فصلنامه دانش امنیتی
سال اول/شماره یکم/ بهار ۱۳۹۶

تاریخ دریافت:۹۵/۱۱/۹
تاریخ پذیرش نهایی:۹۶/۲/۱۶

تبیین نقش حفاظت اطلاعات در ارتقای امنیت پروژه‌های پدافند غیرعامل سازمان های دفاعی

علیرضا تنهایی[۱]
علی قربان آقارضایی[۲]

چکیده

نیروهای مسلح از مؤلفه‌های قدرت کشورها محسوب می‌شوند که وظیفه حفظ امنیت ملی را در شرایط بحرانی، جنگ و ... بر عهده دارند. سازمان های دفاعی به دلیل اهمیت نقش و جایگاه‌شان در ساختار دفاعی کشور و برخورداری از اطلاعات مورد نیاز سرویس‌های اطلاعاتی و گروهک‌های ضد انقلاب، همواره در معرض تهدید امنیتی هستند؛ از این رو ضرورت دفاع غیرعامل در برابر تهدیدهای پیرامونی با استفاده از راهکارهای مختلف تدافعی و تهاجمی امری مهم جلوه می‌نماید.

این تحقیق با هدف «تبیین نقش حفاظت اطلاعات در ارتقای امنیت پروژه‌های پدافند غیرعامل نیروهای مسلح» تدوین شده است. سؤال اصلی پژوهش این است که حفاظت اطلاعات چه نقشی در ارتقای امنیت پروژه‌های پدافند غیرعامل نیروهای مسلح دارد؟ با استفاده از روش تحقیق توصیفی سعی کرده‌ایم توصیفی عینی، واقعی و منظم از اقدامات نظارتی وکنترلی‌حفاظت اطلاعات در ارتقای امنیت پروژه‌های پدافند غیرعامل ارائه دهیم. ابزار جمع‌آوری اطلاعات در این تحقیق مطالعات کتابخانه‌ای و پرسشنامه محقق‌ساخته بوده است. جامعه آماری این تحقیق شامل مسئولان و مدیران عملیات ساحفاها (۲۰ نفر)، کارکنان معاونت حفاظت و پیشگیری دارای سابقه خدمت در امور عملیاتی (۲۲ نفر) و سایر خبرگان و متخصصان در قسمت معاونت پدافند غیرعامل به تناسب سابقه و اشرافیت بر موضوع (۱۸ نفر) بوده که در مجموع ۶۰ نفر بوده‌اند. کل این جامعه به عنوان حجم نمونه بررسی و تجزیه و تحلیل آماری شده است. نتایج حاصل از تجزیه و تحلیل اطلاعات جمع‌آوری‌شده با استفاده از نرم‌افزار SPSS (آزمون خی‌دو) نشان می‌دهد که حفاظت از پروژه‌ها و برنامه‌های دارای طبقه‌بندی، آگاه‌سازی حفاظتی و حفاظت از شبکه‌های رایانه‌ای از مهم‌ترین اقدامات نظارتی و در عین حال ضد جاسوسی، ضد براندازی و ضد فریب از مهم‌ترین اقدامات کنترلی حفاظت اطلاعات در پروژه‌های پدافند غیرعامل نیروهای مسلح به شمار می‌آید.

واژگان کلیدی

پدافند غیرعامل، حفاظت اطلاعات، نظارت، کنترل، امنیت

---

۱ . دانشجوی دکتری مدیریت دانشگاه خوارزمی و عضو هیئت علمی دانشکده فارابی
۲ . کارشناس ارشد پدافند غیرعامل (گرایش امنیت ملی)

مقدمه

دفاع غیرعامل با مفهوم عام و کلی آن، یعنی حفظ ساخت و زیرساخت‌های اساسی در برابر تهاجم بدون درگیری مسلحانه و مستقیم، سابقه‌ای طولانی در تاریخ بشر دارد. مطالعه و بررسی تاریخی تلفات، لطمات، صدمات، ضایعات و خسارات ناشی از جنگ‌ها نشان‌دهنده این واقعیت است که با شناخت و رعایت اصول اقدامات و راهبردهای پدافند غیرعامل به عنوان مکمل اقدامات پدافندی می‌توان با صرف وقت و هزینه‌های کمتر ضمن پر هزینه کردن جنگ برای دشمن از بروز صدمات و خسارات هنگفت به مراکز سرنوشت‌ساز ممانعت کرد. بنابراین انجام اقدامات دفاع غیرعامل در جنگ‌های نامتقارن امروزی برای مقابله با تهدیدها و تهاجمات خصمانه و تقلیل خسارات ناشی از حملات هوایی، زمینی و دریایی دشمن، اقدامی بنیادین است که وسعت و گستره عمل آن تمامی زیرساخت‌ها، مراکز حیاتی و حساس نظامی، غیرنظامی، جمعیتی، صنعتی، ارتباطی، اطلاعاتی، فرماندهی و کنترل و... را دربرمی‌گیرد (مرادیان، ۱۳۸۹: ۳۷۲). مائوتسه تونگ درباره پدافند غیرعامل و اهمیت و ضرورت آن می‌گوید: «برای غلبه بر دشمن و کسب پیروزی باید همه تلاش خود را در مهر و موم کردن چشم‌ها و گوش‌های دشمن و کور و کر کردن او به کار ببندیم و فکر و مغز فرماندهانش را گیج و مغشوش کنیم» (مرادیان، ۱۳۸۹: ۳۸۵).

نیروهای مسلح که به عنوان یکی از منابع قدرت کشورها وظیفه حفظ امنیت ملی را در شرایط بحرانی، جنگ و... دارند، ادامه حیات‌شان از یک سو با تهدیدهای کشورهای حریف و هدف مواجه است و از سوی دیگر به دلیل اهمیت نقش و جایگاهی که در ساختار دفاعی کشور دارند و برخورداری از اطلاعات مورد نیاز سرویس‌های اطلاعاتی و گروهک‌های ضد انقلاب، همواره در معرض تهدید هستند. با این توصیف ضرورت دفاع غیرعامل در برابر تهدیدهای پیرامونی با استفاده از راهکارهای مختلف تدافعی و تهاجمی امری مهم جلوه می‌کند. دشمنان کشور همواره با استفاده از شیوه‌های مختلف و ابزارهای جنگ نرم درصدد ضربه زدن یا تضعیف ارکان نظام جمهوری اسلامی ایران هستند. یکی از بهترین و ارزان‌ترین روش‌های مقابله، دفاع یا پدافند غیرعامل است که با به کارگیری اصول و ملاحظات امنیتی آن می‌توان به حفاظت زیرساخت‌ها و کاهش آسیب‌پذیری، مدیریت صحنه بحران و افزایش پایداری کشور در مقابل انواع تهدیدها مبادرت کرد. در این راستا یکی از مهم‌ترین وظایف حفاظت

اطلاعات، نظارت و کنترل به منظور حفظ و صیانت کشور از طریق اماکن و تأسیسات، اسناد و مدارک، وسایل و تجهیزات و امنیت ارتباطات و حفاظت کارکنان است.

با توجه به موارد یادشده، چنانچه در تهیه و اجرایی کردن پروژه‌های پدافند غیرعاملِ نیروهای مسلح که در کشور اهمیت زیادی دارند، ملاحظات امنیتی در نظر گرفته نشود، باعث مخاطرات سوء امنیتی می‌شود و در عمل با صرف میلیاردها تومان هزینه مالی نتیجه‌ای عاید کشور نخواهد شد.

بیان مسئله

امروزه تهدیدهای منطقه‌ای و فرامنطقه‌ای ناشی از نوپایی، ناپایداری کشورها، ناهماهنگی و تداخل هدایت و منابع فرهنگی متوجه کشور است. موارد مذکور، مسئولان جمهوری اسلامی ایران و نیروهای مسلح را به این فکر واداشته است که برای دفاع و برقراری امنیت پایدار کشور، به خصوص مراکز حیاتی، حساس و کلیدی، رعایت اصول پدافند غیرعامل را در اولویت سیاست کاری خود قرار دهند.

دشمنان کشور همواره با استفاده از شیوه‌های مختلف و ابزارهای جنگ سخت و نرم درصدد ضربه زدن یا تضعیف ارکان نظام جمهوری اسلامی ایران هستند. یکی از بهترین و ارزان‌ترین روش‌های مقابله دفاع یا پدافند غیرعامل است که با به کارگیری اصول و ملاحظات امنیتی آن می‌توان به حفاظت زیرساخت‌ها و کاهش آسیب‌پذیری، مدیریت صحنه بحران و افزایش پایداری کشور در مقابل انواع تهدیدها مبادرت ورزید. بدین منظور یکی از مهم‌ترین وظایف حفاظت اطلاعات‌ها پیشگیری، نظارت و کنترل به منظور حفظ و صیانت کشور از طریق حفاظت اماکن و تأسیسات، اسناد و مدارک، وسایل و تجهیزات و امنیت ارتباطات و حفاظت کارکنان است.

سازمان پدافند غیرعامل با احداث و راه‌اندازی پروژه‌های پدافند غیرعامل سعی در ارتقای توان عملیاتی، افزایش بازدارندگی، کاهش آسیب‌پذیری و تداوم فعالیت‌های ضروری و ارتقای پایداری و تسهیل مدیریت بحران در مقابل تهدیدها و اقدامات نظامی دشمن دارد. در صورت رعایت نکردن ملاحظات امنیتی در طول فعالیت پروژه‌های مورد بحث، قبل، حین و بعد از انجام اقدامات پروژه‌ای ممکن است پیامد سوء امنیتی از قبیل سرقت اطلاعات، ایجاد خرابکاری، جمع‌آوری تلفنی، تقرب، نفوذ و... رخ دهد و ضربات جبران‌ناپذیری به نیروهای مسلح وارد آید.

به علت اهمیت فراوان افزایش امنیت در پروژه‌های پدافند غیرعامل برای رسیدن به اهداف مد نظر و از پیش تعیین‌شده، مهم‌ترین مسئله‌ای که محققان در پی دستیابی به آن هستند این است که «حفاظت اطلاعات در ارتقای امنیت پروژه‌های پدافند نیروهای مسلح چه نقشی دارد؟».

ضرورت و اهمیت تحقیق

جمهوری اسلامی ایران طی سالیان گذشته شاهد چهار جنگ مهم در حریم مرزهای خود بوده است (جنگ تحمیلی عراق علیه ایران، جنگ اول خلیج فارس، جنگ افغانستان و جنگ آخر آمریکا و انگلیس علیه عراق). وقوع مناقشات و جنگ‌هایی دیگر با اهداف ژئوپلیتیک و مهار و مقابله با انقلاب اسلامی جزء اهداف راهبردی استکبار جهانی است. تجارب حاصل از جنگ‌های گذشته به خصوص هشت سال دفاع مقدس، جنگ ۱۱ هفته‌ای ناتو علیه یوگسلاوی، جنگ اخیر آمریکا و انگلیس علیه عراق، جنگ ۳۳ روزه جنوب لبنان و فعالیت‌های جریان‌های تکفیری در عراق و سوریه مؤید این نظر است که نیروهای مهاجم برای در هم شکستن اراده ملت و توان نظامی، اقتصادی و سیاسی کشور مورد تهاجم با اتخاذ استراتژی انهدام مرکز ثقل توجه خود را صرف بمباران مراکز حیاتی و حساس می‌کنند.

سازمان پدافند غیرعامل با احداث و راه‌اندازی پروژه‌های پدافند غیرعامل سعی در ارتقای توان عملیاتی، افزایش بازدارندگی، کاهش آسیب‌پذیری و تداوم فعالیت‌های ضروری و ارتقای پایداری و تسهیل مدیریت بحران در مقابل تهدیدها و اقدامات نظامی دشمن دارد. همچنین تأکید فرماندهی معظم کل قوا(مدظله العالی) در راستای فراگیر شدن پدافند غیرعامل، ایجاب می‌کند ضریب امنیتی پروژه‌های پدافند غیرعامل در مقابل تهدیدهای احتمالی دشمن ارتقا یابد. بنابراین با توجه به موارد یادشده، چنانچه در تهیه و اجرایی کردن پروژه‌های پدافند غیرعامل در کشور ملاحظات امنیتی در نظر گرفته نشود، باعث مخاطرات امنیتی به شرح زیر خواهد شد. برای کاهش این مخاطرات، تبیین نقش حفاظت اطلاعات در ارتقای امنیت پروژه‌های پدافند غیرعامل نیروهای مسلح ضرورت می‌یابد:

ـ سرقت اطلاعات دارای طبقه‌بندی پروژه‌ها و انتشار غیرمجاز آن در فضای مجازی؛

ـ خرابکاری با انجام اقدامات فیزیکی و نرم‌افزاری برای ایجاد اختلال و توقف پروژه‌ها؛

ـ رعایت نکردن حیطه‌بندی و طبقه‌بندی موضوعات مربوط به پروژه‌ها؛
ـ دسترسی به اطلاعات پروژه‌ها از طریق جمع‌آوری تلفنی (رعایت نکردن حفاظت گفتار)؛
ـ تقرب سرویس‌های اطلاعاتی به مسئولان و کارکنان اجرایی پروژه‌های پدافند غیرعامل؛
ـ نفوذ عاملان سرویس‌های اطلاعاتی داخل مجموعه و دسترسی به اطلاعات پروژه‌های مد نظر؛
ـ رعایت نکردن پوشش‌های طبیعی لازم در راستای عادی‌سازی اجرای پروژه‌های پدافند غیرعامل؛
ـ پیشگیری از سرقت اطلاعات طبقه‌بندی‌شده پروژه‌ها و انتشار غیرمجاز آن در فضای مجازی؛
ـ افزایش حیطه‌بندی و طبقه‌بندی موضوعات مربوط به پروژه‌ها؛
ـ ممانعت از دسترسی به اطلاعات پروژه‌ها از طریق جمع‌آوری تلفنی (رعایت نکردن حفاظت گفتار)؛
ـ شناسایی عاملان سرویس‌های اطلاعاتی پس از ورود به مجموعه و جلوگیری از دسترسی آنها به اطلاعات پروژه‌های مد نظر؛
ـ ارتقای پوشش‌های طبیعی لازم در راستای عادی‌سازی اجرای پروژه‌های پدافند غیرعامل؛
ـ افزایش دانش کارکنان دارای دسترسی به اطلاعات پروژه‌ها برای مواجهه با مشکلات امنیتی و انعکاس موضوع به سامانه حفاظت اطلاعات.

پیشینه تحقیق

اگر چه استفاده از اصول پدافند غیرعامل به تناسب حیات بشر سابقه چندانی ندارد، اما عملاً در سه دهه گذشته جایگاه و نقش به‌سزایی در برنامه‌ها و راهبردهای دفاعی کشورها پیدا کرده است و به تناسب این گسترش، کشورهای متفاوت سعی کرده‌اند از این بستر برای پیشبرد امور خود استفاده کنند. با توجه به اهمیت و جایگاه پدافند غیرعامل در سطح کشور، به خصوص برای نیروهای نظامی، مقالات و کتاب‌های متعددی درباره اهمیت و جایگاه پدافند غیرعامل به نگارش درآمده است؛ با این حال به میزان نقش کلیدی پروژه‌های پدافند غیرعامل نیروهای مسلح و تأثیرات آن بر

امنیت ملی کشور و تقویت بنیه دفاعی آن و همچنین طبقه‌بندی زیاد این‌گونه پروژه‌ها کار تحقیقاتی و علمی مستقیمی انجام نگرفته است. محقق در پیشینه مطالعاتی این پژوهش به یک کار پژوهشی با عنوان آسیب‌ها و تهدیدهای امنیتی برون‌سپاری پروژه‌های تحقیقاتی به شرح زیر برخورد کرده است:

ـ جعفر معتمد در سال ۱۳۹۲ در پایان‌نامه کارشناسی ارشد خود با عنوان **آسیب‌ها و تهدیدات امنیتی برون‌سپاری پروژه‌های تحقیقاتی** پس از بیان مفهوم تهدیدها و آسیب‌های امنیتی برون‌سپاری پروژه‌های تحقیقاتی نهاجا در سه بعد تهدیدهای امنیتی، آسیب‌های امنیتی و مدیریت امنیتی، با در نظر گرفتن مؤلفه‌هایی همچون جاسوسی، خرابکاری صنعتی، نشت اطلاعاتی، سرقت اطلاعات، مشخص شدن نیازمندی‌ها، نظارت امنیتی و فرهنگ حفاظتی در نهایت به این نتیجه رسیده که پروژه‌های تحقیقاتی برون‌سپاری در صورت رعایت نکردن مقررات امنیتی ممکن است در آینده مشکلات سوء امنیتی ایجاد کنند.

هدف، سؤال و فرضیه پژوهش

هدف پژوهش تبیین نقش حفاظت اطلاعات در ارتقای امنیت پروژه‌های پدافند غیرعامل نیروهای مسلح است. برای رسیدن به این هدف، سؤال پژوهش این است که حفاظت اطلاعات در ارتقای امنیت پروژه‌های پدافند غیرعامل نیروهای مسلح چه نقشی دارد؟

در پاسخ به این سؤال، فرضیه پژوهش حاکی از آن است که حفاظت اطلاعات در ارتقای امنیت پروژه‌های پدافند غیرعامل نیروهای مسلح نقش «نظارتی و کنترلی» دارد.

مبانی و ادبیات نظری تحقیق

۱. پدافند غیرعامل

مجموعه اقدامات غیرمسلحانه‌ای که موجب افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقای پایداری ملی و تسهیل مدیریت بحران در مقابل تهدیدها و اقدامات نظامی دشمن می‌شود (اسکندری، ۱۳۸۹: ۱۵). پدافند جامع دو جزء دارد: ۱. پدافند عامل؛ ۲. پدافند غیرعامل.

دفاع یا پدافند عامل عبارت است از رویارویی و مقابله مستقیم با دشمن و به کارگیری جنگ‌افزارهای مناسب و موجود به منظور دفع حمله و خنثی کردن اقدامات آفندی دشمن.

پدافند غیرعامل یا دفاع غیرعامل نیز به مجموعه اقداماتی گفته می‌شود که مستلزم به کارگیری جنگ‌افزار نیست و با اجرای آن می‌توان از وارد شدن خسارات مالی به تجهیزات و تأسیسات حیاتی، حساس و مهم نظامی و غیرنظامی و تلفات انسانی جلوگیری کرد یا میزان این خسارات و تلفات را به حداقل ممکن کاهش داد (موحدی نیا، ۱۳۸۶: ۳). پدافند غیرعامل به معنای کاهش آسیب‌پذیری هنگام بحران، بدون استفاده از اقدامات نظامی و صرفاً با بهره‌گیری از فعالیت‌های غیرنظامی، فنی و مدیریتی است. اقدامات پدافند غیرعامل شامل پوشش، پراکندگی، تفرقه و جابه‌جایی، فریب، مکان‌یابی، اعلام خبر، قابلیت بقا، استحکامات، استتار، اختفا، ماکت فریبنده و سازه‌های امن است (خسروجردی، ۱۳۹۲: ۱۱۰). در پدافند غیرعامل تمام نهادها، نیروها، سازمان‌ها، صنایع و حتی مردم عادی می‌توانند نقش مؤثری ایفا کنند؛ در حالی که در پدافند عامل مانند سیستم‌های ضد هوایی و هواپیماهای رهگیر، تنها سازمان های دفاعی مسئولیت برعهده دارند.

کلمه پدافند به معنای دفاع است و در مقابل آفند به معنای هجوم و حمله می‌آید. منظور از پدافند غیرعامل مجموعه اقداماتی است که مستلزم به کارگیری جنگ افزار نیست و با اجرای آنها می‌توان از وارد شدن خسارات مالی به تجهیزات و تأسیسات حیاتی و حساس نظامی و تلفات انسانی جلوگیری کرد یا میزان آنها را به حداقل ممکن کاهش دهد (لطیفی، ۱۳۹۴: ۱۲۵).

در تعریف دیگر پدافند غیرعامل عبارت است از همه اصول و اقدامات احتیاطی غیر از استفاده از جنگ‌افزار و تسلیحات که با رعایت و بهره‌گیری از آنها، از وارد شدن خسارات مالی به تجهیزات، تأسیسات حیاتی و حساس نظامی و غیرنظامی و تلفات انسانی جلوگیری می‌شود یا میزان این خسارات و تلفات را به حداقل ممکن کاهش می‌یابد.

پدافند عامل و غیرعامل مکمل یکدیگرند. به علت نفوذپذیری احتمالی هر سد پدافند عامل، به کارگیری اقدامات و رعایت اصول پدافند غیرعامل در کنار پدافند عامل ضروری است. با تأمین پدافند غیرعامل متناسب با شرایط و ویژگی‌های نقاط حیاتی، حساس و مهم، مناطق اداری و مسکونی و... می‌توان با صرف هزینه‌های نسبتاً کم از وارد شدن خسارات سنگین به تأسیسات حیاتی و حساس، مراکز نظامی و صنعتی که ادامه حیات اقتصادی و ایستادگی در مقابل دشمن به وجود آنها بستگی

دارد، جلوگیری کرد و جان انسان‌هایی را که در معرض خطر هستند، نجات داد (خسروجردی، ۱۳۹۲: ۱۱۰).

دفاع غیرنظامی[1] نیز مجموعه اقدامات و فعالیت‌هایی است که برای حفظ جان و مال مردم و جلوگیری از تباهی ثروت ملی و عمومی هنگام بروز و استمرار سوانح و حوادث طبیعی (مانند سیل، زلزله، آتشفشان، آتش‌سوزی، طوفان و ...) و مصنوعی از قبیل تهدید سیاسی و نظامی (مانند محاصره اقتصادی، بمباران و جنگ) انجام می‌گیرد. تأکید اصلی دفاع غیرنظامی بر حفاظت از مردم غیرنظامی و انجام اقدامات اضطراری برای مرمت و احیای مجدد خدمات و تأسیسات حیاتی، تأمین وسایل زیست موقت برای افراد سانحه‌دیده و ایجاد امکان ادامه حیات و آماده‌سازی آنان برای باز زیستی است. در منابع خارجی، وظایف دفاع غیرنظامی شامل چهار عنوان به شرح زیر است:

۱. اقدامات پیشگیرانه و کاهش‌دهنده؛[2]

۲. آماده‌سازی و امدادرسانی؛[3]

۳. هشدار و اخطار؛[4]

۴. بازسازی مجدد (باز زیستی)[5] (خسروجردی، ۱۳۹۲: ۱۱۱).

حفاظت اطلاعات پدافند غیرعامل

بر اساس تعریف ارائه‌شده از پدافند غیرعامل که اشعار می‌دارد «پدافند غیرعامل مجموعه‌ای از اقدامات غیرمسلحانه است که باعث افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقای پایداری ملی و تسهیل مدیریت بحران در مقابل تهدیدها و اقدامات نظامی می‌شود»، می‌توان حفاظت اطلاعات در حوزه پدافند غیرعامل را این‌گونه تعریف کرد: «حفاظت اطلاعات پدافند غیرعامل عبارت از مجموعه اقداماتی است که باعث افزایش ضریب حفاظتی و محصور نگه داشتن کلیه اطلاعات طبقه‌بندی‌شده پدافند غیرعامل اعم از برنامه‌ها، طرح‌ها و سامانه‌های اطلاعاتی پدافند غیرعامل در برابر تهدیدها و دسترسی دشمن می‌شود» (شیخ‌حسنی، ۱۳۸۹: ۱۹).

1 . Civil Defence
2 . Mitigation
3 . Preparation
4 . Response
5 . Recovery

چشم‌انداز و راهبردهای حفاظت اطلاعات در حوزه دفاع غیرعامل

حفاظت اطلاعات از منظر دفاع غیرعامل از ویژگی‌هایی زیر برخوردار است:

ـ نظام حفاظتی کارامد و مطمئن؛
ـ سامانه ایمن، کارا و پویا متناسب با تهدیدهای روز؛
ـ افرادی متعهد، دلسوز و آشنا به تهدیدهای جدید؛
ـ تأمل مؤثر بر نهادهای مسئول؛
ـ اطمینان از عدم نشت اطلاعات دارای طبقه‌بندی؛
ـ نفوذناپذیری بسیار زیاد؛
ـ چشمانی تیزبین با درایت و نظاره‌گر (شیخ حسنی، ۱۳۸۹: ۲۰).

نقش حفاظت اطلاعات در پدافند غیرعامل

۱. نفوذ نکردن عناصر دشمن در بدنه حفاظت اطلاعات: باید از ورود افراد غیرمجاز داخلی و خارجی در تمامی بخش‌های این مقوله حیاتی جلوگیری کرد تا مانع افشای طرح‌ها و پروژه‌های مد نظر شد.

۲. داشتن پوشش امنیتی برای کارها؛

۳. رعایت اصل حیطه‌بندی حفاظتی: اطلاعات مربوط حیطه‌بندی شود و تنها در دسترس افراد مجاز قرار گیرد.

۴. رعایت حفاظت در اجرای پروژه‌های دفاعی؛

۵. رعایت حفاظت در اجرای عملیات فریب (جلالی، ۱۳۸۷: ۲۹).

نقش حفاظت اطلاعات در اصول پدافند غیرعامل

ـ شناسایی سامانه‌های سنجنده دشمن از نظر توانایی و ضعف‌ها؛
ـ شناسایی طیف‌های مختلف سنجنده‌ها؛
ـ شناسایی مدل‌های استتار در برابر سنجنده‌ها؛
ـ کنترل و مراقبت درز اطلاعاتی سامانه‌ها از هر نظر؛
ـ شناسایی و تجزیه و تحلیل تهدید و سناریوی عمومی کشور؛
ـ تهیه سناریوی تهدیدها در هر حوزه؛
ـ ناتوان‌سازی سامانه اطلاعاتی دشمن در کسب اطلاعات جاسوسی و میدانی؛
ـ استفاده از سامانه‌های منحرف‌کننده فنی برای گمراه کردن دشمن؛

ـ ایجاد سامانه ضد اطلاعات برای کنترل اطلاعات خودی؛
ـ کور کردن زمینه‌های جذب و به کارگیری جاسوس؛
ـ ارسال اطلاعات گمراه‌کننده به منظور ایجاد تشکیک در اطلاعات دریافت‌شده؛
ـ بررسی کامل عوارض جغرافیایی به منظور استفاده برای اختفا؛
ـ اجرای عملیات فریب معماری در سایت‌ها؛
ـ اجرای عملیات فریب در پروژه‌ها؛
ـ ایجاد و تولید اهداف کاذب و مکرر برای دشمن؛
ـ استفاده از طرح فریب مردمی؛
ـ ایجاد تردید و باور غلط در دشمن؛
ـ رعایت اصل فریب در تمام اقدامات خودی؛
ـ حفاظت و حراست از تمام اسناد و مدارک، نقشه‌ها و ... و مراکز طبقه‌بندی‌شده؛
ـ ایجاد اطمینان از نشت نکردن اطلاعات سامانه‌های حیاتی و مهم؛
ـ ایجاد امنیت در ابعاد مختلف و حفظ اطلاعات خودی؛
ـ افزایش دانش افراد و ایجاد انگیزه برای کارکنان مرتبط در حفاظت از اطلاعات طبقه‌بندی‌شده؛
ـ بازتعریف عناوین و مصادیق جدید اطلاعاتی که مورد توجه و استفاده دشمن قرار می‌گیرد.
ـ به‌روزسازی سامانه‌های حفاظت و مراقبت اطلاعات متناسب با پیشرفت فناوری‌های جاسوسی و کسب اطلاعات؛
ـ انجام پژوهش‌های علمی و تخصصی در حوزه‌های امنیت و مراقبت اطلاعات؛
ـ ایجاد زیرساخت های حقوقی، قانونی، اجرایی و آموزشی برای کنترل و مراقبت بیشتر اطلاعات و برخورد جدی با افراد خاطی (جلالی، ۱۳۸۷: ۳۲).

اقدامات حفاظت اطلاعاتی در حوزه پدافند غیرعامل

اقدامات حفاظت اطلاعاتی در حوزه پدافند غیرعامل طیفی وسیع از اعمال عامل (آفندی) و غیرعامل (پدافندی) را شامل می‌شود که هدف‌شان حراست در مقابل تهدیدهای ضد اطلاعاتی است.

ـ **اقدامات عامل (آفندی)**: اقداماتی است که برای خنثی‌سازی تلاش‌های اطلاعاتی چند بعدی و چندجانبه (همه تکنیک‌هایی را که برای جمع‌آوری اطلاعات کاربرد دارند،

همچون جمع‌آوری انسانی، جمع‌آوری علایم و جمع‌آوری تصویری را شامل می‌شود) و اقدامات دشمن برای خرابکاری، براندازی و تروریسم صورت می‌گیرد. اقدامات عامل ضد اطلاعات، شامل ضد جاسوسی، ضد خرابکاری، ضد براندازی، ضد تروریسم، ضد شناسایی، مخفی داشتن و عملیات فریب می‌شود، اما به همین موارد محدود نمی‌شود. نوع اقدامات پیچیده ضد اطلاعاتی نظیر عملیات‌های ضد جاسوسی، عملیات‌های ضد تروریسم، بازجویی و مراقبت و عملیات‌های منبع دفاعی، تنها از طریق کارکنان ضد اطلاعاتی و سایر سازمان‌های تخصصی انجام می‌گیرد که تحت امر نیروی مشترک یا فرمانده سازمان هستند.

ـ اقدامات غیرعامل (پدافندی): اقداماتی است که هدف‌شان مخفی داشتن و ممانعت دشمن از دسترسی به اطلاعات، حمایت از کارکنان در مقابل براندازی و تروریسم، و حراست از ادوات و بناها در مقابل خرابکاری است. اقداماتی مانند حفظ امنیت مطالب طبقه‌بندی‌شده، امنیت کارکنان، امنیت فیزیکی، آموزش امنیتی، امنیت ارتباطات، امنیت اطلاعات خام، امنیت تشریفات الکترومغناطیسی، سانسور، استتار، اختفا و انضباط امنیتی از موضوعات اصلی ضد اطلاعات منفعلانه است (جمعی از مؤلفان، ۱۳۸۶: ۱۱).

اقدامات نظارتی حفاظت اطلاعات در پدافند غیرعامل

از آنجا که تهدیدهای دشمن متنوع و گسترده است، اقدامات حفاظت اطلاعاتی نیروهای خودی باید متنوع و گسترده و متناسب با نوع تهدید دشمن باشد. اهم اقدامات حفاظت اطلاعاتی در پدافند غیرعامل شامل اقدامات نظارتی و اقدامات کنترلی می‌شود (گودرزی، ۱۳۸۸: ۴) که اقدامات نظارتی به شرح زیر هستند:

-حفاظت در گفتار و تبلیغات (اخبار و اطلاعات)

به رازداری در کلام، گفتار و رفتار، حفاظت کلام گفته می‌شود. دشمن با شنود و جاسوسی تلفنی و... اقدام به جمع‌آوری اطلاعات می‌کند؛ بنابراین از مهم‌ترین وظایف کارشناسان و مسئولان، امانت‌داری و حفاظت اسرار و جلوگیری از نشر آن نزد دوستان و آشنایان است. واژه حفاظت کلام یا حفاظت گفتار در سازمان‌های اطلاعاتی برای اصطلاح رازداری متداول شده است؛ با این حال این واژه دقیقاً نمی‌تواند مترادف رازداری باشد زیرا حفظ گفتار به معنی حفظ اسرار نیست.

حفاظت گفتاری در موقعیت‌هایی که فرد در مظان دروغ‌گویی، غیبت کردن، تهمت زدن، سخن لغو گفتن و ده‌ها مورد دیگر قرار می‌گیرد، نیز معنا پیدا می‌کند. کسی

که از زبان و گفتارش در برابر غیبت یا فحش مراقبت می‌کند در واقع از کلام خود محافظت کرده است. اگر حفاظت گفتار و نیز رازداری را به عنوان اخلاق و صفت فاضله تلقی کنیم، می‌توانیم حفاظت کلام را مترادف به حساب آوریم که می‌تواند اوصاف فاضله را در مجموعه خود نظیر راست‌گویی، رازداری و غیبت نکردن دربرگیرد. با این نگاه، یکی از مصادیق حفاظت کلام رازداری خواهد بود. بدین ترتیب حفاظت کلام اعم از رازداری است و رابطه منطقی آن از نوع عموم و خصوص مطلق است؛ یعنی رازداری می‌تواند حفاظت کلام باشد. اگر رازداری و حفاظت گفتار را به عنوان یک تکنیک تأمینی در نظر بگیریم، در این صورت رابطه‌ای که در سطوح فوق بدان اشاره شد، عکس می‌شود؛ یعنی رازداری اعم از حفاظت کلام تلقی می‌شود، زیرا حوزهٔ عمل حفاظت کلام فقط در محدوده زبان و دهان است؛ ولی حوزه عمل رازداری علاوه بر زبان و دهان ناظر به ارکان و رفتار نیز می‌شود.

برخی اوقات نوع لباس پوشیدن، نوع نگاه کردن، حالات برخورد انسان با اشخاص و نیز نوع رفتار که هیچ ارتباطی به گفتار ندارد، عمل رازداری تلقی می‌شود. در خصوص رازداری حفاظت گفتار می‌توان گفت:

ـ بعضی از مصادیق حفاظت کلام، رازداری است و برخی (راست‌گویی و ناسزا گفتن) رازداری نیست.

ـ بعضی از مصادیق رازداری، حفاظت کلام است (نظیر توریه گفتاری، سمت و خاموش) و برخی مصادیق رازداری، حفاظت کلام نیست (نظیر لباس کردی پوشیدن مأموری که در منطقه کردستان عراق نفوذ کرده است) (شیخ‌حسنی، ۱۳۸۹: ۲۱).

حفاظت از اطلاعات شبکه‌های رایانه‌ای

امروزه با افزایش آمار کاربران اینترنت در کشور و آشنایی آنها با نرم‌افزارهای نفوذ به شبکه‌های کامپیوتری و همچنین با رشد میزان اطلاعات موجود روی سرورهای سازمان و پروژه‌های مربوط به پدافند غیرعامل نیاز به نظارت بر امنیت شبکه‌های رایانه‌ای اهمیت زیادی پیدا کرده است. ناآشنایی بسیاری از کاربران و کارکنان سازمان‌ها به نفوذگران کمک می‌کند به راحتی وارد یک شبکه کامپیوتری شوند و از داخل آن به اطلاعات محرمانه دست پیدا کنند یا به اعمال خرابکارانه بپردازند. هر چه رشد اینترنت و اطلاعات روی آن بیشتر می‌شود، نیاز به اهمیت دادن به امنیت شبکه افزایش پیدا می‌کند. توجه به امنیت شبکه، بیمه کردن سخت‌افزارها و نرم‌افزارها در مقابل خرابکاران است (شیخ حسنی، ۱۳۸۹: ۲۲).

وقتی بحث امنیت شبکه در پدافند غیرعامل پیش می‌آید، مباحث زیادی را می‌توان طرح کرد که هر کدام می‌تواند جالب، پرمحتوا و قابل درک باشد؛ اما وقتی صحبت از کار عملی می‌شود، قضیه پیچیده می‌شود. ترکیب علم و عمل، به تجربه نیاز دارد و نهایت هدف یک علم هم به کار آمدن آن است.

وقتی وارد موضوع امنیت شبکه در سامانه‌های مرتبط به پدافند غیرعامل شوید، ممکن است این سؤال را مطرح کنید که «از کجا شروع کنیم؟ اول کجا را ایمن کنیم؟ چه استراتژی را پیش بگیریم؟ و کجا کار را تمام کنیم؟». انبوهی از این قبیل سؤال‌ها فکر شما را مشغول می‌کند و کم کم حس می‌کنید تجربه کافی ندارید و این مسئله طبیعی است.

همیشه در امنیت شبکه موضوع لایه‌های دفاعی، موضوع داغی است و نظرهای مختلفی در این باره مطرح است. برای امنیت شبکه مطلوب باید پنج مرحله را پشت سر بگذاریم تا کارمان تمام شود. این مراحل پنج‌گانه عبارت‌اند از: بازرسی، حفاظت، ردیابی، واکنش و بازتاب (شیخ حسنی، ۱۳۸۹: ۲۷).

مهم‌ترین مزیت و رسالت شبکه‌ها، اشتراک منابع سخت‌افزاری و نرم‌افزاری است. کنترل، دستیابی و نحوه استفاده از منابع به اشتراک گذاشته‌شده از مهم‌ترین اهداف یک سامانه امنیتی در شبکه است. با گسترش شبکه‌ها نگرش به امنیت اطلاعات و سایر منابع به اشتراک گذاشته‌شده وارد مرحله جدیدی شده است. در این راستا ضروری است هر سازمان برای حفاظت از اطلاعات ارزشمند پای‌بند استراتژی خاص خود باشد و بر اساس آن سامانه امنیتی را اجرا و پیاده کند. ایجاد نکردن سامانه امنیتی مناسب ممکن است پیامدهای منفی و دور از انتظاری داشته باشد. سامانه‌های اطلاعاتی و شبکه‌ها معمولاً از چهار ناحیه آسیب می‌بینند:

۱. دسترسی غیرمجاز به اطلاعات: خواه این اطلاعات دارای طبقه‌بندی یا فاقد آن باشد، نشر آنها ممکن است اعتبار دفاعی کشور را خدشه‌دار کند.

۲. تغییر اطلاعات به صورت مخفیانه: این کار ممکن است اعتماد کارکنان را به سامانه فرماندهی و کنترل به شدت کاهش دهد و گاهی فرماندهی یا واحد در حال عملیات را گمراه و به مقصد کاذبی هدایت کند.

۳. هویت کاذب: آسیب‌پذیری عمومی سایر شبکه‌های اطلاعاتی ورود به آنها با هویت تقلبی است. فرد خاطی می‌تواند برای مثال اطلاعات موقعیت جغرافیایی را به دلخواه تغییر دهد. البته گاهی ممکن است هدفش از این کار شکستن روحیه کارکنان

باشد. برای مثال اگر شایع شود که یک فرد غیرمجاز به پرونده شخصی افراد دست یافته است (مانند حساب بانکی)، صدمه روانی آن کمتر از صدمه‌های نظامی نخواهد بود.

۴. اخلال در دسترسی کارکنان: چهارمین روش متعارف آسیب رساندن به شبکه‌ها اخلال در دسترسی به آنهاست. اگر براثر اخلال دشمن دسترسی به اطلاعات هواشناسی مختل شود، طبیعتاً برنامه‌ریزی یک رزمایش یا عملیات واقعی هم به تأخیر خواهد افتاد. همچنین اگر دسترسی به سامانه GPS با مشکل مواجه شود، واحد خودی نسبت به موقعیت و محل استقرار دشمن بی‌اطلاع یا گمراه خواهد شد (رضایی، ۱۳۸۶: ۷۰).

حفاظت از رایانه‌ها و اطلاعات پشتیبان

باید توجه کرد که با اتصال رایانه‌ها به اینترنت این وسیله می‌تواند به عنوان سریع‌ترین و سهل‌ترین روش جمع‌آوری اطلاعات برای جاسوسی مورد استفاده قرار گیرد؛ بنابراین باید از هرگونه اتصال به شبکه‌های اینترنتی از طریق سامانه و شبکه‌های رایانه‌ای اداری و دارای اطلاعات طبقه‌بندی‌شده اجتناب کرد و در عین حال به منظور جلوگیری از هرگونه بهره‌برداری غیر مجاز از هرگونه دستگاه‌های الکترونیکی و رایانه‌ها، قبل از تحویل گرفتن آنها از فروشندگان یا تعمیرکاران تمهیدات لازم را پیش‌بینی کرد (رضایی، ۱۳۸۶: ۲۲).

حفاظت از اسناد و مدارک

ساختار جامعه کنونی و رابطه کشورها موجب برخورد منافع آنها و در نتیجه، درگیری بین سرویس‌های اطلاعاتی شده است. دشمن از طریق عوامل جاسوسی، نفوذی و ستون پنجم با استفاده از خطاهای حفاظتی و نقصان سیستم حفاظت اسناد می‌تواند به بسیاری از اطلاعات طبقه‌بندی‌شده دست یابد.

اطلاعات همواره پشتوانه مؤثر و نیرومندی در پیروزی جنگ‌هاست و در همه تصمیم‌گیری‌ها نقش به‌سزایی ایفا کرده است. نظر به اهمیت حیاتی اطلاعات در عصر کنونی، کشورها می‌کوشند اسرار خود را با تدابیر و اقدامات حفاظتی از دسترسی عوامل غیرمجاز و سایر کشورها مصون نگه دارند. یکی از مهم‌ترین اقدامات به منظور ایجاد مانع در مقابل تلاش‌های اطلاعاتی و فعالیت‌های پنهانی حریف، حفاظت اسناد و مدارک طبقه‌بندی‌شده است که از جمله اقدامات غیرعامل محسوب می‌شود. اقداماتی نظیر تعیین طبقه‌بندی، تقلیل طبقه‌بندی، بسته‌بندی و ارسال اسناد طبقه‌بندی‌شده،

توزیع و انهدام آن از مباحث اصلی در حوزه اسناد و مدارک طبقه‌بندی‌شده است (رضایی، ۱۳۸۶: ۱۲۳).

در واقع هدف از حفاظت از اسناد و مدارک، محافظت از اطلاعاتی است که در برخی اجسام و اعیان فیزیکی ثبت شده است. اسناد طبقه‌بندی‌شده به هر نوع وسیله و شیء حاوی اطلاعات اطلاق می‌شود که صرف نظر از شکل ظاهری و مشخصات آن باید در برابر افشای غیرمجاز حفاظت شود. متداول‌ترین اشکال طبقه‌بندی‌شده عبارت‌اند از: نامه‌ها و گزارش‌ها، نقشه‌ها، نمودارها، فیلم، نوار ضبط صوت، تصاویر نسخه‌های پیش‌نویس، نوار چاپگر، رول‌های فکس و هر گونه وسیله‌ای که اطلاعات روی آن ثبت و ضبط شده باشد (مانند سی‌دی، دیسکت، هارد، فلش و ...). مسئولیت تهیه و آماده‌سازی اسنادی مانند علامت‌گذاری، صفحه‌بندی، بازبینی، طبقه‌بندی و شمارش اسناد به عهده تولیدکنندگان اصلی سند است.

حفاظت اسناد و مدارک را از اقسام حفاظت فیزیکی به معنای عام دانسته‌اند؛ چنان که در تعریف آن گفته‌اند حفاظت اسناد کلیه اقداماتی است که مانع می‌شود که اسناد محرمانه (طبقه‌بندی‌شده) در دسترس اشخاص غیرمجاز قرار گیرد. در واقع هدف از حفاظت از اسناد محافظت از اطلاعاتی است که در برخی اجسام و اعیان فیزیکی (مانند کاغذ، نوار کاست و ...) ثبت شده است. در واقع محافظت از اجسام یادشده بدان علت اهمیت دارد که از طریق آن می‌توان تضمینی برای محافظت از اطلاعات مندرج در آنها به دست آورد.

اگر مراحل یک سند را شامل تولید، گردش، بایگانی و امحا بدانیم، حفاظت اسناد عبارت از تدابیری خواهد بود که دسترسی غیرمجاز به اطلاعات طبقه‌بندی‌شده در هر یک از مراحل چهارگانه فوق را مانع شود. با پذیرش تفاوت‌های موجود در مراحل چهارگانه اسناد، مدیریت حفاظت اسناد هر یک از این مراحل متفاوت خواهد بود (شیخ حسنی، ۱۳۸۹: ۳۳).

حفاظت پیرامونی یا فیزیکی (اماکن و تأسیسات)

مجموعه اقدامات عملی برای حفظ تأسیسات، مؤسسه‌ها و یگان‌ها با اعمال مقررات و قوانین برای مقابله با هرگونه خطر احتمالی طبیعی و مصنوعی در سازمان‌های کشوری و لشکری را حفاظت پیرامونی گویند. منظور از حفاظت پیرامونی، حفظ اسرار سازمان‌های کشوری و لشکری از دستبرد عوامل نفوذی غیرمجاز و اغفال‌شده خودی و جلوگیری از انجام هر نوع فعالیت خرابکاری، جاسوسی، سرقت در محل مورد حفاظت است.

طراحی یک سامانه حفاظت پیرامونی مؤثر و کارامد باید جواب‌گوی خطرهای تهدیدکننده باشد. برای مفید بودن یک سامانه حفاظت پیرامونی باید از ابزارهایی استفاده کرد که در نوع خود کارایی زیادی دارند. چنانچه پیشنهادهای طرح حفاظتی به صورت کامل ارائه، اجرا و به کار گرفته شود، هر گونه اقدام و تعرض به تأسیسات در مراحل اولیه شناسایی و خنثی می‌شود (گودرزی، ۱۳۸۸: ۳۵).

امنیت ارتباطات (حفاظت مخابرات)

پیشرفت و توسعه صنعت الکترونیک در سال‌های اخیر بسیار چشم‌گیر و درخور توجه بوده است. انسان در زمینه ارتباطات در ابعاد گوناگون از تکنیک الکترونیک بهره‌برداری وسیعی کرده است؛ به طوری که می‌توان به جرئت اذعان کرد رکن اساسی حیات و دوام و بقای جوامع در عصر حاضر داشتن یک سامانه ارتباطی الکترونیکی مطمئن، سریع و قابل اطمینان است. امروزه از سامانه‌های ارتباطی و رایانه‌ای در سطح وسیعی در جهان استفاده می‌شود. بالطبع سازمان های دفاعی و سامانه‌های اطلاعاتی و حفاظت اطلاعاتی هر کشور نیز هر یک در حیطه وظایف خود، ناگزیر به استفاده از وسایل و تجهیزات ارتباطی الکترونیکی و رایانه‌ای هستند. از آنجا که بهره‌برداری از این سامانه‌ها دو سویه است و هم استفاده‌کننده بهره می‌برد و هم امکان بهره‌برداری دشمن متصور است، همواره ارتباطات سازمان های دفاعی از جمله ارتش با خطر جمع‌آوری اطلاعات از سوی دشمن روبه‌روست؛ بنابراین موفقیت در بهره‌برداری صحیح از سامانه‌های ارتباطی به اعمال تدابیر و تمهیدات لازم و همچنین فراگیری و درک عمیق کارکنان از موضوع امنیت ارتباطات و رایانه و رعایت دقیق اصول و مقررات مربوط بستگی دارد و دشمن را در جمع‌آوری اطلاعات ارتباطی الکترونیکی از نیروهای خودی با مشکل مواجه خواهد کرد.

عنصر امنیت در ارتباطات و اطلاعات یکی از فاکتورهای مهم، اساسی و حیاتی در یک سامانه ارتباطی الکترونیکی است و همواره تحت تأثیر عوامل سرعت، دقت و تحرک، بُرد و توسعه فناوری تجهیزات ارتباطی، الکترونیکی و اطلاعاتی است. برقراری امنیت ارتباطات نیاز به شناخت تهدیدها (داشتن اطلاعات از آخرین وضعیت امکانات جنگ الکترونیک و سایر آسیب‌رسانی‌های دشمن)، همگامی با تکنولوژی روز، وابسته نبودن به بیگانه به خصوص در بُعد نرم‌افزاری، بهره‌مندی از تکنیک، تاکتیک، پرسنل و تجهیزات مناسب و اِعمال مدیریت قوی دارد که براثر تجارب عملیاتی تکمیل می‌شود.

امنیت ارتباطات و اطلاعات بر اساس پاسخ‌گویی به موضوعات تهدید فراهم می‌شود و از مهم‌ترین و حیاتی‌ترین موضوعات در فناوری ارتباطات و اطلاعات است.

امنیت ارتباطات رادیویی مستلزم وجود همه محاسبات، ارزیابی‌ها، اقدامات تکنیکی، تاکتیکی، توسعه اقدامات و حفاظت از اطلاعات مربوط به آنهاست که به منظور حفاظت فرستنده‌ها، گیرنده‌ها و امکانات وابسته به آنها در برابر عملیات تهاجمی دشمن از جمله رهگیری و ردگیری، موقعیت‌یابی، ترافیک‌سنجی، ضبط و تجزیه و تحلیل سیگنال (شناسایی)، ایجاد اختلال (فریب، پارازیت و ...)، تخریب و انهدام و تهدیدهای ناشی از عوامل محیطی (درونی و بیرونی) طراحی و به خدمت گرفته شده است.

با پیشرفت فناوری اطلاعات و ارتباطات و اتکای بیشتر عملیات‌های نظامی به این فناوری آسیب‌پذیری‌های آن در مقابل جنگ‌های اطلاعاتی افزایش می‌یابد. از طرفی سامانه‌های نظامی به اجبار نیازمند برخورداری از تعامل و سازگاری در کل مجموعه هستند. این نظم و سازگاری فرصت‌های مناسبی برای دشمن این سامانه‌ها فراهم می‌سازد. حفاظت مخابرات به منظور حفظ اطلاعات مخابره‌شده و در راستای جلوگیری از سرقت، تخریب، جعل، افشا و استفاده افراد غیرمجاز مطرح می‌شود. امنیت ارتباطات مخابراتی به سه حوزه مختلف علامت (سیگنال)، پیغام یا داده و سیستم تقسیم می‌شود (رضایی، ۱۳۸۶: ۷۰).

پروژه‌های پدافند غیرعامل

طرح‌ها و پروژه‌های پدافند غیرعامل به اقداماتی گفته می‌شود که فرماندهان یگان‌ها به منظور پدافند در برابر تک هوایی دشمن در منطقه تحت فرماندهی خود تهیه و اجرا می‌کنند تا خسارات و تلفات وارده به تأسیسات، افراد و تجهیزات را به حداقل برسانند. حفظ اسرار نظامی و بهره‌گیری از اصول حفاظتی و امنیتی و طبیعی جلوه دادن فعالیت‌های در دست اقدام پروژه‌های پدافند غیرعامل با توجه به پوشش اتخاذشده همواره در موفقیت عملیات تأثیرگذار بوده است. از آنجا که بسیاری از طرح‌های پدافند غیرعامل که از طرح‌های مهم آجا محسوب می‌شود، به اجرا گذاشته شده است، باید ترتیبی اتخاذ کرد که با رعایت مقررات حفاظتی از دسترسی افراد غیرمجاز به پروژه‌های در دست احداث پدافند غیرعامل ممانعت کرد. باید با نظارت بر اجرای پروژه‌ها و ایجاد سیستم نظارتی و کنترلی مناسب بتوان از خطاهای حفاظتی کاست و

ضریب امنیتی پروژه‌ها را به منظور تعیین روش یکنواخت حفاظتی جهت انجام مراحل اجرای پروژه‌های مرتبط با پدافند غیرعامل افزایش داد. باید برای افزایش ضریب تأمین حفاظتی و به کارگیری اقدامات تأمینی برای حفاظت از کارکنان، تجهیزات و تأمین فیزیکی و انتظامی پروژه‌های پدافند غیرعامل و همچنین جلوگیری از نفوذ افراد خرابکار یا غیرمجاز به داخل محدوده پروژه اقدام کرد و تدابیر لازم را برای جلوگیری از آسیب رسیدن به تأسیسات و تجهیزات، اسناد و مدارک و... اندیشید.

با توجه به اینکه اسناد و اطلاعات و تجهیزات پروژه‌های پدافند غیرعامل به دلیل حساسیت و اهمیت آن به عنوان اسرار نظامی تلقی می‌شود و هر گونه دسترسی به این اطلاعات و پروژه‌ها تحت ضوابط و مقرارت خاصی انجام می‌گیرد، نیاز است به فراخور درجه و اهمیت و حساسیت آن اقدامات حفاظتی لازم انجام گیرد تا از هر گونه موارد سوء امنیتی جلوگیری شود.

هدف از اجرایی کردن ملاحظات و دستورالعمل‌های حفاظتی در پروژه‌های پدافند غیرعامل به شرح زیر است:

ـ تأمین حفاظت پروژه‌ها و تجهیزات با بهره‌گیری از موانع حفاظتی، سیستم‌های شناسایی و اقدامات نظارتی و کنترلی؛

ـ جلوگیری از هرگونه آسیب‌رسانی به پروژه و افشای محل پروژه و مختصات فنی و نوع کاربری آن در آینده توسط گروه‌های خرابکار و عوامل جاسوسی؛

ـ حفاظت از اطلاعات طرح‌های پدافند غیرعامل و پروژه‌های مرتبط با موضوع و مخفی نگه داشتن اهداف اصلی طرح‌های پدافند غیرعامل با استفاده از پوشش‌های مختلف برای منحرف کردن عوامل دشمن؛

ـ طبیعی جلوه دادن فعالیت‌ها و اقدامات در دست اجرا با توجه به پوشش اتخاذشده؛

ـ جلوگیری از افشای محل و مختصات پروژه‌ها؛

ـ هماهنگی‌های لازم پشتیبانی تأمین حفاظتی با سایر ارگان‌ها و سازمان‌ها در خصوص تأمین حفاظتی محل در صورت لزوم؛

ـ رعایت حفاظت گفتار در همه گفت‌وگوهای حضوری و تلفنی درباره پروژه‌ها؛

ـ توجیه مستمر همه کارکنانی که به نحوی با طرح‌های پدافند غیرعامل در ارتباط هستند به اقدام بایسته معمول و ضرورت یادآوری حساسیت موضوع به آنها و ابلاغ توصیه‌های لازم حفاظتی و امنیتی.

ـ اجرای دقیق مقررات انتظامی مربوط به کنترل تردد در محدوده محل‌های استقرار پروژه‌ها؛

ـ جلوگیری از تردد افراد غیرمجاز به محدوده پروژه‌های در دست اقدام؛

ـ انجام اقدام لازم درباره دستگیرشدگانی که به طور غیرقانونی وارد محوطه پروژه شده‌اند با هماهنگی سامانه اطلاعاتی.

ـ انجام مکاتبات در ارتباط با پروژه‌ها با کد و علایم قراردادی از قبل تعیین‌شده؛

ـ ممنوعیت استفاده از تلفن همراه در امور مرتبط با پروژه‌های پدافند غیرعامل.

تجزیه و تحلیل فرضیه پژوهش

فرضیه پژوهش: حفاظت اطلاعات در ارتقای امنیت پروژه‌های پدافند غیرعامل نقش «نظارتی و کنترلی» دارد.

جدول ۱ـ مشخصه‌های آماری فرضیه پژوهش

N	Valid	۷۸۰
	Missing	۰
Mean		۴.۱۱۱۰
Std. Error of Mean		.۰۲۸۷۷
Median		۴.۰۰۰۰
Mode		۴.۰۰
Std. Deviation		.۹۶۹۶۰
Variance		.۹۴۰۱۳
Skewness		-.۸۶۹
Std. Error of Skewness		.۰۷۳
Kurtosis		.۵۷۳
Std. Error of Kurtosis		.۱۴۵
Range		۴.۰۰
Minimum		۱.۰۰
Maximum		۵.۰۰
Sum		۳۲۰۷.۰۰

جدول ۲ـ توزیع فراوانی فرض پژوهش

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	۱.۰۰	۹	۱.۱۵	۱.۱۵	۱.۱۵
	۲.۰۰	۲۹	۳.۷۲	۳.۷۲	۴.۸۷
	۳.۰۰	۱۲۹	۱۶.۵۴	۱۶.۵۴	۲۱.۴۱
	۴.۰۰	۳۱۲	۴۰.۰۰	۴۰.۰۰	۶۱.۴۱
	۵.۰۰	۳۰۱	۳۸.۵۹	۳۸.۵۹	۱۰۰.۰
	Total	۷۸۰	۱۰۰.۰	۱۰۰.۰	

داده‌های جدول شاخصه‌های آماری حاکی از آن است که میانگین، میانه و انحراف استاندارد توزیع به ترتیب ۴/۱۱، ۴ و ۰/۹۶ است. توزیع از کجی منفی برخوردار بوده و در نقطه اوج خود نسبت به توزیع نرمال دارای برآمدگی است. داده‌های جدول توزیع فراوانی نیز نشان می‌دهد که ۷۸/۵۹ درصد پاسخ‌دهنده‌ها در حد زیاد و خیلی زیاد نسبت به محتوای فرضیه پژوهش نظر مساعدی دارند.

جدول ۳ و ۴ـ خی دوی فرضیه پژوهش

	Observed N	Expected N	Residual	
۱.۰۰	۹	۱۵۶	-۱۴۷	
۲.۰۰	۲۹	۱۵۶	-۱۲۷	
۳.۰۰	۱۲۹	۱۵۶	-۲۷	
۴.۰۰	۳۱۲	۱۵۶	۱۵۸	
۵.۰۰	۳۰۱	۱۵۶	۱۴۷	
Total	۷۸۰			

	VAR00001
Chi-Square(a)	620.373
df	4
Asymp. Sig.	.000

داده‌های جدول‌های آزمون خی‌دو حاکی از آن است که ارزش خی‌دوی مشاهده‌شده (۶۲۰/۳۷) در درجه آزادی ۴ معنی‌دار است. در نتیجه تفاوت بین فراوانی‌های مشاهده‌شده تأیید می‌شود و این به معنای تأیید فرضیه پژوهش است.

نتیجه‌گیری

سازمان های دفاعی به عنوان یکی از پارامترهای قدرت کشورها وظیفه حفظ امنیت ملی را در شرایط بحرانی، جنگ و ... برعهده دارند. نیروهای مسلح به علت اهمیت نقش و جایگاهی که در ساختار دفاعی کشور دارند و برخورداری از اطلاعات مورد نیاز سرویس‌های اطلاعاتی و گروهک‌های ضد انقلاب، همواره در معرض تهدید هستند. با این توصیف ضرورت دفاع غیرعامل در برابر تهدیدهای پیرامونی با استفاده از راهکارهای مختلف تدافعی و تهاجمی امری مهم جلوه می‌نماید که تلاش شده است در این پژوهش با عنوان اقدامات نظارتی و کنترلی مورد توجه و بررسی قرار گیرد.

به یقین یکی از عوامل اصلی و اثرگذار در جنگ‌های امروزی، بهره‌گیری از پدافند غیرعامل است و در این راستا حفاظت اطلاعات می‌تواند با شناخت بهتر دشمن (نقاط ضعف، قوت، تهدیدها و فرصت‌ها) و توان نیروهای خودی، به موفقیت پدافند غیرعامل در تقابل با دشمن کمک شایانی کند. هدف این پژوهش «تبیین نقش حفاظت اطلاعات در ارتقای امنیت پروژه‌های پدافند» است. محقق سعی کرده است با تبیین اقدامات نظارتی و کنترلی حفاظت اطلاعات در ارتقای امنیت پروژه‌های پدافند غیرعامل نیروهای مسلح بتواند این نقش را ترسیم کند. محقق بعد از تجزیه و تحلیل اطلاعات جمع‌آوری‌شده به این نتیجه رسیده‌اند:

- حفاظت از طرح‌ها و برنامه‌های دارای طبقه‌بندی
- آگاه‌سازی حفاظتی
- حفاظت از شبکه‌های رایانه‌ای
- حفاظت گفتار و تبلیغات
- حفاظت از اسناد و مدارک
- امنیت ارتباطات (حفاظت مخابرات)
- حفاظت از رایانه‌ها و اطلاعات پشتیبان
- حفاظت تجهیزات عمده و استراتژیک
- حفاظت کارکنان
- حفاظت پیرامونی یا فیزیکی (اماکن و تأسیسات)

پیشنهادهای تحقیق

با توجه به مطالب و رویکردهای یادشده در این پژوهش، حفاظت اطلاعات باید در دفاع غیرعامل متناسب با دنیای دانش امروزی همگام باشد و با توجه به رسالتی که بر دوش دارد، اقدامات زیر را در حد توان اجرایی کند:

۱. استفاده از پتانسیل سامانه فرماندهی در ارتباط با ارتقای فرهنگ خودپایی حفاظتی و امنیتی در سطوح مختلف اجرایی؛

۲. رعایت اصول اولیه حفاظتی از سوی فرماندهان و مقامات بازدیدکننده از پروژه‌ها؛

۳. تعامل با سازمان پدافند غیرعامل کشور به منظور همسوسازی، کسب و بهره‌برداری از اسناد بالادستی در حوزه دفاع غیرعامل؛

۴. جلوگیری از به‌کارگیری اتباع بیگانه توسط پیمانکاران طرف قرارداد با پروژه‌های پدافند غیرعامل در امورات سازه‌ای.

منابع فارسی

ـ اسکندری، حمید (۱۳۸۹)، **دانستنی‌های پدافند غیرعامل (ویژه مدیران و کارشناسان)**، تهران: نشر بوستان حمید.

ـ بنت، مایکل و ادوارد والتز (۱۳۹۳)، **فریب و ضد فریب در امنیت ملی**، تهران: دانشکده اطلاعات، مؤسسه چاپ و انتشار دانشکده اطلاعات.

ـ پوریان، محمدتقی و احمد صفری نژاد (۱۳۹۱)، **حفاظت اطلاعات و پدافند غیرعامل**، چ ۱، تهران: نشر دانشکده فارابی.

ـ جلالی، غلامرضا (۱۳۸۷)، «تشریح مبانی و اصول پدافند غیرعامل»، **مجموعه مقالات همایش نقش حفاظت اطلاعات در پدافند غیرعامل**، تهران: نشر دانشکده امام هادی(ع).

ـ جمعی از مؤلفان (۱۳۸۶)، **مبانی ضداطلاعات**، چ ۱، تهران: نشر دانشکده امام محمدباقر(ع).

ـ حبیبی، نیک‌بخش (۱۳۹۲) **ارتش جمهوری اسلامی ایران، نیروی هوایی**، تهران: مرکز انتشارات راهبردی نهاجا .

ـ خسروجردی، علی (۱۳۹۲)، **چگونگی امکان کاهش خطر تهدیدات هوافضایی دشمن فرامنطقه‌ای علیه مراکز عملیات منطقه‌ای**، تهران: دانشگاه مالک اشتر.

ـ رضایی، بابک (۱۳۸۶)، **مبانی حفاظت اطلاعات ویژه دافوس**، چ ۱، تهران: نشر دانشکده فارابی.

ـ شیخ حسنی، محمود (۱۳۸۹)، جزوه آموزشی «حفاظت اطلاعات در پدافند غیرعامل»، تهران: نشر دانشکده فارابی.

ـ گودرزی، عباس (۱۳۸۸)، **کلیات اقدامات غیرعامل**، چ ۱، تهران: نشر دانشکده فارابی.
ـ معتمد، جعفر (۱۳۹۲)، **آسیب‌ها و تهدیدات امنیتی برون‌سپاری پروژه‌های تحقیقاتی نهاجا**، تهران: نشر دانشکده فارابی.
ـ موحدی، جعفر (۱۳۸۶)، **اصول و مبانی پدافند غیرعامل**، چ ۱، تهران: انتشارات دانشگاه صنعتی مالک اشتر.
ـ موحدی‌نیا، جعفر (۱۳۸۷)، «استراتژی دشمن در انتخاب هدف و انهدام مراکز ثقل»، **مجموعه مقالات همایش نقش حفاظت اطلاعات در پدافند غیرعامل**، تهران: نشر دانشکده امام هادی(ع).
ـ نباتی، عزت‌اله (۱۳۹۰)، **مبانی و اصول پدافند غیرعامل در امنیت ملی**، چ ۱، تهران: نشر دانشکده فارابی.