ماهنامه اداره کل پدافند غیر عامل
شماره ۴۰/ دی ماه ۱۳۹۸

ماهنامه دیجیتالی پدافند غیرعامل

مدیرکل پدافند غیر عامل استان:
هدف و رسالت پدافند غیرعامل، حفاظت از زیرساخت‌ها، صیانت از نیروی انسانی و مدیریت کشور است

رئیس دانشگاه سراسری تبریز:
دانشگاه تبریز برای پیش برد اهداف پدافند غیرعامل آماده هر نوع همکاری است

در این شماره می‌خوانید:

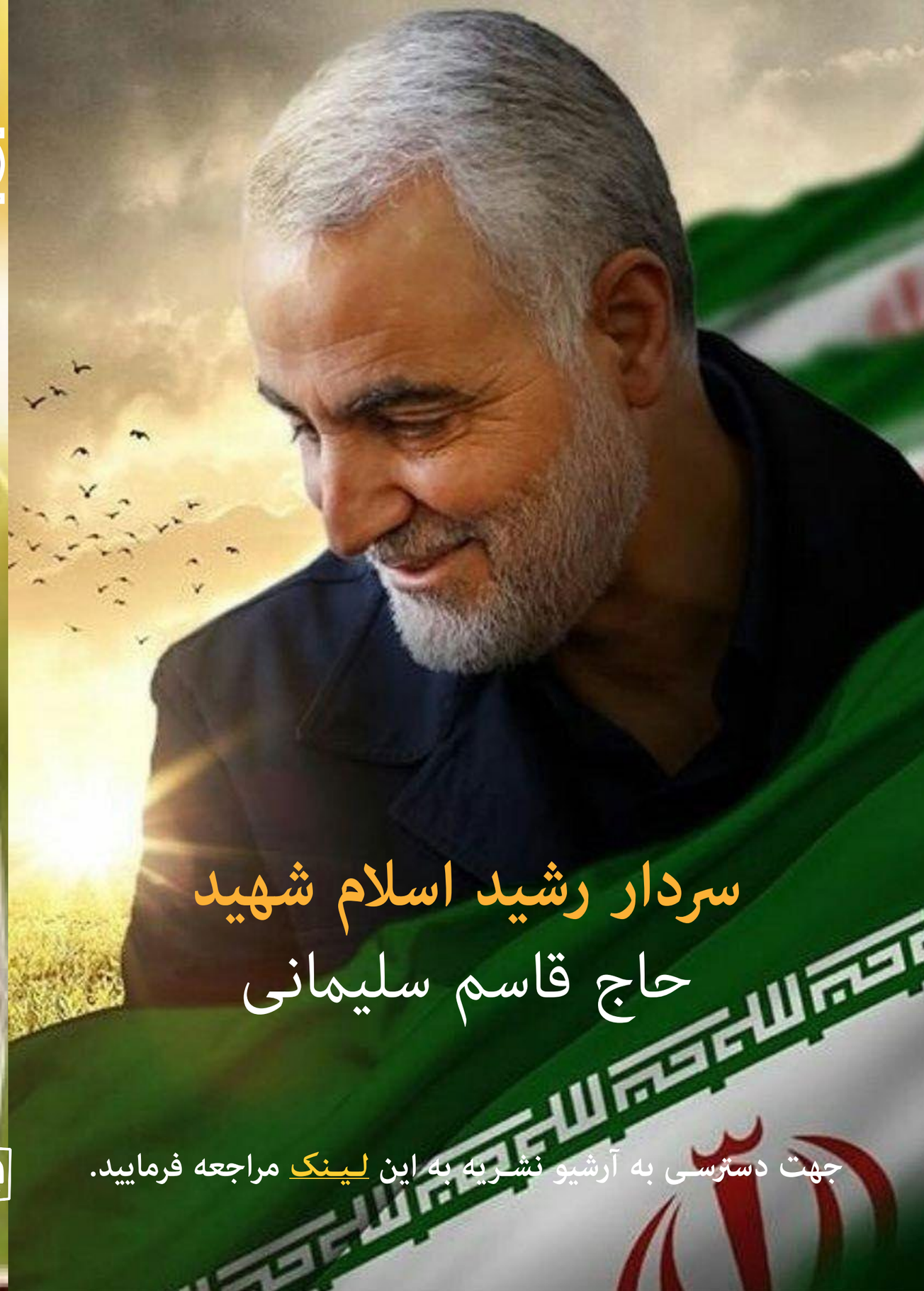
هشدار مایکروسافت در خصوص آسیب‌پذیری روز صفر در مرورگر IE

مهم‌ترین به‌روزرسانی‌های ماه جاری شرکت‌های تولید کننده سخت افزار و نرم افزار

سو، استفاده از RDP در حملات گسترده باج‌افزاری، کاوش رمزارز و سرقت اطلاعات

باج افزار

انتشار نسخه جدید بدافزار سارق گذرواژه Predator the Thief

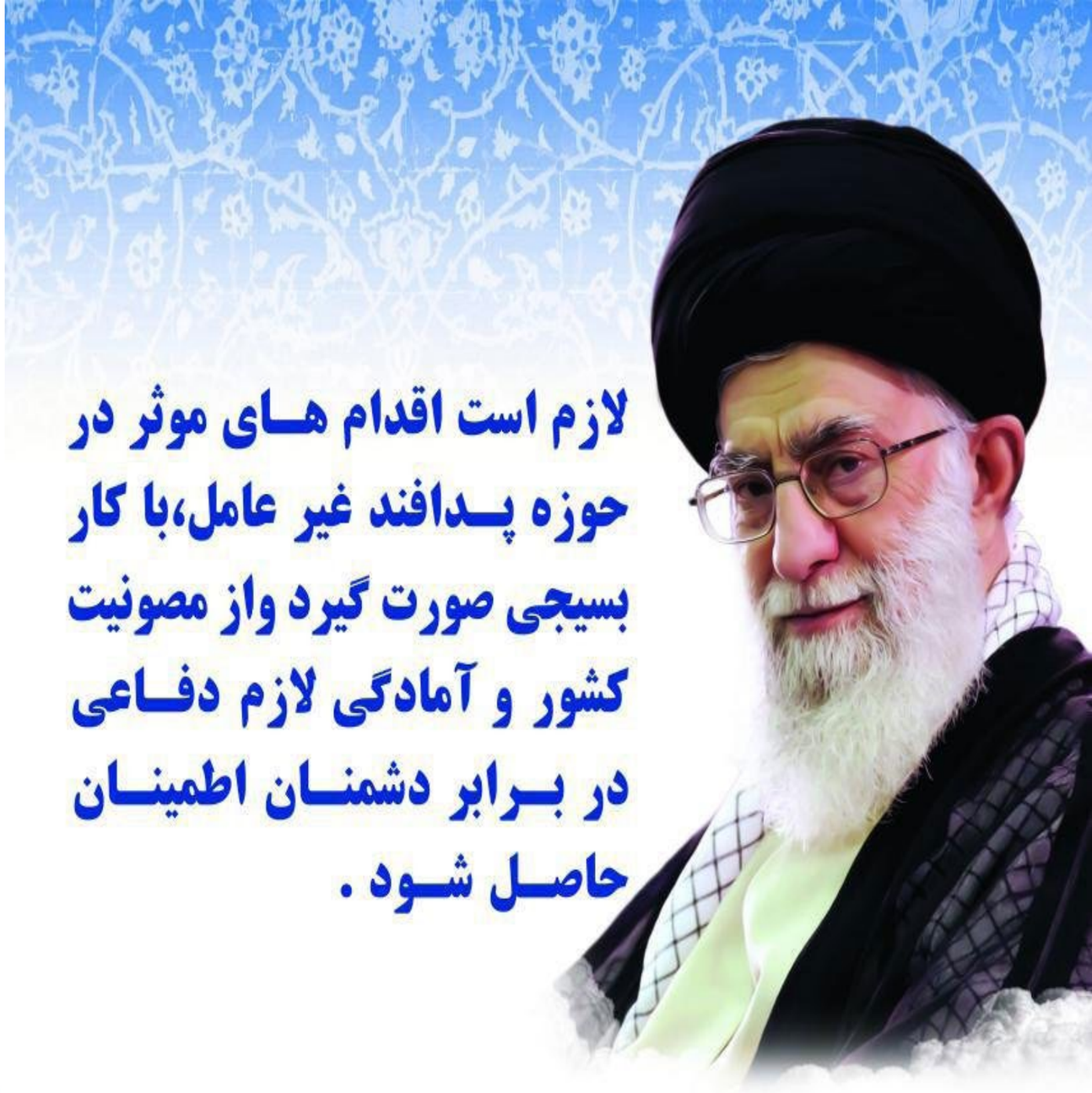


سردار رشید اسلام شهید
حاج قاسم سلیمانی

جهت دسترسی به آرشیو نشریه به این لینک مراجعه فرمایید.

بسم الله الرحمن الرحیم

فهرست مطالب:



پدافند غیر عامل ، حصول اطمینان از مصونیت و آمادگی کشور

مدیر مسئول:
محمد باقر آقایی

سردبیر:
لیدا رسول اهری

نشانی:
تبریز، میدان شهدا، استانداری آذربایجان شرقی، اداره کل پدافند غیرعامل
تلفن: ۳۵۲۹۱۳۱۸-۰۴۱
دورنگار: ۳۵۲۹۱۳۵۹-۰۴۱

استادان، پژوهشگران و دانشجویان علاقمند، می‌توانند مقاله‌های آموزشی، پژوهشی و ترویجی خود را برای درج در نشریه پدافند غیر عامل به نشانی زیر ارسال کنند.

passivedefense@ostan-as.gov.ir

جلسه بررسی تهدیدات زیرساختی در منطقه کجوار تبریز

محمدباقر آقایی، مدیرکل پدافند غیرعامل استانداری آذربایجان شرقی در این جلسه هدف و رسالت پدافند غیرعامل را حفاظت از زیرساخت‌های کشور، صیانت از نیروی انسانی و مدیریت کشور دانست و اظهار داشت: حفاظت از زیرساخت‌ها در این منطقه اهمیت زیادی دارد چرا که پایه‌های اساسی توسعه و بنیان خدمت رسانی به جامعه است، با توجه به پیچیده بودن تهدیدات باید به دانش جدید و علم روز مجهز شویم تا از زیرساخت‌ها بصورت هوشمندانه محافظت کنیم.

وی در ادامه مؤلفه های حفاظت از زیرساخت‌ها را در مرحله اول تهدید شناسی، شناخت ماهیت تهدید و در مرحله بعد رصد و پایش همیشگی این زیرساخت‌ها و تحلیل دائمی تهدیدات مربوط به آن دارایی‌ها دانست.

آقایی با بیان اینکه حفاظت از زیرساخت‌های استان اهمیت زیادی دارد، گفت: استراتژی دشمن در مرحله اول حمله به این زیرساخت‌ها است، ابزارهای حمله نیز عملیات انتحاری، ریز پرنده‌ها، خرابکاری، تروریسم سایبری، کموتروریسم، تروریسم پرتوی و استفاده از سلاح‌های پرتابی است.

در نتیجه هدف حفاظت از این نوع مناطق، کاهش آسیب پذیری‌ها، تداوم خدمات ضروری، پاسخ اضطراری به حوادث و در نهایت تسهیل مدیریت بحران است.

باقری، مدیرعامل شرکت پالایش نفت تبریز و فرمانده ارشد پدافند غیرعامل منطقه کجوار نیز با بیان اینکه یکی از اهداف پدافند غیرعامل افزایش بازدارندگی در برابر تهدیدات دشمن است، اظهار داشت: با وجود واحدهای صنعتی و تولید مواد شیمیایی در منطقه کجوار، انتخاب فرمانده ارشد پدافند غیرعامل برای این منطقه با هدف یکپارچه سازی برنامه‌های مقابله با تهدیدات دشمن است.

وی گفت: اگر در حال حاضر حادثه‌ای در این منطقه رخ دهد در چه سطحی آمادگی داریم، با تمرین و ممارست باید آمادگی خود را ارتقا دهیم.

اعضای جلسه نیز دیدگاه‌های خود را برای مقابله با تهدیدات در شرایط فعلی کشور ارائه کردند.

جلسه قرارگاه پدافند زیستی برگزار شد

مدیرکل پدافند غیرعامل استانداری در جلسه قرارگاه پدافند زیستی، به اهمیت فوق‌العاده این قرارگاه و فعال بودن آن اشاره کرد و گفت: جنگ‌ها به صورت عامل و غیرعامل یا انسان‌ساخت اتفاق می‌افتد، برای مقابله با چنین تهدیداتی باید به‌روز بوده و آسیب‌ها و تهدیدات به طور مرتب رصد شوند.

زیرساخت‌های زیستی باید از هرگونه آسیب در امان بوده و بتوانند تداوم خدمات رسانی در شرایط اضطراری را داشته باشند. امروزه پدافند غیرعامل کم هزینه‌ترین و صلح آمیزترین گزینه دفاع است و کشورهای پیشرفته در این راستا میلیاردها دلار هزینه و مرکز پژوهش و مطالعات زیستی را راه اندازی کرده‌اند.

دفاع زیستی در کشور ما باید به یک فرهنگ عمومی تبدیل شود و با توجه به اهمیت قرارگاه پدافند زیستی، کارگروه‌های این قرارگاه باید بصورت مرتب و ماهانه نسبت به شناسایی آسیب‌ها و تهدیدات و ارائه راهکارهای لازم در برابر هرگونه تهدیدات احتمالی زیستی در استان اقدام کنند.

گل‌محمدزاده، معاون هماهنگی سپاه عاشورا نیز بر تشکیل به موقع جلسات قرارگاه زیستی و کارگروه‌های تخصصی آن به منظور شناسایی تهدیدات و آسیب‌های احتمالی این حوزه تأکید کرد.

دیدار مدیرکل پدافند غیرعامل استانداری آذربایجان شرقی با رئیس دانشگاه تبریز

مدیرکل پدافند غیرعامل استانداری به منظور بررسی زمینه‌های همکاری علمی و آموزشی با دانشگاه تبریز، با رئیس این دانشگاه دیدار و گفت و گو کرد.

محمدباقر آقایی در این دیدار، با بیان اینکه دانشگاه‌ها می‌توانند نقش مؤثر و ارزنده‌ای در پیش برد اهداف پدافند غیرعامل داشته باشند، بر استفاده از ظرفیت دانشگاه تبریز در این راستا تأکید کرد.

با توجه به اینکه تهدیدات عصر حاضر روز به روز پیچیده تر، علمی تر و فناوری محور می‌شود، دانشگاه ها می‌توانند نقش مؤثری در یافتن راهکارهای علمی مؤثر برای مقابله با آن‌ها داشته باشند.

اداره کل پدافند غیرعامل آماده است هرگونه طرح های مطالعاتی و نظارتی، دوره‌های آموزشی و همایش‌های تخصصی را با همکاری دانشگاه تبریز اجرا کند.

مجیدی، رئیس دانشگاه تبریز هم ضمن استقبال از ورود دانشگاه تبریز و دانشکده های تخصصی مربوطه به حوزه پدافند غیرعامل، آمادگی کامل دانشگاه تبریز را در راستای پیش برد اهداف پدافند غیرعامل اعلام کرد.

در این جلسه مقرر شد به منظور تسریع و تسهیل همکاری‌های دوجانبه و استفاده از ظرفیت‌های پژوهشی و علمی دانشگاه تبریز، تفاهم نامه همکاری بین این دانشگاه و اداره کل پدافند غیرعامل استانداری امضا شود.

ساختار شهر و طراحی شهری از منظر پدافند غیرعامل

تهیه و تنظیم: اداره کل پدافند غیر عامل- رضا خوش روا (کارشناس امریه پدافند غیرعامل)
منبع: کتاب ساختار شهر و طراحی شهری از منظر پدافند غیرعامل، پدیدآورنده: مهندس مهدی سالک احمدی

تهدید شناسی و دارایی شناسی

مفهوم تهدید:

تهدید در معنای عام یعنی ترساندن طرف مقابل جهت جلوگیری از حمله وی و یا حصول یک هدف از قبل پیش بینی شده می‌باشد. هر چیز که در مقابل امنیت انسان قرار گرفته و امنیت و ثبات انسان را به خطر اندازد به عنوان «تهدید» مطرح می‌گردد. تهدید از سه بخش اساسی «کارگزار یا عامل تهدید»، «حوزه تهدید» و «موضوع تهدید» تشکیل شده است.

اهداف تهدید:

۱) تهدید نظام سیاسی حاکم بر کشور
۲) تهدید ارکان نظام سیاسی حاکم بر کشور
۳) تهدید ارزش‌های حاکم بر جامعه
٤) تهدید منافع ملی
۵) تهدید تمامیت ارضی کشور
٦) تهدید استقلال کشور
۷) تهدید منابع انسانی

سطوح تهدید:

سطح تاکتیکی: در این سطح نیروهای متخاصم از طریق انتخاب و کنترل ماهرانه فضای نبرد و به کارگیری روش‌های عملیاتی مناسب علیه تأسیسات و تجهیزات و سامانه‌های آن‌ها وارد عمل می‌شوند.

سطح عملیاتی: در این سطح فعالیت نیروهای عمل کننده در جهت تحقق اهداف امنیت ملی کشور و علیه اهداف امنیت ملی کشور مقابل می‌باشد.

سطح راهبردی: سطح تبدیل اهداف سیاسی جنگ به سایر اهداف از جمله اقتصادی، صنعتی، اجتماعی و نظامی و کاربرد تمام ظرفیت‌ها و قابلیت‌های هجومی و نظامی برای دستیابی به پیروزی قطعی است.

جنگ‌های بی‌قاعده:

جنگ بی‌قاعده به عنوان نبردی خشونت‌آمیز بین نیروهای دولتی و غیردولتی و با هدف کسب مشروعیت و تأثیرگذاری بر مردم تعریف می‌شود، این نوع جنگ شیوه‌های غیرمتعارف و غیرمستقیم را پشتیبانی می‌کند. با این وجود ممکن است انواع سلاح‌های نظامی و قابلیت‌های دیگر به منظور ایجاد فرسایش در نیروهای دشمن و تضعیف اراده و برتری آن‌ها به کارگرفته شود. در این دیدگاه، تمرکز جنگ بر مردم است نه نظامیان. جنگ بی‌قاعده تنها به دلاوری و سلحشوری نظامی وابسته نیست بلکه به ادراک ما از جنبش‌های اجتماعی نظیر سیاست‌های قومی، شبکه اجتماعی، تأثیرات مذهبی و آداب و رسوم فرهنگی نیز بستگی دارد.

آنچه که جنگ بی‌قاعده را از سایر جنگ‌ها متمایز می‌کند عبارتند از:

- تمرکز عملیات آن بر مردم
- هدف راهبردی آن یعنی در اختیار گرفتن، کنترل و جلب حمایت مردم با اعمال روش‌های سیاسی، روانی و اقتصادی است. به عبارت دیگر تمرکز بر مشروعیت به منظور اعمال نفوذ یا کنترل مردم است.

پدافند در جغرافیای شهری:

تأثیر پدافند بر فرم شهری و ساختار مورفولوژیکی و همچنین بر جنبه‌های موقعیتی محل شهری با ثبات‌ترین اثرات بر شهر در طول زمان می‌باشد که به صراحت و به صورت چشمگیر قابل مشاهده است. این نمایانی بسیار زیاد و در نتیجه توجه نسبتاً زیاد مفسران به این ویژگی، به نوبه خود خطرناک است. تأسف برانگیزترین مشکل اینکه این جنبه از ارتباط میل به سایه افکندن بر دیگر ارتباطات عملکردی حائز اهمیت ولی کم مشهودتر دارد. مروری بر ادبیات موجود، که ممکن است تنها با مطالعه چند نمونه دیدنی به دست آمده باشد، می‌تواند به راحتی این موضوع را نتیجه دهد که تنها تأثیر مهم پدافند بر شهرها، تأثیر آن بر فرم شهری بوده است.

جغرافیای شهری در علوم نظامی:

معمولاً اثبات این مسئله که پدافند نقشی مهم در بسیاری از ابعاد شهر ایفا می‌کرده بسیار آسان‌تر از این بوده است که نشان دهیم شهر نقشی مرکزی در علوم نظامی داشته است. این مسئله ممکن است عموماً درست‌تر باشد که اگر چه یک «جغرافیای پدافندی» وجود دارد، اما ممکن است در مقایسه با سایر متغیرها صرفاً اهمیت حاشیه‌ای در هدایت فعالیت‌های دفاعی داشته باشد و بارها نیز به عنوان یک طبقه بندی از کاراکترهای دفاعی عوارض زمینی در سطح تاکتیکی و یا ژئومتری فضایی بکار گرفته شده به منظور حرکت در سطح راهبردی تنزل یافته است.

چگونگی استفاده از شهرها در عملیات نظامی نه تنها به کاراکترهای ذاتی شهرها بلکه به ماهیت سیاست و استراتژی دفاعی انتخاب شده نیز وابسته است. به طور خلاصه شهرها مبادله‌ای از زمین‌های دفاعی خوب را برای کنترل فرماندهی ضعیف ارائه می‌نمایند: طیف‌های تسلیحاتی با اثربخشی کوتاه برای تحرک پذیری ضعیف.

دارایی‌های شهر:

دارایی یک منبع با ارزش است که نیازمند حفاظت بوده و می‌تواند ملموس (مانند مردم، ساختمان‌ها، امکانات، تجهیزات، فعالیت‌ها، عملکردها و اطلاعات) یا غیرملموس (مانند فرآیندها یا سابقه و اعتبار یک شرکت) باشد.

دارایی‌ها را می‌توان در سه دسته زیر طبقه بندی کرد:

– دارایی‌های فیزیکی یا کالبدی شامل سه زیر مجموعه سرمایه‌ها، تأسیسات و سازه می‌باشند.

– دارایی نیروی انسانی، به عنوان مهم ترین و حیاتی‌ترین دارایی یک مجموعه است.

– دارایی زیر ساخت تبادل اطلاعات (سایبر)، شامل مجموعه‌ای از سامانه‌ها که در راستای انتقال اطلاعات و داده‌ها طراحی شده‌اند شامل رایانه‌ها، نرم افزارها، اینترنت، ماهواره‌ها، بانک‌های اطلاعاتی و... که برای هر کشور به عنوان ارزش تلقی می‌گردد.

مفهوم جذابیت دارایی:

یکی از گام‌های اساسی در فرآیند مدیریت ریسک ناشی از عملیات خصمانه، شناخت و تحلیل تهدیدات و آسیب پذیری‌هایی است که دارایی‌ها با آن روبرو هستند. مفهوم خطرپذیری از مفهوم احتمال بالای حمله موفق علیه تجهیزات حیاتی ناشی می‌شود که توسط عواملی چون جاذبه هدف برای دشمن، درجه حساسیت و درجه آسیب پذیری دارایی‌ها تعیین می‌گردد. احتمال دارد بیشتر دارایی‌های شهر هیچ تاریخچه‌ای از تهدیدات خصمانه، نداشته باشند. ولی باید این فرض را در نظر داشت که وقوع اقدامات خرابکارانه عموماً علیه هر دارایی باورپذیر است و با عوامل ویژه آن مکان مرتبط می‌باشد. در واقع جاذبه یک دارایی برای دشمن معیاری کمکی جهت محاسبه احتمال حمله است که از تخمین عوامل مختلف نشان دهنده ارزش دارایی برای مورد هدف قرار گرفتن شکل می‌گیرد. دارایی جذاب به دارایی گفته می‌شود که یک هدف مطلوب برای دشمن به شمار می‌آید. ماهیت و میزان گستردگی ارزش دارایی نشان دهنده جذابیت دارایی است، باید توجه داشت که ارزش درک شده یک دارایی جذاب برای دشمن ممکن است از ارزش درک شده توسط نیروهای خودی متفاوت باشد.

معیارهای تأثیرگذار بر جذابیت دارایی‌ها:

همه دارایی‌ها برای دشمن ارزش یکسانی ندارند، یک فرض اساسی این است که ارزش یک دارایی از منظر دشمن عاملی است که احتمال وقوع یک حادثه امنیتی را تحت تأثیر قرار می‌دهد. تحقیقات نشان می‌دهد علاوه بر گستره حوزه نفوذ پیامدها و خسارت‌های ناشی از تهدیدات، عوامل دیگری نظیر اهمیت راهبردی دارایی ها و اهمیت و انحصاری بودن یا دیر بازگشت بودن دارایی‌ها از جمله مواردی است که می‌تواند بر میزان جذابیت دارایی‌ها تأثیرگذار باشد.

میزان انحصاری بودن و دیر بازگشت بودن دارایی:

مراکز مهم و شریان‌های حیاتی به واسطه خسارت و پیامدهای شدید که حمله به آن‌ها یا ایجاد اختلال در کار آن‌ها به دنبال دارد، از جذاب‌ترین دارایی شهرها برای مورد هدف قرار گرفتن از سوی دشمن هستند. در زمینه دیر بازگشت بودن و جبران خسارات وارده به شریان‌های حیاتی، عده‌ای از پژوهشگران، بخشی از مطالعات خودشان را به بازسازی خسارات ناشی از شریان‌های حیاتی اختصاص داده اند. البته هیچ‌گاه یک برنامه و الگوریتم دقیق عملیاتی برای بازگرداندن شریان‌های حیاتی جامعه به حالت عادی مورد تجزیه و تحلیل قرار نگرفته است.

آسیب شناسی در شهر

مفهوم آسیب شناسی:

همان طور که مشخص است آسیب شناسی از ترکیب دو کلمه آسیب و شناسی تشکیل شده است. در تشریح لغت آسیب آمده است:

۱. خسارت فیزیکی بر چیزی یا بر قسمتی از بدن شخص وارد می‌شود و منجر به شکست یا جراحت آن می‌گردد.

۲. خسارت فیزیکی که باعث کاسته شدن از جذابیت، سودمندی یا ارزش چیزی می‌گردد.

۳. عیب و نقص یا شکستگی که به سبب ضربت و زخم پیدا می‌شود، صدمه، زیان و ضرر.

تعریف آسیب پذیری و سطوح آن:

آسیب پذیری یک ابزار تحلیلی در مطالعات ایمنی شهری است. تحلیل و ارزیابی آسیب پذیری یک پایه و اساس جدید برای برنامه‌ریزی شهری فراهم می‌آورد. آسیب پذیری به خودی خود، مبنایی برای تعیین اقدامات کاهش اثر برای حفاظت از دارایی‌های حیاتی را در اختیار قرار می‌دهد. این ارزیابی آسیب‌پذیری، در روش‌شناسی پلی بین تهدید یا خطر، ارزش و دارایی و سطح‌شناسی از ریسک می‌باشد.

سطوح آسیب‌پذیری:

– خیلی زیاد: هیچ اقدام حفاظتی صورت نگرفته

– زیاد: اقدامات حفاظتی کمی صورت گرفته

– متوسط: تعدادی اقدامات حفاظتی صورت گرفته

– پایین: تعدادی اقدامات حفاظتی صورت گرفته ولی حداقل یک ضعف وجود دارد

– بسیار پایین: لایه‌های حفاظتی چندگانه صورت گرفته است

روش ارزیابی کمی آسیب‌پذیری:

در این روش بررسی‌های زیر صورت می‌گیرد:

– بررسی مشخصات کلی دارایی‌ها

– بررسی‌های دقیق بخش‌های مختلف دارایی‌ها و میزان مقاومت آن‌ها در برابر حملات انفجاری

– تهیه جداول و درجه‌بندی دارایی‌ها و اجزای آن‌ها و اولویت‌بندی بر اساس کسب بالاترین نمره

روش ارزیابی کیفی آسیب‌پذیری:

در ارزیابی کیفی، عناصری که به سهولت قابلیت تبدیل عددی را نداشته ولی در موفقیت طرح‌های پدافند مؤثرند، مورد توجه قرار می‌گیرند:

– بررسی وضعیت کارکنان شاغل در هر یک از دارایی‌ها و جمعیت اطراف آن از نظر ملاحظات فرهنگی، اقتصادی، اجتماعی، رضایتمندی، سطح سواد و ...

– بررسی موقعیت مکانی مراکز پشتیبانی عمومی موجود در منطقه مانند مراکز آتش‌نشانی، امداد و نجات، پست، برق و ...

– بررسی ارتباطات و دسترسی‌های مختلف به دارایی‌ها

– بررسی امکانات دستگاه‌های دولتی در نزدیکی دارایی و امکان استفاده از آن‌ها در هنگام بحران

اهمیت محیط‌های شهری در جنگ آینده:

آنچه مشخص است این است که در تهاجمات نظامی جنگ‌های اخیر، بخش زیادی از تهدیدات متوجه شهر و تأسیسات و تجهیزات موجود در آن بوده است. نواحی و مناطق شهری مراکز قدرت تلقی شده و بخصوص در آموزش‌های ارتش آمریکا، نواحی شهری از عمده ترین و معمول ترین مناطق درگیری در جنگ‌های آینده آن‌ها پیش بینی می‌شود.

ویژگی‌های یک منطقه شهری از دیدگاه نظامی و ملاحظات دفاع غیرعامل چیست؟ همواره از نقطه نظر فرماندهان جنگی، شهرها مراکز ثقل و منابع قدرت مالی قلمداد شده و می‌شوند. شهرها مناطقی هستند که به عنوان مراکز جمعیتی، قطب‌های حمل و نقل و ارتباطات، نقاط کلیدی توسعه و صنعت و اقتصاد و سیستم‌های اطلاعاتی، محل استقرار مراکز دولتی و مخازن ثروت نقش ایفا می‌کنند.

مهم ترین هدف‌های تأسیساتی و تجهیزاتی که در زمان جنگ حمله به شهرها را توجیه می‌کند و اغلب بخش‌های غیرنظامی شهرها نیز آسیب می‌بینند، عبارتند از:

۱) پادگان نظامی ۲) صنایع، نیروگاه‌ها، پالایشگاه‌ها و پست‌های فشار قوی ۳) تصفیه‌خانه‌ها، مخازن ذخیره سوخت و آب ٤) فرودگاه‌ها، پایانه‌ها، راه آهن، بنادر، جاده‌ها، پل‌ها و شبکه‌های مخابراتی

فرودگاه‌ها، راه آهن، بنادر، جاده‌ها، پل‌ها، اتوبان‌های عمده و به طور کلی شبکه‌های ارتباطی از عناصر عمده شهرها بوده و در زمره تأسیسات و تجهیزات زیربنایی و زیرساخت‌های کلیدی مورد توجه دشمن در زمان وقوع تهدید و جنگ محسوب می‌گردند.

آسیب پذیری فضاهای شهری:

فضاهای شهری می‌تواند به عنوان فضاهای امن جهت گریز، پناه گیری، امداد رسانی، اسکان موقت و جمع آوری کمک‌ها در زمان بحران باشد. کسانی که در فضاهای شهری قرار دارند به شدت در معرض آسیب‌های جدی قرار می‌گیرند. این آسیب‌ها معمولاً ناشی از عوامل زیر می‌باشند:

– اصابت مستقیم ترکش عامل انفجار

– موج انفجار

– پرتاب تکه‌های اشیاء منهدم شده

– ریزش آوار

– انفجار اتومبیل‌ها و مخازن سوخت داخل محوطه

نتیجه گیری:

از مهمترین تدابیر دفاعی، در نظر گرفتن پدافند غیرعامل در شهرهاست. شهرها به عنوان مراکز تجمع سرمایه مادی و انسانی در زمان جنگ به هدفی عمده برای دشمن تبدیل می‌شوند، در نتیجه حمله به آن‌ها خسارات فراوانی را پدید می‌آورد. برنامه ریزی و طراحی شهری از آنجا که تخصصی ترین رشته مربوط به شهر به ویژه از بعد کالبدی و فضایی می‌باشد قدرت دفاعی را بالا می‌برد.

ضرورت پدافند اقتصادی در فضای داد و ستد بین المللی

تهیه و تنظیم: مهندس علیرضا پویافر- رابط پدافند غیرعامل شهرداری صوفیان

منابع: ۱- سند راهبردي پدافند اقتصادي كشور،۱۳۹۲-۱۳۹۶
۲- صحیفه امام خمینی (ره) ، جلد ۱۱
۳- اسکندری، حمید.۱۳۹۵، دانستنی‌های پدافند غیرعامل، انتشارات بوستان حمید
٤- پدافند اقتصادی، پیش شماره اول، آبان ۱۳۹۳، صفحه ۶ تا ۹
۵- فصلنامه پدافند غیرعامل، سال نهم شماره ۲ (پیاپی ۳۴، تابستان ۱۳۹۷)

مقدمه:

یکی از واقعیت‌های حال حاضر در فضای اقتصاد بین الملل، تقابل و درگیری اقتصادی است؛ امری که در فضای ادبیات علمی اقتصاد، کمتر بدان پرداخته می شود، چون فرض بنیادین در علم اقتصاد، آزادی تجارت و داد و ستد است. تقابل اقتصادی در برخی از موارد، ازجمله مقابلهٔ برخی قدرت‌های غربی با جمهوری اسلامی ایران، از حد متعارف آن خارج شده و به جنگ تمام عیار اقتصادی تبدیل شده است.

تهدیدهای اقتصادی به سه دسته تقسیم می‌شوند:

• در نوع اول از ابزار نظامی علیه زیرساخت‌های اقتصادی کشور هدف استفاده می‌شود. مانند جنگ تحمیلی هشت ساله که کشور مهاجم، زیرساخت‌های اقتصادی مانند پتروشیمی‌ها و سیلوها را ویران می‌کرد.

• نوع دوم، جنگ برای سیطره و به دست آوردن منابع اقتصادی کشور دیگر است، مانند جنگ خلیج فارس که به جنگ نفت معروف است یا سیاستی که آمریکا در آمریکای جنوبی دنبال می‌کند تا بر منابع نفتی آن‌ها خیمه زند.

• نوع سوم، جنگ با استفاده از ابزارهای اقتصادی مانند تحریم و نهادهای بین‌المللی علیه منافع اقتصادی کشورهای دیگر است.

پدافند اقتصادی که یکی از زیرمجموعه‌های پدافند غیرعامل به شمار می‌رود به دنبال این است که بتواند هر سه جنگ را در حوزه‌های اقتصادی بی‌اثر کند.

بر پایه تجارب و شواهد ثبت‌شده در جنگ‌ها، دفاع غیرعامل موجب صرفه‌جویی کلان اقتصادی و ارزی در حفظ تجهیزات می‌گردد؛ موجب زنده ماندن و بقای نیروی انسانی می‌گردد که با ارزش‌ترین سرمایه ملی هر کشوری به شمار می‌رود؛ مراکز حیاتی و حساس اقتصادی، سیاسی، نظامی، ارتباطی و غیره را از حملات دشمن دور نگه می‌دارد و ادامه فعالیت را در شرایط بحرانی ممکن می‌کند؛ همچنین دفاع غیرعامل در مقایسه با دفاع عامل، ساده‌تر و با سیاست‌های خودکفایی و استقلال‌خواهی کشور همسوتر است.

دفاع و پدافند اقتصادی یکی از نیازهای اصلی جامعه اسلامی است که قرآن کریم، به عنوان معجزه جاودانه دین اسلام، در پاسخگویی به این نیاز بی اعتنا نیست. پیامبران الهی در طول دوران رسالت خویش، با انواع تهدیدهای اقتصادی از داخل و خارج جامعه مواجه بوده‌اند و در قرآن کریم به قصص برخی از ایشان اشاره شده است. در این مطلب با بهره گیری از روش تدبر داستان محور در قرآن کریم، به سیره پیامبر اکرم (ص) در مقابله با تهدید نظامی اقتصادی احزاب، سیره حضرت یوسف (ع) در مدیریت بحران اقتصادی خشک سالی در مصر و نیز سیره حضرت شعیب (ع) در مقابله با فساد اقتصادی کم فروشی و آسیب پذیری اقتصادی قوم خویش، به عنوان مصادیقی از راهبردهای دفاع اقتصادی در قرآن کریم پرداخته شده است.

در نهایت با بررسی قصص پیامبران الهی در قرآن کریم، دفاع اقتصادی را می‌توان به سه نوع تقسیم بندی کرد:

دفاع اقتصادی در برابر تهدیدهای داخلی

دفاع اقتصادی در برابر تهدیدهای خارجی (از بیرون مرزها)

دفاع اقتصادی در برابر تهدیدهای طبیعی

بر همین اساس به سه نوع راهبرد سلبی (کنترل و بازدارنده)، ایجابی (سازمان دهنده) و راهبرد فرهنگ سازی اقتصادی، به عنوان راهبردهای دفاع اقتصادی در قصص پیامبران الهی اشاره می‌شود.

اگر چه می‌توان استفاده از ابزارهای اقتصادی در مقابلهٔ کشورها را در دوران پس از جنگ جهانی دوم یعنی دوران به اصطلاح جنگ سرد جستجو کرد. ولی جنگ اقتصادی علیه جمهوری اسلامی ایران هم به لحاظ مدت زمانی که بیش از سه دهه از آغاز آن می‌گذرد و هم به لحاظ ابعاد گستردهٔ آن خصوصاً از زمستان سال ۱۳۹۰ و هم از نظر صف بندی بین المللی، نمونه ای کم نظیر در این نوع جنگ‌هاست.

نکته درخور تأمل دربارهٔ جنگ تمام عیار اقتصادی این است که متأسفانه با وجود اینکه سابقه تحریم و محدودیت اقتصادی در جهان به بیش از یک قرن می رسد، جنگ اقتصادی واژه‌ای ناشناخته برای مجامع علمی محسوب می‌شود و محتوای منسجمی در این حوزه وجود ندارد.

این درحالی است که کشورهای متخاصم با تحمیل ادبیات اقتصادی متعارف به کشورهای مختلف و نگنجاندن راهکارهای مقابله و برون رفت از جنگ اقتصادی، نظریات جنگ اقتصادی را برای به چالش کشیدن زیرساخت‌های حیاتی اقتصادی کشورهای هدف طراحی کرده و با آمادگی کامل وارد این وادی شده اند.

نمونه‌ای از این تلاش‌ها را می‌توان در گزارش ۱۴ آوریل ۲۰۱۴ دربارهٔ شکل گیری اتاق جنگ مدرن اقتصادی آمریکا در وزارت خزانه داری این کشور ملاحظه کرد.
این اتاق جنگ در حکم خط مقدم جبههٔ اقتصادی ایالات متحده و شرکای بین المللی آن محسوب می‌شود. تیم ۱۷۰ نفرهٔ جنگ اقتصادی شامل مجموعه‌ایی از وکلا، استراتژیست‌ها و تحلیلگران اطلاعاتی است که قدرت فوق العاده‌ای در قطع و مسدود کردن تبادلات ارزی دلاری در سراسر جهان دارد.
سیاستگذاری پدافند غیرعامل تابعی از شکل بندی‌های اقتصادی و ضرورت‌های ساختاری در نظام سیاسی تلقی می‌شود. کشورهایی که روند رشد اقتصادی و نوسازی را طی می‌نمایند از قابلیت‌های لازم برای سازماندهی پدافند غیرعامل برخوردارند.
این امر نشان می‌دهد که نوسازی و رشد اقتصادی آثار خود را در حوزه‌های فرهنگی، اجتماعی، ساختاری و راهبردی بجا می‌گذارد. وقتی که بیان می‌شود مسئولیت سازمان پدافند غیرعامل در حوزه اقتصادی، «صیانت از مردم در جنگ تمام عیار اقتصادی» است، گستره این صیانت، هم نیازهای اساسی مردم را در بر می‌گیرد و هم خدماتی که به مردم باید ارائه شود.
در این صورت، چرخه تأمین کالاهای اساسی نیز اهمیت می‌یابد؛ در مواردی که به دلیل خشکسالی یا نبود فناوری به‌روز، امکان تولید کالایی در کشور فراهم نباشد، فرایند تأمین باید از منابع و مراجع امن انجام شود؛ منابعی که در شرایط بحرانی هم بشود روی کمک آن‌ها حساب باز کرد.
از سوی دیگر، در شرایطی که تهدیدهای رنگارنگ کشورمان را آماج خود گرفته‌اند، یکی از گزینه‌ها برای دفع یا کاهش خطر، استفاده از فرصت‌هایی است که به واسطه افزایش سرمایه‌گذاری‌های خارجی حاصل می‌شود.
به نقل از دنیای اقتصاد: بی‌شک استفاده از سرمایه‌گذاری‌های خارجی، موجب بازدارندگی و کاهش تهدیدهای بزرگ و کوچک خواهد شد. به ویژه این که صحنه‌گردان بسیاری از لابی‌های سیاسی در دنیای غرب، سرمایه‌داران و کارتل‌های اقتصادی هستند.
با این نگاه، توجه به پدافند غیرعامل به ویژه در شرایط فعلی که هیأت‌های تجاری و اقتصادی در تکاپوی گرفتن گوی سبقت از یکدیگر برای مذاکره با دولتمردان و بازرگانان ایرانی هستند، لازم است تا با تدوین یک سند فراگیر، مدل‌ها و روش‌هایی برای جذب سرمایه‌گذاری‌های خارجی انتخاب شوند که مبنای آن‌ها بالابردن هزینه‌های غرب نسبت به هر گونه تصمیم‌گیری در مورد تغییر سطح روابط خود با ایران در آینده باشد.
امروزه در فضای اقتصادی به‌جای تعامل، فضای جنگ حاکم است. مثلاً امروزه تحریم‌های دوطرفهٔ آمریکا و روسیه را مشاهده می‌کنیم که نمادی از جنگ اقتصادی است که در گذشته این جنگ متفاوت بوده است.
در واقع امروزه ماهیت و حوزه‌های تهدید تغییر کرده است بنابراین الزامات مقابله با تهدیدات نیز باید تغییر کند.
در تمامی جنگ‌های اقتصادی آمریکا علیه کشورهای مختلف، به واسطه سیطرهٔ نظریات لیبرال سرمایه داری در کشورهای هدف و فقدان ایدئولوژی قوی و ساختار حکومتی منسجم در آن کشورها، آمریکا توانسته بود به بسیاری از اهداف از پیش تعیین شدهٔ خود نائل شود. اما دربارهٔ ایران با پدیدهٔ پیچیده‌ای مواجه شده است که عبارت است از مقاومت مکتبی که در متن رفتارهای مردم و حاکمان اثرات عمیق و خدشه ناپذیری دارد.
این روحیهٔ مقاومت باعث شده است که پس از وضع تحریم‌های گسترده و ایجاد ممنوعیت‌ها و موانع مختلف در مسیر حرکت اقتصاد ایران خصوصاً تحریم‌های سال‌های اخیر که به «تحریم‌های فلج کننده» معروف شده است، اقتصاد ایران نه تنها پابرجا بماند بلکه بتواند همچنان نیازهای مردم را تأمین و معیشت آن‌ها را اداره کند.
این روحیهٔ مقاومت مردمی ریشه در اندیشهٔ اسلامی و نظام حاکمیتی ایران دارد که پس از پیروزی انقلاب اسلامی در قالب جمهوری اسلامی و حکومت ولی فقیه متبلور شده است.
رهبران انقلابی ایران، از همان ابتدای استقرار نظام اسلامی، با توجه به خصومت‌های دشمنان در عرصه‌های مختلف، از تهاجم اقتصادی قدرت‌های جهانی غافل نبوده و در برهه‌های مختلف آن را متذکر شده اند.
حضرت امام خمینی (ره) در همان سال‌های ابتدایی پیروزی انقلاب اسلامی (۹/ ۳/ ۶۱) دربارهٔ جنگ اقتصادی فرمودند: «شما درحال جنگید الان. یک جنگی که جنگ اقتصادی است. یک محاربه الان مابین اسلام و کفر است

که محاربهٔ اقتصادی یکیش است» (صحیفه امام، ج ۱۱، ص: ۴۲۵).
در حالیکه دشمن متخاصم نقشهٔ تحریم فروش نفت را کلید زد حضرت امام خمینی (ره) این تحریم‌ها و جنگ اقتصادی علیه ایران اسلامی را یک تحفه الهی نامیدند (صحیفه امام خمینی .ج ۱۱.ص ۴۲۴).
همچنین در چند سال اخیر، مقام معظم رهبری نیز با الهام از مفاهیم ارزشمند الهی و دینی و همچنین احاطه به نقشه‌های دشمن، با اعلام وضعیت جنگی در حوزهٔ اقتصاد، توجه مردم و مسئولان کشور را به این خطر بزرگ و تهاجم گسترده جلب کرده‌اند و لزوم ایجاد آمادگی‌ها و تدارکات لازم برای مقابله با این جنگ تمام عیار را در مناسبت‌های مختلف متذکر شده‌اند.
ایشان در جلسهٔ تبیین سیاست‌های اقتصاد مقاومتی فرمودند: «تحریم‌ها از قبل بود منتها این تحریم‌ها از حدود زمستان سال ۹۰ تا امروز، تبدیل شده به جنگ اقتصادی. دیگر اسم آن تحریم هدفمند نیست، یک جنگ تمام عیار اقتصادی است که متوجه ملت ما است.
براساس بند ۵ اصل ۱۱۰ قانون اساسی، اعلام جنگ و صلح کشور برعهده رهبری می‌باشد و در این وضعیت، مقام معظم رهبری در تاریخ بیست بهمن ۱۳۹۲ ، کشور را درگیر جنگ تمام عیار اقتصادی ترسیم کردند.
از این رو، سازمان پدافند غیرعامل کشور در راستای دفاع از ساختارهای حیاتی اقتصادی کشور و خنثی کردن تهدید دشمن، وارد عرصهٔ پدافند اقتصادی کشور شد.
قرارگاه پدافند اقتصادی با هدف کاهش آسیب پذیری اقتصادی، مقاوم سازی اقتصاد، تداوم چرخهٔ تولید، ذخیره سازی و نگهداری و تسهیل مدیریت بحران در وضعیت تحقق تهدیدها، افزایش بازدارندگی اقتصادی و درنهایت مصون سازی اقتصادی در برابر تهدیدها و اقدامات خصمانه و مخرب دشمن، به تدوین سیاست‌های مختلف و برنامه ریزی، هدایت و راهبری، طراحی و پیاده سازی راهبردهای جامع دفاع اقتصادی و نیز فرهنگ سازی با رویکرد اقتصاد مقاومتی اقدام کرده است.
اگرچه ابلاغ سیاست‌های اقتصاد مقاومتی با توجه به فشار و تهدید دشمن، خود از امور پدافند غیرعامل محسوب می شود، سازمان پدافند غیرعامل کشور در حوزه‌هایی که مرتبط با دفاع اقتصادی است به صورتی فعال وارد شده است تا در رفع تهدیدات دشمن و کمک به ادارهٔ بهتر مردم از طریق تدوین برنامه‌های راهبردی و راهکارهای عملیاتی به همهٔ ارکان نظام و خصوصاً قوای سه گانه همیاری رساند و وظیفهٔ ذاتی و سازمانی خود را به انجام رساند.
قرارگاه اقتصادی نیز می‌تواند در راستای پدافند اقتصادی مثمر ثمر باشد، نقش قرارگاه اقتصادی، تدوین راهبردهای پدافند اقتصادی است تا بهره‌برداران اقتصادی کشور یعنی مردم و دستگاه‌های ذی‌ربط را به سمت اهداف پدافند اقتصادی، سیاست‌گذاری، برنامه‌ریزی، راهبری و هدایت کند.
قرارگاه اقتصادی مسئولیت اجرایی مشخصی ندارد بلکه تدوین سیاست‌ها، راهبردها و اهداف برعهدهٔ این قرارگاه و اجرا توسط دستگاه‌های اجرایی صورت می‌گیرد.
اهداف کلان قرارگاه تولید پایداری و مصونیت اقتصادی در کشور است که دولت از آن به عنوان ثبات اقتصادی یاد می‌کند که در برابر تهدیدات معنا پیدا می‌کند.

سو. استفاده از *RDP* در حملات گسترده باج‌افزاری، کاوش رمزارز و سرقت اطلاعات

بازیگران تهدید با هدف نفوذ به شبکه سازمان‌ها، در حال انتقال بدافزار از طریق پروتکل دسترسی از راه دور به دسکتاپ (*RDP*)، بدون باقی گذاشتن ردپا در سیستم هدف هستند. در این روش کاوشگرهای رمزارزها، بدافزارهای سارق اطلاعات و باج‌افزارها، از طریق یک اتصال از راه دور در حافظه موقت (*RAM*) اجرا می‌شوند. مهاجم در این رویکرد از یک ویژگی خاص در سرویس دسترسی از راه دور به دسکتاپ بهره می‌برد. این ویژگی به کلاینت اجازه می‌دهد تا درایوهای ذخیره‌سازی محلی را به همراه دسترسی‌های خواندن و نوشتن با یک سرور ترمینال به اشتراک بگذارد.

دسترسی به منابعی که با این شیوه به اشتراک گذاشته می‌شوند از طریق *RDP* امکان‌پذیر است و بدلیل اینکه برنامه‌ها در حافظه اجرا می‌شوند هیچ اثری در دیسک سیستم کلاینت باقی نمی‌ماند. زمانی که نشست *RDP* متوقف شود، فرآیندهای پردازشی مرتبط و حافظه نیز آزاد می‌شوند.

تحلیل‌گرهای بدافزار *Bitdefender* گروهی از مجرمین سایبری را شناسایی کرده‌اند که در حال سوء استفاده از این روش هستند. آن‌ها چندین بدافزار با گونه‌های متنوع را به همراه مؤلفه‌ای با نام *worker.exe* که دستورالعمل خود را از مهاجم دریافت می‌کند، منتقل می‌کنند. مؤلفه *worker.exe* ابزاری است که بدلیل قابلیت‌های جاسوسی خود، توسط چندین بازیگر تهدید استفاده می‌شود.

از جمله اطلاعاتی که این مؤلفه می‌تواند از یک سیستم جمع‌آوری کند موارد زیر است:

- اطلاعات سیستم: معماری، مدل پردازنده، تعداد هسته، اندازه حافظه داخلی، نسخه ویندوز
- نام دامنه، سطح دسترسی کاربر وارد شده، لیست کاربران موجود در دستگاه
- آدرس *IP* محلی، بارگذاری و سرعت دانلود و آپلود، اطلاعات *IP* عمومی
- مرورگر پیش فرض، وضعیت پورت‌های خاص روی میزبان، بررسی سرورهای در حال اجرا و وضعیت گوش دادن به پورت آن‌ها، ورودی‌های خاص در کش *DNS*.
- بررسی وضعیت اجرای برخی از فرایندهای پردازشی، وجود کلیدها و مقادیر خاص در رجیستری

علاوه بر این، مشاهده شده است که *worker.exe* به سه ابزار سارق اطلاعات کلیپ‌بورد (*MicroClip*، *DelphiStealer* و *IntelRapid*)، دو خانواده باج‌افزاری (*Rapid* و ۲٫۰ *Rapid* و *Nemty*)، چندین کاوش‌گر رمزارز *Monero* (همگی مبتنی بر *XMRig*) و از جولای ۲۰۱۸ به بدافزار سارق اطلاعات AZORult مجهز شده است.

تمام اطلاعات جمع‌آوری شده از میزبان در یک فایل *NFO*. قرار داده می‌شوند که در همان مکان فایل پیکربندی ذخیره می‌شود. این کار یک روش مناسب برای دور نگه داشتن داده‌ها از رایانه مورد هدف و دشوارتر کردن فرایند جرم‌شناسی است.

هدف هر سه سارق کلیپ‌بورد شناسایی آدرس کیف پول رمزارز کاربر و جاگزینی آن با کیف پول متعلق به مهاجم است. به این ترتیب، مقصد اصلی تراکنش‌های خروجی به کیف پول مهاجم تغییر می‌کند.

از بین سه بدافزار سارق کلیپ‌بورد، *IntelRapid* پیشرفته‌تر از موارد دیگر است. این بدافزار تعداد بیشتری از کیف پول‌های رمزارز (بیت‌کوین *Litecoin*، *Ethereum*، *Monero*، *Bitcoin Cash*، *Dash*، *Ripple*، *Neo*، *Dogecoin* و *ZCash*) را می‌تواند شناسایی کند و آن‌ها را با گزینه‌های مهاجم جایگزین کند.

نقطه نفوذ مهاجمین بطور واضح برای پژوهشگران امنیتی مشخص نشده است اما استفاده از روش جستجوی فراگیر (brute-*force*) یکی از گزینه‌های امکان‌پذیر است.

مهاجم این حملات قربانی خاصی را مورد هدف ندارد و تنها به تعداد زیاد آن‌ها اهمیت می‌دهد.

کاربران می‌توانند با غیرفعال کردن *drive redirection* از رخ دادن این حملات پیش‌گیری کنند.

محصولات Cisco ASA مورد هدف حملات DoS توسط یک آسیب‌پذیری قدیمی

یک آسیب‌پذیری بحرانی که در سال ۲۰۱۸ در محصولات *Adaptive Security Appliance* و *Firepower* سیسکو مرتفع شد، بار دیگر در حملات منع سرویس (*DoS*) و افشا اطلاعات مورد بهره‌برداری قرار گرفته است.

این آسیب‌پذیری دارای شناسه *CVE*-۲۰۱۸-۰۲۹۶ است که از طریق ارسال یک درخواست *HTTP* دستکاری شده منجر به راه‌اندازی مجدد دستگاه هدف توسط مهاجم احرازهویت نشده با دسترسی راه دور می‌شود.

شرکت سیسکو بار دیگر هشداری را در خصوص این آسیب‌پذیری منتشر کرده است.

یک مهاجم می‌تواند از این نقص برای مشاهده اطلاعات حساس سیستم بدون احرازهویت سوء استفاده کند. در دستگاه‌های آسیب‌پذیر، این امر از طریق تکنیک‌های پیمایش مسیر قابل دستیابی است.

اولین تلاش‌ها برای سوءاستفاده از این آسیب‌پذیری بلافاصله پس از افشای اولیه این نقص توسط سیسکو و انتشار وصله برای محصولات تحت تأثیر انجام شدند. در آن زمان، مهاجمین از این آسیب‌پذیری برای ایجاد وضعیت *DoS* بهره‌برداری کردند.

سیسکو به کاربران *ASA* و *Firepower* توصیه کرد تا نسخه‌ای که به *CVE*-۲۰۱۸-۰۲۹۶ آسیب‌پذیری نیست را مورد استفاده قرار دهند.

سیسکو راه‌کار بررسی آسیب‌پذیر بودن محصول مورد نظر را در توصیه منتشر شده ارائه کرده است. پژوهشگران امنیتی سیسکو هشدار داده‌اند که با وجود قدیمی بودن این آسیب‌پذیری، همچنان تهدیدی در قبال حملات *DoS* و افشا اطلاعات محسوب می‌شود.

هشدار مایکروسافت در خصوص آسیب‌پذیری روز صفر در مرورگر IE

شرکت مایکروسافت یک اطلاعیه امنیتی را منتشر کرده که حاوی اقدامات کاهشی در خصوص یک آسیب‌پذیری روز صفر اجرای کد از راه دور در مرورگر *Internet Explorer* است. به گفته مایکروسافت، حملات هدفمند محدودی در حال حاضر در حال هدف قرار دادن این آسیب‌پذیری هستند .

آسیب‌پذیری اجرای کد از راه دور موجود در مرورگر *Internet Explorer*، با شناسه *CVE*-۲۰۲۰-۰۶۷۴، در نحوه مدیریت اشیا در حافظه توسط موتور این مرورگر وجود دارد. آسیب‌پذیری می‌تواند باعث خرابی حافظه شود، به گونه‌ای که برای مهاجم امکان اجرای کد دلخواه در سطح دسترسی کاربر قربانی فراهم می‌شود.

از آنجایی که وصله‌ای برای این نقص وجود ندارد، مایکروسافت اعلام کرده که در حال کار بر روی یک اصلاحیه است که احتمالا به عنوان یک به‌روزرسانی امنیتی خارج از برنامه منتشر شود.

مهاجمی که با موفقیت از این نقص امنیتی بهره‌برداری کند، می‌تواند سطح دسترسی کاربری که در سیستم وارد شده است را بدست آورد. در صورتی که کاربر با سطح دسترسی ادمین وارد سیستم شده باشد، مهاجم می‌تواند کنترل کامل سیستم را بدست آورد و اقداماتی چون نصب برنامه‌ها، دستکاری داده‌ها یا ایجاد کاربر با سطح دسترسی کامل را انجام دهد.

به گفته مایکروسافت، در یک سناریوی حمله مبتنی بر وب، مهاجم می‌تواند یک وب‌سایت دستکاری شده را ایجاد کند که برای سوءاستفاده از این آسیب‌پذیری از طریق *Internet Explorer* طراحی شده باشد. مهاجم در ادامه کاربر را با روش‌های مهندسی اجتماعی مانند ارسال ایمیل، به مشاهده وب‌سایت مخرب وادار می‌کند.

باج افزار

انتشار نسخه جدید بدافزار سارق گذرواژه Predator the Thief

نسخه جدیدی از بدافزار *Predator the Thief*، تحت شماره ۳.۳.٤، منتشر شده است که با افزودن ویژگی‌های جدید به مهاجمین سایبری امکان انجام حملات کارآمدتر، مخفیانه‌تر و پرسودتر را فراهم می‌کند.

بدافزار *Predator the Thief* قادر به سرقت نام‌های کاربری، گذرواژه، داده‌های مرورگر و محتویات کیف پول رمزارزها و همچنین عکس‌برداری با استفاده از وب کم قربانی است. این بدافزار معمولا در فروم‌های گفتگوی زیرزمینی خرید و فروش می‌شود.

بدافزار *Predator the Thief* بطور مرتب با قابلیت‌های جدید به روز می‌شود. در نسخه جدید، از اسناد فیشینگ جدید مانند صورت‌حساب‌های مالی برای فریب قربانیان استفاده شده است. همچنین، در این نسخه از ترفندهای بیشتری برای جلوگیری از شناسایی و تحلیل بهره‌برداری شده است. بدافزار در نسخه جدید خود مجهز به یک *shellcode* است که هر پنج ثانیه یکبار وجود دیباگرها و سندباکس‌ها را بررسی می‌کند. پژوهشگران همچنین اشاره کردند که پیکربندی سرور فرمان و کنترل اکنون پیچیده‌تر از نسخه‌های قبلی است و از رمزگذاری در این ارتباط استفاده می‌شود. این مورد نیز نمونه دیگری از سخت‌تر شدن تحلیل بدافزار است. از امکانات دیگر اضافه شده به این نسخه، قابلیت‌های اجرای بدون فایل است.

برای محافظت در برابر حملات *Predator the Thief*، پژوهشگرها توصیه کرده‌اند که ماکروها بطور پیش‌فرض غیرفعال شوند و کاربران در مورد خطرات فعال‌سازی آن‌ها آموزش ببینند. اطمینان از به روز بودن سیستم‌عامل و نرم‌افزارها نیز می‌تواند به جلوگیری از حملات بدافزاری کمک کند.

Faketoken

تروجان موبایلی تمام عیار

یکی از تروجان‌های موبایلی که به عنوان یکی از خطرناک‌ترین تروجان‌های بانکی شناخته می‌شود، تروجان بانکی *Faketoken* است. این بدافزار در گذشته به همراه تروجان‌های دسکتاپی یافت می‌شد که به منظور سرقت اطلاعات احرازهویت، تلاش برای برداخت وجه از حساب قربانی و سرقت گذرواژه‌های یک‌بار مصرف، به سیستم قربانی نفوذ می‌کرد.

در نسخه جدید، *Faketoken* می‌تواند بدون وابستگی به سایر تروجان‌ها به سرقت پول اقدام و با استفاده از صفحات ورود فیشینگ، قربانیان کاربران تلفن همراه را وادار به ارائه اطلاعات احرازهویت یا اطلاعات بانکی خود کند.

علاوه بر این، عملکرد باج‌افزاری این بدافزار نیز بهبود یافته است. درصورتی که *Faketoken* به یک دستگاه تلفن همراه با سیستم‌عامل اندروید آسیب‌پذیر متقل شود، قادر به قفل صفحه دستگاه، رمزگذاری فایل‌ها و تقاضای باج خواهد بود.

تاکنون، این تروجان به عنوان یک تهدید بانکی جدی به حساب می‌رفت که بر سرقت اطلاعات و دریافت باج متمرکز شده بود، دسترسی به بخش پیامک تلفن همراه یکی از قابلیت‌های جدید *Faketoken* است.

تروجان‌های موبایلی، بدلیل دستیابی به کدهای احراز هویت دومرحله‌ای و پیامک‌های تایید، نیاز به دسترسی به بخش *SMS* دستگاه هدف را دارند. علاوه بر این، ارسال پیامک توسط تروجان می‌تواند باعث تحمیل هزینه اضافی به قربانی شود.

عدم نصب برنامه‌های موبایل از فروشگاه‌های غیررسمی و منابع نامعتبر و همچنین عدم کلیک روی لینک‌های مشکوک در پیام‌ها، از راهکارهایی است که برای جلوگیری از آلودگی به این بدافزار توصیه شده است.

مهمترین به‌روزرسانی‌های ماه جاری شرکت‌های تولید کننده سخت افـــزار و نرم افـــزار

شرکت *TP-Link* یک آسیب پذیری بحرانی را در روترهای مدل *Archer* کشف کرده است که مهاجم با بهره برداری از این آسیب پذیری می‌تواند رمز عبور *admin* را بدست آورد و سپس این روتر آسیب پذیر را از راه دور و از طریق *Telnet* کنترل کند.

بهره برداری موفق از این آسیب پذیری به مهاجم این اجازه را می‌دهد تا از راه دور کنترل کامل روتر را از طریق *Telnet* و در شبکه *LAN* به دست بگیرد. سپس به *FTP server* شبکه متصل شود.

مهاجم یک بسته *HTTP request* که حاوی یک رشته کاراکتر با اندازه بزرگتر از مقدار مجاز است را برای روتر آسیب پذیر ارسال می‌کند. با این کار، رمز عبور *admin* را با یک مقدار خالی جایگزین می‌کند. با اینکه اعتبار سنجی داخلی انجام می‌شود اما باز هم روتر فریب می‌خورد زیرا فقط هدر بسته *HTTP* را بررسی می‌کند. بنابراین مهاجمان از این طریق سرویس *httpd* روتر را فریب می‌دهند تا با استفاده از *tplinkwifi.net* درخواست را معتبر تشخیص دهد. حتی اگر *admin* واقعی روتر بتواند رمز عبور را تغییر دهد مهاجم می‌تواند دوباره آن را با درخواست *LAN/WAN/CGI* از بین ببرد و به روتر *login* کند.

مایکروسافت اولین به‌روزرسانی امنیتی سال ۲۰۲۰ خود را منتشر کرده که در آن ٤۹ آسیب‌پذیری شامل ۷ نقص بحرانی، ٤۱ نقص با درجه اهمیت مهم و ۱ نقص با درجه اهمیت متوسط رفع شده است. یکی از آسیب‌پذیری‌های بحرانی سیستم‌عامل ویندوز، کاربر را در معرض نفوذ و جاسوسی قرار می‌دهد و مهاجمین بهره‌برداری از آن را به زودی آغاز خواهند کرد.

مهمترین آسیب‌پذیری رفع شده در به‌روزرسانی‌های ماه ژانویه مایکروسافت، نقص *CVE-۲۰۲۰-۰٦۰۱* در (*Crypt۳۲*) *dll.CryptoAPI* است که ویندوز ۱۰، ویندوز سرور ۲۰۱٦ و ویندوز سرور ۲۰۱۹ را تحت تأثیر قرار می‌دهد. این نقص به مهاجم اجازه می‌دهد تا گواهی‌های دیجیتال را جعل کند یا حملات مرد میانی را انجام دهد. با سوء استفاده از این آسیب‌پذیری، که ارتباطات رمزگذاری شده *TLS* را نیز تحت تأثیر قرار می‌دهد، مهاجم می‌تواند اطلاعات محرمانه کاربر در اتصال به برنامه آسیب‌پذیر را رمزگشایی کند.

در وصله منتشر شده برای ماه ژانویه، سه آسیب‌پذیری در *Remote Desktop Gateway* ویندوز رفع شده است. دو مورد از این آسیب‌پذیری‌ها (*CVE-۲۰۲۰-۰٦۰۹* و *CVE-۲۰۲۰-۰٦۱۰*) به مهاجم احراز هویت نشده با دسترسی از راه دور امکان اجرای کد در سیستم آسیب‌پذیر را فراهم می‌کنند. آسیب‌پذیری سوم (*CVE-۲۰۲۰-۰٦۱۲*) منجر به ایجاد وضعیت منع سرویس در سیستم *RDP* ویندوز می‌شود و سرویس‌دهی آن را مختل می‌کند. این کار با ارسال درخواست‌های دستکاری شده توسط مهاجم انجام می‌شود.

اینتل یک آسیب‌پذیری در *Rapid Storage Technology* را برطرف کرده است که به یک مهاجم محلی اجازه می‌دهد امتیازات خود را به امتیاز سیستمی ارتقا دهد. *RST* یک برنامه مبتنی بر ویندوز در بسیاری از رایانه‌هایی است که از تراشه‌های *Intel* برای ارایه عملکرد و قابلیت اطمینان بیشتر هنگام استفاده از دیسک‌های *SATA* بهره می‌برند.

این نقص امنیتی می‌تواند برای دورزدن دفاع‌ها مورد سوءاستفاده قرار گیرد و از طریق بارگذاری یک *DLL* دلخواه امضانشده (*unsigned*) به فرایندی که با امتیازات سیستمی اجرا می‌شود به پایداری برسد. مهاجم برای سوءاستفاده از این آسیب‌پذیری نیاز به امتیازات مدیریتی در سیستم دارد.

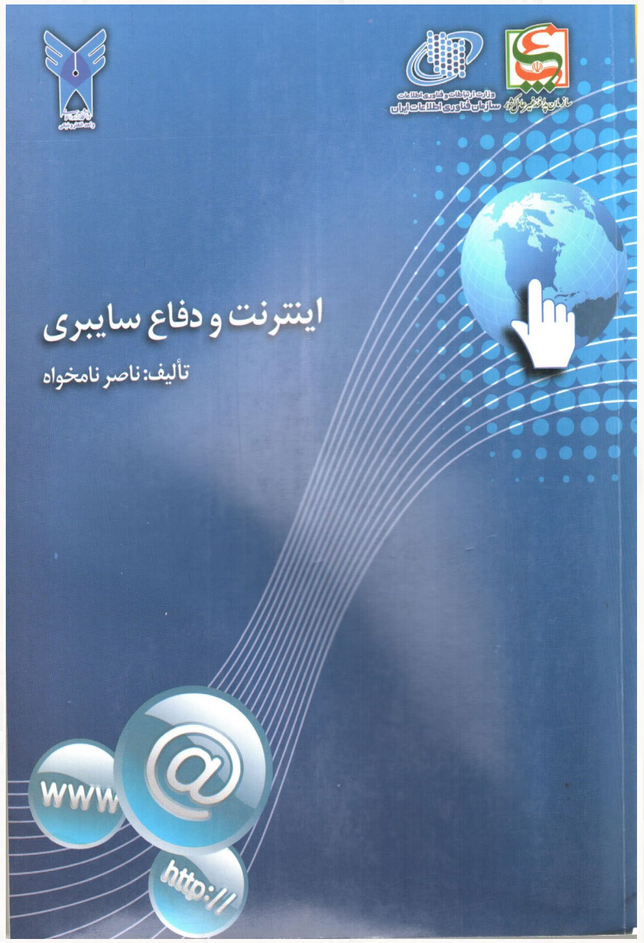
دلیل اصلی این آسیب‌پذیری این است که هیچ اعتبارسنجی امضا علیه فایل‌های *DLL* که سرویس *IAStorDataMgrSvc.exe* (یک فرایند مربوط به *Intel RST* که با امتیازات سیستمی امضا و اجرا می‌شود)، تلاش می‌کند بارگذاری کند، انجام نمی‌شود. از آنجاییکه این فایل‌ها وجود ندارند، یک مهاجم می‌تواند فایل‌های *DLL* دلخواه را جای دهد و این سرویس آن را بارگذاری خواهد کرد.

با سوءاستفاده از این مشکل، مهاجم می‌تواند یک خرابکاری را ضمن فرار از شناسایی‌شدن، بارگذاری و اجرا کند. علاوه بر این، این خرابکاری می‌تواند به صورت مداوم هر بار که این سرویس شروع به کار می‌کند، اجرا شود.

معرفی کتاب حوزه پدافند سایبری

در دهه‌های اخیر و بعد از انقلاب دیجیتالی در دنیا، شاهراه ارتباطی‌ای به نام اینترنت که ابتدا یک پروژه نظامی در وزارت دفاع آمریکا بود، ایجاد شده و کم کم به تمام نقاط تسری پیدا نموده و اکنون تبدیل به اصلی ترین و ارزان ترین ابزار ارتباطی بین تمام نقاط دنیا شده است. با توجه به مقرون به صرفه بودن برای تمام ساختارهای نیازمند به ارتباط با دیگران، اینترنت ضریب نفوذ بالایی را در بین جوامع مختلف کسب نموده است.

پس از کاربری های عادی، کم کم کاربران حرفه‌ای مانند دولت ها، ساختارهای عمومی و مراکز نظامی، علمی و فنی متمایل به استفاده از این مسیر ارتباطی برای گسترش فعالیت های خود شدند که در مدت زمان اندکی تعداد کاربران، از میزان محاسبه شده افزون‌تر گردید. با توجه به این که با گسترش علم و فناوری، امنیت کاهش پیدا می‌نماید، عوامل غیرمجاز به صرافت بهره برداری غیرمجاز از این ابزار برآمده و به انحاء مختلف تلاش در ابداع شیوه‌های نوین استفاده ضد امنیتی از این ابزار را آغاز کردند. امروزه اینترنت در بین اندیشمندان، نیروهای علمی و فنی و در بین عامه مردم، تبدیل به ابزاری ارزان قیمت برای بهره برداری جهت رفع نیازمندی‌های روزمره شده است.



با توجه به خطراتی که استفاده از این ابزار برای کاربران دارد، در این کتاب تلاش می‌گردد تا به صورت توصیفی، کاربردهای مختلف اینترنت، خطرات مربوطه و نیز شیوه‌های استفاده ایمن برای خوانندگان ترسیم گردیده و ضمن بیان اهداف استراتژی نظام سلطه، از ایجاد این بستر گسترده ارتباطی، خطرات واقعی آن برای خوانندگان گرامی بازگو گردد.

طرح‌های کسر خدمت سربازی

به اطلاع می‌رساند که سازمان پدافند غیرعامل کشور (مرکز مطالعات پدافند غیرعامل کشور و مرکز مطالعات فنی و مهندسی پایداری ملی کشور) برای دانش‌آموختگان و فارغ‌التحصیلان مقاطع کارشناسی ارشد و دکتری طرح‌هایی برای کسر خدمت سربازی و نخبگی (جایگزین خدمت سربازی) در نظر گرفته است. علاقمندان می‌توانند علاوه بر مراجعه به وب‌سایت‌های مربوطه با مراجعه به اداره کل پدافند غیرعامل استانداری آذربایجان شرقی از روند ثبت‌نام مطلع شوند.

وب سایت مرکز مطالعات فنی و مهندسی پایداری ملی کشور: http://www.mafpa.ir

وب سایت مرکز مطالعات پدافند غیرعامل کشور: http://www.pdrc.ir

سایت های مرتبط با پدافند غیرعامل

وب سایت پایداری ملی
http://www.paydarymelli.ir

مرکز مطالعات پدافند غیرعامل
http://www.pdrc.ir

استانداری آذربایجان شرقی - پدافند غیرعامل
http://www.ostan-as.gov.ir/Page/۴۲/

پلیس فتا
http://www.cyberpolice.ir

مرکز مطالعات فنی و مهندسی پایداری ملی
http://www.mafpa.ir