

۱۴۱۶/۱۲/۱
۹۵/۴/۸

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

صنعت تبهکاری سایبری

رؤیة‌های اقتصادی، نهادی و راهبردی

مؤلف:

بیر شتری

ترجمه:

مهندس احمد رومانی

۱۳۹۵

سرشناسه	: شتری، نیر Kshetri, Nir
عنوان و نام پدیدآور	: صنعت تبهکاری سایبری: رویه‌های اقتصادی، نهادی و راهبردی / مؤلف نیر شتری؛ مترجم احمد روحانی.
مشخصات نشر	: تهران: احمد روحانی، ۱۳۹۵.
مشخصات ظاهری	: ۲۹۰ ص.: مصور، جدول، نمودار.
شابک	: ۹۷۸۶۰۰۴۱۲۱۱۱
وضعیت فهرست نویسی	: فیبا
یادداشت	: عنوان اصلی: Role Organized Crime in Industry; Cybercrime, Economics, Institutional and Strategic Perspectives (۲۰۱۰)
یادداشت	: واژه‌نامه.
عنوان دیگر	: رویه‌های اقتصادی، نهادی و راهبردی.
موضوع	: راییم کامپیوتری
موضوع	: ترسیم ایانه‌ای
شناسه افزوده	: راجاز، احمد - ۱۳۵۱ - مترجم
رده بندی کنگره	: ۱۳۹۵ / ۶۷۷۳ HV
رده بندی دیویی	: ۱۶۸/۳۶۴
شماره کتابشناسی ملی	: ۳۵۲۵۵۹۴

صنعت تبهکاری سایبری (رویه‌های اقتصادی، نهادی و راهبردی)

ترجمه: مهندس احمد روحانی

ویراستار فنی و ادبی: مرضیه بهلولی اسکویی

تایپ و صفحه آرایی: الناز پوراسد

نوبت چاپ: اول، ۱۳۹۵

شمارگان: ۱۰۰۰ نسخه

چاپ و لیتوگرافی: مطهر

قیمت: ۱۷۰۰۰۰ ریال

نشانی ناشر: تهران، خ ایرانشهر شمالی، یک شاداب، پ ۴

پیش گفتار نویسنده

نفوذ پرشتاب اینترنت و دیجیتالی شدن فعالیت های اقتصادی زمینه ساز نسل جدیدی از بزه کاری ها شده است. پی آمدهای اقتصادی، سیاسی و اجتماعی این بزه کاری ها (سایبری) در سال های اخیر توجه زیادی را به خود جلب کرده است. از این رو، شهروندان، صاحبان مشاغل و دولت ها نگران امنیت سیستم ها، شبکه ها و زیربنای فناوری اطلاعات و ارتباطی (فاوای) خود هستند.

با نگاهی به الگوهای بزه کاری های سایبری، مشخص می شود بسیاری از فرضیه های برجسته درباره آنها ناقص، غیرواقعی و نامعقول است. گزارش های تجربی درباره الگوها و راهبردهای پیش گیری و مقابله با پیس بزه کاری هایی نیز با مؤلفه های جهان سایبری متناسب نیست. چرا که گستره سرقت های رایانه ای و بزه کاری های سایبری دچار دگرگونی های سیاسی، اجتماعی و روانشناختی شده است.

صنعت بزه کاری سایبری، حوزه بسیار جدیدی است. اگر چه باور عمومی بر این است که این صنعت بی اندازه بزرگ (بزرگ کرده) است اما درباره ساختار و گستره واقعی آن دانش اندکی دارند. تحقیقات منتشر شده اندکی عوامل اقتصادی و سازمانی آن را بررسی کرده اند که بر راهبردها و رفتارهای عاملین مختلف آن اثر داشته اند. نظریه پردازان نیز، به بهترین شیوه، در راستای درک کنش های بزه کاران سایبری و نفوذ گر ها (دزدان اطلاعات) و روابط هم زیستی که آنها با عاملین مختلف دارند به بحث می پردازند.

دیده های ما، ماهیت در حال شکل گیری صنعت جهانی بزه کاری های سایبری را برجسته می کند و گویای آن است که بزه کاری های سایبری از هر دو رویه نظری و علمی، شروع مهمی است. در این کتاب تلاش شده است تا آن شکاف های پژوهشی گشته شده برطرف شود و گفتارهای تخصصی بیشتری بیان شود. هدف اصلی این کتاب، بررسی روندهای اقتصادی مرتبط با این صنعت (بزه کاری های سایبری) است تا به درک بهتر این بزه کاری ها به عنوان گونه ای از فعالیت های اقتصادی کمک کند و حامل توسعه راهبردهای پیش گیری از این بزه کاری ها است. هدف دیگر آن، کمک به درک فرایندهای سازمانی در صنعت بزه کاری های سایبری است. این امر با

تحلیل سازمانهای رسمی و غیررسمی^۱ این صنعت پرداخته و ساز و کارهای باز خورد مرتبط را که بر این صنعت اثر دارند بیان می شود. هدف سوم این کتاب، پیشنهادهایی در راستای جنبه کارآفرینی^۲ شرکت های دارای فعالیت های سایبری است. این کتاب، به بررسی این نکته می پردازد که چگونه کارآفرینان در جهان سایبری به سازماندهی و مدیریت مؤلفه های ضروری این کسب و کارها می پردازند. ما هم چنین، به الگوهای فعالیت بزه کاری های سایبری نگاهی دقیق خواهیم انداخت. هدف چهارم این کتاب، شرح تنوع جهانی الگوهای بزه کاری های سایبری است. عوامل اقتصادی پیش روی بزه کاران سایبری و قربانیان آن ها در کشورهای پیشرفته و در حال توسعه بسیار متفاوت است. این عوامل، در برگیرنده ماهیت و کیفیت سخت افزارها، نرم افزارها، زیرساخت ها، اهداف (قربانیان)، جایگاه مهارت های بزه کاری های سایبری و هزینه ها و منافع ناشی از آنها است. در کتاب دیگر این کتاب، درک تهدیدها و رویکردهای گوناگونی است که در این صنعت، توسط عاملین اصلی در پیش گرفته می شود.

در مجموع، با فراهم کردن شرح مختصری از ترکیب ها، نهادها، جنبه های هزینه-فایده و روال کار^۳ عاملین گوناگون بزه کاری های سایبری، امید است که این کتاب به درک بهتر و تحلیل دور

۱- سازمان رسمی، ساختاری برنامه ریزی شده از نقش ها است که در یک سازمان رسمی سامان یافته است. به دیگر سخن، سازمان رسمی، سیستم یا شبکه ای از ارتباطات و اختیارات است که افراد، گروه های یا به هم مرتبط می سازد که وظایف مهمی انجام می دهند. در ورای هر سازمان رسمی، معمولاً یک سازمان غیررسمی (مجموعه ای از روابط کاری غیر رسمی در میان اعضای سازمان) وجود دارد؛ در حالی که سازمان رسمی تعیین می کند چه کسی به چه کسی گزارش می دهد؛ سازمان غیر رسمی براین استوار است که چه کسی عملی را انجام می دهد. تعامل دارد. سازمان های غیر رسمی، شبکه ای از روابط شخصی و اجتماعی هستند که با نقش مستقیم سازمان شکل نگرفته اند؛ بلکه به گونه ای خودجوش با همکاری و معاشرت و تعامل افراد پدید می آیند. سازمان های غیر رسمی ممکن است دربرگیرنده کارکنانی از یک سازمان باشند که مثلاً در تعطیلات باهم به تفریح و ورزش می پردازند؛ یا کارکنانی که در ساعات فراغت، باهم به صرف چای می پردازند. این پیوندهای میان آنها در مدیریت بسیار مهم اند؛ زیرا مدیران باید نسبت به سازمان غیر رسمی آگاه بوده و از فواید آن در اداره سازمان بهره جویند. بررسی اینکه چرا و چگونه گروه غیر رسمی پدید می آید، از موضوعات مطرح در روانشناسی اجتماعی است.

۲- Entrepreneurial (کارفرمایی)

۳- Modus Operandi

نمای این قلمرو از بزه‌کاری‌ها به سرعت در حال فراگیری کمک کند. در این کتاب، هم‌چنین، راه کارهای پژوهشی، مدیریتی و سیاسی مقابله با این بزه‌کاری‌ها را پیشنهاد می‌شود.

این کتاب در تمرکز، جهت‌یابی و چهارچوب، میان رشته‌ای است و حوزه‌های گوناگون اقتصاد، قانون، تجارت و مدیریت، امور بین‌المللی، جامعه‌شناسی، مردم‌شناسی، مطالعات فرهنگی و بزه‌شناسی را در بر دارد تا دیدگاه خواننده به این موضوع کامل شود و اطلاعاتی را فراهم کند که مطالعه نظری و عملی بزه‌کاری‌های سایبری را پوشش دهد. این کتاب، تئوری محور نیز می‌باشد، ولی عملی است و برای مخاطبان گوناگون دسترس‌پذیر است.

مخاطبان اصلی این کتاب، نخست، کارشناسان، متخصصان، حرفه‌ای‌ها و سیاست‌گذاران علاقه‌مند و نگران، میر صنعت بزه‌کاری‌های سایبری است. دانشجویان لیسانس و فوق لیسانس نیز مخاطبان این کتاب می‌باشند. انتظار است این کتاب بتواند برای تمامی علاقه‌مندان و فعالان دنیای سایبری در درک ماهیت آسیب‌پذیرهای سایبری و توسعه ساز و کارهای مناسب دفاعی در برابر حملات سودمند باشد.

به‌مناسبت ایده‌ها، مفاهیم، مضامین و نظریه‌هایی که در این کتاب آمده، اینجانب به خاطر اظهارات، پیشنهادات، پشتیبانی‌ها، ترغیب‌ها و نظرات افراد مختلف، مدیون و سپاس‌گزار هستم. از مطالب این کتاب در همایش‌های دانشگاهی، مقالات گوناگونی ارائه دهنده شده است، مانند: الف) چهارمین کنفرانس بین‌المللی سالانه مدیریت و سیاست عمومی، (CPP) ۱۲-۹ آگوست ۲۰۰۹، بنگلور هند، ب) هفتمین کنفرانس بین‌المللی هفتگی مشاغل، دانشگاه مینهو، براگا، پرتغال، ۲۶ آوریل تا یکم می ۲۰۰۹، در فیرفالدکس، ویرجینیا، ج) کتاب مدیریت اطلاعات ایمن، دالاس، تگزاس، ۴-۳ نوامبر ۲۰۰۸) سومین گردهمایی سالانه سیستم‌های اطلاعاتی مالی و امنیت سایبری، دانشکده اقتصاد روبرت اچ اسمیت در دانشگاه مری‌لند، ۱۱ می ۲۰۰۶، و ششمین گردهمایی سالانه تحقیقات تجاری بین‌المللی، فلدلفیا، ۲-۱ آوریل ۲۰۰۵. از آراء و پیشنهادات منتقدان بدون نام و شرکت‌کنندگان در این همایش‌ها برای بهبود غنای این کتاب بهره‌برده شده است.

بیش از هر کس دیگری مدیون مشاور پایان نامه دکترایم، نیخیلش دلاکیا هستم که به من انگیزه می داد، پشتیبانی می کرد و مشوق من بود. همچنین، از معاونت همکارانم، رالف بین راس، نیکلاس ویلیامسون و دیوید بارگوبین بسیار بهره برده‌ام. کاتارینا و تزل - وندایی، ویراستاران ارشد، علوم مدیریت / اقتصاد، اسپرینگو، سازنده، پشتیبان، کمک کننده و در هدایت و مدیریت این پروژه، ترغیب کننده بوده اند. هم چنین از دستیار لیسانسه خود جون (ژانی) ستیا نیز کمک زیادی دریافت داشته‌ام و مایلم تا سپاس ژرف خود را از همراه زندگی و بهترین رفیقم «مایا» بیان کنم، به خاطر شکریایی و پشتیبانی عاشقانه‌اش در راستای تألیف این کتاب. در آخر، دوست دارم این کتاب را به مادرم، ضامایا شتری، بخاطر عشق، راهنمایی و پشتیبانی‌هایش تقدیم کنم.

www.ketab.ir

پیش درآمد

نفوذ پرشتاب اینترنت و دیجیتال شدن فعالیت های اقتصادی زمینه ساز نسل جدیدی از بزه کاری ها شده است. بی آمدهای اقتصادی، سیاسی و اجتماعی این بزه کاری ها (سایبری) در سال های اخیر توجه زیادی را به خود جلب کرده است. از این رو، شهروندان، صاحبان مشاغل و دولت ها نگران امنیت سیستم ها، شبکه ها و زیربنای فناوری اطلاعات و ارتباطی (فناوری) می گردند.

با نگاهی به الگوهای بزه کاری های سایبری، مشخص می شود بسیاری از فرضیه های برجسته درباره آنها، ناقص، غیر واقعی و نامعقول است. گزارش های تجربی درباره الگوها و راهبردهای پیش گیری، باید با چنین بزه کاری هایی نیز با مؤلفه های جهان سایبری متناسب نیست. چرا که گستردگی سرقت های رایانه ای و بزه کاری های سایبری دچار دگرگونی های سیاسی، اجتماعی و راه انداختی شده است.

صنعت بزه کاری سایبری، حوزه نسبتاً جدیدی جویی انتظامی است. اگر چه باور عمومی بر این است که این صنعت بی اندازه بزرگ (گسترده) است، اما درباره ساختار و گستره واقعی آن دانش اندکی دارند. تحقیقات منتشر شده اندکی عوامل اقتصادی و سازمانی آن را بررسی کرده اند که بر راهبردها و رفتارهای عامین مختلف آن اثر داشته اند. نظریه پردازان نیز، به بهترین شیوه، در راستای درک کنش های بزه کاری سایبری و نفوذگرها (سارقین اطلاعات) و روابط هم زیستی که آنها با عاملین مختلف در دست به بحث می پردازند.

دیده های ما، ماهیت در حال شکل گیری صنعت جهانی بزه کاری های سایبری را برجسته می کند و گویای آن است که بزه کاری های سایبری از هر دو رویه نظری و علمی موضوع مهمی است. در این کتاب تلاش شده است تا آن شکاف های پژوهشی گفته شده برطرف شود و گفتارهای تخصصی بیشتری بیان شود. هدف اصلی این کتاب، بررسی روندهای اقتصادی مرتبط با این صنعت (بزه کاری های سایبری) است تا به درک بهتر این بزه کاری ها

به عنوان گونه‌ای از فعالیت‌های اقتصادی کمک کند و حامل توسعه راهبردهای پیش‌گیری از این بزه‌کاری‌ها است. **هدف دیگر** آن، کمک به درک فرایندهای سازمانی در صنعت بزه‌کاری‌های سایبری است. این امر با تحلیل سازمانهای رسمی و غیررسمی^۱ این صنعت پرداخته و ساز و کارهای باز خورد مرتبط را که بر این صنعت اثر دارند بیان می‌شود. **هدف سوم** این کتاب، پیشنهادهایی در راستای جنبه کارآفرینی^۲ شرکت‌های دارای فعالیت‌های سایبری است. این کتاب، به بررسی این نکته می‌پردازد که چگونه کارآفرینان در جهان، پیوسته به سازماندهی و مدیریت مؤلفه‌های ضروری این کسب و کارها می‌پردازند. ما هم-نیز، **الگوهای فعالیت بزه‌کاری‌های سایبری** نگاهی دقیق خواهیم انداخت. **هدف چهارم** این کتاب، شرح تنوع جهانی الگوهای بزه‌کاری‌های سایبری است. عوامل اقتصادی پیش روی بزه‌آوران سایبری و قربانیان آن‌ها در کشورهای پیشرفته و در حال توسعه بسیار متفاوت است. این عوامل، در برگیرنده ماهیت و کیفیت سخت‌افزارها، نرم‌افزارها، زیرساخت‌ها، اهداف (برای مثال، - ایگان، مهارت‌های بزه‌کاری‌های سایبری و

^۱ - سازمان رسمی، ساختاری برنامه‌ریزی‌شده از نقش‌ها است که به صورت رسمی سامان یافته است. به دیگر سخن، سازمان رسمی، سیستم یا شبکه‌ای از ارتباطات و اختیارات است که افراد و گروه‌هایی را به هم مرتبط می‌سازد که وظایف مهمی انجام می‌دهند. در ورای هر سازمان رسمی، معمولاً یک سازمان غیر رسمی (مجموعه‌ای از روابط کاری غیر رسمی در میان اعضای سازمان) وجود دارد، در حالی که سازمان رسمی تعیین می‌کند چه کسی به چه کسی گزارش می‌دهد؛ سازمان غیر رسمی برای استوار است که چه کسی عملاً با چه کسی تعامل دارد. سازمان‌های غیر رسمی، شبکه‌ای از روابط شخصی و اجتماعی هستند که با نقش مستقیم سازمان شکل نگرفته‌اند؛ بلکه به گونه‌ای خودجوش با همکاری و معاشرت و تعامل افراد پدید می‌آیند. سازمان‌های غیر رسمی ممکن است دربرگیرنده کارکنانی از یک سازمان باشند که مثلاً در تعطیلات باهم به تفریح و ورزش می‌پردازند؛ یا کارکنانی که در ساعتهای فراغت، باهم به صرف چای می‌پردازند. این پیوندهای میان آنها در مدیریت بسیار مهم‌اند؛ زیرا مدیران باید نسبت به سازمان غیر رسمی آگاه بوده و از فواید آن در اداره سازمان بهره‌جویند. بررسی اینکه چرا و چگونه گروه غیر رسمی پدید می‌آید، از موضوعات مطرح در روان‌شناسی اجتماعی است.

هزینه‌ها و منافع ناشی از آنها است. برکت دیگر این کتاب، درک تهدیدها و رویکردهای گوناگونی است که در این صنعت، توسط عاملین اصلی آن در پیش گرفته می‌شود. در مجموع، با فراهم کردن شرح مختصری از ترکیب‌ها، نهادها، جنبه‌های هزینه-فایده و روال کار^۲ عاملین گوناگون بزه‌کاری‌های سایبری، امید است که این کتاب به درک بهتر و تحلیل دور نمای این قلمرو از بزه‌کاری‌ها به سرعت در حال فراگیری کمک کند. در این کتاب، هم‌چنین، راه کارهای پژوهشی، مدیریتی و سیاسی مقابله با این بزه‌کاری‌ها را پیشنهاد می‌شود.

این کتاب در تمرکز، جهت یابی و چهارچوب، میان رشته‌ای است و حوزه‌های گوناگون اقتصاد، فناوری، تجارت و مدیریت، امور بین‌المللی، جامعه‌شناسی، مردم‌شناسی، مطالعات فرهنگی، بهره‌شناسی را در بر دارد تا دیدگاه خواننده به این موضوع کامل شود و اطلاعاتی را فراهم کند که بآلعه نظری و عملی بزه‌کاری‌های سایبری را پوشش دهد. این کتاب، تئوری محور نیز نباشد، ولی عملی است و برای مخاطبان گوناگون دسترس پذیر است.

مخاطبان اصلی این کتاب، نخست، کارشناسان، متخصصان، حرفه‌ای‌ها و سیاست‌گذاران علاقه‌مند و نگران سیر صنعت بزه‌کاری‌های سایبری هستند. دانشجویان لیسانس و فوق لیسانس نیز مخاطبان این کتاب می‌باشند. انتظار است این کتاب بتواند برای تمامی علاقه‌مندان و فعالان دنیای سایبری در درک ماهیت آسیب‌پذیری‌های سایبری و توسعه ساز و کارهای مناسب دفاعی در برابر حملات سودمند باشد.

به‌مناسبت ایده‌ها، مفاهیم، مضامین و نظریه‌هایی که در این کتاب آمده، اینجانب به خاطر اظهارات، پیشنهادات، پشتیبانی‌ها، ترغیب‌ها و نظرات افراد مختلف، مدیون و سپاس‌گزار هستم. از مطالب این کتاب در همایش‌های دانشگاهی مقالات گوناگونی ارائه دهنده شده است، مانند: الف) چهارمین کنفرانس بین‌المللی سالانه مدیریت و سیاست عمومی،

CPP) ۹-۱۲ آگوست ۲۰۰۹، بنگلور هند، ب) هفتمین کنفرانس بین المللی هفتگی مشاغل، دانشگاه مینهو، براگا، پرتغال، ۲۶ آوریل تا یکم می ۲۰۰۹، در فیرفالکس، ویرجینا، ج) کارگاه مدیریت اطلاعات ایمن، دالاس، تگزاس، ۴-۳ نوامبر ۲۰۰۸، د) سومین گردهمایی سالانه سیستم‌های اطلاعاتی مالی و امنیت سایبری، دانشکده اقتصاد روبرت اچ اسمیت در دانشگاه مری لند، ۲۴ می ۲۰۰۶، و ششمین گردهمایی سالانه تحقیقات تجاری بین المللی، فاندلفیا، ۱-۲ آوریل ۲۰۰۵. از آراء و پیشنهادات منتقدان بدون نام و شرکت کنندگان در این نمایش‌ها برای بهبود غنای این کتاب بهره برده شده است.

بیش از هر کسی دیگر من مشاور پایان نامه دکترایم، نیخیلش دلاکیا هستم که به من انگیزه می داد، پشتیبان من بود، و مشوق من بود. همچنین، از معاونت همکارانم، رالف بین راس، نیکلاس ویلیامسون و دیوید بارگرین بسیار بهره برده‌ام. کاتارینا و تزل -وندایی، ویراستاران ارشد، علوم مدیریت، دانشگاه پیرنیگو، سازنده، پشتیبان، کمک کننده و در هدایت و مدیریت این پروژه، ترغیب کننده بودند. همچنین از دستیار لیسانسه خود چون (ژانی) ستیا نیز کمک زیادی دریافت داشته‌ام. من می‌ایلم تا سپاس ژرف خود را از همراه زندگی و بهترین رفیقم «مایا» بیان کنم، به خاطر صبر و پشتیبانی عاشقانه‌اش در راستای تألیف این کتاب. در آخر، دوست دارم این کتاب را به ما، مایا، ضامایا شتری، بخاطر عشق، راهنمایی و پشتیبانی‌هایش تقدیم کنم.

فهرست مطالب

فصل اول - صنعت جهانی بزه کاری سایبری و ساختار آن

چکیده ۱

صنعت جهانی بزه کاری سایبری ۲

تعریف بزه کاری سایبری ۳

پی آمدهای بزه کاری سایبری ۷

چالش های روش شناختی، اخلاقی، امنیتی و آماری برآورد بزه کاری سایبری ۱۱

روندها در بزه کاری های سایبری ۱۴

گونه ها و دسته های بزه کاری سایبری ۱۶

بزه کاری سایبری تجاوزکارانه در برابر بزه کاری سایبری بازار محور ۲۱

عاملین بزه کاری سایبری ۲۱

قربانیان و اهداف بزه کاری سایبری ۲۴

ناظران و دولت ها ۲۶

سازمان های فراملی ۲۹

سازمان های داوطلب، غیرانتفاعی و غیردولتی ۳۱

سازمان های حقوقی و مدنی ۳۳

انگیزه های ارتکاب بزه کاری سایبری ۳۴

ناهمخوانی معیارهای فعالان مبارزه با بزه کاری سایبری ۳۷

سخن پایانی ۳۹

فصل ۲- اقتصاد ساده بزه کاری سایبری و چرخه پیگیری آن‌ها

چکیده ۴۱

پیش‌گفتار ۴۳

مؤلفه‌های اقتصادی مؤثر بر بزه کاری ۴۳

روندهای اقتصادی زمینه‌ساز رفتار بزه کاران سایبری ۴۵

ساختار بزه کاری سایبری: چرخه تبهارانه ۴۷

بازار بزه کاری سایبری ۴۸

سازمان‌های مجرمین ۴۹

بزه کاران سایبری ۵۱

قربانیان بزه کاری سایبری ۵۱

چالش‌های میان دستگاه‌های قضایی ۵۴

واکاوی سود - هزینه بزه کاران سایبری ۵۶

رؤیه سود بزه کاری سایبری ۵۷

رؤیه هزینه‌ای بزه کاری سایبری ۵۸

سخن پایانی ۶۲

فصل ۳- نگرش نهادی به بزه کاری سایبری

چکیده ۶۵

پیش‌گفتار ۶۶

نظری نهادی ۶۷

نهادهای نظارتی ۶۸

نهادهای هنجار بنیاد ۶۹

نهادهای شناختاری ۷۰

روابط مشترک میان ستون‌های سازمانی ۷۰

سازمان‌های درونی و بیرونی ۷۱

سازمان‌گرایی جدید ۷۱

سازمان‌هایی که در چند رده عمل می‌کنند ۷۳

نگرش سازمانی به بزه‌کاری سایبری ۷۴

محدودیت‌های رسمی و بزه‌کاری ۷۴

محدودیت‌های غیررسمی و بزه‌کاری ۷۴

مؤلفه‌های روبرو حملات سایبری ۷۶

مؤلفه‌های پیرامونی ۷۶

مؤلفه‌های میانی ۷۶

مؤلفه‌های صحنی، حرفه‌ای و میان سازمانی ۸۱

مؤلفه‌های شبکه‌ای ۸۱

مؤلفه‌های میان سازمانی ۸۴

سخن پایانی ۸۵

فصل ۴- فزاینده بزه‌کاری سایبری

چکیده ۸۷

پیش‌گفتار ۸۸

فرایندگی بزه‌کاری‌های سایبری و حلقه‌های بازخورد در آن ۸۸

بازخورد اقتصادی ۸۸

بازخورد اجتماعی سیاسی ۹۰

بازخورد شناختاری ۹۱

ساز و کارهای رواج بزه‌کاری سایبری ۹۲

وابستگی راه دستیابی و فزاینده بزه‌کاری‌های سایبری ۹۲

ناکارآمدی و فشردگی کاری در سازمان‌های انتظامی ۹۶

توسعه فن آوری و دانش فنی بزه کاری سایبری ۱۰۰

گرایش روزافزون به بزه کاری سایبری ۱۰۴

سخن پایانی ۱۰۷

فصل ۵- نه‌دها در قلمرو بزه کاری سایبری

چکیده ۱۰۹

پیش‌گفتار ۱۱۰

چهارچوب نظری: تئوری‌های نمادی ۱۱۳

ساز و کارهای تغییر قلمرو نه‌های ۱۱۷

تکان‌های بیرونی ۱۱۷

تغییرات در منطق‌های سازمانی ۱۱۸

تغییر آرام در ساختار قلمرو ۱۱۹

گسترش سازمانی ۱۲۰

ستون سازمانی مربوط به بزه کاری سایبری ۱۲۰

ستون‌های هنجاربنیاد و شناختاری مربوط به بزه کاری سایبری ۱۲۰

قلمروهای نهادی پدید آمده درباره بزه کاری سایبری ۱۲۱

شکل‌گیری ستون نظارتی درباره بزه کاری سایبری ۱۲۱

شکل‌گیری ستون هنجاربنیاد درباره بزه کاری سایبری ۱۲۷

شکل‌گیری ستون شناختاری درباره بزه کاری سایبری ۱۳۰

سخن پایانی ۱۳۲

فصل ۶- فاوا، حملات سایبری و عدم تقارن راهبردی

چکیده ۱۳۵

پیش گفتار ۱۳۶

عدم تقارن راهبردی و فاواها ۱۴۱

عاملین نهادی و سازمانی مربوط به عدم تقارن های منفی و مثبت ۱۴۶

نهادهای فاواها و امنیت ملی ۱۴۹

توانایی ایجاد عدم تقارن مثبت و کاهش آسیب پذیری ناشی از عدم تقارن منفی ۱۵۴

سخن پایانی ۱۵۷

فصل ۷- همگونی جهانی در الگوی بزه کاری سایبری

چکیده ۱۵۹

پیش گفتار ۱۶۰

تهدید جهانی امنیت دیجیتال: تحلیلی مختصر ۱۶۰

ویژگی های کشور چشمه ۱۶۴

نهادهای نظارتی: اقتدارترین ۱۶۴

نهادهای هنجاربنیاد: توانایی توجه اجتماع بزه کاری سایبری ۱۷۶

نهادهای شناختاری: ایدئولوژی ۱۷۶

ملی گرایی و وطن پرستی ۱۸۰

انباشت مهارت های بزه کاری سایبری در دسترسی به مرص های اقتصادی ۱۸۱

نیم رخ سازمان مورد هدف ۱۸۳

اهمیت و حساسیت نمادین ۱۸۳

دیجیتالی شدن ارزش ها و جذابیت هدف ۱۸۳

ناکارآمدی ساز و کارهای دفاعی ۱۸۵

سخن پایانی ۱۸۵

فصل ۸- بزه کاری سایبری در کشورهای در حال توسعه

چکیده ۱۹۱

پیش‌گفتار ۱۹۲

تحقیقات مختصری دربارهٔ بزه‌کاری سایبری در کشورهای در حال توسعه ۱۹۶

ارتباطات جهانی و افزایش بزه‌کاری سایبری ۱۹۷

مؤلفه‌های اقتصادی و حرفه‌ای مربوط به بزه‌کاری سایبری در کشورهای در حال توسعه

۱۹۸

نظرات رسمی: آسان‌گیری نیروهای نظارتی ۱۹۸

منابع مورد علاقه بزه‌کاری سایبری ۲۰۱

اقدامات به نفع بزه‌کاران سایبری ۲۰۲

نهادهای غیررسمی: مسئولیت اجتماعی و بزه‌کاری سایبری ۲۰۱

ساز و کارهای دفاعی در بزه‌کاری سایبری ۲۰۳

الگوی سلسله‌مراتبی بین‌المللی برای تولیدات امنیتی ۲۰۶

تراکم بزه‌کاری ۲۰۶

برون‌گرایی و وابستگی مسیر ایجاد شده توسط بزه‌کاری سایبری و بزه‌کاری‌های سایبری

۲۰۸

الگوهای ارتکاب بزه‌کاری سایبری در کشورهای در حال توسعه ۲۰۹

انگیزه‌های پشت بزه‌کاری سایبری ۲۱۱

سخن پایانی ۲۱۳

فصل ۹- مبانی نهادی و اقتصادی الگوهای ارتکاب بزه‌کاری سایبری

چکیده ۲۱۹

کارآفرینی بزه‌کارانه و الگوهای فعالیت در دنیای دیجیتال ۲۲۰

کاربرد مؤلفه‌های الگوی کسب و کاری در صنعت بزه‌کاری سایبری ۲۲۲

ترکیب‌بندی توانایی‌ها ۲۲۳

ترکیب‌بندی توانایی‌های اینترنت و بزه‌کاران سایبری ۲۲۳

مرزهای شرکت ۲۲۶

اتلاف‌ها: استراتژی شبکه‌های بزه‌کاری سایبری ۲۲۸

عاملین و اعمال قانونی و غیرقانونی مشمول در بزه‌کاری سایبری ۲۲۸

بزه‌کاری سایبری بازار محور و منافع مشتری ۲۲۹

بزه‌کاری سایبری تجاوزکارانه ۲۳۰

عاملین بزه‌کاری سایبری و مشاغل مشروع ۲۳۱

ترکیب عاملین بزه‌کاری بازار محور در برابر عاملین تجاوزکارانه ۲۳۲

عدم فعالیت آنلاین، اطلاعات فن‌آورانه و اطلاعات بازار ۲۳۲

مسئله عدم دایمیت کیفی در بازار الکترونیکی ۲۳۳

اطلاعات فن‌آورانه و اطلاعات بازار در تجارت الکترونیکی ۲۳۴

توسعه ظرفیت‌های پویا ۲۳۵

سخن پایانی ۲۳۷

فصل ۱۰- صنعت جهانی کلاهبرداری کلان

چکیده ۲۴۰

پیش‌گفتار ۲۴۰

کلیک‌ها و ایجاد ارزش در اقتصاد اینترنتی ۲۴۱

تحقیقی درباره کلاهبرداری کلکی ۲۴۳

محاسبات سود- هزینه ذی‌نفعان کلاهبرداران کلکی ۲۴۶

مجرمان ۲۴۶

فرا واسطه‌گری و کلاهبرداری کلکی ۲۴۸

جغرافیای اقتصادی: مکان‌های ارتکاب به کلاهبرداری کلکی ۲۵۰

اقتصاد کار در برابر اقتصاد فن‌آورانه و گستره فن‌آوری ۲۵۱

منافع اقتصادی و روانی / ائتلاف بودجه آگهی رقبا ۲۵۲

نهادها ۲۵۳

نهادهای رسمی نظارتی و کلاهبرداری کلیک ۲۵۵

نهادهای غیر رسمی و کلاهبرداری کلیک ۲۵۶

قربانیان ۲۵۷

نیم‌رخی از قربانیان و اهداف کلاهبرداری کلیک ۲۵۷

آینده‌ای که چندان حفاظت نمی‌شوند و ناتوانی ساز و کارهای دفاعی ۲۵۸

سخن پایانی ۲۵۹

فصل ۱۱- نکته‌های پایداری

پیش‌گفتار ۲۶۱

به کجا باید برسیم ۲۶۲

نکته‌هایی برای کسب و کارها ۲۶۳

نکاتی برای مصرف‌کنندگان ۲۷۰

نکاتی برای سیاستگذاران ۲۷۴

پیشنهادهایی برای تحقیقات آینده ۲۸۰

سخن پایانی ۲۸۶

جداول

جدول ۱-۳ سطوح مختلف مؤلفه‌های اثرگذار بر حملات سایبری ۷۷

جدول ۱-۴ واقعیات مشهود و بازخوردهای افزایشده رواج بزه‌کاری سایبری ۹۶

جدول ۲-۴ ویژگی‌های بزه‌کاری سایبری اثرگذار بر نرخ اشاعه آن‌ها ۱۰۱

جدول ۱-۵ رویدادهای مهم درباره ایجاد نهادهای قانونی برای بزه‌کاری سایبری ۱۱۱

جدول ۱-۶ اصطلاحات تخصصی به کار رفته در این فصل ۱۳۷