تروریسم سایبری و اعمال صلاحیت کیفری
از منظر حقوق بین‌الملل

مؤلفان: سیده پریسا میرابی
رضا خواجه نورالدینی

نشر راشدین

سرشناسه : میرابی، سیده پریسا، ۱۳۶۴ -
عنوان و نام پدیدآور : تروریسم سایبری و اعمال صلاحیت کیفری از منظر حقوق بین‌الملل/مولفان سیده پریسا میرابی ،رضا خواجه‌نورالدینی.
مشخصات نشر : تهران : راشدین ، ۱۳۹۷.
مشخصات ظاهری : ۱۹۱ ص.
شابک : ۵-۵۶۲-۳۶۱-۶۰۰-۹۷۸
وضعیت فهرست نویسی : فیپا
یادداشت : کتابنامه: ص.۲۱۱.
موضوع : تروریسم رایانه‌ای
موضوع : Cyberterrorism
موضوع : صلاحیت رسیدگی به امور کیفری (حقوق بین‌الملل)
موضوع : (International law (Criminal jurisdiction
شناسه افزوده : خواجه نورالدینی، رضا، ۱۳۵۲ -
رده بندی کنگره : ۱۳۹۷HV۶۷۷۳ ۴ت۹م/
رده بندی دیویی : ۳۶۳/۳۲
شماره کتابشناسی ملی : ۵۳۴۶۴۰۰

انتشارات راشدین	
عنوان کتاب:	تروریسم سایبری و اعمال صلاحیت کیفری از منظر حقوق بین‌الملل
مؤلفان:	سیده پریسا میرابی، رضا خواجه نورالدینی
صفحه‌آرا:	مونا اسماعیلی
طراح جلد:	علی زند
نوبت چاپ:	اول -۱۳۹۸
شمارگان:	۱۰۰۰
شابک:	۵-۵۶۲-۳۶۱-۶۰۰-۹۷۸
قیمت:	۳۰۰۰۰۰ ریال
نشانی:	میدان انقلاب ـ کارگر جنوبی- بن‌بست گشتاسب - پلاک ۴ واحد۶
تلفن/ نمابر:	۶۶۴۰۸۲۲۴ ـ ۶۶۱۲۳۴۴۹
پایگاه اینترنتی:	www.siteketab. com
پست الکترونیک:	rashed۱۸۲۹@yahoo. Com heydari_alireza۴۱@yahoo.com

دیباچه

پیشرفت و توسعه رایانه فرصت‌های جدیدی برای اشخاصی که تمایل به فعالیت های غیرقانونی دارند، ایجاد کرده است، به‌طوری که مصادیق جدیدی از فعالیت های مجرمانه پدیدار شده است که چالش های قانونی برای نظام حقوقی و همچنین اجرای قانون فراهم کرده است.
در دنیای سایبر قلمرو یا مرز مشخصی وجود ندارد و فقط با یک کلیک ساده می تواند جرمی صورت گیرد.
جرایم سایبری به صورت پنهان، در سراسر جهان از طریق عبور مرزها بدون نیاز به اسناد یا اطلاعات و نقاط بازرسی ارتکاب می یابند. علاوه بر این، آنها معمولاً توسط ابزار هوشمندانه و قصد مجرمانه مکان های خود را تغییر داده تا بتوانند حملات و صدمات بیشتری ایجاد نمایند.
باتوجه به اینکه حملات تروریستی سایبری می تواند در چند کشور ارتکاب یابد، نحوه اعمال صلاحیت و روند پیگرد قانونی دشوار است. بنابراین، سازوکار مشترک قانونی دولت ها در پاسخگویی به این جرایم ضروری است. این ضرورت ایجاب می‌کندکه کشورها اقدامات لازم برای تدوین و اجرای قوانین در راستای تحقق عدالت و اعمال حاکمیت خود را اتخاذ کنند، همچنین باید اقدامات و راه‌کارهای جلوگیری از رشد سریع تروریسم سایبری را بکار گیرند و سرانجام تعقیب قانونی موثر را که یکی از روشهای بازدارنده و پیشگیرانه در امر مبارزه با تروریسم سایبری است، به واقع بکار گیرند.
هر چند کشورها با سازوکار قانونی خود می‌توانند علیه سوء استفاده از فناوری های جدید اقدام کنند، با این وجود این مکانیسم باید توسط موافقتنامه های بین المللی و مشارکت سازمان های بین المللی در راستای هماهنگ‌سازی قوانین و اجرای آن مورد پشتیبانی قرار گیرد. در این راستا مسئله اصلی، اعمال صلاحیت کیفری در جامعه جهانی تعارضی است که در اعمال صلاحیت سرزمینی و یا تابعیتی، صلاحیت شخصی (فعال و منفعل)، صلاحیت

واقعی یا حمایتی، صلاحیت جهانی (محدود یا نامحدود) در فضای سایبر وجود دارد. به طوری‌که گام‌های بسیاری در مبارزه با تروریسم سایبری، از قانونگذاری تا اجرای قانون صورت گرفته است اما این تلاش ها کافی نبوده و همکاری های بین المللی در این حوزه ضروری به نظر می رسد.

این اصول باید ضمن احترام به حاکمیت دولت ها و با احراز شرایط لازم برای همکاری های بین‌المللی؛ صلاحیت اصلی و اولیه را به عنوان اقتدار قانونی برای یک کشور حفظ نموده و ملاک و مبنای حق اعمال و اجرای قوانین آن کشور بر افعال اشخاص حقیقی و حقوقی وپیامدهای عملکرد آنان را لحاظ نماید.

با این حال تردیدی نیست که گاه تعدد صلاحیت‌ها، عدم شناسایی در انتساب و تعیین هویت مجرمان، پیگرد جرایم سایبری در سطح بین المللی را همچنان دشوار خواهد کرد و اینکه ماهیت فراملی جرایم و تروریسم سایبری منجر به پیچیدگی‌های قانونی شده، در نتیجه تحقیقات و پیگرد قانونی را دشوار نموده است. فضای سایبر یک جهانی فراتر از مرزهای ژئوپلتیک ملی است و صلاحیتها تعیین کننده اقتدار و اختیارات دادگاه کشورها و نقطه کانونی برای رسیدگی به جرایم بین المللی است.

بنابراین دولت‌ها باید در جهت توسعه و تقویت چارچوب قانونگذاری برای استفاده از تکنولوژی ارتباطات و اطلاعات با تکیه بر حقوق ملی و بین المللی تلاش نموده و در جهت ایجاد سازوکار قانونی مشترک در جرایم سایبری با اجتناب از طولانی شدن بی جهت رسیدگی به این هنجارشکنی‌ها تلاش نمایند.

علیرضا دیهیم

اسفندماه ۱۳۹۷

فهرست مطالب

پیشگفتار

درحالی که رشد سریع تکنولوژی برای بشریت سودمند است، تروریسم سایبری، به یکی از تهدیدات خطرناک جهانی تبدیل شده است. فقدان مرز و محدوده به شکل سنتی، اقدامات مجرمانه در این فضا، صلاحیت محاکم رسیدگی کننده را به چالش کشیده است. وقوع حملات سایبری روزافزون علیه کشورهای مستقل و زیرساخت‌های اطلاعات اساسی آنها، واکنش جهانی را ضروری می کنند. جامعه بین المللی همواره تلاش کرده است ازطریق انعقاد معاهدات دو یا چند جانبه، زمینه همکاری در رسیدگی به جرایم سایبری و تروریستی را فراهم کند؛ اما توافقنامه های منطقه ای و دوجانبه و قوانین محلی برای جلوگیری از حملات سایبری کافی نیست. گرچه معاهدات بسیاری وجود دارد، اما هیچ یک از آنها مجوز قانونی لازم برای اعمال قدرت قاهره قضایی، تعقیب و رسیدگی فرامرزی را فراهم نمی کند. اکثر آن معاهدات به طور محدود و در سطح منطقه‌ای اعمال می‌شوند،که البته به منظور دستیابی به درک مشترک در کاهش تهدیدات تروریسم سایبری، باید راه حل های موجود ارائه شده در معاهدات بین المللی در نظر گرفته شوند تا پاسخ‌های موجود در برابر تهدیدهای سایبری فراملی بررسی شود. در حال حاضر، بسیاری از سازمان‌های بین‌المللی تلاش هایی را برای مبارزه با این تهدید انجام داده اند. سازمان ملل متحد و اینترپول امنیت را ترویج می دهند و سعی می کنند از جرایم سایبری در سطح بین المللی جلوگیری کنند. مهمترین معاهده در این خصوص کنوانسیون جرایم سایبری است. گرچه کنوانسیون جرایم سایبری به عنوان یک تلاش منطقه ای در مبارزه با تروریسم سایبری طبقه بندی شده است، اما در این مورد نقش مهمی ایفا می کند، زیرا تعدادی از کشورها که در خارج از منطقه قرار دارند، آن را تصویب نموده و عضو این کنوانسیون شده‌اند؛ با این حال، معروف ترین معاهده در زمینه جرایم سایبری، تروریسم سایبری را شامل نمی شود. تروریسم سایبری یک جنایت بین المللی است و قوانین داخلی به تنهایی قادر

به مقابله با چنین حملاتی نیست؛ بنابراین آنها نیاز به پاسخ فراملیتی و جهانی دارند. جرایم تروریست سایبری ماهیتاً منجر به پیچیدگی های قانونی می شود و تعقیب و تحقیق و پیگرد قانونی را دشوار می سازد. عدم هماهنگی در قانون گذاری در میان کشورها به مشکلاتی در زمینه تعقیب و پیگرد قانونی منجر می گردد. از آنجایی که اعمال صلاحیت (شخصی، سرزمینی، جهانی، واقعی و ...) همه موارد تروریسم سایبری را پوشش نمی دهد، بهترین کار، اضافه کردن یک پروتکل ویژه مربوط به تروریسم سایبری است. همچنین، از آنجایی که قوانین ملی به تنهایی نمی توانند نقش بازدارنده یا مبارزه با این نوع جرایم را داشته باشند؛ به یک سازمان بین المللی برای جلوگیری و دفاع از ملت ها از حملات تروریستی سایبری نیاز است که باید از طریق همکاری های چند ملیتی وسازمان های بین المللی برای مقابله با جنایات تروریستی از آن بهره برد.