Journal of Socio-Political Developments in Contemporary Iran

Vol. 3, No. 6, spring 2024

http://doi.org/ 10.30510/pscci.2024.483661.1101

Countries' commitment policies to international cooperation in dealing with cyber terrorism with a view to Iran

Jamal Yousefi[1]

Hasan Motheghi [2*]

Nasser Rahbarfarash Pira [3]

Received:4 December 2023

Reception: 14 February 2023

Abstract

Cyber terrorism, as one of the challenges of the present era, has been introduced as a serious threat to international peace and security in most of the legal documents related to cyber security, and the need to fight against it has been emphasized. Threats caused by terrorist acts are no longer within the framework of a certain territory and have become a global threat. Terrorism targets values that are the foundation of the United Nations Charter, such as: respect for human rights, the rule of law, laws and regulations regarding the protection of civilians in war, tolerance and tolerance between nations and countries, and the peaceful settlement of disputes. The current research, which was carried out with the descriptive-analytical method and the use of library resources, aims to answer the question of what are the international obligations of governments in dealing with cyber terrorism. Based on the findings of the research, it has come to conclusion that the most important commitment reflected in the international anti-terrorism treaties is the criminalization of such acts in the criminal laws and that the member states should include the field of accepting universal jurisdiction in their criminal laws that includes territorial judicial proceedings, proceedings based on the nationality of the criminal and the victim. According to treaties and judgment, it will be based on the defendant's residence and these requirements include the extradition of criminals.

Keywords: commitment, international cooperation, terrorism, cyber terrorism

1 Doctoral student of Law Department, Aras International Branch, Islamic Azad University, Tabriz, Iran.

2Associate Professor of Law Department, Aras International Branch, Islamic Azad University, Tabriz, Iran. (Corresponding author)

3 Assistant Professor, Department of Law, Aras International Branch, Islamic Azad University, Tabriz, Iran

فصلنامه تحولات سیاسی اجتماعی معاصر ایران، سال سوم، شماره اول(پیاپی۶)، بهار۱۴۰۳ صص ۱۰۵-۸۵

http://doi.org/ 10.30510/pscci.2024.483661.1101

سیاست‌های تعهدآمیز کشورها به همکاری بین‌المللی در مقابله با تروریسم سایبری با نگاهی به ایران

جمال یوسفی[۱]

حسن موثقی[۲*]

ناصر رهبرفرش پیرا[۳]

تاریخ دریافت :۱۷ /۱۴۰۲/۰۹

تاریخ پذیرش: ۱۴۰۲/۱۱/۲۱

چکیده:

تروریسم سایبری، به عنوان یکی از چالش‌های عصر حاضر در اغلب اسناد حقوقی مرتبط با امنیت سایبری، به عنوان یک تهدید جدی علیه صلح و امنیت بین‌المللی معرفی و بر لزوم مبارزه با آن تاکید شده است. تهدیدات ناشی از اقدامات تروریستی، دیگر در چارچوب سرزمین معین نمی‌گنجد و به یک تهدید جهانی مبدل گشته است. تروریسم ارزش هایی را هدف قرار می‌دهد که بنیان منشور ملل متحد، از قبیل: احترام به حقوق بشر، حاکمیت قانون، قوانین و مقررات ناظر به حمایت از غیر نظامیان در جنگ، بردباری و تساهل میان ملت‌ها و کشورها، وحل و فصل مسالمت آمیز اختلافات می‌باشند. پژوهش حاضر که با روش توصیفی-تحلیلی و استفاده از منابع و اطلاعات کتابخانه‌ای صورت گرفته است، در صدد پاسخگویی به این سوال است که تعهدات بین‌المللی دولت‌ها در مقابله با تروریسم سایبری چگونه است و براساس یافته‌های تحقیق به این نتیجه رسیده است که به نظر می‌رسد که مهمترین تعهد منعکس در معاهدات بین‌المللی ضد تروریسم، جرم انگاری اینگونه اعمال در قوانین کیفری است و این که دول عضو باید زمینه پذیرش صلاحیت قضایی جهانی را در قوانین کیفری خود بگنجانند که این موضوع شامل رسیدگی قضائی سرزمینی، رسیدگی بر مبنای تابعیت مجرم و قربانی و مطابق معاهدات و قضاوت بر مبنای محل اقامت متهم خواهد بود که این الزامات شامل استرداد مجرمین نیز می‌گردد.

کلیدواژه‌ها: ایران، تروریسم سایبری، تروریسم، تعهد، سیاستگذاری، همکاری بین‌المللی

[۱] دانشجوی دکتری گروه حقوق، واحد بین‌الملل ارس، دانشگاه آزاد اسلامی، تبریز، ایران. jamaluosefi@gmail.com

[۲] دانشیار گروه حقوق، واحد بین‌الملل ارس، دانشگاه آزاد اسلامی، تبریز، ایران. (نویسنده مسئول) movasaghi@iaut.ac.ir

[۳] استادیار گروه حقوق، واحد بین‌الملل ارس، دانشگاه آزاد اسلامی، تبریز، ایران javaid.rahbar.farshpira@gmail.com

مقدمه

تروریسم پدیده تازه‌ای نیست. شاید بتوان گفت که قدمت آن به درازای حیات اجتماعی بشر و همزاد با ظهور مفهوم قدرت است. تروریسم معمولا در فضا و شرایطی رخ می‌دهد که در آن قدرت به صورت نادعادلانه توزیع شده باشد. در این فضا یک طرف، از قدرت سیاسی، اقتصادی یا اجتماعی بیشتری برخوردار است و طرف دیگر برای جبران ضعف خود، به حربه تروریسم متوسل می‌شود. این پدیده در کشورهای استبدادی کاملا محسوس است. در کشورهای دموکراتیک مانند آمریکا، انگلیس، فرانسه و... نیز، گاه تمرکز قدرت در بخش‌ها و گروه‌هایی از جامعه به حدی می‌رسد که گروه‌های ناراضی را وادار می کند تا برای تحقق آرمان‌های خود به تروریسم متوسل شوند. بسیاری از محققان بر این باورند که پدیده تروریسم بین‌الملل ناشی از سرکوب نهضت‌های مشروع و آزادی بخش است.

برخلاف آنچه امروزه به نظر می‌رسد که هیچ عقیده و ایدئولوژی رسمی در توجیه تروریسم وجود نداشته است، واقعیت این است که اندیشمندان و سیاستمدارانی بوده و هستند که تروریسم را یگانه راه پیکار علیه ستمگری، حق‌کشی و غارت‌گری فرمان‌روایان و زورگویان و ایجاد جامعه‌ای آزاد و عادلانه می‌پندارند و هرگونه روش مبارزه اعتدالی یا انقلابی دیگر را نفی می‌کنند. یکی از شیوه‌ای جدید تروریسم، تروریسم سایبری است. تروریسم سایبری قادر است که با وارد کردن آسیب‌های جدی به شبکه اطلاعات رایانه‌ای دولت‌ها ضربات کاری به حاکمیت و استمرار امور روزانه وارد کرده و زندگی را برای شهروندان و دولتمردان تلخ نمایند.

بنابراین تروریسم به اندازه‌ای تهدید کننده صلح و امنیت بین‌المللی می‌باشد و همسان جنگ قلمداد شده و پاسخ‌های مناسب خود را می‌طلبد. از سوی دیگر با ورود فضای مجازی به عرصه حیات بشری، محیط جدیدی برای خودنمایی و حملات تروریستی برای جنایتکاران ضد بشری فراهم آمده که ساختار اطلاعاتی و حیاتی کشورها و ملت‌ها را مخاطب حمالت خود قرار داده و در صدد تخریب کلیه بخش‌های اقتصادی، حمل و نقل، آموزش عالی، مخابرات، شرکت‌های خصوصی و سرقت اموال و دارائی‌ها و جابجایی سپرده‌های بانکی به حساب‌های خود در بانک‌های جزا یار دور افتاده جهان هستند فضای مجازی محیطی است واجد قابلیت و فرصت برای دستیابی به توسعه پایدار و همین طور تهدیداتی که در برخی موارد

منبع تهدید کاملا نا شـــلناخته می‌ملند و قلبل تعقیب، محاکمه و مجازات نیســت به همین جهت اســت که حملات تروریســت‌ها به ویژه تروریســم سـایبری را می‌توان با لحاظ اهداف تخریبی آن، یک جنگ به حسـاب آورد. حقوق بین‌الملل هنوز راجع به تلقی آن به عنوان جنگ، معاهده و مصوبه‌ای ندارد. (قاسمی و باقرزاده، ۱۳۹۴: ۲۴۶).

بنابراین دولت‌ها باید با نظارت مســتمر بر اینترنت و تعاملات مظنونین به تروریسـم سـایبری مانع از استخدام، بکارگیری، تربیت هکر و متوقف کردن حملات تروریســتی در نطفه شــوند ضــمن آنکه باید نســبت به افزایش آگاهی‌های همگانی شـهروندان همه کشـورها اقدام نمایند تا شـهروند در دام عنکبوتی تروریسـت‌ها نیفتند. علاوه از آن رعایت حقوق بشـر باید با لحاظ منافع جمعی توأم گردد کاه در این راسـتا توجه به سـازوکار پیشـگیری، از اهمیت زیادی بر خوردار اســت. بنابراین جرم انگاری جرایم تروریســتی سایبری گام بعدی در پایان دادن به تروریسم سایبری خواهد بود.

از جمله کنوانسـیون‌هایی که در مبارزه با تروریسـم تصـویب شـده اسـت می‌توان به کنوانسـیون مبارزه با تامین مالی تروریسـم (CFT) اشـاره کرد. کنوانسیونی بین‌المللی برای شـناسـایی و جلوگیری از تامین مالی اقدامات و فعالیت‌های تروریستی محسوب می‌شود. نقش اصلی تعیین استانداردهایی برای مقابله با پولشویی و تأمین مالی تروریسم است که سلامت و شفافیت سـیسـتم مالی کشـورها را ارتقا می دهد. با اجرای این اسـتانداردها منبع و مقصد پول‌ها در نظام مالی مشخص می‌شود.

همچنین کنوانسـیون سـازمان ملل متحد برای مبارزه با جرائم سـازمان‌یافته فراملی، در تاریخ ۲۱ دسامبر سال ۲۰۰۱ در شهر پالرمو در ایتالیا به تصویب رسـید و در تاریخ ۲۹ سـپتامبر سـال ۲۰۰۳، برای کشـورهای عضـو سـازمان ملل متحد لازم‌الاجرا شــد و تاکنون ۱۸۰ کشــور آن را پذیرفته‌اند. این کنوانسـیون همان‌طور که از نامش پیداسـت، گامی در جهت مبارزه با جرائم سـازمان‌یافته فراملی و تشـخیص کشـورهای عضـو برای مصـادیق آن برای جدی بودن مشکلات ناشی از جرائم فراملی است، همچنین این کنوانسیون نشــان می‌دهد که نیاز به تقویت همکاری‌های بین‌المللی به منظور مقابله با این مشکلات در بین کشورهای عضو وجود دارد.

کنوانسیون جرایم سایبری معروف به «کنوانسیون جرایم سایبری بوداپست» یا به اختصار «کنوانسیون بوداپست»، نخستین معاهده‌ی بین‌المللی است که به جرایم رایانه‌ای و اینترنتی می‌پردازد و می‌کوشـد قوانین ملی را سـازگار

کرده، روش‌های تحقیقات را ارتقا دهد و همکاری بین کشـــورها را بهبود بخشد.

شـورای امنیت در قطعنامه ۱۳۷۳ از همه کشـورها خواسـت که مانع تامین مـالی اعمـال تروریســـتی شـــده و آن را متوقف کننـد همینطور مـانع از عضـوگیری گروه های تروریستی شـوند و با تبادل اطلاعات به هشـدار اولیه به سایر کشورها اقدام نمایند (Rosand, 2003, P. 335)

همین طور ســازمان ملل متحد از ســال ۱۹۹۴ با هدف افزایش آگاهی‌های جمعی راجع به افزایش امنیت کامپیوترها هفت شـاخصـــه اصـــلی را برای جلوگیری از نفوذ سـایبری برشـمرده که شـامل: امنیت اداری و سـازمانی، امنیت کارمندان، امنیت فیزیکی، امنیت مخابرات الکترونیکی، امنیت سـخت افزاری و نرم افزاری و امنیت عملیاتی و برنامه‌ریزی می‌گردد.

در قطعنامه و اعلامیه‌های متعدد شورای امنیت و مجمع عمومی سازمان ملل متحد و همچنین در کنوانسیون‌های بین‌المللی مقابله با تروریسـم همواره به عنوان «تهدیدی علیه صـلح و امنیت بین‌المللی» و مغایر با اهداف و اصـول منشور ملل متحد دانسته شده است. ورود شورای امنیت سازمان ملل متحد به مقوله مبارزه با تروریسم بین‌الملل، به مسئولیت‌های این رکن سیاسی ملل متحد در حفظ صـلح و امنیت بین‌المللی باز می‌گردد. طبق ماده ۳۹ منشـور، «شورای امنیت وجود هرگونه تهدید علیه صلح، نقض صلح یا عمل تجاوز را احراز و توصیه‌هایی خواهد نمود یا تصـمیم خواهد گرفت که برای حفظ یا اعاده صـلح و امنیت بین‌المللی به چه اقداماتی بر طبق مواد ۴۱ و ۴۲ باید مبادرت شود» بنابراین در صورت احراز هر یک از این سه وضعیت، شورای امنیت مجاز اسـت که از تدابیر اجرایی مسـالمت آمیز (ماده ۴۱) یا اقدامات قهرآمیز (ماده ۴۲)، برای حفظ یا اعاده صـــلح یا توقف تجاوز بهره گیرد. شـورای امنیت در تلاش خود به منظور امحای تروریسـم در قطعنامه ۱۲۶۹ تروریسـم را فارغ از اهدافی که تروریسـت‌ها دنبال می‌کنند محکوم می‌کند. به موجب بند ۵ این قطعنامه تروریســـم تهدیدی علیه صـــلح و امنیت بین‌المللی را بر عهده دارد، برای اجرای این وظیفه، اقدامات ضـروری را بر اساس فصل هفتم منشور جهت محو تروریسم اتخاذ خواهد کرد.

قطعنامه مذکور مبین تغییر مواضـــع شـــورای امنیت و آمادگی آن در اعمال اقدامات قهری و مسـلحانه برای مقابله بامعضـل تروریسـم اسـت که بسـتر مناســـبی را برای اعمال اقدامات قهر آمیزی که شـــورای امنیت به دنبال حمالت تروریسـتی ۱۱ سـپتامبر ۲۰۰۱ اتخاذ نمود، فراهم سـاخت. شـورای

امنیت در واکنش به حمالت تروریستی ۱۱ سپتامبر، قطعنامه‌های ۱۳۶۸ و ۱۳۷۳ را صادر کرد و در مقدمه قطعنامه ۱۳۶۸ اقدامات تروریستی را به عنوان تهدیدی علیه صلح و امنیت بین‌المللی مطرح کرد و طبق منشور ملل متحد حق ذاتی دفاع مشروع فردی یا جمعی را به رسمیت شناخت. شواری امنیت همچنین در قطعنامه ۱۳۷۳ با تاکید مجدد بر قطعنامه‌های ۱۲۶۹ و ۱۳۶۸ بار دیگر حمالت ۱۱ سپتامبر را به عنوان تهدیدی علیه صلح و امنیت بین‌المللی محکوم و حق ذاتی دفاع مشروع فردی یا جمعی طبق منشور ملل متحد را به رسمیت شناخت. در واقع شورای امنیت تلاش نموده است که بین مفهوم حمله تروریستی و حمله مسلحانه مندرج در ماده ۵۱ منشور ارتباط برقرار کند. در این پژوهش به بررسی این سوال می‌پردازیم که تعهدات بین‌المللی دولت‌ها در مقابله با تروریسم سایبری با توجه به رویه سازمان ملل متحد چگونه است، گستره حقوق و تعهدات بین‌المللی دولت‌ها در مقابله با تروریسم سایبری چگونه است و نیزرویه سازمان ملل متحد در خصوص تعهدات بین‌المللی دولت‌ها در مقابله با تروریسم سایبری چگونه است؟

۱-تروریسم سایبری

تروریسم سایبری از همگرایی تروریسم و فضای سایبربه وجود آمده است. به علاوه، برای اینکه یک تهاجم، تروریسم سایبری تلقی شود، باید منجر به اعمال خشونت علیه اشخاص یا اموال گردد یا حداقل آن قدر خسارت وارد آورد که منجر به وحشت گردد. تهاجماتی که باعث فوت، آسیب جسمی، انفجار، تصادم هواپیماها، آلودگی آب یا لطمه شدید علیه زیر ساخت های حیاتی میتواند اقدامات تروریستی سایبری تلقی شود که البته به میزان آثار آنها بستگی دارد. تهاجماتی که خدمات غیر ضروری را قطع یا نهایتا مزاحمت هزینه بری را ایجاد نمی‌کنند، تحت شمول این تعریف قرار نمی‌گیرند (حسینی مهر و مختاری افراکتی، ۱۳۹۵: ۱۱۸).

تروریسم سایبری برگرفته از دو اصطلاح پیشین یعنی تروریسم و سایبر است، و از این رو در طول این دو قرار می گیرد. همه رفتارهایی که در ذیل تروریسم بررسی می شوند، در تروریسم سایبری جای نمی گیرند و اینکه هر چیزی که بر ضدفضای سایبر باشد در اندرون تروریسم سایبری (در معنای عام) بررسی نمی گردد. پس هرچند تروریسم سایبری بر آن است تا چهره تروریسم را از آیینه فضای سایبر ببیند، ولی با بروز برخی شرایط و عوامل تروریسم سایبری در مفهوم و مصداق بسیار چالش برانگیز تر از دو

واژه پیشین است. با آنکه عمر واژه تروریسم سایبری به دو دهه نمی رسد، ولی در همین مدت تعاریف بسیاری از آن ارائه شده است. این عبارت با ترکیب واژه های فضای سایبر و تروریسم در دهه ۱۹۸۰ توسط «بری کلین»[۱] ارشد موسسه حفاظت اطلاعات در کالیفرنیا، ابداع گردید و آن را این گونه تعریف کرد: «سوءاستفاده عمدی از یک سیستم، شبکه یا مولفه اطلاعاتی رایانه‌ای برای تحقق هدفی که موید یا تسهیل کننده مبارزه یا اقدام تروریستی است.» این عبارت پس از پذیرش از سوی نیروهای مسلح ایالات متحده آمریکا بطور گسترده ای مورد قبول واقع شده است (فرمانی، ۱۳۹۰: ۶۵).

به طور کلی می‌توان گفت تروریسم سایبری به معنی حملات از پیش طراحی شده با انگیزه سیاسی است که توسط گروه های تحت حمایت کشورها یا عوامل خرابکار یا اشخاص، علیه سیستم های رایانه ای و اطلاعاتی، برنامه های رایانه ای و داده ها انجام می شود، به نحوی که منجربه خشونت علیه اهداف غیر نظامی می‌شود. لذا در تروریسم سایبری هدف اصولاً غیر دولتی است و ارتکاب آن نیز لزوماً با هدایت دولت نیست. تروریست‌های فضای مجازی یا اینترنتی به جای استفاده از سلاح‌های رایج، بمب‌ها و موشک‌ها یا سایر ابزارهای معمول از نرم افزارهای مخرب رایانه ای برای پیشبرد اهداف خود استفاده می‌کنند. ویروس‌ها، کرم‌ها تروجان‌ها، اسپم‌ها، ایمیل بمبینگ، گوگل بمبینگ، هک و نفوذ رایانه‌ای، بخشی از ابزارهای تروریست‌های مجازی به شمار می‌رود (خلیل زاده، ۱۳۹۳: ۹۸).سازمان ملل متحد، به عنوان بزرگترین سازمان بین المللی، از سال ۱۹۶۳ تا کنون درباره تروریسم و اقدامات تروریستی سن بین‌الملل به تصویب رسانده است و جالب اینکه در سه سند مراحتاً به عنوان تروریسم اشاره شده و تنها مصادیق اقدامات تروریستی بر شمرده شده است این سه سند عبارتند از: (کنوانسیون بین المللی برای جلوگیری از بمب گذاری تروریستی)، (کنوانسیون بین‌المللی برای جلوگیری از تأمین مال تروریسم، کنوانسیون بین‌المللی برای جلوگیری از اقدامات تروریستی هسته‌ای) (میرعباسی و همکاران، ۱۳۹۷: ۲۶۷).

---

[۱] Bery cline

۲-جایگاه تروریسم سایبری در معاهدات بین‌المللی ضد تروریسم

بسیاری از معاهدات بین‌المللی ضدتروریستی که از دهه ۱۹۶۰ میلادی به این طرف تصویب و لازم‌الاجرا شده‌اند، همین الگو را مدنظر خودقرار داده‌اند. به عنوان مثال می‌توان به کنوانسیون لاهه (۱۹۷۰) در خصوص ممنوعیت تصرف غیرقانونی هواپیما، کنوانسیون مونترال (۱۹۷۱) در مورد جلوگیری ار اعمال غیرقانونی علیه امنیت هواپیمایی کشور و همچنین کنوانسیون بین‌المللی ممنوعیت حمایت مالی از تروریسم . در تمام این معاهدات اقدامات مشخصی با عنوان مجرمانه تعریف شده و دول عضو متعهد شدهاند که صلاحیت جهانی خود را در خصوص رسیدگی به جرایم مذکور اعمال داشته و در این راستا به سایر دولتها مساعدت‌های لازم را مبذول دارند.

نکته قابل توجه این است که علیرغم مطرح شدن بحث تروریسم سایبری به صورت جدی و پذیرش آثار بالقوه خطرناک آن، تاکنون در هیچ معاهده بین‌المللی جهانی به صراحت موضوع تروریسم سایبری نیامده است. اما شاید بتوان با استناد به معاهداتی که به طور کلی بحث تروریسم را مدنظر قرار داده و دامنه وسیعی از اقدامات را تحت شمول خود دارند، به تروریسم سایبری رسید. به عنوان مثال اگر حمله سایبری منجر به بروز اختلال در سیستم امنیتی پرواز و ایجاد خطر برای اموال و سرنشینان هواپیما شود به نحوی که هدایت هواپیما را با مشکل مواجه کند، می‌تواند جزء جرایم بیان شده در ماده ۱ کنوانسیون جرایم و دیگر اقدامات ارتکابی در داخل هواپیما باشد (UN General Assembly, 1963)

یا اگر حمله سایبری موجب توقیف غیر قانونی هواپیما یا کنترل غیر مجاز هواپیمای در حال پرواز شود، می‌تواند با استناد به ماده ۱ کنوانسیون ممنوعیت توقیف غیرقانونی هواپیما جرم محسوب شود. همچنین حملات سایبری میتواند منجر به ایراد خسارت و بروز جراحت به اشخاص تحت حمایت بین‌المللی شود. که در این صورت با استناد به بند دوم از بخش اول ماده ۲ از کنوانسیون منع و مجازات جرایم علیه اشخاص مورد حمایت بین‌المللی از جمله نمایندگان دیپلماتیک (۱۹۷۳) جرم محسوب خواهد شد. (UN General Assembly, 1973)

بر این اساس: هر فردی که تعمدا مرتکب حمله خشونت بار علیه نمایندگان دولتی، اموال شخصی یا وسایل حمل و نقل اشخاص تحت

حمایت بین‌المللی شود بـــه نحـــوی که جان یا آزادی این افراد را به خطر بیندازد مجرم محسـوب می‌شـود. از سـوی دیگر ، اگر حملات تروریسـتی موجـــب مداخله در امنیت دریانوردی، امنیت سکوهای نفتی و یا تخریب گسترده اموال و اماکن و سیستم‌های حمل ونقل عمـومی و یا ایراد خسارت به نیروگاه‌های هستهای و آزاد سازی مـواد رادیـو اکتیویتـه شـود .با استناد به کنوانسیون‌های بین‌المللی لازم الاجرا جرم محسوب می‌شود.

با توجه به مطالب مطرح شده می‌توان مدعی شد کـه در فاصـله سـال‌های ۱۹۶۳ تا ۲۰۰۵ میلادی جامعه بین‌المللی مقررات حقوقی لازم الاجرایی در خصوص مبارزه علیه تروریسم که به نوعی قابل بسط به تروریسم سایبری نیز مـــی‌باشد، تـــدوین و تـــصویب نموده است. در حالی‌که در این برهه زمانی هنوز فضای سایبری به عنـوان یک وسـیله ارتباط جمعی و همه گیر شناخته نشده بود (Condron, 2007: 403).

۳-چارچوب نظری

در عرصـــه حقوق کیفری، مفهوم اقدامات تروریســـتی عموما از ســـه معیار شـکل می‌گیرد که علی رغم نسبیت و پویایی، معیار های نسبتا خوبی برای تمایز اقدامات تروریستی از سایر عناوین مجرمانه است. معیار یکم: موضوع و معیار اصـلی تروریسـم امنیت اسـت که با ایجاد ترس و وحشـت در بین مردم تحقق می یابد. این مورد مهمترین ویژگی اقدامات تروریسـتی اسـت، به طوری که بعضـی این ویژگی را تنها رکن اصـلی در تعریف تروریسـم می‌دانند. تروریســـم یعنی «ایجاد وحشـــت». اینکه آیا امنیت تنها هدف و موضوع تروریست‌هاست و اگر چنین است، چه امنیتی؟ امنیت فردی، ملَی یا بین‌المللی و اصولا تفاوت بین امنیت ملی با حاکمیت سیاسی و منافع آن چیسـت؟ از موضـوعات قابل بحث در فهم اقدامات تروریستی اسـت. معیار دوم: شیوه ارتکاب و وسایل آن است. که به نحو چشمگیری متکثَر و متنوع اسـت. استفاده از خشـونت یا تهدید به آن غالبا به عنوان رکن مادی اقدامات تروریستی مطرح می‌شـود. از عبارت استفاده از خشـونت یا تهدید به آن در تروریســم، مشــخص اســت که برای تحقق تروریســم ضــرورتی ندارد که خشونت به صورت فیزیکی باشد بلکه خشونت روانی هم می‌تواند موجب تحقق اقدامات تروریســتی شــود. تروریســت با اســتفاده از خشــونت و رفتارهای فیزیکی و روانی سعی دارد تا ترس و دلهره بی‌پایانی را در جامعه ایجاد کند و دامنه آن علاوه بر قربانیان مستقیم خود، گروه زیادی از شاهدان و مخاطبین را نیز در بر گیرد.

۱-۳-تروریسم سایبری به مثابه عمل متخلفانه بین‌المللی

دولت‌ها برای برخورد با حملات سایبری یک سری قوانین را وارد قوانین مدون خود نموده اند. ایران در طی سال‌های گذشته بارها هدف حملات سایبری قرار گرفته است و شاید بتوان ادعا کرد یکی از هدف ها و قربانیان اصلی حملات سازمان یافته سایبری در جهان به شمار می‌رود. ولی تاکنون راهبرد مکتوب و مشخصی در این حوزه منتشر نشده است. البته عدم انتشار سندی راهبردی در این موضوع به معنای عدم توجه به فضای مجازی و حملات سایبری نیست بلکه اینترنت اساساً پدیده ای شکل گرفته در دولت های پیشرفته صنعتی است و اغلب شرکت های ارائه دهنده این خدمات در این کشورها قرار دارد، ایران در این حوزه آسیب پذیر تر است.

۲-۳-حمله سایبری به مثابه نقض حقوق توسل بر زور

با مرور اسناد بین المللی مشخص می شود که مفهوم توسل به زور اعم از تجاوز است و تجاوز اعم از حمله مسلحانه است. به عبارت دیگر یکی از اشکال توسل به زور، تجاوز است و یکی از اشکال تجاوز حمله مسلحانه است. طبق ماده ۵۱ منشور ملل متحد: «در صورت وقوع حمله مسلحانه علیه یک عضو ملل متحد تا زمانیکه شورای امنیت اقدام لازم برای حفظ صلح و امنیت بین المللی را به عمل آورد، هیچ یک از مقررات این منشور به حق ذاتی دفاع از خود، خواه فردی یا دسته جمعی، لطمه ای وارد نخواهد کرد. باید توجه داشت که این ماده دفاع مشروع را به حمله مسلحانه محدود کرده است که شامل استفاده از ادوات نظامی علیه دولت دیگری می شود در حالی که اینترنت به عنوان ابزار نظامی در نظر گرفته نمی‌شود. لذا حمله سایبری نمی‌تواند متضمن دفاع مشروع مورد نظر ماده ۵۱ باشد و بر خلاف بیانه‌های متعددی که از سوی برخی مقامات دفاعی ملی منتشر شده است، حمله سایبری نمی‌تواند موجبی برای توسل به دفاع مشروع باشد. (خلیل زاده، ۱۳۹۳: ۵۳).

۳-۳-حمله سایبری به مثابه حمله مسلحانه

همان طور که دیوان بین المللی دادگستری در قضیه نیکاراگوئه بیان کرده است، باید میان شدید ترین صورت‌های کاربردی زور (که به آستانه حمله ای مسلحانه می‌رسند) و آنهایی که صرفا اتفاقات مرزی هستند با توجه به «مقیاس و آثار» آن زور یا نیروی قهری تفکیک قائل شد. از این رو هر درگیری نظامی واجد عنوان حمله مسلحانه‌ای که مجوز دفاع مشروع است

نخواهد بود. بنابراین برای آنکه دولتی طبق ماده ۵۱ منشـــور ملل متحد، به حق دفاع مشروع استناد کند، می باست حمله سایبری را نه تنها توسل به زور بلکه به مثابه حمله ای مســـلحانه تلقی کند. البته منظور آن اســـت که حملات سایبری خود موجد وضعیت مخاصمه مسلحانه شوند، نه آنکه یک مخاصمه کلاسیک و به عنوان یک روش جنگی به کار گرفته شوند. بنابراین باید گفت آیا ابزارهای سایبری می توانند در حکم سلاح بکار گرفته شوند؟ در این باره گفته شـــده اســـت: «این طراحی یا کاربرد متداول یک وســـیله نیست که آن را سلاح می‌کند، بلکه ملاک قصد و اثر بکارگیری آن است.» استفاده از هر وسیله یا تعدادی از وسایل که باعث تلفات معتنا به جانی و یا تخریب گســـترده مالی می شـــود، می‌باســـت حائز شـــرایط یک «حمله مســـلحانه» انگاشـــته شـــود. در بند ۱ ماده ۴۹ پروتکل اول الحاقی نیز آمده است: «حملات به معنای اعمال خشونت آمیز علیه طرف مقابل هستند اعم از آنکه تدافعی یا تهاجمی باشـــند.» معیاری که ژان پیکته در توصـــیف مخاصـمه مسـلحانه وفق ماده ۲ مشـترک کنوانسـیون‌های ژنو ارائه کرده نیز شـــایان توجه اســـت. به نظر وی، کربرد زور در جایی به عنوان «حمله مسـلحانه» شـناخته می شـود که دارای دامنه ، مدت و شـدت کافی باشـد (برادران، ۱۳۹۸: ۶۵).

حمله سایبری به مثابه نقض اصل منع مداخله به نظر می رسد که کل حقوق بین الملل عملاً در اصـل منع مداخله خلاصـه شـده باشـد و آن بدین شـکل است که هر گونه تجاوز به مقررات حقوق بین الملل از جهتی معرّف نوعی دخالت در قلمرو آزادی دولت های دیگری می باشـــد. بر مبنای چنین اندیشـــه ای بود که مجمع عمومی ســـازمان ملل متحد در ۹ دســـامبر ۱۹۸۱ اعلامیه مربوط به عدم پذیرش دخالت و مداخله در امور داخلی دولت ها «قطعنامه ۱۰۳/۳۶» را تصـــویب نمود. از لحاظ فیزیکی و در چارچوب حقوق بین‌الملل کلاسیک بیشتر صحبت از حق مداخله بود تا ممنوعیت آن. زیرا در آن زمان دخالت نه تنها به عنوان وســـیله ای برای دفاع در مقابل تجاوز به حقوق یک دولت محسوب می‌شد بلکه ابزاری برای پیشبرد منافع ملی آن نیز به شـــمار می آمد. در واقع، اصـــل منع مداخله ای که در قرن نوزدهم در اروپا در مقابل دخالت های «اتحاد مقدس» مطرح می شـــد و یا در امریکا «دکترین مونرو» بر ضد مداخلات اروپاییان عنوان میگردید بیشتر مبتنی بر دلایل سیاسی بود تا یک واقعیت حقوقی، بخصوص در دورانی که جنگ هنوز شروع تلقی می گردید. بنابراین صحبت از اصل منع مداخله به

عنوان یک اصل حقوقی چندان رواجی نداشت. امروزه مسئله منع مداخله به شکل دیگری مطرح است. حقوق بین الملل کلاسیک دخالت را به مثاله مداخله مستبدانه یک دولت در امور داخلی یا بین المللی دولت دیگر تعریف می کرد. اولین سند مهم در این خصوص پروتکلی در مورد اصل منع مداخله است که در سال ۱۹۶۳ در کنفرانس «بوئنورس آیرس» به تصویب رسید. این سند اصل منع مداخله را بطورکلی و بدون اشاره به کاربرد زور مد نظر قرار داده است. پس از آن این اصل در ماده ۱۸ اساسنامه سازمان دولت های آمریکایی نیز مدنظر قرار گرفت و الهام بخش قطعنامه ۲۱۳۱ مورخ ۱۹۶۵ مجمع عمومی نیز بود. کلیه اسنادی که بعد از پروتکل بوئنورس آیرس در رابطه با محکومیت مداخله به تصویب رسیده اند هم شامل مداخلات مستقیم و هم در بر گیرنده مداخلات غیر مستقیم می باشند.مداخله غیر مستقیم شامل مداخله نظامی، فشار های سیاسی و اقتصادی و... می باشند که یک دولت از طریق ارکان متعلق به خود انجام نمی دهد بلکه با بکارگیری اشخاص حقیقی و یا حقوقی که در کنترل دارد چنین مداخلاتی را انجام می دهد.مهم با ید توجه داشت حتی اگر حمله سایبری مصداقی از توسل به زور تلقی نشود می تواند اصل منع مداخله در امور داخلی دولت ها را نقض نماید. (محمودی و انصاری مهیاری، ۱۴۰۱: ۲۸).

۴-۳-حمله سایبری به مثابه نقض حقوق بشر دوستانه

عده ای از حقوق دلنان معتقد لند حملات سایبری را میتوان تابع قوانین حقوق جنگ دانست و با پرداختن به قواعد حقوق بشر دوستانه بین المللی سعی در تسری این قواعد به حملات سایبری دارند. از آنجا که قوانین جنگ باید نسبت به تمامی عملیات های نظامی اعمال شود، لذا در صورتی که ویژگی ها و اصول اساسی حقوق مخاصمات را نتوان به حملات سایبری نسبت داد، تلاش برای ممنوعیت حق حاکمیت خود را ندارد. مفهوم حقوق بین الملل بشر دوستانه در کل جایگزین مفهوم حقوق جنگ یا بطور جامع تر حقوق منازعات مسلحانه شده است. البته همه قواعد جنگ، بشر دوستانه نیستند. اغلب قواعد حقوق حاکم بر جنگ را میتوان دارای ماهیت بشر دوستانه دانست، بر خلاف قواعد حقوق جنگ، آنچه که امروز تحت عنوان حقوق بشر دوستانه بین المللی شناخته میشود شامل دو شاخه از مقررات قابل اعمال در مخاصمات مسلحانه یعنی مقررات لاهه و مقررات ژنو است. قوانین لاهه به ویژه مقررات مربوط به قواعد آداب جنگ

زمینی، حقوق و وظایف متخاصمان را در عملیات نظامی آنها تعیین می کند و حق طرفین را در انتخاب و استفاده از ابزار ها و روش ها و وسایل آسیب رساندن به دشمن در یک مخاصمه مسلحانه بین المللی محدود می سازد و افراد انسانی و یا اموال و اشیایی را که در در گیری ها مورد آسیب قرار گرفته یا خواهند گرفت را مورد حمایت قرار می دهد که شامل مقررات ۱۸۹۹ و۱۹۰۷ لاهه به همراه کنوانسیون ها و توافق نامه های مختلف است.

۴-همکاری‌های بین‌المللی در زمینه مبارزه با تروریسم سایبری

عدم هماهنگی کشورها، سبب خواهد شد کشورها به دو قطب مخالف تبدیل شوند؛ برخی کشورها که در برخورد با جرایم رایانه‌ای ضعیف عمل می‌کنند به «بهشت جرایم رایانه‌ای» یا «پناهگاه جرایم رایانه‌ای» بدل خواهند شد و در مقابل کشورهایی که سطح برخورد مناسبی باجرایم رایانه‌ای دارند به «بهشت داده‌ها» یا «پناهگاه داده‌ها» بدل خواهند شد در نتیجه جریان آزاد اطلاعات بین این دو قطب دچار اختلال خواهد شد (حبیبی، ۱۳۷۳: ۳۵۱). بسته به ماهیت تروریسم سایبری، به واقع باید اذعان داشت که مهم‌ترین چاره رویارویی با این پدیده، همکاری‌های بین‌المللی است (پاکزاد، ۱۳۹۰: ۵۴۴). در ادامه به این سه سطح از همکاری‌ها اشاره می‌گردد:

۴-۱-همکاری‌های دوجانبه

همکاری‌های دو جانبه در زمینه موضوعات حقوقی و امنیتی و به تبع آن تأکید بر استرداد مجرمین یکی از راهکارهای شناخته شده برای مقابله طرفینی با پدیده‌های مجرمانه است، که یا به جهت محل وقوع جرم یا متواری شدن متهم یا معماری‌های دیگر، لزوم همکاری بین‌المللی را مشخص می‌کند. این شیوه هر چند در برابر یک پدیده جهان مانند تروریسم سایبری، کمتر کارایی دارد و بیشتر در روابط دو یا چند کشور می‌تواند مؤثر واقع شود، ولی باید گفت در قاره آسیا که امکان شکل گیری اتحادیه به سختی قابل تصور است، توافق‌های دو جانبه یکی از راهکارهای مناسب و ابتدائی تلقی میگرددایران یکی از کشورهایی است که برای مبارزه با تروریسم و نیز جرایم رایلنه‌ای بر توافقات دو جانبه تأکید دارد با آن که قوانین داخلی دوباره تروریسم مبهم هستند ولی مقنن ایران نسبت به تهدیدات بین‌المللی تروریسم و نیز امکان فرار مرتکب بی اعتنا نبوده است؛ از این رو، مبارزه با تروریسم یا پیشگیری از آن در قوانین مرتبط با توافق نامه‌های دو جانبه ایران با سایر کشورها با تأکید و شفافیت بیشتری آمده است (بادروح، ۱۴۰۱: ۱۴).

طبق قانون موافقتنامه امنیتی، انتظامی و مبارزه با مواد مخدر بین دولت جمهوری اسلامی ایران دولت جمهوری یونان مصوب ۱۳۷۹/۲/۲۷ مجلس شورای اسلامی، طبق بند الف ماده ۱، یکی از موارد همکاری در مقابله با تروریسم بین‌المللی و دیگر اعمال جناحی که ماهیت تروریستی دارند، است.

بر اساس قانون موافقتنامه همکاری امنیتی میان جمهوری اسلامی ایران و پادشاهی عربستان سعودی مصوب ۱۳۸۰/۴/۱۷ مجلس شورای اسلامی دولت ایران و عربستان با عنایت به روابط برادرانه اسلامی و دوستانه دو کشور و اهمیت مسایل امنیتی توافق کرده لند. بر اساس ماده ۱ این موافقتنامه، طرف‌های متعاهد در راستای تأمین امنیت و مقابله مؤثر با کلیه جرایم، به ویژه جرایم سازمان یافته و تروریسم، با انجام اقدامات شناسایی، پیشگیری و کشف جرایم و مبارزه با آنها در زمینه های زیر همکاری می‌نمایند.

۱. مبارزه با جعل اسناد دولتی، پول کارت‌های اعتباری و اسکناس و فروش غیر قانونی آنها و نیز جرایم اقتصادی از جمله تطهیر پول
۲. قاچاق اسلحه، مهمات و مواد منفجره
۳. قاچاق کالا و میراث فرهنگی
۴. تجاوز به جان، مال و تجاوز به عنف و اعملا منافی عفت عمومی

۴-۲-همکاری‌های منطقه‌ای

در زمینه همکاری‌های منطقه‌ای چه در زمینه تروریسم و چه در زمینه جرایم رایانه‌ای، منطقه اروپا از همه مناطق جهان پیشتازتر است. در زمینه تروریسم، مناطق جهان در مبارزه با تروریسم یا پیشگیری از آن، اسنادی را پیش‌بینی کرده لند[۲] در کنار قاره‌ها، مناطق فرو قاره‌ای مانند اتحادیه عرب (۱۹۹۸) و کشورهای آسه آن (۲۰۰۷) نیز دوباره مبارزه با تروریسم کنوانسیون‌هایی را تصویب کرده اند. همچنین باید به اقدامات آسه آن در مورد تروریسم سایبری نیز اشاره نمود. گروه کشورهای انجمن ملل آسیای جنوب شرقی که بیشتر با نام اختصاری آسه آن شناخته می‌شود تا کنون به طور خاص پنج سمینار در مورد تروریسم سایبری برگزار نموده‌اند. آخرین آن در سنگاپور در ۲۰۰۸ برگزار گردید. در این سمینار ضمن تأکید بر

۲ htto//www.ioc.utokyo.ac.jp/~worldgpn/documents/texts/arf/20087 24.OIE.html Singapore July 24, 2008 ASEAN

همکاری برای مبارزه با تروریسم سایبری، وزرا از تأسیس نشست مجازی متخصصین در زمینه تروریسم سایبری و امنیت سایبری استقبال کردند و وزرای جمهوری کره و فیلیپین برای رهبری گروه در سال نخست اعالم آمادگی کردند.

در زمینه جرایم رایانه‌ای، تنها در منطقه اروپا اقدام مؤثر انجام شده و آن هم تصویب کنوانسیون جرایم سایبر در سال ۲۰۰۱ در بوداپست است که به تصویب شورای اروپا رسید و از آن به بعد مبنای روابط میان اعضای شورا و سایر کشور های جهان در مورد جرایم سایبری شد. این امر که مطابق اعالم این شورا این کنوانسیون طرح کنوانسیون سازمان ملل برای سایر کشورها نیز خواهد بود اهمیت دو چندان آن را می‌رساند (پاکزاد، ۱۳۹۰: ۱۰۳).

شورای اروپا در این کنوانسیون که به منزله یک قانون مؤثر برای مقابله با جرمهای سایبری است، مبارزه با تروریسم سایبری را هنجارمند نموده است. مواد ۲-۱۰ این کنوانسیون در بردارنده انواع جرم ها و مواد ۱۱-۱۳ نیز حاوی مقررات کلی مربوط همه جرایم با عنوان ضمانت اجراها و مسئولیت‌های تبعی است. جرم‌های مذکور در کنوانسیون تحت عناوین جرایم علیه محرمانگی، تمامیت و دسترس پذیری سیستم‌ها و داده‌های رایانه‌ای، جرایم ربوط به رایانه، جرایم مرتبط با محتوا با نقض حق نشر و حقوق مربوط به آن آمده است. به ویژه عنوان نخست هر چند به تروریسم سایبری اشاره نکرده است ولی جرایم مقدماتی تروریسم سایبری و نیز رفتارهایی که تنها با انگیزه سایسی چهره این پدیده را به خود میگیرند مانند تخریب و اخالل داده یا سامانه‌های رایانه‌ای را جرم دانسته است. این سند همچنین به مقررات شکلی و پیشگیرانه مرتبط با مبارزه با جرایم سایبری اشاره کرده است.

پیشرفته‌ترین سیستم همکاری‌های حقوقی بین‌المللی در کنوانسیون جرایم سایبری شورای اروپا در سال ۲۰۰۱ خصوصاً در فصل ۳ کنوانسیون، یافت می‌شود مثلاً ماده ۲۴ شامل مقررات استرداد مجرمین به دولت متبوعه است و در مواردی که در بردارنده جرایم خاص رایانه‌ای مطابق با ماده‌های ۲ الی ۱۱ است قابل اعمال می‌باشد، مشروط به آنکه مجرمین تحت قوانین هر دو طرف مربوطه قابل مجازات باشند. فصل ۳ نیز حاوی مقررات مشروح خاص رایانه‌ای برای همکاری متقابل است، از جمله همکاری در حیطه‌های حفاظت فوری از داده‌های رایلنه‌ای ذخیره شده، افشای فوری داده‌های

ترافیک حفظ شده، دسترسی به داده‌های رایانه‌ای ذخیره شده، جمع‌آوری فوری داده‌های ترافیک و شنود داده محتوا همچنین اصولی کلی را در رابطه با همکاری متقابل، محرمانگی و محدودیت در استفاده را فراهم می‌آورد و مسئله اطلاعات فوری را مطرح می‌سازد.

ماده ۲۷ بند ۴ به کشور طرف درخواست امکان رد همکاری را در صورتی که آن خواسته در رابطه با جرمی باشد که طرف درخواست شونده، آن را جرمی سیاسی تلقی کند یا چنانچه احتمال دهد اجرای درخواست موجب لطمه زدن به استقلال، امنیت، نظم عمومی یا دیگر مصالح ضروری خواهد شد، می‌دهد. در هر حال برای مقابله بین‌المللی با تروریسم سایبری به‌ویژه در قالب توسلبه جرم انگاری برخی رفتارهای ناقض هنجارهای سایبری، تاکنون تصویب کنوانسیون بوداپست راجع به جرایم محیط سایبری مهم‌ترین اقدام ماهوی و شکلی بوده است.

باید اشاره نمود که علاوه بر گسترش همکاری‌های دو جانبه، همکاری‌های جهانی در قالب رهنمودهای سازمان ملل متحد به ویژه قطعنامه‌ها خود تأثیر بسزایی در امر مقابله با تروریسم سایبری دارد.

۴-۲-همکاری‌های جهانی

همکاری‌های جهانی در مبارزه با تروریسم بیشتر پیرامون کنوانسیون‌های سازمان ملل متحد درباره تروریسم و قطعنامه‌های شورای امنیت می‌چرخد. از دید اسناد بین‌المللی تروریسم دارای یک مفهوم عمومی است که مصادیق فراوان می‌تواند داشته باشد. رویکرد حقوقی مقابله با تروریسم بین‌المللی که در قالب کنوانسیون‌ها پروتکل‌های بین‌المللی تبلور یافته، کلی نگر نبوده بلکه مبتنی بر جرم انگاری و پرداختن به خشن‌ترین و رایج‌ترین مصادیق تروریسم بین‌المللی است، هرکدام از این اسناد مشتمل بر فهرست یا توصیفی عینی از جرایم ممنوعه است و اقداماتی مشخص را برای سرکوبی و مجازات آن‌ها مقرر داشته است؛ » با اتخاذ چنین نگرش بخشی و عملگرایلنه‌ای، نظام ملل متحد توانسته است منظومه‌های حقوقی برای جلوگیری و مجازات بسیاری از اعمال تروریستی عرضه کند. اگرچه هر سند بین‌المللی به جرمی جداگانه مربوط می‌شود اما همه آن‌ها ویژگی‌های مشترکی دارند از جمله: رویکرد موردی به جرم تروریسم بین‌المللی، مسئولیت کیفری که عموماً متوجه اشخاص حقیقی است غیرسیاسی تلقی کردن جرایم تروریستی، اصل استرداد یا محاکمه، و الزام دولت‌ها به

همکاری با یکدیگر. کلیه این اسناد، دولت‌های عضو را ملزم و می‌سازد که با یکدیگر، همکاری قضایی کنند (طیبی فرد، ۱۳۸۴: ۲۷۱).

همچنین طبق این اسناد، دولت‌های عضو ملزم‌اند جرایم فهرست شده، را در قوانین داخلی خود را درباره این جرایم (مانند جرایم ارتکابی در ۴۵ قابل مجازات بشناسند و صلاحیت اولیه و اصلی قلمرو خودشان یا توسط اتباعشان) اعمال کنند. وانگهی تمام دولت‌های عضو ملزم‌اند بر هر جرمی که متهم آن، متعاقباً در سرزمین آنها حضور پیدا کرده باشد، صلاحیت فرعی اعمال نمایند.

تاکنون هیچ کنوانسیون خاصی تحت عنوان تروریسم سایبری تصویب نشده است. اما کنوانسیون‌های موجود در خیلی از موارد قابلیت اعمال در مورد تروریست سایبری را دارد. از دیگر اسنادی که به تصویب مجمع عمومی سازمان ملل متحد رسید، «کنوانسیون بین‌المللی مبارزه با تأمین مالی تروریسم» است که در تاریخ ۹ دسامبر ۱۹۹۹ به تصویب مجمع عمومی رسید. کنوانسیون، سه تعهد عمده برای کشورهای عضو در نظر گرفته است:

۱. جرم‌انگاری تأمین مالی اعمال تروریستی در قوانین ملی خود
۲. همکاری گسترده با سایر کشورهای عضو و ارائه معاضدت قضایی در موضوعات مربوط به کنوانسیون.
۳. وضع مقررات و الزامات مربوط به ایفای نقش مؤسسات ملی در کشف و گزارش دهی موارد هدف مهمی که در قالب اسناد مورد بحث دنبال شده است، هماهنگی بین‌المللی در قوانین شکلی و ماهوی در رویارویی با اقدامات تروریستی است.

همکاری‌های جهانی در مقابله با تروریسم سایبری به اسناد مذکور ختم نمی‌شود، بلکه اسناد و تصمیمات مشورتی و ارشادی متعددی راجع به تروریسم به ویژه پس از سپتامبر ۲۰۰۱ پیشنهاد شده است که مقابله با تروریسم سایبری را نیز می‌توان از لا به لای آن‌ها جست. البته برخی از قطعه نامه‌های شورای امنیت در راستای پیشگیری و زمینه سازی یک فضای اطلاعاتی سالم تأثیر بسیاری در الگودهی به کشورهای عضو سازمان داشته است از جمله قطعنامه‌های ۲۰۵۷۲۳۹ دسامبر ۲۰۰۲ در مورد ایجاد فرهنگ جهانی امنیت سایبری ۴۵۵۶۳ دسامبر ۲۰۰۰ و ۱۹۵۶۱۲۱ دسامبر ۲۰۰۱ در مورد ایجاد مبانی قانونی مبارزه با سوء استفاده مجرمانه از فناوری‌های اطلاعاتی و ۴۵۳۷۰ دسامبر ۱۹۹۸ ـ ۱۵۴۴۹ دسامبر ۱۹۹۹ ـ ۲۰۵۵۲۸ نوامبر

۲۰۰۰ ـ ۲۹۵۶۱۹ نوامبر ۲۰۰۱ـ ۲۲۵۷۵۳ نوامبر ۲۰۰۲ـ ۱۰ ـ ۱۶ هماهنگی در مورد پیشـــرفته ای در زمینه ارتباطات و اطلاعات در مورد امنیت بین‌المللی.

۳-تعهدات بین‌المللی کشورها در مقابله با تروریسم سایبری و ابعاد آن

از هر زاویه‌ای به موضوع تروریسم بنگریم ملاحظه خواهیم کرد که حقوق بین‌الملل تکالیف جدی را بر دوش کشورها برای مبارزه با انواع تروریسم نهاده اما در مورد تروریســـم ســـایبری حقوق بین‌الملل غافل‌گیر شـــده و مصـــوبه‌ای برای مقابله با آن ندارد. از آنجا که تروریســـم، حقوق بشـــر را مخاطب قرار داده و حقوق بشـــر با نظام عمومی داخلی و بین‌المللی گره خورده است بنابراین می‌توان مطمئن بود که وجدان بشریت اجازه ارتکاب این اعمال را نمی‌دهد و باید با روش‌های قانونی نسبت به این طاعون مدرن واکنش نشان داد. از اینترنت می‌توان علیه تروریست‌های سایبری استفاده کرد و به شـــکل پدافند عامل و غیرعامل تمام حملات تروریســـتی آنها را خنثی و ناکام گذاشت (موثقی، ۱۴۰۱: ۱۱۲).

بنابراین دولت‌ها باید با نظارت مســـتمر بر اینترنت و تعاملات مظنونین به تروریسم سایبری مانع از استخدام، بکارگیری، تربیت هکر و متوقف کردن حملات تروریســـتی در نطفه شـــوند ضـــمن آن که باید نســـبت به افزایش آگاهی‌های همگانی شهروندان همه کشورها اقدام نمایند تا شهروند در دام عنکبوتی تروریست‌ها نیفتند. علاوه از آن رعایت حقوق بشـر باید با لحاظ منافع جمعی توأم گردد که در این راســـتا توجه به ســـازوکار پیشـــگیری، از اهمیت زیادی بر خوردار اســـت. بنابراین جرم انگاری جرایم تروریســـتی سایبری گام بعدی در پایان دادن به تروریسم سایبری خواهد بود (قاسمی و باقرزاده، ۱۳۹۴: ۲۴۴). شـــورای امنیت در قطعنامه ۱۳۷۳ از همه کشـــورها خواســـت که مانع تامین مالی اعمال تروریســـتی شـــده و آن را متوقف کنند همین طور مانع از عضـــوگیری گروه های تروریســـتی شـــوند و با تبادل اطلاعات به هشدار اولیه به سایر کشورها اقدام نمایند (Rosand, 2003: 335).

در فرازی دیگر از این قطعنامه آمده که اقدامات کشـورها در اجرای قطعنامه ۱۳۷۳ شـــورای امنیت نباید به موازین بنیادین حقوق بین‌الملل صـــدمه وارد کند. موضوع پیشگیری از جرم در قطعنامه‌های شماره ۱۹۹۵/۹ و ۲۰۰۲/۱۲ شـــورای اقتصـــادی و اجتماعی و همین طور قطعنامه شـــماره ۴۵/۱۱۲ ســـال ۱۹۹۰ مجمع عمومی سـازمان ملل متحد به صـراحت مورد تاکید قرار گرفته

و اصول اساسی و جهت گیری صحیح پیشگیری از جرم به شکل ملی و بین‌المللی تمهید شده است (عباسی کلیمانی و همکاران، ۱۳۹۹: ۱۵۵).

همین طور سازمان ملل متحد از سال ۱۹۹۴ با هدف افزایش آگاهی‌های جمعی راجع به افزایش امنیت کامپیوترها هفت شاخصه اصلی را برای جلوگیری از نفوذ سایبری برشمرده که شامل: امنیت اداری و سازمانی، امنیت کارمندان، امنیت فیزیکی، امنیت مخابرات الکترونیکی، امنیت سخت افزاری و نرم افزاری و امنیت عملیاتی و برنامه ریزی میگردد (همان: ۱۶۶). شورای امنیت سازمان ملل متحد از همه کشورها می‌خواهد که اقدامات قانون گذاری و قضایی را برای پیشگیری از حوادث تروریستی اتخاذ نمایند و تروریست‌ها را دستگیر، محاکمه و مجازات کنند (Bantekas, 2003: 315).

به نظر می‌رسد که مهمترین تعهد منعکس در معاهدات بین‌المللی ضد تروریسم، جرم انگاری اینگونه اعمال در قوانین کیفری است و این که دول عضو باید زمینه پذیرش صلاحیت قضایی جهانی را در قوانین کیفری خود بگنجانند که این موضوع شامل رسیدگی قضائی سرزمینی، رسیدگی بر مبنای تابعیت مجرم و قربانی و مطابق معاهدات و قضاوت بر مبنای محل اقامت متهم خواهد بود که این الزامات شامل استرداد مجرمین نیز می‌گردد. مفاد قطعنامه‌های شورای امنیت سازمان ملل متحد و مجمع عمومی حکایت از حرکت جامعه بین‌المللی برای پذیرش اصل صلاحیت جهانی در ارتباط با جنایات تروریسم و تروریسم سایبری دارد که با توسعه صلاحیت قضایی کشورها انجام خواهد شد.

با توجه به آن که تروریسم سایبری یک جرم بین‌المللی است، مقررات ملی به تنهایی قادر به دفاع در واکنش به چنین حملاتی نیستند، برای دستیابی به یک درک مشترک در زمینه مقابله با تهدیدهای تروریسم سایبری، ابتدا راه حل‌های ارائه شده توسط معاهدات بین‌المللی حاضر در نظر گرفته شود، تا به پاسخ‌های موجود در برابر تهدیدات سایبری بین‌المللی بپردازیم. نکته دوم این که اگر چه دولت‌ها باید برای مقابله با سوءاستفاده از فناوری جدید، سازوکارهای قانونی و نیز نظارتی را خود تقویت کنند، اما این سازوکارها باید با توافق‌های بین‌المللی مناسب حمایت شوند. در صورت تصویب تعداد زیادی از کشورها، سازمان‌های منطقه‌ای ممکن است به عنوان سازمان‌های چند جانبه عمل کنند. نمونه آن کنوانسیون شورای اروپا در مورد جرائم سایبری است که توسط بسیاری از کشورها تصویب شده و

در حال حاضـــر به تنها پیمان بین‌المللی علیه جرایم ســـایبری تبدیل شـــده است.

نتیجه گیری

از تروریســـم به عنوان «ســـرطان» دنیای مدرن یاد می‌کنند. بی‌شـــک جامعه جهانی این معضـــل بین‌المللی شـــده را یکی از دغدغه‌های اصـــلی خود و از عوامل تهدید علیه صـــلح و امنیت بین‌المللی تلقی می‌کنند. از هنگامی‌که ســـازمان ملل متحد در دهه هفتاد ابتکار عمل را در مبارزه با تروریســـم در دســـت گرفت، آشـــکار بود که مشـــکلات غلبه ناپذیری در قالب یک رویکرد سیاسـی برای طراحی یک رژیم مورد توافق برای مبارزه با تروریسـم وجود دارد. به همین دلیل و به علت رشـد اقدامات تروریسـتی در این دهه، جامعه بین‌المللی با نگرشی عملگرایانه برخی از اقدامات خاص را به عنوان اقدامی مجرمانه و تروریستی قلمداد کرد و برای هرکدام رژیم حقوقی مشخصی را تبیین نمود. بدین ترتیب کنوانســـیون‌های بین‌المللی متعددی برای مبارزه با تروریسم به تصویب رسیدند.

تروریسـم سـایبری و سـوء اسـتفاده تروریسـت‌ها از فضـای سـایبر از جمله چالش‌های عصر حاضر است. تروریسم سایبری، جرمی است که دارای آثار و نتایج فراملی بوده و تروریســـت‌ها می‌توانند در هر جای دنیا که باشـــند اهداف خود را در ســـایر نقاط جغرافیایی جهان رصـــد نمایند. امروزه تروریسـت‌ها می‌توانند با شـکستن رمزهای اینترنتی و دسـترسـی غیرمجاز به اطلاعات محرمانه، حملات ســـایبری را علیه دولت‌ها با اهداف مغرضـــانه طراحی نمایند. لذا مقابله با آن به‌صورت جدی مورد توجه جامعه بین‌المللی قرار گرفته اســـت. وجود هشـــدارهای مســـتمر پیرامون خطرهای ناشـــی از تروریســـم ســـایبری، انجام تحقیقات حقوقی ســـازمان یافته بین‌المللی را به منظور درک مشکلات امنیتی و بین‌المللی مرتبط با آن را می‌طلبد. موضوعی که می‌تواند با گسـترش خود و کاربرد سـلاح‌های پیشـرفته سـایبری اصـول بنیادین حقوق بین‌الملل را در خصـوص توسـل به زور و نبردهای مسـلحانه را تحت تأثیر قرار دهد. این در حالیســـت که از یک ســـو اجماع جهانی در خصـوص تعریف یا تحلیل تروریسـم سـایبری وجود ندارد و از سـوی دیگر هنوز نظام حقوقی بین‌المللی لازم‌الاجرای جامعی در خصـوص مقابله با این جرم در سطح جهانی تصـویب نشـده اسـت. کما این که نمی‌توان منکر تأثیر قطعنامه‌های مجمع عمومی و شورای امنیت سازمان ملل متحد در این زمینه شـد. هر چند دسـته اول جزو قواعد حقوقی نرم دسـته بندی شـده و از لحاظ

حقوقی لازم‌الاجرا نیستند و دسته دوم نیز هیچ یک به صراحت و به طور خاص تروریسم سایبری را مد نظر قرار نداده‌اند

برای پیشگیری و مقابله با تروریسم سایبری، ضرورت گسترش همکاری‌های بین‌المللی در عصر حاضر مسجل می‌باشد. در فضای سنتی و با شیوع تروریسم بین‌المللی، تقریباً بیشتر کشورها پذیرفته‌اند که مقابله با تروریسم جز با همکاری‌های بین‌المللی امکان‌پذیر نیست. این نکته در مورد تروریسم سایبری برجسته‌تر است و به علت اینکه فضای سایبری، مکان وقوع جرم است و این مکان نیز بدون مرز و بدون محدودیت است؛ امکان سرزمینی کردن مقابله با تروریسم سایبری وجود نداشته یا محکوم به ناتوانی و ناکامی است. رویارویی مؤثر در برابر اقدامات تروریستی سایبری مستلزم هماهنگ سازی حقوق کیفری ماهوی و شکلی کشورها، بهبود همکاری‌های بین‌المللی و اقدامات پیشگیرانه مانند حفاظت از زیرساخت‌ها و تأمین امنیت فضای سایبر دارد.

منابع

۱. بادروح، مجید (۱۴۰۱). سیاست جنایی مقابله با تروریسم سایبری، نشریه علمی فقه، حقوق و علوم جزا، سال ۷، شماره ۲۴

۲. برداران، نازنین (۱۳۹۸). جنگ سایبری از منظر حقوق بین‌الملل، تهران: مجد، چاپ اول

۳. پاکزاد، بتول (۱۳۹۰). اقدام‌های سازمان‌های بین‌المللی و منطقه‌ای در خصوص جرم‌های رایانه‌ای، مجموعه مقالات همایش بررسی جنبه‌های حقوقی فناوری اطلاعات،

۴. حبیبی، حسن (۱۳۷۳). منطق حقوقی و انفورماتیک حقوقی، تهران: اطلاعات، چاپ اول

۵. حسینی مهر، مهدیه، مختاری افراکتی، مهدیه (۱۳۹۵). تحلیل فقهی تروریسم و بررسی تطبیقی آن با جرم محاربه و فساد فی‌الارض، نشریه دانش انتظامی خراسان جنوبی، سال ۵، شماره ۳، ۱۱۳-۱۳۴

۶. خلیل زاده، مونا (۱۳۹۸). مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری، تهران: مجد، چاپ اول

۷. طیبی فرد، امیرحسین (۱۳۸۴). مبارزه با تامین مالی ترور در اسناد بین‌المللی، مجله حقوقی، شماره ۳۲

۸. عباسی کلیمانی، عاطفه، محبوبی، ملیکا، نوری، فاطمه (۱۳۹۹). راهبردهای نوین پیشگیری از وقوع تروریسم سایبری، فصلنامه راهیافت پیشگیری از جرم، دوره ۳، شماره ۱، ۱۴۵-۱۷۲

۹. فرمانی، مصطفی (۱۳۹۰). حقوق و تعهدات کشورها در مقابله با تروریسم در چارچوب مقررات بین‌المللی و آثار آن بر جمهوری اسلامی ایران، پایان نامه کارشناسی ارشد، دانشگاه پیام نور تهران

۱۰. قاسمی، غلامعلی، باقرزاده، سجاد (۱۳۹۴). جایگاه حقوق بشر در مبارزه با سایبر تروریسم، مجله حقوقی بین‌المللی، شماره ۵۲، ۲۲۷-۲۵۴

۱۱. محمودی، هادی، انصاری مهیاری، علیرضا (۱۴۰۱). بررسی راه‌کارهای تقلیل حملات سایبری از منظر حقوق بین‌الملل بشر دوستانه، مطالعات حقوقی فضای مجازی، سال اول، شماره سوم، ۱۹-۳۶

۱۲. موثقی، حسن (۱۴۰۱). چالش‌های اعمال صلاحیت جهانی در مقابله با ترویسم سایبری، دو فصلنامه علمی-پژوهشی حقوق قضایی، دوره ۳۰، شماره ۳۰، ۱۰۲-۱۲۰

۱۳. میرعباسی، باقر، کورکی‌نژاد قرایی، مجید (۱۳۹۷). قابلیت تحقق سایبر تروریسم و ارتباط آن با حقوق ذاتی دفاع مشروع مقرر در ماده ۵۱ منشور ملل متحد، فصلنامه مطالعات حقوق عمومی دانشگاه تهران، دوره ۴۸، شماره ۲، ۲۶۱-۲۸۰

1. Bantekas, I. the International Law of Terrorist Financing, American Journal of International Law, vol. 97, 2003.

2. Condron, Sean. 2007,“Getting it right: protecting American critical infrastructure in cyberspace”,HARVJ,no. 20: 1-20.

3. Rosand, E. Security Council Resolution 1373, The Counter- terrorism committee and the fight against terrorism, American journal of International Law, vol. 97. No. 2, 2003.

4. UN General Assembly, «Convention on Offenses and certain other Acts Committed on the board Aircraft», 1963. https: //www. unodc. org/tldb/en/1963_ Convention_on %20Board %20 Aircraft. html. (1/28/2017)

5. UN General Assembly, «Convention on the Prevention and Punishment of Crimes against Internationally Protected Person, including Diplomatic Agents», 1973. . http: //www. ilp. gov. la/ database/PDF/I. 6. 5. pdf. (1/28/2017)