

جنگ سایبری

تکنیک‌ها، تاکتیک‌ها و ابزارها برای

مدیران حوزه امنیت



مؤسسه آموزشی و تحقیقاتی صنایع دفاعی

حوزه نوآوری آرایه‌های دفاعی

دارای مجوز سازمانی نشر از شورای سیاست‌گذاری و انتشارات

مؤسسه آموزشی و تحقیقاتی صنایع دفاعی

کلیه حقوق محفوظ و متعلق به مؤسسه آموزشی و تحقیقاتی صنایع دفاعی است.

هر نوع تکثیر یا نشر تمام یا بخش‌های مستقلی از این کتاب، منوط به اجازه کتبی ناشر است.

سرشناسه	: اندرس، جیسن	Andress, Jason
عنوان و نام پدیدآور	: جنگ سایبری: تکنیک‌ها و تاکتیک‌ها و ابزارها برای فعالان حوزه امنیت / [تألیف جیسن اندرس، استیو ویتترفلد]؛ مترجم طرح فراسازمانی فاوا و همکاران.	
مشخصات نشر	: تهران: موسسه آموزشی و تحقیقاتی صنایع دفاعی، حوزه نوآوری سازمان و مدیریت دفاعی، ۱۳۹۶.	
مشخصات ظاهری	: ۶۶۹ ص.	
شابک	: ۹۷۸۶۰۰۸۷۹۳۲۵۰	
عنوان اصلی	: Cyber warfare : techniques, tactics and tools for security practitioners, 2nd. ed, [2014].	
عنوان دیگر	: تکنیک‌ها، تاکتیک‌ها و ابزار امنیتی و کاربردی برای جنگ‌های سایبری.	
عنوان دیگر	: جنگ سایبری: (تکنیک‌ها، تاکتیک‌ها و ابزار برای دست‌اندرکاران امنیتی).	
موضوع	: جنگ اطلاعات — دستنامه‌ها — شبکه‌های کامپیوتری — تدابیر ایمنی — دستنامه‌ها	
شناسه افزوده	: ویتترفلد، استیو	Winterfeld, Steve
شناسه افزوده	: موسسه آموزشی و تحقیقاتی صنایع دفاعی. طرح فراسازمانی فاوای نیروهای مسلح	
شناسه افزوده	: موسسه آموزشی و تحقیقاتی صنایع دفاعی. حوزه نوآوری آرایه‌های دفاعی	
رده بندی کنگره	: ۱۳۹۶ ۷۸۸ الف/۱۶۳/۲۲	
رده بندی دیویی	: ۳۵۵/۳۴۳	
	شماره کتاب: ناسی ملی: ۵۰۸۷۰۴۱	

عنوان: جنگ سایبری، تکنیک‌ها، تاکتیک‌ها و ابزارها برای فعالان حوزه امنیت

مترجم: طرح فراسازمانی فاوا و همکاران

ویراستار و نظارت بر ترجمه و چاپ: طرح فراسازمانی فاوا

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

آماده‌سازی چاپ: مدیریت دانش حوزه نوآوری آرایه‌های دفاعی

نوبت چاپ: اول - زمستان ۱۳۹۶

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

پیش گفتار

چرا یک کتاب درباره جنگ سایبری می‌نویسم؟

«امروزه مشخص شده است که تهدید سایبری به یکی از بزرگ‌ترین چالش‌های امنیتی ملی و اقتصادی تبدیل شده است که ما با آن مواجه هستیم.» ما به عنوان یک کشور یا یک دولت به اندازه کافی برای مقابله با این خطر آماده نیستیم [۱].

بر طبق گفته مدیر سازمان اطلاعات ملی آمریکا آقای «James Clapper»، تهدید جنگ سایبری که آمریکا با آن مواجه است در حال افزایش یافتن است و دشوار است که بتوان درباره تأثیر آن اغراق کرد. بسیاری از مؤسسات آموزشی هم در سطح نظامی و هم در سطح غیرنظامی با این سؤال مواجه هستند که «ما باید درباره امنیت سایبری به دانشجویان خود چه چیزی را آموزش دهیم؟» وقتی این دانشجویان در آینده در جایگاه خود به عنوان مدیر و یا افسر اطلاعاتی، نقش دفاع از کشور را بر عهده دارند باید از تهدیدات پایدار آگاه باشند.

امروزه به‌طور پیوسته مقیاس خطرات در حال تغییر کردن است و ما باید اقدامات متقابل و مأموریت‌های مختلف خود را از شناسایی سارقین گرفته تا شناسایی جرائم و جاسوسی‌ها در سطح ملی و شناسایی کرم‌های کامپیوتری مانند استاکسنت که هدف خرابکاری دارند، ادامه دهیم. حدود یک دهه قبل بود که تعدادی کودک تنها به علت هیجان ناشی از هک کردن، به سیستم‌ها حمله می‌کردند. سپس این عمل به‌عنوان یک عمل مجرمانه شناخته شد. در حال حاضر به نظر می‌رسد این قضیه بیشتر با سانه‌های اجتماعی، ایدئولوژی افراد و تهدیدات خودی مرتبط است. این کتاب توضیحات بسیار خوبی را درباره گستردگی خطرات موجود و چالش‌هایی که ما امروزه با آن‌ها مواجه هستیم فراهم می‌کند.

در ماه مه [سال ۱۳۹۴]، مجله‌ای به نام «the Atlantic Wire» گزارش کرد که چین در حال پیروز شدن در جنگ سایبری است؛ زیرا آن‌ها به برنامه‌های جنگی فیزیکی آمریکا دست پیدا کرده‌اند. همچنین ادوارد اسنودن ادعا کرده است که ایالات متحده و رژیم صهیونیستی با همکاری کدیگر ویروس استاکسنت را علیه برنامه اتمی ایران نوشته‌اند. ما هنوز در حال تلاش برای فهمیدن چگونگی عملکرد این ویروس هستیم. در حالی که ویکی‌لیکس و گروه ناشناس (گروه عقیده محوری که سازمان‌هایی را که از ویکی‌لیکس حمایت نمی‌کنند، مجازات می‌کند) اخیراً اعلام کرده‌اند که سرقت برنامه احراز هویت دو عاملی^۱ به‌شدت باعث ایجاد دلسردی شده است. اگر کنترل دسترسی از بین رود همه چیز از بین خواهد رفت. امروزه سرقت هویت به یک امر عادی تبدیل شده است که دیگر ارزش خبری ندارد. چند نفر از مردم در ایالات متحده اطلاعات هویتی آن‌ها به سرقت رفته است؟ بیشتر متخصصین می‌گویند که اطلاعات همگی مردم به سرقت رفته است. اطلاعات بسیار زیادی به سرقت رفته است که مجرمان حتی هنوز نمی‌دانند چگونه می‌توانند از آن‌ها استفاده

1 Two-factor authentication

کنند، ولی روزی بالاخره خواهند توانست از تمامی آن اطلاعات استفاده کنند. گروه‌های تبهکار، دانشمندان کامپیوتری را استخدام می‌کنند تا کلاه‌برداری‌های سایبری آن‌ها را انجام دهند. اصطلاح جنگ سایبری در حال تبدیل شدن به بحث همیشگی در گفتگوهای امنیت ملی است. امنیت سایبری مسئله‌ای است که در سطح شخصی، مانند کاربران اینترنتی، می‌تواند بر روی زندگی ما تأثیر بگذارد و در سطح دفاع ملی به‌عنوان یک تهدید پیشرفته و پایدار برای کشور مطرح است.

چرا باید این کتاب را بخوانید؟

همگی ما به‌دختراتی که اطلاعات ما با آن‌ها مواجه هستند را درک کنیم تا بتوانیم تصمیمی آگاهانه بگیریم و گام‌های لازم برای امن کردن اطلاعات خود را برداریم.

اینترنتی که در خانه از آن استفاده می‌کند تا با دوستانان از طریق اسکایپ^۱ صحبت کنید و یا بازی برخط انجام دهد و نامه‌های الکترونیکی خود را ارسال کنید، ممکن است برای انجام اعمال مجرمانه، انجام جاسوسی بین‌المللی و یا حتی در مبارزه با نوع جدیدی از جنگ سایبری مورد استفاده قرار گیرد.

این نوع جدید از اینترنت امروزی برای هر یک از ما به‌دخترت شخصی و چه در سطح ملی مهم است. جنگ سایبری بیشتر در سطح ملی در برهه‌ای است که وزارت دفاع (آمریکا) چه عملی را انجام می‌دهد تمرکز می‌کند.

ما حتی یک هفته را هم بدون شنیدن اخبار درباره جنگ سایبری و اینکه گروه‌های هکری در حال گسترش نرم‌افزارهای مخرب در اینترنت هستند، پشت سر نخواهیم گذاشت. جنگ سایبری به‌وسیله نشان دادن ارتباط تمامی حملات با

یکدیگر و نحوه عمل کردن این تهدیدات، خطر موجود را برای مردم قابل درک می‌سازد.

اگر شما برای دولت ایالات متحده کار می‌کنید یا اینکه می‌خواهید بدانید که دولت آمریکا چه کاری را انجام می‌دهد تا به تهدیدات سایبری پاسخ دهند، در فصل اول (جنگ سایبری چیست) با جزئیات کامل به این موضوع پرداخته می‌شود. این کتاب به شما نشان خواهد داد که چگونه حملات سایبری و دفاع در مقابل آن تمامی حوزه‌های جنگی کلاسیک مانند زمینی، دریایی، هوایی، فضایی (مشارک با نیروی هوایی) و سایبری که توسط فرماندهی سایبری آمریکا (USCYBERCOM) سازمان‌دهی می‌شود، درگیر می‌کند.

جنگ سایبری دکترین عامی که در حال توسعه می‌باشد را پوشش می‌دهد و تاکتیک‌ها، تکنیک‌ها و روال عملیات شبکه‌های کامپیوتری (CNO)^۱ که شامل حمله، دفاع و بهره‌برداری^۲ (این یک اصطلاح ناامی برای عملیات جاسوسی و یا شناسایی است) و همچنین جنبه جدیدی از مهندسی اجتماعی است را سازمان‌دهی می‌کند. از نقطه نظر شخصی، آسان است که درباره مهندسی اجتماعی بخوانیم و با خود بگوییم که «بله درست است ولی من در شبکه‌های اجتماعی مابین سایر مردم هستم.» چندی پیش یک شخصیت ساختگی به نام «Robin Sage» توسط یک محقق امنیتی ساخته شد تا بفهمد که چه مقدار اطلاعات را می‌تواند از طریق فیس‌بوک جمع‌آوری کند. در ادامه در فصل‌های این کتاب درباره اینکه جنگ سایبری چیست و اینکه چگونه جنگ سایبری انجام می‌شود توضیح خواهیم داد. همان‌طور که نویسنده در این کتاب مسائل قانونی و اخلاقی پیرامون این میدان نبرد جدید را مطرح می‌کند، دلیل اینکه چرا جنگ سایبری روی می‌دهد مشخص

1 Computer Network Operations

2 Exploit

می‌شود. سپس، این کتاب چالش‌های پیش‌روی فضای سایبر را آنالیز و تعریف می‌کند. درنهایت به تمایلات موجود پیرامون این موضوع می‌پردازد.

جنگ سایبری به خوانندگان یک درک بنیادی قوی از تهدیدات موجود که هر هفته در اخبار مشاهده می‌کنند، می‌دهد. در اینجا به این نکته می‌پردازیم که چرا جنگ سایبری مهم است. در ابتدای این پیشگفتار من با خود گفتم که «چرا من سرگیزه دارم؟» «چون مسائل بسیار زیادی پیرامون این موضوع وجود دارد که من نمی‌توانم همگی آن‌ها را پیگیری کنم؟» جواب این سؤال خیر است. چیزی که باعث گیج شدن من شد این است که ما داریم درباره موضوعی گفتگو می‌کنیم که ۱۳ سال قبل وقتی من به عنوان دانشجو در جنگ سایبری در سازمان دفاع ضد موشکی بودم مطرح شد. امروزه کلمات اختصار پیرامون این موضوع بیشتر شده‌اند و همچنین پول بیشتری در این زمینه هزینه می‌شود. ولی هیچ‌یک از مسائل پایه‌ای و بنیادی تغییر نکرده است. در آن زمان، روسیه به دنبال این بود که توافقات بین‌المللی لازم بر سر این موضوع که با جنگ سایبری باید به‌عنوان یک سلاح راهبردی رفتار کرد را کسب کند. ولی ما گوش نکردیم. من گمان می‌کنم دلیل مخالفت ما این بود که فکر می‌کردیم که فناوری و تکنیک‌های ما پیشرفته‌تر و بهتر هستند. علاوه بر این، بسیاری از مردم با خود می‌گفتند «آیا واقعا جنگ سایبر یک مسئله مهم است؟» بسیار دیگری از مردم حتی از این موضوع اطلاعی نداشتند. از دیدن آن (به شوخی) اگر این موضوع به گاو بازان و تیم «Redskin» ربطی ندارد چرا باید مهم باشد؟ ولی ما چیزی را فراموش کرده‌ایم. ما چیزهای زیادی داریم که می‌توانیم از دستشان دهیم. کشور آمریکا بیشترین اطلاعات برخط^۱ را نسبت به هر کشور دیگری در اینترنت دارد و این امر باعث می‌شود که ما به بزرگ‌ترین هدف برای حملات سایبری تبدیل شویم. ما این فرصت را در پیش از یک دهه قبل داشتیم که برای همکاری

دولت، صنعت و بخش خصوصی گفتگوها را شروع کنیم. ما این فرصت را داشتیم که تا توافقات بین‌المللی بر سر این موضوع را ایجاد کنیم. ولی ما این فرصت‌ها را از دست دادیم. شواهد قانع‌کننده‌ای وجود دارد که نشان می‌دهد تهدید سایبری وجود دارد. ما باید خودمان را تعلیم دهیم و قانون‌گذاران خود را تشویق کنیم که قوانینی را برای این موضوع ایجاد کنند. ما باید دولت خود را قانع کنیم که دلارهای مالیاتی ما را به‌ای انجام سرمایه‌گذاری‌های بیهوده، در زمینه سایبری خرج کند. کتاب جنگ سایبری به شما اجازه می‌دهد که دانش خود را در این زمینه افزایش دهید و تصمیم بگیرید که در این زمینه کشور باید چه عملی را انجام دهد و از خطری که در صورت انجام ندان عملی برای مقابله با جنگ سایبری با آن مواجه خواهید شد مطلع شوید. بیش از یک قرن پیش ما فرصت خود را برای انجام اقدام جامع در سطح بین‌المللی از دست دادیم و ما محرم هزینه‌های زیادی شدیم. این بار ما می‌خواهیم چه کاری انجام دهیم؟

این متن توسط «Stephen Northcutt» نوشته شده است.

منابع

- [1] President Barack Obama. Remarks by the president on securing our nation's cyber infrastructure [home page on the Internet]. Washington, DC: The White House, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/; 2010 [accessed 15.02.10].
- [2] Allen V. Cyber warfare threats to U.S. are increasing: top spy [home page on the Internet]. New York: Thomson Reuters, <http://www.reuters.com/article/2011/02/10/us-usa-intelligence-cyberspaceidUSTRE7194E320110210>; 2010 [accessed 15.02.10].

فهرست مطالب

مقدمه	۲۱
فصل اول: جنگ سایبری چیست؟	۳۱
۱-۱-۱ جنگ سایبری چیست؟	۳۲
۱-۱-۱-۱ پیش زمینه	۳۲
۱-۱-۲ دلایل تاکتیکی و عملیاتی برای جنگ سایبری	۴۰
۱-۱-۳ قدرت و راهبرد سایبری	۴۲
۱-۱-۴ کنترل تسلیحات سایبری	۴۷
۱-۱-۵ ایالات متحده درباره تهدیدات جنگ سایبری چه کاری انجام می دهد؟	۵۰
۱-۲-۱ آیا ما یک جنگ سایبری را دیده ایم؟	۵۴
۱-۲-۱ مطالعات موردی	۵۷
۱-۲-۲ مناظره (آیا تهدید جنگ سایبری واقعی است؟)	۶۲
۱-۳-۱ چرا جنگ سایبری مهم است؟	۶۵
۱-۴-۱ خلاصه	۶۷

منابع	۶۹
فصل دوم: تهدیدات گوناگون سایبری	۷۳
۱-۲ چگونه به اینجا رسیدیم؟	۷۳
۲-۲ شناسایی روش‌های حملات با استفاده از ابزارها و تکنیک‌هایی که برای اجرای آن‌ها	
مورد استفاده قرار می‌گیرند	۸۱
۳-۲ مهاجمان (مهم‌ترین دسته‌بندی تهدیدات)	۹۳
۱-۳-۲ تهدید پایدار پیشرفته	۹۳
۲-۳-۲ جرم سازمان‌یافته	۹۴
۳-۳-۲ تهدید درون‌رمانی	۹۶
۴-۳-۲ فعالان خارجی	۹۷
۵-۳-۲ اسکرپت‌بازها / تجزیه‌ها	۹۸
۴-۲ دفاع در عمق - امروزه چگونه سازمان‌ها دفاع می‌کنند	۱۰۰
۵-۲ تهدید پیش‌رو چیست (در دفاع باید روشن شود چه چیزی تمرکز داشته باشیم).	۱۰۷
۶-۲ خلاصه	۱۰۹
منابع	۱۱۰
فصل سوم: میدان نبرد فضای سایبر	۱۱۱
۱-۳ مرزها در جنگ سایبری	۱۱۲
۱-۱-۳ دفاع در عمق	۱۱۴
۲-۱-۳ زیرساخت فیزیکی	۱۱۶
۳-۱-۳ دید سازمانی	۱۱۹
۲-۲ چه هنگام سایبر در حوزه جنگی کاربرد دارد	۱۲۸
۱-۲-۳ حوزه زمینی	۱۳۰
۲-۲-۳ حوزه دریایی	۱۳۱
۳-۲-۳ حوزه هوایی	۱۳۲
۴-۲-۳ حوزه فضایی	۱۳۴

۱۳۵	۵-۲-۳- حوزه سایبری
۱۳۶	۶-۲-۳- تسلیحات ترکیبی
۱۳۶	۳-۳- بررسی بازیگران تهدید سایبری
۱۳۷	۱-۳-۳- بیشترین تهدیدات فعال
۱۳۹	۲-۳-۳- خطرناک‌ترین تهدیدات
۱۴۴	۲-۳-۳- انگیزه‌ها
۱۴۸	۴-۳- به‌کارگیری سیستم‌های عملیاتی در هنگام نیاز
۱۵۱	۵-۳- خلاصه
۱۵۲	منابع
۱۵۵	فصل چهارم: دکترین سایبری
۱۵۶	۱-۴- دکترین کنونی ایالات متحده
۱۵۹	۱-۱-۴- نیروهای ایالات متحده
۱۶۳	۲-۱-۴- دکترین مشترک
۱۶۹	۳-۱-۴- نیروی هوایی ایالات متحده
۱۷۲	۴-۱-۴- نیروی دریای ایالات متحده
۱۷۴	۵-۱-۴- نیروی زمینی ایالات متحده
۱۷۷	۶-۱-۴- وضعیت عملیات اطلاعاتی وزارت دفاع
۱۸۰	۲-۴- مثال‌هایی از دکترین و راهبردها در گوشه‌کنار جهان
۱۸۱	۱-۲-۴- پیش‌زمینه
۱۸۳	۲-۲-۴- دکترین چین
۱۸۹	۳-۲-۴- سایر کشورهای آسیایی
۱۹۱	۴-۲-۴- کشورهای اروپایی
۱۹۴	۵-۲-۴- نیروهای خصوصی و یا مزدورها
۱۹۵	۳-۴- اصول نظامی کلیدی که باید با جنگ سایبری تطبیق داده شود
۱۹۶	۱-۳-۴- آماده‌سازی اطلاعات نظامی در محیط عملیاتی

- ۱۹۷-۲-۳-۴- میزان اثربخشی مهمات مشترک
- ۱۹۸-۳-۳-۴- مقیاس کارآمدی
- ۱۹۹-۴-۳-۴- ارزیابی خسارت نبرد
- ۲۰۰-۵-۳-۴- پشتیبانی هوایی نزدیک
- ۲۰۰-۶-۳-۴- مقابله با شورش
- ۲۰۱-۴-۴- د. تورالعمل‌ها و رهنمودها
- ۲۰۱-۴-۴- ا. اتنام جامع امنیت سایبری ملی
- ۲۰۲-۴-۴- وزارت امنیت داخلی
- ۲۰۷-۳-۴-۴- د. مورات ریاست جمهوری / امنیت داخلی
- ۲۰۹-۴-۴-۴- مؤسسه ملی فناوری و استاندارد
- ۲۱۲-۵-۴-۴- دانشگاه و امنیت
- ۲۱۴-۵-۴- عملیات و تمرین‌ها
- ۲۱۵-۱-۵-۴- تمرینات فدرال
- ۲۱۶-۲-۵-۴- تمرینات وزارت دفاع
- ۲۱۸-۳-۵-۴- تمرینات آموزشی
- ۲۱۹-۴-۵-۴- نمونه‌ای از لیست همگام‌سازی مأموریت
- ۲۲۰-۶-۴- خلاصه
- ۲۲۱- منابع
- ۲۲۷- فصل پنجم: جنگجویان سایبری
- ۲۲۸-۱-۵- یک جنگجوی سایبری چه شکلی است؟
- ۲۲۸-۱-۱-۵- گواهی‌نامه‌ها
- ۲۳۱-۲-۱-۵- آموزش و تعلیم
- ۲۳۴-۳-۱-۵- تجارت و مهارت‌ها
- ۲۳۵-۲-۵- تفاوت‌های نیروهای سایبری با نیروهای سنتی
- ۲۳۶-۱-۲-۵- سن

۲۳۷	۵-۲-۲- نگرش
۲۳۸	۵-۲-۳- شرایط فیزیکی
۲۳۹	۵-۲-۴- اعتبارنامه‌ها
۲۴۲	۵-۳- نیروهای کنونی جنگ سایبری
۲۴۵	۵-۳-۱- کشور ایالات متحده
۲۴۶	۵-۳-۲- کشور چین
۲۴۷	۵-۳-۱- کشور روسیه
۲۴۷	۵-۳-۲- کشور ژاپن
۲۴۸	۵-۳-۵- رژیم صهیونیستی
۲۴۸	۵-۳-۶- کشور برزیل
۲۴۸	۵-۳-۷- کشور سنگاپور
۲۴۹	۵-۳-۸- کشور کره جنوبی
۲۴۹	۵-۳-۹- کشور کره شمالی
۲۵۰	۵-۳-۱۰- کشور استرالیا
۲۵۰	۵-۳-۱۱- کشور مالزی
۲۵۱	۵-۳-۱۲- کشور ژاپن
۲۵۱	۵-۳-۱۳- کشور کانادا
۲۵۲	۵-۳-۱۴- کشور انگلستان
۲۵۲	۵-۳-۱۵- سایر کشورهای دارای نیروهای سایبری
۲۵۳	۵-۳-۱۶- شرکت‌ها
۲۵۵	۵-۳-۱۷- مجرمان
۲۵۶	۵-۴- تأمین نیرو برای جنگ سایبری
۲۵۷	۵-۴-۱- منابع استعداد
۲۵۸	۵-۴-۲- آموزش نسل بعدی
۲۵۹	۵-۴-۳- الگوی آموزشی

- ۲۶۰ ۵-۴-۴- پرورش مهارت‌های موردنیاز
- ۲۶۱ ۵-۴-۵- مسائل مربوط به آموزش برای جنگ سایبری
- ۲۶۳ ۵-۵- خلاصه
- ۲۶۵ منابع
- ۲۶۷ فصل ششم: تسلیحات منطقی
- ۲۷۱ ۱-۶- ابزارهای شناسایی
- ۲۷۱ ۱-۶-۱- جمع‌آوری اطلاعات عمومی
- ۲۷۲ ۱-۶-۱-۱- وب‌سایت‌ها و سرویس‌دهنده‌های وب
- ۲۷۲ ۱-۶-۱-۱- موت‌رنای جستجوگر
- ۲۷۳ ۱-۶-۲- هک نوگام
- ۲۷۵ ۱-۶-۳- وب پنهان
- ۲۷۵ ۱-۶-۴- Whois ابزار
- ۲۷۹ ۱-۶-۲- سیستم نام دامنه
- ۲۸۱ ۱-۶-۲-۱- فراداده
- ۲۸۲ ۱-۶-۲-۱-۱- Metagoofil ابزار
- ۲۸۳ ۱-۶-۲-۱-۲- Exiftool ابزار
- ۲۸۴ ۱-۶-۲-۱-۳- strings ابزار
- ۲۸۵ ۱-۶-۲-۲- Maltego ابزار
- ۲۸۶ ۱-۶-۳-۲- دفاع از سیستم نام دامنه
- ۲۸۸ ۱-۶-۳- ابزارهای پویش
- ۲۸۸ ۱-۶-۳-۱- Nmap ابزار
- ۲۹۳ ۱-۶-۳-۲- Nessus ابزار
- ۲۹۸ ۱-۶-۳-۳- دفاع در مقابل ابزارهای پویش
- ۲۹۹ ۱-۶-۴- ابزارهای به‌دست آوردن دسترسی و بالا بردن سطح دسترسی
- ۲۹۹ ۱-۶-۴-۱- ابزارهای رمز عبور

۳۰۲.....	۶-۴-۲- پروژه متا اسپلویت
۳۰۲.....	۶-۴-۲-۱- نسخه چارچوب متا اسپلویت
۳۰۴.....	۶-۴-۲-۲- نسخه‌های متا اسپلویت کم حجم و متا اسپلویت حرفه ای
۳۰۶.....	۶-۴-۳- مصونیت CANVAS
۳۰۸.....	۶-۴-۴- دفاع در مقابل ابزارهای به دست آوردن دسترسی و بالا بردن دسترسی ..
۳۱۱.....	۶-۴-۵- ابزارهای خارج کردن غیرمجاز اطلاعات
۳۱۱.....	۶-۴-۵-۱- جمع‌آوری اطلاعات به صورت فیزیکی
۳۱۱.....	۶-۴-۵-۲- رمزنگاری و پنهان سازی اطلاعات
۳۱۳.....	۶-۴-۵-۳- استفاده از پروتکل های رایج
۳۱۴.....	۶-۴-۵-۴- روش های خارج کردن بندن
۳۱۴.....	۶-۴-۵-۵- دفاع در مقابل ابزارهای خارج کردن غیرمجاز اطلاعات
۳۱۵.....	۶-۴-۶- ابزارهای حفظ دسترسی ..
۳۱۶.....	۶-۴-۱- اضافه کردن دسترسی مجاز
۳۱۷.....	۶-۴-۲- در ب های پشتی
۳۱۸.....	۶-۴-۳- دفاع در مقابل ابزارهای حفظ دسترسی
۳۱۹.....	۶-۴-۷- ابزارهای حمله
۳۱۹.....	۶-۴-۷-۱- مداخله در نرم افزار
۳۲۰.....	۶-۴-۷-۱-۱- منابع سیستمی
۳۲۱.....	۶-۴-۷-۲- محیط سیستم
۳۲۳.....	۶-۴-۷-۲- حمله به سخت افزار
۳۲۴.....	۶-۴-۷-۳- دفاع در مقابل ابزارهای حمله
۳۲۵.....	۶-۴-۸- ابزارهای ایجاد ابهام
۳۲۵.....	۶-۴-۸-۱- پنهان سازی موقعیت مکانی
۳۲۷.....	۶-۴-۸-۲- دست کاری لاگ سیستم
۳۲۹.....	۶-۴-۸-۳- دست کاری فایل

- ۳۳۱ ۶-۸-۴- دفاع در مقابل ابزارهای ایجاد ابهام
- ۳۳۲ ۶-۹- خلاصه
- ۳۳۳ منابع
- ۳۳۷ فصل هفتم: تسلیحات فیزیکی
- ۳۳۹ ۷-۱- چگونه حوزه‌های منطقی و فیزیکی به یکدیگر متصل هستند
- ۳۳۹ ۷-۱-۱- سیستم‌های منطقی بر روی سخت‌افزار فیزیکی اجرا می‌شوند
- ۳۴۲ ۷-۲- حملات منطقی ممکن است تأثیرات فیزیکی داشته باشند
- ۳۴۴ ۷-۲- نگرانی‌های: بر ساختی
- ۳۴۶ ۷-۲-۱- CAD چیست؟
- ۳۴۷ ۷-۲-۲- مسایل امنیتی در دنیای SCADA وجود دارند کدام‌اند؟
- ۳۴۹ ۷-۲-۳- عواقب از کار افتادن سیستم‌های SCADA چیست؟
- ۳۵۱ ۷-۳- نگرانی‌های زنجیره تامین
- ۳۵۲ ۷-۳-۱- سخت‌افزارهای در معرض خطر
- ۳۵۴ ۷-۳-۲- مؤلفه‌هایی که عمداً خراب شده‌اند
- ۳۵۵ ۷-۳-۳- مسائل غیر فنی
- ۳۵۶ ۷-۴- ابزارهای حمله فیزیکی و دفاع در مقابل آن‌ها
- ۳۵۸ ۷-۴-۱- حملات الکترومغناطیسی
- ۳۵۹ ۷-۴-۱-۱- تسلیحات پالس الکترومغناطیسی
- ۳۶۱ ۷-۴-۱-۲- پارازیت
- ۳۶۱ ۷-۴-۱-۳- دفاع در مقابل حملات متعارف
- ۳۶۲ ۷-۴-۲- زیرساخت افزونه
- ۳۶۳ ۷-۴-۳- استحکام‌بخشی تأسیسات و تجهیزات
- ۳۶۵ ۷-۴-۴- فعالیت مخفیانه
- ۳۶۶ ۷-۴-۴-۱- استراق سمع در طیف الکترومغناطیسی
- ۳۶۷ ۷-۴-۴-۲- خرابکاری/منع سرویس

۳۶۸	۷-۴-۳- حمله به تجهیزات کنترل دسترسی فیزیکی
۳۶۸	۷-۴-۵- پنهان شدن پشت شخص دیگر
۳۶۹	۷-۴-۶- قفل ها
۳۷۲	۷-۴-۱- دفاع در مقابل حملات پنهانی
۳۷۴	۷-۵- خلاصه
۳۷۵	منابع
۳۷۹	فصل هشتم: تسلیحات روان شناختی
۳۸۱	۸-۱- تعریف مهندسی اجتماعی
۳۸۱	۸-۱-۱- آیا مهندسی اجتماعی یک علم است؟
۳۸۳	۸-۱-۲- تاکتیک ها و تکنیک ها و رویه های مهندسی اجتماعی
۳۸۴	۸-۱-۲-۱- حملات برای دست آوردن دسترسی عمومی
۳۸۷	۸-۱-۲-۲- حملات دسترسی به راه های خاص
۳۸۹	۸-۱-۳- انواع رویکردهای مهندسی اجتماعی
۳۹۱	۸-۱-۴- انواع روش های مهندسی اجتماعی
۳۹۵	۸-۲- چگونه یک نظامی از مهندسی اجتماعی استفاده می کند
۳۹۶	۸-۲-۱- دکرترین نیروی زمینی
۴۰۳	۸-۳- چگونه نظامی در مقابل مهندسی اجتماعی از خود دفاع می کند
۴۰۷	۸-۳-۱- چگونه نیروی زمینی عملیات ضداطلاعاتی را انجام می دهد
۴۰۸	۸-۳-۲- روش نیروی هوایی
۴۰۹	۸-۴- خلاصه
۴۱۰	منابع
۴۱۳	فصل نهم: کاوش از شبکه کامپیوتری
۴۱۵	۹-۱- اطلاعات و ضداطلاعات
۴۱۵	۹-۱-۱- منابع حملات سایبری
۴۱۷	۹-۱-۲- مهاجمین و حامیان حملات

- ۴۱۸ ۲-۹- شناسایی
- ۴۱۸ ۱-۲-۹- اطلاعات منابع آشکار
- ۴۲۲ ۲-۲-۹- شناسایی غیرفعال
- ۴۲۵ ۳-۹- نظارت
- ۴۲۵ ۱-۳-۹- دلایل انجام نظارت مداوم
- ۴۲۷ ۲-۳-۹- تهدید پایدار پیشرفته
- ۴۲۹ ۳-۹- ۱- نظارت بر صوت
- ۴۳۰ ۳-۹- ۱- نظارت بر داده
- ۴۳۰ ۵-۳-۹- ابزارهای نفوذی در مقیاس بزرگ
- ۴۳۳ ۶-۳-۹- موارد استفاده از نظارت بر داده
- ۴۳۴ ۴-۹- خلاصه
- ۴۳۵ منابع
- ۴۳۷ فصل دهم: حمله ابا استفاده از شبکه گاه بیوتی
- ۴۳۹ ۱-۱۰- به راه انداختن جنگ در عصر سایبری
- ۴۳۹ ۱-۱-۱۰- فیزیکی
- ۴۴۰ ۲-۱-۱۰- الکترونیکی
- ۴۴۱ ۳-۱-۱۰- منطقی
- ۴۴۱ ۴-۱-۱۰- واکنش انفعالی در مقابل واکنش فعالانه
- ۴۴۳ ۵-۱-۱۰- عامل زمان
- ۴۴۴ ۲-۱۰- فرآیند حمله
- ۴۴۵ ۱-۲-۱۰- شناسایی
- ۴۴۷ ۲-۲-۱۰- پوش
- ۴۴۸ ۳-۲-۱۰- دسترسی
- ۴۵۱ ۴-۲-۱۰- افزایش سطح دسترسی
- ۴۵۲ ۵-۲-۱۰- جمع‌آوری و خارج کردن داده‌ها

۴۵۳	 ۱۰-۲-۶-تهاجم
۴۵۷	 ۱۰-۲-۷-حفظ دسترسی
۴۵۸	 ۱۰-۲-۸-ایجاد ابهام
۴۶۰	 ۱۰-۳-خلاصه
۴۶۱	 منابع
۴۶۳	 فصل یازدهم: دفاع از شبکه کامپیوتری
۴۶۵	 ۱۱-۱-۱-از چه چیزی محافظت می‌کنیم
۴۶۷	 ۱۱-۱-۱-۱-محرم‌السر، صحت و دسترسی‌پذیری
۴۶۸	 ۱۱-۱-۱-۱-صحت
۴۷۰	 ۱۱-۱-۱-۲-دسترسی‌پذیری
۴۷۰	 ۱۱-۱-۲-احراز هویت، احراز دسترسی و حسابرسی
۴۷۳	 ۱۱-۲-آگاهی امنیتی و آموزش
۴۷۳	 ۱۱-۲-۱-آگاهی
۴۷۶	 ۱۱-۲-۲-آموزش
۴۷۷	 ۱۱-۳-دفاع در مقابل حملات سایبری
۴۷۸	 ۱۱-۳-۱-سیاست و پیروی از آن
۴۷۹	 ۱۱-۳-۲-نظارت، داده‌کاوی و تطبیق الگو
۴۸۱	 ۱۱-۳-۳-تشخیص نفوذ و جلوگیری از آن
۴۸۲	 ۱۱-۳-۴-ارزیابی آسیب‌پذیری و تست نفوذ
۴۸۳	 ۱۱-۳-۵-برنامه‌ریزی برای بازیابی از فاجعه
۴۸۴	 ۱۱-۳-۶-دفاع در عمق
۴۸۶	 ۱۱-۴-خلاصه
۴۸۸	 منابع

- فصل دوازدهم: بازیگران غیردولتی در عملیات شبکه‌های کامپیوتری ۴۹۱
- ۱-۱۲- بازیگران فردی ۴۹۳
- ۱-۱-۱۲- اسکرپت‌بازها ۴۹۵
- ۲-۱-۱۲- نویسندگان بدافزار ۴۹۵
- ۳-۱-۱۲- کلاه‌برداران ۴۹۶
- ۴-۱-۱۲- کلاه سیاه‌ها ۴۹۷
- ۵-۱۲- فعالان هکری ۴۹۸
- ۶-۱۲- هکرهای میهن‌پرست ۴۹۹
- ۲-۱۲- شرکت‌ها ۵۰۰
- ۱-۲-۱۲- اندر شاپ برای حضور در جنگ سایبری ۵۰۰
- ۳-۱۲- تروریسم سایبری ۵۰۱
- ۱-۳-۱۲- دلایل انجام حملات تروریستی سایبری ۵۰۲
- ۲-۳-۱۲- وقتی یک حمله تروریستی سایبری انجام شود چه اتفاقی خواهد افتاد؟ ۵۰۳
- ۴-۱۲- جرم سایبری سازمان‌یافته ۵۰۶
- ۱-۴-۱۲- انگیزه سازمان‌های جنایتکار ۵۰۷
- ۵-۱۲- بازیگران مستقل ۵۰۷
- ۱-۵-۱۲- سیستم‌های اکتشافی ۵۰۸
- ۲-۵-۱۲- سیستم‌های حمله ۵۰۹
- ۳-۵-۱۲- سیستم‌های تدافعی ۵۱۲
- ۶-۱۲- خلاصه ۵۱۳
- منابع ۵۱۴
- فصل سیزدهم: اثرات نظام حقوقی ۵۱۷
- ۱-۱۲- نظام‌های حقوقی ۵۳۷
- ۱-۱-۱۳- قوانین بین‌المللی ۵۴۰
- ۱-۱-۱-۱۳- قانون دریایی ۵۴۰

۵۴۱	۱۳-۱-۱-۲- قانون فضا
۵۴۲	۱۳-۱-۲- قوانین ایالات متحده
۵۴۳	۱۳-۱-۳- قانون کیفری
۵۴۴	۱۳-۱-۳- جستجوی الکترونیکی
۵۴۶	۱۳-۲- قوانین کلیدی ایالات متحده
۵۴۷	۱۳-۱-۲- مقررات داد و ستد جهانی سلاح
۵۴۸	۱۳-۲-۲- قوانین سایبری ایالات متحده
۵۴۹	۱۳-۲-۲-۱- قانون جرائم کامپیوتری
۵۵۰	۱۳-۲-۲-۲- قانون ارتقاء امنیت سایبری
۵۵۲	۱۳-۲-۲-۳- قانون مدیریت امنیت اطلاعات فدرال
۵۵۴	۱۳-۲-۲-۴- استانداردها برای پشتیبانی از امنیت سایبری
۵۵۵	۱۳-۳- اثرات حریم خصوصی
۵۵۵	۱۳-۳-۱- قانون حفظ حریم خصوصی و ارتباطات الکترونیکی
۵۵۶	۱۳-۴- جرم‌شناسی دیجیتالی
۵۶۱	۱۳-۴-۱- گواهی‌نامه
۵۶۳	۱۳-۵- خلاصه
۵۶۴	منابع
۵۶۷	فصل چهاردهم: اصول اخلاقی
۵۶۹	۱۴-۱- اصول اخلاقی در جنگ سایبری
۵۶۹	۱۴-۱-۱- استفاده از زور
۵۷۱	۱۴-۱-۲- نیت حمله
۵۷۲	۱۴-۱-۳- انتساب حمله به افراد و یا دولت‌ها
۵۷۲	۱۴-۱-۴- قوانین نظامی مبتنی بر نظام‌های اخلاقی
۵۷۳	۱۴-۱-۴-۱- قانون درگیری مسلحانه
۵۷۴	۱۴-۲- نظریه جنگ عادلانه

۵۷۶	۱۴-۲-۱- حق توسل به زور
۵۷۷	۱۴-۲-۱-۱- اختیارات درست
۵۷۸	۱۴-۲-۱-۲- نیت درست
۵۷۹	۱۴-۲-۱-۳- احتمال موفقیت
۵۷۹	۱۴-۲-۱-۴- آخرین تلاش
۵۸۰	۱۴-۲-۱-۵- تناسب
۵۸۰	۱۴-۲-۲- حقوق افراد در جنگ
۵۸۰	۱۴-۲-۲-۱- تمایز
۵۸۱	۱۴-۲-۲-۲- اف‌ا، غیرنظامی
۵۸۳	۱۴-۲-۲-۲- تناسب
۵۸۴	۱۴-۲-۲-۴- ضا، ضا، خواسته
۵۸۴	۱۴-۲-۲-۵- محدود کردن حمله
۵۸۵	۱۴-۲-۳- عدالت بعد از جنگ
۵۸۵	۱۴-۲-۳-۱- به دست آوردن صلح پایدار
۵۸۶	۱۴-۲-۳-۲- پاسخگو بودن افراد مقصر
۵۸۷	۱۴-۲-۳-۳- به دست آوردن غرامت
۵۸۷	۱۴-۳- خلاصه
۵۸۸	منابع
۵۹۱	فصل پانزدهم: چالش‌های فضای سایبر
۵۹۴	۱۵-۱- بررسی مسائل موجود در امنیت سایبری
۵۹۷	۱۵-۱-۱- سیاست
۵۹۹	۱۵-۱-۲- فرآیندها
۶۰۱	۱۵-۱-۳- فنی
۶۱۰	۱۵-۱-۴- مهارت‌ها
۶۱۱	۱۵-۱-۵- مردم

۶۱۴	۱۵-۱-۶- سازمان
۶۱۵	۱۵-۱-۷- هسته (تأثیرگذاری بر تمامی حوزه‌ها)
۶۲۲	۱۵-۲- روابط متقابل چالش‌های امنیت سایبری
۶۲۴	۱۵-۳- مسیر پیش‌رو
۶۲۷	۱۵-۴- خلاصه
۶۲۸	منابع
۶۳۱	فصل شانزدهم: آینده‌ی جنگ سایبری
۶۴۶	۱۶-۱- گرایش‌های نوظهور
۶۵۴	۱۶-۲- گرایش‌ها سیر پیش‌روی ما را مشخص خواهند ساخت
۶۵۹	۱۶-۳- خلاصه
۶۶۱	منابع
۶۶۵	پیوست
۶۷۹	واژه‌نامه