
جنگ سایبری

مقدمه ای بر مناقشات در عصر اطلاعات

www.ketab.ir

نویسنده: ایزاک . ر پور شه

مترجمین: فریبرز خاکپور، علی خزائی، حمید عنایتی

سرشناسه: ایزاک.ر پورشه
 عنوان و نام مترجمین: جنگ سایبری (مقدمه ای بر مناقشات در عصر اطلاعات) / خاکپور، فریبرز ۱۳۵۰، خزانی، علی ۱۳۵۴، عنایتی، حمید ۱۳۷۳
 ویراستار: قموشی، علی ۱۳۶۳
 وضعیت ویراست: اول
 مشخصات نشر: تهران: نیروی پدافند ارتش جمهوری اسلامی ایران ۱۳۹۹
 مشخصات ظاهری: ۴۹۶ صفحه، مصور، جدول، رنگی
 شابک: ۹۷۸-۶۰۰-۸۹۸۰-۷۵-۹
 قیمت: ۵۵۰۰۰۰ ریال
 وضعیت فهرست نویسی: فیا
 عنوان اصلی:
 موضوع: جنگ اطلاعاتی
 موضوع: تروریسم رایانه ای - فضای مجازی - تدابیر امنیتی
 شناسه افزوده: خاکپور، فریبرز ۱۳۵۰
 شناسه افزوده: خزانی، علی ۱۳۵۴
 شناسه افزوده: عنایتی، حمید ۱۳۷۳
 شناسه افزوده: قموشی، علی ۱۳۶۳
 شناسه افزوده: تهران: ارتش. نیروی پدافند هوایی آجا
 رده بندی کنگره: U ۱۶۳
 رده بنده دیویی: ۳۵۰ / ۳۴۳
 شماره کتابشناسی ملی: ۶۱۳۵۶۸۰



www.ketab.ir

عنوان: جنگ سایبری (مقدمه ای بر مناقشات در عصر اطلاعات)

مترجمین: فریبرز خاکپور، علی خزانی، حمید عنایتی

ویراستار: علی قموشی

طراح جلد و صفحه آرا: علی قموشی

ناظر نشر: سید محمد رضا عمادی سرخی

مدیر برنامه ریزی: جواد سلطانیان

ناشر: قرارگاه پدافند هوایی خاتم الانبیاء (ص) آجا

چاپ و صحافی: مرکز مطالعات راهبردی ن ق پ ه خ (ص) آجا

شابک: ۹۷۸-۶۰۰-۸۹۸۰-۷۵-۹

شمارگان: ۱۰۰۰ نسخه

چاپ اول: ۱۴۰۰

قیمت: ۵۵۰۰۰۰ ریال

نشانی: تهران، بزرگراه بسیج، بلوار هجرت، ستاد قرارگاه پدافند هوایی خاتم الانبیاء (ص) آجا

تلفن: ۳۳۲۴۰۴۶۸ (۰۲۱) دورنگار: ۳۳۲۴۰۴۶۹ (۰۲۱)

«کلیه حقوق این اثر به انتشارات قرارگاه پدافند هوایی خاتم الانبیاء (ص) آجا تعلق دارد»

ت	فهرست
۱	فصل ۱: اطلاعات و مناقشات
۲	۱-۱-۱ انگیزه و مقدمه فصل
۴	۱-۲-۱ اطلاعات
۴	۱-۲-۱-۱ تعریف اطلاعات
۵	۱-۲-۱-۲ فضای اطلاعات و محیط اطلاعات
۷	۱-۲-۲-۱ اطلاعات و مناقشات
۷	۱-۳-۱ جنگ
۸	۱-۴-۱ شبکه‌ها و فناوری
۹	۱-۴-۱-۱ گره‌ها
۹	۱-۴-۱-۲ پیوندهای سیمی و بی‌سیم
۱۰	۱-۴-۱-۳ تبادل داده‌ها در شبکه‌ها
۱۱	۱-۴-۱-۴ تبادل دستی داده‌ها
۱۲	۱-۴-۱-۵ مورد مطالعه Agent.btz و استیکرنت
۱۳	۱-۴-۱-۶ تعریف ICT
۱۷	۱-۵-۱ عصر اطلاعات، وب و اینترنت
۱۹	۱-۶-۱ تعریف و توصیف فضای سایبری
۱۹	۱-۶-۱-۱ مشخصات متمایزکننده
۲۱	۱-۷-۱ اصطلاحات امنیتی
۲۱	۱-۷-۱-۱ نقص‌ها، آسیب‌پذیری‌ها و کدهای مخرب
۲۳	۱-۷-۱-۲ سیستم‌های اطلاعاتی
۲۳	۱-۷-۱-۳ امنیت اطلاعات
۲۴	۱-۷-۱-۴ امنیت سایبری
۲۸	۱-۷-۱-۵ هویت، اصالت و مجوز
۲۹	۱-۸-۱ تعریف و توصیف عملیات‌های فضای سایبری
۲۹	۱-۸-۱-۱ تعاریف عملیات‌های فضای سایبری
۲۹	۱-۸-۱-۲ اقداماتی که از عملیات‌های فضای سایبری پشتیبانی و آن را فعال‌سازی می‌کنند
۲۹	۱-۸-۱-۳ توصیف جرم در فضای سایبری
۳۳	۱-۸-۱-۴ تفاوت بین حمله و سوءاستفاده
۳۳	۱-۹-۱ جنگ الکترونیکی و عملیات‌ها

۳۳	۱-۹-۱-۱ تعریف جنگ الکترونیکی
۳۴	۱-۹-۲-۱ عملیات مدیریت طیف
۳۶	۱-۹-۳-۱ تفاوت سایبری و جنگ الکترونیکی از حملات جنبشی سنتی
۳۸	۱-۹-۴-۱ اقدامات الکترومغناطیسی و فضای سایبری
۳۹	۱۰-۱-۱ جنگ اطلاعاتی
۳۹	۱-۱۰-۱-۱ تعاریف گسترده
۴۱	۱-۱۰-۱-۲ عملیات نفوذ و اطلاع رسانی
۴۳	۱-۱۰-۱-۳ عملیات فناوری اطلاعات
۴۴	۱۱-۱-۱ تسلیحات و مأموریت‌های جنگ
۴۴	۱-۱۱-۱-۱ رسانه‌های اجتماعی
۴۵	۱-۱۱-۱-۲ مأموریت‌های عمومی
۴۵	۱-۱۱-۱-۳ مأموریت‌های راهبردی
۴۶	۱-۱۱-۱-۴ مأموریت‌های عملیاتی
۴۷	۱-۱۱-۱-۵ رسانه‌ی اجتماعی و انتخابات آمریکا
۴۸	۱۲-۱ خلاصه‌ی فصل
۴۹	فصل ۲ چرخه‌های عمر حمله سایبری
۵۱	۲-۱-۱ انگیزه و مقدمه‌ای بر چرخه‌های عمر حمله سایبری
۵۱	۲-۲-۱ سه مرحله برای عملیات‌های سایبری
۵۲	۲-۲-۱-۱ شناسایی آسیب‌پذیری‌ها
۵۴	۲-۲-۲-۱ دستیابی و حفظ دسترسی
۵۶	۲-۲-۳-۱ سوءاستفاده
۵۷	۲-۳-۱ مراحل حمله
۵۸	۲-۳-۱-۱ برنامه‌ریزی
۵۹	۲-۳-۲-۱ آماده‌سازی
۵۹	۲-۳-۳-۱ نفوذ
۵۹	۲-۳-۴-۱ مدیریت و تواناسازی
۶۰	۲-۳-۵-۱ پایداری و اجرای حمله
۶۰	۲-۴-۱ پایداری و اجرای حمله
۶۱	۲-۴-۱-۱ شناسایی منفعلانه
۶۲	۲-۴-۲-۱ اسکن کردن
۶۳	۲-۴-۳-۱ Enumeration
۶۴	۲-۴-۴-۱ هدف‌گیری و زوج‌سازی تسلیحات

۶۴	۲-۴-۵ سرقت مجوزها
۶۴	۲-۴-۶ ایجاد یک پی‌لود
۶۵	۲-۴-۷ تحویل پی‌لود
۶۵	۲-۴-۸ سوءاستفاده
۶۵	۲-۴-۹ ترفیع امتیاز
۶۵	۲-۴-۱۰ ایجاد فرمان، کنترل و ارتباطات
۶۵	۲-۴-۱۱ حرکت جانبی
۶۶	۲-۴-۱۲ نصب درهای مخفی و دسترسی از راه دور
۶۶	۲-۴-۱۳ استخراج داده‌ها
۶۶	۲-۴-۱۴ پاک‌سازی ردپا
۶۶	۲-۵ ترکیب مراحل و فازها
۶۹	فصل ۳ ریسک سایبری
۷۱	۳-۱-۰ ریسک سایبری
۷۱	۳-۲-۰ تعریف ریسک در فضای سایبری
۷۶	۳-۳-۰ مورد مطالعه اینترنت اشیا
۷۷	۳-۴-۰ مکعب ریسک
۷۹	۳-۵-۰ ارزیابی ریسک
۷۹	۳-۵-۱-۰ تحلیل اهمیت
۸۰	۳-۵-۲-۰ طبقه‌بندی عوامل تهدید
۸۰	۳-۵-۳-۰ عوامل تهدید معلوم: تهدیدات پیشرفته ماندگار
۸۲	۳-۵-۴-۰ عوامل تهدید معلوم: بچه‌ی اسکریپتی
۸۳	۳-۵-۵-۰ روش‌ها و ابزارهای عامل تهدید: مرور
۸۴	۳-۵-۶-۰ روش‌ها و ابزارهای عامل تهدید: روت‌کیت‌ها
۸۵	۳-۵-۷-۰ روش‌ها و ابزارهای عامل تهدید: بات‌نت‌ها
۸۷	۳-۵-۸-۰ مطالعه‌ی موردی بات‌نت: VPNFilter
۸۸	۳-۵-۹-۰ مطالعه‌ی موردی بات‌نت: میرای
۸۹	۳-۵-۱۰-۰ تحلیل آسیب‌پذیری
۸۹	۳-۶-۰ مدیریت ریسک
۹۰	۳-۷-۰ تسکین ریسک
۹۳	۳-۸-۰ تحلیل کمی ریسک
۹۴	۳-۸-۱-۰ محاسبات پایه
۹۵	۳-۸-۲-۰ مراحل اصلی تحلیل