فصلنامه علوم و فنون نظامی
سال چهاردهم، شماره ۴۵، پاییز ۱۳۹۷
صص ۷۴- ۵۳

تاریخ دریافت: ۱۳۹۷/۰۷/۲۷
تاریخ پذیرش: ۱۳۹۷/۱۲/۱۳

تبیین عملیات پایش فضای سایبری ارتش جمهوری اسلامی ایران در جنگ ترکیبی

رحیم بهاری*[۱]
داود آذر[۲]

چکیده

جنگ اطلاعاتی، جنگ نامتقارن، جنگ شبکه‌ای، جنگ سایبری، جنگ کلاسیک، جنگ بی‌قاعده و.... ازجمله حربه‌های اثرگذار در جنگ‌های ترکیبی مورد بهره‌برداری قرار می‌گیرد. با توجه به اینکه آجا از فضای سایبری در فناوری داده و اطلاعات بهره‌برداری وسیع به عمل می‌آورد، شناسایی و احصاء شیوه‌های کار و تمهیدات لازم می‌تواند کمک شایانی به ساماندهی و مدیریت آن در تولید و تبادل اطلاعات در محیط امن بنماید. محقق در این پژوهش عملیات پایش فضای سایبری ارتش جمهوری اسلامی ایران در جنگ ترکیبی را به‌عنوان متغیر تابع و عواملی چون شیوه‌های کار و تمهیدات را به‌عنوان عامل تأثیرگذار بر تابع اصلی مورد بررسی و پژوهش قرار می‌دهد. این تحقیق با استفاده از روش توصیفی و نوع کاربردی-توسعه‌ای اجرا و جامعه نمونه ۱۰۳ نفر تعیین گردیده و به‌منظور جمع‌آوری اطلاعات از ابزارهایی مانند مصاحبه، پرسش‌نامه و مطالعه اسناد و مدارک استفاده به‌عمل‌آمده است. یافته‌های موجود با استفاده از تحلیل محتوا، تحلیل روند، آمار توصیفی و استنباطی و در انتها به‌صورت آمیخته مورد تجزیه و تحلیل قرار گرفت و نتایج فرضیه‌ها حاکی از تأثیر بسیار بالای عملیات پایش فضای سایبری آجا در جنگ ترکیبی است. همچنین پایش پورت‌های «تی.سی.پی» و «یو.دی.پی»، شناسایی آسیب‌پذیری‌های شبکه، استخدام افراد متخصص و متعهد، بومی‌سازی برنامه‌ها و نرم‌افزارهای کاربردی و ایمن‌سازی تجهیزات فعال و غیرفعال شبکه مواردی است که بیشترین تأثیر را در عملیات پایش آجا در جنگ ترکیبی دارند.

واژه‌های کلیدی:
جنگ ترکیبی، فضای سایبر، عملیات پایش

---

[۱] کارشناس ارشد مدیریت دفاعی
[۲] کارشناس ارشد مدیریت دفاعی
* رایانامه نویسنده مسئول: bahari.r81320.ir@gmail.com

مقدمه

برخلاف جنگ‌های دهه‌های گذشته که بر پایه‌ی جنگ کلاسیک، اعمال خسارت و انهدام، فرسایشی و با تکیه بر استفاده از جنگ‌افزارها و تسلیحات پیشرفته، مبتنی بر مرز جغرافیایی و تصرف زمین بود؛ جنگ‌های آینده به‌سوی جنگ‌های هوشمند، ترکیبی، نیابتی، خارج از مرزهای بین‌المللی و مبتنی بر استفاده از زیرساخت‌های سایبری در ابزارها و جنگ‌افزارهای نظامی دارد. بدیهی است که تغییر ماهیت صحنه‌های نبرد آینده، چالشی است که دغدغه‌ی اصلی فرماندهان نظامی و بسیاری از پژوهشگران عرصه‌ی نظامی می‌باشد که این مهم هم‌اکنون با ظهور پدیده‌ی جنگ ترکیبی دوچندان گردیده است؛ در جنگ ترکیبی افزایش سرعت، دقّت، حضور عناصر عمده نیروهای منظم و نامنظم دولتی و غیردولتی، اقدام هم‌زمان، وسعت منازعات، انطباق سطوح مختلف برهم، پیشرفت فن‌آوری، عدم قطعیت صحنه‌ی نبرد و چندوجهی بودن فرماندهی جنگ، موجب پیچیدگی اجرای عملیات در صحنه نبرد شده است.
جنگ اطلاعاتی، جنگ نامتقارن، جنگ شبکه‌ای، جنگ سایبری، جنگ کلاسیک، جنگ بی‌قاعده و.... ازجمله مفاهیم مهم و اثرگذار در جنگ‌های ترکیبی است و بر اساس تعریف ارائه‌شده در اجلاس امنیتی مونیخ ۲۰۱۵، جنگ سایبری یکی از هشت ابزار برای جنگ ترکیبی می‌باشد (Ischinger,2015).

آجا به علت ماهیت مسائل نظامی و برخورداری از ویژگی‌های صحنه جنگ ترکیبی و بخش عمده‌ی آن جنگ سایبری، در این فضا حضور دارد. ازاین‌رو بخش مهمی از پایش فضای سایبر بر عملکرد دفاعی آجا در این فضا تأثیرگذار خواهد بود. مسئله اصلی این پژوهش، فقدان عملیات پایش فضای سایبری آجا در جنگ ترکیبی می‌باشد؛ بنابراین پژوهش حاضر به دنبال ارائه عملیات پایش فضای سایبری آجا در جنگ ترکیبی می‌باشد. هدف اصلی پژوهش، عملیات پایش فضای سایبری ارتش جمهوری اسلامی ایران در جنگ ترکیبی است و اهداف فرعی عبارت‌اند از: شیوه‌های کار پایش فضای سایبری در جنگ ترکیبی؛ تمهیدات لازم پایش فضای سایبری در جنگ ترکیبی. اهمیت وجود این تحقیق آن است که اولاً پورت‌های تی.سی.پی و یو.دی.پی به‌طور دقیق پایش گردیده و آسیب‌پذیری‌های شبکه، زیرساخت و بسترهای ارتباطی شناسایی شوند. ثانیاً از طریق استخدام و به‌کارگیری افراد متخصص و متعهد در حوزه‌های مختلف سایبری در جهت بومی‌سازی برنامه‌ها و نرم‌افزارهای کاربردی تلاش بیشتری به عمل آید. ثالثاً موجب دست‌یابی به یک روش مطالعه شده و سنجیده برای اجرایی شدن عملیات پایش فضای سایبری؛ متناسب با ظرفیت‌ها و توانمندی‌های آجا در جنگ ترکیبی گردد.

نبود تحقیق حاضر باعث می‌گردد تا افراد بدون تخصص در حوزه‌های مختلف سایبری، استخدام و به‌کاررفته شوند و در مورد بومی‌سازی برنامه‌ها و نرم‌افزارهای کاربردی تلاش مؤثر انجام نگیرد. از سوی دیگر، آسیب‌پذیری‌های شبکه، زیرساخت و بسترهای ارتباطی مطالعه و بررسی نگردد.

مبانی نظری و پیشینه پژوهش

جنگ

کلازویتس جنگ را این‌گونه تعریف می‌کند: جنگ عمل خشونت‌باری است که هدفش وادار کردن حریف به اجرای خواسته ماست، جنگ ادامه سیاست است، جنگ نه‌تنها ویژگی نظامی بلکه خصیصه دیپلماتی، روان‌شناختی و اقتصادی را نیز دارد. در تعاریف حقوقی از جنگ با رویکرد حقوق بین‌الملل چنین بیان‌شده است: جنگ عبارت است از درگیری مسلحانه بین دو یا چند کشور با قصد قبولاندن نظرات سیاسی یا اعمال هدف‌های خود با استفاده از تمام وسایلی که برای جنگ در اختیاردارند (ضیای بیگدلی،۱۳۷۳).

اصول هفت‌گانه جنگ ترکیبی

ازنظر تاریخی، فرآیندهای تشکیل هیبرید نقاط مشترکی ازنظر ترکیب و اثرات داشته است که می‌توان بر اساس این نقاط مشترک، هفت اصل را تعریف کرده، همچنین جنگ ترکیبی را می‌توان بر اساس این هفت اصل تشریح کرد:

اصل اول: ترکیب ظرفیت‌ها و اثرات جنگ ترکیبی در بستر و مقطع خاص مربوط به آن نیرو، منحصربه‌فرد است. این بسترها شامل: زمانی، جغرافیایی، اجتماعی، فرهنگی و تاریخی است که در آن مقطع جنگ رخ می‌دهد.

اصل دوم: ایدئولوژی خاصی در جنگ ترکیبی وجود دارد که این ایدئولوژی به‌طورمعمول، به زمینه راهبردی مرتبط است و ریشه در هویت اجتماعی، فرهنگی و دینی نیروی هیبریدی دارد.

اصل سوم: نیروی ترکیبی، معتقد است رقبای بالقوه در پی از بین بردن آن هستند. این احساس تهدید باعث می‌شود نیروی هیبریدی از خِرد نظامی متعارف دست کشیده تا بتواند هر چه بیشتر به بقای خود ادامه دهد.

اصل چهارم: همیشه یک اختلاف ظرفیت بین نیروی ترکیبی و دشمنان بالقوه آن وجود دارد. نیروی ترکیبی، ظرفیت نظامی کمتری نسبت به دشمن خود داشته و درنتیجه باید به دنبال راهی باشد که مزیت رقیب را جبران کند.

اصل پنجم: نیروی ترکیبی، هم دارای اجزای متعارف و هم نامتعارف است. این اجزا به‌طورمعمول شامل فن‌آوری پارتیزانی غیرنظامی است. همچنین ممکن است راهکنش‌های مجرمانه یا تروریستی در اجزای آن وجود داشته باشد.

اصل ششم: سازمان‌های ترکیبی، وابسته به عملیاتی هستند که ماهیت دفاعی دارند. نیروی ترکیبی تلاش می‌کند که از موجودیت خود دفاع کند. این عملیات چندین جزء هجومی نیز دارند اما گرایش اصلی آن دفاعی است.

اصل هفتم: سازمان‌های ترکیبی از راهکنش‌هایی استفاده می‌کنند که فرسودگی دشمن را به دنبال داشته باشد (الهیاری،۱۳۹۵).

ابزارهای جنگ ترکیبی

بر اساس تعریف ارائه‌شده در اجلاس امنیتی مونیخ ۲۰۱۵، هشت ابزار برای جنگ ترکیبی معرفی کرده است که به شرح زیر است (Ischinger,2015).

۱) دیپلماسی
۲) جنگ اطلاعاتی و پروپاگاندا
۳) حمایت از نابسامانی‌ها و شورش‌های محلی
۴) نیروهای نامنظم و چریکی
۵) نیروهای ویژه
۶) نیروهای کلاسیک نظامی
۷) جنگ اقتصادی
۸) حمله‌های سایبری

جنگ سایبر

جنگ سایبر زیرمجموعه‌ای است از جنگ اطلاعاتی که شامل اقداماتی می‌شود که در دنیای سایبر رخ می‌دهند، دنیای سایبر هرگونه واقعیت مجازی است که توسط مجموعه رایانه‌ها و شبکه‌ها ایجاد می‌شود. در جنگ سایبری بلوغ درنبرد وقتی اتفاق می‌افتد که با استفاده از جنگ‌افزارهای متصل به شبکه‌های رایانه‌ای، بدون اینکه لازم باشد در میدان نبرد حضور فیزیکی پیدا کرد، بتوان دشمن را با کمترین خطا مورد هدف قرارداد و نابود کرد (ماه پیشانیان،۱۳۸۹).

شیوه‌های کار تست نفوذ[1]

تست نفوذ، اقدامی پیشگیرانه و با مجوز از طرف سازمان مجری این تست است که وظیفه اصلی آن ارزیابی امنیت ساختارهای مبتنی بر فناوری اطلاعات می‌باشد. تست نفوذ به‌صورت معمول با استفاده از فنّاوری‌های موجود درزمینه‌ی امنیت، به‌صورت روال‌های از قبل تعریف‌شده و یا در صورت نیاز

1. penetration testing (PT)

تعریف توسط نفوذ گر صورت می‌پذیرد کـه ایـن امـر موجـب شناسـایی خطـرات موجـود در سـرورها، کاربران، برنامه‌های تحت وب، شبکه‌های بی‌سیم، تجهیزات شبکه، دستگاه‌های قابل‌حمل و هـر نقطـه‌ی دیگری که ظرفیت آسیب‌پذیری داشـته باشـد را شـامل مـی‌گـردد. وقتـی یـک سیسـتم آسـیب‌پـذیر شناسایی شد، ممکن است نفوذگر از طریق همان سیستم به‌صورت متناوب بـه شناسـایی منـابع دیگـر اقدام نماید که در این صورت به اطلاعات بیشتری از لایه‌های امنیتـی و نفـوذ بیشـتری در تجهیـزات و اطلاعات بدون محدودیت دست پیدا می‌کند.[1]

محیط فضای سایبر و حوزه‌های آسیب‌پذیر

محیط فضای سایبر شامل شش حوزه مشروحه زیر می‌باشـد کـه شـناخت آن، تحلیـل گـران و راهبرهای دفاع سایبری را در شناخت نقاط قوت و ضعف جبهه خـودی و دشـمن و حـوزه‌هـای آسیب‌پذیر آن یاری خواهد نمود (سید مفیدی، ۱۱۷:۱۳۸۸).

۱) کاربران و نیروی انسانی
۲) روش‌ها و رویه‌های اجرایی
۳) سخت‌افزارهای رایانه‌ای
۴) داده‌ها و اطلاعات
۵) نرم‌افزارهای رایانه‌ای
۶) شبکه‌های رایانه‌ای

ابعاد آسیب‌پذیر فضای سایبری

۱) آسیب‌پذیری عملیاتی (فیزیکی، نرم‌افزاری، سخت‌افزاری، شبکه، زیرساخت ارتباطی)
۲) آسیب‌پذیری اطلاعاتی (داده، ناشی از تشعشع)
۳) آسیب‌پذیری نیروی انسانی
۴) آسیب‌پذیری آموزش
۵) آسیب‌پذیری فناوری (سید مفیدی، ۱۱۷:۱۳۸۸).

روش‌های تست نفوذ

۱) سنجش آسیب‌پذیری (تست نفوذ) و ارزیابی امنیتی با داشتن کمینـه اطلاعـات لازم:[2] در این روش کارشناسان تست نفوذ بدون هـیچ‌گونـه اطلاعـاتی از شـبکه، اقـدام بـه تسـت می‌نمایند.

1. https://www.apk.co.ir/solutions/penetration-test/
2. Black box penetration testing

۲) سنجش آسیب‌پذیری (تست نفوذ) و ارزیابی امنیتی با داشتن بیشینه اطلاعات:[1] در این روش کارشناسان تست نفوذ با اطلاعاتی کامل از شبکه و زیرساخت‌های موجود، اقدام به تست می‌نمایند.

۳) سنجش آسیب‌پذیری (تست نفوذ) و ارزیابی امنیتی با داشتن پاره‌ای از اطلاعات:۲ در این روش تستر نفوذ به مانند یک کارمند سازمان، حق دسترسی به تمامی منابع را دارد و با این نوع دسترسی اقدام به ارائه تست می‌نماید.[3]

اکثر تسترها، جهت انجام تست نفوذپذیری معمولاً از روش سوم استفاده می‌نمایند، بدین ترتیب که مدیر شبکه با در اختیار گذاشتن دو نُود از شبکه خود و ارائه دسترسی‌های عمومی، امکان تست را فراهم می‌نماید. سپس تست‌های زیر توسط متخصصان تست نفوذ صورت می‌گیرد:

۱) پیمایش و بازدید از شبکه
۲) مرور کردن وضعیت پورت‌ها
۳) مشخصات نرم‌افزاری سامانه‌ها
۴) پویش در زمینه سرویس‌ها
۵) تست شبکه در مقابل آسیب‌پذیری‌ها
۶) استفاده از اکسپلویت‌های موجود و مقاومت سامانه‌ها
۷) تست برنامه‌های کاربردی
۸) تست‌های نفوذ در به دست آوردن پسوردها
۹) تست حملات تکذیب سرویس
۱۰) ارزیابی امنیتی شبکه‌های بی‌سیم
۱۱) بررسی دسترسی‌های از راه دور
۱۲) تست نفوذپذیری روترها و تجهیزات برقرارکننده ارتباطات
۱۳) تست نفوذپذیری تجهیزات و نرم‌افزارهای امنیتی شامل: سیستم پیشگیری از نفوذ، سیستم تشخیص نفوذگر و دیوارهای آتش و...
۱۴) تست نفوذپذیری بانک اطلاعاتی

شیوه‌های کار سیستم تشخیص نفوذ[4]

یک سیستم تشخیص نفوذ را می‌توان مجموعه‌ای از ابزارها، روش‌ها و مدارکی در نظر گرفت که به

1. White box penetration testing
2. Gray box penetration testing
3. www.armandata.ir/pentest/
4. Intrusion Detection System (IDS)

شناسایی، تعیین و گزارش فعالیت‌های غیرمجاز یا تائید نشده تحت شبکه، کمک می‌کند؛ اما در حقیقت سامانه‌های تشخیص نفوذ به‌صورت مستقیم نفوذ را تشخیص نمی‌دهند. درواقع این سامانه‌ها با بررسی فعالیت‌های در حال انجام در شبکه، به کمک الگوریتم‌ها و یا الگوهایی که در خود دارند فعالیت‌های مشکوک را شناسایی کرده و به‌عنوان نفوذ معرفی می‌کنند.[۱]

روش‌های تشخیص نفوذ

روش‌های تشخیص مورداستفاده در سیستم‌های تشخیص نفوذ به سه دسته تقسیم می‌شوند.[۲]

الف)- روش تشخیص رفتار غیرعادی[۳]

ب)- روش تشخیص سوءاستفاده[۴] یا تشخیص مبتنی بر امضاء[۵]

ج)- تشخیص پروتکل غیرعادی[۶]

انواع سیستم‌های تشخیص نفوذ

۱) سیستم‌های تشخیص نفوذ تحت شبکه:[۷] این‌گونه از سامانه‌ها مانند یک جعبه سیاه هستند که در شبکه قرارگرفته و کارت شبکه آن‌ها در حالت بی‌قید[۸] قرار می‌گیرد و کلیه ترافیک شبکه را دریافت و تجزیه‌وتحلیل می‌کند.

۲) سیستم‌های تشخیص نفوذ میزبان:[۹] این‌گونه از سامانه‌ها با استفاده از ممیزی[۱۰] کردن فایل‌های ثبت یک رخداد بر روی هر سیستم فعالیت می‌کنند و این رویدادها را تجزیه‌وتحلیل می‌کنند. ازاین‌گونه سامانه‌ها به دلیل ایجاد بار کاری زیاد برای هر سیستم پردازشگر[۱۱] معمولاً کمتر استفاده می‌شود. نرم‌افزار این‌گونه سیستم تشخیص نفوذ به‌صورت تک‌به‌تک بر روی تمامی سامانه‌ها نصب می‌شود و به‌صورت مجزا فعالیت می‌کنند.

---

1. http://hafiz-cert.com/Services/article/view.aspx?OId=116&PageIndex=0
2. Paul Innella and Oba McMillan, “An Introduction to Intrusion Detection Systems”, ۲۰۰۱
3. Anomay Detection
4. Misuse Detection
5. Signature-Based Detection
6. Anomaly Protocol
7. Network-based Intrusion Detection System (NIDS)
8. Promiscuous
9. Host-based Detection System (HIDS)
10. audit
11. CPU

۳) **سیستم تشخیص نفوذ توزیع‌شده:**[1] این سامانه‌ها از چندین سیستم‌های تشخیص نفوذ تحت شبکه یا سیستم‌های تشخیص نفوذ میزبان یا ترکیبی از این دو نوع همراه یک ایستگاه مدیریت مرکزی تشکیل‌شده است. بدین‌صورت که هر سیستم تشخیص نفوذ که در شبکه موجود است گزارش‌های خود را برای ایستگاه مدیریت مرکزی ارسال می‌کند. ایستگاه مرکزی وظیفه بررسی گزارش‌های رسیده، به‌روزرسانی پایگاه قوانین تشخیص هر یک از سیستم‌های تشخیص نفوذ و آگاه‌سازی مسئول امنیتی سیستم را بر عهده دارد.

۴) **پایش فایل‌ها**: در این نوع سیستم کلیه رخدادهای روی سامانه‌های شبکه ثبت می‌شود و همه این ثبت رخدادها به یک سرور بر روی شبکه منتقل‌شده و از طریق آن مورد تجزیه‌وتحلیل قرار می‌گیرند.

۵) **وارسی صحت و کامل بودن فایل:** این‌گونه سامانه‌ها معمولاً برای تشخیص انواع تروجان و نرم‌افزارهایی بکار می‌رود که باعث ایجاد تغییرات بر روی سیستم می‌شوند، در این روش از هر فایل بر روی سیستم یک هش[2] گرفته می‌شود و در داخل یک پایگاه داده مرکزی نگهداری می‌شود و در صورت بروز مشکل این هش با هش فایل جدید مقایسه می‌شود و در صورت عدم تطابق اعلام اخطار می‌شود.[3]

عملیات پایش (مانیتورینگ) شبکه

پایش در لغت به معنای نظارت می‌باشد، در سامانه‌هایی که عملکرد صحیح و پایداری آن‌ها اهمیت دارد، از سامانه‌های پایش استفاده می‌شود. عمل پایش در شبکه به پایش المان‌های (جزءهای) شبکه گفته می‌شود که عبارت‌اند از (اکبری،۱۳۹۴:۹-۱۲):

۱) سرورها
۲) لینک‌ها
۳) رایانه‌ها
۴) فایروال‌ها
۵) محتوای جاری در شبکه
۶) سوئیچ‌ها و روترها
۷) تجهیزات اتاق سرور (حس‌گرها و عملکردها)
۸) حجم جریان‌ها (در پایش‌های کلان)
۹) مسیر جریان‌ها (در پایش‌های کلان)
۱۰) تفکیک جریان‌ها (در پایش‌های کلان)

پایش شبکه‌ها به سه صورت اتفاق می‌افتد

۱) پایش از طریق نسخه‌ای از نرم‌افزار پایش که بر روی اجزای شبکه نصب می‌شود.

1. Distributed Intrusion Detection System (DIDS)
2. Hash
3. https://firewall.tosinso.com/articles/20

۲) پایش از طریق خروجی‌هایی که یک جز بر روی شبکه جاری می‌کند و یا تأثیری که بر روی جریان شبکه دارد.
۳) تعریف کردن یک سری از عمل‌ها به‌عنوان امتحان، که به‌صورت ادواری، سیستم پایش از یک جزء شبکه انجام آن عمل را می‌خواهد تا حضور و عملکرد صحیح آن را تأیید کند.[۱]

مزایای پایش

در بحث پایش موارد زیر قابل‌دسترس هستند:

- پایش عملکرد سیستم‌عامل‌های موجود در شبکه.
- پایش عملکرد سخت‌افزارهای موجود در شبکه (یافتن سخت‌افزار معیوب قبل از توقف عملکرد آن).
- تعریف آستانه‌ی عمل[۲] بر اساس موارد مختلف.
- پایش عملکرد سرویس‌ها و سرویس‌دهنده‌ها.
- پایش رفتار کاربران.
- نظارت بر محتوای بسته‌ها و ایمیل‌ها.
- به دست آوردن نقاط بحرانی مصرف (منابع-پهنای باند).
- به دست آوردن نقاط بحرانی در پایداری سیستم.
- اعلام خروجی توسط سیستم پایش بر اساس پارامترهایی که مدیران شبکه تعیین می‌کنند.[۳]

شیوه‌های کار ابزار وارسی

وارسی هدف، همانند کوبیدن به دیوارها برای پیدا کردن درب‌ها و پنجره‌هاست. سرباز سایبری با اقدام‌های قبلی به لیستی از شبکه‌ها و آدرس‌های آی.پی[۴] دست خواهد یافت و می‌دانیم که این تکنیک‌ها اطلاعاتی با قیمت زیاد را برای وی فراهم خواهند کرد. با ابزارهای وارسی می‌توان سامانه‌ای زنده و فعال[۵] و قابل دسترسی از طریق فضای سایبر را مشخص نمود. نمونه‌های کلی این ابزارها شامل موارد زیر می‌باشد:

---

1. https://www.rahaco.net- مانیتورینگ شبکه
2. Trigger
3. https://www.rahaco.net- مانیتورینگ شبکه
4. IP
5. Alive

- انواع وارسی‌کننده‌های پورت‌های تی.سی.پی و یو.دی.پی.
- انواع جاروب‌کننده‌ها.[1]
- ابزار وارسی و تحلیل بسته‌های شبکه.
- ابزار وارسی و آنالیز امنیت در سیستم‌های عامل.
- ابزار وارسی فایل سیستم و خطاهای مربوط به آن.
- ابزار اسکن امنیت نرم‌افزارهای مبتنی بر وب.

تمهیدات ایمن‌سازی زیرساخت‌ها و ارتباطات:

یکی از بحرانی‌ترین و مهم‌ترین مراحل، تأمین امنیت دسترسی و کنترل تجهیزات شبکه است. تجهیزاتی همچون مسیریاب، سوئیچ یا دیوارهای آتش. امنیت تجهیزات به دو علت اهمیت ویژه‌ای دارد که عبارت‌اند از (انصاری، ۱۳۹۴):

۱- عدم وجود امنیت تجهیزات در شبکه به نفوذ گران این اجازه را می‌دهد که با دستیابی به تجهیزات، پیکربندی آن‌ها را به‌گونه‌ای که تمایل دارند تغییر دهند و هرگونه سرقت اطلاعات و یا هر نوع صدمه دیگری به شبکه را وارد کنند.

۲- جهت جلوگیری از حملات نوع عدم پذیرش سرویس، تأمین امنیت تجهیزات بر روی شبکه الزامی است. نفوذ گران توسط این نوع حملات می‌توانند سرویس‌هایی را در شبکه از کار بیندازند که از این طریق در برخی موارد امکان دسترسی به اطلاعات با دور زدن هر یک از فرآیندهای احراز هویت، مجاز شناسی و حسابرسی فراهم می‌شود.

لذا بایستی اقدامات امنیتی خاصی به‌طور جداگانه در مورد هر یک از این تجهیزات صورت گیرد. در حالت کلی، ایمن‌سازی باید بر روی تجهیزات زیر صورت گیرد (داوری دولت‌آبادی، ۱۳۸۹):

۱- امنیت فیزیکی سرورها، سوئیچ‌ها، هاب‌ها، پل‌ها، بروترها، مسیریاب‌ها و دیوارهای آتش
۲- امنیت فیزیکی ارتباطات
۳- امنیت فیزیکی ایستگاه‌های کاری
۴- امنیت فیزیکی ارتباطات بی‌سیم

تمهیدات پدافند غیرعامل

جنگ سایبر دارای اهمیت روزافزون برای بخش‌های دفاعی و امنیتی، اقتصادی و تجاری، سیاسی، فرهنگی و ... است. لازمه یک دفاع موفق در جنگ سایبر همانا بالا بودن سطح امنیتی

1. Sweep

عناصر درگیر است و این مهم جز با افزایش دانش در حوزه سایبر میسر نخواهد بود. بر اساس استانداردهای امنیتی قابل‌قبول، به‌طور خلاصه هر یک از عناصر درگیر در فضای سایبر، باید به‌اندازه ارزش خود حفاظت گردند. در غیر این صورت، مکانیسم‌های دفاعی چندان بهینه نخواهند بود و بدون شک دارای هزینه‌های غیرضروری است. بدیهی است آن‌هایی که قصد حمله داشته باشند تادندان‌مسلح می‌شوند پس باید ابتدا دارائی‌ها و عناصر اصلی و اساسی و اشیاء مهم در فضای سایبری را تعریف و تعیین نموده و بر اساس سیاست‌های کلان و با در نظر گرفتن تمامی تهدیدات، باید همه تمهیدات دفاعی را پی‌ریزی نمائیم.

سهولت دسترسی به فنّاوری‌های اطلاعات، این امکان را به هکرها می‌دهد تا بتوانند با استفاده از ابزارهای رایانه‌ای پیشرفته، به سیستم شبکه هدف نفوذ کنند و یا باعث ایجاد اختلالاتی در آن‌ها از طریق سایر سامانه‌های شبکه‌ای بشوند. این ابزارها، امکان ظهور تروریسم سایبری را فراهم می‌آورد و به آن‌ها توانایی بهره‌برداری از اطلاعات و یا حذف اطلاعات را می‌دهد. توجه به چنین رویکردی در جنگ‌های جدید، جهت تغییر اطلاعات و یا گمراه نمودن بهره‌برداران از اطلاعات، باعث تغییر نگرش‌ها، برای تعیین الگوهای عمومی جنگ‌ها می‌شود.

برخی اقدامات پدافند غیرعامل

(۱)- رایانه‌های سرور و تمامی سخت‌افزارهایی که نیازمند امنیت بیشتر هستند را باید در امن‌ترین نقاط مورد تأیید سازمان قرارداد.

(۲)- باید از ابزارهای مشخص همچون دیوار آتش و سامانه مدیریت یکپارچه تهدیدات برای کنترل و مدیریت ترافیک ورودی و خروجی استفاده کرد.

(۳)- امکان دست‌کاری داده‌ها و اطلاعاتی که بر اساس آن‌ها یک فرد مهاجم می‌تواند یکپارچگی و صحت داده‌ها را تغییر دهد باید از میان برود.

(۴)- امکان شناسایی حملات گوناگون از جانب نفوذگران در سطح شبکه و سامانه‌های رایانه‌ای موجود در آن توسط سیستم تشخیص نفوذ و سیستم شناسایی نفوذ فراهم‌سازی شود.

(۵)- سعی شود در صورت امکان از شیوه‌های کار رمزنگاری داده‌ها استفاده شود تا به این وسیله کشف و بازبینی داده‌ها توسط افراد نفوذ گر با مشکل روبرو شود.

(۶)- باید از ابزارهای مانیتورینگ کارا و مفید برای بازبینی و مدیریت تمامی اقدامات رخ‌داده در سطح شبکه و رایانه‌های قابل‌دسترس در آن استفاده کرد.

(۷)- دسترسی عمومی به سخت‌افزارهای حساس و اتاق‌های امنیتی را نباید به همه کاربران اعطا کرد و باید تنها به کاربران مجاز اجازه دسترسی داده شود.

(۸)- باید کارمندانی که در سازمان مشغول فعالیت هستند به‌درستی آموزش داده شوند و روش‌های درست برقراری ارتباط در سطح شبکه به آن‌ها آموخته شود.
(۹)- برای شناسایی حمله‌های مخرب از جانب افراد نفوذ گر باید از برنامه‌های ضد بدافزار همچون آنتی‌ویروس‌ها در سامانه‌های رایانه‌ای موجود در سازمان استفاده کرد.
(۱۰)- باید از کارشناسان امنیتی باتجربه برای کنترل و مدیریت شبکه استفاده شود تا به این واسطه اگر به هر دلیل اقدامی از جانب یک فرد نفوذ گر بر روی سطح شبکه رخ داد با صرف هزینه کم با آن اقدام به‌درستی مقابله شود (احمدی،۱۳۹۶).

تمهیدات ضروری در برابر تهدیدات سایبری

جمع‌آوری اطلاعات سایبری رابطه مستقیم با پیشرفت فنّاوری‌های ارتباطی دارد و اساساً جمع‌آوری سایبری نتیجه پیشرفت فنّاوری ارتباطی و به‌ویژه رایانه‌ای است. ازاین‌رو کشورها و یا گروهای دارنده فناوری سطح برتر همواره یک‌قدم جلوتر از دیگران هستند. امروز با پیشرفت فنّاوری، حریم خصوصی دیگر وجود خارجی ندارند و در صورت به کار بردن تکنیک‌های جدید استراق سمع و شنود و یا سایر تکنیک‌های جدید به‌صورت صحیح و اصولی می‌توان از محرمانه‌ترین و یا خصوصی‌ترین گفتگوها و مذاکرات افراد مهم سیاسی و نظامی مطلع شد. در برابر جمع‌آوری سایبری و تکنیک‌های جمع‌آوری رایانه‌ای و یا هجوم رایانه‌ای به‌طورکلی می‌توان به تهدیدات در دو حوزه انسانی و فنی اشاره کرد (سید مفیدی،):

تمهیدات انسانی

باوجود پیشرفت ابزارهای جدید اطلاعاتی هنوز عامل انسانی اهمیت سابق خود را حفظ کرده است چراکه این انسان است که ابزارها را جهت اهداف و مقاصد خاص به کار گرفته و یا سعی می‌کند تلاش‌های جمع‌آوری انسان‌ها را با ابزارهایشان خنثی کند؛ بنابراین عامل انسانی فوق‌العاده مهم است. تکنیک‌ها و ابزارهای مدرن همه و همه زائده تفکر و مغزه نو پرداز انسانی است. هم ازاین‌رو لازم است تمهیدات انسانی زیر در برابر جمع‌آوری سایبری مدنظر قرار گیرد:

(۱)- استخدام و به‌کارگیری افراد متخصص و متعهد
(۲)- آموزش صحیح و اصولی نیروی انسانی
(۳)- کنترل بهینه و مؤثر نیروی انسانی
(۴)- دور از دسترس قرار دادن وسایل چون رایانه و به‌ویژه اینترنت در زمان جنگ بحران

تمهیدات فنی

بسیاری از هکرها با اطلاع از آسیب‌پذیری‌ها و ضعف‌های سامانه‌های نرم‌افزاری رایانه‌ای دست به رخنه رایانه‌ای و نفوذ و یا هک می‌زنند بنابراین؛ پیش‌بینی برنامه‌های نرم‌افزاری خنثی‌کننده، قدم مهمی در برابر جمع‌آوری اطلاعات سایبری است. نرم‌افزارها باید به‌گونه‌ای باشند که به‌محض ورود هر پیامی به سامانه آن را کنترل کرده و در صورت یافتن ایراد و اشکالی در آن و یا به‌محض ورود عنصری نفوذ گر سامانه رایانه، هشدار دهد. حتی می‌توان با تعبیه نرم‌افزارهای کنترل با حسگرهای مختلف، امکان دست‌یابی عوامل انسانی گوناگون را به رایانه‌های خاص، محدود به استفاده‌کننده اصلی آن کرد. این علامات می‌تواند اثرانگشت دست، کارت، صدا، رنگ چشم و یا سایر خصوصیات شخصی و فردی شخص استفاده‌کننده باشد. وظیفه طراحی فن‌های حفاظتی برای سامانه‌های رایانه‌ای، تبدیل به رشته‌ای جداگانه به نام امنیت رایانه‌ای شده است که با نام‌های امنیت داده‌پردازی خودکار، سامانه امنیت اطلاعات خودکار، امنیت فناوری اطلاعات و امنیت اطلاعات نیز معروف است. امنیت رایانه‌ای دربرگیرنده کلیه تدابیر لازم برای حفاظت از سامانه‌های رایانه‌ای و اطلاعات حساسی است که به‌صورت الکترونیکی مورد پردازش قرار می‌گیرند.

تمهیدات مرتبط با تدابیر مدیریتی و انسانی

در تمام فعالیت‌های مدرن، استفاده از فنّاوری، سازمان‌ها و انسان‌ها باهم ترکیب‌شده است؛ که در تعامل و ارتباط با یکدیگر عمل نموده و فعالیت‌هایی در راستای دست‌یابی به اهداف خاصی انجام می‌دهند. اجزای ماشینی سامانه یعنی سخت‌افزار و نرم‌افزار از نوع سامانه‌های معلوم و معین بوده، درحالی‌که اجزای انسانی سامانه از نوع سامانه‌های باز، نامعین و احتمالی می‌باشند. رایانه‌ها به‌طورمعمول نقش حمایتی و پشتیبانی‌کننده را به عهده‌دارند ولی انسان‌ها نقش اصلی و پراهمیت را در سامانه به عهده‌دارند.

در بخش نیروی انسانی کیفیت بیش از کمیت اهمیت دارد در عملیات سایبری تعداد نیرو مطرح نیست بلکه متد مورداستفاده و عملکرد مطرح است. به‌منظور خلق و ارائه خدمات فناوری اطلاعات، دسترسی و بهبود توانمندی‌های نیروی کار شایسته، ضروری است. تحقق این امر به‌واسطه تبعیت از روش‌های عملی تعریف شده و مورد توافق که پشتیبان نحوه استخدام، آموزش، ارزیابی عملکرد و بهبود توانمندی‌های نیروی انسانی است، امکان‌پذیر می‌شود. این فرآیند جزو فرآیندهای حیاتی فناوری اطلاعات است.

دسته‌بندی نیروی انسانی مرتبط با سامانه‌ها

دیدگاه‌های زیادی دراین‌باره وجود دارد که آقای قاضی‌زاده فرد در کتاب خود این افراد را به دسته‌های زیر تقسیم می‌نماید. ایشان معتقد است که می‌توان افراد را به‌نوعی که در مراحل مختلف طراحی، استقرار و بهره‌برداری سامانه‌های اطلاعات نقش دارند، به سه گروه ذیل دسته‌بندی نمود (قاضی‌زاده فرد، ۱۳۹۲):

الف) کاربران

کاربران همان مدیران، کارشناسان و کارکنان سازمان می‌باشند که سامانه برای تأمین نیازهای اطلاعاتی آن‌ها ایجاد می‌گردد.

۱- کاربران درونی شامل:

- کارگران خدمات یا منشی‌گری
- بخش فنی و حرفه‌ای
- مدیران ارشد، مدیران میانی و مدیران اجرایی
- کاربران راه دور و در حال حرکت داخلی ولی بدون اتصال

۲- کاربران بیرونی

۳- کاربران و مدیران

ب) راهبران

به کلیه افرادی اطلاق می‌گردد که مسئولیت گردآوری اطلاعات از واحدها و مراکز داده‌ها، آماده‌سازی آن‌ها، ورود اطلاعات به سامانه‌های رایانه‌ای، عملیاتی کردن آن‌ها، آماده نگه‌داشتن سامانه برای ارائه گزارش و خدمات اطلاعاتی، مدیریت کردن سامانه و به هنگام نگاه‌داشتن آن‌ها را بر عهده‌دارند.

ج) طراحان

طراحان سامانه‌ها افرادی هستند که وظیفه طراحی، استقرار و برپا سازی سامانه در سازمان را دارند. طراحان ناچارند برای انجام این کار اقدام به بررسی گردشکارها و اطلاعات در سازمان نموده و نحوه تولید، گردآوری و پردازش داده‌ها و تبدیل آن به اطلاعات را مورد تجزیه‌وتحلیل قرار داده و سامانه مبتنی بر رایانه طراحی و پیاده نمایند که بتواند همین کار را خیلی سریع‌تر و دقیق‌تر انجام داده و نیازهای اطلاعاتی مدیران را مرتفع نمایند (قاضی‌زاده فرد، ۱۳۹۲).

روش‌شناسی تحقیق

این تحقیق از نوع کاربردی است که به روش توصیفی- تحلیلی (موردی زمینه‌ای) با رویکرد آمیخته (کمی و کیفی) انجام شد. قلمرو مکانی آن شامل ارتش جمهوری اسلامی ایران است. قلمرو موضوعی این تحقیق در حوزه ابعاد و مؤلفه‌های عملیات پایش مورداستفاده در فضای سایبر در جنگ ترکیبی است. جامعه آماری این تحقیق شامل کارشناسان و مدیران فناوری اطلاعات، استادان رایانه در دانشگاه‌ها و نیروهای تابعه می‌باشد. برای نمونه‌گیری از جامعه آماری[۱]، از فرمول کوکران با ضریب خطای ۵٪ استفاده‌شده و حجم نمونه ۱۰۳ نفر تعیین و نمونه‌گیری انجام شد. اطلاعات به دو روش اسنادی و میدانی گردآوری شد. در بررسی اسنادی، اطلاعات لازم از کتب و نشریات و مطالعات تطبیقی و سایت‌های مرتبط بهره‌برداری شد. به‌منظور تکمیل اطلاعات کتابخانه‌ای، از بررسی میدانی (مصاحبه-پرسشنامه) استفاده شد. با توجه به شناخت محققین، تعداد ۹ نفر از جامعه آماری برای مصاحبه برگزیده شدند و از نظرات آنان برای تعیین ابعاد و مؤلفه‌های سیستم تست نفوذ، سیستم تشخیص نفوذ، ابزارهای وارسی، تمهیدات ایمن‌سازی زیرساخت‌ها و ارتباطات، تمهیدات پدافند غیرعامل، تمهیدات مرتبط با تدابیر مدیریتی و انسانی استفاده گردید. سپس، پرسش‌نامه محقق ساخته برای اخذ نظر جامعه آماری توزیع شد. در اسناد و مدارک، با توجه به اینکه بیشتر مفاهیم استخراج‌شده از اسناد و مدارک، از اصول و مفاهیم پایه‌ای می‌باشند، احتمال هرگونه تغییر در آن‌ها کم و پایایی این مضامین در حد بالایی بود. به دلیل این‌که برای انتخاب منابع و اسناد موردمطالعه با افراد صاحب‌نظر در امور آموزشی و عملیاتی که در حال حاضر نیز دارای مدارج علمی و تحقیقاتی می‌باشند و با استاد راهنما تبادل‌نظر گردید، اسناد و مدارک مورداستفاده از روایی بالایی برخوردار هستند. در مصاحبه، برای انتخاب صاحب‌نظران متخصص و آگاه و باتجربه، به‌گونه‌ای که بر ابعاد مختلف موضوع تحقیق اشراف داشته باشند، ازنظر کارشناسان و مدیران فناوری اطلاعات، استادان رایانه در دانشگاه‌ها و نیروهای تابعه و استاد راهنما و مشاور بهره‌گیری شد. لذا افراد منتخب از اعتبار بالایی برخوردار می‌باشند. برای بالا بردن روایی مصاحبه اقدامات ذیل انجام گردید: سؤالات با بهره‌گیری از تجارب کارشناسان و صاحب‌نظران طرح گردید؛ به‌گونه‌ای که بتواند محققین را در یافتن پاسخ سؤالات تحقیق یاری نماید. سؤالات مصاحبه بر مبنای ساختار تحقیق حاضر و شاخص‌های مطروحه

۱. حجم جامعه آماری به دلیل ملاحظات امنیتی بیان نشده است.

انتخاب‌شده، شفاف بوده و دارای کمترین ابهام می‌باشد. سؤالات به‌صورت کتبی و در زمان‌های مختلف با مصاحبه‌شوندگان مطرح گردید.

پایایی پرسشنامه‌ها از طریق اجرای آزمون اعتبارسنجی توسط نرم‌افزار اس.پی.اس.اس[۱] و سنجش ضریب آلفای کرونباخ ارزیابی گردید. ضریب پایایی شاخص‌های پرسشنامه (۰/۸۹۴) محاسبه گردید که نشان از دقت بالای ابزار اندازه‌گیری مورداستفاده در این مطالعه دارد. در تهیه پرسشنامه از شاخص‌های کافی، جامع و معتبر و مورد تأیید کارشناسان و صاحب‌نظران استفاده گردید تا روایی پرسشنامه ازنظر محتوا و سازه به بهترین وجه ممکن تأمین گردد. پرسشنامه تهیه‌شده ابتدا به تعداد محدودی از صاحب‌نظران و کسانی که در این راستا فعالیت دارند، ارائه و اصلاح‌های لازم در آن انجام گردید تا روایی آن مورد تأیید قرار گیرد.

تجزیه‌وتحلیل یافته‌ها

ابتدا محقق به مطالعه اسناد و مدارک موجود در ارتباط با فضای سایبری پرداخته و در کنار این کار، با طرح سؤالات نظر سنجی در قالب یک مطالعه اکتشافی و اجرای مصاحبه با خبرگان نسبت به استخراج شاخص‌های متغیرهای موضوع تحقیق اقدام نمود. پس از تعیین شاخص‌ها و زیرشاخه‌های آن، محقق اقدام به تنظیم پرسشنامه نموده و با اجرای آن در نمونه آماری تحقیق، نتایج را جمع‌آوری و با استفاده از آمار توصیفی و آمار استنباطی داده‌های به‌دست‌آمده را تجزیه‌وتحلیل نموده و در آخر با تحلیل نهایی نتایج نظرسنجی، اسناد و مدارک، نظرات صاحب‌نظران و پرسشنامه‌ها نسبت به ارائه عملیات پایش فضای سایبری در جنگ ترکیبی اقدام نمود. آماره آزمون با درجه آزادی ۴ و سطح معنی‌دار ۰/۰۵، بزرگ‌تر از ۹/۴۹ و در حدود ۶۹/۶۲ است که از مقدار بحرانی جدول بزرگ‌تر است، بنابراین بین عملیات پایش به‌عنوان یک عامل مؤثر بر متغیر اصلی و فضای سایبری ارتش جمهوری اسلامی ایران در جنگ ترکیبی تأثیر زیادی وجود دارد. چون نشان‌دهنده آن است که بین عامل تأثیرگذار و متغیر ارتباط معنی‌داری وجود دارد، برای محاسبه شدت آن (ضریب توافقی) از فرمول زیر استفاده گردید.

$$C = \sqrt{\frac{\chi^2}{\chi^2 + n}} = \sqrt{\frac{69.620}{69.620 + 103}} = 0.641$$

---

۱. نام این نرم‌افزار یعنی SPSS مخفف حروف اول عبارت "Statistical Package for the Social Sciences"، به معنای «نرم‌افزار آماری برای علوم اجتماعی» است و در حال حاضر از این نرم‌افزار برای تحلیل و آنالیز آماری مشاهدات و پرسشنامه‌ها و آزمایش‌ها در تمامی رشته‌ها استفاده می‌گردد.

یعنی شدت ضریب همبستگی (ضریب توافقی) بین متغیر اصلی عملیات پایش فضای سایبری ارتش جمهوری اسلامی ایران در جنگ ترکیبی و شیوه‌های کار به‌عنوان عامل مؤثر بر آن به میزان ۶۴٪ بوده است. بنابراین؛ این عامل بر متغیر اصلی، تأثیرگذار می‌باشد.

یافته‌های تحقیق

تحلیل محتوایی حاصل از مطالعه منابع، مدارک، نظریه‌های مرتبط و مصاحبه با صاحب‌نظران گویای این مطلب است که عملیات پایش فضای سایبر باید در دو بعد (شیوه‌های کار و تمهیدات) و شش مؤلفه‌ی تست نفوذ، تشخیص نفوذ، ابزارهای وارسی، ایمن‌سازی زیرساخت‌ها و ارتباطات، پدافند غیرعامل و تدابیر مدیریتی و انسانی موردبررسی قرار گیرد. این بررسی باید قادر باشد با استفاده از ویژگی‌های فضای سایبری پشتیبانی از نیروهای خودی را در جنگ‌های ترکیبی فراهم آورد. ابعاد مؤلفه‌ها و شاخص‌های عملیات پایش به شرح جدول‌های زیر می‌باشد.

جدول (۱): نتایج حاصل از فرآیند تحلیل محتوای داده‌های مصاحبه

متغیر	ابعاد	مؤلفه	شاخص
عملیات پایش فضای سایبری	شیوه‌های کار	تست نفوذ	آسیب‌پذیری
			تحلیل و ارزیابی
			مدل‌سازی تهدید
		تشخیص نفوذ	پایش المان‌های شبکه
			اشکالات امنیتی
			پورت‌های تی.سی.پی و یو.دی.پی
		ابزارهای وارسی	امنیت
			پورت‌های آسیب‌پذیر
			بسته‌های شبکه
	تمهیدات	ایمن‌سازی زیرساخت‌ها و ارتباطات	بومی‌سازی
			ایمن‌سازی
			تجهیزات فعال و غیرفعال شبکه
		پدافند غیرعامل	تهدیدات سایبری
			رمزنگاری داده‌ها
			تاکتیک‌ها و تکنیک‌ها
		تدابیر مدیریتی و انسانی	استخدام افراد متخصص و متعهد
			پذیرفته‌شدگان در دوره‌های تحصیلات تکمیلی
			برنامه‌ریزی آموزشی آگاه‌سازی و فرهنگ‌سازی

ماحصل نظرخواهی در خصوص مؤلفه‌های تأثیرگذار در جنگ‌های ترکیبی، طی۲۸ سؤال از جامعه نمونه مطرح گردید که به‌منظور تجزیه‌وتحلیل و مشخص ساختن اطلاعات به‌دست‌آمده، میانگین پاسخ‌های پرسش‌شوندگان به سؤالات مطرح‌شده در شاخص‌های هر مؤلفه از طریق جدول و ترتیب آزمون مرتبط با آن‌ها به شرح زیر انجام گردیده است:

جدول (۲): تجزیه‌وتحلیل توصیفی ابعاد و شاخص‌های موضوع تحقیق حاصل از داده‌های مصاحبه

میزان تأثیر عوامل زیر در عملیات پایش فضای سایبری	میانگین	میزان تأثیر عوامل زیر در مقابله با تهدیدهای سایبری	میانگین
شناسایی آسیب‌پذیری‌های شبکه، زیرساخت و بسترهای ارتباطی	۴/۲۰	بومی‌سازی برنامه‌ها و نرم‌افزارهای کاربردی	۴/۱۴
تحلیل و ارزیابی آسیب‌پذیری سامانه موردسنجش	۴/۰۹	ایمن‌سازی تجهیزات فعال شبکه	۴/۱۲
مدل‌سازی تهدید	۴/۰۴	ایمن‌سازی تجهیزات غیرفعال شبکه	۴/۱۲
پایش المان‌های شبکه (سرورها، سوئیچ‌ها و روترها، لینک‌ها، رایانه‌ها و ...)	۴/۱۰	شناخت کافی از تهدیدات سایبری	۳/۹۶
شناسایی حملات و تشخیص اشکالات امنیتی	۴/۰۸	بهره‌برداری از شیوه‌های کار رمزنگاری داده‌ها در مسیر تبادل اطلاعات	۴/۰۶
پایش پورت‌های تی.سی.پی و یو.دی.پی	۴/۲۱	تاکتیک ها و تکنیک های مقابله با جنگ‌های سایبری	۴/۰۹
بررسی و آنالیز امنیت در سیستم‌های عامل	۴/۰۱	افزایش تعداد پذیرفته‌شدگان در دوره‌های تحصیلات تکمیلی حوزه سایبری	۳/۹۸
وارسی و کنترل متداول‌ترین پورت‌های آسیب‌پذیر شامل: TCP، UDP و UDP/TCP	۴/۱۵	استخدام و به‌کارگیری افراد متخصص و متعهد در حوزه‌های مختلف سایبری	۴/۱۹
وارسی و تحلیل بسته‌های شبکه	۴/۰۵	برنامه‌ریزی آموزشی و فرهنگ‌سازی، آگاه‌سازی در راستای ارتقاء سطح علمی و عملی برای کارکنان	۴/۰۳

با توجه به جدول فوق، نتایج به‌دست‌آمده گویای این مطلب است که ۹۷٪ افراد جامعه نمونه میزان تأثیر مؤلفه‌های شش‌گانه عملیات پایش فضای سایبری ارتش جمهوری اسلامی ایران در جنگ ترکیبی در سطح بالا، مورد تأیید می‌دانند و در ضمن چون میانگین این مؤلفه ۴/۱۱ است (۵ >۴/۱۱> ۴)، تأثیر آن به میزان خیلی زیاد می‌باشد.

نتیجه‌گیری و پیشنهادها

با توجه به نتایج تجزیه‌وتحلیل اسناد و مدارک و تجزیه‌وتحلیل آماری پرسش‌نامه نتایج زیر به‌دست‌آمده است.

۱- جنگ سایبری ازجمله فناوری مهم و اثرگذار آجا در جنگ‌های ترکیبی است.

۲- اجرای فرآیند منظم، هدف‌دار و مستمر شیوه‌های کار پایش فضای سایبری آجا در موارد زیر ضروری است:

۱) در زمان اضافه شدن تجهیزات و یا نرم‌افزارهای جدید

۲) بعد از ارتقاء، بروز رسانی و یا اعمال تغییرات در لایه زیرساخت شبکه و یا نرم‌افزارها

۳) در زمان تأسیس یک ساختمان یا فضای فیزیکی جدید

۴) در زمان تغییرات در سیاست‌های امنیتی کاربران

۳- شناسایی نقاط و ابعاد آسیب‌پذیری‌های شبکه، زیرساخت و بسترهای ارتباطی و تحلیل و ارزیابی اطلاعات به‌دست‌آمده در عملیات پایش فضای سایبری تأثیر بالایی دارد.

۴- نیروهای جنگ ترکیبی اغلب اوقات از رویارویی مستقیم با نیروهای نظامی کشور هدف خودداری نموده و با توجه به محدودیت نیرو و تجهیزات در تلاش هستند که کنترل فضای سایبری و تأسیسات حیاتی را در دست بگیرند تا بتوانند از آن به‌عنوان اهرم فشاری علیه کشور هدف استفاده نموده و به نحوی از اطلاعات فناوری موجود بهره ببرند.

۵- مطالعه همه‌جانبه در حوزه سایبری، رهگیری حملات سایبری که در دنیا در حال وقوع است، شناسایی و انتخاب پدافند مناسب، انجام تمرین و رزمایش‌های سایبری و از طرفی بومی‌سازی تجهیزات سخت‌افزاری و نرم‌افزاری و ارتباطی و در یک جمع‌بندی و نتیجه‌گیری کلی می‌توان گفت: با کاهش وابستگی آجا به فناوری سایبری و تدابیر مدیریتی و نیروی انسانی آن می‌توان قدرت سایبری را ارتقاء بخشید و توانمندی لازم برای انواع عملیات سایبری را کسب نمود.

۶- با توجه به اینکه، جنگ سایبری یکی از ابزارهای هشت‌گانه در جنگ ترکیبی است؛ لذا طراحی و اجرای موفق آن، مستلزم بهره‌مندی مناسب از برخی شیوه‌های کار و تمهیدات عملیات پایش به شرح زیر است.

۱) تدابیر مدیریتی و انسانی

۲) ایمن‌سازی زیرساخت‌ها و ارتباطات

۳) پدافند غیرعامل مناسب با صحنه‌های مختلف نبرد

۴) تست نفوذ

۵) سیستم تشخیص نفوذ

۶) ابزارهای وارسی

۷- بومی‌سازی سامانه‌های سخت‌افزاری و نرم‌افزاری در فضای سایبری، استخدام و به‌کارگیری افراد متخصص و متعهد در حوزه‌های مختلف سایبری، برنامه‌ریزی آموزشی و فرهنگ‌سازی، آگاه‌سازی در راستای ارتقاء سطح علمی و عملی برای کارکنان، ایمن‌سازی تجهیزات فعال و غیرفعال شبکه، افزونگی در محل استقرار شبکه، اعمال مدیریت مؤثر در سلسله‌مراتب فرماندهی در جهت حفاظت و تأمین امنیت مطلوب فن‌آوری اطلاعات و ارتباطات و ... ازجمله اقدامات مؤثر در جهت حفظ امنیت، پدافند سایبری و ارتقاء بهره‌برداری مناسب در جنگ ترکیبی توس نیروهای متخصص آجا است.

جنگ‌های ترکیبی، جنگ‌های مربوط به کشورهای جهان سوم و گروه‌های مسلح است که به دلیل ضعف و عقب‌ماندگی در بسیاری از حوزه‌ها سعی می‌کنند با ترکیب توانایی‌های ملی راهی را به‌سوی رویارویی با قدرت‌های برتر غربی بگشایند. در جنگ ترکیبی از همه انواع سبک‌های جنگ‌های قدیم و جدید به‌طور همزمان استفاده می‌شود. ازجمله: جنگ اطلاعاتی، جنگ نامتقارن، جنگ شبکه‌ای، جنگ سایبری، جنگ کلاسیک، جنگ بی‌قاعده و.... نمونه‌ای از فناوری‌های مهم و اثرگذاری است که در جنگ‌های ترکیبی مورد بهره‌برداری قرار می‌گیرد. لذا پیشنهادهای زیر در جهت ارتقاء آمادگی این حوزه در جنگ ترکیبی بسیار مؤثر است.

۱- شایسته است؛ سالیانه رزمایش‌های سایبری در سطوح مختلف (راهبردی، عملیاتی و تاکتیکی) جهت ساماندهی بهتر فضای سایبری آجا، کشف آسیب‌پذیری‌های موجود در سامانه‌های مختلف داده و اطلاعات و ارتقاء کیفیت عملکرد آنان درصحنه‌های نبرد واقعی؛ طراحی و به مرحله اجراء در آید.

۲- با توجه به پیشرفت روزافزون دانش در حوزه‌های سایبری، ضروری است که کارکنان، اساتید و متخصصان شاغل در مشاغل سایبر و امنیت داده و اطلاعات از سطح علمی و تجربی بالایی برخوردار باشند.

۳- تعامل سازنده و همکاری با دانشگاه‌های سراسری و علمی کشور در جهت اعزام و افزایش تعداد پذیرفته‌شدگان در دوره‌های تحصیلات تکمیلی حوزه سایبری، افزایش یابد.

۴- اصول پدافند غیرعامل در طرح و پیاده‌سازی زیرساخت‌های سایبری به‌طور مؤثر طراحی و اجرایی گردد.

۵- نظارت مستمر بر فعالیت کارکنان برابر آیین‌نامه‌ها، دستورالعمل‌ها، استانداردها در راستای حفظ امنیت اطلاعات و مقابله بانفوذ احتمالی در شبکه‌ها و زیرساخت‌های حوزه‌های مختلف سایبری ملحوظ نظر باشد.

۶- بومی‌سازی سامانه‌های سخت‌افزاری و نرم‌افزاری در فضای سایبری، استخدام و به‌کارگیری افراد متخصص و متعهد در حوزه‌های مختلف سایبری، برنامه‌ریزی آموزشی و فرهنگ‌سازی، آگاه‌سازی در راستای ارتقاء سطح علمی و عملی برای کارکنان، ایمن‌سازی تجهیزات فعال و غیرفعال شبکه، افزونگی در محل استقرار شبکه، اعمال مدیریت مؤثر در سلسله‌مراتب فرماندهی در جهت حفاظت و تأمین امنیت مطلوب فن‌آوری اطلاعات و ارتباطات و ... ازجمله اقدامات مؤثری است که می‌تواند در جهت حفظ امنیت، پدافند سایبری و ارتقاء بهره‌برداری مناسب از این فضا در جنگ ترکیبی توسط نیروهای متخصص آجا باشد.

۷- تحقیقات آتی در این حوزه‌ها می‌تواند نقش بسیار مؤثری در ارتقاء توان عملیاتی یگان‌های آجا داشته باشد. ازاین‌رو پیشنهاد می‌گردد؛ محققان در تحقیقات آتی به موضوع «تبیین چالش‌های تروریسم سایبری بر سر راه امنیت شبکه‌های آجا در جنگ ترکیبی» بپردازند.

۸- گزارش به‌موقع مخاطرات و حوادث سایبری به همراه اقدامات مقابله‌جویانه، در سطوح راهبردی، عملیاتی و تاکتیکی به مبادی مرتبط در نیروهای چهارگانه نقش سازنده‌ای در آمادگی رزمی آجا دارد.

۹- تعامل سازنده و دانش‌محور با صنایع دفاعی (صا ایران) جهت تهیه، تولید، ایمن‌سازی و بومی‌سازی تجهیزات فعال و غیرفعال شبکه قبل از صحنه نبرد لازم و ضروری است.

منابع

- آذر داود و حسین مسلمی (۱۳۹۳)، *شناخت تهدیدات فضای سایبری و پدافند از آن*، تهران، انتشارات دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران.
- اسکندری حمید، رحمت اله امیر صوفی (۱۳۹۱)، *تهدیدات فضای سایبر و مدیریت امنیت اطلاعات*، تهران، انتشارات بوستان حمید.
- اکبری، رؤیا (۱۳۹۴)، *مانیتورینگ شبکه*، بابل، دانشگاه صنعتی نوشیروانی بابل.
- احمدی، مهدی (۱۳۹۶)، *مدل‌سازی تهدیدها*، تهران، انتشارات پندار پارس.
- انصاری علیرضا و حمید محمدحسین (۱۳۹۴)، *امنیت فناوری اطلاعات در مقابله با حملات سایبری*، تهران، انتشارات دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران.
- تیموتی مک کالو و ریچارد جانسون (۱۳۹۵)، *جنگ ترکیبی*، ترجمه احمد الهیاری، تهران، انتشارات دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران.

- سید مفیدی، کاوه (۱۳۸۸)، *سکیورتارگت (فضای سایبری)، سکیور تارگت (جنگ سایبری)*، تهران، مرکز آینده‌پژوهی علوم و فناوری دفاعی.
- سید مفیدی، کاوه (۲۰۰۹ میلادی)، *سکیورتارگت (فضای سایبری)، نسخه خلاصه شده جنگ سایبری*، تهران، مرکز آینده‌پژوهی علوم و فناوری دفاعی.
- قاضی‌زاده فرد، سید ضیاءالدین (۱۳۹۲)، *مدیریت دانش عامل اثربخشی سازمان‌ها*، تهران، انتشارات سازمان تحقیقات صنعتی.
- ضیایی بیگدلی، محمدرضا (۱۳۷۳)، *حقوق جنگ*، تهران، انتشارات دانشگاه علامه طباطبایی.
- ماه پیشانیان، مهسا، حجت اله مرادی (۱۳۸۹)، *گفتمان جنگ مجازی و رسانه‌های گروهی در قدرت و جنگ نرم از نظریه تا عمل*، تهران، انتشارات ساقی.
- Ischinger, Wolfgang. (2015). *Munich Security Report 2015*: Collapsing Order, Reluctant
- Paul Innella and Oba McMillan, "*An Introduction to Intrusion Detection Systems*", 2001