

مقدمه: ۱۱

بخش اول: مفاهیم و کلیات تحقیق ۱۳

۱- ادبیات نظری تحقیق ۱۳

۱-۱- تروریسم ۱۳

۱-۲- تروریسم سایبری ۱۳

۱-۳- فضای سایبر ۱۴

۱-۴- ادله اثبات دعوی ۱۴

۱-۵- رفتار مجرمانه ۱۴

۱-۶- سیاست جنایی ۱۵

۲- مفهوم شناسی ۱۵

۲-۱- مفهوم و ماهیت فضای سایبر ۱۵

۲-۲- مفهوم و ماهیت تروریسم کلاسیک ۱۷

۲-۲-۱- تعاریف حکومتی ۲۱

الف- تعریف دپارتمان دفاعی ایالات متحده آمریکا ۲۱

ب- تعریف سازمان اف بی ای ایالات متحده آمریکا (FBI) ۲۱

ج- تعریف وزارت امور خارجه آمریکا ۲۱

د- تعاریف ارائه شده در قوانین کشورها ۲۲

۲-۲-۲- تعاریف نظری ۲۳

۲-۲-۳- تعاریف نهادها و سازمان‌های بین‌المللی و منطقه‌ای: ۲۴

الف- قطعنامه‌های شورای امنیت ۲۶

ب- تروریسم از منظر کنوانسیون‌های ضد تروریستی ۲۹

ج- کنوانسیون جرائم سایبری شورای اروپا ۳۱

د- تروریسم در اسناد سازمان کنفرانس اسلامی ۳۲

۲-۳- مفهوم و ماهیت سایبر تروریسم ۳۴

- ۳- تاریخچه و پیشینه تحقیق..... ۳۸
- ۳-۱- تاریخچه و پیشینه تروریسم کلاسیک..... ۳۸
- ۳-۱-۱- تروریسم در عهد باستان..... ۴۰
- الف- یونان..... ۴۰
- ب- روم..... ۴۰
- ۳-۱-۲- قرون وسطی..... ۴۱
- ۳-۱-۳- دوران جدید..... ۴۲
- ۳-۲- تاریخچه و پیشینه تروریسم سایبری..... ۴۵
- ۴- گونه‌های تروریسم..... ۴۷
- ۴-۱- گونه‌های تروریسم کلاسیک..... ۴۷
- ۴-۱-۱- گونه‌های تروریسم از منظر حوزه عمل..... ۴۸
- الف- تروریسم داخلی..... ۴۸
- ب- تروریسم بین‌المللی..... ۴۸
- ۴-۱-۲- گونه‌های تروریسم از منظر دخالت دولت‌ها..... ۴۹
- الف- تروریسم دولتی..... ۴۹
- ب- تروریسم غیر دولتی..... ۵۵
- ۴-۱-۳- گونه‌های تروریسم از منظر مقیاس جغرافیایی و حوزه عملکرد..... ۵۶
- الف- تروریسم داخلی..... ۵۷
- ب- تروریسم منطقه‌ای..... ۵۷
- ج- تروریسم جهانی (تروریسم جدید / فراسرزمینی)..... ۵۸
- ۴-۱-۴- تروریسم بر اساس ابزار و روش‌های مورد استفاده..... ۵۹
- الف- تروریسم متعارف..... ۵۹
- ب- تروریسم نامتعارف..... ۶۰
- ۴-۱-۵- تروریسم بر اساس اهداف سیاسی..... ۶۰
- الف- تروریسم تجزیه طلب یا ملی‌گرا..... ۶۰
- ب- تروریسم مذهبی..... ۶۱
- ج- تروریسم جناح چپ یا راست افراطی..... ۶۱
- ۴-۱-۶- تروریسم بر اساس ساختار سازمانی..... ۶۱
- الف- ساختار سلسله‌مراتبی..... ۶۱

- ب- ساختار شبکه‌ای ۶۲
- ج- سازمان تلماسه ای ۶۲
- ۴-۱-۷. دیگر گونه‌های تروریسم ۶۳
- الف- تروریسم گروهی یا سازمان‌یافته ۶۳
- ب- تروریسم نژادی ۶۴
- ج- تروریسم هوایی ۶۴
- د- تروریسم دریایی ۶۴
- ه- تروریسم هسته‌ای ۶۵
- و- بیو تروریسم ۶۵
- ز- تروریسم شیمیایی ۶۵
- ح- تروریسم سیاسی ۶۶
- ط- تروریسم اقتصادی ۶۶
- ۴-۲- گونه‌های تروریسم سایبری ۶۶
- ۵- شاخصه‌ها و ویژگی‌های تروریسم ۶۷**
- ۵-۱- ویژگی‌های تروریسم کلاسیک ۶۷
- ۵-۲- ویژگی‌های تروریسم سایبری ۶۹
- الف- سرعت ۶۹
- ب- ناشناختگی و امکان گمنامی ۶۹
- ج- حجم جرائم ۷۰
- د- ارزان بودن بزه ۷۰
- ه- عدم حضور در صحنه بزه ۷۱
- و- فراملی بودن ۷۱
- ز- بالا بودن رقم سیاه ۷۲
- ح- اتوماتیک بودن جرم ۷۳
- ط- درونی بودن بزه ۷۳
- ی- ضعف یا فقدان کنترل اجتماعی ۷۴

بخش دوم: جایگاه تروریسم سایبری در نظام حقوقی ایران ۷۷

۱- رویکرد ایران در قانونگذاری فضای سایبر ۷۷

۱-۱- روش قانونگذاری ملی ۷۸

۱-۲- روش مختلط ۷۸

۲- صلاحیت قانونگذاری در فضای سایبر در حقوق ایران ۸۱

الف- صلاحیت سرزمینی ۸۲

ب- صلاحیت شخصی ۸۲

ج- صلاحیت واقعی ۸۲

د- صلاحیت جهانی ۸۳

بخش سوم: چالش‌های اجرائی مقابله با تروریسم سایبری ۸۷

۱- پیشگیری از وقوع تروریسم سایبری ۸۷

۱-۱- اقدامات پیشگیرانه کیفری در نظام حقوقی ایران ۸۸

الف- قانون جرائم رایانه‌های مصوب ۱۳۸۸ ۸۸

ب- قانون تجارت الکترونیکی مصوب ۱۳۸۲ ۹۰

ج- قانون مجازات نیروهای مسلح مصوب ۱۳۸۲ ۹۱

د- قانون مجازات اسلامی مصوب ۱۳۷۰ ۹۲

۱-۲- اقدامات پیشگیرانه کیفری در عرصه بین‌المللی ۹۳

۱-۳- اقدامات پیشگیرانه غیرکیفری در نظام حقوقی ایران ۹۴

۱-۳-۱- پیشگیری اجتماعی از تروریسم سایبری ۹۴

۱-۳-۱-۱- پیشگیری اجتماعی رشد مدار از جرائم سایبری ۹۵

الف- مداخله در فرآیند تحصیل و تدابیر خانواده محور ۹۶

ب- تدابیر آموزشی- سایبری ۹۶

ج- سواد رسانه‌ای ۹۷

۱-۳-۱-۲- پیشگیری اجتماعی مدار از تروریسم سایبری ۹۷

الف- نهادینه کردن فرهنگ استفاده صحیح از فضای سایبری ۹۸

ب- بزه دیده زدایی و تدوین قوانین به روز و کارآمد ۹۹

- ج-اطلاع رسانی عمومی و رفع مشکلات اقتصادی..... ۱۰۰
- د-مشارکت و اجماع گری..... ۱۰۲
- ۱-۳-۲. پیشگیری وضعی از جرائم سایبری..... ۱۰۳
- ۱-۴. اقدامات پیشگیرانه غیرکیفری در اسناد بین المللی و منطقه‌ای..... ۱۰۵
- الف. توصیه نامه‌های نشریه بین المللی سیاست جنایی..... ۱۰۵
- ب. دستورالعمل و توصیه نامه‌های سازمان همکاری و توسعه اقتصادی..... ۱۰۵
- ج. هشتمین نشست سازمان ملل متحد درباره پیشگیری از جرم و اصلاح مجرمین..... ۱۰۵
۲. جرم انگاری تروریسم سایبری..... ۱۰۶
- ۱-۲ جرم انگاری تروریسم به مثابه جنایت علیه بشریت..... ۱۰۸
- ۲-۲ جرم انگاری تروریسم به مثابه ژنوساید..... ۱۰۹
- ۲-۳. جرم انگاری تروریسم به عنوان یک جنایت نفسه المللی فی نفسه..... ۱۱۰
۳. بار اثبات دلیل در سایبر تروریسم..... ۱۱۳
- ۳-۱. ادله سنتی..... ۱۱۴
- الف- اقرار..... ۱۱۴
- ب- شهادت..... ۱۱۵
- ج- سند و نوشته..... ۱۱۵
- د- قسم..... ۱۱۶
- ه- امارات..... ۱۱۶
- ۳-۲. أدله دیجیتال..... ۱۱۷
- ۱-۳-۲. جهات ضعف و قوت دلائل الکترونیکی..... ۱۱۸
- ۲-۳-۲. استناد پذیری ادله الکترونیکی..... ۱۱۹
۴. بررسی داوری و صلاحیت فرامرزی سایبر تروریسم..... ۱۲۳
- ۴-۱. داوری..... ۱۲۳
- ۴-۲. صلاحیت فرامرزی..... ۱۲۴
- الف. نامعین بودن حیطه‌های جغرافیایی و عدم امکان تعیین محل ارتکاب جرائم سایبری..... ۱۲۴
- ب. شناسایی تابعیت شخص مرتکب..... ۱۲۵

ج حل تعارض صلاحیتها ۱۲۵

بخش چهارم: راهکارهای کیفری و حقوقی مقابله با تروریسم سایبری ۱۳۱

۱- چگونگی قانونگذاری کیفری در تروریسم سایبری ۱۳۱

۱-۱- کنوانسیون‌های بین‌المللی جهانی در باب تروریسم ۱۳۴

الف. کنوانسیون توکیو راجع به جرایم و دیگر اعمال ارتكابی دیگر در هواپیما ۱۳۴

ب. کنوانسیون مقابله با اعمال غیر قانونی علیه ایمنی هواپیمایی کشوری ۱۳۴

ج. کنوانسیون بین‌المللی مقابله با بمب گذاری تروریستی ۱۳۵

د. کنوانسیون بین‌المللی مقابله با تامین مالی تروریسم ۱۳۶

۱-۲. روشهای قانونگذاری در فضای سایبر ۱۳۸

۱-۲-۱. قانونگذاری ملی ۱۳۸

الف. صلاحیت سرزمینی ۱۳۸

ب. صلاحیت شخصی ۱۳۹

ج. صلاحیت واقعی ۱۳۹

د. صلاحیت جهانی ۱۳۹

۱-۲-۲. قانونگذاری بین‌المللی ۱۴۰

۱-۲-۳. روش خودانتظامی ۱۴۲

۱-۲-۴. روش مختلط ۱۴۲

۲- حقوق جزای ماهوی و شکلی تروریسم سایبری ۱۴۴

۱-۲-۱- حقوق جزای ماهوی تروریسم سایبری ۱۴۴

الف. عدم حمایت از بزه دیده سهل انگار ۱۴۵

ب. استفاده از روش احاله یا ارجاع در جرم انگاری ۱۴۶

ج. تعریف اعمال مقدماتی به عنوان جرم تام ۱۴۷

د. گسترش مسوولیت کیفری معاونتی ۱۴۸

ه. وضع جرائم مطلق ۱۴۸

و. کاهش عناصر تشکیل دهنده جرم ۱۴۹

۱-۲-۲. حقوق جزای شکلی در تروریسم سایبری (آئین دادرسی کیفری) ۱۴۹

۳- ضرورت گسترش تدابیر امنیتی و عوامل اجرائی در خصوص امنیت فضای سایبر..... ۱۵۲

نتیجه‌گیری و پیشنهادات..... ۱۵۷

منابع و مآخذ..... ۱۵۹

کتاب..... ۱۵۹

مقالات..... ۱۶۱

پایان نامه..... ۱۶۶

avabook.com

avabook.com

مقدمه



تحولات و پیشرفت شگرف تکنولوژی و فناوری اطلاعات و ارتباطات، مولد تغییرات عمده‌ای در زیر ساخت‌های مهم و حیاتی کشور بوده و بسیاری از مفاهیم سنتی حقوق کیفری را با چالش مواجه ساخته است. در این میان حملات تروریستی سایبری گونه‌ای نوین از جرائم سایبری هستند که استعداد ایجاد تغییرات بنیادین در ساختارهای امنیتی را در سطوح مختلف ملی و بین‌المللی دارند. تروریسم سایبری یکی از مهمترین جرائم ارتكابی در بستر فضای سایبر، است. این پدیده مجرمانه از تلاقی اعمال تروریستی و فضای سایبر پا به عرصه وجود نهاده است و از طریق دسترسی به اطلاعات حفاظت شده صورت می‌پذیرد. در حال حاضر یکی از دغدغه‌های نظام قانونگذاری در هر کشوری، جرم‌انگاری کارآمد و مؤثر این پدیده مجرمانه است چراکه تروریسم از رویکردهای سنتی خود رنگ باخته و به سوی فناوریهای نوین روی آورده است. تروریسم سایبری، با وجود نو ظهور بودن به مراتب خطرناک‌تر از تروریسم کلاسیک و سنتی است و تهدیدات آن برای امنیت ملی دولت‌ها و کشورها به خطری بالقوه تبدیل شده است. تروریسم در فضای سایبر طیفی از حملات و تهدیدات غیرقانونی توسط تروریست‌ها علیه رایانه، شبکه‌ها و اطلاعات ذخیره شده برای مرعوب ساختن یا مجبور کردن یک حکومت یا افراد یک کشور جهت پیشبرد اهداف اجتماعی و سیاسی است. حمایت دولتی که زمانی یک از مؤلفه‌های اصلی تروریسم بود، ممکن است از این پس برای تروریست‌ها چندان حیاتی نباشد، زیرا فناوری اطلاعات و فضای سایبر با فراهم آوردن ظرفیت‌های جدید و مؤثرتر برای تروریست‌ها و هم‌چنین آزادی عمل آن‌ها برای انجام حملات سازمان یافته تروریستی در عمل بسیاری از مزایای حمایت دولت‌ها را منسوخ کرده است در عصر حاضر ارتباط میان تروریست‌ها از طریق شبکه‌های بین‌المللی و تبادل افکار و اعمال مجرمانه در سطح بسیار پیچیده است که از ویژگی‌های این نوع ارتباط عدم توانایی پلیس در کنترل

و شنود این ارتباطات می‌باشد از این رو، پیشگیری کارآمد از آن تنها با مشارکت کشورها و مداخله سازمان‌های بین‌المللی قابل تصور است. در پژوهش حاضر نگارندگان بر آن شدند تا ضمن بررسی تفاوت بنیادین میان تروریسم کلاسیک و تروریسم سایبری، به این سوال پاسخ دهند که تفاوت‌های موجود میان این دو پدیده نظام‌های حقوقی افتراقی را می‌طلبد یا صرفاً روش و ابزار و شیوه ارتکاب جرم متفاوت است و درنهایت با روش توصیفی-تحلیلی به شیوه استقرایی-قیاسی، به اثبات این فرضیه می‌پردازد که، میان دو پدیده تروریسم سایبری و تروریسم کلاسیک تفاوت‌های بنیادین حقوقی به نحوی که متضمن دو نظام حقوقی افتراقی باشند وجود ندارد و تنها شیوه‌های ارتکاب جرم و روش‌های اثباتی آن‌ها متفاوت بوده و نیازمند آن است تا قوانین جامعی در خصوص تروریسم سایبری مدون گردد. نوشتار حاضر بدنبال بازخوانی تروریسم با رویکرد ارتکاب در فضای سایبر و استفاده از سامانه‌های رایانه‌ای و مخابراتی، به تبیین جایگاه تروریسم سایبری در نظام حقوقی ایران و آئین اثبات دلیل در این گونه از جرائم تروریستی پرداخته و ضمن بررسی چالش‌های اجرائی تروریسم سایبری به ارائه راهکارهای مطلوب حقوقی و کیفری در جهت مقابله با گسترش تروریسم در فضای سایبر و همچنین پیشگیری از این پدیده مجرمانه در عرصه داخلی و بین‌المللی، جهت تحقق عدالت کیفری می‌پردازد.

بخش اول: مفاهیم و کلیات تحقیق

۱- ادبیات نظری تحقیق

۱-۱- تروریسم

وقتی سخن از واژه «ترور» و «تروریسم» به میان می‌آید، شامل تمامی اعمال خشونت‌آمیزی می‌شود که معمولاً منافع حیاتی یک کشور را هدف قرار می‌دهد و آنچه در این‌گونه اعمال مجرمانه موضوعیت پیدا می‌کند ایجاد ترس و وحشت است. (قدیم‌زاده، ۱۳۹۵، ۲۴۹) در ماده یک لایحه مبارزه با تروریسم پیش‌بینی شده است که «ارتکاب یا تهدید به ارتکاب جرائم و اقدامات خشونت‌آمیز از طریق به وحشت‌افکندن مردم جهت تأثیرگذاری بر خط و مشی، تصمیمات و اقدامات دولت جمهوری اسلامی ایران، سایر کشورها و سازمان‌های بین‌الدولی، جرم تروریستی محسوب می‌شود.» علاوه بر تعریف مذکور، تعریف ساده‌ای که می‌توان از تروریسم ارائه داد عبارتست از: «ارتکاب اعمال خشونت‌آمیز یا تهدید به استفاده از خشونت علیه اشخاص یا اموال برای ایجاد رعب و وحشت عمومی.» (حکیمی‌ها، ۱۳۸۴، ۵-۶)

۱-۲- تروریسم سایبری

امروزه از تلاقی اعمال تروریستی و فضای سایبرگونه‌ای نوپا از اعمال تروریستی تحت عنوان تروریسم سایبری پا به عرصه وجود نهاده‌است، که از طریق دسترسی به اطلاعات حفاظت‌شده صورت می‌پذیرد. (همزی، ۱۳۹۷، ۲) ارتباط میان تروریست‌ها از طریق شبکه‌های بین‌المللی و تبادل افکار و اعمال مجرمانه در سطح بسیار پیچیده صورت می‌پذیرد و از ویژگی‌های این نوع ارتباطات

عدم توانایی پلیس در کنترل و شنود آن‌هاست. با توجه به تعاریف مختلفی که معاهدات و حقوقدانان ارائه نموده‌اند می‌توان گفت تروریسم سایبری عبارت است از: «طیفی از حملات و تهدیدات غیرقانونی توسط تروریست‌ها علیه رایانه، شبکه‌ها و اطلاعات ذخیره شده برای مرعوب ساختن یا مجبور کردن یک حکومت یا افراد یک کشور جهت پیشبرد اهداف اجتماعی و سیاسی.» (عاملی، ۱۳۹۰، ۵۳۰؛ چاووشی، ۱۳۸۸، ۵۶)

۳-۱- فضای سایبر

«محیطی است مجازی و غیر ملموس که در فضای شبکه‌های بین‌المللی وجود دارد. در این محیط تمام اطلاعات مربوط به روابط افراد، ملت‌ها، فرهنگ‌ها، کشورها، به صورت ملموس و فیزیکی در یک فضای مجازی و به صورت دیجیتالی وجود داشته و قابل استفاده و در دسترس استفاده‌کنندگان و کاربران می‌باشد؛ کاربرانی که از طریق کامپیوتر، اجزای آن و شبکه‌های بین‌المللی بهم مرتبط‌اند.» (هرمزی، ۱۳۹۷، ۹) از محیط سایبر به محیط فناوری اطلاعات یا محیط اطلاعات و ارتباطات نیز یاد شده‌است از این رو به جرم‌های محیط سایبر، جرم‌های علیه فناوری اطلاعات نیز گفته می‌شود. (زندی، ۱۳۸۹، ۴۰)

۴-۱- ادله اثبات دعوی

دلیل هر آنچه است که با رعایت حقوق متهم و بدون الزام دادرسی به عناوین خاص مانند اقرار و شهادت و... به کشف حقیقت و اقناع وجدانی دادرسی می‌انجامد و اثبات از نظر حقوقی عبارت است از: اقامه دلیل نزد قاضی به طریقی که قانون آن را معین نموده‌است. (عباسی کلیمانی، ۱۳۹۴، ۲۵-۲۴) در نهایت می‌توان گفت ادله اثبات دعوی یعنی آنچه از مقررات نوشته یا عرفی که در مقام اثبات امری از امور در مراجع قضایی بکار رود خواه آن امور از دعاوی باشند خواه نه، مانند شهادت، امارات، قسم، سند و اقرار. چون غالباً این امور برای اثبات دعاوی بکار می‌آیند، آنها را از باب تغلیب ادله اثبات دعوی گفته‌اند. (جعفری لنگرودی، ۱۳۴۶، ۲۴)

۵-۱- رفتار مجرمانه

عنصر مادی جرم گاه رفتاری است که در وضعی خاص از انسان بروز می‌کند و گاه به ندرت حالتی است که بر او مستولی می‌گردد. رفتار انسان ظهور خارجی اراده او است یعنی نیرویی که در صدد