

جرائم سایبری و پزشکی قانونی دیجیتال

اثری از:

Thomas J. Holt, Adam M. Bossler, and
Kathryn C. Seigfried-Spellar

مترجمین:

دکتر محمد سعید شفیعی	استاد دانشگاه آزاد اسلامی مرکز اصفهان (خوراسگان)
----------------------	--

دکتر مهنوش ابوذری	استادیار دانشکده حقوق دانشگاه تهران
-------------------	-------------------------------------

فرسیما خامسی پور	مدرس دانشگاه و عضو باشگاه پژوهشگران جوان و نخبگان دانشگاه آزاد اسلامی واحد اصفهان (خوراسگان)
------------------	---

سرشناسه	Thomas J. Holt, Adam M. Bossler, and Kathryn C. Seigfried-Spellar
عنوان و نام پدیدآور	جرایم سایبری و پزشکی قانونی دیجیتال / اثری از امون کرین... (و دیگران): مترجمین: محمدسعید شفیعی و دیگران...
مشخصات نشر	تهران، کتاب آوا، ۱۳۹۷
مشخصات ظاهری	۴۵۶ ص
شابک	۹۷۸-۶۰۰-۳۴۶-۴۹۵-۷
وضعیت فهرست نویسی	فیبا
یادداشت	Cybercrime and Digital Forensics
یادداشت	مهرنوش ابوذری ۱۳۶۷، فرسیما خامسی پور ۱۳۷۱
شناسه افزوده	کارین، ایمون
شناسه افزود	شفیعی، محمدسعید، ۱۳۴۸، مترجم
رده‌بند - سنگ	۱۳۹۷۶۷۳۳HV / ۵۹۴
رده‌بندی دیوپی	۲۵۹۶۸/۳۶۳
شماره کتابشناسی	۵۵۵۸۰

جایزه سایبری و پزشکی قانونی دیجیتال



انتشارات کتاب آوا

مؤلفین:	Thomas J. Holt, Adam M. Bossler, and Kathryn C. Seigfried-Spellar
مترجمین:	محمدسعید شفیعی - مهرنوش ابوذری - فرسیما خامسی پور
ناشر:	کتاب آوا
نوبت چاپ:	اول - زمستان ۱۳۹۷
شمارگان:	۱۰۰۰
قیمت:	۵۵,۰۰۰ تومان
شابک:	۹۷۸-۶۰۰-۳۴۶-۴۹۵-۷

نشانی مراکز پخش: تهران، خیابان انقلاب، خیابان ۱۲ فروردین، بن بست حقیت، پلاک ۴، واحد ۴
شماره های تماس: ۶۶۹۷۴۱۳۰ - ۶۶۴۰۷۹۹۳ - ۶۶۹۷۴۴۴۵ - ۶۶۹۷۴۴۴۵ - ۶۶۹۷۴۴۴۵ - ۶۶۹۷۴۴۴۵

www.avabook.com Email: avabook_kazemi@yahoo.com

نشانی فروشگاه: اسلامشهر، خیابان صیاد شیرازی (خیابان دانشگاه)، داخل کوچه فرمانداری
شماره تماس: ۵۶۳۵۴۶۵۱

هرگونه تکثیر این اثر از طریق ارسال یا بارگذاری فایل الکترونیکی، یا چاپ و نشر کاغذی آن بدون مجوز ناشر، به هر شکل، اعم از فایل، سی‌دی، افست، ریسوگراف فتوکپی، زیراکس یا وسایل مشابه، به صورت متن کامل یا صفحاتی از آن، تحت هر نام اعم از کتاب، راهنما، جزوه، یا وسیله کمک آموزشی، در فضای واقعی یا مجازی، و همچنین توزیع، فروش، عرضه یا ارسال اثری که بدون مجوز ناشر تولید شده، موجب پیگرد قانونی است.

فهرست مطالب

۱۳	 مقدمه:
۱۹	 فصل اول: ته‌لوزی و جرایم ساییری
۲۰	 مقدمه
۲۳	 ۱-۱ تکنولوژی بعنوان فضای برای جرم
۲۳	 ۲-۱ تکنولوژی بعنوان میانجی ارتباطی
۲۵	 ۳-۱ تکنولوژی بعنوان هدف یا انزای برای مشارکت در جرم
۲۷	 ۴-۱ تعریف سواستفاده و اسنده نامرست از کامپیوتر
۲۹	 ۱-۴-۱ چه چیزی جرم ساییری 'انحراف' را جذابتر می‌کند؟
۳۴	 ۵-۱ تکنولوژی بعنوان یک اثبات
۳۵	 ۶-۱ پاسخ اجرای قانون به جرایم ساییری
۴۰	 ۷-۱ نمادشناسی جرایم ساییری
۴۰	 ۱-۷-۱ تجاوز ساییری
۴۱	 ۲-۷-۱ دزدی/فریبکاری ساییری
۴۲	 ۳-۷-۱ هرزگی/پورن ساییری
۴۳	 ۴-۷-۱ خشونت ساییری
۴۷	 فصل دوم: هک‌های کامپیوتری و هک کردن
۴۸	 مقدمه
۴۹	 ۱-۲ تعریف هک کردن کامپیوترها
۵۲	 ۲-۲ قربانیان هک
۵۵	 ۳-۲ جنبه‌های انسانی فرهنگ هکری

۵۶	۴-۲ فرهنگ مدرن هکرها
۶۱	۲-۴-۲ دانش
۶۵	۳-۴-۲ راز داری
۶۶	۵-۲ هکرها، ماهر و هک کردن کامپیوترها
۶۷	۶-۲ چارچوب‌های قانونی برای رسیدگی به هک‌های غیرقانونی
۷۴	۷-۲ اعمال و تحقیق در خصوص فعالیت‌های هکری
۷۹	خلاصه

۸۱	فصل دوم: حمله و حملات اتوماتیک کامپیوتری
۸۲	مقدمه
۸۳	۱-۳ اصول اولیه بدافزارها
۸۵	۲-۳ ویروس‌ها، تروجان‌ها، کرم‌ها
۸۶	۱-۲-۳ ویروس‌ها
۹۳	۳-۲-۳ کرم‌ها
۹۵	۳-۳ تهدیدهای تلفیقی و ابزارهای کمک
۹۹	۴-۳ تاثیر جهانی بدافزارها
۱۰۵	۵-۳ هکرها و نویسندگان بدافزار
۱۰۷	۱-۵-۳ دیدار با هکر بانک سوئدی
۱۰۷	۶-۳ بازار نرم افزارهای مخرب
۱۱۳	۸-۳ چالش‌های قانونی در برخورد با بدافزارها
۱۱۷	۹-۳ هماهنگی و مدیریت در پرداختن به بدافزارها
۱۲۱	خلاصه

۱۲۳	فصل چهارم: دزدی دیجیتال آثار ادبی و هنری و سرقت اموال ناشی از مالکیت فکری
۱۲۴	مقدمه
۱۲۶	۱-۴ اموال ناشی از مالکیت فکری چیست؟
۱۲۸	۲-۴ تحولات دزدی آثار ادبی و هنری در طول زمان
۱۲۹	۳-۴ تغییر روش‌های دزدان

۱۳۲	۴-۴ خرده فرهنگ سرقت آثار ادبی و هنری
۱۳۴	۵-۴ تحول قانونگذاری برای مقابله با دزدی آثار ادبی و هنری
۱۳۹	۶-۴ اجرای قانون و پاسخ سازندگان آثار ادبی و هنری
۱۴۲	خلاصه

فصل پنجم: جرایم اقتصادی و کلاهبرداری اینترنتی ۱۴۵

۱۴۶	مقدمه
۱۴۸	۱-۵ کلاهبرداری و ارتباطات با استفاده از کامپیوتر
۱۴۹	۲-۵ سرقت ویب
۱۵۲	۳-۵ کلاهبرداری‌های مبتنی بر ایمیل
۱۵۲	۱-۳-۵ طرح‌های ایمیل خرابی
۱۵۴	۲-۳-۵ فیشینگ این‌ها
۱۵۵	۳-۳-۵ طرح‌های کار در خانه
۱۵۶	۴-۳-۵ طرح‌های افت و خیز بورس
۱۵۸	۵-۳-۵ سایت‌های تجارت آنلاین
۱۶۲	۶-۳-۵ مسئله استفاده از کارت (کاردینک) و تراشه‌های سرقتی
۱۶۴	۷-۳-۵ فرایندهای بازار کارتینگ: عوامل و ارتباطات
۱۶۸	۸-۳-۵ نیروهای اجتماعی در درون بازارهای کاردینک
۱۶۹	۴-۵ سرقت هویت و قوانین مربوط به کلاهبرداری
۱۷۴	۵-۵ قوانین جهانی در مورد کلاهبرداری
۱۷۹	خلاصه

فصل ششم: پورنوگرافی روسپی‌گری و جرایم جنسی ۱۸۱

۱۸۲	مقدمه
۱۸۴	۱-۶ طیف جنسیت آنلاین
۱۸۷	۲-۶ پورنوگرافی در عصر دیجیتال
۱۹۰	۳-۶ شناسایی پورنوگرافی و بهره‌وری از کودکان
۱۹۲	۴-۶ تحقیقات زیرفرهنگی پدوفیلی آنلاین

۱۹۵	۵-۶ روسپیگری و کار جنسی
۱۹۶	۶-۶ مشتریهای کارگران جنسی
۱۹۸	۷-۶ مقابله با محتوای شنیع و پورنوگرافی اینترنتی
۱۹۸	۶-۷ ۱- قوانین موجود
۲۰۶	۶-۷ ۲- قوانین خود تنظیمی توسط صنعت پورنوگرافی
۲۰۷	۶-۷ ۳- اقدامات سازمانهای غیرانتفاعی
۲۰۹	۶-۸ مبارزه با جرایم جنسی به صورت آنلاین و آفلاین
۲۱۳	خلاصه

۲۱۵	فصل هفتم: ارباب، آزار و اذیت آنلاین و مزاحمت سایبری
۲۱۶	۷-۱ تهدیدات ارباب و آزار و اذیت آنلاین
۲۱۸	۷-۲ تعریف ارباب، آزار و اذیت
۲۲۱	۷-۳ رواج ارباب سایبری
۲۲۳	۷-۴ پیشبینی ارباب در فضای آنلاین و آفلاین
۲۲۶	۷-۵ چالش آزار و اذیت و مزاحمت آنلاین
۲۲۷	۷-۶ میزان آزار و اذیت و مزاحمت
۲۳۰	۷-۷ درک تجربیات قربانیان خشونتهای اینترنتی
۲۳۲	۷-۸ گزارش ارباب، آزار و اذیت و مزاحمت آنلاین
۲۳۵	۷-۹ مقررات ارباب، آزار و اذیت و مزاحمت آنلاین
۲۳۷	۷-۱۰ آزار و اذیت (تعرض) و مزاحمت
۲۴۰	۷-۱۱ اجرای قوانین و هنجارهای خشونت سایبری
۲۴۴	نتیجه گیری

۲۴۷	فصل هشتم: افراط گرایی آنلاین، ترور سایبری و جنگ سایبری
۲۴۸	مقدمه
۲۵۰	۸-۱ تعریف ترور، هکتیویسم و ترور سایبری
۲۵۵	۸-۲ نقش حملات دولت ملی در مقابل حملات غیر دولت ملی
۲۵۹	۸-۳ استفاده از اینترنت در تلقین فکری و نیروگیری گروههای افراطی

۲۶۴	۴-۸ حملات الکترونیکی توسط گروههای افراطی
۲۶۷	۱-۴-۸ قدرت سفید آنلاین
۲۷۰	۲-۴-۸ القاعده و جهاد الکترونیکی
۲۷۲	۳-۴-۸ جنگ سایبری و دولت ملی
۲۷۶	۵-۸ وضع قوانین افراطگرایی و ترور سایبری
۲۷۹	۶-۸ تحقیق و تأمین امنیت فضای سایبری در برابر تهدید ترور و جنگ
۲۸۱	۱-۶-۸ اداره تحقیقات فدرال
۲۸۲	۲-۶-۸ وزارت انرژی
۲۸۳	۶-۸ وزارت امنیت داخلی
۲۸۴	۷-۸ جنگ سایبری و امنیت ملی
۲۸۶	خلاصه
۲۸۷	فصل نهم: جرایم اینترنتی نظریه‌ها، جرم‌شناسی
۲۸۸	مقدمه
۲۹۰	۱-۹ نظریه‌های زیر فرهنگی
۲۹۰	۱-۱-۹ بررسی اجمالی
۲۹۱	۲-۱-۹ زیرفرهنگ‌ها و جرایم اینترنتی
۲۹۲	۲-۹ نظریه یادگیری اجتماعی و جرایم اینترنتی
۲۹۲	۱-۲-۹ نگاه اجمالی
۲۹۳	۳-۹ نظریه یادگیری اجتماعی و جرایم اینترنتی
۲۹۷	۴-۹ نظریه عمومی جرم
۲۹۷	۱-۴-۹ بررسی اجمالی
۲۹۸	۵-۹ نظریه عمومی جرم و جرایم اینترنتی
۳۰۱	۶-۹ نظریه عمومی کرنش آگنیو
۳۰۱	۱-۶-۹ نگاه اجمالی
۳۰۲	۷-۹ نظریه عمومی فشار و جرایم اینترنتی
۳۰۴	۸-۹ تکنیک‌های خنثی سازی

۳۰۴	۱-۸-۹ نگاه اجمالی
۳۰۵	۲-۸-۹ تکنیک‌های خنثی سازی و جرایم اینترنتی
۳۰۷	۹-۹ نظریه بازدارندگی
۳۰۷	۱-۹-۹ نگاه اجمالی
۳۰۸	۲-۹-۹ بازدارندگی و جرایم اینترنتی
۳۱۰	۱۰-۹ نظریه‌های قربانی سازی جرایم اینترنتی
۳۱۱	۱۱-۹ نظریه فعالیت روز مره
۳۱۲	۱۲-۹ تئریه فعالیت روزمره و قربانی سازی جرایم اینترنتی
۳۱۶	۱۳-۹ تئریه عمومی جرم و قربانی سازی
۳۱۶	۱۴-۹ عدم خ - کنترل و قربانی سازی جرایم اینترنتی
۳۱۹	۱۵-۹ آیا نیاز بسیاری نظریه‌های جدید فضای مجازی داریم؟
۳۲۰	خلاصه

فصل دهم: سیر تکاملی پزشکی قانونی دیجیتال ۳۲۳

۳۲۴	مقدمه
۳۲۶	از پزشکی قانونی کامپیوتر تا پزشکی قانونی دیجیتال
۳۳۷	۱-۱۰ نقش مدارک دیجیتال
۳۴۰	۲-۱۰ انواع سخت افزار، لوازم جانبی و شواهد الکترونیکی
۳۴۵	۳-۱۰ یکپارچگی و تمامیت مدارک
۳۴۵	خلاصه

فصل یازدهم: حصول و بررسی شواهد جرمیابی ۳۴۷

۳۴۸	مقدمه
۳۴۹	۱-۱۱ حفاظت از داده‌ها
۳۵۰	۲-۱۱ تصویربرداری
۳۵۲	۳-۱۱ تأیید
۳۵۵	۴-۱۱ ابزارهای تصویربرداری جرمیابی دیجیتال
۳۵۷	۵-۱۱ EnCase®

۳۵۹	Forensic Toolkit® (FTK®) ۶-۱۱
۳۶۳	۷-۱۱ آشکارسازی شواهد دیجیتال
۳۶۵	۸-۱۱ استنتاج فیزیکی
۳۶۹	۹-۱۱ استنتاج منطقی
۳۷۵	۱۰-۱۱ تحلیل داده‌ها
۳۷۵	۱۱-۱۱ کاهش داده‌ها و فیلترینگ
۳۷۷	۱۲-۱۱ گزارش دهی یافته‌ها
۳۷۸	خلاصه

فصل دوازدهم: چالش‌های قانونی در تحقیقات قانونی دیجیتال

۳۸۲	مقدمه
۳۸۴	۱-۱۲ مسائل قانونی تحقیقات دیجیتالی
۳۸۴	۲-۱۲ اصلاحیه چهارم
۳۸۵	۳-۱۲ حریم خصوصی
۳۸۸	۴-۱۲ تفتیش و توقیف
۳۹۳	۵-۱۲ استثنائات برای قانون
۴۰۱	۶-۱۲ اصلاحیه پنجم
۴۰۳	۷-۱۲ محافظت در برابر خود مقصر شماری
۴۰۶	۸-۱۲ قانون افشای کلید
۴۰۷	۹-۱۲ محکمه پسندی مدرک در دادگاه
۴۱۳	۱۰-۱۲ استاندارد فرای
۴۱۴	۱۱-۱۲ قوانین اسناد فدرال ۷۰۲
۴۱۵	۱۲-۱۲ استاندارد داوبرت
۴۱۷	۱۳-۱۲ واکنش بین المللی به فرای و داوبرت
۴۱۸	۱۴-۱۲ قابل قبول بودن جرم یابی قانونی دیجیتالی به عنوان شهادت متخصص
۴۲۱	خلاصه

فصل سیزدهم: آینده جرائم اینترنتی، ترور و سیاست

۴۲۴	مقدمه.....
۴۲۵	۱-۱۳ بررسی آینده جرائم اینترنتی.....
۴۲۷	۲-۱۳ با پیدایش تکنولوژی‌های جدید، تکنیک ویز چگونه تغییر می‌کنند؟.....
۴۲۸	۳-۱۳ جنبش‌های اجتماعی، تکنولوژی و تغییرات اجتماعی.....
۴۳۱	۴-۱۳ نیاز برای نظریات جرم‌شناسی جدید حوزه سایبر؟.....
۴۳۳	۵-۱۳ تغییر راهبردهای اجرای قانون در عصر اینترنت.....
۴۳۵	۶-۱۳ بررسی آینده فارنزیک (جرم‌شناسی).....
۴۳۶	۷-۱۳ چالش‌های سیاست‌گذاران در سطح جهانی.....
۴۴۰	خلاصه.....
۴۴۱	منابع.....

مقدمه:

امروزه فناوری اطلاعات صرف نظر از موقعیت جغرافیایی، در تمامی شئون زندگی وارد شده است و هریک از افراد، بسته به نیاز خود از مزایای این علم بهره مند می شوند. گرچه فضای سایبر همانند دیگر عناصر زندگی اجتماعی، از گزند یک پدیده بسیار انعطاف پذیر و لاینفک از اجتماع به نام جرم در امان نماند. است. دنیای ارتباطات و فضای سایبر، فرصتهای جدید و بسیار پیشرفته ای را برای قانون شکنی در اختیار کاربران خود قرار داده که امکان رفتارهای ضد اجتماعی و مجرمانه مهیا شده است.

به طور کلی، آنچه امروزه تحت عنوان جرم سایبر قرار می گیرد، دو طیف از جرائم است: گروه اول جرائمی هستند که نظایر آنها در حیات فیزیکی نیز وجود دارد و فضای سایبر بدون تغییر ارکان مجرمانه شان، با امکاناتی که در اختیار مجرمین قرار می دهد، ارتکابشان را تسهیل می کند. جرائم تحت شمول این حوزه بسیار گسترده اند و از جرائم علیه امنیت ملی و حتی بین المللی نظیر اقدامات تروریستی گرفته تا جرائم علیه اموال و اشخاص را در برمی گیرند. اما طیف دیگر جرائم سایبر، به سوء استفاده های منحصر از این فضا مربوط می شود که امکان ارتکاب آنها در فضای فیزیکی میسر نیست. جرائمی نظیر دسترسی غیرمجاز به داده ها یا سیستمها یا پخش برنامه های مخرب نظیر ویروسها، جز در فضای سایبر قابلیت ارتکاب ندارند و به همین دلیل به آنها جرائم سایبری محض نیز گفته می شود.

جرائم رایانه ای - سایبری را در قالب سه نسل مورد بررسی قرار می دهند که قابل توجه می باشد: نسل اول جرائم رایانه ای: همانگونه که از عنوان پیداست، این نسل به ابتدای ظهور سیستمهای رایانه ای، به ویژه زمانی که برای اولین بار در سطح گسترده ای در دسترس عموم قرار گرفتند، مربوط می شود. در آن زمان، عمده اقدامات غیرمجاز، به ایجاد اختلال در کارکرد این سیستمها و به تبع آن دستکاری داده ها مربوط می شد.



نسل دوم جرائم رایانه‌ای: این نسل از جرائم پل ارتباطی میان نسل اول و سوم بوده و دلیل بارز آن هم عمر بسیار کوتاه این نسل است که به سرعت با ظهور نسل سوم منتفی شد. این رویکرد که از اواخر نسل اول زمزمه‌های آن شنیده می‌شد، به دلیل محوریت یافتن داده‌ها اتخاذ گردید. دلیل آن هم این بود که در دوران نسل اول، سیستمهای رایانه‌ای به تازگی پا به عرصه گذاشته بودند و عمدتاً به شکل سیستمهای شخصی یا رومیزی بوده و به همین دلیل به تنهایی مورد توجه قرار گرفته بودند. اما به تدریج با توسعه و ارتقای فناوری رایانه و به کارگیری آن در بسیاری از ابزارها و به عبارت بهتر رایانه‌ای شدن امور، به تدریج ابزارهای رایانه‌ای جایگاه خود را از دست دادند و محتوای آنها یعنی داده‌ها محوریت یافت. بدیهی است در این مقطع مباحث حقوقی و به تبع آن رویکردهای مقابل جرائم رایانه‌ای نیز تغییر یافت، به نحوی که تدابیر پیشگیرانه از جرائم رایانه‌ای با محوریت داده‌ها و نه واسطه‌ها تنظیم شدند حتی این رویکرد در قوانینی که در آن زمان به تصویب می‌رسید نیز قابل مشاهده است.

به این ترتیب، سیستمهای رایانه‌ای در صورتی در دوران نسل دوم، ایمن محسوب می‌شدند که داده‌های موجود در آنها از سه بُعد، ذخیره‌دار بودند: ۱. محرمانگی: داده‌ها در برابر افشا یا دسترسی غیرمجاز حفاظت شده باشند؛ ۲. تمامیت: داده‌ها در برابر هرگونه تغییر یا آسیب حفاظت شده باشند؛ و ۳. دسترس‌پذیری: با حفظ کارکرد مطلوب سیستم، داده‌ها همواره در دسترس مجاز قرار داشته باشند.

هم اکنون، این سه مولفه در حوزه ی جرائم نسل سوم از جایگاه ویژه‌ای برخوردارند و حتی در اسناد قانونی به صراحت به آنها اشاره شده است.

برای مثال، عنوان اول از بخش اول فصل دوم کنوانسیون جرائم سایبر (بوتل است، ۲۰۰۱)، به جرائم علیه محرمانگی، تمامیت و دسترس‌پذیری داده‌ها و سیستمهای رایانه‌ای اختصاص دارد. در ذیل این عنوان، پنج ماده به طور مفصل جرائم این حوزه را برمی‌شمرند که عبارتند از: دسترسی غیرقانونی، شنود غیرقانونی، ایجاد اختلال در سیستم و سوء استفاده از دستگاهها.

این دوره با وجود عمر کوتاه خود، تاثیر بسزایی در تحول نگرش به جرائم رایانه‌ای داشت. حتی می‌توان گفت، تقریباً از این زمان بود که اصطلاحاتی نظیر جامعه ی اطلاعاتی یا حقوق کیفری اطلاعات به طور رسمی در اسناد قانونی وارد شد.

نسل سوم جرائم رایانه‌ای: از اوایل دهه نود، با جدی شدن حضور شبکه‌های اطلاع‌رسانی رایانه‌ای در عرصه بین‌الملل و به ویژه ظهور شبکه جهانی وب که به فعالیت این شبکه‌ها ماهیتی تجاری بخشید، بحث راجع به ابعاد گوناگون فضای سایبر به ویژه مسائل حقوقی آن، وارد مرحله جدیدی شد. زیرا تا آن زمان شبکه‌های رایانه‌ای در ابعاد منطقه‌ای، محلی و در حوزه‌های محدودی نظیر سیستم‌های تابلوی اعلانات که عمدتاً جهت بارگذاری و پیاده‌سازی برنامه‌ها، پیام‌ها و همچنین ارتباطات پست الکترونیک به کار می‌رفتند به فعالیت می‌پرداختند.

بنابراین می‌توان گفت فضای سایبر، فرصت‌های تازه و بسیار پیشرفته‌ای را برای قانون شکنی در اختیار انسان می‌آورد، همچنین توان بالقوه ارتکاب گونه‌های مرسوم و کلاسیک جرایم را به شیوه‌های غیر مرسوم و بسیار جدید سوق می‌دهد تا مجرمان سایبری بتوانند در این کهنکشان صفر و یک، هرآنچه می‌خواهند در اختیار داشته باشند، به منصفه ظهور برسانند. این امر، علوم مختلف و از جمله جرم‌شناسی را با تحول روبه‌رو ساخته است. لذا با گسترش فرصت‌های فعلیت‌بخش مجرمانه در فضای سایبر و نگرانی مردم از این جرایم، توجه اختصاصی حقوقدانان و جرم‌شناسان به جرایم ارتکابی در فضای مجازی جلب شد و منجر به ایجاد حوزه مطالعاتی جرم‌شناسی سایبری گردید.

گرچه عده‌ای معتقدند حوزه سایبری وسیله‌ای برای ارتکاب جرایم سنتی (جرایم ارتكابی در فضای واقعی) هستند و لذا آورده جدیدی نیستند که برایشان قابل به قانون جدید و مباحث نظری جدید باشیم اما عقیده غالب که با گذشت زمان و توسعه جرایم سایبری از حیث کمی و کیفی و تنوع انواع و اشکال، بر آن صحه گذاشته شده، قائل است اینترنت فضای جدیدی با ماهیتی کاملاً متفاوت از فضای واقعی (جرایمی مانند هک کردن) خلق کرده است.

از این رو جرایم سایبری به علت مزایایی که مجرمان در آن می‌بینند، رو به گسترش است. ویژگی‌های مطلوب و مزایای حضور مجرمانه در فضای سایبر این است که از یک سو ارتکاب آنها آسان بوده و با کمترین ریسک از جهت احتمال دستگیری یا عدم موفقیت و شناسایی، به نتیجه مطلوب خود می‌رسند که با هویت و مکان ناشناس و چه بسا غیرقابل شناسایی، در دنیایی شناور و سیال به فعالیت مجرمانه و حیات خود ادامه می‌دهند که در اغلب موارد بزه‌دیده بر بزه‌دیدگی خود مطلع نمی‌شود یا بسیار دیر بر آن آگاهی می‌یابد و حتی در اغلب موارد غیرقانونی بودن آنها روشن نمی‌باشد. یک ویژگی خاص جرایم سایبری این است که وقوع می‌یابند بدون آنکه صحنه جرم داشته



باشند. به علاوه، مجرمان به دلیل عدم رویت فوری آثار و نتایج رفتار مجرمانه شان، راحت تر مرتکب جرم می شوند. این امر باعث سهولت از بین بردن آثار جرم می گردد. سرعت بالای ارتکاب جرم و قابلیت تکرار فراوان نیز از ویژگی های دیگر این جرایم می باشد. جرایم سایبری غالبا بسیار سریع به وقوع می پیوندند و از شروع جرم تا اجرای آن فاصله ای وجود ندارد. گاهی فاصله، تنها به اندازه فشردن یک کلید است. از سوی دیگر، جرایم سایبری معمولا ماهیت سریالی دارند و با یک بار ارتکاب، مجرم به اعمالش خاتمه نمی دهد. هم چنین این امر به ویژگی خاص این فضا نیز برمی گردد که داده ها در این فضا به سادگی گسترش یافته و به طور خودکار تکرار می گردند و محو آن به سادگی ممکن نیست. تعطیل ناپذیر بودن و امکان وقوع جرم در هر زمان شبانه روز و هر روز هفته، و رکنی دیگر این جرایم است که زمینه گستردگی وقوع آن و افزایش رغبت افراد در ارتکاب این جرایم را فراهم می آورد.

لذا نکته قابل توجه نگاه در ال وقوع جرایم سایبری و ضرورت توجه چندجانبه به این جرایم است. از همین رو، برنامه های که منظور پیشگیری از جرایم سایبری ارائه می شوند باید به این امر توجه داشته باشند. نکته دیگر، قابلیت اءال برخی نظریات جرم شناسانه مربوط به جرایم فضای سنتی بر جرایم این فضای نوین و جستجوی نظریات جدید در تبیین جرایم سایبری است. شکل گیری جرم شناسی سایبری یک تبیین میان رشته ای از جنبه های عملی و مباحث نظری در باب جرایم سایبری را با شناخت علوم رایانه ای فراهم می کند. به دلیل رشد روزافزون اینترنت و علوم کامپیوتری فناوری اطلاعات، باعث شده جرم شناسی سایبری به تدریج از یک مطالعه حاشیه ای به یک شاخه اصلی و با اهمیت در جرم شناسی تبدیل شود.

بحث جرم شناسی سایبری در سال ۲۰۰۷ توسط جایشانکار مطرح شد. در سال ۲۰۰۸ ایشان نظریه ای را در تبیین منسجم جرم شناسی سایبری به نام «نظریه جابجایی مکانی» مطرح کرد و در این نظریه جرایم در فضای سایبری را توضیح داد. جرم شناسی سایبری مطالعه عوامل ایجاد جرم در فضای مجازی و تاثیرات آن بر دنیای حقیقی و راهکارهای پیشگیری از حدوث اینگونه جرایم می باشد. نظریه جابجایی مکانی یا انتقال فضا، تفسیری درباره ماهیت رفتار اشخاصی است که رفتار هنجار و ناهنجار خود را در فضای فیزیکی و سایبری نشان می دهند. این نظریه اختصاصا برای جرایمی که با استفاده از اینترنت واقع می شوند، شکل گرفته است و بیان می دارد که مردم هنگامی که به دنیایی با ویژگی های مطلوبشان وارد می شوند، ممکن است به گونه متفاوتی رفتار کنند که سبب گرایش افراد به ارتکاب جرم و همچنین بزه پدیدی آنان گردد.

لازم به ذکر است در بحث جرم شناسی جرایم سایبری مطالعات اندکی صورت گرفته است که این امر می تواند به دلیل سرعت تغییرات فناوری و نیاز به مشارکت و حضور فعال در فضای سایبری برای تبیین آن و دشواری هایی در رسیدن به یک توافق جامع در هنجارهای رفتاری فضای سایبر است. کمالینکه رقم سیاه بزهکاری در این جرایم نیز بسیار بالا می باشد. در اثر عواملی همچون عدم آگاهی و شناخت کامل بزه دیدگان این جرایم، ترس از لطمه به اعتبار شرکت و از دست دادن اعتبار سرمایه گذاران، عدم تخصص ضابطان قضائی در شیوه کشف و تعقیب این جرایم و فقدان امکانات کافی در این خصوص، مشکلات فنی خاص در کشف و اثبات آنها رقم سیاه در جرایم سایبری بسیار بالاست. لذا متخصصان، اطلاعات موجود در زمینه جرایم سایبری را مانند کوه یخ می دانند.

در واقع این واقعیت را باید پذیرفت که هنوز برداشت عمل مجرمانه در بسیاری از فعالیت های سایبری که فی الواقع جرم هستند، نمی شود. لذا نقش فرهنگ سازی در اینجا پررنگ می گردد. می توان گفت برای تقابلی امن و کاهش جرایم در فضای سایبر، سه مولفه قابل توجه هستند: حاکمیت، پلیس، مردم. در جرایم سایبری، نقش حاکمیت به دو دلیل عمده بسیار برجسته می گردد. نخست آنکه، مجرمان بابت اعمالشان مجازات نمی کنند زیرا عملشان را جرم نمی دانند. در برخی موارد، مشاهده شده فرد به دلیل احساس امنیت، پرستانه اش اقدام به برخی جرایم سایبری نموده است، مانند هک کردن سایت های دولتی، تخریب های متخاصم. این امر، می تواند نتایج بسیار مخرب و خطرناک برای کلیت جامعه و امنیت ملی به بار آورد و چه بسا دامنه جنگی گسترده را فراهم نماید.

عامل دیگر، مباحث مربوط به تبادلات مالی و گسترده شدن بانکداری الکترونیک بدون توجه به فراهم آوردن بسترهای فرهنگی در این زمینه و آگاهی رساندن مناسب به مردم می باشد. لذا حتی گاه مردم از اینکه بزه دیده یک جرم سایبری شده اند، ناآگاه هستند. این ناآگاهی، دامن خانواده ها را نیز می گیرد. فقر علمی خانواده ها در این زمینه و پیشرو بودن فرزندان شان، امری است که منجر به عدم نظارت شایسته والدین بر فعالیت فرزندان شان در این فضا می گردد. این خانواده ها که با سفر چندروزه فرزندان شان با دوستان خود مخالفند، به یکباره فرزند خود را برای سفری جهانی در کنار هزاران غریبه در دنیای سایبر رها می سازند که این امر می تواند افزایش جرایم سایبری - خواه در بزهکاری این نوجوانان و خواه در بزه دیدگی آنان - را در پی داشته باشد.

ویژگی های خاص این فضا و ناآگاهی مردم و نبود زیرساخت های فرهنگی لازم برای حضور در این فضا، عنصری تشویق کننده برای مجرمین گشته است که علاوه بر مجرمان خاص فضای سایبر، مجرمان



فضای واقعی نیز دامنه جرایمشان را از فضای واقعی به دنیای سایبر انتقال داده اند و به نوعی پدیده «کوچ مجرمانه» شکل گرفته است. ارتقاء سطح اطلاعات جامعه نسبت به فضای مجازی و اطلاع رسانی در زمینه جرایم سایبری و راههای مقابله با آن، ارتقاء سطح باورهای اخلاقی خصوصا در بین نوجوانان و جوانان نمونه‌هایی از پیشگیری از شکل گیری جرایم در فضای مجازی است.

هم چنین از آنجا که خسارات وارده بر اثر جرائم سایبری به مراتب گسترده‌تر و جبران ناپذیرتر درمقایسه با جرائم سنتی است، و با توجه به تهدیدات و آسیب‌های این محیط علیرغم مزایای فراوان آن، لازم است به خوبی بر آن اشراف داشته و این تهدیدات مستمرا شناسایی شوند تا بتوان در عصر حاضر با افزایش دراک از تأثیر و کاربرد فضای سایبر بر ماهیت جرم و انحراف بهتر مقابله نموده و از بروز سان پیشگیری نمود.

کتاب حاضر از آثار نوین ارزشمند در حوزه تبیین جرایم سایبر از منظر جرم‌شناختی و نقش آن در دستاوردهای علمی علوم سایبری مدرن می‌باشد که پیرامون ماهیت جرایم سایبری و بررسی اقسام آن شامل هک کردن، کلاهبرداری اینترنتی، جرایم جنسی، آزار و اذیت آنلاین و مزاحمت سایبری، ترور سایبری، نقش ادله اثبات و جرم‌یابی دیجیتال، چشم‌انداز آینده جرایم سایبری مباحثی ارزشمند و بسیار جدید و به روز را مطرح نموده است که قطعا آثار قابل استناد و ارجاع در حوزه شناسایی جرایم سایبری و جرم‌شناسی سایبری می‌باشد.