سایبر تروریسم

در حقوق ایران و بین الملل

مؤلف:

الیاس غریب

کارشناس ارشد حقوق جزا و جرم‌شناسی

سرشناسه	: غریب، الیاس، ۱۳۷۴-
عنوان و نام پدیدآور	: سایبر تروریسم در حقوق ایران و بین‌الملل/مولف الیاس غریب.
مشخصات نشر	: تهران: دانش‌پژوهان شریف‌یار، ۱۴۰۰.
مشخصات ظاهری	: ۲۹۵ص.
شابک	: ۹۷۸-۶۲۲-۷۶۲۳-۹۴-۹
وضعیت فهرست‌نویسی	: فیپا
یادداشت	: کتابنامه.
موضوع	: تروریسم رایانه‌ای
موضوع	: Cyberterrorism
موضوع	: تروریسم رایانه‌ای — قوانین و مقررات
موضوع	: Cyberterrorism -- Law and legislation
موضوع	: تروریسم رایانه‌ای — قوانین و مقررات — ایران
موضوع	: Cyberterrorism -- Law and legislation -- Iran
رده‌بندی کنگره	: H۷۶۷۷۳/۱۵
رده‌بندی دیویی	: ۳۶۳/۳۲۵
شماره کتابشناسی ملی	: ۸۴۱۷۷۴۶

عنوان کتاب

سایبر تروریسم
در حقوق ایران و بین‌الملل

* ناشر	پیشتازان فناوری و ارتباطات شریف‌یار
* مؤلف	**الیاس غریب**
* مدیر تولید	پیشتازان فناوری و ارتباطات شریف‌یار
* ویراستار	پیشتازان فناوری و ارتباطات شریف‌یار
* شمارگان	۱۰۰۰ جلد
* نوبت چاپ	اول، ۱۴۰۰
* چاپ و صحافی	پیشتازان فناوری و ارتباطات شریف‌یار
* ناظر چاپ	پیشتازان فناوری و ارتباطات شریف‌یار
* شابک	۹۷۸-۶۲۲-۷۶۲۳-۹۴-۹
* قیمت	۱۰۳۰۰۰ تومان

شماره‌ی تماس: ۰۲۱۹۱۰۷۰۴۲۶

سخنی با خواننده

حمد و سپاس ایزد منان را که با الطاف بی‌کران خود این توفیق را به ما ارزانی
بتوانیم درراه ارتقای دانش عمومی و فرهنگ این مرزوبوم درزمینه‌ی چاپ و نشر کـ
دانشگاهی، علوم پایه گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر
مؤثر واقع شویم. گستردگی علوم و توسعه روزافزون آن شرایطی را به وجود آورده
شاهد تحولات اساسی چشمگیری در سطح جهان هستیم. این گسترش و توسعه
منابع مختلف ازجمله کتاب راه دستیابی و اطلاع‌رسانی بیش‌ازپیش روشن می‌کند.

چاپ همگانی و سامانمند را می‌توان نقطه آغاز و محرک اصلی رشد روزافزون دانـ
دانش در چند صده گذشته دانست. کتاب از یک‌سو تفکرات نویسنده خود را از
مکان می‌رهاند و از دیگرسو در آستانه همین رهایی خواسته و یا ناخواسته ماهیت
به محک نقد و بررسی وامی‌گذارد تنها در چنین ساحتی و از برخورد دیدگاه‌های
است که بشر گامی به پیش برمی‌دارد.

موسسه فرهنگی با رویکردی جدید و متناسب با تغییرات در دنیای نوین، طرح
کتاب‌های گوناگون در برنامه انتشاراتی قرار داده است. این برنامه از یک
پیشرفت‌ها و نوآوری‌های است که در سطح بین‌الملل در زمینه‌های آموزش علوم
رخ‌داده است و از سوی دیگر، متناسب با نیازهایی است که در جامعه دانشگا
اساس رشد و توسعه سال‌های اخیر به لحاظ کیفی و کمی پدید آمده است.

انتشارات شریف یار با این نگرش در عرصه چاپ و نشر کتب علمی گام نهاده ا
تولید آثار در این مجموعه علمی فرهنگی تمام مراحل پذیرش، داوری، ویراسا
ادبی، اخذ مجوز، چاپ و انتشار به هر دو شیوه «چاپ شمارگانی» و «چاپ درازای
را در برمی‌گیرد.

شما دانش‌پژوه ارجمند می‌توانید آثار مکتوب یا چندرسانه‌ای، پیشنهادات همکاری
راهگشای خود را با فرستادن پیام به نشانی ایمیل order@sharifyar.com با
بگذارید. همه تلاش ما این است که با نگاه کارشناسی و ایجاد یک فضای علمی

آثاری پربار و نوآورانه توفیق یابیم و باور داریم که دستیابی به این خواسته تنها با همراهی شما مشتاقان حقیقی آموزش و پژوهش ممکن است.

پیشتازان فناوری و ارتباطات شریف‌یار

پیشگفتار

پیشرفت و توسعه ارتباطات و فناوری اطلاعات فرصت‌ها و چالش‌های گوناگونی را ایجاد نموده است. گسترش و توسعه روزافزون فضای مجازی و اینترنت برای اشخاصی که قصد مجرمانه و اقدام به اعمال غیرقانونی در آن‌ها وجود دارد، فرصت‌های نوینی را جهت جرایم مختلف فراهم نمود؛ امری که سبب پدیدار گشتن چالش‌های قانونگذاری و ا فراوانی شد. فضای سایبر فاقد قلمرو و مرز مشخصی می‌باشد به گونه‌ای که صرفا با کلیک ساده می‌توان اعمال مجرمانه‌ای با تبعات بالا ایجاد نمود. جرایم سایبری با فراملی بودن به صورت پنهان و از طریق عبور از مرزها بدون احتیاج به اسناد و اطلا وقوع می‌پیوندد؛ علاوه بر این با توجه به بکارگیری ابزار هوشمند جهت ارتکاب فضای سایبر و امکان جابه‌جایی سریع مکان ارتکاب جرم، می‌توان تبعات و آ گسترده و گاها جبران ناپذیری را با وقوع چنین جرایمی فرض نمود. از جمله جرایم سایبری که در قوانین داخلی ایران همچون بسیاری از کشورها و اسناد مورد غفلت قرار گرفته است؛ بزه تروریسم سایبری می‌باشد. تروریسم سایبری گونه‌ای از تروریسم مدرن، نمایان‌گر آسیب‌پذیر بودن تابعان حقوق بین‌الملل در می‌باشد. در واقع امروزه با توجه به گسترش فضای سایبر و وقوع اعمال مجرمانه بستر فضای مذکور تروریسم از یک تهدید ملی به یک تهدید بین‌المللی بدل همواره خوف آن وجود دارد که با گسترش آن صلح و امنیت بین‌المللی به متاسفانه با وجود اهمیت تروریسم سایبری نه در قوانین داخلی ایران و نه در اسناد المللی تاکنون تعریف مشخصی از این بزه صورت نپذیرفته است که به تبع عدم و قانونی و مشخص در این زمینه مصادیق و شمول آن نیز مشخص نمی‌باشد. می‌تواند کشورها را در پیشگیری و مقابله و مواجهه و مجازات مرتکبان این‌گونه جرایم مشکل سازد. مطالعه‌ی حاضر درصدد است تا با بیان مفهوم تروریسم و گونه‌های تعریفی از تروریسم سایبری دست یابد؛ و قوانین داخلی ایران و اسناد بین‌المللی در این خصوص که ایا در آن‌ها اشاره‌ای به تروریسم سایبری شده است یا خیر و مقابله و مواجهه با تروریسم سایبری در قوانین و اسناد مذکور مورد بررسی قرار گیرد. به می‌رسد؛ چه در نظام حقوقی ایران و چه در نظام حقوقی بین‌المللی با توجه به اسناد و

قوانین مذکور می‌بایست تفسیری موسع از آن‌ها ارائه داد تا بتوان اقدام به مقابله و شناسایی بزه تروریسم سایبری نمود در غیر این صورت با توجه به تبعات تروریسم سایبری، مرتکبان آن بدون کیفر باقی می‌مانند؛ از سویی دیگر نیز می‌توان ارائه تفسیری موسع از اسناد و قوانین را نقضی بر اصل قانونی بودن جرم و مجازات به عنوان یکی از اصول مسلم حقوق دانست؛ بنابراین شایسته است که دست‌اندرکاران نظام تقنینی در خصوص جرم‌انگاری تروریسم سایبری و بیان مختصات و مصادیق آن اقدامات لازم را به عمل آورند.

مقدمه

از جمله تهدیداتی که به سبب گسترش فضای اینترنت و سایبر بروز خارجی پیدا نمو
امروزه به عنوان یکی از مهم‌ترین جرایم ارتکابی در فضای سایبر مطرح می‌شود، بزه تر
سایبری می‌باشد. بزه مذکور در تقسیم‌بندی صورت گرفته از تهدیدات سایبری
یکی از مهم‌ترین تهدیدات سایبری نام برده می‌شود که می‌تواند ضربات سنگی
جوامع مختلف وارد سازد. تحولات شگرف و سریع فضای اینترنت و فناوری اطلا
شد تا این فضا بستر مناسبی جهت اعمال تروریستی محسوب شود. در واقع گرو
تروریستی نیز همسو با پیشرفت تکنولوژی و ارتباطات اهداف خویش را پیگیری م
این روست که ضرورت و اهمیت بررسی بزه تروریسم سایبری احساس می‌شود؛ بنا
مطالعه‌ی حاضر تلاش بر این است تا سابقه تقنینی و حقوقی بزه مذکور در نظام حقو
ایران مورد رسیدگی و بررسی قرار گیرد. نگارنده در این مطالعه ابتدائا به بیان کل
موضوع شامل بیان مسئله، ضرورت مطالعه، پیشینه موضوع، ... پرداخته است. سوا
در این خصوص مطرح می‌باشد؛ تروریسم سایبری چیست و آیا در اسناد بین‌المللی
داخلی ایران به صراحت مورد پیش‌بینی قرار گرفته است یا خیر؛ و دیگر این‌که
قابل قبولی در مواجهه با پدیده تروریسم سایبری در نظام حقوقی ایران و اسناد
وجود دارد یا خیر. پاسخ به این سوال می‌طلبد ابتدا مفهوم تروریسم و انواع آن ا
سپس بعد از بیان مفاهیم به جستجوی مفهوم تروریسم سایبری در میان مجموع
اسناد بین‌المللی بپردازیم. به همین جهت فصل اول به بیان مفاهیم و اصطلا
اسناد بین‌المللی، فضای سایبر، تهدیدات سایبری، جرایم سایبری، تروریسم
سایبری، ... می‌پردازد. در بیان مفهوم تروریسم سایبری می‌توان گفت، اصطلاح م
هرگونه تعریف مشخص و صریح در قوانین داخلی و اسناد بین‌المللی می‌باشد.
اصطلاح را می‌توان این‌گونه تعریف نمود که: هرگونه حمله یا تهدید علیه رایانه‌ها، شب
رایانه‌ای و اطلاعات ذخیره شده در سامانه‌های رایانه‌ای را می‌توان تروریسم سایبری
البته با توجه به عدم وجود تعریف متقن و گویایی در این خصوص می‌توان تعریف
را مصداقی از تروریسم سایبری دانست. علاوه بر موارد پیش‌گفته، در فصل اول ویژگی‌های

سایبر تروریسم نیز بیان می‌شود. ویژگی‌هایی چون تعدد بازیگران در فضای سایبر، هزینه کم ورود، صرف زمان کم، ناشناس ماندن مرتکبین این عرصه، تاثیرگذاری شگرف، ... از جمله این ویژگی‌ها می‌باشد. ویژگی‌های مذکور سبب تمایز جدی تروریسم سایبری با دیگر جرایم سنتی و همچنین سایر جرایم رایانه‌ای می‌باشد. در این فصل تقسیم بندی تروریسم به نارکو تروریسم، تروریسم ملی‌گرا، تروریسم سیاسی و مذهبی؛ همچنین بیان گونه‌های تروریسم چون تروریسم فردی و خودانگیخته، گروهی یا سازمان یافته، دولتی، سیاسی یا غیرسیاسی، نژادی، ... صورت پذیرفته است. فصل دوم به بررسی مواجهه با تروریسم سایبری در اسناد بین‌المللی و حقوق کیفری ایران اختصاص یافته؛ در این فصل مبارزه با تروریسم سایبری به عنوان حق و تکلیفی برای دولت‌ها در نظر گرفته شده است. در واقع رشد و گسترش پدیده تروریسم در سال‌های اخیر به ویژه مدرن شدن تروریسم که تروریسم سایبری را می‌توان یکی از اشکال نوین تروریسم دانست؛ حوزه‌های مختلف بین‌المللی را درگیر خود ساخت. در حقوق بین‌الملل تعیین حدود و مقابله با تروریسم سایبری نسبت به دیگر حوزه‌های مطرح، روند حرکتی نسبتا کندی را داشته است که دلیل این امر را می‌توان اصل ممنوعیت استفاده از زور دانست. مطابق اصل مذکور استفاده از زور در روابط بین‌الملل ممنوع می‌باشد؛ امری که با استثنائاتی چون حق دفاع مشروع قابل توجیه می‌باشد. در هر حال اسناد بین‌المللی خاصی وجود دارد که هر چند در مجموع تاکنون نتوانسته‌اند بیان صریح و حد و مرز مشخصی از تروریسم سایبری به دست دهند لکن شایان توجه می‌باشند. اسناد بین‌المللی چون کنوانسیون جامع مقابله با تروریسم، کنوانسیون بین المللی منع بمب‌گذاری‌های تروریستی، کنوانسیون جرایم سایبری اروپا، ... در فصل دوم مورد بررسی قرار گرفته‌اند. تمامی کنوانسیون‌ها و اسناد بین‌المللی مذکور در خصوص تروریسم سایبری وجه مشترکی دارند که طبق آن تمامی اسناد مذکور فاقد تعریف روشن و مبرهنی در خصوص بزه تروریسم سایبری می‌باشد ولی با این وجود می‌توان از کلیت و مقررات مطرح شده در آن‌ها در خصوص تروریسم سایبری نیز بهره جست. موارد دیگری که در فصل دوم مورد بررسی قرار گرفته‌اند؛ راهکارهای حقوقی در مقابله با تروریسم سایبری می‌باشد که در این بخش قواعد شکلی و ماهوی حقوق کیفری ایران مورد بررسی قرار گرفته است. مبحث دیگر پیشگیری از تروریسم سایبری می‌باشد؛ که در دو بخش پیشگیری کیفری و غیرکیفری بیان

شده است. در بحث پیشگیری کیفری قوانین ماهوی موجود در نظام حقوقی ایران همچون قانون جرایم رایانه‌ای، قانون تجارت الکترونیک، ... که به نوعی می‌توان گفت علاوه بر جنبه واکنشی و سرکوب‌گرانه جنبه پیشگیرانه نیز دارند، بیان می‌شود. در بحث پیشگیری، غیرکیفری نیز پیشگیری وضعی و اجتماعی از تروریسم سایبری مورد مطالعه قرار گرفته است. در ادامه، به بیان نتیجه‌گیری و پیشنهادات پرداخته می‌شود که در جای خود مورد بحث قرار می‌گیرد.

گسترش فزاینده «فناوری اطلاعاتی و ارتباطاتی» منجر به تحول و دگرگونی جوامع در ابعاد مختلف سیاسی، امنیتی، اقتصادی و اجتماعی شده است. ویژگی‌های جوامع امروزی همچون «اقتصاد اطلاعاتی»، «فرهنگ مجازی» و کاهش اهمیت زمان و مکان در تعاملات اجتماعی، ویژگی متمایزی به هزاره سوم بخشیده که اصل بنیادین آن اهتمام محوری فرد در عرصه فعالیت‌های اجتماعی، سیاسی و اقتصادی با بهره‌گیری از ابزارهای نوین اطلاعاتی و ارتباطی است. در چنین فضایی که با عنوان «فضای مجازی» توصیف می‌شود، تهدیدهای نوینی همانند جنگ مجازی، «جنگ اطلاعاتی»، تروریسم سایبری، «پدیده هکرها» و سرقت اطلاعات محرمانه نهادهای امنیتی و اطلاعاتی پدید آمده‌اند که می‌توانند امنیت ملی کشورها را با چالش جدی مواجه سازند. به علاوه، پیشرفت فنی در زمینه ارتباطات، موجب ظهور قواعد حقوقی و به تبع آن، رفتارهای نوین فاصله گیر از هنجارها شده است که این موضوع، نه تنها اموال، بلکه اشخاص و دولت‌ها را نیز در بر می‌گیرد و آنها را تحت حمایت قرار می‌دهد.

دوران معاصر، عصر اطلاعات، دانش یا ارتباطات نام گرفته است[1]. در این دوران تمام جوامع در این کره خاکی برای بسیاری از امور خود از جمله فراغت و تفریح، کنترل مراکز و ... بهره‌برداری از دریا، خشکی و فضا از وسایل الکترونیکی و شبکه اینترنت بهره می‌گیرند. با اینکه عصر اطلاعات شرایط زندگی ما را به نحو سودمندی تغییر داده است؛ نمی‌توان از مضرات آن نیز غافل شد. شاید بتوان عصر اطلاعات را تیغی دولبه دانست که در عین خدماتی که به ما ارائه می‌دهد، خطرهایی مثل سایبر تروریسم نیز دارد. امروزه در عرصه بین

[1] Rowe, A.J and S.A Davis: (1996) : the Intelligent Information Systems: Meeting the Challenge in the Knowledge Era, Greenwood Publishing Group.

المللی در پذیرش تروریسم سایبری به عنوان نوع جدیدی از تروریسم کمتر تردیدی وجود دارد. شورای اروپا در گزارش وضعیت خود در سال ۲۰۰۴ با عنوان «جرایم سازمان‌یافته در اروپا: تهدید جرایم سایبری» با تصریح به اینکه تروریسم سایبری تهدید و نوع جدید و ویژه‌ای از تروریسم مدرن است، بر این نظر صحه گذاشته و به تعریف و بررسی جنبه‌های مختلف تروریسم سایبری پرداخته است[1]. این پدیده نوین از لحاظ حقوقی به حد کافی بررسی نشده و بیشتر تحلیل‌ها از لحاظ سیاسی و امنیتی بوده است.

در این میان، یکی از مهم‌ترین تهدیدهای نوظهور، تروریسم سایبری است که به واسطه کاربست فزاینده فناوری‌های اطلاعاتی و ارتباطی از سوی دولت‌ها برای تسریع، افزایش کارایی و کاهش هزینه‌های مرتبط با خدمت‌رسانی به شهروندان، اهمیت فزاینده‌ای پیدا کرده است. به گونه‌ای که حتی دولت‌ها نیز از تروریسم سایبری به عنوان ابزاری در الگوهای تنازعی خود استفاده می‌کنند. در این میان، مهم‌ترین مولدهای ناامن‌کننده فضای مجازی در بعد تروریسم، در دو گروه عمده طبقه بندی می‌شوند؛ گروه اول، کسانی که به یک کشور خارجی وابسته‌اند، از قبیل بخش‌های نظامی، سازمان‌های امنیتی و شرکت‌هایی که وابستگی زیادی به دولت آن کشور دارند؛ و گروه دوم: تروریست‌ها و گروه‌های افراطی. این افراد، ممکن است به دولت خاصی وابستگی نداشته باشند، ولی در جهت اهداف خود به خرابکاری مبادرت می‌کنند[2].

تروریسم سایبری که با ویژگی‌های متمایزکننده‌ای مشخص می‌شود؛ این چالش را که آیا برنامه ضد تروریستی حاضر کفایت می‌کند یا باید اسناد جدیدی تنظیم شود، پیش روی حقوق‌دانان بین‌الملل قرار می‌دهد. مفاد کنوانسیون‌های ضد تروریسم مورد بررسی با مرور زمان پیشرفت کرده است. حقوق از واژه‌شناسی به نسبت محدود کنوانسیون مونترال کامل‌تر شده تا عباراتی مانند «هرگونه ادوات دیگر» یا «به هر وسیله» را در کنوانسیون بین‌المللی سرکوب بمب‌گذاری‌های تروریستی در بر بگیرد. مورد دوم: تفسیر انعطاف‌پذیرتر شروط حقوقی را که باید به منظور اثبات مسئولیت قانونی در برابر تروریست‌های سایبری برآورده

---

[1] Council of Europe. Convention on Cybercrime. European Treaty Series- No. 175. Budapest 2001.

[2] مرتضی نورمحمدی؛ (۱۳۹۰)؛ سایبر تروریسم؛ تروریسم در عصر اطلاعات، (به اهتمام عباس‌علی کدخدایی و نادر ساعد)، تهران: انتشارات مجمع جهانی صلح اسلامی. ص ۷۷

شوند؛ ممکن می‌سازد. قابل تصور است که این تفاوت‌ها که ناشی از پیشرفت و توسعه سریع فناوری مدرن در سه دهه اخیر هستند؛ منجر به تفاهم در میان جامعه حقوقی بر سر این موضوع شده که تروریسم می‌تواند خود را از طریق این فناوری‌ها نشان دهد؛ بنابراین، پیش‌نویس کردن کنوانسیون‌ها حساسیت بیشتری نسبت به ضرورت سازگاری با پیشرفت‌های آینده پیدا کرده است[1].

البته مقابله و مواجهه با سایبر تروریسم با سه چالش عمده و اساسی روبه رو است، مشکلات موجود بر سر راه تعریف صحیح و واقعی از این پدیده، وضعیت نامناسب تقنینی و نیز ضعف زیرساخت‌های حیاتی جوامع در مقابل تروریست‌های سایبری. لذا این نوشتار در پی تبیین بررسی تحلیلی تروریسم سایبری در نظام کیفری و راهکارهای مقابله با آن می‌باشد. بدین منظور رویکرد حقوق کیفری ایران نسبت به جرایم تروریستی سایبری مورد بررسی قرار خواهد گرفت. این بررسی با مقایسه و تطبیق با برخی از اسناد بین‌المللی در این زمینه صورت می‌گیرد.

تروریسم پدیده‌ای است که برخی جوامع و دولت‌ها واقعیت آن را پذیرفته و آن را همچون تهدیدی جدی بر ضد خود می‌دانند و در برابر، برخی جوامع و دولت‌ها آن را نپذیرفته و ساخته و پرداخته‌ی دولت‌های ابرقدرت می‌دانند. قدر مسلم، وجود پدیده تروریسم مسجل و مسلم است و جدا از انگیزه و هدف تروریست‌ها در انجام رفتارشان و تنها با تکیه بر نتیجه عمل آنها باید پذیرفت که تاریخ مشحون از وقایع تروریستی است. با این حال هرچند در جهان گذشته ردپای تروریسم بیشتر به حاکم‌کشی، دولت‌مردکشی و کشتن افراد تعیین شده، برجای مانده است ولی تروریسم آن قدر گسترده و نیرومند است که همگام با تحولات جوامع، متحول شده و هر روز چهره جدیدی از خود نشان می‌دهد؛ چندان که محدود کردن آن به نمونه‌های تاریخی خشونت‌ورزی در جهان فیزیکی شناخت آن را با مشکل مواجه می‌سازد. دست‌یابی تروریست‌ها به سلاح‌های کشنده تشعشعی میکروبی، شیمیایی وهسته‌ای دورنمای خطرناکی را از تروریسم ترسیم می‌نماید و در کنار این‌ها باید اقدامات تروریستی سایبری یعنی تروریسم در جهان مجازی را نیز افزود که به عقیده برخی با توجه به ویژگی‌

---

[1] پیمان نمامیان؛ (۱۳۹۲)؛ مواجهه با تروریسم سایبری در حقوق بین‌الملل کیفری، فصلنامه پژوهش‌های ارتباطی، سال بیستم، شماره‌ی ۱، ص ۴۰

های منحصر به فرد فضای سایبر و دسترسی آسان تروریست‌ها به سلاح‌های سایبری (یک رایانه و اینترنت در هر جایی) به مراتب محتمل‌تر و پیچیده‌تر و خطرناک‌تر از سایر اقسام جدید تروریسم می‌نماید[1]. از این رو ضرورت و اهمیت بررسی موضوع مورد مطالعه را می‌توان توان از چندین منظر بررسی کرد. اولاً سابقه‌ی بررسی حقوقی و تقنینی از این موضوع در ایران اندک و انجام آن امری بدیع و جدید می‌باشد. ثانیاً انجام چنین مطالعه‌ای منجر به آشکار نمودن ضعف حمایتی زیرساخت‌های حیاتی و بنیادین جوامع، نشان دادن فقدان سیاست تقنینی و حمایت‌های اجتماعی لازم شده و به ارائه راه‌کارهای موثر در مقابل پدیده مجرمانه تروریسم سایبری منجر می‌شود. ثالثاً توصیف پدیده تروریسم سایبری و نشان دادن آسیب‌پذیری جوامع مختلف در برابر پدیده مذکور، با انجام چنین مطالعه‌ای صورت می‌گیرد.

- **پیشینه مطالعه**

نامیان (۱۳۹۲)، در پژوهشی با عنوان «مواجهه با تروریسم سایبری در حقوق بین¬الملل کیفری» بیان داشته است: «تروریسم سایبری یکی از روزآمدترین مصادیق تروریسم است که به سبب بهره¬گیری غیرقانونی از فناوری و ابزارهای الکترونیکی و رایانه¬ای در فضای مجازی، به طور عمده از سوی بازیگرانی که به این علوم نوین دسترسی دارند وآنها را در راه اهداف راهبردی علیه ملت¬های جهان سوم به کار می¬گیرند، موجبات تهدیدهای فزاینده¬ای را در عرصه بین¬المللی فراهم کرده است. از این رو، فارغ از اینکه در اغلب موارد، غرب به عنوان منشأ اصلی راهبردی کردن تروریسم سایبری، خود مدعی مقابله با آن است؛ اسنادی بین¬المللی به منظور پیشگیری و سرکوب کلیه اشکال تروریسم به ویژه تروریسم سایبری، تدوین و تصویب شده است که از منظر آسیب¬شناختی می¬توان گفت اسناد مزبور نه تنها توفیقی در مقابله با این پدیده نوظهور نداشته¬اند، بلکه شکاف¬های موجود و زمینه رشد و گسترش فزاینده آن را در عرصه¬های ملی و بین-المللی فراهم کرده¬اند. به این ترتیب، در مقاله حاضر، ضمن بررسی و تبیین تروریسم سایبری و ارائه مفاهیم گوناگون از آن، اسناد بین المللی در چارچوب حقوق بین الملل کیفری مورد ارزیابی قرار خواهد گرفت».

---

[1] Brenner, Susan W. and Goodman, Mark D; In defense of Cyber terrorism: Anargument for anticipating cyber-attacks, Journal of law, technology and policy, 2002, P.12.