

راهبردهای پدافند غیر عامل در پیشگیری از آسیب‌پذیری فاوا ناجا

داود دعاگویان^۱

تاریخ دریافت: ۹۶/۴/۲۱

تاریخ پذیرش نهایی: ۹۶/۶/۵

فصلنامه‌ی مطالعات راهبردی ناجا / سال دوم / شماره چهارم - تابستان ۱۳۹۶

چکیده

گزارش علمی راهبردهای پدافند غیر عامل در پیشگیری از آسیب‌پذیری فاوا ناجا با هدف نظام‌مند کردن تفکرات راهبردی پدافند غیر عامل در موضوع پیشگیری از ناامنی‌های فاوا ناجا صورت گرفته است. نظریه‌های پدافند غیر عامل مشخص می‌کند که زیرساخت‌های فناوری اطلاعات و ارتباطات، مانند مراکز داده، سیستم‌عامل ملی، شبکه تلفن ثابت و همراه، ماهواره، شبکه بی‌سیم، و فیبرنوری، جزو زیرساخت‌های حیاتی و به عنوان حلقه سوم از مدل ۵ حلقه‌ای وارن بوده و کاهش آسیب‌پذیری آن در رویارویی با تهدیدهای دشمن و تهدیدهای طبیعی اهمیت ویژه‌ای دارد. روش پژوهش پیش رو کاربردی و از نظر روش اجرا توصیفی-تحلیلی است. جامعه آماری استادان و کارشناسان حوزه پدافند غیر عامل نفر است که از طریق جدول مورگان، به روش نمونه‌گیری احتمالی طبقه‌ای، انتخاب شدند. ابزار گردآوری داده‌ها پرسشنامه محقق‌ساخته است که پیش از اجرا اعتبار آن از راه اعتبار محتوا و پایایی آن از راه آلفای کرونباخ تأیید شد.

براساس نتایج به دست آمده از پژوهش‌ها، اصول پدافند غیر عامل در فناوری اطلاعات و ارتباطات، به‌طور کامل، مورد توجه قرار نگرفته است. بی‌توجهی به استحکامات فاوا آسیب‌پذیری آن‌ها را در مواقع بحرانی افزایش داده است. همچنین، نسبت به دیگر اصول پدافند غیر عامل، مانند توجه به اصل فریب دشمن، پراکندگی مکان‌های فاوا و داشتن پناهگاه برای کارکنان فاوا توجه نشده است که این مهم آسیب‌پذیری فاوا را در مواقع بحرانی ناشی از جنگ و بحرانی‌های طبیعی به شدت افزایش می‌دهد. به منظور حفاظت از تجهیزات فاوا و برقراری امنیت شبکه‌های ADSL با رویکرد پدافند غیر عامل و به منظور دست یافتن به اهداف ترسیم شده در اسناد پدافند غیر عامل موارد زیر، در دو بخش سخت‌افزاری (پدافند غیر عامل در حوزه مکانی) و نرم‌افزاری (پدافند غیر عامل در حوزه سیستمی نرم‌افزاری) پیشنهاد می‌شود.

واژگان کلیدی

پدافند غیر عامل، فاوا، پیشگیری، آسیب‌ها، بایست‌ها

مقدمه

تحولات گسترده پنجاه سال اخیر در زمینه رایانه و ارتباطات، بیشترین تأثیر را در حیات بشر داشته است. امروزه، فناوری اطلاعات و ارتباطات افق جدیدی را در زمینه تولید و اطلاعات عرضه کرده و ضروری است، هم‌زمان، امکانات موجود را در مسیر فراگیری و ایجاد دانش، سازماندهی و به خدمت گرفت (المر، ۲۰۰۲؛ رئیس‌دانا، فیروزآبادی، ۱۳۸۱: ۵). با وجود این، فاوا واژه‌ای است که به هر نوع دستگاه ارتباطی یا برنامه نظیر رادیو، تلویزیون، تلفن‌های سلولی، رایانه، نرم‌افزار، سخت‌افزارهای شبکه، سیستم‌های ماهواره و نظایر آن اطلاق شده که کارایی‌های فراوانی در آموزش، بهداشت و اطلاع‌رسانی، پردازش و ذخیره‌سازی داده دارد (لی، ۲۰۰۹؛ جلالی، ۱۳۹۲: ۲۴-۵۲؛ آرنس، ۱۹۹۹). بی‌گمان، فناوری اطلاعات و ارتباطات یکی از اصلی‌ترین عوامل پیشرفت و تحولات علمی و صنعتی در دوران جدید است که تمام ابعاد زندگی بشر را تحت تأثیر خود قرار داده است. دسترسی نزدیک به ۱ میلیارد انسان به شبکه جهانی اینترنت، و از این تعداد استفاده بیش از ۶۰۰ میلیون نفر از پست الکترونیکی، تبادل بیش از ۴ هزار میلیارد پیام در هر شبانه‌روز، تنها از طریق یکی از نرم‌افزارهای چت، نشانه‌هایی آشکار از آمیخته شدن جنبه‌های گوناگون زندگی با دستاوردهای این فناوری است. حکومت و مدیریت یکی از عرصه‌هایی است که با گسترش و پیشرفت فناوری اطلاعات و ارتباطات دستخوش تحولاتی شگفت‌انگیز شده است (قاضی نوری، ۲۰۰۵: ۳۳). امروزه با فراهم شدن زمینه‌های دولت الکترونیکی و ماشینی و شبکه‌ای شدن بسیاری از فعالیت‌ها و ارتباطات، افزون بر دسترسی همیشگی، عادلانه و بدون تعطیلی، مردم به خدمات، اطلاعات و نیازهای اداری و حکومتی، وضعیت مناسبی برای هوشمند شدن تصمیم‌گیری و مدیریت و پاسخ‌گویی بیشتر مدیران فراهم شده است. ضمن اینکه این فناوری بسیاری از معادلات قدرت و محاسبات سیاسی را تغییر داده و دسترسی به اطلاعات و در اختیار داشتن شبکه‌های بزرگ ارتباطی را در رتبه و اهمیتی بالاتر از منابع و امکانات مالی و نظامی قرار داده است. کم‌رنگ و کم‌اثر شدن مرزهای ملی و فاصله‌های جغرافیایی نیز از واقعیت‌هایی است که بر اثر گسترش فناوری اطلاعات و ارتباطات بر جامعه جهانی تحمیل شده است (ویکی پدیا، ۱۳۹۲؛ علی احمدی، ۲۰۰۶: ۵۷-۸۳). در ایران سرمایه‌گذاری در ارتباطات طی یک دوره رکود طولانی

1. elmer
2. lee
3. Ahrens

از سال ۱۳۵۶ تا ۱۳۷۵، وارد یک دوره رشد مثبت می‌شود؛ به طوری که، متوسط سالانه سرمایه‌گذاری در ارتباطات طی دوره ۱۳۷۶ تا ۱۳۸۱ معادل ۶/۹ درصد است که معادل نرخ رشد متوسط کل سرمایه‌گذاری در کشور است (باقری، ۲۰۰۸: ۱۴؛ مشیری، جهانگرد، ۱۳۸۳: ۵۵-۷۸). بنابراین، باتوجه به جریان‌های اخیر حمله دشمن به تأسیسات فاوا، که به حمله‌های سایبری معروفاند، مشخص می‌گردد که پدافند غیر عامل در عرصه فاوا باید بیش‌ازپیش کانون توجه قرار گیرند. بی‌شک، نگاه راهبردی به فاوا موجب ایمن‌سازی این فناوری در برابر حملات دشمن است. اکنون کشورهای غربی دریافته‌اند که باید به پاشنه آشیل فاوای کشورهای در حال توسعه حمله کنند و باید با روش‌های گوناگون حملات سایبری و نظامی مانع از به کارگیری کشورهای در حال توسعه از این فناوری شوند. از این رو، هرگونه تدبیری در خنثی‌سازی حملات دشمن به فناوری اطلاعات و ارتباطات باید با رویکرد راهبردی و اتخاذ طرحی عملیاتی به منظور هماهنگی و سازماندهی اقدامات برای دستیابی به روش‌های پدافند غیر عامل در مسیر جلوگیری از آسیب‌ها صورت گیرد، زیرا باتوجه به مدل پنج حلقه‌ای واردن^۱، فاوا جزو تأسیسات زیرساخت‌های کشور به شمار رفته و اندام‌های حرکتی در جامعه تلقی می‌شوند. به نظر می‌رسد که اشاراتی به حمله‌های سایبری در کشور (مانند حمله استاکس‌نت و حمله به بخش صنعتی، گاوس و سیستم بانکی و حمله سایبری شعله آتش به تجهیزات فاوا نفتی ایران) می‌تواند عمق اهمیت فاوا را در کشور مشخص کند. دشمنان باتوجه به بالا بودن هزینه‌های نظامی و احتمال شکست سنگین در این حوزه می‌کوشند که با حملات سایبری نظام حرکتی و جنبشی کشور را فلج کنند. بنابراین، اقدام‌های پدافند غیر عاملی در حوزه فاوا در کشور، به طور اعم، و فاوا ناجا، به طور اخص، امری ضروری است. بدیهی است که تمام برنامه‌های آفندی و پدافندی در این حوزه باید از الگوی ابلاغی پیروی نماید. از این رو، راهبردهای اصلی امنیت فضای تولید و تبادل اطلاعات و ارتباطات عبارت‌اند از:

۱. ایجاد نظام جامع و فراگیر در سطح ملی و سازوکار مناسب برای ایمن‌سازی ساختارهای حیاتی و حساس و مهم در حوزه فناوری اطلاعات و ارتباطات و ارتقای مداوم امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی در کشور به منظور استمرار خدمات عمومی، پایداری زیرساخت‌های ملی، صیانت از اسرار کشور، حفظ فرهنگ و هویت اسلامی، ایرانی و ارزش‌های اخلاقی، حراست از حریم خصوصی و آزادی‌های مشروع و سرمایه‌های مادی و

معنوی؛ ۲. توسعه فناوری اطلاعات و ارتباطات با رعایت ملاحظات امنیتی؛ ۳. ارتقای سطح دانش و ظرفیت‌های علمی، پژوهشی-آموزشی و صنعتی کشور برای تولید علم و فناوری مربوط به امنیت فضای اطلاعاتی و ارتباطی (افتا)؛ ۴. تکیه بر فناوری بومی و توانمندی‌های تخصصی داخلی در توسعه زیرساخت‌های علمی و فنی امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی؛ ۵. پیش، پیشگیری، دفاع و ارتقای توان بازدارندگی در مقابل هرگونه تهدید در حوزه فناوری اطلاعات و ارتباطات؛ ۶. تعامل مؤثر و سازنده منطقه‌ای، جهانی و همکاری و سرمایه‌گذاری مشترک در حوزه‌های دانش، فناوری و امور مربوط به امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباط با حفظ منافع و امنیت ملی؛ ۷. تعیین نهاد متولی و هماهنگ کننده زیر نظر دولت به منظور هدایت، نظارت و تدوین استانداردهای لازم برای حفظ و توسعه امنیت فضای تولید و تبادل اطلاعات و ارتباطات و تهیه پیش‌نویس قوانین مورد نیاز؛ ۸. فرهنگ‌سازی، آموزش و افزایش مهارت‌های عمومی در حوزه فتا (سایت سازمان پدافند غیر عامل، ۱۳۸۹). به‌طور کلی، با توجه به اهمیت و ضرورت توجه به امنیت فضای تولید و تبادل اطلاعات، آیا راهبردهای پدافند غیر عامل در فاوای ناجا کانون توجه قرار گرفته است؟ و ویژگی‌های اصلی تدابیر راهبردی پدافند غیر عامل فاوا چیست؟

پیشینه نظری تحقیق

براساس آمارهای سازمان ملل متحد در ابتدای قرن بیستم نسبت تلفات غیرنظامیان به کل تلفات جنگی، تنها ۵ درصد بوده است، در حالی که این نسبت در طول جنگ جهانی اول به ۱۵ درصد، جنگ جهانی دوم به ۶۵ درصد و در دهه ۱۹۹۰ میلادی به بیش از ۹۰ درصد رسیده است. افزون بر تلفات مستقیم جنگ، تلفات بشماری بر اثر عواقب غیرمستقیم جنگ، از قبیل فقدان یا کمبود مواد غذایی و خدمات دارویی و درمانی و نیز منابع آب آشامیدنی سالم، بروز می‌کند که در این میان افراد آسیب‌پذیر، نظیر کودکان و سالمندان و زنان و بیماران، بیش از دیگران لطمه می‌بینند. نخستین بار، توماس هابز در کتاب "De Cive" تأمین امنیت شهروندان را اصلی‌ترین قانون و مهم‌ترین وظیفه حاکمان در برابر مردم معرفی کرد و نپرداختن به آن را اقدام علیه صلح و قوانین طبیعت بیان نمود. اکنون نیز پدافند غیرعامل هم به صورت یک هدف کلی و هم به عنوان مسئولیت هر دولتی شناخته می‌شود، به طوری که، بسیاری از دولت‌ها مسئولیت‌های گسترده‌ای در باب پدافند غیرعامل برعهده دارند (داعی‌نژاد و امین‌زاده، ۱۳۸۵).

در سال ۱۹۷۷ میلادی تمهیدات قانونی بین‌المللی در قالب پروتکل I ژنو چهارچوب حقوقی لازم به منظور نحوه رفتار با غیرنظامیان در زمان جنگ و نیز وظایف دول جهان در زمینه ارائه و اجرای طرح‌ها و برنامه‌های دفاع غیرنظامی را فراهم نمود. این پروتکل بر لزوم انجام اقدام‌های معینی به منظور دفاع از غیرنظامیان و تضمین محافظت از آنان در زمان جنگ دلالت دارد. بسیاری از کشورهای جهان به منظور تأمین محافظت از شهروندان خود در برابر انواع بلایای طبیعی و انسان‌ساز، روش‌های گوناگونی را به تناسب دیدگاه غالب در زمینه مقابله غیرعامل با بحران، نوع بحران و امکانات در دسترس به کار می‌گیرند. اهم این روش‌ها عبارت‌اند از:

- پیشگیری و هشدار مشتمل بر هشدار و اعلام خطر، ایجاد پناهگاه‌ها
- رویارویی مشتمل بر تخلیه یا استقرار در پناهگاه‌ها
- امداد و نجات
- بازتوانی

بررسی دیدگاه‌های فکری تعدادی از کشورها در امر محافظت از غیرنظامیان در برابر تهاجم‌های نظامی گویای آن است که از دیدگاه پدافند غیرعامل، هر طرح کارآمد می‌بایست تلفات جانی را به حداقل ممکن کاهش دهد، خسارات زیربنایی را به حداقل برساند و ابعاد و دامنه آسیب‌ها را هرچه بیشتر محدود نگاه دارد.

پدافند غیرعامل در ایالات متحده آمریکا ابعاد بسیار گسترده‌ای دارد، گرچه تأکید اصلی در این زمینه بر افزایش فوق‌العاده توان تهاجمی و بازدارندگی است، ولی دیگر اقدام‌ها و تمهیدات پدافندی، نظیر مقابله با شرایط حین و پس از وقوع حمله، عمدتاً حملات هسته‌ای، نیز دیده شده‌اند. این تمهیدات تمام مراحل عمل در پدافند غیرعامل مشتمل بر آمادگی (اعلام خطر)، رویارویی (تخلیه عمودی یا افقی محل)، مقابله (نجات و کاهش دامنه آسیب‌ها) و بازتوانی پس از وقوع حمله را دربر می‌گیرد.

در سوئیس مهم‌ترین ابعاد دفاع از غیر نظامیان در برابر تهاجم‌های نظامی را می‌توان به ترتیب زیر برشمرد: تأمین فضاهای پناهگاهی در برابر حملات هسته‌ای برای هریک از شهروندان سوئسی و هم برای کارکنان صنایع کلیدی (قبل از بحران). تأمین فضاهای بیمارستانی زیرزمینی مقاوم در برابر حملات هسته‌ای (قبل از بحران). هشدار و اعلام خطر مرحله‌ای، متناسب با اوج‌گیری تنش‌های بین‌المللی (حین بحران)، استقرار دائم در پناهگاه

(حین و پس از بحران). بنابراین، اقدام‌های محافظت از غیرنظامیان در برابر تهاجم‌های نظامی در سوئیس، محدود به آمادگی غیرنظامی برای رویارویی با حملات هسته‌ای از طریق تأمین حفاظت پناهگاهی و سپس، مقابله با بحران با تأکید بر امدادهای پزشکی است. در اتحاد شوروی سابق و روسیه کنونی اعتقاد بر آن است که جنگ هسته‌ای، به طور قطع، روزی رخ می‌دهد. از این رو، تمهیدات بسیار گسترده‌ای، به منظور محافظت از غیرنظامیان، پیش‌بینی شده است. این کشور تأکید اصلی خود را بر راهبرد بازدارندگی و نیز استدلال حفظ و بقای کشور، به طور هم‌زمان، قرار داده است. البته، پس از فروپاشی اتحاد شوروی سابق و باوجود پایان یافتن رقابت‌های هسته‌ای دوران جنگ سرد، سرمایه‌گذاری‌های کلانی در زمینه ایجاد پناهگاه‌های ضد هسته‌ای انجام شده و برنامه‌های دولت در راستای نوسازی تسلیحات و صنایع نظامی کشور تنظیم شده است. رژیم اشغالگر قدس، پدافند غیرعامل را جزو جدانشدنی تمام برنامه‌ها و اقدام‌های خود کرده و آن را در تمام پهنه سرزمین گسترش داده است، به گونه‌ای که، از نظر زمان و مکان، مرز مشخصی میان پدافند عامل و غیرعامل وجود ندارد. همه کاربری‌های اراضی، در مقیاس‌های مختلف، مناطق جمعیتی، به ویژه محیط‌های مسکونی، افزون بر کاربری‌های متداول لزوماً از کاربردهای نظامی نیز برخوردار است.

در ایران با توجه به ارزیابی خطرهای بالقوه و تهدیدات منتج از محیط پیرامونی، پدافند غیرعامل اهمیت فوق‌العاده و ابعاد گسترده‌ای دارد. متأسفانه با وجود این امر نه در گذشته و نه در حال حاضر تمهیدات لازم به منظور پدافند غیرعامل فاوا در برابر شرایط جنگ و نیز سوانح طبیعی، مانند زلزله، پیش‌بینی نشده است.

مبانی نظری تحقیق

راهبردهای اصلی پدافند غیر عامل در حوزه فاوا

بر اساس ضرورت تشکیل کمیته دائمی پدافند غیرعامل به منظور هماهنگ‌سازی، سیاست‌گذاری، کنترل، نظارت و تصویب طرح‌های پدافند غیرعامل پروژه‌های عمرانی کشور در ستاد کل نیروهای مسلح و تأمین و توسعه امنیت، ایمنی و پایداری در فضای تبادل اطلاعات کشور و کاهش آسیب در برابر تهدیدات و جنگ، می‌توان راهبردهای اصلی پدافند غیر عامل در حوزه فاوا را چنین برشمرد:

- ۱- نهادینه کردن فرامین و قانونمندی‌سازی تدابیر مقام معظم رهبری^{مدظله‌العالی} درباره پدافند غیرعامل در سازمان‌ها و دستگاه‌های مربوط
- ۲- ساماندهی، انسجام‌بخشی و هدایت راهبردی مجموعه‌های علمی، پژوهشی، آموزشی و صنعتی مرتبط با حوزه تخصصی فاوا در راستای تولید و توسعه دانش و فناوری‌های بومی و ملی مورد نیاز پدافند غیرعامل
- ۳- توسعه امنیت، ایمنی و پایداری در شبکه‌های ارتباطی و الکترونیکی موجود با تأکید بر فناوری‌های بومی
- ۴- نهادینه کردن اصول و ملاحظات پدافند غیرعامل در طرح‌های توسعه شبکه‌های ارتباطی و الکترونیکی
- ۵- توسعه فرهنگ پدافند غیرعامل و ارتقای دانش و شناخت مسئولان و کارشناسان حوزه ارتباطات و الکترونیک از پدافند غیرعامل
- ۶- خوداتکایی از دستگاه‌های پشتیبان آسیب‌پذیر و خودکفایی از منابع خارجی فناوری‌ها
- ۷- حمایت از برنامه ایجاد شبکه ملی اینترنت مبتنی بر مؤلفه‌های امنیت، ایمنی، پایداری و متکی بر فناوری‌های بومی
- ۸- توسعه و تقویت سیستم پست کشور (بهره‌مندی از پست بسیار سریع و امین)
- ۹- بهره‌مندی از شبکه ارتباطی ویژه مدیریت کشور در شرایط بحران جنگ (با مؤلفه‌های امنیتی و پایداری و ایمنی بسیار بالا و دسترسی سریع)
- ۱۰- توسعه توان کنترل و مدیریت بحران و برنامه‌های حراست، حفاظت و ضد جاسوسی
- ۱۱- نهادینه کردن ملاحظات دفاع غیرعامل و امنیت ملی در تعاملات و همکاری با کشورها و شرکت‌های خارجی در حوزه ICT (گزارش سازمان پدافند غیر عامل، ۱۳۹۴).

پدافند غیر عامل

از نظر واژه‌شناسی، واژه «پدافند» از دو جزء «پد» و «آفند» تشکیل شده است. در فرهنگ و ادب فارسی «پاد» یا «پد» پیشوندی است که به معانی «ضد، متضاد، پی و دنبال» بوده و هرگاه قبل از واژه‌ای قرار گیرد معنای آن را معکوس می‌نماید. واژه «آفند» نیز به مفهوم «جنگ، جدال، پیکار و دشمنی» است (دهخدا، ۱۳۵۱: ۴۷). صدری افشار واژه «پدافند» را از نظر لغوی هم‌تراز با واژه «دفاع» و مشتمل بر «کارهایی که برای پیشگیری از حمله دشمن یا پیروزی او

در حمله انجام می‌گیرد» بیان نموده است (صدری افشار و حکمی، ۱۳۷۳: ۲۵۹)، ولی عبارت «پدافند غیرعامل»^۱ یعنی به کار بردن روش‌هایی که آثار زیان‌های ناشی از اقدام‌های دشمن بکاهد یا آن را به حداقل برساند (زیاری، ۱۳۷۸: ۱۳۴). به بیان ساده‌تر، در پدافند غیرعامل از هیچ نوع جنگ‌افزاری در برابر دشمن استفاده نمی‌گردد. برخی نیز پدافند غیرعامل را امکانات معماری در زمینه مهندسی جنگ می‌داند، به‌گونه‌ای که، بدون ابزار و توانمندی، نیروهای رزمی و دفاعی را افزایش دهد. در این تعریف پدافند غیرعامل نیازی به حضور انسان نداشته و هرکسی آنجا را متصرف شود، راندمان دفاعی بیشتری در جنگ خواهد یافت. همچنین، پدافند غیر عامل به استفاده از پوشش، اختفا و پراکندگی، فریب و کنترل حرکات در روشنایی اطلاق می‌شود (جدی، ۱۳۷۴). پدافند غیر عامل به هرگونه عملیاتی اطلاق می‌شود که نیاز به جنگ‌افزار نداشته و از وارد شدن خسارت‌های مالی، نظامی، تأسیسات حساس شهری و تلفات انسانی جلوگیری نماید یا به حداقل برساند (موحدی‌نیا، ۱۳۸۵: ۲۳). پدافند غیر عامل به اقدام‌های احتیاطی و افزایش پایداری و کاهش خسارات و ضایعات به حد صفر اطلاق می‌شود. به‌طور کلی، چنانچه تمهیدات اساسی در اجرای پدافند غیر عامل انجام گیرد، می‌توان جلوه آن را در امنیت ملی و ادامه حیات و زنده ماندن نیروهای انسانی، کاهش آسیب‌پذیری و خسارات به مراکز حیاطی، حساس و مهم نظامی و غیر نظامی، سلب آزادی و ابتکار عمل از دشمن، فریب و تحمیل هزینه بیشتر به دشمن، صرفه‌جویی از هزینه‌های تسلیحاتی و انسانی، افزایش آستانه مقاومت مردم و نیروی خود در برابر دشمن، حفظ روحیه و وحدت ملی و حفظ تمامیت ارزی به خوبی مشاهده کرد (تهامی، ۱۳۷۶: ۴۴؛ نباتی، ۱۳۸۶: ۱۶-۲۱).

اصول پدافند غیر عامل

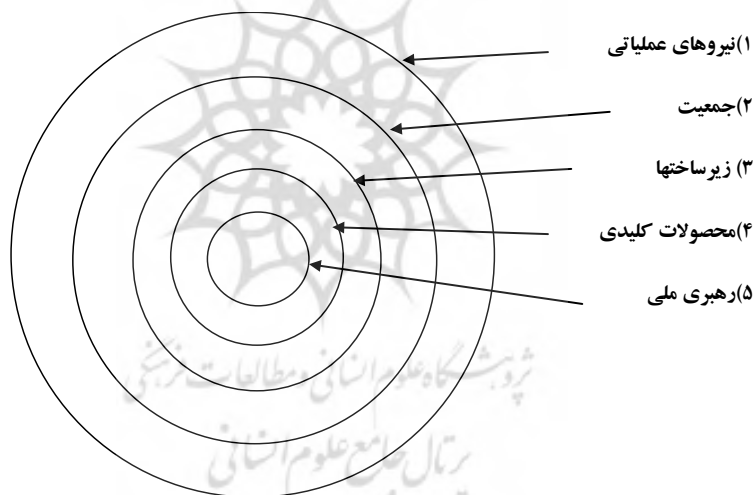
برای پدافند غیرعامل یا دفاع غیرعامل در حوزه نظامی و غیرنظامی و حوزه فرهنگی اصول و مبانی خاصی را در نظر گرفته‌اند. این اصول دربردارنده مجموعه اقدام‌های بنیادی و زیربنایی است که در صورت به کارگیری می‌توان به اهداف پدافند غیر عامل از قبیل تقلیل خسارات، کاهش آسیب‌پذیری و تحمیل هزینه بیشتر به دشمن و ... نائل گردی. این اصول عبارت‌اند از: اصل استتار (قربانی، ۱۳۸۲: ۵۳)، اصل اختفا، اصل پوشش، اصل فریب، اصل تفرقه و پراکندگی، اصل مقاوم‌سازی، اصل اعلام خبر (قرارگاه پدافند هوایی خاتم‌الانبیا، ۱۳۸۳: ۱۷).

در کنار موارد بیان شده موارد دیگری نیز به عنوان اقدام‌های اساسی در بخش دفاع غیر عامل بیان شده است که مکان‌یابی، تحرک، پناهگاه، جان‌پناه، انضباط استتار، حفاظت و مقاوم‌سازی تأسیسات از جمله مهم‌ترین آن‌ها تلقی می‌شود (اکبری، ۱۳۸۵، ۱۳۸۴: ۳-۴؛ طیاری، ۱۳۶۸: ۷۱). در واقع، اصول پدافند غیر عامل در مقابل تئوری جان‌واردن^۱ و به منظور کاهش آسیب‌پذیری مراکز حساس^۲، مراکز حیاتی^۳ و مراکز مهم^۴ کشور کاربردهای وسیعی دارد. در تئوری واردن آمده است که «مهم‌ترین وظیفه در طرح‌ریزی یک جنگ، شناسایی مراکز ثقل کشور مورد تهاجم بوده و چنانچه این مراکز با دقت لازم شناسایی و مورد هدف قرار گیرند، کشور مورد تهاجم در نخستین روزهای جنگ طعم شکست نظامی را چشیده و در کوتاه‌ترین مدت به خواسته‌های کشور مهاجم تن در داده و تسلیم خواهد شد». در تئوری واردن مراکز ثقل هر کشور شامل پنج حلقه دوایر متحد‌المרכזی می‌باشد که در مجموع، ساختارهای اصلی قدرت هر کشور را تشکیل می‌دهند و پدافند غیر عامل در حراست از مراکز مهم کشور اهمیت ویژه‌ای دارد (آیت‌اللهی، ۱۳۸۴؛ عباسی‌پور، ۱۳۸۴) کشورهایی که پدافند غیرعامل را به عنوان راهکاری اصلی برمی‌گزینند به شرایطی از نظر کاهش آسیب‌پذیری دست می‌یابند که مطامع کشورهای تهدیدکننده علیه آن‌ها کاهش می‌یابد (طیاری، ۱۳۶۸). در جهان امروز کشورهایی که نقاط آسیب‌پذیری آن‌ها فراوان است و دشمن می‌تواند با ضربات سریع، حیاتی‌ترین منابع آنان را منهدم کند، عوامل تهدید از بیرون را در درون خود ایجاد می‌کنند. به عبارتی، دشمنان بالقوه را نسبت به خود حریص و فعال می‌نماید. پدافند غیرعامل عنصری پویا و متحرک است، از این رو، می‌تواند در اولویت تلاش‌های علمی و پژوهشی قرار گیرد و در همه سطوح مدیریتی، مهندسی و فنی، آموزش داده شود و توسعه یابد. براین اساس، شیوه‌های پدافند غیرعامل، ایجاد اختلال در شناسایی، کسب اطلاعات و دقت هدف‌گیری دشمن از راه اختفا، استتار، پوشش، فریب، جابه‌جایی، استفاده سامانه‌های اختلال در هدف‌گیری صورت می‌گیرد. همچنین، کاهش آسیب‌پذیری نقاط هدف و تأثیر سلاح دشمن، به عنوان یکی دیگر از شیوه‌های پدافند غیرعامل، از طریق مکان‌یابی صحیح، ایجاد مانع و استحکامات، مستحکم کردن ساختمان‌ها و تأسیسات، استفاده از عوارض طبیعی سطح زمین، استفاده از

۱. در سال ۱۹۸۸ جان واردن، سرهنگ هوایی ارتش ایالات متحده آمریکا، کتابی با عنوان نبرد هوایی را تدوین نمود و در آن نظریه مشهور خود را با نام «تئوری واردن» مطرح کرد.

2. Critical Centers
3. Vital Centers
4. Important Centers

عمق زمین، اعمال تدابیر دفاع سایبری، ایجاد لایه‌های محافظ الکترونیکی و الکترومغناطیسی و رعایت ضوابط ایمنی صورت می‌گیرد. "کاهش اهمیت و حساسیت نقاط هدف" یکی دیگر از شیوه‌های پدافند غیرعامل است که با پراکندگی، تجزیه، پیش‌بینی امکانات جایگزین و موازی و کوچک‌سازی صورت می‌گیرد. "کنترل خسارت" نیز دیگر شیوه پدافند غیرعامل است که با استفاده از سامانه‌های هشداردهنده، ساماندهی امکانات امداد و نجات، تعیین وظایف بخش‌ها و افراد و آموزش و تمرین صورت می‌گیرد (قرارگاه پدافند هوایی خاتم‌الانبیاء، ۱۳۸۳: ۲۰). راهبرد اصلی پدافند غیر عامل، کاهش آسیب‌پذیری در برابر حملات نظامی دشمن براساس مدل ۵ حلقه‌ای واردن است. این مراکز، همانند دوایر متحد‌المركز، حول یکدیگر قرار داشته و هم‌دیگر را حمایت می‌کنند و عبارت‌اند از: رهبری ملی، محصولات کلیدی، زیرساخت‌ها (فاوا)، جمعیت و نیروهای عملیاتی (شکل ۱ و جدول ۱).



شکل شماره ۱: مدل ۵ حلقه‌ای واردن (قرارگاه پدافند هوایی خاتم‌الانبیاء، ۱۳۸۳).

جدول شماره ۱: اجزای پنج حلقه‌ای واردن

حلقه‌ها	عناوین	مقایسه با انسان	مراکز ثقل
اول	رهبری ملی	مغز و سیستم عصبی	رهبری، مراکز امنیتی تصمیم‌گیری‌های کلان سیاسی (مجلس، ریاست جمهوری، صداوسیما، وزارتخانه‌ها، قرارگاه‌های عمده فرماندهی، ستاد کل نیروهای مسلح، مخابرات راه دور)
دوم	محصولات کلیدی	سیستم گردش خون	نیروگاه‌ها، پالایشگاه‌ها، مخازن سوخت، صنایع دفاعی، انبارهای عمده مواد غذایی شامل سیلوها و سردخانه‌ها، انبارهای دارویی و شبکه آبرسانی
سوم	زیرساخت‌ها	اندام‌های حرکتی	فرودگاه‌ها، راه‌آهن، مترو، بندر، سدها، پل‌ها، اتوبان‌ها، شبکه مخابرات شهری
چهارم	جمعیت مردمی و اراده ملی	روح و روان و اراده	کلان‌شهرها، شهرها، روستاها، مراکز جمعیتی مهم
پنجم	نیروهای عملیاتی	سلول‌های دفاعی	سیستم اعلان خبر راداری، توپخانه، سیستم موشکی، پدافند هوایی، پایگاه‌های هوایی-دریایی، مراکز تعمیرگاهی، یگان‌های عملیاتی خطوط مقدم قرارگاه‌های تاکتیکی

(همان: ۲؛ داعی‌نژاد و امین‌زاده، ۱۳۸۵)

چهارچوب نظری تحقیق

براساس مدل واردن، فاوا جزو زیرساخت‌های حیاتی کشور و به عنوان حلقه سوم از مدل ۵ حلقه‌ای واردن تلقی می‌شود. این زیرساخت‌ها شامل مراکز داده، سیستم‌عامل ملی، شبکه تلفن ثابت و همراه، ماهواره، شبکه بی‌سیم، فیبرنوری و غیره، شریان‌های حیاتی ارتباطی کشور محسوب می‌شوند و تدابیر لازم برای پشتیبانی از هر کدام آن‌ها در حالت‌های اضطراری کشور، نکته‌ای است که نباید فراموش شود. مأموریت پدافند غیرعامل در حوزه فاوا تضمین امنیت، ایمنی و پایداری زیرساخت‌های حوزه فناوری اطلاعات و ارتباطات، کاهش آسیب‌پذیری‌ها و افزایش آستانه تحمل در رویارویی با تهدیدات، با تأکید بر ایجاد عزم ملی از طریق فرهنگ‌سازی، سیاست‌گذاری، طرح‌ریزی و برنامه‌ریزی، هدایت راهبردی و تدوین و تصویب ضوابط و دستورالعمل‌های عمومی و تخصصی و نظام‌های هدایت‌بخش کشوری به منظور نهادینه کردن رعایت اصول پدافند غیر عامل در حوزه فناوری اطلاعات و ارتباطات

و نظارت بر اجرای آن با ایجاد قابلیت به روزرسانی است. با این وصف، پدافند غیر عامل در حوزه فاوا به دو بخش نرم‌افزاری و سخت‌افزاری تفکیک می‌گردد. در بخش نرم‌افزاری باید از نرم‌افزارهای ضد جاسوسی و آنتی‌ویروس‌ها در جهت جلوگیری از حمله سایبری دشمن به فاوا اشاره کرد. و در بخش سخت‌افزاری که بیشتر مورد توجه پژوهش پیش‌رو است باید به ساختار فیزیکی و معماری فاوا اشاره نمود.

۱. راهبردهای پدافند غیرعامل معماری و زمین‌شناسی فاوا: بایسته‌های پدافند غیرعامل در حوزه معماری فاوا افزون بر کاهش خسارات تهدیدات انسان‌ساز (جنگ و بمباران هوایی و ...)، برای کاهش خطرپذیری در برابر انواع خطرهای طبیعی نیز کاربرد دارد. تلفیق طراحی پدافند غیر عامل، برای مقابله با خطرهای طبیعی، مانند زلزله، افزون بر تهدیدات انسان‌ساز، در زمان صلح و جنگ، باعث "پایداری" طرح دفاعی فاوا می‌شود. از این رو، الزامات معماری فاوا به گروه‌های خاصی طبقه‌بندی شده است. این گروه‌ها عبارت‌اند از: برنامه‌ریزی شامل مکان‌یابی و آرایش استقرار، موانع، پراکندگی و مدیریت ساخت و بهره‌برداری؛ اغتشاش در دید دشمن شامل ضد مراقبت؛ دید دشمن شامل استتار، اختفا و عوامل فریب؛ طراحی شامل معماری داخلی، فضاهای چند عملکردی، ورودی و خروجی‌های معمولی و اضطراری، مرمت‌پذیری، نمای داخلی و خارجی ساختمان؛ ساخت شامل شبکه‌های زیرساخت، تأسیسات و استحکامات (جدی، ۱۳۸۳؛ داعی‌نژاد، ۱۳۸۵؛ شفیع، ۱۳۶۸). همچنین، باید به راهبردهای زمین‌شناسی و زیرساخت‌های فاوا نیز اشاره کرد. با توجه به عملکرد دینامیک درونی و بیرونی و شکستگی‌های ایجاد شده (یعنی گسل‌ها) در پوسته زمین، باید مکان‌یابی فاوا به گونه‌ای صورت گیرد که حرکات زمین‌ساختی کمترین خطر را برای فاوا ایجاد کند (سهامی، ۱۳۸۶: ۳۷؛ دیوسالار، ۱۳۸۶: ۸۸). بنابراین، آگاهی از گسل‌ها و جهت چین‌خوردگی‌های زمین، سطح آب زیرزمینی بسیار با اهمیت است. براساس مطالعات در ملاحظات پدافند غیر عامل زمین‌شناسی، به ویژه در پنهان‌سازی فاوا، توجه به پرتگاه‌های گسل‌ها و دره‌های گسله کاربرد دارند، زیرا این ساخت‌های طبیعی زمینی، مانعی برای هدف قرار دادن امکانات و تجهیزات فاوا بوده و از طرف دیگر، می‌تواند در ایجاد مانع برای دستیابی زمینی دشمن به اهداف مورد نظر کاربرد داشته باشد (همان: ۶۶).

۳) راهبردهای مکان‌یابی فاوا: تجمعات وسیع انسانی و شناسایی دقیق مکان‌های شهری همواره شهرها را جزو مراکز اصلی حمله دشمن قرار داده است. با توجه به اینکه شهرها کانون

مراکز اقتصادی و اجتماعی و صنعتی هستند و فاوا نیز جزو مراکز حیاتی شهرها محسوب می‌شوند، ضرورت دارد مکان‌یابی فاوا در سطح شهر مورد توجه مسئولان قرار گیرد. به‌طور کلی، در برنامه‌ریزی دفاعی شهر باید به ملاحظات مکان‌یابی فاوا به منظور کمترین آسیب‌رسانی به آن توجه کرد (کارگر، ۱۳۹۰: ۱۴). مکان‌یابی فاوا ارتباط تنگاتنگی با معیارهای هفت‌گانه انتخاب بهترین هدف از سوی دشمن دارد که عبارت‌اند از: ۱. اهمیت و حساسیت هدف. ۲. قابلیت دسترسی هدف. ۳. قابلیت مرمت و احیای مجدد هدف. ۴. آسیب‌پذیری هدف. ۵. تأثیرپذیری هدف. ۶. قابلیت کشف هدف.

دشمن پیوسته براساس ملاحظات یادشده به هدف خود در سطح شهر حمله می‌برد. بنابراین، براساس اصول پدافند غیر عامل در مکان‌یابی فاوا در سطح شهر باید به ملاحظات زیر توجه کرد: اصل کوچک‌سازی، اصل پراکنده‌سازی فاوا در سطح شهر، اصل مکان‌یابی دفاعی، اصل تمرکززدایی، اصل استتار، اصل اختفا، اصل استحکام، اصل اطلاع‌رسانی و اعلان خبر، اصل آمایش دفاعی سرزمینی در سطح شهر، اصل پوشش، اصل فریب، اصل بومی‌سازی (همان: ۴۳).

۴) راهبردهای پدافند غیر عامل در امور فنی و رایانه‌ای فاوا:

- ملاحظات مربوط به مودم‌ها
- ملاحظات مربوط به خطوط ارتباطی مخبراتی
- ملاحظات مربوط به تسهیم‌کننده‌ها
- ملاحظات مربوط به جلوگیری از تهدیدات و حملات علیه شبکه‌ها
- ملاحظات پدافند غیر عامل در شبکه‌های^۱ PAP (ابراهیم‌نژاد، ۱۳۸۶: ۷۶؛ ابهری، ۱۳۸۶: ۶۱؛ پیمانی، ۱۳۸۶: ۵۲).

روش تحقیق

به‌طور کلی، روش این پژوهش توصیفی-تحلیلی است. جامعه آماری استادان و کارشناسان حوزه پدافند غیر عامل ناجا به تعداد نمونه ۳۸ نفر است که از طریق جدول مورگان به روش نمونه‌گیری احتمالی طبقه‌ای انتخاب شدند. نویسنده پس از تعریف عملیاتی متغیرها، مؤلفه‌های دسته اول و دسته دوم را تدوین و به صورت پرسش درآورده و پرسش‌ها را با

1 . PAP: Private Access Provider

مقیاس لیکرت به پرسشنامه محقق ساخته تبدیل کرده و پرسشنامه را به عنوان ابزاری برای گردآوری داده‌ها در اختیار جامعه آماری قرار داد. به منظور سنجش اعتبار^۱ ابزار (پرسشنامه) از روش اعتبار محتوا و سنجش پایایی^۲ ابزار از روش آلفای کرونباخ^۳ (۰/۹۳۴) استفاده شد و این مهم مؤید این واقعیت است که پرسشنامه و داده‌های تحقیق از قابلیت اطمینان بالایی برخوردار بوده است. همچنین، رفت و در **نهایت** داده‌های به دست آمده به نرم افزار SPSS منتقل و مورد تجزیه و تحلیل قرار گرفتند. در تجزیه داده‌ها فقط از جداول توصیفی بهره برده شد و در تحلیل و آزمون فرضیه‌ها از آزمون یک متغیره کای اسکوئر استفاده شد.

یافته‌های تحقیق

درصد	فراوانی	تحصیلات	درصد	فراوانی	شغل
۲۶	۱۰	دکتری	۲۶	۱۰	هیئت علمی
۵۸	۲۲	کارشناس ارشد	۳۲	۱۸	مدیر و کارشناس فاوا
۲۱	۸	کارشناس	۲۶	۱۰	کارشناس پدافند غیر عامل
۱۰۰,۰	۳۸	جمع	۱۰۰,۰	۳۸	جمع

جدول شماره ۲: شغل و تحصیلات پاسخ‌گویان

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی

- 1 .validity
- 2 .Reliability
- 3 . Cronbach's Alpha
- 4 .Statistic Packag For Social Science.

جدول شماره ۳: آزمون یک متغیره راهبردهای پدافند غیر عامل مراکز فاوای ناجا

سطح معناداری	آزمون یک متغیره کای اسکوئر(خی دو)			راهبردها	ردیف	
	تفاضل	فراوانی مورد انتظار	فراوانی مشاهده شده			گزینه
P<۰.۰۱	۹/۵	۹/۵	۱۹	کاملاً مخالفم	راهبرد اختفای مراکز فاوای ناجا	۱
	۱/۵	۹/۵	۱۱	مخالفم		
	-۲/۵	۹/۵	۷	نظری ندارم		
	-۸/۵	۹/۵	۱	موافقم		
	--	--	--	کاملاً موافقم		
	۳۸			جمع		
P<۰.۰۱	-۰/۵	۹/۵	۹	کاملاً مخالفم	راهبرد استحکام‌بنا	۲
	۷/۵	۹/۵	۱۷	مخالفم		
	-۲/۵	۹/۵	۷	نظری ندارم		
	-۴/۵	۹/۵	۵	موافقم		
	--	--	--	کاملاً موافقم		
	۳۸			جمع		
P<۰.۰۱	۱/۳	۱۲/۷	۱۴	کاملاً مخالفم	راهبرد پراکندگی	۳
	۶/۳	۱۲/۷	۱۹	مخالفم		
	-۷/۷	۱۲/۷	۵	نظری ندارم		
	--	--	--	موافقم		
	--	--	--	کاملاً موافقم		
	۳۸			جمع		
P<۰.۰۱	-۰/۵	۹/۵	۹	کاملاً مخالفم	راهبرد فریب	۴
	۹/۵	۹/۵	۱۹	مخالفم		
	-۲/۵	۹/۵	۷	نظری ندارم		
	-۶/۵	۹/۵	۳	موافقم		
	--	--	--	کاملاً موافقم		
	۳۸			جمع		

جمع‌بندی نتایج تحقیق

توجه به راهبردهای پدافند غیر عامل در حوزه فاوا از اهمیت ویژه‌ای دارد. راه‌وروش امنیتی - راهبردی فاوا دربر دارنده توجه به اصول استتار، اختفا، پوشش، فریب، پراکندگی و اصل مقاومت‌سازی مراکز فاوای ناجاست. نتایج جداول توصیفی و آزمون فرضیه‌ها مشخص می‌کند که ابعاد وجودی راهبردهای امنیتی مراکز فاوا در خصوص اصل مقاومت‌سازی و ساخت و توسعه استحکامات بناهای فاوا، یعنی ساخت استحکاماتی که در صورت اضطرار، کارکنان و امکانات ایمن باشند، مورد توجه لازم قرار نگرفته است. همچنین، درباره دیگر راهبردهای پدافند غیر عامل حوزه فاوا، مانند ساماندهی، انسجام‌بخشی و هدایت راهبردی مجموعه‌های علمی، پژوهشی، آموزشی و صنعتی مرتبط با حوزه تخصصی فاوا در راستای تولید و توسعه دانش و فناوری‌های بومی و ملی مورد نیاز پدافند غیرعامل و توسعه امنیت، ایمنی و پایداری در شبکه‌های ارتباطی و الکترونیکی موجود با تأکید بر فناوری‌های بومی و توجه به اصل فریب دشمن و پراکندگی مکان‌های فاوا و درنهایت، توجه به داشتن پناهگاه در فاوا باید گفت که از دیدگاه کارشناسان، به این اصول توجه نشده و باید تمهیدات لازم در این زمینه به کار گرفته شود.

پیشنهاد‌های تحقیق

به منظور حفاظت از تجهیزات فاوا و برقراری امنیت خدمات شبکه‌های ADSL با رویکرد پدافند غیر عامل و به منظور دست یافتن به اهداف ترسیم شده در اسناد پدافند غیر عامل موارد زیر در دو بخش سخت‌افزاری (پدافند غیر عامل در حوزه مکانی) و نرم‌افزاری (پدافند غیر عامل در حوزه سیستمی نرم‌افزاری) پیشنهاد می‌شود.

- حوزه سخت‌افزاری و مکانی

۱. پیشنهاد می‌شود که مکان‌های فاوا از کاربری‌های استتار استفاده کنند. در این زمینه پیشنهاد می‌شود:
 - استتار در حوزه عادی جلوه دادن ساختمان فاوا با درخت کاری و گسترش ساختمان‌های اداری و مسکونی
 - حذف فاوا از روی نقشه استانی و شهری و شبکه‌های تلویزیونی و آگهی‌های محیطی و جراید
 - استفاده از رنگ‌ها با هدف قابل رؤیت نبودن منطقه فاوا از هوا و زمین
 - پوشش ساختمانی فاوا از درخت و شاخ و برگ‌ها به منظور پنهان ماندن ساختمان از دیدبانی هوایی دشمن؛
 - پوشش ساختمانی فاوا با استفاده از نقاشی‌ها و معماری ناهمگون، همانند ساختمان‌های مسکونی و اداری و تجاری یا تفریحی؛
 - توجه به بدل‌سازی و کوچک جلوه دادن ساختمان‌های فاوا و شبیه کردن آن‌ها به ساختمان‌های مسکونی؛
 - توجه به استحکام بنای فاوا در مقابل بمب و موشک دشمن؛
 - توجه به استحکام بنای فاوا در مقابل زلزله و سیل؛
 - توجه به استحکام بنای فاوا با ساخت بنا در دل کوه و سیمان مسلح و بتون.
۲. پیشنهاد می‌شود که مدیران فاوا به موضوع تمرکززدایی و توجه به مراکز متعدد فاوا با ظرفیت کمتر توجه کنند؛
۳. پیشنهاد می‌شود که مدیران فاوا به سیستم تأمین اعلام خطر برای پست‌ها و کارکنان در مواقع خطر توجه کنند؛
۴. پیشنهاد می‌شود که مدیران فاوا با به کارگیری مسئولی برای اعلام خطر به دیگران و به صدا درآوردن آژیر خطر در موارد بحرانی در مواقع خطر توجه کنند؛
۵. پیشنهاد می‌شود که مدیران فاوا به ساختن پناهگاه برای کارکنان توجه کنند؛
۶. پیشنهاد می‌شود که مدیران فاوا به استفاده از مواد دودزای مؤثر در برابر حس‌گرهای ناحیه مری دشمن، مانند پودر برنج، فسفر قرمز، الیاف با پوشش آلومینیم توجه کنند؛
۷. پیشنهاد می‌شود مدیران فاوا به استفاده از تکنیک تولید صداهای فریبنده توسط

آتش‌زنه‌ها، که موجب مخفی ماندن صداهای اصلی در برابر دشمن می‌شود، توجه کنند؛
۸. پیشنهاد می‌شود که مدیران فاوا به استفاده از فریب تبلیغاتی و استفاده از تابلوهایی که نشان دهنده ماهیت تجاری و تفریحی بودن مکان فاوا باشد، توجه کنند.

-حوزه نرم‌افزاری و سیستم‌های الکترونیکی فاوا

۱. تجهیزاتی که در فاوا بیشترین نیاز امنیتی را دارند، در امن‌ترین منطقه قرار گیرند و اجازه دسترسی عمومی به آن‌ها یا از شبکه‌های دیگر به این منطقه داده نشود. دسترسی‌ها باید با کمک یک فایروال یا دیگر امکانات امنیتی، مانند دسترسی از راه دور^۱ به طور امن کنترل شود. همچنین، کنترل شناسایی و احراز هویت و مجاز یا غیرمجاز بودن در این منطقه باید با درجه امنیت بالایی انجام شود؛

۲. سرورهایی که در این شبکه‌ها استفاده می‌شود و در دسترس‌اند، در منطقه‌ای جداگانه و دارای ضریب امنیتی بالاتر نسبت به دیگر بخش‌ها قرار گیرند تا در صورت حمله به یکی از آن‌ها، دیگران تهدید نشوند. به این مناطق، مناطق خارج از تهدیدات نظامی^۲ گفته می‌شود؛

۳. حملات مرتبط با تحلیل ترافیک که طی آن براساس یک‌سری بسته‌های اطلاعاتی، مهاجم می‌تواند ترافیک شبکه را تحلیل کرده و اطلاعات ارزشمندی را کسب کند، شناسایی شود. این حملات از نوع غیر فعال است و بیشتر به دست کاربران خارجی صورت می‌گیرد؛

۴. امکان دستکاری پیام‌ها و داده‌ها که بر اساس آن مهاجم می‌تواند جامعیت و صحت اطلاعات را با تغییرات غیرمجاز برهم زند، از بین برود. این نوع حملات نیز به دست کاربران خارجی صورت می‌گیرد. همچنین، امکان جعل هویت، که طی آن مهاجم هویت یک فرد مجاز شبکه را جعل می‌کند، به حداقل میزان ممکن برسد؛

۵. امنیت ارتباطات که در آن با استفاده از فایروال‌ها، سیستم‌های ضد ویروس، سرورهای کنترل دسترسی و احراز هویت، نرم‌افزارهای مانیتورینگ، ثبت و تحلیل رویدادها می‌توان به تشخیص هویت و کنترل کاربران پرداخت.

1 . RAS: Remote Access Control

2 . DMZ: Demilitarized Zone

منابع

- ابراهیم نژاد، محمد (۱۳۸۶). آشنایی با تسلیحات غیر کشنده، پژوهشکده مهندسی، تهران، دانشگاه صنعتی مالک اشتر.
- ابهری، مریم (۱۳۸۶). مدیریت بحران، پژوهشکده مهندسی، تهران، دانشگاه صنعتی مالک اشتر.
- اصغریان جدی، احمد (۱۳۷۹). «روش تحقیق مهندسی جنگ»، تهران، دانشگاه شهید بهشتی، دانشکده معماری و شهرسازی، مجله صفا، ش ۳.
- ---- (۱۳۸۳). «الزامات معمارانه در پدافند غیر عامل پایدار»، تهران، دانشکده معماری شهید بهشتی، پایان نامه دکتری.
- ---- (۱۳۸۳). «رابطه ترس و معماری»، تهران، دانشگاه شهید بهشتی، دانشکده معماری و شهرسازی، مجله صفا، ش ۳۹.
- ---- (۱۳۷۴). «پدافند غیر عامل در ارگ بم»، مجموعه مقالات کنگره تاریخ معماری و شهرسازی ایران، ارگ بم کرمان، ج ۲، سازمان میراث فرهنگی کشور، تهران.
- اکبری، عباس (۱۳۸۴). آشنایی با سنجنده‌ها و تأسیسات زیر زمینی، تهران، معاونت پدافند غیر عامل، قرارگاه پدافند هوایی خاتم الانبیا (ص).
- ---- (۱۳۸۴). فضاهای امن پناهگاهی، تهران: معاونت پدافند غیر عامل، قرارگاه پدافند هوایی خاتم الانبیا (ص).
- ---- (۱۳۸۵). آشنایی با آمایش و دفاع سرزمینی، تهران، معاونت پدافند غیر عامل، قرارگاه پدافند هوایی خاتم الانبیا (ص).
- ---- (۱۳۸۵). آشنایی با آمایش و دفاع سرزمینی، معاونت پدافند غیر عامل، تهران، قرارگاه پدافند هوایی خاتم الانبیا (ص).
- ---- (۱۳۸۵). آشنایی با روش‌های استتار، تهران، معاونت پدافند غیر عامل، قرارگاه پدافند هوایی خاتم الانبیا (ص).
- آیت‌اللهی (۱۳۸۴). آشنایی با فضاهای امن پناهگاهی، تهران، معاونت پدافند غیر عامل قرارگاه پدافند هوایی خاتم الانبیا، نشریه ش ۵.
- پیمانی، صفا (۱۳۸۶). استحکامات و سازمان‌های امن، تهران، پژوهشکده مهندسی دانشگاه صنعتی مالک اشتر.
- جدی، سیدمجید و دیگران (۱۳۸۵). مدیریت بحران با رویکرد انتظامی، تهران، معاونت آموزش ناچا.

- جلالی، علی اکبر (۱۳۹۲). ارتباطات در زمان بحران در زمان متغیر رسانه‌ها، رسانه. داعی نژاد، فرامرز و دیگران (۱۳۸۵). اصول و رهنمودهای طراحی و تجهیز فضای باز مجموعه‌های مسکونی به منظور پدافند غیرعامل، تهران، مرکز تحقیقات ساختمان و مسکن.
- دفترچه اولین همایش پدافند غیر عامل (آبان ۱۳۹۱)، ناجا.
- دهخدا، علی اکبر (۱۳۵۱). لغت‌نامه دهخدا، دانشگاه تهران، ج ۴، ص ۴۷ و ۴۸.
- دیوسالار، عبدالرسول (۱۳۸۶). مقدمه‌ای بر محیط‌شناسی نظامی و جنگ‌های اطلاعاتی، تهران، پژوهشکده مهندسی دانشگاه صنعتی مالک اشتر.
- رئیس دانا و دیگران (۱۳۸۱). «کاربردها و سودمندی‌های فناوری اطلاعات»، تکنولوژی آموزشی.
- زیاری، کرامت‌الله (۱۳۷۸). برنامه‌ریزی شهرهای جدید، سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها (سمت)، تهران.
- ---- (۱۳۸۰). «برنامه‌ریزی پدافند و پناهگاه شهری»، تهران، دانشگاه شهید بهشتی، دانشکده معماری و شهرسازی، مجله صفا، ش ۳۲.
- سهامی، حبیب‌الله (۱۳۸۶). آمایش و مکان‌یابی، تهران، پژوهشکده مهندسی دانشگاه صنعتی مالک اشتر.
- شرکت سخا روش (۱۳۸۲). جزوه آموزشی پدافند غیر عامل در حوزه فاوا.
- شفیعی اردستانی، احمدرضا (۱۳۶۸). پدافند غیرعامل در آلمان، وزارت مسکن و شهرسازی، معاونت فنی و اجرایی و امور جنگ، دفتر سازه‌های امن.
- صدری افشار، غلامحسین و نسرین حکمی (۱۳۷۳). فرهنگ فارسی امروز، مؤسسه نشر کلمه، تهران.
- ضوابط فنی برای ساخت پناهگاه‌ها، تهران، وزارت مسکن و شهرسازی، دفتر سازه‌های امن، نشریه ش ۳۴.
- طیاری، حمید (۱۳۶۸). پدافند غیرعامل در ۳۱ کشور جهان، وزارت مسکن و شهرسازی، معاونت فنی و اجرایی و امور جنگ، دفتر سازه‌های امن.
- عباس پور سینایی، جمشید (۱۳۸۴). مقدمه‌ای بر اصول و مبانی اساسی پدافند غیر عامل، تهران، معاونت پدافند غیرعامل، قرارگاه پدافند هوایی خاتم‌الانبیا (ص).
- فصلنامه مطالعات دفاعی (بهار ۱۳۸۰). میزگرد ایران‌شناسی، رویکردهای دفاعی و امنیتی، (سخنان سردار اسلامی)، ش ۲۶.

- قربانی، محمود(۱۳۸۲). آیین‌نامه استتار، تهران، معاونت پدافند غیرعامل، قرارگاه پدافند هوایی خاتم‌الانبیا(ص).
- کارگر، بهمن(۱۳۹۰). امنیت شهری، تهران، سازمان جغرافیایی وزارت دفاع و پشتیبانی نیروهای مسلح.
- کالینز، جان ام(۱۳۷۳). استراتژی بزرگ (اصول و رویه‌ها)، ترجمه کوروش بایندر، تهران، دفتر مطالعات سیاسی و بین‌المللی وزارت امور خارجه.
- مشیری سعید و اسفندیار جهانگرد (۱۳۸۳). فناوری اطلاعات و ارتباطات (ICT) و رشد اقتصادی ایران، سایت جهاد دانشگاهی SID.
- معاونت پدافند غیرعامل قرارگاه پدافند هوایی خاتم‌الانبیا(۱۳۸۴). «پدافند غیرعامل و اصول و ملاحظات»، تهران، نشریه ش ۳.
- (۱۳۸۵). «پدافند غیرعامل»، تهران، نشریه ش ۱.
- ، «پدافند غیرعامل» (معماری و طراحی شهری در ایران)، تهران، نشریه ش ۴.
- معاونت پدافند غیرعامل(بی تا). «آشنایی با سنجنده‌ها و تأسیسات عمیق زیرزمینی حساس و راهبردی»، نشریه ش ۶، پدافند غیرعامل، تهران، قرارگاه خاتم‌الانبیا(ص).
- معاونت پدافند غیرعامل، آشنایی با اقدامات پدافند غیرعامل برخی از کشورها، نشریه ش ۸، پدافند غیرعامل، تهران، قرارگاه پدافند هوایی خاتم‌الانبیا(ص).
- موحدی‌نیا، جعفر(۱۳۸۳). دفاع غیر عامل، ستاد تدوین متون درسی دافوس.
- (۱۳۸۶). اصول و مبانی پدافند غیر عامل، تهران، پژوهشکده مهندسی دانشکاه صنعتی مالک اشتر.
- (بی تا). آیین‌نامه فریب، تهران، معاونت پدافند غیرعامل، قرارگاه پدافند هوایی خاتم‌الانبیا(ص).
- مؤسسه علمی- پژوهشی سردار شهید قنبری (۱۳۸۸). پدافند غیر عامل، لوح فشرده.
- نباتی، عزت‌الله(۱۳۸۹). پدافند غیر عامل با رویکر به حوزه تهدیدات، مرکز آموزش شهید سرلشکر صیاد شیرازی (ارتش جمهوری اسلامی ایران).
- (۱۳۸۶). پدافند غیر عامل، مرکز آموزش شهید سرلشکر صیاد شیرازی (ارتش جمهوری اسلامی ایران).
- (۱۳۸۹). پدافند غیر عامل(اصول و مبانی)، مرکز آموزش شهید سرلشکر صیاد شیرازی (ارتش جمهوری اسلامی ایران).

- Ahrens, J. (1999). *Governance and the implementation of technology policy in less developed countries*. UNU/INTECH, Maastricht.
- Ali Ahmadi, A., Fathian, M., & Soltani, F. (2006). A reference model for ICT development in Iran's Universities. *Journal of knowledge management*, 19(73), 57-88. (in Persian).
- Bagheri Nezhad, J. (2008). University-industry relationship system for technology development in Iran: Mechanisms and policy implications. *Journal of Science and Technology Policy*, 1(1), 1-14 (in Persian).
- Elmer, L. (2002). *Vietnam's ICT enabling environment: Policy, infrastructure and applications*. Vietnam: U.S. Agency for International Development Hanoi.
- Ghazinoori, S. (2006). Developing Iran's government strategies for strengthening the national system of innovation using SWOT analysis, *Science and Public Policy*, 33(7) (in Persian).
- Lee, C., Sung, T. (2005). Schumpeter's Legacy: A new perspective on the relationship between firm size and R&D. *Research Policy*, 34, 914-931.
- Meng, Q., & Li, M. (2002). New economy and ICT development in China. *Information Economics and Policy*, 14, 275-295.
- Lee, K., & Lim, C. (2001). Technological regimes, catching-up and leapfrogging: Findings from the Korean industries. *Research Policy*, 30(3), 459-483.
- Lee, K.W. (2006). Effectiveness of government's occupational skills development strategies for small- and medium-scale enterprises: A case study of Korea. *International Journal of Educational Development*, 26, 278-294.
- www.fa.wikipedia.org/wiki/