

معرفی و برآورد تهدیدات سایبری

مؤلف: علیرضا ابوالحسینی

www.ketab.ir

مرشناسه: ابوالحسینی، علیرضا، ۱۳۵۱

عنوان و نام پدیدآور: معرفی و برآورد تهدیدات سایبری / علیرضا ابوالحسینی

مشخصات نشر: تهران، انتشارات دیده بان ۱۳۹۲

مشخصات ظاهری: ۱۳۳ ص. مصور مصور (بخشی رنگی)، جدول (بخش رنگی)

وضعیت فهرست نویسی: فیا

موضوع: شبکه‌های کامپیوتری، تدابیر ایمنی، فضای مجازی، تکنولوژی اطلاعات، جرایم کامپیوتری

رده‌بندی کنگره: ۱۳۹۲ م ۲ الف ۵۱۰۵/۵ TK رده‌بندی دیویی: ۰۰۵/۸ کتابشناسی ملی: ۳۲۱۳۰۰۵



انتشار دیده بان

❖ عنوان کتاب: معرفی و برآورد تهدیدات سایبری

❖ مولف: علیرضا ابوالحسینی

❖ ناشر: انتشارات دیده بان

❖ ویراستار علمی: جواد بزرگی

❖ ویراستار ادبی: میترا مشهدی رجب

❖ طرح روی جلد: رضا حسینی

❖ لیتوگرافی، چاپ و صحافی: چاپ و نشر دانشگاه

❖ شمارگان: ۱۰۰۰ جلد

❖ نوبت چاپ: اول، تابستان ۹۲

❖ قیمت: ۷۵۰۰۰ ریال

ISBN: 978-600-93837-1-9

شابک: ۹۷۸-۶۰۰-۹۳۸۳۷-۱-۹

حق چاپ برای ناشر محفوظ است

آدرس: تهران، چهارراه پاسداران، انتشارات دیده بان، تلفن: ۲۳۱۱۲۲۳۱

فهرست مطالب

پیشگفتار.....	۴
یادداشت مولف.....	ج
فصل اول: کلیات.....	۱
مقدمه.....	۱
الگوی پژوهش.....	۲
فصل دوم: سطح و وسع نبرد سایبری.....	۵
نبرد سایبری.....	۷
هدف از اجرای عملیات سایبری.....	۸
اهداف.....	۱۳
روش‌ها.....	۱۵
ابزارها.....	۱۷
انواع عملیات سایبری قابل اجرا توسط دشمن.....	۱۸
عملیات حمله.....	۱۹
مکانیزم هدف‌گیری.....	۲۰
جمع‌آوری اطلاعات.....	۲۱
شکل‌دهی صحنه عملیات.....	۲۳
اجرای عملیات.....	۲۴
انواع عملیات شبکه‌ای با توجه به اهداف.....	۲۵

۲۷	انواع حملات شبکه‌ای باتوجه به حمله‌کننده
۲۸	روش‌های حمله
۴۵	عملیات دفاع
۴۶	روش‌های دفاع
۴۷	سیاست امنیتی
۵۵	عملیات شناسایی
۵۷	روش‌های شناسایی
۶۸	الگوی طرح ریزی عملیات سایبری دشمن
۷۱	فصل سوم: معرفی رادخانه سایبری آمریکا
۷۱	مفهوم زرادخانه سایبری
۷۴	عناصر و کارکردهای رادخانه‌های سایبری
۷۸	چگونگی ایجاد و مدیریت زرادخانه سایبری
۸۱	فصل چهارم: الگوی برآورد خطر عملیات‌های سایبری دشمن
۸۲	فن آوری و دانش
۹۲	ارزش اهداف
۹۴	استراتژی ملی و سیاست
۹۷	عواقب و نتایج عملیات
۱۰۰	اولویت‌گذاری عملیات سایبری دشمن
۱۰۳	فصل پنجم: چگونگی شناخت، بررسی و مقابله با تهدیدات سایبری
۱۰۳	بررسی تهدیدات
۱۰۴	محرمانگی

۱۰۵.....	صحت
۱۰۶.....	دسترس پذیری
۱۰۷.....	نقض الزامات امنیتی از سوی دشمن
۱۰۸.....	آسیب پذیری منشأ بروز تهدیدات سایبری
۱۰۹.....	شاخص های آماری امنیت فضای سایبری
۱۱۰.....	ورد تهدیدات و تحلیل زیان
۱۱۲.....	انواع نفوذ از راه مهاجمان
۱۱۵.....	شناسایی دامنه ها
۱۱۷.....	نمونه هایی از حملات سایبری
۱۲۰.....	تشخیص تهدید و هشدار به ایستگاه
۱۲۰.....	سامانه ارزیابی تهدیدات سایبری
۱۲۲.....	چگونگی جمع بندی و استفاده از اطلاعات و ارزیابی ها
۱۲۳.....	نمونه دیدگاه ها در مورد توان ایران در نبرد متقارن سایبری
۱۳۱.....	منابع

پیشگفتار ناشر

واقعیت آن است که دشمنان در برنامه‌ریزی و اجرای عملیات سایبری از قابلیت‌ها و امکانات فن‌آورانه گوناگونی که به‌طور عمده با هدف تسهیل در ورود و فعالیت در فضای سایبر توصیه و ترویج شده، بهره‌برداری کرده و انواع مختلفی از عملیات را طرح‌ریزی و اجرا می‌کند بنابراین ضریب حساسیت جهت مقابله با چنین تهدیداتی درک صحیحی از فضای سایبر و نیز انواع عملیات قابل اجرا از سوی دشمن در این فضا داشته باشیم.

اصطلاح فضای سایبری^۱ برای اولین بار در سال ۱۹۸۰ در یکی داستان علمی - تخیلی به‌کار برده شد. ما در گفتارمان از فضای رایانه‌ای، به‌عنوان مکان فیزیکی یاد می‌کنیم اما در واقع این‌طور نیست. فضای رایانه‌ای اگرچه اصطلاحاً نسبتاً جدید است اما مفهوم آن جدید نیست و پیدایش این مفهوم، همزمان با اختراع اینترنت توسط الکساندر گراهام بل در سال ۱۸۷۶م. بوده است.

اگرچه در نگاهی اجمالی می‌توان فضای سایبر را به شبکه‌های رایانه‌ای محلی، گسترده و جهانی خلاصه کرد لیکن نفوذ فن‌آوری اطلاعات و ارتباطات در دیگر شئون زندگی و تداخل آن با دیگر علوم و فن‌آوری‌ها، ابعاد گسترده‌تر و جدیدی را به فضای سایبر ملحق کرده است. از این رو لازم است با رویکردی واقع‌بینانه حد و حدود فضای سایبر را در تمامی شئون و ابعاد حیات کشور و ملت بدانیم و تهدیدات احتمالی ناشی از این حوزه را تهدیداتی بنیادی و همه‌جانبه علیه نظام و مردم در نظر بگیریم.

با این ادعا داشت که پیشرفت سریع فن‌آوری و تقاضای فزاینده مشتریان در سراسر جهان برای رسیدن و بهره‌برداری از محصولات جدید، ظهور فن‌آوری‌های جدیدی را موجب شده است که دشمن می‌تواند از آنها در راستای تحقق اهداف غیرسازنده خود استفاده کند. در هر صورت فن‌آوری مانند شمشیری دو لبه است که با وجود برخورداری از مزایای فراوان، آسیب‌پذیری‌هایی را نیز به دنبال دارد. در عین حال مشخص نیست که دشمن از فن‌آوری‌های جدیدی استفاده می‌کند که به دنبال آن فعالیت‌های پدافندی و دفاعی را دشوار می‌سازد.

اثر حاضر بر سوءاستفاده بالقوه دشمن از فن‌آوری‌های فضای سایبر تمرکز دارد. هدف، شناسایی قابلیت‌های مورد استفاده از سوی دشمن برای اجرای اهداف بدخواهانه از طریق حوزه سایبر و بیان راهکارهایی است که باید در مقابله با این فعالیت‌ها انجام داد.

یادداشت مولف

مطالب این کتاب برای پاسخ به دو پرسش اصلی به شرح زیر استوار است:

(۱) انواع عملیات سائیری (حمله، دفاع و شناسایی) قابل اجرا از سوی دشمن چیست؟

(۲) آرایش عمومی و معماری در ستانه سایبری دشمن چگونه است؟

در راستای پاسخ به پرسش اول تلاش می‌شود معماری عملیات سایبری ترسیم شده، انواع عملیات سایبری قابل اجرا از سوی دشمن، معرفی و سپس با طراحی شاخص‌هایی مناسب، ابعاد مختلف این عملیات را با یکدیگر مقایسه شود. چنین مقایسه‌ای می‌تواند اولویت‌های دشمن برای اجرای عملیات سائیری را تعیین کند. بدون تردید دشمن در راستای اجرای عملیات مدنظرش نیازمند استفاده به اصطلاح تسلیحاتی است که همواره در حال تولید و ذخیره‌سازی آنهاست تا بتواند به‌دقت و با قوه خود برای اجرای عملیات دلخواهش را افزایش دهد. این ابزارها طریقه‌ای و روال‌های مشخصی طراحی، تولید، نگهداری و در زمان مورد نظر مورد بهره‌برداری قرار می‌گیرند. در واقع این ابزارها و تسلیحات از الگویی نظیر زرادخانه‌های تسلیحات نظامی تبعیت می‌کنند. در این کتاب تلاش خواهیم کرد نحوه ایجاد و مدیریت چنین زرادخانه‌ای تبیین و تشریح شود.

این کتاب در نظر دارد تا ضمن ترسیم تصویری از فضا و عملیات سایبری، انواع مختلف عملیات قابل اجرا در این فضا را از ابعاد مختلف مورد بررسی قرار داده توانایی‌ها و قابلیت‌های دشمن برای اجرای هر یک از عملیات مزبور ارزیابی و در نهایت تخمین مناسبی از احتمال بروز و وقوع عملیات سایبری از سوی دشمن علیه نظام مقدس جمهوری اسلامی ایران به عمل آورد.

بدیهی است ارائه یک پیشنهاد مفید، موثر و سازنده در مورد روش مقابله با تهدیدات سایبری برای کشور به ویژه در بخش دفاع مستلزم شناخت صحیح و مناسب از سطح نبرد سایبری و تشریح انواع فعالیت‌های قابل اجرا در مقابل این تهدیدات و ارزیابی قابلیت‌ها و توان بالفعل و بالقوه کشور در این حوزه است.

علیرضا ابوالحسینی

www.ketab.ir