

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

تروریسم سایبری

در

حقوق ایران و بین الملل

مؤلف:

محمدرضا روزبهانی

(مدرس دانشگاه قرآن و حدیث)

شابک	۵-۱۶۳-۳۴۶-۶۰۰-۹۷۸-۵۵۰۰۰ ریال
شماره کتابشناسی ملی	۳۸۸۷۶۸۹
عنوان و نام پدیدآور	تروریزم سایبری در حقوق ایران و بین الملل/مؤلف محمدرضا روزبهانی
مشخصات نشر	تهران: کتاب آوا، ۱۳۹۵
مشخصات ظاهری	۱۳۸ ص
یادداشت	کتابنامه: ص. ۱۳۱-۱۳۷؛ همچنین به صورت زیرنویس
موضوع	تروریزم رایانه‌ای
موضوع	تروریزم
موضوع	فضای مجازی--جنبه‌های حقوقی
رده‌بندی در بی	۳۶۴/۱۶۸
رده‌بندی کنگره	۱۳۶۴-۴۱۳/۹ HV۶۷۷۳
سرشناسه	روزبهانی، محمدرضا، ۱۳۵۴ -
وضعیت فهرست‌نویسی	ف.پ.ا

تروریزم سایبری در حقوق ایران و بین‌الملل



مؤلف:	محمدرضا روزبهانی
ناشر	کتاب آوا
لیتوگرافی	باران مهر
چاپ و صحافی	آوا
نوبت چاپ	اول ۱۳۹۵
شمارگان	۱۰۰ نسخه
قیمت	۸۰۰۰۰ ریال
شابک	۵-۱۶۳-۳۴۶-۶۰۰-۹۷۸-۵۵۰۰۰

نشانی دفتر مرکزی: انقلاب، خیابان ۱۲ فروردین، بن‌بست حقیقت، پلاک ۴، طبقه ۲، واحد ۴
شماره‌های تماس: ۶۶۹۷۴۶۴۵ | ۶۶۹۷۴۱۳۰ | ۶۶۴۰۷۹۹۳ | دورنگار: ۶۶۴۶۱۱۵۸

www.avabook.com avabook_kazemi@yahoo.com

فروشگاه کتاب آوا: اسلام‌شهر، خیابان صیاد شیرازی، روبروی دانشگاه آزاد اسلامی، جنب دادگستری
تلفن: ۵۶۳۵۴۶۵۱

کلیه حقوق این اثر برای ناشر محفوظ است.
هرگونه کپی‌برداری و تهیه جزوه از متن کتاب، استفاده از طرح روی جلد و عنوان کتاب جرم است و متخلفان طبق قانون حمایت از حقوق مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می‌گیرند.

فهرست مطالب

۱۳.....	فصل اول: کلیات و مفاهیم.....
۱۳.....	قسمت اول: کلیات.....
۱۷.....	قسمت دوم: مفاهیم.....
۱۷.....	بررسی معنای لغوی و اصطلاحی تروریسم.....
۱۷.....	بحث اول: مفهوم ترور.....
۱۷.....	تروریسم در لغت و اصطلاح.....
۲۲.....	مفهوم تروریسم.....
۲۲.....	مبحث دوم: تعریف تروریسم در حقوق ایران.....
۲۳.....	مبحث سوم: تعریف تروریسم در حقوق داخلی دیگر کشورها.....
۲۳.....	تعریف تروریسم در حقوق آلمان.....
۲۴.....	تعریف تروریسم در حقوق انگلستان.....
۲۴.....	تعریف تروریسم در حقوق فرانسه.....
۲۵.....	تعریف تروریسم در حقوق آمریکا.....
۲۵.....	مبحث چهارم: تعریف تروریسم در اسناد بین‌المللی.....
۲۵.....	تعریف «تروریسم بین‌المللی».....
۲۶.....	مبحث پنجم: تعریف تروریسم در اسناد سازمان ملل.....
۲۷.....	مبحث ششم: تعریف تروریسم در کنوانسیون مبارزه با بنگذاری تروریستی.....
۲۷.....	مبحث هفتم: تعریف تروریسم در کنوانسیون بین‌المللی سرکشی و ایت مالی از تروریسم.....
۲۸.....	قید «غیر نظامیان» در تعریف تروریسم.....
۲۸.....	شروع به جرم، شرکت، معاونت، رهبری و یا دستور به ارتکاب جرایم یاد شده.....
۲۸.....	مبحث هشتم: تعریف تروریسم در دیگر اسناد بین‌المللی.....
۲۹.....	مبحث نهم: تعریف تروریسم در اسناد اتحادیه اروپا.....
۲۹.....	مبحث دهم: تعریف تروریسم در اسناد سازمان کنفرانس اسلامی.....
۳۰.....	مبحث یازدهم: تعریف نهایی از تروریسم.....
۳۱.....	فصل سوم: گونه‌ها، مصادیق و اشکال تروریسم.....
۳۱.....	مبحث اول: تقسیم‌بندی تروریسم.....
۳۲.....	مبحث دوم: تروریسم به اعتبار فعل.....
۳۲.....	تروریسم فردی و خودانگیخته.....

۳۳	مبحث سوم: تروریسم گروهی یا سازمان یافته
۳۴	مبحث چهارم: تروریسم دولتی و ویژگی های آن
۳۷	مبحث پنجم: تروریسم نژادی
۳۷	مبحث ششم: تروریسم به اعتبار هدف
۳۷	مبحث هفتم: تروریسم سیاسی
۳۸	مبحث هشتم: تروریسم غیر سیاسی
۳۹	مبحث نهم: مصادیق و اشکال تروریسم در حقوق بین الملل و حقوق داخلی
۴۰	مبحث دهم: جرائم تروریستی متعارف (سنتی)
۴۰	مبحث یازدهم: جرائم علیه امنیت پرواز یا تروریسم هوایی
۴۲	مبحث دوازدهم: گروگانگیری
۴۳	مبحث سیزدهم: سوخت به حیات و امنیت اشخاص
۴۴	مبحث چهاردهم: جرائم علیه امنیت عبور و مرور دریایی یا تروریسم دریایی
۴۶	مبحث شانزدهم: تهدید ملل های کشتار جمعی
۴۷	مبحث هفدهم: تروریسم مستعانی
۴۹	مبحث هجدهم: بیوتروریسم
۵۰	مبحث نوزدهم: تروریسم شیمیایی
۵۱	مبحث بیستم: تروریسم اطلاعاتی - سایبری
۵۵	فصل چهارم: تروریسم سایبری
۵۵	مبحث اول: بررسی ابعاد مفهومی تحریم اقتصادی
۵۹	مبحث دوم: بررسی ترور و تروریسم سایبری در ایران
۶۰	تاریخچه حملات اینترنتی
۶۱	ایران و تروریسم مجازی
۶۳	مانورهای ایرانی و ارتش ۱۷ هزار نفری هکرهای آمریکایی
۶۳	تروریسم سایبری و حقوق امنیت بین المللی جدید
۶۶	مبحث سوم: مروری بر حملات سایبری علیه ایران
۶۷	مبحث چهارم: سایبر تروریسم
۶۷	مبحث پنجم: دلایل سایبر تروریسم
۶۸	مبحث ششم: گاوس و سیستم بانکی
۶۸	شعله آتش در تجهیزات نفتی
۶۹	مبحث هفتم: Madi
۷۰	مبحث هشتم: مینی فلیم
۷۱	مبحث نهم: نای: عناصر غیر دولتی بازیگران اصلی جنگ های سایبری



مبحث دهم: جنگ بدون خونریزی	۷۱
مبحث یازدهم: تفاوت جنگ طبیعی با جنگ سایبری چیست؟	۷۳
مبحث دوازدهم: پیشگیری وضعی از تروریسم سایبری	۷۸
مبحث سیزدهم: افزایش زحمات ارتکاب جرم	۷۸
مبحث چهاردهم: تکنیک‌های سخت‌تر کردن هدف	۷۹
مبحث پانزدهم: تکنیک‌های کنترل کننده یا محدود کننده دسترسی	۸۰
مبحث شانزدهم: تکنیک‌های کنترل کننده ورودی‌ها و دسترسی به اهداف در اماکن	۸۰
مبحث هفدهم: کنترل و محدود کردن دسترسی به ابزارهای تسهیل کننده جرم	۸۲
مبحث هجدهم: منحرف نمودن جهت ارتکاب اعمال مجرمانه	۸۴
مبحث نوزدهم: افزایش خطرات قابل پیش‌بینی ارتکاب جرم	۸۴
مبحث بیستم: تحت نظر قرار دادن ورودی و خروجی‌های اماکن عمومی	۸۴
مبحث بیست و یکم: تأثیر نظارتی	۸۵
کاهش گمنامی	۸۵
نظارت غیر رسمی	۸۶
کاهش سود و منافع حاصل از ارتکاب جرم	۸۶
تقویت محافظت از آماج حمله	۸۶
به‌کارگیری تجهیزات کدکی و دکلانه در محل	۸۷
تخصیص مکان‌های امن برای تأسیسات	۸۷
جایگزینی کابل‌های سیمی به ارتباط بی‌سیم	۸۷
پیش‌بینی منابع تغذیه متعدد	۸۷
تمهید راهکارهایی به منظور مقابله با عواما	۸۸
کاهش یا حذف منافع قابل پیش‌بینی از جرم	۸۸
کاهش جذابیت امکانات جرم	۸۹
کاهش عوامل محرک در ارتکاب جرم	۸۹
از بین بردن معاذیر توجیه کننده برای عقلانی جلوه دادن جرم	۹۰
فصل پنجم: حملات سایبری از منظر حقوق بین‌الملل	۹۱
مبحث اول: ویژگی‌های حقوقی تروریسم سایبری	۹۱
مبحث دوم: تقسیم‌بندی اعمال تروریستی	۹۱
مبحث سوم: ابزارهای سایبر تروریسم	۹۲
مبحث چهارم: راهکارهای مقابله با تروریسم سایبری	۹۲
مبحث پنجم: سایبر تروریسم	۹۳
مبحث ششم: نبرد سایبری و توسل به زور؛ حق دفاع از خود	۹۶

مبحث هفتم: بخش اول: تاربخچه.....	۹۸
مبحث هشتم: بخش دوم: بحث اصلی.....	۱۰۱
الف: نبرد سایبری، حقوق معاهدات و عرف‌های بین‌المللی.....	۱۰۱
ب: نبرد سایبری، حقوق بین‌الملل و توسل به زور.....	۱۰۲
ج: نبرد سایبری و استثناء دفاع از خود.....	۱۰۵
مبحث نهم: بخش سوم: تحلیل و بررسی.....	۱۰۸
مبحث دهم: حمله سایبری استاکس‌نت به مثابه توسل به زور در حقوق بین‌الملل.....	۱۰۹
مبحث یازدهم: از جنگ هسته‌ای تا جنگ اینترنتی.....	۱۱۳
مبحث دوازدهم: تعریف جنگ اطلاعاتی و تهدید به حملات الکترونیکی.....	۱۱۵
حمله سایبری به استونی.....	۱۱۶
مبحث یازدهم: مشابهت سازی واکنش‌های زمان صلح با حمله سایبری در حقوق بین‌الملل.....	۱۱۶
الف. قیاس با جنگ هسته‌ای.....	۱۱۷
ب. قیاس با حقوق نظام معاهده‌ای قطب جنوب.....	۱۱۸
مبحث چهاردهم: تحرک به نفع کشتی از طریق سایبری.....	۱۱۹
پی‌نوشت‌ها.....	۱۲۱
نتیجه‌گیری.....	۱۲۹
فهرست منابع و مآخذ.....	۱۳۱
الف) منابع فارسی و عربی.....	۱۳۱
ب) منابع لاتین.....	۱۳۷

اقدامات تروریستی یکی از تهدیدات امنیتی است که همواره ملت‌ها و دولت‌ها را آزار داده، است که عمدتاً با پیامدهای بسیار زیانباری همراه بوده است. بدیهی است «زیرساخت‌های حیاتی» از بهترین اهداف محسوب می‌شوند که با توجه به الکترونیکی شدن آنها، نه تنها ارتکاب اقدامات تروریستی آسان‌تر شده، بلکه نطامات وارد شده بسیار سهمگین هستند. البته ماهیت «چند رسانه‌ای» فضای سایبر، به تروریست‌ها امکان بهره‌برداری‌های سوء دیگری را هم داده است.

امروز، تروریسم سایبری به یکی از چالش‌های عمده‌ی نظام‌های حقوقی به خصوص نظام‌های کیفری تبدیل شده است. تروریسم دیگر از رویکردهای سنتی خود رنگ باخته و به سوی فناوری‌های نوین، روی آورده است. در میان اکثر نظام‌های حقوقی جهان، به جرم‌انگاری تروریسم سایبری صریح و اختصاصی پرداخته نشده و مهم‌تر از آن به حمایت از بزه‌دیدگان تروریسم سایبری که به دنبال دیدگی تحمل خسارت‌های جبران ناپذیر می‌شوند، توجهی نشده است. در این میان آن چه در وهله اول ضروری به نظر می‌رسد، پیشگیری از وقوع تروریسم سایبری به منظور حمایت از بزه‌دیدگان آن است.

در میان انواع پیشگیری، پیشگیری وضعی مناسب‌ترین راهکار برای مقابله با این بزه است که در این نوشتار سعی می‌شود با استفاده از راهکارهای این پیشگیری به حمایت از بزه‌دیدگان آن بپردازیم. بنابراین در این نوشتار به پیشگیری وضعی از بزه تروریسم سایبری با توجه به آماج مورد حمله پرداخته می‌شود. و نیز بر آن است که با تبیین اجمالی مفهوم تروریسم سایبر به عنوان یک پدیده‌ی مجرمانه، راهکارهای حقوقی مقابله با آن و وضعیت کشور را بررسی نماید. با رشد سریع و درعین‌حال نامتوازن ساختار فضای سایبری، این بستر به یکی از نقاط بالقوه آسیب‌پذیر و خطرناک در جهان بدل شده است که ضرورت توجه و رسیدگی سریع، نظام‌مند، معقول و هدفمند به منظور مصون‌سازی این بستر از تهدیدات موجود و پدیده نوظهور سایبر تروریسم را در فضای بین‌المللی می‌طلبد. با بررسی منابع موجود، مقالات، کتاب‌ها، نتایج و دستاوردهای طرح‌های تحقیقاتی در حوزه فضای سایبری، تروریسم بین‌المللی و سایبر

تروریسم به روش غیرآزمایشی، مقایسه‌ای و کتابخانه‌ای، تهدیدات و مخاطرات سایر تروریسم و نقش آن در برهم‌زدن امنیت بین‌الملل مورد تحقیق و پژوهش قرار گرفت.

با وجود نوظهور بودن، سایر تروریسم به مراتب خطرناک‌تر از تروریسم کلاسیک و سنتی می‌باشد و تهدیدات آن برای امنیت ملی دولت‌ها و کشورها به خطری بالقوه تبدیل شده است. پیشگیری، کشف و مقابله با سایر تروریسم برای نهادهای پلیسی و امنیتی بسیار پیچیده و مشکل‌تر از تروریسم سنتی می‌باشد. برنامه‌ریزی‌های جهانی و تصویب قوانین بین‌المللی، افزایش همکاری‌های فنی و آموزشی بین‌المللی، توجه ویژه به مبحث پدافند غیرعامل در فضای سایبری توسط نهادهای داخلی و همکاری‌های میان سازمان‌های امنیتی و پلیسی از جمله راهکارهای مبارزه با سایر تروریسم می‌باشد. اتصال هرچه بیشتر شبکه‌های رایانه‌ای گوناگون در سراسر جهان و فرار گسترده ترجم بیشتری از اطلاعات ارزشمند بر روی این شبکه‌ها، جذابیت رایانه‌ها و شبکه‌های رایانه‌ای را به عنوان اهداف بزهکاران تروریستی هرچه بیشتر ساخته است. بنابراین روز به روز انگیزه مهاجمین احتمالی برای آغاز حمله علیه اهداف سایبری افزوده می‌گردد.

ویژگی‌های فضای سایبر از جمله بی‌حد و مرز بودن، سرعت خیره‌کننده مبادلات در محیط سایبر، و به تبع آن، سرعت ارتکاب جرایم سایبر، و آسان‌تر و بسیار سریع مرتکب، از صحنه جرم (مجازی)، و امکان اختفاء و یا حتی امحاء آثار و تخریب مدرم، ابزار و تجهیزات قابل دسترس، ارزان بودن، دسترسی سریع و عدم نظارت کافی در این فضا، باعث شده که بزهکاران از دنیای فیزیکی روی برگردانده و به دلایل مختلف از جمله شکست آن‌ها در اقدام به عمل مجرمانه در دنیای فیزیکی، عدم اعتماد به نفس در دنیای واقعی و دیگر عوامل که ممکن است ریشه در مباحث روانشناسی داشته باشد، به فضای سایبر کشیده شوند. آن دسته از تهدیدکنندگانی که در این تحقیق مورد توجه قرار گرفته‌اند، تروریست‌هایی هستند که صرف نظر از ماهیت و اهداف اقداماتشان، نتایج زیان‌باری به جای می‌گذارند. با این که حوزه‌ی ارتکاب اعمال تروریسم سایبری با تروریسم سنتی متفاوت است و از شیوه‌های نوینی برای ارتکاب اقدامات تروریستی استفاده می‌شود، اما در بسیاری از اصول اولیه تشکیل‌دهنده‌ی بزه‌های تروریستی از قبیل انگیزه‌های ارتکاب مشابه می‌باشند.