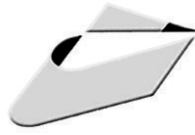


به نام خدا



مؤسسه فرهنگی هنری
دیبگران تهران

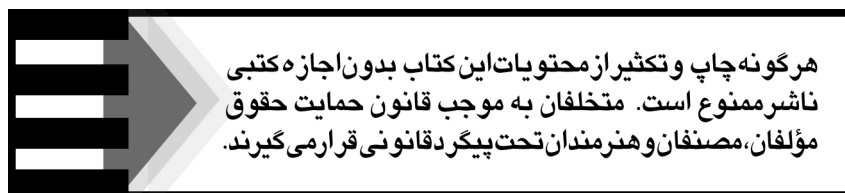
مهندسی پدافند غیرعامل در فناوری اطلاعات

(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 دوست محمدیان - مریم سادات فاضلی

ناشر: مؤسسه فرهنگی هنری دیباگران تهران

حروفچینی و صفحه آرایی: مجتمع فنی تهران

طرح روی جلد: مجتمع فنی تهران

چاپ: نگین

نویت 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: دوست محمدیان، حمید، ۱۳۵۶-
عنوان و نام پدیدآور: مهندسی پدافند غیرعامل در فناوری اطلاعات (امنیت به روش
پیشگیری الکترونیکی) / مؤلفان حمید دوست محمدیان، مریم سادات فاضلی.
مشخصات نشر: تهران: مؤسسه فرهنگی هنری دیباگران تهران، ۱۳۹۲.
مشخصات ظاهری: ۴۲۰ ص: مصور.
شابک: 978-600-124-270-0
وضعیت فهرست نویسی: فیپا
موضوع: شبکه های کامپیوتری -- اقدامات تأمینی
موضوع: پایگاه های اطلاعاتی -- امنیت
موضوع: فاضلی، مریم سادات، ۱۳۶۶-
رده بندی کنگره: ۱۳۹۲ م۹/۵۹/۵۹/TK۵۱۰۵
رده بندی دیویی: ۰۰۵/۸
شماره کتابشناسی ملی: ۳۱۸۶۶۴۳

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

وب سایت: dibagaran.mft.info

صندوق پستی: ۱۴۳۳۵/۹۴۳

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

کد پستی: ۱۳۱۴۹۸۳۱۸۵

تلفن: ۲۲۰۸۵۱۱۱-۱۲

فروش اینترنتی: www.mftshop.com

پست الکترونیکی: bookmarket@mftmail.com

فهرست مطالب

مقدمه ناشر ۹

مقدمه مؤلفان ۱۰

پیشگفتار ۱۲

فصل اول: اصول و مبانی پدافند غیر عامل

۱-۱ پدافند ۱۷

۱-۲ پدافند عامل ۱۷

۱-۳ پدافند غیر عامل ۱۷

۱-۴ تاریخچه پدافند غیر عامل ۱۹

۱-۵ اهداف پدافند غیر عامل ۲۱

۱-۶ نتیجه به کارگیری اقدامات پدافند غیر عامل ۲۱

۱-۷ حوزه‌ها و محورهای اساسی پدافند غیر عامل ۲۲

۱-۸ اصول پدافند غیر عامل ۲۳

۱-۹ منابع دیده‌بانی و انواع آن ۳۴

۱-۱۰ حصول اطمینان از پاسخگویی دائم اقدامات پدافند غیر عامل و تهدیدات (به روز سازی اقدامات) ۳۵

نمونه سؤالات ۳۶

فصل دوم: فناوری اطلاعات

۲-۱ تاریخچه فناوری اطلاعات ۳۷

۲-۲ جهانی شدن دنیای اطلاعات ۳۷

۲-۳ تعریف فناوری اطلاعات ۴۲

۲-۴ داده ، اطلاعات ، دانش ۴۵

۲-۵ سیستم‌های اطلاعاتی ۴۷

۲-۶ آشنایی با مفاهیم بنیادی فرایند فناوری اطلاعات و ارتباطات ۵۰

۲-۷ نقش اینترنت در توسعه فناوری اطلاعات ۵۲

نمونه سؤالات ۵۳

فصل سوم: بررسی نقش جنگ‌ها در توسعه فناوری اطلاعات و برعکس

۳-۱ عصر (موج)‌های مختلف زندگی ۵۵

۳-۲ جنگ و تاریخچه آن ۵۹

۳-۳ سیر تحولات تاریخ جنگ ۶۰

۶۴	۳-۴ مشخصه جنگ‌های این دوره.....
۶۵	۳-۵ مراکز تحت پوشش.....
۶۶	۳-۶ انواع جنگ‌های قرن حاضر.....
۷۷	۳-۷ نقش سلاح‌های اطلاعاتی در میادین آتی جنگ.....
۷۹	۳-۸ جدول تقسیم‌بندی انواع جنگ‌ها.....
۸۰	۳-۹ تأثیر جنگ در پیشرفت فناوری اطلاعات.....
۸۲	۳-۱۰ تأثیر فناوری اطلاعات در پیشرفت جنگ‌ها.....
۸۸	۳-۱۱ نقش جنگ‌ها در توسعه فناوری اطلاعات و برعکس.....
۸۹	نمونه سؤالات.....

فصل چهارم: اصول و مبانی امنیت داده‌ها و اطلاعات

۹۱	۴-۱ اهمیت امنیت اطلاعات و ایمن‌سازی کامپیوترها.....
۹۱	۴-۲ مبانی امنیت اطلاعات.....
۹۴	۴-۳ طراحی برای امنیت.....
۱۰۱	۴-۴ امنیت اطلاعات.....
۱۰۲	۴-۵ معرفی سیستم مدیریت امنیت اطلاعات.....
۱۱۸	۴-۶ مستندات مدیریت امنیت اطلاعات.....
۱۲۰	نمونه سؤالات.....

فصل پنجم: مبانی امنیت شبکه

۱۲۱	۵-۱ تعریف امنیت.....
۱۲۴	۵-۲ زیرساخت امنیت اطلاعات.....
۱۲۵	۵-۳ دسته بندی مکانیزم مقابله با حملات.....
۱۲۶	۵-۴ رمزنگاری.....
۱۲۷	۵-۵ رمزنگاری پیشرفته.....
۱۲۷	۵-۶ انواع رمزنگاری.....
۱۵۹	۵-۷ درهمی و انتشار.....
۱۶۰	۵-۸ تاریخچه امضای دیجیتال.....
۱۶۷	۵-۹ استراتژی‌های حمله.....
۱۶۸	۵-۱۰ دیواره آتش.....
۱۷۳	۵-۱۱ سرور پراکسی.....
۱۷۵	۵-۱۲ فناوری شبکه خصوصی مجازی.....
۱۹۰	نمونه سؤالات.....

فصل ششم: پدافند غیرعامل در سیستم عامل و مسیریاب‌ها

- ۶-۱ سیستم عامل و نقش آن در جامعه اطلاعاتی ۱۹۱
- ۶-۲ پدافند غیرعامل در حوزه مسیریاب ۲۰۱
- ۶-۳ پدافند غیرعامل در حوزه امنیت فیزیکی و کنترل دسترسی ۲۱۰
- ۶-۴ سازمان پدافند غیرعامل در حوزه فناوری اطلاعات اهداف کلان ۲۲۲
- نمونه سؤالات ۲۲۶

فصل هفتم: پدافند غیرعامل در حوزه سامانه مدیریت تهدید یکپارچه

- ۷-۱ پدافند غیرعامل در حوزه سامانه مدیریت تهدید یکپارچه و علل استفاده از آن ۲۲۹
- ۷-۲ حالت‌های کاری سامانه‌های مدیریت تهدید یکپارچه ۲۳۰
- ۷-۳ قابلیت‌های امنیتی سامانه‌های مدیریت تهدید یکپارچه ۲۳۲
- ۷-۴ تشخیص و جلوگیری از نفوذ ۲۳۴
- ۷-۵ مدیریت و پالایش محتوای وب ۲۳۵
- ۷-۶ کنترل برنامه‌های کاربردی ۲۳۶
- ۷-۷ ضد هرزنامه ۲۳۶
- ۷-۸ گزارش دهی، رویدادنگاری و نظارت ۲۳۸
- ۷-۹ سایر امکانات سامانه‌های مدیریت تهدید یکپارچه ۲۳۸
- ۷-۱۰ مشخصه‌های متمایزکننده سامانه‌های مدیریت تهدید یکپارچه ۲۴۰
- نمونه سؤالات ۲۴۲

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

- ۸-۱ مانور فناوری اطلاعات (خشم فناوری اطلاعات) ۲۴۳
- ۸-۲ مدیریت بحران و پدافند غیرعامل ۲۴۹
- ۸-۳ قابلیت‌های پدافند غیرعامل ۲۴۹
- ۸-۴ بحران ۲۵۰
- ۸-۵ مدیریت بحران ۲۵۳
- ۸-۶ اصول پایه برای مقابله با بحران‌ها ۲۵۵
- ۸-۷ بخش‌های مختلف فرایند ارزیابی آسیب‌پذیری ۲۵۷
- ۸-۸ مشکلات فرایند ارزیابی آسیب‌پذیری ۲۵۸
- ۸-۹ فرایند مدیریت بحران ۲۵۹
- ۸-۱۰ منابع اصلی کمک‌کننده در مراحل مختلف مدیریت بحران ۲۶۳
- ۸-۱۱ مهم‌ترین عناصر در پیاده‌سازی سیستم اطلاعاتی ۲۶۵

نمونه سؤالات ۲۶۶

فصل نهم: پدافند غیرعامل در فناوری اطلاعات

- ۹-۱ پروژه‌های فناوری اطلاعات ۲۶۷
- ۹-۲ ساختار سیستم مدیریت پروژه ۲۶۹
- ۹-۳ ویژگی‌های مدیریت فناوری اطلاعات ۲۷۲
- ۹-۴ بررسی اصول و مبانی پدافند غیرعامل در پروژه‌های فناوری اطلاعات ۲۷۴
- ۹-۵ زیر ساخت اطلاعات ۲۷۴
- ۹-۶ انواع زیرساخت‌ها و منابع کلیدی کشور ۲۷۵
- ۹-۷ مرکز داده ۲۷۶
- ۹-۸ مرکز داده و تجارت الکترونیک ۲۸۱
- ۹-۹ موارد مهم در طراحی مرکز داده ۲۸۳
- ۹-۱۰ ویژگی‌ها ۲۸۴
- ۹-۱۱ کاربری‌های مراکز داده ۲۸۴
- ۹-۱۲ پدافند غیرعامل در مرکز داده ۲۸۵
- ۹-۱۳ استفاده از سیستم‌های بیومتریک در امنیت مراکز داده ۲۹۱
- ۹-۱۴ تاثیر بیومتریک بر امنیت مراکز داده تجارت الکترونیک ۲۹۸
- ۹-۱۵ پدافند غیرعامل در حوزه فناوری اطلاعات ۳۰۲
- ۹-۱۶ معرفی نظریه پنج حلقه سرهنگ نیروی هوایی جان واردن ۳۰۳
- نمونه سؤالات ۳۰۶

فصل دهم: مهندسی اجتماعی

- ۱۰-۱ مهندسی اجتماعی ۳۰۷
- ۱۰-۲ یک مفهوم نزدیک و مرتبط: مهندسی اجتماعی معکوس ۳۰۸
- ۱۰-۳ استراتژی‌های مهندسی اجتماعی ۳۰۹
- ۱۰-۴ بررسی روان‌شناختی حملات مهندسی اجتماعی ۳۱۱
- ۱۰-۵ چرخه حملات مهندسی اجتماعی ۳۱۳
- ۱۰-۶ تکنیک‌های مهندسی اجتماعی ۳۱۴
- ۱۰-۷ مثال‌هایی از مهندسی اجتماعی ۳۱۸
- ۱۰-۸ ویروس‌ها و فریب‌هایی که از مهندسی اجتماعی استفاده می‌کنند ۳۲۰
- ۱۰-۹ نمونه‌هایی از معروف‌ترین هک‌ها ۳۲۴
- ۱۰-۱۰ دفاع در برابر مهندسی اجتماعی ۳۲۷

نمونه سؤالات ۳۳۸

فصل یازدهم: چالش‌ها و ارائه راهکار

- ۱-۱۱ چالش‌های ارتباطی مدیریت فناوری اطلاعات ۳۳۹
- ۲-۱۱ مشکلات موجود در زمینه پیاده‌سازی ISMS ۳۴۰
- ۳-۱۱ پدافند غیرعامل و چالش‌های نظام بانکی ۳۴۱
- ۴-۱۱ فرهنگ پایداری (پدافند غیرعامل) ۳۴۳
- ۵-۱۱ چالش‌های پیش روی پدافند غیرعامل در مقابل جهانی شدن ۳۴۴
- ۶-۱۱ شکاف دیجیتالی، چالش بزرگ قرن بیست و یکم ۳۴۷
- ۷-۱۱ راه‌حل‌های دیجیتالی ۳۵۳
- ۸-۱۱ راهبردها ۳۵۴
- ۹-۱۱ ماهیت اساسی پدافند غیرعامل ۳۵۵
- ۱۰-۱۱ ارائه راهکار پدافند غیرعامل در فناوری اطلاعات بر اساس تئوری سرهنگ جان واردن ۳۵۷

پیوست ۱: آشنایی با بالاترین مخاطرات امنیتی وبگاه‌ها

- مخاطرات امنیتی برنامه‌های کاربردی ۳۶۱
- ده مخاطره مهم در مورد امنیت برنامه‌های کاربردی - OWASP 2010 ۳۶۳
- تزریق ۳۶۴
- پردازه گذاری فرا- وب‌گاهی ۳۶۶
- مدیریت نشست و اصالت سنجی فروشکسته ۳۶۷
- ارجاعات شیء واره‌ای مستقیم ناامن ۳۶۸
- جعل درخواست فرا-وب‌گاهی ۳۷۰
- پیکربندی نادرست امنیت ۳۷۲
- شکست در محدودسازی دسترسی به URL ۳۷۳
- تغییر مسیره‌ی و انتقال‌های نامعتبر ۳۷۵
- ذخیره‌سازی رمزنگاری ناامن ۳۷۷
- حفاظت غیرکافی از لایه ترابرد ۳۷۸
- گام بعدی برای برنامه نویسان چیست؟ ۳۸۰

پیوست ۲: رایانش ابری

- رایانش ابری ۳۸۳
- مدل‌های استقرار ۳۸۶

۳۸۷	تاریخچه.....
۳۸۸	زیرساخت‌های رایانش ابری.....
۳۹۲	کاربردهای رایانش ابری.....
۳۹۴	مزایا و نقاط قوت رایانش ابری.....
۳۹۷	نقاط ضعف رایانش ابری.....
۳۹۸	چه کسانی باید از رایانش ابری استفاده کنند؟.....
۳۹۹	چه کسانی نباید از رایانش ابری استفاده کنند؟.....
۴۰۱	رایانش ابری در هوای کامپیوتری.....
۴۰۵	پیش‌برندگان تجاری رایانش ابری حرفه‌ای به سمت بازار.....
۴۰۷	زنجیره تأمین ابر.....
۴۰۹	الگوی نفوذ رایانش ابری در کسب و کار.....
۴۱۰	کاربردهای تجاری.....
۴۱۲	بانک‌ها بازار هدف رایانش ابری در ایران.....
۴۱۲	امنیت چالش بزرگ رایانش ابری.....
۴۱۳	پهنای باند و سرعت اینترنت.....
۴۱۳	پردازش ابری و شرکت‌های خودروسازی.....
۴۱۵	منابع.....

خط‌مشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرضه کتاب‌هایی است که تواند

خواسته‌هایی 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. گسترده‌گی 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 سرکار خانم 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، انسبه پارسا

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

تقدیم به:

مادر مهربانم و پدر بزرگوایم و
خواهر دوست داشتینم 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 ببیماید 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 می‌گردد که 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 بین‌المللی 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^۱ حیاتی کشور، مخصوصاً زیرساخت‌های فناوری اطلاعات 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.

نتیجه این تفکر به ساخت و عرضه محصول « سامانه مدیریت تهدید یکپارچه^۱ » 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 باشد که 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 در کشور ما نیز همانند سایر کشورهای 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 فناوری اطلاعات و ارتباطات شکل گرفته است.

اهداف کلان راهبردی^۲ 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 پدافند غیرعامل در سایر بخش‌های زیر ساختی کشور

الزامات و ویژگی‌های دفاع مؤثر در **جنگ‌های نسل ششم^۳** بر اساس اظهارنظر کارشناسان، ضرورت **برنامه‌ریزی^۴** و آغاز 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 ایمن، 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**^۱ 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 نگرستند. حتی کشوری مانند سوئیس با وجود **بی‌طرفی**^۲ 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 شئون 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 به‌سزایی 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 تأمین‌کنندگان 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 اطلاع‌رسانی، 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.

در حالی 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 آگه 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 و خطرناک 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.