تاریخ دریافت: ۱۳۹۹/۰۵/۲۲
تاریخ پذیرش: ۱۳۹۹/۰۸/۰۵

از صفحه ۵۴ تا صفحه ۸۲

فن آوری ها و روش های اجرای بازی جنگ سایبری

محمدطاهری[۱]، سپهر محمد زهرایی[۲]، محمدرضا محمدی تودشکی[۳]

چکیده

با پیشرفت فن آوری های مرتبط با حوزه های سایبری، تهدیدات مربوط به نفوذ، اختلال و خرابکاری در این حوزه ها نیز بیشتر شده است و تصمیم گیران سازمان های ذی نفع در این حوزه ها بایستی قادر باشند در صورت بروز هریک از تهدیدات تصمیمات مناسبی اتخاذ و کاربران مربوطه نیز بایستی قادر باشند این تصمیمات را به نحو صحیح عملی نمایند. یکی از مواردی که این توانایی را در تصمیم گیران و کاربران ایجاد و تقویت می نماید بازی جنگ سایبری بوده که در صورت ارتقای معلومات، مهارت ها و توانایی های مرتبط با این حوزه، تا حدود زیادی می توان از اثرات این تهدیدات کاست.

مقاله حاضر با هدف تبیین فن آوری ها در حوزه های مرتبط با بازی جنگ سایبری، با روش تحلیل محتوا، پس از جمع آوری اطلاعات به روش کتابخانه ای و ذکر فن آوری های بازی جنگ سایبری به توضیح آن ها پرداخته و نسبت به تشریح چارچوب ها و مدل های تبیین بازی جنگ سایبری، بسترهای اجرای بازی جنگ سایبری، فضای تمرین و ابزار بازی جنگ سایبری، شبیه سازی های قابل اجرا برای بازی جنگ سایبری، باز نمایی ها و فریب های دشمن در بازی جنگ سایبری، تمرینات موجود و سناریوهای موجود در بازی جنگ سایبری اقدام شده است و نهایتا بصورت تجزیه و تحلیل محتوایی نتایج مربوط ارائه گردیده است.

واژه‌های کلیدی: بازی جنگ، سایبر، بازی وارسازی، سناریوی بازی

---

۱ پژوهشگر پژوهشکده عالی جنگ دانشگاه فرماندهی و ستاد آجا
۲ پژوهشگر پژوهشکده عالی جنگ دانشگاه فرماندهی و ستاد آجا
۳ پژوهشگر پژوهشکده عالی جنگ دانشگاه فرماندهی و ستاد آجا

Optimal Allocation of Security Resources by Using Game Theories

Taheri M.[۱], Zahraei S.M.[۲], Mohammadi Todashki M.R.[۳]

ABSTRACT

With the advancement of technologies related to cyber domains, the threats related to intrusion, disruption and sabotage in these domains have also increased and the decision makers of stakeholder organizations in these domains should be able to In the event of any threat, appropriate decisions should be made and the relevant users should be able to implement these decisions correctly. One of the things that builds and strengthens this ability in decision makers and users is the game of cyber wargaming.

In the present article, with the aim of explaining the technologies and technologies of cyber wargaming after collecting information

Libraries and mentions of cyber wargame technologies explain them and explain the frameworks and models of cyber wargame explanation, cyber wargame platforms, training space and cyber wargame tools, similar to Applicable constructions for cyber warfare game, representations and deceptions of the enemy in cyber war game, existing exercises and scenarios in cyber wargame have been performed and finally the relevant results have been presented as a content analysis.

KEYWORDS: wargame, cyber, gamification, game senarios

[1] Researcher, Institute for the study of war, Aja Command and Staff University
[2] Researcher, Institute for the study of war, Aja Command and Staff University
[3] Researcher, Institute for the study of war, Aja Command and Staff University

۱- مقدمه

بازی جنگ سایبری روشی است برای بررسی آنچه در یک سیستم یا سازمان به خصوص در مواجهه با حملات سایبری فرضی یا واقعی اتفاق می افتد. بازی جنگ سایبری در بسیاری از مقالات بدین صورت تعریف شده است: " یک تمرین تعاملی است که شرکت کنندگان را در یک سناریوی حمله سایبری شبیه سازی شده، مانند شکاف داده ها، حذف وب سایت، رد حمله سرویس یا کشف بدافزارهای پیشرفته در یک شبکه مشارکتی، شرکت می دهد".

ابزار بازی جنگ سایبری برای ارزیابی قابلیت های فعلی و آینده، برنامه ریزی، بررسی سناریوهای احتمالی و کارکنان آموزشی در سازمان ها ابزار مفیدی است. هدف اصلی از بازی جنگ سایبری، در یک محیط مدل سازی، روشی را برای تمرین و بررسی عملکرد انسان و تصمیم گیری یا ویژگی های سیستم و نتایج آن، در متن یک سناریوی حمله سایبری فراهم می کند .

در خصوص کاربرد بازی جنگ باید گفت که بازی جنگ سایبری می تواند مورد استفاده های بسیاری قرار گیرد، از جمله ارزیابی اثربخشی قابلیت های فعلی در برابر حمله سایبری، بررسی موارد اضافی یا تغییرات احتمالی برای اهداف برنامه ریزی، مجهز کردن کارمندان کلیدی به تجربه مقابله با حمله سایبری و نهایتاً هنگامی که برای چندین سازمان با وابستگی متقابل مشخص استفاده می شود، به شناسایی خطرات سیستمیک ناشی از حملات سایبری کمک می کند. پشتیبانی از ارزیابی توانایی های فعلی، یکی از کاربردهای مهم بازی جنگ سایبری است، به این ترتیب که بازی های جنگ برنامه ریزی شده و کنترل شده فرصتی بی نظیر برای شناسایی نقاط قوت و ضعف شبکه های سازمان و معماری سیستم ها، فناوری های دفاعی و فرآیندها و رویه های سازمان را ارائه می دهند. همچنین سازمان ها در راستای برنامه ریزی های خود، تمایل دارند از برنامه بازی جنگ سایبری جهت برنامه ریزی برای آینده استفاده کنند. این می تواند به دنبال پیشرفت به سمت توانایی های فنی آینده، تغییر در روش ها و رویه های فنی یا ارزیابی استراتژی و تغییرات معماری باشد.

با توجه به اینکه آموزش کارکنان یکی از وظایف مهم سازمان ها است، در یک سناریوی بازی جنگ سایبری، بوسیله بسیاری از فشارها و اتفاقاتی که سریع اتفاق می افتد بر آموزش دقیق کارکنان توجه خاصی می گردد، تا توجه و تمرکز افراد را به چالش بکشد. در یک رویداد خوب هماهنگ، شرکت کنندگان احساس می کنند که در یک وضعیت دنیای واقعی قرار دارند. این فرصتی برای یادگیری چگونگی عملکرد پرسنل و مدیریت در بحران، ضمن ارزیابی همزمان نقاط قوت و ضعف مهارت های آن ها و کمک به آن ها در بهبود مهارت های خود یا شناسایی خود در زمینه های بهبود مورد نیاز، ارائه می دهد. نهایتاً در یک بازی جنگ سایبری نسبت به شناسایی ریسک سیستمیک اقدام می شود.

۲- روش‌شناسی تحقیق

هدف این مقاله تبیین فن‌آوری‌های بازی جنگ سایبری است.

مرحله گردآوری اطلاعات آغاز فرآیندی است که طی آن محقق یافته‌های میدانی و کتابخانه‌ای را گردآوری می‌کند و به روش استقرایی به فشرده‌سازی آن‌ها از طریق طبقه‌بندی و سپس تجزیه و تحلیل می‌پردازد و فرضیات تدوین شده خود را مورد ارزیابی قرار می‌دهد و در نهایت حکم صادر می‌کند و پاسخ مسئله را به اتکای آن‌ها می‌یابد. در این تحقیق جمع‌آوری اطلاعات بصورت کتابخانه‌ای و با استفاده از مقالات و کتب تدوین شده در این حوزه صورت گرفته است.

در این پژوهش بر اساس تحلیل محتوای کیفی داده‌ها در خصوص فن‌آوری‌های بازی جنگ سایبری، تجزیه و تحلیل صورت گرفته است.

۳- تاریخچه بازی جنگ

بازی جنگ مدت هاست که روشی برای ایفای نقش بازی برای تهیه، درک، پیش بینی و حتی برنامه ریزی برای جنگ است. بازی جنگ از همان ابتدای استفاده از بازی هایی مانند «چاتورانگا[1]» که (در غیر این صورت) با نام شطرنج شناخته می شد، توسعه یافته

[1] chaturanga

است. «وی چی[1]» که بیشتر با نام Go شناخته می شود، به عنوان نسخه های انتزاعی بازی جنگ از آنها استفاده شده است [۱]. استفاده از نقشه ها و کشتی های مدل باعث پیشرفت و توسعه آن شد. اولین بازیکنان بازی جنگ از این روش های اولیه برای به دست آوردن بینش و درک برنامه های خود قبل از اجرای برنامه استفاده می کردند و به بازیکنان این امکان را می دادند تا در مورد تأثیر تصمیمات خود فکر کنند [۲]. بازی جنگ در سال های ابتدایی توسط ارتش های آلمان و پروس از سال ۱۸۲۴ استفاده شده است. اولین استفاده مدرن از بازی جنگ و روش های آن توسط افسر ارتش پروس «بارن ون ریسویتز[2]» بوده است. ولی قدیمی ترین نسخه بازی جنگ مربوط به سال ۱۸۱۱ است.

اولین استفاده از بازی جنگ در ایالات متحده به سال ۱۸۸۳ میلادی برمی گردد که سرگرد «ویلیام آر. لیورمور[3]» نسخه «پروسین کرایسپیل[4]» را برای استفاده از هنر جنگ بر روی نقشه های توپوگرافی تصویب و توسعه داد[۳]. اشکال اولیه بازی جنگ، روش هایی را شکل داد که هنوز هم در حال استفاده است. اولین نسخه های بازی جنگ در ایالات متحده فقط بازی-های آلمانی بودند که به انگلیسی ترجمه شده و به همراه جداول اسناد مربوط به جنگ داخلی ارائه شدند. بازی جنگ مدرن هنوز هم با استفاده از نقشه های ساده انجام می شود. با این حال، بازی جنگ به طور کامل نیاز به کامپیوتر برای کار با الگوریتم و ارائه رابط با بازیکنان دارد. امروزه بازی جنگ در مقیاس بزرگ در قالب عنوان هایی مانند "نامزدی جهانی" و "ارتش بعد از بعدی" قرار دارد[۴]. بازی جنگ و بازی وارسازی همچنان به عنوان روش هایی برای کسب بینش در مورد تأثیر تصمیمات آینده در ارتش و سایر موارد در حال توسعه هستند .

استفاده از مفاهیم و تکنیک های بازی وارسازی به اوایل دهه ۱۹۰۰ بر می گردد. اولین نمونه های استفاده از بازی وارسازی در تجارت و آموزش پیاده سازی شده اند. «بوی اسکات[5]» نمونه اولیه ای از بازی سازی در آموزش را با استفاده از نشان ها و یک

[1] Wei-Chi
[2] Baron von Reisswitz
[3] Major William R. Livermore
[4] Prussian Kriegsspiel
[5] Boy Scouts

سیستم رتبه بندی ارائه می دهد تا موفقیت در هنگام پیشرفت از طریق برنامه را نشان دهد.

نکته مهم در این زمینه در دهه ۱۹۸۰ هنگامی رخ داد که مقالات دانشگاهی استفاده از بازی ها را برای یادگیری در هر دو زمینه آموزش و پرورش و کسب و کار شروع کردند، گرچه هنوز اصطلاح بازی وارسازی مورد استفاده قرار نگرفته بود. به طور فزاینده ای و در دسترس تر در دهه ۱۹۹۰ دانش آموزان با بازی هایی در کلاس مانند «مث بلستر[1]» و ماشین افسانه ای[2] آشنا شدند. این بازی ها بسیار مورد انتقاد قرار گرفتند، اما تأثیرات مثبتی بر یادگیری دانش آموزان از مهارت های اساسی با استفاده از تکرار نشان داده اند[۵].

اصطلاح بازی وارسازی اولین بار توسط «نیک پیلینگ[3]» استفاده شد، که بر اساس فعالیت وی به عنوان مشاور کار در

«آی جی اس[4]» انجام شده است[۶]. او اولین بار این اصطلاح را در سال ۲۰۰۲ به عنوان بخشی از توسعه «آی جی اس» استفاده کرد. این ابتکارات اولیه تحولاتی را در این زمینه به وجود آورد که امروزه همچنان تأثیر می گذارد. «جی۴سی[5]» از دل این تغییرات و پیشرفت ها تشکیل و بزرگ شد. «جی۴سی» در سال ۲۰۰۴ تأسیس شد و هدف آنها تمرکز بر استفاده از بازی وارسازی برای تأثیرات مثبت اجتماعی بود[۷].

پیشرفت در فن آوری نرم افزار و اینترنت به دو پیشرفت بعدی در زمینه بازی سازی مانند «بانچبال[6]» کمک کرد. نمونه-هایی از بازی وارسازی اغلب در فن آوری هایی که روزانه از آنها استفاده می کنیم وجود دارد. تغییر استفاده از رایانه های شخصی به استفاده از تلفن های هوشمند و تبلت ها برای دسترسی به اینترنت، به رشد برنامه های بازی گونه کمک کرده است. افزایش استفاده از تلفن های هوشمند و تبلت ها به طور

[1] Math Blaster
[2] The Incredible Machine
[3] Nick Pelling
[4] Initiative Games Serious
[5] Game for changes
[6] Bunchball

کلی باعث افزایش میزان بازی در این سیستم عامل ها شده است[۸]. بانچبال که در سال ۲۰۰۷ تاسیس شد به شرکت ها و سازمان ها اجازه می دهد تا از عناصر بازی مانند امتیاز، تابلوهای تبلیغاتی و نشان ها برای تقویت تعامل کارمندان و وفاداری مشتری استفاده کنند[۹].

با افزایش علاقه به بازی وارسازی اجلاسی در سطح جهان تشکیل شد تا ایده های خود را در مورد پیشرفت ها به اشتراک بگذارند. یک کنفرانس تحت وب هم به میزبانی «دی آی سی ایی[1]» تشکیل و با فعالیت خود کمک زیادی به پیشرفت بازی وارسازی کرده است. موفقیت کنفرانس وب منجر به ایجاد اولین اجلاس بازی سازی در سال ۲۰۱۱ در سانفرانسیسکو شد که بیش از ۴۰۰ نفر در آن شرکت کردند. در همان سال اصطلاح بازی وارسازی[2] وارد دیکشنری آکسفورد شد و اینگونه تعریف شد " استفاده از مفاهیم و تکنیک های بازی در سایر حوزه های فعالیت"[۱۰]. طبق تحقیقات انجام شده توسط «ام۲ریسرچ[3]» درسال ۲۰۱۱ درآمد بازی وارسازی نزدیک به ۱۰۰ میلیون ارزش داشته داشت[۱۱].

۴- نحوه انجام بازی جنگ

در این بازی مدافعین سایبری به عنوان تیم سفید و مهاجمین به عنوان تیم قرمز نقش خود را ایفا می‌نمایند. مراحل بازی توسط مدیر آزمون و تیم سفید طراحی و ساخته می‌شود. در حین اجرای تمرین، افرادی که نقش‌های مختلفی را بازی می‌کنند، با سیستم ارتباط برقرار می‌کنند، چه از طریق گفتگو با تیم سفید و چه با استفاده از اقدامات از پیش تعریف شده روی کاغذ یا از طریق تعامل با محیط بازی که توسط تیم قرمز ساخته شده است. نقش‌های شرکت‌کنندگان مختلف با توجه به ماهیت و وسعت بازی جنگ توسط تیم‌های انسانی یا به‌وسیله شبیه‌سازی مشخص می‌شود و شرکت کنندگان را به عنوان بخشی از «گیم پلی» انتخاب می‌کند.

در ابتدا، مهاجمان سایبری اقداماتی را که نشان از انجام فعالیت‌های خصمانه است انجام می‌دهند. از طرفی مدافعان فضای مجازی فعالیت‌هایی از قبیل سخت شدن

[1] Design, Innovate, Communicate, Entertain
[2] gamification
[3] M2 Research

محیط، نظارت بر سیستم‌های تشخیص و یا پاسخ به هرگونه شواهد نقض را انتخاب و انجام می‌دهند. هریک از این گروه‌ها فهرستی از فعالیت‌هایی که می‌توانند انتخاب کنند را در اختیار خواهند داشت که هر کدام از این انتخاب‌ها تأثیرات و نتایج خود را دارد که پس از انتخاب می‌توان از آن‌ها نتیجه‌گیری کرد. اگرچه این نتایج از قبل تنظیم شده است ولی از قبل برای بازیکنان مشخص نمی‌شود.

همانطور که در حین بازی، طرفین فعالیت‌های خود را انجام می‌دهند، بازی اثرات این اقدامات را در نظر گرفته و وضعیت سیستم را که توسط پلت فرم بازی جنگ نگهداری می‌شود، چه از طریق قضاوت تیم سفید، چه از طریق شبیه‌سازی و چه از طریق یک عمل واقعی که روی سیستم هدف انجام و ترکیبی از موارد ذکر شده است، بروز رسانی می‌کند. با توجه به تأثیراتی که بر روی سیستم‌های سطح شغلی، دفاع سایبری و سیستم‌های IT ایجاد شده است، بازخورد جدیدی به بازیکنان ارائه می‌شود که آن‌ها هنگام انتخاب اقدامات بعدی این بازخوردها را در نظر بگیرند تا بهترین تصمیم را اتخاذ کنند. در طول تمرین، مدیر آزمون و تیم سفید بر پیشرفت بازی نظارت می‌کنند و می‌توانند محرک‌های جدیدی را تنظیم کرده و آن را طبق نظر خود به زنجیره رویدادها اضافه کنند.

یکی از مهم‌ترین کارکردهای پلت‌فرم بازی جنگ سایبری ثبت و ضبط کلیه فعالیت‌ها و نتایج است که از این نتایج می‌توان برای ارائه معیارها و مؤلفه‌های زنده در طول بازی و هم برای گزارشات بعد از این تمرین و در طول جلسه بحث و انتقاد[1] برای استفاده مشترک هر دو طرف استفاده کرد.

برگزارکنندگان بازی جنگ می‌توانند از این داده‌ها برای برنامه‌ریزی بهتر و آماده‌سازی مناسب برای رویدادهای آتی و همچنین برای انجام اصلاحات یا ایجاد پیشرفت‌هایی در سیستم استفاده کنند[۱۲].

[1] Hotwash

۵- اجزای بازی جنگ سایبری

بازی جنگ سایبری در قالب چارچوب‌ها و در بسترهایی انجام می‌شوند، نیاز به فضای تمرین مرتبط داشته، برای اینکه بازی بوقوع بپیوندد بایستی شبیه‌سازی‌هایی با واقعیت صورت پذیرد و همه اینها تحت یک سناریو اجرا شود، در این بخش اجزای مختلف مربوط به بازی جنگ که در «بخش خدمات مالی[1]» مدل‌سازی شده و به‌طور بالقوه قابل استفاده در بازی جنگ سایبری است توصیف شده و تمرین‌های موجود برای هر کدام از اجزا به شرح زیر بررسی می‌گردد.

- چارچوب‌ها و مدل‌های تعیین بازی جنگ سایبری
- بسترهای اجرایی بازی جنگ سایبری
- فضای تمرین و ابزار آن
- شبیه‌سازی‌های قابل اجرا برای بازی جنگ سایبری
- بازنمایی‌های دشمن
- تمرین‌های موجود و سناریوها

۵-۱ چارچوب‌ها و مدل‌ها

در بخش زیر چارچوب‌ها و مدل‌هایی که از طریق این مطالعه مشخص شده‌اند، تشریح می‌شود. این‌ها غالباً پایه‌ای برای سازگاری سناریوهای ویژه بازی جنگ سایبری هستند.

۵-۱-۱ کیت ساخت و ساز بازی جنگ

کیت ساخت و ساز بازی جنگ ابزاری برای توسعه بازی جنگ‌های رومیزی است[۱۳]. به عنوان بخشی از برنامه درسی آموزشی برای توسعه بازی جنگ، قوانین، سناریوها، نقشه‌های زمینی و تکه‌های بازی را می‌توان انتخاب کرد و برای ایجاد یک بازی جنگ مناسب تنظیم کرد. این ابزار می‌تواند در مورد میزان استفاده و تطبیق آن با سایبر مورد بررسی قرار گیرد.

[1] Financial Services Sector

۵-۱-۲ بازی‌های جنگ تجاری

کتاب بازی‌های جنگ تجاری، مواردی را به شرکت‌های بزرگ، کوچک و جدید ارائه می‌دهد که چگونه می‌توانند استراتژی‌های خود را به شدت بهبود بخشند[۱۴]، و نحوه استفاده از استراتژی‌های بازی جنگ را برای انجام برنامه‌های تجاری پیشنهادی در برابر رقبا بیان می‌کند. این اقدامی برای تطبیق مفاهیم است تا بتواند یک مدل عملیاتی را در برابر حرکت‌های رقبای احتمالی آزمایش کند که شامل شناسایی تیم‌ها و نقش‌ها و همچنین شناسایی افراد طرف مقابل است.

۵-۱-۳ پیشنهادهای تجاری با ابزارهای اختصاصی

ساخت و اجرای بازی‌های جنگ سایبری به‌طور فزاینده‌ای ارائه‌دهنده خدمات تجاری است. برای مثال می‌توان به خدمات سایبری سیسکو[۱۵]، خدمات دیلویت[۱۶]، خدمات ارائه شده توسط اوپتیمال ریسک[۱۷] و ... اشاره کرد. با این حال چنین پیشنهاداتی به چارچوب‌ها و ابزار خاصی متکی می‌باشد.

۵-۲ زمینه ها و بسترها

در بخش زیر به تشریح زمینه‌ها و بسترهای تسهیل‌کننده عناصر بازی جنگ سایبری می‌پردازیم.

۵-۲-۱ فضای طراحی شده برای تمرین‌های تصمیم‌گیری در شرایط بحرانی

فضای طراحی شده برای تمرین‌های تصمیم‌گیری در شرایط بحرانی یک بستر بازی جنگ چند شرکت‌کننده‌ای است که توسط مؤسسه تحقیقات پیشرفته دانشگاه نورویچ ساخته شده است. سناریوهای بازی جنگ به سبک رومیزی به برنامه اضافه شده و از طریق کاربری گرافیکی به دیگران ارائه می‌شود. پاسخ‌های شرکت‌کنندگان به کارت‌های سفید ضبط می‌شود و توسط برنامه به سایر شرکت کنندگان برای تعامل و هماهنگی مطابق با سناریو ارسال می‌شود. به روز رسانی‌هایی که توسط شرکت‌کنندگان و یا سرپرستان انجام می‌گردد مراحل تمرین را دائماً هدایت می‌کند.

۵-۲-۲ مایلستروم[۱]

مایلستروم[۱۸] یک بازی روی صفحه[۲] است که با موضوع فعالیت پیشرفته دشمن در حمله به یک شبکه دفاعی ایجاد و طراحی شده است. این بازی بر پایه مدل چرخه زنجیره‌ای برای حملات سایبری[۳] مارتین لاکهید[۱۹] و تاکتیک‌های مهاجمان، تکنیک-ها و دانش «ام آی تی آر ایی[۴]» ، «ا تی تی و سی ک[۵]» و شمارش و طبقه بندی الگوی مشترک حمله[۶] («سی ا پی ایی سی») و چارچوب مهندسی انعطاف پذیری سایبر[۷] می‌باشد[۲۱].

«ا تی تی و سی ک» یک مدل تهدید جمعیتی است که تاکتیک‌ها و تکنیک‌های مفصلی را که توسط مهاجمان سایبری استفاده می‌شود در شبکه‌های سازمانی به کار می‌برد. «سی ا پی ایی سی» یک مدل و کاتالوگ از الگوهای حمله است.

این بازی دارای چندین سطح دشواری است، به دو یا چند بازیکن اجازه می‌دهد تا نقش‌های مهاجم و مدافع را به عهده بگیرند. بازیکنان به نمایندگی از مهاجمان سعی می‌کنند از طریق قدم‌های زنجیره‌ای کشتن سایبر حرکت کنند تا به هدف "اقدام بر روی اهداف" برسند، در حالی که بازیکنان مدافع تلاش می‌کنند از طریق اقدامات مختلف به دنبال راه حلی باشند که از پیشرفت مهاجمان جلوگیری کند. بازی در یک تخته بازی با کارت، تاس، تکه‌های بازی، کاغذ، قلم و پول بازی صورت می‌گیرد. این کارت‌ها با توازن نقش فناوری و تجارت، اقداماتی را که مهاجمان و مدافعان می‌توانند انجام دهند ، نشان دهد. بازی مذکور قابل دانلود می‌باشد[۸].

[1] Mael strom
[2] Board Game
[3] cyber kill chain lifecycle model for cyber attacks
[4] MITRE
[5] MITRE's Adversarial Tactics, Techniques & Common KnowledgeTM (ATT&CKTM) (https://attack.mitre.org)
[6] Common Attack Pattern Enumeration and ClassificationTM (CAPECTM) (https://capec.mitre.org)
[7] Cyber Resiliency Engineering Framework
[8] https://github.com/maelstromthegame/defcon24.

۵-۲-۳ باشگاه سایبر

باشگاه سایبر[1] توسط شرکتی از رژیم اشغالگر قدس ساخته شده است. باشگاه سایبر برای تسهیل تمرینات رومیزی در سازمان‌های خدمات مالی اروپا و انگلستان استفاده می‌شود که عمدتاً از یک بستر کاربردی دستی برای شبیه‌سازی سناریوهای دفاع و حمله سایبری استفاده می‌کند. این برنامه شامل تیم‌های قرمز، تیم آبی و نقش‌های مدیریت/تیم سفید است.

۵-۲-۴ سیم اسپیس[2]

سیم اسپیس برای تجاری‌سازی و گسترش فناوری‌های بودجه دولتی برای آزمایش امنیت سایبری، از جمله شبیه‌سازی حجم حملات خوش خیم سایبری شکل گرفت. این شرکت همچنین چندین محصول پشتیبانی بازی جنگ سایبری از جمله تست فنی و اتوماسیون ساخت محیطی را تولید می‌کند. علاوه بر این این شرکت براساس سناریوی از طرف مقابل که در داخل شبکه فعالیت می‌کند آموزش‌هایی ارائه می‌دهد. یکی دیگر از خدمات این شرکت ایجاد تمرین‌هایی برای بهبود واکنش‌ها در زمان واقعی در برابر حملات زنده و چندمرحله‌ای از منابع خارجی و داخلی می‌باشد.

۵-۲-۴ زبان دشمن سایبری و موتور تصمیم‌گیری برای اتوماسیون تیم قرمز «سی ا ال دی ایی آر ا»

زبان دشمن سایبری و موتور تصمیم‌گیری برای اتوماسیون تیم قرمز[۲۲] یک فناوری توسعه یافته مدل «ام آی تی آر ایی» و یک چارچوب برای مدل تهدید دشمن «ا تی تی و سی ک» است. هدف آن خودکارسازی تقلید از رفتارهای تهدید سایبری است که برای آزمایش دفاعی و گسترش تجزیه و تحلیل مؤثر است. مدل «سی ا ال دی ای آر ا» این امکان را فراهم می کند که با خودکار کردن اجرای متوالی تکنیک های تهـاجمی «ا تی تی و سی ک» از یک تیم قرمز شبیه‌سازی شده و یک موتور برنامه‌ریزی استفاده شود. در حال حاضر اتوماسیون نفوذ برای تأثیر در پرونده‌ها، پردازش‌ها، فعالیت‌های شبکه و پیکربندی‌های سیستم به عنوان مبنایی برای آزمایش و بهبود تجزیه و تحلیل

[1] https://www.cybergym.com/
[2] SimSpace

تشخیص استفاده می‌شود. همچنین از این مدل برای آزمایش فناوری‌های دفاعی در بستر خودکار استفاده می‌شود.

۵-۳ محیط تمرین و ابزارهای آن

در این بخش محیط‌هایی که برای پشتیبانی از تمرینات پیشرفته بازی جنگ سایبری استفاده می‌شود خلاصه و دسته‌بندی می‌گردد. در حالی که برخی از آنها ممکن است برای استفاده از بخش خدمات مالی از طریق یک فروشنده تجاری در دسترس باشند، برخی دیگر به عنوان نمونه محیط‌هایی که در جای دیگر برای این تمرینات استفاده می‌شوند گنجانده شده است.

۵-۳-۱ آزمایش جنگ سایبری فورت مید[1]

آزمایشگاه فورت مید، واحد جنگ سایبری سفارشی است که در فورت‌مید[۲۳] ایالت مریلند واقع شده است و مسئول شکار هکرهای دشمن، شناسایی نحوه عمل آنها و توسعه تسلیحات سایبری برای استفاده علیه مجموعه‌ای از اهداف آنلاین است. این آزمایشگاه دارای محیطی آزمایشی برای آموزش و تربیت هکرها است. محیط آزمایشی آن بدینگونه است که افراد تحت آموزش به دو دسته قرمز و آبی تقسیم شده اند و هرکدام مسئولیت و مأموریت‌های خاصی را بر عهده دارند. در این محیط، تیم قرمز بایستی دیوار حفاظت اطلاعاتی شبیه‌سازی شده توسط سازمان امنیت ملی را دور زده و وارد آن شود و به اطلاعات مهم در آن دست یابد، همزمان تیم آبی مسئولیت حفاظت این اطلاعات را داشته و باید در برابر هجوم هکرهای تیم قرمز مقاومت کرده و اجازه شکستن دیوار اطلاعاتی را به آنها ندهد. درنتیجه این تمرینات و آموزش‌ها، هکرها تجربه و توانایی لازم برای انجام مأموریت‌های سایبری را کسب کرده و از آن استفاده می‌کنند.

۵-۳-۲ سازمان امنیت ملی

سازمان امنیت ملی[2] یک دپارتمان در وزارت دفاع ایالات متحده (DoD) است که مسئولیت ایجاد یک محیط امن و غیرقابل نفوذ برای انجام آموزش، آزمایش بوده و همچنین امکان ارزیابی عملیات‌های واقعی انجام شده برای امنیت سایبری را فراهم

[1] Fort Maede
[2] National Cyber Range

می‌کند[۲۴]. این سازمان قادر به ارائه تست‌هایی در سطوح مختلف و طبقه‌بندی شده را دارد تا جایی که قادر به برگزاری چهار تست مختلف و غیر مرتبط به هم است. این مرکز از چهار جزء مهم تشکیل شده است که عبارتند از: بخش ایجاد تأسیسات ایمن، بخش تکمیل ابزار و وسایل لازم برای انجام آزمایشات سایبری، بخش تهیه ابزار اتوماتیک برای بسترسازی و ایجاد یک آزمایش سایبری، متناسب با ساختارهای سایبری شکست خورده و بخش تربیت و پرورش کارمندان ماهر برای پشتیبانی از وقایع سایبری.

۵-۳-۳ آزمایش تطابق فضای تمرینی با عملیات حقیقی لینکلن[1]

آزمایش تطابق فضای تمرینی با عملیات حقیقی لینکلن، توسط آزمایشگاه فناوری ماساچوست (MIT) طراحی و راه اندازی شده است که می‌تواند یک محیط آزمایشی شبیه‌سازی شده را فراهم کند، این محیط به تقلید از شبکه‌ای ایجاد شده است که دارای ویژگی‌هایی ازقبیل: وجود تعداد بسیار زیادی میهمان‌های مجازی به همراه نرم-افزارهای کاربردی مرتبط و امکان شبیه‌سازی فعالیت‌های کاربر مانند مرور وب و پردازش ایمیل، می‌باشد[۲۵]. همچنین این محیط آزمایشی، امکان ارزیابی حملات و دفاعیات صورت گرفته در لایه‌های شبکه‌ای با تقلید در اتصال به اینترنت را فراهم می-آورد.

۵-۳-۴ سیم‌اسپیس

سیم‌اسپیس در واقع یک پلتفرم (محصول) برای اندازه‌گیری نحوه واکنش سیستم امنیتی شما هنگام روبرو شدن با حملات سایبری واقعی و پایدار است. این پلتفرم ابزار اتوماتیکی را ارائه می‌دهد که توانایی پشتیبانی از محدوده سایبری ملی را داشته و قالبیت‌هایی از قبیل ایجاد یا بازآفرینی، دسته‌بندی و اعتبار سنجی محیط‌های مجازی شکل گرفته برمبنای زیرساخت‌های موجود را دارد. این پلتفرم همچنین ابزارهای ارزیابی برای جمع آوری و تجزیه و تحلیل داده‌ها را در طی یک رویداد آزمایشی فراهم می‌کند علاوه بر این، یک مجموعه تکرار شونده از زیرساخت‌های موجود را برای پشتیبانی از کنترل اندازه‌گیری‌های موثر تولید می‌کند.

---

[1] LARIAT

۵-۴ شبیه‌سازی‌ها

شبیه‌سازی‌ها در واقع نمونه‌هایی ساده از عملیات‌های احتمالی سایبری را فراهم می‌کند که کاربران و تصمیم‌گیران با توجه به آن قادر خواهند بود تصمیمات صحیح اتخاذ نمایند، در زیر مثال‌هایی از مؤلفه‌های شبیه‌سازی آورده شده است که بطور خاص برای انواع مختلف بازی جنگ سایبری، تهیه و استفاده شده‌اند.

۵-۴-۱ تجزیه و تحلیل اثرات مأموریت اقدامات سایبری «ا ام آی سی ا»[1]

تجزیه و تحلیل اثرات مأموریت اقدامات سایبری یک نمونه ساده و اولیه از سیستم شبیه‌سازی سایبری است که طرح عملیات (مدل فرآیند)، شبیه‌سازی‌های انجام شده برای رویدادهای مجزا در حین عملیات، طرح‌های مبتنی برنمودار و واقعیت مجازی عملیات را باهم ترکیب می‌کند[۲۶]. این سیستم، فرآیند انجام شده برای مدل‌سازی وظایف مأموریت و تاکتیک‌ها، تکنیک‌ها و روش‌های اتخاذ شده برای مهاجم و مدافع سایبری را ضبط می‌کند. این سیستم را می‌توان به همراه یک مدل کاربردی در اختیار مأموران و اپراتورهای وزارت دفاع (افرادی که مسئول یک مأموریت نظامی در دنیای واقعی بوده‌اند) قرارداد تا از آن برای مدل‌سازی و شبیه‌سازی کردن تأثیر حملات سایبری مأموریت‌های واقعی استفاده کنند.

۵-۴-۲ هزارتوی هک شبکه‌ای[2]

هزارتوی هک شبکه‌ای، یک شبیه‌ساز هکری چند کاربره، مبتنی بر ترافیک کاربر برای رایانه‌های شخصی است که تحت پلتفرم شرکت استیم[3] منتشر شده است. این برنامه، اقدامات تهاجمی را با استفاده از روش‌های رایج و ابزارهای هک و تقلیدهایی مبتنی بر سیستم یونیکس، شبیه‌سازی می‌کند. این سیستم تاکتیک‌های تدافعی تیم آبی (محافظت‌کننده از اطلاعات) را گسترش می‌دهد. نحوه امتیازگیری در این سیستم به صورت میزان اقدامات دفاعی موفق می‌باشد و همچنین این بازی از پروژه منبع باز «هکنت[4]» گرفته شده است.

---

[1] AMICA
[2] Hacknet Labyrinths
[3] Steam Gaming
[4] Hacknet

۵-۵ تاکتیک تقلید متقابل[1]

برای هدایت و پیشبرد بازی در بازی‌های سایبری، به یک سری تاکتیک‌ها و روش‌هایی مانند روش تقلید متقابل نیاز است. تقلید متقابل به یک سری عملیاتی گفته می‌شود که شما با آنالیز طرف مقابل (دشمن) عیناً همان حرکات و تاکتیک را برای پیشبرد اهداف خود در بازی، درنظر می‌گیرید. اما به طور کلی انجام این تاکتیک نیازمند یک سری روش‌های دقیق می‌باشد.

تقلید متقابل، نیازمند آنالیز دقیق از مدل رفتاری و قابلیت‌ها و توانایی‌های خاص فردی دشمن و هچنین انگیزه‌های دشمن و ارتباط بین آنها دارد که این می‌تواند بسته به نوع دشمن متفاوت باشد (همه دشمنان به یک روش عمل نمی‌کنند) البته این دشمن می‌تواند از دسته تیم‌های انسانی باشد که به منظور شبیه‌سازی بازی، در نقش دشمن، وظیفه انتخاب و هدایت تاکتیک حمله را داشته باشد.

حالت اول از طریق استفاده از یک مدل تهدید خاص، به همراه مجموعه‌ای از قواعد و وظایف ارائه می‌شود. این حالت شامل گزارشاتی از قبیل: مدل‌سازی تهدید سایبری، بررسی، ارزیابی و چارچوب نمایشگر تاکتیکی می‌باشد. این گزارشات یک چارچوب و بنای مدل‌سازی تهدید سایبری را فراهم می‌کند و نمونه‌ای از مدل تهدید سطح بالا را که روی بخش خدمات مالی تأکید شده است ارائه می‌دهد[۲۷]. ممکن است بسته به سطح بازی جنگ سایبری، ابزار نشان کردن نقش دشمن متفاوت باشد. در تمرینات تهاجمی/ دفاع تیمی، از رنگ قرمز برای بازی کردن در نقش مقابل استفاده می‌شود. تیم‌های قرمز معمولاً متشکل از افرادی هستند که در نفوذ مستقیم سیستم‌های رایانه‌ای آموزش دیده و با تجربه هستند. افرادی که برای نفوذ انتخاب می‌شوند معمولاً استعداد خوبی در جلب توجه دارند زیرا این افراد مهارت‌های لازم برای ورود به سیستم، ایجاد کنترل و پایداری و حرکت جانبی (عرضی) به روش دشمن پیشرفته (افرادی درتیم مقابل با قابلیت فنی بالا) را دارند. در محدوده آزمایش نفوذ، مجموعه مهارت‌های مختلفی از جمله هک زیرساخت‌ها، هک کردن برنامه‌های وب و تخصص‌های مربوط به سازش و پایداری در ویندوز، لینوکس یا سایر سیستم عامل‌ها در دسترس است. کیت ابزاراستفاده شده توسط تیم قرمز (تیم حمله کننده یا مهاجم)

[1] Adversary Emulation

شامل ترکیبی از محصولات منبع باز مانند: «متاسپلویت[1]» ، «ان مپ[2]» و «نسوس[3] » با محصولات رایج و تجاری مانند: «کورایمپکت[4] »، «کوبالت استریک[5]» و «برپ سوویت[6] » می‌باشد. در بازی‌های جنگ سایبری رومیزی، تقلید از طرف مقابل می‌تواند با داشتن اطلاعات و آگاهی کمتری نسبت به مراحل انجام حمله سایبری نیز انجام شود و لزوماً نیازی به تجربه عملی ندارد. در این بازی (تمرین) می‌توان اقدامات دشمنان را تحت عنوان اقداماتی موسوم به اقدامات کارت سفید یا اختصاص دادن یک سری لغات خاص از قبل تعیین شده، که نشان دهنده اقدامات دشمن می‌باشد، به عنوان بخشی از تمرین نیز در نظرگرفت. علاوه بر اینها یکسری روش‌های جدید تقلید متقابل اتوماتیک، مبتنی بر وجود اطلاعات بیشتری درباره تاکتیک و تکنولوژی استفاده شده توسط دشمن، مانند روش حمله میتر[7] در حال ظهوراست.

۵-۶ تمرین‌ها و سناریوها

برای بازی جنگ سایبری و تمرین‌های مربوطه، برخی سناریوها در نظر گرفته می‌شود که در زیر تعدادی از انواع تمرین‌ها و سناریوهای مشخص تشریح می‌گردد.

۵-۶-۱ سری همیلتون

تمرین اتحاد همیلتون یکی از سلسله تمرینات مشترک دولت ایالات متحده و شرکت تأمین کننده نرم‌افزارها و سیستم‌های بانک جهانی بود که توسط وزارت خزانه‌داری و سازمان امنیت ملی تحت حمایت بود. آمارهای اولیه سری همیلتون برروی پیامدهای بوجود آمده ناشی از سناریوهای خاص تهاجمی، قابلیت‌های مرتبط به هم و فرآیندهای موجود در هر بخش سازمان، متمرکز بود. تمرین اتحاد همیلتون شامل شرکت‌های FSS، شورای هماهنگی بخش خدمات مالی، تنظیم کننده‌های فدرال و سازمان امنیت ملی بود. سناریوهای بازی جنگی، مبتنی بر اشتراک اطلاعات بین مؤسسات دولتی و بخش خصوصی بود و انواع مکانیزم ارتباطی در زمان وقوع حادثه، با هدف تقویت

[1] Metasploit
[2] Nmap
[3] Nessus
[4] CORE Impact
[5] Cobalt Strike
[6] Burp Suite
[7] Mitre’s Attacking

کارآیی و اثربخشی تدکرات در راستای خصوصی‌سازی و طبقه‌بندی مرزهای بین آنها از طریق رابطهایی مانند مرکز اشتراک اطلاعات و تجزیه و تحلیل خدمات مالی تمرین شد.

۵-۶-۲ سری سِحر کوانتومی

سری سِحر کوانتومی بازی‌های سایبری، در واقع از سری تمرینات رومیزی بودند، که به منظور واکنش به اتفاقات رخ داده، تجزیه و تحلیل آنها و هماهنگ سازی عملیات‌های آنها، برای شرکت‌های تأمین کننده نرم‌افزارها و سیستم‌های بانک جهانی و زیرمجموعه‌های آنها که با سطح وسیعی از حملات سایبری مواجه بودند، درنظر گرفته شد[۲۸].

بازی‌های جنگی سِحر کوانتومی[1] توسط انجمن صنایع و اوراق بهادار و بازارهای مالی ارائه شد. محصول تولید شده تحت عنوان «نوآری دیساید[2]» به منظور پشتیبانی از اتوماتیک‌سازی سناریوها استفاده می‌شد. شرکت‌کنندگان در این بازی، شامل تعداد بسیار زیادی از اعضای بخش خدمات مالی، مرکز اشتراک اطلاعات و تجزیه و تحلیل خدمات مالی، سازمان امنیت ملی آمریکا، ضابطهای‌قضایی (پلیس و نیروی انتظامی و..) و آژانس‌های نظارتی بودند.

۵-۶-۳ تمرین 2016 آر اس آ

بخش یادگیری آزمایشی کنفرانس ۲۰۱۶ آر اس آ، شامل تمرینی برای مقابله با بحران سایبری خدمات مالی بین المللی، تحت عنوان "بخش مالی و ارزیابی چشم انداز تهدیدها" بود[۲۹]. این رویداد برای انجام تمرینی بود که برنامه‌ریزان و بازیکنان در یک اتاق برای اجرای تمرین در کنار هم بوده و اینکار بحث و گفتگو را درمورد سناریوی نوشته شده آسان می‌کرد.

5-6-4 2016 آر اس آ سنگاپور

دربخش یادگیری آزمایشی کنفرانس RSA ناحیه آسیا و اقیانوسیه و ژاپن که در سنگاپور برگزار گردید، تمرین میمون سایبری[3]، یک تمرین رومیزی مبتنی بر سناریو از

[1] Quantum Dawn War Games
[2] NUARI DECIDE
[3] Cyber-Monkey

پیش نوشته شده (نقش‌ها در آن مشخص شده‌اند مانند بازی دزد و پلیس)، برای بخش مدیریت اجرایی بود تا نقش یک نفوذ سازماندهی شده‌ای را بازی کند که در حوزه‌ی مدیریت و پیام رسانی عمومی قرار دارد[۳۰]. این تمرین بر روی عملکرد مدیریت مرکز عملیات امنیتی و به طور ویژه بر روی مدیریت ارشد اطلاعات متمرکز بوده است؛ این مدیر ارشد با هیئت مدیره در ارتباط است؛ سخنگوی هیئت مدیره با رسانه‌ها در ارتباط است و مدیر ارشد اجرایی تحت نظارت نهاد دولتی است.

۵-۶-۵ مجموعه طوفان سایبری امنیت ملی آمریکا[1]

مجموعه‌ی بازی‌های جنگی طوفان سایبری امنیت ملی آمریکا توسط دفتر پشتیبانی امنیت سایبری و ارتباطات امنیت ملی آمریکا پشتیبانی می‌شود. بازی‌های طوفان سایبری سازمان امنیت ملی آمریکا تمریناتی هستند که معمولاً در سطح ملی بر روی فرایندهای پاسخ به رخدادها و آمادگی در برابر آن‌ها متمرکز هستند. این تمرینات که بر پایه‌ی سناریو طراحی شده‌اند و حملات سایبری را بر روی پارامترهای زیرساختی حیاتی از جمله سرویس نام دامنه[2] و مسیریابی ترافیک اینترنتی شبیه‌سازی می‌کند و بر سیستم‌های شرکتی و دولتی تأثیر می‌گذارد. پاسخ‌ها با محوریت پیشگیری، محافظت، کاهش، پاسخ‌گویی و بازیابی از رخدادها مورد ارزیابی قرار می‌گیرند. این بازی‌ها به منظور افزایش آگاهی از تهدیدات، تقویت اشتراک‌گذاری اطلاعات و بهبود پاسخ‌گویی به رخدادهای پروتکل‌های حساس به زمان طراحی شده‌اند.

۵-۶-۶ کنفرانس لاس وگاس[3]

این کنفرانس، یک کنفرانس سالانه است که در کنار همایش‌های «بلک هت[4]» و «دفکان[5]» برگزار می‌شود. یکی از فعالیت‌هایی که در آن صورت می‌گیرد؛ رویداد بازی فناوری جنگی بین تیم‌های دفاعی که باهم در رقابت هستند، می‌باشد. و این رویداد شامل یک تیم قرمز، تیم آبی، تیم سفید و فرآیندهای اداری است. این رویداد،

---

[1] DHS Cyber Storm
[2] DNS
[3] B Sides Las Vegas
[4] Black Hat
[5] DEFCON

سناریویی که مربوط به نظارت بر مدیریت حوادث غیر فنی باشد را شامل نمی‌شود؛ با این حال، سناریو شامل یک سری وظایف اجرایی است که باید توسط تیم آبی انجام بپذیرد که به منظور شبیه‌سازی وظایف و نقش‌های انسانی، همانند تمرینات سازمان یافته شرکتی طراحی شده است. در محدوده وظایف تیم آبی، سیستم اجرایی در اختیار آنها قرار داده شده و از آنها خواسته می‌شود ضمن حفظ سرویس‌های مهم بیرونی مانند وب و ایمیل، سیستم‌های خود را پیکربندی کنند. اعضای تیم قرمز به ابزارها و سیستم هکری برای شروع حملات مجهز شده‌اند. روش امتیازدهی بر اساس مدت زمان طی شده برای اجتناب کردن از علامت "flags" یا ضبط فایل‌ها، انجام وظایف اجرایی و توانایی مدافعان در محدود کردن نفوذ مهاجمان می‌باشد که این توانایی از طریق تعداد سیگنال‌های راهنمایی که با موفقیت در سیستم‌های دفاعی توسط مهاجمان برای ارسال اطلاعات درون سیستم کاشته شده‌اند، قابل ارزیابی است. رویداد لاس وگاس ۲۰۱۷ شامل معرفی اولیه عناصر بازی جنگ ترکیبی بود. مفهوم پول به عنوان یک منبع محدود و قابل جمع‌آوری در بازی به عنوان تمرین فنی به تیم آبی یا تیم قرمز، معرفی شدند. تیم آبی می‌تواند از پول برای بالا بردن قابلیت‌هایی بهره ببرد که باعث تقویت مکانیسم دفاعی در زیرساختارهای سامانه‌های این تیم می‌گردد. دفاع موفقیت-آمیز در برابر حملات تیم قرمز، باعث افزایش موجودی پول با گذشت زمان شود. هدف بازی از افزودن المان‌های جدید در راستای مفهوم بازگشت سرمایه قرار دارد.

۵-۶-۷ سری بانک‌های انگلیس

بانک مرکزی انگلیس برای بخش مالی انگلستان مجموعه‌ای از بازی‌های سایبری رومیزی را راه‌اندازی کرده است. این بازی‌ها شامل، رزیلینت شیلد[1] است که در سال ۲۰۱۵ با همکاری U.S.8 برگزار شد[۳۱]، که هیچ مشکلی در سیستم زنده نداشت و بر روی اشتراک‌گذاری اطلاعات و برنامه‌ریزی متمرکز بود. تمرینات قبلی، واکینگ شارک[2] در ۲۰۱۱ و واکینگ شارک۲ در ۲۰۱۳ ، شامل چندین سناریو با حملات شبیه‌سازی شده بود[۳۲].

[1] Resilient Shield
[2] Walking Shark

۵-۶-۸ رویداد ضبط سیگنال‌های راهنما

رویدادهای ضبط سیگنال‌های راهنما، رویدادهای سایبری زنده است که در آن، به شرکت کنندگان چالش‌هایی مانند تغییر پرونده یا به دست آوردن امتیازات ویژه، برای دستیابی به سیستم هدف داده می‌شود. رویدادهای ضبط سیگنال‌های راهنما معمولاً ساختار کمتری دارند و مبتنی بر سناریوی مأموریت نیستند. این رویدادها توسط طیف گسترده‌ای از سازمان‌های مختلف در محیط‌های علمی، همایش‌های دولتی یا شرکت‌ها برگزار می‌شود. زیر مجموعه‌های توضیح داده شده در زیر نمونه‌هایی از این پروژه هستند[۳۳].

۵-۶-۹ هفته آگاهی از امنیت سایبری دانشگاه نیویورک

هفته‌های آگاهی از امنیت سایبری دانشکده مهندسی دانشگاه تندون دانشگاه نیویورک هر ساله برگزار می‌شود و شامل یک مسابقه ضبط سیگنال است. این مسابقات مربوط به هک کردن در سطح ورودی بدون ساختار است که بر حملات تهاجمی به برنامه‌های آسیب‌پذیر متمرکز است. معیارها بر اساس "سیگنال های راهنما" یا پرونده‌های ضبط شده است با اختصاص دادن امتیازهای متفاوتی برای هر یک ساخته شده‌اند. هیچ سناریوی عملیاتی برای هدایت فعالیت‌ها استفاده نمی‌شود و فقط یک تیم سفید اجرایی برای ارزیابی و کنترل بازی استفاده می‌شود.

۵-۶-۱۰ ضبط سیگنال دیفکن

رویداد ضبط سیگنال به عنوان بخشی از کنفرانس امنیتی دفکن هر سال در لاس وگاس برگزار می‌شود. این یک بازی به سبک دفاعی است که به یک سری تیم‌های پخش کننده نیاز دارد تا با استفاده از مهندسی معکوس دودویی، به شناسایی نقاط ضعف سیستم مقابل و حمله به آنها پرداخته و با به خطر انداختن سیستم‌های رقبا ضمن دفاع از خود، امتیاز برای خود بدست آورند. این یک فرمت بدون سناریو با تجهیزات، مهندسی و عملیات نسبتاً ساده است که بر ایجاد چالش‌های فردی در بازی، با محوریت مهندسی معکوس دودویی، سرهم بندی و بهره برداری از آنها متمرکز است. معیارها و امتیاز دهی‌ها براساس تکمیل چالش‌های فردی صورت می‌گیردکه مشروط بر انجام سایر کارها نیست.

۵-۶-۱۱ همایش ملی ضبط سیگنال دانشگاه سانتا باربارا

همایش ملی ضبط سیگنال توسط دانشگاه کالیفرنیا سانتا باربارا با استفاده از آزمایش امنیتی و چارچوب آی سی تی اف[1] (در یک بازی جنگی چند منظوره و چند تیمی با حضور تیم‌هایی که به طور مستقل در مقابل یکدیگر به رقابت می‌پردازند) برگزار می-شود و از الگوی معمولی تمرینات تیم آبی که شامل محافظت از خدمات سیستم و پرونده‌های موجود در سیستم در برابر ضبط شدن آنها توسط بازیکنان تیم مقابل است، پیروی می‌کند. امتیازدهی به صورت سیگنال‌های ضبط شده از سیستم‌های تیم‌های دیگر می‌باشد.

۵-۶-۱۲ نمایش توانایی‌های دفاعی

فعالیت‌های اجرایی در حال پیشرفت هستند، تا بتواند توانایی‌های آگاهی و درک موقعیتی را برای شناسایی فعالیت‌های پس از سازش در شبکه ها و سیستم ها بهبود بخشد. پروژه های تجاری و منبع باز در حال پیشرفت و رسیدن به یک بلوغ در توانایی و قابلیت ها هستند. این فعالیت‌ها اغلب به منظور یکپارچه‌سازی فعالیت‌های قبلی هستند و همچنین حمایت از توسعه سنسورهای جدید سایبری مبتنی بر آنالیز و تعریف روابط بین داده‌ها، برای پشتیبانی از پاسخ‌های دفاعی سایبری در برابر وقایع کمک می‌کند. توسعه یک منبع اطلاعاتی مشترک و قابل استفاده مجدد از تجزیه و تحلیل برای تشخیص در برابر بردارهای تهاجمی شناخته شده و حمایت از واکنش سریعتر نسبت به بردارهای در حال تغییر، موضوعی رایج در صنعت است.

۵-۷ منبع تحلیلی سایبری[2]

با استفاده از چهارچوب تهاجمی، یک منبع سایبری آنالیتیکس برای پشتیبانی از مدافعان سایبری ساخته شده است. برای هر تحلیلی ، این مخزن شامل موارد زیر است:

- فرضیه ای که ایده تحلیلی را توضیح می دهد
- زمینه عملیاتی (به عنوان مثال ، میزبان ، شبکه ، فرآیند ، خارجی)

[1] iCTF
[2] CAR

• مراجع مقابل چارچوب‌های تهاجمی

• تشریح مفصل از وظایفی که برنامه پتانسیل انجام آن‌را دارد

• شناسایی آن دسته از اطلاعات سنسور که برای تحلیل نیاز است

آنالیز و تعریف روابط بین داده‌ها نظیر آنچه در سی ای آر تعبیه شده است می‌تواند مبنای لازم را برای ایجاد یک مدل بازنگری شده از عملکرد سنسورها و تجزیه و تحلیل آن‌ها در یک بازی جنگ سایبری فراهم کند. همچنین درک و واقع‌گرایی بیشتری را نسبت به رویدادهای دارای کارت سفید فراهم می‌کند، بدون اینکه در واقع سنسورها و آنالیزها را در یک بستر آزمایشی به عنوان بخشی از بازی اجرا کند[۳۴].

۶- خلاصه و نتیجه گیری

۱- اجزای بازی جنگ سایبری عبارتند از:

- چارچوب‌ها و مدل‌های تعیین بازی جنگ سایبری
- بسترهای اجرایی بازی جنگ سایبری
- فضای تمرین و ابزار آن
- شبیه‌سازی‌های قابل اجرا برای بازی جنگ سایبری
- بازنمایی‌های دشمن
- تمرین‌های موجود و سناریوها

۲- از چارچوب‌ها و مدل‌های تعیین بازی جنگ می‌توان کیت ساخت و ساز بازی جنگ، بازی جنگ تجاری و پیشنهادات تجاری با ابزار اختصاصی را نام برد.

۳- بسترهای انجام بازی جنگ که در این پژوهش ارائه شده است فضای طراحی شده برای تمرین‌های تصمیم‌گیری در شرایط بحرانی، مایلستروم، باشگاه سایبر، سیم اسپیس، زبان دشمن سایبری و موتور تصمیم‌گیری برای اتوماسیون تیم قرمز می‌باشد.

۴- فضای های تمرینی ذکر شده عبارتند از: آزمایش جنگ سایبری فورت مید، سازمان امنیت ملی، آزمایش تطابق فضای تمرینی با عملیات حقیقی لینکلن.

۵- در بخش شبیه‌سازی‌های قابل اجرا تجزیه و تحلیل اثرات ماموریت اقدام سایبری و هزارتوی هک شبکه‌ای معرفی شده‌اند.

۶- برخی از سناریوهای تمرین، سری همیلتون، سری سحر کوانتومی، مجموعه طوفان سایبری امنیت ملی آمریکا، سری بانک‌های انگلیس، رویداد ضبط سیگنال-های راهنما، نمایش توان‌هایی دفاعی می‌باشند.

۷- پیشنهادات

- معاونت آموزش ستاد آجا و نیروها نسبت به مزید نمودن موضوع « بازی جنگ و بازی جنگ سایبری» تحت عنوان یکی از سرفصل‌های آموزشی در تمامی مقاطع تحصیلی و دوره‌های آموزشی طولی در دانشگاه‌ها و مراکز آموزشی اقدام نمایند.
- در تمام رزمایش‌هایی که در نیروهای مسلح صورت می‌گیرد، یک مرحله از رزمایش به بازی جنگ سایبری اختصاص یافته و بسته به سطح رزمایش توسط معاونت‌های عملیات یا معاونت‌های آموزش در طراحی رزمایش‌ها لحاظ گردد.
- دانشگاه‌ها و مراکز پژوهشی نیروهای مسلح نسبت به ایجاد یک حرکت همه جانبه برای تولید محتوا در زمینه بازی جنگ سایبری در قالب پایان‌نامه‌ها، طرح‌های پژوهشی، ترجمه کتب و مقالات معتبر اقدام نمایند.
- مراکز تدوین آئین‌نامه در سطح نیروهای مسلح نسبت به تدوین دکترین و آئین‌نامه بازی جنگ سایبری اقدام نمایند.
- معاونت‌های فاوا نسبت به تهیه تجهیزات به روز، برای اجرای بازی جنگ یگان‌ها اقدام و در اختیار آن‌ها قرار دهند.
- معاونت‌های طرح و برنامه در سطح نیروهای مسلح پیش‌بینی ساختار و تجهیزات مناسب جهت اجرای وسیع بازی جنگ سایبری برای یگان‌های تابعه خود به عمل آورند.

مراجع

[1] Matthew Caffery Jr., “Toward a History-Based Doctrine for Wargaming,” Air and Space Power Journal 13, no. 3 (Fall 2000): 33.

[2] Michael E. Freeman, “Pushing the Envelope of Pedagogical Gaming: Dark Networks,” PS: Political Science & Politics 50, no. 04 (October 2017): 1, https://doi.org/10.1017/S1049096517001251.

[3] Caffery Jr., “Toward a History-Based Doctrine for Wargaming,” 36.

[4] Caffery Jr., “Toward a History-Based Doctrine for Wargaming,” 56.

[5] Daniel Griffin, “Resources: Gamification in e-Learning,” Ashridge Executive Education, 4, accessed August 14, 2017, https://www.ashridge.org.uk/virtual-ashridge/elearning-insights/resources-gamification-in-e-learning/.

[6] Dale, “Gamification,” June 1, 2014, 3.

[7] Daniel Griffin, “Resources: Gamification in e-Learning,” Ashridge Executive Education, 5, accessed August 14, 2017, https://www.ashridge.org.uk/virtual-ashridge/elearning-insights/resources-gamification-in-e-learning/; Steve Dale, “Gamification: Making Work Fun, or Making Fun of Work?,” Business Information Review 31, no. 2 (June 1, 2014): 3, https://doi.org/10.1177/0266382114538350.

[8] Kim and Lee, “Dynamical Model for Gamification of Learning (DMGL),” 9.

[9] Bunchball, “Bunchball,” April 29, 2011, http://www.bunchball.com.

[10] Griffin, “Resources,” 5.

[11] Sam S. Adkins, “The 2016–2021 Global Game-Based Learning Market — Serious Play Conference” (Ambient Insight, July 26, 2016), 7, http://seriousplayconf.com/downloads/the-2016-2021-global-game-based-learning-market/.

[12] David B.Fox, Catherine D.McCollum, Eric I.Arnoth, Darrell J.Mak,” Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context, Department of Homeland Security, 2018, pp15.

[13] Perla,P.,etal.2002.“Wargame-Creation Skills and the Wargame Construction Kit.” https://www.cna.org/cna_files/pdf/D0007042.A3.pdf

[14] Gilad, Benjamin, 2009, Business War Games: How Large, Small, and New Companies Can Vastly Improve Their Strategies and Outmaneuver the Competition, The Career Press, Inc.

[15] Cisco’sCyberRange,https://www.cisco.com/c/dam/global/en_au/solutions/security/pdfs/cyber_range_aag_v2.pdf and https://www.cisco.com/c/dam/en/us/products/collateral/security/spa-overview.pdf

[16] Deloitte’s offering, https://www2.deloitte.com/us/en/pages/risk/articles/cyber-risk-services-cyber-war-gaming.html and https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-cyber-war-gaming-sales-sheet-07272014.pdf

Optimal Risk, http://www.optimalrisk.com/Advanced-Cyber-Defence-Services/Cyber-War-Games [17]

Steiger, S. 2016. “Maelstrom: Are you playing with a full deck? Using an Attack Lifecycle Game to Educate, Demonstrate and Evangelize,” 2016. [18]

Lockheed Martin, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,” Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, Ph.D. [19]

Strom, B., et al. 2017. “Finding Cyber Threats with ATT&CKTM-Based Analytics,” MTR 170202, PR16-3713, The MITRE Corporation, June 2017. [20]

Bodeau, D., and Graubart, R. 2011. “Cyber Resiliency Engineering Framework,” MTR 110237, P114436, The MITRE Corporation, 2011 [21]

Applebaum, A., et al. 2016. “Intelligent, automated red team emulation,” Proceedings of the Annual Computer Security Applications Conference, December 2016. [22]

The MITRE Corporation. 2012b. “MITRE’s Fort Meade eXperiment (FMX): Research in Intra-Enclave-Level Cyber Defenses,” PR 12-3942, 2012 [23]

National Cyber Range (NCR). 2015. “National Cyber Range Overview.” http://www.acq.osd.mil/dte-trmc/docs/20150224_NCR%20Overview_DistA.pdf. [24]

Rossey, L., et al. 2002 .“LARIAT: Lincoln Adaptable Real-time Information Assurance Testbed,” Proceedings of the IEEE Aerospace Conference, 2002. [25]

Noel, S., et al. 2015. “Analyzing Mission Impacts of Cyber Actions (AMICA),” NATO IST-128 Workshop on Cyber Attack Detection, Forensics, and Attribution for Assessment of Mission Impact, Istanbul, Turkey. [26]

http://csis.gmu.edu/noel/pubs/2015_AMICA.

Bodeau, D., et al. 2018. “Cyber Threat Modeling: Survey, Assessment, and Representative Framework,” HSSEDI, The Mitre Corporation, April, 2018. [27]

Deloitte. 2014. “An introduction to cyber war games,” CIO Journal, September 22, 2014. http://deloitte.wsj.com/cio/2014/09/22/an-introduction-to-cyber-war-games/ [28]

Fox-IT. 2016. “Financial Sector and the Evolving Threat Landscape: Live Cyber Exercise,” RSA Conference Learning Labs. 2016. [29]

McCombie, S., et al. 2016. “Cyber-Monkey 2016, Learning Lab Summary,” RSA Conference Learning Labs. 2016. [30]

https://www.gov.uk/government/news/transatlantic-exercise-to-tackle-cyber-threat [31]

http://www.bankofengland.co.uk/financialstability/fsc/Documents/wakingshark2report.pdf [32]

More examples, and links to toolkits for developing capture-the-flag (CTF) events, can be found at http://resources.infosecinstitute.com/tools-of-trade-and-resources-to-prepare-in-a-hacker-ctf-competition-or-challenge/#gref [33]

David B.Fox, Catherine D.McCollum, Eric I.Arnoth, Darrell J.Mak,” Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context, Department of Homeland Security, 2018, pp23. [34]