



دانشگاه افسری امام علی (ع)

معاونت پژوهش

جنگ و دفاع سایبری: مفاهیم، راهبردها و راهکارها

نیما فرزام‌نیا

تهران

۱۳۹۸

سرشناسه	فرزام نیا، نیما، ۱۳۵۷
عنوان و نام پدیدآور	جنگ و دفاع سایبری: مفاهیم، راهبردها و راهکارها/ مؤلف: نیما فرزام نیا
مشخصات نشر	تهران: دانشگاه افسری امام علی (ع)، مرکز نشر، ۱۳۹۸
مشخصات ظاهری	۱۳۵ ص
شابک	978-600-7922-53-8
وضعیت فهرست‌نویسی	فیبا
یادداشت	کتابنامه
موضوع	کامپیوترها—ایالات متحده—ایمنی اطلاعات
موضوع	Computer security—United States
موضوع	شبکه های کامپیوتری—ایالات متحده—تدابیر ایمنی
موضوع	Computer networks—Security measures—United States
موضوع	تروریسم رایانه‌ای — ایالات متحده — پیشگیری
موضوع	Cyberterrorism—Prevention—United States
موضوع	جنگ اطلاعاتی — ایالات متحده — پیشگیری
موضوع	Information Warfare—Prevention—United States
شناسه افزوده	دانشگاه افسری امام علی (ع)، مرکز نشر
شناسه افزوده	Press Imam Ali Military University
رده‌بندی کنگره	۳۹۸ س ۵۹/۹۱: QAY۶
رده‌بندی دیوینی	۴۲۵۶۵۲۴
شماره کتابشناسی ملی	

عنوان کتاب:	جنگ و دفاع سایبری: مفاهیم، راهبردها و راهکارها
نویسنده:	نیما فرزام نیا
ویراستار و صفحه آرا:	سید نعیم محسنی
طراح جلد:	امیر مسعود احمدی
ناشر:	انتشارات دانشگاه افسری امام علی (ع)
شمارگان:	۱۰۰۰
قیمت:	۲۹۰۰۰ ریال
توبت چاپ:	اول، ۱۳۹۸
شابک:	۹۷۸-۶۰۰-۷۹۲۲-۵۳-۸
صندوق پستی:	۱۳۱۷۸۹۳۴۷۱
تلفن:	۶۶۴۶۷۴۴۴
پست الکترونیک:	pub.iau.1300@gmail.com

نشانی: تهران، خیابان امام خمینی (ع)، روبه‌روی مجلس سابق، دانشگاه افسری امام علی (ع)، معاونت پژوهش
 کلیه حقوق برای دانشگاه افسری امام علی (ع) محفوظ است

فهرست مطالب

صفحه

عنوان

۱	فصل اول: مفاهیم فضای سایبر
۱	مقدمه
۲	زیر ساخت‌های اساسی
۳	نفوذ فناوری اطلاعات در کلیه عرصه‌ها
۴	اشتراک زیرساخت‌ها در فن‌آوری اطلاعات
۵	افزایش پیچیدگی‌ها در زیرساخت اطلاعاتی
۶	تعریف فضای سایبری
۷	تعریف جامعه
۸	تفاوت فضای سایبری و فضای مجازی
۹	جغرافیای فضای سایبر
۹	ساختار فضای سایبری
۱۱	ویژگی‌ها
۱۲	سرمایه ملی سایبری
۱۳	آسیب‌پذیری سایبری
۱۴	آسیب‌پذیری‌های عمده سایبری کشور
۱۶	تهدیدات سایبری
۱۹	سطوح تهدیدات سایبری
۱۹	شدت تهدیدات سایبری
۲۱	سلاح سایبری
۲۱	هشدار سایبری
۲۴	فصل دوم: جنگ سایبری
۲۴	تکامل در محیط‌های عملیاتی جنگ‌ها
۲۴	۱- میدان جنگ کلاسیک (زمین، هوا و دریا)
۲۵	۲- میدان جنگ کلاسیک با قابلیت شبکه‌های ارتباطی
۲۶	۳- میدان جنگ آینده (مواضع کلاسیک + مواضع سایبری)
۲۷	حمله سایبری
۲۸	جنگ سایبری
۲۸	انواع جنگ‌های سایبری
۲۸	۱- جنگ سایبری عملیاتی
۲۹	۲- جنگ سایبری راهبردی

۲۹	تاریخچه جنگ سایبری
۳۰	نمونه‌هایی واقعی از جنگ‌های سایبری که تا کنون رخ داده است:
۳۱	اقدامات اخیر دشمنان علیه نظام
۳۳	ارزیابی سلاح‌های سایبری
۳۳	مراحل فرآیند طرح‌ریزی جنگ سایبری
۳۴	ویژگی‌های جنگ سایبری
۳۵	مقایسه هزینه به کارگیری سلاح‌های جدید با سلاح سایبری
۳۵	ویژگی‌های سربازان سایبری
۳۶	شاخص‌های جنگ سایبری
۳۶	پیامدهای جنگ سایبری
۳۷	سناریوهای جنگ سایبری
۳۸	نمونه‌هایی از عرصه‌ای غیر جنگ سایبری
۳۹	دیدگاه‌ها و ارتش‌های سایبری دنیا
۳۹	۱- ارتش سایبری آمریکا
۴۱	۲- روسیه
۴۲	۳- کره شمالی
۴۳	۴- چین
۴۳	۵- رژیم صهیونیستی
۴۵	۶- انگلستان
۴۵	چند نمونه از حملات سایبری منتسب به کشور ایران
۴۸	چند نمونه از تهدیدات سایبری محتمل در سطح ملی
۵۱	فصل سوم: دفاع سایبری
۵۱	دفاع سایبری
۵۳	پدافند غیرعامل سایبری
۵۳	نحوه رویارویی با تهدیدات سایبری
۵۳	پدافند(دفاع) سایبری
۵۳	پدافند غیرعامل سایبری
۵۴	رویکردهای دفاع سایبری
۵۴	دستورات اجرایی مقابله با تهدیدات عمومی حوزه سایبری
۵۵	دستورات اجرایی خاص حوزه سایبری
۵۶	مراکز پدافند سایبری
۵۶	مأموریت مرکز پدافند سایبری
۵۶	شرح وظایف مرکز پدافند سایبری:

۵۸	تخصص کارشناسان مرکز پدافند سایبری
۵۸	مهارت‌های مدیر مرکز پدافند سایبری
۵۹	مهارت‌های عمومی کارشناسان مرکز پدافند سایبری
۵۹	وظایف مدیر مرکز پدافند سایبری
۵۹	وظایف گروه پایش در مرکز پدافند سایبری
۶۰	وظایف گروه واکنش سریع در مرکز پدافند سایبری
۶۰	وظایف گروه تحلیل مخاطرات در مرکز پدافند سایبری
۶۰	ملاحظات در خصوص مرکز پدافند سایبری
۶۱	سند راهبردی پدافند سایبری کشور
۶۱	اسناد بالادستی
۶۱	قلمرو سند
۶۲	اصول حاکم بر حوزه پدافند سایبری کشور:
۶۲	بیانیه رسالت قرارگاه پدافند سایبری کشور
۶۲	مأموریت پدافند سایبری کشور
۶۳	چشم‌انداز پدافند سایبری کشور
۶۴	اهداف کلان پدافند سایبری کشور
۶۵	راهبردهای نظام پدافند سایبری کشور
۶۹	فصل چهارم: دستورالعمل آمادگی دستگاه‌ها و منظور قابلخاطر تهدیدات سایبری دشمن
۶۹	بخش اول: دستورالعمل آمادگی دستگاه‌ها به منظور مقابله با تهدیدات سایبری دشمن
۷۰	مأموریت مراکز پدافند سایبری در دستگاه‌ها
۷۴	هدف تشکیل مراکز پدافند سایبری در دستگاه‌ها
۷۴	منظور تشکیل مراکز پدافند سایبری در دستگاه‌ها
۷۵	دستورات اجرایی برای مقابله با تهدیدات عمومی حوزه سایبر در دستگاه‌ها
۷۶	وظایف و مسئولیت‌ها
۷۸	دستورات هماهنگی عمومی حوزه سایبری در دستگاه‌ها
۷۹	دستورات هماهنگی خاص حوزه سایبری در دستگاه‌ها/ یگان‌ها/ قسمت‌ها
۸۱	بررسی عملیاتی تهدیدات
۸۲	دلایل و عوامل تفاوت تهدیدات فضای سایبری از تهدیدات دنیای واقعی
۸۶	ویژگی‌های حملات سایبری
۸۶	کاربردهایی از حملات سایبری
۸۷	هشدار سایبری
۹۴	مأموریت‌ها و شرح خدمات مرکز پدافند سایبری دستگاه
۹۸	مأموریت‌ها و شرح خدمات مرکز پدافند سایبری قرارگاه‌ها/ یگان‌ها/ قسمت‌ها

۱۰۳	بخش دوم: دستورالعمل امن سازی فضای سایبری دستگاه‌های/یگان‌ها/ قسمت‌ها
۱۰۴	وظایف و مسئولیت‌ها
۱۰۶	دستورات هماهنگی
۱۰۶	بخش سوم: ساختار سازمانی و وظایف مراکز پدافند سایبری دستگاه‌ها
۱۰۶	الف) مأموریت
۱۰۷	ب) شرح وظایف
۱۰۸	ج) سازمان
۱۱۱	د) شرح وظایف مدیر و کارکنان
۱۱۲	ه) تجهیزات
۱۱۲	و) ملاحظات
۱۱۳	فرایند ایجاد ساختار مرکز دفاع سایبری و امن سازی فضای سایبری دستگاه‌ها
۱۱۴	نحوه عملکرد مرکز پدافند سایبری دستگاه‌های اجرایی برای مقابله با تهدیدات سایبری
۱۱۴	وظایف و مسئولیت‌ها
۱۱۹	منابع و مآخذ

پیشگفتار مؤلف

رشد سریع فناوری‌های نو به خصوص تکنولوژی‌های اطلاعاتی و همچنین علم الکترونیک و رایانه فضاها و ابعاد جدیدی را در دنیا به وجود آورده است. یکی از این فضاها که دارای دو بعد فیزیکی و مجازی است، فضای سایبری است. نکته حائز اهمیت اینجاست که هر دو بعد فیزیکی و مجازی بر زندگی بشر تأثیرات بسزایی دارد و چه بسا در بعضی مواقع فضای مجازی آن اثرات عمیق‌تری را به جای می‌گذارد.

در این کتاب کوشش شده است که ابتدا مفاهیم اولیه و جدید فضای سایبر بیان شود و سپس به راسخ‌های حوزه جنگ سایبری پرداخته شده و چهارچوب این جنگ‌ها ارائه گردد و در نهایت چالش‌هایی در خصوص افند سایبری بیان شده و راهکارها، ساختارها و روش‌های لازم در این راستا ارائه می‌گردد.

در این نوشته از دیدگاه‌های علمی احتراز گردیده و بیشتر از زاویه مدیریتی و فرماندهی به این فضا نگاه شده است؛ چرا که در صورت عدم وجود نگاه‌های مدیریتی درست به این فضا و قابلیت‌های آن، تشخیص اینکه چه افند متناسب و چگونه به کار گرفته شوند و همچنین تعیین افق و مأموریت‌های آن‌ها به درستی صورت نخواهد پذیرفت و در نتیجه رشد سازمانی قابل ملاحظه‌ای در این راستا نخواهیم داشت. البته شایان ذکر است که ان شاءالله در کتاب دیگری به ابزارها و روش‌های عملیاتی و فنی در این فضا خواهیم پرداخت.

نیما فرزامنیا