

مبانی اطلاعات در فضای سایبر

مؤلفان:

رضا قاسمی

وحید مجید

دانشگاه علوم انتظامی امین

۱۳۹۴



دانشگاه علوم انتظامی امین

مبانی اطلاعات در فضای سایبر

مؤلف: رضا قیاسی، وحید مجید

ناظر علمی: سید کمال هادیانفر

ناشر: دانشگاه علوم انتظامی امین

آماده سازی کتاب: عصر دانش

طراح جلد: مجید خان محمدزاده

چاپ اول: ۱۳۹۴

شمارگان: ۵۰۰ نسخه

قیمت: ۱۸۰۰۰۰ ریال

لیتوگرافی، چاپ و صحافی: راه فردا

نشانی: تهران - ابتدای بزرگراه شهید خرازی - خیابان شهید مدنی اردبیلی - دانشگاه علوم انتظامی امین -

معاونت پژوهش و فناوری - تلفن: ۴۸۹۳۱۲۹۳

سرشناسه: قیاسی، رضا، ۱۳۶۷ -

عنوان و نام پدیدآور: مبانی اطلاعات در فضای سایبر / مؤلفان رضا قیاسی، وحید مجید ناظر علمی سید کمال هادیانفر؛

[برای] دانشگاه علوم انتظامی امین، معاونت پژوهش و فناوری.

مشخصات نشر: تهران: دانشگاه علوم انتظامی امین، ۱۳۹۴.

مشخصات ظاهری: ۴۴۰ ص.

شابک: ۲۵۰۰۰۰ ریال 6-110-363-600-978

وضعیت فهرست نویسی: فیا

یادداشت: کتابنامه: ص. ۴۳۱ - ۴۴۰؛ همچنین به صورت زیرنویس.

موضوع: فضای مجازی - تدابیر ایمنی

موضوع: شبکه های کامپیوتری - تدابیر ایمنی

موضوع: کامپیوترها - ایمنی اطلاعات

موضوع: جرایم کامپیوتری - پیشگیری

شناسه افزوده: مجید، وحید، ۱۳۴۳ -

شناسه افزوده: هادیانفر، کمال، ناظر

شناسه افزوده: دانشگاه علوم انتظامی امین. معاونت پژوهش و فناوری

شناسه افزوده: دانشگاه علوم انتظامی امین

رده بندی کنگره: HM۱۳۹۴۸۵۱/۹۲ق/ رده بندی دیویی: ۴۸۳۳/۳۰۳ شماره کتابشناسی ملی: ۴۰۶۷۸۲۵

پیشگفتار مؤلف

فضای سایبری شرایط نوینی پدید آورده که موجب شکل گیری نظامی نوین در گستره جهان شده است زیرا در جمع آوری، نگهداری، دسترسی، پردازش، تجزیه، تحلیل و تبادل اطلاعات، تحولی شگرف رخ نموده است که در پرتو این تحول، فرصت ها و تهدیدات جدیدی پدید آمده است. این فرایند تناقض آمیز است زیرا همزمان فرصت می آفریند و تهدید می زاید. فضای سایبری همراه با نیروی انسانی دانا و پویا، زیرساخت و بستر اعمال قدرت از راه دور است. به عبارت دیگر بهره گیری گسترده و هوشمند از فناوری اطلاعات و ارتباطات، شکل حاکمیت و اقتدار در هر دایره ملی و دشوری را دستخوش تغییر می کند و در نتیجه دامنه نفوذ حاکمیت را متحول می سازد و ظرفیت ایجاد تهدید و فرصت و پوشش رقابت های ساخت یافته اقتصادی و فرهنگی را اطلاعاتی را نشان می دهد.

از سویی جوامع امروزی بدون در نظر گرفتن زیرساخت های فضای سایبری نمی توانند پیشرفتی همسان و همگام با دیگر کشورهایی که این فضا را در اختیار دارند داشته باشند اما از سوی دیگر این فضا تهدیدات امنیتی جدیدی را در جوامع پدید می آورد زیرا بنیان های رفتاری در حوزه امنیت بر مبنای اطلاعات برپایه این فضا شکل می گیرد. در این شرایط بخش اعظم جنگ های سخت تبدیل به جنگ نرم می شود، در واقع شکل تهدیدات به شدت دگرگون می شود. در این حالت امنیت نیز مفهومی جدید می یابد و اهداف در چارچوب امنیت متحول می گردند و چون ماهیت نموده است، تامین امنیت نیز دگرگون می گردد.

ایجاد امنیت در این فضا قبل از هر اقدامی از اهمیت بالاتر برخوردار است که برای انجام این مهم، ابتدا باید شناختی کامل از آن حوزه به ویژه از نظر آسیب ها و تهدیداتی که بر آن مترتب می گردد به دست آورد و سپس اقدامات امنیتی که برای

حفاظت از این فضا و امن سازی آن ضروری می شود را طراحی و اجرا نمود. یکی از اقدامات مهم امنیتی در این فضا اقدامات پدافند غیرعامل است. همچنان که رعایت اصول و ملاحظات اساسی پدافند غیرعامل بخشی از ارکان دفاعی محسوب می گردد در امن سازی فضای سایبری نیز موثر خواهد بود.

www.ketab.ir

سخن ناشر

کسب علم و دانش و تلاش برای بهره‌گیری از علوم جدید و بومی‌سازی آن برای رفع نیازهای علمی، فرهنگی، اجتماعی و اقتصادی به منظور اعتلای اقتدار امت اسلامی از توصیه‌های مهم اسلام است. علوم پلیسی که همگام با پیشرفت بسیاری از علوم محض و تلفیق آنها با یکدیگر، روز به روز نو می‌شود و مرزهایی تازه از دانش می‌سازد، از جمله علمی است که درخت آن در کشورمان در حال رشد و نمو و ثمر دادن است. تأات آثار علمی برجسته و معتبر و اشاعه مفاهیم آنها از جمله رهیافت‌های کارآمد و اثربخش است که می‌توان در سایه آن بستری مناسب برای بهره‌گیری از تجربه‌های ارزشمند و دانش برجسته نخبگان و کارشناسان علوم پلیسی در کشورمان ساخت. بدیهی است اندیشمندان، محققان و کارشناسان امور پلیسی داخلی می‌توانند با تلفیق همگن تجربه‌های خود با علوم و تجربیات کارشناسان علوم پلیسی دیگر کشورها باعث پیشبرد دانش پلیسی در کشور شوند. بدست با نشر آثار تألیفی از این دست، گامی هر چند کوچک در این مسیر بلند برداریم. نویسندگان، محققان، کارشناسان و استادان را برانگیزانیم تا تجربه‌ها و توان علمی خود را سبیل و اشاعه دهند.

انتشارات نگاه علوم انتظامی امین

فهرست مطالب

صفحه	عنوان
۲۱	فصل اول: کلیات اطلاعات
۲۲	۱-۱- مقدمه
۲۳	۱-۲- کلیات اطلاعات
۳۶	۱-۳- تاریخچه اصول و مبانی اطلاعات
۳۸	۱-۴- مفاهیم اطلاعات
۳۹	۱-۵- تعاریف اصول و مبانی اطلاعات
۴۰	۱-۶- آشنایی با اهمیت و ضرورت اطلاعات
۴۱	۱-۷- کارکرد اطلاعات
۴۱	۱-۸- جمع آوری اخبار و اطلاعات
۴۲	۱-۸-۱- بررسی
۴۲	۱-۸-۲- اقدام پنهان
۴۲	۱-۸-۳- ضد اطلاعات
۴۲	۱-۹- اصول اطلاعات
۴۵	فصل دوم: مفاهیم خبر
۴۶	۲-۱- مقدمه
۴۷	۲-۲- ماهیت جمع آوری اخبار
۴۷	۲-۳- تعاریف اخبار
۵۰	۲-۴- تعاریف دیگر اخبار
۵۱	۲-۵- ویژگی های جمع آوری اخبار
۵۱	۲-۶- اصول جمع آوری اخبار
۵۱	۲-۷- اهداف جمع آوری اخبار
۵۳	۲-۸- منشأ اخبار

۵۴	۲-۹- انواع منشأ خبر
۵۴	۲-۱۰- منبع اخبار
۵۶	۲-۱۱- استخدام منبع و ارتباط پنهانی او با سازمان
۵۸	۲-۱۲- ویژگی منابع انسانی
۶۳	۲-۱۳- همکا
۶۴	۲-۱۴- مأمور
۶۷	فصل سوم: فوری و مدار اطلاعاتی
۶۸	۳-۱- مقدمه
۶۹	۳-۲- فناوری و تاثیر آن بر مدار اطلاعات
۷۲	۳-۳- سازمان‌های اطلاعاتی در فضای مجازی
۷۳	۳-۴- ساختار اتصالات شبکه در اینترنت
۷۴	۳-۵- نشان‌دار کردن سوژه‌ها در فضای سایبر
۷۶	۳-۶- ارتباط با منابع
۸۰	۳-۷- فناوری اطلاعات
۸۰	۳-۸- ارتباط
۸۰	۳-۹- منابع انسانی
۸۱	۳-۱۰- جستجو در اینترنت
۸۳	۳-۱۱- موتورهای جستجو و تکنیک‌های استفاده از آنها
۸۴	۳-۱۲- تعریف موتور جستجو
۸۵	۳-۱۳- راهبرد جستجو در اینترنت
۸۷	۳-۱۴- نکات کلیدی جستجو به زبان فارسی
۸۸	۳-۱۵- مبانی جستجو در اینترنت
۹۲	۳-۱۶- اسرار جستجوی موفق در اینترنت
۹۳	۳-۱۷- طرح جمع‌آوری اطلاعات از اینترنت
۹۴	۳-۱۸- موقعیت در اینترنت

۹۴	۱۹-۳- زمان جمع آوری اطلاعات
۹۵	۲۰-۳- مراحل طرح جمع آوری اطلاعات اینترنتی
۹۸	۲۱-۳- استفاده از طرح جمع آوری اطلاعات اینترنتی
۹۸	۲۲-۳- منابع اینترنت
۱۱۳	۲۳-۳- تحلیل حرکات در اینترنت
۱۱۴	۲۴-۳- ارتباط داشتن با دیگران
۱۱۵	۲۵-۳- نتیجه گیری
۱۱۵	۲۶-۳- ارزیابی منابع
۱۱۶	۲۷-۳- تعیین منابع صفحات اینترنتی
۱۱۹	۲۸-۳- فهرست ارزیابی برای صفحات خبری اینترنتی
۱۲۲	۲۹-۳- فهرست ارزیابی برای صفحه اینترنتی اطلاعاتی
۱۲۴	۳۰-۳- فهرست ارزیابی برای صفحات اینترنتی شخصی
۱۲۶	۳۱-۳- انواع جمع آوری
۱۲۶	۳۱-۳-۱- جمع آوری آشکار
۱۲۶	۳۱-۳-۲- جمع آوری پنهان
۱۲۷	۳۲-۳- اطلاعات
۱۲۷	۳۳-۳- اهمیت جمع آوری اطلاعات از طریق فناوری اطلاعات
۱۲۸	۳۴-۳- کاربردهای فناوری اطلاعات
۱۲۹	۳۵-۳- شبکه جهانی اینترنت (World - Wide - Web)
۱۲۹	۳۵-۳-۱- اینترنت
۱۳۲	۳۵-۳-۲- اینترنت چیست؟
۱۳۴	۳۵-۳-۳- شبکه جهانی چیست و چگونه کار می کند؟
۱۳۴	۳۶-۳- پست الکترونیکی (e-mail):
۱۴۳	فصل چهارم: فضای سایر
۱۴۴	۱-۴- مقدمه

۱۴۴	۲-۴- فضای سایبری چیست؟
۱۴۵	۳-۴- چرا فضای سایبری اهمیت دارد؟
۱۴۶	۴-۴- ویژگی‌های فضای سایبری
۱۴۹	فصل پنجم: آسیب پذیری‌های فضای سایبری
۱۵۰	۱-۵- مقدمه
۱۵۲	۲-۵- آسیب‌پذیری دلیلی برای تهدید
۱۵۶	۳-۵- آسیب‌پذیری‌های فضای سایبری
۱۵۷	۴-۵- حفظ حریم خصوصی کاربران در گوگل
۱۶۵	فصل ششم: تهدیدات فضای سایبری
۱۶۶	۱-۶- مقدمه
۱۶۸	۲-۶- تهدیدات فضای سایبری
۱۶۹	۳-۶- تهدیدات توسعه یافته ترامل ن
۱۶۹	۱-۳-۶- مجرمین
۱۷۰	۲-۳-۶- دولت‌ها
۱۷۰	۳-۳-۶- تروریست‌ها
۱۷۱	۴-۶- توانمندی علمی مهاجمین در فضای سایبری
۱۷۶	۵-۶- انواع حملات در فضای سایبری
۱۷۹	۱-۵-۶- حمله خواندن
۱۸۲	۲-۵-۶- دستکاری
۱۷۴	۳-۵-۶- جعل
۱۸۸	۴-۵-۶- سیل
۱۹۲	۵-۵-۶- حمله هدایت
۱۹۳	۶-۵-۶- حملات ترکیبی
۱۹۶	۷-۵-۶- نتایج حمله
۱۹۷	۶-۶- عوامل تهدیدزا در فضای سایبری

- ۱۹۸ -۷-۶ دسته بندی عوامل تهدیدزا در فضای سایبری از نظر شدت
- ۱۹۹ -۸-۶ شیوه‌های حمله به فضای سایبری
- ۲۰۱ -۹-۶ حملات غیرفعال
- ۲۰۲ -۱۰-۶ حملات فعال
- ۲۰۴ -۱۱-۶ برنامه‌های اسب تراوا
- ۲۰۴ -۱۲-۶ اشتراک‌های ویندوزی حفاظت نشده
- ۲۰۵ -۱۳-۶ کدهای قابل انتقال
- ۲۰۷ -۱۴-۶ اسکریپت‌های کراس سایت
- ۲۰۷ -۱۵-۶ پست‌های الکترونیکی جعلی
- ۲۰۹ -۱۵-۱-۱-۱۵-۶ ریزس‌های داخل پست الکترونیکی
- ۲۰۹ -۱۶-۶ پسوندهای مخفی فایل
- ۲۱۱ -۱۷-۶ خدمات گیرندگان
- ۲۱۱ -۱۸-۶ شنود بسته‌های اطلاعات
- ۲۱۲ -۱۹-۶ حمله به برنامه‌های وبی
- ۲۱۵ -۲۰-۶ حمله تزریق اسکریپت
- ۲۱۹ -۲۱-۶ دزدی هویت
- ۲۲۱ -۲۲-۶ پنج روش محافظت در مقابل فیشینگ
- ۲۲۴ -۲۳-۶ گوگل ارث تهدیدی جدی برای امنیت ملی
- ۲۲۵ -۱-۲۳-۶ گوگل ارث چیست؟
- ۲۲۶ -۲-۲۳-۶ تاریخچه گوگل ارث
- ۲۲۷ -۳-۲۳-۶ تهدیدات گوگل ارث
- ۲۲۹ -۲۴-۶ جاسوسی گوگل برای سازمان اطلاعات آمریکا
- ۲۳۴ -۲۵-۶ سانسورهای گوگل ارث
- ۲۳۷ فصل هفتم: جاسوسی در فضای سایبری
- ۲۳۸ -۱-۷ مقدمه

- ۲۴۰ -۲-۷ فضای سایبری و جمع آوری پنهان
- ۲۴۰ -۳-۷ جمع آوری اطلاعات تصویری در فضای سایبری
- ۲۴۳ -۴-۷ جمع آوری اطلاعات فنی در فضای سایبری
- ۲۴۴ -۵-۷ جمع آوری انسانی در فضای سایبری
- ۲۴۴ -۶-۷ جمع آوری اطلاعات رایانه ای در فضای سایبری
- ۲۴۶ -۷-۷ راهبری و هدایت جاسوسان در فضای سایبری
- ۲۴۷ -۸-۷ ارتباطات ماهواره ای
- ۲۴۸ -۹-۷ ارتباطات اینترنتی
- ۲۴۹ -۱۰-۷ ارتباطات با استفاده از شیوه های مبتنی بر رمزنگاری و پوشیده-نگاری
- ۲۵۱ -۱۱-۷ ضد جاسوسی در فضای سایبری
- ۲۵۱ -۱-۱۱-۷ الف) تبادل اطلاعات در فضای سایبری
- ۲۵۱ -۲-۱۱-۷ ب) کنترل مظنونین و فضای سایبری
- ۲۵۲ -۳-۱۱-۷ پ) تعقیب و مراقبت در فضای سایبری
- ۲۵۲ -۴-۱۱-۷ ت) ورود پنهان در فضای سایبری
- ۲۵۴ -۵-۱۱-۷ ث) نرم افزارهای جاسوسی و چگونگی مقابله با آن
- ۲۵۶ -۱۲-۷ نرم افزارهای جاسوسی در فضای سایبری
- ۲۵۷ -۱۳-۷ انواع نرم افزارهای جاسوسی
- ۲۵۷ -۱-۱۳-۷ نرم افزار جاسوسی خانگی
- ۲۵۸ -۲-۱۳-۷ نرم افزار جاسوسی تجاری
- ۲۵۹ -۱۴-۷ انواع و اهداف نرم افزارهای جاسوسی مختلف
- ۲۵۹ -۱-۱۴-۷ ثبت کنندگان نشانی های وب و صفحات نمایش
- ۲۵۹ -۲-۱۴-۷ ثبت کنندگان چت و پست الکترونیکی
- ۲۶۰ -۳-۱۴-۷ ثبت کنندگان کلید و کلمات عبور
- ۲۶۲ -۱۵-۷ نصب نرم افزار جاسوسی و روش مقابله با آن

۲۶۷ ۱۶-۷- روش های حمله به سامانه پست الکترونیکی

۲۷۰ ۱۷-۷- توانمندی دیوار آتش و ضد ویروس

۲۷۱ ۱۸-۷- رویکرد پیشگیرانه برای حفاظت از رایانه ها

۲۷۳ فصل هشتم: امنیت و پدافند در فضای سایبری

۲۷۴ ۱-۸- مقدمه

۲۷۴ ۲-۸- مفهوم امنیت

۲۷۶ ۳-۸- رابرد امنیتی در فضای سایبری

۲۷۷ ۴-۸- استفاده از فرصت های فضای سایبری

۲۷۷ ۵-۸- ارتقای دانش علمی

۲۷۸ ۶-۸- مفهوم امنیت فضای سایبری

۲۸۳ فصل نهم: جرایم سایبری

۲۸۴ ۱-۹- مقدمه

۲۸۵ ۲-۹- جرم رایانه ای (ایستاد)

۲۸۶ ۳-۹- مبنای تشخیص جرایم اینترنتی

۲۸۷ ۴-۹- مهم ترین جرم های اینترنتی در جهان

۲۸۹ فصل دهم: شبکه پنهان

۲۹۰ ۱-۱۰- آشنایی با شبکه های اجتماعی

۲۹۰ ۱-۱-۱۰- وب ۲

۲۹۱ ۲-۱-۱۰- تفاوت وب ۲ و وب ۱

۲۹۲ ۳-۱-۱۰- مولفه های وب ۲

۲۹۳ ۴-۱-۱۰- انواع سایت های وب ۲

۲۹۳ ۲-۱۰- شبکه های اجتماعی مجازی

۲۹۶ ۱-۲-۱۰- خصوصیات شبکه های اجتماعی مجازی

۲۹۶ ۲-۲-۱۰- کارکردهای شبکه های اجتماعی مجازی

۲۹۶ ۳-۲-۱۰- گونه شناسی مراجعین

- ۲۹۹ ۳-۱۰- کلیات اقدامات سازمان‌های اطلاعاتی در رابطه با شبکه‌ها
- ۳۰۰ ۱-۳-۱۰- نیازسنجی
- ۳۰۱ ۲-۳-۱۰- شناخت کافی
- ۳۰۱ ۳-۳-۱۰- الفا و مدیریت افکار عمومی
- ۳۰۲ ۴-۳-۱۰- افکارسنجی
- ۳۰۳ ۴-۱۰- اهمیت شبکه منابع پنهان برای سازمان‌های اطلاعاتی
- ۳۰۵ ۵-۱۰- جمع‌آوری در شبکه‌های اجتماعی مجازی
- ۳۰۵ ۱-۵-۱۰- جمع‌آوری آشکار
- ۳۱۰ ۶-۱۰- نشان و استخدام منابع در شبکه‌های اجتماعی مجازی
- ۳۱۰ ۱-۶-۱۰- آشنایی کامل، فرهنگ حاکم بر شبکه‌های اجتماعی مجازی
- ۳۱۱ ۲-۶-۱۰- ثبت نام و عضویت
- ۳۱۱ ۳-۶-۱۰- آشنایی با روش‌ها و ترفندهای جذب مخاطب
- ۳۱۲ ۴-۶-۱۰- پوشش و هم‌رنگی
- ۳۱۳ ۵-۶-۱۰- ایجاد و جلب اعتماد
- ۳۱۵ ۷-۱۰- عملیات نشان در شبکه‌های اجتماعی مجازی
- ۳۱۵ ۸-۱۰- شاخص‌ها و معیارهای کاربران نشان شونده و نشان‌ها در شبکه‌های اجتماعی
- ۳۱۹ ۹-۱۰- مراحل و ملاحظات استخدام منابع پنهان در شبکه‌های اجتماعی مجازی
- ۳۱۹ ۱-۹-۱۰- رعایت ویژگی‌ها و شاخص‌های عملیاتی نشان در شبکه‌ها
- ۳۱۹ ۲-۹-۱۰- طبقه‌بندی کاربران و اخذ تماس
- ۳۲۰ ۳-۹-۱۰- بررسی انگیزشی و روانی کاربر منتخب یا کاندیدا
- ۳۲۰ ۴-۹-۱۰- انجام ارتباط و تبادل آزمایشی اطلاعات با کاربر منتخب یا کاندید
- ۳۲۰ ۵-۹-۱۰- طرح دعوت به همکاری

- ۳۲۳ ۱۰-۹-۶- ملاقات و توجیه اولیه
- ۳۲۴ ۱۰-۹-۷- واگذاری مأموریت آزمایشی
- ۳۲۴ ۱۰-۹-۸- آموزش
- ۳۲۵ ۱۰-۹-۹- پشتیبانی و هدایت
- ۳۲۵ ۱۰-۹-۱۰- ارتباط هادی یا منبع
- ۳۲۶ ۱۰-۹-۱۱- واگذاری مأموریت به منبع (به کارگیری)
- ۳۲۶ ۱۰-۹-۱۱- اخذ نتیجه مأموریت از منبع
- ۳۲۷ ۱۰-۹-۱۲- ارزیابی دائمی هادی از منبع
- ۳۲۷ ۱۰-۹-۱۳- طایفه بندی اطلاعات و بررسی صحت آن
- ۳۲۷ ۱۰-۹-۱۴- حذف منبع
- ۳۳۱ ۱۰-۱۰-۱- پیدایش فیس بوک
- ۳۳۲ ۱۰-۱۱-۱- ویژگی ها و اصول فیس بوک
- ۳۳۵ ۱۰-۱۲- حمایت اطلاعاتی فیس بوک و حمایت سازمان های اطلاعاتی از آن
- ۳۳۸ ۱۰-۱۳- چگونگی هدایت منابع پنهان در شبکه های اجتماعی و فیس بوک توسط سازمان های اطلاعاتی آمریکا
- ۳۳۹ ۱۰-۱۳-۱- مرحله نشان (نشان و تحقیق)
- ۳۴۰ ۱۰-۱۳-۲- جذب و جلب همکاری (انتخاب و دعوت به همکاری)
- ۳۴۱ ۱۰-۱۳-۳- واگذاری مأموریت و اخذ نتیجه (بهره کشی)
- ۳۴۲ ۱۰-۱۳-۴- ارائه آموزش های لازم
- ۳۴۳ ۱۰-۱۳-۵- پشتیبانی
- ۳۴۳ ۱۰-۱۳-۶- کنترل و ارزیابی
- ۳۴۴ ۱۰-۱۳-۷- حذف
- ۳۴۵ ۱۰-۱۴- چیستی ها در فضای سایبر
- ۳۴۵ ۱۰-۱۵- سایبر و فضای سایبر (cyber&cyberspace)

- ۳۴۶ ۱۰-۱۶- قدرت سایبر
- ۳۴۶ ۱۰-۱۷- فضای سایبر و ویژگی‌های آن
- ۳۵۰ ۱۰-۱۸- ورود سایبر به عرصه نبردهای اطلاعاتی
- ۳۵۱ ۱۰-۱۹- حضور نهادهای اطلاعاتی در فضای سایبر
- ۳۵۲ ۱۰-۲۰- اطلاعات و روش‌های جمع‌آوری آن
- ۳۵۵ ۱۰-۲۱- شبکه پنهان
- ۳۵۵ ۱۰-۲۲- مجموعه عناصر هدایت
- ۳۵۶ ۱۰-۲۳- فرآیندهای مورد استفاده برای منابع و عوامل
- ۳۵۸ ۱۰-۲۴- اهمیت جمع‌آوری مان
- ۳۵۹ ۱۰-۲۵- ضرورت‌های هدایت شبکه پنهان در فضای سایبر
- ۳۶۳ ۱۰-۲۶- هدایت منابع پنهان در فضای سایبر
- ۳۶۴ ۱۰-۲۷- ویژگی‌های هدایت منابع در فضای مازی
- ۳۷۰ ۱۰-۲۸- بازیگران هدایت منابع پنهان در فضای سایبر
- ۳۷۳ ۱۰-۲۹- ابزارهای هدایت منابع پنهان و فضای سایبری
- ۳۷۴ ۱۰-۳۰- محیط‌های هدایت منابع پنهان در فضای سایبری
- ۳۷۴ ۱۰-۳۱- کارکردهای هدایت منابع پنهان در فضای سایبری
- ۳۷۵ ۱۰-۳۲- تشابهات و افتراقات هدایت منابع در فضای فیزیکی و سایبری
- ۳۸۳ ۱۰-۳۳- شرحی پیرامون جنگ اطلاعاتی
- ۳۸۴ ۱۰-۳۴- تروریسم سایبری
- ۳۸۵ ۱۰-۳۵- جنگ اطلاعات
- ۳۸۵ ۱۰-۳۶- نقش فضای سایبر در انتقال اطلاعات
- ۳۸۷ ۱۰-۳۷- عوامل درگیر در فضای سایبر
- ۳۸۹ ۱۰-۳۸- جنگ اطلاعاتی
- ۳۹۰ ۱۰-۳۹- تعریف جامع جنگ اطلاعاتی
- ۳۹۲ ۱۰-۴۰- ابزارهای جنگ اطلاعاتی

- ۳۹۴ ۱۰-۴۱- روش‌های جنگ اطلاعات
- ۳۹۵ ۱۰-۴۲- حملات اطلاعاتی
- ۳۹۶ ۱۰-۴۳- تهدیدات سایبری علیه جمع‌آوری پنهان
- ۴۰۳ فهرست منابع