

جنگ سایبر

و راه‌های مقابله با حملات سایبری

نویسندگان:

علیرضا ملکی

داود آذر



انتشارات دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

پائیز ۱۳۹۸

سرشناسه	ملکی، علیرضا، ۱۳۴۸ -
عنوان و نام پدیدآور	جنگ سایبر و راه‌های مقابله با حملات سایبری / نویسندگان علیرضا ملکی، داود آذر.
مشخصات نشر	تهران: ارتش جمهوری اسلامی ایران، دانشگاه فرماندهی و ستاد آجا، انتشارات دافوس، ۱۳۹۸.
مشخصات ظاهری	۱۶۴ ص: مصور، جدول.
شابک	۹۷۸-۶۲۲-۸۷۸-۰۰۲-۵
وضعیت فهرست نویسی	فیبا
موضوع	Computer networks -- Security measures شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع	Computer security کامپیوترها -- ایمنی اطلاعات
موضوع	Cyberspace -- Security measures فضای مجازی -- تدابیر ایمنی
موضوع	Data protection حفاظت داده‌ها
موضوع	Information technology -- Security measures تکنولوژی اطلاعات -- تدابیر ایمنی
شناسه اف	آذر، داود، ۱۳۵۵ -
شناسه افزود	ایران. ارتش. دانشگاه فرماندهی و ستاد. انتشارات دافوس
شناسه افورده	Staff College. Dafoos Publisher & Iran. Army. Command
رده بندی کنگره	۵۹/۵۱۰۵TK
رده بندی دیویی	۸/۰۸
شماره کتابشناسی ملی	۵۷' ۴۵'

عنوان: جنگ سایبر و راه‌های مقابله با حملات سایبری

مؤلفین: علیرضا ملکی، داود آذر

ویراستار: سامان آزاد

ناظر ویراستار: حمید همت

طرح روی جلد: علیرضا قانع

صفحه‌آرایی: علی غلامی

ناشر: انتشارات دافوس

شمارگان: ۱۰۰۰

تعداد صفحه: ۱۸۷

تاریخ نشر: پائیز ۱۳۹۸

چاپ اول

لیتوگرافی، چاپ و صحافی: مدیریت چاپ، انتشارات و فصلنامه دانشگاه فرماندهی و ستاد آجا

قیمت: ۳۰۰,۰۰۰ ریال

نشانی: تهران، میدان پاسستور، خیابان دانشگاه جنگ، دانشگاه فرماندهی و ستاد آجا، انتشارات دافوس

تلفن: ۰۲۱-۶۶۴۷۰۴۸۶؛ ۰۲۱-۶۶۴۱۴۱۹۱ - ۰۲۱

مسئولیت صحت مطالب بر عهده مؤلفین می‌باشد.

کلیه حقوق برای دافوس آجا محفوظ است. (نقل مطالب با ذکر مأخذ بلامانع است).

فهرست عناوین

صفحه	عنوان
۹	پیشگفتار
۱۱	مقدمه
۱۳	فصل اول
۱۴	تعاریف و مفاهیم فضای مجازی و سایبری
۲۵	فصل دوم
۲۶	۱-۲-۱- امنیت سایبری در دنیای امروزی
۲۸	۲-۲-۲- پروتکل‌های فضای سایبری
۲۹	۳-۲-۳- اشکال مختلف جنگ سایبر
۳۰	۴-۲-۴- قلمرو جنگ سایبری
۳۱	۵-۲-۵- محدوده جنگ سایبر
۳۳	۶-۲-۶- ویژگی‌های جنگ سایبری
۳۶	۷-۲-۷- هدف جنگ سایبری
۳۸	۸-۲-۸- محدودیت‌های جنگ سایبر
۴۲	۹-۲-۹- هدایت جنگ سایبری
۴۴	۱۰-۲-۱۰- ابزار، سلاح و تجهیزات سایبری
۴۶	۱۱-۲-۱۱- ابزارهای شناسایی سایبری
۴۸	۱۲-۲-۱۲- سلاح‌های پنهان
۴۹	۱۳-۲-۱۳- سلاح اجتماعی
۴۹	۱۴-۲-۱۴- ابزار و سلاح سایبری و حوزه اثر آن‌ها
۵۱	فصل سوم
۵۴	۱-۳-۱- الزامات فضای سایبر
۵۴	۲-۳-۲- الزامات بسترسازی
۵۵	۳-۳-۳- الزامات بومی‌سازی
۵۵	۴-۳-۴- الزامات کنترل امنیتی
۶۳	۵-۳-۵- الزامات آموزشی

۶۹	فصل چهارم
۷۶	۴-۱- ساختار سایبری
۷۸	۴-۲- استانداردهای سایبری
۸۰	۴-۳- ساختار سازمانی
۸۲	۴-۵- جنبه نیروی انسانی جنگ سایبر
۸۲	۴-۶- روابط بین نیروی انسان و سامانه‌ها
۸۳	۴-۷- دسته‌بندی انسان‌های مرتبط با سامانه‌ها
۸۳	فصل پنجم
۹۰	آسیب‌های فضای سایبری
۹۰	۵-۱- فضای سایبر و حوزه‌های آسیب‌پذیر
۸۵	۵-۲- نفاذ آسیب‌پذیری
۸۷	۵-۳- ابعاد آسیب‌پذیر فضای سایبر
۹۷	۵-۴- آسیب‌پذیری‌های نیروی انسانی
۹۵	فصل ششم
۹۶	۶-۱- آفندها یا تهدیدهای سایبری
۱۰۵	۶-۲- انواع تهدیدات سایبری
۱۰۷	۶-۳- عوامل مؤثر بر تهدیدات سایبری
۱۱۰	۶-۴- عوامل مؤثر در مقابله با تهدیدات سایبری
۱۱۴	۶-۵- چالش‌های اساسی در برابر تهدیدات سایبری
۱۱۸	۶-۶- اقدامات ضروری در برابر تهدیدات سایبری
۱۱۹	۶-۷- مدیریت پیامدهای جنگ سایبری
۱۲۲	۶-۸- سازمان‌دهی عملیات سایبری
۱۲۷	۶-۹- فعالیتهای آفندی سایبری
۱۲۸	۶-۱۰- نقش عملیات تلافی‌جویانه در جنگ سایبری
۱۲۱	فصل هفتم
۱۳۲	۷-۱- مقابله با حملات سایبری
۱۳۲	۷-۲- دفاع سایبری

۱۳۳	۷-۳- مراحل دفاع سایبری
۱۳۵	۷-۴- هدف دفاع سایبری
۱۲۹	۷-۵- بازدارندگی و چشم انداز دفاع سایبری
۱۳۲	۷-۶- حوزه‌های آسیب‌پذیر
۱۴۷	۷-۷- انواع حملات سایبری
۱۵۲	۷-۸- حملات فیشینگ
۱۳۵	۷-۹- بگیزه حملات سایبری
۱۶۵	۷-۱۰- مراحل حملات سایبری و روش دفاع در مقابل آن‌ها
۱۷۲	۷-۱۱- سطوح - لایه‌ها در مقابله با حملات سایبر
۱۷۶	۷-۱۲- خط‌شی - مقابله با حملات سایبری
۱۷۹	۷-۱۳- راهبرد مقابله با حملات سایبری
۱۸۰	۷-۱۴- نقش دولت در دفاع در برابر حمله سایبری
۱۶۹	فصل هشتم
۱۸۶	۸-۱- ساختار سایبر آمریکا
۱۸۷	۸-۲- راهبرد بین‌المللی آمریکا در فضای سایبر
۱۸۸	۸-۳- رویکرد راهبرد بین‌المللی آمریکا در فضای مجازی
۱۹۰	۸-۴- اقدامات دولت و مجلس آمریکا در خصوص سایبر
۱۹۱	۸-۵- سیاست تهاجم سایبری آمریکا علیه کشورها
۱۹۲	۸-۶- ساختار فرماندهی سایبری آمریکا
۱۹۳	۸-۷- مأموریت قرارگاه سایبری آمریکا
۱۹۳	۸-۸- حوزه فعالیت قرارگاه سایبری آمریکا
۱۹۴	۸-۹- اجزای فرماندهی سایبری آمریکا
۱۹۵	۸-۱۰- ساختار سایبری در ایران
۲۰۲	منابع علمی
۱۸۷	منابع لاتین
۱۸۷	تارنما وبگاهها

پیشگفتار

برابر دستور دین مبین اسلام و اطاعت از فرامین الهی پیامبران و امامان ما، هرگز بر کسی تیغ نمی‌کشیم ولی اگر دشمنان قسم‌خورده ما بر ما هجوم آورده و قصد جان و مال ما را نمایند در مقابل آن‌ها می‌ایستیم و از دین و کشور و فرهنگ خود حفاظت می‌کنیم. پس باید در برابر تهدیدات دشمن مقابله نمود نظر به اینکه مقوله امنیت و آسایش ملی در هزاره‌ای که تمام نیروی دشمن متوجه و متمرکز بر تجاوز و رخنه است، امری کاملاً محسوس و ملزوم است، بدون شک اکنون دشمن در حال طرح‌ریزی حمله است. تنها یک راه نفوذ کافی است تا وی به قصد خود نائل گردد.

(امروز برای ضعیف دشمن لزومی ندارد حتماً خطوط راه‌آهن آن را بمباران کنیم؛ یک مودم و یک pc کافی است!)

با گسترش روزافزون استفاده از فضای سایبری که به‌اندازه کهکشان گسترده یافته باید در این گسترده نیز مودم‌ها و توانائی مقابله با دشمن سایبری را داشت. چراکه حفاظت از مرزهای مجازی Virtual Network erimers به‌اندازه حفاظت از مرزهای روی نقشه برای هر کشوری دارای اهمیت است. مرزهای مجازی که اطلاعات، این عامل نیروبخش و حیاتی را در درون خود جای داده؛ مرزهایی که تمام عناصر وابسته به دنیای مجازی را در خود دارند... از دنیای مجازی خود، حفاظت کنیم.

پس اگر در جنگ بر ایشان دست‌یافتی، چنان تا و تانسان کن که عبرت آیندگان‌شان شود؛ باشد که پند گیرد.

((قرآن کریم، سوره الانفال - آیه ۵۷))

لذا با نگاهی واقع‌بینانه حدود فضای سایبر را می‌توان در تمام سنون و ابعاد زندگی یک کشور و ملت دانست و تهدیدات این حوزه را تهدیدی بنیادی و همه‌جانبه بر علیه نظام و کشور در نظر گرفت. فناوری اطلاعات به‌عنوان یک شمشیر دو لبه است که با داشتن مزایای بسیار زیاد، آسیب‌های فراوانی نیز برای آن متصور است. دشمنی که صاحب فناوری است و مشخص نیست از چه فناوری جدیدی استفاده می‌نماید و همین امر فعالیت‌های پدافندی و دفاعی را مشکل می‌سازد.

یکی از حوزه‌های مهم و کاربردی در این عصر، حوزه‌ی سایبر می‌باشد. ورود دشمنان بالفعل و بالقوه‌ی جمهوری اسلامی ایران به حوزه‌ی سایبر برای ضربه زدن و ایجاد اختلال در سامانه‌های رایانه‌ای کشور، نیاز مبرم به آشنایی با جوانب، الزامات و ساختار و آسیب‌های چنین فضایی را می‌طلبد، به‌ویژه برای فرماندهان و تصمیم‌گیرندگان و سیاست‌گذاران، که توان دفاعی خود را با تجهیز و ارتقای توان علمی و سامانه‌های جنگ و دفاع سایبری برای جنگ‌های نوین آینده آماده‌تر نمایند.

علیرضا ملکی

داود آذر

www.ketab.ir