

پیشگیری از جرایم سایبری علیه امنیت ملی در ایران

مؤلف

احمد شکری

انتشارات قانون یار

۱۳۹۹

سرشناسه	:	شکری، محمد، ۱۳۶۵ -
عنوان و نام پدیدآور	:	پیشگیری از جرایم سایبری علیه امنیت ملی در ایران / مولف محمد شکری.
مشخصات نشر	:	تهران: انتشارات قانون یار، ۱۳۹۹.
مشخصات ظاهری	:	۱۹۰ ص.
شابک	:	۹۷۸-۶۲۲-۲۲۹۱۱۴-۳
وضعیت فهرست نویسی	:	فیا
یادداشت	:	کتابنامه: ص. ۱۸۱.
موضوع	:	جرایم کامپیوتری - ایران -- پیشگیری
موضوع	:	Computer crimes-- Iran -- Prevention
موضوع	:	فضای مجازی - ایران -- تدابیر ایمنی
موضوع	:	Cyberspace-- Iran -- Security measures
موضوع	:	امنیت ملی - ایران
موضوع	:	National security-- Iran
رده بندی کنگره	:	۶۳۳۲
رده بندی دیویی	:	۱۶۱ . ۵۳ . ۴۴
شماره کتابشناسی ملی	:	۶۰۹۴۱۰

انتشارات قانون یار

پیشگیری از جرایم سایبری علیه امنیت ملی در ایران

تألیف: محمد شکری

ناشر: قانون یار

ناظر فنی: محسن فاضلی

نوبت چاپ: اول-۱۳۹۹

شمارگان: ۱۱۰۰ جلد

قیمت: ۵۶۰۰۰ تومان

شابک: ۹۷۸-۶۲۲-۲۲۹-۱۱۴-۳

مرکز پخش: تهران، میدان انقلاب، خ منیری جاوید، پلاک ۹۲

۰۲۱۶۶۹۷۹۵۱۹

۰۲۱۶۶۹۷۹۵۲۶

فهرست مطالب

پیشگفتار.....	۱۷
فصل اول.....	۲۱
ساختمان‌شناسی فضای سایبر و مفهوم شناسی جرایم سایبری امنیتی ، امنیت ملی و جرایم امنیتی	
.....	۲۱
سخن آغازین فصل.....	۲۱
بخش اول: انواع تعاریف ارائه شده از جرایم سایبری.....	۲۲
بند اول: تعریف جامع جرایم سایبری.....	۲۳
بند دوم: ساختار فضای سایبر.....	۲۳
بند سوم: راه‌های ارتباطی.....	۲۳
بند چهارم: شبکه‌های رایانه‌ای.....	۲۵
بند پنجم: ارائه‌دهندگان خدمات اینترنتی و حملات اینترنتی.....	۲۶
بخش دوم: علت شناسی جرایم سایبری.....	۲۸
بند اول: علل فردی.....	۲۸
بند دوم: علل اجتماعی.....	۲۹
بند سوم: ضعف فرهنگی.....	۲۹
بند چهارم: شرایط نامساعد اقتصادی.....	۳۰
بند پنجم: خانواده‌های نابسامان.....	۳۰
بند ششم: هم‌سالان معارض.....	۳۰
بند هفتم: نقش بزه‌دیده سایبری.....	۳۱
بخش سوم: اوصاف شناسی جرایم سایبری امنیتی.....	۳۱
بند اول: امنیت ملی و جرایم امنیتی.....	۳۲
بند دوم: آشنایی با مجرمین سایبر و جرایم سایبری نوین.....	۳۳
بند سوم: سابوتاژ و اخاذی رایانه‌ای.....	۳۴
بند چهارم: استراق سمع غیر مجاز.....	۳۴
بند پنجم: سرقت و تکثیر غیر مجاز برنامه‌های رایانه‌ای حمایت شده.....	۳۴
بند ششم: پورنوگرافی غیر مجاز رایانه‌ای.....	۳۵
بند هفتم: کلاهبرداری کارت اعتباری در سایبر سپس و پولشویی.....	۳۵

- بند هشتم: افترآ و نشر اطلاعات از طریق پست الکترونیک ۳۶
- بند نهم: قاچاق مواد مخدر از طریق سایبر ۳۶
- بند دهم: سرقت اطلاعات اشخاص حقوقی ۳۷
- بند یازدهم: اخاذی در قبال محرومیت از خدمات ۳۷
- بند دوازدهم: حملات سایبری در مقیاس بزرگ ۳۷
- بند سیزدهم: فیشینگ، حمله فیشینگ و اسپیم ۴۰
- بند چهاردهم: فارمینگ ۴۲
- بند پانزدهم: ویشینگ ۴۲
- بند شانزدهم: اسمیشینگ ۴۲
- بند هجدهم: درو، های و ویروس های رایانه ای ۴۳
- بند هیجدهم: بایب منداقی ۴۳
- بند نوزدهم: هک و رد ۴۴
- بخش چهارم: آثار مرتب جرایم سایبری ۴۴
- بند اول: آثار و آسیب های روانی ۴۴
- بند دوم: اعتیاد مجازی ۴۴
- بند سوم: بحران هویت ۴۴
- بند چهارم: سوء استفاده جنسی ۴۵
- بند پنجم: آثار اجتماعی و فرهنگی ۴۶
- بند ششم: آثار سیاسی (تزلزل در حاکمیت و اقتدار سیاسی) ۴۶
- بخش پنجم: خصوصیات مرتکبین (مجرمین) جرایم سایبری ۴۷
- بند اول: خصوصیات سازمانی ۴۷
- بند دوم: عضوگیری یا جذب ۴۸
- بند سوم: ارتباطات بین المللی ۴۸
- بند چهارم: خصوصیات عملیاتی ۴۸
- بند پنجم: ویژگی فردی ۴۹
- بند ششم: نقاط ضعف اجتماعی ۴۹
- بند هفتم: خصوصیات منابع ۴۹
- بند هشتم: بهبود وضعیت امنیت اطلاعات از طریق آموزش ۴۹
- بند نهم: ساختار پشتیبانی ۵۰



۵۰	بخش ششم: مشکلات و موانع کشف جرایم سایبری
۵۱	بند اول: چالش‌های امنیتی شبکه‌های اجتماعی
۵۱	بند دوم: سرقت و جعل هویت
۵۱	بند سوم: مهندس اجتماعی
۵۲	بند چهارم: نقض حریم خاص
۵۳	بند پنجم: آسیب پذیری فضای سایبر
۵۳	بخش هفتم: ویژگی شناسی جرایم سایبری امنیتی
۵۳	بند اول: توسعه و تغییرپذیری
۵۴	بند دوم: ملی و نامحدود بودن محیط سایبر
۵۵	بند سوم: استفاده گسترده از فضای سایبر
۵۵	بند چهارم: در دسترس بودن
۵۶	بند پنجم: پنهانی پوشش و ناملموس بودن محیط سایبر
۵۷	بند ششم: دستیابی آسان به این اطلاعات
۵۷	بند هفتم: پیچیده و تخصصی بودن فضای سایبر
۵۷	بند هشتم: دسترسی آسان و سریع
۵۷	بند نهم: جاذبه فضای سایبر
۵۸	بند دهم: آزادی اطلاعات و ارتباطات
۵۸	بخش هشتم: محدودیت‌های اندک در ارتکاب جرایم سایبری
۵۸	بند اول: تنوع زمان وقوع جرم
۵۸	بند دوم: تفاوت نوع مجرمین
۵۹	بند سوم: سرعت وقوع جرم
۵۹	بند چهارم: مکان ارتکاب جرم
۶۰	بند پنجم: ناشناس نگه داشتن هویت واقعی
۶۰	بند ششم: انگیزه‌ی رفع نیازهای جنسی
۶۱	بخش نهم: تحولات اینترنت و تلفن همراه در ایران
۶۱	بند اول: آسیب‌های امنیتی تلفن همراه
۶۲	بند دوم: تهدیدات امنیتی ناشی از تلفن همراه
۶۳	بند سوم: تهدیدات نرم‌افزاری تلفن همراه
۶۳	بند چهارم: ویروس‌های تلفن همراه

- بخش دهم: راه‌های پیشگیری از شنود مکالمات به وسیله تلفن همراه ۶۳
- بند اول: نکات کلیدی در امنیت تلفن‌های همراه ۶۴
- بند دوم: تکامل جرایم سایبری ۶۵
- بند سوم: آشننگی سایبری ۶۵
- بند چهارم: ضرورت و فوریت بهبود امنیت سایبری ۶۶

فصل دوم ۶۹

- پیشگیری از جرم سایبری از بعد حقوقی ۶۹
- بخش اول: تدابیر پیشگیرانه کیفری از جرایم سایبری امنیتی ۶۹
- بند اول: پیشگیری کیفری عام ۷۱
- بند دوم: پیشگیری کیفری خاص ۷۲
- بخش دوم: انواع پیشگیری کیفری از جرایم سایبری امنیتی ۷۳
- بند اول: پیشگیری کیفری از رد در ترم انگاری (قوانین ماهوی) ۷۳
- بند دوم: پیشگیری کیفری جرم انگاری (قوانین ماهوی) ۷۳
- بند سوم: پیشگیری کیفری جرم انگاری (قوانین ماهوی) ۷۴
- بخش سوم: تعریف و ماهیت تروریسم سایبری ۷۴
- بند اول: جاسوسی سایبری ۷۶
- بند دوم: پیشگیری کیفری از گذر تدابیر شکلی ۷۷
- بند سوم: اصول حاکم بر آیین دادرسی افتراقی ۷۷
- بند چهارم: خاص و فنی کردن فرآیند رسیدگی ۷۸
- بند پنجم: مسائل اجرای قانون ۷۸
- بند ششم: جرایم سایبری ابتدایی در کشور و قوانین مصوب ۷۹
- بخش چهارم: طبقه‌بندی جرایم سایبری توسط سازمان‌های بین‌المللی و اسناد داخلی ایران ۸۰
- بند اول: اقدامات شورای اروپا در رابطه با جرایم سایبری ۸۰
- بند دوم: اقدامات انجمن بین‌المللی حقوق جزا در خصوص جرایم رایانه‌ای ۸۱
- بند سوم: طبقه‌بندی سازمان ملل متحد از جرایم رایانه‌ای ۸۱
- بخش پنجم: طبقه‌بندی اینترپول (سازمان پلیس جنایی بین‌المللی) از جرایم رایانه‌ای ۸۲



۸۳.....	بند اول: طبقه‌بندی کنوانسیون بوداپست
۸۳.....	بند دوم: طبقه اول ماده ۲ تا ۶ کنوانسیون
۸۳.....	بخش ششم: جرایم مرتبط با رایانه که شامل ماده ۷ و ۸ کنوانسیون
۸۵.....	بخش هفتم: طبقه‌بندی جرایم سایبری با توجه به اسناد داخلی و ملی (ایران)
۸۵.....	بند اول: قانون جرایم نیروهای مسلح
۸۵.....	بند دوم: قانون تجارت الکترونیکی ۱۳۸۲
۸۶.....	بند سوم: قانون جرایم رایانه‌ای ۱۳۸۸
۸۶.....	بند چهارم: جرایم مرتبط با حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای
۸۶.....	بند پنجم: جرایم رایانه‌ای در قانون تجارت الکترونیکی
۸۹.....	فصل سوم
۸۹.....	تدابیر پیشگیرانه اجباری (فن مدار)
۸۹.....	سخن آغازین فصل
۸۹.....	بخش اول: پیشگیری اجتنابی از جرایم سایبری امنیتی
۹۲.....	بند اول: پیشگیری رشدمدار
۹۴.....	بخش دوم: نواح برنامه‌ها پیشگیری رشدمدار
۹۴.....	بند اول: برنامه‌ها و تدابیر خانواده مدار
۹۶.....	بند دوم: تدابیر کاربری صحیح و نهادینه کردن فردنگ استفاده صحیح از فضای سایبر
۹۷.....	بند سوم: تدابیر همیاری همسالان
۹۷.....	بند چهارم: تدابیر کاهنده آثار سوء
۹۸.....	بند پنجم: تدابیر آموزشی آموزش سلامت اینترنت و مداخله در آسیب‌ها
۹۸.....	بند ششم: ادبیات اطلاعات و رسانه
۹۹.....	بند هفتم: بزه دیده زدایی
۱۰۰.....	بند هشتم: پیشگیری اجتماع‌مدار
۱۰۱.....	بند نهم: توسل به کدهای رفتاری
۱۰۱.....	بند دهم: مفهوم‌شناسی کدهای رفتاری
۱۰۲.....	بند یازدهم: گونه‌شناسی کدهای رفتاری
۱۰۳.....	بند دوازدهم: کدهای رفتاری عام
۱۰۴.....	بند سیزدهم: کدهای رفتاری خاص

بخش سوم: اطلاع‌رسانی عمومی و اطلاع‌گیری در راستای پیشگیری اجتماعی از جرایم

- رایانه‌ای ۱۰۵
- بند اول: حکمرانی خوب در فضای سایبر ۱۰۶
- بند دوم: رفع مشکلات اقتصادی ۱۰۹
- بخش چهارم: محدودیت‌های پیشگیری اجتماعی از جرایم سایبری ۱۰۹
- بند اول: تدابیر پیشگیرانه وضعی (فن مدار) مفهوم پیشگیری وضعی ۱۱۱
- بند دوم: ایمن‌ساختن فضای سایبر ۱۱۵
- بند سوم: افزایش ریسک ارتکاب جرم ۱۱۵
- بخش پنجم: حفاظت از سیستم‌های رایانه‌ای ۱۱۶
- بند اول: حفاظت فیزیکی ۱۱۶
- بند دوم: حفاظت ارتباطات ۱۱۶
- بند سوم: حفاظت از رکودان ۱۱۷
- بند چهارم: حفاظت عملیات ۱۱۷
- بخش ششم: راهبردهای پیشگیری وضعی از منظر کلارک راهبردهای ایجابی ۱۱۸
- بند اول: افزایش میزان تلاش برای ارتکاب جرم ۱۱۸
- بند دوم: تقویت آماج‌ها ۱۱۸
- بند سوم: کنترل ورودی‌ها ۱۱۹
- بند چهارم: کنترل و بازرسی خروجی‌ها ۱۲۰
- بند پنجم: تغییر مسیر بزه‌کاران ۱۲۰
- بند ششم: کنترل ابزارها ۱۲۱
- بند هفتم: افزایش خطر ارتکاب جرم ۱۲۱
- بند هشتم: توسعهٔ محافظت‌ها ۱۲۱
- بند نهم: کاهش ناشناختگی ۱۲۲
- بند دهم: استفاده از مدیریت مکان ۱۲۳
- بند یازدهم: ارتقای نظارت رسمی ۱۲۳
- بند دوازدهم: راهبردهای سلبی ۱۲۴
- بند سیزدهم: کاهش دستاوردها ۱۲۴
- بند چهاردهم: پنهان کردن آماج ۱۲۴
- بند پانزدهم: جابه‌جا کردن آماج ۱۲۵



۱۲۵	بند شانزدهم: کاهش عوامل محرک
۱۲۵	بند هیفدهم: اجتناب از اغتشاش
۱۲۶	بند هیجدهم: کاهش برانگیختگی
۱۲۶	بند نوزدهم: تدابیر آموزشی - آگاهی ساز
۱۲۷	بند بیستم: اعلان جرم بودن یک عمل و اطلاع رسانی نسبت به آن
۱۲۷	بند بیست و یکم: آگاهی سازی کاربران و آمادگی مقابله با جرایم سایبری
۱۲۸	بخش هفتم: فن آوری های دفاعی و مسائل سیاست عمومی مشترک
۱۲۹	بند او: دفاع های مبتنی بر شبکه
۱۳۰	بند دوم: سیستم های جلوگیری از نفوذ مبتنی بر شبکه
۱۳۰	بند سوم: پروتکل امنیت اینترنت
۱۳۱	بند چهارم: نفاذات
۱۳۲	بند پنجم: دیوار آتش (فایروال های سخت افزاری و نرم افزاری)
۱۳۳	بند ششم: فایروال های سخت افزاری
۱۳۴	بند هفتم: فایروال های نرم افزاری
۱۳۴	بخش هشتم: انواع دیوار آتش و اساس عملکرد
۱۳۵	بند اول: پالایش گر بسته ها
۱۳۵	بند دوم: بازرسی همه جانبه
۱۳۵	بند سوم: سرورهای پراکسی
۱۳۶	بند چهارم: دیواره آتش سطح - مدار
۱۳۶	بند پنجم: دیواره آتش سطح - کاربردی
۱۳۷	بند ششم: ابزارهای ناشناس کننده و رمزگذاری
۱۳۹	بند هفتم: هانی پات
۱۴۰	بند هشتم: هانی پات های تولیدی (تجاری)
۱۴۰	بند نهم: هانی پات های پژوهشی
۱۴۰	بند دهم: سیستم های کشف مزاحمت
۱۴۲	بند یازدهم: فیلترینگ (کنترل)
۱۴۳	بخش نهم: انواع فیلترینگ
۱۴۳	بند اول: فیلترینگ از طریق DNS
۱۴۳	بند دوم: فیلترینگ به وسیله پروکسی

پیشگفتار

امنیت ملی حالتی است که یک کشور با تهدید داخلی و خارجی روبرو نباشد. در گذشته امنیت ملی ناظر به نبود تهدید علیه مرزهای کشور و تمامیت سرزمینی تلقی می شد، ولی امروزه با وجود اینترنت و فضای سایبر امنیت ملی مفهومی گسترده تر پیدا کرده است. حجم فراوانی از اطلاعات مورد نیاز جامعه امروز، با استفاده از رایانه ها و شبکه های مرتبط به آن تولید، ذخیره ارسال و توسعه می یابد. فضای سایبر و اینترنت فارغ از مرزهای جغرافیایی عمل می کند؛ مبنای آن به چارچوب خطوطی که دولتمردان در طراحی نقشه های سیاسی رسم می کنند نیست و از هیچ گونه محدودیت مکانی تبعیت نمی کنند. در کسری از ثانیه حملاتی از این سوی جهان عده اهدای در آن سوی جهان ممکن شده است. این فضای بی پاسبان و رها که هر لحظه بر گستره آن امرود می شود، فرصت بسیار مناسبی را برای ارتکاب و اختفای جرایم سایبری به مرتکب اعطای می کند. در این فضا نمی توان هیچ چهار چوب اخلاقی، ارزشی یا هنجاری مشخصی برای مبارزه با جرم گیری تعریف نمود. در اواخر سده ۲۰ و در عصر فرا صنعتی، جهانی شاهد ظهور پدیده های نوگانی در اثر پیشرفت های علمی و فن آوری های جدید بود. ابداعی که دنیای اقتصاد، سیاست و فرهنگ را مجذوب خود ساخت. این دنیای جدید فضای مجازی یا فضای سایبر نام گرفت. انسانها پس از ظهور این پدیده بسیاری از روابط خود را به این فضا وارد نمودند. تبلیغات گسترده، فعالیتهای اقتصادی، تجارت و داد و ستد، بانکداری، الکترونیک، اشاعه فرهنگ، آموزش و اطلاع رسانی، مکانی تنها بخشی از فعالیت های روزمره انسانها بوده که به این دنیای جدید کشانده شد. به موازات اتفاقاتی در دنیای مجازی از جمله ارتکاب جرایم سایبری و تبعات و آثار منفی و مخرب فرهنگی این محیط، دخالت علم حقوق را ضرورت بخشیده است. هیچ معلولی شناخته و درمان نمی گردد مگر اینکه علل ایجاد کننده آن شناسایی و خنثی گردند، بنابراین باید علل ارتکاب این طیف از جرایم کشف شود. در این راستا باید علاوه بر دخالت عدالت کیفری، عدالت ترمیمی و تدابیر پیشگیرانه نیز در جهت جلوگیری از ارتکاب این جرایم و همچنین دادن ارائه

راهکارهای مقابله با جرایم سایبری و ایجاد خدشه در نقش مثبت فضای سایبر مداخله نموده و با نگاهی ویژه به خصوصیات فضای سایبر ابزارها و مکانیسم خود را بکار گیرند تا بتوان به جامعه عاری از تخلفات سایبری و نهادینه شدن اخلاق حرفه‌ای استفاده صحیح و ایمن از این فضا در آینده امیدوار بود. در این فضا، همه چیز با همه چیز مرتبط و برهم تأثیر می‌گذارند، آن‌هم نه در یک گستره محدود و مشخص، بلکه در یک دنیای بیکران که به واقع هیچ حد و مرزی برای آن قابل تصور نیست. جهان مجازی به دلیل ظرفیت دیجیتالی و قدرت انتقال هم زمان درخاسته و فرمان‌ها، جهانی بودن، ارزان‌تر بودن، فشرده‌تر بودن، قابل دسترس‌تر بودن، راحت‌تر بودن، استفاده بهینه از انرژی و پنهان ماندن هویت و انتشار سریع اطلاعات، همراه با کارآمدی و سهولت و تنوع می‌باشد و از سوی دیگر منشأ چالش‌های اجتماعی، سیاسی امنیتی، اقتصادی و فرهنگی به‌شمار می‌آید. گسترش روزافزون جرایم رایانه‌ای در ایران مانند سرقت از کارت‌های اعتباری، سرقت اینترنتی، سرقت از دستگاه‌های عابر بانک، نفوذ در شبکه‌های اطلاعاتی و موسسات ملی و خصوصی و نیز احیاناً سوء استفاده‌های مالی، هرزه‌نگاری اینترنتی و ... غیره ایجاب می‌کند در جهت پیشگیری از این نوع جرایم تلاش شود. کارآمد و سالم بودن فضای سایبر در اقتصاد، امنیت ملی کشورها از اهمیت ویژه‌ای برخوردار است. امنیت اطلاعات در محیط‌های مجازی، فضای سایبر بعنوان مهمترین الزام در کاربری توسعه‌ای و فراگیر فن‌آوری اطلاعات و ارتباطات می‌باشد. اگر چه امنیت مطلق در محیط‌های واقعی و مجازی امکان پذیر نیست ولی ایجاد سطحی از امنیت که به اندازه کافی و متناسب با نیازها و سرمایه‌گذاری‌ها انجام شده باشد تقریباً در همه رابط محلی ممکن می‌باشد. بنیاد هر کشوری بر اساس مجموعه‌ای از زیر ساخت‌های حیاتی آن کشور در بخش‌های ارتباطات، دفاع، انرژی، حمل و نقل، کشاورزی، بهداشت و امور اقتصادی است که فضای سایبر به مثابه یک سیستم عصبی آنها را به هم مرتبط می‌سازد. با ایجاد یک راهبرد ملی در استقرار حداکثر امنیت در فضای سایبر می‌توان به کاهش آسیب پذیری کشور در مقابل حملات پرداخته و از بروز خسارت به زیر ساخت‌های اطلاعاتی پایه و حیاتی و همچنین دارایی‌های ملی جلوگیری نمود. اگرچه این فضا و به کارگیری فناوری اطلاعات و ارتباطات



امکانات بسیاری را فراهم آورده تا بخش قابل توجهی از فعالیت‌های انسانی با سرعت بیشتر و هزینه کمتر انجام گیرند، لیکن همین فناوری اطلاعات با تسهیل زمینه و شیوه ارتکاب جرم و توسعه خسارت مادی و معنوی ناشی از جرم و ایجاد جرائم جدید و پدید آوردن شیوه‌های مجرمانه نوین، فرصتهای طلایی زیادی را برای مجرمین فراهم نموده است. در کشورهای در حال توسعه با افزایش استفاده از فن‌آوری‌های اطلاعات، نگرانی‌های امنیتی در زمینه‌های مختلف در حال ازدیاد است. عرصه فضای مجازی با دسترسی به طیف گسترده‌ای از مخاطبان که عموماً شامل نوجوانان و جوانان است، می‌تواند با اطلاع‌رسانی مستمر شبانه‌روزی و بدون محدودیت در این فضا و از طریق تعاملات چند وجهی صوتی و تصویری به مخاطب خود نزدیکتر شده و مانع ایجاد فاصله میان کارگزاران امنیت در جامعه و عموم مردم شود. کشورهای تحت تأثیر بنیادین سائیری غالباً نیاز بیشتری به اشتراک گذاشتن دانش فنی، مهارت‌ها و اطلاعات مربوط به جرائم سائیری دارند؛ لذا جوامع بین‌المللی با تشخیص این نیاز، به دنبال هماهنگی بیشتری میان ملت‌ها در سراسر جهان برای مقابله با مسایل حقوقی و فنی مربوط به جرائم سائیری هستند. مسائل امنیتی مرتبط با این فن‌آوری‌ها از نکته نظر حمله و دفاع تجزیه و تحلیل می‌شود تا درک بهتری از گزینه‌های فن‌آوری در دسترس مهاجمان و مدافعان و مسائل خط‌مشی مرتبط با فن‌آوری‌های امنیتی به دست می‌آید. لازم به ذکر می‌باشد هرگونه مقابله با هنجار شکنی‌های سائیری در جهت برقراری موازین اخلاقی سائیری، می‌تواند با ایرادات جدی حقوقی و اخلاقی مواجه گردد. مداخله و مشارکت بین‌المللی کشور در فرآیند پیشگیری از جرم که هر کدام قوانین خاص خود را داشته و چه بسا وابسته به نظام‌های حقوقی متفاوتی نیز باشند، همکاری بین‌المللی برای پیشگیری از جرائم سائیری را با مشکلات متعددی مواجه می‌کند. به موازات این چالش، در برخی از موارد، نیروهای مسئول پیشگیری از بزه، سطح دانش یکسانی نداشته یا به فناوری‌های نوین پیشگیری از بزه دسترسی نداشته و نمی‌توانند درخواست‌های طرف مقابل برای پیشگیری از موقعیت‌های پیش‌جنایی را فراهم آورند. سیاست‌جنایی در مقابله با جرائم سائیری علیه امنیت ملی نیازمند اتخاذ تدابیر پیشگیرانه غیر کیفری در قالب پیشگیری‌های اجتماعی و وضعی (فنی)



است. به همین منظور در این کتاب بررسی روش های پیشگیرانه علیه جرایم سایبری در ج.ا.ا. مورد بررسی قرار می گیرد.