Military Science and Tactics
https://www.qjmst.ir/

The components of the strategic cyber war game system of the armed forces of I. R. I

Sepehr Mohamadzahraei[1] ✉| Mohammad Reza Movahedisefat[2]| Shahram Norouzani[3]| Hamid Bigdeli[4]

Article type:
Research Article

Article history:
Received
13 January 2024
Received in revised form
30 July 2024
Accepted
23 November 2025
Published online
14 December 2025

Keywords:
Cyber war game, system, armed forces of the Islamic Republic of Iran

Abstract

Background and Objective: Determining the components of the Armed Forces' strategic cyber warfare game system.

Methodology: This research is of an applied type, which was conducted with the method of qualitative content analysis with a summarizing approach and using Max. QDA 2020 software. After analyzing the text, interviews were conducted with 7 experts and experts in the field of cyber war games in the armed forces. Since these experts are among the most experienced and specialized people in the field of armed forces war games, who were selected by a purposeful method of judgment, they have proper credibility. On the other hand, since the coding and theoretical sources of the interviews were carried out in the environment of Max. QDA 2020 software and it has great accuracy, the reliability of the research is also ensured.

Findings: 6 dimensions were counted to create a strategic cyber warfare game system. The research findings express the six main dimensions in the field of creating a strategic cyber war game system, which are: inputs and outputs of the war game system, war game processes, technologies, directional elements, Security and threats of the cyber environment of the game of cyber war

Conclusion: Among the dimensions of the cyber strategic war game, outputs and inputs are the most frequent, and cyber environmental factors are the least frequent components of the war game system.

Cite this article: Mohamadzahraei, S. Movahedisefat, MR. Norouzani, S & Bigdeli, D. (2025). The components of the strategic cyber war game system of the armed forces of I. R. I. *Military Science & Technics*, 73(21), 41-75.
DOI: http//doi. org/ 10. 22034/qjmst. 2025. 2020351. 2004
Publisher: AJA University of Command and Staff, https: //www. qjmst. ir

DOI: 10. 22034/qjmst. 2025. 2020351. 2004

1. Corresponding Author, Assistant Professor, Aja Command and Staff University, Tehran, Iran. E-mail: sep0319@gmail. com
2. Associate Professor, National Defense University, Tehran, Iran. E-mail: movahedisefat@gmail. com
3. Associate Professor, National Defense University, Tehran, Iran. E-mail: shahramkoohi@yahoo. com
4. Associate Professor, Aja Command and Staff University, Tehran, Iran. E-mail: h. bigdeli@casu. ac. ir

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

اجزاء سامانه بازی جنگ راهبردی سایبری نیروهای مسلح ج. ا. ا

سپهر محمدزهرایی [۱]✉| محمدرضا موحدی‌صفت [۲]| شهرام نوروزانی [۳]| حمید بیگدلی [۴]

اطلاعات مقاله

نوع مقاله:
پژوهشی

تاریخ دریافت:
۱۴۰۲/۱۰/۲۳

تاریخ بازنگری:
۱۴۰۳/۰۵/۰۹

تاریخ پذیرش:
۱۴۰۴/۰۹/۰۲

تاریخ انتشار:
۱۴۰۴/۹/۲۳

کلیدواژه‌ها:
بازی جنگ سایبری، سامانه، نیروهای مسلح جمهوری اسلامی ایران.

چکیده

زمینه و هدف: تعیین اجزاء سامانه بازی جنگ راهبردی سایبری نیروهای مسلح.

روش‌شناسی: این پژوهش از نوع کاربردی است که با روش تحلیل محتوای کیفی با رویکرد تلخیصی و با استفاده از نرم افزار مکس. کیو. دی. ای ۲۰۲۰ انجام شده است. پس از تحلیل متن، مصاحبه با ۷ نفر از خبرگان و صاحب‌نظران حوزه بازی جنگ سایبری در نیروهای مسلح انجام گرفت. از آنجا که این کارشناسان از خبره‌ترین و متخصص‌ترین اشخاص حوزه بازی جنگ نیروهای مسلح هستند که به روش هدفمند قضاوتی انتخاب شده‌اند، دارای اعتبار مناسب هستند. از طرفی چون کدگذاری و منابع نظری مصاحبه‌ها در محیط نرم افزار مکس. کیو. دی. ای ۲۰۲۰ انجام گرفته و دارای دقت فوق العاده‌ای است، پایایی تحقیق نیز تامین می‌شود.

یافته‌ها: ۶ بُعد برای ایجاد سامانه بازی جنگ راهبردی سایبری احصا شد. یافته‌های پژوهشی بیان‌کنندهٔ شش بُعد اصلی در زمینهٔ ایجاد سامانه بازی جنگ راهبردی سایبری است که عبارت‌اند از: درون‌دادها و برون‌دادهای سامانهٔ بازی جنگ، فرایندهای بازی جنگ، فناوری‌ها، ارکان جهت‌ساز، امنیت و تهدیدهای محیطی سایبری بازی جنگ سایبری.

بحث و نتیجه‌گیری: در بین ابعاد بازی جنگ راهبردی سایبری به ترتیب برون‌دادها و درون‌دادها بیشترین فراوانی و عوامل محیطی سایبری کمترین اجزاء سامانه بازی جنگ هستند.

استناد: محمدزهرایی، سپهر؛ موحدی‌صفت، محمدرضا؛ شهرام نوروزانی و بیگدلی، حمید. (۱۴۰۴). اجزاء سامانه بازی جنگ راهبردی سایبری نیروهای مسلح ج. ا. ا. *علوم و فنون نظامی*، ۲۱(۷۳)، ۷۵- ۴۱.

DOI: http//doi. org/ 10. 22034/qjmst. 2025. 2020351. 2004

ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران، https: //www. qjmst. ir

DOI: 10. 22034/qjmst. 2025. 2020351. 2004

۱. نویسنده مسئول، استادیار دانشگاه فرماندهی و ستاد آجا، تهران، ایران. رایانامه: sep0319@gmail. com

۲. دانشیار دانشگاه عالی دفاع ملی، تهران، ایران. رایانامه: movahedisefat@gmail. com

۳. دانشیار دانشگاه عالی دفاع ملی، تهران، ایران. رایانامه: shahramkoohi@yahoo. com

۴. دانشیار دانشگاه فرماندهی و ستاد آجا، تهران، ایران. رایانامه: h. bigdeli@casu. ac. ir

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

The components of the strategic cyber war game system of the armed forces of I. R. I
Extended Abstract

Background and Objective:
With the advancement of technologies related to cyber areas, threats related to infiltration, disruption, and sabotage in these areas have also increased, and decision-makers of organizations interested in these areas must be able to make appropriate decisions in the event of any of the threats, and the relevant users must also be able to act on these decisions correctly. The emergence of the number and variety of cyber attacks requires that countries take decisive measures against them. These precautionary measures range from personal measures such as awareness of cyber risks, having situational awareness to strategic measures such as having a national cybersecurity document, and forming a computer incident response team. One of the cases that creates and strengthens this ability in decision-makers and users is the cyber war game, which can greatly reduce the effects of these threats if the information, skills, and abilities related to this area are improved (Mohammadi; Zahraei, 2010). Also, the cyber strategic war game is a suitable method for depicting the international, regional and domestic situation and conditions of both sides of the geographical area of possible conflict, which, while explaining the war scene of the Islamic Republic of Iran, takes into account the political and military goals of the opponents and ultimately describes how their armed forces will perform in the form of a military invasion of the Islamic Republic of Iran and its consequences from the perspective of both sides, and formulates the exercise of possible future war options according to operational requirements (Afshardi; Norouzani, 2018). Cyber strategic war games, by providing realistic battlefield conditions, can lead to the creation of an integrated and homogeneous structure among armed forces. Cyber wars are like real physical wars, they start in cyberspace and have an impact in real life. (Karaman et al. , 2016) The game of strategic cyber war can lead to the creation of a unified and homogeneous structure between the armed forces due to providing the real environmental conditions of the battle scene. It will also be a suitable tool for depicting the international, regional and domestic situation of the warring parties in the cyber field. For this reason, the question of the current research is, what are the components of the strategic cyber war game system of the armed forces?
Methodology:
This research aims to identify the components of the cyber strategic war game system and its results will be used in the Armed Forces of the Republic of Iran, therefore, the research method, in terms of its purpose, is of an applied type and will have scientific utility. The research method is qualitative in nature and is carried out by analyzing the content of documents, a summary approach, and using the Max. QDA 2020 software. In qualitative content analysis with a summary approach, data analysis is performed by searching for specific words and open coding. Numerous words for each term are identified and calculated, and axial coding is performed. Then, the relationship between dimensions and components is obtained through interview analysis, and various graphs are extracted with the software. Here, the researcher wants to know how many times and by whom the term in question has been used, either directly or indirectly, in order to thematize the codes based on them. (Iman; Noshadi, 2011).
Findings:
6 dimensions were counted to create a strategic cyber warfare game system.
The research findings express the six main dimensions in the field of creating a strategic cyber war game system, which are: inputs and outputs of the war game system, war game processes, technologies, directional elements, Security and threats of the cyber environment of the game of

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

cyber war.

In other historical studies, Jahromi (2019) considers the various components of a war game to include the environment and scenario, players and their decisions, rules and procedures and arbitration, simulation, database, support and analysis. Moradian (2012) divides the role of topologies in a war game into operations topology, command topology and information topology. Afshardi et al. (2018) consider war game approaches in design to include analysis approach, architecture approach and artistic approach. Bay Fox (2018) introduces the key elements of a cyber war game as scope, organizational performance, system environment, cyber defense technologies, threats and scenarios. In its research paper, the prestigious article Rand Research Institute has introduced the variables of the cyber strategic warfare game scene: the number and type of enemies and opponents, the level of accuracy and security equipment of the enemies, the type and capabilities of the players' defensive and offensive systems, the location and area of the enemy's communication networks and servers, the level of difficulty and complexity of the game stages, military strategies and tactics of battle in cyberspace.

Among the dimensions of the cyber strategic war game, outputs and inputs are the most frequent, and cyber environmental factors are the least frequent components of the war game system.

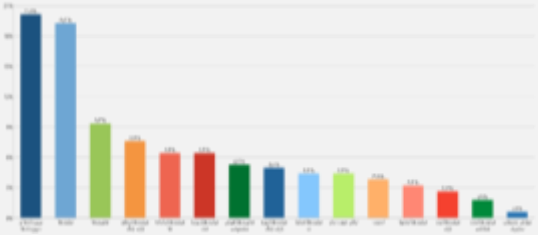


Chart (1): Showing the percentage of frequency of components of the cyber strategic warfare game system

Chart (2): Frequency of dimensions and components of the cyber strategic war game

Conclusion:

Based on the study and review of texts obtained from interviews with experts, the components of the Iranian Armed Forces' strategic cyber war game system were identified and categorized into six dimensions, which are: 1- Inputs and outputs of the war game system, 2- War game processes, 3- Technologies involved in the war game, 4- Direction-making elements, 5- Security, and 6- Cyber environmental threats of the cyber war game.

Keywords: *Cyber war game, system, armed forces of the Islamic Republic of Iran*

مقدمه

نیروهای مسلّح جمهوری اسلامی ایران باید جهت مقابله با هرگونه تهدید، آمادگی رزمی خود را ارتقاء دهند. این آمادگی باید در هر یک از پنج حوزهٔ تعریف شده جنگ (زمین، دریا، هوا، فضا و فضای سایبر) باشد. جنگ سایبری با شروع دورهٔ انقلاب علوم و فناوری‌ها، به خصوص فناوری اطلاعات، ارتباطات، الکترونیک و رایانه در سال‌های اخیر طراحی شده است و در حال حاضر سیر تکاملی خود را طی می‌نماید. کشورهایی که ابزار و سهم و توان بیشتر در استفاده از آن را داشته باشند جهت دستیابی به اهداف مدنظر خود موفق‌تر عمل می‌کنند. توجه و حساسیت به مقوله امنیت ملی، در هزاره‌ای که تمام نیروی اکثر حاکمان زورگو متوجه و متمرکز بر تجاوز و نفوذ است، امری کاملاً ضروری و اجتناب ناپذیر است. بدون شک هر لحظه دشمن می‌تواند در حال طرح‌ریزی حمله باشد و تنها یک راه یا روزنه نفوذ کافی است تا وی به قصد خود نائل گردد. در تعریفی سنتی سربازان از مرزهای جغرافیایی حفاظت می‌کنند و مسئولین فرهنگی به تهاجم فرهنگی می‌اندیشند. با پیشرفت فناوری‌های مرتبط با حوزه‌های سایبری، تهدیدات مربوط به نفوذ، اختلال و خرابکاری در این حوزه‌ها نیز بیشتر شده است و تصمیم‌گیران سازمان‌های ذی‌نفع در این حوزه‌ها باید قادر باشند در صورت بروز هریک از تهدیدها، تصمیم‌های مناسبی اتخاذ و کاربران مربوطه نیز باید بتوانند به این تصمیم‌ها به نحو صحیح عمل نمایند. ظهور تعداد و تنوع حملات سایبری ایجاب می‌کند که کشورها اقدامات قاطعانه‌ای را علیه آنها انجام دهند. این اقدامات احتیاطی از اقدامات شخصی مانند آگاهی از خطرات سایبری، داشتن آگاهی موقعیتی تا اقدامات راهبردی مانند داشتن یک سند ملی امنیت سایبری، تشکیل تیم واکنش به حوادث رایانه‌ای[1] را شامل می‌شود. [2] یکی از مواردی که این توانایی را در تصمیم‌گیران و کاربران ایجاد و تقویت می‌نماید بازی جنگ سایبری بوده که در صورت ارتقای معلومات، مهارت‌ها و توانایی‌های مرتبط با این حوزه، تا حدود زیادی می‌توان از اثرات این تهدیدها کاست (محمدی و زهرایی، ۱۳۹۹: ۱۲). بازی جنگ راهبردی سایبری به دلیل مهیاکردن شرایط محیطی واقعی صحنهٔ نبرد می‌تواند به ایجاد یک ساختار یکپارچه و همگن بین

[1] CERT

[2] کارامان و همکاران، ۲۰۱۶

نیروهای مسلح بینجامد. جنگ‌های سایبری مانند جنگ‌های فیزیکی واقعی هستند، در فضای سایبری شروع می‌شوند و در زندگی واقعی اثر می‌گذارند (کارامان و همکاران، ۲۰۱۶). همچنین بازی جنگ راهبردی سایبری، روش مناسب برای به تصویر کشیدن وضعیت و شرایط بین‌المللی منطقه‌ای و داخلی دو طرف حوزه جغرافیایی درگیر محتمل بوده که ضمن تبیین صحنه جنگ جمهوری اسلامی ایران، اهداف سیاسی نظامی حریفان را مدنظر قرار می‌دهد و در نهایت چگونگی عملکرد نیروهای مسلح آنها را در قالب تهاجم نظامی به جمهوری اسلامی ایران و پیامدهای آن از دیدگاه دو طرف توصیف کرده و تمرین گزینه‌های جنگ محتمل آینده را با توجه به نیازمندی‌های عملیاتی تدوین می‌کند (افشردی و نوروزانی، ۱۳۹۷). می‌توان مدعی شد که بهره بردن از بازی جنگ واقعی، بسیاری از زوایا و مشکلات نادیده یک جنگ را آشکار نموده و مزایای رقابتی نسبت به حریف را عیان خواهد نمود. طبیعی است هر کشوری به این نکات و الزامات دست‌یابد، ابتکار عمل را به دست خواهد گرفت و نسبت به حریف برتری و اشراف اطلاعاتی خواهد داشت. نکته اینجاست که از عوامل برترساز در بکارگیری بازی جنگ در فضاهای ذکرشده‌ی قبل از فضای سایبری (زمین، دریا، هوا، فضا) می‌توان به مزایایی چون صرفه‌جویی در وقت و منابع سازمان، افزایش اعتماد به طرح‌ها و برنامه‌ها و ایجاد فرهنگ سازمانی مطلوب اشاره نمود.[۱] بدیهی است که عوامل ذکر شده فوق در فضای سایبر تعیین‌کننده، حتی پررنگ‌تر نیز شده‌اند. اما فضای سایبری دارای ویژگی‌های خاص خود است که مستقیما به جنسیت متفاوت آن نسبت به سایر حوزه‌های سنتی برمی‌گردد؛ پرداختن به سامانه بازی جنگ راهبردی سایبری مسائل خاص خود را دارد. از جمله این مسائل، جدید بودن (به این معنا که به هرجهت با بازی جنگ در سایر عرصه‌ها متفاوت است.)، ابهام آمیزبودن (متاثر از خاصیت خود فضای سایبری)، پویایی بسیار زیاد (متاثر از خاصیت خود فضای سایبری)، پیچیدگی بسیار زیاد (متأثر از خاصیت خود فضای سایبری)، بررسی تلفیقی سطح راهبردی جنگ سایبری در حوزه‌های گوناگون جنگ (سیاسی، اقتصادی، نظامی، فناوری، عملیات روانی و...) به صورت توامان برای راهبردپردازان جنگ و تصمیم گیرندگان سیاسی – نظامی دشوار خواهد بود. فراهم‌سازی طرح اولیه اختصاص و گسترش بازیگران سایبری در

[۱] اورمه، ۲۰۱۳

صحنه‌های عملیاتی سایبری در سطح نیروهای مسلح نیاز به مطالعات پیشینه‌ای و اکتشافی بسیار زیاد و عمیقی دارد. افزون بر موارد بالا، برآورد هزینه‌های احتمالی ناشی از تصمیمات راهبردی جنگ سایبری در صحنه جنگ و عملیات بسیار مشکل به نظر می‌رسد.

نگارندگان مقاله حاضر نشان داده‌اند، ایجاد سامانه بازی جنگ راهبردی سایبری نیروهای مسلح جمهوری اسلامی ایران نقش مهمی در ایجاد آگاهی وضعیتی، اشراف اطلاعاتی و درک نزدیک به واقعیت مسئولان از صحنه جنگ دارد.

بنابراین پژوهش حاضر با هدف یافتن اجزاء سامانه بازی جنگ راهبردی سایبری نیروهای مسلح ج. ا. ا، مورد بررسی قرار گرفته است. سپس دربخش های بعدی، روش پژوهش پیشنهادی به صورت کامل شرح داده شده و نتایج حاصل گزارش شده است. در انتها نیز پس از جمع‌بندی محتوای ارائه شده، روش‌هایی برای پیشبرد مطالعات آتی پیشنهاد شده است.

با نگرش به مراتب یاد شده بالا، چنین به نظر می‌رسد که باید سامانه‌ای برای بازی جنگ سایبری طراحی گردد و در آن، اجزاء در سطح نیروهای مسلح کشور مشخص و روشن شود. در همین راستا دغدغه اصلی محقق این است که اجزاء سامانه بازی جنگ راهبردی سایبری نیروهای مسلح جمهوری اسلامی ایران کدامند؟

مبانی نظری و پیشینه‌های پژوهش

سامانه [1]

واژه «سامانه» از علوم دقیقه، به‌ویژه فیزیک، به علوم اجتماعی راه‌یافته است. در علوم اجتماعی که با متغیرهایی بسیار پیچیده‌تر و اغلب چند بُعدی سروکار دارند، این نوع تعریف کاربرد کمتری دارد. تعریفی که در اینجا ارائه می‌گردد یک تعریف کاربردی است. باوجودآنکه این تعریف غیر کمّی است، ولی مانند آنچه در علوم دقیقه مطرح می‌شود، تعریفی کاملاً دقیق و جامع است:

سامانه، مجموعه‌ای از اجزا و روابط میان آن‌ها است که توسط ویژگی‌هایی معین، به هم وابسته یا مرتبط می‌شوند و این اجزا با محیطشان یک کل را تشکیل می‌دهند (هال و فاگن، ۱۹۶۸: ۸۱). این تعریف دو ویژگی دارد:

[1] system

اول آنکه، به‌اندازه کافی جامع است و کاربرد گسترده‌ای دارد. دوم آنکه، به‌اندازهٔ کافی ژرف‌نگری دارد؛ به‌گونه‌ای که همه‌ی عناصر لازم برای تمیز و شناسایی سامانه‌ها را معرفی می‌کند (رضائیان، ۱۳۸۲: ۲۷).

سامانه مجموعه‌ای از دو یا چند عنصر است که دو شرط زیر را داشته باشد: ۱- هر عنصر سامانه بر رفتار و یا ویژگی‌های کل سامانه، مؤثر است. ۲- بین عناصر سامانه ازنظر رفتاری و نوع تأثیر بر کل سامانه، وابستگی متقابل وجود دارد.

بازی جنگ راهبردی سایبری

فرایند، الگوسازی و شبیه‌سازی جنگ در قالب بازی جنگ به منظور به‌کارگیری همه‌جانبه عوامل قدرت سایبری در سطح ملی به منظور دستیابی به اهداف جنگ را گویند (محقق ساخته).[۱]

عناصر سامانه

عناصر یک سامانه عبارت‌اند از: درونداد، فراگرد (خانه پردازش)، برونداد و بازخور کنترلی (رضائیان، ۱۳۸۲: ۲۸).

جنگ[۲]

جنگ یک درگیری شدید مسلحانه میان دولت‌ها، حکومت‌ها، جوامع یا گروه‌های شبه‌نظامی مانند مزدورها، شورشگران و شبه‌نظامیان است. از آن‌جا که جنگ یک درگیری مسلحانه واقعی، ارادی و گسترده بین جوامع سیاسی است می‌توان آن را نوعی خشونت سیاسی تلقی کرد (میرشکاری، ۱۳۹۶).

زدوخورد با جنگ‌افزار میان گروه‌ها، اقوام، یا کشورهای دشمن، مقابله و برخورد نیروهای نظامی، تعریف راهبرد، عمل تجهیز و به‌کارگیری نیروها و توانایی‌ها در جهت دستیابی به هدفی معین (فرهنگ سخن انوری، ۱۳۸۶: ۲۲۰۰).

بازی جنگ سایبری

بازی جنگ سایبری روشی است برای بررسی آنچه در یک سامانه یا سازمان به‌خصوص

---

[۱] بر اساس نشست خبرگی با حضور پنج تن از صاحب‌نظران این عرصه، در تاریخ ۱۴۰۱/۸/۱ ، در دانشکده امنیتِ دانشگاه عالی دفاع ملی، حاصل شد.

[۲] میرشکاری، جواد؛ فرهنگ واژه‌های مصوب فرهنگستان، دفتر چهارم؛ انتشارات فرهنگستان زبان و ادب فارسی، ۱۳۹۶

در مواجهه با حمله‌های سایبری فرضی یا واقعی اتفاق می‌افتد. بازی جنگ سایبری بدین‌صورت تعریف‌شده است: "یک تمرین تعاملی است که شرکت‌کنندگان را در یک سناریوی حمله سایبری شبیه‌سازی شده، مانند شکاف داده‌ها، حذف وب‌گاه،"حمله ممانعت از خدمات"[۱] یا کشف بدافزارهای پیشرفته در یک شبکه مشارکتی، دخالت می‌دهد. "[۲] (آندرس، ۲۰۱۱) ابزار بازی جنگ سایبری برای ارزیابی قابلیت‌های فعلی و آینده، برنامه‌ریزی، بررسی سناریوهای احتمالی و کارکنان آموزشی در سازمان‌ها ابزار مفیدی است. (طاهری، زهرایی، ۱۳۹۹: ۲۷)

یک تمرین تعاملی است که شرکت‌کنندگان را در یک سناریوی حمله سایبری شبیه‌سازی شده، مانند شکاف داده‌ها، حذف وب‌گاه، "حمله ممانعت از خدمات"[۳] یا کشف بدافزارهای پیشرفته در یک شبکه مشارکتی، دخالت می‌دهد. "[۴و۵]

صحنه جنگ سایبری

«صحنه جنگ» آن قسمت از خشکی، دریا و فضا است که به‌طور مستقیم درگیر عملیات جنگی است و یا در آینده خواهد بود. با توجه به پیشرفت فناوری و توسعه جنگ‌افزارها ممکن است صحنه جنگ تمام کره زمین و حتی در آینده کرات دیگر را نیز دربر گیرد. لذا برای صحنه جنگ نمی‌توان حدومرز مشخصی قائل شد، همچنین با توجه به وسعت و دامنه جنگ، ممکن است صحنه جنگ، فرماندهان متعددی داشته باشد. [۶] «کیائو» و «وانگ»، دو استراتژیست چینی، میدان جنگ سایبری را این‌گونه تعریف می‌کنند: «میدان نبرد در کنار شماست و دشمن در شبکه است. فقط نه بوی باروت می‌آید و نه بوی خون». [۷]

---

[1] DOS

[2] Frank Anders, "Unexpected Game Calculations in Educational Wargaming: Design Flaw or Beneficial to Learning?" in *DiGRA '11 - Proceedings of the 2011 DiGRA International Conference: Think Design Play* (DiGRA/Utrecht School of the Arts, 2011), 3, http://www.digra.org/wp-content/uploads/digital-library/11310.31521.pdf.

[3] DOS

[4] Frank Anders, "Unexpected Game Calculations in Educational Wargaming: Design Flaw or Beneficial to Learning?" in *DiGRA '11 - Proceedings of the 2011 DiGRA International Conference: Think Design Play* (DiGRA/Utrecht School of the Arts, 2011), 3, http://www.digra.org/wp-content/uploads/digital-library/11310.31521.pdf.

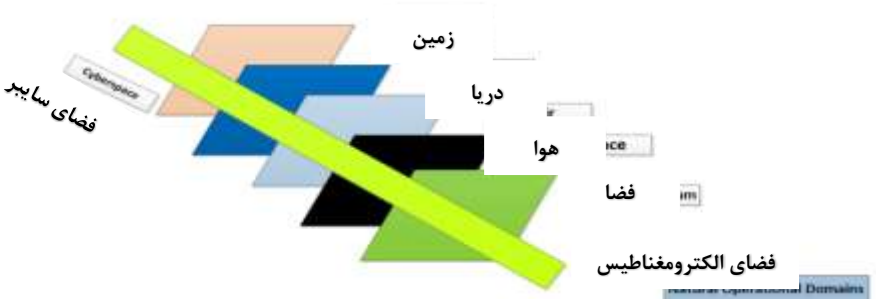
[۵] آندرس، ۲۰۱۱

[۶] ملکی و همکاران، ۱۴۰۰

[۷] کارامان و همکاران، ۲۰۱۶

فضای نبرد سایبری

فضای نبرد سایبری منحصر به فرد است و چالش‌های قابل توجهی را برای طراحان بازی‌های جنگ ارائه می‌دهد. فضای سایبری به شکل واقعیت افزوده با «دنیای واقعی» همپوشانی دارد. این فضا بی‌نهایت بزرگ و کوچک است. این فضا یک نوع انتقال از راه دور در اختیار ما قرار می‌دهد که به کاربر اجازه می‌دهد فوراً در هر نقطه از فضای سایبری حرکت کند. فضای سایبری را می‌توان به عنوان یک بعد موازی در نظر گرفت. از طریق شش حوزه عملیاتی طبیعی مشترک در درگیری‌های متعارف می‌گذرد. شکل ۱ - (حوزه‌ها شامل زمین، دریا، هوا، فضا و طیف الکترومغناطیسی هستند). (میسون: ۲۰۲۰)[1]



شکل (۱) حوزه‌های عملیاتی طبیعی و رابطهٔ آن‌ها با حوزه سایبری (آیین نامه مشترک ۱۲-۳ وزارت دفاع آمریکا)

عناصر کلیدی جنگ سایبری

تمرینات جنگ سایبری شامل عناصر کلیدی زیر است. شیوع و عمق عناصر خاص می‌تواند از یک نوع تمرین به دیگری متفاوت باشد، اما همه آن‌ها به شکلی مورد توجه قرار می‌گیرند.

- ✓ **دامنه**

دامنه یک تمرین بر اساس هدف آن شکل می‌گیرد. در اینجا دامنه تعریف‌شده شامل زمینه‌های سامانه فناوری اطلاعات سازمانی و شبکه‌ای است. دامنه سامانه‌های فناوری اطلاعات شبکه‌ای که باید در تمرین گنجانده شوند، توسط حوزه سازمانی تنظیم و اعلام می‌شود.

[1] https://www.lecmgt.com/blog/designing-cyber-wargames

✓ **عملکردهای کسب‌وکار**

بیشتر بازی‌های سایبری فراتر از وجود آسیب‌پذیری و برای یک بهره‌برداری خاص استفاده می‌شود؛ و بررسی می‌کند که چگونه برخی از سطوح عملکردهای تجاری می‌توانند تحت تأثیر قرار گیرند. این‌ها می‌توانند هر چیزی از عملکردهای سطح پایین، مانند انجام یک تراکنش بانکی برخط، عملیات راهبردی در داخل یک موسسه مانند انجام ادغام و پشتیبانی خرید تا عملکردهای چند موسسه مانند پردازش پرداخت‌ها باشند. در هر سطحی که باشد، عملکردهای کسب‌وکار به‌نوعی در جنگ سایبری تعریف و نشان داده می‌شوند. عملکردهای کسب‌وکار شامل کاربران، رویه‌ها، برنامه‌های کاربردی، کسب‌وکار خودکار و دارایی‌های اطلاعاتی است. [۱]

✓ **محیط سامانه**

محیط سامانه فناوری اطلاعات، اگرچه ممکن است در مورد تمرین روی میز یا شبیه‌سازی واقعی در بستر آزمایش در مورد تمرین تیم قرمز بسیار انتزاعی باشد، یک عنصر حیاتی در جنگ سایبری است. محیط سامانه تا حد زیادی تعیین می‌کند که چه مجموعه‌ای از استراتژی‌ها و مکانیسم‌های حمله مرتبط هستند و چه ارتباطات متقابلی در دسترس هستند تا به مهاجمان اجازه دهند از یک نقطه ورودی اولیه به سمت دارایی‌های هدف حرکت کنند. محیط سامانه شامل اجزای شبکه، نقاط پایانی کاربر، سرورهای برنامه و داده، توپولوژی و اتصالات خارجی است. [۲]

✓ **فناوری‌های دفاعی سایبری**

سازمان‌ها باید به‌طور مداوم یاد بگیرند که باوجود تدابیر امنیتی موجود، دشمن چه‌کاری می‌تواند انجام دهد. برای اینکه بازی سایبری به یک موقعیت واقعی مرتبط باشد، حفاظت‌های امنیت سایبری که در محیط فناوری اطلاعات تعبیه شده است، مانندبخش بندی، فایروال‌ها و پالایه[۳]ها، پیکربندی‌های امنیتی نقطه

---

[۱] بی‌فاکس، دی‌مک‌کلام و آی‌آرنوت و جی‌مک، ۲۰۱۸، ص۶

[۲] همان، ص۶

[۳] معادل پارسی «فیلتر»

پایانی، احراز هویت و کنترل دسترسی باید در مدل سامانه مورداستفاده قرار گیرند. بازی جنگ علاوه بر این، مجموعه ابزار دفاع سایبری سازمان، مانند حسگرهای تشخیص و ابزارهای نظارت و مدیریت امنیت سایبری باید ارائه شود. این‌ها باید شامل قابلیت‌های دفاع سایبری در شبکه و سامانه‌های دفاع‌شده باشد، نه فقط در محیط‌ها. بخشی از بازی جنگی شامل برخورد با دشمنانی است که قبلاً از طریق ابزارهای مختلف به محیط نفوذ کرده‌اند و در دارایی‌های دفاع شده عمل می‌کنند. [۱]

- ✓ **تهدید**

یک مدل تهدید خاص یک ضرورت برای جنگ سایبری است. برای مؤثرتر بودن، باید نوع دشمنانی که محیط‌های فناوری اطلاعات سازمان‌ها را در بازی جنگ هدف قرار می‌دهند، همراه با اهداف و قابلیت‌های خاص آن‌ها تعریف شود. (تهدیدها همچنین می‌توانند شامل تهدیدهای غیر انسانی، مانند بلایای طبیعی، یا به‌عنوان یک تهدید مستقل یا همراه با تهدیدات دیگر باشند.) لازم نیست تهدید به آنچه سازمان واقعاً در دنیای واقعی تجربه کرده است محدود شود. یک بازی جنگ سایبری می‌تواند سطحی از قابلیت‌های دشمن را ایجاد کند که سازمان هنوز در عمل ندیده است و درواقع می‌تواند مهم باشد که دفاع سایبری و کارکنان سازمان به چنین چالشی واکنش نشان دهند. با این حال، از یک جنگ سایبری که در آن تهدید یا دست‌کم گرفته‌شده و محدود به حملات فرصت طلبانه بی‌اهمیت است، یا اغراق آمیز و قادر به انجام حملات غیرواقعی و غیرقابل اجرا هستند، چیز کمی می‌توان آموخت. [۲]

- ✓ **سناریوها**

یک سناریو داستانی را ارائه می‌دهد که شرکت کنندگان در طول جنگ سایبری تجربه می‌کنند و به آن واکنش نشان می‌دهند. این سناریو مشخص می‌کند که وضعیت خاص چیست: در زمینه کسب‌وکار چه اتفاقی می‌افتد، دشمن کیست، چه دارایی‌هایی هدف قرارگرفته‌اند و برای چه هدفی. این سناریو همچنین ممکن

---

[۱] همان، ص۷

[۲] همان، ص۸

است مشخص کند که چگونه دشمن با استفاده از دسترسی به دست آمده، به سازمان آسیب می‌رساند، نتایج حملات سایبری علیه سایر سازمان‌ها، اقدامات واقعی انجام شده در ارتباط با حمله سایبری، اطلاعات گزارش شده در مطبوعات یا از طریق منابع اطلاعاتی تهدید و چگونه دشمن، شدت تلاش خود را افزایش می‌دهد یا در صورت ناکام ماندن حمله، حملات دیگری را دنبال می‌کند. (بی‌فاکس، دی‌مک‌کلام و آی‌آرنوت و جی‌مک، ۲۰۱۸، ص۸)

پیشینه‌های پژوهش

جدول (۱) پیشینه تحقیقات انجام شده

کشور	اهداف	افق زمانی	نتایج	روش‌شناسی‌ها
ایالات متحده (۲۰۱۹)	انتشار راهبرد "دفاع رو به جلو". تفکر وزارت دفاع امریکا به‌عنوان تامین کننده اصلی امنیت ملی آمریکا در مواجهه با حملات سایبری از سوی مهاجمین به زیرساخت های حیاتی ایالات متحده	۱۵ سال	در این گزارش در مرحله اول یک سناریو معرفی شده است و سپس بازی جنگ با مفروض دانستنِ کشورهای آبی، قرمز، سبز و بی‌طرف با معرفی قابلیت‌های این کشورها در حوزه‌های حاکمیتی، اقتصادی، دیپلماسی، نظامی و سیاسی اجرا شده است. دربخش دوم، یافته‌های بازی جنگی با استفاده از داده‌های جمع‌آوری‌شده از بازی، تمرکز بر اقدامات‌بخش خصوصی و تأثیرگذاری بر آن، مورد بحث قرار گرفته است. در نهایت پیامدهای بالقوه برای راهبردهای سایبری و همچنین مسائلی برای تحقیقات بیشتر، تجزیه و تحلیل و بازی جنگ ارائه شده است.	تحلیل سناریو
جمهوری اسلامی ایران (۱۳۹۹)	تبیین چارچوب بازی جنگ سایبری	۱۰ سال	هردو نوع بازی جنگ؛ تحلیلی و عملیاتی، ثابت کرده‌اند برای کمک به پیشرفت تأثیرگذاری امنیت و کنترل در بسیاری زمینه‌های عملیاتی، فرآیند سودمندی بوده‌اند. تمرینات تحلیلی شامل؛ ارتباطات مقطعی بین تیم‌ها، واکنش‌های ناگهانی،	دلفی فناورانه

کشور	اهداف	افق زمانی	نتایج	روش‌شناسی‌ها
			جمع‌آوری و توزیع اطلاعات و مدیریت سناریوهای پاسخ‌دهی، است. این موارد به طور مؤثر به عنوان ابزاری برای شناسایی شکاف‌ها در فرآیندها و فناوری و همچنین در تمرینات آموزشی برای عملیات‌های اداری، به کار رفته‌اند. تیم عملیاتی، آزمایش نفوذ و تمرینات تصرف سیگنال‌های راهنما، هر دو تکنیک‌های تهاجمی و دفاعی در رویدادهای بر پایه سناریو و غیر سناریو را شامل می‌شود.	
ایالات متحده (۲۰۲۲)	چگونگی استفاده از هوش مصنوعی در مدل‌سازی سیاسی-نظامی، شبیه‌سازی و بازی جنگ در درگیری با کشورهایی که دارای سلاح‌های کشتار جمعی و سایر قابلیت‌های پیشرفته شامل فضا، فضای سایبری و دقت دوربرد هستند.	۵ تا ۱۰ سال	هوش مصنوعی باید به شرکت‌کنندگان در بازی‌های جنگ و سایر عوامل آن در شبیه‌سازی کمک کند تا دیدگاه‌ها، برداشت‌ها و محاسبات احتمالی دشمنانی را که با عدم قطعیت‌ها و اشتباهاتی که می‌توانند مرتکب شوند، درک کند. محتوای هوش مصنوعی باید خطرات تشدیدِ منجر به فاجعه (بدون برنده)، اما همچنین احتمال نتایجی که می‌تواند منجر به برنده شدن یا بازنده شدن معنی‌دار را تشخیص دهد. همچنین در مورد مفاهیم طراحی و توسعه خانواده‌های الگوها، شبیه‌سازی‌ها و بازی‌های جنگ با استفاده از چندین نوع عملکرد هوش مصنوعی بحث شده است. همچنین درباره کمک‌های تصمیم‌گیری برای بازی‌های جنگ، با هوش مصنوعی یا بدون استفاده از هوش مصنوعی، با استفاده از تئوری و کار اکتشافی با استفاده از شبیه‌سازی، تاریخچه و بازی‌های جنگ قبلی صحبت شده است.	تحلیل سناریو
چین (۲۰۲۱)	یک روش انتخاب راهبرد	۱۰ سال	کارشناسان شبکه همیشه با محیط شبکه پیچیده‌تر و روش‌های حمله متنوع، با این	تحلیل سناریو

کشور	اهداف	افق زمانی	نتایج	روش‌شناسی‌ها
	دفاعی بر اساس الگوی بازی جنگ فضای سایبری		مشکل مواجه هستند که چگونه از منابع محدود برای اتخاذ معقول‌ترین تصمیم استفاده کنند و تمام عیوب شبکه را حل کنند و در برابر همه حملات دفاع کنند. الگوی بازی حمله-دفاع شبکه‌ای وسیله‌ای موثر برای حل این مشکل است. با این حال، الگوهای بازی حمله-دفاع شبکه موجود، معمولاً فرض می‌کنند که کارشناسان دیگر پس از استقرار راهبردهای دفاعیِ خود را، تغییر نخواهند داد. در یک رویارویی حمله-دفاع شبکه پیشرفته، کارشناسان معمولاً راهبردهای دفاعی را برای موقعیت‌های حمله مختلف بازنگری می‌کنند. بنابراین، الگوهای بازی حمله-دفاع شبکه موجود برای توصیف دقیق فرآیند حمله-دفاع شبکه پیشرفته چالش برانگیز هستند. در این جا برای پرداختن به چالش‌های فوق، یک روش انتخاب راهبرد دفاعی بر اساس الگوی جنگی حمله-دفاع شبکه‌ای پیشنهاد گردیده است. در این مقاله فرآیند رویارویی حمله-دفاع شبکه پیشرفته به‌عنوان یک بازی جنگ مبتنی بر نوبت مدل‌سازی شده است که در آن هم مهاجمان و هم مدافعان می‌توانند به طور مداوم راهبردهای خود را در پاسخ به وضعیت حمله-دفاع تنظیم کنند و از روش جستجوی درخت مونت کارلو برای حل راهبرد دفاعی بهینه استفاده کنند. در نهایت از یک مثال شبکه برای نشان دادن اثربخشی مدل و روش در انتخاب راهبرد دفاعی بهینه استفاده شده است. انتخاب راهبرد دفاع شبکه به دنبال نقطه	

کشور	اهداف	افق زمانی	نتایج	روش‌شناسی‌ها
			تعادل برای بازی حمله-دفاع شبکه است. در حال حاضر، فناوری‌های انتخاب راهبرد دفاع شبکه عمدتاً شامل الگوهای حمله-دفاع، کمی‌سازی و انتخاب راهبرد و نظریه بازی است. الگوی بازی حمله-دفاع شبکه‌ای ابزاری موثر برای حل این مشکل است. به منظور تجزیه و تحلیل کمی عناصر فرآیند بازی مانند سناریوهای حمله-دفاع، فرآیندها و درآمد هزینه، الگوی بازی حمله-دفاع ضروری است.		
ایالات متحده (۲۰۱۷)	جنگ سایبری بازی جنگ تعاملی: ۲۰۲۵	۵ سال	در این پایان‌نامه آمده که: عملیات در فضای مجازی به طور فزاینده‌ای کانون تمرکز ماموریتی و حوزه رزمی در وزارت دفاع (DOD) است. به همین منظور تعدادی دوره آموزشی و تمرین‌های آموزشی برای آشنایی فرماندهان در راستای برنامه‌ریزی و اجرای اثرات فضای سایبر جهت پشتیبانی از عملیات ایجاد شده است. با این حال، درحال حاضر هیچ شبیه‌ساز مجازی که توسط ارتش ایالات متحده برای آموزش پرسنل که در درک مفاهیم اساسی عملیات فضای مجازی استفاده شده باشد، وجود ندارد. همچنین مواردی چون ۱- اهداف، ۲- موضوعات آموزشی، ۳- بررسی و مشکلات ۴- ویژگی‌ها، ۵- روش‌های بکارگرفته شده برای توسعه‌ی بازی جنگ سایبری در سال ۲۰۲۵، آمده است. فضای سایبر حوزه‌ای است که به طور مداوم در حال رشد، پویا و کاملاً غیرقابل مشاهده است و توصیه می‌شود بهترین راه برای درک این فضا (سایبر)، شبیه‌سازی و بازی‌سازی در آن محیط انجام شود.	تحلیل سناریو
رژیم	امنیت سایبری	۱۵	در این مقاله آمده که چگونه می‌توان	تحلیل سناریو

کشور	اهداف	افق زمانی	نتایج	روش‌شناسی‌ها
صهیونیستی (۲۰۱۴)	- سناریوهای تهدید، چارچوب خط‌مشی و بازی جنگ سایبری	سال	امنیت خدمات دولت الکترونیکی را بهبود بخشید و با شناسایی اینکه مسئولیت آن چیست، چه اولویت‌های کاری در چه زمانی باید انجام گیرد. همچنین اشاره شده که کدام ریسک‌ها قابل چشم‌پوشی و به کدام باید توجه شود. در این مقاله گزارش ریستسکی و همکارانش با موضوعات امنیتی پیچیده‌ای که در ارتباط با زیرساخت و ارتباطات از راه دور است و بایستی عوامل تاثیرگذار برآن به دقت بررسی شوند، آمده است. از آنجا که هر فناوری شامل سازوکارهای امنیتی خاصی است، لازم است با در نظر گرفتن نه تنها مسائل فنی، بلکه چارچوب خط‌مشی و وجوه قانونی، یک سیستم امنیتی مناسب برای زیرساخت‌ها طراحی و ایجاد شود. در این مقاله، در مورد مسائل امنیتی مربوط به تلفن‌های هوشمند بحث شده است. از آنجا که چنین دستگاه‌هایی دارای اطلاعات حساس هستند و با انواع مختلفی از خطوط ارتباطی بی‌سیم در ارتباطند، لذا چنین ارتباطاتی خطر انتقال داده‌های ناخواسته را افزایش می‌دهد. ویژگی‌های این تلفن‌ها (ابعاد، قدرت پردازش، شبکه‌سازی و غیره)، محیط‌کار، اطلاعات ذخیره شده و ارزش آنها، این وسیله را برای سرقت و سوءاستفاده مناسب می‌کند. در این رابطه مشکل اقدامات متقابل مورد نیاز برای ایمن‌سازی تلفن‌های هوشمند و تبلت‌ها بررسی شده است. در این مقاله چندین جنبه از جمله رویکرد جامعِ پرداختن به جرایم سایبری (اطلاعات ضداطلاعاتی، حفاظت از	

کشور	اهداف	افق زمانی	نتایج	روش‌شناسی‌ها
			زیرساخت‌های مهم اطلاعات و مدیریت بحران، دیپلماسی سایبر و مدیریت سایبری) مورد بحث قرار گرفته است. در این تحقیق آمده که، آموزش امنیت سایبری باید یکی از مؤلفه‌های اصلی آموزش مداوم و مادام‌العمر همه باشد. برای حمایت از این راهبرد، باید مراکز ملی برای افزایش آگاهی و آموزش گسترده ایجاد شوند که دانشگاه‌ها را به دلیل بینش عمیق آکادمی‌ها در توسعه امنیت سایبری و دخالت آن در توسعه روش‌ها و ابزارهای آموزشی، به شدت پیوند دهند.	
آلمان (۲۰۱۹)	بازی جنگ سایبری: پیداکردن، طراحی و اجرای بازی جنگ راهبردی سایبری برای آموزش امنیت سایبری	۱۰ سال	در این رساله ابزار اولیه تحقیق، ایجاد یک بازی جنگ اصلی بر اساس راهبرد امنیت سایبری ملی بریتانیا (هر دو نسخه ۲۰۱۱ و ۲۰۱۶) است. در این بازی بریتانیا در مقابل روسیه قرار داده شده که از نظر قدرت سایبری نزدیکترین دشمن به همتای بریتانیایی است. دو طرف به پنج نهاد به نمایندگی از دولت، کسب و کار، افراد (تثلیث اصلی موجود در راهبرد)، ارتش/اطلاعات، و زیرساخت‌های حیاتی ملی تقسیم شدند. بازیکنان برای دستیابی به اهداف متناقض با استفاده از منابع محدودی که در اختیار داشتند، کنترل این نهادها را در دست گرفتند. هدف از این بازی این بوده است که بازیکنان را در معرض طیف گسترده‌ای از مفاهیم امنیت سایبری، از بازیگران کلیدی در فضای سایبری و روابط آنها، حمله‌های سایبری و پویایی دفاع، تا واقعیت‌های ژئوپلیتیکی راهبردی قرار دهد. به منظور پرداختن به این هدف، محقق یک بازی جنگ سایبری را توسعه داده و	تحلیل سناریو

کشور	اهداف	افق زمانی	نتایج	روش‌شناسی‌ها
			آن را در سازمان‌های مختلفی برای جمع‌آوری داده‌ها در مورد اثربخشی آموزشی آن به کار گرفته است.	

روش‌شناسی پژوهش

این پژوهش در صدد شناسایی اجزاء سامانه بازی جنگ راهبردی سایبری است و نتیجه آن در نیروهای مسلح ج. ا. ایران استفاده خواهد شد، بنابراین روش تحقیق، از نظر هدف آن، از نوع کاربردی بوده و سودمندی علمی خواهد داشت. روش تحقیق از نظر ماهیت کیفی بوده و با تحلیل محتوای مستندات، رویکرد تلخیصی و با استفاده از نرم افزار مکس. کیو. دی. ای ۲۰۲۰ انجام می‌شود. در تحلیل محتوای کیفی با رویکرد تلخیصی، تحلیل داده‌ها با جست و جوی کلمات مشخص، و کدگذاری باز انجام می‌شود. واژگان پرشمار برای هر اصطلاح، مشخص و محاسبه شده و کدگزاری محوری انجام می‌شود. سپس ارتباط بین ابعاد و مولفه‌ها از طریق تحلیل مصاحبه به دست آمده و نمودارهای مختلف با نرم افزار استخراج می‌شود. در اینجا پژوهشگر می‌خواهد بداند که واژهٔ مورد نظر چه به صورت مستقیم و چه غیرمستقیم به چه تعداد و توسط چه کسانی به کار برده شده است تا براساس آن‌ها به مضمون سازی رمزها بپردازد (ایمان و نوشادی: ۱۳۹۰).

برای شناسایی اجزاء سامانه بازی جنگ راهبردی سایبری در نیروهای مسلح، روش نمونه‌گیری هدفمند، در دسترس و نظری به کار رفته است. به طوری که کارشناسان و خبرگانِ دارای سطح تحصیلات دکتری، فارغ التحصیل هر یک از رشته‌های علوم نظامی، ریاضیات، رایانه دارای سابقه کار در مسائل بازی جنگ و روش‌های حل مسئله، صاحب‌نظر بودند از طریق گروه آموزشی دانشگاه و مشورت با معاونت آموزش و پژوهش دانشگاه عالی دفاع ملی شناسایی شدند و مصاحبه با آنها تا آنجا صورت گرفت که مشارکت کننده بعدی، اطلاعات جدید دیگری در اختیار مصاحبه‌گر قرار ندهد. در مجموع ۷ نفر مورد مصاحبه قرار گرفتند. همهٔ مصاحبه شوندگان دارای مدرک دکتری بودند. در میان مصاحبه شوندگان یک نفر فارغ التحصیل رشته علوم نظامی (از موسسه تحقیقاتی وزارت دفاع) و یک نفر فارغ التحصیل دکترای ریاضیات بودند، همچنین یک

نفر دیگر از مصاحبه شوندگان فارغ التحصیل رشته سایبری با تخصص شناختی بود. از آنجا که ایشان دارای تجربه و سابقه کاری بالایی در حوزه بازی جنگ نیروهای مسلح و ارتش بودند، از نظرات آنها بهره‌گیری شده است. اطلاعات بیشتر در مورد مشارکت کنندگان در جدول شماره ۲ قید شده است.

جدول (۲) مشخصات مصاحبه شوندگان

کد مصاحبه شونده	سابقه کاری	رشته تحصیلی	محل خدمت	تخصص	محل اخذ مدرک
۱.	۳۴ سال	برق	ستادکل	سایبر – برق	کشور ژاپن
۲.	۳۳ سال	رایانه	وزارت دفاع	رایانه – بازی جنگ	دانشگاه مالک اشتر
۳.	۳۸ سال	علوم نظامی	دانشگاه امام حسین(ع)	الکترونیک	دانشگاه دفاع ملی
۴.	۲۶ سال	الکترونیک	دافوس آجا	الکترونیک – مخابرات – سایبر – شناختی	دانشگاه دفاع ملی
۵.	۶ سال	ریاضیات	دافوس آجا	ریاضیات – تئوری بازی‌ها - بازی جنگ	دانشگاه تبریز
۶.	۳۲ سال	صنایع	دافوس آجا	ریاضیات – رایانه – بازی جنگ	دانشگاه تهران
۷.	۳۴ سال	برق - مخابرات	نیروی هوایی	الکترونیک - تئوری بازی‌ها	دانشگاه صنعتی امیرکبیر

شیوهٔ گردآوری و تحلیل داده‌ها

برای شناسایی و تبیین اجزاء سامانه بازی جنگ راهبردی سایبری، از مصاحبه نیمه ساختار یافته استفاده شده است. متن مصاحبه (سؤالات مصاحبه) مورد تأیید اساتید دانشگاهی قرار گرفته است. در متن مصاحبه علاوه بر پرسش در مورد اطلاعات بیوگرافی معلمان، چهار سؤال اساسی مطرح شد: مهم‌ترین اجزاء یک سامانه بازی جنگ راهبردی سایبری نیروهای مسلح ج. ا. ا کدامند؟ مهمترین عوامل تهدید آمیزی که باید در ایجاد سامانه‌های بازی جنگ راهبردی سایبری نیروهای مسلح ج. ا. ا مد نظر قرار گیرند، کدامند؟ نقش فناوری‌ها، خاصه هوش مصنوعی در ایجاد و توسعه سامانه‌های بازی جنگ راهبردی سایبری نیروهای مسلح ج. ا. ا چیست؟ و در نهایت، سایر پیشنهادت

تکمیلی مصاحبه شوندگان. جلسه‌های مصاحبه‌ها در مجموع حدود ۱۴ ساعت به طول انجامید. مکالمات ضبط و پس از شنیدن، واژه به واژه و عبارت به عبارت، روی کاغذ درج و به دقت بررسی شدند. با توجه به پیشینه و ادبیات پژوهشی حوزه بازی جنگ و متن مصاحبه، واحد تحلیل عبارت بود از همهٔ کلمات و عبارت‌هایی که به طراحی سامانه بازی جنگ ارتباط داشتند. برای هر مصاحبه شونده یک کد اختصاص یافت. متن مصاحبهٔ هر یک از آنها مطالعه و واحدهای تحلیل در هر یک بر اساس اولین مرتبهٔ ظهور آن در فهرست اجزا نوشته شد. به عبارت دیگر هرچند یک مصاحبه شونده به تکرار به برخی موارد در متن پرداخته بود، تنها یک بار آن مورد در فهرست عوامل قید شد. با این حال اگر همان مورد را مصاحبه شونده دیگری تکرار می‌کرد، این بار در فهرست عوامل درج می‌شد. به این صورت فهرست ابعاد و مولفه‌های سامانه بازی جنگ سایبری مورد نظر مصاحبه شوندگان تهیه شد، فراوانی آنها محاسبه و با توجه به معنای کلمات و کاربردشان، طبقه‌بندی شدند و زیر یک محور اصلی قرار گرفتند. به منظور بررسی اعتبار یافته‌ها، متن مصاحبه به همراه نتایج تحلیل اولیه به پژوهشگر دیگری ارائه شد. فهرست تهیه شده از عوامل، تأیید و محورهای اصلی با توافق به صورت نهایی ثبت شدند. همچنین مصاحبه با ۷ نفر از صاحب‌نظران و خبرگان حوزه بازی جنگ که با تجربیات بالا بودند و نیز شرح مبسوط ویژگی‌های مصاحبه شوندگان (طبق جدول شماره ۲) و نحوه گردآوری و تحلیل داده‌ها می‌تواند مبین اعتبار یافته‌ها باشد.

تجزیه و تحلیل داده‌ها

بر اساس مطالعه و بررسی متون حاصل از مصاحبه با صاحب‌نظران، اجزاء سامانه بازی جنگ راهبردی سایبری نیروهای مسلح ج. ا. ایران، در شش بعد شناسایی و دسته‌بندی شدند که عبارت‌اند از: ۱- درون‌دادها و برون‌دادهای سامانه‌ی بازی جنگ، ۲- فرایندهای بازی جنگ، ۳- فناوری‌های دخیل در بازی جنگ، ۴- ارکان جهت‌ساز، ۵- امنیت و ۶- تهدیدهای محیطی سایبری بازی جنگ سایبری.

جدول (۳) فهرست ابعاد و مولفه‌های سامانه بازی جنگ راهبردی سایبری نیروهای مسلح از نظر مصاحبه شوندگان

ابعاد	مولفه‌ها	فراوانی	مصاحبه شوندگان							شماره
			کد۱	کد۲	کد۳	کد۴	کد۵	کد۶	کد۷	

ابعاد	مولفه‌ها	فراوانی	مصاحبه شوندگان							شماره
			کد۱	کد۲	کد۳	کد۴	کد۵	کد۶	کد۷	
امنیت	دسترس پذیری	۳	❋					❋	❋	۱.
	تهدید انسانی	۱						❋		۲.
	آشکارسازی در حمله	۱							❋	۳.
	ایمنی	۱						❋		۴.
	حداکثر لطمه زدن	۱				❋				۵.
	فریب	۱				❋				۶.
	تخریب	۱				❋				۷.
	نفوذ	۲				❋		❋		۸.
	حمله ممانعت از سرویس[1]	۲				❋			❋	۹.
مجموع فراوانی		**۱۳**	**۱**	**۰**	**۰**	**۵**	**۰**	**۴**	**۳**	–
فناوری‌ها	واقعیت افزوده	۴	❋			❋	❋		❋	۱۰.
	هوش مصنوعی	۲					❋		❋	۱۱.
	حقیقت مجازی	۴	❋			❋	❋		❋	۱۲.
	بیگ دیتا	۲	❋					❋		۱۳.
	کوانتوم	۴	❋			❋	❋		❋	۱۴.
	ترکیب افزوده	۴	❋			❋	❋		❋	۱۵.

[1] DDOS

ابعاد	مولفه‌ها	فراوانی	مصاحبه شوندگان							شماره
			کد۱	کد۲	کد۳	کد۴	کد۵	کد۶	کد۷	
مجموع فراوانی		۲۰	۵	۰	۰	۴	۵	۱	۵	–
عوال تهدیدهای محیطی سایبری	سرعت	۱						❋		.۱۶
	حجم	۱						❋		.۱۷
	تنوع	۱						❋		.۱۸
	هوشمندی	۱						❋		.۱۹
	ویژگی‌های محیطی صحنه نبرد	۱			❋					.۲۰
مجموع فراوانی		۵	۰	۰	۱	۰	۰	۴	۰	–
ارکان جهت ساز	دکترین	۵		❋	❋	❋	❋	❋		.۲۱
	ماموریت	۵		❋	❋	❋	❋	❋		.۲۲
	هدف	۵		❋	❋	❋	❋	❋		.۲۳
مجموع فراوانی		۱۵	۰	۳	۳	۳	۳	۳	۰	–
درون دادها و برون دادها	کاربران	۵		❋		❋	❋	❋	❋	.۲۴
	اطلاعات مربوط به محتوا	۳		❋			❋	❋		.۲۵
	اطلاعات مربوط به سامانه‌ها	۲				❋	❋			.۲۶
	اطلاعات مربوط به زیرساخت‌ها	۳				❋	❋	❋		.۲۷
	طراحان	۱					❋			.۲۸

ابعاد	مولفه‌ها	فراوانی	مصاحبه شوندگان							شماره
			کد۱	کد۲	کد۳	کد۴	کد۵	کد۶	کد۷	
	برنامه نویسان	۳				❋	❋		❋	۲۹.
	سناریوها	۵	❋	❋		❋	❋	❋		۳۰.
	نتایج بازی جنگ	۲	❋					❋		۳۱.
	متخصصین	۴				❋	❋	❋	❋	۳۲.
	تجزیه و تحلیل نتایج	۴				❋	❋	❋	❋	۳۳.
	نظام فکری طرفین بازی	۱						❋		۳۴.
مجموع فراوانی		**۳۳**	**۲**	**۳**	**۰**	**۷**	**۹**	**۸**	**۴**	–
فرایندها	طرح‌ریزی	۳				❋	❋		❋	۳۵.
	بانک‌های اطلاعاتی	۳				❋	❋	❋		۳۶.
	تجزیه و تحلیل	۲	❋						❋	۳۷.
	نوع بازی جنگ	۶	❋	❋	❋	❋		❋	❋	۳۸.
	ماهیت بازی جنگ	۴		❋	❋	❋	❋	❋		۳۹.
	ساختار طرفین بازی جنگ	۵	❋	❋		❋		❋	❋	۴۰.
	پروتکل‌های بازی	۵		❋	❋	❋	❋	❋		۴۱.
مجموع فراوانی		**۲۸**	**۳**	**۴**	**۳**	**۶**	**۴**	**۵**	**۴**	–

جزء محوری اول در زمینهٔ شناسایی اجزاء سامانه بازی جنگ راهبردی سایبری مربوط

به «درون‌دادها و برون‌دادها» با فراوانی ۳۳ مورد است. این بُعد اشاره به ورودی‌ها و خروجی‌های سامانه بازی جنگ دارند که منجر به اشاره به مولفه‌هایی که بیشترین تاثیر را در ارایه اجزاء سامانه بازی جنگ دارد از جمله: «کاربران»، «سناریو»، «متخصصین» و «تجزیه و تحلیل نتایج»، می‌شود. در این مورد مصاحبه شوندگان علاوه بر اشاره به موارد فوق، توصیه‌هایی برای شرایط پذیرش کاربران در بازی، همچنین شرایط سناریوها، ارائه کردند:

کد۵: *کاربران در بازی جنگ شامل (ارتش، سپاه، ودجا، فراجا) هستند. (نفر پنجم, Pos. 36)*

کد۴: *کاربران باید ورزیده، متخصص، دوره‌های خاص دیده و کاربلد باشند. همچنین گروه‌هایی که بتوانند این پروتکل‌ها و قواعد را به زبان ماشین تبدیل کنند. (برنامه‌نویسان) (نفر پنجم, Pos. 22)*

کد۷: *در حالتی که تعداد بازیگران کم و نوع بازی آموزشی است، زمان پاسخگویی شاید زیاد مهم نباشد. و کم بودن تعداد کاربران نیاز به رایانه‌ها و ماشین‌ها را دیکته نمی‌کند. (نفر چهارم, Pos. 28)*

کد۷: *یکی از نکات مهم در شبیه‌سازی جنگ، حس گیری است. با فناوری‌هایی که نام برده شد، سعی می‌شود حس واقعی صحنه جنگ به کاربران منتقل شود. (نفر هفتم, Pos. 22)*

کد۱: *هوش مصنوعی می‌تواند سناریوهای دقیق‌تر، متنوع‌تر، ایجاد می‌کند. بررسی و تحلیل سریع‌تر انجام داده. پاسخ دقیق‌تری ارائه می‌کند. (نفر اول, Pos. 25)*

کد۴: *از مزایای بازی جنگ یکی اینکه کمک در ایجاد طیف وسیعی از سناریوها است. (نفر چهارم, Pos. 36)*

جزء محوری دوم در زمینهٔ شناسایی اجزاء سامانه بازی جنگ راهبردی سایبری مربوط به «فرایندها» با فراوانی ۲۸ مورد است. این بعد اشاره به تمامی فرایندهایی که در سامانه بازی جنگ باهم در ارتباط بوده و از ورودی تا خروجی را شامل می‌شود، هستند. بیشترین تاثیر در اجزاء سامانه بازی جنگ راهبردی سایبری: «نوع بازی جنگ»، «ساختار طرفین بازی جنگ»، «پروتکل‌های بازی» و «ماهیت بازی جنگ»، است. در این مورد مصاحبه شوندگان علاوه بر اشاره به موارد فوق، توصیه‌هایی را جهت تکمیل

نظرات خود آوردند:

کد۱: *در حالتی که تعداد بازیگران کم و نوع بازی آموزشی است، زمان پاسخگویی شاید زیاد مهم نباشد. (نفر اول, Pos. 15)*

کد۵: *ماهیت بازی جنگ (آموزشی / تحلیلی) باید مشخص شود. (نفر پنجم, Pos. 6)*

کد۶: *نوع جنگ‌ها هم مهم است. (همتراز، ناهمتراز، کلاسیک، آبخاکی، تارشکری-تکفیری، مرکب، مشترک، اطلاعاتی، شناختی) (نفر ششم, Pos. 21)*

کد۳: *ساختار طرفین بازی به چه صورت است. (عِدّه و عُدّه مشخص شود.) (نفر سوم, Pos. 13)*

جزء محوری سوم در زمینهٔ شناسایی اجزاء سامانه بازی جنگ راهبردی سایبری مربوط به «فناوری‌ها» با فراوانی ۲۰ مورد است. این دسته عوامل اشاره به فناوری‌هایی دارد که بیشترین تاثیر را در سامانه بازی جنگ دارند. بیشترین تاثیر در اجزاء سامانه بازی جنگ شامل: «هوش مصنوعی»، «کوانتوم»، «ترکیب افزوده» و «واقعیت افزوده»، است. در این مورد مصاحبه شوندگان علاوه بر اشاره به موارد فوق، توصیه‌هایی را جهت تکمیل نظرات خود آوردند:

کد۱: *بهتر است در اینجا فقط هوش مصنوعی را بیان نکنیم. بلکه نقش فناوری‌های نوظهور یا شالوده شکن را نیز مطرح نماییم. مثلا کوانتوم (افزایش بسیار بالای سرعت پردازش داده‌ها)، حقیقت مجازی، واقعیت افزوده، ترکیب افزوده و... (حس-گیری). یکی از نکات مهم در شبیه‌سازی جنگ، حس گیری است. با فناوری‌هایی که نام برده شد، سعی می‌شود حس واقعی صحنه جنگ به کاربران منتقل شود. (نفر اول, Pos. 20-22)*

کد۶: *اجزاء بازی جنگ آن باید عوامل فناورانه (سخت افزار، نرم افزار) و عوامل فرایندی (امور قوانین، مقررات، پروتکل‌ها) و عوامل انسانی (مهاجم، مدافع، کاربر) را لحاظ نمود. (نفر ششم, Pos. 32)*

کد۷: *هوش مصنوعی هم تکیه سنگینی بر علم داده دارد. تکیه بر بیگ داده دارد. داده‌ها چگونه ایجاد، پردازش، ذخیره و انتشار یا حذف شوند. در عالم داده بسیار مهم و پیچیده است. (نفر هفتم, Pos. 23)*

کد۴: *هوش مصنوعی می‌تواند سناریوهای دقیق‌تر، متنوع‌تر، ایجاد می‌کند. بررسی و*

تحلیل سریع‌تر انجام داده. پاسخ دقیق‌تری ارائه می‌کند. (نفر چهارم, Pos. 44)

کد۴: *هوش مصنوعی به دلیل داشتن منطق و ریاضی، از احساسات دور بوده و بدون جانبداری نتایج دقیق و صحیح را ارائه می‌دهد. (نفر چهارم, Pos. 43)*

جزء محوری چهارم در زمینهٔ شناسایی اجزاء سامانه بازی جنگ راهبردی سایبری مربوط به «ارکان جهت‌ساز» با فراوانی ۱۵ مورد است. این دسته اجزاء اشاره با اجزائی دارد که در سطح راهبردی و کلان بیشترین تاثیر را در ایجاد سامانه بازی جنگ دارند. بیشترین تاثیر در تعیین اجزاء سامانه بازی جنگ شامل: «دکترین»، «ماموریت»، «هدف»، است. در این مورد مصاحبه شوندگان علاوه بر اشاره به موارد فوق، توصیه‌هایی را جهت تکمیل نظرات خود آوردند:

کد۵: *ماموریت باید مشخص شود که از چه نوعی است. آیا تهاجمی است یا تدافی؟ (آفندی / پدافندی) (نفر پنجم, Pos. 1)*

کد۴: *هدف چیست؟ (حمله / دفاع) (نفر چهارم, Pos. 1)*

کد۶: *دکترین حمله طرفین بازی جنگ مشخص شود. (نفر ششم, Pos. 10)*

جزء محوری پنجم در زمینهٔ شناسایی اجزاء سامانه بازی جنگ راهبردی سایبری مربوط به «امنیت» با فراوانی ۱۳ مورد است. این دسته اجزاء اشاره به مواردی دارد که بیشترین تاثیر را در امنیت سامانه بازی جنگ دارند. بیشترین تاثیر این دسته عوامل شامل: «دسترسی‌پذیری ، «نفوذ»، «حمله ممانعت از سرویس»[1] است. در این مورد مصاحبه شوندگان علاوه بر اشاره به موارد فوق، توصیه‌هایی را جهت تکمیل نظرات خود آوردند:

کد۱: *بحث دسترسی مهم است. مثلا استاکسنت از بیرون که دسترسی نبود. بلکه توسط نفوذی و تهدید انسانی اتفاق افتاد. یا مثلا دسترسی به شبکه آرمان که آیا امکان پذیر است یا خیر؟ (نفر اول, Pos. 7)*

کد۴: *نیت بازی (آیا نفوذ یا تخریب یا فریب، حراکثر لطمه زدن، عملیات ایزایی، تاثیر در آن، تاثیر در دراز مدت، عملیات شناختی، مسائل حریم خصوصی، مد نظر است؟) (نفر چهارم, Pos. 19)*

کد۷: *باید شما آشکارسازی در حمله را مشخص کنید. همچنین باید بتوانید حملاتی*

[1] DDOS

چون DDOS را شبیه‌سازی کنید. (نفر هفتم, Pos. 19)

کد۶: *باید نحوه کنترل آثار و پیامدهای اقدامات در بازی جنگ سایبری دیده شود تا نحوه کنترل آثار آبشاری حملات و تهدیدهای سایبری لحاظ گردد (نفر ششم, Pos. 24).*

و در نهایت جزء محوری ششم در زمینهٔ شناسایی اجزاء سامانه بازی جنگ راهبردی سایبری مربوط به «تهدیدهای محیطی سایبری» با فراوانی ۵ مورد است. این دسته اجزاء اشاره به بیشترین تاثیر عوامل محیطی معروف به 3V را دارد که بیشترین تاثیر را در سامانه بازی جنگ دارند و شامل: «سرعت»، «حجم»، «تنوع» است. در این مورد مصاحبه شوندگان علاوه بر اشاره به موارد فوق، توصیه‌هایی را جهت تکمیل نظرات خود آوردند:

کد۳: *ویژگی‌های محیطی صحنه نبرد را باید به دقت مورد توجه قرار داد. (عوارض جغرافیایی / شرایط جوی) (نفر سوم, Pos. 5)*

کد۶: *در نظر گرفتن عواملی چون سرعت، حجم، تنوع و هوشمندی حملات سایبری بازی جنگ بسیار مهم و حائز اهمیت فراوان است. (نفر ششم, Pos. 23)*

نتیجه‌گیری و پیشنهادها

در این مطالعه کارشناسان نظرات خود در مورد اجزاء مورد نیاز بازی جنگ راهبردی سایبری ارائه نمودند. یافته‌های پژوهشی بیان کنندهٔ شش محور اصلی در زمینهٔ اجزا تشکیل دهنده سامانه بازی جنگ راهبردی سایبری است که عبارت‌اند از: درون‌دادها و برون‌دادهای سامانه‌ی بازی جنگ، فرایندهای بازی جنگ، فناوری‌ها، ارکان جهت‌ساز، امنیت و تهدیدهای محیطی سایبری بازی جنگ سایبری. در سایر مطالعات پیشینه‌ای، جهرمی (۱۳۹۸) انواع مولفه‌های بازی جنگ را شاملِ محیط و سناریو، بازیکنان و تصمیم‌های آنها، قوانین و رویه‌ها و داوری، شبیه‌سازی پایگاه داده، پشتیبانی و تحلیل می‌داند. مرادیان (۱۴۰۱) نقش توپولوژی‌ها در بازی جنگ را به توپولوژی عملیات، توپولوژی فرماندهی و توپولوژی اطلاعات تقسیم می‌کند. افشردی و همکاران (۱۳۹۷) رویکردهای بازی جنگ در طراحی را شامل رویکرد تحلیل، رویکرد معماری و رویکرد هنری می‌داند. بای فاکس[1] (۲۰۱۸) عناصر کلیدی بازی جنگ سایبری را محدوده،

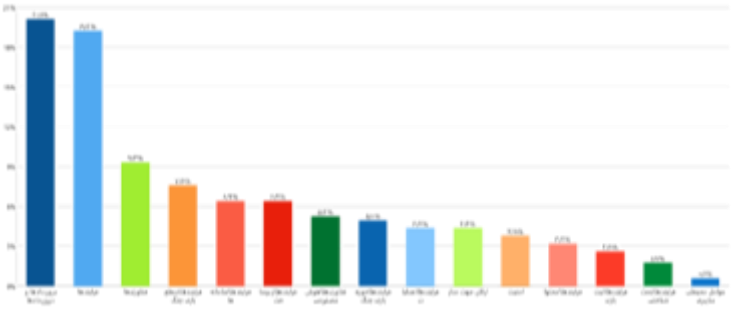
[1] Bay Fox

عملکرد سازمانی، محیط سامانه، فناوری‌های دفاعی سایبری، تهدید و سناریوها، معرفی می‌کنند. موسسه معتبر تحقیقاتی رند در مقاله تحقیقاتی خود[1] متغیرهای صحنه بازی جنگ راهبردی سایبری را: تعداد و نوع دشمنان و حریفان، سطح دقت و تجهیزات امنیتی دشمنان، نوع و قابلیت‌های سامانه‌های دفاعی و حمله‌ای بازیکنان، محل و مساحت شبکه‌های ارتباطی و سرورهای دشمن، سطح دشواری و پیچیدگی مراحل بازی، راهبردهای نظامی و راه‌کنش‌های نبرد در فضای سایبری معرفی کرده است. پاول کی. دیویس[2] (۲۰۲۲) در تحقیقی با عنوان "*هوش مصنوعی برای بازی‌های جنگ و الگوسازی*" معتقد است: هوش مصنوعی باید به شرکت‌کنندگان در بازی‌های جنگ و سایر عوامل آن در شبیه‌سازی کمک کند تا دیدگاه‌ها، برداشت‌ها و محاسبات احتمالی دشمنانی را که با عدم قطعیت‌ها و اشتباهاتی که می‌توانند مرتکب شوند، درک کند. محتوای هوش مصنوعی باید خطرات تشدیدِ منجر به فاجعه (بدون برنده)، همچنین احتمالا نتایجی که می‌تواند منجر به برنده شدن یا بازنده شدن معنی‌دار را، تشخیص دهد. همچنین در مورد مفاهیم طراحی و توسعه الگوها، شبیه‌سازی‌ها و بازی‌های جنگ با استفاده از چندین نوع عملکرد هوش مصنوعی بحث شده است. همچنین درباره کمک‌های تصمیم‌گیری برای بازی‌های جنگ، با هوش مصنوعی یا بدون استفاده از هوش مصنوعی، با استفاده از تئوری و کار اکتشافی با استفاده از شبیه‌سازی، تاریخچه و بازی‌های جنگ قبلی صحبت شده است. از نگاه ادوارد جی. ام. کالبرت[3] (۲۰۱۹) مدیر علوم محاسباتی و اطلاع رسانی در مقاله‌ای با عنوان "*الگوسازی بازی جنگ سایبر – فیزیکی*" فرایند طراحی، پیاده‌سازی و اجرای یک بازی سایبری را شاملِ دفاع، تهدیدها، حمله‌ها، بازیکنان، نیروهای خودی، داوران، مشاوران، مهاجمین و دشمنان، تجهیزات و وسایل بازی، قواعد و منطق بازی، تجزیه و تحلیل، و در نهایت نتیجه‌گیری می‌دانند. (اکثر مراحل لزوماً متوالی یا به ترتیب است). همچنین وی نتیجه گرفته‌است که: نتایج و مزایای بازی جنگ سایبری بسته به اهداف سازمان متفاوت است. در مورد "*نقاط قوت بازی جنگ سایبری*" از مواردی چون بازی جنگ سایبری برای تأیید فناوری‌های نوآورانه پدافند سایبری که پتانسیل بهبود امنیت سایبر و کاهش خطر از سوی منابع

[1] RAND: RR2086.pdf
[2] Paul K. Davis
[3] Edward J. M. Culbert

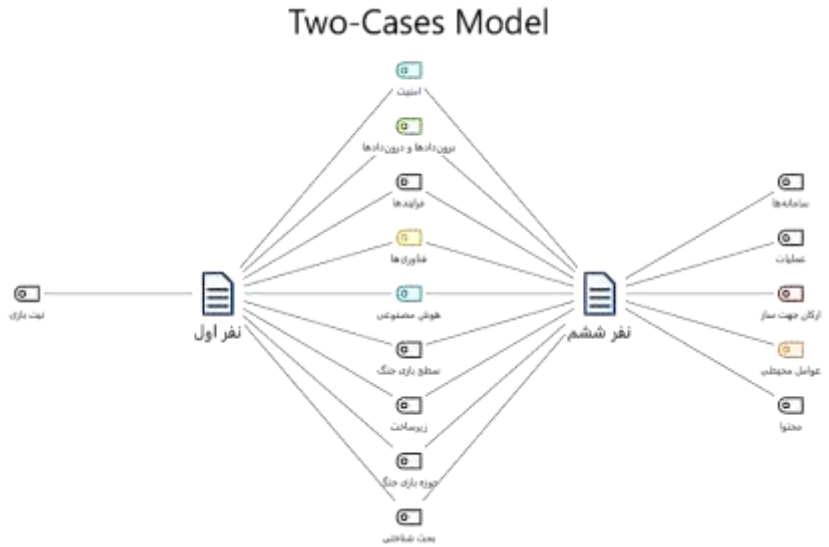
مهاجم سایبری را دارند، می‌تواند مورد استفاده قرار گیرد. همچنین با طراحی یک چارچوب و سناریوی مناسب و مطلوب بازی جنگ سایبری، این تمرین‌ها می‌توانند توسط سایربخش‌های مهم زیرساختی استفاده شوند. علاوه بر این، به راحتی قابل تنظیم بوده و با تغییر سناریو، ایجاد فرصت‌های یادگیریِ تقریبا نامحدود، که می‌توانند کاملاً جدید باشند، ایجاد کرد. در نهایت محصولات جدید فناوری که در حین تمرینات بازی جنگ سایبری ایجاد و به بازی اعمال می‌شوند، می‌توانند ارزیابی کنند که به چه میزان می‌توانند شکاف‌ها و فواصل شناخته شده معایب سامانه را پوشش دهند. فناوری‌هایی که پوشش مؤثرتری بر شکاف‌ها دارند، می‌توانند برای ارزیابی بیشتر در نظر گرفته شوند. همان‌طور که ملاحظه می‌شود نتایج پژوهش‌های صورت گرفته، تأییدکننده لزوم شناسایی اجزاء بازی جنگ راهبردی سایبری بر مبنای نتایج تحقیق انجام شده است. از نظر کارشناسان و متخصصین باید از اسناد و مدارک دست اول سایر کشورها استفاده نمود. همچنین سایر مراکز ذی‌نفع از این قضیه باید مشارکت فعال و همه‌گیر داشته باشند. سازمان‌هایی چون شورای عالی فضای مجازی کشور، شورای عالی پدافند کشور، نیروهای مسلح، شورای عالی امنیت ملی، همکاری با مراکز دانشگاهی و نهادهای خصوصی مربوطه، نگاه دقیق و تخصصی به جنگ‌های سایبری اخیر جهان همچون اوکراین و روسیه، حماس و رژیم صهیونیستی، منازعه قره‌باغ. کارشناسان معتقدند باید مسابقات سایبری ملی موسوم به "فتح پرچم سایبری". در این تحقیق فراوانی اجزاء سامانهٔ بازی جنگ راهبردی سایبری در نمودار زیر نمایش داده شده است.

همانطور که قبلا ذکر گردید، طبق نمودار۱ به ترتیب برون‌دادها و درون‌دادها بیشترین فراوانی و عوامل محیطی سایبری کمترین اجزاء سامانه بازی جنگ هستند که توسط مصاحبه شوندگان اشاره شده است.



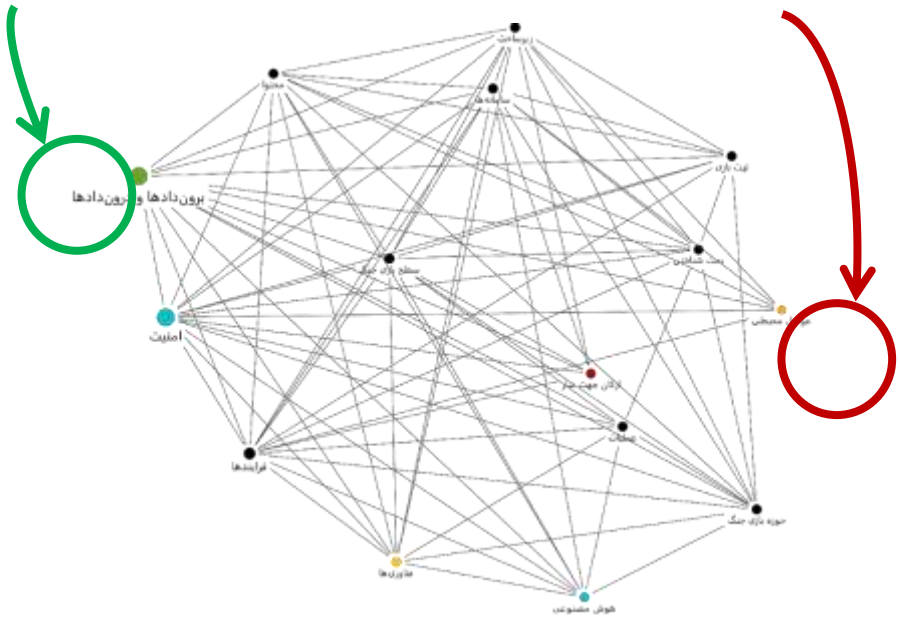
نمودار (۱) نمایش درصد فراوانی اجزاء سامانه بازی جنگ راهبردی سایبری

در نمودار۲ به عنوان مثال روابط ابعاد و مولفه‌های بین مصاحبه شوندگان شماره ۱ و ۶ آمده است. همانطور که دیده می‌شود برخی از این اجزاء مشترک و برخی مجزا از نظر مشترک مصاحبه شوندگان است.



نمودار (۲) گراف مصاحبه شوندگان ۱ و ۶

در شکل۲ تمامی ارتباطات بین ابعاد و مولفه‌های تشکیل دهنده اجزای بازی جنگ راهبردی سایبری یکجا به نمایش درآمده است. همانطور که مشاهده می‌شود، به ترتیب، برون‌دادها و درون‌دادها با ۱۴ اتصال بیشترین (دایره سبز رنگ) و عوامل محیطی با ۵ اتصال کمترین ارتباط (دایره قرمز رنگ) را با سایر ابعاد و مولفه‌ها برای اجزاء این سامانه دارند.



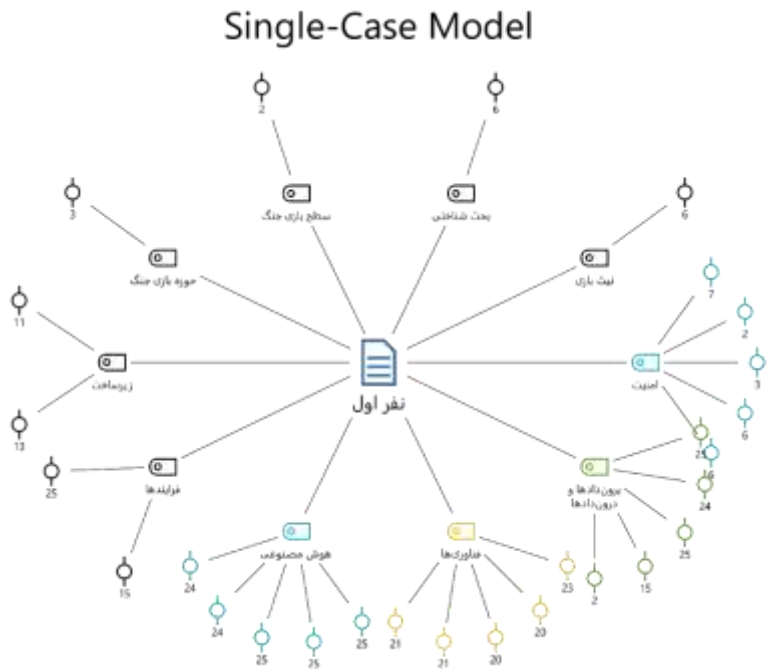
شکل (۲) نقشه کامل ارتباطات بین اجزاء سامانه بازی جنگ راهبردی سایبری

در نمودار۳ جدول ماتریسی فراوانی ابعاد و مولفه‌های بازی جنگ راهبردی سایبری از تقاطع ابعاد و مولفه‌ها و نظر مصاحبه شوندگان و تاکید آن‌ها بر این اجزاء، نمایش داده شده است.

Code System	نفر اول	نفر دوم	نفر سوم	نفر چهارم	نفر پنجم	نفر ششم	نفر هفتم
امنیت	24	25	22	76	51	56	38
فناوری‌ها	8			7	8	2	7
هوش مصنوعی	7			4	2	1	4
عوامل محیطی						1	
ارکان جهت ساز		3	3	3	3	3	
برون‌دادها و برون‌دادها	24	25	22	76	51	56	39
فرایندها	2	10	10	17	14	15	6
حوزه بازی جنگ	1		2	4	5	3	2
محتوا		2		4	3	1	1
زیرساخت	2	1		9	3	3	4
سامانه‌ها		2		8	4	5	3
سطح بازی جنگ	1	4	3	7	4	5	2
بعد شناختی	1		1	1	1	1	1
بعد بازی	1			7			1
عملیات		1	4	1	3	4	2

نمودار (۳) فراوانی ابعاد و مولفه‌های بازی جنگ راهبردی سایبری

در شکل۳ ارتباط بین متن مصاحبه‌ی مصاحبه شونده شماره ۱ و ابعاد و مولفه‌های تحقیق و همچنین فراوانی آن‌ها به طور یکجا و در این شکل آمده است.



شکل (۳) مصاحبه شونده ۱ و رابطه آن با ابعاد و مولفه‌ها و فراوانی آن‌ها

در نمودار۴ در یک ارتباط ماتریسی ابعاد، مولفه‌ها و مصاحبه‌ی مصاحبه شوندگان نمایش داده شده است. طبق نمودار هرچه مربعات بزرگتر هستند درصد فراوانی مولفه‌ها بیشتر است.

نمودار (۴): ارتباط بین کدها و مصاحبه شوندگان

بعد از تجزیه و تحلیل نمودارها و اشکال بالا، نتایج پژوهش ذکر شده حاضر بر اجزاء مورد نیاز در سامانه بازی جنگ راهبردی سایبری اشاره دارد. در این راستا علاوه بر اجزاء محوری که در این تحقیق با کدگذاری، اندازه گیری شد، به اجزاء دیگری چون

خطرهای شناسایی شده، محدودیت‌های بازی، چشم انداز، خط مشی‌ها، سازمان، آموزش و تربیت، مدیریت و رهبری، سیاست، قوانین و رویه‌های بازی جنگ، اشاره شده است.

قدردانی

از کلیهٔ اندیشمندان و پژوهشگرانی که در خلال تحقیق خالصانه دیدگاه‌ها و نقطه نظرات علمی و کارشناسی خود را ارائه نمودند، تشکر و قدردانی می‌گردد.

منابع

- افشردی، محمدحسین. ، نوروزانی، شهرام. و شجاعی، شهرام. (۱۳۹۷). *مبانی بازی جنگ راهبردی*، چاپ اول، انتشارات مرکز تحقیقات راهبردی دفاعی.
- جهرمی، امین. (۱۳۹۸). *کاربرد دانش نظامی در مدیریت و کسب و کار*، چاپ اول، انتشارات آتی‌نگر.
- درویش‌زاده، مهدی‌رضا، رضایتی چتران، آرمان. و جلیلی، ریحانه. (۱۳۹۴). *نظریه بازی در روابط* بین‌الملل، چاپ اول، انتشارات زلال کوثر.
- دفتر واژه‌گزینی نظامی دانشگاه و پژوهشگاه عالی دفاع ملی. (۱۳۹۷).
- طاهری، محمد، محمدزهرایی، سپهر. (۱۳۹۹). تبیین چارچوب بازی جنگ سایبری، *فصلنامه بازی جنگ*. ۶(۳): ۱۲۱- ۸۶.
- فان کرفلد، مارتین. (۱۳۸۶). *بازاندیشی مفهوم جنگ*، موسسه آموزشی و تحقیقاتی صنایع دفاعی.
- کمیسیون کنترل امنیت ارتباطات و فنآوری اطلاعات ن. م، (۱۳۹۴). *آیین‌نامه جامع فناوری اطلاعات و ارتباطات ستاد کل نیروهای مسلح*.
- محمدی، (۱۳۹۵). *ذی‌نفعان فضای سایبری کشور*، دانشکده امنیت دانشگاه عالی دفاع ملی.
- مرادیان، محسن. (۱۳۸۹). *بازی جنگ در ردهٔ لشکر*، چاپ اول، انتشارات دافوس آجا.

- میرشکاری، جواد. (۱۳۹۶). *فرهنگ واژه‌های مصوب فرهنگستان*، دفتر چهارم؛ انتشارات فرهنگستان زبان و ادب فارسی

- Bailey, T, Kaplan, J, & Weinberg, A (2012*), Playing war games to prepare for a cyberattack*, McKinsey & Company, viewed 15 May 2017
- Catalkaya H. , Karaman M. (2015). Institutional Cybersecurity: The Risk of Open Source Intelligence (OSINT) and Social Networks, *International Conference on Military Security Studies (ICMSS- 2015 , Istanbul).*
- Davis, P. K. , *Rand Experience in Applying Artificial Intelligence Techniques to Strategic Level-Military-Political War Gaming*, Rand Report No. P6977, The RAND Corporation, Santa Monica, CA, 1984.
- Goztepe, K. , Kahraman, C. (2015) A New Approach to Military Decision Making Process: Suggestions from MCDM Point of View, *International Conference on Military and Security Studies-2015*, Istanbul, 118-122.
- Goztepe, K. , Kilic, R. , & Kayaalp, A. (2014). Cyber Defense In Depth: Designing Cyber Security Agency Organization For Turkey. *Journal of Naval Science and Engineering, 10(1)*, 1-24.
- Hejase, A. J. , Hejase, H. J. , & Hejase, J. A. (2015) Cyber Warfare Awareness in Lebanon: Exploratory Research. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)* 4(4): 482-497