سازد. این حلقه بازخورد باعث تقویت سازگاری و ارتقای کارایی کلی سایبر رنج می‌شود (دوباتی و همکاران، ۲۰۱۹).

پژوهش حاضـــر با تمرکز بر این ابعاد کوشـــیده اســـت تا چارچوبی نظام‌مند برای تعریف، طراحی و به‌کارگیری سـایبر رنج در سـامانه بازی جنگ سـایبری ارائه دهد تا بدین‌وسـیله قابلیت‌های پاســـخ‌دهی، تحمل‌پذیری و اثربخشـــی مکانیزم‌های دفاعی در مواجهه با تهدیدات پیچیده و پویا ارتقاء یابد. با توجه به ظرفیت‌های موجود آجا، شـــکل‌گیری تهدیدات نوین در حوزه سایبری و پیچیدگی روزافزون صحنه نبرد، انجام چنین تحقیقی نتایج و آثار مثبت زیر را در پی خواهد داشت:

- متخصصان می‌توانند در محیطی شبیه‌سازی شده، با انواع حملات و تهدیدات سایبری مواجه شده و مهارت‌های خود را در شناسایی کنند.
- شناسایی دقیق مولفه‌ها و نحوه تعامل آنها با یکدیگر، منجر به طراحی و پیاده‌سازی سامانه‌های آموزشی کارآمدتر و جذاب‌تر می‌شود.
- سازمان‌ها می‌توانند نقاط ضعف و آسیب‌پذیری‌های سیستم‌های خود را شناسایی کرده و قبل از اینکه مورد سوء استفاده قرار گیرند، آنها را برطرف کنند.

و از طرفی عدم انجام این تحقیق، نتایج و آثار منفی زیر را در پی خواهد داشت:

- باعث می‌شود سازمان‌ها در برابر حملات سایبری آسیب‌پذیرتر شوند.
- باعث می‌شود اعضای تیم نتوانند با همکاری یکدیگر به حل مسائل پیچیده امنیتی بپردازند.
- باعث می‌شود متخصصان امنیت سایبری نتوانند مهارت‌های خود را در شناسایی و مقابله با تهدیدات سایبری واقعی تقویت کنند.

مهمترین جنبه نوآوری این پژوهش، خلا دانش در این حوزه است. موضوع خاص شناسایی مولفه‌های سایبر رنج در سامانه‌های بازی جنگ سایبری به طور کامل در پژوهش‌های پیشین مورد بررسی قرار نگرفته است. در حالی که برخی تحقیقات مانند تحقیق لاتس و همکاران (۲۰۲۳)، به بررسی فناوری‌های سایبر رنج می‌پردازد، اما هیچ‌یک از این مطالعات به طور خاص به شناسایی مولفه‌های سایبر رنج در زمینه بازی‌های جنگ سایبری نپرداخته‌اند. این خلا دانش نشان‌دهنده ضرورت انجام تحقیقاتی است که به طور خاص بر روی این مولفه‌ها و تأثیرات آن‌ها آمادگی در برابر تهدیدات سایبری تمرکز کنند.

بنا بر موارد عنوان شده، هدف از انجام این پژوهش شناسایی مولفه‌های سایبر رنج در سامانه بازی جنگ سایبری است به گونه‌ای که منجر به ایجاد یک محیط آموزشی جامع و موثر گردد تا بتواند با توسعه الگوها و رویکردهای نوین در حوزه آموزش در سامانه بازی جنگ سایبری، زمینه‌ساز افزایش سطح امنیت سایبری در سازمان‌ها و بویژه سامانه بازی جنگ سایبری، گردد.

سوال اصلی پژوهش حاضر اینست که مولفه‌های سایبر رنج در سامانه بازی جنگ سایبری کدامند؟

مبانی نظری و پیشینه‌های پژوهش

مبانی نظری

سایبر رنج به عنوان یک چارچوب پیشرفته و سازمان‌یافته برای شبیه‌سازی محیط‌های فناوری اطلاعات و ارتباطات، نقشی حیاتی در ارتقای آمادگی امنیت سایبری سازمان‌ها ایفا می‌کند. این فضا با فراهم آوردن بسترهای کنترل‌شده و واقع‌گرایانه، امکان تمرین سناریوهای حمله و دفاع، ارزیابی اثربخشی راهکارهای امنیتی و تحلیل رفتار مهاجمان را بدون به‌خطرانداختن زیرساخت‌های عملیاتی فراهم می‌سازند. در چنین محیط‌هایی، تیم‌های امنیتی می‌توانند فرآیندهای کشف، پاسخ و بازیابی را تحت فشار زمانی و شرایط متنوع آزمون کنند، آسیب‌پذیری‌ها و نقاط ضعف را شناسایی و اولویت‌بندی کنند و مدل‌های تهدید را با داده‌های تجربی تقویت نمایند. علاوه بر این، سایبر رنج‌ها امکان سنجش سازگاری و پایداری کنترل‌ها در مواجهه با حملات پیچیده و ترکیبی را می‌دهند و از طریق تمرین مداوم، دانش فنی و هماهنگی میان‌سازمانی را بهبود می‌بخشند (بلایکنز و همکاران، ۲۰۲۴).

بازی جنگ سایبری به‌عنوان یک حوزه نوین و پیچیده از عملیات نظامی و امنیتی در فضای سایبری تعریف می‌شود که در آن بازیگران دولتی و غیردولتی با استفاده از ابزارها و تکنیک‌های پیشرفته اطلاعاتی و نرم‌افزاری تلاش می‌کنند تا اهداف استراتژیک خود را از طریق حمله، نفوذ و یا دفاع در زیرساخت‌های حیاتی دیجیتال محقق سازند. در واقع انتقال دکترین‌های جنگی و استراتژی‌های امنیتی از میدان‌های نبرد سنتی به بستر دیجیتال، نیازمند بازنگری در مفاهیم حاکمیت، مسئولیت‌پذیری و نسبت میان حقوق بین‌الملل و فنّاوری‌های نوین است (خرّمی. (۲۰۲۴)).

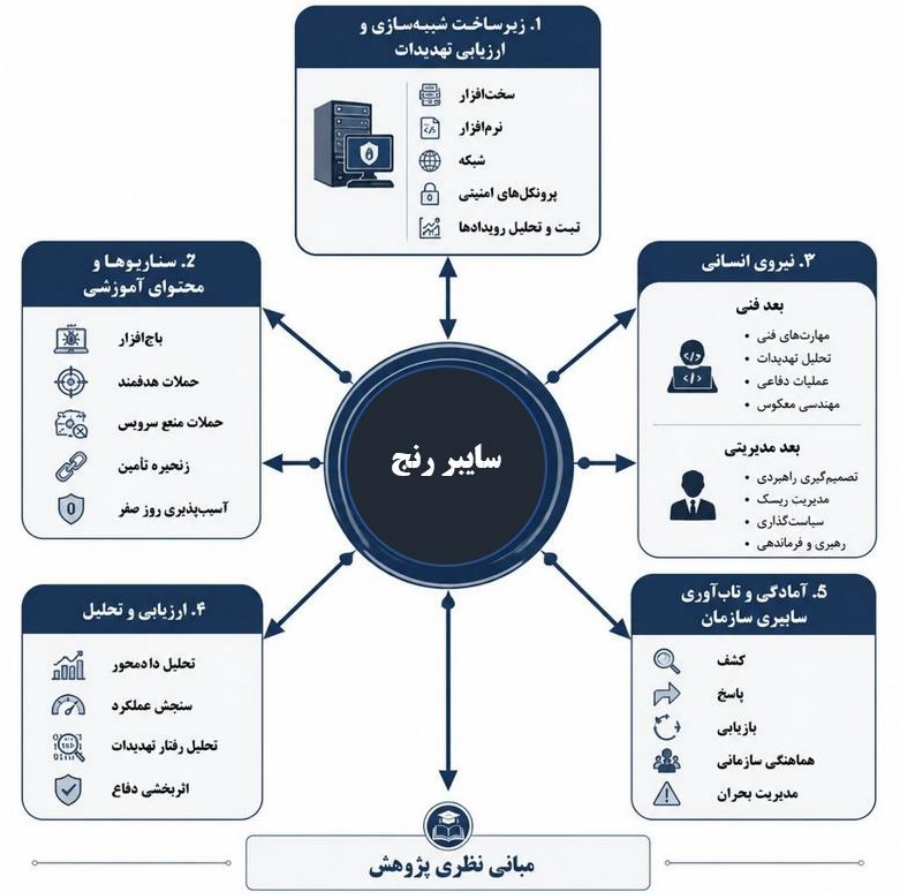
زیرساختی که برای شبیه‌سازی و ارزیابی تهدیدات سایبری طراحی می‌شود، ترکیبی پیچیده و منسجم از سخت‌افزارها، نرم‌افزارها، شبکه‌ها و پروتکل‌های امنیتی است که وظیفه ایجاد محیطی واقع‌نما و قابل اعتماد برای تمرین، آزمایش و ارزیابی سناریوهای حمله و دفاع را بر عهده دارد. این زیرساخت باید توانایی مدیریت بارهای سنگین ناشی از اجرای هم‌زمان سناریوهای متنوع حملات، واکنش‌های دفاعی و تعاملات متعدد بین بازیگران شبیه‌سازی‌شده را داشته باشد و در عین حال امکان ضبط، تحلیل و بازتولید رویدادها را با دقت بالا فراهم آورد (یامین و همکاران، ۲۰۲۲).

سناریوها و محتوای آموزشی در طراحی و اجرای تمرینات و شبیه‌سازی‌های بازی جنگ سایبری نقشی محوری ایفا می‌کنند و به‌عنوان چارچوبی ساختاریافته برای بازآفرینی محیط‌های واقعی و تقویت مهارت‌های عملی شرکت‌کنندگان عمل می‌نمایند. سناریوها باید با دقت و هوشمندی طراحی شوند تا نه‌تنها منعکس‌کننده تهدیدات سایبری واقعی، پویا و نوظهور در دنیای کنونی باشند، بلکه با اهداف آموزشی و سطح توانمندی‌های شرکت‌کنندگان نیز هم‌خوانی داشته باشند. این سناریوها باید طیف گسترده‌ای از چالش‌های سایبری، از حملات پیچیده نظیر باج‌افزارها، نفوذهای هدفمند و حملات منع سرویس گرفته تا تهدیدات نوین مانند حملات زنجیره تأمین یا بهره‌برداری از آسیب‌پذیری‌های روز صفر، را در بر گیرند (لاتس و همکاران، ۲۰۲۳).

نیروی انسانی به‌عنوان ستون فقرات و عامل محوری در سیستم‌های فناوری اطلاعات، به‌ویژه در محیط‌های پویا و پیچیده نظیر شبیه‌سازی‌های بازی جنگ سایبری، نقشی غیرقابل‌انکار ایفا می‌کند. این مؤلفه، که از مجموعه‌ای از مهارت‌ها، دانش‌ها، تجربیات و شایستگی‌های چندوجهی تشکیل شده است، افراد را قادر می‌سازد تا در سناریوهای چالش‌برانگیز و پرفشار سایبری به‌صورت مؤثر عمل کنند و پاسخ‌های مناسب به تهدیدات ارائه دهند. نیروی انسانی در این حوزه به دو بعد اصلی تقسیم می‌شود: بعد فنی و بعد مدیریتی. بعد فنی شامل مهارت‌های تخصصی نظیر تحلیل رفتار و عملکرد نرم‌افزارها، شناسایی و ردیابی تهدیدات سایبری پیشرفته (مانند بدافزارها، حملات فیشینگ یا نفوذهای مبتنی بر مهندسی اجتماعی)، و طراحی و اجرای راهکارهای دفاعی و پاسخ‌گویی به حوادث سایبری است. بعد مدیریتی بر توانایی‌های راهبردی و سازمانی تمرکز دارد که شامل رهبری تیم‌های چندرشته‌ای، مدیریت بحران در شرایط اضطراری، تصمیم‌گیری سریع و مؤثر تحت فشارهای شدید، و هماهنگی بین واحدهای مختلف در محیط‌های عملیاتی پویا می‌شود. این بعد به‌ویژه در شبیه‌سازی‌های بازی جنگ سایبری اهمیت دارد، جایی که هماهنگی بین اعضای تیم و مدیریت منابع در زمان واقعی می‌تواند تفاوت بین موفقیت و شکست را تعیین کند (شین و همکاران، ۲۰۲۴).

ارزیابی و تحلیل در حوزه امنیت سایبری، به‌ویژه در بستر تمرینات و شبیه‌سازی‌های سایبری مانند سایبر رنج، مجموعه‌ای جامع از روش‌ها، تکنیک‌ها و ابزارهای تخصصی را در بر می‌گیرد که برای جمع‌آوری، پردازش و تفسیر داده‌های پیچیده تولیدشده در طول این فعالیت‌ها طراحی شده‌اند. این فرآیند حیاتی به تحلیل‌گران و متخصصان امنیت

سایبری امکان می‌دهد تا با بهره‌گیری از رویکردهای داده‌محور، عملکرد سیستم‌ها، رفتار تهدیدات سایبری، اثربخشی استراتژی‌های دفاعی و معیارهای عملکردی مرتبط با تیم‌ها و زیرساخت‌ها را به‌صورت دقیق مورد بررسی قرار دهند (ویلبرت و همکاران، ۲۰۲۳).



شکل ۱: مبانی نظری پژوهش

پیشینه‌های پژوهش

در رابطه با موضـــوع تحقیق، گلاس‌ام و همکاران (۲۰۲۳)، در تحقیقی با عنوان ارزیابی آموزش‌های ســایبری در ســایبر رنج، بیان می‌کند، یک چارچوب ســاختار یافته با هدف تسهیل ارزیابی تمرینات سایبر رنج وجود دارد. این چارچوب بر اساس یک فرآیند ارزیابی

پنج مرحله ای ادغام شـــده اســـت. این رویکرد ســـاختار یافته برای افزایش کیفیت و اثربخشی تمرینات محدوده سایبری در آموزش امنیت سایبری در نظر گرفته شده است.
اســلاوچو (۲۰۲۱)، در تحقیقی با عنوان اســتفاده از ســایبر رنج در برنامه‌های آموزشــی مدیریت امنیت ســـایبری، بیان می‌کند، تفاوت‌های بین پلتفرم‌های ســـایبر رنج منتخب برای پارامترهای مورد بررسی، کوچک و ناچیز هستند. براساس تحلیل ویژگی‌های سایبر رنج‌های مورد بررســی، Kypo به‌عنوان مناســب‌ترین گزینه برای نیازهای جهانی انتخاب شده است.
دایر و همکاران (۲۰۲۳)، در تحقیقی با عنوان کاربرد و پیامدهای راهبردی سایبر رنج در زمینه‌های نظامی، بیان می‌کند، سایبر رنج‌ها به‌عنوان ابزارهای استراتژیک برای نیروهای نظامی کاربردی هســتند. ســایبر رنج‌های حاکمیتی که برای توســعه قابلیت‌های حمله و دفاع ســـایبری، تمرین عملیات پیچیده و اســـتفاده از شـــبیه‌ســـازی‌های دقیق و سخت‌افزارهای تخصصی به‌کار می‌روند، و سایبر رنج‌های تقویت ظرفیت که بر آموزش، اشتراک‌گذاری اطلاعات و تمرین‌های مشترک بین‌المللی متمرکزند.
لاتس و همکاران (۲۰۲۳)، در تحقیقی با عنوان بررســـی فناوری‌های ســـایبر رنج، بیان می‌کند، استفاده از فناوری‌های مختلف در معماری سایبر رنج‌ها می‌تواند به بهبود امنیت ســـایبری و افزایش کارآیی آموزشـــی کمک کند. این مطالعه بر اهمیت اســـتفاده از مجازی‌سازی، اورکستراسیون و مدیریت پیکربندی در طراحی و پیاده‌سازی سیستم‌های سایبر رنج تأکید دارد.
پژوهش‌های پیشــین در زمینه شــناســایی مولفه‌های ســایبر رنج در ســامانه بازی جنگ سایبری به ابعاد مختلفی همچون ارزیابی نحوه انجام تمرینات، ویژگی‌های محیط تمرین، پلتفرم‌های مورد نیاز، تاثیر ســـایبر رنج‌ها به عنوان یک ابزار راهبردی بویژه در حوزه نظامی، اشــاره کرده‌اند که از این جهت با تحقیق حاضر مشــابه اســت اما هیچکدام از آنها به موضــوع خاص شــناســایی مولفه‌های ســایبر رنج در ســامانه بازی جنگ ســایبری به‌طور کامل نپرداخته‌اند و با توجه به اینکه این پژوهش به دنبال ارائه یک چارچوب جامع برای بهبود فرآیندهای آموزشی و امنیت سایبری است، با پژوهش‌های انجام شده در گذشته متفاوت است.

روش‌شناسی پژوهش

نوع تحقیق کاربردی است و محقق به دنبال یافتن پاسخی برای شناسایی مولفه‌های سایبر رنج در سامانه بازی جنگ سایبری است روش این تحقیق توصیفی است و محقق بر اساس آنچه که هست به توصیف منظم و نظام‌مند وضعیت فعلی می‌پردازد. در این تحقیق متغیرها دست‌کاری نمی‌شوند بلکه متغیرها انتخاب می‌شوند و مورد مشاهده قرار می‌گیرند.

جامعه آماری برای بخش کیفی و مصاحبه، شامل ۱۰ نفر از صاحب‌نظران آشنا به موضوع تحقیق است که به روش قضاوتی هدفمند انتخاب شدند و برای بخش کمی و پرسشنامه، جامعه آماری شامل ۳۷ نفر از کارشناسان بود که با مفاهیم سایبر رنج و بازی جنگ سایبری آشنا بودند و در بخش کمی، تحقیق به صورت تمام‌شمار انجام شده است.

جهت روایی مصاحبه، مصاحبه‌شوندگان از میان صاحب‌نظرانی برگزیده شده‌اند که علاوه بر صلاحیت علمی، از شناخت کافی در موضوع سایبر رنج و سامانه بازی جنگ سایبری، برخوردارند. در حوزه اسناد و مدارک، از جدیدترین کتاب‌ها و مقاله‌های معتبر علمی و مورد تائید استاد راهنما و مشاور ، استفاده شده است. در رابطه با روایی پرسشنامه سعی شده است پس از مطالعه کامل و استفاده از اسناد و مدارک، سوالات بگونه‌ای طرح شوند که محقق را به اهداف نزدیک نمایند و پرسش‌شوندگان در پاسخگویی، دچار ابهام نگردند.

در مورد پایایی ابزارها در مرحله مصاحبه میزان هم‌پوشانی پاسخ‌ها با یکدیگر تعیین گردید و با منابع و اسناد و مدارک مورد مقایسه قرار گرفت. برای پایایی پرسش‌نامه از ضریب آلفای کرونباخ در رابطه (۱) استفاده گردید که نتایج آن در جدول (۱) آمده است.

$$\alpha = \frac{k}{k-1}\left(1 - \frac{\sum_{i=1}^{k}\delta_i^2}{\delta^2}\right) \qquad (1)$$

که در این رابطه: k تعداد پرسش ها، δ_i^2 واریانس هر پرسش، δ^2 واریانس کل پرسش‌ها، است.

جدول ۱: بررسی پایایی پرسش‌نامه با استفاده از آزمون آلفای کرونباخ

بعد	شماره گویه‌ها	تعداد گویه‌ها	آلفای کرونباخ
زیرساخت‌های مورد نیاز	۱-۲۴	۲۴	۰/۸۵۷
سناریو و محتوا	۲۵-۴۲	۱۸	۰/۷۹۳
نیروی انسانی	۴۳-۶۷	۲۵	۰/۸۶۹
ارزیابی و تحلیل	۶۸-۸۶	۱۹	۰/۸۶۹
نتیجه نهایی	۱-۸۶	۸۶	۰/۹۲۳

روش تجزیه و تحلیل داده‌ها به این صورت است که، محقق به صورت توصیفی و با استفاده از روش تحلیل محتوا با کمک نرم‌افزار مکس کیو دی ای، داده‌ها و اطلاعات به‌دست آمده از مصاحبه و اسناد و مدارک را تجزیه و تحلیل می‌نماید. داده‌ها و اطلاعات به‌دست آمده از پرسش‌نامه، با استفاده از روش‌های آمار توصیفی مورد تجزیه و تحلیل قرار می‌گیرد. داده‌های کمی نیز به روش کمی و با نرم‌افزار SPSS تجزیه و تحلیل می‌شوند. در تحلیل کمّی از روش‌های آماری برای تجزیه و تحلیل داده‌ها استفاده می‌شود.

تجزیه و تحلیل داده‌ها

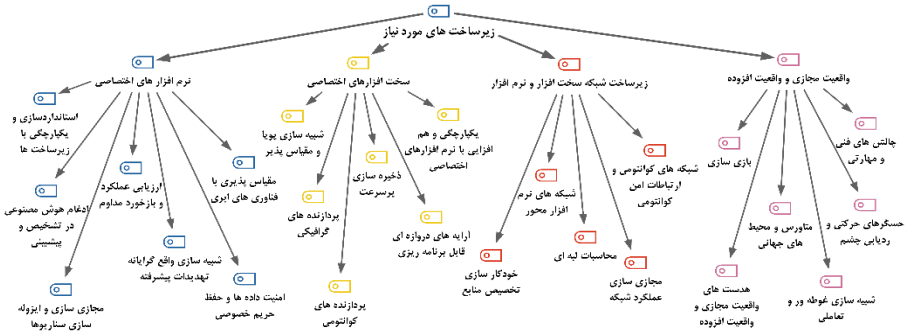
کلیات: در نخستین گام، طبقه‌بندی اطلاعات شامل پالایش، تلخیص و نمایش داده‌ها، با بهره‌گیری از تجزیه‌وتحلیل کیفی، بر اساس هدف پژوهشی و نظرات صاحب‌نظران و منابع معتبر موجود صورت پذیرفت. مرحله دوم شامل فهرست‌بندی و سازماندهی اطلاعات طبقه‌بندی شده است تا داده‌ها در قالب یک ساختار منسجم بررسی و مقایسه شوند و از طریق بهره‌گیری از مفهوم تقارب یا همگرایی نسبی، روابط پنهان میان داده‌ها کشف و به استنباطی دقیق و معتبر به دست آید. نهایتاً در گام سوم، بر اساس تحلیل‌های انجام شده و شواهد به دست آمده، مرحله قضاوت و تصمیم‌گیری صورت گرفت که به تدوین نتایج قطعی و کاربردی پژوهش منجر شد.

تجزیه و تحلیل کیفی

چهار بعد که دارای بیشترین تاثیر در شناسایی مولفه‌های سایبر رنج در سامانه بازی جنگ سایبری هستند، شامل: زیرساخت‌های مورد نیاز با مولفه‌های نرم‌افزارهای اختصاصی، سخت‌افزارهای اختصاصی، زیرساخت شبکه سخت‌افزاری و نرم‌افزاری، واقعیت مجازی و واقعیت افزوده، است. سناریو و محتوا شامل فرایندهای طراحی و اجرا برای سناریوی حمله و سناریوی دفاع، و نیز سامانه‌های تولید خودکار سناریو است. نیروی انسانی به عنوان بعدی حیاتی متشکل از تعیین دقیق نقش‌ها و مسئولیت‌ها، پیاده‌سازی سامانه‌های احراز هویت چندعاملی، مکانیزم‌های ردیابی و تحلیل فعالیت کاربران، و برنامه‌های آموزش و ارتقای مهارت است. ارزیابی و تحلیل شامل سامانه‌های امتیازدهی، ابزارهای تحلیل رفتاری و مکانیسم‌های گزارش‌دهی و ارتقا است.

زیرساخت‌های مورد نیاز: با دسته‌بندی داده‌ها، در بررسی اسناد و مدارک تعداد ۶ مولفه و ۳۲ شاخص و در بررسی مصاحبه با خبرگان تعداد ۵ مولفه و ۲۸ شاخص احصاء

گردید که پس از تقارب و تقاطع داده‌ها و اطلاعات بدســـت آمده تعداد ۴ مولفه و ۲۴ شـــاخص به عنوان شـــاخص‌های اصـــلی در نظر گرفته شـــد که خروجی آن در نرم افزار MAXQDA به صورت زیر نمایش داده شده است.



نمودار ۱: شاخص های احصا شده زیرساخت‌های مورد نیاز

بررسی مولفه اول حاکی از آنست که امکان شناسایی زیرساخت‌های مورد نیاز سایبر رنج در ســامانه بازی جنگ ســایبری، با توجه به مولفه نرم‌افزارهای اختصــاصــی، وجود دارد و بنابر داده‌های پردازش شده "شبیه‌سازی واقع‌گرایانه تهدیدات پیشرفته"، "مجازی‌سازی و ایزوله‌ســازی ســناریوها"، "ادغام هوش مصــنوعی در تشــخیص و پیش‌بینی"، "امنیت داده‌ها و حفظ حریم خصوصی"، "ارزیابی عملکرد و بازخورد مداوم"، "اســتانداردسازی و یکپارچگی با زیرســاخت‌ها"، "مقیاس‌پذیری با فناوری ابری"، از مهمترین شــاخص‌های اســاســی و تاثیرگذار در این مولفه به شــمار می‌رود. با تجزیه و تحلیل داده‌های مربوط به اسناد و مدارک و همچنین داده‌های مصاحبه‌های انجام شده، با توجه به همگرایی اسناد و مدارک و مصــاحبه برای مولفه نرم‌افزارهای اختصــاصــی، در بخش مصــاحبه ها ۱۹ و در بخش اســناد و مدارک ۲۲ عبارت بیانی بدســت آمد و در نهایت با پردازش این داده‌ها ۷ شاخص به شرح زیر به عنوان مهمترین گویه‌های تاثیرگذار تعیین گردید.

جدول ۲: شاخص‌های احصا شده در نرم‌افزارهای اختصاصی

بعد	مولفه	شاخص
زیرساخت‌های مورد نیاز	نرم‌افزارهای اختصاصی	۱) شبیه‌سازی واقع‌گرایانه تهدیدات پیشرفته
		۲) مجازی‌سازی و ایزوله‌سازی سناریوها
		۳) ادغام هوش مصنوعی در تشخیص و پیش‌بینی
		۴) امنیت داده‌ها و حفظ حریم خصوصی
		۵) ارزیابی عملکرد بازخورد مداوم

		۶) استانداردسازی و یکپارچگی با زیرساخت‌ها
		۷) مقیاس‌پذیری با فناوری ابری

بررسی مولفه دوم حاکی از آنست که امکان شناسایی زیرساخت‌های مورد نیاز سایبر رنج در سامانه بازی جنگ سایبری ، با توجه به مولفه سخت‌افزارهای اختصاصی وجود دارد و بنابر داده‌های پردازش شده "شبیه‌سازی پویا و مقیاس‌پذیر"، "پردازنده‌های گرافیکی"، "آرایه‌های دروازه‌ای قابل برنامه‌ریزی"، "ذخیره‌سازی پرسرعت"، "پردازنده‌های کوانتومی"، "یکپارچگی و هم‌افزایی با نرم‌افزارهای اختصاصی"، از مهمترین شاخص‌های اساسی و تاثیرگذار در این مولفه به شمار می‌رود. با تجزیه و تحلیل داده‌های مربوط به اسناد و مدارک و همچنین داده‌های مصاحبه‌های انجام شده، با توجه به همگرایی اسناد و مدارک و مصاحبه برای مولفه سخت‌افزارهای اختصاصی، در بخش مصاحبه ها ۲۴ و در بخش اسناد و مدارک ۲۹ عبارت بیانی بدست آمد و در نهایت با پردازش این داده‌ها ۶ شاخص به شرح زیر به عنوان مهمترین گویه‌های تاثیرگذار تعیین گردید.

جدول ۳: شاخص‌های احصا شده در سخت‌افزارهای اختصاصی

بعد	مولفه	شاخص
زیرساخت‌های مورد نیاز	سخت‌افزارهای اختصاصی	۱) شبیه‌سازی پویا و مقیاس‌پذیر
		۲) پردازنده‌های گرافیکی
		۳) آرایه‌های دروازه‌ای قابل برنامه‌ریزی
		۴) ذخیره‌سازی پرسرعت
		۵) پردازنده‌های کوانتومی
		۶) یکپارچگی و هم‌افزایی با نرم‌افزارهای اختصاصی

بررسی مولفه سوم حاکی از آنست که امکان شناسایی زیرساخت‌های مورد نیاز سایبر رنج در سامانه بازی جنگ سایبری، با توجه به مولفه زیرساخت شبکه سخت‌افزار و نرم‌افزار وجود دارد و بنابر داده‌های پردازش شده "شبکه‌های نرم‌افزارمحور"، "مجازی‌سازی عملکرد شبکه"، "محاسبات لبه‌ای"، "خودکارسازی تخصیص منابع"، "شبکه‌های کوانتومی و ارتباطات امن کوانتومی"، از مهمترین شاخص‌های اساسی و تاثیرگذار در این مولفه به شمار می‌رود. با تجزیه و تحلیل داده‌های مربوط به اسناد و مدارک و همچنین داده‌های مصاحبه‌های انجام شده، با توجه به همگرایی اسناد و مدارک و مصاحبه برای مولفه زیرساخت شبکه سخت‌افزار و نرم‌افزار، در بخش مصاحبه‌ها

۱۸ و در بخش اسناد و مدارک ۲۴ عبارت بیانی بدست آمد و در نهایت با پردازش این داده‌ها ۵ شاخص به شرح زیر به عنوان مهمترین گویه‌های تاثیرگذار تعیین گردید.

جدول ۴: شاخص‌های احصا شده در زیرساخت شبکه سخت‌افزار و نرم‌افزار

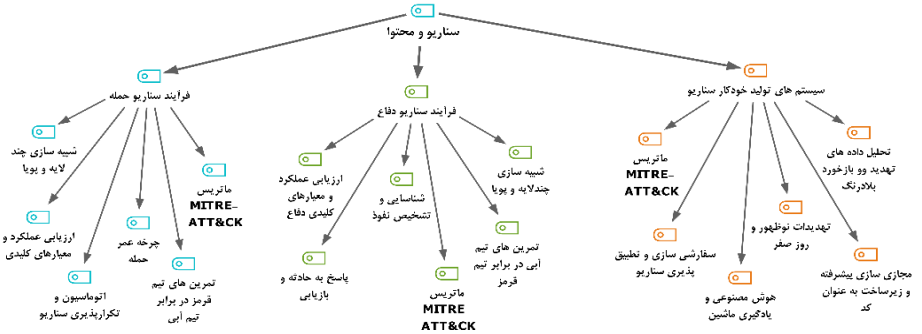
بعد	مولفه	شاخص
زیرساخت‌های مورد نیاز	زیرساخت شبکه سخت‌افزار و نرم‌افزار	۱) شبکه‌های نرم‌افزارمحور
		۲) مجازی‌سازی عملکرد شبکه
		۳) محاسبات لبه‌ای
		۴) خودکارسازی تخصیص منابع
		۵) شبکه‌های کوانتومی و ارتباطات امن کوانتومی

بررسی مولفه چهارم حاکی از آنست که امکان شناسایی زیرساخت‌های مورد نیاز سایبر رنج در سامانه بازی جنگ سایبری، با توجه به مولفه واقعیت مجازی و واقعیت افزوده وجود دارد و بنابر داده‌های پردازش شده "شبیه‌سازی غوطه‌ور و تعاملی"، "هدست‌های واقعیت مجازی و واقعیت افزوده"، "بازی‌سازی"، "متاورس و محیط‌های جهانی"، "حسگرهای حرکتی و ردیابی چشم"، "چالش‌های فنی و مهارتی"، از مهمترین شاخص‌های اساسی و تاثیرگذار در این مولفه به شمار می‌رود. با تجزیه و تحلیل داده‌های مربوط به اسناد و مدارک و همچنین داده‌های مصاحبه‌های انجام شده، با توجه به همگرایی اسناد و مدارک و مصاحبه برای مولفه واقعیت مجازی و واقعیت افزوده، در بخش مصاحبه ها ۱۹ و در بخش اسناد و مدارک ۲۵ عبارت بیانی بدست آمد و در نهایت با پردازش این داده‌ها ۶ شاخص به شرح زیر به عنوان مهمترین گویه‌های تاثیرگذار تعیین گردید.

جدول ۵: شاخص‌های احصا شده در واقعیت مجازی و واقعیت افزوده

بعد	مولفه	شاخص
زیرساخت‌های مورد نیاز	واقعیت مجازی و واقعیت افزوده	۱) شبیه‌سازی غوطه‌ور و تعاملی
		۲) هدست‌های واقعیت مجازی و واقعیت افزوده
		۳) بازی‌سازی
		۴) متاورس و محیط‌های جهانی
		۵) حسگرهای حرکتی و ردیابی چشم
		۶) چالش‌های فنی و مهارتی

سناریو و محتوا: با دسته‌بندی داده‌ها، در بررسی اسناد و مدارک تعداد ۴ مولفه و ۳۰ شاخص و در بررسی مصابه با خبرگان تعداد ۳ مولفه و ۲۵ شاخص احصاء گردید که پس از تقارب و تقاطع داده‌ها و اطلاعات بدست آمده تعداد ۳ مولفه و ۱۸ شاخص به عنوان شاخص‌های اصلی در نظر گرفته شد که خروجی آن در نرم افزار MAXQDA به صورت زیر نمایش داده شده است.



نمودار ۲: شاخص های احصا شده در بعد سناریو و محتوا

بررسی مولفه اول حاکی از آنست که امکان شناسایی مولفه‌های سناریو و محتوا در سایبر رنج در سامانه بازی جنگ سایبری، با توجه به مولفه فرآیند سناریو حمله وجود دارد و بنابر داده‌های پردازش شده "ماتریس MITRE-ATT&CK"، "شبیه‌سازی چندلایه و پویا"، "چرخه عمر حمله"، "تمرین‌های تیم قرمز در برابر تیم آبی"، "ارزیابی عملکرد و معیارهای کلیدی"، "اتوماسیون و تکرارپذیری سناریو"، از مهمترین شاخص‌های اساسی و تاثیرگذار در این مولفه به شمار می‌رود. با تجزیه و تحلیل داده‌های مربوط به اسناد و مدارک و همچنین داده‌های مصاحبه‌های انجام شده، با توجه به همگرایی اسناد و مدارک و مصاحبه برای مولفه فرآیند سناریو حمله، در بخش مصاحبه ها ۲۰ و در بخش اسناد و مدارک ۲۴ عبارت بیانی بدست آمد و در نهایت با پردازش این داده‌ها ۶ شاخص به شرح زیر به عنوان مهمترین گویه‌های تاثیرگذار تعیین گردید.

جدول ۶: شاخص‌های احصا شده در فرآیند سناریو حمله

بعد	مولفه	شاخص
سناریو و محتوا	فرآیند سناریو حمله	۱) ماتریس MITRE-ATT&CK
		۲) شبیه‌سازی چند لایه و پویا
		۳) چرخه عمر حمله

		۴) تمرین‌های تیم قرمز در برابر تیم آبی
		۵) ارزیابی عملکرد و معیارهای کلیدی
		۶) اتوماسیون و تکرار پذیری سناریو

بررسی مولفه دوم حاکی از آنست که امکان شناسایی مولفه‌های سناریو و محتوا در سایبر رنج در سامانه بازی جنگ سایبری ، با توجه به مولفه فرآیند سناریو دفاع وجود دارد و بنابر داده‌های پردازش شده " ماتریسMITRE-ATT&CK "، "شبیه‌سازی چندلایه و پویا"، "تمرین‌های تیم آبی در برابر تیم قرمز"، "شناسایی و تشخیص نفوذ"، "پاسخ به حادثه و بازیابی"، "ارزیابی عملکرد و معیارهای کلیدی دفاع"، از مهمترین شاخص‌های اساسی و تاثیرگذار در این مولفه به شمار می‌رود. با تجزیه و تحلیل داده‌های مربوط به اسناد و مدارک و همچنین داده های مصاحبه های انجام شده، با توجه به همگرایی اسناد و مدارک و مصاحبه برای مولفه فرآیند سناریو دفاع، در بخش مصاحبه ها ۲۷ و در بخش اسناد و مدارک ۳۱ عبارت بیانی بدست آمد و در نهایت با پردازش این داده‌ها ۶ شاخص به شرح زیر به عنوان مهمترین گویه‌های تاثیرگذار تعیین گردید.

جدول ۷: شاخص‌های احصا شده در فرآیند سناریو دفاع

بعد	مولفه	شاخص
سناریو و محتوا	فرآیند سناریو دفاع	۱) ماتریس MITRE-ATT&CK
		۲) شبیه‌سازی چندلایه و پویا
		۳) تمرین تیم‌های آبی در برابر قرمز
		۴) شناسایی و تشخیص نفوذ
		۵) پاسخ به حادثه و بازیابی
		۶) ارزیابی عملکرد و معیارهای کلیدی دفاع

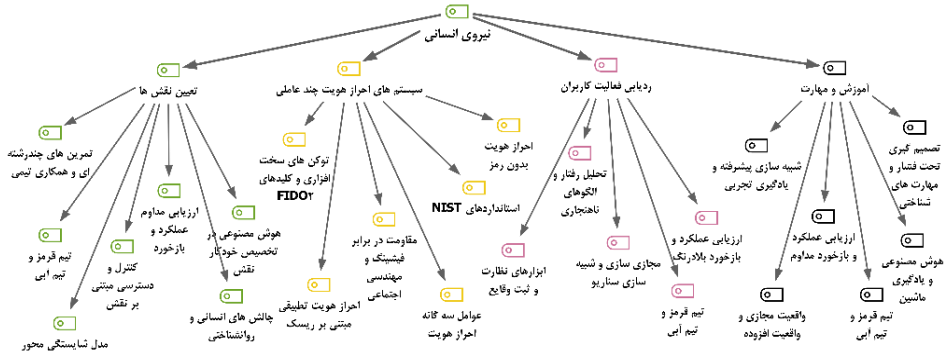
بررسی مولفه سوم حاکی از آنست که امکان شناسایی مولفه‌های سناریو و محتوا در سایبر رنج در سامانه بازی جنگ سایبری ، با توجه به مولفه سیستم‌های تولید خودکار سناریو وجود دارد و بنابر داده‌های پردازش شده " ماتریس MITRE-ATT&CK "، "هوش مصنوعی و یادگیری ماشین"، "مجازی‌سازی پیشرفته و زیرساخت به عنوان کد"، "تهدیدات نوظهور و روز صفر"، "سفارشی‌سازی و تطبیق‌پذیری سناریو"، "تحلیل داده‌های تهدید و بازخورد بلادرنگ"، از مهمترین شاخص‌های اساسی و تاثیرگذار در این مولفه به شمار می‌رود. با تجزیه و تحلیل داده‌های مربوط به اسناد و مدارک و همچنین داده های مصاحبه های انجام شده، با توجه به همگرایی اسناد و مدارک و مصاحبه برای

مولفه سیستم‌های تولید خودکار سناریو، در بخش مصاحبه ها ۲۶ و در بخش اسناد و مدارک ۲۸ عبارت بیانی بدست آمد و در نهایت با پردازش این داده‌ها ۶ شاخص به شرح زیر به عنوان مهمترین گویه‌های تاثیرگذار تعیین گردید.

جدول ۸: شاخص‌های احصا شده در سیستم‌های تولید خودکار سناریو

بعد	مولفه	شاخص
سناریو و محتوا	سیستم‌های تولید خودکار سناریو	۱) ماتریس MITRE-ATT&CK
		۲) هوش مصنوعی و یادگیری ماشین
		۳) مجازی‌سازی پیشرفته و زیرساخت به عنوان کد
		۴) تهدیدات نوظهور و روز صفر
		۵) سفارشی‌سازی و تطبیق‌پذیری سناریو
		۶) تحلیل داده‌های تهدید و بازخورد بلادرنگ

نیروی انسانی: با دسته‌بندی داده‌ها، در بررسی اسناد و مدارک تعداد ۶ مولفه و ۳۴ شاخص و در بررسی مصابه با خبرگان تعداد ۵ مولفه و ۲۹ شاخص احصاء گردید که پس از تقارب و تقاطع داده‌ها و اطلاعات بدست آمده تعداد ۴ مولفه و ۲۵ شاخص به عنوان شاخص‌های اصلی در نظر گرفته شد که خروجی آن در نرم افزار MAXQDA به صورت زیر نمایش داده شده است.



نمودار ۳: شاخص های احصا شده در بعد نیروی انسانی

بررسی مولفه اول حاکی از آنست که امکان شناسایی مولفه‌های نیروی انسانی در سایبر رنج در سامانه بازی جنگ سایبری، با توجه به مولفه تعیین نقش‌ها وجود دارد و بنابر داده‌های پردازش شده "کنترل و دسترسی مبتنی بر نقش"، "مدل شایستگی‌محور"، "تیم قرمز و تیم آبی"، "هوش مصنوعی در تخصیص خودکار نقش"، "تمرین‌های

چندرشته‌ای و همکاری تیمی"، "ارزیابی مداوم عملکرد و بازخورد"، "چالش‌های انسانی و روان‌شناختی"، از مهمترین شاخص‌های اساسی و تاثیرگذار در این مولفه به شمار می‌رود. با تجزیه و تحلیل داده‌های مربوط به اسناد و مدارک و همچنین داده‌های مصاحبه‌های انجام شده، با توجه به همگرایی اسناد و مدارک و مصاحبه برای مولفه تعیین نقش‌ها، در بخش مصاحبه ها ۲۴ و در بخش اسناد و مدارک ۲۹ عبارت بیانی بدست آمد و در نهایت با پردازش این داده‌ها ۷ شاخص به شرح زیر به عنوان مهمترین گویه‌های تاثیرگذار تعیین گردید.

جدول ۹: شاخص‌های احصا شده در تعیین نقش‌ها

بعد	مولفه	شاخص
نیروی انسانی	تعیین نقش‌ها	۱) کنترل و دسترسی مبتنی بر نقش
		۲) مدل شایستگی‌محور
		۳) تیم قرمز و تیم آبی
		۴) هوش مصنوعی در تخصیص خودکار نقش
		۵) تمرین‌های چندرشته‌ای و همکاری تیمی
		۶) ارزیابی مداوم عملکرد و بازخورد
		۷) چالش‌های انسانی و روان‌شناختی

بررسی مولفه دوم حاکی از آنست که امکان شناسایی مولفه‌های نیروی انسانی در سایبر رنج در سامانه بازی جنگ سایبری، با توجه به مولفه سیستم‌های احراز هویت چند عاملی وجود دارد و بنابر داده‌های پردازش شده "عوامل سه‌گانه احراز هویت"، "احرازهویت تطبیقی مبتنی بر ریسک"، "استانداردهای NIST"، "توکن‌های سخت‌افزاری و کلیدهای FIDO2 "، "بیومتریک و احراز هویت رفتاری"، "احراز هویت بدون رمز"، "مقاومت در برابر فیشینگ و مهندسی اجتماعی"، از مهمترین شاخص‌های اساسی و تاثیرگذار در این مولفه به شمار می‌رود. با تجزیه و تحلیل داده‌های مربوط به اسناد و مدارک و همچنین داده های مصاحبه های انجام شده، با توجه به همگرایی اسناد و مدارک و مصاحبه برای مولفه سیستم‌های احراز هویت چندعاملی، در بخش مصاحبه ها ۲۲ و در بخش اسناد و مدارک ۲۶ عبارت بیانی بدست آمد و در نهایت با پردازش این داده‌ها ۷ شاخص به شرح زیر به عنوان مهمترین گویه‌های تاثیرگذار تعیین گردید.

جدول ۱۰: شاخص‌های احصا شده در سیستم‌های احراز هویت چندعاملی

بعد	مولفه	شاخص
نیروی انسانی	سیستم‌های احراز هویت چندعاملی	۱) عوامل سه‌گانه احراز هویت
		۲) احراز هویت تطبیقی مبتنی بر ریسک
		۳) استانداردهای NIST
		۴) توکن‌های سخت‌افزاری و کلیدهای FIDO2
		۵) بیومتریک و احراز هویت رفتاری
		۶) احراز هویت بدون مرز
		۷) مقاومت در برابر فیشینگ و مهندسی اجتماعی

بررسی مولفه سوم حاکی از آنست که امکان شناسایی مولفه‌های نیروی انسانی در سایبر رنج در سامانه بازی جنگ سایبری، با توجه به مولفه ردیابی فعالیت کاربران وجود دارد و بنابر داده‌های پردازش شده "تیم قرمز و تیم آبی"، "تحلیل رفتار و الگوهای ناهنجاری"، "ابزارهای نظارت و ثبت وقایع"، "ارزیابی عملکرد و بازخورد بلادرنگ"، "مجازی‌سازی و شبیه‌سازی سناریو"، از مهمترین شاخص‌های اساسی و تاثیرگذار در این مولفه به شمار می‌رود. با تجزیه و تحلیل داده‌های مربوط به اسناد و مدارک و همچنین داده های مصاحبه های انجام شده، با توجه به همگرایی اسناد و مدارک و مصاحبه برای مولفه ردیابی فعالیت کاربران، در بخش مصاحبه ها ۲۶ و در بخش اسناد و مدارک ۳۰ عبارت بیانی بدست آمد و در نهایت با پردازش این داده‌ها ۵ شاخص به شرح زیر به عنوان مهمترین گویه‌های تاثیرگذار تعیین گردید.

جدول ۱۱: شاخص‌های احصا شده در ردیابی فعالیت کاربران

بعد	مولفه	شاخص
نیروی انسانی	ردیابی فعالیت کاربران	۱) تیم قرمز و تیم آبی
		۲) تحلیل رفتار و الگوهای ناهنجاری
		۳) ابزارهای نظارت و ثبت وقایع
		۴) ارزیابی عملکرد و بازخورد بلادرنگ
		۵) مجازی‌سازی و شبیه‌سازی سناریو

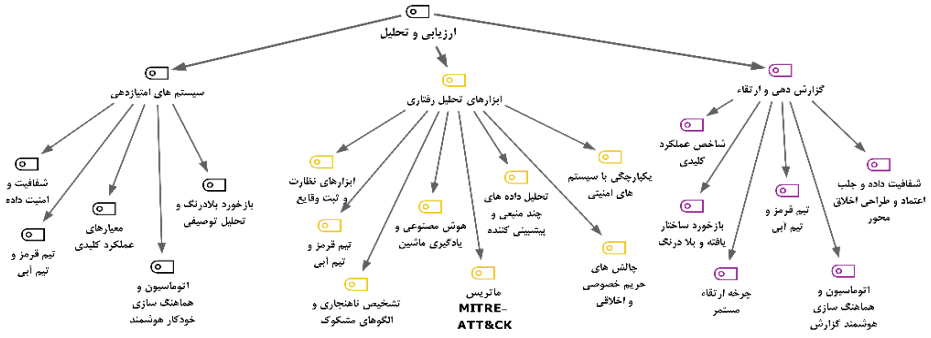
بررسی مولفه چهارم حاکی از آنست که امکان شناسایی مولفه‌های نیروی انسانی در سایبر رنج در سامانه بازی جنگ سایبری ، با توجه به مولفه آموزش و مهارت وجود دارد و بنابر داده‌های پردازش شده "تیم قرمز و تیم آبی"، "شبیه‌سازی پیشرفته و یادگیری

تجربی"، "هوش مصـــنوعی و یادگیری ماشـــین"، "واقعیت مجازی و واقعیت افزوده"، "ارزیابی عملکرد و بازخورد مداوم"، "تصـمیم‌گیری تحت فشـار و مهارت‌های شـناختی"، از مهمترین شـاخص‌های اسـاسـی و تاثیرگذار در این مولفه به شـمار می‌رود. با تجزیه و تحلیل داده‌های مربوط به اســـناد و مدارک و همچنین داده های مصـــاحبه های انجام شـــده، با توجه به همگرایی اسـناد و مدارک و مصـاحبه برای مولفه آموزش و مهارت، در بخش مصـــاحبه ها ۲۹ و در بخش اســـناد و مدارک ۳۳ عبارت بیانی بدســـت آمد و در نهایت با پردازش این داده‌ها ۶ شـــاخص به شـــرح زیر به عنوان مهمترین گویه‌های تاثیرگذار تعیین گردید.

جدول ۱۲: شاخص‌های احصا شده در آموزش و مهارت

بعد	مولفه	شاخص
نیروی انسانی	آموزش و مهارت	۱) تیم قرمز و تیم آبی
		۲) شبیه‌سازی پیشرفته و یادگیری تجربی
		۳) هوش مصنوعی و یادگیری ماشین
		۴) واقعیت مجازی و واقعیت افزوده
		۵) ارزیابی عملکرد و بازخورد مداوم
		۶) تصمیم‌گیری تحت فشار و مهارت‌های شناختی

ارزیابی و تحلیل: با دسـته‌بندی داده‌ها، در بررسـی اسـناد و مدارک تعداد ۵ مولفه و ۲۶ شـاخص و در بررسـی مصـابه با خبرگان تعداد ۴ مولفه و ۲۲ شـاخص احصـاء گردید که پس از تقارب و تقاطع داده‌ها و اطلاعات بدســـت آمده تعداد ۳ مولفه و ۱۹ شـــاخص به عنوان شاخص‌های اصلی در نظر گرفته شد که خروجی آن در نرم افزار MAXQDA به صورت زیر نمایش داده شده است.



نمودار ۴: شاخص های احصا شده در بعد ارزیابی و تحلیل

بررسی مولفه اول حاکی از آنست که امکان شناسایی مولفه‌های ارزیابی و تحلیل در سایبر رنج در سامانه بازی جنگ سایبری، با توجه به مولفه سیستم‌های امتیاز دهی وجود دارد و بنابر داده‌های پردازش شده "تیم قرمز و آبی"، "معیارهای عملکرد کلیدی"، "بازخورد بلادرنگ و تحلیل توصیفی"، "اتوماسیون و هماهنگ‌سازی خودکار و هوشمند"، "چالش شفافیت و امنیت داده"، از مهمترین شاخص‌های اساسی و تاثیرگذار در این مولفه به شمار می‌رود. با تجزیه و تحلیل داده‌های مربوط به اسناد و مدارک و همچنین داده‌های مصاحبه‌های انجام شده، با توجه به همگرایی اسناد و مدارک و مصاحبه برای مولفه سیستم‌های امتیازدهی، در بخش مصاحبه ها ۱۸ و در بخش اسناد و مدارک ۲۲ عبارت بیانی بدست آمد و در نهایت با پردازش این داده‌ها ۵ شاخص به شرح زیر به عنوان مهمترین گویه‌های تاثیرگذار تعیین گردید.

جدول ۱۳: شاخص‌های احصا شده در سیستم‌های امتیازدهی

بعد	مولفه	شاخص
ارزیابی و تحلیل	سیستم‌های امتیازدهی	۱) تیم قرمز و تیم آبی
		۲) معیارهای عملکرد کلیدی
		۳) بازخورد بلادرنگ و تحلیل توصیفی
		۴) اتوماسیون و هماهنگ‌سازی خودکار و هوشمند
		۵) چالش شفافیت و امنیت داده

بررسی مولفه دوم حاکی از آنست که امکان شناسایی مولفه‌های ارزیابی و تحلیل در سایبر رنج در سامانه بازی جنگ سایبری، با توجه به مولفه ابزارهای تحلیل رفتاری وجود دارد و بنابر داده‌های پردازش شده "هوش مصنوعی و یادگیری ماشین"، "تیم قرمز و تیم آبی"، "تشخیص ناهنجاری و الگوهای مشکوک"، "ماتریس MITRE-ATT&CK"، "ابزارهای نظارت و ثبت وقایع"، "تحلیل داده‌های چندمنبعی و پیش‌بینی‌کننده"، "چالش‌های حرم خصوصی و اخلاقی"، "یکپارچگی با سیستم‌های امنیتی"، از مهمترین شاخص‌های اساسی و تاثیرگذار در این مولفه به شمار می‌رود. با تجزیه و تحلیل داده‌های مربوط به اسناد و مدارک و همچنین داده های مصاحبه های انجام شده، با توجه به همگرایی اسناد و مدارک و مصاحبه برای مولفه ابزارهای تحلیل رفتاری، در بخش مصاحبه ها ۲۸ و در بخش اسناد و مدارک ۳۴ عبارت بیانی بدست

آمد و در نهایت با پردازش این داده‌ها ۸ شـــاخص به شـــرح زیر به عنوان مهمترین گویه‌های تاثیرگذار تعیین گردید.

جدول ۱۴: شاخص‌های احصا شده در ابزارهای تحلیل رفتاری

بعد	مولفه	شاخص
ارزیابی و تحلیل	ابزارهای تحلیل رفتاری	۱) هوش مصنوعی و یادگیری ماشین
		۲) تیم قرمز و تیم آبی
		۳) تشخیص ناهنجاری و الگوهای مشکوک
		۴) ماتریس MITRE-ATT&CK
		۵) ابزارهای نظارت و ثبت وقایع
		۶) تحلیل داده‌های چندمنبعی و پیشبینی‌کننده
		۷) چالش‌های حریم خصوصی و اخلاقی
		۸) یکپارچگی با سیستم‌های امنیتی

بررسـی مولفه سـوم حاکی از آنسـت که امکان شـناسـایی مولفه‌های ارزیابی و تحلیل در سـایبر رنج در سـامانه بازی جنگ سـایبری، با توجه به مولفه گزارش‌دهی و ارتقاء وجود دارد و بنابر داده‌های پردازش شـــده "چرخه ارتقاء مســـتمر"، "تیم قرمز و تیم آبی"، "بازخورد ســـاختاریافته و بلادرنگ"، "شـــاخص عملکرد کلیدی"، "اتوماســـیون و هماهنگ‌ســـازی خودکار هوشـــمند گزارش"، "شـــفافیت داده و جلب اعتماد و طراحی اخلاق‌محور"، از مهمترین شاخص‌های اساسی و تاثیرگذار در این مولفه است. با تجزیه و تحلیل داده‌های مربوط به اســـناد و مدارک و همچنین داده های مصـــاحبه های انجام شـــده، با توجه به اســـناد مدارک و مصـــاحبه برای مولفه گزارش‌دهی و ارتقاء، در بخش مصـاحبه ها ۲۰ و در بخش اسـناد و مدارک ۲۳ عبارت بیانی بدسـت آمد و در نهایت با پردازش این داده‌ها ۶ شاخص به شرح زیر به عنوان مهمترین گویه‌های تاثیرگذار تعیین گردید.

جدول ۱۵: شاخص‌های احصا شده در گزارش‌دهی و ارتقاء

بعد	مولفه	شاخص
ارزیابی و تحلیل	گزارش‌دهی وارتقاء	۱) چرخه ارتقاء مستمر
		۲) تیم قرمز و تیم آبی
		۳) بازخورد ساختاریافته و بلادرنگ
		۴) شاخص عملکرد کلیدی

۵) اتوماسیون و هماهنگ‌سازی خودکار هوشمند گزارش		
۶) شفافیت داده و جلب اعتماد و طراحی اخلاق‌محور		

تجزیه و تحلیل کمی داده‌ها:

در بین شاخص‌های مطرح‌شده در بعد زیرساخت‌های مورد نیاز، حسگرهای حرکتی و ردیابی چشم، بیشترین اولویت و شاخص هدست‌های واقعیت مجازی و واقعیت افزوده، کمترین اولویت را در شناسایی مولفه‌های سایبر رنج در سامانه بازی جنگ سایبری دارد.

جدول ۱۶: آمار توصیفی بعد زیرساخت‌های مورد نیاز

	تعداد	محدوده	مجموع	میانگین	انحراف معیار	واریانس
شبیه سازی واقع گرایانه تهدیدات پیشرفته	۳۷	۴.۰۰	۱۵۱.۰۰	۴.۰۸۱۱	۱.۰۱۰۴۶	۱.۰۲۱
مجازی سازی و ایزوله سازی سناریو ها	۳۷	۴.۰۰	۱۴۰.۰۰	۳.۷۸۳۸	۱.۲۵۰۲۳	۱.۵۶۳
ادغام هوش مصنوعی در تشخیص و پیش بینی	۳۷	۴.۰۰	۱۵۰.۰۰	۴.۰۵۴۱	۱.۱۲۹۰۶	۱.۲۷۵
امنیت داده ها و حفظ حریم خصوصی	۳۷	۴.۰۰	۱۴۳.۰۰	۳.۸۶۴۹	۱.۰۸۴۲۹	۱.۱۷۶
ارزیابی عملکرد و بازخورد مداوم	۳۷	۴.۰۰	۱۴۰.۰۰	۳.۷۸۳۸	۱.۱۸۱۶۹	۱.۳۹۶
استانداردسازی و یکپارچه سازی با زیرساخت ها	۳۷	۴.۰۰	۱۵۳.۰۰	۴.۱۳۵۱	۱.۱۵۸۵۹	۱.۳۴۲
مقیاس پذیری با فناوری ابری	۳۷	۴.۰۰	۱۴۸.۰۰	۴.۰۰۰۰	۱.۱۳۰۳۹	۱.۲۷۸
شبیه سازی پویا و مقیاس پذیر	۳۷	۴.۰۰	۱۵۴.۰۰	۴.۱۶۲۲	۱.۱۴۲۹۴	۱.۳۰۶
پردازنده های گرافیکی	۳۷	۴.۰۰	۱۴۴.۰۰	۳.۸۹۱۹	۱.۱۷۳۴۰	۱.۳۷۷
آرایه های دروازه ای قابل برنامه ریزی	۳۷	۴.۰۰	۱۵۴.۰۰	۴.۱۶۲۲	.۹۵۷۸۲	.۹۱۷
ذخیره سازی پر سرعت	۳۷	۴.۰۰	۱۴۴.۰۰	۳.۸۹۱۹	۱.۱۰۰۱۰	۱.۲۱۰
پردازنده های کوانتومی	۳۷	۴.۰۰	۱۵۰.۰۰	۴.۰۵۴۱	۱.۲۲۳۵۲	۱.۴۹۷
یکپارچگی و هم افزایی با نرم افزارهای اختصاصی	۳۷	۴.۰۰	۱۳۰.۰۰	۳.۵۱۳۵	۱.۳۴۶۲۲	۱.۸۱۲
شبکه های نرم افزار محور	۳۷	۴.۰۰	۱۴۸.۰۰	۴.۰۰۰۰	۱.۱۵۴۷۰	۱.۳۳۳
مجازی سازی عملکرد شبکه	۳۷	۴.۰۰	۱۴۹.۰۰	۴.۰۲۷۰	۱.۱۱۷۷۰	۱.۲۴۹
محاسبات لبه ای	۳۷	۴.۰۰	۱۵۴.۰۰	۴.۱۶۲۲	۱.۰۱۴۱۶	۱.۰۲۹
خودکارسازی تخصیص منابع	۳۷	۴.۰۰	۱۴۸.۰۰	۴.۰۰۰۰	۱.۰۰۰۰۰	۱.۰۰۰
شبکه های کوانتومی و ارتباطات امن کوانتومی	۳۷	۴.۰۰	۱۶۴.۰۰	۴.۴۳۲۴	.۹۵۸۶۰	.۹۱۹
شبیه سازی غوطه ور و تعاملی	۳۷	۴.۰۰	۱۵۱.۰۰	۴.۰۸۱۱	.۸۲۹۲۷	.۶۸۸
هدست های واقعیت مجازی و واقعیت افزوده	۳۷	۴.۰۰	۱۲۸.۰۰	۳.۴۵۹۵	۱.۱۴۴۹۱	۱.۳۱۱
بازی سازی	۳۷	۴.۰۰	۱۵۱.۰۰	۴.۰۸۱۱	۱.۱۱۵۰۱	۱.۲۴۳
متاورس و محیط های جهانی	۳۷	۴.۰۰	۱۵۱.۰۰	۴.۰۸۱۱	.۹۸۲۵۸	.۹۶۵

حسگر های حرکتی و ردیابی چشم	۳۷	۴.۰۰	۱۵۸.۰۰	۴.۲۷۰۳	۱.۱۲۱۷۲	۱.۲۵۸
چالش های فنی و مهارتی	۳۷	۴.۰۰	۱۵۸.۰۰	۴.۲۷۰۳	۱.۰۹۶۶۸	۱.۲۰۳
Valid N (listwise)	۳۷					

در بین شاخص‌های مطرح‌شده در بعد سناریو و محتوا، بازخورد ساختار یافته و بلادرنگ، بیشترین اولویت و شاخص‌های تیم قرمز و تیم آبی، کمترین اولویت را در شناسایی مولفه‌های سایبر رنج در سامانه بازی جنگ سایبری دارد.

جدول ۱۷: آمار توصیفی بعد سناریو و محتوا

	تعداد	محدوده	مجموع	میانگین	انحراف معیار	واریانس
ماتریسMITRE-ATT&CK	۳۷	۴.۰۰	۱۵۷.۰۰	۴.۲۴۳۲	۱.۰۳۸۳۱	۱.۰۷۸
شبیه سازی چند لایه و پویا	۳۷	۴.۰۰	۱۵۸.۰۰	۴.۲۷۰۳	۱.۱۹۳۷۰	۱.۴۲۵
چرخه عمر حمله	۳۷	۴.۰۰	۱۵۶.۰۰	۴.۲۱۶۲	۱.۱۳۳۷۰	۱.۲۸۵
تمرین های تیم قرمز در برابر تیم آبی	۳۷	۴.۰۰	۱۶۰.۰۰	۴.۳۲۴۳	۱.۰۸۱۵۱	۱.۱۷۰
ارزیابی عملکرد و معیارهای کلیدی حمله	۳۷	۴.۰۰	۱۴۹.۰۰	۴.۰۲۷۰	۱.۲۳۵۷۳	۱.۵۲۷
اتوماسیون و تکرار پذیری سناریو	۳۷	۴.۰۰	۱۵۹.۰۰	۴.۲۹۷۳	.۹۹۶۲۴	.۹۹۲
ماتریسMITRE-ATT&CK	۳۷	۴.۰۰	۱۶۳.۰۰	۴.۴۰۵۴	۱.۰۱۲۶۸	۱.۰۲۶
شبیه سازی چند لایه و پویا	۳۷	۴.۰۰	۱۴۶.۰۰	۳.۹۴۵۹	۱.۱۰۴۱۸	۱.۲۱۹
تمرین های تیم آبی در برابر تیم قرمز	۳۷	۴.۰۰	۱۴۸.۰۰	۴.۰۰۰۰	۱.۰۸۰۱۲	۱.۱۶۷
شناسایی و تشخیص نفوذ	۳۷	۴.۰۰	۱۵۹.۰۰	۴.۲۹۷۳	۱.۰۷۶۶۴	۱.۱۵۹
پاسخ به حادثه و بازیابی	۳۷	۴.۰۰	۱۵۹.۰۰	۴.۲۹۷۳	۱.۱۲۷۰۶	۱.۲۷۰
ارزیابی عملکرد و معیارهای کلیدی دفاع	۳۷	۴.۰۰	۱۵۳.۰۰	۴.۱۳۵۱	۱.۱۸۲۳۳	۱.۳۹۸
ماتریسMITRE-ATT&CK	۳۷	۴.۰۰	۱۵۶.۰۰	۴.۲۱۶۲	۱.۲۲۷۸۱	۱.۵۰۸
هوش مصنوعی و یادگیری ماشین	۳۷	۴.۰۰	۱۵۱.۰۰	۴.۰۸۱۱	۱.۲۵۵۶۲	۱.۵۷۷
مجازی سازی پیشرفته و زیرساخت	۳۷	۴.۰۰	۱۶۰.۰۰	۴.۳۲۴۳	۱.۰۸۱۵۱	۱.۱۷۰
تهدیدات نوظهور و روز صفر	۳۷	۳.۰۰	۱۴۶.۰۰	۳.۹۴۵۹	۱.۱۲۹۰۶	۱.۲۷۵
سفارشی سازی و تطبیق پذیری سناریو	۳۷	۴.۰۰	۱۵۸.۰۰	۴.۲۷۰۳	۱.۱۴۶۲۲	۱.۳۱۴
تحلیل داده های تهدید و بازخورد بلادرنگ	۳۷	۴.۰۰	۱۶۳.۰۰	۴.۴۰۵۴	.۹۸۴۸۷	.۹۷۰
Valid N (listwise)	۳۷					

در بین شـــاخص‌های مطرح‌شـــده در بعد نیروی انســـانی، مقاومت در برابر فیشـــینگ و مهندسی اجتماعی، بیشترین اولویت و شاخص واقعیت مجازی و واقعیت افزوده، کمترین اولویت را در شناسایی مولفه‌های سایبر رنج در سامانه بازی جنگ سایبری دارد.

جدول ۱۸: آمار توصیفی بعد نیروی انسانی

	تعداد	محدوده	مجموع	میانگین	انحراف معیار	واریانس
کنترل و دسترسی مبتنی بر نقش	۳۷	۴.۰۰	۱۴۹.۰۰	۴.۰۲۷۰	۱.۰۱۳۴۲	۱.۰۲۷
مدل شایستگی محور	۳۷	۴.۰۰	۱۴۷.۰۰	۳.۹۷۳۰	۱.۰۶۶۸۴	۱.۱۳۸
تیم قرمز و تیم آبی	۳۷	۴.۰۰	۱۵۵.۰۰	۴.۱۸۹۲	۱.۱۲۶۴۰	۱.۲۶۹
هوش مصنوعی در تخصیص خودکار نقش	۳۷	۴.۰۰	۱۵۹.۰۰	۴.۲۹۷۳	۱.۰۷۶۶۴	۱.۱۵۹
تمرین های چند رشته ای و همکاری تیمی	۳۷	۴.۰۰	۱۵۷.۰۰	۴.۲۴۳۲	۱.۰۹۰۵۰	۱.۱۸۹
ارزیابی مداوم عملکرد و بازخورد	۳۷	۴.۰۰	۱۶۰.۰۰	۴.۳۲۴۳	۱.۰۵۵۵۲	۱.۱۱۴
چالش های انسانی و روان شناختی	۳۷	۳.۰۰	۱۵۵.۰۰	۴.۱۸۹۲	۱.۱۰۱۴۶	۱.۲۱۳
عوامل سه گانه احراز هویت	۳۷	۴.۰۰	۱۵۴.۰۰	۴.۱۶۲۲	۱.۲۵۸۶۰	۱.۵۸۴
احراز هویت تطبیقی مبتنی بر ریسک	۳۷	۴.۰۰	۱۴۸.۰۰	۴.۰۰۰۰	۱.۲۲۴۷۴	۱.۵۰۰
استانداردهایNIST	۳۷	۴.۰۰	۱۵۸.۰۰	۴.۲۷۰۳	۱.۰۷۱۰۵	۱.۱۴۷
توکن های سخت افزاری و کلیدهایFIDO2	۳۷	۴.۰۰	۱۵۱.۰۰	۴.۰۸۱۱	۱.۲۳۳۳۰	۱.۵۲۱
بیومتریک و احراز هویت رفتاری	۳۷	۴.۰۰	۱۵۴.۰۰	۴.۱۶۲۲	۱.۰۴۱۱۹	۱.۰۸۴
احراز هویت بدون رمز	۳۷	۳.۰۰	۱۵۱.۰۰	۴.۰۸۱۱	.۹۵۳۸۹	.۹۱۰
مقاومت در برابر فیشینگ و مهندسی اجتماعی	۳۷	۴.۰۰	۱۶۰.۰۰	۴.۳۲۴۳	۱.۰۰۱۵۰	۱.۰۰۳
تیم قرمز و تیم آبی	۳۷	۴.۰۰	۱۵۷.۰۰	۴.۲۴۳۲	۱.۱۴۰۳۱	۱.۳۰۰
تحلیل رفتار و الگوهای ناهنجاری	۳۷	۴.۰۰	۱۵۰.۰۰	۴.۰۵۴۱	۱.۱۰۴۱۸	۱.۲۱۹
ابزارهای نظارت و ثبت وقایع	۳۷	۳.۰۰	۱۶۲.۰۰	۴.۳۷۸۴	.۹۸۱۸۲	.۹۶۴
ارزیابی عملکرد و بازخورد بلادرنگ	۳۷	۴.۰۰	۱۵۴.۰۰	۴.۱۶۲۲	۱.۱۱۸۳۷	۱.۲۵۱
مجازی سازی و شبیه سازی سناریو	۳۷	۴.۰۰	۱۵۶.۰۰	۴.۲۱۶۲	۱.۲۰۴۹۷	۱.۴۵۲
تیم قرمز و تیم آبی	۳۷	۴.۰۰	۱۴۴.۰۰	۳.۸۹۱۹	۱.۲۸۶۳۳	۱.۶۵۵
شبیه سازی پیشرفته و یادگیری تجربی	۳۷	۴.۰۰	۱۵۶.۰۰	۴.۲۱۶۲	۱.۰۰۳۷۵	۱.۰۰۸
هوش مصنوعی و یادگیری ماشین	۳۷	۴.۰۰	۱۵۶.۰۰	۴.۲۱۶۲	.۹۱۶۹۷	.۸۴۱
واقعیت مجازی و واقعیت افزوده	۳۷	۴.۰۰	۱۴۲.۰۰	۳.۸۳۷۸	۱.۲۱۳۶۶	۱.۴۷۳
ارزیابی عملکرد و بازخورد مداوم	۳۷	۴.۰۰	۱۵۹.۰۰	۴.۲۹۷۳	.۹۹۶۲۴	.۹۹۲
تصمیم گیری تحت فشار و مهارت های شناختی	۳۷	۴.۰۰	۱۵۸.۰۰	۴.۲۷۰۳	۱.۰۹۶۶۸	۱.۲۰۳

Valid N (listwise)	۳۷					

از دیدگاه مخاطبان در بین شاخص‌های مطرح‌شده در بعد ارزیابی و تحلیل، بازخورد ساختار یافته و بلادرنگ، ماتریسMITRE-ATT&CK بیشترین اولویت است و شاخص‌های تیم قرمز و تیم آبی و چالش شفافیت و امنیت داده، کمترین اولویت را در شناسایی مولفه‌های سایبر رنج در سامانه بازی جنگ سایبری دارد.

جدول ۱۹: آمار توصیفی بعد ارزیابی و تحلیل

	تعداد	محدوده	مجموع	میانگین	انحراف معیار	واریانس
تیم قرمز و تیم آبی	۳۷	۴.۰۰	۱۵۸.۰۰	۴.۲۷۰۳	۱.۰۴۴۷۹	۱.۰۹۲
معیار های عملکرد کلیدی	۳۷	۴.۰۰	۱۵۳.۰۰	۴.۱۳۵۱	۱.۳۱۵۷۶	۱.۷۳۱
اتوماسیون و هماهنگ سازی خودکار هوشمند	۳۷	۴.۰۰	۱۵۱.۰۰	۴.۰۸۱۱	.۹۵۳۸۹	.۹۱۰
چالش شفافیت و امنیت داده	۳۷	۴.۰۰	۱۲۵.۰۰	۳.۳۷۸۴	۱.۳۱۹۷۵	۱.۷۴۲
بازخورد بلادرنگ و تحلیل توصیفی	۳۷	۴.۰۰	۱۵۴.۰۰	۴.۱۶۲۲	۱.۰۶۷۵۴	۱.۱۴۰
هوش مصنوعی و یادگیری ماشین	۳۷	۴.۰۰	۱۵۰.۰۰	۴.۰۵۴۱	.۹۴۱۲۲	.۸۸۶
تیم آبی و تیم قرمز	۳۷	۴.۰۰	۱۶۲.۰۰	۴.۳۷۸۴	۱.۰۰۹۷۱	۱.۰۲۰
تشخیص ناهنجاری و الگوهای مشکوک	۳۷	۴.۰۰	۱۵۰.۰۰	۴.۰۵۴۱	۱.۳۱۱۱۹	۱.۷۱۹
ماتریسMITRE-ATT&CK	۳۷	۴.۰۰	۱۵۶.۰۰	۴.۲۱۶۲	۱.۲۰۴۹۷	۱.۴۵۲
ابزارهای نظارت و ثبت وقایع	۳۷	۴.۰۰	۱۵۴.۰۰	۴.۱۶۲۲	۱.۲۳۶۳۴	۱.۵۲۹
تحلیل داده های چند منبعی	۳۷	۴.۰۰	۱۴۳.۰۰	۳.۸۶۴۹	۱.۳۷۷۶۴	۱.۸۹۸
چالش های حریم خصوصی و اخلاقی	۳۷	۴.۰۰	۱۵۳.۰۰	۴.۱۳۵۱	۱.۲۷۲۸۴	۱.۶۲۰
یکپارچگی با سیستم های امنیتی	۳۷	۴.۰۰	۱۵۱.۰۰	۴.۰۸۱۱	۱.۳۲۰۳۲	۱.۷۴۳
چرخه ارتقاء مستمر	۳۷	۴.۰۰	۱۵۲.۰۰	۴.۱۰۸۱	۱.۱۰۰۱۰	۱.۲۱۰
تیم قرمز و تیم آبی	۳۷	۴.۰۰	۱۲۴.۰۰	۳.۳۵۱۴	۱.۴۷۶۰۳	۲.۱۷۹
بازخورد ساختار یافته و بلادرنگ	۳۷	۴.۰۰	۱۵۷.۰۰	۴.۲۴۳۲	۱.۰۶۴۷۲	۱.۱۳۴
شاخص عملکرد کلیدی	۳۷	۴.۰۰	۱۴۲.۰۰	۳.۸۳۷۸	۱.۱۱۸۳۷	۱.۲۵۱
اتوماسیون و هماهنگ سازی خودکار هوشمند	۳۷	۳.۰۰	۱۵۴.۰۰	۴.۱۶۲۲	۱.۰۱۴۱۶	۱.۰۲۹
شفافیت داده و جلب اعتماد	۳۷	۴.۰۰	۱۴۹.۰۰	۴.۰۲۷۰	۱.۳۲۲۵۹	۱.۷۴۹
Valid N (listwise)	۳۷					

بررسی اطلاعات استخراج شده از مطالعه اسناد و مدارک و پاسخ مصاحبه‌شوندگان نشان می‌دهد، در بعد زیرساخت‌های مورد نیاز ۴ مولفه و ۲۴ شاخص، در بعد سناریو و محتوا

۳ مولفه و ۱۸ شاخص، در بعد نیروی انسانی ۴ مولفه و ۲۵ شاخص و در بعد ارزیابی و تحلیل ۳ مولفه و ۱۹ شاخص توسط پژوهشگر شناسایی شد.

جدول ۲۰: جمع‌بندی نهایی اهداف تحقیق

موضوع	بعد	مولفه	شاخص	میانگین	درصد پاسخ گویی
شناسایی مولفه‌های سایبر رنج در سامانه بازی جنگ سایبری	زیرساخت های مورد نیاز	نرم‌افزارهای اختصاصی	۷	۳/۹۷	۷۵
		سخت‌افزارهای اختصاصی	۶		
		زیرساخت شبکه سخت‌افزار و نرم‌افزار	۵		
		واقعیت مجازی و واقعیت افزوده	۶		
	سناریو و محتوا	فرآیند سناریو حمله	۶	۴/۲۴	۸۳
		فرآیند سناریو دفاع	۶		
		سیستم‌های تولید خودکار سناریو	۶		
	نیروی انسانی	تعیین نقش‌ها	۷	۴/۲۲	۸۲
		سیستم‌های احراز هویت چندعاملی	۷		
		ردیابی فعالیت کاربران	۵		
		آموزش و مهارت	۶		
	ارزیابی و تحلیل	سیستم‌های امتیازدهی	۵	۴/۰۵	۷۸
		ابزارهای تحلیل رفتاری	۸		
		گزارش‌دهی و ارتقاء	۶		

نتیجه‌گیری و پیشنهادها

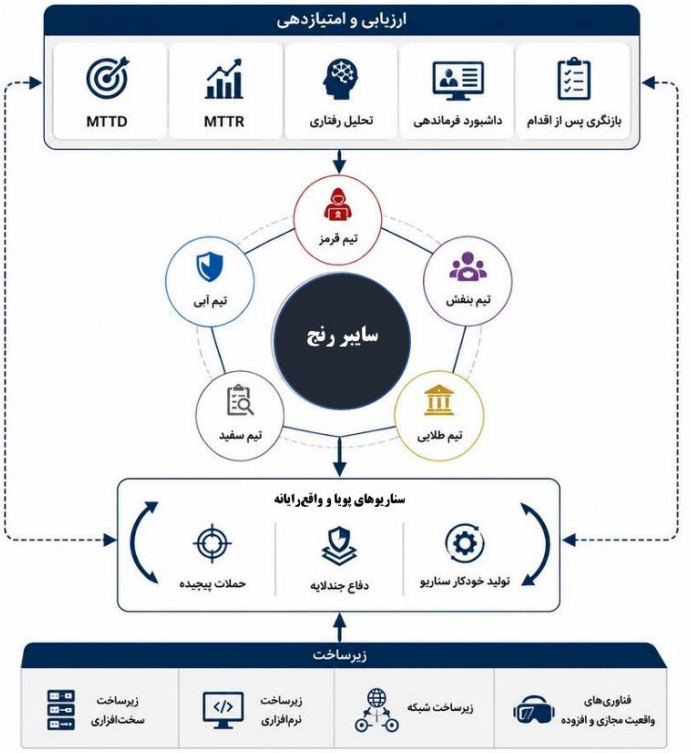
نتیجه‌گیری:

نتایج تحقیق نشان می‌دهد، ایجاد یک سایبر رنج کارآمد و نزدیک به واقعیت، مستلزم طراحی و پیاده‌سازی چهار لایه زیرساختی اصلی است که به‌صورت یکپارچه و هم‌افزا عمل می‌کنند. زیرساخت سخت‌افزاری، زیرساخت نرم‌افزاری، زیرساخت شبکه سخت‌افزار و نرم‌افزار و فناوری‌های واقعیت مجازی و واقعیت افزوده. این مولفه‌ها نه تنها به‌عنوان بستر فنی سایبر رنج عمل می‌کنند، بلکه مهم‌ترین عامل در ایجاد حس حضور، واقع‌گرایی سناریوها و قابلیت تکرارپذیری تمرین‌های سایبری به شمار می‌روند.

قلب تپنده‌ی هر سایبر رنج مؤثر، نه صرفاً زیرساخت فنی، بلکه سناریوهای پویا، واقع‌گرایانه و قابل تطبیق است. این سناریوها باید به‌گونه‌ای طراحی شوند که همزمان قابلیت اجرای فرآیندهای حمله‌ی پیچیده، فرآیندهای دفاع چندلایه و پویا و مهم‌تر از همه، تولید خودکار و هوشمند سناریوهای جدید را داشته باشند.

نیروی انسانی فراتر از نقش بهره‌بردار ساده، به‌عنوان مهم‌ترین عامل تعیین‌کننده موفقیت یا شکست کلی سایبر رنج ملی مطرح است. این مولفه که برخلاف زیرساخت و سناریو ماهیتی کاملاً پویا، حساس به مسایل امنیتی و نیازمند مدیریت دقیق هویت، رفتار و شایستگی دارد، نخستین مولفه کلیدی متناظر با ضرورت تعریف نقش‌های استاندارد و دقیق به‌صورت سلسله‌مراتبی و وظیفه‌محور است که پنج نقش اصلی و غیرقابل حذف دارد. تیم قرمز برای اجرای حملات واقعی، تیم آبی برای دفاع فعال، تیم بنفش برای همکاری مستمر میان قرمز و آبی، تیم سفید به‌عنوان ناظر، داور و طراح سناریوی کلان و تیم طلایی به‌عنوان هسته فرماندهی راهبردی و تصمیم‌گیرنده نهایی.

سیستم‌های امتیازدهی، به عنوان یکی از ارکان اساسی اندازه‌گیری و بهبود عملکرد در آزمون‌ها و تمرین‌های امنیت سایبری، با طراحی مبتنی بر مدل‌های بازی‌سازی و مجموعه‌ای از معیارهای کلیدی عملکرد مانند MTTD وMTTR ، امکان سنجش کمّی و کیفی توانمندی‌های تیم‌های قرمز، آبی و بنفش را فراهم می‌آورند. ابزارهای تحلیل رفتاری پیشرفته به ردیابی و تحلیل رفتارهای دفاعی و تهاجمی در شرایط فشار و استرس کمک می‌کنند. گزارش‌دهی به‌عنوان یک مولفه پویا، نقش محوری در ارائه گزارش‌های بلادرنگ و تحلیل‌های ریشه‌ای از طریق داشبوردهای فرماندهی و فرآیندهای بازنگری پس از اقدام، ایفا می‌کند.



شکل ۲: روابط متغیرهای پژوهش

پیشنهاد ها:

۱. بررسی تأثیر هوش مصنوعی بر تولید سناریوهای پویا با تمرکز بر ادغام الگوریتم‌های یادگیری ماشین در فرآیند تولید خودکار سناریوهای تمرینی سایبر رنج به‌عنوان یک جهت‌گیری نوآورانه.

۲. ارزیابی نقش واقعیت مجازی و افزوده در آموزش نیروی انسانی با تمرکز بر بهره‌گیری از فناوری‌های واقعیت مجازی و واقعیت افزوده در طراحی محیط‌های تمرینی تیم قرمز و آبی در سایبر رنج به‌عنوان یک رویکرد نوین.

۳. انجام پژوهشی متمرکز بر ارزیابی و ارتقای مقاومت سایبر رنج‌های بومی در برابر تهدیدات محاسبات کوانتومی به‌عنوان یک جهت‌گیری آینده‌نگرانه.

۴. انجام پژوهشی متمرکز بر بررسی و بهینه‌سازی همکاری انسان و هوش مصنوعی در تیم‌های دفاعی آبی سایبر رنج.

۵. انجام پژوهشی جامع در زمینه تحلیل هزینه و فایده، استقرار و بهره‌برداری از سایبر رنج در ساختار نیروهای نظامی به‌عنوان یک ضرورت مدیریتی و بودجه‌ای.
۶. انجام پژوهشی متمرکز بر شبیه‌سازی و مقابله با حملات زنجیره‌ای علیه زیرساخت‌های حیاتی در محیط سایبر رنج به‌عنوان یک اولویت راهبردی.
۷. انجام پژوهشی متمرکز بر بهره‌گیری از فناوری داده‌های بزرگ در تحلیل رفتاری کاربران در محیط سایبر رنج به‌عنوان یک رویکرد تحلیلی پیشرفته پیشنهاد می‌گردد.

قدردانی

از کلیه استادان دانشگاه فرماندهی و ستاد آجا و نیز کلیه اندیشمندان و پژوهشگران بویژه استادان محترم راهنما و مشاور که در انجام مراحل این پژوهش، خالصانه دیدگاه‌ها و نقطه‌نظرات علمی و کارشناسی خود را ارائه نمودند، تشکر و قدردانی می‌شود.

منابع

- Ask, T. F., Knox, B. J., Lugo, R. G., Hoffmann, L., & Sütterlin, S. (2023, June). Gamification as a neuroergonomic approach to improving interpersonal situational awareness in cyber defense. In *Frontiers in Education* (Vol. 8, p. 988043). Frontiers Media SA. Volume 8 - 2023 | https://doi.org/10.3389/feduc.2023.988043
- Banks, D. E. (2024). The Methodological Machinery of Wargaming: A Path toward Discovering Wargaming's Epistemological Foundations. *International Studies Review*, *26*(1), viae002. https://doi.org/10.1093/isr/viae002
- Costa, G., Russo, E., & Armando, A. (2020). Automating the generation of cyber range virtual scenarios with VSDL. *arXiv preprint arXiv:2001.06681*. DOI: 10.22667/JOWUA.2022.03.31.0033
- Glas, M., Messmann, G., & Pernul, G. (2024). Complex yet attainable? An interdisciplinary approach to designing better cyber range exercises. *Computers & Security*, *144*, 103965. https://doi.org/10.1016/j.cose.2024.103965
- Harris, B. N., & Freeman, S. (2023). Crossing a Virtual Divide: Wargaming as a Remote Teaching Tool. *PS: Political Science & Politics*, *56*(3), 431-437. https://doi.org/10.1017/S1049096523000045
- Hirst, A. (2022). States of play: evaluating the renaissance in US military wargaming. *Critical Military Studies*, *8*(1), 1-21. https://doi.org/10.1080/23337486.2019.1707497
- Jelo, M., & Helebrandt, P. (2022, October). Gamification of cyber ranges in cybersecurity education. In *2022 20th International Conference on*

Emerging eLearning Technologies and Applications (ICETA) (pp. 280-285). IEEE. DOI: 10.1109/ICETA57911.2022.9974714
- Katsantonis, M. N., Manikas, A., Mavridis, I., & Gritzalis, D. (2023). Cyber range design framework for cyber security education and training. *International Journal of Information Security*, *22*(4), 1005-1027. https://doi.org/10.1007/s10207-023-00680-4
- Karjalainen, M., & Kokkonen, T. (2020, September). Comprehensive cyber arena; the next generation cyber range. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 11-16). IEEE. DOI: 10.1109/EuroSPW51379.2020.00011
- Khan, M. T. (2024). The Future of Space Wargaming: Conflicting or Reasonable With What's Ahead?. *Space Education & Strategic Applications*, *4*(4). doi: 10.18278/sesa.4.4.2
- Lates, I. (2022). Cyber Ranges Implementation Methodology. In *Proceedings of the International Conference on Business Excellence* (Vol. 16, No. 1, pp. 1259-1269). DOI: 10.2478/picbe2022.0115
- Slavchev, V. (2021). Using Cyber Ranges in Cybersecurity Management Educational Programmes. *Information & Security*, *50*(2), 161-168. https://doi.org/10.11610/isij.5007
- Sarjakivi, p., ihanus, j., & moilanen, p. (2024, june). Using wargaming to model cyber defense decision-making: observation-based research in locked shields. In *european conference on cyber warfare and security* (vol. 23, no. 1, pp. 457-464). https://doi.org/10.34190/eccws.23.1.2270