جایگاه ستاد پدافند غیر عامل در کاهش تهدیدات امنیتی و سایبری (مطالعه موردی: شهر کرمان)

سمیرا حسن زاده[۱]، محدثه حامدی[۲]

تاریخ دریافت: ۱۴۰۰/۰۱/۲۵ تاریخ پذیرش: ۱۴۰۰/۰۳/۲۷

چکیده

هدف و زمینه: تمایل روز افزون به استفاده از فناوری‌های پیشرفته از جمله رایانه و اینترنت شرایط وبستر مساعدی برای ظهور جرایم سایبری بوجود آورده است. از آنجا که این جرایم در فضای مجازی انجام می‌گیرد و مانند سایر جرایم ملموس نیستند مراجع قضایی و انتظامی برای پیشگیری از این جرایم با چالش‌های نوینی مواجه هستند. در چنین فضایی که از آن به عنوان فضای مجازی یاد می‌گردد. افراد و مجموعه‌هایی در آن خارج از حوزه دولت‌ها نقش آفرینی می‌کنند.

روش: این تحقیق از نظر هدف کاربردی است. مقاله حاضر از نوع توصیفی –تحلیلی می‌باشد. همچنین از آنجا که در این تحقیق با استفاده از روش اسنادی به تحلیل محتوای اسناد، مقالات، پایان نامه‌ها، کتاب‌های مختلف مرتبط با موضوع تحقیق پرداخته شده است. اطلاعات وداده‌های مورد نیاز برای انجام تحقیق بر حسب نوع آن‌ها از منابع مختلفی گردآوری شده است.

نتایج: کنترل سنتی دولت‌ها بر حوزه‌های کارکردی همچون امنیت، ایجاد نظم سیاسی، مدیریت و ساماندهی و فعالیت‌های اقتصادی، اجتماعی و فرهنگی را با چالش‌های جدی مواجه ساخت‌هاند. جرائم اقتصادی در راس جرائم سایبری قرار دارد، کرمان جزء ۱۰ استان اول کشور در زمینه جرائم سایبری است. همچنین کرمان در زمینه کشف جرائم سایبری در رده بین چهار و پنج کشور قرار دارد. طی شش ماه نخست سال جاری ۹۵ درصد جرائم سایبری در کرمان کشف شده است. در این مقاله ضمن شناسایی تهدیدات و چالش‌های سایبری در استان کرمان به اقدامات ایران در مقابله با جنگ نرم و تهدیدات سایبری با توجه ظرفیت پدافندغیر عامل اشاره می‌نماید که می‌تواند مورد استفاده در نقاط گوناگون کشورمان از جمله استان کرمان بدلیل لرزه خیز بودن و نزدیکی به مرزهای استان‌های جنوب شرقی کشور ایران که به تبع آن می‌تواند سبب بحران‌های گوناگون شود قرا رگیرد.

واژگان کلیدی: سایبر، فضای سایبر، جرایم سایبری، جنگ سایبری، پدافند غیر عامل، کرمان

[۱]– دانش آموخته کارشناسی ارشد مدیریت بحران دانشگاه شهید باهنر کرمان، (نویسنده مسئول)، تلفن: ۰۹۱۱۹۲۴۱۸۲– samira_۱۳۶۷@yahoo.com

[۲]– دانش آموخته کارشناسی ارشد مدیریت بحران دانشگاه شهید باهنر کرمان، تلفن: ۰۹۳۵۰۷۵۳۸۱۱– mmoh.haooo@yahoo.com

مقدمه

تکنولوژی اطلاعات با سرعت شگفت انگیزی تمامی ارکان حیات بشری از جمله مقوله نظم و امنیت و آرامش عمومی را دستخوش تحولات و دگرگونی‌های اساسی قرار داده است. همزمان با ظهور رایانه و اینترنت و فرایندهای جهانی شدن در عصر حاضر فناوری اطلاعات و ارتباطات امکان ظهور جامعه شبکه‌ای را فراهم اورده است که تعاریف جدیدی از هویت‌ها و جوامع انسانی عرضه می‌کند و بافت اصلی آن را اطلاعات و نظام ارتباطات الکترونیک تشکیل می‌دهد. در نتیجه پیدایش این جامعه شبکه‌ای، مراودات اجتماعی از شکل سنتی خود به صورت جوامع مجازی معاشرت‌های دیجیتالی از طریق متون الکترونیک و سیستم‌های چند رسانه‌ای، تغییر ماهیت داده‌اند که این امر باعث پیدایش نوعی ناامنی اجتماعی و ظهور جرایم و بزهکاری نوین در فضای مجازی شده است (احمدوند، ۱۳۸۳: ۵)

با توسعه رسانه‌های الکترونیکی در کنار جرایم سنتی فرصت‌های جدیدی نیز برای بزهکاری فراهم شده است. اموری از قبیل حمله ویروس‌ها، ورود غیر مجاز به وب سایت‌ها و هک کردن آن‌ها، سرقت و سوء استفاده از داده‌ها در زمره‌ی رفتارهای بزهکارانه‌ای تلقی می‌گردد که قابلیت ارتکاب در محیط‌های خارج از رایانه را ندارند به همین ترتیب پیشرفت فناوری رایانه، شرایط و بسترهای مناسبی برای سرقت اطلاعات (وایلدینگ، ۱۳۷۹: ۲۹)، تکثیر نرم افزارهای غیر مجاز، سوء استفاده از بازار سهام، تجاوز به حقوق مالکیت معنوی و تهاجم فرهنگی را فراهم کرده است. (دزیانی ۱۳۸٤: ۱۹) با در نظر گرفتن آنچه که بیان شد در آغاز به تبیین ماهیت سایبر و فضای آن، ویژگی‌های محیط سایبرحمله‌ی سایبری و روش‌ها و ابزار آن، ابعاد مختلف جنگ سایبری، و ویروس

رایانه‌ای می‌پردازیم. در ادامه با طرح مباحث و اصول و کارکردهای ستاد پدافند غیر عامل به دنبال راهکارهای کاهش چالش‌ها و تهدیدات سایبری هستیم.

بیان مساله

پیوند و اتصال شبکه جهانی اینترنت به روشنی گویای این واقعیت که ویرانگری و آسیب رسانی می‌تواند در یک لحظه سرتاسر جهان را فراگیرد. سوء استفاده از فناوری‌های رایانه‌ای و اینترنتی می‌تواند امنیت ملی- آسایش عمومی و موجودیت یک جامعه را به مخاطره انداخته و تأثیرهای منفی بی شماری را بر زندگی افراد اجتماع تحمیل می‌کند (وایلدینگ، ۱۳۷۹: ۱۱)

با کمی دقت در این خصوص می‌توان به این نتیجه دست یافت که اغلب مرتکبان جرایم سایبری را جمعیت جوان تشکیل می‌دهند (ایکاو، ۱۳۸۳: ۵۵). این مجرمان هم از ظرفیت جنایی بالایی برخوردارند و هم استعداد خوبی برای انطباق اجتماعی از خود نشان می‌دهند (جعفری، ۱۳۸۵: ۷۰). در بیشتر جرایم سایبری خشونت و جود ندارد بلکه طمع، غرور ویا درگیر دیگر ضعف‌های شخصیتی قربانی است که در ارتکاب این جرایم نقش اصلی رابازی می‌کند (خداقلی، ۱۳۸۳: ٤١).

جرایم سایبری در محیطی غیر فیزیکی علیه فناوری اطلاعات ارتکاب می‌یابند. تعداد قابل توجهی از جرایم سنتی امروزه با پیشرفت فناوری اطلاعات و ارتباطات به شدت متحول شده ودر سطح وسیعی صورت می‌گیرند. جرم جاسوسی از جرایم سنتی است که در ارتکاب آن وسیله‌ای استفاده شده است. این جرم با هر وسیله‌ای انجام می‌گیرد و در قالب مقررات موجود قابل مجازات است (خداقلی، ۱۳۸۳: ۱۰۲).

از آنجا که در حال حاضر شبکه‌های ارتباط و پیوندی جهان شمول یافته‌اند جرایم این حوزه، اغلب دارای وصف بین‌المللی شده‌اند. به علاوه با پیدایش فناوری‌های جدید در

این حوزه از قبیل رایانه‌های لب تاپ- تلفن و مودم‌های سیار جرایم ارتکابی نیز این قابلیت را خواهند یافت که در هر زمان و مکان، با وصف امحای آثار صحنه ارتکاب جرم و تأثیر بالقوه‌ی آن بر تمامیت شبکه اتصال جهانی تحقق یابند. متأسفانه در حال حاضر اطلاعات دقیق، مشخص و قابل اطمینانی در خصوص میزان و تأثیر جرایم سایبری نه تنها در کشور، بلکه در سایر نقاط جهان نیز به چشم نمی‌خورد و شمار زیادی از آن‌ها نامکشوف محسوب می‌گردند و در حال حاضر این جرایم به عنوان یکی از دغدغه‌ای بزرگ هزاره سوم میلادی مطرح شده‌اند. مساله اخیر یکی از معضلاتی است که متصدیان تحقیق در مرحله کشف و تعقیب جرایم مزبور با آن مواجه شده‌اند. (خداقلی، ۱۳۸۳: ۳۵) این مطالعه با هدف شناسایی و معرفی راهکارهایی کارامد برای به حداقل رساندن چالشها و تهدیدات سایبرنتیکی می‌باشد. پدافند غیر عامل نیازی به حضور انسان ندارد و قادر است که در فقدان نیروهای نظامی و جنگ افزارها امنیت سکونت‌گاه‌های انسانی و تاسیسات حیاتی و مهم را افزایش داده و نیروی دفاعی را تقویت نماید. تاکید بر پدافند غیر عامل عبارت است از مجمو عه‌ای اقدامات تغییر مسلحانه‌ای که موجب افزایش بازدارندگی، کاهش آسیب پذیری، تداوم فعالیت‌های ضروری، ارتقای پایداری ملی در مقابل تهدیدات و اقدامات نظامی دشمن است.

تعریف عملیاتی واژه‌ها

چالش: چالش به وضعت و پدیده‌ای جدید و دشوار که مواجهه با آن تلاشی سخت و تعیین کننده را ایجاب می‌کند اطلاق می‌گردد. یکی از واژه‌هایی که به تازگی در ادبیات و مباحث اجتماعی در جامعه ماکاربرد فراوانی پیدا کرده است واژه چالش می‌باشد. کاربرد این واژه تا اواسط دهه ۱۳۷۰چندان رایج نبود.

سایبر: سایبر پیشوندی برای اسامی متعدد و متنوعی است که همگی براساس انتشار روز افزون رایانه پدید امده‌اند. ضمنا اغلب عناصر در گیر با اینترنت با این پیشوند در ارتباط می‌باشند.

فضای سایبر: مجمو عه‌ای از تمامی شبکه‌های ارتباطی رایانه‌ای است که از میان آن‌ها اینترنت بزرگ‌ترین شبکه محسوب می‌گردد (Good man, ۲۰۰۸: ۲٤). بنابراین فضای سایبری اعم است از اینترنت و دیگر سامانه‌های رایانه‌ای، ارتباطی و مخابراتی.

حمله‌ی سایبری: در معنای عام و کلی حمله به شبکه‌های رایانه ای- ارتباطی و مخابراتی با هدف تخریب و یا سرقت داده‌ها و اطلاعات معنا می‌گردد.

امنیت اطلاعاتی: امنیت اطلاعاتی عبارت است از فرایند شناسایی و تحلیل اطلاعاتی که برای عملیات نیروهای خودی حیاتی می‌باشد که شامل شناسایی اطلاعاتی است که سیستم‌های اطلاعاتی دشمن می‌توانند آن هارا مشاهده نمایند و و تعیین شاخص‌هایی که نشان می‌دهد سیستم‌های اطلاعاتی مهاجم چگونه اطلاعات حیاتی را در زمان مناسب برای بهره برداری نیروهای دشمن استخراج کنند. گزینش و اجرای اقداماتی که اسیب پذیری اقدامات نیروهای خودی را دربرابر سوءاستفاده نیروهای د شمن از بین برده یا کاهش می‌دهند.

ویروس رایانه‌ای: مفهوم ویروس از تعاریف ارگانیگی ویروس بر گرفته شده است. ویرو س موجود ریز میکروبی است که توان به خدمت گرفتن موجودات زنده دیگر در جهت تکثیر –بقا- واعمال‌های خود را دارا می‌باشد و بدون استفاده از یک موجود زنده دیگر قادر به تکثیر و اعمال نقش نمی‌باشد. این نوع ویروس‌ها برنامه‌های کامپیوتری هستند که وقتی اجرا می‌گردند به دیگر برنامه‌های اجرایی که در یک سیستم ویادر یک شبکه

کامپیوتری هستند سرایت می‌کنند و خودشان را تکثیر کرده و پس از سرایت و اجرای آثار، خود را بر روی سیستم میزبان بروز می‌دهند.

هکر: هکر در دنیای کامپیوتر کسی است که با سیتم‌های رایانه‌ای اشنا باشد و می‌تواند با روش‌های خاصی بدون اجازه وارد آن‌ها گردد.

کرم رایانه ای: کرم‌ها برنامه‌های مخربی هستند که از اتصالات شبکه برای انتشار خود از یک سیستم به سیستم دیگر استفاده می‌کنند. کرم‌ها به برنامه میزبان نیازی ندارند وبا اتکا به خود می‌توانند منتشر شوند و به محض فعال شدن در یک سیستم کرم می‌توتند به مانند یک ویروس یا باکتری عمل کند.

دیواره آتش: دیواره‌های آتش، ابزارها و نرم افزارهایی هستند که می‌توان قواعدی را از جهت صحیح یا غیر صحیح بودن ارتباطات داخلی را کنترل گردیده از قبیل قطع ارتباط یا انحراف ان عمل نماید و حکم حصار و قلعه‌ای را دارد که به دور بخشی که امنیت آن باید تأمین شود، کشیده می‌شود.

جنگ الکترونیک: اقداماتی جهت کاهش ممانعت از بهره برداری دشمن از طیف امواج الکترو مغناطیس در عین حراست از بهره برداری نیروهای خودی از این طیف می‌باشد.

پدافند: پدافند در مفهوم کلی دفع، خنثی کردن و یا کاهش تأثیرات اقدامات آفندی دشمن و ممانعت از دستیابی به اهداف خودی است.

پدافند عامل: عبارت است از رویارویی و مقابله مستقیم با دشمن و به کار گیری جنگ افزارهای مناسب و موجود به منظور دفع حمله و خنثی کردن اقدامات آفندی دشمن می‌باشد. پدافند غیر عامل به مجمو عه اقداماتی اطلاق می‌گردد که مستلزم به کارگیری جنگ افزارها نبوده با اجرای آن می‌توان از وارد شدن خسارات مالی به تجهیزات حیاتی و

حساس نظامی و غیر نظامی و تلفات انسانی جلو گیری نموده و یا میزان خسارات و تلفات را به حداقل ممکن کاهش داد.

سایبر و فضای سایبر

واژه «فضای سایبر» را نخستین بار ویلیام گیبسون نویسنده داستان علمی تخیلی در کتاب نورومنسر در سال ۱۹۸٤ به کار برده است. فضای سایبر در معنا به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق کامپیوتر و مسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود. یک سیستم آنلاین نمونه‌ای از فضای سایبر است که کاربران آن می‌توانند از طریق ایمیل با یکدیگر ارتباط بر قرارکنند. بر خلاف فضای واقعی، در فضای سایبر نیاز به جابجایی‌های فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلیدها یاحرکات ماوس صورت می‌گیرد. فضای سایبر یا فضای مجازی در تعریف برخی نویسندگان عبارت است از: «مجموعه‌ای از ارتباطات درونی انسان‌ها از طریق رایانه و وسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی است» البته شاید بهتر باشد آن را چنین تعریف کنیم: «محیط الکترونیکی واقعی است که ارتباطات انسانی به شیوه‌ای سریع، فراتر از مرزهای جغرافیایی و با ابزار خاص، خود؛ در آن، زنده و مستقیم روی می‌دهد». ضمن اینکه فضای سایبر در واقع یک «محیط» است که ارتباطات در آن انجام می‌شود؛ نه صرف مجموعه‌ای از ارتباطات. از سوی دیگر، این ارتباطات گرچه ممکن است در همه حال بر خط نباشد، ولی زنده و واقعی و مستقیم است. از این رو، تأثیر و تأثر بالایی در این روابط رخ می‌دهد.

تاریخچه پدافند غیر عامل ایران در دوران قدیم و معاصر

یکی از راه‌های شناخت هر مساله مطالعه گذشته ان یعنی تاریخ است و شاید در میان دستاوردهای بشری هیچ پدیده‌ای به اندازه تاریخ، انسان را به مرزهای رشدوبلوغ نزدیک نکرده است. انسان‌های اولیه برای درامان ماندن از تهاجم حیوانات وحشی و دیگر دشمنان خود و همچنین برای کاستن از نگرانی‌های خود به غارها، بالای درختان و دیگر پناهگاه‌های طبیعی پناه بردند. وجود خندق در اطراف شهرها و ایجاد دروازه‌های مستحکم برای پیشگیری از حملات غافلگیرانه دشمن در تمام نقاط جهان امری رایج بود. در ایران، سرزمین گسترده ایران باستان به علت وضع جغرافیایی که میان دو جلگه آباد بین‌النهرین و پنجاب سند قرار گرفته بود، همچون پلی بوده که طوایف مهاجم به طرف شرق یا غرب، مجبور می‌شده‌اند از آن عبور کنند. وضعیت جغرافیایی و محیط ناامن، ایرانیان را وادار نمود تا به منظور در امان بودن از حمله متجاوزین، خانه‌های مسکونی خودرا به شکل دژ کوچکی بسازند، بنابراین به هر گوشه این سرزمین نگاه کنید، قلعه، برج و بارو، ارگ، کهندژ، دربند، خندق و دروازه از ناامنی محیط زندگی و توجه و تدبیر آگاهانه ایرانیان به ملاحظات دفاعی و امنیتی حمایت دارد. در دوران هخامنشی پیشرفت‌های زیادی در استحکامات دفاعی حاصل شد که مهم‌ترین آن‌ها عبارتند از: برج‌های نیمه استوانه‌ای به برج‌های مستطیلی شکل و ایجاد دیواره‌های کنگره دار به منظور تأمین امکانات بهتر برای دفاع. ساخت بناهای گروهی حصاردار در ایران با طرح‌ها و نقشه‌های گوناگون از سه هزار سال پیش ساخته شده است. قبل از انقلاب سازمانی با عنوان سازمان دفاع غیرنظامی وجود داشت که سه دسته مأموریت را برعهده این سازمان بود. مأموریت اول این سازمان، هدایت، کنترل و پشتیبانی از مردم حین حوادث و بلایای طبیعی است. مأموریت دوم کمک امداد و نجات در حوادث و دسته سوم کاهش آسیب‌پذیری‌های کشور در برابر

تهدیدات خارجی بوده است. بعد از پیروزی انقلاب اسلامی، این سازمان منحل شد و مأموریت‌های آن به بسیج واگذار گردید. بعد از انقلاب این سه دسته مأموریت بین گروه‌ها و سازمان‌های مختلف دست به دست شد. در مقطعی به سازمان مدیریت و برنامه‌ریزی واگذار شد و سپس به شورای عالی امنیت ملی محول شد. در مرحله بعد با فرمان مقام معظم رهبری این وظیفه به ارتش واگذار شد. در نهایت به قرارگاه پدافند هوایی کشور و سازمانی که وظیفه پوشش هوایی کشور را دارد، واگذارشد. عمده هدف کلانی که این سازمان دنبال می‌کند، کاهش آسیب‌پذیری زیر ساخت‌های کشور در برابر تهدیدات خارجی و افزایش پایداری ملی و در واقع تولید بازدارندگی برای کشور است.

ویژگی‌های فضای سایبر

– جهانی و فرامرزی بودن از ویژگی‌های منحصر به فردی که فضای سایبر را از دیگر رسانه‌ها ممتاز می‌سازد، جهانی بودن آن است. هر فردی در هر نقطه از جهان می‌تواند از طریق آن به آسانی، به جدیدترین اطلاعات دست یابد؛

– دستیابی آسان به آخرین اطلاعات؛

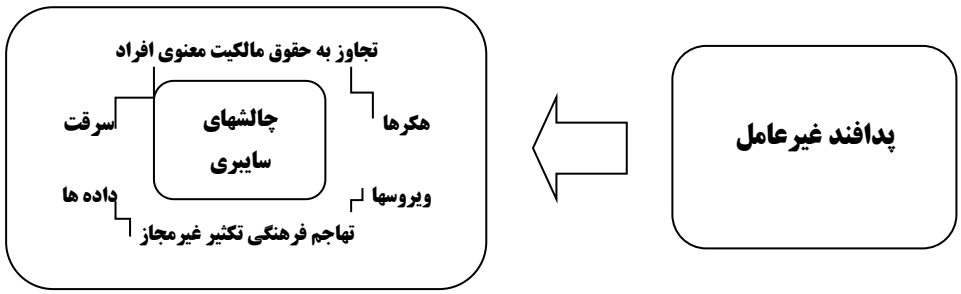
– جذابیت و تنوع رسانه‌ها از فیلم، عکس، متن و یا هر هنر دیگری برای جذاب کردن خویش به کار می‌گیرند و این ابزارها در فضای سایبر قابل دستیابی است؛ به ویژه آن گاه که هیچ نظارت و فیلتری توان محدود کردنش را نداشته باشد. از ویژگی‌های منحصر به فردی که در تنوع و جذابیت فضای سایبر تأثیر بسزایی دارد، مشتری محوری محض است؛

– آزادی اطلاعات و ارتباطات معنای واقعی آزادی اطلاعات، در فضای سایبر محقق شده است. از این رو، شما هر نوع اطلاعاتی را که بخواهید بدون محدویت‌های حاکم بر دیگر رسانه‌ها، در فضای سایبر قابل دسترسی است. آزادی ارتباطی نیز از ویژگی‌های دیگر فضای مجازی است که در دیگر وسایل ارتباطی تا این حد قابل دستیابی نیست.

چارچوب نظری

چارچوب نظری مدل مفهومی است از چگونگی نظریه پردازی در مورد روابط بین چند عامل که به عنوان مربوط به مساله تعریف شده‌اند. چارچوب نظری روابط متقابل بین متغیرهایی که فرض شده جزء لاینفک پویایی‌های وضعت مورد بررسی است مورد بحث قرار می‌دهد. تدوین چنین چارچوبی موضوعی مارا کمک می‌کند تا برای بهبود شناخت خود از پویایی‌های وضعیت، روابط خاصی را مورد بررسی و آزمون قرار می‌دهیم. (دانایی فرد و همکاران، ۱۳۸۳: ۱۲٤). با توجه به دید گاههای صاحب نظران، نظریات مختلفی را برای جنگ اطلاعاتی، جنگ سایبر و جنگ شبکه‌ای پیشنهاد داده‌اند. می توان جنگ اطلاعاتی رابه دو حوزه جنگ سایبر و جنگ شبکه‌ای تقیسم کرد. البته مرز دقیقی بین آن‌ها تعریف نشده و با یکدیگر تعامل دارند. جنگ سایبر توسط نظامیان انجام شده و اهداف نظامی را کاملاً مد نظر قرار می‌دهددر حالیکه در جنگ شبکه‌ای شاهد حضور عناصر غیر نظامی و حتی غیر دولتی مانند گروه‌های تروریستی می‌باشیم. در حوزه جنگ سایبر برخی از مفاهیم نام آشنا مانند: جنگ الکترونیک یا فریب نظامی جزءطبقه بندی بزرگ‌تر جنگ فرماندهی و کنترل قرار می‌گیرند. اما برخی از مفاهیم مانند آفند و پدافند شبکه‌ای رایانه‌ای در اینترنت یا اینترنت طبقه جداگانه‌ای را تشکیل می‌دهند که منعکس کننده رشد و گسترش محیط اطلاعاتی جهانی و محلی می‌باشد. جرایم سایبری عمتدا توسط نیروهای سازمان‌های یافته و طراحی نقشه قبلی ونیز توسط اشخاص رقیب یا اخراج شده از سازمان مزبور صورت می‌گیرد. بررسی‌های انجام شده در سده‌های اخیر مبین افزایش چشم گیر میزان بزهکاری و گرایش‌های مجرمانه در فضای مجازی است. براساس این بررسی‌ها تهدیدات ناشی از جرایم سایبری به شکل مهار ناپذیری رو به افزاش بودو زیان‌های مالی فراوانی نیز بر بخش‌های مختلف وارد آورده است (ایکاو، ۱۳۸۳: ۱۵). در عصر اطلاعات

جهان به شبکه‌ای تبدیل شده که بافت اصلی آن را اطلاعات و نظام ارتباطات الکترونیک تشکیل می‌دهد. در این شبکه به جزء گروهی از نخبگان، دیگران کنترل خود بر زندگی خویش و محیط پیرامون را از دست داده و یا به سرعت در حال از دست دادن هستند. جنگ مجازی واقعیتی است که مأموریت‌های شبیه سازی شده توسط جنگ افزارها و مهمات دقیق و ظریف، دوربین‌های از راه دور که بر روی شبکه قرار گرفته‌اند می‌باشند و از پایگاه‌های فضایی کنترل می‌شوند و از تماس فناوری‌های دیجیتالی دیگر در نقش تقویت کنترل عمل می‌کنند نشات می‌گیرد. پیشرفت فناوری رایانه‌ای، شرایط و بسترهای مناسبی برای سرقت اطلاعات فراهم کرده ست. (وایلدینگ، ۱۳۷۹: ۲۹) تکثیر نرم افزارهای غیر مجاز، سوءاستفاده از بازار سهام، تجاوز به حقوق مالکیت معنوی و مهم‌تر از همه تهاجم فرهنگی را فراهم کرده است (دزیانی، ۱۳۸٤: ۱۹). دلایل ارتکاب جرایم سایبری غالبا ادله‌ی الکترونیک است که با سرعت قابل ملاحظه‌ای امکان تغییر و از بین بردن آن‌ها و جود دارد (رضایی، ۱۳۸۵: ۱۳). بنابراین باسرعت عمل در شناسایی و جمع اوری این دلایل بسیار ضروری خواهد بود. (گاتن، ۱۳۸۳: ۳۱) انجام اقدامات دفاع غیر عامل در جنگ‌های امروزی در جهت مقابله با تهاجمات دشمن و تقلیل خسارات ناشی از ان، موضوع بنیادی است که وسعت و گستره ان تمام زیر ساخت‌های کلیدی، مراکز حیاتی حساس و مهم نظامی و غیر نظامی، نیروگاه‌ها، بنادر، فرودگاه‌ها، مجتمع‌های بزرگ صنعتی، قرارگاه‌ها و مراکز عمده فرماندهی نظامی و هدایت و تصمیم‌گیری‌های ارتباطی، پل‌های استراتژیک، صنایع نظامی، پایگاه‌های هوایی، سایت‌های موشکی، مراکز و ایستگاه‌های رادیویی و تلویزیونی، دارویی، مراکز جمعیتی و قرارگاه‌های تاکتیکی، مقرهای عمده اماری و پشتیبانی را در بر می‌گیرد (به نقل ازجانعلی زاده).



شکل شماره (۱): پدافند غیرعامل و چالش‌های سایبری

نوع و روش تحقیق

هر تحقیق علمی دارای هدفی است. تحقیقات علمی را می‌توتن براساس هدف به سه دسته تقسیم کرد: بنیادی- کاربردی- علمی (سرمد و همکاران، ۱۳۸٦) از انجا که انتخاب روش تحقیق بستگی به اهداف –ماهیت و موضوع پژوهش و نیز امکانات اجرایی ان دارد، بنابراین می‌توان گفت این تحقیق از نظر هدف کاربردی است. همچنین از آنجا که در این تحقیق از مطالعه مقالات- پایان نامه‌ها- کتاب‌های مختلف استفاده شده است. مقاله حاضر از نوع توصیفی –تحلیلی می‌باشد. اطلاعات و داده‌های مورد نیاز برای انجام تحقیق بر حسب نوع آن‌ها از منابع مختلفی گرداوری شده است. الگوو ماهیت تحقیق علمی در علوم انسانی و تربیتی از علوم مادی گرفته شده است و هدف آن حقیقت یابی است. محقق واقعیت (انچه که هست) را بر می‌گزیند و از طریق یک سلسله تلاش‌ها به نام تحقیق به دنبال کشف حقیقت (انچه که باید باشد) کاوش می‌کند. (نادری و سیف نراقی، ۱۳۷۳) برای اینکه بتوان نتایج درستی از یک پژوهش به دست اورد لازم است روش تحقیق مناسب استفاده شود تابا هزینه کمتر و سرعت و دقت بیشتر نتیجه مطلوب حاصل آید.

یافته‌های تحقیق

ابعاد مختلف جنگ سایبری

میادین جنگ مدرن به خاطر انقلاب اطلاعات در سطوح استراتژیک و تاکتیکی کاملاً دگرگون می‌شوند. افزایش روز افزون دامنه و عمق منطقه عملیاتی از یک سو و افزایش فوق العاده دقت تخریب حتی توسط سلاح‌های متعارف از سوی دیگر نشانگر اهمیت چشم گیر فناوری‌های مربوط با سی٤ای بوده و نشان‌گر ان است که برتری در این حوزه به تنهایی می‌توتند نوید بخش پیروزی در عملیات‌های نظامی باشد. برای جنگ سایبر فقط حضور فناوری پیشرفته الزامی نیست بلکه ابعاد روانی و سازمانی ان به اندازه ابعاد فنی اهمیت دارد. در تحت شرایط خاص شاید واقعا بتوان با استفاده از فناوری سطح پایین یک جنگ سایبر را آغاز کرد. اهمیت نسبی جنگ علیه نظام فرماندهی و کنترل و ارتباطات دشمن تقریبا همگام با ظهور جنگ مکانیزه مطرح شد. در طی جنگ جهانی دوم، دکترین حمله برق آسا که به نوعی ویژ گی‌های جنگ سایبر را در بر داشت در دو سطح تاکتیکی و استراتژیک هدف اصلی خودرا به صورت ایجاد اختلال در توانمندی ارتباطات و کنترل دشمن تعریف کرد.

مثال‌های از سایر حملات سایبری:

سازمان‌های امنیتی کشورهای دنیا به هیچ وجه مایل به برملا شدن حملات صورت گرفته به سایت‌ای کشور خود نیستند لذا نمی‌توان حملات صورت گرفته را فقط همین چند حمله ذکر کرد. در ذیل به اختصار نمونه‌هایی از این حملات بیان شده است: ۱) در سال ۱۹۹۷ببرهای تامیل باارسال پر تراکم نامه‌های الکترونیکی سیستم سفارتخانه‌های سریلانکارا را مختل نمودند. ۲) در سال ۱۹۹۸شبکه ارتش هند مورد حمله نفوذ گران اینترنتی قرار گرفت. ۳) نیروهای روسی که به کمک تصاویر ماهواره‌ای ونیز رهگیری

نامه‌های الکترونیکی، جوهر دو دایف، رهبر جنگجویان چچنی را تعقیب و در خانه‌ای در یک روستای دور افتاده ردیابی و با پرتاب دقیق موشک اورا از پای در آوردند. ٤) در جریان جنگ کوزوو، ویروس‌هایی از چین، روسیه و یو گسلاوی سابق منابع شبکه‌ای نیروهای هوایی امریکا را مورد حمله قرار دادند. در طول بحران کوزوو، شبکه‌های کامپیوتری ناتو توسط ویروس هامورد حمله واقع شده بودند. در این حملات از یک راهبرد مخصوص جهت تخریب سراسری شبکه‌های کامپیوتری ناتو استفاده شد که هیچ‌گاه ماهیت ان فاش نگردید.

ابزارهای جنگ سایبر

هر جنگی روش و ابزار جنگیدن می‌خواهد و جنگ سایبری هم از این امر مستثنی نیست. ویژگی که جنگ سایبری دارد و ان را از بقیه جنگ‌ها متمایز می‌کند این است که در بقیه جنگ‌ها یگان عمل کننده با استفاده از تسلیحات یگانی (سازمانی)طراحی روش جنگیدن می‌کند و با تاکتیک خاص خود را وارد صحنه نبرد می‌کند اما در جنگ‌های سایبری تاکتیک در تولید سلاح نهفته است ودر هر نوع سلاحی که توسط برنامه نویس کامپیوتر داده می‌شود (اعم از ویروس- کرم- اسب تراواو.. .) تاکتیک جنگ همان عملکرد سلاح است که به عنوان الگ. ریتم برنامه استفاده می‌گردد. نکته مهم این است که در جنگ سایبری فرد نفوذ کننده یا به اصطلاح فنی هکر می‌تونند حسب شرایط موجود و نیز ابزار در دسترس اعم از برنامه سرقت یا نفوذ اطلاعاتی خود را با سیستم و یا شبکه کامپیوتری هدف طرح‌ریزی و اجرا نماید.

حملات جنگ سایبری با تکیه بر بسترهای رایانه ای

۱- از کار انداختن کل سیستم رایانه ای، ۲- خاموش شدن پی در پی سیستم، ۳- پیدایش اشکالات تصادفی در اطلاعات، ٤- سرقت گسترده و سریع اطلاعات، ٥- سرقت از خدمات ارائه شده، ٦- استراق سمع غیر قانونی از سیستم و جمع آوری اطلاعات سری، ۷- وارد نمودن پیام‌های نادرست، ۸- دسترسی به داده‌ها و اطلاعات به منظور اخاذی کردن.

تهدیدات سایبری علیه ایران

تهدیدات سایبری در کشور که امروزه از مهم‌ترین نوع تهدیدها به شمار می‌رود به سه دسته فردی، اجتماعی و ملی تقسیم می‌گردد. تهدید سوم در برابر امنیت ملی است که به جنگ سایبری معروف است و نمونه ان علیه زیر ساخت‌های فنی و ارتباطی است که امنیت ملی کشور را به خطر می‌اندازد. حوزه اصلی پدافند غیر عامل نظارت بر دستگاه‌های اجرایی و شرکت‌های خصوصی است که دارای زیر ساخت‌های حیاتی هستند. مخاطرات به سه دسته خطربالا، متوسط و پایین دسته بندی می‌گرددودراین دسته بندی دستگاه‌هایی که خطرات وتهدیدات سایبری بیشتری دارد در اولویت برنامه‌های سازمان پدافند غیر عامل قرار دارند. دفاع غیر سایبری را به سه دسته اموزش و فرهنگ سازی، مدیریت ارتباطات و امنیت فناوری اطلاعات و تولید نرم افزارهای بومی تقسیم می‌کنیم. بخش نرم افزار خود شامل سیستم عامل و نرم افزارهای کاربردی، بانک اطلاعات و نرم افزارهای اجرایی است که باید کاملاًبومی تولید شود و دارای امنیت لازم باشد. تمام دستگاه‌های اجرایی باید سطح اول و دوم دفاع سایبری یعنی کنترل و مدیریت دسترسی‌ها را در سازمان خود اجرایی کنندبخش نرم افزار خود شامل سیستم عامل و نرم افزارهای

کاربردی، بانک اطلاعات و نرم افزارهای اجرایی است که باید کاملاً بومی تولید شود و دارای امنیت لازم باشد. تمام دستگاه‌های اجرایی باید سطح اول و دوم دفاع سایبری یعنی کنترل و مدیریت دسترسی‌ها را در سازمان خود اجرایی کنند. طی دو سال گذشته بیشترین تهدیدات سایبری در حوزه انرژی هسته‌ای، مدیریتی، بانکی و مالی، ارتباطات و مخابرات، صداو سیما و حوزه‌های خدماتی بوده است. جنگ سایبری و حملات سایبری، از جمله عرصه‌هایی است که به ویژه پس از جنگ سرد، از سوی سرویس‌های اطلاعاتی و واحدهای امنیتی به شدت پی‌گیری و بهره بهره برداری می‌شود.. این حملات فقط به سطح تهدید امنیتی محدود نمی‌گردند و در مبارزه کلی قدرت، این اعمال و روش‌ها به شکلی سریع تغییر می‌یابند. با توسعه دنیای دیجیتال، عرصه‌های ضعف هم عمیق می‌گردد و اهداف (دشمن) خیلی راحت‌تر و به شکلی مؤثرتر مورد تهدید قرار می‌گیرند.. قابل ذکر است که کرم رایانه‌ای موسوم به «استوکس نت» که مشخصاً از سوی یک دولت ساخته و توسعه یافته شده است، به تأسیسات هسته‌ای ایران در بوشهر و نطنز از اوایل سال جاری تا کنون حملاتی انجام گرفته است. ویروس مذکور فقط رایانه‌های شخصی را آلوده ساخته است و به مراکز هسته‌ای آسیب نرسانده است. نشانه‌هایی وجود دارد که طی ماه ژوئن حملاتی به مرکز تأسیسات اتمی نطنز انجام شده است. در خصوص نفوذ ویروس رایانه‌ای استاکس نت به دستگاه‌های کشور باید گفت که انتشار این ویروس ناشی از نبود انسجام و پیوستگی در این حوزه بوده و باعث میشد که هر دستگاهی در برابر تهدیدات تشخیصی داشته باشد. دشمن هنگامی که ویروسی را منتشر می‌کند به دنبال این است که بفهمد کارایی ویروس چه میزان بوده، چه نوع مقابله‌ای با ان صورت گرفته و این مقابله چقدر ان را خنثی کرده که این یک نوع جنگ است.. بنا به اظهارات رسمی، حدود ۶۰ هزار رایانه در ایران تحت تأثیر قرار گرفته‌اند. هدف کرم مذکور شبکه صنعتی است و به

نوعی کنترل کننده ویروس است. اگر سیستم صنعتی، مثلاً یک مرکز اتمی باشد، کرم مذکور می‌تواند سیستم کنترل را مختل سازد و یا آن را تحت اختیار قرار دهد.
متخصصین ذی ربط اظهار می‌کنند که چنین کرمی فقط از سوی یک کشور می‌تواند ایجاد و توسعه یابد که مستلزم فعالیت یک گروه حداقل ده نفره و به مدت شش ماه است. بسیاری از محافلی که آثار حمله مذکور را بررسی می‌کنند، بانی آن را اسرائیل می‌دانند.

چالش‌ها و تهدیدات سایبری و سایر جرایم در کرمان

فضای مجازی و اینترنت در کنار مزایایی که دارد می‌تواند خطرآفرین باشد چرا که چنانچه افراد آگاهی کافی نداشته باشند می‌توانند قربانی افراد سودجو شوند. جرائم اقتصادی در راس جرائم سایبری قرار دارد، کرمان جزء ۱۰ استان اول کشور در زمینه جرائم سایبری است. همچنین کرمان در زمینه کشف جرائم سایبری در رده بین چهار و پنج کشور قرار دارد. طی شش ماه نخست سال جاری ۹۵ درصد جرائم سایبری کشف شده است. (خبرگزاری مهر: رئیس پلیس فتا استان کرمان، ۱۳۹۳)

مبارزه با سرقت و کاهش روند سرقت در جامعه، مبارزه با موادمخدر و قاچاق آن، طرح ارتقای امنیت اجتماعی با رویکرد تلفات ناشی از تصادفات و حوزه فعالیت و تقویت مرزهای کشور، از ٤ اولویت پلیس در برنامه ٤ ماهه سال جاری می‌باشد. با وجود اینکه ٦درصد در حوزه سرقتها کاهش وجود داشته، استان کرمان در کشف سرقت‌ها ۳۸ درصد نسبت به چهار ماهه نخست سال گذشته افزایش داشته و در مجموع جرائم ۵درصد کاهش پیدا کرده است. ۲۰ درصد افزایش کشف جرائم تحقق پیدا کرده، در بعضی ازموضوعات مثل قتل یک کاهش ۲۰ درصدی نسبت به سال گذشته بود که در زمینه آدم ربایی نیز کاهش وجود داشته است. اقدامات امنیت در حوزه شرارت ٤١ درصد و نیز ۲۸درصد شرارت به عنف در استان کرمان نسبت به سال گذشته کاهش وجود داشته است. جرائم

خشن مثل جرائم به عنف ۲۸ درصد کاهش پیدا کرده که از جرائم مهم بوده است کـه کـل جرائم ۵ درصد نسبت به سال گذشته کاهش پیدا کرده است. در مبارزه با مواد مخـدر و در کشف محموله‌ها و باند ۷۰ درصد افزایش کشف داریم، در سال گذشته ۲۱تـن و در سـال جاری ۳۷/۵ تن کشف مواد مخدر دراستان کرمان وجود داشته است

در حوزه سلاح که به عنوان یک عامل ناامنی در جامعه به شمار می‌رود می‌توان گفـت: ۲٦ درصد افزایش کشف سلاح داریـم کـه درسـال جـاری بـیش از ٦ بانـد سـلاح دسـتگیر و متلاشی شده است.

بیش از ٦٥ درصد زندانیان را که جرمشان مرتبط با مـواد مخـدر اسـت تشـکیل می‌دهنـد، همچنین در زمینه معتادان پر خطر بیش از ٤ درصد کاهش جرم بوده که تعداد قابل توجهی از خرده فروشان دستگیر و بیش از ٤۰۰ نفر از آنان در همین مدت چهار ماهـه طبـق مـاده ١٦ تحویل شده‌اند.

در سال گذشته رتبه اول کاهش تلفات و کشته‌های جاده‌ای را در سطح کشور داشتیم ولـی متأسفانه در چهار ماهه نخست امسال ٤ درصد افزایش تلفات جاده‌ای را وجود داشـته کـه به سبب مسائل و مشکلاتی از قبیل دو بانده شدن جاده و نیز تصادفات قاچاقچیان بوده که تلاش می‌شود با همکاری سایر دستگاه‌ها این امر کاهش پیدا کند. شرط ادامه ایـن عمـل را همکاری، مشارکت و حمایت مردم می‌باشد. (گزارش بوتیا: فرمانده انتظامی اسـتان کرمـان، ۱۳۹۳)

اقدامات ایران در مقابله با جنگ نرم و تهدیدات سـایبری ایـران: (بـا توجـه ظرفیـت پدافندغیر عامل)

- ضرورت اعلام حالت اضطراری جنگ نرم به مردم؛
- شناخت نقاط ضربه پذیر فرهنگی و اهداف دشمن برای برنامه‌ریزی پدافند غیرعامل؛

- اطلاع رسانی بموقع برای ایجاد آمادگی دائمی در مردم؛
- جلب اعتماد عمومی به منابع اطلاع رسانی داخلی؛
- تدوین استراتژی امنیتی برای حفظ امنیت شبکه‌های رایانه‌ای در کشور؛
- ارائه آموزش‌های لازم به نیروهای مرتبط با شبکه‌ها برای حفظ امنیت شبکه؛
- به کارگیری نرم افزارها، ضد ویروس‌ها، دیواره‌های آتش در شبکه‌ها؛
- تعیین سطوح دسترسی به شبکه‌ها و سیستم‌های سایبری؛
- تشکیل کارگروه مشترکی بین ایران و سازمان انرژی اتمی؛
- همکاری با سازمان فناوری اطلاعات به خصوص مرکز (ماهر)؛
- ایجاد مراکز دفاع سایبری و تولید نرم افزارهای بومی با همکاری وزارت دفاع؛
- تشکیل کارگروه مقابله با کرم جاسوسی صنعت؛
- پاکسازی سیستم‌های الوده با سیتم‌های عملیاتی؛

نتیجه گیری

اتخاذ تدابیر امنیتی در زمینه فناوری‌های رایانه‌ای و سایبرنتیک مهم‌ترین اقدام برای پیشگیری از آسیب‌های احتمالی در برابر هر گونه اقدامات تروریسم سایبری می‌باشد. امنیت شبکه‌های سایبری و کلیه سیستم‌های رایانه‌ای در هر کشوری از اهمیت زیادی برخوردار است. تقویت زیرساخت‌های سایبری همچنین جایگاه ویژه‌ای در پدافند غیر عامل که به تازگی از سوی مراجع ذی صلاح در ایران ابلاغ شده است، دارد. اتخاذ تدابیر امنیتی در زمینه فناوری‌های رایانه‌ای و سایبرنتیک مهم‌ترین اقدام برای پیشگیری از آسیب‌های احتمالی در برابر هر گونه اقدامات تروریسم سایبری می‌باشد. میل و اشتیاق به استفاده از رایانه و اینترنت و بهره مند یاز مزایای ان اگرچه زمینه مشارکت جوامع مختلف در فناوری های پیشرفته را فراهم کرده است اما در عین حال شرایط و بستر مساعدی برای

ظهور جرایم سایبری به وجود اورده است. بررسی‌های انجام شده در سال‌های اخیر، مبین افزایش چشم گیر تهدیدات سایبری و گرایش‌های مجرمانه در فضای سایبری می‌باشد. بر اساس این بررسی‌ها تهدیدات ناشی از جرایم سایبری رو به افزایش بوده و زیان‌های مالی و امنیتی فراوان و مخربی را بر بخش‌های مختلف وارد اورده است. بیشترین تهدیدات سایبری علیه کشور ایران از جانب آمریکا و اسرائیل صورت می‌گیرد و اکثر این تهدیدات در حوزه انرژی هسته ای- مدیریتی- بانکی و مالی- ارتباطات و مخابرات- صدا و سیما و حوزه‌های خدماتی بوده است و در این زمینه نیازمند به ساختاری هستیم تا بتوانیم در برابر این تهدیدات چه در حوزه دفاعی و یا دستگاه‌های کشوری مقابله کنیم. پدافند غیر عامل به دنبال کاهش اسیپ پذیری زیر ساخت‌های حیاتی کشور در برابر تهدیدات خارجی و افزایش پایداری ملی و بعبارت دیگر تولید بازدارندگی می‌باشدو طی سال‌های اخیر با افزایش تهدیدات سایبری، به ویژه حمله ویروس استاکس نت به ایران این مقوله از اهمیت شایانی برخوردار گشته است. از جمله اقدامات پدافند غیر عامل در زمینه چالش‌ها و حملات سایبری می‌توان به موارد ذیل اشاره کرد:

تشکیل کارگروه مشترکی بین ایران و سازمان انرژی اتمی، همکاری با سازمان فناوری اطلاعات به خصوص مرکز (ماهر)، ایجاد مراکز دفاع سایبری و تولید نرم افزارهای بومی با همکاری وزارت دفاع، همکاری با پلیس فتا، تشکیل کارگروه مقابله با کرم جاسوسی صنعت و پاکسازی سیستم‌های الوده با سیتم‌های عملیاتی. نتیجتا این نکته قابل برداشت است که اقدامات ایران در مقابله با این تهدیداتشایان توجه می‌باشد. راه اندازی رشته کارشناسی دفاع سایبری در دانشگاههای دفاعی کشور از جمله اقدامات اساسی ایران در این زمینه می‌باشد و منجر می‌گردد تا مقابله با این تهدیدات را در کشور به صورت اکادمیک دنبال گردد. از انجایی که طیف و تبعات این حملات در عرصه جهانی به طور

چشم‌گیری درحال افزایش می‌باشد نیازمند تدابیر و ارائه راهکارها و اقدامات امنیتی بیشتری در این زمینه از جانب دولت می‌باشیم.

منابع

– ابراهیمی، عباس. (۱۳۸۸)؛ فناوری اطلاعاتی، مرکز تالیف کتاب‌های درسی سپاه، تهران.

– ابهری، مریم. (۱۳۸٦)؛ مدیریت بحران، دانشگاه صنعتی مالک اشتر؛ مجتمع آمایش و پدافند غیر عامل، تهران.

– ایکاو؛ دیوید چی. (۱۳۸۳)؛ راهکارهای پیشگیری و مقابله با جرایم رایانه ای؛ ترجمه اکبراسترکی، محمد صادق روز بهانی، تورج ریحانی و راحله الیاسی؛ تهران: معاونت پژوهش دانشگاه علوم انتظامی.

– جعفری، مجتبی. (۱۳۸۵)؛ بزهکاری رایانه‌ای در رویارویی با حقوق جزای فرانسه؛ نشریه حقوقی گواه، شماره ٦و۷، بهارو تابستان.

– خداقلی، زهرا. (۱۳۸۳)؛ جرایم کامپوتری؛ اب اول، تهران: آریان.

– دزیانی، محمد حسن. (۱۳۸٤)؛ اخبار جرایم سایبری؛ خبرنامه انفورماتیک، سال بیستم، شماره ۹۸، بهمن.

– رضایی، روح الله. (۱۳۵۸)؛ اعتبار اسناد الکترونیک با توجه به قوانین داخلی و بین‌المللی؛ نشریه حقوقی گواه، شماره ٦و۷ بهار و تابستان.

– سرمد، زهره. (۱۳۷۸)، مقدمه‌ای بر روش تحقیق در علوم انسانی؛ انتشارات نیل.

– موحدی نیا. (۱۳۸٤)؛ ج، نشریه ٤پدافند غیر عامل، معاونت پدافند غیر عامل قرار گاه پدافند هوایی خاتم النبیا.

– محمود زاده؛ امیر، نشریه علم افرین. (۱۳۸۷)؛ اشنایی با پدافند غیر عامل.

– مجید ی، داود . (۱۳۸٦)؛ مبانی استتار و اختفاء و پوشش؛ دانشگاه صنعتی مالک اشتر، مجمع آمایش و پدافند غیر عامل.