# فهرست مطالب


| عنوان | صفحه |
| --- | --- |
| پیشگفتار مؤلف | (یک) |
| پیشگفتار | (هفت) |
| **بخش اول: معرفی** | |
| **فصل اول:جنگ خلیج ـ جنگ اطلاعات** | ۱ |
| جنگ خلیج | ۱ |
| جنگ اطلاعات | ۱۰ |
| از طبیعت تا تراشه‌ها | ۱۳ |
| **فصل دوم: نظریه جنگ اطلاعات** | ۲۳ |
| منابع اطلاعات | ۲۳ |
| ارزش منابع اطلاعات | ۲۵ |
| بازیگران | ۲۸ |
| تهاجم | ۲۸ |
| دفاع | ۳۰ |

نقش دوگانه ۳۱
جنگ اطلاعات تهاجمی ۳۲
دسترسی بیشتر برای بازیگر تهاجمی ۳۵
دسترسی کمتر برای بازیگر مدافع ۳۸
کاهش جمعیت ۳۹
انواع دیگر طبقه‌بندی طرح‌ها ۴۰
جنگ اطلاعات دفاعی ۴۱
انواع دفاع ۴۲
امنیت اطلاعات و تضمین اطلاعات ۴۵
مدل CIA و مجوز ۴۶

**فصل سوم: از میدان بازی تا میدان جنگ** ۴۹
بازی و سرگرمی ۵۰
انگیزه ۵۲
فرهنگ ۵۴
چیزی بیش از بازی کودکانه ۵۸
جرم ۶۰
جرایم مربوط به مالکیت معنوی ۶۱
تقلب ۶۲
سوء استفاده و تقلب رایانه‌ای ۶۵
مبارزه با جرم ۶۹
حقوق فردی ۷۱
امنیت ملی ۷۲
سرویس‌های اطلاعات خارجی ۷۳
جنگ و مناقشه نظامی ۷۶
تروریسم ۷۹
جنگ‌های شبکه ۸۵
حفاظت از زیرساختارهای ملی ۸۷

## بخش دوم: جنگ اطلاعات تهاجمی


**فصل چهارم: منابع آشکار** ۹۳

منابع آشکار و اطلاعات رقابتی ۹۳

حریم شخصی (خصوصی) ۹۷

جاسوسی افراد از طریق منابع آشکار ۹۷

جستجو (مرور) در وب ۱۰۰

مقررات حریم شخصی ۱۰۳

دزدی انتشاراتی ۱۰۶

نقض حق تکثیر ۱۰۶

نقض علایم تجاری ۱۱۳

جنبه‌های سیاه ۱۱۷

**فصل پنجم: مدیریت جنگ روانی و مدیریت ادراک** ۱۲۱

دروغ و تحریف ۱۲۳

تحریف ۱۲۵

جعل ۱۲۷

فریب و حقه ۱۳۰

مهندسی اجتماعی ۱۳۳

تقبیح ۱۳۴

نظریه‌های توطئه ۱۳۷

هتک آبرو ۱۴۰

اذیت و آزار ۱۴۲

تبلیغات ۱۴۴

شیادان ۱۴۴

جنگ آگهی‌های تبلیغاتی ۱۴۷

ممیزی ۱۵۰

محدودیت‌های ایالات متحده ۱۵۴

**فصل ششم: درون حصار** ۱۵۷
افراد خائن و نفوذی‌ها ۱۵۸
جاسوسی دولتی و نظامی ۱۵۸
جاسوسی اقتصادی ۱۶۲
جاسوسی شرکت ۱۶۶
تعدی به حریم فردی ۱۷۰
روابط بازرگانی ۱۷۲
بازدیدها و درخواست‌ها ۱۷۵
تقلب و کلاه‌برداری ۱۸۰
معاملات قلابی ۱۸۰
دستکاری در اطلاعات ۱۸۲
خرابکاری داخلی ۱۸۳
حملات فیزیکی ۱۸۳
حملات نرم‌افزاری ۱۸۴
نفوذ به فضای کاری ۱۸۷
دزدی و نفوذهای فیزیکی ۱۸۷
جستجو و تصرف ۱۹۰
جستجوی زباله‌ها ۱۹۲
بمب‌ها ۱۹۳

**فصل هفتم: ربودن سیگنال‌ها** ۱۹۵
استراق‌سمع مکالمات ۱۹۷
شنود تلفن‌همراه ۱۹۹
رهگیری فراخوان (پیجر) ۲۰۱
قانون استراق‌سمع پلیس ۲۰۲
کنترل اخبار خارجی ۲۰۴
کشف رمز کردن پیام‌ها ۲۰۸
تحلیل ترافیک ۲۱۱

ثبت مدادی و تله و ردپا ۲۱۱
ردیابی محل ۲۱۲
تقلب‌های مخابراتی ۲۱۲
جعبه‌های آبی ۲۱۳
PBX و تقلب‌های مربوط به آن ۲۱۴
تقلب در پست‌های صوتی ۲۱۶
تقلب در کارت‌های تلفن ۲۱۷
تلفن‌های شبیه‌سازی شده و تقلب در تلفن همراه ۲۱۹
نظارت بر شبکه‌های رایانه‌ای ۲۲۱
ردیاب‌های بسته ۲۲۱
نظارت بر ضربه‌های کلید ۲۲۲
نظارت بر محیط ۲۲۳
دوربین و ویدئو ۲۲۳
ماهواره‌ها و تصویر برداری ۲۲۵
گیرنده‌های ون اک ۲۲۸
حسگرهای گوناگون ۲۲۸
پاییدن از روی شانه ۲۳۱
حریم فردی و مسئولیت ۲۳۲
خراب‌کاری ۲۳۳
دستکاری در سرویس‌های تلفن ۲۳۳
پارازیت انداختن ۲۳۵
سلاح‌های بسامد رادیویی ۲۳۸
حملات فیزیکی ۲۴۲

**فصل هشتم: نفوذ به رایانه و ضربه‌زدن (هک کردن)** ۲۴۵
حساب‌ها ۲۴۶
دسترسی یافتن ۲۴۷
ابزارها و روش‌ها ۲۴۹

یک نمایش ۲۵۰
اسکنرهای شبکه ۲۵۳
بوکش‌ها (ردیاب‌های) بسته ۲۵۵
شکافنده‌های کلمات عبور ۲۵۶
سرریز از حافظ‌ها و دیگر سوءاستفاده‌ها ۲۵۹
مهندسی اجتماعی ۲۶۲
ردگم کردن ۲۶۴
دزدی اطلاعات ۲۶۵
جمع‌آوری غنایم ۲۶۶
چیزی بیش از عنیمت ۲۶۸
دستکاری کردن ۲۷۵
هک‌های وب ۲۷۷
هک‌های خدمات نام حوزه ۲۸۰
تخریب ۲۸۱
خاموش کردن از راه دور ۲۸۵
وسعت ۲۸۹

**فصل نهم: فریب** ۲۹۳
سرقت هویت ۲۹۳
پیام‌ها و اسناد جعلی ۳۰۰
جعل نامهٔ الکترونیکی ۳۰۱
جعل آگهی اینترنتی ۳۰۶
سیل نامه‌های الکترونیکی ۳۰۹
کلاهبرداری اینترنتی ۳۱۱
تقلب ۳۱۲
اسب‌های تروا ۳۱۵
تروا‌های نرم‌افزاری ۳۱۶
سوار بر وب ۳۱۹

رلهٔ نامه‌های الکترونیکی ۳۲۳
تراشه‌سازی ۳۲۴
تله‌ها و عملیات مخفی ۳۲۴

**فصل دهم: آفت‌های رایانه‌ای** ۳۲۷
ویروس‌ها ۳۲۸
ویروس‌های برنامه ۳۳۰
ویروس‌های راه‌اندازی ۳۳۰
ویروس‌های ماکرو ۳۳۱
راهکارهای پنهان‌سازی ۳۳۳
چه کسی ویروس‌ها را می‌نویسد؟ ۳۳۴
درجهٔ شیوع ۳۳۵
کلک‌های ویروسی ۳۳۶
RTM III ۳۴۰
کرم‌های رایانه‌ای ۳۴۰

## بخش سوم: جنگ اطلاعات تدافعی

**فصل یازدهم:کدهای محرمانه و پنهان راهها** ۳۴۵
قفل‌ها و کلیدها ۳۴۵
رمزنگاری ۳۴۶
رمزهای دیجیتال ۳۴۷
کد (رمز) شکنی ۳۵۰
تولید و توزیع کلیدها ۳۶۱
توزیع کلید همگانی و دیفی - هلمن ۳۶۳
رمزنگاری کلید عمومی و RSA ۳۶۶
ذخیره و بازیافت کلید ۳۶۹
کاربردهای رمزنگاری ۳۷۲

محدودیت‌های رمزگذاری ۳۷۶
پنهان نگاری (استگانوگرافی) ۳۷۹
گمنامی ۳۸۳
سانسور (بهگزینی) ۳۸۶
آشغال‌های دور ریختنی ۳۸۸
حفاظ گذاری ۳۸۹

**فصل دوازدهم: چگونگی تشخیص موارد جعلی** ۳۹۱
زیست‌سنجی ۳۹۲
کلمات عبور و رمزهای دیگر ۳۹۷
حاصل جمع کنترل جامعیت ۴۰۱
امضاهای دیجیتال ۴۰۴
مدیریت کلید عمومی و گواهی‌نامه‌ها ۴۰۹
آب نشان‌ها ۴۱۳
تماس با منزل و بازخوانی ۴۱۵
تصدیق هویت بر اساس مکان ۴۱۶
کارت‌ها و علائم شناسائی ۴۱۹

**فصل سیزدهم: نظاره‌گرها و نگهبانان** ۴۲۳
کنترل‌های دسترسی ۴۲۴
سیاست‌های اعطای مجوز ۴۲۴
ناظران کنترل دسترسی ۴۲۸
محدودیت‌ها ۴۳۲
صافی‌ها ۴۳۳
دیوارهای آتش ۴۳۳
صافی‌های پست الکترونیکی آشغال ۴۳۵
صافی‌های وب ۴۳۷
نفوذ و شناسایی سوء استفاده ۴۴۱

نظارت محل کار ۴۴۲
شناسایی خودکار (اتوماتیک) ۴۴۵
نفوذ رایانه‌ای و شناسایی سوء استفاده ۴۴۷
قیاس با سیستم ایمنی بدن انسان ۴۵۱
شناسایی و حذف ویروس و کدهای سیار نامطلوب (مضر) ۴۵۳

**فصل چهاردهم: در دنیای پرخطر** ۴۵۵
نظارت بر نقاط آسیب‌پذیر ۴۵۶
یافتن نقاط ضعف امنیت شبکه و رایانه ۴۵۶
نظارت بر نشریات امنیتی ۴۵۹
امن ساختن نرم‌افزارها ۴۶۰
کتاب نارنجی ۴۶۱
ملاک ارزیابی امنیت فن‌آوری اطلاعات و ملاک‌های مشترک ۴۶۴
ارزیابی ۴۶۵
معیارهای تجاری ۴۶۵
گواهی(تصدیق) انجمن ملی امنیت رایانه (ICSA) ۴۶۶
تأییدیه ۴۶۸
الگوی بلوغ توانایی ۴۶۸
آگاهی وآموزش امنیتی ۴۶۹
اجتناب از نکات ضعف خاص ۴۷۱
پشتوانه‌های پشتوانه ۴۷۲
مدیریت خطر ۴۷۳
ارزیابی خطر و قیمت‌گذاری دارایی‌ها ۴۷۳
بیمه ۴۷۶
نشان‌دار کردن ۴۷۷
مراقبت و مسئولیت‌پذیری مناسب ۴۷۸
رسیدگی به حوادث ۴۷۹
تحقیقات و ارزیابی ۴۷۹

محتویات و بازیابی ۴۸۰
بالا بردن (بهبود) امنیت ۴۸۰
اطلاع رسانی ۴۸۱
مقابله به مثل ۴۸۱
راه‌حل‌های مدنی و قانونی ۴۸۲
واکنش‌های نظامی و اقتصادی ۴۸۴
آمادگی اضطراری ۴۸۴
موانع ۴۸۵

**فصل پانزدهم: ماهواره‌ها و سیستم‌های ارسال کابلی** ۴۸۷
اصول عموماً پذیرفته شده امنیت سیستم‌ها ۴۸۷
حفاظت از زیر ساختارهای حیاتی ۴۹۱
کمیسیون حفاظت از زیرساختارهای حیاتی رئیس‌جمهور ۴۹۱
دستورالعمل ۶۳ رئیس جمهور ۴۹۴
سیاست رمزگذاری ۴۹۷
کدسازی ۴۹۷
کد شکنی ۴۹۸
سیاست‌های بین‌المللی ۵۰۰
سیاست ایالات متحده ۵۰۲
چالش‌های قانونی ۵۰۷
قانون‌گذاری ۵۰۹
دورنمای خط‌مشی رمزگذاری ۵۱۵

**کتاب شناسی** ۵۱۹

**واژه‌نامه فارسی به انگلیسی** ۵۲۳

**واژه‌نامه انگلیسی به فارسی** ۵۳۳

**یادداشت پایانی** ۵۴۳

# پیشگفتار مؤلّف

در سال‌های اخیر، جنگ اطلاعات توجه بسیاری از مقامات دولتی، کارشناسان امنیت اطلاعات و ناظران کنجکاو را به خود جلب کرده است. این اصطلاح، طیف وسیعی از فعالیت‌ها را در برمی‌گیرد، امّا به‌طور خاص، سناریویی است که در آن تروریست‌های اطلاعات فقط با استفاده از یک صفحه کلید و موشواره، به رایانه‌های دیگر نفوذ می‌کنند و باعث سقوط هواپیماها، وقوع خاموشی‌های بی‌سابقهٔ برق و یا مسمومیت مواد غذایی می‌شوند. تروریست‌ها ممکن است در کار رایانه‌های بانک‌ها و مسائل مالی اختلال کنند و شاید باعث سقوط بازار سهام و یا فروپاشی اقتصادی شوند. هیچ‌یک از این فجایع هنوز رخ نداده است، امّا نگرانی در اینجاست که وقوع این موارد و موارد مشابه دیگر، با تصور سهولتی که نوجوانان می‌توانند بدون دغدغه حتی به رایانه‌های وزارت دفاع ایالات متحده نفوذ کنند، زیاد غیرمحتمل نیست.

این کتاب، مقدمه‌ای است بر جنگ اطلاعات؛ جنگی که در آن فرد از همهٔ امکانات و ابزارهای اطلاعاتی بهره می‌جوید تا با کسب امتیازی، بر حریف خود برتری بیابد. این مبارزه، گسترهٔ وسیعی از فعالیت‌ها، ازجمله نفوذ و خراب‌کاری رایانه‌ای، عملیات جاسوسی و اطلاعاتی، شنود مخابراتی و شیادی، مدیریت هوشمند و جنگ الکترونیکی را در برمی‌گیرد. این کتاب دربارهٔ نوجوانانی است که از اینترنت به عنوان زمین بازی بزرگی برای شکستن و هک‌کردن رایانه‌ها استفاده می‌کنند و یا رقبایی که اسرار تجاری را به سرقت می‌برند، یا نیروهای انتظامی که از جنگ اطلاعات برای مبارزه با جنایت و تروریسم بهره می‌برند و یا افسران نظامی که

جنگ اطلاعات را به میدان جنگ می‌برند. این کتاب در مورد تهدیدات اطلاعات محور علیه کشورها، تجارت و افراد و اقدام متقابل در برابر آن‌ها است و چندین حوزه ازجمله جنایت، تروریسم، امنیت ملی، حقوق فردی و امنیت اطلاعات را دربرمی‌گیرد.

این کتاب چهار هدف را دنبال می‌کند. اولین هدف، ارائهٔ یک بررسی جامع و منسجم از جنگ اطلاعات دفاعی و تهاجمی از جهت عاملین، اهداف، شیوه‌ها، فناوری، نتایج، سیاست‌ها و قوانین است. جنگ اطلاعات می‌تواند هر نوع محیط اطلاعاتی، از قبیل: محیط‌های فیزیکی، رسانه‌های چاپ و ذخیره، رسانه‌های خبر پراکنی، مخابرات و شبکه‌های رایانه‌ای را مورد هدف و یا بهره‌برداری قرار دهد. تمامی این موارد در این کتاب مورد بررسی قرار می‌گیرند؛ هر چند که تأکید عمده بر رسانه‌های رایانه‌ای است. هدف دوم کتاب ارائهٔ نظریهٔ جنگ اطلاعات است که در آن بتوان توصیفی برای کلیهٔ این فعالیت‌ها که مجموعه‌ای متنوع از عاملان و ابزارهای جنگ است ارائه کرد و آن‌ها را در یک چارچوب واحد یکپارچه کرد. این نظریه براساس ارزش منابع اطلاعات و عملیات "برد - باخت" که آن ارزش را تحت تأثیر قرار می‌دهند، قرار دارد. هدف سوم، جداکردن واقعیت از توّهم است. کتاب قصد دارد تا تصویری درست از تهدیدات، با تأکید بر آمار و حوادث واقعی و تعمق نسبت به آنچه ممکن است رخ دهد، ارائه کند. به هرحال، از تصور این موارد غفلت نمی‌کنیم، چرا که پیش‌بینی آینده و آمادگی برای حملات محتمل، ضروری است. هدف چهارم، توصیف فناوری‌های جنگ اطلاعات و محدودیت‌های آن، به‌خصوص محدودیت‌های فناوری‌های دفاعی است. هیچ گلولهٔ نقره‌ای در مقابل حملات جنگ اطلاعات وجود ندارد.

در این کتاب دربارهٔ "چگونگی" انجام یک حمله یا دفاع در برابر حمله صحبت نمی‌کنیم. با وجود این، از آنجا که کتاب طرز عملی جامع و مستدل از روش‌ها و راهکارهای جنگ اطلاعات ارائه می‌کند، ممکن است برای انجام قضاوت‌های آگاهانه در مورد تهدیدات و دفاع‌های مستعد مفید باشد.

این کتاب برای طیف وسیعی از مخاطبین در نظر گرفته شده است، از یک دانشجو و فرد مبتدی علاقه‌مند به یادگیری بیشتر در این زمینه و راه‌های حفاظت از سرمایه‌های اطلاعاتی گرفته تا سیاست‌گذارانی که مایل‌اند ماهیت این تهدیدها و فناوری‌ها و مسائل را بهتر بفهمند و همچنین متخصصین امنیت اطلاعات که مایل‌اند آگاهی گسترده‌ای در مورد همهٔ انواع حملات و اقدامات مقابله با آن‌ها برای حفاظت از سرمایه‌های سازمانی داشته باشند. این کتاب همچنین برای مخاطبین بین‌المللی نگارش یافته است. هر چند کانون توجه، فعالیت‌های درون ایالات متحده است، امّا فعالیت‌های بیرون از این کشور نیز لحاظ شده‌اند.

این کتاب در درس جنگ اطلاعات که من در دانشگاه *جورج‌تاون* برای دانشجویان سال آخر کارشناسی تدریس می‌کنم، استفاده می‌شود. دانشجویان این درس از طیف وسیعی از رشته‌ها، سیاست بین‌الملل، مطالعات امنیت ملی، علوم و فناوری در امور بین‌الملل، ارتباطات، فرهنگ و فناوری، بازرگانی، اقتصاد، دولت، علوم پایه و علوم انسانی، هستند.

کتاب به ۳ بخش تقسیم شده است. بخش اول به معرفی مفاهیم و اصول جنگ اطلاعات می‌پردازد که خود شامل سه فصل است. فصل اول، "جنگ خلیج - جنگ اطلاعات"، که با نمونه‌هایی از جنگ اطلاعات مربوط به زمان جنگ خلیج فارس و ادامهٔ منازعه با عراق شروع می‌شود. این فصل اصول جنگ اطلاعات را خلاصه می‌کند و به بحث دربارهٔ شیوه‌های جنگ اطلاعات و فناوری می‌پردازد. فصل دوم، "نظریهٔ جنگ اطلاعات"؛ که به ارائهٔ الگوی جنگ اطلاعات از زاویهٔ چهار عنصر اصلی: منابع اطلاعات، عوامل، عملیات تهاجمی و عملیات دفاعی می‌پردازد و جنگ اطلاعات را با امنیت اطلاعات و تضمین اطلاعات مرتبط می‌سازد. فصل سوم، "از زمین بازی تا میدان جنگ"، جنگ اطلاعات را در درون چهار حوزهٔ فعالیت انسانی قرار می‌دهد: سرگرمی، جرم، حقوق فردی و امنیت ملی. بعضی از فعالیت‌ها را در هر یک از این حوزه‌ها به‌طور اجمال بررسی می‌کنیم.

بخش دوم به بررسی عملیات جنگ اطلاعات تهاجمی می‌پردازد و محور رسانه‌ها و شیوه‌های کارکرد سازماندهی‌شده و نمونه‌های متعددی از وقایع را در هر مقوله ارائه می‌دهد، که دارای هشت فصل است. فصل چهارم، "منابع آزاد"، در مورد رسانه‌هایی است که عموماً در دسترس همه قرار دارند. این فصل شامل سایت‌های اینترنت، منابع آزاد و اطلاعات رقابتی است و به مسایلی همچون تجاوز به حریم شخصی افراد و یا سرقت‌هایی می‌پردازد که حقوق مربوط به چاپ، ضبط یا نشر آثار و حقوق مربوط به نام تجاری کالا را نقض می‌کند، پوشش می‌دهد. فصل پنجم، "عملیات روانی و مدیریت هوشمند"، در مورد عملیاتی است که رسانه‌های خبر رسانی، به‌خصوص رسانه‌های پخشی و اینترنت را برای تحت تأثیر قرار دادن افکار و اعمال مردم مورد بهره‌برداری قرار می‌دهند. فصل ششم، "در درون حصار"، در مورد عملیاتی علیه منابع یک سازمان از طریق عوامل درونی و یا کسانی است که به منابع داخلی دسترسی دارند و آن شامل خیانت‌کاران و عوامل نفوذی، روابط تجاری، بازدیدها و درخواست‌ها، فریب افراد درونی، اختلاس در خراب‌کاری و سرقت‌های فیزیکی می‌شود. فصل هفتم، "گرفتن علائم و سیگنال‌ها"، در مورد عملیاتی است که باعث قطع ارتباطات می‌شود و با استفاده از حسگرها به جمع‌آوری اطلاعات از محیط فیزیکی می‌پردازند. تقلب‌های مربوط به ارتباطات راه دور و حملات فیزیکی و الکترونیکی که باعث اختلال یا از کار اندازی ارتباطات می‌شوند نیز مورد بررسی قرارمی‌گیرند. فصل هشتم، "نفوذ و هک رایانه‌ای"، در مورد نفوذهای رایانه‌ای و حملات از راه دور به شبکه‌ها است و توصیف می‌کند که هکرها چگونه دسترسی پیدا می‌کنند و وقتی دسترسی پیدا کردند، چه‌کار می‌کنند. فصل نهم، "فریبکاری"، در مورد دغل‌کارانی است که در پس ظاهر معمولی به بررسی سرقت هویت، جعل و ساخت اسب‌های تروا می‌پردازند. سرانجام، فصل دهم، "آفت‌های رایانه‌ای"، در مورد ویروس‌ها و کرم‌های رایانه‌ای است.

بخش سوم به بررسی جنگ اطلاعات دفاعی می‌پردازد و نقاط ضعف و قوت برخی روش‌های خاص را بررسی می‌کند. این قسمت دارای ۵ فصل است. فصل یازدهم، "کدهای

سری و مخفی‌گاه‌ها"، در مورد شیوه‌هایی است که اسرار را پنهان نگه می‌دارند از قبیل رمز نگاری، پنهان‌نگاری[1]، گمنامی قفل و کلید. فصل دوازدهم، "چگونه موارد نادرست را شناسایی کنیم"، در مورد شیوه‌های تعیین ارزشمند بودن و صحّت اطلاعات است و شامل بررسی زیست‌سنجی[2]، کلمهٔ عبور، بررسی صحت، امضاهای عددی، ته نقش‌های کاغذی[3]، و نشان‌ها و کارت‌ها می‌شود. فصل سیزدهم، "ناظران و نگهبانان[4]"، در مورد کنترل‌گرهایی است که دسترسی به منابع اطلاعاتی را کنترل می‌کنند، اطلاعات را از صافی می‌گذرانند و نفوذ به سیستم‌های اطلاعات و یا سوء استفاده از منابع را شناسایی می‌کنند. فصل چهاردهم، "در دنیای خاطره‌آمیز"، در مورد کارهایی است که سازمان‌ها می‌توانند برای مقابله با خطرات انجام دهند. این فصل دربارهٔ درجهٔ آسیب‌پذیری، ارزیابی و کنترل ساخت و راه‌اندازی سیستم‌های امن، مدیریت خطر و مدیریت حادثه است. سرانجام فصل پانزدهم، "دفاع از ملت"، دربارهٔ نقش دولت در جنگ اطلاعات دفاعی است. که در سه حوزه مورد بررسی قرار می‌گیرند: اصول امنیت سیستم مورد قبول عموم، حفاظت از زیرساخت‌های حیاتی و سیاست رمزگذاری کردن.

در تمامی این فصول، کتاب به توصیف حوادث، شرکت‌ها و محصولات متعدد می‌پردازد. این موارد برای روشنگر ساختن مفاهیم و شیوه‌ها ارائه شده‌اند. من هیچ یک از شرکت‌ها و یا محصولات نام‌برده شده را تأیید نمی‌کنم و سعی کرده‌ام که تمامی اطلاعات را منصفانه و به درستی گزارش کنم و از پیشنهادات اصلاحی استقبال می‌کنم.

نگارش این کتاب چندین چالش را پیش روی قرار داده است. اوّلینِ آن، تصمیم‌گیری دربارهٔ این مسئله بود که چه چیزی در حوزهٔ جنگ اطلاعات می‌گنجد. در حالی‌که همه می‌پذیرند که نفوذ به رایانه‌های وزارت دفاع، جنگ اطلاعات است، حداقل در شرایط خاص دیگری، همه ممکن است قبول نکنند که بسیاری از موضوعات مورد بررسی این کتاب جنگ اطلاعات محسوب می‌شوند. در پایان، تصمیم گرفتم که چشم‌انداز وسیعی را در پیش بگیرم چرا که اصول مشترکی زیربنای تمامی این فعالیت‌های مجزا را تشکیل می‌داد. علاوه بر این، من مجذوب این حوزه‌ها شدم، نوعی ارتباط در بین آن‌ها مشاهده کردم و در نتیجه تصمیم گرفتم که آن‌ها را در کتاب بگنجانم. بی‌شک، بعضی‌ها خواهند گفت که من زیاده‌روی کرده‌ام؛ جنگ اطلاعات بیشتر به تهدیدات در سطح ملی و به فعالیت‌هایی نظیر تقلب و سرقت مربوط می‌شود. این انتقاد منصفانه‌ای است. من لغات متعدد دیگری را در نظر گرفتم به عنوان نمونه، جرائم رایانه‌ای، جنگ رایانه‌ای و تروریسم اطلاعات، اما ظاهراً هیچ‌کدام به خوبی "جنگ اطلاعات" نمی‌توانست جوهرهٔ فعالیت مورد بحث این کتاب را برساند.

---

[1]. Steganography
[2]. Biometry
[3]. Watermarking
[4]. Gate - keepers

چالش دوم، که بخشی از آن به‌خاطر تصمیم برای گنجاندن این همه موضوع بود، مربوط به چگونگی سازمان‌دهی‌کردن مطالب می‌شد. کتاب دو بار سازماندهی شد. که بار دوم پس از استفاده از یک پیش‌نویس در کلاس درس بود. هرچند که از چارچوب فعلی کتاب راضی هستم، اما ادعا نمی‌کنم که بهترین راه ممکن برای ارائه مطالب کتاب بوده است.

چالش سوم، که به‌خاطر مسئلهٔ اول برجسته‌تر می‌شد، تلاش برای پوشش معقولانهٔ موضوعاتی بود که من در آن‌ها زمینهٔ اندکی داشتم. می‌توانستم آن‌ها را به کناری بگذارم، اما می‌خواستم که حوزهٔ تخصصی خود، یعنی رایانه و رمزنگاری را در بافت بزرگ‌تری قرار دهم. هکرهای رایانه تنها تهدید برای منابع اطلاعات نیستند، همان‌طور که رمزنگاری تنها راه‌حل جادویی نیست. نتیجهٔ گنجاندن چنین زمینه‌های متنوعی در کتاب آن است که کتاب یکنواخت نیست و بعضی از موضوعات عمیق‌تر از بقیه بررسی شده‌اند. تعداد جملات مربوط به یک موضوع لزوماً در ارتباط با اهمیت کلی آن موضوع نیست. برای کسانی که مایل‌اند موضوعی را بیشتر مطالعه کنند، منابع کافی در کتاب ارائه شده است.

و بالاخره چالش اصلی ما آن بوده است که با تحولاتی که در این زمینه روی می‌دهد همگام باشیم. تحولاتی که در زمینهٔ فن‌آوری‌های جدید، روش‌های جدید حمله و یا قوانین صورت می‌گیرد. ما حتی به مطالعات و تحولات انجام شده در زمینهٔ جرایمی که در کتاب آمده‌اند توجه داشته‌ایم. به طور متوسط من در هر روز، در پست الکترونیکی خود بیش از شش مورد از موارد مربوط به مطالب این کتاب را می‌یابم. ممکن است یک یا دو مورد هم در روزنامهٔ *واشنگتن پست* یا یک کتاب و مجلهٔ دیگر پیدا کنم. تا هنگام زیر چاپ رفتن این کتاب، بی‌شک انبوه عظیمی از مطالب جمع‌آوری خواهد شد که ای کاش بتوانم آن‌ها را در کتاب بگنجانم.جنگ اطلاعات، خود مسائل بحث برانگیزی را مطرح می‌سازد. سطح قابل قبول خطر کردن چیست؟ اگر یک رایانه در اینترنت برای یک حمله‌ی مخرب و علیه یک سایت دیگر مورد استفاده قرار گیرد، چه کسی مسئول است؟ اگر مطالبی موهن یا دارایی معنوی مسروقه‌ای در یک خط آن‌لاین[1] در اختیار همگان قرار گیرد، چه کسی مسئول است؟ تحت چه شرایطی جنگ اطلاعات تهاجمی حتی اگر قانونی هم به‌حساب بیاید غیر اخلاقی محسوب می‌شود؟ چه کسی مسئول حفاظت از زیرساخت‌های حیاتی است؟ چطور جرایم را می‌توان با موفقیت مورد بررسی و تحت تعقیب قرار داد، هنگامی که مجرم در یک ایالت یا کشور دیگر دور از دسترس قربانی و یا منابع اطلاعاتی، مورد تهاجم، قرار گیرد. این‌ها و موارد دیگر در این کتاب مورد بررسی قرار می‌گیرند و هدف آن بالا بردن درک تهدیدات، دفاع و مسائل مربوط به این‌ها است.

تحقیق این کتاب مدیون تلاش افراد بسیار دیگری است که قبل از من وجود داشته و به دانش من در این زمینه کمک کرده‌اند و نیز کسانی که طرح اولیه کتاب را خوانده و در مورد آن اظهار نظر کرده‌اند. نام بردن از تمامی آن‌ها غیرممکن است اما تعدادی شایسته‌ی ذکر

---

[1]. On - line

هستند. گروه اول دانشجویان کلاس جنگ اطلاعات‌اند. علاقهٔ من در نگارش این کتاب در هنگام تدریس این درس در بهار سال ۱۹۷۷ به وجود آمد. طرح‌های ترمی برجستهٔ *مایکل براون*، *اریک هیس*، *بروس کامر*، *هولی‌کیلو* و *هیثریو*، *چاد لهب* و *کلی مک‌اینتر*؛ و همچنین سایت اینترنتی "*۱۰۰ رخداد جنگ اطلاعات*" که *داگ کیسی*، *جو کالگیوتو* و *مارک سمپل* ایجاد کردند، همگی منابع لازم را در اختیار من گذاشتند. نسخهٔ اولیهٔ این کتاب را به موقع برای کلاس‌های بهار سال ۱۹۹۸ آماده کردم و بازخوردهای طول ترم، نسخهٔ بعدی کتاب را شکل دادند. از افراد زیر تشکر می‌کنم: *اصیل احمد*، *گرت آلن*، *دیوید بونی*، *لورا بَردی*، *ریچارد کلارک*، *مایکل کلینگ*، *رابرت کاپلی*، *آلن فاچت*، *آرون فرانک*، *کالین کالاگر*، *اسکات هالیدی*، *نیکل هیدر*، *جیمز هایدز*، *م. بلک*، *مثیو هیل آر*، *هیون هرست*، *جان جکسن*، *تِروسِ لارسن*، *جنیفر لِی*، *کاترین لوتریو*، *گریگوری لوکاس*، *جسیکا مک‌اینتر*، *جان مک‌کی*، *دراسی نوریک*، *برایان ریلی*، *سارا روک*، *جنیفر شین*، *ریچارد تایلر*، *جنیفر ریگر*، *استفان ینگ* و *امیت یوران*.

بیشتر مطالب منبع از طریق اینترنت از شبکه‌های خبری و همکاران به دست آمده‌اند. از *اریک نلسون* به‌خاطر راه‌اندازی فهرست لیست الکترونیکی (g2i) "get-the-world-out-intelligence" و تمامی کسانی که به آن نامه می‌فرستند، از *بیل چرچ* به خاطر اطلاعات و تحلیل‌های ارزشمند ارائه شده توسط مرکز مطالعات جنگ زیرساختاری (www.iwar.org)، از *وین شوارتاو* و *بتی اوهِرن* به خاطر منابع گستردهٔ ارائه شده در سایتشان (www.infowar.com)، از *دیو فاربر* برای فهرست توزیع پست الکترونیکی خود و از *بیل بونی* به خاطر e-mail پست‌های الکترونیکی مدام، همراه با مقالات مرتبش تشکر می‌کنم. از *ویلیام باگ*، *کریستین فرای*، *فرانک هوستون*، *جورج هوستون*، *مارتین لیبیکی*، *آوی رابین*، *پیتر سالوس*، *گری‌گوری وایت* و بازبین‌های گمنامی که نسخهٔ اولیهٔ کتاب را خواندند و پیشنهاد و نظر سودمندی ارائه کردند، تشکر می‌کنم. از *لئونارد ادلمان*، *آلن بریل*، *کاویکا داگیو*، *چاک دکارو*، *پیتر دنینگ*، *دان فارمر*، *میک کابی*،*کارلوکاپ*، *استیون لیپنر*، *جاناتان لیتمان*، *ویل اوزیر*، *بل پراکتر*، *جوشواکویتنر*، *دیوید نفلت*، *یوجین شولتز* و *ایرا وینکلر* به‌خاطر اظهار نظر در مورد بخش‌هایی از کتاب تشکر می‌کنم. از کارمندان *ادیسن - وِسلی* به‌خاطرحمایت بی‌دریغشان، به‌خصوص *هلن گلدشتاین*، که هماهنگی طرح را در اختیار داشت، *جکی یانگ*، که امر تولید و *پیتر گوردَن* که با اشتیاق تمام سه کتاب من را مورد پشتیبانی قرار داد، از همگی تشکر می‌کنم و سرانجام، از شوهرم، *پیتر دنینگ* به‌خاطر حمایت عاشقانه‌اش سپاسگزارم.

***دروثی ای دنینگ***
***دانشگاه جورج تاون***
**اکتبر ۱۹۹۸**
www.cs.georgetown.edu/_denning

# پیشگفتار

با توسعه فناوری‌های اطلاعـات و ارتباطـات (ICT)، موضـوع جنـگ اطلاعـات در میـان جوامع و سازمانهای اطلاعاتی، امنیتی و دفاعی در سالهای اخیر مورد توجه بیشتری قرار گرفتـه است. این موضوع عمدتاً از این واقعیت نشأت می‌گیرد که فناوریهای اطلاعات و ارتباطات به‌طور اعّم برای امنیت ملی و به‌طور اخص برای موضوعات اطلاعاتی، امنیتـی، نظـامی و دفـاعی حـایز اهمیت هستند و بر همین اساس امروزه شاهد جنگهای پیشرفته با محوریت فناوریهای اطلاعات و ارتباطات هستیم. برتری سیستم‌های اطلاعاتی و ارتباطاتی یک نظام در دنیای کنونی، تقریبـاً معادل برتری و مزیت نسبی آن نظام در عرصه‌های مختلف می‌باشد و این حقیقت بخودی خود شیوه‌های سنتی مربوط به فعالیتهای اطلاعاتی، امنیتی، نظامی و دفاعی را تحت‌الشعاع قرارداده و کم اهمیت و کم کارآمد خواهد ساخت. از اینرو به نظر رسید که ترجمه این کتاب تحت عنوان "جنـگ اطلاعات و امنیت" در این برهه از زمان از اهمیت خاصی برخوردار بـوده و بـرای آحـاد مـردم و به‌خصوص برای کارشناسان، محققین و مدیران مرتبط با موضوع خیلی مفید می‌باشد.

کتاب حاضر، مقدمه‌ای است بر جنگ اطلاعات و مسائل امنیتی مـرتبط بـا آن کـه در دانشـگاه جرج‌تاون آمریکا برای دانشجویان مقطع لیسانس (سال آخر) تـدریس مـی‌شـود. محتـوای ایـن کتاب به‌طور کل شامل محتوای یک کتاب جامع دانشگاهی نیست، ولی مطالعهٔ آن بـرای کلیـه کارشناسان و متخصصین در مقاطع مختلف لیسانس، فوق‌لیسانس و دکتری، بـه‌خصـوص بـرای

کارشناسان و دست‌اندرکاران فعالیتهای اطلاعاتی، امنیتی، نظامی و دفاعی و حتی برای آحاد مردم نیز، مفید است. این کتاب شامل سه بخش است که طیف وسیعی از مطالب مربوط به جنگ اطلاعات و امنیت را شامل می‌باشد. در بخش اول که سرفصل است درخصوص مفاهیم و اصول جنگ اطلاعات بحث می‌شود. بخش دوم به بررسی عملیات جنگ اطلاعات تهاجمی می‌پردازد که شامل هشت فصل است. در بخش، جنگ اطلاعات تدافعی بحث و بررسی می‌شود که این بخش نیز خود شامل پنج فصل است. در تمامی این فصول، کتاب به معرفی شرکتها و محصولات و نیز از همه مهمتر به حوادث و وقایع مرتبط با جنگ اطلاعات و امنیت می‌پردازد و سعی می‌کند که فضای موجود در این عرصه را تا حدودی برای خوانندگان ترسیم کند. قابل ذکر است که مترجمان، تدریس این کتاب را برای مقاطع دانشگاهی (به‌خصوص برای مقاطع کارشناسی ارشد و دکتری) توصیه نمی‌کنند ولی مطالعه آن را برای همه مفید می‌دانند.

ترجمه این کتاب مدیون تلاش افراد زیادی است که بدینوسیله لازم است مراتب تشکر و قدردانی خود را از همهٔ آنها، به‌خصوص از مسئولین و دست‌اندرکاران پژوهشکده پردازش هوشمند علائم به‌خاطر حمایت‌ها و پشتیبانی‌های مادی و معنوی‌شان، از مساعدتهای مؤثر و گرانبهای جناب آقای محمدعلی حسین‌نژاد و جناب آقای محمودرضا روحانی در امر ترجمه، از همکاریهای بی‌دریغ جناب‌آقای محمداسماعیل قاصدی و سرکار خانم نازیلا خلخالی در امر ویرایش و از زحمات ارزشمند جناب آقای جواد باقری و سرکار خانم طاهره درمانی که در حروفچینی و صفحه‌آرایی این اثر از هیچ کمکی مضایقه ننمودند، اعلام نمایم.

***والسلام***

***پژوهشکده پردازش هوشمند علائم***

***جواد شیخ‌زادگان***

***بهار ۱۳۸۳***