Iranian Journal of Wargaming
AJA Command and Staff University
http://www.ijwg.ir/
Online ISSN: 2676-7708
Print ISSN: 2676-5284

Designing a cyber exercise system of the Islamic Republic of Iran

Ali Bakhtiary [1✉] | **Naser Modiri** [2]

1. Corresponding Author, Supreme National Defence University, Tehran, Iran.
   E-mail: ali.bakhtiary.d.57@gmail.com
2. Lecturer, Supreme National Defence University, Tehran, Iran.
   E-mail: Nassermodiri@yahoo.com

Article Info

Article type:
Research Article

Article history:
Received
2 December 2024
Received in revised form 27 February 2025
Accepted
8 March 2025

Keywords:
Cyberspace, System, Exercise, Cyber exercise, Cyber exercise system

ABSTRACT

Objective: Given the increasing cyber threats and the increasing complexity in this area, organizations and critical infrastructures need to prepare themselves against these threats. One of the main methods in this regard is to hold cyber exercises that simulate practical situations in controlled environments. Therefore, the aim of this article is to present a cyber exercise model to evaluate and strengthen this critical cyber infrastructure of the Islamic Republic of Iran.

Methodology: The current research is applied and is carried out with a descriptive-case study method and a mixed approach (qualitative and quantitative).

Findings: Identifying the concepts, nature, principles, resources, consequences, and outcomes of the Islamic Republic of Iran's Cyber Exercise System. Designing the Islamic Republic of Iran's Cyber Exercise System along with its components, including inputs, processes, components, outputs, results, and feedback.

Conclusion: The results of the questionnaire analysis indicate that using this model in cyber exercises can improve the efficiency of cyber exercises and enhance the cybersecurity level of the critical infrastructure of the Islamic Republic of Iran.

Cite this article: Bakhtiari,A. and Modiri,N. (2025). Designing cyber exercise system of Islamic republic of Iran. (e216884). Iranian Journal of Wargaming, 7(15), 117- 136.
DOI: 10.22034/ijwg.2025.491655.1107

Publisher: Command and Staff University

دوفصلنامه علمی بازی جنگ
دانشگاه فرماندهی و ستاد آجا
http://www.ijwg.ir/
شاپای چاپی: ۵۲۸۴-۲۶۷۶ شاپای الکترونیکی: ۷۷۰۸-۲۶۷۶

طراحی نظام رزمایش سایبری جمهوری اسلامی ایران

علی بختیاری [۱] ✉ | ناصر مدیری [۲]

۱. نویسنده مسئول، دانشگاه عالی دفاع ملی، تهران، ایران، **رایانامه:** ali.bakhtiary.d.57@gmail.com

۲. مدرس، دانشگاه عالی دفاع ملی، تهران، ایران، **رایانامه:** Nassermodiri@yahoo.com

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخ دریافت:
۱۴۰۳/۰۹/۱۲

تاریخ بازنگری:
۱۴۰۳/۱۲/۰۹

تاریخ پذیرش:
۱۴۰۳/۱۲/۱۸

کلیدواژه‌ها:
فضای سایبر، نظام، رزمایش، رزمایش سایبری، نظام رزمایش سایبری

چکیده

هدف: با توجه به افزایش تهدیدهای سایبری و پیچیدگی‌های روزافزون حمله‌ها در این حوزه، سازمان‌ها و زیرساخت‌های حیاتی نیازمند تقویت آمادگی خود در برابر این تهدیدها هستند. یکی از روش‌های مؤثر در این راستا، برگزاری رزمایش‌های سایبری است که به شبیه‌سازی حمله‌های واقعی در محیط‌های کنترل‌شده می‌پردازد. به همین جهت هدف این مقاله، ارائه نظام رزمایش سایبری برای ارزیابی و تقویت آمادگی سایبری زیرساخت‌های حیاتی جمهوری اسلامی ایران است.

روش: تحقیق حاضر از حیث ماهیت از نوع توصیفی - موردی است. همچنین رویکرد مورد استفاده برای جمع‌آوری و تجزیه و تحلیل داده‌ها آمیخته (کیفی و کمّی) است.

یافته‌ها: احصا مفاهیم، ماهیت، اصول، منابع، پیامدها و دستاوردهای نظام رزمایش سایبری ج.ا.ا؛ ترسیم نظام رزمایش سایبری ج.ا.ا به همراه اجزای تشکیل‌دهنده آن شامل ورودی‌ها، فرایندها، مؤلفه‌ها، خروجی، نتایج و بازخورد است.

نتیجه‌گیری: نتایج تجزیه و تحلیل پرسش‌نامه نشان می‌دهد که استفاده از نظام رزمایش سایبری پیشنهادی می‌تواند به بهبود کارایی رزمایش‌های سایبری و افزایش سطح امنیت سایبری زیرساخت‌های جمهوری اسلامی ایران منجر شود.

استناد: بختیاری، علی و مدیری، ناصر (۱۴۰۴). طراحی نظام رزمایش سایبری جمهوری اسلامی ایران. دو فصلنامه بازی جنگ. ۷(۱۵)، ۱۱۷- ۱۳۶.

DOI: 10.22034/ijwg.2025.491655.1107

ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

مقدمه

در دنیای امروز فضای سایبری به‌عنوان یکی از ارکان اساسی جوامع امروزی در تمامی حوزه‌ها از جمله اقتصاد، سیاست، نظامی‌گری و فرهنگ شناخته می‌شود. بخش عمده‌ای از فعالیت‌ها و تعامل‌های اقتصادی، تجاری، فرهنگی، اجتماعی و حاکمیتی کشور، در کلیه سطوح، اعم از افراد، مؤسسات غیردولتی و نهادهای دولتی و حاکمیتی، در فضای سایبر انجام می‌گیرد. زیرساخت‌ها و سامانه‌های حیاتی و حساس کشور یا خود بخشی از فضای سایبری کشور را تشکیل می‌دهند و یا از طریق این فضا، کنترل، مدیریت و بهره‌برداری می‌شوند و عمده اطلاعات حیاتی و حساس کشور نیز به این فضا منتقل و یا اساساً در این فضا، شکل‌گرفته است.

با توجه به مجموعه تهدیدهای سایبری که کشور را احاطه کرده و دامنه آن در حال افزایش است، یکی از چالش‌های اساسی، توانایی دفاع در برابر این حمله‌های سایبری است. در این راستا، ارتقای آمادگی و توانمندی‌های دفاعی در فضای سایبری به یکی از ضروریات اساسی تبدیل شده است. یکی از روش‌های مؤثر برای تحقق این هدف، اجرای رزمایش‌های سایبری است. رزمایش‌های سایبری به‌عنوان تمرینی عملیاتی و شبیه‌سازی‌شده به سازمان‌ها و کشورها این امکان را می‌دهند که با سناریوهای مختلف تهدیدهای سایبری روبه‌رو شده و توانایی خود را در پاسخ به حمله‌های سایبری ارزیابی و تقویت کنند.

با توجه به اینکه تهدیدهای سایبری به‌سرعت در حال تحول هستند و روزبه‌روز پیچیده‌تر می‌شوند، لزوم برگزاری رزمایش‌های سایبری به‌منظور آمادگی بهتر، هماهنگی مؤثرتر و واکنش سریع‌تر در برابر حمله‌ها، امری غیر قابل انکار است. در این راستا، رزمایش‌ها به سازمان‌ها و دولت‌ها کمک می‌کنند تا با شبیه‌سازی شرایط بحرانی، روند پاسخگویی به بحران‌ها را بهبود بخشند و در مقابل تهدیدهای سایبری، استراتژی‌های دفاعی کارآمدتر را طراحی و اجرایی کنند؛ بنابراین ایجاد و برگزاری رزمایش‌های سایبری به‌عنوان ضرورتی استراتژیک، نه‌تنها به تقویت توان دفاعی کمک می‌کند؛ بلکه نقشی کلیدی در حفظ امنیت ملی و زیرساخت‌های حیاتی دارد.

در پژوهش حاضر، از الگوی منطق در طراحی نظام و فرایندهای مربوط به آن استفاده شده است؛ چراکه برای پیاده‌سازی کامل و موفق یک نظام جامع و مانع، لازم است که تفکر سیستمی و جامع‌نگر بر سازمان و محیط کار و فعالیت حاکم بوده و فرهنگ سازمانی با اصول و الزامات آن هماهنگی داشته و روحیهٔ کارِگروهی و انعطاف‌پذیری در سازمان جاری و ساری باشد. در این الگو به دلیل وجود ساختار سلسله‌مراتبی و وجود روابط منطقی علّی

و معلولی بین سطوح مختلف در این سلسله‌مراتب، امکان ردیابی بهتر و دقیق‌تر مشکلات و نواقص وجود دارد. این شرایط ضمن تسهیل رفع مشکلات، گزارش‌دهی دقیق‌تر از عملکردها را ممکن می‌سازد. نظام رزمایش سایبری به معنی تعیین ابعاد مؤلفه‌ها و زیرمؤلفه‌های مؤثر در رزمایش سایبری با تبیین کارکرد مستقل و وابسته هر یک از آن‌ها با هم برای فهم و جهت‌گیری سیستمی در ارتباط با نهادینه کردن مؤلفه‌های رزمایش سایبری به‌منظور زمینه‌سازی و ایجاد چارچوب‌هایی برای انجام تکالیف فردی و سازمانی و هم‌افزایی بین آن‌ها است.

با توجه به موارد فوق هدف این تحقیق ایجاد چارچوب مناسبی برای سازمان‌دهی رزمایش‌های سایبری خواهد بود. با داشتن یک نظام سایبری در کشور، برآورد صحیحی از شرایط و آمادگی سامانه‌ها و تجهیزات جهت مقابله با تهدیدها و حمله‌های سایبری صورت خواهد گرفت و ضمن افزایش امنیت فضای سایبر و ارتقای قدرت سایبری، شرایط لازم جهت مشارکت در رزمایش‌های سایبری بین‌المللی برای کشور فراهم خواهد شد. در تحقیق پیش رو مفاهیم، ماهیت، اصول، منابع، پیامدها و دستاوردهای نظام رزمایش سایبری ج.ا.ا احصا می‌شود و بر این اساس الگو نظام رزمایش سایبری ج.ا.ا به همراه اجزای شکل‌دهنده آن شامل ورودی‌ها، فرایندها، مؤلفه‌ها، خروجی، نتایج و بازخورد ترسیم خواهد شود.

مبانی نظری و پیشینه‌های پژوهش

پیشینه و ادبیات تحقیق

روسیه و آمریکا به‌صورت مشترک فضای سایبر را یک رسانه الکترونیکی معرفی کرده‌اند که از طریق آن اطلاعات تولید، منتقل، دریافت، ذخیره، پردازش یا حذف می‌شوند (Rauscher & Yaschenko, 2011).

واژه رزمایش از ترکیب دو واژه رزم و آزمایش به وجود آمده است و به معنای «تمرین گستردهٔ نیروهای مسلح به‌طور جداگانه یا همراه با هم است» (رزاق زاده، ۱۳۸۹). رزمایش یا مانور نظامی به تمرینی نظامی در مقیاس بزرگ گفته می‌شود که در آن روش‌های گوناگون رزمی اجرا و شبیه‌سازی می‌شوند. رزمایش در اصل، شبیه‌سازی شرایط جنگی است و هدف از آن آزمودن و همچنین آموختن شگردهای جنگی است. منظور از برگزاری رزمایش نظامی، آموزش افراد، آموزش یگان‌های کوچک به‌عنوان جزئی از یک یگان بزرگ‌تر و بالاخره آموزش فعالیت‌های هماهنگ دیگر یگان‌های رزمی، پشتیبانی رزمی و پشتیبانی خدمات رزمی به یگان‌های بزرگ‌تر است. رزمایش می‌تواند در سطح یک نیرو یا بیشتر از یک نیرو برگزار

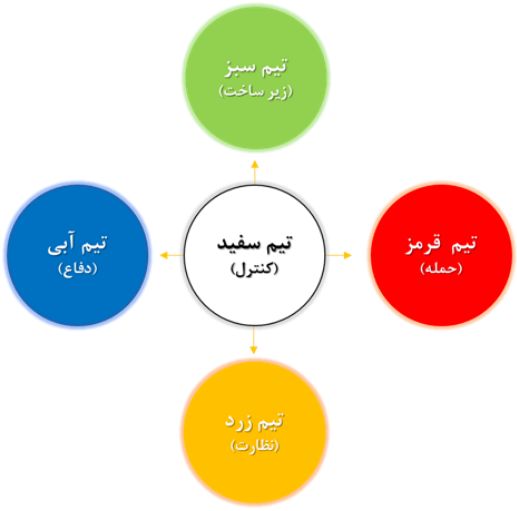
شود (رائی، فرورش و نخعی کمال‌آبادی، ۱۳۹۷). تابه‌حال هیچ تفسیر واحدی از رزمایش سایبری[۱] پذیرفته نشده است. به‌طوری‌که در موقعیت‌های مختلف اصطلاحات مختلفی برای آن استفاده شده است که تعلیم سایبری[۲] و محدوده سایبری[۳] نمونه‌هایی از این اصطلاحات هستند. در این زمینه گاهی اوقات از اصطلاح آموزش سایبری[۴] استفاده شده که در هنگام سازمان‌دهی رزمایش‌های سایبری از راه دور بیشتر به کار رفته است. این اصطلاح به‌طور عمده بر کسب دانش نظری متمرکز است که برخلاف آن، «تعلیم سایبری» و «محدوده سایبری» متمرکز بر کسب مهارت‌های عملی امنیت سایبری هستند (Kick, 2014; Seker & Ozbenli, 2018; Yamin, Katt & Gkioulos, 2020).

اصطلاحاتی مانند رزمایش امنیت سایبری[۵] و رزمایش دفاع سایبری[۶] اغلب می‌توانند جایگزین هم شوند. رزمایش سایبری را به‌عنوان فرایندی برای آماده‌سازی، ارزیابی، تمرین و بهبود اثربخشی سازمان برای اطمینان از امنیت سایبری توصیف می‌کنند. آن‌ها فعالیت‌های مدل‌سازی کامپیوتری در مقیاس بزرگ و همچنین رزمایش‌های روی میز را پوشش می‌دهند (Vykopal, et al. 2017).

به‌طورکلی طبق تعریف مرکز ملی امنیت سایبری فنلاند[۷] «رزمایش سایبری رویدادی است که با مدل‌سازی یک سناریو خیالی که ممکن است سازمان با آن مواجه شود، آمادگی سازمان را در برابر حادثه سایبری موجود، آزمایش می‌کند» (مرکز ملی امنیت سایبری فنلاند، ۲۰۲۱). همچنین افراد گوناگونی در مطالعات خود، تعاریف مختلفی را برای رزمایش سایبری استفاده کرده‌اند. طبق تعریف سکر[۸] و اوزبنلی[۹] (۲۰۱۸)، «رزمایش سایبری یک سازوکار کارآمد برای آموزش و آگاهی از امنیت فناوری اطلاعات شناسایی شده است که به‌عنوان ابزار نهایی برای آشکارسازی و تعریف نیازهای امنیتی مختلف هر سازمان شناخته می‌شود». همچنین طبق تعریف آقای موحدی‌راد و مدیری (۱۳۹۳) «رزمایش سایبری رزمایشی است که اهداف آن به‌طور عمده بر حفاظت، دفاع و بازیابی دارایی‌ها بوده و عملیات سایبری حیاتی برای ارائه سرویس در برابر حمله‌ها یا حوادث سایبری است». آقای یمین[۱۰]

1. Cyber exercise
2. Cyber training
3. Cyber range
4. Cyber learning
5. Cybersecurity exercises
6. Cyber defense exercises
7. National Cyber Security Centre Finland
8. Ensar
9. Ozbenli
10. Yamin

و همکاران (۲۰۲۰) رزمایش سایبری را به‌عنوان «یک تمرین آموزشی که سناریوهای حمله یا دفاع را در محیط‌های مجازی یا فیزیکی با هدف بهبود درک و مهارت‌های هجومی یا دفاعی شرکت‌کنندگان اجرا می‌کند»، تعریف کردند. امروزه عملاً رزمایش‌های سایبری به سه روش دورمیزی، ترکیبی و در مقیاس کامل انجام می‌گیرد (موحدی‌راد و مدیری، ۱۳۹۳). در هر رزمایش سایبری چندین تیم نقش‌آفرینی می‌کنند که در این زمینه، تیم آبی مسئول تضمین و دفاع از امنیت سیستم‌های اطلاعاتی یک شرکت یا سازمان در برابر مهاجمان مجازی (تیم قرمز) بوده و هدف تیم قرمز دستیابی به حمله‌های سایبری به‌طور یکسان به تمام تیم‌های آبی شرکت‌کننده در تمرین است. تیم سبز مسئولیت تهیه و نگهداری سیستم‌ها و زیرساخت‌های ورزشی را بر عهده دارد. نقش تیم زرد این است که در طول تمرین ابتدا برای تیم سفید و سپس برای همه شرکت‌کنندگان در رزمایش، آگاهی موقعیتی را فراهم کند. تیم سفید مسئول سازمان‌دهی تمرین و بررسی آن در حین اجراست. (مرکز تعالی دفاع سایبری تعاونی ناتو[1] ، ۲۰۱۶) .



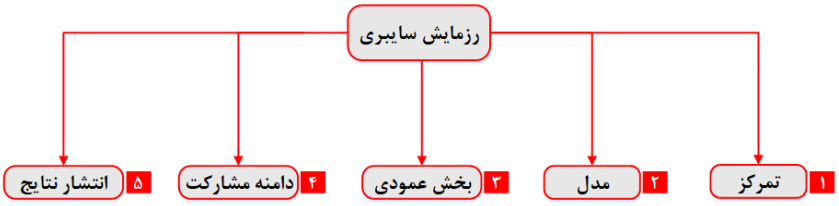
شکل (۱) تیم‌های رزمایش سایبری (منبع: مرکز تعالی دفاع سایبری تعاونی ناتو، ۲۰۱۶)

سازمان امنیت سایبری ایالات‌متحده آمریکا، رزمایش‌های ملی مختلفی از جمله طوفان سایبری[2] و رزمایش رومیزی رای[3] را انجام می‌دهد (آژانس امنیت سایبری و امنیت

1. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

2. Cyber Storm
3. Tabletop the Vote

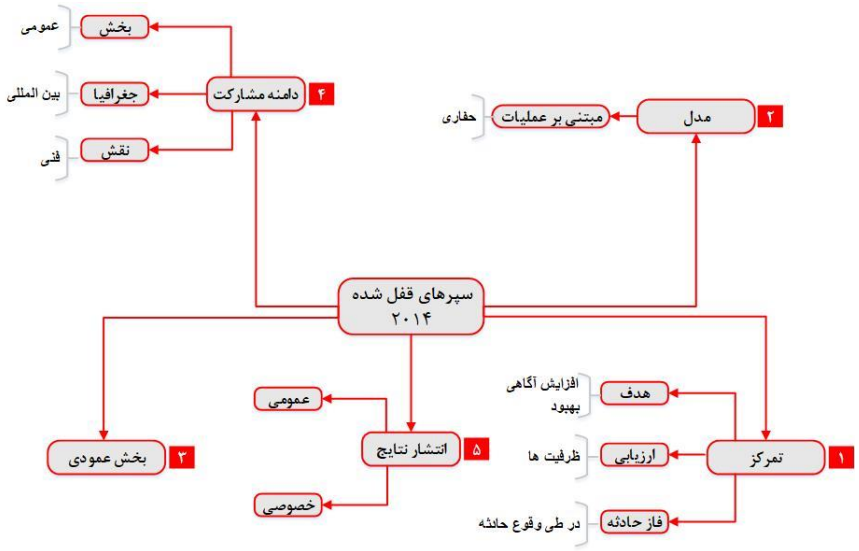
زیرساخت[1]، ۲۰۲۲). همچنین سکوی رزمایش سایبری[2] پاسخ آژانس امنیت سایبری اتحادیه اروپا به چالش‌های سایبری است که با مدیریت تمرین‌های پیچیده و نزدیک‌تر کردن جامعه رزمایش به این امر می‌پردازد (آژانس امنیت شبکه و اطلاعات اتحادیه اروپا، ۲۰۲۲). جدای از برنامه اروپای سایبری، آژانس امنیت شبکه و اطلاعات اتحادیه اروپا[3] در تمرین‌های دیگر با ذی‌نفعان مختلف شرکت کرده از آن‌ها حمایت می‌کند. رزمایش سایبری واکنش به بحران سیاسی ۲۰۱۴، رزمایش سایبری یورو کنترل، مدیریت بحران داخلی کمیسیون اروپا، رزمایش منطقه‌ای سوپکس و سایبر آتلانتیک ۲۰۱۱ نمونه‌ای از سایر فعالیت‌های این اتحادیه است (آژانس امنیت شبکه و اطلاعات اتحادیه اروپا، ۲۰۱۸). موسسه ملی امنیت سایبری اسپانیا[4] با همکاری آژانس امنیت شبکه و اطلاعات اتحادیه اروپا طبقه‌بندی پیشنهادی خود را با توجه به تجزیه و تحلیل قبلی و پروفایل‌های سایبری موجود و با در نظر گرفتن مطالعات انجام‌شده توسعه داده است. طبقه‌بندی شامل پنج عنصر اساسی است که در شکل ۲ نشان داده شده است.



شکل (۲) پنج عنصر اصلی ساختار رزمایش سایبری (منبع: آژانس امنیت شبکه و اطلاعات اتحادیه اروپا، ۲۰۱۸)

همچنین سپرهای قفل‌شده[5] نمونه‌ای از رزمایش‌های سایبری است که مرکز تعالی دفاع سایبری تعاونی ناتو برگزار کرده است. شکل ۳ ساختار رزمایش سپرهای قفل‌شده را به تصویر کشیده است (مرکز تعالی دفاع سایبری تعاونی ناتو، ۲۰۱۶).

1. Cybersecurity and Infrastructure Security Agency (CISA)
2. CEP
3. European Network and Information Security Agency (ENISA)
4. INCIBE
5. Locked Shields

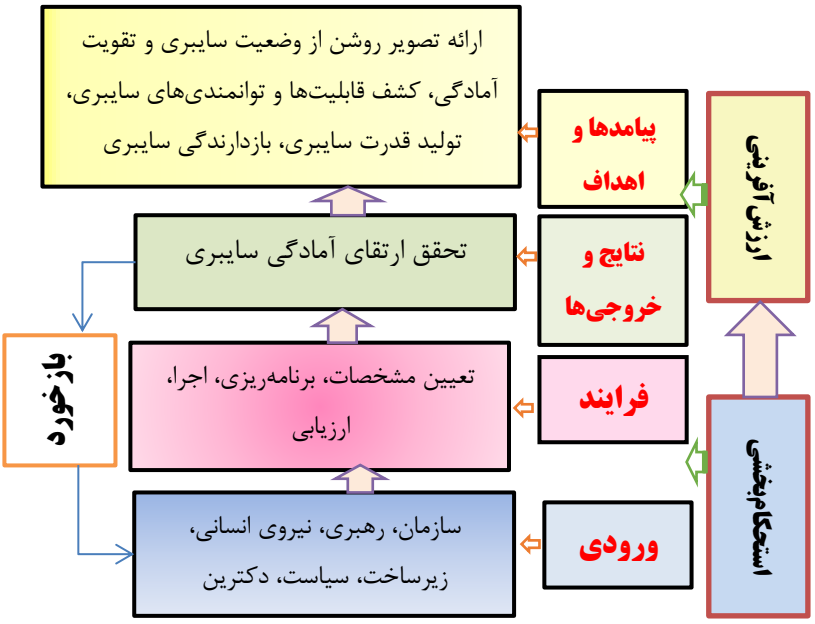


شکل (۳) نمودار شماتیکی ساختار رزمایش سپرهای قفل‌شده (منبع: مرکز تعالی دفاع سایبری تعاونی ناتو، ۲۰۱۶)

با در نظر گرفتن تحقیقات ذکر شده و با توجه به مطالعات میدانی و شباهت‌سنجی صورت گرفته، مشخص شد به حوزه رزمایش دفاع سایبری در کشور، توجه چندانی نشده است و با در نظر گرفتن شرایط کنونی کشور و ظهور فناوری‌های نوظهور و لزوم به‌کارگیری این فناوری‌ها در حوزهٔ دفاعی، توجه به نظام رزمایش دفاع سایبری کشور، بسیار حائز اهمیت است که تاکنون کسی به این موضوع نپرداخته است و لذا نتایج آن از نوآوری خوبی برخوردار است. نوآوری ویژه این تحقیق را می‌توان مفهوم‌سازی، شناخت ماهیت، دروندادها، فرایندها، برون‌دادها، بازیگران، پیامدها و دستاوردهای مبتنی بر فناوری‌های نوظهور در نظام رزمایش دفاع سایبری کشور دانست؛ زیرا یک نظام نوین و با ادبیات بومی ارائه خواهد شد.

چارچوب و مدل مفهومی تحقیق

با توجه به ارائه دیدگاه‌های نظری پیرامون موضوع تحقیق و با استناد به منابع علمی و مصاحبه عمیق با خبرگان درباره مسائل و اهداف پژوهش، الگوی مفهومی این پژوهش از چهار بخش به شرح شکل ۴ تشکیل شده است.

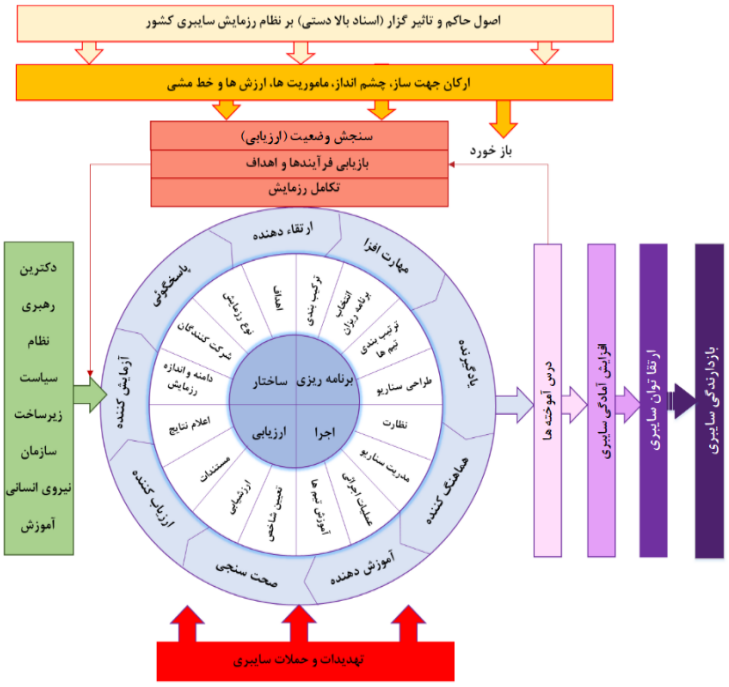


شکل (۴) چارچوب نظام رزمایش سایبری (منبع: پژوهشگر)

همان‌گونه که ملاحظه می‌شود، این تصویر دارای دو بخش کلان شامل: الف) استحکام‌بخشی درونی (سرمایه‌های انسانی / فناوری‌ها و فرایندها) و ب) ارزش‌آفرینی بیرونی (نتایج / خروجی‌ها و پیامدها / اهداف نهایی) است.

در بخش ورودی که اساس و جان‌مایهٔ اصلی برای تحقق حرکت بیرونی است و مشتمل بر: سازمان، رهبری، سرمایه‌های انسانی، زیرساخت‌ها، سیاست، دکترین سرمایه‌های اصلی است. با توجه به شکل بعدی و بر اساس الگوی منطق علّی و معلولی، برای به فعلیت درآوردن و آماده نگه‌داشتن ظرفیت‌های عناصر ورودی، اتخاذ رویکرد فرایندی از قبیل (فرایندهای مدیریتی، عملیاتی و فنی جهت تعیین مشخصات، برنامه‌ریزی، اجرا و ارزیابی) ضرورت دارد. در این بخش عملکرد نحوه مدیریت و هدایت سازمان و تعاملات درون و برون‌سازمانی در اجرای رزمایش سایبری مورد ارزیابی و بررسی قرارگرفته و نتیجه این بخش در خروجی نظام مذکور منظور شد. در انتها بازخوردهای مراحل خروجی و فرایندها برای اصلاح، بهبود و تکامل عملیات رزمایش در تطابق با اهداف از پیش تعیین شده نظام مذکور، ترازیابی و به مرحله ورودی‌ها انتقال می‌یابد.

پس از تعیین چارچوب و مفهوم‌شناسی رزمایش سایبری و فرایندهای آن، مدل مفهومی کلان برای نظام رزمایش سایبری جمهوری اسلامی ایران مطابق شکل ۵ ارائه شد.



شکل (۵) الگوی مفهومی نظام رزمایش سایبری (منبع: پژوهشگر)

روش‌شناسی پژوهش

روش پژوهش در این رساله از نظر ماهیت و نحوه گردآوری داده‌ها توصیفی است و با عنایت به اینکه درصدد است در یک مورد خاص (ارائه نظام رزمایش سایبری کشور) عمیق شود؛ بنابراین این پژوهش از حیث ماهیت از نوع توصیفی - موردی هست. همچنین رویکرد مورداستفاده برای جمع‌آوری و تجزیه و تحلیل داده‌ها آمیخته (کیفی و کمّی) است.

داده‌های جمع‌آوری‌شده از مطالعه عمیق و گسترده ادبیات تحقیق شامل: منابع موجود در حوزه رزمایش سایبری، بررسی اسناد بالادستی، بررسی اسنادی کشورهای مختلف، مصاحبه با خبرگان و مدنظر قرار دادن وظایف و مأموریت سازمان‌های مسئول در این حوزه بر اساس سؤالات اصلی و فرعی تحقیق به دست آمده است. این اطلاعات با به‌کارگیری رویکرد کیفی و استفاده از ابزار تحلیل مضمون به‌منظور استخراج ابعاد و مؤلفه‌ها و زیر مؤلفه‌های اصلی رزمایش سایبری مورد بهره‌برداری قرار گرفته است. در این مرحله مضامین پایه (زیر مؤلفه‌های اصلی) به‌دست‌آمده پس از دسته‌بندی و همگن‌سازی (در قالب مضامین فراگیر (مؤلفه) و سازمان‌دهنده (ابعاد) به جامعه خبرگان پژوهش ارائه شدند. سرانجام و پس از

اعمال اصلاحات لازم، در مرحله بعد به روش کمّی و از طریق پیمایش با استفاده از ابزار پرسش‌نامه محقق ساخته، اعتباریابی ابعاد، مؤلفه‌ها و زیرمؤلفه‌های اصلی نظام و همچنین بررسی روابط بین آن‌ها به کمک روش‌های مدل‌سازی معادلات ساختاری انجام شده است. جامعهٔ آماری این تحقیق با توجه به داده‌های آن به دو جامعهٔ کیفی و کمّی تقسیم می‌شوند که جامعهٔ کیفی به دو دسته اسنادی و خبرگی تقسیم می‌شود. به‌منظور ارزیابی مضامین پایه، فراگیر و سازمان‌دهنده به‌دست‌آمده در قالب ابعاد، مؤلفه و زیر مؤلفه‌های نظام رزمایش سایبری و تحلیل روابط بین آن‌ها از ۵۰ نفر از خبرگان و صاحب‌نظران آشنا با فضای سایبر و رزمایش سایبری استفاده شد.

روش نمونه‌گیری در جامعهٔ اسنادی برای شناسایی و تعریف اجزا به‌صورت تمام شمار بوده و برای جامعهٔ میدانی (پیمایشی) از نوع هدفمند قضاوتی و گلوله‌برفی بوده و حجم آن‌ها تا اشباع نظری ادامه پیدا کرد. همچنین با توجه به محدود بودن تعداد جامعهٔ آماری در این پژوهش حجم نمونه برابر با حجم جامعهٔ آماری یعنی تعداد ۵۰ نفر است؛ لذا روش نمونه‌گیری به‌صورت تمام شمار است.

برای گردآوری داده‌ها در این رساله، از هر دو روش گردآوری اطلاعات یعنی روش‌های کتابخانه‌ای و میدانی استفاده شده است. بخش مربوط به ادبیات موضوع و مبانی نظری، بررسی مفاهیم و انجام مطالعات تطبیقی با استناد به منابع کتابخانه‌ای، کتب تخصصی، وب‌سایت‌های معتبر، مجلات علمی، پایگاه‌های اطلاعاتی، اسناد بالادستی، رساله‌ها و پروژه‌های تحقیقاتی داخلی و خارجی و غیره است که با استفاده از ابزار فیش تهیه شده است. بخش دیگر مربوط به کسب نظرات نخبگان، اساتید، صاحب‌نظران و متخصصان حوزه سایبری و علوم شناختی است که با استفاده از ابزارهای میدانی شامل مصاحبه، پرسش‌نامه و طوفان فکری گردآوری شد. در پژوهش حاضر ابتدا با فیش‌برداری از مطالعات کتابخانه‌ای و مصاحبه‌های عمیق با خبرگان و تحلیل داده‌های به‌دست‌آمده با استفاده از تکنیک تحلیل مضمون، نظام رزمایش سایبری احصاء و به تأیید خبرگان مرتبط رسید. سپس در گام دوم به‌منظور تجزیه و تحلیل داده‌های حاصل از این بخش و بررسی روابط بین اجزاء نظام از مدل‌یابی معادلات ساختاری استفاده شد.

همچنین در این پژوهش برای بررسی روایی محتوایی به شکل کمّی از ضریب نسبی روایی محتوا[1] (CVR) استفاده شد. برای تعیین CVR، در مرحله پیش‌آزمون پرسش‌نامه از تعدادی

1 Content Validity Ratio

از متخصصان و صاحب‌نظران حوزه موردمطالعه درخواست شد نظر خود را درباره اهمیت عوامل مندرج در پرسش‌نامه با انتخاب یکی از گزینه‌های پنج‌گانه که بر اساس مقیاس پنج‌گزینه‌ای طیف لیکرت ((۵) خیلی زیاد؛ (۴) زیاد؛ (۳) متوسط؛ (۲) کم و (۱) خیلی کم) بیان کنند. سپس ضریب نسبی روایی محتوا با روش زیر محاسبه شد.

$$CVR=\frac{\frac{\text{تعداد کل متخصصین}}{۲}-\text{تعداد متخصصینی که گزینه مربوط را انتخاب کرده‌اند}}{\frac{\text{تعداد کل متخصصین}}{۲}}$$

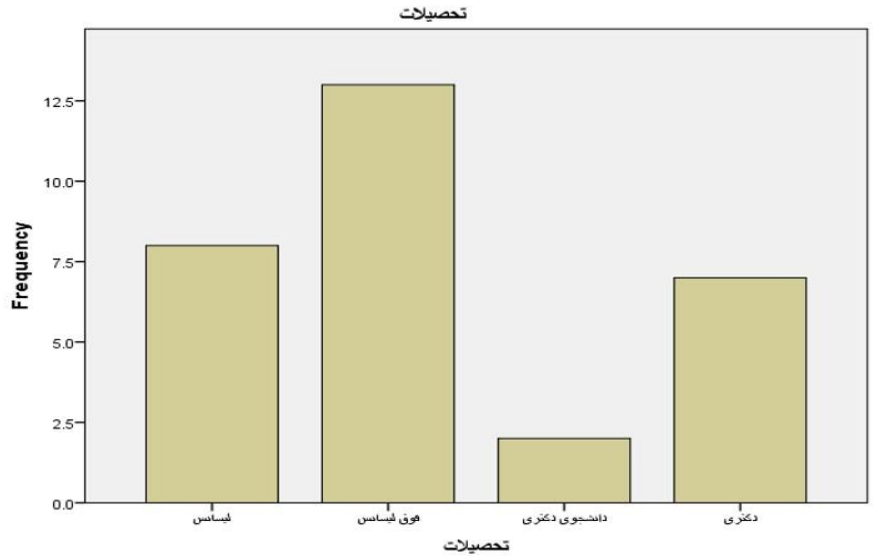
در تحقیق حاضر برای سنجش پایایی پرسش‌نامه از روش مقیاس آلفای کرونباخ استفاده شد. مقدار ضریب آلفای کرونباخ به‌دست‌آمده از نرم‌افزار SPSS برای کل سؤالات پرسش‌نامه باید بیشتر از (۰/۷) باشد که می‌توان نتیجه گرفت که پایایی مربوط به این سؤالات مورد تأیید است.

تجزیه و تحلیل داده‌ها

در این تحقیق از پرسش‌نامه به‌منظور اخذ نظر صاحب‌نظران در رابطه با الگوی کلی نظام رزمایش سایبری جمهوری اسلامی ایران استفاده شده است و سپس داده‌های خام با استفاده از نرم‌افزار و فنون آماری مورد تجزیه و تحلیل قرار گرفته‌اند. در ادامه نتایج تجزیه و تحلیل داده‌ها آمده است.

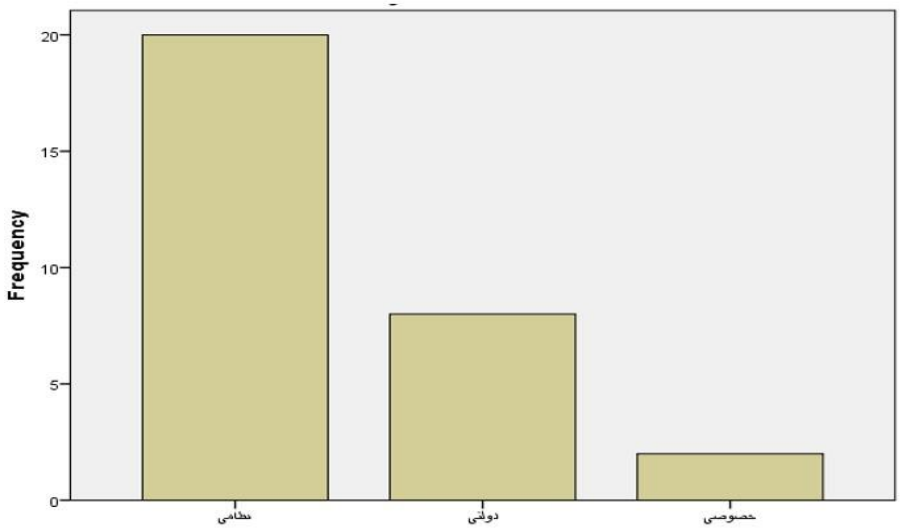
تجزیه و تحلیل توصیفی پرسش‌های جمعیت‌شناختی

آمار توصیفی شامل آمار توصیفی پرسش‌های جمعیت‌شناختی و آمار توصیفی پرسش‌های اصلی (به تفکیک سؤالات) است.



شکل (۶) توزیع درصد فراوانی سطح تحصیلات

در شکل ۶ میزان تحصیلات شرکت‌کنندگان مشاهده می‌شود که بر این اساس ۴۳ درصد پاسخ‌دهندگان دارای مدرک فوق لیسانس هستند و از این حیث بیشترین فراوانی را نسبت به سایر پاسخ‌دهندگان دارند. بنابراین نمونه آماری تحقیق با توجه به سطح مدارک دانشگاهی از میزان درک و اطلاعات کافی در خصوص نظام رزمایش سایبری جمهوری اسلامی ایران برخوردار است و این مسئله اعتبار بالای نتایج این پژوهش را نشان می‌دهد.



شکل (۷) توزیع درصد نوع مسئولیت در حوزه رزمایش سایبری

همچنین در شکل ۷ پاسخ‌دهندگان به پرسش‌نامه از نظر نوع مسئولیت در سازمان تفکیک‌شده‌اند که با توجه به نمودار اکثریت پاسخ‌دهندگان را با فراوانی ۶۶ درصد افراد نظامی تشکیل می‌دهند. از این تعداد ۴۰ درصد مدیر عملیاتی و ۳۰ درصد مدیر راهبردی در حوزه رزمایش سایبری بودند؛ بنابراین نمونه آماری از سابقه کار کافی و اشراف لازم در خصوص رزمایش سایبری برخوردار است و این مسئله اعتبار بالای نتایج این پژوهش را نشان می‌دهد.

تجزیه و تحلیل توصیفی سؤالات پرسش‌نامه

در این بخش هر یک از سؤالات پرسش‌نامه در مورد قسمت‌های مختلف الگو پیشنهادی نظام رزمایش سایبری به تفکیک، مورد تجزیه و تحلیل آماری قرار گرفته و نتایج در ادامه آورده شده است.

جدول (۱) تحلیل آماری اجزا کلان نظام رزمایش سایبری

	تعداد								
	معتبر (valid)	گمشده (missing)	میانه	انحراف استاندارد	واریانس	چولگی	خطای استاندارد ضریب چولگی	کشیدگی	خطای استاندارد ضریب کشیدگی
ورودی‌ها	30	0	4.6667	.47946	.230	-.745	.427	-1.554	.833
عوامل ظرفیت ساز	30	0	4.3667	.76489	.585	-.755	.427	-.836	.833
فرایندها	30	0	4.6000	.67466	.455	-2.194	.427	6.363	.833
مؤلفه‌ها	30	0	4.2333	.93526	.875	-1.045	.427	.223	.833
عوامل تأثیرگذار	30	0	4.2333	.81720	.668	-1.282	.427	2.014	.833
نتایج	30	0	4.6667	.54667	.299	-1.407	.427	1.201	.833
بازخورد	30	0	4.7333	.52083	.271	-1.867	.427	2.934	.833

طبق جدول (۱) مشاهده می‌شود که همه اجزا کلان رزمایش سایبری توسط پاسخ‌دهندگان تأییدشده‌اند. در ضمن با توجه به اینکه خطای استاندارد ضریب چولگی و ضریب کشیدگی بین ۲ و ۲- قرار دارد نرمال بودن توزیع داده‌ها تأیید می‌شود.

جدول (۲) تحلیل آماری ورودی‌های نظام رزمایش سایبری

	تعداد		میانه	انحراف استاندارد	واریانس	چولگی	خطای استاندارد ضریب چولگی	کشیدگی	خطای استاندارد ضریب کشیدگی
	معتبر	گمشده							
اصول حاکم و تأثیرگذار (اسناد بالادستی)	30	0	4.2667	.58329	.340	-.086	.427	-.357	.833
ارکان جهت‌ساز در حوزه رزمایش سایبری	30	0	4.5000	.73108	.534	-1.702	.427	3.475	.833
خط‌مشی و چشم‌اندازها در حوزه رزمایش سایبری	30	0	4.6667	.60648	.368	-1.693	.427	1.958	.833
مأموریت‌ها و عملیات انجام‌شده در حوزه رزمایش سایبری (ملی و فراملی)	30	0	4.2667	.82768	.685	-.942	.427	.350	.833
ارزش‌های ملی در حوزه رزمایش سایبری	30	0	3.9000	.88474	.783	-1.716	.427	3.916	.833

با توجه به جدول (۲) مشاهده می‌شود که همه ورودی‌های نظام رزمایش سایبری توسط پاسخ‌دهندگان تأییدشده‌اند. در ضمن با توجه به اینکه خطای استاندارد ضریب چولگی و ضریب کشیدگی بین ۲ و ۲- قرار دارد نرمال بودن توزیع داده‌ها تأیید می‌شود.

جدول (۳) تحلیل آماری ظرفیت سازهای نظام رزمایش سایبری

	تعداد		میانه	انحراف استاندارد	واریانس	چولگی	خطای استاندارد ضریب چولگی	کشیدگی	خطای استاندارد ضریب کشیدگی
	معتبر	گمشده							
رهبری	30	0	4.8333	.37905	.144	-1.884	.427	1.657	.833
نظام	30	0	4.6000	.56324	.317	-1.042	.427	.176	.833
دکترین	30	0	4.6000	.62146	.386	-1.330	.427	.831	.833

سیاست	30	0	4.3667	.71840	.516	-1.290	.427	2.614	.833
زیرساخت‌ها	30	0	4.6667	.54667	.299	-1.407	.427	1.201	.833
سازمان‌ها و نیروی انسانی	30	0	4.5333	.57135	.326	-.732	.427	-.429	.833
آموزش	30	0	4.6000	.56324	.317	-1.042	.427	.176	.833

با توجه به جدول (۳) مشاهده می‌شود که همه ظرفیت‌سازها توسط پاسخ‌دهندگان تأیید شده‌اند. در ضمن با توجه به اینکه خطای استاندارد ضریب چولگی و ضریب کشیدگی بین ۲ و ۲- قرار دارد نرمال بودن توزیع داده‌ها تأیید می‌شود.

جدول (۴) تحلیل آماری فرآیندهای نظام رزمایش سایبری

	تعداد		میانه	انحراف استاندارد	واریانس	چولگی	خطای استاندارد ضریب چولگی	کشیدگی	خطای استاندارد ضریب کشیدگی
	معتبر	گمشده							
ساختار	30	0	4.8333	.37905	.144	-1.884	.427	1.657	.833
برنامه‌ریزی	30	0	4.7667	.43018	.185	-1.328	.427	-.257	.833
اجرا	30	0	4.6000	.56324	.317	-1.042	.427	.176	.833
ارزیابی	30	0	4.6000	.56324	.317	-1.042	.427	.176	.833

با توجه به جدول ۴ مشاهده می‌شود که همه فرایندهای نظام رزمایش سایبری توسط پاسخ‌دهندگان تأیید شده‌اند. در ضمن با توجه به اینکه خطای استاندارد ضریب چولگی و ضریب کشیدگی بین ۲ و ۲- قرار دارد نرمال بودن توزیع داده‌ها تأیید می‌شود.

جدول (۵) تحلیل آماری مصادیق بازخورد در نظام رزمایش سایبری

	تعداد		میانه	انحراف استاندارد	واریانس	چولگی	خطای استاندارد ضریب چولگی	کشیدگی	خطای استاندارد ضریب کشیدگی
	معتبر	گمشده							
سنجش میزان موفقیت و پیشرفت	30	0	4.9333	.25371	.064	-3.660	.427	12.207	.833

بازیابی فرایندها و اهداف	30	0	4.7000	.53498	.286	-1.621	.427	1.950	.833
بهبود و تکامل رزمایش	30	0	4.8667	.34575	.120	-2.273	.427	3.386	.833

با توجه به جدول (۵) مشاهده می‌شود که همه مصادیق بازخورد توسط پاسخ‌دهندگان تأیید شده‌اند. در ضمن با توجه به اینکه خطای استاندارد ضریب چولگی و ضریب کشیدگی بین ۲ و ۲- قرار دارد نرمال بودن توزیع داده‌ها تأیید می‌شود.

جدول (۶) تحلیل آماری خروجی‌های نظام رزمایش سایبری

	تعداد		میانه	انحراف استاندارد	واریانس	چولگی	خطای استاندارد ضریب چولگی	کشیدگی	خطای استاندارد ضریب کشیدگی
	معتبر	گمشده							
افزایش آمادگی سایبری در برابر تهدیدها	30	0	4.8333	.37905	.144	-1.884	.427	1.657	.833
ارتقا، یکپارچه‌سازی و همگام‌سازی توان رزمایش سایبری	30	0	4.6333	.55605	.309	-1.216	.427	.623	.833
افزایش بازدارندگی سایبری در مقابل تهدیدها	30	0	4.5333	.62881	.395	-1.025	.427	.113	.833

با توجه به جدول (۶) مشاهده می‌شود که همه مصادیق خروجی توسط پاسخ‌دهندگان تأییدشده‌اند. در ضمن با توجه به اینکه خطای استاندارد ضریب چولگی و ضریب کشیدگی بین ۲ و ۲- قرار دارد نرمال بودن توزیع داده‌ها تأیید می‌شود.

نتیجه‌گیری و پیشنهادها

در این مقاله با بررسی ضرورت‌ها و چالش‌های موجود در زمینه رزمایش سایبری، به ارائهٔ الگوی نظام رزمایش سایبری کشور پرداخته شد. با توجه به پیچیدگی و تنوع تهدیدهای سایبری که می‌تواند به زیرساخت‌های حیاتی کشور آسیب وارد کند، ایجاد یک نظام رزمایش سایبری جامع و کارآمد به‌عنوان یک ضرورت استراتژیک مطرح می‌شود. این نظام نه‌تنها در

ارتقای آمادگی سازمان‌ها و نهادهای مختلف در مواجهه با بحران‌های سایبری مؤثر است، بلکه می‌تواند به شبیه‌سازی حملات سایبری، ارزیابی نقاط ضعف و بهبود فرایندهای پاسخگویی کمک کند. مدل مفهومی به‌دست‌آمده بر اساس مطالعات و بررسی‌های گسترده صورت گرفته و پس از اعتبارسنجی مدل اولیه از طریق اخذ نظر صاحب‌نظران در قالب پرسش‌نامه و تجزیه و تحلیل نتایج آن احصا شد. بر این اساس عوامل شکل‌دهندهٔ نظام رزمایش دفاع سایبری ج.ا.ا شامل ۷ بخش ورودی‌ها، عوامل ظرفیت ساز، فرایندها، مؤلفه‌ها، عوامل تأثیرگذار، نتایج و بازخورد است.

الگوی پیشنهادی شامل چهار فرایند ساختار، برنامه‌ریزی، اجرا و ارزیابی است. این فرایندها در چرخه رزمایش سایبری به‌هم‌پیوسته و ضروری هستند تا یک رزمایش مؤثر و کارآمد ایجاد شود. ساختار رزمایش بیانگر مواردی همچون اهداف، دامنه مشارکت، مدل و نوع رزمایش است. برنامه‌ریزی دقیق و هدفمند، پایه‌گذار موفقیت سایر مراحل است، طراحی سناریو، ترتیب‌بندی تیم‌ها و آماده‌سازی منابع، شرایط لازم برای یک رزمایش مؤثر را فراهم می‌کند. در مرحله اجرا به‌کارگیری سناریوهای طراحی‌شده، آموزش و مدیریت هماهنگی بین تیم‌ها و سیستم‌ها، عملکرد واقعی آن‌ها را در شرایط بحرانی آزمایش می‌کند. پس از اجرا، ارزیابی نتایج و تعیین شاخص‌ها و تجزیه و تحلیل عملکرد، امکان شناسایی نقاط ضعف و قوت را فراهم می‌آورد. یکی از موارد حائز اهمیت در نظام رزمایش سایبری پیشنهادی، بررسی بازخورد و نتایج رزمایش است. این ارزیابی‌ها امکان شناسایی نقاط ضعف و قوت سیستم‌ها، تجهیزات و تاکتیک‌ها را فراهم می‌آورد. تحلیل دقیق نتایج می‌تواند به بهبود آمادگی عملیاتی، ارتقای توانمندی‌های تیم‌ها و تقویت فرایندهای دفاعی کمک کند. همچنین، این بازخوردها به طراحی رزمایش‌های آتی کمک می‌کنند تا با توجه به مشکلات و چالش‌های شناسایی‌شده، برنامه‌ها و استراتژی‌ها بهبود یابند و نیروی انسانی آموزش‌دیده‌تر و آماده‌تر شود؛ بنابراین بررسی نتایج به‌عنوان یک گام کلیدی در فرایند بهینه‌سازی امنیت سایبری و ارتقای آمادگی سازمان‌ها عمل می‌کند.

یکپارچگی و هماهنگی بین بخش‌ها و نهادهای مختلف نیز از موارد ضروری به‌منظور کارآمدی و موفقیت در رزمایش سایبری است. در دنیای سایبری، تهدیدها پیچیده و متنوع هستند و مقابله با آن‌ها نیازمند همکاری میان نهادها و سازمان‌های مختلف مانند سازمان‌های دولتی، شرکت‌های خصوصی، نیروهای امنیتی، تیم‌های فنی و حتی نهادهای آموزشی و تحقیقاتی است. اگر این نهادها و سازمان‌ها نتوانند به‌طور مؤثر با یکدیگر هماهنگ شوند، ممکن است هرکدام به‌صورت جداگانه عمل کنند و این عدم هماهنگی می‌تواند باعث

ضعف در پاسخگویی به تهدیدها، هدررفت منابع و زمان و حتی بروز اشتباهات جدی شود. هماهنگی بین نهادها باعث می‌شود که اطلاعات به‌موقع و دقیق بین واحدهای مختلف به اشتراک گذاشته شود، واکنش‌ها سریع‌تر و هدفمندتر انجام شود و در نهایت فرایند شبیه‌سازی تهدیدها با دقت بیشتری انجام شود. علاوه بر این، این هماهنگی موجب افزایش هم‌افزایی، بهره‌وری بالاتر و امکان یادگیری از تجربیات مشترک خواهد شد. الگوی رزمایش سایبری ارائه‌شده در این مقاله مورد تأیید صاحب‌نظران و متخصصان در زمینهٔ امنیت سایبری قرار گرفته است.

نتایج تجزیه و تحلیل پرسش‌نامه‌ها نشان می‌دهد که تمامی اجزای تعریف شده شامل ابعاد، مؤلفه‌ها، زیر مؤلفه‌ها و روابط بین آن‌ها مورد تأیید پاسخ‌دهندگان قرار گرفته است که بیانگر تعریف درست الگوی نظام رزمایش سایبری است. این الگو با توجه به تجزیه و تحلیل‌های دقیق و به‌کارگیری بهترین شیوه‌ها و استانداردهای بین‌المللی و در نظر گرفتن ادبیات داخلی، قابلیت اجرای مؤثر در مقیاس‌های مختلف را دارد و می‌تواند به افزایش آمادگی و پاسخگویی در برابر تهدیدهای سایبری کمک کند.

پیشنهادها

- ایجاد زیرساخت‌های لازم برای پیاده‌سازی نظام رزمایش سایبری؛
- ایجاد بستری برای امکان مشارکت سایبری زیرساخت‌های حیاتی به‌منظور رزمایش؛
- تعیین خط مشی، اهداف و چشم‌اندازهای رزمایش سایبری ج.ا.ا؛
- بررسی الزامات فنی و تجهیزات مورد نیاز به‌منظور پیاده‌سازی الگو رزمایش سایبری؛
- تعیین قوانین و مقررات اطلاعاتی و سایبری برای سازمان‌ها به‌منظور شرکت در نظام رزمایش سایبری.

قدردانی

از همه استادان و پژوهشگرانی که با ارائه نظرات ارزشمند خود، در ارتقای کیفیت این مقاله ما را یاری کرده‌اند؛ تقدیر و تشکر می‌کنیم.

منابع

– رزاق‌زاده، امیر (۱۳۸۹). آموزش نظامی در جنگ عراق علیه ایران، مجله نگین ایران، ۹ (۳۴): ۲۰-۹۵.

- عباسی رائی، علی؛ فرورش، حمید و نخعی کمال‌آبادی، عیسی (۱۳۹۷). مکان‌یابی، استقرار و ضد استقرار یگان‌ها در رزمایش‌های نظامی با استفاده از رویکرد برنامه‌ریزی دوسطحی، فصلنامه مدیریت نظامی. ۱۸(۷۱): ۱۵۹-۱۸۱.
- موحدی‌راد، محمدرضا؛ مدیری، ناصر (۱۳۹۳). رزمایش سایبری رویکردی نوین جهت آمادگی در برابر تهدیدات سایبری، نهمین سمپوزیوم بین‌المللی پیشرفت‌های علوم و تکنولوژی، مشهد.
- C.I.S.A. (2022). Cyber Storm: Securing Cyberspace.
- ENISA. (2018). Exercises Supported by ENISA.
- ENISA. (2022). Cyber Exercises.
- Kick, J. (2014). Cyber Exercise Playbook.
- NATO CCD COE. (2016). Cyber Defence Exercise Locked Shields 2016. After Action Report.
- National Cyber Security Centre Finland. (2021). Instructions for organising cyber exercises. A manual for cyber exercise organisers.
- Rauscher, K.F. & Yaschenko, V. (2011). Critical Terminology Foundations. New York: East West Institute.
- Seker, E. & Ozbenli, H.H. (2018). The Concept of Cyber Defence Exercises (CDX): Planning, Execution, Evaluation. 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), 1-9.
- Vykopal, J. Vizváry, M. Ošlejšek, R. Čeleda, P. & Tovarňák, D. (2017). Lessons learned from complex hands-on defence exercises in a cyber range. 2017 IEEE Frontiers in Education Conference (FIE), 1-8.
- Yamin, M.M. Katt, B. & Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Comput. Secur. 88.