به‌نام خدا

مؤسسه فرهنگی هنری
دیباگران تهران

مهندسی پدافند غیرعامل در فناوری اطلاعات

(امنیت به روش پیشگیری الکترونیکی)

مؤلفان
حمید دوست محمدیان
مریم سادات فاضلی

مهندسی پدافند غیرعامل در فناوری اطلاعات (امنیت به روش پیشگیری الکترونیکی)

مؤلفان: حمید دوست‌محمدیان - مریم سادات فاضلی

ناشر: مؤسسه فرهنگی هنری دیباگران تهران

حروفچینی و صفحه‌آرایی: مجتمع فنی تهران

طرح روی جلد: مجتمع فنی تهران

چاپ: نگین

نوبت چاپ: اول

تاریخ نشر: مرداد ماه ۱۳۹۲

تیراژ: ۵۰۰ نسخه

قیمت: ۱۸۰۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۱۲۴-۲۷۰-۰

ISBN: 978-600-124-270-0

سرشناسه: دوست‌محمدیان، حمید، ۱۳۵۶-

عنوان و نام پدیدآور: مهندسی پدافند غیرعامل در فناوری اطلاعات (امنیت به روش پیشگیری الکترونیکی)/ مؤلفان حمید دوست‌محمدیان، مریم سادات فاضلی.

مشخصات نشر: تهران: مؤسسه فرهنگی هنری دیباگران تهران، ۱۳۹۲.

مشخصات ظاهری: ۴۲۰ ص.: مصور.

شابک: 978-600-124-270-0

وضعیت فهرست‌نویسی: فیپا

موضوع: شبکه‌های کامپیوتری -- اقدامات تامینی

موضوع: پایگاه‌های اطلاعاتی -- امنیت

موضوع: فاضلی، مریم‌سادات، ۱۳۶۶-

رده‌بندی کنگره: ۱۳۹۲ ۹م۹د/۵۹/TK۵۱۰۵

رده‌بندی دیویی: ۰۰۵/۸

شماره کتابشناسی ملی: ۳۱۸۶۶۴۳

نشانی دفتر مرکزی: تهران، سعادت آباد، میدان کاج، خ سرو شرقی، روبه‌روی خ علامه، پلاک ۴۹

صندوق پستی: ۱۴۳۳۵/۹۴۳ وب سایت: **dibagaran.mft.info**

نشانی واحد فروش: تهران، میدان انقلاب، خ کارگر جنوبی، قبل از چهارراه لبافی‌نژاد، پلاک ۱۲۵۱

تلفن: ۱۲-۲۲۰۸۵۱۱۱ کد پستی: ۱۳۱۴۹۸۳۱۸۵

پست الکترونیکی: **bookmarket@mftmail.com** فروش اینترنتی: **www.mftshop.com**

فهرست مطالب

فصل چهارم: اصول و مبانی امنیت داده‌ها و اطلاعات

فصل پنجم: مبانی امنیت شبکه

فصل ششم: پدافند غیرعامل در سیستم عامل و مسیریاب‌ها

فصل هفتم: پدافند غیرعامل در حوزه سامانه مدیریت تهدید یکپارچه

فصل هشتم: مانور فناوری اطلاعات (مدیریت بحران فناوری اطلاعات)

فصل نهم: پدافند غیرعامل در فناوری اطلاعات

فصل دهم: مهندسی اجتماعی

فصل یازدهم: چالش‌ها و ارائه راهکار

پیوست ۱:آشنایی با بالاترین مخاطرات امنیتی وب‌گاه‌ها

پیوست ۲: رایانش ابری

مقدمه ناشر

خط مشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرضه کتاب‌هایی است که بتواند خواسته‌های به روز جامعه فرهنگی و علمی کشور را تا حد امکان پوشش دهد

حمد و سپاس ایزد منان را که با الطاف بیکران خود این توفیق را به ما ارزانی داشت تا بتوانیم در راه ارتقای دانش عمومی و فرهنگ این مرز و بوم در زمینه چاپ و نشر کتب علمی دانشگاهی، علوم پایه و به ویژه علوم کامپیوتر و انفورماتیک گام‌هایی هر چند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم. گستردگی علوم و توسعه روزافزون آن، شرایطی را به وجود آورده که هر روز شاهد تحولات اساسی چشمگیری در سطح جهان هستیم. این گسترش و توسعه نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی‌ترین و راحت‌ترین راه دستیابی به اطلاعات و اطلاع‌رسانی، بیش از پیش روشن می‌نماید. در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری جمعی از اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران، محققان و نیز پرسنل ورزیده و ماهر در زمینه امور نشر درصدد هستند تا با تلاش‌های مستمر خود برای رفع کمبودها و نیازهای موجود، منابعی پربار، معتبر و با کیفیت مناسب در اختیار علاقه‌مندان قرار دهند.

کتابی که در دست دارید با همت "**جناب آقای حمید دوست محمدیان و سرکارخانم مریم سادات فاضلی**"و تلاش جمعی از همکاران انتشارات میسر گشته که شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

ویرایش و صفحه‌آرایی کامپیوتری: معصومه گنجی‌پور

ویراستاری: شیوا غمگسار، انسیه پارسافر

طراح جلد: مینا دیده‌بان

ناظر چاپ: منصور عزیزی

در خاتمه ضمن سپاسگزاری از شما دانش‌پژوه گرامی درخواست می‌نماید با مراجعه به **آدرس dibagaran.mft.info** (ارتباط با مشتری) فرم نظرسنجی را برای کتابی که در دست دارید تکمیل و ارسال نموده، انتشارات دیباگران تهران را که جلب رضایت و وفاداری مشتریان را هدف خود می‌داند، یاری فرمایید.

امیدواریم همواره بهتر از گذشته خدمات و محصولات خود را تقدیم حضورتان نماییم.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران

publishing@mftmail.com

مقدمه مؤلفان

تقدیم به:
مادرمهربانم و پدر بزرگوارم و
خواهر دوست داشتنیم و برادران عزیزم
که با نهایت عشق مرا پشتیبانی کردند.
مریم سادات فاضلی

شکی نیست که امپراطوری‌های آینده امپراطوری اندیشه خواهد بود. «چرچیل»
لغت غیر ممکن را باید از قاموس‌ها محو کرد. «ناپلئون بناپارت»

سپاس بیکران پروردگار را که به انسان قدرت اندیشیدن بخشید تا به یاری این موهبت راه ترقی و تعالی را بپیماید و امید به این که عنایت الهی شامل حال ما باشد تا با دانش اندک خود در خدمت کشور عزیزمان باشیم.

امروزه جنگ و کشمکش به صورت خواسته یا ناخواسته با زندگی و حیات جوامع بشری آمیخته شده است. در نیمه اول قرن بیستم، جنگ جهانی دوم عامل اصلی طراحی و ساخت اولین کامپیوتر به سبک امروزی و در نیمه دوم این قرن جنگ سرد دلیل اصلی طراحی و راه‌اندازی شبکه ارتباطی مبتنی بر کامپیوترها به نام آرپانت بود. پیش از سال ۱۹۷۰ در انتهای موج دوم (عصر صنعتی) اطلاعات، علم و دانش عامل پیشرفت و توسعه فناوری‌ها و بعد از سال ۱۹۷۰ یعنی در آغاز موج سوم (عصر اطلاعات یا فراصنعتی) فناوری‌ها عامل اصلی پیشرفت و توسعه سریع اطلاعات، علم و دانش بوده است.

مشاهده می‌گرددکه عناصر جنگ، دانش، علوم و فناوری‌ها خصوصاً فناوری اطلاعات همواره در کنار هم بوده و بر هم اثر متقابل گذاشته‌اند.

از ابتدای زندگی بشری تاکنون فقط ۲۶۹ سال بدون جنگ بوده است و تجارب حاصله از جنگ‌های گذشته مؤید این نظر است که کشور مهاجم جهت در هم شکستن اراده ملت و توان اقتصادی، نظامی و سیاسی کشور مورد تهاجم و با اتخاذ استراتژی انهدام مراکز ثقل، توجه خود را صرف بمباران و انهدام مراکز حیاتی و حساس می‌نماید. انجام اقدامات دفاع غیرعامل در جنگ‌های نامتقارن امروزی در جهت مقابله با تهاجمات خصمانه و تقلیل خسارات ناشی از حملات هوایی، زمینی و دریایی کشور مهاجم، موضوعی بنیادی است.

اکنون در اوج رشد عصر مجازی قرار داریم که در آن شاهد وقوع جنگ‌های موازی (اطلاعاتی، روانی، نرم و سایبری) هستیم. با رشد فناوری رایانه‌ای و ذخیره‌سازی اطلاعات بر روی آن‌ها حملات سایبری برای ربودن اطلاعات یا تغییر آن به‌طور چشم‌گیری افزایش یافته است و به عنوان نمونه می‌توان به کرم صنعتی Stuxnet اشاره کرد که سیستم‌های صنعتی کشور خصوصاً سیستم‌های مرکز اتمی ایران را نشانه گرفت و هدف آن دستیابی و آسیب به اطلاعات صنعتی ایران بود. بنابراین موضوع مهندسی پدافند غیرعامل در

فناوری اطلاعات و رعایت اصول آن به منظور امنیت، ایمنی و پایداری زیرساخت‌های حیاتی، حساس و مهم کشور در مقابل تهدیدات سایبری دشمن یک بحث حیاتی است.

این کتاب علاوه بر تأکید به رعایت اصول پدافند غیرعامل در فناوری اطلاعات با ارائه راهکارهایی به پیشبرد آن در حوزه جنگ‌های نوین خصوصاً جنگ الکترونیک، نرم و اطلاعات دیجیتال پرداخته است.

کتاب حاضر کوشیده است تا با بیان اصول پدافند غیرعاملی در حوزه جنگ‌های نوین در دنیای امروز با تأمین اصولی امنیت مبادلات اطلاعات الکترونیکی در فضای مجازی و شبکه‌های کامپیوتری به روش پیشگیری الکترونیکی تا حدودی امکان ایجاد بستری امن در فضای مبادلات الکترونیکی را مهیا سازد، تا در زمان‌های مخاطره آمیز (جنگ‌های الکترونیک)، اطلاعات حیاتی مورد دستبرد قرار نگیرد.

در آخر از تمام عزیزانی که ما را در تهیه این کتاب یاری کرده‌اند تشکر و قدردانی می‌نماییم و توفیقات روزافزون از خداوند متعال برای شما عزیزان خواستاریم.

حمید دوست‌محمدیان
Hdmohamadian@ind.just.ac.ir
مریم سادات فاضلی
m.fazeli303@gmail.com

پیشگفتار

با توجه به اهمیت فناوری اطلاعات در عصر حاضر و رشد سریع و در عین حال نامتوازن ساختار فناوری اطلاعات این بستر به یکی از نقاط بالقوه آسیب‌پذیر و خطرناک در جهان بدل شده است که ضرورت توجه و پرداخت سریع و در عین حال نظام‌مند، معقول و هدفمند به منظور مصون‌سازی این بستر از تهدیدات موجود در جهت حفظ امنیت ملی و حریم شخصی شهروندان در فضای جنگ و مخاصمات امروز بین المللی را می‌طلبد.

دفاع غیرعامل در واقع مجموعه تمهیدات، اقدامات و طرح‌هایی است که با استفاده از ابزار، شرایط و حتی‌المقدور بدون نیاز به نیروی انسانی به صورت خود اتکا صورت گیرد چنین اقداماتی از یک سو توان دفاعی مجموعه را در زمان بحران افزایش داده و از سوی دیگر پیامدهای بحران را کاهش و امکان بازسازی مناطق آسیب دیده را با کمترین هزینه فراهم می‌سازد. در حقیقت طرح‌های پدافند غیرعامل قبل از انجام مراحل تهاجم و در زمان صلح تهیه و اجرا می‌گردند. با توجه به فرصتی که در زمان صلح جهت تهیه چنین طرح‌هایی فراهم می‌گردد ضروری است این قبیل تمهیدات در متن طراحی‌ها لحاظ گردند.

یکی از مأموریت‌های مهم نظام جمهوری اسلامی ایران صیانت از میهن عزیزمان و ***زیرساخت‌های***[1] حیاتی کشور، مخصوصاً زیرساخت‌های فناوری‌اطلاعات در مقابل حملات احتمالی متجاوزان است.

هم زمان با ظهور و گسترش استفاده از فناوری اطلاعات و ارتباطات، برقراری امنیت در فضای سایبر به عنوان یکی از مسائل اصلی در این حوزه مطرح شده است. افزایش وابستگی فعالیت دولت‌ها زیرساخت‌های جدیدی را پدید آورده است که ممکن است موجب نفوذ و ایراد ضربه یا از کار انداختن کامل آن‌ها شود. با توجه به سرعت گسترش حملات در فضای سایبر و تنوع آن‌ها، تأمین امنیت این حوزه تنها با استفاده از آخرین فناوری‌ها و به روز نمودن روش‌ها میسر است.

در این میان، بخش قابل توجهی از بار فنی و مسئولیتی برقراری امنیت بر عهده کارشناسان امنیت شبکه سازمان‌ها و شرکت‌ها است. این کارشناسان باید با پیاده‌سازی مکانیزم‌ها و استفاده از تجهیزات امنیتی مختلف موجبات برقراری امنیت، ایمنی و پایداری داده‌ها و زیرساخت سازمان متبوع خود را فراهم آورند.

در گذشته، اغلب کارشناسان امنیت با مشکلات زیادی در استفاده از تجهیزات امنیتی مواجه بوده‌اند از جمله این مشکلات می‌توان به عدم سازگاری دستگاه‌ها با یکدیگر و عدم وجود دستگاهی برای تحلیل گزارشات تولید شده توسط تجهیزات مختلف اشاره نمود.

از این رو متخصصین امنیت شبکه، مجتمع کردن دستگاه‌های متفاوت و حذف وظایف موازی آن‌ها را به عنوان یک راه حل مناسب جهت حذف مشکلات موجود و ایجاد یک نگاه جامع امنیتی مطرح نمودند.

1- Infrastructures

نتیجه این تفکر به ساخت و عرضه محصول « ***سامانه مدیریت تهدید یکپارچه***[1]» و توسعه آن به وسیله شرکت‌های مطرح فعال در این حوزه منتهی گردیده است که در این پروژه به معرفی آن پرداخته شده است.

حفظ امنیت اطلاعات ، یکپارچگی و در دسترس بودن سیستم‌های اطلاعاتی برای کار، تجارت و جامعه ضروری و حتی حیاتی به نظر می‌رسد. اطلاعات می‌تواند در ساختار یک فرم، نقشه یا دستورالعمل باشدکه توسط افراد مختلف مطالعه و تفسیر می‌شود یا در یک ماشین به طور اتوماتیک پردازش و نگهداری می‌شود. این اطلاعات حتی ممکن است در حافظه ذهنی افراد ذخیره و نگهداری شود ولی به هر جهت برای بقای کسب و کار لازم و ضروری هستند. سیستم مدیریت امنیت اطلاعات به حفاظت این اطلاعات ارزشمند سازمان می‌پردازد، تا از تهدیدهایی که ممکن است آن‌ها را عمداً یا سهواً به خطر بیندازد محافظت کرده یا شدت خطر را کاهش دهد. آمار نشان می‌دهد که سازمان‌ها مبالغ هنگفتی را بابت از دست دادن اطلاعات یا در دسترس نبودن آن‌ها می‌پردازند. روند رشد سیستم‌های اطلاعاتی و وابستگی بیش از پیش به اطلاعات، ایجاد سیستم مدیریت امنیت اطلاعات را درکشور ما نیز همانند سایرکشورهای جهان ضروری می‌نماید. همچنین با تدوین سند راهبرد ملی امنیت فضای تبادل اطلاعات کشور و ابلاغ بخشنامه معاون اول ریاست جمهوری، خطاب به کلیه سازمان‌های دولتی و وابسته به دولت، لزوم ارائه برنامه عملیاتی امنیت فضای تبادل اطلاعات به سازمان مدیریت و برنامه‌ریزی کشور مطرح گردیده است.

پدافند غیرعامل در حوزه فناوری اطلاعات و ارتباطات و جنگ سایبر به منظور امنیت، ایمنی و پایدارسازی زیرساخت‌های حیاتی کشور در مقابل تهدیدات دشمن از ناحیه فناوری‌اطلاعات و ارتباطات شکل گرفته است.

اهداف کلان راهبردی[2] **پدافند غیرعامل حوزه فناوری اطلاعات و ارتباطات عبارتند از:**

- توسعه و تعمیق فرهنگ و دانش پدافند غیرعامل در جامعه تخصصی فناوری اطلاعات و ارتباطات
- نهادینه‌سازی امنیت، ایمنی و پایداری در طرح‌های توسعه‌ای مرتبط با فناوری اطلاعات و ارتباطات
- کمک به توسعه پدافندغیرعامل در سایر بخش‌های زیر ساختی کشور

الزامات و ویژگی‌های دفاع مؤثر در ***جنگ‌های نسل ششم***[3] بر اساس اظهارنظر کارشناسان، ضرورت ***برنامه‌ریزی***[4] وآغاز طرح‌های جامع دفاع قبل از شروع درگیری‌های آشکار، توسعه همه جانبه تدابیر

1- Unified Threat Management (UTM)
2- Strategic Goal
3- The Sixth-Generation Wars
4- Planning

دفاعی به منظور افزایش ضریب پایداری ملی، گسترش طرح‌های دفاعی در سطح تمامی نقاط هدف در جغرافیای کشور و حوزه سرزمینی ملی به روش دفاع نقطه‌ای است. تأکید ویژه بر دفاع غیرعامل، اتکا به ایمان، هوشیاری، روحیه و توان دفاعی مردمی، توجه و تأکید بر راهبرد و اصول دفاع نامتقارن، شناسایی و رفع ضعف‌های ذاتی فناوری‌ها و آسیب‌پذیری‌های ساختاری و سیستمی، تمرکز بر اولویت‌های دفاعی و تمرکز تلاش‌ها بر ارتقای روحیه و اراده ملی برای دفاع از دیگر الزامات و ویژگی‌های دفاع مؤثر در جنگ‌های نسل ششم است.

دانش «پدافند غیرعامل» در حوزه ***فاوا***[1] یکی از دانش‌های روز است و موضوعات آن به صورت طبقه‌بندی شده به سختی قابل انتشار است. پدافند غیرعامل به عنوان یکی از مؤثرترین و پایدارترین روش‌های دفاع در مقابل تهدیدات همواره مدنظر اکثر کشورهای جهان می‌باشد. کشورهایی مانند آمریکا و روسیه، با وجود برخورداری از توان نظامی، به این موضوع به صورت ویژه نگریستند. حتی کشوری مانند سوئیس با وجود ***بی‌طرفی***[2] در دو جنگ جهانی و مواجه نبودن با تهدید، به این موضوع توجه بسیاری دارد.

پیشرفت سریع علوم رایانه و فناوری‌های ارتباطی و اطلاعاتی نوین و پیوند تنگاتنگ این علوم با همه شئونات زندگی بشر سبب وابستگی شدید کشورها و ملت‌ها به فناوری اطلاعات و ارتباطات، جهت اداره امور جامعه شده است، به گونه‌ای که امروزه حتی تصور ادامه زندگی بدون بهره‌گیری از این دانش و فناوری محال به نظر می‌رسد.

به تناسب افزایش ارتباطات و پیشرفت فناوری، مخاطرات پیش رو نیز افزایش یافته است از این رو توجه به ارتقای ضریب امنیت، ایمنی و پایداری شبکه‌های رایانه‌ای و تمامی تجهیزات آن باید بیش از پیش مورد توجه قرار گیرد. یکی از اجزای اصلی شبکه، مسیریاب است. تأمین امنیت مسیریابی و مسیریاب امن، نقش به سزایی در حفظ امنیت شبکه ایفا می‌نماید.

یک مسیریاب، گره‌ای از شبکه است که نقطه یا گره بعدی شبکه را که باید بسته به سمت آن ارسال شود و در نهایت به مقصد برسد، مشخص می‌کند. هر مسیریاب حداقل به دو شبکه متصل است و براساس درک خود از وضعیت شبکه‌های مرتبط، در مورد ارسال بسته‌های اطلاعاتی تصمیم می‌گیرد.

از دیگر موضوعات حائز اهمیت در یک شبکه ارتباطی، پایداری آن است. با توجه به سرعت تغییرات و اهمیت دسترس‌پذیری در حوزه شبکه‌های اطلاعاتی و ارتباطی، از نکات مهم در حفظ پایداری سامانه‌های این حوزه، مسائل مربوط به پشتیبانی است.

۱- فناوری اطلاعات و ارتباطات

۲- البته تحقیقات و بررسی‌های دقیق‌تر نشان داده است که کشور سوئیس خیلی هم بی‌طرف نبوده است و حتی یکی از تأمین کنندگان اصلی تسلیحات نظامی برای آلمان‌ها در جنگ جهانی دوم بوده و بانک‌های سوئیس بیشترین منافع مالی را از جنگ جهانی دوم برده‌اند.

شبکه‌های ارتباطات سیار به عنوان یکی از زیرساخت‌های مهم کشور، بستری برای بهره‌برداری‌های گوناگون ارتباطی اطلاع رسانی، تجاری، سیاسی و فرهنگی در کشور است و روز به روز بر کاربردهای آن افزوده می‌شود. عدم توجه به امنیت شبکه‌های ارتباطی سیار در کنار مزایای غیر قابل انکار حاصل از آن، می‌تواند معضلات مهم و غیر قابل جبرانی را در سطح کشور ایجاد نماید.

شناخت جامع مشکلات امنیتی حاصل از شبکه‌های ارتباطات سیار و اقدام جهت مرتفع نمودن معضلات عمده این حوزه نقش قابل ملاحظه‌ای در ارتقای امنیت، ایمنی و پایداری زیرساخت ارتباطات سیار ایفا می‌نماید و گاهی در راستای تأمین اهداف پدافند غیرعامل در این خصوص به شمار می‌آید.

درحالی که بسیاری از شرکت‌ها برای مقابله با هکرها از ابزار دفاع تکنیکی مانند فایروال‌ها و سرورهای مقاوم در برابر حمله اینترنت و احتمالاً مقاوم سازی شبکه داخلی شرکت استفاده می‌کنند، بسیاری از آن‌ها از این موضوع غافلند که «مهمات هکرها» شامل ابزارهای بسیار ساده از جمله تلفن و پست الکترونیکی نیز هست. تلاش هکرها برای دست اندازی به «بخش انسانی امنیت» نشان‌دهنده یک ضعف قطعی امنیتی می‌باشد. در واقع بسیاری از شرکت‌ها از این ضعف تا زمانی که با آن‌ها مواجه نشوند، غافلند.

مهندسی اجتماعی یک خطر بالقوه برای شرکت‌ها می‌باشد که معمولاً کوچک شمرده می‌شود و می‌توان آن را توسط آموزش، سیاست‌گذاری و رویه‌های اجرایی تضمین نمود. در حالی که شرکت‌ها هزینه زیادی را برای مقابله با آن صرف می‌کنند، تنها راه حصول اطمینان از اثر بخشی این کارها، ممیزی می‌باشد. به هر حال قبل از ممیزی باید راه‌های حمله و دفاع مهندسی اجتماعی را شناخت و سپس می‌توان برای ممیزی آن برنامه‌ریزی نمود.

مهندسی اجتماعی، تکنیکی است که بر فریب دادن مردم استوار است. در این تکنیک شما با انسان‌ها سر و کار دارید نه با کامپیوترها. حال اگر مثلاً یک کاربر را گول بزنید، می‌توانید اطلاعات او را مثل پسورد و ... را به دست بیاورید که نمونه‌ای است از Client Hacking یا هک کاربر و اگه مدیر شبکه یک سایت را گول بزنید و سایت را هک کنید، نمونه‌ای است از Server Hacking. پس با مهندسی اجتماعی می‌توان هم کلاینت و هم سرور را هک کرد.

با توجه به اهمیت فناوری اطلاعات در عصر حاضر و رشد سریع و در عین حال نامتوازن ساختار IT، این بستر به یکی از نقاط بالقوه آسیب پذیر وخطرناک در جهان بدل شده است؛ که ضرورت توجه و پرداخت سریع و در عین حال نظام‌مند، معقول و هدفمند به منظور مصون سازی این بستر از تهدیدات موجود در جهت حفظ امنیت ملی و حریم شخصی شهروندان در فضای جنگ و مخاصمات امروز بین المللی را می‌طلبد.

دفاع غیرعامل در واقع مجموعه تمهیدات، اقدامات و طرح‌هایی است که با استفاده از ابزار، شرایط و حتی‌المقدور بدون نیاز به نیروی انسانی به صورت خود اتکا صورت گیرد چنین اقداماتی از یک سو توان

دفاعی مجموعه در زمان بحران را افزایش داده و از سوی دیگر پیامدهای بحران را کاهش داده و امکان بازسازی مناطق آسیب دیده را با کمترین هزینه فراهم می‌سازد. در حقیقت طرح‌های پدافند غیرعامل قبل از انجام مراحل تهاجم و در زمان صلح تهیه و اجرا می‌گردند. با توجه به فرصتی که در زمان صلح جهت تهیه چنین طرح‌هایی فراهم می‌گردد، ضروری است این قبیل تمهیدات در متن طراحی‌ها لحاظ شوند.