



Achievements of Conducting Cyber Exercises: A Case Study of the United States' Cyber Storm Exercise

Farhad Ghatei Dargahi

Master's Specialist in Strategic Defense Studies, Imam Hossein University; Researcher at the Faculty of Command and Management, Velayat University, IRGC (DAFOS), Tehran, Iran
Email: alialavi200020@gmail.com

Hossein Falakinia

Instructor, Faculty of Command and Management, Velayat University, IRGC (DAFOS), Imam Hossein University, Tehran, Iran
Email: h-falakiniya@ihu.ac.ir

Abstract

In light of the increasing frequency of cyber-attacks and intrusions in recent years targeting critical infrastructures and vital centers, one of the measures taken in recent years by relevant authorities to defend against and prevent such attacks is the implementation of cyber exercises. The main objective of this research is to identify the achievements derived from conducting cyber exercises, using the United States' Cyber Storm exercise as a case study. This study adopts an exploratory approach, utilizing inductive methods and content analysis with a coding technique. The publicly available experiences of the U.S. Department of Homeland Security were qualitatively analyzed. After the process of open coding and axial coding, 12 key achievements of conducting cyber exercises were identified. Based on this analysis, the major achievement identified was "clarification of roles and responsibilities, and the improvement of processes for integrating and coordinating responses to cyber incidents," with 25 related sub-achievements. Other significant findings include: "the establishment of numerous public and private communications among stakeholders through platforms for information sharing," and "assessment of resources and capabilities for responding to cyber incidents," with 23 related achievements; "collaboration across the public and private sectors," with 21 items; "evaluation of a comprehensive range of policies, doctrines, and communication methods for cyber response," and "assessment of the performance of the National Cybersecurity and Communications Integration Center," with 17 items. These were identified as the primary achievements of conducting cyber exercises

Keywords: Cyber Exercise, Cyber Storm, Critical Infrastructure





سال هشتم، ویژه‌نامه (پیاپی ۲۸)، زمستان ۱۴۰۴، صص. ۵۴-۱۱
تاریخ دریافت: ۱۴۰۳/۰۲/۱۶ - تاریخ پذیرش: ۱۴۰۳/۰۳/۱۲

مقاله پژوهشی

دستاوردهای برگزاری رزمایش سایبری: مطالعه موردی رزمایش طوفان سایبری ایالات متحده

فرهاد قاطعی درگاهی

کارشناس ارشد مطالعات دفاعی استراتژیک، دانشگاه جامع امام حسین^(ع)، پژوهشگر دانشکده فرماندهی و مدیریت ولایت سپاه (دافوس)، تهران، ایران

Email: alialavi200020@gmail.com

حسین فلکی نیا

مربی، دانشکده فرماندهی و مدیریت ولایت سپاه (دافوس)، دانشگاه جامع امام حسین^(ع)، تهران، ایران
Email: h-falakiniya@ihu.ac.ir

چکیده

با توجه به فراوانی حملات و تهاجمات سایبری در سال‌های اخیر علیه زیرساخت‌ها و مراکز حیاتی، یکی از اقداماتی که در چند سال اخیر به‌منظور دفاع و پیش‌گیری از حملات سایبری توسط نهادهای متولی دنبال می‌گردد اجرای رزمایش سایبری است؛ مسئله اصلی این تحقیق، شناسایی دستاوردهای برگزاری رزمایش سایبری با مطالعه موردی رزمایش طوفان سایبری ایالات متحده بوده است. در این پژوهش با رویکرد اکتشافی و با استفاده از روش استقرایی و به شیوه کدگذاری مبتنی بر تحلیل محتوا، تجربیات منتشرشده وزارت امنیت داخلی ایالات متحده، مورد تجزیه و تحلیل کیفی قرار گرفته که پس از انجام فرایند کدگذاری باز و کدگذاری محوری، ۱۲ مورد به‌عنوان دستاوردهای برگزاری رزمایش سایبری معرفی شد. بر این اساس، کلان دستاورد «روشن شدن نقش‌ها و مسئولیت‌ها و بهبود فرایندهای ادغام و هماهنگی پاسخ رویدادهای سایبری» با ۲۵ دستاورد خرد مرتبط، «ارتباطات عمومی و خصوصی متعدد بین بازیگران با ایجاد بستر اشتراک‌گذاری اطلاعات» و «ارزیابی منابع و قابلیت‌های واکنش به حوادث سایبری» با ۲۳ مورد، «همکاری در گستره فرابخشی دولتی و خصوصی» با ۲۱ مورد، «ارزیابی طیف کاملی از سیاست‌ها، دکترین و روش‌های ارتباطی واکنش سایبری» و «ارزیابی عملکرد مرکز ادغام امنیت سایبری و ارتباطات ملی» با ۱۷ مورد، به‌عنوان مهم‌ترین دستاوردهای برگزاری رزمایش سایبری شناسایی گردید.

کلیدواژه‌ها: رزمایش سایبری، طوفان سایبری، زیرساخت حیاتی

دانشگاه عالی دفاع ملی ♦ پژوهشکده آماد، فناوری دفاعی و عرصه‌های نوپدید / فصلنامه آماد و فناوری دفاعی



20.1001.1.28212606.1404.8.5.1.4

<https://amfad.sndu.ac.ir/> E-ISSN: 2980-8073



صحت مطالب بر عهده نویسنده مقاله است و بیانگر دیدگاه دانشگاه عالی دفاع ملی نیست.



مقدمه و بیان مسئله

تا به امروز رزمایش‌ها در انواع مختلف در زمینه‌های نظامی و غیرنظامی در کشور اجرا شده است؛ اما واژه رزمایش سایبری، یک واژه جدید و تا حدی ناملموس بوده که کمتر مورد توجه قرار گرفته است. این گونه رزمایش‌ها و تمرین‌های ارتقای آمادگی، نیازمند سازمان‌دهی، هماهنگی و برخورداری از دستورالعمل‌های فنی و عملیاتی خاص هستند که در آن به مواردی نظیر مفاهیم، اهداف، سازمان‌دهی، وظایف و تکالیف عناصر رزمایش و ارتقای آمادگی و دستورات هماهنگی پرداخته می‌شود. این دستورالعمل بر مبنای تهدیدات سایبری شناسایی شده علیه جمهوری اسلامی ایران و حملات سایبری احتمالی متخاصمین علیه امنیت ملی و زیرساخت‌های کشور، توسط نهادهای حاکمیتی مانند سازمان پدافند غیرعامل کشور و ریاست جمهوری به عنوان مرجع در این امر تهیه و به زیرساخت‌های حیاتی و حساس کشور جهت اجرا ابلاغ می‌گردد.

کشورهای مختلفی در زمینه برگزاری رزمایش سایبری از تجربیاتی برخوردار هستند که بررسی فرایند طرح‌ریزی و اجرای آن‌ها از یکسو، نتایج و دستاوردهای مهم حاصل از برگزاری در سال‌های مختلف از سوی دیگر می‌تواند منجر به بهبود و اثرگذاری هرچه بیشتر برگزاری رزمایش‌های سایبری در کشور شود. از این‌رو در این مقاله با توجه به کمبود فعالیت‌های پژوهشی جامع و به‌منظور زمینه‌سازی برای انجام پژوهش‌های بیشتر، دستاوردهای برگزاری رزمایش طوفان سایبری توسط وزارت امنیت داخلی ایالات متحده و خلاصه‌ای از فعالیت‌های آن‌ها در زمینه برگزاری رزمایش سایبری مورد بررسی قرار گرفته است.

علی‌رغم برگزاری رزمایش‌های سایبری به‌صورت دوره‌ای و به طرق گوناگون در سطح زیرساخت‌های حیاتی کشور، متأسفانه همچنان شاهد آسیب‌پذیری‌ها و تهدیدات گوناگون در این بخش‌ها هستیم که عدم پیش‌بینی و ایمن‌سازی آن‌ها منجر به تحمیل هزینه‌های زیادی برای کشور می‌گردد و این موضوع نشانگر وجود مشکلاتی در بخش سیاست‌گذاری و اجرا است؛ مشکلاتی که در اجرای موفق و باکیفیت رزمایش نقش بسزایی دارند.



از مهم‌ترین مفاهیمی که به بهبود این فرایند کمک می‌کند پاسخ به سؤالاتی است از قبیل «دستاوردهای رزمایش سایبری کدامند؟» از این‌رو در این پژوهش به بررسی پاسخ به این سؤال با استفاده از تجربیات مشابه در سایر کشورها (مطالعه موردی رزمایش طوفان سایبری ایالات متحده) پرداخته شده است.

از جمله مواردی که با توجه به کیفیت و سابقه برگزاری، شناسایی دستاوردهای آن در بخش‌های خرد و کلان می‌تواند منجر به روشن شدن هدف و بالا رفتن کیفیت برگزاری رزمایش‌های سایبری در کشور شود رزمایش طوفان سایبری ایالات متحده است. طوفان سایبری به عنوان بخشی از تلاش‌های مداوم وزارت امنیت داخلی برای ارزیابی و تقویت آمادگی سایبری، بررسی فرایندهای واکنش به حادثه در پاسخ به تهدیدات در حال تکامل و افزایش اطلاعات اشتراک‌گذاری بین شرکای فدرال، ایالتی، بین‌المللی و بخش خصوصی است. از طریق این تلاش‌ها، جامعه واکنش به حوادث سایبری هم قابلیت‌ها و هم فرایندهای واکنش خود را بهبود و در نتیجه انعطاف‌پذیری سایبری را تقویت می‌کند.

بنابراین محقق در این پژوهش برای افزایش تأثیرگذاری اجرای رزمایش سایبری و شناسایی میزان اهمیت هر یک از دستاوردهای شناسایی شده در ارتقای رزمایش سایبری، به دنبال یک بررسی علمی در خصوص شناسایی و بررسی میزان اهمیت دستاوردهای کلان بر ارتقای رزمایش سایبری در بخش سیاست‌گذاری، نظارت و در بخش اجرا براساس منابع و تجربیات خارجی و خبرگی است تا با اجرای هرچه بهتر رزمایش سایبری، شاهد دفاع مؤثر و پیشگیرانه در جهت حفاظت از زیرساخت‌های حیاتی کشور باشیم، بنابراین مسئله اساسی در این تحقیق شناسایی دستاوردهای حاصل از تجربیات منتشر شده در رزمایش‌های سایبری در ایالات متحده است تا برای دفاع برای حفاظت از زیرساخت‌های حیاتی کشور مورد استفاده قرار گیرد.

در اهمیت پژوهش حاضر می‌توان گفت که یکی از مهم‌ترین اقداماتی که در چند سال اخیر به منظور ایمن‌سازی و پیش‌گیری از حملات سایبری توسط نهادهای حاکمیتی از جمله سازمان پدافند غیرعامل کشور دنبال می‌گردد، موضوع اجرای رزمایش پدافند سایبری در

زیرساخت‌های حیاتی کشور است که با توجه به اهمیت این‌گونه رزمایش‌ها در سطح زیرساخت‌های حیاتی کشور، شناخت دستاوردهای سایر رزمایش‌های مهم دنیا به سیاست‌گذاران و بازیگران عملیاتی امکان طرح‌ریزی هدفمند و جهت‌دهی رزمایش به سمت نتایج بزرگ و قابل توجه را ایجاد می‌کند.

آنچه مسلم است شناسایی و رسیدن به کلان دستاوردهای رزمایش سایبری در یک مدت کوتاه قابل انجام نیست و نیاز به برنامه‌ریزی بلندمدت و استمرار در اقدامات اجرایی و شناخت هرچه دقیق‌تر تجربیات و دستاوردهای رزمایش سایبری در دنیا دارد؛ ازاین‌رو در پژوهش حاضر به معرفی دستاوردهای برگزاری رزمایش طوفان سایبری ایالات متحده و دستاوردهای کلان حاصل از اجرای آن با هدف تعیین دستاوردهای کلان مورد انتظار اجرای رزمایش سایبری در زیرساخت‌های حیاتی پرداخته می‌شود.

۱. پیشینه پژوهش

براساس نتایج مطالعات، 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 ضمن کلی بودن دسته‌بندی‌ها و عدم تعیین شاخص از یک‌سو و عدم تفکیک انواع رزمایش سایبری با تمرکز بر یک نوع خاص، به معرفی دستاوردهای برگزاری رزمایش سایبری پرداخته است.

قاطعی درگاهی (۱۴۰۳) در پژوهش خود با معرفی رزمایش سایبری اقدام به احصای عوامل ساختاری مؤثر بر ارتقای رزمایش سایبری براساس برخی تجربیات منتشرشده دنیا در اجرای رزمایش سایبری پرداخته است و با انجام پژوهش آماری عوامل شناسایی‌شده خود را ارزش‌گذاری نموده است که برخی از آن‌ها به‌صورت محدود در قالب دستاوردهای اجرای رزمایش سایبری جای می‌گیرند.



سکر و دیگران (۲۰۱۸) در پژوهش خود به چرخه اجرای رزمایش سایبری و اقداماتی که در هر مرحله صورت می‌پذیرد اشاره کرده است؛ براساس چرخه ارائه شده در پژوهش ایشان، چرخه اجرای رزمایش سایبری شامل چهار مرحله شناسایی، برنامه‌ریزی، هدایت و ارزیابی می‌گردد. در این پژوهش شاخص‌سازی و تعیین نقش هر عامل در اجرای یک رزمایش سایبری به‌عنوان دستاورد هدف‌گذاری 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 ایالات متحده آمریکا پرداخته است نگاه موردی به دستاورد اجرای رزمایش آن هم محدود به ارتش ایالات متحده آمریکا به‌عنوان هدف پژوهش مذکور مطرح است.

موحدی راد و دیگران (۱۳۹۳) در پژوهش خود به تعاریف و مقایسه انواع رزمایش سایبری براساس 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 و در خصوص مطالعه دستاوردهای برگزاری رزمایش سایبری مطلبی اشاره نشده است. با توجه به اهمیت موضوع، مطالعات متعدد و مختلفی در ارتباط با پژوهش موردنظر انجام شده است که در جدول (۱) به تعدادی از آن‌ها به همراه نتایج آن اشاره شده است.

جدول ۱: مقایسه فعالیت‌های پژوهشی گذشته در خصوص رزمایش سایبری

عنوان	نویسندگان	سال	ویژگی‌های برجسته پژوهش
رزمایش دفاع سایبری	جورجیانا سوباسو، لیویا روسو، ویکتور والریا	۲۰۱۷	رویکردهای آموزشی تعیین چرخه رزمایش سایبری
بررسی عوامل ساختاری مؤثر بر ارتقای رزمایش سایبری	فرهاد قاطعی درگاهی	۱۴۰۳	معرفی عوامل ساختاری مؤثر تجزیه و تحلیل به روش آماری
مفهوم تمرینات دفاع سایبری	انصار سکر	۲۰۱۸	بررسی چرخه اجرای رزمایش سایبری و اقدامات هر مرحله

عنوان	نویسندگان	سال	ویژگی های برجسته پژوهش
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. مفهوم شناسی پژوهش

۲-۱. رزمایش سایبری

تمرین میدانی (با به کارگیری تجهیزات) یا ستادی (دور میزی) است که براساس سناریوهای احتمالی شبیه سازی و با روش های گوناگون اجرا می گردد و باعث کشف آسیب پذیری و ارتقای آمادگی های دستگاهی و انفرادی و ارزیابی کار آیی اقدامات برای مقابله با تهدیدات می شود (وزارت امنیت داخلی ایالات متحده، ۲۰۰۶: ۱).

۲-۲. اهداف رزمایش سایبری

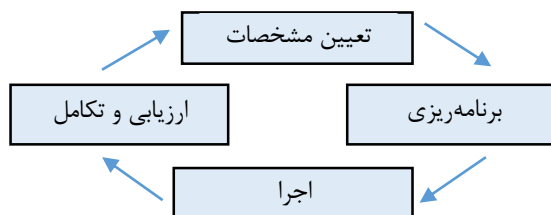
ارزیابی آمادگی دستگاه های اجرایی در برابر حوادث، تهدیدات و اقدامات خصمانه سایبری دشمن در راستای ارتقای پایداری، تاب آوری و تداوم کارکردهای ضروری کشور و صیانت از مردم با تأکید بر اجرای رزمایش های سایبری (مصوبه کمیته پدافند غیرعامل کشور در خصوص نظام آمادگی و رزمایش دستگاه های اجرایی در برابر تهدیدات، ۱۳۹۹: ۳).

۲-۳. چرخه حیات رزمایش سایبری

برنامه ریزی و اجرای کارآمد یک رزمایش اهدافی چالش برانگیز 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 درعین حال حساسیت های سازمان ها 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 داده شده است (موحدی راد و دیگران، ۱۳۹۳: ۹).



شکل ۱: چرخه حیات رزمایش سایبری

۲-۴. تعیین مشخصات رزمایش

در این بخش «سازمان‌دهنده»^۱ 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. براساس این نیاز برنامه‌ریز می‌تواند نوع رزمایش و سازمان‌های شرکت‌کننده را انتخاب کند.

۲-۵. 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 وسایل آموزشی رزمایش، انتخاب ناظران و سایر نقش‌ها و تعیین چگونگی انجام وظایف آن‌ها می‌شود.

۲-۶. اجرای رزمایش

در این بخش خود رزمایش اجرا می‌شود. طبق آنچه در فرایند برنامه‌ریزی مشخص شده 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.

1. Organizer

۲-۷. ارزیابی و تکامل رزمایش

در نهایت پس از اجرای رزمایش فرایند ارزیابی انجام می‌شود. این فرایند معمولاً شامل یک گزارش ارزیابی نهایی، یا چندین گزارش تهیه شده 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.

۳. مقایسه رزمایش‌های سایبری و فیزیکی

طراحان رزمایش معمولاً بین رویدادها و اهداف تمایز قائل می‌شوند. اهداف رزمایش، هدف از برگزاری رزمایش را مشخص می‌کند. رویدادهای رزمایش، چیزی است که در رزمایش اتفاق می‌افتد، به خصوص رویدادهای تهدیدآمیز (حوادث) و تأثیرات به وجود آمده از این رویدادها (پیامدها). در جدول زیر ترکیب‌های مختلف حوادث و پیامدهای سایبری و فیزیکی آورده شده است.

جدول ۱: مقایسه رزمایش‌های سایبری و فیزیکی

مثال	ترکیب‌ها
بلایای طبیعی منجر به خسارات فیزیکی قابل توجهی می‌شوند	حادثه فیزیکی با پیامد فیزیکی
آتش‌سوزی گسترده منجر به از بین رفتن سیستم‌های ارتباطی و اتصال به شبکه می‌شود	حادثه فیزیکی با پیامد سایبری
حمله سایبری به مرکز کنترل نظارتی و اکتساب داده‌ها منجر به اختلال گسترده در نیروی برق می‌شود	حادثه سایبری با پیامد فیزیکی
بدافزار جاسازی شده، یک حمله گسترده شبکه روباتی علیه قابلیت‌های تجارت الکترونیک مؤسسات صورت می‌دهد	حادثه سایبری با پیامد سایبری



۳-۱. سطوح رزمایش سایبری

رزمایش فراملی: رزمایشی که به صورت مشترک بین دو یا چند کشور براساس توافقنامه‌ها یا پیمان‌های بین‌المللی و منطقه‌های برای ارزیابی آمادگی و مهارت‌های راهبردی و ارتقای هماهنگی با دیگر کشورها انجام می‌شود.

رزمایش ملی: سطحی از رزمایش است که برای ارزیابی و ارتقای سطح آمادگی و مهارت‌های راهبردی و عملیاتی بین چندین دستگاه و چند استان در موضوعات مشترک برای مقابله با حوادث و تهدیدات اجرا می‌گردد.

رزمایش منطقه‌ای: سطحی از رزمایش است که برای ارزیابی و ارتقای سطح آمادگی و مهارت‌های راهبردی، عملیاتی و تاکتیکی در حداکثر ۵ استان در موضوعات مشترک برای مقابله با حوادث و تهدیدات اجرا می‌گردد.

رزمایش استانی: سطحی از رزمایش است که برای ارزیابی و ارتقای سطح آمادگی و مهارت‌های راهبردی، عملیاتی و تاکتیکی در یک استان در موضوعات مختلف برای مقابله با حوادث و تهدیدات اجرا می‌گردد.

رزمایش محلی: سطحی از رزمایش است که برای ارزیابی و ارتقای سطح آمادگی و مهارت‌های عملیاتی و تاکتیکی یک شهرستان در موضوعات مختلف برای مقابله با حوادث و تهدیدات اجرا می‌گردد.

رزمایش دستگاهی: سطحی از رزمایش است که برای ارزیابی و ارتقای سطح آمادگی و مهارت‌های راهبردی و عملیاتی در یک دستگاه برای مقابله با حوادث و تهدیدات اجرا می‌گردد.

۴. وزارت امنیت داخلی ایالات متحده^۱

وزارت امنیت داخلی ایالات متحده یک اداره اجرایی فدرال ایالات متحده است که مسئولیت امنیت عمومی را بر عهده دارد که تقریباً با وزارتخانه‌های کشور یا کشور سایر کشورها

1. U.S. Department of Homeland Security (DHS)

قابل مقایسه است. مأموریت‌های اعلام شده آن شامل مبارزه با تروریسم، امنیت مرزی، مهاجرت و گمرک، امنیت سایبری و پیشگیری و مدیریت بلایا است. این سازمان در سال ۲۰۰۳ فعالیت خود را آغاز کرد که در نتیجه قانون امنیت داخلی سال ۲۰۰۲ که در پاسخ به حملات ۱۱ سپتامبر تصویب شد، شکل گرفت. این سازمان با بیش از ۲۶۰۰۰۰ کارمند، ۲۲ اداره و آژانس مختلف فدرال را در یک آژانس ادغام کرد و سومین بخش بزرگ کابینه پس از وزارت دفاع و امور کهنه سربازان در ایالات متحده است. سیاست امنیت داخلی در کاخ سفید توسط شورای امنیت داخلی هماهنگ می‌شود. وظایف این سازمان طیف گسترده‌ای از حمل و نقل هوایی و امنیت مرزی گرفته تا واکنش اضطراری، از تحلیلگر امنیت سایبری تا بازرس تأسیسات شیمیایی را شامل می‌شود (وزارت امنیت داخلی ایالات متحده، ۲۰۲۳).

۴-۱. عمده مأموریت‌های وزارت امنیت داخلی ایالات متحده

مأموریت‌های این سازمان در بخش سایبری در قالب «آژانس امنیت سایبری و امنیت زیرساخت»^۱ دنبال می‌گردد. این آژانس با شرکای خود برای دفاع در برابر تهدیدات امروزی و همکاری برای ایجاد زیرساخت ایمن‌تر و انعطاف‌پذیرتر برای آینده ایالات متحده همکاری می‌کند. در واقع، یک رهبر عملیاتی برای امنیت سایبری فدرال و هماهنگ‌کننده ملی برای امنیت زیرساخت‌های حیاتی باهدف ایجاد یک زیرساخت حیاتی امن و قابل انعطاف برای مردم آمریکا در حوزه سایبری، محسوب می‌گردد (آژانس امنیت سایبری و امنیت زیرساخت، ۲۰۲۳).

۴-۱-۱. رزمایش طوفان سایبری^۲

مهم‌ترین رزمایش سایبری در ایالات متحده رزمایش طوفان سایبری است؛ این رزمایش یک رزمایش شبیه‌سازی شده دوسالانه است که توسط وزارت امنیت داخلی ایالات متحده نظارت می‌شود که اولین بار از ۶ فوریه تا ۱۰ فوریه ۲۰۰۶ باهدف آزمایش قدرت دفاعی کشور در

1. Cybersecurity and Infrastructure Security Agency (CISA)

2. Cyber Storm



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).

مجموعه رزمایش‌های دوسالانه وزارت امنیت داخلی ایالات متحده با مسئولیت آژانس امنیت سایبری و امنیت زیرساخت، چهارچوبی را برای گسترده‌ترین رزمایش امنیت سایبری تحت حمایت دولت در نوع خود را فراهم می‌کند. مجموعه رزمایش‌ها، بخش‌های دولتی و خصوصی را برای شبیه‌سازی کشف و پاسخ به یک حادثه سایبری مهم که بر زیرساخت‌های حیاتی کشور تأثیر می‌گذارد، گرد هم می‌آورد. رزمایش‌های طوفان سایبری بخشی از تلاش‌های مداوم وزارت امنیت داخلی ایالات متحده برای ارزیابی و تقویت آمادگی سایبری و بررسی فرایندهای واکنش به حادثه است.

۴-۱-۲. عمده فعالیت‌های شرکت‌کنندگان در رزمایش طوفان سایبری

- ❖ بررسی توانایی سازمان‌ها برای آماده شدن، محافظت و پاسخ به اثرات احتمالی حملات سایبری؛
- ❖ اعمال تصمیم‌گیری استراتژیک و هماهنگی بین سازمانی واکنش (های) حادثه مطابق با سیاست‌ها و رویه‌های سطح ملی؛
- ❖ اعتبار روابط اشتراک‌گذاری اطلاعات و مسیرهای ارتباطی برای جمع‌آوری و انتشار آگاهی، واکنش و اطلاعات بازبازی رویدادهای سایبری؛
- ❖ بررسی ابزارها و فرایندهایی که از طریق آن‌ها اطلاعات حساس در سراسر مرزها و بخش‌ها بدون به خطر انداختن منافع اختصاصی یا امنیت ملی، به اشتراک گذاشته شود.

هر رزمایش طوفان سایبری بر درس‌های آموخته‌شده از حوادث قبلی در دنیای واقعی استوار است و تضمین می‌کند که شرکت‌کنندگان هر دو سال یک‌بار با رزمایش‌های پیچیده‌تر

و چالش برانگیزتری روبه‌رو می‌شوند (رزمایش طوفان سایبری، آژانس امنیت سایبری و امنیت زیرساخت، ۲۰۲۳).

۵. روش‌شناسی پژوهش

پژوهش حاضر از نوع کیفی و با رویکردی اکتشافی بوده که به روش تحلیل محتوا انجام می‌شود. اصلی‌ترین کاربرد تحلیل محتوا، فراهم آوردن امکان بررسی نکات تلویحی و نهفته پیام‌هاست؛ یعنی امکان مطالعه آنچه در پیام هست ولی در نگاه اول دیده نمی‌شود. تحلیل محتوا را پرسش‌نامه معکوس نیز نامیده‌اند؛ زیرا بیشتر بررسی‌های اجتماعی مبتنی بر پرسش‌نامه هستند؛ یعنی آنچه توسط محقق تحلیل می‌شود، داده‌هایی است که از پرسش‌نامه حاصل شده‌اند. در تحلیل محتوا درست عکس این شیوه عمل می‌شود. به این ترتیب که پاسخ‌ها جملگی مشخص و مضبوط هستند و هنر محقق در طرح پرسش‌نامه‌ای است متناسب با این پاسخ‌ها که امکان جمع‌بندی و تحلیل را فراهم آورد (رحیم سلمانی، ۱۳۹۱: ۴۰).

این شیوه بر استفاده از تحلیل داده‌ها از طریق کدگذاری (واحد متن، واحد نمونه‌گیری و واحد تحلیل) که نقش کلیدی در نتیجه‌گیری ایفا می‌کند، تأکید دارد. کدگذاری شامل سازمان‌دهی واحدهای معانی در طبقات از پیش تعریف‌شده است. هر چه طبقات مفهومی‌تر باشند، برای حصول اطمینان از کدگذاری صحیح می‌بایست قوانین کدگذاری واضح‌تر تعریف گردند.

در این روش، در مرحله اول متونی که به دنبال تحلیل آن‌ها هستیم، شناسایی و انتخاب می‌شوند. سپس براساس مجموعه طبقات و واحد معانی که قرار است کدگذاری شوند، سطح تحلیل متون انتخابی مشخص می‌گردد. در مرحله بعد کدگذاری و سازمان‌دهی واحدهای معانی در طبقات از پیش تعریف‌شده، صورت می‌پذیرد و کدگذاری توسعه می‌یابد. در ادامه با مرور متون، تمامی داده‌های مرتبط در طبقات مناسب کدگذاری ثبت می‌شوند و در مرحله پایانی هنگامی که کدگذاری کامل شد، برای پاسخ به سؤال تحقیق، داده‌های جمع‌آوری‌شده جهت یافتن الگو و نتیجه‌گیری تحلیل می‌گردند.



در تحلیل محتوا، دو دسته واحد داریم: واحدهای محتوا و واحدهای پژوهش. واحدهای محتوا عناصری هستند که به طور خاص به معنی و تولید محتوا مربوط می‌شوند و بیانگر عناصری هستند که به طور مستقل از پژوهش و اغلب به وسیله تولیدکننده محتوا تعریف می‌شوند. منظور از واحدهای پژوهش، واحدهایی هستند که برای انجام یک پژوهش از نوع تحلیل محتوا می‌بایستی مشخص شوند. این واحدها اجزایی از محتوا هستند که از سوی پژوهشگر انتخاب و تعریف می‌شوند.

در شکل (۲)، مراحل تجزیه و تحلیل داده‌های پژوهش براساس روش تحلیل محتوا نشان داده است.



شکل ۲: مراحل تجزیه و تحلیل داده‌ها مبتنی بر تحلیل محتوا

در این پژوهش تجربیات منتشرشده وزارت امنیت داخلی ایالات متحده در اجرای رزمایش طوفان سایبری مورد تجزیه و تحلیل قرار گرفت و بازه زمانی منتهی به سال ۱۴۰۳ هجری شمسی با توجه به برخی تجربیات منتشرشده وزارت امنیت داخلی ایالات متحده در اجرای رزمایش طوفان سایبری به عنوان قلمرو زمانی در این تحقیق تعیین می‌گردد.

۵-۱. شرح علائم اختصاری

ذکر چند نکته پیرامون علائم اختصاری استفاده شده در تحلیل محتواهای مورد بررسی ضروری است:

- ❖ CS (برگرفته از Cyber Storm): بیانگر رزمایش طوفان سایبری است؛
- ❖ I, II, III, ...: مشخص کننده هریک از محتواهای منتشر شده وزارت امنیت داخلی ایالات متحده است؛
- ❖ A: نشان دهنده «دستاوردهای کلیدی رزمایش» است؛
- ❖ 1,2,3: بیان گر شماره نکته کلیدی است، به طور مثال CS-VI-A4 نشان گر دستاورد کلیدی چهارم از محتوای VI (شماره پنجم) محتواهای منتشر شده وزارت امنیت داخلی ایالات متحده از رزمایش طوفان سایبری است.

۶. تجزیه و تحلیل یافته ها

داده ها به عنوان اطلاعات پردازش نشده، ابتدایی ترین پاسخ های احتمالی هر پژوهشگر در رابطه با مسئله تحقیق است. پژوهشگر پس از دستیابی به این داده ها، با توجه به روش تحقیق و نوع متغیرها، مناسب ترین آزمون آماری را برمی گزیند تا بتواند استنتاج ها و نتیجه گیری های معتبر و دقیق را به عمل آورد؛ همان گونه که اشاره شد، در این پژوهش با اتکا به روش تحلیل محتوا، دستاوردهای کلیدی رزمایش طوفان سایبری ایالات متحده در سه رویه کدگذاری باز، محوری و انتخابی، شناسایی و استخراج شده است. دستاوردها مشتمل بر ۷۰ مورد شناسایی گردید که پس از انجام فرایند خلاصه سازی و یکپارچه سازی مشترکات، ۱۲ مورد به عنوان دستاوردهای برگزاری رزمایش سایبری معرفی شد. در تحلیل نهایی، کلان دستاوردهای پژوهش با رنگ های متفاوت مشخص و آمار فراوانی هر کدام، در قالب یک جدول مشخص شده است.

در ادامه نتایج حاصل از بررسی رزمایش طوفان سایبری که توسط وزارت امنیت داخلی ایالات متحده برگزار شده قابل مشاهده است.

۶-۱. رزمایش سایبری Cyber Storm I

در فوریه ۲۰۰۶، وزارت امنیت داخلی، Cyber Storm I را به عنوان یک رزمایش امنیت سایبری سرتاسری که قابلیت های واکنش را در طول یک حادثه سایبری با اهمیت ملی ارزیابی می کرد،



اجرا نمود. طوفان سایبری I اولین رزمایش سایبری تحت حمایت DHS بود که پاسخ را در بخش خصوصی و دولت‌های بین‌المللی، فدرال و ایالتی آزمایش کرد.

۶-۱-۱. اهداف رزمایش

- ❖ انجام هماهنگی بین سازمانی مانند رویه‌های عملیاتی استاندارد، ارتباطات و مکانیسم‌های پشتیبانی تصمیم از طریق فعال‌سازی «گروه ملی هماهنگی و پاسخ سایبری»^۱ و «گروه مدیریت حوادث بین سازمانی»^۲؛
- ❖ تمرین هماهنگی بین دولتی (بین‌المللی) و درون دولتی (فدرال-ایالتی) و واکنش به حوادث؛
- ❖ شناسایی خط‌مشی‌ها و مسائلی که الزامات امنیت سایبری را مختل یا پشتیبانی می‌کنند؛
- ❖ شناسایی ارتباطات عمومی و خصوصی و آستانه هماهنگی برای بهبود واکنش و بازیابی حوادث سایبری و همچنین شناسایی مسیرها و مکانیسم‌های اشتراک‌گذاری اطلاعات حیاتی؛
- ❖ شناسایی، بهبود و ترویج تعامل بخش عمومی و خصوصی در فرایندها و رویه‌ها برای انتقال اطلاعات مناسب به سهامداران کلیدی و مردم؛
- ❖ شناسایی وابستگی متقابل فیزیکی و سایبری زیرساخت‌ها با تأثیرات اقتصادی و سیاسی در دنیای واقعی؛
- ❖ افزایش آگاهی از تأثیرات اقتصادی و امنیت ملی مرتبط با یک حادثه سایبری؛
- ❖ برجسته‌سازی ابزارها و فناوری موجود با واکنش تحلیلی به حوادث سایبری.

۶-۱-۲. سناریوهای رزمایش

- ❖ حملات سایبری که عناصر زیرساخت انرژی و حمل‌ونقل را مختل می‌کند؛

1. National Cyber Response Coordination Group (NCRCG)
2. Interagency Incident Management Group (IIMG)

- ❖ حملات سایبری که دولت‌های فدرال، ایالتی و بین‌المللی را باهدف ایجاد اختلال در عملیات دولت و تضعیف اعتماد عمومی هدف قرار می‌دهند؛
- ❖ شناسایی و استفاده بهینه از کلیه کانال‌های ارتباطی؛
- ❖ تشدید مجموعه‌ای از حوادث مرتبط به هم که درمجموع، تهدیدی قابل‌توجه برای راه‌اندازی و عملیات «گروه ملی هماهنگی و پاسخ سایبری»^۱ NCRCG است؛
- ❖ راه‌اندازی و عملکرد «گروه مدیریت حوادث بین سازمانی»^۲ در حین آزمایش رابطه ارتباطی بین NCRCG و IIMG؛
- ❖ هماهنگی مداوم همه شرکت‌کنندگان عمومی و خصوصی از طریق برنامه‌ریزی و فعالیت‌های بازیابی؛
- رزمایش طوفان سایبری یک نقطه عطف مهم در واکنش به حوادث سایبری ملی و بین‌المللی و همچنین در راستای منافع مشارکت عمومی و خصوصی در حفاظت از زیرساخت‌های حیاتی فیزیکی و مرتبط با سایبری بود.

۳-۱-۶. دستاوردهای کلیدی رزمایش

جدول ۲: دستاوردهای کلیدی رزمایش طوفان سایبری I

عنوان	شناسه
بزرگ‌ترین، پیچیده‌ترین رزمایش سایبری چندملیتی، فرابخشی که تا سال ۲۰۰۶ اجرا شده است	CS-I-A1
سازمان‌دهی هم‌زمان سازمان‌های واکنش سایبری بیش از ۱۰۰ سازمان، انجمن و شرکت دولتی و خصوصی در بیش از ۶۰ مکان و پنج کشور	CS-I-A2
همکاری چندملیتی در واکنش به بحران در سطوح عملیاتی، سیاستی و امور عمومی	CS-I-A3
مشارکت مستقیم و گسترده بیش از ۳۰ شرکت و انجمن بخش خصوصی در برنامه‌ریزی، اجرا و تجزیه و تحلیل پس از اقدام رزمایش	CS-I-A4

1. National Cyber Response Coordination Group (NCRCG)

2. Interagency Incident Management Group (IIMG)



شناسه	عنوان
CS-I-A5	دستیابی به همکاری بی سابقه و به اشتراک گذاری اطلاعات در میان آژانس های فدرال از جمله اطلاعات، نظامی و غیرنظامی فراتر از مرزهای بخش خصوصی و دولت و در بین شرکای بین المللی
CS-I-A6	آزمایش طیف کاملی از سیاست ها، دکترین و روش های ارتباطی واکنش سایبری که در یک بحران دنیای واقعی مورد نیاز است
CS-I-A7	بررسی خط مشی ها و رویه های آزمایش شده مرتبط با یک رویداد سایبری با اهمیت ملی
CS-I-A8	ایجاد روابط عمومی و خصوصی متعدد که در آماده سازی آینده و پاسخ به حوادث سایبری بین بخشی ارزشمند خواهد بود
CS-I-A9	شناسایی مسائل بازایی که مستلزم بررسی بیشتر از طریق همکاری بین بخش دولتی و خصوصی است

منبع: (وزارت امنیت داخلی ایالات متحده، گزارش رزمایش طوفان سایبری ۱، ۲۰۰۶)

۲-۶. رزمایش سایبری Cyber Storm II

رزمایش طوفان سایبری II در ۱۰ تا ۱۴ مارس ۲۰۰۸ در سراسر ایالات متحده و همچنین در موقعیت شرکای بین المللی در استرالیا، کانادا، نیوزیلند و بریتانیا اجرا شد.

۲-۶-۱. اهداف رزمایش

- ❖ بررسی قابلیت های سازمان های شرکت کننده برای آماده سازی، محافظت و پاسخ به اثرات حملات سایبری؛
- ❖ اعمال تصمیم گیری با محوریت رهبری ارشد و هماهنگی بین سازمانی در واکنش به حوادث مطابق با خط مشی ها و رویه های سطح ملی؛
- ❖ ارزیابی روابط اشتراک گذاری اطلاعات و مسیرهای ارتباطی برای جمع آوری و انتشار آگاهی وضعیت، واکنش و اطلاعات بازایی حوادث سایبری؛
- ❖ بررسی ابزارها و فرایندهای به اشتراک گذاری که اطلاعات حساس و طبقه بندی شده را در سراسر مرزهای استاندارد، می بایست به روش های ایمن و مطمئن بدون به خطر انداختن منافع اختصاصی یا امنیت ملی به اشتراک گذارند؛

۶-۲-۲. سناریوهای رزمایش

سناریوی این رزمایش حول مجموعه‌ای از بردارهای حمله سایبری ساخته شد که در محدوده قابلیت‌های فنی مجموعه دشمن قرار داشتند. گه‌گاه قابلیت‌های ویژه‌ای به حریف مناسب اضافه می‌شد که با برنامه‌ریزی برای پرداختن به اهداف خاص شرکت‌کننده پیش می‌رفت. در این رزمایش حملات شبیه‌سازی شده به اندازه‌ای شدید بودند که شرکت‌کنندگان باید به فراتر از منابعی که مستقیماً کنترل می‌کنند دست یابند و با سایر اعضای بخش خود، دولت‌های ایالتی و فدرال و همچنین شرکا و متحدان خود در سراسر جهان همکاری کنند. سناریوی طوفان سایبری ۲ توسط دشمنان سرسخت و ساختگی با دستور کار سیاسی و اقتصادی مشخص اجرا شد. دشمن Cyber Storm II از بردارهای حمله پیچیده برای ایجاد یک حادثه در مقیاس بزرگ استفاده کرد که بازیکنان را ملزم به تمرکز بر روی پاسخ می‌کرد. برنامه‌ریزان این سناریو را طی یک فرایند برنامه‌ریزی ۱۸ ماهه توسعه دادند که در طی آن برنامه‌ریزان به‌طور منظم چه به‌صورت حضوری و چه به‌صورت مجازی تعامل داشتند.

۶-۲-۳. دستاوردهای کلیدی رزمایش

جدول ۳: دستاوردهای کلیدی رزمایش طوفان سایبری II

عنوان	شناسه
بهبود «رویه‌های عملیاتی استاندارد» ^۱ و روابط ایجاد شده با هدف تسهیل اشتراک‌گذاری سریع اطلاعات در میان اعضای جامعه	CS-II-A1
شناسایی وابستگی‌های متقابل فیزیکی و سایبری	CS-II-A2
احصای اهمیت ابزارهای ارتباطی بحران قابل اعتماد و آزمایش شده و نیازمندی‌های اصلاح و ارتقا	CS-II-A3
روشن شدن نقش‌ها و مسئولیت‌ها و بهبود فرایندهای ادغام و هماهنگی پاسخ رویدادهای سایبری با رهبری ارشد در سراسر مرزهای بین سازمانی	CS-II-A4
افزایش تعامل بدون بحران در جامعه واکنش سایبری از طریق ابزارهای تعیین شده	CS-II-A5

منبع: (وزارت امنیت داخلی ایالات متحده، گزارش نهایی طوفان سایبری ۲، ۲۰۰۹)



۳-۶. رزمایش سایبری Cyber Storm III

رزمایش سایبری طوفان سایبری ۳ از ۲۷ سپتامبر تا ۱ اکتبر ۲۰۱۰ برگزار گردید و شامل مشارکت ۸ بخش در سطح کابینه، ۱۳ ایالت، ۱۲ شریک بین‌المللی و تقریباً ۶۰ شرکت بخش خصوصی و نهادهای هماهنگ‌کننده بود. مشارکت بر روی بخش‌های زیرساخت‌های حیاتی فناوری اطلاعات، ارتباطات، انرژی (برق)، شیمیایی و حمل‌ونقل متمرکز شد و سطوح مختلف بازی از دیگر بخش‌های زیرساخت حیاتی را در بر گرفت. این نهادها باهم در طراحی، اجرا و تجزیه و تحلیل پس از رزمایش بزرگ‌ترین، جامع‌ترین رزمایش سایبری در مقیاس کامل تحت رهبری دولت، شرکت کردند و شرکت‌کنندگان این رزمایش را با موفقیت در سراسر ایالات متحده و در سطح بین‌المللی با مرکزیت اصلی «کنترل رزمایش»^۱ واقع در دفتر مرکزی «سرویس مخفی ایالات متحده»^۲ در واشنگتن دی. سی، اجرا کردند.

۳-۶-۱. اهداف رزمایش

- ❖ اعمال و فعال کردن برنامه‌ها، قابلیت‌ها و رویه‌های لازم برای تضمین امنیت زیرساخت‌های سایبری گسترده و وابسته به یکدیگر؛
- ❖ استفاده از تلاش‌ها، ابتکارات، منابع و یافته‌های گذشته و حال؛
- ❖ تمرین فرایندهای «طرح ملی واکنش به حوادث سایبری»^۳؛
- ❖ بررسی نقش DHS را در یک رویداد سایبری؛
- ❖ تمرکز بر مسائل اشتراک‌گذاری اطلاعات مانند الزامات، وضعیت اطلاعات-سطوح هشدار، نقش‌ها و مسئولیت‌های پاسخ؛
- ❖ بررسی رویه‌ها و مکانیسم‌های هماهنگی و تصمیم‌گیری در سراسر حوزه انتخابی شامل فدرال، ایالتی، بخش خصوصی و بین‌المللی؛

1. Exercise Control (ExCon)

2. U.S. Secret Service (USSS)

3. The National Cyber Incident Response Plan (NCIRP)

❖ ارزیابی میدانی عناصر ابتکارات گذشته یا در حال انجام، یافته‌های رزمایش‌های گذشته و سایر تلاش‌های مرتبط با امنیت سایبری.

۶-۳-۲. سناریوهای رزمایش

در طول CS III، بازیکنان به مجموعه‌ای از حملات شبیه‌سازی شده و هدفمند ناشی از به خطر افتادن «سیستم نام دامنه»^۱ و زنجیره اعتماد اینترنتی یعنی اعتبار گواهی‌ها و مقامات گواهی^۲ [CAs] پاسخ دادند. به دلیل اتکا به DNS و زنجیره اعتماد برای طیف گسترده‌ای از توابع، تراکنش‌ها و ارتباطات اینترنتی، دشمن توانایی بازیکنان را برای کار در یک محیط قابل اعتماد، تکمیل تراکنش‌های قابل اعتماد و پشتیبانی از عملکردهای حیاتی به چالش می‌کشد. علاوه بر این، دشمن از این مصالحه‌ها برای انجام انواع حملات هدفمند علیه شرکت‌های بخش خصوصی، بخش‌های حیاتی، شرکت‌های بخش عمومی و هم‌تایان بین‌المللی استفاده کرد.

۶-۳-۳. دستاوردهای کلیدی رزمایش

جدول ۴: دستاوردهای کلیدی رزمایش طوفان سایبری III

شناسه	عنوان
CS-III-A1	شتاب‌دهنده یادگیری جامعه واکنش به حوادث سایبری در تجزیه و تحلیل عملیاتی
CS-III-A2	ارزیابی کارایی طرح ملی واکنش به حوادث سایبری و شناسایی مناطقی که نیاز به اصلاح دارند
CS-III-A3	هدایت پاسخ به یک حادثه سایبری مهم با حمایت بین سازمانی، ایالت‌ها، بخش خصوصی و سازمان‌های بین‌المللی
CS-III-A4	ارزیابی عملکرد «مرکز ادغام امنیت سایبری و ارتباطات ملی» ^۳ در طی یک حادثه سایبری مهم و شناسایی مناطق قابل بهبود برای هماهنگی و ارتباطات این مرکز و شرکای آن
CS-III-A5	مشارکت قابل توجه رهبری ارشد در بخش‌های دولتی و خصوصی، که در تصمیم‌گیری‌های کلیدی کمک می‌کند

1. Domain Name System (DNS)

2. Certificate Authorities

3. National Cybersecurity and Communications Integration Center (NCCIC)



شناسه	عنوان
CS-III-A6	نمایش مزایای هماهنگی و تصمیم‌گیری سازمان‌یافته، کارآمد، منسجم، اقدام مدار و عمومی-خصوصی
CS-III-A7	شناسایی زمینه‌ها برای پاسخ‌گویی مؤثر به یک حادثه سایبری مهم با ادغام مشارکت‌کنندگان بخش خصوصی در عملیات، اشتراک‌گذاری اطلاعات و برنامه‌ریزی اقدام
CS-III-A8	تقویت مکانیسم‌های هماهنگی موجود و تسهیل روابط جدید در جامعه واکنش به حوادث سایبری در طول فرایند برنامه‌ریزی رزمایش
CS-III-A9	شناسایی و فهرست‌بندی نیازهای مربوط به آگاهی وضعیت، به اشتراک‌گذاری اطلاعات و پیام‌رسانی مداوم در سراسر جامعه واکنش به حوادث سایبری

منبع: (وزارت امنیت داخلی ایالات متحده، گزارش نهایی طوفان سایبری ۳، ۲۰۱۱).

۴-۶. رزمایش سایبری Cyber Storm IV

طوفان سایبری IV چهارمین قسمت از مجموعه رزمایش‌های طوفان سایبری بود که بخشی از تلاش‌های مداوم وزارت امنیت داخلی برای ارزیابی و تقویت آمادگی سایبری، بررسی فرایندهای واکنش به حادثه در پاسخ به تهدیدات در حال تکامل و افزایش اطلاعات اشتراک‌گذاری بین شرکای فدرال، ایالتی، بین‌المللی و بخش خصوصی است.

۴-۶-۱. اهداف رزمایش

❖ شناسایی، بهبود، اعمال و تقویت فرایندها، رویه‌ها، تعاملات و مکانیسم‌های اشتراک‌گذاری اطلاعاتی که تحت پیش‌نویس طرح ملی واکنش به حوادث سایبری وجود دارد یا باید وجود داشته باشد؛

❖ بررسی نقش DHS و اجزای مرتبط با آن را در طول یک رویداد سایبری جهانی؛

❖ اجرای مکانیسم‌های هماهنگی، تلاش‌های به اشتراک‌گذاری اطلاعات، توسعه آگاهی موقعیتی مشترک و رویه‌های تصمیم‌گیری جامعه امنیت سایبری (فدرال، ایالتی، بخش خصوصی و بین‌المللی) در طول رویدادهای سایبری؛

❖ حفظ آگاهی از سایر ابتکارات رزمایش سایبری.

۶-۴-۲. سناریوهای رزمایش

سری رزمایش‌های CS IV شامل مشارکت از سراسر جوامع سنتی ذی‌نفع از جمله: ادارات و آژانس‌های فدرال، دولت‌های «ایالتی، محلی، طایفه‌ای و سرزمینی»^۱ نهادهای هماهنگی، بخش خصوصی و شرکای بین‌المللی بود. این رزمایش متشکل از ۱۵ رویداد جداگانه بود که بین نوامبر ۲۰۱۱ و ژانویه ۲۰۱۴ انجام شد، رویدادهای رزمایش‌های CS IV از سمینارهای مقیاس کوچک گرفته تا «رزمایش‌های روی میز»^۲ متمرکز بر پاسخ در سطح ایالت تا رزمایش‌های مبتنی بر عملیات در مقیاس بزرگ را شامل می‌شد.

۶-۴-۳. دستاوردهای کلیدی رزمایش

جدول ۵: دستاوردهای کلیدی رزمایش طوفان سایبری IV

شناسه	عنوان
CS-IV-A1	ارزیابی قابلیت‌های واکنش به حوادث سایبری با ایجاد یک انجمن برای کشورهای شرکت‌کننده، سازمان‌های دولتی، شرکای بین‌المللی و سایر سازمان‌ها و افراد
CS-IV-A2	بررسی گروه‌های ذی‌نفع خاص، مانند افراد و مراکز سایبری مجاز
CS-IV-A3	ارزیابی رویه‌های تخصیص منابع و مقامات واکنش اضطراری فدرال در طول یک رویداد سایبری بزرگ با تشدید یک حادثه از سطح محلی به فدرال و شناسایی مسائل مربوط به تشدید اضطراری مخاطرات سایبری
CS-IV-A4	ارتقای آگاهی سایبری و قابلیت‌های نسبی کشورهایی با مشارکت کم یا بدون مشارکت و ادغام این کشورها در برنامه‌ریزی رزمایش‌های آینده
CS-IV-A5	افزایش آگاهی از منابع فدرال و دیگر منابع موجود برای هماهنگی، پاسخ‌گویی و کاهش اثرات حوادث سایبری
CS-IV-A6	قرار گرفتن در معرض رزمایش‌های واکنش سایبری و آموزش برای طیف گسترده‌ای از ذینفعان در سطح ملی و بین‌المللی
CS-IV-A7	تعیین پروتکل‌ها و طرح‌های واکنش سایبری در برابر تشدید شبیه‌سازی‌شده یک حادثه سایبری همراه با شناسایی شکاف‌ها در ارتباطات، برنامه‌های واکنش و منابع مورد نیاز
CS-IV-A8	تسهیل توسعه روابط بلندمدت و بهبود مشارکت بین ذینفعان مرکز ادغام امنیت سایبری و ارتباطات ملی و رزمایش طوفان سایبری

منبع: (وزارت امنیت داخلی ایالات متحده، درس‌های آموخته‌شده از طوفان سایبری ۴، ۲۰۱۵)

1. State, Local, Tribal and Territorial (SLTT)
2. Tabletop exercise (TTX)



۵-۶. رزمایش سایبری Cyber Storm V

رزمایش CS V که در مارس ۲۰۱۶ اجرا گردید شامل بیش از ۱۲۰۰ شرکت‌کننده به‌عنوان نماینده نهادهای بخش دولتی و خصوصی در داخل ایالات متحده و خارج از کشور بود. شرکت‌کنندگان ۹ بخش در سطح کابینه، ۸ ایالت، ۱۲ شریک بین‌المللی و نزدیک به ۷۰ شرکت بخش خصوصی و سازمان هماهنگ‌کننده را نمایندگی کردند و مشارکت بر روی بخش‌های زیرساخت حیاتی «فناوری اطلاعات»^۱، ارتباطات، «مراقبت‌های بهداشتی و بهداشت عمومی»^۲ و تأسیسات تجاری (بخش خرده‌فروشی) متمرکز بود.

۵-۶-۱. اهداف رزمایش

- ❖ اعمال مکانیسم‌های هماهنگی، تلاش‌های به اشتراک‌گذاری اطلاعات، توسعه آگاهی موقعیتی مشترک و رویه‌های تصمیم‌گیری جامعه واکنش به حوادث سایبری در طول یک رویداد سایبری؛
- ❖ ارزیابی سیاست‌های مربوطه، مسائل قانونی و مالی که بر مقامات واکنش به حوادث سایبری و اولویت‌بندی منابع حاکم است؛
- ❖ ایجاد یک انجمن برای شرکت‌کنندگان در رزمایش برای تمرین، ارزیابی و بهبود فرایندها، رویه‌ها، تعاملات و مکانیسم‌های به اشتراک‌گذاری اطلاعات در سازمان یا جامعه موردعلاقه خود؛
- ❖ ارزیابی نقش، عملکردها و قابلیت‌های DHS و سایر نهادهای دولتی در یک رویداد سایبری.

۵-۶-۲. سناریوهای رزمایش

در این رزمایش بازیکنان به یک سناریوی سایبری خاص پاسخ دادند که از نقاط ضعف در پروتکل‌ها و سرویس‌های رایج مورد استفاده در اینترنت استفاده می‌کرد. این سناریو شامل

1. Information Technology (IT)
2. Healthcare and Public Health (HPH)

تأثیراتی بر روش شناسی مسیریابی، «سیستم نام دامنه»^۱ مورد استفاده برای نگاشت نام میزبان به آدرس های «پروتکل اینترنت»^۲ و «زیر ساخت کلید عمومی»^۳ مورد استفاده برای تأیید اعتبار و محرمانگی بود. شرایط سناریو طیف گسترده ای از سیستم های شرکتی و دولتی، دستگاه های پزشکی و سیستم های پرداخت را تحت تأثیر قرار داد. در طول بازی سناریو، بدافزار دارای نوعی ویژگی بود که سیستم های آلوده را هنگامی که بازیکنان در برابر IP های مخرب مسدود می کردند، مختل می کرد. این قطعنامه نیازمند واکنش هماهنگ دولت و بخش خصوصی بود.

۳-۵-۶. دستاوردهای کلیدی رزمایش

جدول ۶: دستاوردهای کلیدی رزمایش طوفان سایبری V

عنوان	شناسه
شتاب دهنده یادگیری جامعه واکنش به حوادث سایبری از طریق فرایند برنامه ریزی و اجرای رزمایش توسط شرکت کنندگان	CS-V-A1
واکنش به یک حادثه سایبری مهم با حمایت فدرال، ایالتی، بخش خصوصی و سازمان های بین المللی	CS-V-A2
ادغام دی نفعان جدید شامل دو بخش و هشت ایالت، قرار گرفتن آن ها در رزمایش های واکنش سایبری و ایجاد پایه ای برای رزمایش های آینده	CS-V-A3
فراهم کردن راهی برای نهادهای هماهنگ کننده، مانند «مراکز به اشتراک گذاری و تجزیه و تحلیل اطلاعات» ^۴ و «سازمان های به اشتراک گذاری و تجزیه و تحلیل اطلاعات» ^۵ برای آزمایش و اصلاح مکانیسم های هماهنگی خود و نشان دادن ارزش مشارکت یا عضویت	CS-V-A4
فراهم شدن فرصتی تا سازمان های بخش خصوصی از شرایط سناریو رزمایش برای همکاری و توسعه طیف وسیعی از راه حل های بالقوه استفاده کنند و در مورد آن با هم تیان دولتی خود بحث کنند	CS-V-A5
افزایش آگاهی از «الگوهای حمله» ^۶ و ایجاد فرصتی برای سازمان های شرکت کننده برای ارزیابی گزینه های پاسخ در برابر پیامدهای بالقوه و تأکید بر انعطاف پذیر ماندن سیاست ها و رویه ها	CS-V-A6

1. Domain Name System (DNS)
2. Internet Protocol (IP)
3. Public Key Infrastructure (PKI)
4. Information Sharing and Analysis Centers (ISAC)
5. Information Sharing and Analysis Organizations (ISAO)
6. Attack Vectors



شناسه	عنوان
CS-V-A7	فراهم کردن فرصتی برای بررسی و شناسایی پیشرفت در فرایندها و رویه‌های سازمانی داخلی، ازجمله اینکه چگونه ممکن است به واکنش بخش یا سطح ملی وارد شود
CS-V-A8	از میان پاسخ‌دهندگان به پرسش‌نامه پس از اقدام ۹۶ درصد اظهار داشتند که شرکت در رزمایش به آن‌ها کمک کرد تا برای مقابله موفقیت‌آمیز با یک حادثه سایبری آمادگی بهتری داشته باشند و ۸۵ درصد برنامه‌های واکنش به حوادث سایبری دارند.

منبع: (وزارت امنیت داخلی ایالات متحده، گزارش پس از اقدام طوفان سایبری ۵، ۲۰۱۶)

۶-۶. رزمایش سایبری Cyber Storm VI

این رزمایش در سال ۲۰۱۸ با حمایت مالی «آژانس امنیت سایبری و امنیت زیرساخت»^۱ وزارت امنیت داخلی (DHS) با بیش از ۱۰۰۰ بازیکن در سراسر ایالات متحده برگزار شد و مرکز CISA با موفقیت Cyber Storm VI (CS VI) را از مرکزیت اصلی «کنترل رزمایش‌ها»^۲ خود در دفتر مرکزی «سرویس مخفی ایالات متحده»^۳ و همچنین از مکان‌های پخش‌شده بازیکنان از ۹ تا ۱۳ آوریل ۲۰۱۸ اجرا کرد.

۶-۶-۱. اهداف رزمایش

- ❖ تکیه بر نتایج رزمایش‌های قبلی و تغییرات در چشم‌انداز امنیت سایبری؛
- ❖ ارزیابی و ارتقای توانمندی‌های جامعه واکنش سایبری؛
- ❖ ترویج مشارکت‌های دولتی و خصوصی و تقویت روابط بین دولت فدرال و شرکای آن؛
- ❖ ادغام شرکای زیرساخت حیاتی جدید در بازی تمرینی برای ارتقای بلوغ و ادغام ۱۶ بخش زیرساخت حیاتی؛
- ❖ فراهم کردن مکانی برای شرکای بین‌المللی DHS تا اهداف، بهبود و تقویت روابط، بررسی رویه‌های عملیاتی استاندارد و مسیرهای ارتباطی و ارتقای نمایه کلی رویدادهای سایبری و حملات سایبری در کشورشان را فراهم کنند؛

1. Cybersecurity and Infrastructure Security Agency (CISA)

2. Exercise Control (ExCon)

3. U.S. Secret Service (USSS)

- ❖ تقویت آمادگی امنیت سایبری و قابلیت‌های پاسخ‌گویی با اعمال سیاست‌ها، فرایندها و رویه‌ها برای شناسایی و پاسخ به یک حمله سایبری چندبخشی که زیرساخت‌های حیاتی را هدف قرار می‌دهد؛
- ❖ اعمال مکانیسم‌های هماهنگی و ارزیابی اثربخشی طرح ملی واکنش به حوادث سایبری در هدایت واکنش؛
- ❖ ارزیابی به اشتراک‌گذاری اطلاعات به گونه‌ای که شامل مسیرها، به موقع بودن، مفید بودن اطلاعات به اشتراک گذاشته شده و موانع اشتراک‌گذاری داخلی و خارجی در جامعه واکنش به حوادث سایبری باشد؛
- ❖ ادامه دادن به بررسی نقش، کارکردها و قابلیت‌های DHS، زیرا این وزارتخانه با نهادهای تحت تأثیر در طول یک رویداد سایبری هماهنگ می‌شود؛
- ❖ یک انجمن برای شرکت‌کنندگان در رزمایش برای تمرین، ارزیابی و بهبود فرایندها، رویه‌ها، تعاملات و مکانیسم‌های اشتراک اطلاعات در سازمان یا جامعه موردعلاقه خود فراهم گردد.

۲-۶-۶. سناریوهای رزمایش

«تیم برنامه‌ریزی»^۱ رزمایش، فرایند برنامه‌ریزی ۱۶ ماهه را به پنج مرحله محدود، طراحی و توسعه؛ آماده‌سازی، انجام و ارزیابی فازها برای پشتیبانی از برنامه‌ریزی، اجرا و ارزیابی رزمایش CS VI تقسیم کرد.

سناریوی اصلی CS VI ناشی از یک آسیب‌پذیری شبیه‌سازی شده در یک ریزپردازنده تعبیه شده که در طیف گسترده‌ای از دستگاه‌های فناوری اطلاعات سستی و غیر سستی استفاده می‌شود، بوده است. حمله شبیه‌سازی شده علیه فناوری پردازنده‌های زیربنایی، به سیستم‌عامل و نرم‌افزاری که بر روی این دستگاه‌ها اجرا می‌شود، آسیب می‌رساند و تأثیرات سناریویی گسترده‌ای را در صنایع مختلف ایجاد می‌کند و به سرعت به سطح اهمیت ملی می‌رسد. اثرات



سناریوی ناشی از حمله شامل ناتوانی در استارت زدن خودروها بود. خرابی رباتیک در کف کارخانه و دستگاه‌های اینترنت اشیا برای حملات به شبکه‌های شرکتی یا دولتی مورد استفاده قرار می‌گیرند.

۶-۳-۳. دستاوردهای کلیدی رزمایش

جدول ۷: دستاوردهای کلیدی رزمایش طوفان سایبری VI

شناسه	عنوان
CS-VI-A1	ارزیابی واکنش فدرال، ایالتی، بخش خصوصی و بین‌المللی به یک حادثه سایبری مهم که بر دستگاه‌های غیرسنجی فناوری اطلاعات تأثیر می‌گذارد
CS-VI-A2	ادغام ذی‌نفعان جدید در سطح ملی و قرار گرفتن در معرض رزمایش‌های سایبری در مقیاس بزرگ، حمایت از ایجاد روابط و ایجاد پایه‌ای برای رزمایش‌های آینده و تلاش‌های بهبود بخش پشتیبانی از تلاش‌های برنامه‌ریزی و اجرای طبقه‌بندی‌شده در هماهنگی با «مرکز هماهنگی امنیت جامعه اطلاعاتی» ^۱ برای سایر رزمایش‌ها
CS-VI-A3	به‌روزرسانی مکانیسم‌های بین‌المللی اشتراک‌گذاری اطلاعات و ارتباط در طول یک حادثه سایبری
CS-VI-A4	افزایش آگاهی در مورد چشم‌انداز حملات سایبری که به‌سرعت در حال گسترش است و شناسایی تفاوت‌های ظریف واکنش به حوادث تأثیرگذار بر «اینترنت اشیا» ^۲ و دستگاه‌های «فناوری عملیاتی» ^۳
CS-VI-A5	فراهم کردن مکان مناسبی برای کشورهای ذی‌نفع تا به تأثیرات مبتنی بر مخاطرات سایبری که بر سیستم‌ها و فرایندهای حامی انتخابات تأثیر می‌گذارد، واکنش نشان دهند
CS-VI-A6	به‌کارگیری یک رسانه شبیه‌سازی‌شده و به‌روز شده پویا و پلت فرم رسانه‌های اجتماعی برای مخاطبین و اجزای عمومی یک حادثه و ایجاد یک محیط یادگیری بدون خطا برای رزمایش استراتژی‌هایی که از این جنبه از پاسخ پشتیبانی می‌کند
CS-VI-A7	فراهم کردن فرصتی برای بررسی و شناسایی پیشرفت‌ها در فرایندها و رویه‌های سازمانی داخلی از جمله چگونگی اطلاع‌رسانی یا تشدید بهبودهایی که به بخش یا سطح ملی ارائه شده است
CS-VI-A8	

1. The IC Security Coordination Center (IC SCC)

2. Internet of Things (IoT)

3. Operational Technology (OT)

عنوان	شناسه
تأثیر مثبت در مجموعه شرکت کنندگان به گونه ای که از پاسخ دهندگان به پرسش نامه پس از اقدام ^۱ ۹۸ درصد نشان دادند که شرکت در رزمایش به آن ها کمک می کند تا برای مقابله موفقیت آمیز با یک حادثه سایبری آماده شوند.	CS-VI-A9

منبع: (آژانس امنیت سایبری و امنیت زیرساخت، گزارش پس از اقدام طوفان سایبری ۶، ۲۰۱۸)

۶-۲. رزمایش سایبری Cyber Storm 2020

طوفان سایبری ۲۰۲۰ که در آگوست ۲۰۲۰ برگزار شد بخش عمومی و خصوصی را گرد هم آورد تا پاسخ به یک بحران سایبری را که بر زیرساخت های حیاتی کشور تأثیر می گذارد، شبیه سازی کنند. رزمایش Cyber Storm 2020 اولین رزمایش طوفان سایبری در محیط مجازی توزیع شده و شامل بیش از ۲۰۰۰ بازیکن در سراسر کشور بود که در سه روز بازی تمرینی زنده شرکت کردند.

۶-۲-۱. اهداف رزمایش

- ❖ بررسی اجرا و اثربخشی طرح ها و سیاست های ملی امنیت سایبری؛
- ❖ تقویت مکانیسم های به اشتراک گذاری اطلاعات و هماهنگی مورد استفاده در سراسر زیست بوم «اکوسیستم»^۲ سایبری در طول یک حادثه سایبری؛
- ❖ تقویت مشارکت های دولتی و خصوصی و بهبود توانایی آن ها برای به اشتراک گذاری اطلاعات مرتبط و به موقع؛
- ❖ اعمال جنبه های ارتباطی واکنش به حوادث سایبری برای اصلاح و توسعه استراتژی های ارتباطی.

۶-۲-۲. سناریو رزمایش

سناریوی اصلی CS 2020 بر سه سرویس اصلی اینترنت شامل DNS، CA و BGP متمرکز بود، این خدمات برای معماری اینترنت حیاتی هستند و به کاربران اجازه می دهند به صفحات وب دسترسی ایمن داشته باشند. علی رغم اهمیت آن ها، دشمنان باانگیزه راه های زیادی برای

1. After Action Questionnaire (AAQ)

2. Ecosystem



ایجاد اختلال یا حتی استراق سمع از طریق حمله «مردمیانی»^۱ به ترافیک مسیریابی شبکه پیدا کرده‌اند.

در حقیقت میدان رزمایش فرض می‌کرد که دو دشمن در سطح دولت با شرکت‌های وابسته کار می‌کنند تا ابزارهایی را به اشتراک بگذارند که از آسیب‌پذیری‌های DNS، CA و BGP برای حمله به اهداف استفاده می‌کنند. گروه‌های مجرم «هکتیویست»^۲، «اسکرپت کیدی»^۳ و «آندرنت»^۴ از این ابزارها برای حمله به سازمان‌های دولتی و بخش خصوصی در سراسر ایالات متحده و خارج از کشور باهدف به خطر انداختن محرمانگی، یکپارچگی و در دسترس بودن سیستم‌هایشان استفاده می‌کنند.

۳-۷-۶. دستاوردهای کلیدی رزمایش

جدول ۸: دستاوردهای کلیدی رزمایش طوفان سایبری ۲۰۲۰

عنوان	شناسه
انجام واکنش مشترک فدرال، ایالتی، بخش خصوصی و بین‌المللی به یک حادثه سایبری قابل توجه که خدمات اصلی زیربنایی اینترنت، از جمله «سیستم نام دامنه» ^۵ ، «مقامات صدور گواهی» ^۶ و «پروتکل دروازه مرزی» ^۷ را هدف قرار می‌دهد	CS-2020-A1
فراهم شدن فرصتی برای بررسی فرایندهای ارتباطی، رویه‌های سازمانی داخلی، شناسایی پیشرفت‌ها و در نظر گرفتن نحوه اطلاع‌رسانی آن‌ها به بخش ملی و بین‌المللی	CS-2020-A2
گسترش شرکت کنندگان جدید در سراسر دولت فدرال، دولت‌های ایالتی و بخش خصوصی در مسائل گوناگون از جمله مشارکت قابل توجه در بخش خدمات مالی	CS-2020-A3
پشتیبانی از تلاش‌های برنامه‌ریزی و اجرای طبقه‌بندی‌شده با رزمایش STORM ICE ^۸ و تسهیل تعامل بین جامعه اطلاعاتی و سهامدارانی که تحت تأثیر حوادث سایبری شبیه‌سازی شده قرار گرفتند	CS-2020-A4

1. Man-in-the-Middle (MITM)
2. Hactivist
3. Script Kiddie
4. UnderNet
5. Domain Name System (DNS)
6. Certificate Authorities (CA)
7. Border Gateway Protocol (BGP)
8. <https://tx.epa.gov/IceStorm۳.html>

شناسه	عنوان
CS-2020-A5	بررسی فرایند لازم برای تشکیل یک «گروه هماهنگی یکپارچه» ^۱ سایبری
CS-2020-A6	فرصت گفت‌وگو بین سازمانی فدرال در مورد مسائل مربوط به سیاست های امنیت سایبری در طول جلسه «گروه پاسخ سایبری» ^۲
CS-2020-A7	شناسایی فرصت‌ها برای بهبود جریان اطلاعات بین بخش خصوصی و سازمان‌های دولتی به منظور اطمینان از آگاهی وضعیت
CS-2020-A8	ارزیابی ظرفیت دولت‌های ایالتی و محلی شرکت‌کننده برای پاسخ به حوادث سایبری و هماهنگی از طریق «مرکز تجزیه و تحلیل اطلاعات چند ایالتی» ^۳
CS-2020-A9	برنامه‌ریزی و اعمال فرایند پاسخ‌گویی به حادثه در بخش‌های زیرساخت‌های حیاتی: شیمیایی، تأسیسات تجاری، ارتباطات، تولید حیاتی، انرژی، خدمات مالی، بهداشت و سلامت عمومی، فناوری اطلاعات و سیستم‌های حمل‌ونقل
CS-2020-A10	ارزیابی فرایندهای موردبررسی برای هماهنگی واکنش به حادثه و آگاهی موقعیتی مشترک در میان شرکای «شبکه بین‌المللی دیده‌بان و هشدار» ^۴

منبع: (آژانس امنیت سایبری و امنیت زیرساخت، گزارش پس از اقدام طوفان سایبری ۲۰۲۰، ۲۰۲۰)

۶-۸. رزمایش سایبری Cyber Storm VIII

طوفان سایبری هشتم در مارس ۲۰۲۲ به شرکت‌کنندگان اجازه داد تا برنامه‌های واکنش به حادثه خود را اعمال کنند و فرصت‌هایی را برای هماهنگی و اشتراک‌گذاری اطلاعات شناسایی کنند. این رزمایش شامل بیش از ۲۰۰۰ بازیکن بود که درس‌های آموخته‌شده مربوط به آسیب‌پذیری‌های رایج و سیاست‌ها، فرایندها و رویه‌های بازیابی از یک حادثه سایبری بزرگ را تمرین کردند.

۶-۸-۱. اهداف رزمایش

- ❖ بررسی اثربخشی طرح‌ها و سیاست‌های ملی امنیت سایبری؛
- ❖ کاوش در نقش‌ها و مسئولیت‌ها در طول یک حادثه سایبری با اثرات فیزیکی بالقوه یا واقعی؛

-
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 مکانیسم‌های به اشتراک‌گذاری اطلاعات و هماهنگی مورد استفاده در یک حادثه سایبری؛

❖ تقویت مشارکت عمومی و خصوصی و بهبود توانایی آن‌ها برای به اشتراک گذاشتن اطلاعات مرتبط و به‌موقع بین شرکا.

۶-۸-۲. سناریو رزمایش

رزمایش CS VIII از یک سناریوی واقع‌بینانه برای انعکاس محیط عملیاتی فعلی شامل حملات علیه «سیستم‌های کنترل صنعتی»^۱، «فناوری عملیاتی»^۲ و حملات علیه شبکه‌های سازمانی سنتی بود. در تلاش برای ایجاد اختلال در اجزای زیرساخت ایالات متحده، مهاجمی به نام Network Controller (NC) یک سوءاستفاده «روز صفر»^۳ به نام DVER ایجاد کرد. این اکسپلویت برای ایجاد فضایی در شبکه‌ها طراحی شده است که به دشمنان اجازه می‌دهد دستورات از راه دور را اجرا کنند، به‌صورت جانبی در شبکه‌های شرکتی و صنعتی حرکت کنند و امتیازات را برای مهاجمان افزایش دهند.

۶-۸-۳. دستاوردهای کلیدی رزمایش

جدول ۹: دستاوردهای کلیدی رزمایش طوفان سایبری VIII

شناسه	عنوان
CS-VIII-A1	فراهم کردن موقعیتی برای یادگیری و پیشرفت از طریق فرایند برنامه‌ریزی رزمایش و اجرا
CS-VIII-A2	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

1. Industrial Control Systems (ICS)
2. Operational Technology (OT)
3. Zero-Day

عنوان	شناسه
ادغام شرکت کنندگان جدید از جمله سیستم های آب و فاضلاب، قرار گرفتن در معرض رزمایش های سایبری در مقیاس بزرگ با حمایت از ایجاد رابطه و ایجاد پایه ای برای رزمایش ها و تلاش های بهبود آینده	CS-VIII-A3
ارائه یک بردار حمله چندوجهی براساس شرایط سناریوی اصلی مشترک که مکانیسمی را برای افزایش مشارکت در درون و بین سازمان های شرکت کننده فراهم می کند و درعین حال امکان مشارکت سازمان های قدیمی را نیز فراهم می کند	CS-VIII-A4
افزایش آگاهی در مورد حمله سایبری که به سرعت در حال گسترش است و تفاوت های ظریف واکنش به حوادثی که بر شبکه های «سیستم کنترل صنعتی» ^۱ ، «فناوری عملیاتی» ^۲ و فناوری اطلاعات سازمانی تأثیر می گذارد.	CS-VIII-A5
تشکیل «گروه هماهنگی یکپارچه» ^۳ سایبری توسط ذی نفعان دولتی براساس رویه های مندرج در فرایندهای «طرح ملی واکنش به حوادث سایبری» ^۴	CS-VIII-A6
بهبود هماهنگی و فعالیتهای پاسخ گویی دولت و بخش خصوصی با پشتیبانی موفق از تلاش های برنامه ریزی و اجرای «مرکز هماهنگی امنیت جامعه اطلاعاتی» ^۵ برای ICE STORM ^۶	CS-VIII-A7
تاکید بر اشتراک گذاری اطلاعات و ارتباطات کشورهای شریک «شبکه بین المللی دیده بان و هشدار» ^۷ در جهت بهبود ارتباطات واکنش به حادثه از نظر فراوانی، مکانیسم و نوع اطلاعات به اشتراک گذاشته شده	CS-VIII-A8
ایجاد یک سناریوی چندلایه که به شرکت کنندگان این فرصت را می دهد تا بر واکنش کل سازمان (کارشناسان فنی سازمان ها، نمایندگان امور عمومی، نمایندگان امور حقوقی و رهبری سازمانی) به یک حادثه تأکید کنند	CS-VIII-A9
بهره برداری از یک پلت فرم رسانه های اجتماعی و سنتی شبیه سازی شده و به روز شده پویا برای مخاطب و اجزای عمومی یک حادثه و فراهم کردن یک محیط یادگیری بدون خطا برای تمرین استراتژی هایی که از این جنبه از پاسخ پشتیبانی می کند	CS-VIII-A10

1. Industrial Control Systems (ICS)
2. Operational Technology (OT)
3. Unified Coordination Group (UCG)
4. The National Cyber Incident Response Plan (NCIRP)
5. The IC Security Coordination Center (IC SCC)
6. <https://ttx.epa.gov/IceStorm/>.html
7. International Watch and Warning Network (IWWN)



عنوان	شناسه
بررسی نقش‌ها و مسئولیت‌های مرتبط آژانس‌های پشتیبانی در چهارچوب‌های واکنش به حوادث سایبری به دولت‌های شرکت‌کننده	CS-VIII-A11
توسعه و انتشار یک سند «مشاوره امنیت سایبری» ^۱ مشترک در حین رزمایش	CS-VIII-A12

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

۹-۶. رزمایش سایبری Cyber Storm IX^۲

رزمایش Cyber Storm IX که برای ۲۰۲۴ برنامه‌ریزی شده است با ارزیابی سیاست‌های مربوط به امنیت سایبری ملی و روشن کردن نقش‌های واکنش در طول یک رویداد سایبری، بر رزمایش‌های گذشته استوار و شرکت‌کنندگان شامل دولت فدرال، ایالتی و محلی، بخش خصوصی و شرکای بین‌المللی خواهند بود.

۹-۶-۱. سناریوهای رزمایش

برنامه‌ریزی و شناسایی فرصت‌ها برای هماهنگی و اطلاعات اشتراک‌گذاری در یک محیط شبیه‌سازی شده مانند تکرارهای قبلی است، طوفان سایبری IX بیش از ۲۰۰۰ شرکت‌کننده توزیع شده را در سراسر جهان درگیر خواهد کرد.

در این رزمایش، با به تصویر کشیدن یک حمله سایبری هماهنگ که بر زیرساخت‌های حیاتی تأثیر می‌گذارد، محرمانه بودن، یکپارچگی و در دسترس بودن سیستم سازمان‌ها را به چالش کشیده و ضمن هماهنگی با سطوح فدرال، ایالتی، محلی و بخش خصوصی، برنامه‌های داخلی واکنش به حوادث سایبری را ارزیابی می‌گردد. در طول چرخه عمر رزمایش، شرکت‌کنندگان باهم کار می‌کنند تا نقاط قوت و ضعف قابل اجرا را شناسایی کرده و در نهایت راه‌حل‌هایی برای تقویت آمادگی امنیت سایبری پیدا شود.

1. Cybersecurity Advisory (CSA)

۲. رزمایش طوفان سایبری نهم، تا زمان تهیه این پژوهش وارد فاز عملیاتی نشده و نتایج با هدف شناخت براساس مستندات ارائه‌شده توسط انجمن طرح‌ریزی رزمایش مدنظر قرار گرفته است.

ذی نفعان رزمایش:

- ❖ ادارات و آژانس های فدرال؛
- ❖ شرکای صنعت از بخش های زیر ساختی حیاتی؛
- ❖ شرکای بین المللی؛
- ❖ دولت های ایالتی و محلی؛
- ❖ مشارکت کنندگان رزمایش.

طوفان سایبری IX شامل سازمان هایی در سراسر دولت های فدرال، ایالتی و بین المللی و بخش خصوصی است.

سازمان های شرکت کننده مستقیماً با CISA کار می کنند تا نقش و قابلیت های CISA در یک حمله سایبری را درک کنند.

شرکت کنندگان در گروه های کاری برای دستیابی به اهداف خاص سازمان و بخش فعالیت می کنند.

مزایای مشارکت شامل اجرای طرح ها و قابلیت های واکنش سازمانی، تقویت روابط با هم تایان و بهبود آمادگی سایبری سازمانی و ملی است.

۶-۹-۲. اهداف رزمایش

- ❖ تمرین و ارزیابی پاسخ امنیت سایبری، همکاری عملیاتی و پشتیبانی؛
- ❖ بررسی و شفاف سازی نقش ها و مسئولیت ها در پاسخ به یک رویداد مهم سایبری؛
- ❖ ارزیابی قابلیت های به اشتراک گذاری اطلاعات و نیاز به منابع در طول یک حادثه سایبری؛
- ❖ بررسی و ارزیابی سیاست، راهنمایی و دکرین ملی مربوط به امنیت سایبری (آژانس امنیت سایبری و امنیت زیر ساخت، اوراق طوفان سایبری ۲۰۲۴، ۲۰۲۳).

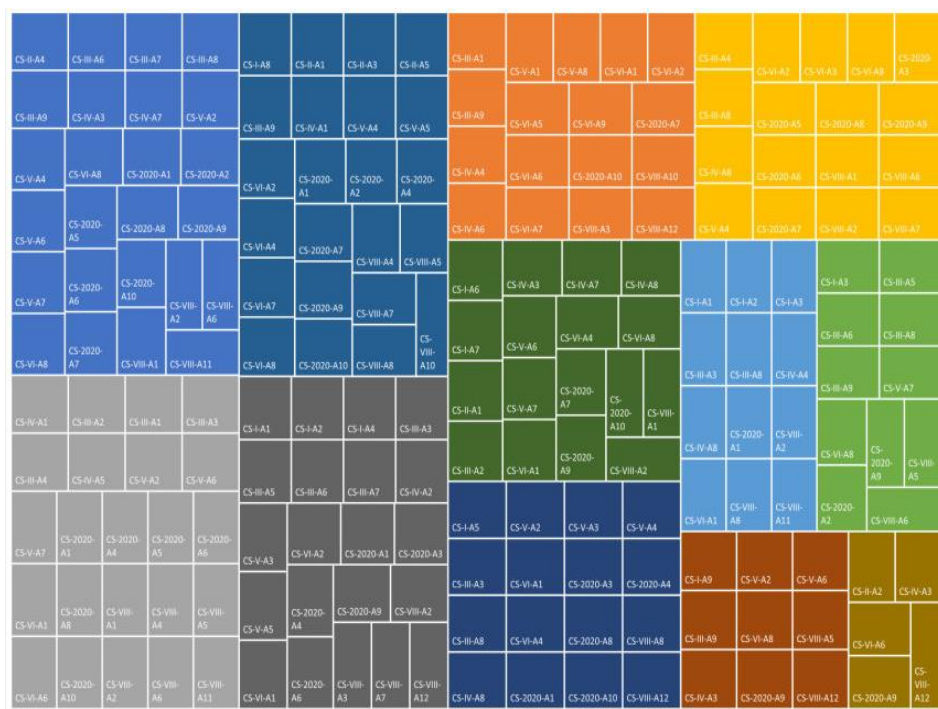


۳-۹-۶. کلان دستاوردهای رزمایش

براساس تحلیل داده‌ای صورت پذیرفته بر روی گزاره‌های پژوهش در هریک از مجموعه دستاوردهای رزمایش‌های دوسالانه طوفان سایبری، با احصاء ۱۲ دستاورد کلان به روش خبرگی محقق، اقدام به دسته‌بندی و برچسب‌زنی به هریک از دستاوردهای کلان تعیین شد در این بخش گردید که در قالب جدول (۱۰) و شکل (۲) قابل مشاهده است.

جدول ۱۰: کلان دستاوردهای رزمایش طوفان سایبری

ردیف	کلان دستاورد	تعداد دستاورد مرتبط	رنگ
۱	روشن شدن نقش‌ها و مسئولیت‌ها و بهبود فرایندهای ادغام و هماهنگی پاسخ رویدادهای سایبری	۲۵	
۲	ارتباطات عمومی و خصوصی متعدد بین بازیگران با ایجاد بستر اشتراک‌گذاری اطلاعات	۲۳	
۳	ارزیابی منابع و قابلیت‌های واکنش به حوادث سایبری	۲۳	
۴	همکاری در گستره فرابخشی دولتی و خصوصی	۲۱	
۵	ارزیابی طیف کاملی از سیاست‌ها، دکترین و روش‌های ارتباطی واکنش سایبری	۱۷	
۶	ارزیابی عملکرد مرکز ادغام امنیت سایبری و ارتباطات ملی	۱۷	
۷	شتاب‌دهنده یادگیری جامعه واکنش به حوادث سایبری	۱۷	
۸	همکاری در گستره جغرافیایی و فرابخشی در ابعاد اطلاعاتی-نظامی	۱۶	
۹	همکاری در گستره جغرافیایی چندملیتی و فرابخشی	۱۲	
۱۰	همکاری در سطوح مختلف سلسله‌مراتب سازمانی	۱۱	
۱۱	شناسایی مسائل بازیابی شرایط مطلوب	۹	
۱۲	شناسایی وابستگی‌های متقابل فیزیکی و سایبری	۵	



شکل ۲: فراوانی دستاورد مرتبط با کلان دستاوردهای رزمایش طوفان سایبری

فراوانی کلان دستاوردهای رزمایش طوفان سایبری به بازیگران راهبردی و عملیاتی امکان نشان دادن قابلیت‌های حیاتی رزمایش و در نتیجه آشکار کردن اینکه تا چه حد در هماهنگ کردن افراد، فرایندها و تکنولوژی‌ها برای حفاظت از دارایی‌های اطلاعاتی و سرویس‌های مرتبط کارآمدی دارد را فراهم می‌آورد. با تغییر و تکامل تهدیدات متوجه زیرساخت‌های حیاتی، دولت و بخش خصوصی باید قابلیت‌های فردی و جمعی خود برای حفظ امنیت و انعطاف‌پذیری زیرساخت‌های سایبری را به‌طور مداوم بیازماید و با ارزیابی کلیه دستاوردها و قابلیت‌ها، همچنین شناسایی نقاط ضعف و کاستی‌ها در این جهت گام بردارد. بدین منظور همکاری بین این بخش‌ها امری ضروری است. در سطوح عملیاتی رزمایش‌های سایبری به متخصصان امنیتی کمک می‌کنند با قرار دادن مدیران و پرسنل در یک محیط تحت فشار قبل از وقوع خطر، چگونگی واکنش سازمان به یک حادثه واقعی اما بدون ریسک را بیازمایند و فرصت اصلاح نواقص موجود را داشته باشند. ذی‌نفعان با شرکت در رزمایش‌های سایبری



می‌توانند قابلیت‌های واکنشی خود را ارزیابی کنند و متوجه شوند آیا به شیوه‌ای درست و کارآمد عمل می‌کنند یا خیر. همچنین می‌توانند روابط میان سازمانی و مکانیسم‌های اشتراک اطلاعات و روش‌های دفاع سایبری کارآمد را تشخیص دهند و توسعه دهند. این رزمایش‌ها امکان اصلاح واکنش‌ها و طرح‌های بازیابی، افزایش تبادل اطلاعات و همکاری بین ذی‌نفعان، تعیین و اصلاح نقش‌ها و مسئولیت‌های خاص و کشف تهدیدات جدید را فراهم می‌آورند. یافته‌های پس از رزمایش برای متخصصان امنیت سایبری گزارش‌های ارزیابی، تکنیک‌ها و ایده‌هایی را فراهم می‌آورند که می‌توانند با کمک آن‌ها امنیت و انعطاف‌پذیری زیرساخت‌های سایبری را افزایش دهند و ریسک در سیستم‌های حیاتی را کاهش دهند. همچنین با به اشتراک گذاری یافته‌های رزمایش با شرکای مورد اطمینان، تمام افراد و سازمان‌های مرتبط با امنیت سایبری می‌توانند قابلیت‌های جمعی خود را برای مقابله با تهدیدات در زیرساخت‌های سایبری کشور ارتقاء دهند.

نتیجه‌گیری و پیشنهاد

رزمایش‌های سایبری به سازمان‌ها امکان نشان دادن قابلیت‌های حیاتی خود و در نتیجه آشکار کردن اینکه تا چه حد در هماهنگی کردن افراد، فرایندها و تکنولوژی‌ها برای حفاظت از دارایی‌های اطلاعاتی و سرویس‌های مرتبط کارآمدی دارند را فراهم می‌آورد. با تغییر و تکامل تهدیدات متوجه زیرساخت‌های حیاتی، دولت و بخش خصوصی باید قابلیت‌های فردی و جمعی خود برای حفظ امنیت و انعطاف‌پذیری زیرساخت‌های سایبری را به‌طور مداوم بیازماید. امروزه 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 و اثربخشی کافی در این حوزه وجود ندارد.

ضعف در اثربخشی رزمایش در سطوح مختلف راهبردی، عملیاتی، تاکتیکی و تکنیکی قابل‌بررسی است که در این مقاله به بررسی دستاوردهایی که در بخش راهبردی و عملیاتی نقش بیشتری دارد پرداخته شده است. با توجه به اهمیت شناسایی قابلیت‌ها و دستاوردهای

هر اقدام به‌منظور تعیین چشم‌انداز راهبردی و طرح‌ریزی عملیاتی صحیح منطبق با اهداف اقدام، رزمایش سایبری نیز به‌عنوان یک اقدام نیازمند شناسایی دستاوردهای خرد و کلان است که این امر با استفاده از تجربیات منتشرشده مشابه مانند رزمایش طوفان سایبری ایالات متحده در این پژوهش و استفاده از ظرفیت خبرگی مورد احصا قرار گرفت.

براساس نتایج به‌دست‌آمده، دستاوردهای برگزاری رزمایش سایبری با مطالعه موردی رزمایش طوفان سایبری ایالات متحده مشتمل بر ۷۰ مورد شناسایی گردید که پس از انجام فرایند خلاصه‌سازی و یکپارچه‌سازی مشترکات، ۱۲ مورد مطابق جدول ۱۰ به‌عنوان دستاوردهای برگزاری رزمایش سایبری معرفی شد.

بر این اساس، کلان دستاورد «روشن شدن نقش‌ها و مسئولیت‌ها و بهبود فرایندهای ادغام و هماهنگی پاسخ رویدادهای سایبری» با ۲۵ دستاورد خرد مرتبط، «ارتباطات عمومی و خصوصی متعدد بین بازیگران با ایجاد بستر اشتراک‌گذاری اطلاعات» و «ارزیابی منابع و قابلیت‌های واکنش به حوادث سایبری» با ۲۳ دستاورد خرد مرتبط، به‌عنوان مهم‌ترین دستاوردهای برگزاری رزمایش سایبری شناسایی گردید.

پیشنهادهای پژوهش

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 که قصد تحقیق مشابه را دارند، باشد؛ بنابراین می‌توان این تحقیق را باب جدیدی برای پاره‌ای از تحقیقات به‌شمار آورد و 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.

✓ مطالعه موردی سایر رزمایش‌های سایبری در دنیا مانند رزمایش سایبری آژانس

امنیت سایبری اتحادیه اروپا؛

✓ پژوهش آماری روی دستاوردهای کلان شناسایی‌شده در این تحقیق؛



- ✓ طراحی و پیاده‌سازی مدل مفهومی رزمایش سایبری با هدف کسب دستاوردهای کلان شناسایی‌شده در این تحقیق در کشور؛
- ✓ وظایف و اختیارات نهادهای حاکمیتی، کشوری، لشکری و بخش خصوصی در رسیدن به دستاوردهای کلان شناسایی‌شده در این تحقیق.

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.
- موحدی راد، محمدرضا؛ مدیری، ناصر (۱۳۹۳). رزمایش سایبری رویکردی نوین جهت آمادگی در برابر تهدیدات سایبری، مشهد، مقاله ارائه شده به نهمین سمپوزیوم پیشرفت‌های علوم و تکنولوژی
- وزارت امنیت داخلی ایالات متحده (۲۰۲۳). چشم‌انداز سازمان.



References

- Department of Homeland Security (2011). Cyber Storm III Final Report, United States, Department of Homeland Security Office of Cybersecurity and Communications.
- DHS CISA CYBER+ INFRASTRUCTURE (2018). Informing Cyber Storm VI:After Action Report, U.S., Department of Homeland Security
- 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
- DHS Cybersecurity and Infrastructure Security Agency (2023). Cyber Storm IX: National Cyber Exercise Fact Sheet, U.S., Cybersecurity and Infrastructure Security Agency
- DHS National Cyber Security Communications Integration Center (2015). Lessons Learned from Cyber Storm IV, U.S., Department of Homeland Security
- DHS National Cyber Security Communications Integration Center (2016). Informing Cyber Storm V:After Action Report, U.S., Department of Homeland Security
- DHS National Cyber Security Division (2006). Cyber Storm I Exercise Report, U.S., Department of Homeland Security
- DHS Office of Cybersecurity and Communications National Cyber Security Division (2009). Cyber Storm II Final Report, U.S., Department of Homeland Security
- DHS Office of Cybersecurity and Communications National Cyber Security Division (2011). Cyber Storm III Final Report, U.S., Department of Homeland Security
- Lance,J. Hoffman, Ragsdale,Daniel (2005). Cyber Storm III Final Report, United States, IEEE Security and Privacy, Vol. 3, Issue 5.
- Rock, Lee, U.S. Department of Homeland Security (2011). Cyber Atlantic 2011 tabletop exercise, Washington, D.C, U.S. Department of Homeland Security. <https://www.dhs.gov/blog/2011/11/03/united-states-and-european-union-hold-first-ever-joint-cyber-tabletop-exercise>

