

شناخت تهدیدات فضای سایبر و پداقند از آن

مؤلفین:

داود آذر

حسین مسلم



انتشارات دانشگاه فرماندهی و ستاد دانشگاه جنگ

ارتش جمهوری اسلامی ایران

بهار ۱۳۹۳

سرشناسه	: آذر، داود، ۱۳۵۵ -
عنوان و نام پدیدآور	: شناخت تهدیدات فضای سایبری و پدافند از آن / مولفین داود آذر، حسین مسلمی.
منشخصات نشر	: تهران: ارتش جمهوری اسلامی ایران، دانشگاه فرماندهی و ستاد آجا، انتشارات دافوس، ۱۳۹۲.
منشخصات ظاهری	: ۱۱۸ص: جدول.
شابک	: ۹۷۸-۹۶۴-۲۵۲۳-۶۹-۶
وضعیت فهرست نویسی	: فیپا
یادداشت	: کتابنامه: ص. ۱۰۹-۱۱۱.
موضوع	: شبکه‌های کامپیوتری — تدابیر امنیتی
موضوع	: کامپیوترها — ایمنی، اطلاعات
موضوع	: فضای مجازی — تدابیر امنیتی
شناسه افزودن	: مسلمی، حسین، ۱۳۴۹
شناسه افزوده	: ایران. ارتش، دانشگاه فرماندهی و ستاد. انتشارات
رده بندی کنگره	: ۱۳ ش ۹۱۴/۵/۵۹/۱۰ TK۵۱۰
رده بندی دیویی	: ۵/۱
شماره کتایشناسی ملی	: ۳۷۲ ۲



عنوان	: شناخت تهدیدات فضای سایبری و پدافند از آن
مؤلفین	: داود آذر، حسین مسلمی
ویراستار	: حسین موسوی ف
طرح روی جلد	: محمدرضا حریشه رلو
صفحه‌آرایی	: مرتضی جباری
ناشر	: انتشارات دانشگاه فرماندهی و ستاد آجا، دانشگاه جنگ آجا
شمارگان	: ۱۰۰۰ جلد
تاریخ انتشار	: بهار ۱۳۹۳
چاپ	: اول
لیتوگرافی، چاپ و صحافی:	: چاپخانه دانشگاه فرماندهی و ستاد آجا
قیمت	: ۶۰۰۰ تومان
نشانی	: تهران، میدان پناستور، خیابان دانشگاه جنگ، دانشگاه فرماندهی و ستاد آجا

تلفن: ۰۲۱-۶۶۴۱۴۱۹۱

www.dafoosaja.ac.ir

مسئولیت صحت مطالب بر عهده‌ی مؤلفین می‌باشد.
کلیه حقوق برای دافوس آجا محفوظ است. (نقل مطالب با ذکر مأخذ بلامانع است).

پیش‌گفتار:

از آن‌جا که امنیت امری نسبی است، مقابله با تهدیدهای سایبری به‌منظور از بین بردن و محو کامل آن‌ها، امر غیرممکنی می‌باشد. بنابراین حفاظت از اطلاعات و داده‌ها در برابر این تهدیدهای، بدون آن‌که اختلالی در رشد و نوآوری و توسعه ایجاد شود، یک مسئله مهم به‌شمار می‌آید. مقابله با تهدیدهای سایبری به‌معنی حفاظت از مالکیت مادی و معنوی اطلاعات ارزشمند در حوزه اقتصاد، سیاست و نظامی به‌صورت دیجیتال (نرم‌افزاری)، در برابر سرقت، جعل، تحریف، از کاراندازی و هر نوع سوءاستفاده است. در حال حاضر این موضوع به‌طور فزاینده‌ای تبدیل به یک مسئله مهم شده است، به‌طوری‌که امروزه مقابله با تهدیدهای سایبری یکی از جدی‌ترین چالش‌های امنیت ملی و نظامی و انتظامی برای دولت‌ها محسوب می‌شود. به‌عبارت دیگر حفاظت از مرزهای مجازی به اندازه حفاظت از مرزهای روی نقشه، برای هر کشوری دارای اهمیت است.

ورود به هر موضوعی ابتدا به شناخت آن نیاز دارد. معرفی راه‌کارهای مقابله با تهدیدهای سایبری، قبل از هر چیز مستلزم شناخت تهدیدهای سایبری است با توجه به پیشرفت علوم و بالا گرفتن سطح تهدیدات به‌صورت فرامنطقه‌ای، بی‌طلبی هر چه زودتر اقداماتی در ارتباط با تجهیز و ارتقای توان علمی و سامانه‌های جنگ و دفاع سایبری اندیشده، و خود را برای جنگ‌های نوین آینده آماده‌تر نماییم.

داود آذر

حاکمین مسلمی

فهرست

صفحه

پیش‌گفتار	۰
مقدمه	۷
فصل اول	۹
تعاریف و مفاهیم فضای سایبر	۹
فصل دوم	۱۹
تأثیر جنگ‌ها در فضای سایبر	۱۹
فصل سوم	۳۱
ویژگی‌ها و ابزارهای سایبری	۳۱
فصل چهارم	۳۹
شکل‌گیری جنگ سایبر	۳۹
فصل پنجم	۵۳
اصول امنیت در فضای سایبر	۵۳
فصل ششم	۸۱
امنیت پایگاه‌های داده	۸۱
فصل هفتم	۹۱
رویکردی عملی به امنیت شبکه	۹۱
فصل هشتم	۱۰۵
رویکرد و اقدامات کشورهای مختلف	۱۰۵
منابع	۱۱۴

مقدمه:

امروزه با گسترش بدون مرز زیر ساخت‌های الکترونیک در دنیا و متعاقب آن در تمامی ارگان‌ها، بُعد جدیدی به سایر ابعاد زندگی ما اضافه شده است که همان بُعد مجازی (سایبر) است. این بُعد جدید تعاریف و ویژگی‌هایی مختص به خود را دارد و لازم است که با توجه به ماهیت بسیار پویا و متغیر آن، نگاه متفاوتی به مفاهیمی همچون تدوین و اجرای راهبرد، یا مدیریت راهبردی در آن حوزه داشته باشیم، زیرا نوع تهدیدهایی و ویژگی‌هایی که در این فضا انسان‌ها، جوامع و زیرساخت‌ها هر نهادی را هدف قرار می‌دهند نیز با تهدیدهای روزمره دیگر بسیار متفاوت دارد. برای واضح شدن مطلب شاید گفتن این جمله که "با یک ویروس ۱۵ کیلوبایتی رایانه‌ای می‌توانید هزاران بمب اتمی را کنترل کنید ولی همین هزاران بمب اتمی به هیچ عنوان نمی‌تواند این ویروس ۱۵ کیلو بایتی را از بین ببرند" خود به خوبی بیانگر ماهیت متفاوت تهدیدهای سایبری می‌باشد. جامعه امن به گونه‌ای که در افق ۱۴۰۴ نوید داده شده، جامعه‌ای است که در همه بخش‌های آن، تهدید یا خطری در میان نباشد. از این‌رو در سند چشم انداز بیست ساله امنیت سایبری یکی از مفاهیم کلیدی است. امنیت، استقلال و اقتدار به‌عنوان سه ویژگی، به عنوان نظام جمهوری اسلامی ایران است که هر سه پیوند تنگاتنگی با امنیت سایبری برقرار می‌کنند. طبق این اصول، جامعه‌ی ایرانی در افق این آینده خود چنین ویژگی‌هایی خواهد داشت: این استقلال و مقتدر با سامانه‌ی دفاعی مبتنی بر بازدارندگی همه جانبه و پیوستگی مردم و جوامع ارگان‌های نظامی و انتظامی. از این‌رو، در شرایطی که حمله سایبری از دیدگاه برخی از کشورها از قبیل آمریکا و رژیم اشغالگر اسرائیل به‌عنوان حمله نظامی تلقی و زمینه‌های جدی جنگ‌های فیزیکی نظامی را فراهم خواهد نمود و در این مبنا نیز مراکز دفاع سایبری پیشرفته‌ای را باید از این‌رو از این‌رو به روشنی می‌توان دریافت که جنگی جدی در فضای سایبر در حال شکل‌گیری است، جنگی که به شدت زیر ساخت‌های سایبری و غیرسایبری کشور را در تمامی ابعاد تهدید می‌کند. از این‌رو اهمیت دفاع سایبر با نگاه راهبردی بیش از هر موضوع دیگری خود نمایی می‌کند.

نظر به این که فضای سایبری از علوم نوپای جوامع علمی امروزی بوده و نقاط ابهام بسیاری در زمینه امنیت آن وجود دارد، به‌عقبر می‌رسد که شناسایی تشابهات این فضا با علوم دیگری که از سابقه مطالعاتی بیشتری برخوردارند، می‌تواند کمک شایانی به پیشبرد اهداف

این فضا نماید. تأمین امنیت فضای سایبر بدون همکاری تنگاتنگ کلیه اقشار کارکنان میسر نمی‌باشد.

هدف اصلی در این نوشتار پاسخ‌گویی به مباحث دفاع سایبری، مرتبط با ساختار غیر عامل است. هم‌چنین سعی شده تا پس از نگاهی جمالی بر جایگاه، ساختار، ویژگی‌ها، روش‌های ایجاد امنیت و دفاع به طور مفصل در فصل‌های زیر مورد بررسی قرار گیرد.

فصل اول تعاریف و مفاهیم فضای سایبر

فصل دوم بررسی تاریخچه جنگ‌ها در فضای سایبر

فصل سوم تحلیل و بررسی ویژگی‌ها و جنگ‌ها در فضای سایبر

فصل چهارم شکل‌گیری جنگ سایبر

فصل پنجم اصول امنیت در فضای سایبر

فصل ششم مروری بر امنیت بسترهای داده

فصل هفتم رویکردی عکس به امنیت شبکه

فصل هشتم رویکرد و اقدامات کلیدی در دفاع سایبر

امید است که این کتاب بتواند آشنایی لازم را در مورد شناخت تهدیدات فضای سایبری و دفاع از آن‌ها به خواننده منتقل کرده و راه را برای سیراحی سیستم‌های امن فراهم نماید.