

# کلاهبرداری سایبری در

## حقوق کیفری ایران

(با تأکید بر رایحه اینترنتی و تروریسم سایبری در حقوق کیفری آمریکا)

م. ل. ف.

عبداله یوسفی

(مدرس دانشگاه)

انتشارات هوشمند تدبیر

h

انتشارات هوشمند تدبیر

سرشناسه	:	میرفردی، عبدالله، ۱۳۶۱-
عنوان و نام پدیدآور	:	کلاهبرداری سایبری در حقوق کیفری ایران (با تاکید بر جرایم اینترنتی و تروریسم سایبری در حقوق کیفری آمریکا) // مولف عبدالله میرفردی.
مشخصات نشر	:	تهران : هوشمند تدبیر، ۱۳۹۷.
مشخصات ظاهری	:	۳۴۸ ص.
شابک	:	۹۷۸-۶۰۰-۴۱۸-۱۷۹-۲ :
وضعیت فهرست نویسی	:	فیا
موضوع	:	جرایم کامپیوتری -- قوانین و مقررات -- ایران
موضوع	:	Computer crimes -- Law and legislation-- Iran
موضوع	:	جرایم کامپیوتری -- قوانین و مقررات -- ایالات متحده
موضوع	:	-- Law and legislation -- United Computer crimes
موضوع	:	تروریسم رایانه‌ای -- قوانین و مقررات -- ایالات متحده
موضوع	:	Cyberterrorism -- Law and legislation -- United States
موضوع	:	شبکه‌های کامپیوتری -- ایران -- تدابیر ایمنی
موضوع	:	Computer networks -- Security measures -- Iran
موضوع	:	شبکه‌های کامپیوتری -- ایالات متحده -- تدابیر ایمنی
موضوع	:	Computer networks -- Security measures--United States
موضوع	:	حقوق تطبیقی
موضوع	:	Comparative law
موضوع	:	۹۱۳۹۷/۵۲۰ (MH)
رده بندی کنگره	:	۳۴۳/۵۵۰۹.۴۴
رده بندی دیویی	:	۵۰۲۶۶۵۵
شماره کتابشناسی ملی	:	

نام کتاب ..... کلاهبرداری سایبری در حقوق کیفری ایران

(با تاکید بر جرایم اینترنتی و تروریسم سایبری در حقوق کیفری آمریکا)

مولف ..... عبدالله میرفردی

نوبت چاپ ..... اول ۱۳۹۷

تیراژ ..... ۱۰۰ نسخه

ناشر ..... انتشارات هوشمند تدبیر

مدیرمسئول نشر ..... محمد قجر

قیمت ..... ۱۸۰۰۰۰ ریال

شابک ..... ۹۷۸-۶۰۰-۴۱۸-۱۷۹-۲

آدرس و شماره تلفن ناشر: تهران، خیابان انقلاب، بین خیابان دانشگاه و خیابان ابوریحان، پلاک ۱۱۷۶، طبقه اول

تلفن : ۶۶۴۷۹۶۶۵ و ۹۱۳۳۸۶۱۳۶۷

## فهرست مطالب

صفحه	عنوان
۲۳	پیشگفتار.....
۲۷	مقدمه.....
۳۱	فصل اول: مفاهیم و مبانی.....
۳۲	۱-۱- مفاهیم.....
۳۲	۱-۱-۱- مفهوم کلاهبرداری اینترنتی:.....
۳۲	۱-۱-۲- مفهوم اینترنت.....
۳۲	۱-۱-۳- مفهوم کارهای رایانه ای.....
۳۳	۱-۱-۴- تعریف جرم.....
۳۳	۱-۱-۵- تعریف فضای سایبر.....
۳۴	۱-۱-۶- مفهوم جرایم رایانه ای.....
۳۵	۱-۱-۷- مفهوم فضای سایبر.....
۳۶	۱-۱-۸- مفهوم پلیس سایبر.....
۳۷	۱-۱-۹- تعریف تروریسم سایبری.....
۳۸	فصل دوم: مبانی نظری جرایم رایانه ای.....
۳۹	۲- مبانی نظری جرایم رایانه ای.....
۴۰	۲-۱- اهداف کلی پلیس سایبر:.....
۴۰	۲-۱-۲- پلیس اداری.....
۴۰	۲-۱-۳- پلیس قضایی.....

- ۴۱..... ۱-۲-۴-عنصر تشکیل دهنده جرم کلاهبرداری:
- ۴۲..... ۱-۲-۵-مجازات مرتکب جرم کلاهبرداری
- ۴۳..... ۱-۲-۶-دلایل وقوع جرم کلاهبرداری
- ۴۴..... ۲-۲-مبانی نظری تحقیق
- ۴۴..... ۱-۲-۲-خطرات مختلف حقوقدانان در موضوع کلاهبرداری
- ۴۶..... ۲-۲-۲-کلاهبرداری رایانه ای
- ۴۸..... ۳-۲-۲-مجازات های قانونی جرم کلاهبرداری رایانه ای
- ۴۹..... ۲-۲-۳-عناصر تشکیلی دهنده جرم کلاهبرداری
- ۴۹..... ۱-۳-۲-۲-عنصر قانونی
- ۴۹..... ۲-۳-۲-۲-عنصر مادی
- ۵۰..... ۳-۳-۲-۲-عنصر روانی
- ۵۱..... ۴-۲-۲-انواع جرایم رایانه ای
- ۵۴..... ۵-۲-۲-پولشویی کامپیوتری
- ۵۵..... ۴-۴-۲-جاسوسی کامپیوتری
- ۵۵..... ۶-۲-۲-جرایم سایبری
- ۵۶..... ۳-۲-ماهیت جرایم سایبری:
- ۵۸..... ۱-۳-۲-سه نسل از جرایم سایبری:
- ۵۹..... ۲-۳-۲-جرایم کامپیوتر افراد خارج از کشور ایران:
- ۵۹..... ۱-۲-۳-۲-نمونه هایی از جرایم اینترنتی
- ۶۰..... ۲-۳-۲-آمار جرایم اینترنتی در ایران:

- ۶۰-۳-۳-۲: شاخه های حقوقی جرایم سایبری .....
- ۶۱-۴-۲: صلاحیت برون مرزی در قانون مجازات اسلامی .....
- ۶۱-۴-۲-۱: صلاحیت درون مرزی مراجع کیفری .....
- ۶۳-۴-۲-نامعین بودن حیطه های جغرافیایی .....
- ۶۵-۴-۲-۱: تعیین محل ارتکاب جرم سایبر : .....
- ۶۶-۴-۲-۲: حل تعارض صلاحیت ها: .....
- ۶۷-۴-۲-۳: جرم سایبر: جرم آینده .....
- ۶۸-۴-۲-۳: عدالت انفورماتیک؛ مجرمان سایبر .....
- ۶۹-۵-۲: معرفی و شناخت بستر فضای تولید و تبادل اطلاعات اینترنتی (فتا) .....
- ۷۱-۵-۲-۱: ضرورت به کارگیری فناوری اطلاعات اینترنتی در پلیس فتا .....
- ۷۵-۵-۲-۲: فرصت های پلیس از سنای حازر و پیشگیری از جرایم سایبری .....
- ۸۰-۵-۲-۳: نقش پلیس در پیشگیری اجتماعی از جرایم اینترنتی .....
- ۸۲-۵-۲-۳-۱: پلیس و پیشگیری اجتماعی جامعه مدار از جرایم اینترنتی .....
- ۸۸-۵-۲-۳-۲: پلیس و پیشگیری اجتماعی رشد مدار از جرایم سایبری .....
- ۹۲-۵-۲-۳-۳: نقش پلیس در پیشگیری وضعی از جرایم سایبری .....
- ۹۳-۵-۲-۳-۱: تدابیر نظارتی .....
- ۹۴-۵-۲-۳-۲: تدابیر صدور مجوز .....
- ۹۵-۵-۲-۳-۳: ناشناس کننده ها و رمزنگارها .....
- ۹۶-۵-۲-۳-۴: تدابیر سالب دسترسی (فیلترینگ) .....
- ۹۹: فصل سوم: جرم کلاهبرداری در حقوق کیفری ایران .....

- ۱-۳-جرم کلاهبرداری :..... ۱۰۰
- ۱-۱-۳-روند تاریخی جرم کلاهبرداری..... ۱۰۱
- ۲-۱-۳-کلاهبرداری از دیدگاه فقه اسلامی..... ۱۰۲
- ۳-۱-۳-کلاهبرداری از دیدگاه حقوقی..... ۱۰۲
- ۴-۱-۳-کلاهبرداری از دیدگاه قانون مجازات اسلامی..... ۱۰۳
- ۵-۱-۳-نبه مومی جرم کلاهبرداری..... ۱۰۵
- ۶-۱-۳-رور زمان در جرم کلاهبرداری..... ۱۰۶
- ۲-۳-عناصر تشکیل دهنده جرم کلاهبرداری..... ۱۰۷
- ۱-۲-۳-عناصر قانونی..... ۱۰۷
- ۲-۲-۳-عناصر مادی..... ۱۰۹
- ۱-۲-۲-۳-رفتار مادی فیزیکی..... ۱۰۹
- ۲-۲-۲-۳-شرایط و اوضاع و احوال لازم برای تحقق جرم کلاهبرداری..... ۱۱۰
- ۳-۳-مصادیق وسایل متقلبانه در کلاهبرداری ساده..... ۱۱۳
- ۱-۳-۳-فریب دادن مردم به وجود شرکتها یا تجارت خانه ها یا کا.خانه ها یا مؤسسات موهوم..... ۱۱۳
- ۲-۳-۳-فریب دادن مردم بهداشتن اموال و اختیارات..... ۱۱۴
- ۳-۳-۳-امیدوار کردن مردم به امور غیر واقع..... ۱۱۴
- ۴-۳-۳-ترساندن مردم از حوادث و پیش آمدهای غیر واقع..... ۱۱۵
- ۵-۳-۳-اختیار اسم و یا عنوان مجعول..... ۱۱۵
- ۶-۳-۳-وسایل تقلبی دیگر..... ۱۱۶
- ۴-۳-مصادیق وسایل متقلبانه در کلاهبرداری مشدد (موارد تشدید مجازات کلاهبرداری)..... ۱۱۸

- ۱۲۰-۱-۴-۳- اغفال و فریب قربانی جرم.....
- ۱۲۲-۲-۴-۳- تعلق مال برده شده به غیر (دیگری).....
- ۱۲۳-۳-۴-۳- نتیجه حاصله از رفتار متهم.....
- ۱۲۵-۵-۳- شروع به جرم کلاهبرداری.....
- ۱۲۷-۱-۵-۳- عنصر معنوی (روانی).....
- ۱۳۰-۲-۵-۳- صور مختلف همکاری در ارتکاب جرم کلاهبرداری.....
- ۱۳۰-۱-۲-۵-۳- شرکت در کلاهبرداری.....
- ۱۳۱-۲-۵-۳- معاونت در کلاهبرداری.....
- ۱۳۶-۳-۲-۵-۳- رهبر، شبکه‌ها، مجرمانه در جرم کلاهبرداری.....
- ۱۳۷-۴-۲-۵-۳- صور خاص جرم کلاهبرداری (جرایم در حکم کلاهبرداری).....
- ۱۳۸-۳-۵-۳- ورشکستگی به تقصیر یا تقلب.....
- ۱۳۹-۱-۳-۵-۳- ورشکستگی عادی:.....
- ۱۴۰-۲-۳-۵-۳- ورشکستگی تقصیر:.....
- ۱۴۳-۳-۳-۵-۳- ورشکستگی به تقلب:.....
- ۱۴۵-۶- نحوه رسیدگی و پیگیری جرم کلاهبرداری اینترنتی.....
- ۱۴۶-۷- جرایم سایبری و کلاهبرداری اینترنتی.....
- ۱۴۷- فصل چهارم: تحلیل و ارزیابی جرایم اینترنتی (سایبری).....
- ۱۴۸-۱-۴- تحلیل و ارزیابی جرایم اینترنتی (سایبری).....
- ۱۵۰-۱-۱-۴- انحراف و خرده فرهنگ های مجرمانه در فضای سایبر (قمار اینترنتی).....
- ۱۵۱-۱-۱-۴- آنتیگوا.....

- ۱۵۲.....۴-۱-۱-۲-۱-۲-برونده جی کوهن (۲۰۰۱).....
- ۱۵۳.....۴-۱-۱-۳-۱-۳-سازمان تجارت جهانی.....
- ۱۵۷.....۴-۱-۱-۴-۱-۴-اعضای هیئت حل اختلاف.....
- ۱۶۰.....۴-۱-۱-۴-۱-۴-حکم هیئت استینافی.....
- ۱۶۳.....۴-۱-۱-۲-۴-۲-ظهار نظر اتحادیه اروپا به عنوان شخص ثالث.....
- ۱۶۶.....۴-۲-۴-۲-۴-مراحت سایبری گونه شناسی، علت شناسی و قربانیان.....
- ۱۶۸.....۴-۲-۴-۱-۲-۴-مراحت سایبری بر خط در مقابل مزاحمت سنتی آفلاین.....
- ۱۷۳.....۴-۲-۲-۲-۲-اینترنت، به e دان، سان های تجاوز بر خط.....
- ۱۷۴.....۴-۲-۲-۱-۲-۲-نفوذ/شیوع.....
- ۱۷۵.....۴-۲-۲-۲-۲-۲-رایانامه به مثابه ابزار و ادت.....
- ۱۷۷.....۴-۳-۴-۳-۴-گونه شناسی و علت شناسی مزاحمت سایبری و قربانیان گونه شناسی مزاحمت سایبری.....
- ۱۷۹.....۴-۳-۱-۳-۴-علت شناسی مزاحمت توضیحات روانشناسی ممکن.....
- ۱۷۹.....۴-۳-۲-۳-۴-نظریه یادگیری اجتماعی.....
- ۱۸۰.....۴-۳-۳-۳-۴-نظریه انتخاب عقلانی.....
- ۱۸۲.....۴-۴-۴-۳-۴-قربانیان مزاحمت سایبری.....
- ۱۸۴.....۴-۴-۱-۴-۴-مسائل قانونی و اجتماعی مربوط به مزاحمت سایبری چالش.....
- ۱۸۴.....اجرای قانون.....
- ۱۸۵.....۴-۴-۲-۴-۴-قانون گذاری علیه مزاحمت در سطح ایالات متحده.....
- ۱۸۷.....۴-۴-۳-۴-۴-قوانین موضوعه ایالتی در خصوص مزاحمت سایبری.....
- ۱۸۷.....۴-۴-۴-۴-۴-مداخله و پیشگیری اجتماعی.....
- ۱۸۹.....۴-۴-۵-۴-۴-شبکه های اجتماعی بر خط و زنان بزه دیده.....



- ۱۹۱-۱-۵-۴-اجتماعی سازی مجازی و رشد جرایم فرا تکنولوژی.....
- ۱۹۲-۲-۵-۴-مشکل مفهوم سازی جرایم سایبری در شبکه اجتماعی.....
- فصل پنجم تحلیل و ارزیابی کلاهبرداری های ناشی از تروریسم سایبری در حقوق کیفری ایران و آمریکا.....
- ۱۹۷-۱-۵-۱-ماهیت مسئولیت کیفری در تروریسم.....
- ۲۰۰-۲-۵-ویژگیهای تروریسم سایبری.....
- ۲۰۰-۱-۲-۵-نام خود بودن.....
- ۲۰۱-۲-۵-نام اوس بودن.....
- ۲۰۱-۳-۲-۵-توسعه تغییر پذیری.....
- ۲۰۲-۴-۲-۵-پیچیدگی و تخصص بودن.....
- ۲۰۲-۵-۲-۵-دسترسی آسان و سریع.....
- ۲۰۲-۶-۲-۵-استفاده گسترده از فضای سایبر.....
- ۲۰۳-۳-۵-سیر تاریخی ، مبانی و علت شناسی مجازات تروریسم سایبری.....
- ۲۰۳-۱-۳-۵-سیر تاریخی تروریسم سایبری در قوانین کیفری.....
- ۲۰۴-۱-۱-۳-۵-تروریسم سایبری در قوانین کیفری ایران.....
- ۲۰۵-۲-۱-۳-۵-تروریسم سایبری در قوانین کیفری آمریکا.....
- ۲۰۷-۴-۵-انواع و گونه های تروریسم.....
- ۲۰۹-۱-۴-۵-تروریسم پیشامدرن ( سنتی).....
- ۲۱۰-۲-۴-۵-تروریسم مدرن.....
- ۲۱۰-۳-۴-۵-تروریسم پسامدرن.....
- ۲۱۱-۴-۴-۵-تروریسم در عصر اتم و جنگ اجتماعی.....

- ۲۱۲ ..... ۱-۴-۴-۵- تروریسم مجازی ( سایر تروریسم )
- ۲۱۳ ..... ۲-۴-۴-۵- تروریسم دولتی و خارجی
- ۲۱۳ ..... ۳-۴-۴-۵- تروریسم مذهبی
- ۲۱۴ ..... ۴-۴-۴-۵- تروریسم نوین
- ۲۱۵ ..... ۵-۴-۴-۵- تروریسم بین المللی
- ۲۱۶ ..... ۵-۵- ریفه اصلی سایر تروریسم
- ۲۱۶ ..... ۱-۵-۵- استفاده از تهدید به استفاده از خشونت، به صورت غیرقانونی و نامأنوس
- ۲۱۷ ..... ۲-۵-۵- انتخاب و استخدام از بزه‌دیدگان بی دفاع
- ۲۱۷ ..... ۳-۵-۵- ایجاد رعب و وحشت
- ۲۱۷ ..... ۴-۵-۵- سازمان‌یافتگی عملیات‌های تروریستی
- ۲۱۸ ..... ۵-۵-۵- استفاده از ابزارها و شیوه‌های مدرن
- ۲۱۸ ..... ۶-۵- ارکان و آیین دادرسی جرایم تروریسم سایبری رویکرد به سیستم حقوقی کیفری ایران
- ۲۱۹ ..... ۱-۶-۵- ارکان جرایم تروریسم سایبری
- ۲۱۹ ..... ۱-۶-۵- رکن قانونی
- ۲۲۰ ..... ۲-۶-۵- رکن مادی
- ۲۲۰ ..... ۱-۲-۶-۵- رفتار مجرمانه
- ۲۲۰ ..... ۲-۲-۶-۵- موضوع جرم
- ۲۲۰ ..... ۳-۲-۶-۵- نتیجه مجرمانه
- ۲۲۱ ..... ۳-۶-۵- رکن روانی
- ۲۲۲ ..... ۷-۵- ضمانت اجرای کیفری تروریسم سایبر در مقررات کیفری ایران

- ۲۲۳ ..... ۱-۷-۵- سایبر تروریسم و جرائم علیه امنیت
- ۲۲۴ ..... ۲-۷-۵- سایبر تروریسم و محاربه
- ۲۲۸ ..... ۳-۷-۵- سایبر تروریسم و افساد فی الارض
- ۲۲۹ ..... ۴-۷-۵- سایبر تروریسم و جاسوسی سایبری
- ۲۳۱ ..... ۵-۷-۵- سایبر تروریسم و جرایم علیه مذهب
- ۲۳۲ ..... ۸-۵- آیین کشف و دادرسی تروریسم سایبری
- ۲۳۳ ..... ۹-۵- مراد کشف جرایم مربوط به تروریسم سایبری
- ۲۳۳ ..... ۱-۹-۵- اصول اولیه حاکم بر تحقیقات مجازی
- ۲۳۴ ..... ۲-۹-۵- جمع آوری و حفظ ادله
- ۲۳۵ ..... ۳-۹-۵- اداره صحنه جرم
- ۲۳۵ ..... ۴-۹-۵- تهیه صورت جلسه ثبت جزئیات
- ۲۳۷ ..... ۵-۹-۵- روند کشف جرایم در داده‌های در حال مباد
- ۲۳۷ ..... ۶-۹-۵- آیین دادرسی کیفری مربوط به جرم تروریسم سایبری
- ۲۳۸ ..... ۷-۹-۵- تشخیص دادگاه داخلی صالح در تروریسم سایبری
- ۲۳۹ ..... ۸-۹-۵- گسترش صلاحیت کیفری
- ۲۴۴ ..... ۱۰-۵- راهکارهای پیشگیری و حمایت از بزه‌دیدگان تروریسم سایبری در حقیقت کیفری ایران
- ۲۴۵ ..... ۱-۱۰-۵- پیشگیری واکنشی یا کیفری
- ۲۴۶ ..... ۲-۱۰-۵- قانون جرایم رایانه‌ای مصوب ۱۳۸۸
- ۲۵۱ ..... ۳-۱۰-۵- قانون تجارت الکترونیکی مصوب ۱۳۸۲
- ۲۵۲ ..... ۴-۱۰-۵- قانون مجازات نیروهای مسلح مصوب ۱۳۸۲

- ۲۵۲ ..... ۵-۱۰-۵- قانون مجازات اسلامی مصوب ۱۳۷۰
- ۲۵۴ ..... ۶-۱۰-۵- سایر قوانین و مقررات موجود
- ۲۵۴ ..... ۱۱-۵- پیشگیری غیر کیفری
- ۲۵۵ ..... ۱-۱۱-۵- پیشگیری اجتماعی
- ۲۵۵ ..... ۲-۱۱-۵- پیشگیری اجتماعی جامعه مدار
- ۲۵۶ ..... ۳-۱۱-۵- برنامه جامع توسعه تجارت الکترونیکی مصوب ۱۳۸۴
- ۲۵۷ ..... ۴-۱۱-۵- برنامه چهارم توسعه مرتبط با فناوری اطلاعات
- ۲۵۷ ..... ۵-۱۱-۵- قانون برنامه پنجم توسعه جمهوری اسلامی ایران
- ۲۵۸ ..... ۶-۱۱-۵- مقررات و ضوابط شبکه‌های اطلاع رسانی رایانه‌ای
- ۲۵۸ ..... ۷-۱۱-۵- ابلاغیه مقام معظم رهبری درباره سیاست‌های کلی شبکه‌های اطلاع رسانی رایانه‌ای
- ۲۵۹ ..... ۸-۱۱-۵- مصوبه شورای عالی امنیت ملی در خصوص اتوماسیون نظام اداری و اتصال به شبکه جهانی اطلاع رسانی
- ۲۵۹ ..... ۹-۱۱-۵- سیاست تجارت الکترونیکی جمهوری اسلامی ایران
- ۲۶۰ ..... ۱۰-۱۱-۵- سند راهبردی امنیت فضای تبادل اطلاعات مصوب ۱۳۸۴
- ۲۶۰ ..... ۱۲-۵- پیشگیری اجتماعی رشد مدار
- ۲۶۱ ..... ۱-۱۲-۵- پیشگیری وضعی
- ۲۶۲ ..... ۲-۱۲-۵- اقدامات فنی
- ۲۶۲ ..... ۳-۱۲-۵- تدابیر فنی پیشگیرانه در سازمان‌ها و ادارات کشور
- ۲۶۳ ..... ۴-۱۲-۵- صب و استقرار دیوار آتشین
- ۲۶۴ ..... ۵-۱۲-۵- سیستم‌های تشخیص نفوذ
- ۲۶۵ ..... ۶-۱۲-۵- سیستم‌های پیشگیری از نفوذ

- ۲۶۶ ..... ۵-۱۲-۷- استفاده از برنامه‌های ضد ویروس
- ۲۶۶ ..... ۵-۱۲-۸- مستقل نمودن شبکه‌های کنترل و اداری
- ۲۶۷ ..... ۵-۱۲-۹- انجام سنجش نفوذپذیری
- ۲۶۷ ..... ۵-۱۲-۱۰- اقدامات سازمان‌ها و مؤسسات
- ۲۶۸ ..... ۵-۱۲-۱۱- وزارت ارتباطات و فناوری اطلاعات
- ۲۶۹ ..... ۵-۱۲-۱۲- سازمان تنظیم مقررات و ارتباطات رادیویی
- ۲۶۹ ..... ۵-۱۲-۱۳- حرکت ارتباطات زیرساخت
- ۲۷۰ ..... ۵-۱۲-۱۴- سازمان فناوری اطلاعات
- ۲۷۰ ..... ۵-۱۲-۱۵- کارگروه مبارزه با ویروس‌های صنعتی جاسوسی
- ۲۷۰ ..... ۵-۱۲-۱۶- قرارگاه دفاع سایبری
- ۲۷۱ ..... ۵-۱۲-۱۷- مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای (ماهر)
- ۲۷۲ ..... ۵-۱۳- پلیس فضای تولید و تبادل اطلاعات ناجا
- ۲۷۲ ..... ۵-۱۳-۱- سازمان بررسی جرایم سازمان یافتگان
- ۲۷۴ ..... ۵-۱۴- بازارهای پیشگیرانه و تدابیر کیفی و غیرکیفی تروریسم سایبری در آمریکا
- ۲۷۷ ..... ۵-۱۴-۱- قانون امنیت سایبری در آمریکا در تروریسم
- ۲۷۷ ..... ۵-۱۴-۲- سابقه تقنینی تروریسم سایبری
- ۲۸۲ ..... ۵-۱۴-۳- تروریسم رایانه‌ای در سایه تلاش‌های بین‌المللی آمریکا
- ۲۸۳ ..... ۵-۱۴-۴- کشف و دادرسی تروریسم سایبری
- ۲۸۵ ..... ۵-۱۵- تقسیم بندی بزه‌دیدگان تروریسم سایبری
- ۲۸۵ ..... ۵-۱۵-۱- بزه‌دیدگان حقیقی تروریسم سایبری

- ۲۸۸.....۲-۱۵-۵-بزه‌دیدگان حقوقی تروریسم سایبری
- ۲۸۸.....۱۶-۵-طبقه بندی تروریسم سایبری و افعال مرتبط با آن در آمریکا
- ۲۸۹.....۱-۱۶-۵-جنگ اطلاعاتی
- ۲۹۰.....۲-۱۶-۵-جنگ سایبری
- ۲۹۰.....۳-۱۶-۵-جاسوسی سایبری
- ۲۹۱.....۱-۱۶-۵-خرابکاری سایبری
- ۲۹۱.....۵-۱۶-۵-اختلال ساختی
- ۲۹۱.....۶-۱۶-۵-دفعه‌های سایبری
- ۲۹۲.....۱-۶-۱۶-۵-حملات سایبری
- ۲۹۲.....۲-۶-۱۶-۵-هزینه و عواقب حملات سایبری
- ۲۹۲.....۳-۶-۱۶-۵-تقسیم بندی حملات سایبری
- ۲۹۳.....۱۷-۵-حملات ویروس‌ها، کرم‌ها و تروجان‌ها
- ۲۹۳.....۱-۱۷-۵-حملات خودی
- ۲۹۳.....۲-۱۷-۵-حملات توزیع شده انکار سرویس
- ۲۹۴.....۳-۱۷-۵-نفوذ غیر مجاز
- ۲۹۴.....۱۸-۵-تدابیر کیفی و غیرکیفری جرایم نرم افزاری تروریسم سایبری
- ۲۹۵.....۱۹-۵-راهکارهای کیفی در تروریسم سایبری
- ۲۹۷.....۲۰-۵-حمایت کیفی از بزه‌دیدگان تروریسم سایبری
- ۳۰۰.....۱-۲۰-۵-اینترانت
- ۳۰۱.....۲-۲۰-۵-یافتن خلأهای امنیتی

- ۳۰۳..... ۲۱-۵- تدابیر سازمانی در امریکا
- ۳۰۴..... ۱-۲۱-۵- تأسیس نهادهای تخصصی پیشگیری و کنترل تروریسم سایبری در امریکا
- ۳۰۴..... ۲-۲۱-۵- تعیین مسوولیت ارائه دهندگان خدمات اینترنتی
- ۳۰۶..... ۳-۲۱-۵- بازرسی سیستمهای اطلاعاتی
- ۳۰۸..... ۴-۲۱-۵- پلیس رایانه‌ای
- ۳۰۹..... ۶-۲۱-۵- افزایش آگاهی و مشارکت مردمی
- ۳۱۰..... ۲۲-۵- کنسپشن سازمان کشورهای آمریکایی راجع به پیشگیری و مجازات اعمال تروریستی
- ۳۱۱..... نتایج پژوهش
- ۳۲۲..... پیشنهادات کاربردی
- ۳۲۵..... پیشنهادات کاربردی جریان رایانه‌ای
- ۳۲۲..... منابع و مأخذ
- ۳۲۲..... کتب
- ۳۳۸..... مقالات و نشریات
- ۳۴۶..... پایان نامه ها
- ۳۴۷..... قوانین
- ۳۴۸..... سایت ها
- ۳۴۸..... منابع خارجی (کتب و مقالات)

## پیشگفتار

متصل کردن رایانه های بی شمار در سراسر دنیا به یکدیگر منجر به پیشرفتهای حیرت‌آوری در زمینه های آموزشی، فناوری و اقتصاد شده است. نامه‌های الکترونیک یا ایمیل، به ما امکان می‌دهد که ظرف چند ثانیه با دیگران ارتباط برقرار کنیم. "اتاق های گپ" و "گپ‌های مبتنی بر اینترنت" (IRC) به ما امکان می‌دهد که به وسیله صفحه کلید، بطور همزمان با افراد متعددی در سراسر دنیا ارتباط برقرار کنیم. اینترنت به خودی خود گستره‌ای از اطلاعات بسیار متنوع است و بهانه پیدا نکردن یک مفهوم در دائره المعارف را از دانش‌آموزان آینده سلب می‌کند اما در عین حال شبکه جهان گستر باعث شده است که انواع حیرت‌انگیزی از جرایم (رفتارها، کیفری) پدید آید، که برخی از این جرایم عبارتند از:

اختلاس، کلاهبرداری یا جاسوسی صنعتی (سرقت اطلاعات محرمانه یک شرکت) تنها بخش کوچکی از اهداف احتمالی هکرها می‌باشد. جاسوسی سایبر همانطور که بین شرکت‌ها وجود دارد، میان کشورها نیز در جریان است. بنابراین امنیت ملی ما را با مخاطره مواجه می‌کند. تروریسم‌های سایبر، توسعه رایانه‌ای وحشتناک دیگری است که شاید بیش از یک میلیون‌ها انسان را در سراسر دنیا تهدید کند. هیچ بحثی در این نیست که آنچه هکرها انجام می‌دهند، نفوذ که غیر قانونی است، مخاطره آمیز نیز می‌باشد. فریک‌های تلفن. شکل دیگری از جرایم رایانه‌ای را "فریک دی تلفن" مرتکب می‌شوند، فریک‌ها بجای دسترسی به سیستم‌های رایانه‌ای، از طریق خطوط تلفن در دنیای سایبر گشت می‌زنند. فریک‌ها از میان اولین هکرها در دهه ۱۹۷۰ پدید آمدند. اما خود رایانه‌ها تنها یک ابزارند. این افراد هستند که مرتکب جرایم سایبر می‌شوند و مردم نیز مانند فایل‌های رایانه‌ای می‌توانند به عنوان منابع اطلاعات حفاظت شده یا حساس مورد استفاده قرار گیرند. نکته خوبی که در این میان وجود دارد آن است که ما هم نیز می‌توانند از جرایم سایبر جلوگیری کنند. هر قدر ما بیشتر درباره انواع مختلف جرایم سایبر و ابزارهای آنها، برای جلوگیری از آن ایجاد شده است بدانیم، امنیت بیشتری خواهیم داشت. اصطلاح جرم رایانه‌ای (جرایم) را شامل می‌شود که بوسیله یک رایانه، درون یک فضای سایبر و علیه یک رایانه ارتکاب می‌یابد. بعضی از این جرایم کاملاً جدید هستند در حالیکه جرایم دیگر، جرایم قدیمی تری هستند که از رایانه به عنوان ابزار استفاده می‌کنند. رشد دائم و تنوع بی پایان جرایم سایبر، تدوین قوانینی با احاطه مناسب بر جرایم سایبر جدید را دشوار ساخته است. بعضی جرایم مانند اختلاس، کلاهبرداری و جعل سند توسط سایبر و جاسوسی سایبر نسبتاً جدید هستند. برای این جرایم جدیدتر، نص قوانین موجود گاهی اوقات اجازه تحت پیگرد قرار دادن آنچه بطور وضوح جز رفتار کیفری محسوب می‌شود را نمی‌دهد.



یکی از مهم ترین و پیچیده ترین جرایم مالی، جرم کلاهبرداری خصوصاً کلاهبرداری های اینترنتی است که هرروزه به صورت متنوع و تکامل یافته در جوامع مختلف از جمله کشور ما شایع است. آنچه جرم کلاهبرداری را از سایر جرایم علیه اموال متمایز می سازد، این است که در اکثر این جرایم، مال بدون رضایت یا آگاهی صاحب مال و یا حتی گاه به دلیل توسل مجرم به زور و اعمال خشونت آمیز، از قربانی جرم به مجرم منتقل می گردد، در حالی که در جرم کلاهبرداری، فرد کلاهبردار به گونه ای عمل می کند که مالک یا متصرف مال، فریب خورده و از روی میل و رضایت به امید کسب ثروت و منفعت، مال خود را اختیار مجرم قرار می دهد. اغفال و فریب قربانی جرم، نیاز به انجام مانورهای متقلبانه و عملیات اجرایی خاصی از سوی مجرم دارد. ممکن است جرم کلاهبرداری توسط افرادی که دارای مناصب اجتماعی، اقتصادی، یا حتی دولتی هستند صورت گیرد. به همین دلیل جرم کلاهبرداری را از زمره «جرایم یقه سفیدها» محسوب کرده اند. در واقع این جرم بیش از آن که جرم فقرا و نیازمندان باشد، جرم ثروتمندان محسوب می گردد.

امروزه جرم کلاهبرداری به رهبرهای سنتی و قدیمی آن محدود نمی گردد و دارای وسعت و پیچیدگی های فراوانی شده است. با پیشرفت علوم و تکنولوژی و تسهیل ابزارهایی ارتباطی، راه های ارتکاب جرایم از جمله کلاهبرداری نیز به هم پیوسته تر شده است. ایران با شرفیافته کرده و موجبات تسهیل آن فراهم گشته است. به طوری که یکی از پیچیده ترین و مرموز ترین انواع کلاهبرداری در دنیای امروزه، کلاهبرداری رایانه ای (الکترونیک) است که در کشورهای مختلف از جمله کشور ما سالیانه پرونده های زیادی از این نوع کلاهبرداری به مراجع قضایی ارجاع می گردد. البته کلاهبرداری های رایانه ای اشکال پیچیده و مختلفی است که به تفصیل به بررسی آنها پرداخته شده است. پیچیدگی های این جرم از یک سو و نداشتن آگاهی و اطلاعات لازم از جانب مردم، باعث ایجاد مشکلات فراوانی برای جامعه شده است. بنابراین لزوم وجود کتابی تخصصی و تفصیلی در مورد جرم کلاهبرداری در جهت آموزش به جامعه ضروری به نظر می آید.

تروریسم سایبری یکی از پیچیده ترین و خطرناک ترین انواع جرایم اینترنتی است. برآیندی است که در آن، مجموعه ای از برنامه ریزی ها و تهدیدها به وسیله اینترنت منجر به ایجاد آسیب و تخریب در جهان واقعی و از بین رفتن امنیت روانی و فیزیکی افراد جامعه می شود. به دلیل رشد روزافزون ساختار اقتصادی و خدمات رسانی بسیاری از کشورها، مبتنی بر فناوری های اطلاعاتی و ارتباطی، دنیای ما به قدری به دادوستد اطلاعات وابسته شده است، که اختلال یا وقفه در آن، چرخ صنعت و زندگی روزمره را از حرکت بازمی دارد. در این رابطه ایجاد خلل در رآکتورهای هسته ای، سیستم های اطلاعاتی فرودگاه ها و ترمینال ها و تأسیسات عمومی مثل برق، آب و فاضلاب، می تواند بسیار فاجعه آمیز باشد.

در حقوق کیفری آمریکا تروریسم سایبری، حاصل تلاقی تروریسم و فضای مجازی است. در این روش، تروریست‌ها با هزینه کم و با استفاده از یک رایانه شخصی متصل به اینترنت می‌توانند به اقدامات تروریستی دست بزنند. همچنین فضای مجازی این امکان را برای تروریست‌ها فراهم می‌کند که همانند دیگر کاربران اینترنت، به عنوان کاربر مهمان و با استفاده از اسامی مستعار وارد سایت مورد نظرشان شوند و با پنهان سازی هویت، دست به اقدامات تروریستی بزنند، بدین گونه امکان ردیابی آن‌ها برای نیروهای پلیس و امنیتی دشوارتر خواهد بود. مزیت دیگری که فضای مجازی، برای تروریست‌ها ایجاد کرده است، امکان هدایت از راه دور می‌باشد که آموزش فیزیکی، فشار روانی و خطر مرگ کمتری را به همراه دارد. اصولاً ارائه یک تعریف جامع و قابل قبول در روابط بین‌الملل برای واژه «تروریسم» دشوار است.

زیرا اعمال تروریستی در بسیاری از مواقع حالت دو وجهی دارد. یعنی ممکن است عمل یک فرد از نظر یک شخص تروریستی تلقی شود و از نظر دیگری شخص مزبور یک مبارز راه آزادی محسوب شود. با این حال برای تعریف تروریسم می‌توان به تعریفی که سازمان ملل متحد در سال ۱۹۹۲ منتشر کرده است، اشاره کرد که بیان می‌دارد: «روش اعمال تروریستی از طریق خشونت که به وسیله بازیگران دولتی، گروه‌ها یا افراد (نیمه) مخفی که به دلایل سیاسی، جنسیتی یا مذهبی انجام می‌شود». در قوانین آمریکا «اقدام تروریستی» به معنی «تشکیل، معاونت یا مشارکت در یک عمل خصمانه غیرموجه یا بی‌پروایانه با بی‌تفاوتی کامل نسبت به خطر کشتن یا ایراد صدمه شدید جسمانی به سائمی که در مخاصمات مسلحانه شرکت ندارند» به کار رفته است. این امکان وجود دارد که حملات تروریستی از سوی یک دولت از سوی افرادی وابسته به دولت‌ها و کشورهای دیگر واقع گردد و یا ممکن است فرد بزه دیده از نقض قوانین بین‌المللی از سوی یک دولت در نهادهای بین‌المللی طرح شکایت کند. این مراجع در صورتی شکایت سیدگی می‌کنند که حداقل فرد شاکی تبعه‌ی دولتی باشد که آن دولت عضو اساستامه یا کنوانسیون می‌باشد نهادهای بین‌المللی باشد. با عنایت به این مسئله مشاهده می‌شود که مبارزه همه جانبه علیه سایبر تروریسم در سطوح بین‌المللی یا دشواری‌های قانونی و همکاری کامل کشورهای و دولت‌ها همراه است. از آنجاکه به جهت بررسی حاکمیت‌ها، دادگاه داخلی یک کشور اصولاً نمی‌تواند علیه جرایم ارتكابی کشوری دیگر حکم صادر نماید و به دلیل فرامرزی و بین‌المللی بودن فضای سایبر و همچنین جرایم سایبری، بهترین روش برای مبارزه با سایبر تروریسم و جرایم سایبری رجوع به محاکم بین‌المللی و ایجاد همکاری‌های پلیسی و حقوقی در سطح بین‌المللی است.

یکی از تهدیدات امنیتی که همواره ملت‌ها و دولت‌ها را آزار داده، اقدامات تروریستی است که عمدتاً با پیامدهای بسیار زیانباری همراه هستند. بدیهی است «زیرساخت‌های حیاتی» از بهترین اهداف محسوب می‌شوند که با

توجه به الکترونیکی شدن آنها، نه تنها ارتکاب اقدامات تروریستی آسان‌تر شده، بلکه لطمات وارد شده بسیار سهمگین هستند. البته ماهیت «چند رسانه‌ای» فضای سایبر، به تروریستها امکان بهره‌برداریهای سوء دیگری را هم داده است. این نوشته بر آن است که با تبیین اجمالی مفهوم عام تروریسم سایبر به عنوان یک پدیده مجرمانه، راهکارهای حقوقی مقابله با آن و وضعیت کشورمان را بررسی نماید.

جمهوری اسلامی ایران که از بزرگترین قربانیان تروریسم می باشد مورد حمله و حمله حملات سایبری نیز قرار دارد. استفاده گسترده از بدافزارهای خرابکاری و جاسوسی از نمونه های این حملات هستند. استفاده از انواع کدها، برنانه نویسی به قدری گسترده است که یقیناً از حد و اندازه حملات انفرادی یا حتی گروهی خارج بوده پشتیبانی اطلاعاتی و تکنولوژیکی قدرت‌های بزرگ و صاحب تکنولوژی را می‌طلبد. به طوری که گاهی خود دولت‌ها نیز از امنیت در حملات، نقش عامل را نیز بر عهده می‌گیرند و در برخی از موارد حاضر نیستند این ابزار یا عمل را به هر دلیلی در دست گروه‌های مزدور قرار دهند. زیرا از یکسو ذات چنین تروریسمی نیز به دلیل این برون هزینه‌های سیاسی و حقوقی آن نیازی به برون‌سپاری دولت‌ها برای پنهان‌سازی نقش مستقیم ندارد؛ به عبارت دقیق‌تر عدم امکان تشخیص دقیق مهاجمان و هویت واقعی آنها و مشکل بودن ارزیابی زمان و محل حمله و همچنین ضربه به زیرساخت‌های کشور هدف، از قبیل سیستم‌های مالی و بانکداری، کارخانجات و حتی شبکه‌های خدمات‌رسانی شهری از دلایل تمایل دولت‌ها در مدیریت و اجرای مستقیم این نوع حمله‌ها است. ر س‌وی دیگر نیز می‌توان به ارزش علمی و تکنولوژیکی این پدیده را در نظر گرفت که با برون‌سپاری آن به گروه‌ها رسان‌مان‌ها مزدور حتی می‌تواند در شرایطی مختل امنیت خود کشورهای صادر کننده و منافع آنها باشد.

عبداله میرفردی