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

Factors Influencing the Cyber Range: A Framework for Preparing and Simulating Future Cyber-Based Battles

Mohammad Ghasemi Tadavani [1] | Mohammad Taghi Partovi [2]✉ | Hamid Bigdeli [2] | Mojtaba Ramezanzadeh[2]

1- PHD Student of Defense Management, IRI Military Command and Staff University, Tehran, Iran.
E-mail: m.ghasemi@casu.ac.ir
2- Assistant Professor of Operations Research, IRI Military Command and Staff University, Tehran, Iran.
E-mail: m.partovi@casu.ac.ir
3- Associate Professor of Operations Research, IRI Military Command and Staff University. Tehran. Iran.
E-mail: h.bigdeli@casu.ac.ir
4- Assistant Professor of Cyber, IRI Military Command and Staff University, Tehran, Iran.
E-mail: m.ramezanzadeh@casu.ac.ir

Article Info

Article type:
Research Article

Article history:
Received:
2025-12-10
Received in revised form:
2026-2-6
Accepted:
2026-2-7
Published online:
2026-5-22

Keywords:
Cyber range layer, Physical layer, Virtual layer, Command/management layer

ABSTRACT

Background and Objective: The rapid integration of information technologies into the operational domains of land, sea, air, and space has transformed the battlefield into a multilayered, data-driven environment that depends on human–machine interaction. The cyber range, as a critical infrastructure, enables force training, doctrinal testing, and improved decision-making. The objective of this study is to analyze the effects of the physical, virtual, and command/management layers on the effectiveness of the cyber range.

Methods: This research is descriptive in nature and employs a mixed-methods approach. The qualitative analysis involved reviewing specialized documents and conducting expert interviews. The quantitative analysis was carried out using correlation analysis and multivariate regression in order to determine the extent to which each layer influences the dependent variable.

Findings: The results indicate that the physical, virtual and command/management layers all have positive, direct, and statistically significant relationships with the cyber range. The physical layer, with the highest standardized beta coefficient, was identified as the strongest predictor, emphasizing the critical role of infrastructure and hardware in ensuring realism and stability. The virtual and command layers respectively contribute to enhancing interactivity and the effective utilization of the range. The coefficient of determination ($R^2 = 0.941$) demonstrates the high explanatory power of the proposed model.

Conclusions: The success of cyber ranges requires integration and synergy among all three layers. These findings suggest that the design and development of cyber ranges are not only a technological necessity, but also a strategic imperative for readiness, deterrence, and superiority in future multi-domain warfare.

Cite this article: Ghasemi Tadavani,M , Partovi,M T , Bigdeli,H and Ramezanzadeh,M . (2026). Factors Influencing the Cyber Range: A Framework for Preparing and Simulating Future Cyber-Based Battles. (e734033). *Defensive Future Studies*, *11*(40), 203-238.

DOI: https://doi.org/10.22034/dfsr.2026.2080098.1990

Publisher: IRI Military Command and Staff University

Extended Abstract

INTRODUCTION

The research problem addresses the growing inadequacy of traditional wargaming models in representing the multi-domain and cyber-integrated nature of contemporary warfare. With cyberspace emerging as a decisive arena influencing command, control, perception, and decision-making processes, failure to incorporate cyber dynamics results in strategically misleading outcomes. This study is significant because it proposes a reconceptualized cyber wargaming framework capable of simulating cognitive, informational, and infrastructural interactions within future conflict environments. By integrating cyber variables into scenario design and decision matrices, the research enhances predictive accuracy, supports doctrinal innovation, and strengthens the capacity of military decision-makers to anticipate and manage complex, hybrid threats.

METHODOLOGY

This applied study employed a descriptive mixed-methods design integrating grounded theory and quantitative correlation–regression analysis. Qualitative data were collected through semi-structured interviews with ten purposefully selected experts in cyber operations and wargaming, complemented by a comprehensive documentary review of scientific sources. The data were systematically analyzed in ATLAS.ti using the Strauss and Corbin coding paradigm, including open, axial, and selective coding, leading to the development of a conceptual model. For quantitative validation, a Likert-scale questionnaire was distributed among 77 specialists. Content validity was confirmed using Lawshe's CVR method. Statistical analysis in SPSS included multiple linear regression, ANOVA, and standardized beta coefficients to determine the strength and direction of relationships among variables.

RESULT

The qualitative analysis, conducted through a grounded theory approach, revealed that the effective design and implementation of a cyber training field for wargaming purposes is fundamentally dependent on a systematic, multi-layered, and interconnected structure. Through line-by-line and concept-by-

concept coding of expert interviews and technical documents, a comprehensive set of open codes was initially generated across four principal dimensions: the physical layer, virtual layer, managerial-command layer, and the cyber training field itself. These codes reflected the essential infrastructural, technological, organizational, and operational components required for an advanced cyber-enabled wargaming environment.

After validation using Lawshe's Content Validity Ratio (CVR), a refined set of indicators was retained, including eleven key factors in the physical layer, twenty-one in the virtual layer, twenty-three in the managerial/command layer, and nine core elements defining the cyber training field. The distribution and complexity of the codes indicated that while the physical and virtual layers provide the technological backbone of the system, the managerial/command layer plays a central integrative and coordinating role in ensuring operational coherence, scenario control, strategic alignment, and performance assessment.

Quantitatively, the multiple linear regression model demonstrated a remarkably strong relationship between the three independent variables and the dependent variable. The multiple correlation coefficient ($R = 0.970$) and coefficient of determination ($R^2 = 0.941$) confirmed that 94.1% of the variance in the cyber training field could be explained by the combined influence of the physical, virtual, and managerial layers. The adjusted R^2 (0.938) further indicated that the model was not affected by overfitting and retained substantial explanatory power.

The ANOVA results ($F = 385.523$, $p < 0.001$) verified the overall statistical significance of the model, rejecting the null hypothesis and confirming that at least one of the independent variables significantly predicts the dependent variable. Analysis of standardized beta coefficients demonstrated that the physical layer exerted the greatest influence ($\beta = 0.748$), followed by the virtual layer ($\beta = 0.192$) and the managerial/command layer ($\beta = 0.139$). Although differing in magnitude, all three variables exhibited a significant and positive effect on the cyber training field.

These findings highlight that, despite the strategic and organizational importance of command structures, robust physical infrastructure—including hardware, network architecture, and secure environments—remains the most critical driver for creating an effective cyber wargaming platform. The conceptual model derived from this mixed-methods analysis provides a validated, empirically grounded framework for the design of next-generation

cyber training fields capable of supporting complex, multi-domain, and future-oriented wargaming scenarios.

DISCUSSION and CONCLUSIONS

Rapid advancements in information technologies and their integration across land, sea, air, and space domains have fundamentally transformed the nature of warfare, rendering the battlefield a multi-layered, complex, and data-driven environment dependent on continuous human–machine interaction. In this context, the cyber training field has evolved beyond a mere educational environment into a strategic platform for force preparation, doctrine testing, response evaluation, and decision-making enhancement under uncertainty.

Qualitative findings indicate that the cyber training field functions as a multi-dimensional ecosystem where physical infrastructures, software architectures, network systems, data, scenarios, control mechanisms, command structures, and human behavior operate in a coordinated and integrated manner. The field achieves its role as a "strategic laboratory" only when structural alignment and synergy exist among the physical, virtual, and managerial/command layers.

Quantitative analysis using correlation and multiple regression confirmed that all three independent variables—physical layer, virtual layer, and managerial/command layer—exert a positive, direct, and statistically significant effect on the effectiveness of the cyber training field. Among these, the physical layer emerged as the strongest predictor (standardized $\beta = 0.748$), emphasizing the critical role of robust hardware, network infrastructure, processing systems, sensors, and simulation devices in establishing a reliable and operationally realistic field. The virtual layer contributes to realism and adaptability by supporting dynamic scenarios, intelligent tools, and interactive simulations ($\beta = 0.192$). While the managerial/command layer displayed the lowest beta value ($\beta = 0.139$), its significance underscores the indispensable role of human decision-making, hierarchical coordination, scenario management, and post-operation analysis. The high coefficient of determination ($R^2 = 0.941$) demonstrates that the integrated model explains over 94% of the variance in the cyber training field. Overall, these results highlight that a strategic, multi-layered, and coordinated design is essential to maximize the operational effectiveness and strategic value of cyber wargaming platforms for future multi-domain conflicts.

ACKNOWLEDGEMENTS

This article is derived from a doctoral dissertation. The author wishes to express their sincere gratitude to their esteemed supervisor for invaluable academic guidance and continuous support throughout the research process. Special thanks are also extended to the advisory professors, whose expert insights, constructive feedback, and scholarly perspectives greatly contributed to the rigor and quality of this study. Their dedication and encouragement have been instrumental in the successful completion of this research.

فصلنامه علمی آینده‌پژوهی دفاعی
شاپای چاپی: ۲۳۸۸-۴۲۸X شاپای الکترونیکی: ۲۶۴۵-۷۱۷۲ http://www.dfsr.ir/ دانشگاه فرماندهی و ستاد آجا

عوامل مؤثر در میدان تمرین بازی جنگ سایبری: چارچوبی برای آماده‌سازی و شبیه‌سازی نبردهای سایبرپایه آینده

محمد قاسمی تادوانی [۱] | محمدتقی پرتوی [۲]✉ | حمید بیگدلی [۳] | مجتبی رمضان‌زاده [۴]

۱ - دانشجوی دکتری مدیریت دفاعی، دانشگاه فرماندهی و ستاد آجا، تهران، ایران. رایانامه:m.ghasemi@casu.ac.ir

۲ - استادیار تحقیق در عملیات، دانشگاه فرماندهی و ستاد آجا، تهران، ایران. رایانامه:m.partovi@casu.ac.ir

۳ - دانشیار تحقیق در عملیات، دانشگاه فرماندهی و ستاد آجا، تهران، ایران. رایانامه:h.bigdeli@casu.ac.ir

۴ - استادیار سایبر، دانشگاه فرماندهی و ستاد آجا، تهران، ایران. رایانامه:m.ramezanzadeh@casu.ac.ir

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخچه مقاله:

تاریخ دریافت:
۱۴۰۴/۰۹/۱۹

تاریخ بازنگری:
۱۴۰۴/۱۱/۱۷

تاریخ پذیرش:
۱۴۰۴/۱۱/۱۸

تاریخ انتشار:
۱۴۰۴/۰۳/۰۱

کلیدواژه‌ها:
میدان تمرین سایبری، لایه فیزیکی، لایه مجازی، لایه مدیریتی/فرماندهی

چکیده

زمینه و هدف: ادغام شتابان فناوری‌های اطلاعاتی با حوزه‌های عملیاتی زمین، دریا، هوا و فضا، میدان نبرد را به محیطی چندلایه، داده‌محور و وابسته به تعامل انسان_ماشین تبدیل کرده است. در چنین شرایطی، «میدان تمرین سایبری» به‌عنوان یک زیرساخت، امکان آماده‌سازی نیروها، آزمون دکترین‌ها و ارتقای تصمیم‌گیری در شرایط عدم قطعیت را فراهم می‌کند. هدف این پژوهش، تحلیل تأثیر لایه‌های فیزیکی، مجازی و فرماندهی و مدیریت بر میدان تمرین سایبری است.

روش‌ها: پژوهش از رویکرد آمیخته بهره برده است. تحلیل کیفی شامل بررسی اسناد تخصصی، مصاحبه با خبرگان بوده و تحلیل کمی با استفاده از همبستگی و رگرسیون چندمتغیره انجام شد تا میزان تأثیر هر یک از لایه‌ها بر متغیر وابسته، یعنی میدان تمرین سایبری، مشخص گردد.

یافته‌ها: نتایج نشان داد که هر سه لایه فیزیکی، مجازی و فرماندهی و مدیریت، رابطه‌ای مثبت، مستقیم و معنادار با کارایی میدان تمرین سایبری دارند. لایه فیزیکی با بالاترین ضریب بتای استاندارد، قوی‌ترین پیش‌بینی‌کننده اثربخشی میدان شناخته شد و نقش زیرساخت‌ها و تجهیزات سخت‌افزاری در واقع‌نمایی و پایداری میدان تأکید شد. لایه مجازی و فرماندهی نیز به ترتیب در ارتقای واقع‌گرایی، تعامل‌پذیری و بهره‌برداری مؤثر از میدان اهمیت دارند. ضریب تعیین مدل (۰.۹۴۱)نشان‌دهنده توان بالای آن در تبیین تغییرات میدان تمرین است.

نتیجه‌گیری‌ها: موفقیت میدان‌های تمرین سایبری نیازمند یکپارچگی میان لایه‌های فیزیکی، مجازی و فرماندهی است. این یافته‌ها نشان می‌دهند که طراحی و توسعه این میدان‌ها نه تنها یک ضرورت فناورانه، بلکه یک الزام راهبردی برای آمادگی، بازدارندگی و برتری در جنگ‌های چنددامنه‌ای آینده محسوب می‌شود.

استناد: قاسمی تادوانی،محمد؛ پرتوی،محمد تقی؛ بیگدلی،حمید و رمضان زاده،مجتبی. (۱۴۰۵). عوامل مؤثر در میدان تمرین بازی جنگ سایبری: چارچوبی برای آماده‌سازی و شبیه‌سازی نبردهای سایبرپایه آینده. *آینده‌پژوهی دفاعی، ۱۱(۴۰)، ۲۰۳-۲۳۸.*

DOI: https://doi.org/10.22034/dfsr.2026.2080098.1990

ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

مقدمه

محیط عملیاتی معاصر در نتیجه رشد شتابان فناوری‌های اطلاعاتی، از جمله الکترونیک پیشرفته، زیرساخت‌های نوین مخابراتی و سامانه‌های هوشمند پردازش اطلاعات، دستخوش تحولی بنیادین شده است. بهره‌گیری فراگیر از این فناوری‌ها، ظهور و تثبیت حوزه‌ای نوین تحت عنوان «فضای سایبری» را رقم زده است؛ حوزه‌ای که نه‌تنها مکمل میدان‌های سنتی عملیات، بلکه در بسیاری از ابعاد به تعیین‌کننده اصلی مناسبات قدرت تبدیل شده است (Kuehl, 2009).

فضای سایبری به‌مثابه دامنه‌ای جهانی در بستر محیط اطلاعاتی تعریف می‌شود که از شبکه‌ای به‌هم‌پیوسته از زیرساخت‌های فناوری اطلاعات و داده‌های مستقر در آن تشکیل شده است و اینترنت، شبکه‌های مخابراتی، سامانه‌های رایانه‌ای و انواع پردازنده‌ها و کنترل‌کننده‌های تعبیه‌شده را در بر می‌گیرد (Gortney, 2010: 58). این فضا امکان انتقال، ذخیره و پردازش دیجیتال اطلاعات را تقریباً در هر زمان و مکان و برای طیف گسترده‌ای از کاربران فراهم ساخته و درنتیجه، ساختار شناخت انسانی را دگرگون کرده است. دسترسی سریع، گسترده و پیوسته به اطلاعات، فرآیندهای ادراکی، رفتاری و تصمیم‌گیری انسان را وارد مرحله‌ای نوین کرده و بر شیوه ارزیابی تهدید، فرصت و اقدام تأثیری عمیق بر جای گذاشته است (Morgan, 2019).

در افق آینده، برتری در حوزه‌های سنتی قدرت، یعنی زمین، دریا، هوا و فضا، بیش از پیش وابسته به تسلط در فضای سایبری خواهد بود. این فضا نه‌تنها به‌عنوان بستری برای پشتیبانی عملیات، بلکه به‌عنوان یک واسط راهبردی برای اجرای فعالیت‌های اطلاعاتی، تصمیم‌سازی انسانی و ماشینی و همچنین اعمال نفوذ شناختی و رفتاری بر دشمن ایفای نقش می‌کند (Singh, 2022). ازاین‌رو، کشورهایی که بتوانند توانمندی‌های سایبری خود را به‌صورت هوشمندانه توسعه و یکپارچه‌سازی کنند، قادر خواهند بود مزیت‌های پایدار عملیاتی ایجاد نمایند. دسترسی به اینترنت و سایر دامنه‌های فضای سایبری، امکان اثرگذاری مستقیم و غیرمستقیم بر زیرساخت‌های حیاتی، بدون نیاز به حضور فیزیکی در میدان را فراهم می‌سازد و همین ویژگی، فضای سایبری را به یکی از کلیدی‌ترین عرصه‌های رقابت قدرت در آینده بدل کرده است (قاسمی، ۱۴۰۲).

در محیط عملیاتی نوین، تصمیم‌گیری راهبردی در شرایط آکنده از عدم قطعیت، پیچیدگی، محدودیت منابع و دسترسی ناقص به اطلاعات صورت می‌گیرد. هدف غایی این تصمیمات، کاهش، مهار یا خنثی‌سازی تهدیداتی است که اغلب ماهیتی پویا و پیش‌بینی‌ناپذیر دارند و لزوماً با فرضیات اولیه تصمیم‌گیرندگان هم‌خوان نیستند. در چنین بستری، «بازی جنگ» به‌عنوان ابزاری تحلیلی و آموزشی، امکان به‌کارگیری دانش نظری در قالب سناریوهای نزدیک به واقعیت آینده را فراهم می‌سازد و ظرفیت تفکر انتقادی، تحلیل چندبعدی و حل مسئله فرماندهان و تصمیم‌گیرندگان را ارتقا می‌دهد (Kuehn, 2021). افزون بر این، بازی‌های جنگ به‌عنوان آزمایشگاهی مفهومی برای آزمون ایده‌ها، فناوری‌ها و دکترین‌های نوظهور عمل می‌کنند و به بازیگران نظامی کمک می‌کنند مسیرهای جایگزین عمل را مجسم کرده و پیامدهای هر انتخاب را پیش از وقوع واقعی آن ارزیابی کنند؛ مسیری که در نبردهای آینده می‌تواند تفاوت میان پیروزی و شکست را رقم بزند(Work, 2015: 20) .

با گسترش سریع عملیات سایبری، این نوع درگیری به یکی از ارکان اصلی نبردهای نوین بدل شده و دیگر نمی‌توان آن را از جنگ متعارف جدا دانست. هم‌گرایی عملیات سایبری و عملیات فیزیکی، به شکل‌گیری میدان‌های نبرد چندلایه و فوق پیچیده منجر شده است؛ امری که ضرورت بازطراحی مدل‌های بازی جنگ را بیش از پیش آشکار می‌سازد. در واقع، ادغام ابعاد سایبری در طراحی و اجرای بازی‌های جنگ آینده، نه یک انتخاب، بلکه یک الزام راهبردی است (Reddie, 2024: 18).

با افزایش توانمندی‌های سایبری و رشد نمایی پیچیدگی فنی جنگ‌ها، بازیگرانی که بتوانند به‌طور مؤثر از اثرات سایبری بهره بگیرند، عملاً ابتکار عمل و تسلط بر میدان نبرد را در اختیار خواهند گرفت (Singh, 2022).ازاین‌رو، مدل‌های سنتی بازی جنگ که عمدتاً بر ابعاد فیزیکی متمرکز بوده‌اند، دیگر قادر به بازنمایی دقیق واقعیت عملیاتی آینده نیستند. تمرکز این پژوهش بر بازتعریف و تبیین ویژگی‌های «بستر بازی جنگ سایبری» به‌عنوان میدانی انسان‌ساخته، پویا و چندبعدی است؛ میدانی که اگرچه از محیط عملیات نظامی فیزیکی متمایز است، اما در آینده‌ای نه‌چندان دور، نقشی تعیین‌کننده‌تر از آن در شکل‌دهی به معادلات امنیتی و نظامی ایفا خواهد کرد. این میدان، نه صرفاً یک محیط شبیه‌سازی، بلکه آزمایشگاهی برای درک، پیش‌بینی و مدیریت جنگ‌های نسل آینده به شمار می‌رود.

این پژوهش با هدف یافتن عوامل مؤثر در میدان تمرین بازی جنگ سایبری و تحلیل تأثیر آن انجام شده است.

مرور پیشینه و مبانی نظری

مرور پیشینه

کولبرت و سالیوان، (۲۰۱۷)، در تحقیقی با عنوان بازی جنگ فیزیکی_سایبری راهبردهای بازی جنگ در این فضا را بررسی کردند و نشان دادند که داده‌های ضبط‌شده از فعالیت تیم‌ها می‌تواند برای آزمون و اعتبارسنجی مدل‌های دفاع سایبری استفاده شود. آن‌ها شباهت ساختاری میان بازی‌های جنگ سنتی و سایبری را تبیین کردند و با اشاره به خلأ مبانی نظری این حوزه، رویکردی مبتنی بر نظریه بازی را برای تحلیل راهبردهای تیم‌های قرمز، آبی و سفید ارائه دادند. روش‌شناسی این پژوهش مبتنی بر استفاده از نظریه بازی برای تحلیل تعاملات راهبردی میان تیم‌ها در سناریوهای سایبری، تبیین ساختار مراحل اجرای بازی جنگ و طراحی روش امتیازدهی علمی برای ارزیابی عملکرد تیم‌ها بوده است (Colbert, 2017).

کارول، (۲۰۲۳)، در تحقیقی با عنوان روش‌های چابک برای بهبود برنامه‌ریزی عملیات سایبری، نشان داد که روش‌های چابک مانند اسکرام[۱] می‌توانند چرخه‌های توسعه، آموزش و اجرای عملیات سایبری در محدوده‌های سایبری را به‌طور قابل‌توجهی بهبود دهند. این تحقیق تأکید می‌کند که ترکیب روش‌های چابک با چارچوب‌های توسعه، امنیت و عملیات[۲] موجب تسریع توسعه، افزایش چابکی، یادگیری فعال و بهینه‌سازی عملیات تهاجمی و دفاعی می‌شود. روش‌شناسی این تحقیق مبتنی بر یک تحلیل کیفی جامع بوده است که شامل مرور ادبیات، بررسی چارچوب‌های توسعه چابک، تحلیل کاربرد اسکرام در شبیه‌سازی‌های جنگ سایبری و استخراج الگوهای موفقیت از تجربیات عملی دانشگاهی و نظامی می‌شود (Carroll, 2023).

هیکی لانتو و همکاران (۲۰۱۹)، در تحقیقی با عنوان تاب‌آوری سایبری شبکه‌های مختلف ساختاری و فناورانه، یک بازی جنگ رومیزی مبتنی بر روش بازی ماتریسی ارائه کردند که

۱- اسکرام (Scrum) چارچوبی است که به اعضای تیم‌ها کمک می‌کند تا با همدیگر کار کنند و از طریق تجربیات خود چیزهای تازه‌ای بیاموزند و برد و باخت‌های خود را جهت بهبود مداوم مورد استفاده قرار دهند.

2 -Development, Security and Operations (DevSecOps)

امکان مقایسه انعطاف‌پذیری بین شبکه‌های ملی بسته و باز را فراهم می‌کند. در این سناریو، تیم‌های آبی در دو نوع شبکه سازمانی و ملی سازمان‌دهی شده و تیم قرمز در نقش تهدید خارجی عمل می‌کنند و کنترل‌کننده بازی نتایج را بر اساس کیفیت استدلال‌ها تعیین می‌کند. این چارچوب ابعادی مانند جنبه‌های فنی، منطقه‌ای، سازمانی و ملی تاب‌آوری را پوشش می‌دهد و چالش‌هایی نظیر تعریف قوانین تعامل، تضمین قابلیت مقایسه و نیاز به تیم متخصص را برجسته می‌سازد. روش‌شناسی این پژوهش بر استفاده از روش بازی ماتریسی و استدلال ساخت‌یافته استوار است؛ بدین‌صورت که اقدامات پیشنهادشده توسط تیم‌ها تحلیل و نتایج بر پایه کیفیت استدلال‌ها و شرایط شبکه‌ها مدل‌سازی می‌شود. این رویکرد امکان تحلیل دقیق تفاوت‌ها و پیامدهای شبکه‌های بسته و باز را فراهم می‌کند (Lantto, 2019).

رسمی ولاد محمود و همکاران (۲۰۲۱)، در پژوهشی توصیفی، معماری یک پلتفرم آزمایشگاهی مجازی به نام «دفآت» را برای آموزش و تحقیق در حوزه امنیت سایبری معرفی و تحلیل کرده‌اند؛ بستری خودکار، مقیاس‌پذیر و مبتنی بر بازی‌وارسازی که با شبیه‌سازی یک مرکز عملیات امنیتی، امکان اجرای سناریوهای تیم قرمز و آبی، پایش و پاسخ به حملات شبکه‌ای را در محیطی واقع‌گرایانه فراهم می‌سازد. این پلتفرم در سه مرحله آماده‌سازی، شبیه‌سازی و بازبینی طراحی‌شده و با ادغام نظام‌مند عناصر بازی‌وارسازی، موجب افزایش انگیزه، مشارکت و کیفیت یادگیری می‌شود. پژوهشگران با اتکا به تحلیل ادبیات، مصاحبه با متخصصان و بررسی زیرساخت‌های موجود، ویژگی‌های کلیدی همچون خودکارسازی، پویایی، مقیاس‌پذیری و شبیه‌سازی مرکز عملیات امنیتی را به‌عنوان مؤلفه‌های اصلی طراحی استخراج کرده‌اند و نتایج آنان نشان می‌دهد که «دفآت» می‌تواند به‌عنوان زیرساختی مؤثر برای ارتقای مهارت‌های عملی، کاهش شکاف نیروی متخصص و توسعه سناریوهای پیچیده و کاربردی در آموزش و تحقیق سایبری مورد استفاده قرار گیرد (Mahmoud, 2021).

در یک نگاه تحلیلی و تطبیقی پیشینه‌ها به ابعاد مختلف پیچیدگی، چندلایه بودن و ضرورت واقع‌نمایی در میدان نبرد سایبری اشاره دارند، اما از زاویه‌های متفاوتی به مسئله می‌پردازند. پژوهش نخست بر نظریه‌پردازی و مدل‌سازی رفتاری مبتنی بر نظریه بازی تمرکز دارد و تلاش می‌کند تعامل راهبردی تیم‌های مهاجم و مدافع را برای سامانه‌های

سایبر–فیزیکی تبیین کند؛ پژوهش دوم بر چابک‌سازی عملیات و چرخه‌های توسعه سناریوهای سایبری با بهره‌گیری از روش‌های اسکرام تأکید دارد؛ پژوهش سوم با رویکرد بازی ماتریسی، تاب‌آوری شبکه‌های ملی را در برابر تهدیدات خارجی تحلیل کرده و نشان می‌دهد که ساختار شبکه چگونه رفتار دفاعی و فرصت‌های عملیاتی را تغییر می‌دهد؛ و پژوهش چهارم، دفآت را به‌عنوان یک سکوی عملیاتی خودکار، مقیاس‌پذیر و بازی‌وارسازی شده معرفی می‌کند که قادر است چرخه کامل تمرین از آماده‌سازی تا بازبینی را برای تیم‌های قرمز و آبی شبیه‌سازی کند. مقایسه این چهار پیشینه نشان می‌دهد که هر یک بخشی از پازل میدان تمرین سایبری را حل کرده‌اند: یکی نظریه و مدل رفتاری، دیگری روش‌های توسعه و بهره‌برداری، سومی تحلیل ساختاری و تاب‌آوری و چهارمی ساخت بستری عملیاتی برای اجرای رزمایش.

پژوهش انجام شده با چهار پیشینه مذکور هم‌راستایی مفهومی دارند، اما آن‌ها را به‌طور هم‌زمان و یکپارچه پوشش نمی‌دهند. پیشینه‌ها هرکدام تنها به بخشی از چرخه عملیات سایبری پرداخته‌اند و از یک مدل چندلایه، یکپارچه و عملیاتی که بتواند لایه‌های فیزیکی، سایبری و فرماندهی را در کنار سازوکارهای سناریوسازی، پایش، تیم‌سازی، مدیریت و امتیازدهی ادغام کند، غافل مانده‌اند. نوآوری پژوهش حاضر در این است که این اجزا را در قالب یک چارچوب جامع برای طراحی، اجرای و ارزیابی بازی جنگ سایبری ارائه می‌دهد؛ چارچوبی که پیچیدگی تعاملات انسان_ماشین، ماهیت چندلایه عملیات سایبری، نقش سامانه‌های سایبر_فیزیکی و نیازهای عملیاتی میدان نبرد مدرن را هم‌زمان در نظر می‌گیرد. این پژوهش با ترکیب دیدگاه‌های نظری شکاف میان مدل‌های نظری موجود و الزامات واقعی رزمایش‌های سایبری را پر کرده و نقشه‌ای علمی برای توسعه سکوهای پیشرفته بازی جنگ سایبری فراهم می‌سازد.

مبانی نظری

بازی جنگ سایبری

بازی جنگ سایبری فرآیندی پیچیده، چندلایه و بین‌رشته‌ای است که تنها با بهره‌گیری از متخصصان باتجربه و دارای صلاحیت عملیاتی و در اختیار داشتن ابزارهای فنی مناسب قابل انجام است. از آن‌جا که هدف بازی جنگ سایبری، ایجاد تجربه‌ای نزدیک به شرایط واقعی عملیات در زمان واقعی برای شرکت‌کنندگان است، پیش از تعریف دامنه، باید

سطح مهارت و آمادگی نیروهای شرکت‌کننده ارزیابی شود، چراکه میزان بلوغ عملیاتی آنان مستقیماً بر نتایج رزمایش تأثیر دارد. طراحان این نوع رزمایش‌ها باید به‌طور کامل با جدیدترین فناوری‌ها، روش‌های حمله و دفاع سایبری و تاکتیک‌های رزم سایبری آشنا باشند. دامنه رزمایش می‌تواند از سطح تاکتیکی تا عملیاتی و حتی راهبردی گسترده باشد. مقیاس رزمایش، تعداد شرکت‌کنندگان، مدت زمان (از چند روز تا چند هفته یا ماه) و سطح پیچیدگی سناریوها، همگی بر اساس این دامنه تعیین می‌شوند (Evensen, 2019). در واقع، بازی جنگ سایبری نه تنها ابزاری برای آموزش فرماندهان و تحلیل‌گران است، بلکه بستری برای ارزیابی واقع‌گرایانه تعامل میان حوزه‌های سایبری و فیزیکی جنگ محسوب می‌شود. موفقیت در چنین بازی‌هایی مستلزم شناخت عمیق از چرخه عملیات سایبری، دینامیک تصمیم‌گیری در شرایط اطلاعات ناقص و مدیریت هم‌زمان تهدیدات است. بازی جنگ سایبری، جایی است که عقلانیت نظامی و محاسبات فناورانه به‌صورت هم‌زمان به محک گذاشته می‌شوند امن‌ترین و کارآمدترین گزینه برای اجرای بازی جنگ سایبری در محیطی واقع‌گرایانه، استفاده از یک سکوی میدان تمرین سایبری[1] قدرتمند است. چنین سامانه‌ای امکان شبیه‌سازی دقیق محیط‌های دیجیتال، شبکه‌ها و سرویس‌های عملیاتی سازمان را فراهم می‌کند، بدون آنکه با سامانه‌های زنده تداخل داشته باشد (Hoffendahl, 2022: 43).

شبیه‌سازی مؤثر در بازی جنگ برای شناسایی و مدیریت وظایف کلیدی و شرایط حیاتی برای موفقیت یک عملیات نظامی در جنگ‌های آینده حیاتی است و به‌طور مستقیم کیفیت طرح‌ریزی‌ها را ارتقا داده و زمان تصمیم‌سازی و برنامه‌ریزی عملیاتی را کاهش می‌دهد (Bruvoll, 2015). برای تحقق این مزایا، بازی جنگ مبتنی بر شبیه‌سازی معمولاً شامل فرآیندهای اساسی هستند که به طراحان کمک می‌کنند تا بازی را بر اساس سناریوهای واقعی و تأثیرگذار، به‌درستی مدل‌سازی نمایند (Evensen, 2019).

بازی جنگ سایبری برای سامانه‌های سایبر_فیزیکی

1 - Cyber Range Platform

سامانه‌های کنترل صنعتی[1]، سامانه‌هایی هستند که با ترکیب سخت‌افزار و نرم‌افزار، فرآیندهای فیزیکی را به‌صورت خودکار کنترل می‌کنند. سامانه‌های کنترل نظارتی و گردآوری داده(اسکادا)[2] زیرمجموعه‌ای از سامانه‌های کنترل صنعتی است که معمولاً بر دستگاه‌های پراکنده جغرافیایی نظارت دارد. در گذشته این سامانه‌ها از شبکه‌های سازمانی جدا بودند، اما با ادغام در زیرساخت‌های فناوری اطلاعات برای افزایش بهره‌وری، اکنون در معرض تهدیدات سایبری قرار گرفته‌اند لذا بسیاری از سامانه‌های سایبر- فیزیکی[3] شامل سامانه‌های کنترل صنعتی، سامانه‌های کنترل نظارتی و گردآوری داده(اسکادا) و همچنین اشیای متصل در اینترنت اشیا[4] در برابر تهدیدهای سایبری آسیب‌پذیرند (Colbert, 2016).

با توجه به این‌که سامانه‌های کنترل نظارتی و گردآوری داده (اسکادا) و دیگر سامانه‌های سایبر- فیزیکی معمولاً در حال کار عملیاتی هستند، اجرای آزمایش‌های امنیتی بر روی سامانه‌های واقعی اغلب دشوار یا غیرممکن است. می‌توان از داده‌های ضبط‌شده از رفتار بازیکنان در این بازی‌ها برای آزمون و اعتبارسنجی مدل‌های دفاع سایبری استفاده کرد. با وجود آسیب‌پذیری سخت‌افزارهای کنترل‌کننده سامانه‌های سایبر- فیزیکی در برابر حملات سایبری اغلب آن‌ها در برابر مهاجمان بالقوه محافظت کافی ندارند. کشورها، به‌منظور ارتقای آگاهی اپراتورها، مالکان و کاربران این سامانه‌ها، اقدام به برگزاری بازی جنگ سایبری با مشارکت تیم‌های قرمز (مهاجم) و آبی (مدافع) در محیطی تا حد امکان واقعی می‌کنند. تصمیم‌ها و حرکات بازیکنان در این بازی‌ها ثبت می‌شود تا با تحلیل آن‌ها بتوان درک بهتری از نحوه مدل‌سازی، پیش‌بینی و ارزیابی حملات علیه سامانه‌های واقعی اسکادا و سامانه‌های سایبر- فیزیکی به‌دست آورد. در سطح فرماندهی، درک رفتار تیم قرمز (مهاجم) در چنین محیطی می‌تواند مبنای تصمیم‌سازی آینده برای واکنش به

1- Industrial Control Systems (ICSs)
2 -SCADA: Supervisory Control and Data Acquisition
3 -Cyber-Physical Systems (CPSs)
4 -Internet of Things (IOT)

حملات علیه زیرساخت‌های حیاتی نظامی یا ملی باشد. برای مثال، دانستن این‌که مهاجم چگونه اولویت‌بندی اهداف را انجام می‌دهد، یا مدافع چگونه باید منابع دفاعی را در لایه‌های مختلف (فیزیکی، شبکه‌ای و مدیریتی) تخصیص دهد، برای طراحان راهبردی حیاتی است (Colbert, 2017). برای کسب نتایج مطلوب‌تر از سخت‌افزار در چرخه[1] استفاده می‌شود؛ یعنی کنترل‌گر صنعتی واقعی است، اما پروسه فیزیکی (مثل چرخش توربین) شبیه‌سازی می‌شود.

در سطح نظامی، اسکاداها معادل سامانه‌های کنترل مأموریتی یا لجستیکی هستند (مانند کنترل خطوط سوخت، آب، انرژی یا رادار). نقطه کلیدی این بخش آن است که مرز بین شبکه‌های عملیاتی و شبکه‌های اطلاعاتی از بین رفته و دشمن می‌تواند از مسیر دوم برای حمله به اولی استفاده کند. از آن‌جا که این سامانه‌ها به‌ویژه اسکادا و سامانه‌های کنترل صنعتی در حالت عملیاتی دائمی هستند، امکان آزمون امنیتی واقعی بر روی آن‌ها محدود است. لذا نیروهای نظامی از بازی جنگ میزگردی و زنده برای شبیه‌سازی تعامل مهاجم (تیم قرمز) و مدافع (تیم آبی) استفاده می‌کند. داده‌های ثبت‌شده از رفتار تیم‌ها سپس برای اعتبارسنجی مدل‌های نظری دفاع سایبری به‌ویژه مدل‌های نظریه بازی‌ها مورد استفاده قرار می‌گیرند (Colbert, 2015).

این رویکرد در واقع یک محیط تمرینی نیمه‌واقعی برای نیروهای سایبری است که به فرماندهان اجازه می‌دهد الگوهای رفتاری، تاکتیکی و تصمیم‌گیری مهاجمان و مدافعان را در شرایط کنترل‌شده اما واقع‌نما مطالعه کنند. از منظر نظامی، چنین بازی‌هایی معادل تمرینات شبیه‌سازی‌شده رزمی (مانند شبیه‌سازی میدان نبرد در سطح فیزیکی) هستند، با این تفاوت که در حوزه زیرساخت‌های حیاتی ملی و نظامی عمل می‌کنند. کارکرد اصلی این بخش، ایجاد بانک داده‌های رفتاری[2] برای طراحی مدل‌های پیش‌بینی حمله و پاسخ است (Colbert, 2017).

1- Hardware-in-the-Loop (HIL)

2 -Behavioral Intelligence

میدان تمرین سایبری[1]

برای حفظ و مدیریت بازی جنگ سایبری و محیط‌های مرتبط با آن، مفهوم «میدان تمرین سایبری» مطرح شده است. در سال‌های اخیر، این مفهوم و اصطلاح توجه زیادی را به خود جلب کرده، اما در زمینه‌های مختلف با معانی متفاوتی مورد استفاده قرار گرفته است. برخی از متخصصان آن را به‌عنوان یک محیط مجازی تعریف می‌کنند، درحالی‌که دیگران عناصر فیزیکی را نیز در تعریف میدان جنگ سایبری لحاظ می‌نمایند. این محیط می‌تواند از یک آزمایشگاه دانشگاهی تا یک بستر رزمایش امنیتی طبقه‌بندی‌شده متغیر باشد (Pham, 2016).

از دیدگاه دکترین جنگ سایبری، میدان نبرد سایبری چندوجهی است؛ بنابراین، در بازی جنگ سایبری مدل نظری سه لایه هم‌زمان را در بر می‌گیرد:

لایه فیزیکی – میدان نبرد عملیاتی

در این سطح، تهدیدات به تأثیر واقعی بر زیرساخت‌ها یا سامانه‌های حیاتی منجر می‌شوند: نیروگاه، خط انتقال انرژی، سامانه فرماندهی هواپیما یا سامانه لجستیک نظامی را در بر می‌گیرد. در رزمایش‌های نظامی، این لایه معادل صحنه عملیات واقعی است، جایی که هر تصمیم سایبری می‌تواند به آسیب یا ازکارافتادگی واقعی منجر شود. دفاع فیزیکی و امنیت سایبری باید هم‌پوشانی کامل داشته باشند.

لایه مجازی – جبهه نبرد اطلاعاتی

این لایه حوزه درگیری مستقیم تیم‌های قرمز و آبی است. تیم قرمز با استفاده از ابزارهای نفوذ، فیشینگ، بهره‌برداری از آسیب‌پذیری‌ها یا حملات مرد میانی وارد عمل می‌شود. تیم آبی نیز با مانیتورینگ، تحلیل لاگ‌ها و هماهنگی با فرماندهی به دفاع می‌پردازد. در سطح نظامی، این لایه نماینده فضای نبرد الکترونیکی و اطلاعاتی است. اینجا، سرعت تصمیم و آگاهی موقعیتی تعیین‌کننده بقا است.

1- Cyber Range

لایه مدیریتی / فرماندهی – سطح راهبردی و تصمیم‌گیری

در این لایه، سیاست‌ها، قواعد درگیری و دکترین‌های دفاعی و تهاجمی تعیین می‌شوند. فرماندهی باید درک کاملی از وضعیت لایه‌های پایین‌تر داشته باشد و بتواند بین منافع عملیاتی، امنیت اطلاعات و تداوم مأموریت تعادل برقرار کند. در رزمایش‌های نظامی، این لایه معادل ستاد فرماندهی سایبری است (Colbert, 2015).

اجزای میدان تمرین سایبری

۱. سناریوها[1]

سناریو، محیط اجرایی و خط داستانی تمرین یا آزمایش سایبری را تعریف می‌کند. سناریو باید بازتاب دقیقی از محیط عملیاتی واقعی و الزامات آموزشی باشد و فرآیند اجرای تمرین را هدایت کند تا اطمینان حاصل شود که اهداف آموزشی و تحقیقاتی محقق می‌گردند (Yamin, 2020). به این دلیل سناریو شامل مستندات، خلاصه مأموریت‌ها، دستورات عملیاتی، نقشه‌های تهدید و سایر اسناد پشتیبان است تا محیط تمرینی، بیشترین شباهت ممکن را با میدان واقعی نبرد سایبری داشته باشد (Staff, 2015: 22). همچنین سناریو بیانگر مأموریت اصلی آن است، خواه برای آموزش نیروهای سایبری در مقابله با تهدیدات، خواه برای آزمون و ارزیابی فناوری‌ها، ابزارها یا روش‌های جدید دفاع یا تهاجم سایبری. بر مبنای این اهداف، محیط سناریو طراحی می‌شود (Yamin, 2020).

محیط سناریو همان توپولوژی یا ساختار فنی است که تمرین در آن انجام می‌شود. اگر تمرین عملیاتی باشد، محیط شامل زیرساخت‌های فنی مانند سامانه‌های رایانه‌ای، شبکه‌های فیزیکی، محیط‌های مجازی یا ترکیبی از آن‌ها خواهد بود. در تمرین‌های میزگردی[2] که تصمیم‌گیری تاکتیکی در سطح فرماندهی تمرین می‌شود، محیط می‌تواند

1- Scenarios
2 -Tabletop

غیررایانه‌ای و صرفاً مفهومی باشد. این نوع تمرین‌ها گاهی با پشتیبانی نرم‌افزاری انجام می‌شوند اما الزاماً نیاز به تجهیزات دیجیتال ندارند (Gurnani, 2014: 19).

روایت سناریو، چارچوب داستانی عملیات را توصیف می‌کند و مجموعه‌ای از رخدادها و واکنش‌ها را در بر می‌گیرد که جریان کلی تمرین را تشکیل می‌دهند. روایت به فرماندهان تمرین کمک می‌کند تا کنترل و ارزیابی جامعی از سناریوهای پیچیده داشته باشند و بتوانند نتایج عملیات (یا آزمایش) را تحلیل کنند (Staff, 2015: 34).

سناریوها به دو نوع تقسیم می‌شوند:

- ایستا[1]: محیط ثابت است و در طول تمرین تغییری ایجاد نمی‌شود.
- پویا[2]: شامل مؤلفه‌هایی است که در طول اجرا تغییر می‌کنند (مثلاً تزریق تهدید، تولید ترافیک شبیه‌سازی‌شده یا فعال‌سازی حمله‌های جدید در حین تمرین).

دامنه بیانگر حوزه کاربردی سناریو است؛ مانند شبکه، رایانش ابری، سامانه‌های صنعتی[3]، اینترنت اشیاء[4] و غیره.

ابزارهایی که برای ساخت محیط یا ایجاد روایت سناریو به‌کار می‌روند، مانند شبیه‌سازهای شبکه، مولدهای ترافیک، ابزارهای تزریق آسیب‌پذیری، یا موتورهای سناریونویسی (Yamin, 2020).

۲. پایش[5]

پایش شامل مجموعه‌ای از روش‌ها، ابزارها و سطوحی است که برای نظارت بلادرنگ بر عملکرد نیروها و سامانه‌ها در طول تمرین‌های سایبری مورداستفاده قرار می‌گیرند (طاهری، ۱۳۹۹). نظارت می‌تواند توسط ناظران انسانی یا سامانه‌های خودکار انجام شود (Kick, 2014: 39).

---

1 -Static
2- Dynamic
3 -ICS/SCADA
4 -IoT
5 -Monitoring

پایش می‌تواند خودکار (با استفاده از ابزارهای جمع‌آوری داده و تحلیل عملکرد) یا دستی (توسط ناظران انسانی) صورت گیرد. ابزارها شامل ابزارهای نرم‌افزاری و سخت‌افزاری برای نظارت بر تمرین، مانند سامانه‌های تشخیص و جلوگیری از نفوذ، حسگرهای شبکه و سیستم‌های تحلیل رفتار ترافیک است. پایش در تمرین‌های عملیاتی یا در سطح اجتماعی و تصمیم‌سازی و در تمرین‌های میزگردی ممکن است در لایه‌های مختلف شبکه انجام شود (Yamin, 2020).

۳. تیم‌سازی[1]

بازی جنگ سایبری تمرین در میدان نبرد سایبری است. در آن، هماهنگی بین تیم‌ها شبیه به ساختار گروه رزمی مشترک است. تیم سفید نقش ستاد فرماندهی، تیم آبی نقش نیروهای مدافع و تیم قرمز نقش دشمن نامتقارن را دارد. از منظر تصمیم‌سازی فرماندهی، داده‌های حاصل از این تمرین به طراحان امکان می‌دهد پویایی تصمیم انسانی را با مدل‌های نظری مقایسه کرده و خطای پیش‌بینی مدل‌ها را کاهش دهند (Rege, 2019). در بازی جنگ سایبری، تیم‌سازی یکی از ارکان کلیدی است. هر تیم بر اساس نقش خود در چرخه تمرین، با رنگ خاصی شناسایی می‌شود (Tsai, 2018).

(الف) تیم قرمز: تیم مهاجم که نقش دشمن را ایفا کرده و مسئول شناسایی و بهره‌برداری از آسیب‌پذیری‌ها در محیط تمرین است. وظیفه آن، تقلید از رفتار واقعی تهدیدات پیشرفته و نفوذ به سامانه‌هاست.

(ب) تیم آبی: تیم مدافع که در برابر حملات تیم قرمز واکنش نشان می‌دهد و مأمور شناسایی، مهار و ترمیم آسیب‌پذیری‌هاست.

(ج) تیم سفید: ناظر و طراح تمرین؛ این تیم سناریو، قوانین درگیری[2]، شاخص‌های ارزیابی و شرایط تمرین (تزریق رویداد، پایش امتیازات) را تعریف می‌کند. همچنین ممکن است در نقش داور یا مربی عمل کند.

1- Teaming
2- Rules of Engagement

(د) تیم سبز: مسئول آماده‌سازی، نگهداری و پشتیبانی زیرساخت تمرین است و در صورت بروز خطا یا خرابی، بازی را به وضعیت عملیاتی بازمی‌گرداند.

(ه) تیم‌های خاص تمرین[1]: در برخی تمرین‌ها، تیم‌های اضافی به‌صورت موقت اضافه می‌شوند:

- تیم نارنجی: تعیین‌کننده وظایف خاص برای تیم آبی؛ اعطای امتیاز بر اساس موفقیت در انجام مأموریت‌ها.
- تیم بنفش: پل ارتباطی میان تیم قرمز و آبی برای بهبود هماهنگی و تبادل اطلاعات تهدید.
- تیم زرد: شبیه‌ساز کاربران عادی که ترافیک مشروع شبکه را تولید می‌کنند تا سناریو به واقعیت نزدیک‌تر شود (Yamin, 2020).

(و) تیم‌های خودمختار[2]: با پیشرفت فناوری، برخی نقش‌های انسانی با ابزارهای خودکار جایگزین شده‌اند. به‌عنوان‌مثال:

- تولید کننده سناریو امنیتی برای خودکارسازی ایجاد محیط سناریو (وظیفه تیم سبز).
- اسوید[3] برای خودکارسازی وظایف تیم قرمز مانند حمله و نفوذ (Holm, 2016).

۴. امتیازدهی[4]

سیستم امتیازدهی، داده‌های حاصل از پایش را تحلیل می‌کند تا رویدادهای فنی سطح پایین به شاخص‌های عملکردی قابل‌تفسیر تبدیل شوند. این سیستم میزان پیشرفت تیم‌ها، میزان موفقیت در دفاع یا حمله و انطباق با اهداف مأموریت را ارزیابی می‌کند. امتیازدهی ممکن است بر اساس اهداف مشخص (مانند تسخیر پرچم‌ها) یا از طریق

1 -Specialized Teams
2 -Autonomous Teams
3- SVED
4 -Scoring

تحلیل خودکار لاگ‌های سیستم انجام شود. ابزارهای امتیازدهی شامل داشبوردهای ثبت پرچم، تحلیلگرهای داده و سامانه‌های خودکار ارزیابی عملکرد هستند (Staff, 2015: 33).

۵. مدیریت[1]

مدیریت، رکن فرماندهی میدان سایبری است و شامل تخصیص نقش‌ها، منابع و نظارت کلی بر روند تمرین می‌شود.

(الف) مدیریت نقش[2]: مدیریت هویت‌ها، مجوزها و نقش‌های افراد و تیم‌ها در ساختار تمرین.

(ب) مدیریت منابع[3]: مدیریت منابع پردازشی، حافظه، ذخیره‌سازی و سایر منابع فنی مورد نیاز برای اجرای تمرین یا آزمایش.

(ج) مدیریت میدان[4]: ارائه دید کلی و عملیاتی از کل میدان سایبری از طریق پورتال‌ها و داشبوردهای فرماندهی؛ این بخش امکان رصد وضعیت لحظه‌ای، ترافیک شبکه و عملکرد تیم‌ها را فراهم می‌کند (Yamin, 2020).

روش‌شناسی

این پژوهش کاربردی است که به روش توصیفی انجام شده است؛ اطلاعات به دو روش میدانی و کتابخانه‌ای جمع‌آوری شده است. ابزار جمع‌آوری اطلاعات میدانی، مصاحبه با سؤالات نیمه ساختاریافته از ده صاحب نظر آگاه به موضوع تحقیق بود که به شیوه قضاوتی هدفمند انتخاب شدند و ارائه پرسش‌نامه تنظیم شده بر مبنای طیف لیکرت (خیلی کم تا خیلی زیاد) به ۷۷ کارشناس این حوزه بود، اطلاعات کتابخانه‌ای از اسناد و مدارک (کتاب‌ها، فصلنامه‌ها، مقالات، گزارش‌ها و سایت‌های معتبر علمی) شناسایی و جمع‌آوری شده است.

1- Management
2 -Role Management
3 -Resource Management
4 -Range Management

تجزیه‌وتحلیل داده‌ها و اطلاعات با رویکرد آمیخته انجام‌شده است. در تحقیق کیفی این پژوهش، نظریه داده‌بنیاد به‌منظور شناسایی مؤلفه‌ها و ابعاد مؤثر بر «میدان تمرین سایبری» اتخاذ شد. داده‌ها از طریق مطالعه اسناد تخصصی و انجام مصاحبه‌های نیمه‌ساختاریافته با خبرگان حوزه سایبری و بازی جنگ گردآوری گردید و سپس با استفاده از نرم‌افزار اطلس تی.آی مورد تحلیل نظام‌مند قرار گرفت. فرآیند تحلیل داده‌ها بر اساس رهیافت استراوسی–کوربینی و طی سه مرحله اصلی کدگذاری باز، محوری و انتخابی انجام شد. در مرحله کدگذاری باز، مفاهیم اولیه و مضامین اصلی از متن داده‌ها استخراج گردید؛ در مرحله کدگذاری محوری، ارتباط میان مفاهیم شناسایی‌شده تبیین و در قالب مقوله‌های اصلی سازمان‌دهی شد و در نهایت، در مرحله کدگذاری انتخابی، چارچوب مفهومی نهایی بر اساس مقوله‌های هسته شکل گرفت.

عوامل به‌دست آمده به منظور تعیین شاخص‌های مناسب در ابعاد تحقیق، پرسش‌نامه‌ای از عوامل مهم و کلیدی مرحله قبل تهیه شد و تعداد ۱۰ نفر خبره آگاه به موضوع تحقیق انتخاب شدند از آنان خواسته شد بر مبنای طیف (۱. شاخص ضروری است. ۲. شاخص مفید است ولی ضروری نیست. ۳. شاخص ضرورتی ندارد.) شاخص‌ها را طبقه‌بندی کنند. در نهایت بر مبنای قضاوت آنان ضریب روایی محتوایی لاوشه محاسبه شد. عواملی که مقدار ضریب روایی محتوایی آنان براساس قضاوت خبرگان بیش از ۰.۶۲ بود (Lawshe, 1975) در مدل نهایی حفظ گردیدند. این رویکرد ترکیبی، منجر به استخراج مجموعه‌ای معتبر از عوامل کلیدی در چهار بعد «لایه فیزیکی»، «لایه مجازی»، «لایه مدیریتی/فرماندهی» و «میدان تمرین سایبری» شد و چارچوبی مفهومی، منسجم و علمی فراهم آورد.

در تحلیل کمی، روش توصیفی_تحلیلی از نوع همبستگی و رگرسیونی برای بررسی روابط بین متغیرها استفاده شده است. داده‌ها به‌وسیله پرسشنامه مبتنی بر مقیاس پنج‌درجه‌ای لیکرت گردآوری گردید؛ بدین ترتیب متغیرهای پژوهش به صورت عددی کمّی‌سازی شدند و امکان تحلیل آماری فراهم آمد. متغیرهای مستقل شامل سه بُعد «لایه فیزیکی»،

«لایه مجازی» و «لایه مدیریتی/فرماندهی» و متغیر وابسته «میدان تمرین سایبری» در نظر گرفته شد.

پس از ورود داده‌ها به نرم‌افزار آماری اس.پی.اس.اس، پیش‌فرض‌های اساسی تحلیل از جمله رابطه خطی بین متغیرها، عدم وجود داده‌های پرت و نرمال بودن نسبی توزیع داده‌ها مورد بررسی قرار گرفت. برای مدل‌سازی رابطه میان متغیرهای مستقل و وابسته از رگرسیون خطی چندمتغیره استفاده شد که روشی کارآمد برای تحلیل اثر هم‌زمان چند متغیر پیش‌بین بر یک متغیر ملاک است.

به‌منظور ارزیابی کفایت و معناداری مدل، شاخص‌های آماری از جمله ضریب همبستگی چندگانه، ضریب تعیین، آماره آزمون در تحلیل واریانس و سطح معناداری محاسبه و تفسیر شد. همچنین برای بررسی شدت و جهت رابطه هر یک از متغیرهای مستقل با متغیر وابسته، از ضرایب رگرسیونی استاندارد و آزمون تی استفاده شد.

در مجموع، روش تحقیق به‌کاررفته یک چارچوب معتبر و مبتنی بر روش‌های استنباطی پیشرفته است که امکان تبیین علمی و دقیق اثرگذاری متغیرهای ساختاری بر میدان تمرین سایبری را فراهم کرده و از نظر آماری دارای قابلیت اتکا و تعمیم‌پذیری مناسب است.

تجزیه‌وتحلیل یافته‌ها

در گام نخست، داده‌های متنی به‌صورت خط‌به‌خط و مفهوم‌به‌مفهوم تحلیل شده و مفاهیم پایه استخراج گردید، در این مرحله، مجموعه‌ای از کدهای باز اولیه که بیانگر اجزای مفهومی و عملیاتی هر یک از لایه‌ها بودند، از روایت‌ها و محتوای مصاحبه‌ها استخراج شد. این کدها که معرف عناصر کلیدی، کارکردها، الزامات و سازوکارهای مؤثر در طراحی و پیاده‌سازی یک میدان تمرین سایبری کارآمد بودند در کدهای محوری مناسب طبقه‌بندی شدند و در نهایت این کدهای محوری در چهار کد انتخابی لایه فیزیکی، لایه مجازی، لایه مدیریتی/فرماندهی و میدان تمرین سایبری قرار رفته و سازه تحقیق شکل گرفت.

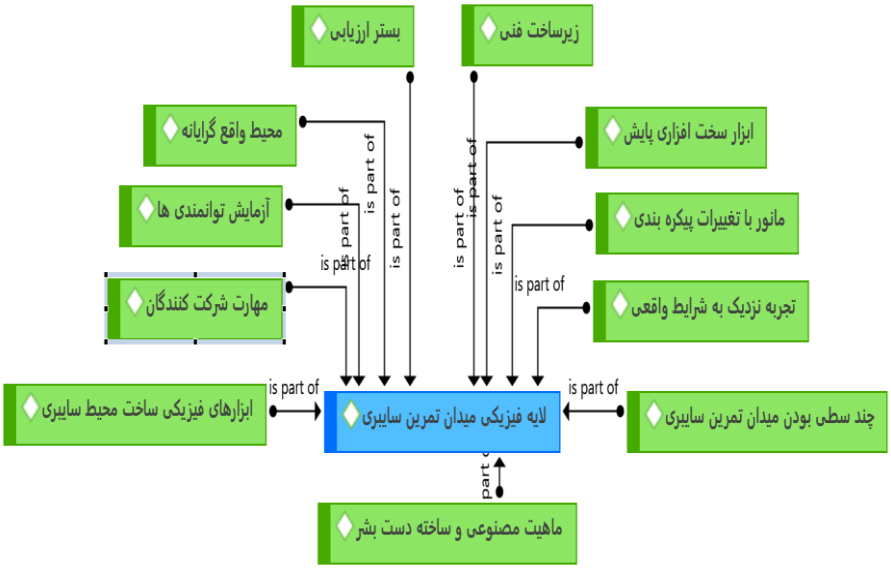
در مرحله دوم و به‌منظور اعتبارسنجی و غربال مفاهیم استخراج‌شده، ده نفر از خبرگان آگاه به حوزه سایبری و دارای تجربه عملی و پژوهشی مرتبط، به‌صورت هدفمند انتخاب شدند. از این خبرگان درخواست شد تا کدهای شناسایی‌شده را بر اساس طیف

سه‌گزینه‌ای لاوشه، ارزیابی و طبقه‌بندی نمایند. عواملی که مقدار ضریب روایی محتوایی آنان براساس قضاوت خبرگان بیش از ۰.۶۲ بود به‌عنوان عوامل مناسب در هر لایه انتخاب شد و در لایه انتخابی مربوطه قرار گرفتند.

نتایج این فرآیند نشان داد که در:

لایه فیزیکی، تعداد یازده کد انتخابی واجد شرایط روایی محتوایی بوده و به‌عنوان عوامل کلیدی این لایه شناسایی شدند. این عوامل عمدتاً ناظر بر زیرساخت‌های سخت‌افزاری، تجهیزات شبکه، محیط‌های شبیه‌سازی، سامانه‌های ذخیره‌سازی و تجهیزات امنیتی فیزیکی هستند که بنیان مادی میدان تمرین سایبری را تشکیل می‌دهند.

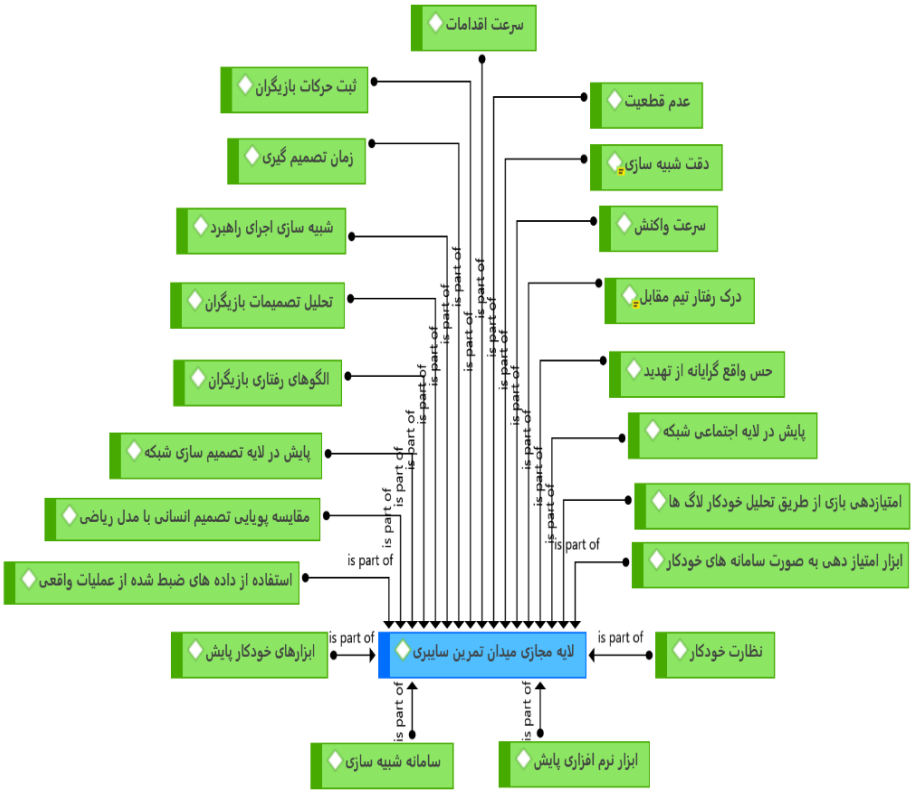
این عوامی در نمودار ۱ ارائه شده است.



نمودار ۱ عوامل لایه فیزیکی

در لایه مجازی، ۲۱ کد معتبر استخراج گردید که بیانگر مؤلفه‌های نرم‌افزاری، پلتفرم‌های شبیه‌سازی، ماشین‌های مجازی، سامانه‌های مدیریت سناریو، ابزارهای تهاجمی و تدافعی و محیط‌های تعامل سایبری هستند. این لایه به‌عنوان بُعدی پویا، نقش اصلی را در بازنمایی واقع‌گرایانه تهدیدات و سناریوهای سایبری ایفا می‌کند.

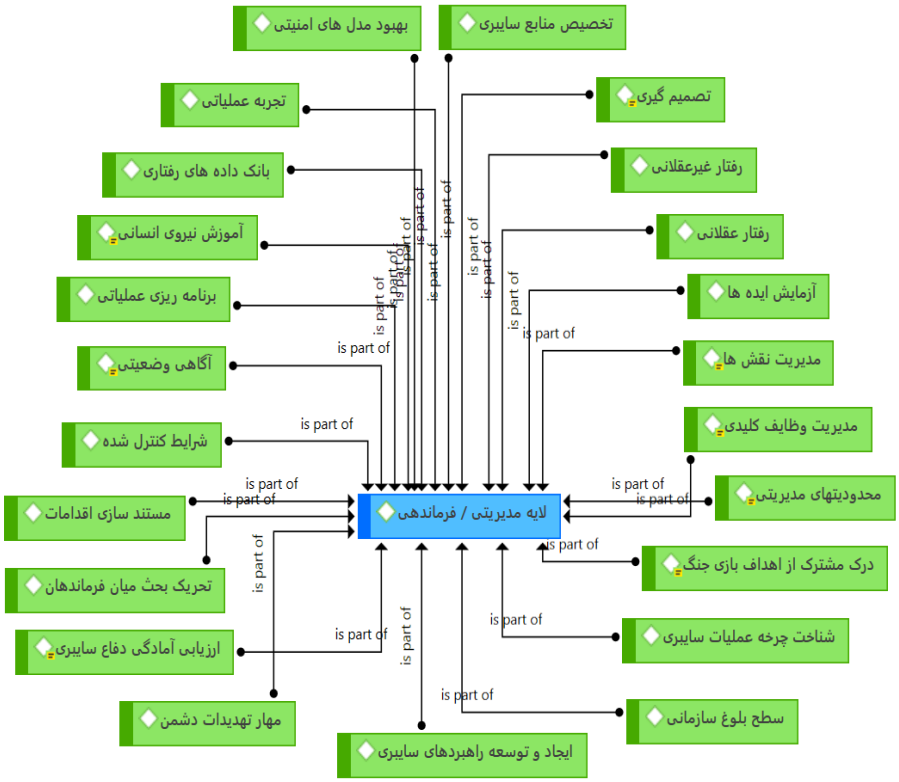
عوامل مناسب شناخته شدند مربوط به این لایه در نمودار ۲ ارائه شده است.



نمودار ۲ عوامل لایه مجازی

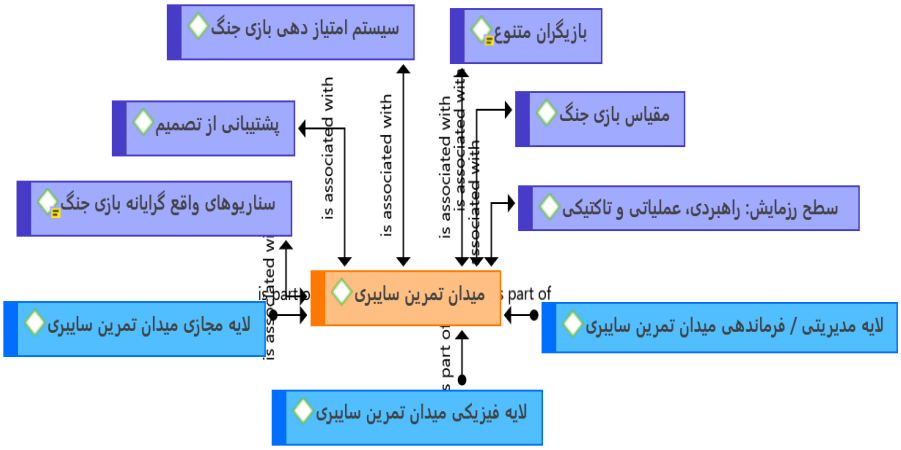
در لایه مدیریتی/فرماندهی، ۲۳ کد انتخابی واجد معیارهای لازم تشخیص داده شد. این مؤلفه‌ها بیشتر به حوزه‌های سیاست‌گذاری، مدیریت عملیات، کنترل سناریوها، ارزیابی عملکرد، تصمیم‌گیری راهبردی، ساختار فرماندهی و مدیریت دانش مربوط می‌شوند. نتایج نشان داد که این لایه به لحاظ تعداد و تنوع کدها، بالاترین پیچیدگی مفهومی را داراست که بیانگر نقش محوری آن در راهبری هوشمند میدان تمرین سایبری است.

عوامل مناسب این لایه در نمودار ۳ ارائه شده است.



نمودار ۳ عوامل لایه فرماندهی و کنترل

در نهایت، در بخش میدان تمرین سایبری، ۹ عامل کلیدی به‌عنوان مؤلفه‌های اصلی شناسایی شدند. سه عامل لایه مجازی، فیزیکی و فرماندهی/مدیریتی متغیرهای مستقل هستند و ۶ عامل دیگر ارائه شده در نمودار ۴، متغیرهای آشکار میدان تمرین سایبری هستند و به صورت مستقیم در این متغیر اثرگذارند. این عوامل بازتاب‌دهنده شاخص‌هایی نظیر واقع‌گرایی، انعطاف‌پذیری، مقیاس‌پذیری، قابلیت ارزیابی، سازگاری با تهدیدات نوظهور و پشتیبانی از سناریوهای چندلایه هستند که کیفیت و کارآمدی یک میدان تمرین سایبری را تعیین می‌کنند.



نمودار ۴ عوامل میدان تمرین سایبری

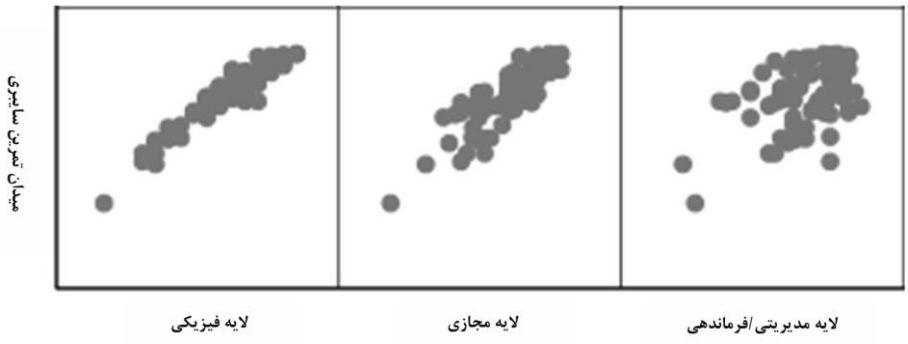
نتایج حاصل از تحلیل کیفی نشان داد که طراحی و استقرار یک میدان تمرین سایبری مؤثر، تابع یک ساختار چندلایه، سیستماتیک و به‌هم‌پیوسته است که هر یک از لایه‌ها کارکردی متمایز و درعین‌حال مکمل دیگر لایه‌ها دارند.

تحلیل کیفی انجام شده، موجب شکل‌گیری یک چارچوب مفهومی و بومی‌سازی‌شده میدان‌های تمرین سایبری در سطوح مختلف بازی جنگ شد که با بررسی روابط آن به‌صورت کمی می‌تواند مبنای طراحی مدل‌های پیشرفته آموزشی و میدان تمرین سایبری در بازی جنگ سایبری در محیط‌های عملیاتی آینده قرار گیرد.

به‌منظور بررسی روابط بین متغیرهای پژوهش، داده‌های کمی اولیه از طریق پرسشنامه مبتنی بر طیف لیکرت جمع‌آوری گردید. نظر به ماهیت داده‌ها و هدف مدل‌سازی رابطه بین چند متغیر مستقل و یک متغیر وابسته، از مدل رگرسیون خطی چندمتغیره به‌عنوان ابزار اصلی تحلیل استفاده شد. در این مدل، سه متغیر مستقل شامل لایه فیزیکی، لایه مجازی و لایه مدیریتی/فرماندهی به‌منظور تبیین و پیش‌بینی متغیر وابسته یعنی میدان تمرین سایبری وارد مدل شدند.

بررسی پیش‌فرض خطی بودن

در گام نخست، به‌منظور بررسی اولیه فرض خطی بودن رابطه بین متغیرها، نمودارهای پراکنش[1] ترسیم گردید. الگوی توزیع داده‌ها در نمودارها نشان داد که نقاط داده حول یک خط روند صعودی متمرکز شده‌اند که مؤید وجود رابطه‌ای خطی و مثبت میان متغیرهای مستقل و میدان تمرین سایبری است. از این‌رو، استفاده از رگرسیون خطی چندمتغیره برای مدل‌سازی روابط بین متغیرها، از نظر آماری توجیه‌پذیر و مناسب است.



نمودار ۵ پراکنش داده‌ها

برازش مدل رگرسیونی چندمتغیره

پس از آن، مدل رگرسیونی چندمتغیره بر داده‌ها برازش داده شد. مقدار ضریب همبستگی چندگانه (۰.۹۷۰) بیانگر وجود همبستگی بسیار قوی بین مجموعه متغیرهای مستقل و متغیر وابسته است. نتایج حاصل از مدل نشان داد که مقدار ضریب تعیین برابر با ۰.۹۴۱ است که بیانگر آن است که ۹۴،۱ درصد از واریانس (پراکندگی) متغیر میدان تمرین سایبری توسط سه متغیر مستقل موجود در مدل تبیین می‌شود. این مقدار بسیار بالا نشان‌دهنده قدرت تبیین‌کنندگی قابل‌توجه مدل و مناسب بودن متغیرهای انتخابی در توضیح تغییرات متغیر وابسته است. همچنین مقدار ضریب تعیین تعدیل‌شده برابر با ۰.۹۳۸ است نشان می‌دهد که حتی با در نظر گرفتن تعداد متغیرهای مستقل، مدل همچنان از قدرت تبیینی بسیار بالایی برخوردار است و دچار بیش‌برازش[2] نشده است.

1- Scatter Plot
2 - Overfitting

مقدار خطای استاندارد برآورد نیز برابر با ۰.۰۷۷محاسبه شد که نشان‌دهنده انحراف اندک مقادیر واقعی از مقادیر پیش‌بینی‌شده توسط مدل است.

جدول ۱ مدل رگرسیونی چند متغیره

مدل رگرسیونی چندمتغیره				
Model	ضریب همبستگی	ضریب تعیین	ضریب تعیین تعدیل‌شده	مقدار خطای استاندارد برآورد
۱	.۹۷۰A	.۹۴۱	.۹۳۸	.۰۷۷
متغیرهای مستقل: لایه مدیریتی/فرماندهی، لایه فیزیکی، لایه مجازی				

آزمون معناداری کلی مدل رگرسیونی

به‌منظور بررسی معناداری کلی مدل رگرسیونی، از تحلیل واریانس استفاده شد. نتایج این آزمون نشان داد که مقدار آمارهF برابر با ۳۸۵.۵۲۳ و سطح معناداری آن (Sig = ۰.۰۰۰ ۰.۰۵ > است؛ بنابراین فرض صفر مبنی بر عدم تأثیر همزمان متغیرهای مستقل بر متغیر وابسته، رد می‌شود و می‌توان نتیجه گرفت که مدل رگرسیونی در سطح اطمینان ۹۵ درصد از نظر آماری کاملاً معنادار است و برازش بسیار مناسبی با داده‌های مشاهده‌شده دارد. به‌عبارت‌دیگر، حداقل یکی از متغیرهای مستقل تأثیر معناداری بر میدان تمرین سایبری دارد.

جدول ۲ آنالیز واریانس

آنالیز واریانس						
منبع تغییرات		مجموع مربعات	درجه آزادی	میانگین مربعات	F	Sig.
Regression	۱	۶.۹۱۷	۳	۲.۳۰۶	۳۸۵.۵۲۳	.۰۰۰B
Residual		.۴۳۷	۷۳	.۰۰۶		
Total		۷.۳۵۳	۷۶			
متغیر وابسته: میدان تمرین سایبری						
متغیرهای مستقل: لایه مدیریتی/فرماندهی، لایه فیزیکی، لایه مجازی						

تحلیل ضرایب رگرسیونی و همبستگی

نتایج ضرایب رگرسیونی در جدول ۳ آمده است:

جدول ۳ همبستگی

همبستگی					
مدل		همبستگی استاندارد نشده		همبستگی استاندارد شده	t	Sig.
		B	Std. Error	Beta		
۱	(Constant)	-.۷۲۸	.۱۸۵		-۳.۹۲۷	.۰۰۰
	لایه فیزیکی	.۷۸۳	.۰۵۵	.۷۴۸	۱۴.۲۷۱	.۰۰۰
	لایه مجازی	.۲۱۸	.۰۶۰	.۱۹۲	۳.۶۴۲	.۰۰۱
	لایه مدیریتی/فرماندهی	.۱۶۷	.۰۳۶	.۱۳۹	۴.۵۹۸	.۰۰۰
متغیر وابسته: میدان تمرین سایبری						

تحلیل ضرایب استانداردشده (Beta) نشان می‌دهد که:

لایه فیزیکی با مقدار ۰.۷۴۸ = β بیشترین اثرگذاری را بر میدان تمرین سایبری دارد و قوی‌ترین پیش‌بین مدل محسوب می‌شود.

لایه مجازی با ۰.۱۹۲ = β در رتبه دوم قرار دارد و دارای تأثیر مثبت و معنادار بر متغیر وابسته است.

لایه مدیریتی/فرماندهی نیز با ۰.۱۳۹ = β کمترین میزان اثرگذاری نسبی را دارد، اما همچنان از نظر آماری معنادار است.

ضرایب غیراستاندارد (B) نشان می‌دهند که با افزایش یک واحد در هر یک از متغیرهای مستقل و در صورت ثابت بودن سایر متغیرها، مقدار میدان تمرین سایبری به ترتیب به‌اندازه ۰.۷۸۳، ۰.۲۱۸ و ۰.۱۶۷ واحد افزایش می‌یابد. منفی بودن مقدار ثابت مدل (۰.۷۲۸-) نشان‌دهنده سطح پایه پایین متغیر وابسته در غیاب متغیرهای مستقل است.

بحث و نتیجه‌گیری:

تحولات شتابان در حوزه فناوری‌های اطلاعاتی و ادغام گسترده آن با تمامی ابعاد نبرد در حوزه‌های زمین، دریا، هوا و فضا، ماهیت جنگ را به‌طور بنیادین متحول ساخته و

میدان نبرد را به محیطی چندلایه، پیچیده، داده‌محور و وابسته به تعامل مستمر انسان–ماشین تبدیل کرده است. در چنین شرایطی، «میدان تمرین سایبری» دیگر صرفاً یک محیط آموزشی نیست، بلکه به یک بستر برای آماده‌سازی نیروها، آزمون دکترین‌های آینده، ارزیابی واکنش‌ها و ارتقای توان تصمیم‌گیری در شرایط عدم قطعیت تبدیل شده است. در همین چارچوب، پژوهش حاضر با تمرکز بر شناسایی و تحلیل تأثیر سه متغیر مستقل شامل لایه فیزیکی، لایه مجازی و لایه فرماندهی و کنترل بر میدان تمرین سایبری به‌عنوان متغیر وابسته، تلاش کرده است یک تصویر جامع، ساختاریافته و مبتنی بر شواهد کیفی و کمی از عوامل اثرگذار بر کارآمدی و اثربخشی این میدان ارائه دهد.

یافته‌های کیفی این پژوهش مانند پیشینه‌ها نشان می‌دهد که میدان تمرین سایبری یک اکوسیستم چندبعدی است که در آن زیرساخت‌های سخت‌افزاری و تجهیزات فیزیکی، معماری‌های نرم‌افزاری و شبکه‌ای، داده‌ها، سناریوها، سازوکارهای کنترل، ساختارهای فرماندهی و رفتار عامل انسانی به‌صورت هم‌زمان و یکپارچه عمل می‌کنند؛ آنچه این پژوهش را متمایز می‌کند سنجش وزن لایه‌ها و مقایسه اثربخشی بین لایه‌های مختلف میدان تمرین است. میدان تمرین سایبری زمانی می‌تواند نقش یک «آزمایشگاه» را ایفا کند که میان ابعاد فیزیکی، مجازی و فرماندهی و کنترل آن، نوعی هم‌راستایی و هم‌افزایی ساختاری برقرار باشد.

در بعد کمی، نتایج حاصل از تحلیل همبستگی و رگرسیون چندمتغیره به‌روشنی نشان داد که هر سه متغیر مستقل – لایه فیزیکی، لایه مجازی و لایه فرماندهی و کنترل – دارای رابطه‌ای مثبت، مستقیم و از نظر آماری معنادار با میدان تمرین سایبری هستند. این بدان معناست که با ارتقای کیفیت و کارآمدی هر یک از این لایه‌ها، سطح اثربخشی میدان تمرین نیز به‌طور معناداری افزایش می‌یابد. در میان این متغیرها، لایه فیزیکی با برخورداری از بالاترین ضریب بتای استاندارد، به‌عنوان قوی‌ترین پیش‌بینی‌کننده میدان تمرین سایبری شناسایی شد. این نتیجه تأکیدی است بر نقش بنیادین زیرساخت‌های سخت‌افزاری، تجهیزات شبکه، سامانه‌های پردازشی، حسگرها و تجهیزات صنعتی شبیه‌سازی‌شده در شکل‌گیری یک میدان تمرین واقعی، پایدار و قابل اتکا. بدون وجود یک بستر فیزیکی قدرتمند و قابل اطمینان، حتی پیشرفته‌ترین معماری‌های نرم‌افزاری نیز قادر به بازنمایی دقیق پیچیدگی‌های میدان نبرد سایبری نخواهند بود.

در رتبه بعد، لایه مجازی نشـان داد که معماری شـبکه، سـاختار داده، منطق سـناریوها، شـبیه‌سـازی حملات و دفاع‌ها و به‌کارگیری ابزارهای هوشـمند در محیط تمرینی، سـهم قابل توجهی در ارتقای سطح واقع‌گرایی و کارآمدی میدان تمرین دارند. این لایه، میدان تمرین را از یک محیط ایستا به یک محیط پویا، تعاملی و تطبیق‌پذیر تبدیل می‌کند که قادر است رفتار دشمن، عدم قطعیت محیط و پیچیدگی تصمیم‌گیری در نبرد واقعی را به‌صورت قابل قبولی بازنمایی کند.

در این میان، اگرچه لایه فرماندهی و کنترل کمترین مقدار بتای اسـتاندارد را به خود اختصـاص داد، اما معناداری آماری آن نشـان می‌دهد که نقش عوامل انسـانی، سـاختار سلسله‌مراتب تصمیم‌گیری، هماهنگی بین واحدها، مدیریت سناریو، کنترل جریان بازی و تحلیل پس از عملیات، همچنان نقشـی اسـاسـی و غیرقابل‌چشـم‌پوشـی در موفقیت میدان تمرین سایبری ایفا می‌کند. به‌بیان‌دیگر، حتی در حضور پیشرفته‌ترین فناوری‌ها، این فرماندهی آگاه، تصمیم‌گیری هوشمند و مدیریت منسجم است که می‌تواند ظرفیت واقعی میدان تمرین را بالفعل سـازد و آن را به یک ابزار مؤثر برای تولید دانش نظامی و ارتقای آمادگی رزمی تبدیل کند.

ضریب تعیین بسیار بالا (۰/۹۴۱) بیانگر آن است که مدل ارائه‌شده در این پژوهش قادر است بیش از ۹۴ درصد از تغییرات مربوط به متغیر وابسته، یعنی میدان تمرین سایبری را تبیین کند.

در نهایت، تلفیق یافته‌های کیفی و کمی این پژوهش نشـــان می‌دهد که میدان تمرین سایبری باید نه به‌عنوان یک ابزار جانبی، بلکه به‌عنوان یک زیرساخت راهبردی و بخشی از توان رزمی آینده در نظر گرفته شـــود. کشـــوری که قادر باشـــد میان لایه فیزیکی قدرتمند، معماری مجازی پیشرفته و نظام فرماندهی و کنترل کارآمد یک پیوند منسجم برقرار کند، از مزیتی پایدار در حوزه آمادگی برای نبردهای آینده برخوردار خواهد شـد. بر این اساس، طراحی و توسعه میدان‌های تمرین سایبری نه‌تنها یک ضرورت فناورانه، بلکه یک ضـــرورت راهبردی-نظامی برای بقا، بازدارندگی و برتری در جنگ‌های چنددامنه‌ای آینده محسوب می‌شود؛ جنگ‌هایی که در آن‌ها، داده، تصمیم و زمان، به اندازه سلاح و آتش، تعیین‌کننده سرنوشت نبرد خواهند بود.

توصیه‌های کلیدی برای سیاست‌گذاران دفاعی

۱. **تقویت زیرساخت‌های فیزیکی:** زیرساخت فیزیکی میدان تمرین بازی جنگ سایبری باید به‌عنوان بخشی از توان رزمی ملی تعریف و در ردیف سرمایه‌گذاری‌های زیرساختی بلندمدت قرار گیرد، نه به‌صورت پروژه‌های مقطعی فناورانه. این امر مستلزم ایجاد مراکز تمرین سایبری دائمی، مستقل از شبکه‌های اداری و غیرنظامی، با سطح طبقه‌بندی امنیتی متناسب با مأموریت‌های مورد نیاز است. معماری این مراکز باید بر استفاده هم‌زمان از تجهیزات واقعی عملیاتی (مانند کنترل‌گرهای صنعتی، تجهیزات شبکه مأموریتی و سامانه‌های ذخیره‌سازی امن) و شبیه‌سازی فرآیندهای فیزیکی متکی باشد تا زنجیره «تصمیم سایبری–اثر فیزیکی» به‌صورت ملموس بازنمایی شود. علاوه بر این، طراحی زیرساخت باید مبتنی بر اصول تداوم مأموریت، تاب‌آوری در برابر حملات ترکیبی سایبری-فیزیکی و قابلیت اجرای تمرین‌های پیوسته و چند سناریویی باشد، زیرا یافته‌های پژوهش نشان می‌دهد که بدون یک بستر فیزیکی قدرتمند، سایر لایه‌های میدان تمرین توان تحقق کارکرد راهبردی خود را نخواهند داشت.

۲. **یکپارچگی لایه‌ها:** کارآمدی میدان تمرین سایبری زمانی محقق می‌شود که سه لایه فیزیکی، مجازی و فرماندهی/کنترل به‌صورت یک سامانه رزمی یکپارچه عمل کنند؛ به‌گونه‌ای که هر تصمیم در سطح فرماندهی، به‌صورت بلادرنگ به تغییر در محیط مجازی و درنهایت به اثر ملموس در لایه فیزیکی منجر شود. تحقق این یکپارچگی مستلزم طراحی سناریوهای چندلایه، استقرار داشبوردهای فرماندهی با نمایش هم‌زمان اثر فنی و پیامد مأموریتی و همسان‌سازی نقش تیم‌ها با ساختار واقعی رزم مشترک است تا تمرین سایبری به تمرین واقعی تصمیم‌گیری عملیاتی تبدیل شود.

۳. **سرمایه‌گذاری راهبردی و استفاده داده‌محور:** سرمایه‌گذاری در میدان تمرین سایبری باید با رویکرد داده‌محور و پیش‌دستانه انجام شود؛ به این معنا که هر بازی جنگ سایبری به‌عنوان منبع تولید داده رفتاری مهاجم و مدافع تلقی گردد و خروجی آن در بانک‌های داده تحلیلی برای بهبود مدل‌های پیش‌بینی، تصمیم‌یارهای فرماندهی و دکترین‌های دفاع سایبری به‌کار گرفته شود.

سیاست‌گذاران دفاعی می‌توانند با بهره‌گیری از این داده‌ها، پیش از اجرای واقعی قواعد درگیری، راهبردها و تصمیمات کلان، آن‌ها را در محیط کنترل‌شده میدان تمرین آزمون کرده و ریسک راهبردی تصمیم‌سازی در شرایط بحران واقعی را به‌طور معناداری کاهش دهند.

تشکر و قدردانی

این مقاله برگرفته از رساله دکتری مدیریت دفاعی دانشگاه فرماندهی و ستاد آجا است. نویسنده صمیمانه از استاد راهنمای محترم خود برای راهنمایی‌های ارزشمند علمی و حمایت مستمر در طول فرآیند پژوهش سپاسگزاری می‌کنند. همچنین تشکر ویژه‌ای از اساتید مشاور دارد که با ارائه دیدگاه‌های تخصصی، بازخوردهای سازنده و نظرات علمی خود، به ارتقای دقت و کیفیت این مطالعه کمک شایانی کردند. تعهد و تشویق آنان نقش مؤثری در موفقیت این پژوهش داشته است.

تضاد منافع:

بدین‌وسیله نویسندگان تصریح می‌نمایند که هیچ‌گونه تضاد منافعی در خصوص پژوهش حاضر وجود ندارد.

منابع

منبع فارسی

- طاهری، محمد، محمد زهرایی، سپهر و محمدی تودشکی، محمدرضا. (۱۳۹۹). فن‌آوری‌ها و روش‌های اجرای بازی جنگ سایبری. (e۱۲۲۳۲۹). دو فصلنامه بازی جنگ، ۳(۶)(DOI: https://doi.org/10.22034/ijwg.2020.122329)
- قاسمی تادوانی، محمد، علی محمدی، سجاد و حاجی علی اکبری، محمد. (۱۴۰۳). تاب‌آوری در فرماندهی و کنترل سایبری آینده. آینده‌پژوهی دفاعی، ۶۰-۲۷ ,(۳۵)۹. (DOI:https://doi.org/10.22034/dfsr.2025.2046026.1852)

منابع انگلیسی

- Bruvoll, S, Hannay, J. E. Svendsen, G, Asprusten, M. L, Fauske, K. M, Kvernelv, V. B, ... & Hyndøy, J. I. (2015, October). Simulation-supported wargaming for analysis of plans. In Proc. NATO Modelling and Simulation Group Symp. on M&S Support to Operational Tasks

Including War Gaming, Logistics, Cyber Defence (STO-MP-MSG-133). DOI: https://doi.org/10.1177/1548512919896855

- Carroll, J. M. (2023, June). Agile Methods For Improved Cyber Operations Planning. In ECCWS 2023 22nd European Conference on Cyber Warfare and Security (No. 1). Academic Conferences and publishing limited. DOI: https://doi.org/10.1016/j.promfg.2020.01.314
- Colbert, E. J, & Kott, A. (Eds). (2016). Cyber-security of SCADA and other industrial control systems (Vol. 66). Springer International Publishing. DOI: https://doi.org/10.1007/978-3-319-32125-7
- Colbert, E. J, Sullivan, D. T, & Kott, A. (2017). Cyber-physical war gaming. Journal of Information Warfare, 16(3), 119-133. DOI: https://doi.org/10.48550/arXiv.1708.07424
- Colbert, E, Sullivan, D, Wong, K, Smith, S, Stephenson, S, Sfakianoudis, V, ... & Andes, R. (2015). RED and BLUE teaming of a US Army SCADA system: table-top exercise final report. US Army Research Lab. Technical Report ARL-TR-7497. DOI: https://doi.org/10.1177/1548512918795061
- Evensen, P. I, Martinussen, S. E, Halsør, M, & Bentsen, D. H. (2019). Wargaming evolved: Methodology and best practices for simulation-supported wargaming. URL: https://hdl.handle.net/11250/2652599
- Ghasemi Tadavani,M, Ali Mohammadi,S. and HAJI ALIAKBARI,M. (2025). Resilience in future cyber command and control. Defensive Future Studies, 9(35), 27-60. [in Persian] DOI: https://doi.org/10.22034/dfsr.2025.2046026.1852
- Gortney, W. E. (2010). Department of defense dictionary of military and associated terms (No. JP102). URL: https://apps.dtic.mil/sti/tr/pdf/AD1024397.pdf
- Gurnani, R, Pandey, K, & Rai, S. K. (2014, March). A scalable model for implementing Cyber Security Exercises. In 2014 International Conference on Computing for Sustainable Global Development (INDIACom). DOI: https://doi.org/10.1109/IndiaCom.2014.6828048
- Hoffendahl, A. (2022). The Cyber Wargame Commodity Course of Action Automated Analysis Method. Theses and Dissertations. 5389. URL: https://scholar.afit.edu/etd/5389
- Holm, H, & Sommestad, T. (2016, November). Sved: Scanning, vulnerabilities, exploits and detection. In MILCOM 2016-2016 IEEE

Military Communications Conference (pp. 976-981). IEEE. DOI: https://doi.org/10.1109/MILCOM.2016.7795457

- Kick, J. (2014). Cyber exercise playbook. Tech. rep. MITRE CORP BED FORD MA, (No. MP140714). URL: https://apps.dtic.mil/sti/tr/pdf/ADA624910.pdf
- Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. Cyberpower and national security, 30. URL: https://ndupress.ndu.edu/ -Chap-02.pdf
- Kuehn, K. (2021). Assessment strategies for educational wargames. Journal of Advanced Military Studies, 12(2), 139-153. DOI: https://doi.org/10.21140/mcuj.20211202005
- Lantto, H, Åkesson, B, Suojanen, M, Tuukkanen, T, Huopio, S, Nikkarila, J. P, & Ristolainen, M. (2019). Wargaming the cyber resilience of structurally and technologically different networks. Security and Defence Quarterly, 24(2), 51-64. DOI: https://doi.org/10.35467/sdq/103346
- Lawshe, C.H. (1975). A QUANTITATIVE APPROACH TO CONTENT VALIDITY. Personnel Psychology, 28, 563-575. URL: https://doi.org/10.1111/j.1744-6570.1975.tb01393.x
- Mahmoud, R.V, Kidmose, E, Broholm, R, Pilawka, O. P, Dominika Illés, D, Magnussen, R, & Pedersen, J.M. (2020). Attack and Defend: Combining Game-Based Learning with Virtual Cyber Labs. In P. Fotaris (Ed.), Proceedings of the 14th European Conference on Games Based Learning (pp. 364-371). Academic Conferences International (ACI). DOI: https://doi.org/10.34190/GBL.20.150
- Morgan, A. S, & Stone, S. W. (2019). Command and Control for Cyberspace Operations-A Call for Research. Military Cyber Affairs, 4(1), 2378-0789. DOI: https://doi.org/10.5038/2378-0789.4.1.1051
- Pham, C, Tang, D, Chinen, K. I, & Beuran, R. (2016, December). Cyris: A cyber range instantiation system for facilitating security training. In Proceedings of the 7th Symposium on Information and Communication Technology (pp. 251-258). DOI: https://doi.org/10.1145/3011077.3011087
- Reddie, A. W, Booth, R. E, Goldblum, B. L, Lakkaraju, K, Reinhardt, J. C, Schneider, J, ... & DeMuth, J. (2024). Cyber Wargaming: Research and Education for Security in a Dangerous Digital World. Georgetown University Press. URL: https://press.georgetown.edu/Book/Cyber-Wargaming

- Rege, A, & Adams, J. (2019, July). The need for more sophisticated cyber-physical systems war gaming exercises. In ECCWS 2019 18th European conference on cyber warfare and security (p. 403). Academic Conferences and publishing limited. DOI: https://doi.org/10.1145/3375708.338031
- Singh, A. & Gupta, B. B. (2022). Distributed Denial-of-Service (DDoS) Attacks and Defense Mechanisms in Various Web-Enabled Computing Platforms: Issues, Challenges, and Future Research Directions. *International Journal on Semantic Web and Information Systems (IJSWIS)*, *18*(1), 1-43. DOI: https://doi.org/10.4018/IJSWIS.297143
- Staff, J. (2015). Joint training manual for the armed forces of the united states. Deparment of Defense, Washington DC. URL:https://www.jcs.mil/ CJCSM%203500.03F.pdf
- Taheri,M, Mohammad Zahraei,S. and mohammadi toudeshki,M. R. (2020). Technologies and approaches of cyber wargaming. (e122329). *Iranian Journal of Wargaming*, *3*(6), e122329. [in Persian] DOI: https://doi.org/10.22034/ijwg.2020.122329
- Tsai, P. W, & Yang, C. S. (2018). Testbed@ TWISC: A network security experiment platform. International Journal of Communication Systems, 31(2), e3446. DOI:: https://doi.org/10.1002/dac.3446
- Work, B, & Selva, P. (2015). Revitalizing wargaming is necessary to be prepared for future wars. War on the Rocks, 8. URL: https://warontherocks.com/2015/12/ for-future-wars
- Yamin, M. M, Katt, B, & Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security, 88, 101636. DOI:https://doi.org/10.1016/j.cose.2019.101636