معرفی و برآورد تهدیدات سایبری

مولف: علیرضا ابوالحسینی

سرشناسه: ابوالحسینی، علیرضا، ۱۳۵۱
عنوان و نام پدیدآور: معرفی و برآورد تهدیدات سایبری/ علیرضا ابوالحسینی
مشخصات نشر: تهران، انتشارات دیده‌بان ۱۳۹۲
مشخصات ظاهری: ۱۳۳ ص. مصور مصور(بخشی رنگی)، جدول(بخش رنگی)
وضعیت فهرست‌نویسی: فیپا
موضوع: شبکه‌های کامپیوتری، تدابیر ایمنی، فضای مجازی، تکنولوژی اطلاعات، جرایم کامپیوتری
رده‌بندی کنگره: ۱۳۹۲ ٦ م۲ الف/۵/۵۱۰۵ TK رده‌بندی دیویی: ۰۰۵/۸ کتابشناسی ملی: ۳۲۱۳۰۰۵

انتشارات دیده‌بان

❖ عنوان کتاب: معرفی و برآورد تهدیدات سایبری
❖ مولف: علیرضا ابوالحسینی
❖ ناشر: انتشارات دیده‌بان
❖ ویراستار علمی: جواد بزرگی
❖ ویراستار ادبی: میترا مشهدی رجب
❖ طرح روی جلد: رضا حسنی
❖ لیتوگرافی، چاپ و صحافی: چاپ و نشر دانشگاه
❖ شمارگان: ۱۰۰۰ جلد
❖ نوبت چاپ: اول، تابستان ۹۲
❖ قیمت: ۷۵۰۰۰ ریال

شابک: ۹-۱-۹۳۸۳۷-۶۰۰-۹۷۸ ISBN: 978-600-93837-1-9

آدرس: تهران، چهارراه پاسداران، انتشارات دیده‌بان، تلفن: ۲۳۱۱۲۲۳۱

فهرست مطالب

پیشگفتار ناشر

واقعیت آن است که دشمن 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 ضرورت 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[1] برای اولین بار در سال ۱۹۸۲ در یک داستان علمی ـ تخیلی به‌کار برده شد. ما در گفتارمان از فضای رایانه‌ای، به‌عنوان یک مکان فیزیکی یاد می‌کنیم اما در واقع اینطور نیست. فضای رایانه‌ای اگرچه اصطلاح نسبتا جدید است اما مفهوم آن جدید نیست و پیدایش این مفهوم، همزمان با اختراع تلفن توسط الکساندر گراهام بل در سال ۱۸۷۶م. بوده است.

1- Cyber Space

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.

باید اذعان داشت که پیشرفت سریع فن‌آوری و تقاضای فزاینده مشتریان در سراسر دنیا برای خرید 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 در چه زمانی 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 در پاسخ به دو پرسش اصلی به شرح زیر استوار است:

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

۲) آرایش عمومی و معماری زرادخانه 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 عملیات‌ها با یکدیگر مقایسه شود. چنین مقایسه‌ای می‌تواند اولویت‌های دشمن برای اجرای عملیات سایبری را تعیین کند. بدون تردید دشمن در راستای اجرای عملیات مدنظرش نیازمند ابزارهایی است که به اصطلاح تسلیحاتی است که همواره در حال تولید و ذخیره‌سازی آنهاست تا بتواند با تلفیق توان بالقوه خود برای اجرای عملیات دلخواهش را افزایش دهد. این ابزارها طی مکانیزم 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 صحنه نبرد سایبری و تشریح انواع فعالیت‌های قابل اجرا در مقابل این تهدیدات و نیز ارزیابی قابلیت‌ها و توان بالفعل و بالقوه کشور در این حوزه است.

علیرضا ابوالحسینی