مجله حقوقی بین‌المللی/ شماره ۶۰/ بهار ـ تابستان ۱۳۹۸/ صفحات ۲۶۷ ـ ۲۳۷

بررسی تطبیقی حقوق کیفری ایران با اسناد بین‌المللی در زمینه مقابله و پیشگیری از وقوع تروریسم سایبری

محسن قدیر *

حسین کاظمی فروشانی **

شناسه دیجیتال اسناد (DOI) : 10.22066/cilamag.2019.35084

تاریخ دریافت: ۱۳۹۶/۱۰/۲۰ تاریخ پذیرش: ۱۳۹۶/۱۱/۲۸

چکیده

پیشگیری از وقوع تروریسم سایبری به منظور حمایت از بزه‌دیدگان آن است اما در میان اکثر نظام‌های حقوقی جهان، به جرم‌انگاری تروریسم سایبری، صریح و اختصاصی پرداخته نشده است. بررسی منابع قانونی در حقوق ایران نشان می‌دهد که در خصوص پیشگیری از این بزه در مقررات کیفری، مقرره خاصی وجود ندارد بلکه با استناد به برخی قوانین عام همچون قانون جرایم رایانه‌ای و قانون مجازات اسلامی می‌توان به مواضع پیشگیرانه حقوق کیفری ایران در زمینه پیشگیری از این بزه و حمایت از بزه‌دیدگان آن اشاره کرد. لذا قانون کیفری ایران فاقد جرم‌انگاری مستقل در مورد تروریسم و جرایم آن است و در واقع، سیاست جنایی ایران مبتنی بر سیاست مصداقی است و می‌توان از مواردی که با مفهوم تروریسم منطبق است (مانند محاربه)، آن را تشخیص داد. به منظور ممانعت از هرگونه ایراد خسارت بیشتر بر زیرساخت‌های اطلاعاتی کشور، لزوم اتخاذ تدابیر پیشگیرانه احساس می‌شود. با نگاهی به اسناد بین‌المللی درباره جرایم سایبری و تروریستی و انواع قطعنامه‌های سازمان‌های بین‌المللی، جهانی و منطقه‌ای که سازمان ملل متحد در رأس آن‌ها قرار دارد، می‌توان به این نتیجه رسید که در سطح فراملی اقدامات کافی و شایسته‌ای به منظور پیشگیری از تروریسم سایبری صورت نپذیرفته است.

واژگان کلیدی

تروریسم سایبری، پیشگیری، بزه‌دیدگان، حقوق ایران، اسناد بین‌المللی

* نویسنده مسئول، استادیار حقوق بین‌الملل دانشگاه قم mnghadir@gmail.com

** کارشناسی ارشد حقوق بین‌الملل دانشگاه قم kazemibehzad75@ymail.com

مقدمه

تروریسم اغلب متضمّن حمله به بزه‌دیدگانی بوده که در ایجاد شرایطی که به‌طور آشکار محرّک یا توجیه‌کننده خشونت تروریستی بوده است، هیچ‌گونه نقش یا مسئولیتی نداشته‌اند.[۱] حمایت مؤثر از بزه‌دیدگان تروریسم، بخشی از عدالت حقوقی است که جامعه بین‌المللی با وجود تأکید بر چنین حمایتی، سازوکارهای لازم برای عملی‌کردن آن را تدارک ندیده است.[۲] بررسی مواد و منابع قانونی در حقوق ایران نشان می‌دهد که در خصوص پیشگیری از این بزه در مقررات کیفری، مقرره خاصی وجود ندارد، بلکه با استناد به برخی قوانین عام همچون قانون جرایم رایانه‌ای، قانون مجازات اسلامی و سایر قوانین متفرقه می‌توان به مواضع پیشگیرانه حقوق کیفری ایران در زمینه پیشگیری از این بزه و حمایت از بزه‌دیدگان آن اشاره کرد. همچنین با نگاهی به اسناد بین‌المللی درباره جرایم سایبری و تروریستی و انواع قطعنامه‌های سازمان‌های بین‌المللی و منطقه‌ای که سازمان ملل متحد در رأس آن‌ها قرار دارد، می‌توان به این نتیجه رسید که در سطح فراملّی، اقدامات کافی و شایسته‌ای به منظور پیشگیری از تروریسم سایبری صورت نپذیرفته است. سازمان ملل متحد، به‌عنوان بزرگ‌ترین مرجع بین‌المللی، از سال ۱۹۶۳ تاکنون، درباره تروریسم و اقدامات تروریستی، سیزده سند بین‌المللی به تصویب رسانده و جالب اینکه تنها در سه سند صراحتاً به‌عنوان تروریسم اشاره شده و در بقیه تنها مصادیق اقدامات تروریستی برشمرده شده است.[۳] با توجه به مستندات ارائه‌شده، ازجمله قطعنامه‌های(۴۵/۱۲۱)، (۴۶/۱۵۲)، (۱۹۹/۲۲) تا سال ۱۹۹۰ و همچنین توصیه‌نامه‌های متعدد که منجر به تصویب کنوانسیون ۸ نوامبر ۲۰۰۱ شورای اروپا شد، تروریسم رایانه‌ای یا سایبری را تعریف کرده و همچنین راهکارهای جدید را برای مقابله بین‌المللی و داخلی توسط کشورها ارائه کرده است.[۴] در ایران نیز در سال‌های اخیر، قوانین و مقرراتی در مورد مبارزه با تهدیدات سایبری توسط اشخاص حقیقی و حقوقی تدوین شده است که به نظر می‌رسد ناکافی بوده ولی توانسته تا حدودی مشکلات حقوقی را در این مورد مرتفع سازد.[۵]

---

1. Curavic, Danica, "Compensating Victims of Terrorism or Frustrating Cultural Diplomacy?", *Cornell International Law Journal*, vol. 43, 2010, pp. 405- 407.

2. Reisman, Micheal, "Illusion & Reallity in the Compensation of Victims of International Terrorism", *Alabama Law Review*, Winter, vol. 54, No 2, 2003, pp. 217-219.

3. Cherrif Bassioni, "International Terrorism", *Transnational Journal of China*, 2015, pp. 487-490.

4. Aberenthly, A.D, "Anger Management Training for Law Enforcement Perssonel", *Journal of Criminal Justice*, vol. 22, No. 5, 1994, p. 21.

۵. نمامیان، پیمان؛ *واکنش‌های عدالت کیفری به تروریسم*، میزان، ۱۳۹۱، ص ۱۷۸.

۱. پیشگیری از وقوع تروریسم سایبری در حقوق ایران

۱ـ۱. اقدامات پیشگیرانه کیفری

الف. قانون جرایم رایانه‌ای، مصوب ۱۳۸۸

در خصوص مواد قانونی کیفری، در رابطه با پیشگیری از وقوع تروریسم سایبری و به تبع حمایت از بزه‌دیدگان آن، می‌توان به موادی از این قانون اشاره کرد که شباهت خاصی به جرم‌انگاری تروریسم سایبری دارد. یکی از مقررات این قانون مقرر می‌دارد:

«هر کس به قصد به‌خطرانداختن امنیت، آسایش و امنیت عمومی، اعمال مذکور در مواد ۸، ۹ و ۱۰ این قانون را علیه سیستم‌های رایانه‌ای و مخابراتی که برای ارائه خدمات ضروری عمومی به کار می‌روند، از قبیل خدمات درمانی، آب، برق، گاز، مخابرات، حمل‌ونقل و بانکداری مرتکب شود، به حبس از سه تا ده سال محکوم خواهد شد».[۶]

مقرره فوق، دو دسته از بزهکاران، یعنی اشخاص حقیقی و حقوقی را خطاب قرار داده است که با تعیین کیفر در انتهای ماده، به بازدارندگی مرتکبان افعال مندرج در ماده ۱۱ اشاره کرده است. بزه‌دیدگان مورد حمایت در این مقرره، سامانه‌های رایانه‌ای و مخابراتی هستند که برای ارائه خدمات ضروری عمومی به کار می‌روند. با توجه به اینکه در تروریسم سایبری به تأسیسات مورد استفاده عمومی حمله می‌شود، اقدام شایسته‌ای توسط قانونگذار به شمار می‌رود. در این راستا قانونگذار با تعیین مجازات، به ارعاب بزهکاران بالقوه که قصد ارتکاب اعمال مندرج در این ماده را دارند و همچنین تکرار بزه توسط بزهکاران بالفعل اقدام کرده است.[۷]

قانون جرایم رایانه‌ای در مبحث دوم از این قانون به موضوع تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی پرداخته است که با جرم‌انگاری اعمال غیرمجاز از قبیل حذف یا تخریب یا مختل یا غیرقابل‌پردازش‌کردن داده‌های رایانه‌ای و مخابراتی، دو گونه مجازات را برای مرتکب این افعال در نظر گرفته است: یکی حبس از شش ماه تا دو سال و دیگری، جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات که گام مفیدی در جهت برحذرداشتن افرادی است که با توسل به چنین اعمالی به زیرساخت‌های اطلاعاتی کشور، به منظور دستیابی به اهداف مختلف استفاده می‌کنند.[۸]

---

۶. قانون جرایم رایانه‌ای، مصوب ۱۳۸۸، ماده ۱۱.

۷. کیفر تعیین‌شده در این ماده عبارت است از: سه تا ده سال حبس؛ اما با کمی دقت در اعمال ارتکابی و نتایج زیان‌بار آن بر امور اجرایی کشور، عدم تناسب کیفر تعیین‌شده با خسارت‌های حاصله نمایان می‌شود زیرا کیفر تعیین‌شده با گستردگی خسارات حاصل‌شده یکسان نیست. ایراد دیگر مجازات تعیین‌شده در این ماده این است که جا داشت قانونگذار، با توجه به چالش‌برانگیزبودن مجازات حبس که امروزه اکثر حقوق‌دانان با آن مخالف‌اند، در کنار آن، جریمه نقدی تعیین می‌کرد.

۸. قانون جرایم رایانه‌ای، مصوب ۱۳۸۸، ماده ۸.

یکی دیگر از جلوه‌های پیشگیری واکنشی از جانب قانونگذار کیفری، به منظور پیشگیری و مقابله با جرایمی از قبیل تروریسم سایبری، ماده دیگری از همین قانون است که به‌طور غیرحصری و مصداقی به افعال غیرمجازی اشاره کرده است که منجر به توقف یا اختلال عملیات سامانه‌های رایانه‌ای یا مخابراتی می‌شود. قانونگذار در این مقرره، مرتکب یا مرتکبان را به مجازات حبس از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات محکوم کرده است.[۹]

دسته‌ای دیگر از اعمال غیرمجازی که به‌طور معمول توسط تروریست‌های سایبری به منظور تخریب یا اختلال در داده‌ها و سامانه‌های رایانه‌ای و مخابراتی استفاده می‌شود، افعالی از قبیل مخفی‌کردن داده‌ها، تغییر گذرواژه یا رمزنگاری داده‌هاست که بدین وسیله، منجر به ممانعت از دسترسی اشخاص مجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی می‌شود. در این صورت قانونگذار با مجرمانه قلمدادکردن اعمال فوق، برای مرتکب، حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات را تعیین کرده است که با غیرحصری‌شمردن اعمال مذکور، اقدام شایسته‌ای را در جهت محافظت از داده‌ها و سامانه‌های رایانه‌ای، و همچنین با اعمال کیفر حبس یا جزای نقدی، بازدارندگی را برای انواع بزهکاران شکل داده است.[۱۰]

قانونگذار در این سه ماده به‌صورت کامل و غیرحصری به شایع‌ترین اعمال ارتکابی که علیه تأسیسات حیاتی کشور انجام می‌شود پرداخته است که اقدام شایسته‌ای در خصوص جرم‌انگاری افعال مرتبط با تروریسم سایبری به شمار می‌رود. علاوه بر قوانینی که به‌طور مستقیم به بیان مجازات اشخاصی که به تأسیسات حیاتی کشور، اعم از رایانه‌ای و مخابراتی تعرّض می‌کنند، اشاره دارند، در لابه‌لای موادی دیگر از قانون جرایم رایانه‌ای، دسته‌ای از افعال جرم‌انگاری‌شده وجود دارد که برای ارتکاب تروریسم سایبری در اولویت قرار دارند. نمونه‌ای از افعال مذکور، جاسوسی رایانه‌ای، شنود و دسترسی غیرمجاز است که نفوذگران تروریستی از بدافزارهای گوناگونی برای دستیابی به اطلاعات محرمانه و حیاتی از آن‌ها استفاده می‌کنند.[۱۱] عناصر این

---

۹. *همان*، ماده ۹.

۱۰. *همان*، ماده ۱۰.

۱۱. *همان*، مواد ۱ تا ۴.

ماده ۱، برای کسی که مرتکب دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی شود، حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هردوی آن‌ها را تعیین کرده است. ماده ۲ به جرم‌انگاری شنود غیرمجاز و تعیین کیفر از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دوی آن‌ها و ماده سه به جاسوسی رایانه‌ای اشاره دارد. نفوذگران تروریستی برای طرح‌ریزی حملات سایبری نیاز به اطلاعات در مورد زیرساخت‌های

جرم در حقیقت، هر نوع پردازش، مشاهده، شنود، دریافت یا ذخیره غیرقانونی اطلاعات در حال انتقالی است که مجرم، مجاز به دریافت یا شنود آن نیست. آنجا که داده غیرعمومی و خصوصی است، اگر غیرتجاری باشد، مشمول ماده ۳ قانون مجازات جرایم رایانه‌ای می‌شود. اما اگر تجاری باشد مشمول ماده ۵۸ قانون تجارت الکترونیک است. اما اگر عمومی و جزء اطلاعات سرّی باشد، مشمول ماده ۴ قانون مجازات جرایم رایانه‌ای است.

ماده ۳ فروع مختلف شنود و دریافت غیرمجاز، اعم از شنود داده‌های خصوصی، تجاری، عمومی سرّی و مربوط به امنیت ملی را شامل می‌شود. اما مواد خاصی، چون ماده ۵۸ قانون تجارت الکترونیکی و ماده ۴ قانون مجازات جرایم رایانه‌ای موارد تجاری و مربوط به امنیت ملی را تخصیص می‌زند.[۱۲]

ب. قانون تجارت الکترونیکی، مصوب ۱۳۸۲

با توجه به اینکه داده‌های رایانه‌ای و مخابراتی، اصلی‌ترین آماج جرم برای تروریست‌های سایبری محسوب می‌شود، لزوم حمایت از آن در برابر افعال غیرمجاز که به تمامیت و محرمانه‌بودن آن‌ها تعرّض می‌کند ضروری است. فصل دو از مبحث سوم این قانون، مجازات اشخاصی را بیان می‌کند که شرایط داده‌های مورد حمایت در مواد ۵۸ و ۵۹ این قانون را نقض می‌کنند و برای مرتکب کیفر، یک تا سه سال حبس را تعیین کرده است.[۱۳] در جایی دیگر از این قانون، به حمایت کیفری ویژه از داده‌پیام‌های شخصی پرداخته شده که جرایم علیه این داده‌ها توسط نهادهای مسئول و دفاتر خدمات صدور گواهی الکترونیکی ارتکاب می‌یابد. در این صورت برای مرتکب، حداکثر کیفر تعیین‌شده در ماده ۷۱ مقرر شده است.[۱۴] همچنین قانون تجارت الکترونیکی نیز با بی‌مبالاتی و بی‌احتیاطی دفاتر خدمات صدور گواهی (که مسئول حفظ داده‌پیام‌های شخصی نیز هستند) برخورد می‌کند.

ماده ۶۴ قانون تجارت الکترونیکی بر اصل ممنوعیت دسترسی غیرمجاز تأکید کرده و با ناقضین این اصل، برخورد شدیدتری کرده است. ماده ۷۵ این قانون، مجازات شدیدتری نسبت به ماده ۲ قانون مجازات جرایم رایانه‌ای تعیین کرده است. به‌موجب این ماده: «متخلّفین از ماده ۶۴

حیاتی یا اطلاعاتی دارند تا با استفاده از اطلاعات کسب‌شده و نحوه پیکربندی سامانه‌ها، علیه داده‌ها و سامانه‌های رایانه‌ای و مخابراتی مرتکب عملیات غیرقانونی بشوند.

۱۲. الهویی نظری و فامیل زوار جلالی؛ «مسئولیت بین‌المللی دولت‌های تأمین‌کننده مالی تروریسم»، *مجله مطالعات حقوق عمومی*، شماره ۳، دوره چهل‌وهفتم، پاییز ۱۳۹۶، صص ۷۴۲-۷۴۱.

۱۳. ماده ۷۱ قانون تجارت الکترونیکی، مصوب ۱۳۸۲.

۱۴. *همان*، ماده ۷۲.

این قانون... به حبس از شش ماه تا دو سال و نیم، و جزای نقدی معادل پنجاه میلیون ریال محکوم خواهند شد». البته شدّت برخورد ماده ۷۵، گرچه کمتر از برخورد با دسترسی به داده‌های سرّی موضوع ماده ۴ قانون مجازات جرایم رایانه است، با توجه به اهمیت ویژه داده‌های سرّی که مرتبط با امنیت ملی کشور است، مجازات مقرر در ماده ۴ قانون مجازات جرایم رایانه‌ای از تناسب لازم برخوردار نبوده، شدّت بیشتری را می‌طلبد.[۱۵]

ج. قانون مجازات نیروهای مسلّح، مصوب ۱۳۸۲

امنیت اطلاعاتی یک کشور، زمانی حفظ خواهد شد که مأمورین ذی‌ربط با جدّیت تمام در برابر حملات اطلاعاتی بایستند و هوشیارانه و بدون کمترین اشتباهی از اطلاعات سرنوشت‌ساز کشور حراست کنند. ازاین‌روست که قانونگذاران به دلیل اهمیت حیاتی این امر، برخورد قاطعانه‌ای با کمترین کوتاهی در انجام وظیفه در آن دارند. قانونگذار در ماده ۵۰۶ قانون مجازات اسلامی، مأمورین آموزش‌دیده دولتیِ مسئول امور حفاظتی و اطلاعاتی طبقه‌بندی‌شده را که به دلیل بی‌مبالاتی و عدم رعایت اصول حفاظتی توسط دشمنان تخلیه اطلاعاتی شوند، به یک تا شش ماه حبس محکوم می‌کند. این قانون نیز در راستای جرم‌انگاری افعال غیرمجاز، اقسام اَعمال رایانه‌ای نظامیان را جرم‌انگاری کرده است که با توجه به مجازات‌های تعیین‌شده، بازدارندگی خاصی را برای این دسته از افراد تخصیص داده است. ازجمله جرایم رایانه‌ای مورد اشاره در این قانون، که افعال تشکیل‌دهنده تروریسم سایبری محسوب می‌شود و تروریست‌های سایبری از این طریق به فلج‌کردن زیرساخت‌های کشور اقدام می‌کنند، عبارت‌اند از: تخریب اطلاعات یا نرم‌افزارهای رایانه‌ای، تخریب سامانه‌های رایانه‌ای، سرقت یا معدوم‌کردن حامل‌های اطلاعات رایانه‌ای که قانونگذار حسب مورد، مرتکب را به مجازات‌های مقرر در این قانون محکوم می‌کند.[۱۶] با توجه به اینکه نیروهای نظامی و امنیتی به دلیل موقعیت شغلی در موقعیت حساس و ویژه‌ای قرار دارند، تدوین ضمانت اجراهای قوی به منظور ارعاب کارکنان سازمان‌های امنیتی حیاتی است. در این قانون به جرم‌انگاری دسته‌ای از افعال غیرقانونی نظیر تخریب اطلاعات اشاره شده است که رکن اصلی افعال تشکیل‌دهنده تروریسم سایبری به شمار می‌رود. حملات خودی که از شایع‌ترین حملات سایبری محسوب می‌شود، بیشتر توسط کارکنان ناراضی ارتکاب می‌یابد و نیروهای مسلّح نیز از این امر مستثنا نیستند. به همین دلیل، مفاد ماده ۱۳۱ قانون مجازات نیروهای مسلّح می‌تواند در زمینه پیشگیری کیفری از تروریسم سایبری مؤثر واقع

۱۵. احمری، حسین، غلامرضا کحلکی و حامد رحیم‌پور اصفهانی؛ «تحلیل سازه‌انگارانه تروریسم سایبری و رویکرد نظام حقوقی به آن»، *فصلنامه پژوهش‌های روابط بین‌الملل*، دوره نخست، شماره ۱۹، بهار ۱۳۹۵، ص ۳۲۷.

۱۶. ماده ۱۳۱ قانون مجازات جرایم نیروهای مسلّح، مصوب ۱۳۸۲.

شود.[۱۷]

د. قانون مجازات اسلامی، مصوب ۱۳۷۰

قانون مجازات اسلامی، یکی دیگر از تلاش‌های قانونگذار در زمینه پیشگیری واکنشی از تروریسم سایبری است. در این قانون، موادی مانند ماده ۱۱ قانون جرایم رایانه‌ای وجود دارند که به زیرساخت‌های اطلاعاتی کشور توجه کرده‌اند، یعنی آنچه مدنظر تروریست‌های سایبری به‌عنوان هدف ایده‌آل انجام عملیات‌های تروریستی است. ماده ۶۸۷ قانون مجازات اسلامی (تعزیرات ۷۵) بیان می‌دارد:

«هر کس در وسایل و تأسیسات مورد استفاده عمومی از قبیل شبکه‌های آب و فاضلاب، برق، نفت، گاز، پست و تلگراف و تلفن و مراکز فرکانس و ماکروویو (مخابرات) و رادیو و تلویزیون و متعلقات مربوط به آن‌ها اعم از سد و کانال و انشعاب لوله‌کشی و نیروگاه‌های برق و خطوط انتقال نیرو و مخابرات (کانال‌های هوایی یا زمینی یا نوری) و دستگاه‌های تولید و توزیع و انتقال آن‌ها که به هزینه یا سرمایه دولت یا با سرمایه مشترک دولت و بخش غیردولتی یا توسط بخش خصوصی برای استفاده عمومی ایجاد شده و همچنین در علایم راهنمایی و رانندگی و سایر علائمی که به منظور حفظ جان اشخاص یا تأمین تأسیسات فوق یا شوارع و جاده‌ها نصب شده است، مرتکب تخریب یا ایجاد حریق یا ازکارانداختن یا هر نوع خرابکاری دیگر شود، بدون آنکه منظور او اخلال در نظم و امنیت عمومی باشد به حبس از سه ماه تا ده سال محکوم خواهد شد».

در ادامه همین ماده، قصد خاص و سوءنیت مرتکب یا مرتکبین را مدنظر قرار داده است و در این خصوص بیان می‌دارد:

«تبصره ۱: در صورتی که اعمال مذکور به منظور اخلال در نظم و امنیت جامعه و مقابله با حکومت اسلام است، مجازات محارب را خواهد داشت».[۱۸]

این ماده، شباهت خاصی به جرم‌انگاری تروریسم سایبری دارد. در این ماده، به انواع زیرساخت‌های حیاتی کشور توجه شده و در صورت داشتن قصد خاص مرتکب به اخلال در نظم و امنیت عمومی، مجازات مرتکب، اعدام خواهد بود و همچنین در صورت نبود سوءنیت خاص مذکور، مرتکب به حبس از سه ماه تا ۱۰ سال محکوم می‌شود. این ماده نیز همانند ماده ۱۱ قانون جرایم رایانه‌ای، گام مهمی در زمینه مقابله و پیشگیری از تروریسم سایبری است، با این تفاوت که در ماده ۱۱ قانون جرایم رایانه‌ای، قصد اخلال در نظم و مقابله با نظام قید نشده است.

۱۷. پوربافرانی، حسن؛ *حقوق جزای بین‌الملل*، جنگل، ۱۳۹۶، ص ۱۸۹.

۱۸. *همان*، تبصره ۱.

البته هرچند ماده ۶۸۷، به‌صورت جامع‌تر به بیان تروریسم سایبری پرداخته، از نظر بیان افعال تشکیل‌دهنده جرم، با ابهام مواجه است. بنابراین، قانونگذار با تعیین کیفر محارب، به بیان شدّت آثار ارتکاب بزه، علیه تأسیسات مذکور توسط بزهکاران بالقوه یا بالفعل اشاره کرده که این تعیین کیفر، دارای سطح بالای بازدارندگی در میان افراد جامعه است تا مرتکب چنین اعمالی نشوند.[۱۹]

۱ـ۲. اقدامات پیشگیرانه غیرکیفری

الف. پیشگیری اجتماعی

پیشگیری اجتماعی، علل و عوامل اجتماعی مؤثر بر ظهور بزه را مدنظر داشته و با توجه به عوامل اقتصادی، سیاسی، فرهنگی و اجتماعی و تأمین حقوق اجتماعی، سیاسی و اقتصادی و... سعی در کاهش یا ریشه‌کن‌کردن جرم دارد. به عبارت دیگر، پیشگیری اجتماعی به دنبال ازبین‌بردن انگیزه‌های مجرمانه و منحرفانه است.[۲۰] این نوع از پیشگیری، به دو دسته پیشگیری اجتماعی جامعه‌مدار[۲۱] و پیشگیری اجتماعی رشدمدار[۲۲] تقسیم می‌شود.

در پیشگیری جامعه‌مدار، سعی بر این است که با استفاده از تدابیری مانند برنامه‌ریزی در حوزه اشتغال و تلاش در جهت ازبین‌بردن عوامل اجتماعی مولّد جرم، نظیر عدم پایبندی به اخلاق سایبری یا فقر، به پیشگیری از پیدایش انحرافات و انگیزه‌های مجرمانه در فضای سایبر که دارای منشأ اجتماعی هستند، اقدام شود. در حوزه جرایم تروریستی سایبری، با مطالعه ویژگی‌ها و شخصیت‌های مرتکبان و همچنین بررسی موقعیت و نفوذپذیری بزه‌دیدگان مذکور می‌توان به ارائه راهکارهای متفاوت به منظور ممانعت از شکل‌گیری انحرافات و انگیزه‌های مجرمانه در بزهکاران و بزه‌دیده‌شدن اشخاص اقدام کرد.[۲۳] در زمینه اقدامات پیشگیرانه در حوزه پیشگیری اجتماعی از تروریسم سایبری، مسئله آموزش کاربران اینترنت، اعم از کاربران خانگی و کارکنان ادارات و فرهنگ‌سازی در جامعه، مؤثرترین عامل در انصراف بزهکاران بالقوه از ارتکاب جرم در محیط سایبر است. کاربران خانگی و کارکنان ادارات که با تأسیسات رایانه‌ای و مخابراتی مخصوصاً در مراکز حساس سروکار دارند، باید در زمینه امنیت سایبری با هدف تربیت نیروی انسانی ممتاز و متعهد، مباحث مربوط به امنیت، شامل امنیت شبکه، امنیت در سرویس‌های وب، امنیت سامانه عامل، رمزنگاری، تحلیل بدافزار، مهندسی اجتماعی معکوس، ردگیری در فضای

۱۹. صنوبر، ناصر؛ *اقتصاد تروریسم*، بورس، ۱۳۹۳، ص ۶۶-۶۴.

۲۰. جلالی فراهانی، امیرحسین و رضا باقری اصل؛ «پیشگیری اجتماعی از جرایم سایبری، راهکاری اصلی برای نهادینه‌سازی اخلاق سایبری»، فصلنامه اطلاع‌رسانی و کتابداری ره‌آورد نور، شماره ۲۴، پیاپی ۴۱، پاییز ۱۳۸۷، صص ۱۹-۱۰.

21. Social based – crime prevention

22. Social developmental based – crime prevention

۲۳. جلالی فراهانی و باقری اصل؛ *همان*، ص ۱۳۲.

سایبر و امنیت سامانه‌های تلفن همراه، آموزش و آگاهی کافی داشته باشند. لذا در خصوص مقررات مربوط به فعالیت‌های آموزشی و امنیتی اتخاذشده، می‌توان به مقررات غیرکیفری گوناگونی ازجمله موارد زیر اشاره کرد:[۲۴] برنامه جامع توسعه تجارت الکترونیکی، مصوب ۱۳۸۴، برنامه چهارم توسعه مرتبط به فناوری اطلاعات، قانون برنامه پنج‌ساله پنجم توسعه جمهوری اسلامی ایران، مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه‌ای، مصوبه شورای عالی اداری در خصوص اتوماسیون نظام اداری و اتصال به شبکه جهانی اطلاع‌رسانی، سیاست تجارت الکترونیکی جمهوری اسلامی ایران، سند راهبردی امنیت فضای تبادل اطلاعات، مصوب ۱۳۸۴.

پیشگیری رشدمدار، به مجموعه تدابیری اشاره دارد که با خنثی‌سازی عوامل اجتماعی جرم‌زا و منحرفانه در سنین رشد و دوران تکامل شخصیتی کودکان به اجرا درمی‌آید. با توجه به اینکه بیشترین طرفداران محیط سایبر، جوانان و نوجوانان هستند، به طبع، بیشترین آمار بزهکاری و بزه‌دیدگی را نسبت به سایر اقشار جامعه به خود اختصاص می‌دهند. لذا با استفاده از رهیافت‌های پیشگیری رشدمدار می‌توان با مداخله در مراحل اولیه شکل‌گیری شخصیت کودکان و سنین رشد آن‌ها با استفاده از تدابیر محدود و کنترل‌کنندهٔ دسترسی به فضای مجازی توسط والدین، رسانه‌های جمعی، مدرسه و تدابیر الزام‌آور قانونی، به‌طور فزاینده‌ای از بزهکاری یا بزه‌دیدگی آن‌ها در آینده جلوگیری کرد.[۲۵]

برای نمونه‌ای از تلاش‌های صورت‌گرفته به منظور پیشگیری از بروز انحرافات سایبری، می‌توان به برگزاری دوره‌های آموزشی رایانه در مدارس فنی حرفه‌ای و اماکن فرهنگی کشور اشاره کرد که از سنین پایین کودکی برای کودکان و نوجوانان اعمال می‌شود. به‌طور کلی، روند شکل‌گیری جرم، تابع سه عامل است. این سه عامل که به مثلث جرم شهرت دارند، عبارت‌اند از: انگیزه مجرمانه که نقش اولیه را در پیدایش بزه ایفا می‌کند، مقدمه‌ای برای پیدایش قصد مجرمانه است که به دنبال انگیزه در فرد بزهکار به وجود می‌آید. عامل دوم، فرصت‌های ارتکاب جرم و عامل سوم، وسایل و ابزار ارتکاب است. پیشگیری اجتماعی از طریق روش‌هایی چون بالابردن ارزش‌ها و تقویت نهادهای اجتماعی، مانند خانواده و مدرسه، ازبین‌بردن انگیزه‌های مجرمانه از طریق اصلاحات فردی و اجتماعی، مانند نارسایی‌های ذهنی و جسمی اقدام می‌کند. در زمینه موضوعات مورد بحث، این نوع پیشگیری در زمینه علت‌یابی و جلوگیری از به‌وجودآمدن ریشه‌های تروریسم در جامعه تأثیر بسزایی دارد.[۲۶]

---

۲۴. ناصری، علی اکبر؛ *هندبوک مجموعه قوانین و مقررات فناوری اطلاعات و ارتباطات (ICT)*، خرسندی، ۱۳۸۷، صص ۱۶۵-۱۵۵.

۲۵. جلالی فراهانی و باقری اصل؛ *همان*، ص ۱۲.

۲۶. *پیشین*، ص ۱۳۱.

ب. پیشگیری وضعی[۲۷]

یکی از راهکارهای مهم برای پیشگیری از بزه‌دیدگی ناشی از تروریسم سایبری، پیشگیری وضعی است. پیشگیری وضعی از جرم را به‌عنوان اقدامات قابل سنجش و ارزیابی مقابله با جرم می‌داند. این اقدامات، معطوف به اشکال خاصی از جرم بوده و از طریق اعمال مدیریت یا مداخله در محیط بلاواسطه به شیوه‌های پایدار و نظام‌مند، منجر به کاهش فرصت‌های جرم و افزایش خطرات جرم می‌شود که همواره مدنظر تعداد زیادی از مجرمین بوده است.[۲۸]

این پیشگیری به‌وسیله دستکاری و تغییر موقعیت و محیط در فرآیند وقوع جرم، به کاهش فرصت‌های ارتکاب جرم کمک می‌کند. از میان روش‌های مختلف پیشگیری از جرم، پیشگیری وضعی، بهترین راهکارها را برای کاهش فرصت‌های ارتکاب جرم در جرایم سایبر و به تبع آن، تروریسم سایبری پیشنهاد می‌کند. در خصوص اقدامات پیشگیرانه وضعی، می‌توان به اقدامات فنی پیشگیرانه در قوانین و مقررات کشور و اقدامات سازمان‌ها و مؤسسات کشور در زمینه ایمن‌سازی فضای سایبر اشاره کرد که به‌وسیله دستکاری و تغییر موقعیت در آماج بالقوه جرم به کاهش فرصت‌ها و افزایش زحمات ارتکاب بزه تروریسم سایبری می‌انجامد. تدابیر فنی، بیشتر از هر راهکاری در مقابله با تروریسم سایبری مفید واقع می‌شود. هرچند تدابیر دیگری همچون حمایت‌های تقنینی را نباید نادیده گرفت، با توجه به تفاوت بستر ارتکاب جرایم سایبری با جرایم دیگر، تدابیر فنی و محدودکننده، بیشترین بازدهی را در این زمینه خواهد داشت.[۲۹]

دیوارهای آتشین، یکی از کارآمدترین راهکارهای حفاظت و امنیت شبکه و سامانه‌های رایانه‌ای در مقابل حملات سایبری است.[۳۰]

---

27. Situational prevention

28. Colarik, A. M., *Cyber Terrorism Political and Economic Implication*, Massachusetts, United States: Idea Group Pub, 2006, p. 172.

۲۹. موسوی، سیدرضا؛ پیشگیری وضعی از جرایم سایبری در قالب تدابیر فنی و محدودیت‌های پیش روی آن، همایش منطقه‌ای چالش‌های جرایم رایانه‌ای در عصر امروز، انجمن‌های علمی، ادبی و هنری دانشگاه آزاد اسلامی واحد مراغه، ۱۳۹۰، صص ۹-۱.

۳۰. دیوار آتشین در اصطلاح علوم رایانه‌ای عبارت است از:

یک سامانه ایمنی برای محافظت از شبکه یک سازمان در مقابل تهدیدهای خارجی همچون نفوذگران که از شبکه‌های خارجی همچون اینترنت وارد می‌شوند. دیوار آتش که به‌طور معمول، ترکیبی از سخت‌افزار و نرم‌افزار است، از ارتباط مستقیم کامپیوترهای عضو شبکه داخلی یا شبکه‌های خارجی و برعکس جلوگیری می‌کند. مهسا ماه‌پیشانیان؛ «فضای سایبر و شیوه‌های نوین درگیری ایالات متحده امریکا با جمهوری اسلامی ایران»، *نامه پژوهش فرهنگی*، سال دوازدهم، شماره ۱۳، بهار ۱۳۹۰.

۲. پیشگیری از بزه‌دیدگان تروریسم سایبری در اسناد بین‌المللی

۲ـ۱. اقدامات پیشگیرانه کیفری در اسناد بین‌المللی و منطقه‌ای

الف. کنوانسیون راجع به جلوگیری از اعمال غیرقانونی علیه امنیت هواپیمایی کشوری[۳۱]

کنوانسیون راجع به جلوگیری از اعمال غیرقانونی علیه امنیت هواپیمایی کشوری، یکی از تلاش‌های مجمع عمومی سازمان ملل متحد در مبارزه با اعمال تروریستی است که در ۲۳ سپتامبر ۱۹۷۱ در *شیکاگو* تصویب شد.[۳۲] در مقدمه این کنوانسیون، در خصوص به‌مخاطره‌افتادن امنیت افراد، اموال و بهره‌برداری از خدمات هوایی از طریق اعمال غیرقانونی ابراز نگرانی شده است. در زمینه تطبیق این کنوانسیون با اعمال تروریستی سایبری می‌توان به مقرره عامی اشاره کرد که با ذکر دو عنوان «خشونت» و «خسارات جدّی»، به ارتکاب جرایم خشونت‌بار به هر وسیله‌ای علیه تأسیسات هواپیمایی پرداخته است.[۳۳] در جای دیگر، این کنوانسیون، شروع به جرم اعمال مذکور در ماده ۱ و شرکت در انجام افعال غیرقانونی مندرج در این کنوانسیون را جرم و دولت‌های عضو را برای جلوگیری از وقوع چنین اعمالی، به اتخاذ تدابیر سریعی به منظور مجازات آن‌ها ملزم می‌کند.[۳۴] در خصوص مجازات مرتکبین جرایم این کنوانسیون نیز دولت‌ها متعهد به اعمال کیفرهای شدیدی در جرایم مندرج در ماده ۱ شده‌اند.[۳۵] صلاحیت کیفری در ماده ۵ این کنوانسیون ذکر شده و دولت‌ها به اتخاذ تدابیر لازم به منظور اعمال صلاحیت خود ملزم شده‌اند. بعد از اشاره به صلاحیت کیفری، به توقیف، تعقیب کیفری و اقدامات مربوطه توسط دولت‌ها و اقدامات مقتضی برای انجام این امور اشاره شده است.[۳۶] استرداد مجرمین که یکی از چالش‌برانگیزترین مسائل در حقوق بین‌الملل است، در مقررات این کنوانسیون گنجانده شده و دولت‌ها را به انعقاد معاهدات استرداد، تشویق کرده و بیان می‌دارد که دولت‌ها جرایم مندرج در این کنوانسیون را ازجمله جرایم قابل استرداد در دولت‌های عضو قلمداد کنند.[۳۷]

با توجه به اینکه تروریسم سایبری می‌تواند از سرتاسر جهان به‌وسیله رایانه ارتکاب یابد، معاضدت‌های قضایی، مهم‌ترین عامل در تعقیب مؤثر و به‌محاکمه‌کشاندن افراد بزهکار است

31. Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation

32. United Nations, 1971: 12325.

۳۳. بخش ۱ از ماده ۱ کنوانسیون راجع به جلوگیری از اعمال غیرقانونی علیه امنیت هواپیمایی کشوری، مصوب ۱۹۷۱.

۳۴. *همان*، بند دو از ماده ۱.

۳۵. *همان*، ماده ۳.

۳۶. *همان*، ماده ۶.

۳۷. *همان*، ماده ۸.

که مقررات منسجمی در این خصوص وجود ندارد. بزهکارانی مانند تروریست‌های سایبری که از نبوغ زیادی برخوردارند، قادر خواهند بود در کوتاه‌ترین زمان، رد پای خود را محو کنند که این عامل، منجر به شکست یا طولانی‌ترشدن پیگردهای قضایی خواهد شد. بنابراین معاضدت‌های قضایی که به شکل سریع انجام شود، برای پیگیری مجرمان بین‌المللی ضرورتی آشکار است.[۳۸]

ب. کنوانسیون جلوگیری از بمب‌گذاری تروریستی[۳۹]

این کنوانسیون ثمره یکی از تلاش‌های مجمع عمومی سازمان ملل متحد در مقابله با تروریسم و حفظ صلح و امنیت بین‌المللی و در راستای ارتقای سطح حسن هم‌جواری و روابط دوستانه و همکاری بین کشورها در ۱۵ دسامبر سال ۱۹۹۷ تصویب شد.[۴۰] کنوانسیون مذکور در تعریف ارکان تشکیل‌دهنده اعمال تروریستی در این سند، به مواد منفجره دیگر یا ابزار انفجاری مهلک در ارتکاب جرایم تروریستی اشاره کرده است. کنوانسیون در تعریف وسیله منفجره یا دیگر وسائل کشنده، سه معیار یا ویژگی را در نظر گرفته است. بر اساس تعریف کنوانسیون، وسیله منفجره یا وسائل کشنده دیگر باید دارای سه ویژگی ایجاد مرگ، آسیب جانی یا جسمی شدید و نهایتاً واردآوردن خسارت مادی اساسی باشد. سلاح‌ها و وسائلی که دارای ویژگی‌های فوق باشند مشمول تعریف کنوانسیون قرار می‌گیرند. کنوانسیون در ادامه (قسمت ب بند ۳ ماده ۱) به مصادیق معمولی سلاح‌ها یا وسائلی که دارای چنان ماهیت و ویژگی هستند اشاره می‌کند و توضیح می‌دهد که سلاح‌ها و وسائلی که مواد شیمیایی سمّی، مواد بیولوژیکی یا رادیو اکتیویته و هسته‌ای منتشر و پخش می‌کند، ازجمله سلاح‌ها و وسائلی هستند که سه ویژگی فوق را دارند. با عطف به تعریف مذکور باید گفت که از نظر کنوانسیون، تحویل، جاسازی، شلیک و انفجار غیرقانونی با سلاح‌های شیمیایی بیولوژیکی و هسته‌ای و هر نوع وسیله یا سلاح دیگری که موجب مرگ، آسیب جسمی شدید یا خسارت مادی اساسی می‌شود، در اماکن عمومی تأسیسات دولتی و زیربنایی و سامانه حمل‌ونقل عمومی، جرم بین‌المللی و متضمّن تروریسم است. نکته‌ای که در اینجا باید اضافه کرد این است که کنوانسیون، شروع به ارتکاب جرایم فوق را نیز جرم

---

۳۸. بند ۱ از ماده ۱۱ کنوانسیون راجع به جلوگیری از اعمال غیرقانونی علیه امنیت هواپیمایی کشوری، مصوب ۱۹۷۱.
در ادامه همین کنوانسیون در رابطه با همکاری‌های قضایی بیان می‌دارد:
«مقررات بند ۱ این ماده در تعهدات ناشی از سایر معاهدات دو یا چندجانبه فعلی یا آتی که کلاً یا بعضاً ناظر به همکاری‌های قضایی باشد مؤثر نخواهد بود». بند ۲ از ماده ۱۱ کنوانسیون راجع به جلوگیری از اعمال غیرقانونی علیه امنیت هواپیمایی کشوری، مصوب ۱۹۷۱.

39. International Convention for the Suppression of Terrorist Bombings

۴۰. هاشمی، سیدحسین؛ *تروریسم از منظر حقوق اسلام و اسناد بین‌المللی*، پژوهشگاه حوزه و دانشگاه، قم، ۱۳۹۰ ص ۲۵.

تلقی کرده و مستلزم مجازات مقتضی از جانب دولت‌های عضو دانسته است.

این کنوانسیون، صریحاً بر وجود عنصر روانی یا معنوی را در ارتکاب عمل مجرمانه و متضمن تروریسم، تأکید و در بند ۱ ماده ۲ اشاره کرده است که شخص در صورتی مرتکب جرم می‌شود که اولاً، در انجام عمل مجرمانه دارای قصد باشد. ثانیاً، قصد و نیت او ایجاد مرگ، آسیب جسمی شدید یا نابودی گسترده و واردآمدن خسارت اقتصادی وسیع به اماکن عمومی تأسیسات دولتی و زیربنایی و سیستم حمل‌ونقل عمومی باشد. به‌طوری‌که پیداست، کنوانسیون وجود سوءنیت عام (قصد فعل) و سوءنیت خاص (قصد نتیجه) در شخص مرتکب عمل مجرمانه را لازم دانسته است. بنابراین عنصر معنوی جرایم مقررشده در کنوانسیون، زمانی تحقق خواهد یافت که اولاً، شخص در انجام عمل خود، قصد و اراده داشته باشد. ثانیاً، قصد او از انجام اعمال مجرمانه، ایجاد مرگ یا آسیب جسمی شدید یا واردآمدن خسارت اقتصادی باشد.[۴۱]

نکته‌ای که باید در اینجا توضیح داده شود این است که اعمال مجرمانه شامل اشخاص نظامی در جریان مخاصمات مسلّحانه نمی‌شود. به عبارت دیگر اگر یک نظامی در جریان جنگ یا درگیری‌های مسلّحانه، مرتکب یکی از اعمال مجرمانه مقرر در ماده ۲ بشود مشمول مقررات کنوانسیون مورد بحث نخواهد بود.

ج. کنوانسیون سرکوب حمایت مالی از تروریسم[۴۲]

کنوانسیون مذکور، یکی از قطعنامه‌های معروف (۱۳۷۳) در زمینه منع حمایت مالی از تروریسم است که در ۹ دسامبر ۱۹۹۹ در مجمع عمومی سازمان ملل متحد تصویب شد.[۴۳] در این کنوانسیون سه دسته عمده از اعمالی که حمایت مالی از اعمال تروریستی محسوب می‌شوند عبارت‌اند از: جرم‌انگاری تأمین مالی تروریسم در قوانین جزایی در مواد ۲ و ۳، همکاری گسترده با سایر کشورهای عضو و ارائه معاضدت‌های قضایی در موضوعات مرتبط با کنوانسیون در مواد ۱۲ الی ۱۵، اتخاذ اقدامات پیشگیرانه در ماده ۱۸، مسئولیت اشخاص حقوقی در ارتکاب اعمال غیرقانونی در کنوانسیون در ارتباط با تأمین مالی تروریسم در ماده ۵. این موارد از عمده مقررات الزام‌آور در این کنوانسیون راجع به مبارزه با تأمین مالی تروریسم است.[۴۴]

---

۴۱. نمامیان، پیمان؛ «مواجهه با تروریسم سایبری در حقوق بین‌الملل کیفری»، *فصلنامه حقوق ارتباطی*، سال بیستم، شماره ۱، بهار ۱۳۹۲، ص ۱۸.

42. International Convention for the Suppression of the Financing of Terrorism

۴۳. طیبی‌فرد، امیرحسین؛ «مبارزه با تأمین مالی تروریسم در اسناد بین‌المللی»، *مجله حقوقی*، نشریه دفتر خدمات حقوقی بین‌المللی، شماره ۳۲، بهار- تابستان ۱۳۸۴.

۴۴. *پیشین*، صص ۲۶۸-۲۶۷.

کنوانسیون بین‌المللی جلوگیری از تأمین مالی تروریسم، بسته‌ای از مقررات الزام‌آور برای دولت‌های عضو جامعه بین‌المللی در مبارزه با تروریسم است که این هنجارها یا در قالب قواعد عرفی از شفافیت و صراحت کافی برخوردار نیستند و این کنوانسیون در تلاش برای ارائه چارچوبی صریح‌تر و شفاف‌تر در مورد تعهدات دولت‌ها در این زمینه است یا این کنوانسیون دارای آن دسته از قواعدی است که قبل از این، از طریق ابزاری در حقوق بین‌الملل بیان شده بود که برای دولت‌ها به لحاظ حقوقی اجبار کافی ایجاد نمی‌کرد. در برداشت کلّی، کنوانسیون بین‌المللی مقابله با تأمین مالی تروریسم تلاش می‌کند هفت محور اساسی را در قوانین داخلی کشورها لحاظ کند: جرم‌انگاری تأمین مالی تروریسم، اعمال صلاحیت قضایی نسبت به متهمان ارتکاب این جرایم، توقیف و ضبط اموال مجرمان، استرداد و محاکمه مجرمان، معاضدت قضایی و تبادل اطلاعات و مدارک، اقدامات پیشگیرانه و نظام‌های پرداخت جایگزین. با توجه به آنچه گفته شد، معاهداتی نظیر کنوانسیون بین‌المللی مقابله با تأمین مالی تروریسم، علاوه بر اینکه تعهداتی را بر دوش دولت‌ها در عرصه روابط بین‌المللی ایجاد می‌کند، خط‌مشی و جهت کلّی قوانین داخلی در برخورد با جرایم تروریستی را تعیین می‌کند که عموماً از مجرای قوانین و رویه‌های اداری داخل کشورها اجرا می‌شود.[۴۵]

علاوه بر کنوانسیون ۱۹۹۹، قطعنامه شماره ۱۳۷۳ شورای امنیت سازمان ملل متحد به‌طور خلاصه در دو محور کلّی، به موضوع حمایت مالی از تروریسم توجه کرده است. محور اول، ایجاد هنجارهای بین‌المللی مبارزه با تأمین مالی تروریسم است که شامل جرم‌انگاری تأمین مالی اقدامات تروریستی در ردیف‌های (الف) و (ب) بند ۱ قطعنامه و مکلف‌کردن دولت‌ها به منظور تلاش برای پیشگیری و مقابله با تأمین مالی تروریسم در قالب فعالیت‌های مختلف در ردیف (ث) بند ۲ است.[۴۶] شورای امنیت در این قطعنامه، اقدامات تروریستی را بار دیگر مجرمانه قلمداد کرد و جرم‌انگاری آن را در بین قوانین داخلی کشورها به‌عنوان تعهدی سازمانی بر تمامی دولت‌های جهان، تکلیف و تحمیل می‌کند. در مجموع، از مفاد این کنوانسیون، چهار موضوع اساسی استناد می‌شود که عبارت‌اند از: الزام دولت‌ها به همکاری و معاضدت با یکدیگر به منظور سرکوب تروریسم، مقابله با تأمین مالی تروریسم، عدم پشتیبانی مستقیم و غیرمستقیم از تروریسم، جرم‌انگاری و تعقیب کیفری تروریسم، از عمده نکاتی است که در این قطعنامه بر آن تأکید شده است.[۴۷] علاوه بر موارد فوق، این قطعنامه از دولت‌ها

45. Dandurand, Yvon, "Links between Terrorism and Other Forms of Crimes", *International Center for Criminal Law Reform and Criminal Justice Policy*, 2005, pp. 587-596.

۴۶. شمس ناتری، ابراهیم و داود اسلامی؛ «ماهیت کیفری تأمین مالی تروریسم»، *مطالعات حقوق کیفری و جرم‌شناسی*، شماره ۵ و ۶ پاییز و زمستان ۱۳۹۴، ص ۲۷۶.

47. See: SC/Res/1373, 2001.

می‌خواهد راه‌هایی را برای تشدید و تسریع مبادله اطلاعات در مواردی از قبیل استفاده گروه‌های تروریستی از فناوری‌های مخابراتی اتخاذ کنند.[۴۸] قطعنامه ۱۳۷۳ شورای امنیت دارای وصف شبه قانونگذاری نیز هست.

د. کنوانسیون توکیو راجع به جرایم و برخی از اعمال ارتکابی دیگر در هواپیما[۴۹]

این کنوانسیون شامل هفت فصل و ۲۶ ماده است، شامل جرایم موضوع قوانین جزایی، اعمالی که متضمّن ارتکاب جرم بوده یا نباشد ولی سلامت هواپیما و سرنشینان و محمولات آن را به مخاطره اندازد یا سبب اختلال نظم و آرامش داخلی هواپیما شود (ماده ۱ کنوانسیون توکیو راجع به جرایم و برخی از اعمال ارتکابی دیگر در هواپیما، مصوب ۱۹۶۳). این اولین سند چندجانبه حقوقی بود که به معضل رو به رشد هواپیماربایی پرداخت. این کنواسیون، تعریف یا فهرست خاصی از اعمالی را که باید سرکوب شوند ارائه نمی‌کند اما ماده ۱۱ آن به نوع خاصی از تروریسم یعنی راهزنی هوایی پرداخته است. این سند بین‌المللی، همانند کنوانسیون *پالرمو*، با قید اعمال ارتکابی که امنیت هواپیما را به مخاطره می‌اندازد، از تأسیسات هواپیمایی که ممکن است مورد حمله تروریست‌های سایبری قرار گیرند، حمایت کیفری کرده و با جرم‌انگاری اعمالی که منجر به مخاطره‌افتادن سلامت هواپیما و غیره می‌شود، به پیشگیری کیفری نسبت به وقوع چنین اعمالی از هر طریقی اقدام کرده است. با توجه به اینکه هواپیما به سامانه‌های مخابراتی وابستگی شدیدی دارد، با اختلال در دستگاه‌های هدایتی و کنترلی آن به‌وسیله تروریست‌های سایبری و از طریق رایانه یا دیگر دستگاه‌های مخابراتی می‌توانند نسبت به تخریب یا اختلال داده‌ها یا تأسیسات هواپیما اقدام کنند. بنابراین در صورت وقوع حملات تروریستی سایبری علیه این تأسیسات، بر اساس این کنوانسیون، مرتکب یا مرتکبان به استناد مقررات این سند، مجازات خواهند شد. فصل دوم این کنوانسیون نیز به صلاحیت کیفری اختصاص یافته و مواد ۳ و ۴ به قواعد مختلف درباره اعمال صلاحیت دولت‌ها در خصوص ارتکاب جرم اشاره دارد.[۵۰]

هـ. اعلامیه راجع به اقدامات ناظر به امحای تروریسم بین‌المللی

این اعلامیه که در سال ۱۹۹۴ صادر شد، بار دیگر در سال ۱۹۹۵، همراه با قطعنامه ۵۰/۵۳ مورد تأیید مجدد مجمع عمومی سازمان ملل قرار گرفت. در این اعلامیه، مجمع عمومی، به اهمیت

۴۸. بند ۳ اجرایی قطعنامه ۱۳۷۳ شورای امنیت، مصوب سال ۲۰۰۱.

49. Convention on Offences and Certain Other Acts Committed on Board Aircraft

50. 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.

اقدام همه‌جانبه در خصوص ازبین‌بردن و مبارزه با تمام اشکال تروریسم توجه کرده است. اقدامات پیشگیرانه کیفری یکی از موارد مشمول این اعلامیه خواهد بود و با استناد به این اقدامات می‌توان مفاد این سند را به پیشگیری از تروریسم سایبری توسعه داد.[۵۱]

ضمیمه این قطعنامه، اعلامیه‌ای راجع به تکمیل اعلامیه ۱۹۹۴ درباره امحای تروریسم بین‌المللی بود و این امر را از نو تأیید کرد که دولت‌ها قبل از اعطای وضعیت پناهندگی باید اقداماتی مناسب انجام دهند تا اطمینان حاصل کنند که یک پناهجو در اقدامات تروریستی مشارکت نداشته باشد و بعد از اعطای وضعیت پناهندگی نیز تضمین کنند که چنین وضعیتی به منظور زمینه‌سازی یا سازماندهی اقداماتی تروریستی علیه دولت‌های دیگر یا شهروندان آن‌ها استفاده نمی‌شود. این اعلامیه تأکید می‌کند که پناهجویانی که منتظر رسیدگی به درخواست‌های خود هستند از تعقیب به علت اقدامات تروریستی معاف نیستند. این اعلامیه دوباره بر اهمیت کاری مؤثر میان دولت‌ها تأکید می‌کند تا از این طریق، افرادی که در اقدامات تروریستی مشارکت کرده‌اند ازجمله کسانی که آن‌ها را از نظر مالی تأمین، برای آن‌ها برنامه‌ریزی و آن‌ها را ترغیب کرده‌اند محاکمه شوند.

و. کنوانسیون اروپایی مقابله با تروریسم[۵۲]

اتحادیه اروپا در حوزه‌های متنوعی از امنیت فضای سایبر فعالیت کرده است. اتحادیه کشورهای اروپایی، سیاست‌های متعددی را در خصوص حملات علیه شبکه‌های رایانه‌ای، انتشار ویروس‌ها، کرم‌های رایانه‌ای، تروجان‌ها، هرزنامه‌های اینترنتی، حملات فیشینگ و سرقت هویت صادر کرده است. با توجه به اینکه موارد فوق، به‌طور غالب در تروریسم سایبری به کار می‌رود، می‌توان نتیجه گرفت که اتحادیه اروپا یکی از مهم‌ترین سازمان‌هایی است که به منظور پیشگیری از تروریسم سایبری گام برداشته است. این اتحادیه در سال ۲۰۰۴ به منظور اطمینان از امنیت اطلاعات و شبکه در جامعه اروپا، «آژانس امنیت اطلاعات و شبکه اروپا»[۵۳] را تأسیس کرد. هدف از تأسیس این آژانس، کمک به تقویت و توسعه فرهنگ امنیت اطلاعات و شبکه برای حفاظت از منافع شهروندان، مشتریان، سرمایه‌گذاران و سازمان‌های عهده‌دار امور اجرایی کشور در اتحادیه اروپاست.[۵۴]

51. Follmar Otto, Petra and Rabe, Heike, *Human Trafficking in Germany*, Berlin: German Institute for Human Rights Pub, 2009, p. 95.

52. European Convention on Fighting Terrorism

53. European Network and Information Security Agency (ENISA)

54. http://www.enisa.europa.eu/about-enisa,retrieved at:3/10/2017.

معاهده *لیسبون* که معاهده اصلاحات نیز نامیده می‌شود و از دسامبر ۲۰۰۹ لازم‌الاجرا شده، برای نخستین بار، وظایف و حوزه فعالیت ثابت و مشخص را در زمینه جرایم رایانه‌ای برای اتحادیه اروپا تعریف کرد. در بند ۱ ماده ۸۳، جرم رایانه‌ای به‌طور مشخص به‌عنوان یکی از حوزه‌های مرتبط جرم ذکر شده است. از آنجا که جرم سایبری گسترده‌تر از جرم رایانه‌ای است، این تفاوت به اتحادیه اروپا اجازه می‌دهد تا به قاعده‌مندسازی هر دو حوزه بپردازد.[۵۵] در پایان دوره برنامه *استکهلم* در سال ۲۰۱۴، از راهبرد امنیت سایبری اتحادیه اروپا[۵۶] رونمایی شد. ازجمله اهداف این راهبرد، اجرایی‌کردن یک دوره دوساله قانونگذاری در اتحادیه اروپا در زمینه‌های امنیت و جرایم سایبری بود. در همین راستا کارگروهی تحت عنوان «کارگروه مشترک امنیت و جرایم سایبری اتحادیه اروپا ـ ایالات متحده»[۵۷] به منظور پیگیری قاعده‌مندسازی جرایم سایبری درون اتحادیه تشکیل شد.[۵۸] در سال ۲۰۰۱ کمیسیون اروپا توصیه‌نامه‌ای با عنوان «ایجاد جامعه اطلاعاتی ایمن‌تر از طریق بهبود امنیت زیرساخت‌های اطلاعاتی و مبارزه با جرایم مرتبط با رایانه»[۵۹] صادر کرد که در آن مشکلات ناشی از جرایم سایبری را تجزیه و تحلیل و به لزوم انجام اقدامات مؤثر برای مقابله با تهدیدات نسبت به صحت، دسترسی و قابلیت اعتماد سامانه‌ها و شبکه‌های اطلاعاتی اشاره کرد.[۶۰]

ز. کنوانسیون سازمان همکاری‌های منطقه‌ای آسیای جنوبی[۶۱]

کنوانسیون منطقه‌ای سازمان همکاری‌های منطقه‌ای آسیای جنوبی در مورد پیشگیری از تروریسم، یکی دیگر از تلاش‌های منطقه‌ای کشورهای جهان در مبارزه با تروریسم است که هفت عضو این سازمان، یعنی بنگلادش، بوتان، هند، مالدیو، نپال، پاکستان و سریلانکا با جهت‌گیری مقابله با رشد روزافزون جرایم تروریستی و الگوگرفتن از کنوانسیون‌های بین‌المللی در مقابله با تروریسم، آن را در تاریخ چهار نوامبر ۱۹۸۷ در *کاتماندو* تصویب کردند. بر اساس مقررات این کنوانسیون، جرایم زیر، جرم سیاسی تلقی نخواهند شد؛ بنابراین باید به استرداد

55. *Ibid.*, p. 69.

56. EU Cyber Security Strategy: An Open, Safe and Secure Cyberspace 2013.

57. EU-US Cybercrime and Cyber Security Working Group (WGCC)

58. Elain, Fahey, "The EU Cybercrime & Cyber – Security Rule-Making: Maping the Internal & External Dimensions of EU Security", University of Amesterdam, *Forthcoming European Journal of Risk Resoloution*, vol. 1, 2014, p. 2.

59. Communication from the Commision to the Council, The European Parliament, The Economic & Social Committee & The Committee of Regions, 2001.

۶۰. پورنقدی، بهزاد و ارشد بختیاری؛ «تروریسم سایبری و اهمیت آن در برهم‌زدن امنیت بین‌المللی»، *مطالعات بین‌المللی پلیس*، دوره چهارم، شماره ۱۴، تابستان ۱۳۹۲، ص ۴۲.

61. Convention of the Organization of Regional Co-operation of South-Asia

مرتکبان جرایم ذیل اقدام شود:

۱. جرایم مذکور در محدوده کنوانسیون مقابله با تصرف غیرقانونی هواپیما، مصوب ۱۹۷۰ *لاهه*.

۲. جرایم مذکور در محدوده کنوانسیون مقابله با اقدامات غیرقانونی علیه امنیت هواپیمایی کشوری مصوب ۱۹۷۱ *مونترال*.

۳. جرایم مذکور در محدوده کنوانسیون پیشگیری و مجازات علیه اشخاص مورد حمایت بین‌المللی ازجمله مأمورین دیپلماتیک مصوب ۱۹۷۳ *نیویورک*.

۴. وقوع جرایم مذکور در محدوده هر کنوانسیون ضدتروریستی که دولت‌های عضو «سارک» با آن ارتباط دارند و عضو آن هستند، اعضا توافق کنند که مجریان را تعقیب و استرداد کنند.

۵. قتل (عمد و غیرعمد)، حمله و ضرب و شتمی که منجر به آسیب شدید جسمانی شود، آدم‌ربایی، گروگان‌گیری و جرایمی که مرتبط با تیراندازی، سلاح‌های انفجاری به‌عنوان ابزار، خطرات جدّی برای حیات و دارایی‌های اشخاص ایجاد کند.

۶. تلاش برای توطئه برای ارتکاب هریک از جرایم مذکور در بندهای فوق، از طریق مساعدت و معاونت در جرم.[۶۲]

ح. کنوانسیون سازمان کنفرانس اسلامی در زمینه مبارزه با تروریسم بین‌المللی[۶۳]

سازمان کنفرانس اسلامی، در اسناد متعدد به مقوله تروریسم و مبارزه با آن پرداخته است. شاخص‌ترین سند در رابطه با تروریسم، کنوانسیون سازمان کنفرانس اسلامی برای مبارزه با تروریسم بین‌المللی است که در بیست‌وششمین کنفرانس وزرای امور خارجه کشورهای اسلامی، بر اساس قطعنامه ۵۹/۲۶ در ژوئیه سال ۱۹۹۹ به تصویب اعضا و همچنین در ۱۳۸۰/۳/۲۱ به تصویب مجلس شورای اسلامی رسید.[۶۴] این کنوانسیون چهل‌ودو ماده‌ای، تقریباً به تمام مسائل مرتبط با پدیده تروریسم، تعاریف، نحوه همکاری دولت‌ها و مسائل قضایی مرتبط با جرایم تروریستی می‌پردازد و فضای مناسبی را برای مبارزه با تروریسم و تمایز آن با جنبش‌های استقلال‌طلبی و آزادسازی سرزمین‌های ملی ایجاد کرده است. سازمان کنفرانس اسلامی، تروریسم را عملی می‌داند که «همراه با خشونت یا تهدید به خشونت و با انگیزه‌های سیاسی، مالی، مذهبی، فردی، گروهی در قالب اعمال جنایی (جرایم علیه تمامیت جسمانی، روانی یا

---

۶۲. ماده ۱ کنوانسیون منطقه‌ای سازمان همکاری‌های منطقه‌ای آسیای جنوبی، مصوب ۱۹۸۷.

63. Convention of the Organisation of the Islamic Conference on Combating International Terrorism

۶۴. کدخدایی، عباسعلی و نادر ساعد؛ «تروریسم و مقابله با آن»، *مجمع جهانی صلح جهانی*، ۱۳۹۰، ص ۳۹۵.

امنیت ملی)، با هدف ایجاد ترس در جامعه یا تهدید به ایراد صدمه به مردم یا اموال عمومی یا خصوصی یا امنیت ملی، خواه اقدامات مذکور انجام بشود یا اینکه در حالت تهدید باقی بماند، ارتکاب یابد».[۶۵]

ک. معاهده همکاری میان دولت‌های عضو کشورهای مستقل مشترک‌المنافع در مبارزه با تروریسم

معاهده همکاری میان دولت‌های عضو کشورهای مستقل مشترک‌المنافع در مبارزه با تروریسم، در تاریخ چهار ژوئن ۱۹۹۹ در مینسک روسیه سفید، تدوین و سند آن نیز نزد دبیرخانه کشورهای مشترک‌المنافع تودیع شده است.[۶۶]

دولت‌های عضو با درک خطرات اقدامات تروریستی، به متعهدبودن نسبت به کنوانسیون‌های سازمان ملل متحد تأکید می‌کنند و متعهد می‌شوند که اقدامات لازم را در زمینه همکاری‌های لازم در رابطه با امور کیفری مرتبط با جرایم تروریستی انجام دهند. اقدامات غیرقانونی تروریستی در این کنوانسیون عبارت‌اند از:

۱. خشونت یا تهدید به خشونت علیه اشخاص حقیقی یا حقوقی؛

۲. تخریب یا تهدید به تخریب و واردآوردن خسارت به دارایی سایر اشیای مادی به نحوی که زندگی افراد را به مخاطره اندازد و همچنین پیامدهای ناگواری برای جامعه به دنبال داشته باشد.

۳. به منظور انتقام‌گیری از سیاست‌های دولت، حیات یک دولتمرد یا یک شخصیت سیاسی را تهدید کنند.

۴. عمل منجر به تعرض علیه نماینده یک دولت بیگانه، پرسنل عضو سازمان بین‌المللیِ برخوردار از مصونیت ویژه بین‌المللی شود.

۵. تروریسم تکنولوژیکی، استفاده یا تهدید به استفاده از تسلیحات هسته‌ای، رادیولوژیکی، شیمیایی، بیولوژیکی یا میکروارگانیسم‌های بیماری‌زا، مواد رادیواکتیو یا سایر مواردی که به سلامت افراد، آسیب جدّی وارد می‌کند.[۶۷]

---

۶۵. ماده ۱ کنوانسیون سازمان کنفرانس اسلامی در زمینه مبارزه با تروریسم بین‌المللی، مصوب ۱۹۹۹.

۶۶. کدخدایی و ساعد؛ *همان*، ص ۳۹۰.

۶۷. ماده ۱ کنوانسیون همکاری میان دولت‌های عضو کشورهای مستقل مشترک‌المنافع در مبارزه یا تروریسم، مصوب ۱۹۹۹.

ل. کنوانسیون سازمان وحدت افریقا درباره پیشگیری و مبارزه با تروریسم و پروتکل سال ۲۰۰۴ الحاقی به آن

کنوانسیون سازمان وحدت افریقا درباره پیشگیری و مبارزه با تروریسم، در تاریخ ۱۴ ژانویه سال ۱۹۹۹ از سوی سازمان وحدت افریقایی (OAU) تصویب و سند آن نزد دبیرکل این سازمان تودیع شده است.[۶۸] مقدمه این کنوانسیون به مسائل مختلفی ازجمله اشکال مختلف تروریسم و انگیزه‌های مرتکبان اشاره کرده و در ادامه به قطعنامه ۴۹/۶۰ مجمع عمومی مصوب ۹ دسامبر ۱۹۹۴ و اعلامیه ضمیمه آن، قطعنامه۵۱/۲۱۰ مجمع عمومی، مصوب ۱۷ دسامبر ۱۹۹۶ پرداخته و نگرانی خود را نسبت به پدیده مجرمانه تروریسم بیان می‌دارد. اقدامات تروریستی مورد اشاره در این کنوانسیون شامل:

۱. اقدام یا تهدید به نقض قوانین کیفری دولت‌های عضو این کنوانسیون؛

۲. اقدامی که منجر به آسیب به حیات، تمامیت جسمانی و آزادی فردی یا گروهی شود یا موجب خسارت به دارایی خصوصی و عمومی افراد، منابع طبیعی، محیط‌زیست، میراث فرهنگی شود یا قصد ارتکاب چنین عملی را داشته باشد.

۳. کسی که ایجاد وحشت کند و حالت ترس یا وحشت را تحریک کند. همچنین کسی که بر روی دولت یا نهاد، جمعیت و گروهی متوسل به اعمال فشار و تهدید شود.

۴. کسی که در خدمات عمومی و خدمات مالی عمومی اختلال ایجاد کند یا وضعیت آشوب در جمعیتی ایجاد کند.

۵. کسی که آشوب و قیام عمومی را در درون خاک دولت عضو این کنوانسیون ایجاد یا اقدام به چنین عملی را تحریک کند.

۶. کسی که اقدام به حمایت مالی، تأمین مالی، مساعدت، تحریک و تشویق، توطئه و سازمان‌دهی و تجهیز اشخاص به قصد ارتکاب هریک از جرایم مذکور در این کنوانسیون کند.[۶۹]

در این کنوانسیون، هم صرف تهدید و ایجاد ترس در افراد جامعه یا گروه و هم اقدامی که منجر به اخلال در ارائه خدمات عمومی و خدمات مالی شود، اقدامی تروریستی معرفی شده است. عمده‌ترین آماجی که تروریست‌های سایبری از آن برای رسیدن به اهداف عمدتاً سیاسی، اقتصادی خود استفاده می‌کنند، تخریب داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی است که از آن‌ها برای اداره امور عمومی کشور استفاده می‌شود. با استناد به برخی از مفاد عام این

۶۸. جلالی فراهانی، *امیرحسین؛ پیشگیری از جرایم رایانه‌ای*، پایان‌نامه کارشناسی ارشد، حقوق جزا و جرم‌شناسی، دانشگاه امام صادق (ع)، ۱۳۸۴، ص ۵۶.

۶۹. بند ۳ ماده ۱ کنوانسیون سازمان وحدت آفریقا درباره پیشگیری و مبارزه با تروریسم، مصوب ۱۹۹۹.

کنوانسیون، اگر فرد یا گروهی دست به تخریب تأسیساتی بزند که منجر به اخلال در ارائه خدمات عمومی، مانند اخلال در خدمات مخابراتی اورژانس یا پلیس شود، تروریسم سایبریِ مشمول مقررات این کنوانسیون خواهد بود.[۷۰]

م. کنوانسیون عربی مقابله با تروریسم[۷۱]

کنوانسیون عربی مقابله با تروریسم، یکی از اسناد منطقه‌ای است که وزیران و دادگستری کشورهای عربی آن را در آوریل ۱۹۹۸ تصویب کردند.[۷۲] در این کنوانسیون، هرگونه جرم یا شروع به جرمی که به قصد اجرای هدف تروریستی در هریک از کشورهای هم‌پیمان یا علیه هریک از اتباع یا مصالح آن دولت‌ها که طبق قوانین داخلی آن‌ها موجب پیگرد یا کیفر باشد، ارتکاب یابد، مشمول عنوان تروریسم دانسته شده است.[۷۳] این سند همانند برخی دیگر از اسناد مبارزه با تروریسم، به مصادیق تروریسم اشاره‌ای نداشته، بلکه مجموعه افعالی را برشمرده که بر اساس مفاد این کنوانسیون، تروریستی محسوب می‌شوند. از عام‌بودن حوزه ارتکاب مفاد این کنوانسیون، این‌چنین استدلال می‌شود که در صورتی که عملی تروریستی از طریق رایانه ارتکاب یابد و منجر به اختلال یا تخریب تأسیسات رایانه‌ای و مخابراتی شود، بر اساس این کنوانسیون قابل پیگرد است؛ هرچند به‌طور صریح به این بزه اشاره نشده است. بنابراین می‌توان گفت که این کنوانسیون نیز از زمره اسنادی است که به پیشگیری کیفری از افعال مرتبط با تروریسم سایبری پرداخته است.[۷۴]

ن. توصیه‌نامه‌ها و کنوانسیون جرایم سایبر شورای اروپا[۷۵]

کنوانسیون جرایم سایبر در سال ۲۰۰۱ در کنفرانس بین‌المللی که با شرکت کشورهای عضو شورای اروپا و چهار کشور دیگر (امریکا، ژاپن، آفریقای جنوبی و کانادا) تشکیل شد، به تصویب رسید و به کامل‌ترین سند بین‌المللی در مورد جرایم رایانه‌ای تبدیل شد. کنوانسیون مذکور، سه تعهد ضروری را بر دولت‌های عضو تحمیل می‌کند که عبارت‌اند از:

---

70. Furnell, S., *Cybercrime: Vandalizing the Information Society*, London, Addison Wesley Pub., 2016, p. 219.

71. Arab Convention on Fighting against Terrorism

۷۲. کیهانلو، فاطمه و وحید رضادوست؛ «حملات سایبری به مثابه توسل به زور در سیاق منشور سازمان ملل متحد»، *فصلنامه تحقیقات حقوقی*، شماره ۶۹، ۱۳۹۳، ص ۳۹۰.

۷۳. ماده ۱ کنوانسیون عربی مقابله با تروریسم، مصوب ۱۹۹۸.

74. Rohas. N., "Cyber Terrorism in the Context of Globalization, II World Congress on Informatics and Law Madrid", retrieved from:www.barzaloo.com, 2012, pp. 255-256.

75. Budapest Convention on Cybercrime or the Budapest Convention

۱ـ «جرم‌انگاری برخی رفتارهای مرتبط با سامانه‌های رایانه‌ای.

۲ـ وضع آیین دادرسی برای تحقیق و تضمین دسترس‌پذیری آن‌ها برای مجریان قانون داخلی برای تحقیق درباره جرایم سایبری.

۳ـ ایجاد نظام همکاری بین‌المللی گسترده».[۷۶]

کنوانسیون جرایم سایبر و پروتکل الحاقی آن، همانند دیگر اسناد بین‌المللی به‌صراحت به پیشگیری از بزه‌دیدگان تروریسم سایبری نپرداخته است و ماهیت و محتوای این کنوانسیون، جرایم عادی رایانه‌ای است و نمی‌تواند الگوی مناسبی برای مبارزه با تروریسم باشد. فصل دوم این کنوانسیون در خصوص مسائل کیفری مربوط به جرایم رایانه‌ای در قالب حقوق جزای ماهوی، حقوق شکلی و صلاحیت پرداخته و به تدابیری که باید در سطح ملی در کشورها اتخاذ شود اشاره کرده است. مواد ۲ الی ۱۳ این کنوانسیون به حقوق جزای ماهوی اختصاص یافته که به دسته‌ای خاص از جرایم شامل افعال تشکیل‌دهنده تروریسم سایبری اشاره کرده که شامل مختل‌کردن داده‌ها، مختل‌کردن سامانه‌ها و سوءاستفاده از دستگاه‌هاست. این فصل از کنوانسیون با هدف ارتقای ابزارهای پیشگیرانه از جرایم مندرج در این سند، در سطح ملی و بین‌المللی تدوین شده است. در خصوص ضمانت اجراها و تدابیر اتخاذشده، این کنوانسیون بیان می‌دارد:

«هریک از اعضا باید به‌گونه‌ای وضع قوانین و سایر تدابیر کند که در صورت لزوم، اطمینان دهد که جرایم مندرج مصوب در مواد ۲ الی ۱۱ مجازات‌های مؤثر، بازدارنده و مناسب، که شامل مجازات‌های سالب آزادی می‌شود، در پی داشته باشند».[۷۷]

س. کنوانسیون سازمان کشورهای امریکایی راجع به پیشگیری و مجازات اعمال تروریستی

کنوانسیون منطقه‌ای سازمان کشورهای امریکایی، در تاریخ ۲ فوریه ۱۹۷۱ توسط ۳۵ عضو این سازمان در *واشنگتن* تصویب شد.[۷۸] بر اساس قواعد این کنوانسیون، دولت‌های متعاهد پذیرفته‌اند که اقدامات مؤثر را بر اساس حقوق داخلی خود در مقابله با تروریسم و به‌کیفررساندن افرادی که دست به اقدامات تروریستی می‌زنند، با همکاری یکدیگر انجام دهند. کنوانسیون مزبور مقرر می‌دارد: «هریک از دولت‌های عضو مکلف است نسبت به جرایمی که به حقوق عامه مردم

76. Pedro García-Teodoro, Jesús E. Díaz-Verdejo, Enrique Vázquez, "Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges", *Computers & Security*, vol. 28, Issues 1–2., 2009, pp. 18-28. DOI:10.1016/j.cose.2008.08.003.

۷۷. ماده ۱۳ کنوانسیون جرایم سایبر و پروتکل الحاقی آن، مصوب ۲۰۰۱.

۷۸. *پیشین*، ص ۵۶.

تعرض می‌کند و خصیصه بین‌المللی داشته باشد و شامل جرایمی از قبیل ناامنی، آدم‌ربایی و قتل بشود، حمایت‌های خود را بر اساس حقوق بین‌المللی از اشخاص بزه‌دیده به عمل آورد».[۷۹] کنوانسیون سازمان کشورهای امریکایی، همانند دیگر اسناد منطقه‌ای یا بین‌المللی، به‌طور صریح و روشن به پیشگیری از جرایم رایانه‌ای، بخصوص تروریسم سایبری اشاره‌ای نکرده است، بلکه با عناوین کلی سعی داشته به جرایمی که منجر به تضییع حقوق عامه مردم می‌شود و بازتاب بین‌المللی داشته باشد توجه کند. بنابراین به نظر می‌رسد جرایمی مانند تروریسم سایبری که اغلب دارای خصیصه فراملی است و منجر به تعرض مستقیم و غیرمستقیم به حقوق شهروندان می‌شود، بر اساس این سند منطقه‌ای قابل پیگرد باشد.[۸۰]

از سایر اسناد مهم بین‌المللی که در این خصوص تدوین شده می‌توان به موارد ذیل اشاره کرد:

قطعنامه ایجاد فرهنگ جهانی امنیت سایبری و تلاش‌های ملی برای حفاظت از زیرساخت‌های اطلاعاتی حساس،[۸۱] قطعنامه ایجاد فرهنگ جهانی در رابطه با امنیت سایبر،[۸۲] قطعنامه مبارزه با سوءاستفاده جنایتکارانه از فناوری اطلاعات،[۸۳] قطعنامه ایجاد فرهنگ جهانی امنیت سایبر و حمایت از زیرساخت‌های اطلاعاتی حساس.[۸۴]

۲ـ۲. اقدامات پیشگیرانه غیرکیفری در اسناد بین‌المللی و منطقه‌ای

الف. توصیه‌نامه‌های نشریه بین‌المللی سیاست جنایی

نشریه بین‌المللی سیاست جنایی، یکی از اقدامات سازمان ملل به منظور نشر و توسعه آگاهی‌های مربوط به امنیت رایانه است. سازمان ملل متحد در سال ۱۹۹۴ در این نشریه به امنیت سامانه‌های رایانه‌ای پرداخته و امنیت این سامانه‌ها را در امنیت سامانه‌های EDP[۸۵] بیان داشته است؛ با این توضیح که امنیت سامانه‌های EDP از هفت مؤلفه اساسی تشکیل شده است که شامل امنیت اداری و سازمانی، امنیت پرسنلی، امنیت فیزیکی، امنیت مخابرات الکترونیکی،

۷۹. ماده ۲ کنوانسیون پیشگیری و سرکوب اعمال تروریستی سازمان کشورهای امریکایی، مصوب ۱۹۷۱.

۸۰. علیزاده، اکبر و مهدی باباپور؛ «تروریسم هسته‌ای و راهکارهای مقابله با آن از منظر حقوق بین‌الملل»، *مطالعه بین‌المللی پلیس*، دوره چهارم، شماره ۱۶، زمستان ۱۳۹۲، ص ۸۵.

81. Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures

82. Creation of a global culture of cybersecurity

83. Combating the criminal misuse of information technologies

84. Creation of a global culture of cybersecurity and the protection of critical information infrastructures

۸۵. EDP عبارت است از: سامانه‌های پردازش داده‌های الکترونیکی در سازمان‌ها.

امنیت سخت‌افزاری و نرم‌افزاری، امنیت عملیاتی و برنامه‌ریزی است.[۸۶]

ب. دستورالعمل و توصیه‌نامه‌های سازمان همکاری و توسعه اقتصادی

کمیته تخصصی این سازمان در سال ۱۹۸۹ اقداماتی را به منظور اتخاذ سیاستی مشترک برای مقابله با جرایم اینترنتی و هماهنگی قوانین کیفری، همچنین حمایت از حقوق فردی و جریان فراملّی داده‌های شخصی شروع کرد. در ژوئیه سال ۲۰۰۲ این سازمان، سند جامع «خط‌مشی‌هایی برای امنیت سامانه‌های اطلاعاتی و شبکه‌ای: به سوی فرهنگ امنیتی»[۸۷] را منتشر کرد. در مورد ایمن‌سازی سامانه‌های اطلاعاتی، این سازمان، شالوده‌ای را پی‌ریزی کرده است که بر اساس آن، کشورها و بخش‌های خصوصی، به‌صورت انفرادی یا هماهنگ با یکدیگر، خواهند توانست چارچوبی برای امنیت سامانه‌های اطلاعاتی به وجود آورند. این چارچوب شامل قوانین، ضوابط رفتاری، تدابیر فنی، تجربیات مدیران و کاربران، آموزش و آگاه‌ساختن مردم می‌شود. دستورالعمل‌های سازمان همکاری و توسعه اقتصادی، بخش‌های عمومی و خصوصی (اشخاص) را مخاطب خود قرار می‌دهد و در تمامی سامانه‌های اطلاعاتی و شبکه‌ای قابل استناد است.[۸۸]

ج. هشتمین نشست سازمان ملل متحد درباره پیشگیری از جرم و اصلاح مجرمین

این قطعنامه، نتیجه تلاش سیزدهمین نشست پیشگیری از جرم و اصلاح مجرمین، درباره جرایم رایانه‌ای بود که با شماره ۴۵/۱۲۱ در ۱۴ دسامبر سال ۱۹۹۸ در مجمع عمومی سازمان ملل پذیرفته شد. مجمع عمومی در این قطعنامه از کشورهای عضو خواسته است که به منظور مبارزه با جرایم رایانه‌ای، مواردی از این قبیل را در دستور کار خود قرار دهند: به‌روزکردن قوانین و دادرسی‌های کیفری ملّی، تقویت و ایجاد سازوکارهای پیشگیرانه و امنیتی برای هرگونه استفاده از رایانه با درنظرگرفتن حریم خصوصی کاربران و آزادی‌های مشروع افراد، افزایش آگاهی عمومی و توجه قانونگذاران و مردم نسبت به جرایم رایانه‌ای و توسل به اقدامات پیشگیرانه، آموزش به دست‌اندرکاران قوه قضاییه در زمینه فرایندهای کیفری مربوط به جرایم رایانه‌ای و اقتصادی، مطالعه و همکاری با سازمان‌های ذی‌نفع در زمینه اخلاق استفاده از رایانه و اقدام به تدوین مواد درسی و آموزشی به منظور ارتقای سطح آگاهی جامعه و همچنین اتخاذ سیاست‌های مربوط به بزه‌دیدگان جرایم رایانه‌ای، بر اساس اعلامیه اصول بنیادین عدالت برای بزه‌دیدگان و

86. 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.
87. Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security
88. Kenneth J. K., and Boulton R. W, *op. cit*., pp. 98-104.

قربانیان سوءاستفاده از قدرت تلاش کنند.[۸۹]

نتیجه

در حقوق کیفری ایران برای جرم‌انگاری تروریسم سایبری و حمایت از بزه‌دیدگان آن، قاعده یا قانونی دیده نمی‌شود و در خصوص پیشگیری از این بزه در مقررات کیفری، مقرره خاصی وجود ندارد بلکه در قوانینی ازجمله قانون جرایم رایانه‌ای بخصوص ماده ۱۱ به‌طور مبهم و عام به بزهی پرداخته که با استفاده از تفسیر موسّع می‌توان به جرم‌انگاری تروریسم سایبری استدلال کرد. همچنین با استناد به برخی قوانین عامی همچون قانون جرایم رایانه‌ای، قانون مجازات اسلامی و سایر قوانین متفرقه می‌توان به مواضع پیشگیرانه حقوق کیفری ایران در زمینه پیشگیری از این بزه و حمایت از بزه‌دیدگان آن اشاره کرد. در خصوص بزه‌دیدگان مورد بحث، این نکته روشن است که بزه‌دیدگان سایبری، یکی از بی‌دفاع‌ترین و بی‌گناه‌ترین اشخاصی هستند که در اثر فرایند بزه‌دیدگی، متحمّل خسارت‌های مادی، عاطفی، اجتماعی و در برخی موارد، پزشکی می‌شوند، اما به دلیل برخی ویژگی‌های فضای سایبر، چالش‌های تعقیب مجرمان و فقدان مقررات کافی، نیازهای آنان بدون جبران می‌ماند. بزه‌دیدگان تروریسم سایبری نیز به نوعی بزه‌دیده سایبری محسوب می‌شوند. بنابراین وضعیت کنونی نیازمند توجه قانونگذاران و سازمان‌های بین‌المللی در جهت حمایت از آنان است. با وجود اهتمام ویژه به موضوع تروریسم در قالب قطعنامه‌ها و اعلامیه‌های الزام‌آور و غیرالزام‌آور در زمینه جرم‌انگاری رفتارهای بزهکارانه تروریستی، سندی بین‌المللی نیز مختص به تروریسم سایبری وجود ندارد و در دیگر اسناد مرتبط با تروریسم، به جرم‌انگاری تروریسم سایبری و حمایت از بزه‌دیدگان آن پرداخته نشده است. لذا در سطح فراملّی اقدامات کافی و شایسته‌ای به منظور پیشگیری از تروریسم سایبری صورت نپذیرفته است. آنچه در اسناد بین‌المللی در رابطه با عنصر قانونی تروریسم سایبری می‌توان یافت، جرایمی است که بیشترین ظهور را در مفهوم تروریسم سایبری دارند و به‌صورت عام و غیرمستقیم به تروریسم سایبری اشاره کرده‌اند. سازمان‌های بین‌المللی که در رأس آنان سازمان ملل متحد وجود دارد و همچنین شورای وزرای اروپا که نقش فزاینده‌ای را در جهت تقویت و گسترش جرم‌انگاری جرایم سایبری در دهه اخیر ایفا کرده‌اند، می‌توانند با استفاده از کمیته‌های تخصصی و استفاده از متخصصان دیگر کشورها که در زمینه تروریسم سایبری و جرم‌انگاری آن پیشتاز بوده‌اند، برای تدوین کنوانسیون‌های الزام‌آور بین‌المللی در خصوص پیشگیری از تروریسم سایبری و حمایت ویژه از بزه‌دیدگان آن اقدام کنند. لذا تأسیس کمیته‌هایی به منظور بررسی تخصصی جنگ‌های الکترونیکی ضروری به نظر می‌رسد. بنابراین شایسته است هم در حقوق

89. UN Resolution, 45/121, 1998.

کیفری ایران و هم در اسناد بین‌المللی، بخصوص سازمان ملل متحد و شورای اروپا اسناد الزام‌آور خاصی در زمینه پیشگیری از تروریسم سایبری تهیه شود و به منظور مقابله هرچه سریع‌تر نسبت به عواقب این بزه به تصویب دولت‌ها برسد.

منابع:

الف. فارسی

ـ کتاب

- اردبیلی، محمدعلی؛ *مفهوم تروریسم، گزیده مقالات همایش تروریسم از دیدگاه اسلام و حقوق بین‌الملل*، مرکز مطالعات توسعه قضایی و دانشکده علوم قضایی و خدمات اداری، ۱۳۸۱.
- باستانی، برومند؛ *جرایم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری*، چاپ سوم، بهنامی، ۱۳۹۰.
- پوربافرانی، حسن؛ *حقوق جزای بین‌الملل*، جنگل، ۱۳۹۶.
- تقی‌زاده انصاری، مصطفی؛ *سازمان جهانی پلیس جهانی اینترپل*، خرسندی، ۱۳۸۸.
- جلالی فراهانی، امیرحسین و رضا باقری اصل؛ *پیشگیری اجتماعی از جرایم سایبری راهکاری اصلی برای نهادینه سازی اخلاق سایبری*، اطلاع‌رسانی و کتابداری«ره‌آورد نور»، شماره ۲۴، ۱۳۸۷.
- جلالی فراهانی، امیرحسین؛ *کنوانسیون جرایم سایبر و پروتکل الحاقی آن (به همراه گزارش‌های توجیهی آن‌ها)*، خرسندی، ۱۳۸۹.
- _____؛ *پیشگیری از جرایم رایانه‌ای*، پایان‌نامه کارشناسی ارشد، حقوق جزا و جرم‌شناسی، دانشگاه امام صادق (ع)، ۱۳۸۴.
- حسن‌بیگی، ابراهیم؛ *حقوق و امنیت در فضای سایبر*، مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران، ۱۳۸۴.
- رحیمی‌نژاد، اسمعیل؛ *جرم‌شناسی*، فروزش، تبریز، ۱۳۸۹.
- روزنهان دیوید.ال و سلیگمن مارتین. ای بی.؛ *روان شناسی نابهنجاری (آسیب‌شناسی روانی)*، ترجمه: سیدمحمدی، یحیی؛ جلد اول، چاپ دوازدهم، ساوالان، ۱۳۸۹.
- زیبر، اولریش، *جرایم رایانه‌ای*، ترجمه: محمد علی نوری و همکاران؛ چاپ دوم، گنج دانش، ۱۳۹۰.
- ساعد، نادر؛ *منابع حقوق مبارزه با تروریسم در ایران*، خرسندی، ۱۳۸۹.
- سلامتی، یعقوب؛ *تروریسم و حقوق بین‌الملل*، هشترود، دانشگاه آزاد اسلامی واحد هشترود، ۱۳۸۷
- شیرزاد، کامران؛ *جرایم رایانه‌ای از منظر حقوق جزای ایران و حقوق بین‌الملل*، بهینه فراگیر، ۱۳۸۸.

- صنوبر، ناصر؛ *اقتصاد تروریسم*، بورس، ۱۳۹۳.
- طیب، علیرضا؛ *تروریسم، تاریخ، جامعه شناسی، گفتمان*، حقوق، چاپ دوم، نی، ۱۳۸۴.
- عالی‌پور، حسن؛ *حقوق کیفری فناوری اطلاعات*، خرسندی، ۱۳۹۰.
- فامیلی زوار جلالی، امیر؛ *مسئولیت بین‌المللی دولت‌ها ناشی از تأمین مالی دهشت‌افکنی با تأکید بر گروه دهشت‌افکن داعش*، پایان‌نامه کارشناسی ارشد حقوق بین‌الملل، دانشگاه تهران، ۱۳۹۴.
- کدخدایی، عباسعلی و نادر ساعد؛ *تروریسم و مقابله با آن*، مجمع جهانی صلح جهانی، ۱۳۹۰.
- کلاریک، اندرو. ام، و یانچوسکی، لخ.؛ *مقدمه‌ای بر جنگ سایبر و تروریسم سایبر*، ترجمه: ابراهیم‌نژاد شلمانی، بوستان حمید، ۱۳۸۹.
- موسوی، سیدرضا؛ *پیشگیری وضعی از جرایم سایبری در قالب تدابیر فنی و محدودیت‌های پیش روی آن*، همایش منطقه‌ای چالش‌های جرایم رایانه‌ای در عصر امروز، انجمن‌های علمی، ادبی و هنری دانشگاه آزاد اسلامی واحد مراغه، ۱۳۹۰.
- ناصری، علی‌اکبر؛ *هندبوک مجموعه قوانین و مقررات فناوری اطلاعات و ارتباطات (ICT)*، خرسندی، ۱۳۸۷.
- نجفی ابرندآبادی، علی‌حسین؛ *مباحثی در علوم جنایی*؛ تقریرات درس جرم‌شناسی مقاطع دکتری و کارشناسی ارشد، نیمسال دوم تحصیلی، دانشگاه شهید بهشتی، مجموعه دو جلدی به کوشش شهرام ابراهیمی، ۱۳۸۳.
- نمامیان، پیمان؛ *واکنش‌های عدالت کیفری به تروریسم*، میزان، ۱۳۹۰.
- هاشمی، سیدحسین؛ *تروریسم از منظر حقوق اسلام و اسناد بین‌المللی*، پژوهشگاه حوزه و دانشگاه، قم، ۱۳۹۰.

ـ مقاله

- الهویی نظری، حمید و امیر فامیل زوار جلالی؛ «مسئولیت بین‌المللی دولت‌های تأمین‌کننده مالی تروریسم»، *مجله مطالعات حقوق عمومی*، شماره ۳، دوره چهل‌وهفتم، پاییز ۱۳۹۶.
- احمری، حسین، غلامرضا کحلکی و حامد رحیم‌پور اصفهانی؛ «تحلیل سازه‌انگارانه تروریسم سایبری و رویکرد نظام حقوقی به آن»، *فصلنامه پژوهش‌های روابط بین‌الملل*، دوره نخست، شماره ۱۹، بهار ۱۳۹۵.
- پورنقدی، بهزاد و ارشد بختیاری؛ «تروریسم سایبری و اهمیت آن در برهم‌زدن امنیت بین‌المللی»، *مطالعات بین‌المللی پلیس*، دوره چهارم، شماره ۱۴، تابستان ۱۳۹۲.

- پلیس فضای تولید و تبادل اطلاعات ناجا؛ «معرفی پلیس فضای تولید و تبادل اطلاعات ناجا (فتا)»، پنجمین نمایشگاه بین‌المللی رسانه‌های دیجیتال. ۱۳۹۱، ۱۲ صفحه. قابل دسترس در: http://www.cyberpolice.ir/publication/7001، بازدید: ۱۳۹۶/۹/۲۲.
- پوربافرانی حسن، علی امیدی و بهروز قلی‌زاده؛ «درآمدی بر یکسان‌انگاری جرم دزدی دریایی با تروریسم»، *مجله مطالعات حقوقی*، شیراز، دوره نهم، شماره ۲، تابستان ۱۳۹۶.
- جلالی فراهانی، امیرحسین و رضا باقری اصل؛ «پیشگیری اجتماعی از جرایم سایبری، راهکاری اصلی برای نهادینه‌سازی اخلاق سایبری»، فصلنامه اطلاع‌رسانی و کتابداری ره‌آورد نور، شماره ۲۴، پیاپی ۴۱، پاییز ۱۳۸۷.
- شمس ناتری، ابراهیم و داود اسلامی؛ «ماهیت کیفری تأمین مالی تروریسم»، *مطالعات حقوق کیفری و جرم‌شناسی*، شماره ۵ و ۶، پاییز- زمستان ۱۳۹۴.
- طیبی‌فرد، امیرحسین؛ «مبارزه با تأمین مالی تروریسم در اسناد بین‌المللی»، *مجله حقوقی*، نشریه دفتر خدمات حقوقی بین‌المللی، شماره ۳۲، بهار- تابستان ۱۳۸۴.
- علیزاده، اکبر و مهدی باباپور؛ «تروریسم هسته‌ای و راهکارهای مقابله با آن از منظر حقوق بین‌الملل»، *مطالعه بین‌المللی پلیس*، دوره چهارم، شماره ۱۶، زمستان ۱۳۹۲.
- کیهانلو، فاطمه و وحید رضادوست؛ «حملات سایبری به مثابه توسل به زور در سیاق منشور سازمان ملل متحد»، *فصلنامه تحقیقات حقوقی*، شماره ۶۹، ۱۳۹۳.
- ماه‌پیشانیان، مهسا؛ «فضای سایبر و شیوه‌های نوین درگیری ایالات متحده امریکا با جمهوری اسلامی ایران»، *نامه پژوهش فرهنگی*، سال دوازدهم، شماره ۱۳، بهار ۱۳۹۰.
- نمامیان، پیمان؛ «مواجهه با تروریسم سایبری در حقوق بین‌الملل کیفری»، *فصلنامه حقوق ارتباطی*، سال بیستم، شماره پیاپی ۱، بهار ۱۳۹۲.

ب. انگلیسی

- Books

- Andrew Lewis. James, *The Cyber War Has Not Begun*, Center for Strategic and International Studies, 1-4. Available at: http://csis.org/files/publication/100311 _TheCyberWarHasNotBegun, 2010.
- Clarke. R., V., *Situational Crime Prevention Successful Case Studies*, Second Edition, London: Harrow and Heston Pub, 1997.
- Gonzalez, Elise, *The Nexus between Human Trafficking and Terrorism, Orgenaized Crime, Combating Human Trafficking by Creating a Cooperative Law Enforcement System*, Student Scholarship Pub, 2013.
- Wouters Jan & Sanderjin Duquet, *The UN, The European Union and Multilateral Actions against Terrorism*, Leuven center for global

Governance studies, working paper, No. 113, 2013.
- Colarik, A. M., *Cyber Terrorism Political and Economic Implication*, Massachusetts, United States: Idea Group Pub, 2006.
- 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.
- Furnell, S., *Cyber Crime: Vandalizing the Information Society*, London, Addison Wesley Pub, 2016.
- Lucas A. and Campbell L., *A Guide for Victims of Crime in Queensland*, Department of Justice and Attorney, General Pub, 2011.
- Scarfone K. and Mall. P, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, NIST Special Publication, vol. 1, 127, 2007.
- Schmid, A. P., and Jongman A. J., *Political Terrorism: A New Guide to Actors, Authors, Concepts, Database, Theories and Leteratare*, New Brunswick: Transaction Books Pub, 2015.
- Shinder, Debra Littlejohn, *Scene of the Cyber Crime, Computer Forensics Handbook*, Synergy Press Publication, 2002.
- Scarfone K. and Mall P., *Guide to Intrusion Detection and Prevention Systems (IDPS)*, NIST Special Publication, vol. 1, 127, 2007.

- Articles
- Cherrif Bassioni, "International Terrorism", *Transnational Journal of China*, 2015.
- Cox, S. J., "Confronting Threat through Unconventional Means: Offensive Information Warefare as a Covert Alterntive to Preemptive War", *Houston Law Review*, vol. 42, No. 3, 2005.
- Dandurand, Yvon, "Links between Terrorism and Other Forms of Crimes", *International Center for Criminal Law Reform and Criminal Justice Policy*, 2005.
- Dunn. Myriam, Mauer, V., (eds.), "International CIIP Handbook", *ETH Zurich: Center for Security Studies*, vol. II, 2006.
- Elain, Fahey, "The EU Cybercrime & Cyber – Security Rule-Making: Maping the Internal & External Dimensions of EU Security", University of Amesterdam, *Forthcoming European Journal of Risk Resoloution*, vol. 1, 2014.
- Janet, J. P., and Laurie E. M., "Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks", *Journal of Information Technology Education*, vol. 3, 2004.
- Julian L. R., "SCADA Intrusion Prevention System", *Journal of Information*, http://perso.telecom-paristech.fr/~legrand/CI2RCO-conf/Article/scada_rrushi, 2006.

- Marin, Floria, "Terrorism Financing Connectors to Organized Crime", *Criminal Law Journal*, 2015.
- Ngo, Fawn T., Paternoster, Raymond., "Cybercrime Victimization: an Examination of Individual and Situational Level Factors", *International Journal of Cyber Criminology*, vol. 5, Issue1, 2011.
- Nicholson A., Webber S., Dyer S., Patel T., Janicke H., "SCADA Security in the Light of Cyber-Warfare", *Computers & Security* 3, 2012.
- Ponemon Institute LLC, "First Annual Cost of Cyber Crime Study Benchmark Study of U.S. Companies", 22. Available at: http://www.hpenterprisesecurity.com/collateral/report/HPEnterpriseSecurity_Report_HPArcSightFirstAnnualCostCyberCrimeStudyPonemon, 2010.
- Rohas N., "Cyber Terrorism in the Context of Globalization, Second World Congress on Informatics and Law Madrid", Spain. pp. 1-26, retrieved from: www.barzaloo.com, 2012.
- Teodoro P. Garcı´a., Verdejo. J. Dı´az., Ferna´ndez. G. Macia., Vazquez. E., "Anomaly-based Network Intrusion Detection: Techniques, Systems and Challenges", *Computers & Security*, vol. 28, Issues 1–2, 2009.
- Thanh Dang, S., "The Prevention of Cyberterrorism and Cyberwar", *ODUMUNC International Security* (DISEC) 2011, Issue Brief for the GA First Committee: Disarmament and International Security (DISEC). retrieved from: http://al.odu.edu.

- Documents

- United Nation Resolutions:45/121:1998.
- United Nation Resolutions:Con.Annex to Res.No. 26/59/P, 1999.
- United Nation Resolutions:SC/1373, 2001.
- United Nation Resolutions:56/121, 2001.
- United Nation Resolutions:56/121, 2002.
- United Nation Resolutions:57/239, 2003.
- United Nation Resolutions:58/199, 2004.
- United Nation Resolutions:58/199, 2004.
- United Nation Resolutions:64/211, 2010.