Journal of Socio-Political Developments in Contemporary Iran

http://doi.org/10.30510/pscci.2025.545896.1334

# Cyberterrorism and the policy of measures to prevent it in international documents and Iran

Jamal Yousefi1
Hassan Moosaghi2*
Naser Rahbarfarshpira3

Received: 26 April 2025

Reception: 6 September 2025

Abstract

Cyberterrorism is one of the latest examples of terrorism that leads to the illegal use of technology and electronic and computer devices in the cyber world, prominently by individuals who have access to this new knowledge and use it for fundamental purposes against underdeveloped countries. It has caused numerous threats in the international framework. The goal of cyberterrorism is to prevent the occurrence of cyberterrorism in favor of the victims, but in most legal systems in the world, cyberterrorism has not been explicitly and specifically criminalized. The present article, which was conducted using a descriptive-analytical method and using library resources, seeks to identify and analyze the strategies for preventing cyberterrorism in international documents. The results of the research show that international documents have been developed and approved regarding the prevention and suppression of all types of terrorism, especially cyberterrorism, but these documents have not been successful in dealing with this phenomenon in terms of pathology, but have caused gaps in this field.

Keywords: terrorism, cyberterrorism, criminal prevention, non-criminal prevention

1- PhD student, Department of Law, Aras International Branch, Islamic Azad University, Tabriz, Iran.
2- Associate Professor, Department of Law, Aras International Branch, Islamic Azad University, Tabriz, Iran. (Corresponding author)
3- Assistant Professor, Department of Law, Aras International Branch, Islamic Azad University, Tabriz, Iran. Email: javaid.rahbar

فصلنامه تحولات سیاسی اجتماعی معاصر ایران، سال چهارم، شماره پنجم، ویژه نامه۱٤۰٤، صص ۳۰۰-۲۷۶

http://doi.org/10.30510/pscci.2025.545896.1334

# تروریسم سایبری و سیاست تدابیر پیشگیری از آن در اسناد بین المللی و ایران

جمال یوسفی[۱]
حسن موثقی[۲*]
ناصر رهبرفرش پیرا[۳]

تاریخ دریافت :۰٦ /۱٤۰٤/۰۲
تاریخ پذیرش: ۱٤۰٤/۰٦/۱۵

## چکیده

تروریسم سایبری یکی از جدیدترین مصادیق تروریسم می‌باشد که منجر به استفاده غیرقانونی از فناوری و وسایل الکترونیکی و کامپیوتری در دنیای سایبری، به شکل برجسته از جانب اشخاصی که به این دانش نوین دسترسی دارند وآن را در راه مقاصد اساسی علیه کشورهای توسعه نیافته مورد استفاده قرار می‌دهند. سبب تهدیدهای فراوانی را در چارچئب بین المللی مهیا نموده است. پیشگیری از وقوع تروریسم سایبری به طرفداری از بزه دیدگان هدف آن است، لیکن در بین بیشتر نظام‌های حقوقی دنیا، به صورت صریح و ویژه به جرم‌انگاری تروریسم سایبری اقدام نشده است. نوشتار حاضر که با روش توصیفی-تحلیلی و استفاده از منابع کتابخانه‌ای انجام شده است، در پی شناخت و تحلیل راهبردهای پیشگیری از تروریسم سایبری در اسناد بین‌المللی می‌باشد. نتایج پژوهش نشان می‌دهد که اسناد بین المللی در رابطه با پیشگیری و سرکوب همه‌ی انواع تروریسم به ویژه تروریسم سایبری تدوین و تصویب شده، اما این اسناد از لحاظ آسیب شناختی نه موفقیتی در امر با این پدیده نداشته، بلکه موجب شکاف های موجود در این زمینه شده است.

**کلیدواژه‌ها**: تروریسم، ترویسم سایبری، پیشگیری کیفری، پیشگیری غیر کیفری

۱دانشجوی دکتری گروه حقوق، واحد بین‌الملل ارس، دانشگاه آزاد اسلامی، تبریز، ایران.
۲دانشیار گروه حقوق، واحد بین‌الملل ارس، دانشگاه آزاد اسلامی، تبریز، ایران. (نویسنده مسئول)
۳ستادیار گروه حقوق، واحد بین‌الملل ارس، دانشگاه آزاد اسلامی، تبریز، ایران.

**مقدمه**

یکی از معضلات دنیای حاضر جرایم در فضای سایبر است و یکی از انواع جرایم سایبری، تروریسم سایبری است. تروریسم پدیده جدیدی نیست، تاریخ آکنده از اقدامات منحوس تروریستی است که با اهداف مختلف ارتکاب یافته زندگی افراد بی‌گناه فراوانی را سلب کرده و حقوق، آزادی‌ها و امنیت اشخاص را به خطر لنداخته است. با ورود به دوره اطلاعات، چگونگی و شرایط جنگ‌ها از ابهام مفهومی و روش خیلی زیادی برخوردار شده و ابعاد جدیدی از درگیری در محیط سایبر ایجاد شده است. البته ماهیت چند رسانه‌ای فضای سایبر، به تروریست‌ها مکان بهره‌برداری‌های سوء دیگری را هم داده است. تروریسم سایبر، اقدامی خشونت آمیز و مجرمانه است، که با اهداف سیاسی و براندازی حکومت‌ها یا صدمه زدن به آن‌ها ارتکاب می‌یلبد. در این گونه عملیات و اقدامات نوک پیکان حمله به سمت حکومت است و در این میان تاسیسات و زیرساخت‌های حیاتی، به طور مستقیم و جان و مال افراد به صورت غیرمستقیم مورد تعرض قرار می‌گیرد. این موضوع ضرورت مبارزه و برخورد کیفری با این قبیل جرایم را دو چندان می‌کند.

پیشگیری از تروریسم سایبری با هدف حمایت از بزه‌دیدگان آن می‌باشد، لیکن در بیشتر نظام‌های حقوقی، به جرم انگاری تروریسم سایبری به شکل صریح و ویژه اقدام نشده است. بعضی مواد قانونی در حقوق ایران حاکی از آن است که در مورد پیشگیری از این جرم در حقوق کیفری ایران، مقرره‌ی مخصوصی وجود ندارد، بلکه با اتکاء به بعضی قوانین عام نظیر قانون جرایم رایانه‌ای و قانون مجازات اسلامی می‌توان مواضع پیشگیرانه حقوق کیفری ایران را در خصوص پیشگیری از جرم تروریسم سایبری و طرفداری از بزه دیدگان آن اشاره نمود. علاوه بر این با ملاحظه‌ی اسناد بین‌المللی در مورد جرایم سایبری و تروریستی و انواع قطعنامه‌های سازمان‌های بین‌المللی و منطقه‌ای که سازمان ملل متحد در اساس آن‌ها واقع شده است، به این نتیجه نایل می‌شویم که در عرصه فراملّی، اقدامات مناسب و کافی با هدف پیشگیری از تروریسم سایبری صورت نگرفته است. سازمان ملل متحد، به مثابه عظیم‌ترین نهاد بین‌المللی، از سال ۱۹۶۳ تا امروزه، در خصوص تروریسم و اعمال تروریستی، ۱۳ سند بین‌المللی به تصویب رسانده ولی صرفا در سه سند به صورت صریح به اصطلاح «تروریسم» اشاره نموده و در سایر آن‌ها صرفا مصادیق اعمال تروریستی را احضا نموده است. لذا در این نوشتار به بررسی اسناد بین‌المللی که برای مقابله با تروریسم سایبری تدوین شده و

نیز اقدامات پیشگیرانه از تروریسم سایبری (کیفری و غیرکیفری) که در اسناد بین‌المللی بدان اشاره شده است، می‌پردازیم.

**۱-تروریسم سایبری**

تروریسم سایبری برگرفته از دو اصطلاح «تروریسم» و «سایبر» است، از این رو در طول این دو قرار می‌گیرد. با وجود آن که عمر واژه‌ی «تروریسم سایبری» به دو دهه نمی‌رسد، ولی در همین مدت تعاریف بسیاری برای آن ارائه شده است. عبارت فوق با ترکیب کلمه‌های «تروریسم» و «سایبر« در دهه ۱۹۸۰ به وسیله‌ی بری کلین[1]، محقق ابداع شد و آن را این گونه تعریف نمود: «سوء استفاده عمدی از یک سیستم، شبکه یا مولفه اطلاعاتی رایانه‌ای جهت تحقق هدفی که نشانگر یا تسهیل‌گر مقابله با اعمال تروریستی می‌باشد» (پاکزاد، ۱۳۹۰: ۲۲۱).

در مجموع می‌توان گفت «تروریسم سایبری» یک واژه جدلی است. برخی نویسندگان به این تعریف محدود بسنده کرده‌اند و آن را مرتبط با تجهیز نیرو از راه سازمان‌های تروریستی معروف برای حمله مخرب بر ضد سیستم‌های اطلاعاتی با اهدافی نظیر هشداردهی یا ایجاد هرا می‌دانند. با این توصیف محدود سخت بتوان یک نمونه تروریستی معرفی نمود. در مقابل تعریف جهانی و عام، تروریسم سایبری چنین عنوان گردیده است: «استفاده عامدانه اقدامات ویرانگر یا تهدید به آن علیه کامپیوترها یا شبکه‌ها با هدف ایجاد صدمه جمعی، عقیدتی، مذهبی، سیاسی یا موضعات نظایر آن» (روزبهانی، ۱۳۹۸: ٥٤)

**۲-مقابله با تروریسم سایبری در اسناد بین‌المللی**

در این قسمت به بررسی اسناد بین‌المللی که در خصوص تروریسم سایبری تصویب شده‌اند، می‌پردازیم:

**۲-۱-کنوانسیون‌مونترال**

ماده اول کنوانسیون مونترال جرایم را در حیطه اجرای کنوانسیون تعریف نموده است. به این مفهوم کشورها ضمن تامل در خصوص پیش‌نویس کنوانسیون، دیدگاه برشمردن را بر می‌گزینند که تعداد کمی از جرایم ویژه را در بر می‌گیرد. در صورتی که بقیه حامی تعریفی کلی بودند (ICAO, 1981: 21) استدلال دسته دوم، این است که قبول فهرست جرایم ضرورتا به این معنا است که اقدامات آتی که در هنگام پیش نویس کنوانسیون پیش بینی نبودند، بیرون از قلمرو اجرای کنوانسیون قرار می‌گیرد (Abramovsky, 1975: 280) بعد از کشمکس‌های فراوان با وجود این که تعریف به شکل تمام جامع پیشنویس گردید، لیکن سبب تردید در خصوص اختلاف حقیقی این دیدگاه فوقشد. ماده (۱) ۵ جرم

1

جایگزن ارتکابی از جانب بزهکار اصـلی را بیان نموده و ماده (۲) اقدام و معاونت را جرم‌انگاری نموده اسـت (کوشـا و نمامیان، ۱۳۸۷؛ نمامیان، 1388و گلدوزیان و نمامیان، ۱۳۸۹). با عنایت به ترس تروریسـم سایبری که در زمان پیشنویس کنوانسیون مونترال بیان نشده، این مسئله به ذهن خطور می‌کند که آیا جرایم مذکور در ماده ۱ برای تروریسم سـایبری امکان پذیر هسـتند؟ کنوانسـیون مـونترال عکس سایر کنوانسیون‌ها، بندی از مفاهیم را در بر ندارد کـه بـه توضیح مصادیق آن یاری نماید. لذا، تشریح حقوقی متن بر اساس مبانی تعبیر بیان شده در کنوانسـیون وین و دیگر رهنمودهـای تفسـیر متکی اسـت کـه در اصـل دربرگیرنـده دستورالعمل‌های کنفرانس مونترال که پـیش نویس کنوانسیون را تصویب نمود و ادبیات مربوط می‌گردد (Cohen, 2010: 16).

نقطه شروع موضوع، هر ۵ مورد بیان شده در ماده ۱ می‌باشد که حاکی از این برداشت عمومی است که مقصود کنوانسیون به جای مخاقطت از جان افراد، حفـظ امنیت هواپیمای در حال پرواز بوده اسـت. لذا، به خطر انداختن عامدانه زندگی یک مسافر بدون بـه خطـر انداختن امنیت هواپیما از بیان‌های تحت پوشـش این کنوانسـیون نیسـت. همچنین، می‌توان چنین استدلال نمود که در حقیقت نمی‌تـوانیم این دو امر را از یکدیگر تفکیک نماییم؛ فردی قادر نیسـت امنیت هواپیما را بدون به خظر انداختن زندگی خدمت‌کارها و مسـافران آن بـه خطر بیندازد، همان طور که نمی‌تواند تندرسـتی خدمه و مسـافران را بدون به خطر انداختن امنیت هواپیما در معرض خطر قرار دهد.

علاوه بر این باید گفت که براساس محتوای بیان شده در ماده ۱ هیچ شرط لازمی وجـود ندارد که مرتکب جرم یا معاون او سوار بر هواپیما باشد. این خصـوصـیت دیگر کنوانسـیون مونترال بوده که سـبب گشـته اسـت از کنوانسـیون لاهـه مترقی‌تر باشـد. برعکس پروتکل‌هـای لاهـه، قواعـد کنوانسیون مونترال در موقعیتی که بزهکار سوار بر هواپیما یا روی خشکی باشـد، کاربرد دارند و این، سـبب ازیاد احتمال مناسـب بودن پروتکل مونترال جهت رسـیدگی به تروریسـم سـایبری در مقابل یک هواپیما می‌گردد؛ چرا همان طور که قبلا ذکر گردید، یکی از برتری‌های تروریسـم سـایبری امکان اجرای هجوم از موقعیت دور دسـت می‌باشـد (همان، ۱۹) پروتکل مونترال به جرایم ارتکابی در یک هواپیمـای مورد بهره‌گیری هم که با هواپیمای در حال پرواز متفاوت می‌باشـد، رسـیدگی می‌نماید. این موضـوع، سـبب تمدید زمان اسـتفاده قواعد پروتکل می‌گردد. اکثر

کشـورهای شرکت کننـده، در خصوص قبول پیشنویس پروتکل در زمینه «مورد کار بردن قرار گرفتن هواپیما» تردید داشـــتند. ایشان، بر این نظر هسـتند تا هنگامی که بزهکار سـوار بر هواپیمـــا متضـمن بازداشـت و بازپرسـی در دولتی باشـد که هواپیما در آنجا به اشـغال در آمده، نیازی به مداخله بین‌المللی وجود ندارد.

**۲-۲-راهبرد کنوانسیون بین‌المللی‌منع بمب‌گذاری‌های‌تروریستی**

ماده ۲ کنوانسیون بین‌المللی، بمب‌گذاری‌های تروریستی بره‌ها را در حیطه اجرای کنوانسیون تعریف نموده است. ماده فوق، دربرگیرنده سه گروه از جرایم می‌گردد: جرایم ارتکابی از جانب مرتکب اصـلی، اقدام به ارتکاب جرم و هر گونه معاونت در جرم‌بندهای زیر به اسـتدلال امکان پذیری کنوانسیون بین‌المللـی بمب گذاری‌های تروریستی در خصوص تروریسم سایبری اقدام نموده است.

جرایم درج شـده در ماده (۱) ۲ کنوانسیون بین‌المللی منع بمب‌گذاری‌های تروریستی، عناصر زیادی را شامل می‌شود؛ زیرا که تروریسم سایبری و تروریســـم فیزیکی صرفا از لحاظ عمل صورت گرفته شده با یکدیگر متفاوت هستند و از حیث شکل درونی تروریســـت مجری آن کار، فرای بین آن‌ها نمی‌باشـد. دو گزینه در ارتباط با نیت بزهکار، تفسیر نمی‌شـوند. تروریست شبکه‌ای همان مقاصد یک ترویست معمولی را دارد و بنابراین، هـــیچ تفاوت قانونی در عام بودن هدف آن وجود ندارد. قضـیه زیر به بررسـی کاربردپذیری قوانین تعریف شـده در ماده فوق‌الذکر برای موضـوع تروریسـم سـایبری می‌پردازد. جرم، حکم می‌کند که بزهکار یکی از ٤ فعل (مانند پرتاب، کار گذاشـــتن، شـــلیک، یا منفجر نمودن مواد انفجاری یا ابزارهای مرگبار دیگر) را بر علیه یکی از چهار مکان نظیر مکان جمعی، تأسیسات کشوری یا دولتی، سامانه حمل و نقل همگانی یا تأسیسات زیرساختی انجـــام دهد. استفاده قسمت (۱) برای حملات تروریستی ســـایبری در وهله ابتدایی متکی به معنایی اســـت که به اصـــطلاح «مواد منفجره یا ادوات مرگبار دیگر» داده می‌شود.

بر طبق تعریف مذکور در ماده (۳) ۱ مواد منفجره یا ادوات مرگبـــــار دیگـــر، یکـــی از دو تفسیر احتمالی را ذکر می‌کند؛ ابتدا، می‌تواند به این مفهوم باشـد: ماده منفجره و آلات آتش‌زا که برای تسـبیب مرگ، زخم‌های بدنی جدی یا زیان مالی اسـاسـی در نظر گرفته شـده یا امکان آن را داشـته باشد. یک زیر ساخت رایانه‌ای شـــده احتمالا دارای شرایط این توضیح نیســـت. می‌توان از کامپیوتر برای چکلندن بمب بهره برد ، لیکن کامپیوتر خود به خود نمی‌تواند همچون یک بمـــب عمل نماید. صرفا راه ایجـــاد

انفجار مرتبط با زیرساخت رایانه‌ای، نصب یک بمب خارجی روی رایانه یا استفاده از کامپیوتر به مثابه دکمه قرمز چکاندن منفجرکننده است (Cohen, 2010: 43).

دومین تفسیر برای تعریف فوق، یک افزودنی به دنباله آن به بحث و مذاکره کار گروه بود که انواع مختلف موادی را معین می‌کند که رها کردن آن قادر است جان اشخاص را به خطر بیندازد. براساس ماده (ب) (۳) ماده منفجره یا دیگر ابزارهای کشنده، قادر است وسایل یا ادواتی باشد که برای تسبیب مرگ، جراحات جسمی جدی یا ضرر مالی اساسی از راه رهاسازی، منتشر کردم، یا تصادم مواد شیمیایی سنتی، علل‌های زیستی یا سم‌ها یا مواد مثل آن یا تشعشع ماده رادیواکتیو برنامه ریزی شده یا توانایی آن را داشته باشد. این مفهوم، عکس تفسیر اول، به صورت کامل دربرگیرنده چگونگی تروریسم سایبری می‌باشد.

در آخر اینکه کنوانسیون بمب گذاری تفسیری نسبت به انعطاف‌پذیر بودن از جرایم درج شده در ماده ۲ بیان می‌کند. هر عنصر جرم قادر است نشانگر معانی خیلی وسیعی باشد که پوششی را برای کنوانسیون به وجود می‌آورد. به واسطه این اصل، یک بزهکار در سطح کنوانسیون بین‌المللی، از بین بردن و بمب‌گذاری‌های تروریستی می‌تواند یک تروریست سایبری نیز باشد؛ لذا سیستم‌های کامپیوتری را به شیوه‌ای آشفته کند که سبب رها شدن مواد مرگبار در مکان‌های عمومی یا بر ضد آن بشود (نامیان، ۱۳۹۱: ۱٤۱).

**۲-۳-پیشنویس کنوانسیون جامع مقابله با تروریسم بین‌المللی**

در سال ۱۹۹٦، هند پیشنویس کنوانسیون جامع مبارزه با تروریسم بین‌المللی را به هدف تحلیل به وسیله کشورهای عضو، برای دبیر کل سازمان ملل متحد فرستاد. پیشنویس فوق، چندین بار مورد بازنگری قرار گرفته و ویراش شد تا زمانی که کمیته موردی در سال ۲۰۰۲ واپسین پیشنویس را لنتشار داد. پیش نویس فوق از لبعاد مختلفی به کنوانسیون‌های قبلی شبیه است. اصلاحاتی که پش نویس کنوانسیون بیان نموده است با پوشش‌دهی همه‌ی اقدامات تروریستی و تا حد، زیادی با پوشش‌دهی تعهد نسبت به پیشگیری و همکاری در ارتباط می‌باشد.

ادبیات حقوقی، نقش پیشنویس کنوانسیون را در زشتی تروریسم از جانب جامعه بین‌الملل معین نموده است. هر چند پیش نویس کنوانسیون دولت‌های طرفدار تروریسم را در جلنب تهاجمی قرار می‌دهد (پاکزاد، ۱۳۹۰: ۲۲۱) افزون بر این، پیش نویس مذکور مکمل و راهنمای کار

مجمع ضد تروریسم می‌باشد کـــه به وسیله شـــورای امنیـــت تشکیل گردیده است

پیشـنویس کنوانسـیون صـرفا تعریف کمی از تروریسـم را شـامل می‌شـود (هـــافنر، ۲۰۰۳: ۱۵٦) هر زمان قرار باشـــد پـــیشنویس کنوانسیون پایه‌ی کاملی را جهت مقابله بـــا تروریسم بین‌المللی مهیا نماید ، باید برای همه اقدامات، طروق، و روش‌های تروریســـــــم در هر مکان و از جانب هر شخصی، کاربرد داشته باشـد (Harrison, 2015: 176).

ایراد تعریف فوق در دو بحـث بنیـادین ذکر می‌شـــود؛ انجـام اعمـال تروریســـــتی در طی جنگ مسلحانه و پناه دادن به تروریست‌های تحت حفاظت کشورها و توطئه کردن جهت جرایم تروریستی (گرانـــت، ۲۰۰۵: ٤۲۸) با وجـــود این ضعف‌ها، پـــیش‌نـــویس کنوانسیون همواره مرحله بارزی به سـوی یکپارچـــــه کردن همکاری بـــــین‌المللی علیه تروریسـم محسـوب می‌شـود. کاربردپذیری پیشـنویس کنوانسـیون جهت تروریسـم ســـــایبری، با عنایت به جرم تعریف شده در پیشنویش مورد بررسی قرار می‌گیرد ؛ لیکن، باید یادآوری کرد که پیشـــگفتار پیشـــنویس کنوانســـیون قلمروی اجرای کنوانسیون را جهت تحلیل طبقه کلی «اقدامات، روش‌ها و طروق تروریسم» معین نموده است و لذا، مقدمه بـــــه نسبت کمی را بیان نموده که بر اساس آن امکان دارد تروریسم سـایبری را در قلمروی اجرای پیشنویس کنوانسیون قرار داد.

برطبق پیشـــنویس پروتکل، هر کشـــور عضـــو قبول می‌کند که جرایم درج شده در ماده را بـــــه سبب حقوق ملی خویش، بزه جزایی در نظر بگیرد. پیش نویس به موضـــوعات صـــلاحیت قضـــایی، معاضـــدت بین دولت‌ها، دادرسی و اجرای معیارها و نظایر آن هم اقدام نموده است. ماده (ب) (۱) ۲ بیان می‌نماید: «هر فردی در قلمرو معنایی کنوانســـیون فوق، در حالتی مرتکب بزه گردیده که به هر نوع و وسیله، به صورت نامشروع و عامدانه، سـبب آسـیب‌های مهم بـــــه اموال ملی یا افراد، مانند مکان‌های جمعی، تأسیسـات کشـوری یا دولتی، سـامانه حمل و نقل عمـــــومی و تأسیسـات زیرسـاختی یا محیط زیسـت شـود تا از راه تهدید افراد، یک دولت یا نهاد بین‌المللـی را به اجرا یا جلوگیری از انجام هر امری مجبور نماید».

تاکید ماده (ب) (۱) ۲ به «هر روش و وسیله» در کنار اصطلاح «تأسیسات زیرســـاختی» نظیر ارتباطات، مخابرات و شـــبکه‌های اطلاعاتی، بهره‌بردن جـــــرم مدار در پیشـنویس را برای حمله‌های تروریسـتی سـایبری ممکن می‌کند. خسارت آن به میزانی زیاد و آشکار است که قادر است به صورت بی واسطه به تروریســـم ســـایبری رسیدگی کند؛ ویژگی مهم اصلی آن هم

این اســت که احتیاجی به تکیه کردن بر روش‌های تفسـیری ندارد تا مورد عدم سازش نمایندگان یک رویکرد فکری یـــا حقوقی مختلف قرار گیرد (Cohen, 2010: 27).

**۲-٤-کنوانسیون‌جرم‌سایبری‌شورای‌اروپا**

در سال ۲۰۰۱، شورای اروپا «کنوانسیون جرم سایبری» را تصـــویب نمود. کنوانســـــیون فوق، حاصل چهار سال سعی صاحبنظران شـورای اروپا، ایالات متحده، کانادا، ژاپن و سـایر کشـورهایی بوده که در انتظار امضـای همه‌ی کشورهاست. مقصود اصـــــلی این کنوانسیون، دنبال کردن سیاستی کیفـــــــری یکپارچه و هماهنگ با هدف حمایت از جامعه در مقابل جرم سایبری، مخصوصا با به استفاده از قانون‌گذاری شایسته و تحکیم همکاری بین‌المللی می‌باشد.

با وجود این که اصـطلاح «جرم سـایبری» در محتوا جرمی می‌باشـد که در اینترنت یا از طریق اینترنت واقع می‌شـود، حیطه عمل کنوانسـیون بیشـتر از این حد و دربرگیرنده بزه‌هایی اســـت که با بهره‌گیری از کامپیوتر ایجاد می‌شود یا بزه‌هایی که در کل، رایانـــه‌هـــا را دخالت می‌دهند (Much, 2006: 72).

جهت اثبات مسئولیت کیفری، همه جرایم فوق در کنوانسیون جرم سایبری بایسـتی به شـکل عامدانه انجام شـده باشـند. لذا، سـوال ابتدایی که به میان می‌آید ، ایـــن اســـت که آیا قصد ارتکاب بزه یک خرابکار سایبری بـــا هدف ارتکـاب جرم یـک تروریسـت سایبری فرق دارد ؟ همان گونه که بیان شـد، قصـد تنها برای بـــــه انجام رسـاندن یک اقدام، از آن حمله‌ای تروریســـتی به وجود نمی‌آورد. در زمینه تروریســـــــــت، عکس تبهکار، ضروری است که قصد، اجرای حمله به هدف تاثیرگذاری بر سیاستمداران باشـد. لذا، معلوم نیسـت که عبارت «به شـکل عمد» در کنوانسـیون این نوع قصد را تحـت پوشش خود قرار دهد.

لذا چنانچه فرض نماییم که قصـد ویژه تروریســـــت‌ها با در نظر گرفتن کلمه «قصـد» در کنوانسـیون به اثبات می‌رسـد، خیلی جرایم درج شـده در کنوانســـــیون برای تروریسـم سـایبری کاربردپذیر می‌شـوند. حمله‌های تروریسـتی سـایبری از راه دسـترسـی غیرقانونی به سیسـتم‌های کامپیوتری بی‌حق یـا از راه رهگیری انتقال داده‌های الکترونیکی غیرعلنی قابل اجرا هســتند. نیز، می‌توان فرض نمود که آسـیب زدن به هماهنگی و اسـتفاده مناسب کامپیوتر یا بهره‌گیری از برنامـــه‌ها و پیام‌های ذخیره شده رایانه‌ای از جمله موارد حمله تروریستی سـایبری می‌باشـد. لذا، بقیه بزه‌های مذکور در کنوانسیون نیز می‌تواننـــد در فرآیند یک اقدام تروریستی سایبری؛ مثلا،

متوقف نمودن سیستم رایانه‌ای، استفاده غیرصحیح از دستگاه‌ها و جعل کامپیوتری و کلاه‌برداری انجام شود. «جرایم مخصوص مرتبط با هرزه‌نگاری برای کودکان» و «حقوق مالکیت فکری» ارتباط محدودتری با فعالیت‌های تروریسم سایبری دارند (Cohen, 2010: 34).

در پایان، کنوانسیون جرم سایبری شورای اروپا، فقط برخی از جرایمی را شامل می‌شود که از راه تروریسم سایبری قابل اجرا می‌باشد. قصد ارتکاب جرم صرفا همان قصد است و این قصد ویژه‌ای که عوامل مرتبط با تروریسم پیش بینی می‌شود و پیامدها و صدمه‌های فوری را در نظر می‌گیرد، نیست. علاوه بر این، از میان دولت‌هایی که کنوانسیون را جهت امضا به آنها داده‌اند، فقط ۲۶ کشور آن را مورد قبول کردند. این واقعیت نشان می‌دهد که میل و رغبت سیاسی دولت‌ها نقش مهمی در معین نمودن تاثیرگذاری مدارک حقوقی بازی می‌کنند؛ به این ترتیب، اگر کنوانسیون مذکور دربرگیرنده «قصد ارتکاب جرم» مرتبط با تروریسم بود، باز هم جانبداری کشورها عامل مهمی در تحلیل ارزش آن به شمار می‌رود (نامیان، ۱۳۹۱: ۱۵۳).

**۲-۵-پیشنویس کنوانسیون استانفورد در مورد جرم سایبری و تروریسم**

در اگوست ۲۰۰۰، کارشناسان «دانشگاه استانفورد» طرح پیشنهادی خود را برای کنوانسیون بین‌المللی جرم و تروریسم سایبری بیان نمودند (پیش‌نویس استانفورد) (Sofaer, 2000: 257). این پیشنویس که براساس کنوانسیون جرم سایبری شورای اروپا می‌باشد، جرم‌انگاری اعمال زیادی از جمله استفاده از سیستم‌های سایبری جهت اجرای جرایم مشخص شده در دیگر معاهدات ویژه و نشانه‌گیری زیرساخت‌های پیش بحرانی را توصیه داده است. از سویی، پیش نویس مذکور، تحقق یک خبرگذاری بین‌المللی را هم راستای پشتیبانی از زیر ساخت اطلاعاتی توصیه نموده که شرایطی برای بررسی در مورد ایجاد استانداردها و روش‌های در ارتباط با امنیت مجازی می‌باشد.

پیشنویس فوق، عکس کنوانسیون جرم سایبری شورای اروپا، به شکل ویژه به منطبق نمودن بین زیرساخت مبتنی بر ارتباطات کامپیوتری و تروریسم اقدام کرده است. این پیشنویس با ابعادی از اقدامات شبکه‌ای بی‌ارتباط است که ممکن است جرم سایبری باشند، لیکن تروریسم سایبری به حساب نمی‌آید. پیش‌نویس استانفورد عکس پیشنویس کنوانسیون جامع، به صورت آشکار بیان کرده است که جهت اقدامات مرتبط به به جنگ‌های مسلحانه کنونی مورد بهره قرار نمی‌گیرد.

با این حال، از هنگام پیشـــنویس، دو ترقی بارز صـــورت گرفتـــــه که مـی‌تواننـد کنوانسیون تروریسم سایبری را نسخ نمایند:

۱- کنوانسیون فوق قلمروی را ایجاد کرده که به موضوعات فراوانی که در پیشـنویس اسـتانفورد هم بیان شـده‌اند، اقدام کرده اسـت. این علامت پرسـش پیش روی طرفداران پیشـنویس اسـتانفورد می‌باشـد که آیا شـایسـته اسـت با موضـوعات متفاوت به شـکل یکسـان در هر دو مدرک برخورد گردد یا اینکه کنوانسـیون جرم سایبری کافی می‌باشد.

۲- پیشـنویس کنوانسـیون جامع تا الان در دسـت اجرا می‌باشـد و همان گونه که بیان شـــد، تعریف جرایم در آن ممکن اســـت تروریسم سایبری را هم در برگیرد.

از سـوی دیگر، در این خصـوص یک کنوانسـیون جامع می‌تواند ســـــند شـایسـته و همه‌ی عیاری برای پرداختن به تروریسـم سـایبری باشـد. یک کنوانسیون مستقل می‌توانـــد بندهای ویژه‌ای را ارائه نماید که برای تحلیل خصوصیات مخصوص تروریسم سایبری لحاظ شده‌اند.

کنوانسـیونی، قادر اسـت تدابیر فوق‌الذکر و رویه‌های همکاری دوجانبه در ارتباط با تروریســـم ســـایبری را بیان نماید، لیکن ممکن اســـت به دلیل ویژگی عاکی که دارد، از کنوانسـیون جامع حذف شـود؛ مانع مهم در زمینه چنـــین تدابری، نبود پیشنویس به روز شده برای ارائه به مجمع ششم، یا هر مکان مورد بررسی دیگـری می‌باشد که به این موضوع اختصاص یافته باشد (نمامیان، ۱۳۹۱: ۱۵۵).

**۳-پیشگیری از بزه‌دیدگی تروریسم سایبری در اسناد بین‌المللی**

بزه‌دیدگان سـایبری، یکی از بی‌دفاع‌ترین و بی‌گناه‌ترین اشـخاصـی هسـتند که در اثر فرایند بزه‌دیدگی، متحمّل خسـارت‌های مادی، عاطفی، اجتماعی و در برخی موارد، پزشکی می‌شـوند، اما به دلیل برخی ویژگی‌های فضـای سـایبر، چالش‌های تعقیب بزهکاران و نبود مقررات ضـروری، نیازهای آنان بدون تلافی می‌ماند. بزه‌دیدگان تروریســـم ســـایبری نیز به نوعی بزه‌دیده ســـایبری به شـــمار می‌روند. بنابراین شـــرایط امروزی لازمه دقت مقن و نهادهای بین‌المللی در راستای پشتیبانی از آنان می‌باشـد. در این قسـمت به بررسـی راهکارهای پیشـگیری از بزه دیدگی تروریسـم سـایبری در اسـناد بین‌المللی می‌پردازیم.

**۳-۱-اقدامات پیشگیرانه کیفری در اسناد بین‌المللی و منطقه‌ای**

اســـتراتژی های دقیق پیشـــگیری از جرم نـه تنها از جرم و بزه دیدگی جلوگیری می کند بلکه به توسـعه پایدار نیز کمک می‌کند. مهمترین اسـناد بین‌المللی و منطقه‌ای که به پیشـــگیری کیفری از تروریســـم ســـایبری پرداخته‌اند، عبارت است از:

**۳-۱-۱-کنوانســیون راجع به جلوگیری از اعمال غیرقانونی علیه امنیت هواپیمایی کشوری**

این کنوانســـیون، یکی از کوشـــش‌های مجمع عمومی در مقابله با اعمال تروریستی می‌باشد که در ۲۳ سپتامبر ۱۹۷۱ در شیکاگو به تصویب رسید (United Nations, 1971: 12325). دیباچه این کنوانســـیون، در مورد به به خطر انداختن سلامتی اشخاص، دارایی و بهره‌مندی از خدمات هوایی از راه اعمال غیرمجاز دل نگران شـده اسـت. در خصـوص، انظباق کنوانسیون فوق با اقدامات تروریستی سایبری می‌توان به قاعده کلی اشاره نمود که با نام بردن از دو واژه‌ی «خشونت» و «زیان‌های مهم»، به ارتکاب بزه‌های خشونت‌بار به هر راهی علیه زیرساخت‌های هواپیمایی اقدام کرده است. همچنین، کنوانسیون فوق‌الذکر، شروع به جرم اقدامات فوق در ماده ۱ و پیوسـتن در اجرای کارهای غیرمجاز درج شـده در این کنوانسـیون را بزه و کشـــورهای عضـــو را جهت ممانعت از ایجاد چنین اقداامی، به بکارگیری راهکارهای فوری به هدف مجازات آنها مکلف می‌نماید در مورد مجـازات مرتکبین، کشـــوراهـا مکلف بـه در نظر گرفتن کیفرهـای سنگینی در جرایم درج شده در ماده ۱ شده‌اند صلاحیت کیفری در ماده ۵ این کنوانسـیون بیان شـده و کشـورها به بکارگیری راهکارهای مناسـب به هدف در نظر گرفتن صلاحیت خود مکلف شده‌اند. پس از ذکر صلاحیت کیفری، به توقیف، تعقیب کیفری و اعمال مربوطه به وســـیله دولت‌ها و کارهای مناســـب برای انجام این اقدامات اشـــاره شـــده اســـت. اســـترداد مجرمین که یکی از چالش برانگیزترین موضـــوعات در حقوق بین‌الملل می‌باشـــد، در این کنوانســـیون لحاظ شـــده و کشـــورها را به منعقد کردن معاهدات استرداد، ترغیب نموده و بیان کرده است که دولت‌ها جرایم درج شـــدن در این کنوانســـیون را من جمله جرایم قابل اســـترداد در دولت‌های عضو در نظر بگیرند.

با عنایت به این که تروریســـم ســـایبری قادر اســـت از همه جهان توســـط کامپیوتر انجام شـــود، معاضـــدت‌های قضـــایی، بارزترین دلیل در تعقیب شـــایســـته و به محاکمه کشـــاندن اشـــخاص تبهکار اســـت که مقررات یکپارچه‌ای در این زمینه وجود ندارد. مجرمانی همچون تروریســـت‌های

سایبری که از هوش فراوانی بهره‌مند هستند ، می‌توانند در کمترین زمان، رد پای خود را از بین ببرند که این امر، باعث شکست یا طولانی تر شدن رسیدگی‌های قضایی می‌شود. لذا معاضدت‌های قضایی که به صورت فوری انجام گردد، برای تعقیب مجرمان بین‌المللی ضرورتی واضح و مبرهن می‌باشد.

**۳-۱-۲-کنوانسیون جلوگیری از بمب‌گذاری تروریستی**

کنوانسیون مذکور نتیجه یکی از کوشش‌های مجمع عمومی سازمان ملل متحد در مبارزه با تروریسم و حمایت صلح و امنیت بین‌المللی و در جهت بهبود سطح حسن همسایگی و رابطه دوستانه همکاری میان کشورها در ۱۵ دسامبر سال ۱۹۹۷ تصویب شد (هاشمی، ۱۳۹۵: ۲۵). کنوانسیون فوق در تعریف عناصر متشکله اعمال تروریستی در این مدرک، به مواد انفجاری دیگر یا ادوات انفجاری کشنده در ارتکاب بزه‌هایی تروریستی تاکید کرده است. کنوانسیون در شرح دوات منفجره یا سایر آلات مرگبار، سه ملاک یا خصوصیت را لحاظ نموده است. بر طبق تعریف کنوانسیون، ابزار منفجره یا وسائل مرگ بار دیگر باید دارای سه خصوصیت ایجاد مرگ، صدمه جانی یا جسمی سنگین و در پایان وارد نمودن آسیب مادی زیاد باشد. سلاح‌ها و ابزارها که دارای خصوصیات مذکور باشند، شامل تعریف کنوانسیون واقع می‌شوند. کنوانسیون در دنباله (قسمت ب بند ۳ ماده ۱) به نمونه‌های عادی سلاح‌ها یا ادواتی که دارای چنان ویژگی و کارکردی هستند، اشاره می‌نماید و تحلیل می‌دهد که سلاح‌ها و ابزاهایی که مواد شیمیایی سمّی، مواد بیولوژیکی منتشر و پخش می‌کنند، ازجمله سلاح‌ها و ابزارهایی هستند که سه ویژگی مذکور را دارند. با بازگرد به مفهوم مذور باید گفت که از نظر پروتکل، تحویل، جاسازی، شلیک و انفجار غیرمجاز با سلاح‌های شیمیایی بیولوژیکی و هر نوع ابزار یا اسلحه دیگری که منجر به فوت، صدمه فیزکی سنگین یا زیان مادی می‌شود، در مکان‌های جمعی تأسیسات دولتی و زیرساختی و سامانه حمل ونقل عمومی، جرم بین‌المللی بوده و تروریسم محسوب می‌شود.

کنوانسیون مذکور، به صورت صریح بر وجود عنصر روانی را در اعمال امر مجرمانه و دربرگیرنده تروریسم، تأکید و در بند ۱ ماده ۲ اشاره نموده است که فرد در حالتی مرتکب جرم می‌گردد که اولاً، در اجرای امر مجرمانه قاصد باشد. ثانیا، قصد و نیت وی منجر به فوت، صدمه فیزیکی سنگین یا از بین بردن وسیع و وارد نمودن زیان اقتصادی فراوان به مکان‌های جمعی، نهادهای دولتی و زیرساختی و سامانه حمل و نقل عمومی باشد. همان گونه که مبرهن است، کنوانسیون وجود سوءنیت عام

و سوءنیت خاص در شخص مرتکب امر بزهکارانه را لازم می‌داند. لذا عنصر معنوی جرایم بیان شده در کنوانسیون، هنگامی به وجود می‌آید که اول اینکه، فرد در انجام کار خود، قصد و اراده داشته باشد. دوم اینکه، قصد وی از انجام اقدامات مجرمانه، ایجاد مرگ یا صدمه فیزیکی سنگین یا وارد آمدن زیان مالی باشد. (نمامیان، ۱۳۹۲: ۱۸).

**۳-۱-۳-کنوانسیون سرکوب حمایت مالی از تروریسم**

این کنوانسیون ، یکی از قطعنامه‌های مشهور ۱۳۷۳ در خصوص ممانعت از حمایت اقتصادی از تروریسم می‌باشد در که در ۹ دسامبر ۱۹۹۹ در مجمع عمومی سازمان ملل متحد تصویب شد (طیبی فرد، ۱۳۸٤: ۲٦٥). پروتکل ۳ گروه اصلی از اعمالی که حمایت اقتصادی از اعمال تروریستی به حساب می‌آیند از جمله جرم‌انگاری تأمین مالی تروریسم در قوانین کیفری در مواد ۲ و ۳، معاضدت وسیع با سایر کشورهای عضو و مساعدت قضایی در امور مربوط با پروتکل در مواد ۱۲ الی ۱۵، بکارگیری اعمال پیشگیرلنه در ماده ۱۸، تعهد اشخاص حقوقی در اجرای اعمال غیرمجاز در پروتکل در مورد تأمین مالی تروریسم در ماده ۵. این امور از اصلی‌ترین مقررات ضروری در پروتکل می‌باشد. (همان: ۲٦۸).

کنوانسیون فوق، دسته‌ای از مقررات لزوم برای دولت‌های عضو جامعه بین‌المللی در مقابله با تروریسم می‌باشد که این ارزش‌ها یا در قالب قواعد عرفی از صراحت شایسته بهره‌مند نیستند و این کنوانسیون سعی در بکارگیری قلمروی واضح‌تر و روشن‌تر در خصوص تعهدات دولت‌ها در این خصوص می‌باشد یا این کنوانسیون دارای آن گروه از قواعدی می‌باشد که پیش از این، از راه اعمال در حقوق بین‌الملل ذکر شده بود که برای دولت‌ها از نظر حقوقی اجبار مناسب به وجود نمی‌آورد. در برداشت عام، کنوانسیون فوق سعی می‌کند ۷ محور اصلی را در قوانین ملی کشورها در نظر بگیرد: تأمین مالی تروریسم، عمال صلاحیت قضایی نسبت به متهمان ارتکاب این جرایم، توقیف و ضبط اموال مجرمان، استرداد و محاکمه بزهکاران، معاضدت قضایی و مبادله کردن اطلاعات و مداسنادارک، اقدامات پیشگیرلنه و نظام‌های پرداخت جایگزین. با توجه به آنچه بیان شد، معاهده‌هایی از جمله کنوانسیون تامین مالی تروریسم، علاوه بر اینکه تعهداتی را بر عهده‌ی دولت‌ها در حیطه روابط بین‌المللی به وجود می‌آورد، سیاست و روندی غمومی قوانین داخلی در مواجهه با جرایم تروریستی را مشخص می‌کند که به صورت عمومی از مجرای قوانین و رویه‌های اداری داخل کشورها اجرا می‌شود (Dandurand, 2005: 288).

افزون بر بر کنوانسیون ۱۹۹۹، قطعنامه شماره به طور مختصر در دو اصل کلّی، به موضوع حمایت مالی از تروریسم دقت کرده است. مبنای اول، ایجاد قواعد بین‌المللی مبارزه با تأمین مالی تروریسم می‌باشد که دربرگیرنده جرم‌انگاری تأمین مالی اعمال تروریستی در ردیف‌های (الف) و (ب) بند ۱ قطعنامه و متعهد نمودن دولت‌ها به منظور تلاش برای جلوگیری و مبارزه با تأمین مالی تروریسم در چارچوب اقدامات مختلف در ردیف (ث) بند ۲ است (شمس ناتری و اسلامی، ۱۳۹٤: ۲۷٦). شورای امنیت در قطعنامه فوق، اقدامات تروریستی را بار دیگر بزهکارانه در نظر گرفت و جرم‌انگاری آن را در میان قوانین داخلی کشورها به مثابه تعهدی سازمانی بر همه‌ی دولت‌های دنیا، تکلیف و بار می‌شود. در کل، از محتوای کنوانسیون مذکور، ٤ موضوع اصلی دریافت می‌گردد که: اجبار دولت‌ها به همکاری با همدیکر با هدف از بین بردن تروریسم، مبارزه با تأمین مالی تروریسم، پشتیبانی نکردن با واسطه و بدن واسطه از تروریسم، جرم‌انگاری و تعقیب جزایی تروریسم، از اصلی‌ترین مسائلی است که در قطعنامه مذکر بر آن تاکید گشته است. ( SC/Res/1373, : 2001.).

افزون بر موارد مذکور، این قطعنامه از دولت‌ها می‌خواهد روش‌های برای تشدید و سریع شدن رد و بدل کردن اطلاعات در مسائلی از جمله بکارگیری گروه‌های تروریستی از تکنولوژی‌های مخابراتی استفاده نمایند. قطعنامه ۱۳۷۳ شورای امنیت هم دارای ویژگی شبه قانونگذاری نیز می‌باشد.

**۳-۱-٤-کنوانسیون توکیو راجع‌به جرایم و برخی از اعمال ارتکابی دیگر در هواپیما**

کنوانسیون مذکور دارای ۷ فصل و ۲٦ ماده می‌باشد، که در برگیرنده جرایم موضوع قوانین جزایی، اقداماتی که دربرگیرنده ارتکاب جرم بوده یا نباشد، لیکن سلامت هواپیما و سرنشینان و محوله‌های آن را به خطر اندازد یا باعث بر هم زدن نظم و راختی داخلی هواپیما گردد. این کنوانسیون، نخستین کنوانسیون چند سویه حقوقی بود که به مشکل روزافزون هواپیماربایی اقدام نموده است. این کنواسیون، تعریف یا فهرست ویژه‌ای از اقداماتی را که باید سرکوب شوند، ذکر نمی‌کند، لیکن ماده ۱۱ آن به گونه مخصوصی از تروریسم یعنی دزدی هوایی اقدام نموده است. این مدرک بین‌المللی، همچون کنوانسیون پالرمو، با درج افعال ارتکابی که ایمنی هواپیما را به خطر انداخته، از تأسیسات هواپیمایی که احتمال دارد مورد هجوم تروریست‌های سایبری قرار گیرد، حمایت

جزایی نموده و با جرم‌انگاری اقداماتی که سبب به مخاطره افتادن ایمنی هواپیما و .... می‌گردد، به ممانعت کیفری نسبت به ایجاد چنین اقداماتی از هر راهی پرداخته است. با عنایت به اینکه هواپیما به سیستم‌های مخابراتی وابستگی زیادی دارد، با مختل شدن دستگاه‌های هدایتی و کنترلی آن به وسیله تروریست‌های سایبری و از طریق کامپیوتر یا سایر تاسیسات مخابراتی قادر است نسبت به محو یا اختلال داده‌ها یا تأسیسات هواپیما بپردازد. لذا در صورت ایجاد هجوم تروریستی سایبری علیه زیرساخت‌های فوق، بر اساس این کنوانسیون، مرتکب یا مرتکبان به اتکاء قواعد سند فوق، مجازات می‌شوند. (Dorothy, 2007: 16).

**۳-۱-۵-اعلامیه راجع به اقدامات ناظر به امحای تروریسم بین‌المللی**

اعلامیه مذکور که در سال ۱۹۹٤ صادر شد، بار دیگر در سال ۱۹۹۵ همراه با قطعنامه ۵۰/۵۳ مورد تأیید مجدد مجمع عمومی سازمان ملل واقع شد. اعلامیه فوق‌الذکر، به اهمیت اعمال همه جانبه در مورد از بین بردن و مقابله با همه انواع تروریسم توجه نموده است. افعال پیشگیرانه جزایی یکی از موارد دربرگیرنده این پروتکل است و با اتکاء به این اعمال می‌توان مفاد این سند را به جلوگیری از تروریسم سایبری گسترش داد (Follmar, 2009: 95).

ضمیمه این قطعنامه، اعلامیه‌ای راجع به تکمیل اعلامیه ۱۹۹٤ در خصوص از بین بردن تروریسم بین‌المللی بود و این مسئله را از ابتدا تأیید کرد که دولت‌ها پیش از دادن وضعیت پناهندگی باید اعمالی شایسته انجام دهند تا مطمعن شوند که یک پناهجو در اعمال تروریستی شرکت نداشته باشد و پس از دادن پناهندگی هم تضمین نمایند که چنین شرایطی با هدف زمینه چینی یا ساملندهی اعمال تروریستی علیه کشورهای دیگر یا شهروندان ایشان بکار گرفته نمی‌شود. اعلامیه فوق تأکید می‌کند که پناه‌جویانی که امید رسیدگی به مطالبات خود هستند از تعقیب به سبب اعمال تروریستی مبرا نیستند. اعلامیه مذکور بار دیگر بر اهمیت کاری سازنده بین دولت‌ها تأکید می‌نماید تا از این راه، اشخاصی که در اعمال تروریستی مشارکت نموده‌اند، از جمله افرادی که آنها را از لحاظ مالی تأمین، برای آنها برنامه‌ریزی و ایشان را تشویق کرده‌اند، محاکمه گردند.

**۳-۱-٦-کنوانسیون اروپایی مقابله با تروریسم**

اتحادیه اروپا در حیطه‌های مختلفی از امنیت فضای سایبر عمل است. اتحادیه کشورهای اروپایی، تدابیر گوناگونی را در خصوص حمله علیه شبکه‌های کامپیوتری، منتشر کردن ویروس‌ها، کرم‌های رایانه‌ای،

تروجان‌ها، هرزنامه‌های اینترنتی، حملات فیشینگ و سرقت هویت صادر نموده است. با عنایت به اینکه موارد مذکور، اکثرا در تروریسم سایبری مورد استفاده قرار می‌گیرد ، می‌توان به این نتیجه رسید که اتحادیه اروپا یکی از بارزترین سازمان‌هایی است که با هدف پیشگیری از تروریسم سایبری اقدام نموده است. اتحادیه فوق در سال ۲۰۰٤ با هدف مطمعن شدن از امنیت اطلاعات و شبکه در مجمع اروپا را راه لندازی نمود. مقصود از راه اندازی این آژانس، کمک به ارتقا و توسعه فرهنگ امنیت اطلاعات و شبکه در راستای حفاظت از منافع اشخاص، مشتریان، سرمایه‌گذاران و نهادهای متصدی امور اجرایی کشور در اتحادیه اروپاست. معاهده لیسبون از دسامبر ۲۰۰۹ لازم‌الاجرا شده، برای اولیت بار، وظایف و ناحیه فعالیت ثابت و معین را در خصوص جرایم کامپیوتری برای اتحادیه اروپا تعریف نمود. در بند ۱ ماده ۸۳ جرم رایانه‌ای به صورت واضح به مثابه یکی از حیطه‌های مرتبط جرم نام برده شده است. ابا توجه به این که جرم سایبری وسیع‌تر از جرم رایانه‌ای است، این اختلاف به اتحادیه اروپا اذن می‌دهد تا به ضابطه هر دو حیطه بپردازد. در آخر دوره برنامه استکهلم در سال ۲۰۱٤ از تدابیر امنیت سایبری اتحادیه اروپا معرفی شد. قصد این رهنمودها، اجرایی نمودن یک نوبت ۲ قانونگذاری در اتحادیه اروپا در حیطه‌های امنیت و جرایم سایبری بود. در همین راستا، کمیته‌ای با نام «کارگروه مشترک امنیت و جرایم سایبری اتحادیه اروپا ــ ایالات متحده» به قصد رسیدگی قاعده‌مندسازی جرایم سایبری در اتحادیه شکل گرفت. در سال ۲۰۰۱ کمیسیون اروپا توصیه‌نامه‌ای با نام «ایجاد جامعه اطلاعاتی ایمن‌تر از راه توسعه امنیت زیرساخت‌های اطلاعاتی و مقابله با جرایم مرتبط صادر نمود که در آن معضلات ناشی از جرایم سایبری را بررسی و به ضرورت انجام اعمال شایسته برای مبارزه با تهدیدهای نسبت به درستی، دستیابی و استحقاق اعتماد سامانه‌ها و شبکه‌های اطلاعاتی اشاره نمود (پورنقدی و بختیاری، ۱۳۹۲: ٤۲).

**۳-۱-۷-کنوانسیون سازمان همکاری‌های منطقه‌ای آسیای جنوبی**

کنوانسیون منطقه‌ای سازمان همکاری‌های منطقه‌ای آسیای جنوبی در خصوص جلوگیری از تروریسم، یکی دیگر از کوشش‌های منطقه‌ای دولت‌ها در مقابله با تروریسم می‌باشد که ۷ عضو این نهاد، یعنی بنگلادش، بوتان، هند، مالدیو، نپال، پاکستان و سریلانکا با هدف مبارزه با زیاد شدن جرایم تروریستی و الگو گرفتن از کنوانسیون‌های بین‌المللی در مبارزه با تروریسم، آن را در تاریخ ٤ نوامبر ۱۹۸۷ در کاتماندو تصویب

کردند. بر طبق مقررات کنوانسیون فوق، جرایم زیر، جرم سیاسی در نظر گرفته نمی‌شوند؛ لذا باید به بازگرداندن مرتکبان جرایم ذیل اقدام شود:

۱- جرایم فوق در چارچوب کنوانسیون مبارزه با تصرف غیرقانونی هواپیما، مصوب ۱۹۷۰ لاهه

۲- جرایم مذکور در چارچوب کنوانسیون مبارزه با اقدامات غیرقانونی علیه امنیت هواپیمایی کشوری مصوب ۱۹۷۱ مونترال

۳- جرایم مذکور در محدوده کنوانسیون پیشگیری و مجازات علیه اشخاص مورد حمایت بین‌المللی از جمله مأمورین دیپلماتیک مصوب ۱۹۷۳ نیویورک

۴- وقوع جرایم مذکور در چارپوب هر کنوانسیون ضدتروریستی که کشورهای عضو «سارک» با آن ارتباط دارند و عضو آن هستند، اعضا سازش نمایند که مجریان را تعقیب و استرداد نمایند.

**۳-۱-۸-کنوانسیون سازمان کنفرانس اسلامی در زمینه مبارزه‌با تروریسم بین‌المللی**

سازمان کنفرانس اسلامی، در مدارک زیادی به مسئله تروریسم و مبارزه با آن پرداخته است. این کنوانسیون ٤٢ ماده‌ای، به تمام مباحث مرتبط با امر، تعاریف، نحوه‌ی معاضدت دولت‌ها و مسئله قضایی در ارتباط با جرایم تروریستی اقدام و فضای مناسبی را برای مبارزه با تروریسم و تفکیک آن با جنبش‌های استقلال طلبی و رهاسازیی سرزمین‌ها یداخلی ایجاد نموده است. سازمان کنفرانس اسلامی، تروریسم را مسئله‌ای می‌داند که «همراه با خشونت یا تهدید به خشونت و با مقاصد سیاسی، مالی، مذهبی، شخصی، دسته جمعی در قلمرو عمل جنایی، با هدف ایجاد ترس در جامعه یا تهدید به صدمه وارد کردن به اشخاص یا اموال عمومی یا فردی یا امنیت ملی، خواه اقدامات مذکور انجام بشود یا اینکه در قالب تهدید باقی بماند، ارتکاب یابد».

**۳-۱-۹-معاهده همکاری میان دولت‌های عضو کشورهای مستقل مشترک المنافع در مبارزه با تروریسم**

این معاهده، در تاریخ چهار ژوئن ۱۹۹ در مینسک روسیه، تدوین و سند آن نیز پیش دبیرخانه کشورهای مشترک المنافع تصویب شده است (کدخدایی و ساعد، ۱۳۹۰: ۳۹۵).

دولت‌های عضو با درک دشوارهای‌های اقدامات تروریستی، به متعهد بودن نسبت به کنوانسیون‌های سازمان ملل متحد تأکید نموده و ملزم

می‌شوند که اقدامات فوری را در مورد معاضدت‌هایی در خصوص با امور جزایی مرتبط با جرایم تروریستی انجام دهند. اعمال غیرقانونی تروریستی کنوانسیون عبارت‌اند از:

۱- خشونت یا ارعاب به خشونت علیه افراد حقیقی یا حقوقی؛

۲- امحا یا تهدید به تخریب و وارد نمودن زیان به اموال دیگر به نحوی که زندگی افراد را به مخاطره انداخته و نیز پیامدهای سنگین برای افراد را در پی داشته باشد.

۳- با قصد انتقام‌گیری از سیاست‌های دولت، حیات یک سیاستمدار یا یک فرد سیاسی را تهدید نماید.

۴- اقدام سبب تجاوز علیه نماینده یک دولت خارجی، اعضای سازمان بین‌المللیِ بهره‌مند از مصونیت خصوصی بین‌المللی گردد (ماده ۱).

**۳-۱-۱۰-کنوانسیون عربی مقابله با تروریسم**

کنوانسیون فوق، یکی از اسناد منطقه‌ای بوده که وزیران و دادگستری کشورهای عربی آن را در آوریل ۱۹۹۸ تصویب نمودند (کیهانلو و رضادوست، ۱۳۹۳: ۳۹۰). در کنوانسیون مذکور، هر صورت جرم یا شروع به جرمی که به هدف اجرای هدف تروریستی در هر کدام از دولت‌های همکار یا بر ضد هریک از تابعین یا مصلحت‌های آن دولت‌ها که براساس قوانین ملی آن‌ها سبب رسیدگی یا کیفر باشد، این سند مانند بعضی دیگر از اسناد مبارزه با تروریسم، به مصداق‌های تروریسم اشاره‌ای نکرده، بلکه دسته‌ی اعمالی را برشمرده که بر طبق محتوای این کنوانسیون، تروریستی به شمار می‌روند. از عمومی بودن حیطه ارتکاب محتوای این کنوانسیون، این چنین استنباط می‌گردد که در حالتی که امری تروریستی از راه رایانه ارتکاب یابد و سبب به اخلال یا امحای تأسیسات رایانه‌ای و مخابراتی گردد، بر طبق این کنوانسیون قابل پیگرد بوده؛ با وجود این که به شکل آشکار به این جرم اشاره نشده است. لذا می‌توان گفت که کنوانسیون فوق نیز از گروه اسنادی است که به جلویگری کیفری از اعمال مرتبط با تروریسم سایبری اقدام نموده است.

**۳-۲-اقدامات پیشگیرانه غیرکیفری در اسناد بین‌المللی و منطقه‌ای**

این قسم پیشگیری که پیش از حدوث جرم صورت می‌گیرد، یعنی استفاده به اعمال غیرسرکوب‌گر و غیر خشم آمیز که دارای ماهیت مالی، فرهنگی، اجتماعی، وضعی، آموزشی و ... می‌باشند به هدف جامعه‌پذیر و قانون مدار کردن اشخاص و حفاظت از اهداف جرم برای ممانعت از رخداد

جرم. در این بخش به بررسی اقدامات پیشگیرانه غیر کیفری از تروریسم سایبری در اسناد بین‌المللی و منطقه‌ای می‌پردازیم.

**۳-۲-۱- توصیه‌نامه‌های نشریه بین‌المللی سیاست جنایی**

نشریه بین‌المللی سیاست جنایی، یکی از اقدامات سازمان ملل با هدف انتشار و توسعه آگاهی مربوط به امنیت کامپیوتر می‌باشد. سازمان ملل متحد در سال ۱۹۹٤ در نشریه فوق به امنیت سامانه‌های کامپیوتری اقدام و امنیت این سامانه‌ها را در امنیت سامانه‌های EDP نام برده است؛ با این مقدمه که امنیت سامانه‌های EDP از ۷ عامل اساسی ایجاد شده است که دربرگیرنده امنیت اداری و سازمانی، امنیت پرسنلی، امنیت مادی، امنیت مخابرات الکترونیکی، امنیت سخت‌افزاری و نرم‌افزاری، امنیت عملیاتی و برنامه‌ریزی می‌باشد (Kenneth, 2006: 78).

**۳-۲-۲-دستورالعمل و توصیه‌نامه‌های سازمان همکاری و توسعه اقتصادی**

کمیته تخصصی این سازمان در سال ۱۹۸۹ اعمالی را با هدف استفاده‌ی سیاستی مشترک برای مبارزه با جرایم اینترنتی و سازش قوانین کیفری، نیز حفاظت از حقوق شخصی و روند فراملّی داده‌های فردی آغاز نمود. در ژوئیه سال ۲۰۰۲ این سازمان، سند جامع «تدابیری برای امنیت سامانه‌های اطلاعاتی و شبکه‌ای: به طرف فرهنگ امنیتی» را انتشار داد. در مورد ایمن کردن سامانه‌های اطلاعاتی، سازمان فوق، قاعده‌ای را ایجاد اجرا است که بر اصل آن، کشورها و قسمت‌های خصوصی، به صورت غیر گروهی یا سازگار با همدیگر، می‌توانند قلمرویی برای امنیت سامانه‌های اطلاعاتی ایجاد نمایند. این حیطه شامل قوانین، قواعد رفتاری، تدابیر فنی، تجربه‌های مدیران و کاربران، تعلیم و مطلع نمودن اشخاص می‌شود. تدابیر نهاد همکاری و توسعه اقتصادی، بخش‌های عمومی و خصوصی (افراد) را مخاطب خود قرار داده و در همه‌ی سیستم‌های اطلاعاتی و شبکه‌ای قابل اتکاء است.( Kenneth, 2006: 102).

**۳-۲-۳-هشتمین نشست سازمان ملل متحد درباره پیشگیری از جرم و اصلاح مجرمین**

قطعنامه مذکور، حاصل کوشش سیزدهمین نشست جلوگیری از جرم و آگاهی مجرمین، در مورد جرایم کامپیوتری بود که با شماره ٤٥/١٢١ در ١٤ دسامبر سال ۱۹۹۸ در مجمع عمومی سازمان ملل مورد قبول واقع شد. مجمع عمومی در قطعنامه فوق از کشورهای عضو می‌خواهد که به هدف مبارزه با جرایم رایانه‌ای، مواردی از این دست را در دستور کار خود قرار دهند: به‌روزکردن مقررات و رسیدگی‌های جزایی ملّی، ارتقا و اجرای

تدابیر پیشـــگیرانه و امنیتی برای هر نوع بهره بردن از کامپیوتر با لحاظ حریم خصـــوصـــی کاربران و آزادی‌های قانونی اشـــخاص، ازدیاد آگاهی عمومی و دقت مقنین و افراد نسبت به جرایم کامپیوتر و تمسک به اعمال پیشگیرانه، آموزش به صاحبنظران قوه قضاییه در خصوص تدابیر کیفری مربوط به جرایم رایانه‌ای و مالی، بررســی و همکاری با نهادهای ذینفع در خصـــوص رفتار اســـتفاده از رایانه و مبادرت به گردآوری مواد درســـی و آموزشـــی بـه هـدف بـالا بردن رونـد اطلاع عمومی و نیز بکـار بردن سـیاسـت‌های مربوط به بزه‌دیدگان جرایم رایانه‌ای، بر طبق اعلامیه اصـول اساسی عدالت برای بزه‌دیدگان قربانیان سوءاستفاده از قدرت تلاش نمایند (UN Resolution, 45/121, 1998)

در پـایـان می‌توان نتیجـه گرفـت کـه در جهـت حمـایـت از بزه دیـدگـان تروریسـم سـایبری در نظام حقوقی ایران، هیچ نوع مقررات مخصـوصـی پیش بینی نشـده اسـت. با انتخاب کیفر برای مرتکبان جرایم سایبری صـرفا حمایت های کیفری برای بزه دیدگان ســـایبری به کار برده شـــده و دیگر احتیاج بزه دیدگان بدون ترمیم باقی مانده اســـت. لذا، برطرف کردن زیان مادی ناشی از بزه دیدگی سایبری هم، صرفا با اتکا به بعضی اصول کلی، مانند قانون مسئولیت مدنی جهت برطرف نمودن زیان مادی از بزه دیدگان سـایبری پرداخته و برای مسـئولیت روانی هم تدابیری در نظر گرفته نشـده اسـت. اسـناد بین المللی هم با وجود توجه خاص به مسـئله تروریسـم در چارچوب قطعنامه ها، پروتکل ها و اعلامیه‌های الزام آور در خصـــوص جرم انگاری اعمال بزهکارانه تروریستی، سندی ویژه به تروریسم سایبری وجود نداشته و در سایر اسناد مرتبط با تروریسم، به جرم انگاری تروریسم سایبری و حمایت از بزه دیدگان اقدام نشده است.

**نتیجه‌گیری**

تروریسم سایبری به یکی از چالش‌های اصلی نظام‌های حقوقی، به ویژه نظام‌های کیفری مبدل گشته است. بزه تروریسم، دیگر از مواضع قدیمی خود کم رنگ شده و به سوی فناوری‌های نوین متمایل شده است. در بیشتر کشورهای دنیا به خصوص جوامع پیشرفته از تاسیسات رایانه ای و مخابراتی در انجام امور روزمره و اجرایی کشور مانند امور اعتباری و مالی. اتوماسیون های اداری، کنترل و نظارت‌های زیرساختی در حوزه‌های صنعتی، نظامی، بهداشتی. و... استفادهمی شود. زیرساخت های حیاتی و اطلاعاتی، به عنوان عمده ترین بزه دید گان تروریسم سایبری، بیشترین جذابیت و مطلوبیت را برای تروریست‌های سایبری دارند. با نگاهی به افزایش رخدادها و حمله‌های سایبری علیه بیشتر کشورهای توسعه یافته وبروز خسارات شدید در زیرساخت های حیاتی» می توان به فاجعه آمیز بودن نتایج حملات تروریستی سایبری علیه سیستم هاو دارایی‌های پی برد که تاثیرات شدیدی بر امنیت فیزیکی، اقتصاد ملی یا ایمنی همگانی خواهند گذاشت. در سال هایاخیر استفاده از این گونه حملات. علیه تاسیسات مهم و حیاتی دولت ها گسترش یافته و به دلیل خصیصه پنهان ماندن هویتبزهکاران مذ کور این گونه از تروریسم مورد توجه ویره اشخاص و دولت ها قرار گرفته است.

جهت پیشگیری و مقابله با تروریسم سایبری، لزوم توسعه معاضدت بین المللی در دنیای کنونی امری واجب می‌باشد. در فضای سنتی و با رواج تروریسم بین‌المللی، تقریباً اکثر کشورها قبول کرده‌اند که مبارزه با تروریسم مگر با معاضدت‌های بین المللی ممکن نیست. این امر در خصوص تروریسم سایبری بارزتر می‌باشد و به دلیل اینکه فضای سایبری، احتمال وقوع جرم می‌باشد و این احتمال هم بی مرز و بدون محدودیت می‌باشد؛ امکان داخلی کردن مبارزه با تروریسم سایبری وجود نداشته یا این امر با شکست مواجه می‌شود. مواجهه کارآمد در مقابل اعمال تروریستی سایبری دربرگیرنده یکپارچه سازی حقوق کیفری ماهوی و شکلی دولت‌ها، ارتقای همکاری‌های بین المللی و اعمال پیشگیرانه همجون حفاظت از زیرساخت ها و تأمین امنیت فضای سایبر دارد.

بنابراین در سطح بین‌المللی اقدامات مناسب و درخوری با هدف پیشگیری از تروریسم سایبری انجام نشده است. امری در اسناد بین‌المللی در خصوص عنصر قانونی تروریسم سایبری امکان دارد، از آن استنباط کرد؛ جرایمی است که زیادترین ظهور را در معنی تروریسم سایبری دارند و به شکل عام و بلاواسطه به تروریسم سایبری تاکید نموده‌اند. نهادهای

بین‌المللی که در راس آنان سازمان ملل متحد قرار گرفته است و نیز شورای وزرای اروپا که نقش زیادی را در راستای ارتقا و توسعه جرم‌انگاری جرایم سایبری در دهه گذشته بازی نموده‌اند، قادر هستند با به کارگیری از مجمع‌های تخصصی و بهره‌گیری از صاحبنظران سایر کشورها که در خصوص تروریسم سایبری و جرم‌انگاری آن پیشرو بوده‌اند، برای گردآوری پروتکل‌های الزام‌آور بین‌المللی در مورد جلوگیری از تروریسم سایبری و پشتیبانی مخصوص از بزه‌دیدگان آن اقدام نمایند. لذا ایجاد کمیسیون‌هایی به هدف تحلیل و تبیین تخصصی کارزارهای الکترونیکی ضروری می‌نماید.

## منابع و مآخذ

منابع فارسی:


۱) پاکزاد، بتول (۱۳۹۰). ماهیت تروریسم سایبری، مجله تحقیقات حقوقی، دوره ١٤، شماره ٤، ٢٤٩-٢١٥

۲) پورنقدی، بهزاد و بختیاری، ارشد (۱۳۹۲). تروریسم سایبری و اهمیت آن در بر هم زدن امنیت بین‌الملل، مطالعات بین‌المللی پلیس، شماره ١٤، ٢٩-٤٦

۳) روزبهانی، محمدرضا (۱۳۹۸). تروریسم سایبری در حقوق ایران و بین‌الملل، تهران: مجد، چاپ دوم

٤) طیبی فرد، امیرحسین (١٣٨٤). مبارزه با تأمین مالی تروریسم در اسناد بینالمللی، مجله حقوقی دفتر خدمات حقوقی بینالمللی، شماره ،32

٥) کدخدایی، عباسعلی، ساعد، نادر (۱۳۹۰). تروریسم و مقابله با آن، مطالعات راهبردی سیاستگذاری عمومی، دوره ۳، شماره ٦

٦) کوشا، جعفر، نامیان، پیمان (۱۳۸۷). جایگاه اعمال تروریستی در پرتو حقوق بین‌الملل کیفری. فصلنامه حقوق، شماره ۳

۷) کیهانلو، فاطمه، رضادوست، وحید (۱۳۹۳). حملات سایبری به مثابه توسل به زور در سیاق منشور سازمان ملل متحد، فصلنامه تحقیقات حقوقی، شماره ٦٩

۸) نمامیان، پیمان و عباسی، صمد (۱۳۹۱). تأملی در قطعنامه ۱۳۷۳ شورای امنیت: تغییر ماهیت در تعهدات و الزامات حقوقی مبارزه با تروریسم . فصلنامه مطالعات بین‌المللی‌پلیس، شماره ۳، ١٤٩-١٦٨

۹) هاشمی، حسین (۱۳۹۵). تروریسم از منظر حقوق اسلام و اسناد بین‌المللی، قم: پژوهشگاه حوزه و دانشگاه، چاپ دوم

منابع انگلیسی


1) Abramovsky, A. ( 1975). Multilateral Conventions for the Suppression of Unlawful Seizure and Interference with Aircraft, Part II: The Montreal Convention, 14 (2) colum. J. Transnat'l l, Vol. 14, No. 2
2) Cohen, A. (2010). Cyberterrorism: Are we Legally Ready?, The Journal of International Business & Law, Vol. 4, No. 15.
3) Dandurand, Yvon, "Links between Terrorism and Other Forms of Crimes", International Center for Criminal Law Reform and Criminal Justice Policy, 2005, pp. 587-596
4) Dorothy E. Denning, A View of Cyberterrorism Five Years Later, Chapter 7 in Internet Security: Hacking, Counterhacking, and Society (K. Himma ed.), Boston: Jones and Bartlett Pub, 2007, pp. 1-19
5) Follmar Otto, Petra and Rabe, Heike, Human Trafficking in Germany, Berlin: German Institute for Human Rights Pub, 2009, p. 95
6) Harrison dinniss H. Cyber Warfare and the Laws of 3War, Gorouhe Tadvin va Tarjomeh Sazman Padafand Gheire Amel. Tehran: Jahan Jame Jam; 2015.
7) ICAO, International Conference on Air Law: Minutes and Documents, ICAO Doc. 9801, p. 21, Delegates of France and Japan (hereinafter: "ICAO Documents").
8) Kenneth J. K., and Boulton R. W., "Cyber-Warfare Threatens Corporations: Expansion into Commercial Environments", Information Systems Management, vol. 23, Issues 2, 2006, pp. 76-87
9) Much, C. (2006). The International Criminal Court (ICC) and Terrorism as an International crime, MICH. ST. J. INT'L L, No.
10) Sofaer, A. & Goodman, E. (2000). A Proposal for an International Convention on Cyber Crime and Terrorism, Hoover Institution, Stanford
11) Nations Counterterrorism Implementation Task Force. "The use of the Internet for terroris