سال هشتم، شماره یکم (پیاپی ۲۵)، بهار ۱۴۰۴، صص.۱۳۳-۱۵۸
تاریخ دریافت: ۱۴۰۳/۱۱/۲۹ ـ تاریخ پذیرش: ۱۴۰۴/۰۱/۲۱

مقاله پژوهشی

بررسی عوامل ساختاری مؤثر بر ارتقای رزمایش سایبری

فرهاد قاطعی درگاهی
کارشناسی ارشد مطالعات دفاعی استراتژیک، دانشگاه جامع امام حسین (ع) و پژوهشگر دانشکده فرماندهی و مدیریت ولایت سپاه (دافوس)، تهران، ایران.
Email: alialavi200020@gmail.com

چکیده

در سال‌های اخیر حملات و تهاجمات مختلفی علیه زیرساخت‌ها و مراکز حیاتی که به نحوی به فضای سایبری وابسته بوده‌اند، صورت گرفته است؛ مسئله اصلی این تحقیق، بررسی میزان اثرگذاری عوامل ساختاری اصلی بر روند ارتقای رزمایش سایبری بوده است که با استفاده از جمع‌آوری داده‌ها به روش کتابخانه‌ای و میدانی و با نگاه به تجربیات منتشر شده وزارت امنیت داخلی ایالات متحده و آژانس امنیت سایبری اتحادیه اروپا، منجر به شناسایی ۲۰ عامل مؤثر گردید. همچنین با تهیه پرسش‌نامه که بین جامعه نمونه آماری ۲۹ نفر توزیع گردید، شروط روایی و پایایی پژوهش، با حذف ۱ گزاره و مقدار آلفای کرونباخ ۰/۸۶ پذیرفته شد. بر اساس نتایج و یافته‌ها، در پاسخ به سؤال اصلی تحقیق بر اساس آزمون فریدمن، عامل «چابکی ستادها در اجرای عملیات رزمایش» با میانگین ۲/۱۴ در رتبه اول، عامل «ره نامه‌ها و آیین‌نامه‌های آموزشی رزمایش» با میانگین ۲/۰۳ در رتبه دوم و عامل «نظارت و ارزیابی مستمر تغییرات در فرایند رزمایش» با میانگین ۱/۹۳ در رتبه سوم عوامل ساختاری مؤثر بر ارتقای رزمایش سایبری قرار گرفت.

کلیدواژه‌ها: عوامل ساختاری مؤثر، رزمایش سایبری، زیرساخت حیاتی.

مقدمه

اهمیت فناوری اطلاعات و سایبر که به‌عنوان پسوندی که بر مجموعه تکنولوژی‌های اطلاعاتی، ارتباطی و هوش مصنوعی اطلاق می‌شود، 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، از جمله 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 با هدف 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.

با توجه به کمبود فعالیت‌های پژوهشی جامع و به‌منظور زمینه‌سازی برای انجام پژوهش‌های بیشتر، در این مقاله عوامل ساختاری مؤثر بر ارتقای رزمایش‌های سایبری، شناسایی و میزان تأثیرگذاری هر عامل با استفاده از روش‌های آماری بررسی شده است.

۱. پیشینه پژوهش

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 آیین‌نامه حاوی قوانین و تعیین سطوح دسترسی خاص را به‌عنوان الزامات اجرای رزمایش سایبری معرفی کرده‌اند که کلی‌بودن 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 ارتقای رزمایش سایبری نگردیده است. سکر و دیگران (۲۰۱۸) در پژوهش خود به چرخه اجرای رزمایش سایبری و اقداماتی که در هر مرحله صورت می‌پذیرد اشاره کرده‌اند؛ بر اساس چرخه ارائه شده در این پژوهش، چرخه اجرای رزمایش

سایبری شامل چهار مرحله شناسایی، برنامه‌ریزی، هدایت و ارزیابی می‌گردد. در این پژوهش اقدام به شاخص‌سازی 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 با هدف تربیت افسران امنیت اطلاعات در ارتش ایالات‌متحده آمریکا پرداخته ولی در خصوص رزمایش سایبری در زیرساخت‌های کشوری و عوامل مؤثر در اجرای آن را مورد بررسی قرار نداده‌اند. موحدی راد و دیگران (۱۳۹۳) در پژوهش خود به تعاریف و مقایسه انواع رزمایش سایبری بر اساس منابع مختلف در این بخش پرداخته و در انتهای پژوهش خود با بررسی چرخه اجرای رزمایش سایبری، صرفاً الزامات کلی اجرای رزمایش را هدف پژوهش خود قرار داده‌اند.

جدول ۱: مقایسه فعالیت‌های پژوهشی گذشته در خصوص رزمایش سایبری

عنوان	نویسندگان	سال انجام پژوهش	ویژگی‌های برجسته پژوهش
رزمایش دفاع سایبری	جورجیانا سوباسو، لیویا روسو، ویکتور والریا	۲۰۱۷	رویکردهای آموزشی تعیین چرخه رزمایش سایبری
مفهوم تمرینات دفاع سایبری	انصار سکر	۲۰۱۸	بررسی چرخه اجرای رزمایش سایبری و اقدامات هر مرحله
تمرین دفاع سایبری	جی شپنز، راگسدال، سوردو، شفر	۲۰۰۱	ارزیابی اثربخشی آموزش تضمین اطلاعات
رزمایش سایبری رویکردی نوین جهت آمادگی در برابر تهدیدات سایبری	موحدی راد، مدیری	۱۳۹۳	تمرکز بر تعاریف و مقایسه انواع رزمایش سایبری

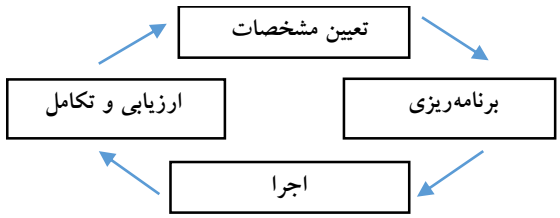
۲. چهارچوب مفهومی

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 ارتقای آمادگی‌های دستگاهی و انفرادی و ارزیابی کارایی اقدامات برای مقابله با تهدیدات می‌شود (وزارت امنیت داخلی ایالات‌متحده، ۲۰۰۶:۱).

اهداف رزمایش سایبری: ارزیابی آمادگی دستگاه‌های اجرایی در برابر حوادث، تهدیدات و اقدامات خصمانه سایبری دشمن در راستای ارتقای 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، ۱۳۹۹:۳).

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 پیشرَوی 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 ۱ نشان داده‌شده است (موحدی راد و دیگران، ۱۳۹۳:۹).



شکل ۱: چرخه حیات رزمایش سایبری

تعیین مشخصات رزمایش: در این بخش سازمان‌دهنده[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 سازمان‌دهنده فرایند برنامه‌ریزی را آغاز می‌کند. این فرایند شامل عضوگیری شرکت‌کنندگان، تأمین منابع مالی رزمایش، انتخاب مکان، تهیه سناریو، قوانین، ابزار و

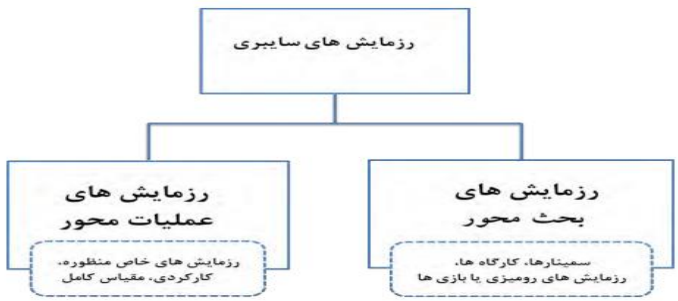
1. Organizer

وسایل آموزشی رزمایش، انتخاب ناظران و سایر نقش‌ها و تعیین چگونگی انجام وظایف آن‌ها می‌شود.

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 تبادل نظر 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 ارتقا و تکامل رزمایش ارائه می‌شوند. همچنین این فرایند می‌تواند شامل جلسات تبادل نظر دنباله‌داری باشد که در آن‌ها بررسی نقطه‌ضعف‌ها و توصیه‌های ارائه شده ادامه پیدا کند.

انواع رزمایش: انواع بسیار مختلفی از رزمایش‌ها وجود دارند که هرکدام فرمت، مزایا، چالش‌ها و هزینه‌های متفاوتی دارند. طبقه‌بندی بین‌المللی استانداردی برای انواع رزمایش در این پژوهش شناسایی نگردید، اما اصطلاحات و دسته‌بندی بسیار متداولی در این زمینه وجود دارند. همان‌گونه که در شکل زیر مشاهده می‌گردد، اکثر متخصصان رزمایش بین رزمایش‌های بحث محور و رزمایش‌های عملیات محور تمایز قائل می‌شوند (موحدی راد و دیگران، ۱۳۹۳:۴).



شکل ۲: تقسیم‌بندی رزمایش سایبری

در جدول زیر نمونه‌هایی از موضوعات و اهداف رزمایش‌های سایبری که در هر قالب رزمایش حاصل می‌شود، نشان داده‌شده است.

جدول ۲: انواع قالب‌ها و موضوعات مورد بحث در رزمایش سایبری

رزمایش بحث محور	موضوعات
سمینار	معرفی ریسک‌های در حال ظهور برای سازمان‌ها و شرکت‌ها به دلیل گسترش کرم‌های اینترنتی به‌سرعت در حال تغییر و مراحل دفاع در برابر آن‌ها؛ معرفی موارد اخیر حملات درون‌سازمانی و اقدامات توصیه‌شده برای سازمان‌ها برای به حداقل رسانده خطرات آن‌ها.
کارگاه	ایجاد راه‌کارهایی برای راه‌اندازی مجدد تمام شبکه‌های شرکت‌ها و حساب‌های کاربری ایمیل در واکنش به نفوذهای گسترده در شبکه؛ ایجاد راه‌کارهایی برای واکنش به از بین رفتن داده‌های حساس؛ ایجاد راه‌کارهای برای به حداقل رساندن تأثیر منفی سوءاستفاده افراد دارای امتیازات مدیریتی.
رزمایش رومیزی	اعتبارسنجی راه‌کارهای واکنشی بین سازمانی در مقابل شیوع گسترده ویروس‌ها و کرم‌ها؛ اعتبارسنجی راه‌کارهای واکنشی در برابر حملات گسترده علیه وب‌سایت شرکت‌ها در واکنش به رویدادهای ژئوپلیتیکی.
بازی	بررسی فرایند تصمیم‌گیری در مورد اجازه دادن به پیشرَوی یک نفوذ به شبکه کشف‌شده به‌منظور جمع‌آوری اطلاعات و شواهد؛ بررسی متدهای بالقوه که افراد درون سازمان می‌توانند با آن‌ها سیستم‌های شرکت را مورد سوءاستفاده قرار دهند و بررسی کنترل‌های کیفی بالقوه برای به حداقل رساندن خطر این سوءاستفاده‌ها.
رزمایش عملیات محور	**اهداف**
رزمایش‌های خاص‌منظوره	اعتبارسنجی برنامه‌های ارتباطی قابل اجرا در صورت کشف خطر برای اطلاعات حساس مشتریان؛ اعتبارسنجی برنامه‌های واکنشی درصورتی‌که یک مقام اجرایی ارشد احساس کند که پسورد ایمیلش برای چند هفته مورد خطر قرار گرفته است؛ اعتبارسنجی برنامه‌های واکنشی درصورتی‌که سیستم‌های تشخیص نفوذ، یک فعالیت شناسایی از یک کشور خارجی را تشخیص دهند.
رزمایش کارکردی	تمرین تصمیم‌گیری‌ها در سطح مدیران ارشد و هماهنگی‌های بین سازمانی برای واکنش به تهدیدات بر طبق سیاست‌ها و راه‌کارهای کشوری؛ بررسی ابزارها و فرایندهای تبادل اطلاعات حساس و طبقه‌بندی‌شده با روش‌های ایمن بدون به خطر افتادن منافع امنیت ملی یا خصوصی.

رزمایش مقیاس کامل	تمرین راه‌کارهای تیم واکنش سریع به حملات کامپیوتری[1] برای کشف شیوع گسترده کرمی که برای شروع یک حمله انکار سرویس توزیع‌شده[2] علیه سازمان‌های کشور در آینده‌ای نامعلوم طراحی‌شده است؛ تمرین ارتباطات بین تیم فناوری اطلاعات[3] یک سازمان یا شرکت به هنگام نفوذ به شبکه کنترل نظارت و اکتساب داده‌ها[4].

مدل تحلیلی سه‌شاخگی[5]: 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 هست 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 جدایی ناپذیرند. در واقع، نوع روابط موجود بین این سه‌شاخه از نوع لازم و ملزوم بوده و به‌مثابه سه‌شاخه روییده از تنه واحد حیات سازمان می‌باشند (میرزایی، ۱۳۷۷).

عوامل ساختاری: این عوامل «نظم ترکیبی» یا «نظم چینشی» عناصر اصلی تشکیل‌دهنده سازمان را برهم زده و ساختارهای اصلی سازمان را که عبارت‌اند از ساختارهای طبیعی و فیزیکی، ساختارهای مالی و اقتصادی، ساختارهای انسانی و ساختارهای اطلاعاتی را در معرض بحران قرار می‌دهند.

- عوامل ساختاری در برگیرنده مجموعه روابط منظم حاکم بر اجزای داخلی سازمان است که بدنه آن را می‌سازند؛ مانند ساختار سازمانی، قوانین و مقررات (میرزایی، ۱۳۷۷).
- عوامل ساختاری در برگیرنده تمام عناصر، عوامل و شرایط فیزیکی و غیرانسانی سازمان است که با نظم، قاعده و ترتیب خاص و به‌هم‌پیوسته، چهارچوب، قالب، پوسته و بدنه فیزیکی و مادی سازمان را می‌سازد، بنابراین تمام منابع مادی، مالی، اطلاعاتی و فنی که با ترکیب خاصی در بدنه کلی سازمان جاری می‌شوند، جزء شاخه ساختاری قرار می‌گیرند (میرزایی اهرنجانی و سرلک، ۱۳۸۴).

1. Computer Emergency Response Team(CERT)
2. Distributed Denial-of-Service (DDoS) Attack
3. Information Technology(IT)
4. Supervisory Control and Data Acquisition(SCADA)
5. Three Dimentional Model of Structure- Content-Context

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 ساختاری مؤثر بر ارتقای 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 مورد بررسی قرار گرفته است؛ اشاره می‌گردد.

۱. رزمایش وزارت امنیت داخلی ایالات‌متحده[1]: مهم‌ترین رزمایش سایبری در ایالات‌متحده رزمایش طوفان سایبری[2] است؛ این رزمایش یک رزمایش شبیه‌سازی شده دوسالانه است که توسط وزارت امنیت داخلی ایالات‌متحده نظارت می‌شود که اولین بار از ۶ فوریه تا ۱۰ فوریه ۲۰۰۶ با هدف 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:
  - به‌عنوان بزرگ‌ترین و پیچیده‌ترین رزمایش سایبری چندملیتی 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؛

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

- ❖ 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 که در یک بحران دنیای واقعی مورد نیاز 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 سایبری۱، ۲۰۰۶).

➢ دستاوردهای کلیدی رزمایش طوفان سایبری ۲۰۲۰:

- ❖ انجام واکنش فدرال- ایالتی، بخش خصوصی و بین‌المللی به یک حادثه سایبری قابل توجه که خدمات اصلی زیربنایی اینترنت، ازجمله سیستم نام دامنه[1]، مقامات صدور گواهی[2] و پروتکل دروازه مرزی[3] را هدف قرار می‌دهد؛
- ❖ فرصتی برای بررسی رویه‌های سازمانی داخلی، شناسایی پیشرفت‌ها و در نظر گرفتن نحوه اطلاع‌رسانی آن‌ها به بخش، ملی و بین‌المللی فراهم شد. سازمان‌ها همچنین فرصتی برای شناسایی پیشرفت‌ها در فرایندهای ارتباطی و هماهنگی توزیع شده که به دلیل محدودیت‌های همه‌گیر به‌طور فزاینده‌ای در حال انجام است، به دست آوردند؛

1. Domain Name System (DNS)
2. Certificate Authorities (CA)
3. Border Gateway Protocol (BGP)

- ❖ مجموعه شرکت‌کننده CS را گسترش داد تا شامل سهامداران جدید در سراسر دولت فدرال، دولت‌های ایالتی و بخش خصوصی در مسائل گوناگون ازجمله مشارکت قابل توجه در بخش خدمات مالی، شود؛
- ❖ از تلاش‌های برنامه‌ریزی و اجرای طبقه‌بندی‌شده همراه با رزمایش طبقه‌بندی‌شده ICE STORM پشتیبانی کرد و تعامل را در سطح طبقه‌بندی نشده بین جامعه اطلاعاتی و سهامدارانی که تحت تأثیر حوادث سایبری شبیه‌سازی شده قرار گرفتند، تسهیل کرد؛
- ❖ بررسی فرایند لازم برای تشکیل یک گروه هماهنگی یکپارچه[1] سایبری؛
- ❖ بحث بین سازمانی فدرال در مورد مسائل مربوط به سیاست در طول جلسه گروه پاسخ سایبری[2] را فعال کرد؛
- ❖ شناسایی فرصت‌ها برای بهبود جریان اطلاعات بین بخش خصوصی و سازمان‌های دولتی به‌منظور اطمینان از آگاهی موقعیت؛
- ❖ ظرفیت دولت‌های ایالتی و محلی شرکت‌کننده برای پاسخ به حوادث سایبری و هماهنگی از طریق مرکز تجزیه‌وتحلیل اطلاعات چند ایالتی[3] را آزمایش کرد؛
- ❖ برای پاسخ‌گویی به حادثه در بخش‌های زیرساخت‌های حیاتی زیر برنامه‌ریزی و اعمال شده است: شیمیایی، تأسیسات تجاری، ارتباطات، تولید حیاتی، انرژی، خدمات مالی، بهداشت و سلامت عمومی، فناوری اطلاعات و سیستم‌های حمل‌ونقل؛
- ❖ ارزیابی فرایندهای مورد بررسی برای هماهنگی واکنش به حادثه و آگاهی موقعیتی مشترک در میان شرکای شبکه بین‌المللی دیده‌بان و هشدار[4](آژانس امنیت سایبری و امنیت زیرساخت، گزارش پس از اقدام رزمایش طوفان سایبری ۲۰۲۰، ۲۰۲۰).

➢ دستاوردهای کلیدی رزمایش طوفان سایبری ۸

- ❖ رزمایش طوفان سایبری هشتم بر اساس تکرارهای قبلی ساخته شد تا از طریق فرایند برنامه‌ریزی رزمایش و اجرا مکانی برای یادگیری و پیشرفت فراهم کند؛

1. Unified Coordination Group (UCG)
2. Cyber Response Group (CRG)
3. Multi-State Information Sharing and Analysis Center (MSISAC)
4. International Watch and Warning Network (IWWN)

- تقویت آمادگی امنیت سایبری و قابلیت‌های پاسخ‌گویی با اعمال سیاست‌ها، فرایندها 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، از جمله 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 چند وجهی 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- فناوری- عملیاتی و فناوری اطلاعات سازمانی تأثیر می‌گذارد؛
- ذی‌نفعان دولتی را وادار کرد تا گروه هماهنگی یکپارچه[1] سایبری را بر اساس رویه‌های مندرج در فرایندهای طرح ملی واکنش به حوادث سایبری[2] تشکیل دهند؛
- شرکت‌کنندگان به اشتراک‌گذاری اطلاعات و ارتباطات به‌عنوان کشورهای شریک شبکه بین‌المللی دیده‌بان و هشدار[3] 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 واکنش کل سازمان به یک حادثه تأکید کنند که شامل کارشناسان فنی سازمان‌ها، نمایندگان امور عمومی، نمایندگان امور حقوقی و رهبری سازمانی می‌شود؛
- یک پلتفرم 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؛

1. Unified Coordination Group (UCG)
2. The National Cyber Incident Response Plan (NCIRP)
3. International Watch and Warning Network (IWWN)

- ❖ به دولت‌های شرکت‌کننده اجازه داده شد تا نقش‌ها و مسئولیت‌های مرتبط با آژانس‌های پشتیبانی را در چهارچوب‌های واکنش به حوادث سایبری خود بررسی کنند.

۲. رزمایش آژانس امنیت سایبری اتحادیه اروپا[1]: 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 می‌دهند.

رزمایش سایبری اروپا که به‌صورت دو سالانه 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. در واقع یکی از اولویت‌های اتحادیه اروپا که در دستور کار دیجیتالی برای اروپا تعیین شده 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: 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 ۲۰۱۸:
  - ❖ رزمایش به تیم‌های فنی این فرصت را داد تا مهارت‌های خود را در امنیت سایبری با انواع چالش‌های فنی از جمله تجزیه‌وتحلیل بدافزار، پزشکی قانونی، بدافزار موبایل، حملات

1. The European Union Agency for Cybersecurity (ENISA)
2. Cyber Stress Test

مخفیانه هدفمند (تهدید پایدار پیشرفته)، حملات شبکه، آلودگی دستگاه‌های اینترنت اشیا و غیره آزمایش کنند؛

- این رزمایش اهمیت همکاری بین بازیکنان مختلف (قربانیان و مقامات) حوادث امنیت سایبری شبیه‌سازی‌شده، ارائه‌دهندگان امنیتی و مقامات ملی را نشان داد؛ این موضوع به شرکت‌کنندگان ثابت کرد که تنها با تبادل اطلاعات و همکاری می‌توان به چنین موقعیت‌های پرفشار با تعداد زیادی حوادث هم‌زمان، پاسخ داد؛
- در این رزمایش شاهد تعداد زیادی از موارد همکاری دولتی و خصوصی هستیم. شرکت‌کنندگان باید فرایندهای تجاری، توافق‌نامه‌ها، پروتکل‌های ارتباطی و مقررات موجود را دنبال می‌کردند تا موقعیت‌های ارائه شده به آن‌ها را به‌طور مؤثر کاهش دهند. بااین‌وجود، سطح آمادگی بین شرکت‌کنندگان به‌طور قابل توجهی متفاوت بود، جریان اطلاعات گاهی اوقات یک‌طرفه احساس می‌شد و رویه‌های همکاری خصوصی- عمومی ساختاریافته یا وجود نداشت یا به بلوغ نرسیده بود. در این موقعیت دستورالعمل امنیت شبکه و اطلاعات اتحادیه اروپا[1] بسیاری از کاستی‌های مرتبط را شناسایی کرده و اقداماتی را برای بهبود وضعیت پیشنهاد کرد؛
- همکاری در سطح اتحادیه اروپا بدون شک در سال‌های گذشته بهبود یافته است. به‌ویژه، همکاری در سطح فنی بلوغ‌یافته و به‌طور مؤثر ثابت‌شده است. معرفی شبکه CSIRTs همان‌طور که در دستورالعمل امنیت شبکه و اطلاعات اتحادیه اروپا تعریف شده است، به کشورهای عضو اتحادیه اروپا یک ساختار رسمی مؤثر برای تبادل اطلاعات فنی و همچنین برای همکاری به‌منظور حل‌وفصل حوادث پیچیده و در مقیاس بزرگ ارائه کرده است. این رزمایش ثابت کرد که اتحادیه اروپا در این سطح به‌خوبی برای پاسخ‌گویی مجهز است. برخی از شکاف‌های جزئی نیز شناسایی شده و توسط دست‌اندرکاران رفع شده است. از سوی دیگر، همکاری در سطح عملیاتی به میزان کمتری اعمال شد. این‌که چگونه در زندگی واقعی این سطوح با یکدیگر تعامل خواهند کرد و به‌علاوه چگونه دیدگاه استراتژیک رهبران سیاسی را اجرا خواهند کرد چندان واضح نیست. رزمایش‌های آینده باید سعی کنند این جنبه‌ها را نیز آزمایش کنند.

1. The Network & Information Systems (NIS) directive

- حوادث فنی این رزمایش فرصتی عالی برای تیم‌های امنیت سایبری فراهم کرد تا توانایی‌ها و تخصص خود را برای مقابله با انواع چالش‌های امنیت سایبری افزایش دهند. ظرفیت عملیاتی و همچنین مهارت‌های فنی در تمام سازمان‌های شرکت‌کننده در بالاترین سطح ارزیابی شد. تیم‌های شرکت‌کننده از شرکت‌های خصوصی غیر امنیت سایبری در بخش هوانوردی اکثر حوادث را با موفقیت تجزیه‌وتحلیل کردند و ثابت کردند که مهارت‌های آن‌ها قطعاً بسیار بالاست. تنها کاستی در برخی از موارد به جهت کمبود منابع موجود برای امنیت فناوری اطلاعات و نه کمبود مهارت شناسایی گردید. این چالشی است که توسط مدیریت بالاتر در چنین سطحی حل شده است، زیرا بازگشت سرمایه[1] در تخصص امنیت سایبری قطعاً برای چنین بخش‌های حیاتی بالا است (آژانس امنیت سایبری اتحادیه اروپا، گزارش پس از اقدام رزمایش سایبری، ۲۰۱۸).

➢ دستاوردهای کلیدی رزمایش اروپای سایبری ۲۰۲۲

- 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، فرایندهای 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 مورد نیاز است، زیرا شکاف‌ها و نقاط توسعه را با موفقیت شناسایی می‌کند؛
- رزمایش Cyber Europe 2022 به‌طور قابل توجهی توانست چندین ذی‌نفع از بخش خصوصی و دولتی را در همکاری با یکدیگر در جهت دستیابی به یک رویکرد مشترک با هدف بهبود هماهنگی اتحادیه اروپا در طول بحران‌های سایبری بزرگ، مشارکت دهد؛
- سکوی رزمایش سایبری[2] 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؛

1. Return on Investment (ROI)
2. ENISA's Cyberskills Exercise Platform

- این رزمایش اهمیت آمادگی بهینه برای چنین رزمایش بزرگی را تایید 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 تایید کرد.

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

۲. روش‌شناسی

در این بخش با هدف آشنایی با 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 پرداخته شده است.

تحقیق حاضر از لحاظ نوع تحقیق به جهت قابلیت استفاده در مجموعه‌های متولی اجرای رزمایش سایبری در کشور، کاربردی است و به روش توصیفی- تحلیلی انجام‌شده است و بازه زمانی منتهی به سال ۱۴۰۳ هجری شمسی با توجه به برخی تجربیات منتشر شده دنیا در اجرای رزمایش سایبری به‌عنوان قلمرو زمانی در این تحقیق تعیین می‌گردد.

الف. جامعه آماری، حجم نمونه آماری و روش نمونه‌گیری: جامعه آماری در این تحقیق ۳۵ نفر است که از بین این تعداد پرسش‌نامه توزیع شده 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.

ب. روایی[1] و پایایی[2] تحقیق: پس از انجام مطالعات کتابخانه‌ای و بررسی میدانی، پرسش‌نامه تحقیق با ۲۰ گزاره تهیه و به تایید اساتید و خبرگان موضوع با جامعه آماری محدود رسید. برای

1. Validity
2. Reliability

روایی ابزار، پرسش‌نامه در بین ۱۰ نفر از خبرگان توزیع و با بهره‌گیری از روش اعتبار صوری تحلیل شد. همچنین با استفاده از دو روش نسبت روایی محتوایی[1] و شاخص روایی محتوایی[2] اقدام به سنجش روایی پرسش‌نامه گردید. بر اساس نتایج حاصل از نظرسنجی به ازای هریک از عوامل، عامل «انتقال صحیح و شفاف فرمان‌ها، سمت پایین سلسله‌مراتب» از لیست عوامل ساختاری مؤثر بر ارتقای رزمایش سایبری حذف و از آزمون کنار گذاشته شد. برای به دست آوردن پایایی سؤالات پرسش‌نامه، از روش آلفای کرونباخ استفاده شد. بدین‌جهت، از همسانی درونی داده‌های حاصل از تحقیق که قابلیت اعتماد درونی پرسش‌نامه را در یک دامنه از صفر تا یک می‌سنجد، استفاده گردید. بر اساس خروجی‌ها، میزان آلفای کل پرسش‌نامه ۰/۸۶۱ و برای هرکدام از عامل‌ها بین ۰/۷ تا ۰/۹ بود و در نهایت پرسش‌نامه تحقیق و عوامل آن مورد قبول واقع شد. پس از بررسی روایی و پایایی، درنهایت پرسش‌نامه با ۱۹ گزاره در بُعد عوامل ساختاری، مورد تایید قرار گرفت.

۳. تجزیه‌وتحلیل یافته‌ها

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 مورد نظر استخراج و مورد تجزیه‌وتحلیل قرار گرفت. معمولاً برای تجزیه‌وتحلیل اطلاعات در این‌گونه پژوهش‌ها از دو روش آماری توصیفی[3] و استنباطی[4] 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 مورد مطالعه 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

1. Content Validity Ratio(CVR)
2. Content Validity Index(CVI)
3. Descriptive
4. Inferential

فراوانی پاسخگویان، میزان درصد هرکدام و نمودار توزیع فراوانی برحسب متغیرهای مختلفی مانند تحصیلات و حوزه کاری نیز بر همین اساس تهیه گردید؛ در بخش آمار استنباطی و برای بررسی نرمال بودن داده‌ها از آزمون کولموگروف 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.

الف. آزمون آمار توصیفی: در این بخش، با هدف 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 (جدول ۳ و ۴).

جدول ۳: توزیع فراوانی پاسخگویان بر اساس تحصیلات

تحصیلات	فراوانی	درصد فراوانی	درصد فراوانی تجمعی
کارشناسی	۷	۲۴/۱	۲۴/۱
کارشناسی ارشد	۱۶	۵۵/۲	۷۹/۳
دکتری	۶	۲۰/۷	۱۰۰

جدول ۴: 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

ب. آزمون آمار استنباطی: در این بخش، برای قضاوت پیرامون پارامتر جامعه بر اساس مقادیر حاصل از نمونه از آزمون آمار استنباطی استفاده شده 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 است.

تحلیل معناداری توزیع پرسش‌نامه: بدین منظور و برای بررسی توزیع یکسان و به‌طور نرمال داده در این پژوهش از «آزمون کولموگروف اسمیرنوف» بهره گرفته شده است. همان‌گونه که در جدول زیر مشاهده می‌گردد در همه مقیاس‌ها مقدار معناداری از پنج صدم کمتر است، درنتیجه مقیاس‌ها دارای توزیع غیر نرمال هستند و از آزمون‌های ناپارمتریک در خصوص تحلیل داده‌های مرتبط با عوامل ساختاری مؤثر بر ارتقای رزمایش سایبری استفاده می‌شود.

جدول ۵: آزمون کولموگروف–اسمیرنوف نرمال بودن توزیع داده‌ها

حوزه کاری	فراوانی
سؤال	۹
میانگین	۱/۶۷
واریانس	۱/۷۸
دامنه	۰/۲۲
میانه	۰/۶۷
معناداری	۰/۰۰۱

تحلیل معناداری پاسخ‌های پرسش‌نامه: در این بخش با هدف تعیین درصد معناداری پاسخ جامعه نمونه آماری به سؤالات پرسش‌نامه در تبیین عوامل ساختاری مؤثر بر ارتقای رزمایش سایبری، برای هر یک از عوامل مورد سؤال از روش آماری «آزمون خی– اسکوئر» استفاده شده که یافته‌های حاصل از این آزمون در ادامه قابل مشاهده است. در این آزمون دو فرض برای بررسی معناداری تعیین شده است، فرض اول به این معناست که پاسخ‌دهندگان بین گزینه‌های مختلف برای پاسخ به سؤالات مرتبط با عوامل ساختاری مؤثر بر ارتقای 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 ۴ 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

جدول ۶: آزمون خی۲-کای اسکوئر معناداری پاسخ جامعه آماری

ردیف	عوامل ساختاری مؤثر بر ارتقای رزمایش سایبری	کای اسکوئر	درجه آزادی	معناداری
۱	بودجه کافی جهت برگزاری رزمایش	a ۵/۰۳۴	۲	۰/۰۸۱
۲	وجود ساختار سازمانی مناسب رزمایش	a ۴/۲۰۷	۲	۰/۱۲۲
۳	توانایی اجرای عملیات مشترک رزمایش	a ۳/۳۷۹	۲	۰/۱۸۵
۴	چابکی ستادها در اجرای عملیات رزمایش	a ۹/۱۷۲	۲	۰/۰۱۰
۵	رهنامه‌ها و آیین‌نامه‌های آموزشی رزمایش	a ۰/۸۹۷	۲	۰/۶۳۹
۶	سامانه یکپارچه فرماندهی و کنترل رزمایش	a۱۱/۶۵۵	۲	۰/۰۰۳
۷	آیین‌نامه‌ها و دستورالعمل‌های امنیت عملیات	a ۱/۳۱۰	۲	۰/۵۱۹
۸	سازمان‌دهی نیروها در صحنه رزمایش سایبری	a ۸/۷۵۹	۲	۰/۰۱۳
۹	هوشمندی سلاح‌های سایبری با هدف نقطه زنی	a ۵/۲۴۱	۲	۰/۰۷۳
۱۰	نظارت و ارزیابی مستمر تغییرات در فرایند رزمایش	a ۴/۶۲۱	۲	۰/۰۹۹
۱۱	انجام تمرینات و رزمایش‌های محدود درون‌سازمانی	a۱۱/۲۴۱	۲	۰/۰۰۴
۱۲	تخصیص مسئولیت‌ها و وظایف به‌صورت شفاف و رسمی	a ۳/۳۷۹	۲	۰/۱۸۵
۱۳	قابلیت پاسخ‌گویی به‌موقع به انواع تهدیدات در تیم مدافع	a ۹/۵۸۶	۲	۰/۰۰۸
۱۴	طرح‌ریزی مشترک تمرکزی و اجرای غیرمتمرکزی رزمایش	a ۵/۰۳۴	۲	۰/۰۸۱
۱۵	اجرای جنگ نرم و هم‌سو کردن افکار عمومی توسط مهاجم	a ۲/۱۳۸	۲	۰/۳۴۳
۱۶	وجود شبکه یکپارچه جهت پایش زیرساخت‌های هدف رزمایش	a ۱/۳۱۰	۲	۰/۵۱۹
۱۷	هماهنگی نیروها در حوزه‌های مختلف رومیزی، کارکردی، رقابت سایبری	a ۲/۱۳۸	۲	۰/۳۴۳
۱۸	بهبود مستمر امنیت سامانه‌ها و تجهیزات در زیرساخت و بسترهای ارتباطی	a ۵/۲۴۱	۲	۰/۰۷۳
۱۹	تجمیع نتایج و داده‌های تیم‌های رزمایش، تحلیل و تصمیم‌سازی برای فرمانده	a ۹/۵۸۶	۲	۰/۰۰۸

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 ارتقای رزمایش سایبری و در ادامه اقدام به نرمال‌سازی عوامل ارتقا در قالب مؤلفه‌های ساختاری برحسب اولویت میانگین، وزن و نمره وزن موزون جدول ۷ 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 است؛

- 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.

جدول ۷: نرمال‌سازی گزاره‌های ساختاری مؤثر بر ارتقای رزمایش سایبری

ردیف	گزاره‌های ساختاری مؤثر بر ارتقای رزمایش سایبری	میانگین	وزن	نمره وزن موزون
۱	چابکی ستادها در اجرای عملیات رزمایش	۲/۱۴	۰/۰۶۳	۰/۱۳۵
۲	ره‌نامه‌ها و آیین‌نامه‌های آموزشی رزمایش	۲/۰۳	۰/۰۶۰	۰/۱۲۲
۳	نظارت و ارزیابی مستمر تغییرات در فرایند رزمایش	۱/۹۳	۰/۰۵۷	۰/۱۱۰
۴	انجام تمرینات و رزمایش‌های محدود درون‌سازمانی	۱/۹	۰/۰۵۶	۰/۱۰۷
۵	وجود ساختار سازمانی مناسب رزمایش	۱/۸۳	۰/۰۵۴	۰/۰۹۹
۶	آیین‌نامه‌ها و دستورالعمل‌های امنیت عملیات	۱/۸۳	۰/۰۵۴	۰/۰۹۹
۷	اجرای جنگ نرم و هم‌سو کردن افکار عمومی توسط مهاجم	۱/۸۳	۰/۰۵۴	۰/۰۹۹
۸	وجود شبکه یکپارچه جهت پایش زیرساخت‌های هدف رزمایش	۱/۸۳	۰/۰۵۴	۰/۰۹۹
۹	هماهنگی نیروها در حوزه‌های مختلف رومیزی، کارکردی، رقابت سایبری	۱/۸۳	۰/۰۵۴	۰/۰۹۹
۱۰	سازمان‌دهی نیروها در صحنه رزمایش سایبری	۱/۷۶	۰/۰۵۲	۰/۰۹۲
۱۱	توانایی اجرای عملیات مشترک رزمایش	۱/۷۲	۰/۰۵۱	۰/۰۸۸
۱۲	تخصیص مسئولیت‌ها و وظایف به‌صورت شفاف و رسمی	۱/۷۲	۰/۰۵۱	۰/۰۸۸
۱۳	بودجه کافی جهت برگزاری رزمایش	۱/۶۹	۰/۰۵۰	۰/۰۸۴
۱۴	طرح‌ریزی مشترک تمرکزی و اجرای غیرمتمرکزی رزمایش	۱/۶۹	۰/۰۵۰	۰/۰۸۴
۱۵	هوشمندی سلاح‌های سایبری با هدف نقطه زنی	۱/۶۶	۰/۰۴۹	۰/۰۸۲
۱۶	بهبود مستمر امنیت سامانه‌ها و تجهیزات در زیرساخت و بسترهای ارتباطی	۱/۶۶	۰/۰۴۹	۰/۰۸۲
۱۷	تجمیع نتایج و داده‌های تیم‌های رزمایش، تحلیل و تصمیم سازی برای فرمانده	۱/۶۶	۰/۰۴۹	۰/۰۸۲
۱۸	سامانه یکپارچه فرماندهی و کنترل رزمایش	۱/۵۵	۰/۰۴۶	۰/۰۷۱
۱۹	قابلیت پاسخ‌گویی به‌موقع به انواع تهدیدات در تیم مدافع	۱/۵۵	۰/۰۴۶	۰/۰۷۱

بر اساس آزمون صورت پذیرفته و تحلیل داده‌ای گزاره‌های پژوهش در مؤلفه عوامل ساختاری، سه عامل «چابکی ستادها در اجرای عملیات رزمایش» با نمره وزن موزون ۰/۱۳۵، «ره‌نامه‌ها و آیین‌نامه‌های آموزشی رزمایش» با نمره وزن موزون ۰/۱۲۲ و «نظارت و ارزیابی مستمر تغییرات در فرایند رزمایش» با نمره وزن موزون ۰/۱۱۰، به‌عنوان تأثیرگذارترین عوامل مؤلفه ساختاری مؤثر بر ارتقای رزمایش سایبری و عامل «قابلیت پاسخ‌گویی به‌موقع به انواع تهدیدات در تیم مدافع» با نمره وزن موزون ۰/۰۷۱، به‌عنوان کم اثرترین عامل مؤلفه ساختاری مؤثر بر ارتقای رزمایش سایبری محسوب می‌گردند.

ج. پاسخ سؤال اصلی تحقیق: با توجه به تحلیل داده‌ای گزاره‌های پژوهش و نرمال‌سازی مؤلفه عوامل ساختاری مؤثر بر ارتقای رزمایش سایبری؛ در این بخش به تجزیه‌وتحلیل نتایج به‌دست‌آمده و تبیین عوامل ساختاری مؤثر بر ارتقای رزمایش سایبری از طریق آزمون فریدمن[1] با هدف رتبه‌بندی (جدول ۸) و پاسخ به سؤال اصلی پژوهش مبنی بر «اثرگذاری عوامل ساختاری مؤثر بر ارتقای رزمایش سایبری چه میزان است؟» پرداخته می‌شود.

جدول ۸: رتبه‌بندی گزاره‌های عوامل ساختاری مؤثر بر ارتقای رزمایش سایبری

ردیف	گزاره‌های ساختاری مؤثر بر ارتقای رزمایش سایبری برحسب اولویت	میانگین رتبه‌ای
۱	چابکی ستادها در اجرای عملیات رزمایش	۱۲/۷۶
۲	ره‌نامه‌ها و آیین‌نامه‌های آموزشی رزمایش	۱۱/۸۶
۳	نظارت و ارزیابی مستمر تغییرات در فرایند رزمایش	۱۱/۰۳
۴	انجام تمرینات و رزمایش‌های محدود درون‌سازمانی	۱۰/۸۶
۵	آیین‌نامه‌ها و دستورالعمل‌های امنیت عملیات	۱۰/۵۰
۶	هماهنگی نیروها در حوزه‌های مختلف رومیزی، کارکردی، رقابت سایبری	۱۰/۴۰
۷	وجود ساختار سازمانی مناسب رزمایش	۱۰/۳۳
۸	اجرای جنگ نرم و همسو کردن افکار عمومی توسط مهاجم	۱۰/۲۸
۹	وجود شبکه یکپارچه جهت پایش زیرساخت‌های هدف رزمایش	۱۰/۱۶
۱۰	سازمان‌دِهی نیروها در صحنه رزمایش سایبری	۱۰/۱۴

1. Friedman

ردیف	گزاره‌های ساختاری مؤثر بر ارتقای رزمایش سایبری برحسب اولویت	میانگین رتبه‌ای
۱۱	تخصیص مسئولیت‌ها و وظایف به‌صورت شفاف و رسمی	۹/۵۹
۱۲	توانایی اجرای عملیات مشترک رزمایش	۹/۵۷
۱۳	بودجه کافی جهت برگزاری رزمایش	۹/۲۶
۱۴	تجمیع نتایج و داده‌های تیم‌های رزمایش، تحلیل و تصمیم‌سازی برای فرمانده	۹/۲۶
۱۵	طرح‌ریزی مشترک تمرکزی و اجرای غیرمتمرکزی رزمایش	۹/۱۹
۱۶	هوشمندی سلاح‌های سایبری باهدف نقطه زنی	۹/۰۷
۱۷	بهبود مستمر امنیت سامانه‌ها و تجهیزات در زیرساخت و بسترهای ارتباطی	۸/۸۳
۱۸	سامانه یکپارچه فرماندهی و کنترل رزمایش	۸/۶۲
۱۹	قابلیت پاسخ‌گویی به‌موقع به انواع تهدیدات در تیم مدافع	۸/۳۱

بر اساس یافته‌های تحلیلی گزاره‌های پژوهش در این بخش، در خصوص پاسخ به سؤال اصلی پژوهش نتایج جدول ۶ نشان می‌دهد که معناداری محاسبه شده برای ۱۳ عامل از سطح آلفای ۰/۰۵ بزرگ‌تر و ۶ عامل دیگر از معناداری در سطح آلفای ۰/۰۵ کوچک‌تر است؛ ازهمین‌رو بین آن بخش از گزاره‌های عوامل ساختاری مؤثر بر ارتقای 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 قابل مشاهده است که بر این اساس در بین عوامل ساختاری مؤثر بر ارتقای رزمایش سایبری، عامل «چابکی ستادها در اجرای عملیات رزمایش» با نمره میانگین رتبه‌ای ۱۲/۷۶به‌عنوان تأثیرگذارترین و عامل «قابلیت پاسخ‌گویی به‌موقع به انواع تهدیدات در تیم مدافع» با نمره میانگین رتبه‌ای ۸/۳۱ به‌عنوان کم اثرترین عامل ساختاری مؤثر بر ارتقای رزمایش سایبری محسوب می‌گردد.

۴. نتیجه‌گیری و پیشنهاد

با توجه به اینکه عرصه سایبر متغیر و به‌سرعت در حال تغییر است، سطح تغییر و ابهامی که در این بخش به وجود می‌آید بالا است، انعطاف‌پذیری ستاد و برنامه ریزان حوزه رزمایش سایبری در اشکال مختلف چابکی استراتژی، عملیاتی و مشارکت‌ها ضروری است.

در پژوهش حاضر، بر اساس نتایج به‌دست‌آمده: عوامل ساختاری مؤثر بر ارتقای رزمایش سایبری مشتمل بر ۱۹ عامل مطابق جدول ۶ است که سه عامل «چابکی ستادها در اجرای عملیات رزمایش» با میانگین ۲/۱۴ و نمره وزن موزون ۰/۱۳۵، «رهنامه‌ها و آیین‌نامه‌های آموزشی رزمایش» با میانگین ۲/۰۳ و نمره وزن موزون ۰/۱۲۲ و «نظارت و ارزیابی مستمر تغییرات در فرایند رزمایش» با میانگین ۱/۹۳ و نمره وزن موزون ۰/۱۱۰ به‌عنوان تأثیرگذارترین و دو عامل «سامانه یکپارچه فرماندهی و کنترل رزمایش» و «قابلیت پاسخ‌گویی به‌موقع به انواع تهدیدات در تیم مدافع» با میانگین ۰/۴۶ و نمره وزن موزون ۰/۰۷۱ به‌عنوان کم اثرترین عامل ساختاری مؤثر بر ارتقای رزمایش سایبری محسوب می‌گردد.

بر اساس نتایج محاسباتی عوامل در این تحقیق، چابکی و انعطاف‌پذیری بالا در کلیه اجزای رزمایش از یک‌سو و تهیه و تدوین آیین‌نامه‌ها و منابع آموزشی کاربردی همراه با ارزیابی مستمر فرایندها از جهت کارایی و تأثیرگذاری کافی در رزمایش سایبری به‌عنوان مهم‌ترین عصاره عوامل ساختاری مؤثر در اجرای رزمایش سایبری و نتیجه تحقیق حاضر مطرح است. در این راستا، افزایش توانایی ستاد برای تجدید خود، سازگاری، تغییر سریع و موفقیت در یک محیط با تغییرات متغیر، آشفته و مبهم از اهمیت بالایی برخوردار است و برای رسیدن به «چابکی ستادها در اجرای عملیات رزمایش»، باید بتوانند با توجه به موقعیتی که در آن حضور دارند تصمیمات مختلف و متنوعی اخذ کنند که این امر می‌بایست توسط متولیان این امر مورد توجه قرار گیرد.

پیشنهاد

تحقیق و پژوهش برای چاره‌جویی مشکلات و توسعه روش‌ها و فرایندهای 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 باشد که قصد تحقیق مشابه را دارند؛ بنابراین می‌توان این تحقیق را باب جدیدی برای پاره‌ای از تحقیقات به شمار آورد و به سایر محققین پیشنهاد می‌شود در موضوعات زیر به‌صورت خاص و با توجه به هر موضوع به‌صورت جداگانه کار تحقیق و پژوهش انجام دهند.

- شناسایی و بررسی سایر گزاره‌های مؤثر بر ارتقای رزمایش سایبری؛
- عملیاتی‌سازی مؤثرترین گزاره‌های ارتقای 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

- 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.
- میرزایی (۲۰۱۹). پایگاه اطلاعاتی مدیریت و پژوهش مدیربام. مدل تحلیلی سه‌شاخگی.
- میرزایی اهرنجانی، حسن؛ سرلک، محمدعلی (۱۳۸۴)، ***نگاهی به معرفت‌شناسی سازمانی: سیر تحول، مکاتب و کاربردهای مدیریتی***، فصلنامه پیک نور، سال سوم، شماره ۳.
- موحدی راد، محمدرضا؛ مدیری، ناصر (۱۳۹۳). ***رزمایش سایبری رویکردی نوین جهت آمادگی در برابر تهدیدات سایبری***، مشهد، مقاله ارائه‌شده به نهمین سمپوزیوم پیشرفت‌های علوم و تکنولوژی.
- وزارت امنیت داخلی ایالات‌متحده (۲۰۲۳). ***چشم‌انداز سازمان***.

References

- Christoforatos, Christoforatos, Lella, Ifigenia, Rekleitis, Evangelos, Van Heurck, Christian, Zacharis, Alexandros (2022). Cyber Europe 2022 After Action Report PUBLIC, EU, European Network and Information Security Agency (ENISA)
- European Union Agency for Network and Information Security(2018). Cyber Europe 2018 After Action Report PUBLIC, EU, European Network and Information Security Agency (ENISA)
- DHS Cybersecurity and Infrastructure Security Agency (2020). Cyber Storm 2020:After Action Report, U.S., Cybersecurity and Infrastructure Security Agency
- DHS Cybersecurity and Infrastructure Security Agency (2022). Cyber Storm VIII:After Action Report, 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 (2010). CYBER EUROPE 2010 – EVALUATION REPORT, EU, European Network and Information Security Agency (ENISA)