



پیشگیری از جرایم سایبری علیه امنیت ملی در ایران

مؤلف

محمد شکری

انتشارات قانون یار

۱۳۹۹

سرشناسه	: شكري، محمد، ۱۳۶۵ -
عنوان و نام پديدآور	: پيشگيري از جرايم سايبري عليه امنيت ملي در ايران / مولف محمد شكري.
مشخصات نشر	: تهران: انتشارات قانون يار، ۱۳۹۹.
مشخصات ظاهري	: ۱۹۰ ص.
شابک	: ۹۷۸-۶۲۲-۲۲۹۱۱۴-۳
وضعيت فهرست نوبسي	: فيبا
يادداشت	: کتابنامه: ص. ۱۸۱.
موضوع	: جرايم کامپيوتري - ايران - پيشگيري
موضوع	: Computer crimes-- Iran -- Prevention
موضوع	: فضاى مجازى - ايران - تدابير ايمني
موضوع	: Cyberspace-- Iran -- Security measures
موضوع	: امنيت ملي - ايران
موضوع	: National security-- Iran
رده بندي كنگره	: ۶۷۳HV
رده بندي ديويي	: ۱۶۸۰۹۵۵/۳۶۴
شماره كتابشناسي ملي	: ۶۱۲۹۴۱۰

انتشارات قانون يار

پيشگيري از جرايم سايبري عليه امنيت ملي در ايران

تأليف: محمد شكري

ناشر: قانون يار

ناظر فني: محسن فاضلي

نوبت چاپ: اول - ۱۳۹۹

شمارگان: ۱۱۰۰ جلد

قيمت: ۴۶۰۰۰ تومان

شابک: ۹۷۸-۶۲۲-۲۲۹-۱۱۴-۳

مرکز پخش: تهران، ميدان انقلاب، خ منيري جاويد، پلاک ۹۲

۰۲۱۶۶۹۷۹۵۱۹

۰۲۱۶۶۹۷۹۵۲۶

اهمیت فضای مجازی ، امروز به اندازه اهمیت انقلاب اسلامی است.

مقام معظم رهبری (حفظه ...)

فهرست مطالب

پیشگفتار.....	۱۷
فصل اول.....	۲۱
ساختار شناسی 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 شناسی فضای سایبر.....	۲۳
بند سوم: سامانه‌های 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: علت فردی.....	۲۸
بند دوم: علت 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 سپیس و پولشویی.....	۳۵



- بند هشتم: افترا 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 اسپم ۴۰
- بند چهاردهم: فارمینگ ۴۲
- بند پانزدهم: ویشینگ ۴۲
- بند شانزدهم: اسمیشینگ ۴۲
- بند هیفدهم: گروه‌های ویروس‌های رایانه‌ای ۴۳
- بند هیجدهم: بمب منطقی ۴۳
- بند نوزدهم: هک کردن ۴۴
- بخش چهارم: آثار مخرب جرایم سایبری ۴۴
- بند اول: آثار و آسیب‌های 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 بین‌المللی 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



بخش ششم: مشکلات و موانع کشف جرایم سایبری	۵۰
بند اول: چالش‌های امنیتی شبکه‌های اجتماعی	۵۱
بند دوم: سرقت و جعل هویت	۵۱
بند سوم: مهندس اجتماعی	۵۱
بند چهارم: نقض حریم خاص	۵۲
بند پنجم: آسیب پذیری فضای سایبر	۵۳
بخش هفتم: ویژگی شناسی جرایم سایبری امنیتی	۵۳
بند اول: توسعه و تغییرپذیری	۵۳
بند دوم: بین‌المللی و نامحدود بودن محیط سایبر	۵۴
بند سوم: استفاده گسترده از فضای سایبر	۵۵
بند چهارم: دولت زدایی	۵۵
بند پنجم: پنهانی، پوشیده و ناملموس بودن محیط سایبر	۵۶
بند ششم: دست یابی آسان به آخرین اطلاعات	۵۷
بند هفتم: پیچیده و تخصصی بودن فضای سایبر	۵۷
بند هشتم: دسترسی آسان و سریع	۵۷
بند نهم: جاذبه فضای سایبر	۵۷
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 مجرمان	۵۸
بند سوم: سرعت وقوع جرم	۵۹
بند چهارم: مکان ارتکاب جرم	۵۹
بند پنجم: ناشناس نگه داشتن هویت واقعی	۶۰
بند ششم: انگیزه‌ی رفع نیازهای جنسی	۶۰
بخش نهم: تحولات اینترنت و تلفن همراه در ایران	۶۱
بند اول: آسیب‌های امنیتی تلفن همراه	۶۱
بند دوم: تهدیدات امنیتی ناشی از تلفن همراه	۶۲
بند سوم: تهدیدات نرم‌افزاری تلفن همراه	۶۳
بند چهارم: ویروس‌های تلفن همراه	۶۳



- 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: آشفتگی سایبری ۶۵
- بند چهارم: ضرورت و فوریت بهبود امنیت سایبری ۶۶

فصل دوم ۶۹

- پیشگیری از جرایم سایبری از بعد حقوقی ۶۹
- سخن آغازین فصل 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 رهگذر جرم انگاری (قوانین ماهوی) ۷۳
- بند دوم: پیشگیری کیفری جرم انگارانه با معیار وسیله محور ۷۳
- بند سوم: پیشگیری کیفری جرم انگارانه با معیار موضوع محور 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 رایانه ای ۸۱
- بند سوم: طبقه‌بندی سازمان ملل متحد از جرایم رایانه ای ۸۱
- بخش پنجم: طبقه‌بندی اینترپول (سازمان پلیس جنایی بین‌المللی) از جرایم رایانه ای ۸۲



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	۸۳
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	۸۵
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	۸۶

فصل سوم ۸۹

تدابیر پیشگیرانه اجتماعی و وضعی (فن مدار)	۸۹
سخن آغازین فصل	۸۹
بخش اول: پیشگیری اجتماعی از جرایم سایبری امنیتی	۸۹
بند اول: پیشگیری رشدمدار	۹۲
بخش دوم: نواح برنامه‌ها پیشگیری رشدمدار	۹۴
بند اول: برنامه‌ها و تدابیر خانواده مدار	۹۴
بند دوم: تدابیر کاربری صحیح و نهادینه کردن فرهنگ استفاده صحیح از فضای سایبر	۹۶
بند سوم: تدابیر همیاری همسالان	۹۷
بند چهارم: تدابیر کاهنده آثار سوء	۹۷
بند پنجم: تدابیر آموزشی آموزش سلامت اینترنت و مداخله در فرآیند تحصیل	۹۸
بند ششم: ادبیات اطلاعات و رسانه	۹۸
بند هفتم: بزه دیده زدایی	۹۹
بند هشتم: پیشگیری اجتماع‌مدار	۱۰۰
بند نهم: توسل به کدهای رفتاری	۱۰۱
بند دهم: مفهومی‌شناسی کدهای رفتاری	۱۰۱
بند یازدهم: گونه‌شناسی کدهای رفتاری	۱۰۲
بند دوازدهم: کدهای رفتاری عام	۱۰۳
بند سیزدهم: کدهای رفتاری خاص	۱۰۳



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 کارکنان 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: توسعه 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



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



- بند سوم: فیلتر کردن به کمک مسیریاب‌ها..... ۱۴۳
- بند چهارم: لیست سیاهو لیست سفید..... ۱۴۴
- بخش دهم: محدودیت های پیشگیری وضعی از جرایم سایبری..... ۱۴۶
- بند اول: محدودیت‌های فنی..... ۱۴۶
- بند دوم: محدودیت‌های قانونی..... ۱۴۷

فصل چهارم..... ۱۴۹

- سیاست جنایی و تدابیر نظارتی..... ۱۴۹
- سخن آغازین فصل..... ۱۴۹
- بخش اول: ماهیت و تعریف سیاست جنائی..... ۱۴۹
- بند اول: مدل‌های سیاست جنایی..... ۱۵۰
- بند دوم: سیاست جنایی کنشی (پیشگیرانه)..... ۱۵۰
- بند سوم: سیاست جنایی از حیث مراجع سیاست‌گذاری..... ۱۵۰
- بند چهارم: سیاست جنایی تقنینی..... ۱۵۱
- بند پنجم: سیاست جنایی قضایی..... ۱۵۱
- بند ششم: تدابیر نظارتی..... ۱۵۳
- بند هفتم: تدابیر صدور مجوز..... ۱۵۵
- بخش دوم: نقش اشخاص حقیقی و حقوقی در جهت نظارت و پیشگیری از وقوع جرم و جرایم سایبری در ایران..... ۱۵۵
- بند اول: نقش و جایگاه قانونگذار..... ۱۵۵
- بند دوم: نقش دادستان و مقامات قضایی کشور برای پیشگیری از وقوع جرایم سایبری .. ۱۵۵
- بند سوم: اقدامات قضایی و نمونه‌هایی از جرایم سایبری در ایران..... ۱۵۶
- بند چهارم: اقدامات حقوقی در نظام حقوقی بین الملل و نظام حقوقی ایران و تعارض قوانین..... ۱۵۷
- بخش سوم: مهمترین اقدامات سازمان ملل متحد در خصوص جرایم سایبری..... ۱۵۸
- بند اول: همکاری کشورها با اینترنتپل در خصوص مجرمان سایبری..... ۱۵۸
- بند دوم: چالش های حقوقی..... ۱۵۸
- بند سوم: ارتش سایبری ایران..... ۱۵۹
- بند چهارم: نقش و جایگاه پلیس در پیشگیری از جرایم سایبری..... ۱۶۰



بخش چهارم: عامل تأثیرگذار بر سیاست جنایی قضایی در جرایم رایانه‌ای ۱۶۱
بند اول: مراجع قضایی تأثیرگذار ۱۶۱
بخش پنجم: اقدامات پیشگیرانه پلیس در جرایم فضای مجازی ۱۶۲
بند اول: گشت اینترنتی ۱۶۲
بند دوم: آموزش همگانی ۱۶۲
بند سوم: شناسایی و کنترل افراد خطرناک ۱۶۳
بند چهارم: مراقبت از سامانه‌های اطلاعاتی حساس کشور ۱۶۳
بند پنجم: نیروهای واکنش سریع سایبری ۱۶۴
بخش ششم: نقش دولت‌ها در مقابله و پیشگیری از اشاعه جرایم سایبری ۱۶۴
بند اول: پروژه بی ثبات سازی علیه جمهوری اسلامی ایران در فضای سایبر ۱۶۷
بند دوم: سایر اقدامات انجام شده در فضای سایبر علیه امنیت جمهوری اسلامی ایران ... ۱۶۷
بند سوم: تدوین اجرای نقشه طرح ملی آموزش عمومی جامعه ۱۶۷
بند چهارم: استفاده از فنون سایبری جهت تقویت نفوذ مؤثر به منظور پیشگیری‌های امنیتی
..... ۱۶۸
بند پنجم: امنیت فضای سایبر و زیر ساخت‌ها ۱۶۹
بند ششم: فضای سایبر و راهبردها ۱۶۹
بخش هفتم: ماهیت نامشخص چالش‌های امنیتی موجود در فضای سایبر ۱۶۹
بند اول: امنیت ملی جمهوری اسلامی ایران در دنیای جدید ۱۷۰
نتیجه‌گیری ۱۷۱
پیشنهادات ۱۷۷
منابع و ماخذ ۱۸۳

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 رایانه‌ها و شبکه‌های مرتبط به آن تولید، ذخیره، ارسال و توسعه می‌یابد. فضای سایبر و اینترنت فارغ از مرزهای جغرافیایی عمل می‌کند؛ محدود به چارچوب خطوطی که دولتمردان در طراحی نقشه‌های سیاسی رسم می‌کنند نیست و از هیچ گونه محدودیت مکانی تبعیت نمی‌کنند. در کسری از ثانیه حملاتی از این سوی جهان علیه اهدافی در آن سوی جهان ممکن شده است. این فضای بی‌پاسبان و رها که هر لحظه بر گستره آن افزوده می‌شود، فرصت بسیار مناسبی را برای ارتکاب و اختفای جرایم سایبری به مرتکب اعطای کند و در این فضا نمی‌توان هیچ چهار چوب اخلاقی، ارزشی یا هنجاری مشخصی برای مبارزه و درگیری تعریف نمود. در اواخر سده ۲۰ و در عصر فرا صنعتی، جهانی شاهد ظهور پدیده‌ای شگرف در اثر پیشرفت‌های علمی و فن‌آوری‌های جدید بود. ادعای 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 اطلاع‌رسانی همگانی تنها بخشی از فعالیت‌های روزمره انسان‌ها بوده که به این دنیای جدید کشانده شده است. بروز 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 نمی‌گردد مگر اینکه علل ایجاد کننده‌ی 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 بر هم 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 هم‌زمان درخواست‌ها 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 جذابیت و تنوع می‌باشد و از سوی دیگر منشأ چالش‌های اجتماعی، سیاسی امنیتی، اقتصادی و فرهنگی بی‌شماری خواهد بود. گسترش روزافزون جرایم رایانه‌ای در ایران مانند سرقت از کارت‌های اعتباری، سرقت اینترنتی، سرقت از دستگاه‌های عابر بانک، نفوذ در شبکه‌های اطلاعاتی و موسسات مالی و خصوصی و نیز احیانا سوء استفاده‌های مالی، هزینه‌نگاری اینترنتی و ... غیره ایجاب می‌نماید در جهت پیشگیری از این نوع جرایم تلاش شود. کارآمد و سالم بودن فضای سایبر در اقتصاد و امنیت ملی کشورها از اهمیت ویژه‌ای برخوردار است. امنیت اطلاعات در محیط‌های مجازی و فضای سایبر بعنوان مهمترین الزام در کاربری توسعه‌ای و فراگیر فن آوری اطلاعات و ارتباطات می‌باشد. اگر چه امنیت مطلق در محیط‌های واقعی و مجازی امکان‌پذیر نیست ولی ایجاد سطحی از امنیت که به اندازه کافی و متناسب با نیازها و سرمایه‌گذاری‌ها انجام شده باشد تقریباً در همه شرایط محیطی 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 آسیب‌پذیری 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 جنایات سایبری غالباً نیاز بیشتری به اشتراک گذاشتن دانش فنی، مهارت‌ها و اطلاعات مربوط به جرایم سایبری 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 جرایم سایبری 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 دهند. لازم به ذکر می‌باشد هرگونه مقابله با هنجار شکنی‌های سایبری در جهت برقراری موازین اخلاقی سایبری، می‌تواند با ایرادات جدی حقوقی و اخلاقی مواجه گردد. مداخله و مشارکت چندین 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 سایبری 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. سیاست جنایی در مقابله با جرایم سایبری 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.