فصلنامه مدیریت و پژوهش‌های دفاعی

بررسی عوامل زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری

فرهاد قاطعی درگاهی[۱] | حسین فلکی نیا[۲] | مهدی نطاق‌پور[۳]

۱۰۱

سال بیست و دوم
پاییز ۱۴۰۲

مقاله پژوهشی

تاریخ دریافت:
۱۴۰۲/۰۸/۰۹
تاریخ پذیرش:
۱۴۰۲/۱۱/۱
صص: ۱۵۹-۱۲۵

شاپا چاپی: ۶۱۲۱-۲۰۰۸
الکترونیکی: ۵۲۱۸-۲۶۴۵

چکیده

در سال‌های اخیر حملات و تهاجمات مختلفی علیه زیرساخت‌ها و مراکز حیاتی که به نحوی به فضای سایبری وابسته بوده‌اند، صورت گرفته است؛ علی‌رغم برگزاری رزمایش‌های سایبری به‌صورت دوره‌ای در زیرساخت‌های مذکور، متأسفانه همچنان شاهد آسیب‌پذیری‌ها و تهدیدات گوناگون هستیم و تحقیقی که به بررسی عوامل مؤثر بر ارتقاء رزمایش سایبری پرداخته باشد به دست نیامده است. به همین جهت بررسی عوامل زمینه‌ای به‌عنوان یکی از مهم‌ترین مجموعه عوامل مؤثر بر ارتقاء رزمایش سایبری مسئله اصلی این تحقیق قرار گرفت و "اثرگذاری عوامل زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری چه میزان است؟" به‌عنوان سؤال اصلی این تحقیق است. این مقاله با استفاده از جمع‌آوری داده به روش کتابخانه‌ای و میدانی با نگاه به تجربیات منتشرشده وزارت امنیت داخلی ایالاتمتحده و آژانس امنیت سایبری اتحادیه اروپا صورت پذیرفت که منتج به شناسایی ۲۴ عامل مؤثر گردید؛ در ادامه با تهیه پرسشنامه شرط روایی و پایایی آن با حذف ۲ گزاره و مقدار آلفای کرونباخ ۰/۶۱ بااحتیاط پذیرفته شد. پرسشنامه با جامعه نمونه آماری ۲۹ نفر توزیع شد که بر اساس نتایج و یافته‌ها، در پاسخ به سؤال اصلی تحقیق بر اساس آزمون فریدمن، عامل " فرماندهی و مدیریت اثربخش با ایجاد فضای حمایتی و اعتماد متقابل" با میانگین ۱۳/۵۰ در رتبه اول، عامل "ارتباط با شرکت‌های فناور و تولیدکننده تجهیزات توسط مهاجم" با میانگین ۱۳/۲۶ در رتبه دوم و عامل " شناخت درهم تنیدگی و تأثیرگذاری متقابل تهدیدات سایبری و امنیتی" با میانگین ۱۳/۹ در رتبه سوم عوامل زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری قرار گرفت.

کلیدواژه‌ها: عوامل زمینه‌ای؛ رزمایش سایبری؛ زیرساخت.

DOR: 20.1001.1.20086121.1402.22.101.5.9

۱. نویسنده مسئول: کارشناس ارشد مطالعات دفاعی استراتژیک دانشگاه جامع امام حسین(ع) و پژوهشگر دانشکده فرماندهی و مدیریت ولایت سپاه (دافوس)، تهران، ایران. alialavi200020@gmail.com

۲. مربی دانشکده فرماندهی و مدیریت ولایت سپاه (دافوس)، دانشگاه جامع امام حسین(ع)، تهران، ایران.

۳. عضو هیئت علمی دانشکده فرماندهی و مدیریت ولایت سپاه (دافوس)، دانشگاه جامع امام حسین(ع)، تهران، ایران.

مقدمه

اهمیت فناوری اطلاعات در عصر حاضر و توسعه سریع آن بر کسی پوشیده نیست. باوجود اهمیت فوق‌العاده و رسوخ آن در لایه‌های مختلف زندگی بشری، اما رشد نامتوازن ساختارها و افزایش آسیب‌پذیری‌ها، ازجمله مواردی است که می‌تواند خطرآفرین باشد و بستر فناوری اطلاعات را با مشکلاتی مواجه سازد. شناخت تهدیدات و عناصر و مؤلفه‌های آسیب‌زا و زمینه‌های شکل‌گیری آن‌ها از موضوعات ضروری در این راستاست. رزمایش‌های سایبری و تمرینات میدانی با همین هدف، و به‌منظور کاهش این آسیب‌پذیری‌ها طراحی و اجرا می‌شوند، و نمونه‌هایی از آن نیز در ایران به اجرا درآمده است.

یکی از اقدامات مهم در این زمینه، اجرای رزمایش سایبری باهدف شناسایی به‌موقع تهدیدات و آسیب‌پذیری‌ها؛ و تصمیم‌سازی در جهت پیش‌گیری، رفع یا کاهش نقاط ضعف زیرساخت‌های حیاتی کشور است. علی‌رغم برگزاری رزمایش‌های سایبری گوناگون در سطح زیرساخت‌های حیاتی کشور، متأسفانه همچنان شاهد آسیب‌پذیری‌های متعددی هستیم که منجر به تحمیل هزینه‌های زیادی برای کشور می‌گردد. شناسایی عوامل تأثیرگذار و بررسی میزان تأثیر هرکدام از آن‌ها ارتقاء رزمایش پدافند سایبری در زیرساخت‌های حیاتی کشور که در اجرای موفق و باکیفیت رزمایش نقش بسزایی دارند، حائز اهمیت است.

با توجه به تعدد عوامل مؤثر و دسته‌بندی یافته‌ها از یک‌سو؛ عدم وجود پژوهشی جامع در این حوزه و ایجاد زمینه برای انجام پژوهش‌های بیشتر از سوی دیگر، این نوشتار در پی استخراج عوامل زمینه‌ای مؤثر و میزان اثرگذاری آن‌ها بر ارتقاء رزمایش سایبری است.

در این مقاله قصد داریم با طرح سؤال "اثرگذاری عوامل زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری چه میزان است؟"، عوامل زمینه‌ای مؤثر بر ارتقاء رزمایش را شناسایی و میزان تأثیرگذاری هر عامل را با استفاده از روش‌های آماری تعیین نماییم.

پیشینه تحقیق

سوباسو و دیگران (۲۰۱۷) در پژوهش خود وجود سناریوها، مجموعه‌ای از ابزارها، چند سطحی بودن رزمایش با توجه به سطوح آموزش و نیازهای سازمان، نقش‌ها و آئین‌نامه حاوی

قوانین و تعیین سطوح دسترسی خاص را به‌عنوان الزامات اجرای رزمایش سایبری معرفی کرده است که کلی بودن دسته‌بندی‌ها و عدم تعیین شاخص از یک‌سو؛ و عدم تفکیک انواع رزمایش سایبری با تمرکز بر یک نوع خاص، در آن اقدام به تعیین نقش هر عامل در ارتقاء رزمایش سایبری نگردیده است. سکر و دیگران (۲۰۱۸) در پژوهش خود به چرخه اجرای رزمایش سایبری و اقداماتی که در هر مرحله صورت می‌پذیرد اشاره‌کرده است؛ بر اساس چرخه ارائه‌شده در پژوهش ایشان، چرخه اجرای رزمایش سایبری شامل چهار مرحله شناسایی، برنامه‌ریزی، هدایت و ارزیابی می‌گردد. در این پژوهش اقدام به شاخص سازی و تعیین نقش هر عامل در اجرای یک رزمایش سایبری نشده است. جی شپنز و دیگران (۲۰۰۱) در پژوهش خود به الزامات آموزشی و فرایند اجرای رزمایش سایبری در حوزه نظامی باهدف تربیت افسران امنیت اطلاعات در ارتش ایالات‌متحده آمریکا پرداخته است و در خصوص رزمایش سایبری در زیرساخت‌های کشوری و عوامل مؤثر در اجرای آن را موردبررسی قرار نداده است. موحدی راد و دیگران (۱۳۹۳) در پژوهش خود به تعاریف و مقایسه انواع رزمایش سایبری بر اساس منابع مختلف در این بخش پرداخته است و در انتهای پژوهش خود با بررسی چرخه اجرای رزمایش سایبری، صرفاً الزامات کلی اجرای رزمایش را هدف پژوهش خود قرار داده است.

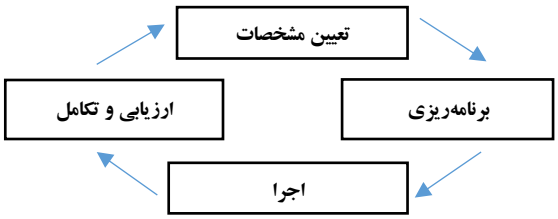
مبانی نظری

رزمایش سایبری: تمرین میدانی (با به‌کارگیری تجهیزات) یا ستادی (دور میزی) است که بر اساس سناریوهای احتمالی شبیه‌سازی و با روش‌های گوناگون اجرا می‌گردد و باعث کشف آسیب‌پذیری و ارتقاء آمادگی‌های دستگاهی و انفرادی و ارزیابی کار آیی اقدامات برای مقابله با تهدیدات می‌شود. (وزارت امنیت داخلی ایالات‌متحده، ۱:۲۰۰۶)

رزمایش سایبری تمرینی است که اهداف آن عمدتاً بر حفاظت، دفاع و بازیابی دارایی‌ها و عملیات سایبری حیاتی برای ارائه سرویس در زمان وقوع حملات یا حوادث سایبری تمرکز دارند. این اهداف شامل آموزش یا ارزیابی پرسنل برای روش‌های پیش‌گیری، حفاظت، واکنش، بازیابی و همچنین شامل فرایندهای ارتباط، هدایت و کنترل با ذینفعان و سازمان‌های شریک نیز می‌شود. (موحدی راد و دیگران، ۳:۱۳۹۳)

اهداف رزمایش سایبری: ارزیابی آمادگی دستگاه‌های اجرایی در برابر حوادث، تهدیدات و اقدامات خصمانه سایبری دشمن در راستای ارتقاء پایداری، تاب‌آوری و تداوم کارکردهای ضروری کشور و صیانت از مردم با تأکید بر اجرای رزمایش‌های سایبری. (مصوبه کمیته پدافند غیرعامل کشور در خصوص نظام آمادگی و رزمایش دستگاه‌های اجرایی در برابر تهدیدات، ۳:۱۳۹۹)

چرخه حیات رزمایش سایبری: برنامه‌ریزی و اجرای کارآمد یک رزمایش اهدافی چالش‌برانگیز هستند. برای دستیابی به موفقیت باید با دقت و تلاش در طول مراحل مختلفی پیشروی کرد، مقدار بسیار زیادی از جزئیات را بررسی کرد و عین حال حساسیت‌های سازمان‌ها و افراد مختلف دخیل در رزمایش را در نظر گرفت. این مراحل مختلف که همگی چرخه حیات یک رزمایش را تشکیل می‌دهد در شکل زیر نشان داده‌شده است. (موحدی راد و دیگران، ۹:۱۳۹۳)



شکل ۱. چرخه حیات رزمایش سایبری

تعیین مشخصات رزمایش: در این بخش سازمان دهنده[1] باید نیاز به رزمایش را تشخیص دهد. این نیاز شامل تعیین روال‌ها یا اقداماتی است که نیازمند تمرین یا بهبود است و باید برای آن‌ها رزمایش برگزار شود. بر اساس این نیاز برنامه‌ریز می‌تواند نوع رزمایش و سازمان‌های شرکت‌کننده را انتخاب کند.

برنامه‌ریزی رزمایش: در این بخش سازمان دهنده فرایند برنامه‌ریزی را آغاز می‌کند. این فرایند شامل عضوگیری شرکت‌کنندگان، تأمین منابع مالی رزمایش، انتخاب مکان، تهیه سناریو، قوانین، ابزار و وسایل آموزشی رزمایش، انتخاب ناظران و سایر نقش‌ها و تعیین چگونگی انجام وظایف آن‌ها می‌شود.

1. Organizer

اجرای رزمایش: در این بخش خود رزمایش اجرا می‌شود. طبق آنچه در فرایند برنامه‌ریزی مشخص‌شده است شرکت‌کنندگان طبق سناریو پیش می‌روند و اقدامات واکنشی خود را با تبادل‌نظر یا اجرای واقعی انجام می‌دهند. ناظران این اقدامات را مشاهده و یادداشت‌برداری می‌کنند.

ارزیابی و تکامل رزمایش: درنهایت پس از اجرای رزمایش فرایند ارزیابی انجام می‌شود. این فرایند معمولاً شامل یک گزارش ارزیابی نهایی، یا چندین گزارش تهیه‌شده برای مخاطبان مختلف است. در این گزارش‌ها رزمایش بازبینی می‌شود، نقاط ضعف مشخص می‌گردند و توصیه‌هایی برای ارتقاء و تکامل رزمایش ارائه می‌شوند. همچنین این فرایند می‌تواند شامل جلسات تبادل‌نظر دنباله‌داری باشد که در آن‌ها بررسی نقطه‌ضعف‌ها و توصیه‌های ارائه‌شده ادامه پیدا کند.
(همان، ۹)

مدل تحلیلی سه‌شاخگی[1]**:** در مدل سه‌شاخگی پدیده سازمان و مدیریت برحسب سه دسته عوامل زمینه‌ای، رفتاری و ساختاری بررسی و تجزیه‌وتحلیل می‌شود. علت نام‌گذاری این مدل به سه‌شاخگی آن است که ارتباط بین عوامل زمینه‌ای، رفتاری و ساختاری به‌گونه‌ای می‌باشد که هیچ پدیده یا رویداد سازمانی نمی‌تواند خارج از تعامل این سه‌شاخه صورت گیرد. به‌عبارت‌دیگر، رابطه بین این سه‌شاخه یک رابطه تنگاتنگ بوده و در عمل از هم جدایی‌ناپذیرند. درواقع، نوع روابط موجود بین این سه‌شاخه از نوع لازم و ملزوم بوده و به‌مثابه سه‌شاخه روییده از تنه واحد حیات سازمان می‌باشند. (مدل تحلیلی سه‌شاخگی، میرزایی، ۱۳۷۷)

الگوی سه‌شاخگی در طبقه‌بندی الگوها، از نوع الگوهای منطقی به شمار می‌آید و می‌توان بسیاری از مفاهیم، رویدادها و پدیده‌های فراگیر را در قالب این الگو موردبررسی و تجزیه‌وتحلیل قرار داد. الگوی سه‌شاخگی دارای سه بعد ساختاری، زمینه‌ای و رفتاری است (میرزایی اهرنجانی، ۱۳۷۶).

عوامل زمینه‌ای: عوامل زمینه‌ای یا محیطی شامل محیط و شرایط بیرونی که سبب‌ساز عوامل رفتاری و ساختاری هستند مانند سلسله‌مراتب فرماندهی، تعامل منطقی با محیط علمی بیرونی، محیط‌شناسی برای هم راستاسازی منافع نهادی با منافع سازمان‌های هم‌ردیف، بالادستی و دیگران،

1. Three Dimentional Model of Structure- Content-Context

بسترهای قانونی و حقوقی، منابع و مبادی پشتیبانی‌کننده. عوامل زمینه‌ای به‌عنوان علل و عواملی پایه‌ای هستند که بر رابطه و تعامل مناسب و واکنش به‌موقع و درست سازمان را با سیستم‌های هم‌جوار محیطی‌اش اثر می‌گذارند (مدل تحلیلی سه‌شاخگی، میرزایی، ۱۳۷۷).

این عوامل شرایط و عوامل محیطی، برون‌سازمانی هستند که محیط سازمان را احاطه نموده، با سازمان تأثیر و تأثر متقابل داشته و خارج از واپایش سازمان می‌باشند. هر نظام یا سازمانی در جایگاه خاص خود همواره با نظام‌های محیطی در کنش و واکنش دائمی است، ازاین‌رو همه علل و عواملی که امکان برقراری، تنظیم و واکنش به‌موقع و مناسب سازمان نسبت به سایر نظام‌ها را فراهم می‌آورند، زمینه یا محیط نامیده می‌شوند (میرزایی اهرنجانی و سرلک، ۱۳۸۴).

بررسی تاریخی رزمایش سایبری: در سال‌های اخیر با توجه به توسعه روزافزون تهدیدات سایبری، رزمایش‌های سایبری به‌عنوان ابزار بسیار مهمی جهت افزایش آگاهی ایمنی از فضای مجازی، آزمایش توانایی سازمان برای مقاومت و پاسخ دادن به رویدادهای مختلف سایبری برای ایجاد یک محیط امن، جمع‌آوری داده‌های تجربی مرتبط با امنیت و بررسی آن، آموزش عملی کارشناسان در این زمینه معرفی گردید. رزمایش سایبری می‌تواند در مورد اقدامات احتیاطی به تصمیم‌گیرندگان حوزه امنیت سایبری و به مسئولان، نهادها، سازمان‌ها و کارکنانی که در زمینه ابزارهای سایبری، تکنیک‌ها و رویه‌هایی که می‌توان برای این حوزه توسعه داد؛ ایده دهد. (آژانس امنیت سایبری اتحادیه اروپا، ۲۰۲۲)

به‌منظور شناسایی عوامل زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری با هدف پیشگیری و کاهش تهدیدات در حوزه فناوری اطلاعات، مجموعه‌های دولتی و خصوصی متعددی در دنیا در زمینه طرح‌ریزی و اجرای رزمایش‌های سایبری، فعالیت نموده‌اند که در ادامه به برخی از مهم‌ترین رزمایش‌ها و خلاصه‌ای از فعالیت مجموعه‌ها در زمینه رزمایش سایبری که موردبررسی قرارگرفته است؛ اشاره می‌گردد.

رزمایش وزارت امنیت داخلی ایالات‌متحده[1]: مهم‌ترین رزمایش سایبری در ایالات‌متحده رزمایش طوفان سایبری[2] است؛ این رزمایش یک رزمایش شبیه‌سازی‌شده دوسالانه است که توسط وزارت امنیت داخلی ایالات‌متحده نظارت می‌شود که اولین بار از ۶ فوریه تا ۱۰ فوریه

1. U.S. Department of Homeland Security (DHS)
2. Cyber Storm

۲۰۰۶ باهدف آزمایش قدرت دفاعی کشور در برابر جاسوسی دیجیتال انجام شد. این شبیه‌سازی عمدتاً سازمان‌های امنیتی آمریکایی را هدف قرار داد، اما مقامات بریتانیا، کانادا، استرالیا و نیوزلند نیز در آن شرکت کردند. (رزمایش طوفان سایبری، ویکی‌پدیا، ۲۰۲۳)

دستاوردهای کلیدی رزمایش طوفان سایبری ۱[1]:

- به‌عنوان بزرگ‌ترین، پیچیده‌ترین رزمایش سایبری چندملیتی، فرا بخشی که تا به آن روز اجراشده بود.
- به‌طور هم‌زمان سازمان‌دهی سازمان‌های واکنش سایبری بیش از ۱۰۰ سازمان، انجمن و شرکت دولتی و خصوصی در بیش از ۶۰ مکان و پنج کشور.
- دستیابی به همکاری چندملیتی در واکنش به بحران در سطوح عملیاتی، سیاستی و امور عمومی.
- مشارکت مستقیم و گسترده بیش از ۳۰ شرکت و انجمن بخش خصوصی در برنامه‌ریزی، اجرا و تجزیه‌وتحلیل پس از اقدام یک رزمایش واکنش اضطراری و بازیابی با بودجه فدرال و کنگره.
- دستیابی به همکاری بی‌سابقه و به اشتراک‌گذاری اطلاعات در میان آژانس‌های فدرال، فراتر از مرزهای بین بخش خصوصی و دولت و بین شرکای بین‌المللی.
- برای اولین بار، طیف کاملی از سیاست‌ها، دکترین و روش‌های ارتباطی واکنش مرتبط با سایبری را که در یک بحران دنیای واقعی موردنیاز است، آزمایش گردید.
- بررسی خط‌مشی‌ها و رویه‌های آزمایش‌شده مرتبط با یک رویداد سایبری با اهمیت ملی.
- از طریق برنامه‌ریزی و اجرای آن، روابط عمومی و خصوصی متعددی ایجاد گردید که در آماده‌سازی آینده و پاسخ به حوادث سایبری بین بخشی ارزشمند خواهد بود.
- شناسایی مسائل بازیابی که مستلزم بررسی بیشتر از طریق همکاری بین بخش دولتی و خصوصی است.

(وزارت امنیت داخلی ایالات‌متحده، گزارش رزمایش طوفان سایبری ۱، ۲۰۰۶)

دستاوردهای کلیدی رزمایش طوفان سایبری ۸[2]:

1. Cyber Storm I
2 Cyber Storm I

- رزمایش طوفان سایبری هشتم بر اساس تکرارهای قبلی ساخته شد تا از طریق فرآیند برنامه‌ریزی رزمایش و اجرا مکانی برای یادگیری و پیشرفت فراهم کند.
- تقویت آمادگی امنیت سایبری و قابلیت‌های پاسخگویی با اعمال سیاست‌ها، فرآیندها و رویه‌ها برای شناسایی و واکنش به یک حادثه سایبری مهم چندبخشی که بر زیرساخت‌های حیاتی تأثیر می‌گذارد.
- ادغام سهامداران جدید در رزمایش ملی طوفان سایبری، ازجمله یک بخش جدید مانند سیستم‌های آب و فاضلاب، قرار گرفتن در معرض رزمایش‌های سایبری در مقیاس بزرگ، حمایت از ایجاد رابطه و ایجاد پایه‌ای برای رزمایش‌ها و تلاش‌های بهبود آینده.
- ارائه یک بردار حمله چندوجهی بر اساس شرایط سناریوی اصلی مشترک که مکانیسمی را برای افزایش مشارکت در درون و بین سازمان‌های شرکت‌کننده فراهم می‌کند و درعین‌حال امکان مشارکت رکورد تعداد سازمان‌های قدیمی را نیز فراهم می‌کند.
- افزایش آگاهی در مورد سطح حمله سایبری که به‌سرعت در حال گسترش است و تفاوت‌های ظریف واکنش به حوادثی که بر شبکه‌های سیستم کنترل صنعتی[1]/فناوری عملیاتی[2] و فناوری اطلاعات سازمانی تأثیر می‌گذارد.
- ذینفعان دولتی را وادار کرد تا گروه هماهنگی یکپارچه[3] سایبری را بر اساس رویه‌های مندرج در فرایندهای طرح ملی واکنش به حوادث سایبری[4] تشکیل دهند.
- شرکت‌کنندگان به اشتراک‌گذاری اطلاعات و ارتباطات به‌عنوان کشورهای شریک شبکه بین‌المللی دیده‌بان و هشدار[5] در جهت بهبود ارتباطات واکنش به حادثه (ازنظر فراوانی، مکانیسم و نوع اطلاعات به اشتراک گذاشته‌شده) تأکید کردند.
- ایجاد یک سناریوی چندلایه که به شرکت‌کنندگان این فرصت را می‌دهد تا بر

1. Industrial Control Systems (ICS)
2. Operational Technology (OT)
3. Unified Coordination Group (UCG)
4. The National Cyber Incident Response Plan (NCIRP)
5. International Watch and Warning Network (IWWN)

واکنش کل سازمان به یک حادثه تأکید کنند که شامل کارشناسان فنی سازمان‌ها، نمایندگان امور عمومی، نمایندگان امور حقوقی و رهبری سازمانی می‌شود.

- یک پلت فرم رسانه‌های اجتماعی و سنتی شبیه‌سازی‌شده و به‌روز شده پویا را برای تکرار مشتری و اجزای عمومی یک حادثه ادغام کرد و یک محیط یادگیری بدون خطا را برای تمرین استراتژی‌هایی که از این جنبه از پاسخ پشتیبانی می‌کند، فراهم کرد.
- به دولت‌های شرکت‌کننده اجازه داده شد تا نقش‌ها و مسئولیت‌های مرتبط آژانس‌های پشتیبانی را در چارچوب‌های واکنش به حوادث سایبری خود بررسی کنند.
- برای اولین بار در یک رزمایش، طوفان سایبری به توسعه و انتشار یک مشاور امنیت سایبری[1] مشترک در حین رزمایش دست‌یافت. این CSA مشترک توسط آژانس امنیت سایبری و امنیت زیرساخت[2]، دفتر تحقیقات فدرال[3] و آژانس امنیت ملی[4] و همچنین سازمان امنیت ارتباطات کانادا[5]، مرکز امنیت سایبری استرالیا[6]، مرکز ملی سایبری بریتانیا[7] و مرکز امنیت سایبری ملی نیوزلند[8] ایجادشده است.

(آژانس امنیت سایبری و امنیت زیرساخت، گزارش پس از اقدام طوفان سایبری ۲۰۲۲، ۲۰۲۲)

رزمایش آژانس امنیت سایبری اتحادیه اروپا[9]: رزمایش‌های سایبری اروپا، شبیه‌سازی حوادث امنیت سایبری در مقیاس بزرگ است که به بحران‌های سایبری تبدیل می‌شوند. این رزمایش‌ها فرصت‌هایی را برای تجزیه‌وتحلیل حوادث فنی پیشرفته امنیت سایبری و همچنین برای مقابله با تداوم کسب‌وکار پیچیده و موقعیت‌های مدیریت بحران ارائه می‌دهد.

1. Cybersecurity Advisory (CSA)
2. Cybersecurity and Infrastructure Security Agency (CISA)
3. Federal Bureau of Investigation (FBI)
4. National Security Agency (NSA)
5. Canada’s Communication Security Establishment (CSEC)
6. Australia's Cyber Security Centre (ACSC)
7. United Kingdom's National Cyber Security Center (NCSC-UK)
8. New Zealand's National Cyber Security Centre (NCSC-NZ)
9. The European Union Agency for Cybersecurity (ENISA)

رزمایش سایبری اروپا که به‌صورت دو سال یک‌بار برگزار می‌شود، دارای سناریوهای جذاب است که از رویدادهای واقعی زندگی الهام گرفته‌شده است و توسط کارشناسان امنیت سایبری اروپایی توسعه‌یافته است؛ بنابراین هر یک از بخش‌های این رزمایش به‌طور مؤثر یک تجربه یادگیری انعطاف‌پذیر برای شرکت‌کنندگان است. درواقع یکی از اولویت‌های اتحادیه اروپا که در "دستور کار دیجیتالی برای اروپا" تعیین‌شده است، پشتیبانی و سازمان‌دهی رزمایش‌های آمادگی امنیت سایبری در سطح اتحادیه اروپا است. این امر به‌عنوان یکی از راه‌های تضمین امنیت آنلاین کسب‌وکارها و شهروندان شناخته می‌شود. (آژانس امنیت سایبری اتحادیه اروپا، ۲۰۲۲)

دستاوردهای کلیدی رزمایش اروپای سایبری ۲۰۱۰[1]: یافته‌های موقت و توصیه‌های کشورهای عضو اتحادیه اروپا در اولین رزمایش سایبری تمام اروپایی نشان می‌دهد که این رزمایش یک "آزمون استرس سایبری[2]" مفید برای نهادهای عمومی در اروپا بود. کشورهای عضو تمایل به ادامه تلاش‌های خود در زمینه رزمایش‌های ملی و تمام اروپایی ابراز و در مورد اهمیت مشارکت بخش خصوصی در رزمایش‌های آینده و تبادل درس‌های آموخته‌شده با آن‌ها در سایر رزمایش‌های ملی یا بین‌المللی توافق داشتند. (آژانس امنیت سایبری اتحادیه اروپا، ارزیابی رزمایش سایبری، ۲۰۱۰)

دستاوردهای کلیدی رزمایش اروپای سایبری ۲۰۲۲[3]:

- اگرچه هر نهاد شرکت‌کننده قادر به مشارکت در همه زمینه‌ها نبود، سناریوی رزمایش این فرصت را به همه کشورهای شرکت‌کننده و مؤسسات برای رسیدن به اهداف داد.
- یافته‌های تفصیلی در سطح اهداف که با برنامه‌ریزان به اشتراک گذاشته‌شده است، باید منجر به بهبود رویه‌ها، فرآیندهای ارتباطی و هماهنگی شود که در سطح محلی، بخشی، ملی و همچنین سطوح مرزی و سرتاسری اتحادیه اروپا وجود دارد.
- رزمایش‌هایی مانند Cyber Europe به‌عنوان یک زمین رزمایش و آزمایش موردنیاز است، زیرا شکاف‌ها و نقاط توسعه را با موفقیت شناسایی می‌کند.
- رزمایش Cyber Europe 2022 به‌طور قابل‌توجهی توانست چندین ذینفع از بخش

1. Cyber Europe 2010
2. Cyber Stress Test
3. Cyber Europe 2010

خصوصی و دولتی را در همکاری و کار با یکدیگر در جهت دستیابی به یک رویکرد مشترک باهدف بهبود هماهنگی اتحادیه اروپا در طول بحران‌های سایبری بزرگ، مشارکت دهد.

- سکوی رزمایش سایبری[1] که برای برنامه‌ریزی و اجرای رزمایش استفاده می‌شود، می‌تواند از به‌روزرسانی بهره‌مند شود تا بتواند انتظارات و انتظارات آینده را باهدف بهبود تجربه کاربری برای همه افراد درگیر برآورده کند.
- این رزمایش اهمیت آمادگی بهینه برای چنین رزمایش بزرگی را تائید کرد و تلاش بیشتری برای آماده‌سازی نتایج به‌منظور تولید خروجی مفیدتر را انجام داد.
- برنامه‌ریزان موافقت کردند که دریافت پشتیبانی و آموزش بهتر برای نقش حیاتی خود به‌عنوان برنامه‌ریز به آن‌ها کمک می‌کند تا از رزمایش‌های آینده سایبری اروپا بهره بیشتری ببرند.
- این رزمایش اهمیت تخصیص بودجه و منابع کافی به تیم‌های امنیت سایبری در بخش مراقبت‌های بهداشتی را با توجه به‌شدت چالش‌های مرتبط با حملات سایبری تائید کرد.

(آژانس امنیت سایبری اتحادیه اروپا، گزارش پس از اقدام رزمایش سایبری، ۲۰۲۲)

روش‌شناسی تحقیق

ازجمله ویژگی‌های مطالعه علمی که هدف آن حقیقت‌یابی است، استفاده از یک روش تحقیق مناسب می‌باشد و انتخاب روش تحقیق مناسب به هدف‌ها، ماهیت و موضوع موردتحقیق و امکانات اجرایی بستگی دارد و هدف از تحقیق دسترسی آسان و دقیق جهت پاسخ به پرسش‌های تحقیق است (خاکی، ۱۳۹۰: ۱۴۲- ۱۴۳). بدون روش‌شناسی علمی، نتایج بررسی و تحلیل‌های مربوطه معتبر و قابل‌تعمیم نخواهد بود. ازاین‌رو در این بخش باهدف آشنایی خواننده از نحوه عمل تحقیق و با توجه به اهداف تحقیق به توضیح روش تحقیق، روش‌های جمع‌آوری اطلاعات، بررسی اعتبار و روایی پرسشنامه و چگونگی تحلیل آماری پرداخته‌شده است.

1. ENISA's Cyberskills Exercise Platform

نوع و روش تحقیق: تحقیق حاضر ازلحاظ نوع تحقیق به جهت قابلیت استفاده در مجموعه‌های متولی اجرای رزمایش سایبری در کشور، کاربردی است و به روش توصیفی – تحلیلی انجام‌شده است.

قلمرو زمانی: بازه زمانی منتهی به سال ۱۴۰۲ هجری شمسی با توجه به برخی تجربیات منتشرشده دنیا در اجرای رزمایش سایبری به‌عنوان قلمرو زمانی در این تحقیق تعیین می‌گردد.

قلمرو مکانی: در این تحقیق، بخشی از موجودیت‌های سایبری زیرساخت‌های حیاتی جمهوری اسلامی ایران با تمرکز بر جامعه آماری نخبگانی قابل‌دسترس از زیرساخت‌ها که در جهت جمع‌آوری اطلاعات و پر کردن پرسشنامه در این تحقیق همکاری نموده‌اند به‌عنوان قلمرو مکانی تحقیق تعیین می‌گردد.

قلمرو موضوعی: در این تحقیق، عوامل زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری به‌عنوان قلمرو موضوعی تعیین می‌گردد.

جامعه آماری، حجم نمونه آماری و روش نمونه‌گیری: جامعه آماری در این تحقیق ۳۵ نفر می‌باشد که از بین این تعداد پرسشنامه توزیع‌شده تعداد ۲۹ نفر در جهت تکمیل و تحویل آن همکاری نمودند؛ ویژگی مشترک جامعه آماری در این تحقیق بخشی از خبرگان متخصص در حوزه فناوری اطلاعات و امنیت سایبری است که در چهار بخش دانشگاهی، نظارتی، اجرایی و سیاست‌گذاری نقش ایفا می‌کنند.

ابزار گردآوری اطلاعات: یکی از مهم‌ترین مراحل در انجام هر تحقیقی انتخاب ابزار اندازه‌گیری مناسب است که بتواند پژوهشگر را در جمع‌آوری اطلاعات به بهترین وجه کمک کند. در بخش مبانی نظری این تحقیق از کتاب‌ها، اسناد و مدارک، مجلات و فصلنامه‌های معتبر بهره‌برداری شد و در بخش پاسخ به سؤالات تحقیق از پرسشنامه استفاده گردید.

روایی[1] و پایایی[2] تحقیق: برای اینکه پرسشنامه به‌عنوان یک ابزار گردآوری اطلاعات، بتواند به‌خوبی نظرات جامعه آماری موردمطالعه را منعکس کند باید از روایی و پایایی مناسبی

1. Validity
2. Reliability

برخوردار باشد. در این بخش با توزیع پرسشنامه زیر در بین ۱۰ نفر از خبرگان موضوع، اساتید و فرماندهان، اقدامات لازم به‌منظور بررسی روایی و پایایی لازم صورت گرفت.

جدول ۲. محاسبات اعتبارسنجی پرسشنامه

ردیف	میزان اثرگذاری هریک بر ارتقاء رزمایش سایبری چگونه است؟	ضروری است	مفید است و ضروری نیست	ضرورتی ندارد	نسبت روایی محتوایی	شاخص روایی محتوایی	ضروری است	مفید است و ضروری نیست	ضرورتی ندارد	ضروری +مفید است و ضروری نیست	ضرورتی ندارد
۱	همکاری دولت با گروه‌های هکری	۷	۳	۰	۱	۱	۷۰٪	۳۰٪	۰٪	۱۰	۰
۲	به‌کارگیری ابزارها و سامانه‌های بومی	۷	۲	۱	۰.۸	۰.۹	۷۰٪	۲۰٪	۱۰٪	۹	۱
۳	مناسب بودن فضای اداری محیط کار	۴	۰	۶	-۰.۲	۰.۴	۴۰٪	۰٪	۶۰٪	۴	۶
۴	استفاده از تجهیزات پیشرفته و خودکار	۶	۴	۰	۱	۱	۶۰٪	۴۰٪	۰٪	۱۰	۰
۵	همکاری دولت با مجموعه‌های خصوصی	۶	۴	۰	۱	۱	۶۰٪	۴۰٪	۰٪	۱۰	۰
۶	شفافیت نقش دستگاه‌های حاکمیتی در رزمایش	۷	۳	۰	۱	۱	۷۰٪	۳۰٪	۰٪	۱۰	۰

جدول ۲. محاسبات اعتبارسنجی پرسشنامه

ردیف	میزان اثرگذاری هریک بر ارتقاء رزمایش سایبری چگونه است؟	ضروری است	مفید است و ضروری نیست	ضرورتی ندارد	نسبت روایی محتوایی	شاخص روایی محتوایی	ضروری است	مفید است و ضروری نیست	ضرورتی ندارد	ضروری +مفید است و ضروری نیست	ضرورتی ندارد
۷	اشتراک‌گذاری به‌موقع اطلاعات در حوزه رزمایش	۱۰	۰	۰	۱	۱	۱۰۰٪	۰٪	۰٪	۱۰	۰
۸	تمرکز و یکپارچه‌سازی آماد و پشتیبانی رزمایش	۶	۴	۰	۱	۱	۶۰٪	۴۰٪	۰٪	۱۰	۰
۹	همسویی سیاست‌های دفاعی کشور در حوزه سایبر	۷	۲	۱	۰.۸	۰.۹	۷۰٪	۲۰٪	۱۰٪	۹	۱
۱۰	بهره‌گیری از ظرفیت‌های مردمی در عملیات رزمایش	۴	۳	۳	۰.۴	۰.۷	۴۰٪	۳۰٪	۳۰٪	۷	۳
۱۱	ارتقاء مستمر تسلیحات، تجهیزات و فناوری‌های موجود	۹	۱	۰	۱	۱	۹۰٪	۱۰٪	۰٪	۱۰	۰

جدول ۲. محاسبات اعتبارسنجی پرسشنامه

ردیف	میزان اثرگذاری هریک بر ارتقاء رزمایش سایبری چگونه است؟	ضروری است	مفید است و ضروری نیست	ضرورتی ندارد	نسبت روایی محتوایی	شاخص روایی محتوایی	ضروری است	مفید است و ضروری نیست	ضرورتی ندارد	ضروری +مفید است و ضروری نیست	ضرورتی ندارد
۱۲	بهره‌گیری از ظرفیت‌های ارتباطی با شبکه‌های اجتماعی	۶	۴	۰	۱	۱	۶۰٪	۴۰٪	۰٪	۱۰	۰
۱۳	تعامل اطلاعاتی حوزه رزمایش با سایر سازمان‌های اطلاعاتی	۷	۳	۰	۱	۱	۷۰٪	۳۰٪	۰٪	۱۰	۰
۱۴	هماهنگی بین نیروهای مسلح و سایر زیرساخت‌های کشوری	۹	۱	۰	۱	۱	۹۰٪	۱۰٪	۰٪	۱۰	۰
۱۵	ارتباط با شرکت‌های فناور و تولیدکننده تجهیزات توسط مهاجم	۵	۵	۰	۱	۱	۵۰٪	۵۰٪	۰٪	۱۰	۰

جدول ۲. محاسبات اعتبارسنجی پرسشنامه

ردیف	میزان اثرگذاری هریک بر ارتقاء رزمایش سایبری چگونه است؟	ضروری است	مفید است و ضروری نیست	ضرورتی ندارد	نسبت روایی محتوایی	شاخص روایی محتوایی	ضروری است	مفید است و ضروری نیست	ضرورتی ندارد	ضروری +مفید است و ضروری نیست	ضرورتی ندارد
۱۶	فرماندهی و مدیریت اثربخش با ایجاد فضای حمایتی و اعتماد متقابل	۷	۳	۰	۱	۱	۷۰٪	۳۰٪	۰٪	۱۰	۰
۱۷	زیرساخت ارتباطی امن و مستقل در تبادل داده‌های دارای طبقه‌بندی	۱۰	۰	۰	۱	۱	۱۰۰٪	۰٪	۰٪	۱۰	۰
۱۸	بهره‌مندی از ائتلاف‌های همکاری بین‌المللی در زمینه رزمایش سایبری	۶	۴	۰	۱	۱	۶۰٪	۴۰٪	۰٪	۱۰	۰
۱۹	آشنایی با دانش فنی تولید سامانه‌ها و سخت‌افزارهای رایانه‌ای و ارتباطی	۳	۶	۱	۰.۸	۰.۹	۳۰٪	۶۰٪	۱۰٪	۹	۱

جدول ۲. محاسبات اعتبارسنجی پرسشنامه

ردیف	میزان اثرگذاری هریک بر ارتقاء رزمایش سایبری چگونه است؟	ضروری است	مفید است و ضروری نیست	ضرورتی ندارد	نسبت روایی محتوایی	شاخص روایی محتوایی	ضروری است	مفید است و ضروری نیست	ضرورتی ندارد	ضروری +مفید است و ضروری نیست	ضرورتی ندارد
۲۰	شناخت درهم تنیدگی و تأثیرگذاری متقابل تهدیدات سایبری و امنیتی	۵	۵	۰	۱	۱	۵۰٪	۵۰٪	۰٪	۱۰	۰
۲۱	آشنایی با تجربیات و آموزش‌های دشمن در رزمایش‌ها و عملیات سایبری	۸	۲	۰	۱	۱	۸۰٪	۲۰٪	۰٪	۱۰	۰
۲۲	توجه کافی به شرکت‌کنندگان جهت فراهم آوردن تسهیلات رفاهی مناسب	۴	۵	۱	۰.۸	۰.۹	۴۰٪	۵۰٪	۱۰٪	۹	۱
۲۳	اجرای رزمایش به‌صورت حداقل دوسالانه به‌منظور آمادگی و طرح‌ریزی همه‌جانبه	۶	۴	۰	۱	۱	۶۰٪	۴۰٪	۰٪	۱۰	۰

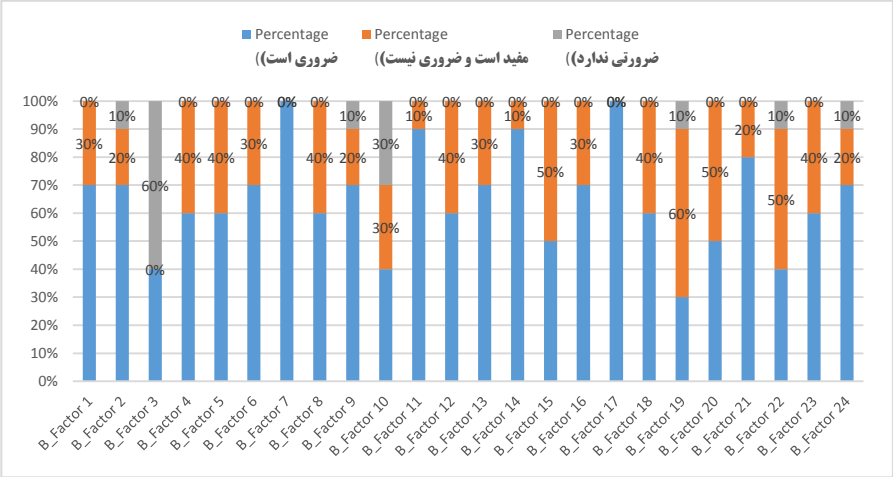
جدول ۲. محاسبات اعتبارسنجی پرسشنامه

ردیف	میزان اثرگذاری هریک بر ارتقاء رزمایش سایبری چگونه است؟	ضروری است	مفید است و ضروری نیست	ضرورتی ندارد	نسبت روایی محتوایی	شاخص روایی محتوایی	ضروری است	مفید است و ضروری نیست	ضرورتی ندارد	ضروری +مفید است و ضروری نیست	ضرورتی ندارد
۲۴	بهره‌گیری از قابلیت‌های پیچیدگی، نهان بودن، توزیع‌پذیر و خودانهدامی تسلیحات	۷	۲	۱	۰.۸	۰.۹	۷۰٪	۲۰٪	۱۰٪	۹	۱

روایی: منظور از روایی این است که مقیاس و محتوای ابزار یا سؤالات مندرج در ابزار دقیقاً متغیرها و موضوع موردمطالعه را بسنجد. (حافظ نیا، ۸۴:۱۳۸۱)؛ برای نیل به این هدف به ترتیب مراحل زیر اقدام گردید.

الف) با انجام مطالعه گسترده در رابطه با موضوع بررسی میدانی و با استفاده از تجربه و مصاحبه حضوری با خبرگان و اساتید، سؤالات تعیین شد.

ب) با نظر اساتید محترم راهنما و مشاور، سؤالات طرح‌شده موردبررسی و اصلاح قرارگرفته و پرسشنامه تنظیم گردید؛ و روایی ابزار با بهره‌گیری از روش اعتبار صوری به لحاظ اینکه پرسشنامه به تائید اساتید راهنما و مشاور، خبرگان موضوع، فرماندهان و سایر اساتید با جامعه آماری محدود رسیده است، به‌طور نسبی تأمین گردید و نتایج حاصل از نظرسنجی افراد مذکور به ازای هریک از عوامل در پرسشنامه، در جدول ۲ و نمودار زیر ارائه گردیده است.



شکل ۲. نظر جامعه آماری با بهره‌گیری از روش اعتبار صوری

بر اساس درصد بالای نظر جامعه آماری (۶۰ درصد) مبنی بر عدم ضرورت؛ عامل "مناسب بودن فضای اداری محیط کار" (فاکتور شماره ۳) از لیست عوامل زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری حذف می‌گردد.

ج) با استفاده از دو روش نسبت روایی محتوایی[1] و شاخص روایی محتوایی[2] اقدام به سنجش روایی پرسشنامه گردید. جهت محاسبه این نسبت ازنظرات کارشناسان متخصص در زمینه محتوای آزمون موردنظر استفاده و از آن‌ها خواسته شد تا هریک از سؤالات را بر اساس طیف سه‌بخشی لیکرت زیر طبقه‌بندی کنند.

- ضروری است.
- مفید است ولی ضروری نیست.
- ضرورتی ندارد.

سپس جهت محاسبه نسبت روایی محتوایی لاوشه[3] بر اساس فرمول، بر اساس تعداد متخصصینی که عوامل را مورد ارزیابی قرار داده‌اند، حداقل مقدار CVR قابل‌قبول بر اساس استاندارد برای ۱۰ خبره، مقدار ۰/۶۲ بایستی باشد. درنتیجه عوامل زیر که مقدار CVR محاسبه‌شده

1. Content Validity Ratio(CVR)
2. Content Validity Index(CVI)
3. Lawshe

برای آن‌ها کمتر از میزان موردنظر تعیین گردید با توجه به تعداد متخصصین ارزیابی‌کننده عوامل، بر اساس محاسبات روایی پرسشنامه به علت اینکه بر اساس نسبت روایی محتوایی، روایی محتوایی قابل‌قبولی ندارند، از آزمون کنار گذاشته شدند.

جدول۳. گزاره‌های هدف نسبت روایی محتوایی گزاره‌های پرسشنامه

نام گزاره اصلی	گزاره فرعی	مقدار CVR
عوامل زمینه‌ای	مناسب بودن فضای اداری محیط کار	-۰/۲
	بهره‌گیری از ظرفیت‌های مردمی در عملیات رزمایش	۰/۴

در ادامه به‌منظور محاسبه شاخص روایی محتوایی بر اساس فرمول، تعداد خبرگانی که گزینه ۱ و ۲ را انتخاب کرده‌اند بر تعداد کل خبرگان تقسیم گردید. حداقل مقدار CVI قابل‌قبول بر اساس استاندارد اگر مقدار حاصل از ۰/۷ کوچک‌تر بود گویه رد می‌شود اگر بین ۰/۷ تا ۰/۷۹ بود باید بازبینی انجام شود و اگر از ۰/۷۹ بزرگ‌تر بود قابل‌قبول است؛ بر اساس محاسبات روایی پرسشنامه، گزاره‌های هدف شناسایی و اقدامات بر اساس جدول زیر صورت پذیرفت.

جدول۴. گزاره‌های هدف شاخص روایی محتوایی گزاره‌های پرسشنامه

نام گزاره اصلی	گزاره فرعی	مقدار CVI
عوامل زمینه‌ای	مناسب بودن فضای اداری محیط کار	۰/۴
	بهره‌گیری از ظرفیت‌های مردمی در عملیات رزمایش	۰/۷

پایایی: در خصوص پایایی ابزار که از آن اعتبار، دقت و اعتمادپذیری نیز تعبیر می‌شود، عبارت است از اینکه وسیله اندازه‌گیری که برای سنجش متغیر یا صفتی ساخته‌شده است، اگر در شرایط مشابه و در زمان و مکان دیگر مورداستفاده قرار گیرد، نتایج مشابهی از آن حاصل شود؛ به‌عبارت‌دیگر ابزار پایا یا معتبر، ابزاری است که از خاصیت تکرارپذیری و سنجش نتایج یکسان برخوردار باشد. (حافظ نیا به نقل از بادپروا، ۱۳۹۲)

برای به دست آوردن پایایی سؤالات پرسشنامه در این تحقیق از روش آلفای کرونباخ استفاده‌شده است. بدین‌جهت، از همسانی درونی داده‌های حاصل از تحقیق که قابلیت اعتماد درونی پرسشنامه را در یک دامنه از صفر تا یک می‌سنجد، استفاده‌شده است؛ در این روش هرچه مقدار آلفا بیشتر باشد، پایایی پرسشنامه بیشتر خواهد بود. بر اساس این روش، مقدار آلفای بیشتر از

۰/۷ معتبر خواهد بود، آلفای ۰/۵ تا ۰/۷ بااحتیاط قابل‌قبول و آلفای کمتر از ۰/۵ قابلیت اعتماد نخواهد داشت؛ جزئیات محاسبات در این بخش در جدول ۳ قابل‌مشاهده است.

جدول۵. محاسبات پایایی پرسشنامه

ردیف	میزان اثرگذاری بر ارتقاء رزمایش سایبری	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
۱	همکاری دولت با گروه‌های هکری	۳۲/۵	۱۷/۸۳۳	۰/۰۸۲	۰/۶۱۲
۲	به‌کارگیری ابزارها و سامانه‌های بومی	۳۲/۴	۱۸/۷۱۱	-۰/۱۳۲	۰/۶۴۷
۳	مناسب بودن فضای اداری محیط کار	۳۱/۶	۱۴/۴۸۹	۰/۳۶۲	۰/۵۷۲
۴	استفاده از تجهیزات پیشرفته و خودکار	۳۲/۴	۱۶/۷۱۱	۰/۳۳۷	۰/۵۸۵
۵	همکاری دولت با مجموعه‌های خصوصی	۳۲/۴	۱۶/۷۱۱	۰/۳۳۷	۰/۵۸۵
۶	شفافیت نقش دستگاه‌های حاکمیتی در رزمایش	۳۲/۵	۱۷/۱۶۷	۰/۲۵	۰/۵۹۵
۷	اشتراک‌گذاری به‌موقع اطلاعات در حوزه رزمایش	۳۲/۸	۱۸/۴	۰	۰/۶۱۲
۸	تمرکز و یکپارچه‌سازی آماد و پشتیبانی رزمایش	۳۲/۴	۱۶/۰۴۴	۰/۵۰۵	۰/۵۶۶
۹	همسویی سیاست‌های دفاعی کشور در حوزه سایبر	۳۲/۴	۱۸/۰۴۴	-۰/۰۲۲	۰/۶۳۲
۱۰	بهره‌گیری از ظرفیت‌های مردمی در عملیات رزمایش	۳۱/۹	۱۶/۵۴۴	۰/۱۵۳	۰/۶۱۲
۱۱	ارتقاء مستمر تسلیحات، تجهیزات و فناوری‌های موجود	۳۲/۷	۱۷/۳۴۴	۰/۳۶۳	۰/۵۹۲
۱۲	بهره‌گیری از ظرفیت‌های ارتباطی با شبکه‌های اجتماعی	۳۲/۴	۱۸/۴۸۹	-۰/۰۸	۰/۶۳
۱۳	تعامل اطلاعاتی حوزه رزمایش با سایر سازمان‌های اطلاعاتی	۳۲/۵	۱۷/۸۳۳	۰/۰۸۲	۰/۶۱۲
۱۴	هماهنگی بین نیروهای مسلح و سایر زیرساخت‌های کشوری	۳۲/۷	۱۷/۵۶۷	۰/۲۷۷	۰/۵۹۸
۱۵	ارتباط با شرکت‌های فناور و تولیدکننده تجهیزات توسط مهاجم	۳۲/۳	۱۵/۳۴۴	۰/۶۷۳	۰/۵۴۵
۱۶	فرماندهی و مدیریت اثربخش با ایجاد فضای حمایتی و اعتماد متقابل	۳۲/۵	۱۶/۹۴۴	۰/۳۰۷	۰/۵۹
۱۷	زیرساخت ارتباطی امن و مستقل در تبادل داده‌های دارای طبقه‌بندی	۳۲/۸	۱۸/۴	۰	۰/۶۱۲
۱۸	بهره‌مندی از ائتلاف‌های همکاری بین‌المللی در زمینه رزمایش سایبری	۳۲/۴	۱۸/۰۴۴	۰/۰۲	۰/۶۱۹
۱۹	آشنایی با دانش فنی تولید سامانه‌ها و سخت‌افزارهای رایانه‌ای و ارتباطی	۳۲	۱۵/۳۳۳	۰/۵۳۸	۰/۵۵۳

جدول۵. محاسبات پایایی پرسشنامه

ردیف	میزان اثرگذاری بر ارتقاء رزمایش سایبری	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
۲۰	شناخت درهم تنیدگی و تأثیرگذاری متقابل تهدیدات سایبری و امنیتی	۳۲/۳	۱۵/۷۸۹	۰/۵۵۷	۰/۵۵۹
۲۱	آشنایی با تجربیات و آموزش‌های دشمن در رزمایش‌ها و عملیات سایبری	۳۲/۶	۲۰/۲۶۷	-۰/۵۳۹	۰/۶۶۱
۲۲	توجه کافی به شرکت‌کنندگان جهت فراهم آوردن تسهیلات رفاهی مناسب	۳۲/۱	۱۴/۹۸۹	۰/۵۶۶	۰/۵۴۶
۲۳	اجرای رزمایش به‌صورت حداقل دوسالانه به‌منظور آمادگی و طرح‌ریزی همه‌جانبه	۳۲/۴	۱۸/۲۶۷	-۰/۰۳	۰/۶۲۴
۲۴	بهره‌گیری از قابلیت‌های پیچیدگی، نهان بودن، توزیع‌پذیر و خودانهدامی تسلیحات	۳۲/۴	۱۷/۱۵۶	۰/۱۳	۰/۶۱۱

در ادامه همان‌گونه که در جدول زیر مشاهده می‌گردد عوامل زمینه‌ای، با احتیاط قابل‌قبول می‌باشد.

جدول۶. پایایی گزاره‌های پرسشنامه

نام گزاره اصلی	تعداد سؤال	مقدار آلفا
عوامل زمینه‌ای	۲۴	۰/۶۱۱

در پایان این بخش، پس از بررسی نتایج تحلیل روایی و پایایی پرسشنامه و انجام اصلاحات لازم؛ اقدام به حذف ۲ مورد جدول فوق گردید و درنهایت پرسشنامه با ۲۲ گزاره در بعد عوامل زمینه‌ای، مورد تائید قرار گرفت.

تجزیه‌وتحلیل یافته‌های تحقیق

داده‌ها به‌عنوان اطلاعات پردازش نشده، ابتدایی‌ترین پاسخ‌های احتمالی هر پژوهشگر در رابطه با مسئله تحقیق است. پژوهشگر پس از دستیابی به این داده‌ها، با توجه به روش تحقیق و نوع متغیرها، مناسب‌ترین آزمون آماری را برمی‌گزیند تا بتواند استنتاج‌ها و نتیجه‌گیری‌های معتبر و دقیق را به عمل آورد.

اطلاعات پرسشنامه‌های تحقیق پس از جمع‌آوری، وارد نرم‌افزار SPSS و سپس با استفاده از امکانات نرم‌افزار، نتایج موردنظر استخراج و مورد تجزیه‌وتحلیل قرار گرفت. معمولاً برای تجزیه‌وتحلیل اطلاعات در این‌گونه پژوهش‌ها از دو روش آماری توصیفی[1] و استنباطی[2] استفاده می‌گردد. آمار توصیفی، شرایط موجود را توصیف می‌کند، بدین ترتیب که محقق از طریق به دست آوردن فراوانی، اندازه‌های گرایش به مرکز، شاخص‌های پراکندگی، رسم نمودار و غیره، متغیرهای موردمطالعه را توصیف می‌کند. در این پژوهش متناسب با تحلیل داده‌ها و برای توصیف قسمت اول پرسشنامه شامل اطلاعات عمومی پاسخ‌دهنده‌ها از آمار توصیفی استفاده گردید. جداول توزیع فراوانی پاسخگویان، میزان درصد هرکدام و نمودار توزیع فراوانی برحسب متغیرهای مختلفی مانند سن، تجربه، تحصیلات و حوزه کاری نیز بر همین اساس تهیه گردید؛ در بخش آمار استنباطی و برای بررسی نرمال بودن داده‌ها از آزمون کلوموگروف اسمیرنف؛ و به‌منظور پاسخ به پرسش‌های پژوهش از آزمون میانگین و انحراف معیار و آزمون پارامتریک تی برای معناداری استفاده شد؛ در قسمت پایانی نیز برای رتبه‌بندی عوامل از آزمون فریدمن استفاده گردید.

آزمون آمار توصیفی: در این بخش، باهدف محاسبه پارامترهای جامعه با استفاده از سرشماری تمامی عناصر جامعه؛ جهت بررسی و توصیف ویژگی‌های عمومی پاسخ‌دهندگان از روش‌های موجود در آمار توصیفی مانند جداول توزیع فراوانی، درصد فراوانی، درصد فراوانی تجمعی و میانگین استفاده می‌گردد.

جدول۷. توزیع فراوانی پاسخگویان بر اساس سن

سن	فراوانی	درصد فراوانی	درصد فراوانی تجمعی
زیر ۲۰ تا ۳۰	۱	۳/۴	۳/۴
۳۱-۴۰	۱۵	۵۱/۷	۵۵/۲
۴۱-۵۰	۱۳	۴۴/۸	۱۰۰/۰
۵۱ به بالا	۰	۰/۰	۰/۰

1. Descriptive
2. Inferential

جدول۸. توزیع فراوانی پاسخگویان بر اساس سابقه

سابقه	فراوانی	درصد فراوانی	درصد فراوانی تجمعی
10-1	۶	۲۰/۷	۲۰/۷
20-11	۱۴	۴۸/۳	۶۹
30-21	۸	۲۷/۶	۹۶/۶
31 به بالا	۱	۳/۴	۱۰۰

جدول۹. توزیع فراوانی پاسخگویان بر اساس تحصیلات

تحصیلات	فراوانی	درصدفراوانی	درصد فراوانی تجمعی
فوق‌دیپلم	۰	۰/۰	۰/۰
لیسانس	۷	۲۴/۱	۲۴/۱
فوق‌لیسانس	۱۶	۵۵/۲	۷۹/۳
دکتری	۶	۲۰/۷	۱۰۰/۰

جدول۱۰. توزیع فراوانی پاسخگویان بر اساس حوزه کاری

حوزه کاری	فراوانی	درصد فراوانی	درصد فراوانی تجمعی
سیاست‌گذاری	۴	۱۳/۸	۱۳/۸
نظارتی	۶	۲۰/۷	۳۴/۵
اجرایی	۱۷	۵۸/۶	۹۳/۱
دانشگاهی	۲	۶/۹	۱۰۰/۰

آزمون آمار استنباطی: در این بخش، برای قضاوت پیرامون پارامتر جامعه بر اساس مقادیر حاصل از نمونه از آزمون آمار استنباطی استفاده‌شده است. در مطالعات مختلف به دلایل متفاوت دستیابی به همه افراد جامعه امکان‌پذیر نیست بنابراین لازم است تا با استفاده از نمونه به تخمین اندازه‌های واقعی در جامعه پرداخت. در این پژوهش‌ها هدف پژوهشگر تعمیم نتایج به‌دست‌آمده از یک گروه کوچک به یک جامعه بزرگ‌تر می‌باشد.

تحلیل معناداری توزیع پرسشنامه: بدین منظور و برای بررسی توزیع یکسان و به‌طور نرمال داده در این پژوهش از آزمون کولموگروف اسمیرنوف[1] بهره گرفته‌شده است.

1. Kolmogorov-Smirnov(K-S)

همان‌گونه که در جدول زیر مشاهده می‌گردد در همه مقیاس‌ها مقدار معناداری[1] از ۵ صدم کمتر است، درنتیجه مقیاس‌ها دارای توزیع غیر نرمال هستند و از آزمون‌های ناپارمتریک در خصوص تحلیل داده‌های مرتبط با عوامل زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری استفاده می‌شود.

جدول۱۱. آزمون کولموگروف، اسمیرنوف نرمال بودن توزیع داده‌ها

حوزه کاری	فراوانی
سؤال	۲۲
میانگین	۱/۷۶
واریانس	۱/۸۶
دامنه	۰/۲۵
میانه	۱/۲۳
معناداری	۰/۰۰۱

تحلیل معناداری پاسخ‌های پرسشنامه: در این بخش باهدف تعیین درصد معناداری پاسخ جامعه نمونه آماری به سؤالات پرسشنامه در تبیین عوامل زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری، برای هریک از عوامل مورد سؤال از روش آماری آزمون خی ۲(کای اسکوئر)[2] استفاده‌شده که یافته‌های حاصل از این آزمون در ادامه قابل‌مشاهده است.

در این آزمون دو فرض برای بررسی معناداری تعیین‌شده است، فرض اول به این معناست که پاسخ‌دهندگان بین گزینه‌های مختلف برای پاسخ به سؤالات مرتبط با عوامل زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری تفاوت قائل بوده‌اند و اختلاف بین ارقام معنادار بوده است؛ فرض دوم بدین معناست که عوامل مذکور معنادار نبوده و پاسخ‌دهندگان در این خصوص تفاوتی قائل نبوده‌اند و درنتیجه از روی شانس بوده است.

در جدول زیر معنی‌داری آزمون در جهت اینکه آیا تفاوت معنی‌داری بین یافته‌های جدید با نسبت فرض شده قبلی وجود دارد یا خیر، بر مبنای زیر بررسی می‌گردد.

- تفاوت معنی‌دار نیست: عدد به‌دست‌آمده بزرگ‌تر از ۰/۰۵
- تفاوت معناداری وجود دارد: عدد به‌دست‌آمده کمتر از ۰/۰۵

1. Significance (Sig)
2. Chi-square

جدول۱۲. آزمون خی ۲-کای اسکوئر معناداری پاسخ جامعه آماری

ردیف	عوامل زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری	کای اسکوئر	درجه آزادی	معناداری
1	همکاری دولت با گروه‌های هکری	۵/۲۴۱a	۲	۰/۰۷۳
2	به‌کارگیری ابزارها و سامانه‌های بومی	۷/۸۲۸a	۳	۰/۰۵۰
3	استفاده از تجهیزات پیشرفته و خودکار	۱/۷۲۴a	۲	۰/۴۲۲
4	همکاری دولت با مجموعه‌های خصوصی	۵/۲۴۱a	۲	۰/۰۷۳
5	شفافیت نقش دستگاه‌های حاکمیتی در رزمایش	۷/۵۱۷a	۲	۰/۰۲۳
6	اشتراک‌گذاری به‌موقع اطلاعات در حوزه رزمایش	۷/۵۱۷a	۲	۰/۰۲۳
7	تمرکز و یکپارچه‌سازی آماد و پشتیبانی رزمایش	۰/۴۸۳a	۲	۰/۷۸۶
8	همسویی سیاست‌های دفاعی کشور در حوزه سایبر	۵/۴۴۸a	۲	۰/۰۶۶
9	ارتقاء مستمر تسلیحات، تجهیزات و فناوری‌های موجود	۰/۸۹۷a	۲	۰/۶۳۹
10	بهره‌گیری از ظرفیت‌های ارتباطی با شبکه‌های اجتماعی	۰/۸۹۷a	۲	۰/۶۳۹
11	تعامل اطلاعاتی حوزه رزمایش با سایر سازمان‌های اطلاعاتی	۲/۹۶۶a	۲	۰/۲۲۷
12	هماهنگی بین نیروهای مسلح و سایر زیرساخت‌های کشوری	۷/۱۰۳a	۲	۰/۰۲۹
13	ارتباط با شرکت‌های فناور و تولیدکننده تجهیزات توسط مهاجم	۷/۲۷۶a	۳	۰/۰۶۴
14	فرماندهی و مدیریت اثربخش با ایجاد فضای حمایتی و اعتماد متقابل	۱/۳۱۰a	۲	۰/۵۱۹
15	زیرساخت ارتباطی امن و مستقل در تبادل داده‌های دارای طبقه‌بندی	۰/۳۱۰a	۱	۰/۵۷۷
16	بهره‌مندی از ائتلاف‌های همکاری بین‌المللی در زمینه رزمایش سایبری	۱۱/۱۳۸a	۳	۰/۰۱۱
17	آشنایی با دانش فنی تولید سامانه‌ها و سخت‌افزارهای رایانه‌ای و ارتباطی	۸/۵۵۲a	۲	۰/۰۱۴
18	شناخت درهم تنیدگی و تأثیرگذاری متقابل تهدیدات سایبری و امنیتی	۷/۸۲۸a	۳	۰/۰۵۰
19	آشنایی با تجربیات و آموزش‌های دشمن در رزمایش‌ها و عملیات سایبری	۳/۳۷۹a	۲	۰/۱۸۵
20	توجه کافی به شرکت‌کنندگان جهت فراهم آوردن تسهیلات رفاهی مناسب	۰/۲۷۶a	۲	۰/۸۷۱
21	اجرای رزمایش به‌صورت حداقل دوسالانه به‌منظور آمادگی و طرح‌ریزی همه‌جانبه	۹/۱۷۲a	۲	۰/۰۱۰
22	بهره‌گیری از قابلیت‌های پیچیدگی، نهان بودن، توزیع‌پذیر و خودانهدامی تسلیحات	۴/۲۰۷a	۲	۰/۱۲۲

تحلیل داده‌ای گزاره‌های پژوهش: به‌منظور ارزیابی و دستیابی به پاسخ سؤالات تحقیق در ابتدا بر اساس داده‌های جمع‌آوری‌شده، میزان تأثیر تمامی گزاره‌ها (عوامل مؤثر) در ارتقاء رزمایش سایبری و در ادامه اقدام به نرمال‌سازی عوامل ارتقاء در قالب مؤلفه‌های سه‌گانه زمینه‌ای، رفتاری و ساختاری برحسب اولویت میانگین، وزن و نمره وزن موزون به شرح زیر گردید.

- میانگین: این متغیر با محاسبه "میانگین عددی نظرات پاسخ‌دهندگان" بر اساس طیف لیکرت نسبت به هر یک از گزاره‌ها محاسبه می‌گردد و عملاً مقدار آن برابر یک می‌باشد.
- وزن: این متغیر با محاسبه حاصل‌ضرب "میانگین هر گزاره" در "مجموع میانگین گزاره‌ها" محاسبه می‌گردد.
- نمره وزن موزون: این متغیر با محاسبه حاصل‌ضرب "وزن" در "میانگین هر یک از گزاره‌ها" محاسبه می‌شود.
- اولویت‌بندی گزاره‌ها: به‌منظور تعیین موقعیت و اولویت‌بندی هریک از گزاره‌ها، از مرتب‌سازی متغیر نمره وزن موزون بر اساس بیشترین به کمترین استفاده می‌گردد.

جدول۱۳. نرمال‌سازی گزاره‌های زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری

ردیف	گزاره‌های زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری	میانگین	وزن	نمره وزن موزون
1	ارتباط با شرکت‌های فناور و تولیدکننده تجهیزات توسط مهاجم	۲/۱۰	۰/۰۵۱۳	۰/۱۰۸
2	فرماندهی و مدیریت اثربخش با ایجاد فضای حمایتی و اعتماد متقابل	۲/۱۰	۰/۰۵۱۳	۰/۱۰۸
3	شناخت درهم تنیدگی و تأثیرگذاری متقابل تهدیدات سایبری و امنیتی	۲/۱۰	۰/۰۵۱۳	۰/۱۰۸
4	ارتقاء مستمر تسلیحات، تجهیزات و فناوری‌های موجود	۲/۰۳	۰/۰۴۹۵	۰/۱۰۱
5	استفاده از تجهیزات پیشرفته و خودکار	۲/۰۰	۰/۰۴۸۸	۰/۰۹۸
6	توجه کافی به شرکت‌کنندگان جهت فراهم آوردن تسهیلات رفاهی مناسب	۲/۰۰	۰/۰۴۸۸	۰/۰۹۸
7	به‌کارگیری ابزارها و سامانه‌های بومی	۱/۹۷	۰/۰۴۸۱	۰/۰۹۵

جدول۱۳. نرمال‌سازی گزاره‌های زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری

ردیف	گزاره‌های زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری	میانگین	وزن	نمره وزن موزون
8	تمرکز و یکپارچه‌سازی آماد و پشتیبانی رزمایش	۱/۹۷	۰/۰۴۸۱	۰/۰۹۵
9	تعامل اطلاعاتی حوزه رزمایش با سایر سازمان‌های اطلاعاتی	۱/۹۷	۰/۰۴۸۱	۰/۰۹۵
10	آشنایی با دانش فنی تولید سامانه‌ها و سخت‌افزارهای رایانه‌ای و ارتباطی	۱/۹۳	۰/۰۴۷۱	۰/۰۹۱
11	بهره‌گیری از ظرفیت‌های ارتباطی با شبکه‌های اجتماعی	۱/۹۰	۰/۰۴۶۴	۰/۰۸۸
12	همکاری دولت با گروه‌های هکری	۱/۸۶	۰/۰۴۵۴	۰/۰۸۴
13	همکاری دولت با مجموعه‌های خصوصی	۱/۸۶	۰/۰۴۵۴	۰/۰۸۴
14	بهره‌مندی از ائتلاف‌های همکاری بین‌المللی در زمینه رزمایش سایبری	۱/۸۶	۰/۰۴۵۴	۰/۰۸۴
15	شفافیت نقش دستگاه‌های حاکمیتی در رزمایش	۱/۸۳	۰/۰۴۴۷	۰/۰۸۲
16	همسویی سیاست‌های دفاعی کشور در حوزه سایبر	۱/۷۶	۰/۰۴۳	۰/۰۷۶
17	آشنایی با تجربیات و آموزش‌های دشمن در رزمایش‌ها و عملیات سایبری	۱/۷۶	۰/۰۴۳	۰/۰۷۶
18	بهره‌گیری از قابلیت‌های پیچیدگی، نهان بودن، توزیع‌پذیر و خودانهدامی تسلیحات	۱/۶۹	۰/۰۴۱۲	۰/۰۷۰
19	هماهنگی بین نیروهای مسلح و سایر زیرساخت‌های کشوری	۱/۶۲	۰/۰۳۹۵	۰/۰۶۴
20	اجرای رزمایش به‌صورت حداقل دوسالانه به‌منظور آمادگی و طرح‌ریزی همه‌جانبه	۱/۶۲	۰/۰۳۹۵	۰/۰۶۴
21	اشتراک‌گذاری به‌موقع اطلاعات در حوزه رزمایش	۱/۵۹	۰/۰۳۸۸	۰/۰۶۲
22	زیرساخت ارتباطی امن و مستقل در تبادل داده‌های دارای طبقه‌بندی	۱/۴۵	۰/۰۳۵۴	۰/۰۵۱

بر اساس آزمون صورت پذیرفته و تحلیل داده‌ای گزاره‌های پژوهش در مؤلفه عوامل زمینه‌ای، سه عامل "ارتباط با شرکت‌های فناور و تولیدکننده تجهیزات توسط مهاجم"، "فرماندهی و

مـدیریت اثـربخش بـا ایجـاد فضـای حمـایتی و اعتمـاد متقابـل" و "شـناخت درهـم تنیـدگی و تأثیرگذاری متقابل تهدیدات سایبری و امنیتی" با نمره وزن موزون ۰,۱۰۸، به‌عنوان تأثیرگذارترین عوامل مؤلفه زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری؛ و عامل "زیرساخت ارتبـاطی امـن و مسـتقل در تبادل داده‌های دارای طبقه‌بندی" با نمره وزن موزون ۰,۰۵۱، به‌عنوان کم اثرترین عامـل مؤلفـه زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری محسوب می‌گردند.

پاسخ سؤال اصلی تحقیق: با توجه به تحلیل داده‌ای گـزاره‌هـای پـژوهش و نرمـال‌سـازی مؤلفه عوامل زمینه‌ای مـؤثر بـر ارتقـاء رزمـایش سـایبری؛ در ایـن بخـش بـه تجزیـه‌وتحلیـل نتـایج به‌دست‌آمده و تبیین عوامل زمینه‌ای مؤثر بـر ارتقـاء رزمـایش سـایبری از طریـق آزمـون فریـدمن[1] باهدف رتبه‌بندی و پاسخ به سؤال اصلی پژوهش مبنی بر "اثرگذاری عوامل زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری چه میزان است؟" پرداخته می‌شود.

جدول۱۴. رتبه‌بندی گزاره‌های عوامل زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری

ردیف	گزاره‌های زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری برحسب اولویت	میانگین رتبه‌ای
1	فرماندهی و مدیریت اثربخش با ایجاد فضای حمایتی و اعتماد متقابل	۱۳/۵۰
2	ارتباط با شرکت‌های فناور و تولیدکننده تجهیزات توسط مهاجم	۱۳/۲۶
3	شناخت درهم تنیدگی و تأثیرگذاری متقابل تهدیدات سایبری و امنیتی	۱۳/۱۹
4	ارتقاء مستمر تسلیحات، تجهیزات و فناوری‌های موجود	۱۲/۹۵
5	استفاده از تجهیزات پیشرفته و خودکار	۱۲/۶۴
6	توجه کافی به شرکت‌کنندگان جهت فراهم آوردن تسهیلات رفاهی مناسب	۱۲/۶۴
7	تعامل اطلاعاتی حوزه رزمایش با سایر سازمان‌های اطلاعاتی	۱۲/۴۱
8	به‌کارگیری ابزارها و سامانه‌های بومی	۱۲/۳۸
9	آشنایی با دانش فنی تولید سامانه‌ها و سخت‌افزارهای رایانه‌ای و ارتباطی	۱۲/۲۲
10	تمرکز و یکپارچه‌سازی آماد و پشتیبانی رزمایش	۱۲/۱۹
11	بهره‌گیری از ظرفیت‌های ارتباطی با شبکه‌های اجتماعی	۱۲/۰۷
12	همکاری دولت با گروه‌های هکری	۱۱/۷۱
13	همکاری دولت با مجموعه‌های خصوصی	۱۱/۵۵
14	بهره‌مندی از ائتلاف‌های همکاری بین‌المللی در زمینه رزمایش سایبری	۱۱/۴۰

1. Friedman

جدول۱۴. رتبه‌بندی گزاره‌های عوامل زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری

ردیف	گزاره‌های زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری برحسب اولویت	میانگین رتبه‌ای
15	شفافیت نقش دستگاه‌های حاکمیتی در رزمایش	۱۱/۱۷
16	همسویی سیاست‌های دفاعی کشور در حوزه سایبر	۱۰/۵۵
17	آشنایی با تجربیات و آموزش‌های دشمن در رزمایش‌ها و عملیات سایبری	۱۰/۴۰
18	بهره‌گیری از قابلیت‌های پیچیدگی، نهان بودن، توزیع‌پذیر و خودانهدامی تسلیحات	۱۰/۲۴
19	اجرای رزمایش به‌صورت حداقل دوسالانه به‌منظور آمادگی و طرح‌ریزی همه‌جانبه	۹/۶۶
20	هماهنگی بین نیروهای مسلح و سایر زیرساخت‌های کشوری	۹/۴۱
21	اشتراک‌گذاری به‌موقع اطلاعات در حوزه رزمایش	۹/۳۶
22	زیرساخت ارتباطی امن و مستقل در تبادل داده‌های دارای طبقه‌بندی	۸/۱۰

اساس یافته‌های تحلیلی گزاره‌های پژوهش در این بخش، در خصوص پاسخ به سؤال اصلی پژوهش نتایج جدول ۱۲ نشان می‌دهد که معناداری محاسبه‌شده برای عوامل فوق از معناداری در سطح آلفای ۰/۰۵ کوچک‌تر است، لذا بین اولویت گزاره‌های عوامل زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری تفاوت معنی‌داری وجود دارد. همچنین در جدول فوق رتبه‌بندی مهم‌ترین عوامل بر اساس اهمیت و نظر خبرگان را به ترتیب اولویت میانگین رتبه‌ای قابل‌مشاهده است که بر این اساس در بین عوامل زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری، عامل " فرماندهی و مدیریت اثربخش با ایجاد فضای حمایتی و اعتماد متقابل" با نمره میانگین رتبه‌ای ۱۳/۵۰ به‌عنوان تأثیرگذارترین و عامل "زیرساخت ارتباطی امن و مستقل در تبادل داده‌های دارای طبقه‌بندی" با نمره میانگین رتبه‌ای ۸/۱۰ به‌عنوان کم اثرترین عامل زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری محسوب می‌گردد.

نتیجه گیری

بر اساس پژوهش صورت گرفته، عوامل زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری مشتمل بر ۲۲ عامل مطابق جدول ۱۴ است که سه عامل "ارتباط با شرکت‌های فناور و تولیدکننده تجهیزات توسط مهاجم"، "فرماندهی و مدیریت اثربخش با ایجاد فضای حمایتی و اعتماد متقابل" و

"شناخت درهم تنیدگی و تأثیرگذاری متقابل تهدیدات سایبری و امنیتی" با میانگین ۲/۱۰ و نمره وزن موزون ۰/۱۱ به‌عنوان تأثیرگذارترین و عامل "زیرساخت ارتباطی امن و مستقل در تبادل داده‌های دارای طبقه‌بندی" با میانگین ۱/۴۵ و نمره وزن موزون ۰/۰۵ به‌عنوان کم اثرترین عامل زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری محسوب می‌گردد.

عناصر حوزه رزمایش: راهکارهای پیشنهادی ارائه‌شده در این بخش متناسب با میانگین رتبه‌ای و اولویت گزاره‌های عوامل زمینه‌ای مؤثر بر ارتقاء رزمایش سایبری، یعنی گزاره‌هایی که به‌طور متوسط حائز میانگین رتبه‌ای بالای ۳۰ هستند را شامل می‌گردد.

۱- اهتمام در موضوع "فرماندهی و مدیریت اثربخش با ایجاد فضای حمایتی و اعتماد متقابل" در سطوح مختلف رزمایش سایبری با استفاده از حداکثر توانایی و استعداد افراد در رسیدن به هدف‌های تعیین‌شده، ایجاد فضای حمایتی و اعتماد متقابل؛ که از راه‌های افزایش انگیزش کارکنان در عرصه آشفته و پرتلاطم سایبری محسوب می‌شود. ایجاد فضای حمایتی با شناخت عوامل انگیزش کارکنان، ایجاد شور و شوق با تمرکز بر آن‌ها از اهمیت بالایی برخوردار است. مدیران در این گزاره به کارکنان فرصت بهبود می‌دهند تا ابتکار عمل را به دست گیرند و در کار خود بهتر عمل کنند. مدیران نیز به کارکنان کمک می‌کنند تا به اهداف شخصی معین خودشان، مثل ترفیع یا کسب مهارت‌های جدید دست یابند. در این مدل، مدیر درباره‌ی اهداف شغلی کارکنان از آن‌ها سؤال و به آن‌ها کمک می‌کند تا برنامه‌ای عملی شکل دهند تا در کنار هم به موفقیت برسند؛ علاوه بر ایجاد فضای حمایتی، یکی از اصلی‌ترین جنبه‌های هر رابطه‌ی سازنده‌ای، اعتماد است، میزان اعتماد نقش اساسی در دلبستگی کارکنان دارد. برای ایجاد اعتماد در افراد، فرماندهان و مدیران می‌بایست منتقدانه رفتار خود را بررسی و به دنبال بهره‌گیری از روش‌های اعتماد ساز از قبیل پذیرفتن اشتباهات خود، عمل به حرف‌های خود، اعتبار دادن به افراد، شفافیت و رک صحبت کردن، رازداری و افزایش اختیارات افراد مؤثر در اجرای رزمایش برای بهبود اوضاع سازمان خود باشند.

۲- اهتمام در موضوع "ارتباط با شرکت‌های فناور و تولیدکننده تجهیزات توسط مهاجم"، این موضوع نیازمند ارتباط فعال افراد تیم قرمز رزمایش سایبری با مجموعه‌های تولید و پشتیبانی سامانه‌ها و تجهیزات سخت‌افزاری و نرم‌افزاری با هدف اشراف اطلاعاتی و توانمندسازی در حوزه

محصولات فناوری اطلاعات است. این ارتباط به طرق گوناگون برگزاری جلسات فنی مشترک، دسترسی به اسناد فنی سامانه‌ها و تجهیزات، ارائه نسخه تست در محیط آزمایشگاه جهت بررسی تیم قرمز و برگزاری دوره‌های آموزشی راه‌اندازی و کاربری سامانه‌ها و تجهیزات محقق می‌گردد. پیشنهاد می‌گردد فرماندهان و مدیران رزمایش سایبری پس از شناسایی شرکت‌های مذکور اقدام به انعقاد تفاهم‌نامه همکاری در موضوعات مذکور نمایند.

۳- تهدیدات سایبری به جهت برخورداری از ویژگی‌هایی چون قیمت پایین ورود، گمنامی و تأثیرگذاری شگرف، پدیده‌ای به نام انتشار قدرت را به وجود آورده است که نه‌تنها باعث شده دولت‌های کوچک از ظرفیت بیشتری برای اعمال قدرت در این فضا برخوردار شوند، بلکه منجر به ورود بازیگران جدیدی همچون شرکت‌ها، گروه‌های سازمان‌یافته و افراد به معادلات قدرت جهانی شده است؛ بنابراین، این پدیده امنیت ملی را از ابعاد مفهوم امنیت، دولت‌محوری در امنیت، بعد جغرافیایی تهدید، گستردگی آسیب‌پذیری‌ها، شیوه مقابله با تهدیدها و تعدد بازیگران در این عرصه، تحت تأثیر قرار داده است و "شناخت درهم تنیدگی و تأثیرگذاری متقابل تهدیدات سایبری و امنیتی" به‌عنوان یکی از مؤثرترین گزاره‌های مؤثر بر ارتقاء رزمایش سایبری نیازمند اهتمام بیشتری از سوی عناصر حوزه رزمایش سایبری است.

عناصر حوزه رزمایش: تحقیق و پژوهش برای چاره‌جویی مشکلات و توسعه روش‌ها و فرآیندهای جاری در هر حوزه، امری ضروری و اجتناب‌ناپذیر است. آنچه مسلم است محقق در پایان پژوهش خود دیدگاه‌های جدیدی را خواهد شناخت که می‌تواند راهنمای پژوهشگرانی که قصد تحقیق مشابه را دارند، باشد؛ بنابراین می‌توان این تحقیق را باب جدیدی برای پاره‌ای از تحقیقات به شمار آورد.

اینجانب در این تحقیق موضوعات را به‌طور کلان موردبررسی قرار داده‌ام. لذا به سایر محققین محترم پیشنهاد می‌شود در موضوعات زیر به‌صورت خاص و با توجه به هر موضوع به‌صورت جداگانه کار تحقیق و پژوهش انجام دهند.

- جایگاه رزمایش سایبری در زیرساخت‌های حیاتی کشور.
- شناسایی و بررسی سایر گزاره‌های مؤثر بر ارتقاء رزمایش سایبری.
- عملیاتی سازی مؤثرترین گزاره‌های ارتقاء رزمایش سایبری در کشور.

- شناخت انواع تهدیدهای سایبری و روش‌های مقابله‌ای در زیرساخت‌های حیاتی کشور.
- طراحی و پیاده‌سازی مدل مفهومی رزمایش سایبری بر اساس زیرساخت‌های حیاتی کشور.

وظایف و اختیارات نهادهای حاکمیتی، کشوری، لشکری و بخش خصوصی در انواع رزمایش سایبری.

فهرست منابع

آژانس امنیت سایبری اتحادیه اروپا (۲۰۲۲). رزمایش سایبری.https://www.enisa.europa.eu

آژانس امنیت سایبری و امنیت زیرساخت (۲۰۲۳). چشم‌انداز سازمان. https://www.cisa.gov/about

آژانس امنیت سایبری و امنیت زیرساخت (۲۰۲۳). رزمایش طوفان سایبری. https://www.cisa.gov/cyber-storm-securing-cyber-space

دهقان، رضا، طالبی، کامبیز، عربیون، ابوالقاسم (۱۳۹۱)، پژوهشی پیرامون عوامل مؤثر بر نوآوری و کارآفرینی سازمانی در دانشگاه‌های علوم پزشکی کشور، پیاورد سلامت، دوره ۶.

دهقان، رضا، طالبی، کامبیز، عربیون، ابوالقاسم (۱۳۹۱)، توسعه کارآفرینی در نظام اداری، تهران، کنفرانس ملی کارآفرینی و مدیریت کسب‌وکارهای دانش‌بنیان.

سامانه ملی قوانین و مقررات جمهوری اسلامی ایران (۱۳۹۹). مصوبه کمیته پدافند غیرعامل کشور در خصوص نظام آمادگی و رزمایش دستگاه‌های اجرایی در برابر تهدیدات. https://qavanin.ir/Law/PrintText/289581

شرکت دانش‌بنیان مهندسی دنیای فناوری امن ویرا (۱۴۰۱). پدافند غیرعامل سایبری. https://cyberno.ir/page/posts/85

عمید، حسن، فرهنگ فارسی عمید، تهران، امیرکبیر، چاپ هفدهم، ۱۳۶۱

میرزایی، پایگاه اطلاعاتی مدیریت و پژوهش مدیربام (۲۰۱۹). مدل تحلیلی سه‌شاخگی.

مدل تحلیلی سه‌شاخگی https://modirbam.com/

میرزایی اهرنجانی، حسن (۱۳۷۶)، در جست‌وجوی یک طرح نظری برای شناخت و تجزیه‌وتحلیل عوامل مؤثر بر وجدان کاری و انضباط اجتماعی در سازمان، قزوین، مجموعه مقالات دومین اجلاس بررسی راه‌های علمی حاکمیت وجدان کاری و انضباط اجتماعی.

میرزایی اهرنجانی، حسن و سرلک، محمدعلی (۱۳۸۴)، نگاهی به معرفت‌شناسی سازمانی: سیر تحول، مکاتب و کاربردهای مدیریتی، فصلنامه پیک نور، سال سوم، شماره ۳.

موحدی راد، محمدرضا و مدیری، ناصر (۱۳۹۳). رزمایش سایبری رویکردی نوین جهت آمادگی در برابر تهدیدات سایبری، مشهد، مقاله ارائه‌شده به نهمین سمپوزیوم پیشرفت‌های علوم و تکنولوژی

موسسه ملی استاندارد و فناوری آمریکا (۲۰۲۳). واژه‌نامه تهدید سایبری. https://csrc.nist.gov/glossary/term/cyber_threat

موسسه بین‌المللی 4C Strategies (۲۰۲۳). https://www.4cstrategies.com/case_study/eu-cyber-atlantic-exercise

وزارت امنیت داخلی ایالات‌متحده (۲۰۲۳). چشم‌انداز سازمان. https://www.dhs.gov/about-dhs

ویکی‌پدیا (۲۰۲۳) رزمایش طوفان سایبری. https://en.wikipedia.org/wiki/Cyber_Storm_Exercise

هیئت مؤلفان آکسفورد، فرهنگ لغات آکسفورد، تهران، فرهنگ نما ، چاپ سوم، ۱۳۸۶

Commission of the European Communities (2017). COMMISSION RECOMMENDATION (EU) 2017/1584, EU, Official Journal of the European Union

Christoforatos, Christoforatos, Lella, Ifigenia, Rekleitis, Evangelos, Van Heurck, Christian, Zacharis, Alexandros(20۲۲). Cyber Europe 20۲۲ After Action Report PUBLIC, EU, European Network and Information Security Agency (ENISA)

DHS National Cyber Security Division (2006). Cyber Storm I Exercise Report, U.S., Department of Homeland Security

DHS Cybersecurity and Infrastructure Security Agency (2022). Cyber Storm VIII:After Action Report, U.S., Cybersecurity and Infrastructure Security Agency

DHS Cybersecurity and Infrastructure Security Agency (2023). Cyber Storm IX: National Cyber Exercise Fact Sheet, U.S., Cybersecurity and Infrastructure Security Agency

E. Joyce, Robert (2022). Committee on National Security Systems(CNSS) Glossary, United States, CNSS

H. Winter, System security assessment using a cyber range(2012). 7th IET International Conference on System Safety, incorporating the Cyber Security Conference.

Seker, Ensar(2018). The Concept of Cyber Defence Exercises (CDX):Planning, Execution, Evaluation, Estonia, NATO CCD COE, Tallinn

SUBASU, Georgiana; ROSU, Livia; PATRICIU , Victor Valeriu (2017). Cyber Defence Exercises:Approaches for Training, Romania, The Military Technical Academy of Bucharest

TRIMINTZIOS, Panagiotis, GAVRILA, Razvan, Ogée, Adrien, Zacharis, Alexandros (۲۰۱۵). Cyber Europe 2014 After Action Report PUBLIC, EU, European Network and Information Security Agency (ENISA)

Trimintzios, Panagiotis (2010). CYBER EUROPE 2010 – EVALUATION REPORT, EU, European Network and Information Security Agency (ENISA)