جنگ سایبری

ایجاد پایه و اساس علمی

مؤسسه آموزشی و تحقیقاتی صنایع دفاعی
حوزه نوآوری آرایه‌های دفاعی

عنوان و نام پدیدآور : جنگ سایبری (ایجاد پایه و اساس علمی)/ نویسندگان سوشیل جاجودیا ... [و دیگران]؛ مترجم حوزه نوآوری آرایه‌های دفاعی.

مشخصات نشر : تهران: موسسه آموزشی و تحقیقاتی صنایع دفاعی، حوزه نوآوری آرایه‌های دفاعی، ۱۳۹۶.

مشخصات ظاهری : ۵۳۷ ص.

شابک : ۹۷۸۶۰۰۸۷۹۳۲۶۷

عنوان اصلی : Cyber Warfare Building the Scientific Foundation, c2015

موضوع : شبکه‌های کامپیوتری -- تدابیر ایمنی-- تروریسم رایانه‌ای -- ایمنی اطلاعات-- پیشگیری-- فضای مجازی --امنیت ملی

شناسه افزوده : جاجودیا، سوشیل ۱۹۴۱ - م. Jajodia, Sushil

شناسه افزوده : موسسه آموزشی و تحقیقاتی صنایع دفاعی. حوزه نوآوری آرایه‌های دفاعی

رده بندی کنگره : ۱۳۹۶ ۹ج/TK ۵۱۰۹/۵۹

رده بندی دیویی : ۰۰۵/۸

شماره کتابشناسی ملی: ۵۰۸۷۰۶۳

عنوان: جنگ سایبری، ایجاد پایه و اساس علمی

مترجم: حوزه نوآوری آرایه‌های دفاعی

ناشر: مؤسسه آموزشی و تحقیقاتی صنایع دفاعی ـ حوزه نوآوری آرایه‌های دفاعی

آماده‌سازی و نظارت بر ترجمه و چاپ: مدیریت دانش حوزه نوآوری آرایه‌های دفاعی

نوبت چاپ: اول- زمستان۱۳۹۶

شمارگان: ۵۰۰ جلد

قیمت: ۴۰۰۰۰ تومان

نشانی: بالاتر از میدان نوبنیاد، پاسداران شمالی، نبش کوهستان هشتم، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی،

تلفن: ۲۲۸۰۸۷۰۷ نمابر:۲۲۸۰۸۷۷۴

پیش‌گفتار نویسنده

وابستگی هرچه بیشتر روزافزون به شبکه‌های کامپیوتری، گوشی‌های هوشمند و اینترنت هدف جدیدی در زمینه درگیری‌ها فراهم ساخته است. درواقع، جنگ سایبری[1] به عنوان بخشی از سیاست‌های کشور از قبل شکل گرفته است. برای درک آثار آشکار شده این حوزه در جریان درگیری‌ها فقط کافی است سرخط اختیار رادیو و تلویزیون و تیتر درشت روزنامه‌ها را در جریان جنگ روسیه و گرجستان در زمینه‌های استاکس‌نت[2]، آئوروا[3] یا حملات سایبری مورد توجه قرار دهیم.

در حالی که ما شاهد بسیاری مفاهیم پیشرفته مهندسی (مانند ایجاد دیوارهای آتش، ابزار متا اسپلویت) یا حتی بدافزارهای پیشرفته مانند «Flame» که به‌طور مستقیم بر روی جنگ سایبری تأثیر می‌گذارند، هستیم، تمامی این مفاهیم‌ها براساس بهترین تجربیات، قانون کلی، فنون سعی و خطا توسعه یافته‌اند. هرچند که این اختراعات تأثیر زیادی دارند و از اهمیت بالایی برخوردارند، تاریخ به‌طور مکرر به

1 Cyber Warfare
2 Stuxnet
3 Aurora

ما آموخته است که استقرار اصول علمی منجر به پیشرفت سریع و قابل‌توجه خواهد شد.

ازاین‌رو، این کتاب برای استقرار پایه و اساس علمی برای جنگ سایبری طراحی شده است. در این کتاب مجموعه‌ای از آخرین نتایج تحقیقات در این زمینه که حاصل کار چندین محقق برتر در گوشه‌کنار جهان است، گردآوری شده است. در این کتاب بسیاری از جنبه‌های مهم درگیری‌های سایبری که شامل استفاده از باتنت‌ها، موقعیت‌یابی کندوهای عسل، انکار و فریب، عامل انسانی و مشکل انتساب می‌شود، موردبررسی قرار می‌گیرد. افزون بر این، در این کتاب تلاش شده است که تنها بر روی جنبه‌های ساده مختلف از جنگ سایبری تمرکز نشود، بلکه به بسیاری از فنون علمی گسترده‌ای که می‌توانند برای حل کردن مشکلات موجود در این حوزه مورد استفاده قرار گیرند پرداخته شود. فصل‌های این کتاب به مسائلی مانند نظریه بازی، مدل‌سازی شناختی، بهینه‌سازی، برنامه‌نویسی منطقی، تجزیه‌وتحلیل داده‌های عظیم و چندین مورد دیگر می‌پردازد.

امیدواریم که این کتاب الهام‌بخش محققان برای ایجاد دانش‌های بیشتر در حوزه جنگ سایبری گردد و درنهایت بتوان اینترنت را امن‌تر و قابل‌اعتمادتر نمود.

درباره کتاب

سه فصل اول این کتاب بعضی از دیدگاه‌ها و اصول جنگ سایبری را معرفی می‌کنند. در فصل اول، تأثیر استفاده از حملات سایبری به‌عنوان تسلیحات راهبردی کلیدی در درگیری‌های بین‌المللی بررسی می‌شود و مدل‌های تئوری مبتنی بر بازی برای حل مشکلات موجود درزمینه جنگ سایبری ارائه می‌شوند. در فصل دوم، قابلیت جدیدی بر اساس مدل‌سازی چند فرمالیسمی ارائه می‌شود و سپس این قابلیت تجزیه‌وتحلیل می‌شود و تأثیرات حملات سایبری در زمینه هماهنگی برای

تصمیم‌گیری در سازمان‌ها گفته می‌شود. در فصل سوم، توضیح داده می‌شود که چگونه مهاجمی که از برتری سایبری برخوردار است دارای مزایای خوبی در به دست آوردن اهداف مأموریتی خود می‌باشد.

فصل‌های بعدی فریب سایبری و رویکردهای مبتنی بر بازی را بررسی می‌کنند. در فصل چهارم، یک چارچوب نظریه بازی برای برنامه‌ریزی در زمینه ایجاد طرح‌های موفق برای فریب دشمن در فضای سایبر ارائه می‌شود. در فصل پنجم، استفاده از نظریه بازی برای امنیت شبکه بررسی می‌شود و چندین مدل برای نظریه بازی ارائه می‌شود که بر روی استفاده از *تله‌های عسل*[1] برای امنیت شبکه تمرکز دارند. در فصل ششم، مبارزه با فریب‌کاری سایبری توضیح داده می‌شود و اینکه چگونه می‌توان آن را در دفاع سایبری برای شناسایی و مقابله با مهاجمان سایبری به کار برد. در فصل هفتم، چالش‌های یافتن دشمنان سایبری از طریق نظارت بر شبکه توضیح داده می‌شود، حتی وقتی‌که دشمنان از عملیات فریب‌کاری برای پنهان‌سازی فعالیت‌ها و نیت خود استفاده می‌کنند. در فصل هشتم، یک سیستم مبتنی بر استدلال رسمی که به تحلیل‌گر در زمینه انتساب حملات سایبری کمک می‌کند (حتی درزمانی که اطلاعات در دسترس، متناقض و یا نامشخص هستند) ارائه می‌شود.

در فصل‌های ۹ تا ۱۲ جنبه‌های رفتاری و اجتماعی امنیت سایبر و جنگ سایبری بررسی می‌شوند. در فصل نهم، نقش عامل انسانی در امنیت سایبری (هم برای مهاجمان و هم برای مدافعان) بررسی می‌شود. در فصل دهم، یک مدل معروف، چندعاملی و شناختی برای تصمیم‌گیری (که از طریق تجربه و مطالعه رفتاری به‌دست‌آمده است) ارائه می‌شود. در فصل یازدهم، مشکل یافتن گره‌های پنهان در

1 Hony Pots

شبکه‌های اجتماعی برای انجام حملات سایبری بررسی می‌شود. در فصل دوازدهم، الگوریتم‌هایی که ساختار جامعه را درون شبکه‌ها کشف می‌کنند و آن‌ها را با یکدیگر مقایسه می‌کنند بررسی می‌شوند.

فصل‌های سیزدهم و چهاردهم بر مبنای فیلد داده‌های مقیاس بزرگ از میان میلیون‌ها میزبان واقعی می‌باشند. در فصل سیزدهم، نتایج مطالعات تجربی انجام شده در زمینه امنیت جهان واقعی با استفاده از داده‌های جمع‌آوری‌شده از ۱۰ میلیون میزبان واقعی ارائه شده است. در فصل چهاردهم، تکنیک‌های استفاده از کاوش گراف در مجموعه‌های فیلد داده بزرگ برای حل مشکلات امنیت سایبری بررسی می‌شوند. نهایتاً در فصل پانزدهم، توضیح داده می‌شود که چگونه پیشرفت در زمینه زبان برنامه‌نویسی می‌تواند مشکلات سایبری و امنیت کامپیوتری را حل کند. همچنین در این فصل توضیح داده می‌شود که تکنیک‌های تحقیقاتی کنونی برای ضمانت امنیت ناکافی هستند.

فهرست مطالب