Two scientific and research quarterly journals of judicial law, 2022, year 13, number 30. P: 102-120.

https://judicial.ntb.iau.ir/

The challenges of Applying Global Jurisdiction in Dealing with Cyber Terrorism

Hasan Movassaghi[1]

Associate Professor, Department of International Law, Tabriz Branch, Islamic Azad University, Tabriz, Iran.

(Received: 23 July 2022 - Accepted: 11 September 2022)

Abstract

Undoubtedly, one of the crimes that threatens the peace and internal security of countries and the international community in a mysterious and widespread way is the crime of terrorism, which has caused deep concern for almost all the nations and states of the world, and dealing with it as a Erga Omnes obligation Inclusion is demanded from all countries and because some Countries do not have the experience of threats and terrorist attacks, they have no desire and inclination to cooperate with the international community to eliminate the crime of terrorism And this seemingly simple issue has caused the continuation of terrorist attacks in the world. In this research, we will deal with the obstacles of applying the principle of universal jurisdiction in the fight against terrorism and we will provide guidelines for its acceptance and application. The research method in this article is descriptive and comparative, and the findings of the research show that the governments act completely monopolistically in the field of jurisdiction of the domestic courts, and it does not go too far to exercise global jurisdiction.

Keywords: Cyber Terrorism, Global Jurisdiction, United Nations, Territorial Jurisdiction, Extradition of Terrorists**.**

Corresponding author: Email: Movassaghi@iaut.ac.ir

How to Cite:

Mousavifard, H. (2022**).** « The challenges of Applying Global Jurisdiction in Dealing with Cyber Terrorism». Judicial law, 2022, 13 (30), 102-120.

Published by University of Islamic Azad University, North Tehran branch, Tehran, Iran:
https://ntb.iau.ir/fa

Online ISSN: 2008-7500

دو فصلنامهٔ علمی و پژوهشی حقوق قضایی، ۱۴۰۱، سال سیزدهم، شماره سی، ۱۰۲-۱۲۰.

https://judicial.ntb.iau.ir/

چالشهای اعمال صلاحیت جهانی در مقابله با تروریسم سایبری

حسن موثقی[۱]

دانشیار گروه حقوق بین الملل، واحد تبریز، دانشگاه آزاد اسلامی، تبریز، ایران.

(**دریافت:** ۱۴۰۱/۵/۱ ـ **پذیرش نهایی:** ۱۴۰۱/۶/۱۳)

چکیده

بدون شک یکی از جنایاتی که به شکل مرموز و گسترده صلح و امنیت داخلی کشورها و جامعه بین‌المللی را تهدید کرده و می‌کند جنایت تروریسم است که تقریباً موجبات نگرانی عمیق همه ملل و دول جهان را فراهم کرده است و مقابله با آن به عنوان یک تعهد عام الشمول از همه کشورها مطالبه می‌گردد و چون برخی از کشورها تجربه تهدیدات و حملات تروریستی را ندارند هیچ تمایل و گرایشی به همکاری با جامعه بین‌المللی برای حذف جنایت تروریسم ندارند و همین موضوع به ظاهر ساده موجب استمرار حملات تروریستی در جهان شده که در این تحقیق به چالشهای اعمال صلاحیت جهانی در مقابله با تروریسم خواهیم پرداخت و رهنمودهایی را جهت پذیرش و اعمال آن ارائه خواهیم داد. روش تحقیق در این مقاله توصیفی و مقایسه‌ای است و یافته‌های تحقیق ثابت می‌کند که دولتها در زمینه صلاحیت محاکم داخلی کاملاً انحصاری عمل می‌کنند و چندان تمایلی به اعمال صلاحیت جهانی در مقابله با تروریسم سایبری ندارند.

واژگان کلیدی: تروریسم سایبری، صلاحیت جهانی، سازمان ملل متحد، صلاحیت سرزمینی، استرداد تروریستها

۱. **نویسنده مسئول: تلفن:** ۹۱۴۸۲۳۲۴۱۲ **رایانه:** Movassaghi@iaut.ac.ir

نحوهٔ آدرس‌دهی: موثقی، حسن (۱۴۰۱)، «**چالشهای اعمال صلاحیت جهانی در مقابله با تروریسم سایبری**»، حقوق قضایی، ۱۳(۳۰)، ۱۰۲-۱۲۰.

ناشر: دانشگاه آزاد اسلامی، واحد تهران شمال، تهران، ایران: https://ntb.iau.ir/fa

شاپای الکترونیکی: ۷۵۰۰-۲۰۰۸

طرح مسئله

تروریسم سایبری قادر است که با وارد کردن آسیب‌های جدی به شبکه اطلا عات رایانه‌ای دولتها ضربات کاری به حاکمـ یت و ا ستمرار ا مور روزا نه وارد کرده و زندگی را برای شهروندان و دولتمردان تلخ نمایند.

در نتیـ جهٔ حـ ملات تروریـ ست‌های سایبری، بازار، تو سعه پا یدار، حـ مل و نـ قل، سیستم مخابرات و آینده یک کشور و شهروندان آن به شدت آ سیب می‌بیـ ند و ا گر کشور مورد تهاجم از تکنولوژی سایبری مناسبی برخوردار نباشد ماند کـ شورهای آفریقایی یا برخی از کشورهای آسیایی و آمریکای لاتین، در این صورت آ سیب‌های وارده در نتیجه حملات تروریست‌های سایبری غیرقابل جـ بران خوا هد بود و هـ مین موضوع تعهد به مقابله با تروریست‌ها در همه اشکال و ا نواع آن را مـ جدداً یادآوری می‌کند (بیگی، احمدی سربرزه و رحیمی، ۱۳۹۸، ص ۷۵۷).

بنابراین تروریسم به اندازه‌ای تهد ید کـ نده صلح و امنـ یت بین‌المللـ می‌با شد و همسان جنگ قلمداد شده و پاسخ‌های مناسب خود را می‌طلبد. از سوی دیگر با ورود فضای مجازی به عرصه حـ یات بـ شری، مـ حیط جد یدی برای خودنـ مایی و حـ ملات تروریستی برای جنایتکاران ضد بشری فراهم آ مده که ساختار اطلا عاتی و حـ یاتی کشورها و ملت‌ها را مخاطب حملات 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 یر دور افتاده جهان هستند فضای مجازی محیطی است واجد قابلیت و فرصت برای دستیابی به توسعه پایدار و همینطور تهدیداتی که در برخی موارد منبع تهدید کاملاً نا شناخته می‌ماند و قابل تعقیب، محاکمه و مـ جازات نیـ ست به هـ مین جـ هت ا ست که حـ ملات تروریست‌ها به ویژه تروریسم سایبری[1] را می‌توان با لحاظ ا هداف تخریـ بی آن، یک جنگ به حساب آورد. حقوق بین‌الملل هنوز راجع به تلقی آن به عنوان جنگ، معاهده و مصوبه‌ای ندارد.

دولتها علاوه بر مردم، خودشان در موضوع این حملات قربانی هـ ستند و هر یک تلاش دارند که به تنهایی به این حملات خاتمه داده و نظم عمومی مختل شده را ا عاده نمایند (ضیائی و خلیل زاده، ۱۳۹۲، ص ۸۹) اما موانع و چالش‌های مو جود صلاحیت جهانی[2] در مقابله با تروریسم سایبری شده است و دنیا هنوز به اهمـ یت ا ین حقیـ قت

---

1 - Cyber Terrorism

2 - universal principle

پی نبرده است که جنایت تروریسم سایبری یک تبهکاری فرامرزی و یک جنگ بی‌سر و صدا علیه شهروندان دهکده جهانی در مرحلهٔ اول و دولت ها و ک شورها در مرحله دوم است که می‌تواند آثاری مهلک تر از ویروس کوو ید ۱۹ بر جای گذارد و ث بات روابط بین‌الملل را مختل کرده و دولتها را نسبت به هم بی‌اعت ماد و شکاک سازد و روند حرکت به سوی توسعه پایدار و صلح و امنیت بین‌المللی را به چالش ک شیده و متوقف نماید. قطعاً حملات تروریست‌ها اگر با آثار ویرانی و تخریب و صدمات جانی توام باشد می‌تواند یک حمله مسلحانه به حساب آید. در ا ین خ صوص سؤال ا صلی تحقیق به شرح ادامهٔ بحث است.

۱.سؤال اصلی تحقیق:سؤال اصلی تحقیق در این خصوص چنین است:
چالشهای اعمال صلاحیت جهانی در مقابله با تروریسم سایبری چیست؟

۲.پیشینهٔ مسئله ضرورت تحقیق

سنتی بودن تفکر حاکمیت سرزمینی و تاکید بر صلاحیت انح صاری ک شورها در خصوص سؤال تحقیق موجب شده است که هیچ توافق جم عی در زمی نه راهکار های شناسایی و تعقیب تروریست‌های سایبری تح قق نیاف ته و کما کان شاهد ت صمیمات یکجانبه کشورها جهت مقابله با تروریست‌های فرامرزی و سایبری هستیم که کارآمد نبوده و رشد قارچ گونه تروری سم سایبری و ح ملات رایا نه‌ای به ترین دل یل برای ناتوانی تصمیمات یکجانبه در مقابله با تروریست‌های سایبری می‌باشد. کانون و نقطه شروع ح ملات تروری ست‌ها قا بل شنا سایی نی ست و سی ستم‌های کامپیوتری و زیرساخت‌های اساسی کشورها اسا ساً آ ماده مقابله با چ نین ح ملات تروری ستی نیستند و نقاط ضعف موجود در سرورها درست مانند نق طه کور و فر صت آفری نی برای تروریست‌ها عمل می‌کند. از سوی دی گر قوانین ح قوقی و کی فری ک شورها در زمینه مقابله با تروریست‌های سایبری کاملاً متمایز از هم می‌با شند و رو یه وا حدی در این زمینه وجود ندارد (ترابی، ۱۳۹۴، ص ۱۴۷-۱۴۳).[۱]

۱- سازمان پیمان آتلانتیک شمالی (ناتو) در سال ۲۰۰۷ با هدف مقابله با حملات سایبری دستورالعمل تالین ۲-۱ را تصویب کرد تا مانع آسیب کشورهای عضو ناتو از سوی حملات سایبری گردد و مورد موافقت همه کشورهای مطرح جهان قرار گرفت که حملات سایبری، جنگ تلقی شده و پاسخ نظامی با تمسک به اصل دفاع مشروع داده شود (ترابی، ۱۳۹۴، ص ۱۴۷-۱۴۳). برای مطالعه بیشتر رک: صلاحی، س و کشفی، س م. «جنگ سایبری از منظر حقوق بین الملل با نگاه به دستورالعمل تالین»، دو فصلنامه علمی- پژوهشی مطالعات قدرت نرم، سال ششم، شماره چهاردهم، بهار و تابستان ۱۳۹۵، ص ۳۶.

تحولات علمی در دنیای تکنولوژی میزان آسیب‌پذیری کشورها را افزایش داده و دولتها حتی دولتهای مقتدر جهان کنونی نیز به راحتی قربانی حملات غافلگیرانه تروریستی می‌شوند و از ابعاد مختلف اجتماعی، اقتصادی و فرهنگی صدمات جدی را دریافت می‌کنند. تجربیات تاریخی ثابت می‌کند که تکنیک حملات تروریستهای سایبری، حمله و اختفاء است که یادآور یک جنگ های نامنظم و پارتیزانی است و هدف قرار دادن نقاط ضعیف یا حساس کشورها از نگاه تیزبین تروریستهای سایبری غیرعامل اجتناب است.

بدین ترتیب می توان نتیجه گرفت که تروریسم سایبری یک جنگ علیه نوع بشر است و پاسخ‌های موقت، موردی و سطحی قادر به مقابله با سونامی اندهام و ارعاب ایجاد شده توسط تروریستهای سایبری نیست و کاربرد مقطعی صلاحیت سرزمینی[1]، صلاحیت حمایتی[2] و صلاحیت مبتنی بر تابعیت فعال و منفعل در مقابله با تروریست‌های سایبری نتیجه‌ای نخواهد داشت زیرا تروریستها در حال حمله به ساختار اطلاعاتی کشورها به صورت مذسجم و یکپارچه عمل می‌کنند حال آنکه کشورها بدون توجه به حجم هنگفت خسارات وارده به شکل انحصاری، جزیره ای، موردی و مقطعی با این جنایت مقابله می‌کنند اما چون برخی از کشورها هیچ تجربه‌ای در زمینه جنگ ناهمگون یا نامتقارن ندارند به همین جهت نمی توان از برچیده شدن قطعی تروریسم سایبری در حال و آینده مطمئن بود ضمن آنکه محرمانه بودن زیرساختهای اطلاعاتی کشورها و ملتها موضوع همکاری سایبری را کم رنگ کرده است و در نتیجه در فضای سایبری شاهد یک نوع شک و تردید و بی‌اعتمادی از سوی کشورها در زمینه تبادل اطلاعات و همکاری لجستیکی در زمینه جنگ با تروریست‌های سایبری هستیم (جعفری و توتونچیان، ۱۴۰۰، ص ۳۳۳- ۳۳۲)

مفهوم حمله مسلحانه در قضیه نیکاراگوئه که راجع به شکایت نیکاراگوئه علیه آمریکا در سال ۱۹۸۴ بود در پاراگراف ۱۹۵ و ۸۸۷ رای دیوان بین‌المللی دادگستری تعریف شد همینطور در پاراگراف ۲۴۲ رای دیوان در قضیه سرنگونی هواپیمای کره جنوبی و در قضیه خلیج تونکن در پاراگراف ۹۰۱ راجع به حملات مسلحانه دیوان به طور صریح نظر داد (Harris, 1998, P. 898- 899).

۳.ترمینولوژی صلاحیت، فضای مجازی و تروریسم سایبری

واژه تروریسم برای اولین بار بعد از انقلاب کبیر فرانسه در سالهای ۱۷۹۴-۱۷۹۳ از سوی ژاکوبن‌ها مطرح شد که مخالفین انقلاب را با گیوتین اعدام می‌کردند و بیانگر آغاز یک تروریسم دولتی بود که با خشونتی غیرقابل و صف برعلیه مردم بی‌دفاع

---

1 - Territorial Principle
2 - Protective principle

ارتکاب می‌یافت که در واقع یک نوع قتل سیاسی بحساب می‌آمد که با گرو گانگیری و آدم ربایی نیز توام میشد که بعدها از سوی دیگر تبهکاران نیز به صورت مکرر تکرار شد و هنوز هم ادامه دارد (Friedlander, 1986, P. 371).

واژه تروریسم سایبری یا سایبر تروریسم برای اولین بار در سال ۱۹۸۰ تو سط باری کالین[1] بکار رفت و دنینگ[2] جامعترین تعریف را از سایبر تروری سم بع مل آورده به این ترتیب که «سایبر تروریسم، حاصل تلاقی تروریسم و ف ضای م جازی ا ست». در این نوع تروریسم، شاهد وقوع حم له یا تهد ید جدی به کامپیوتر ها، اطلا عات و سیستم‌های کامپیوتری ه ستیم که تروری ست‌های م هاجم ق صد به زا نو درآوردن دولتها یا شهروندان یک کشور را دارند در ج هت تح قق ا هداف مخت لف سیا سی یا اجتماعی خاص. وجود خشونت علیه اموال یا ا شخاص و ه مین طور ای جاد ر عب و وح شت عنا صر ت شکیل ده نده ا ین جنا یت میبا شند از جم له سقوط هواپیما های مسافربری، آلوده سازی آبهای شهری یا دیگر خسارات هنگفت اقتصادی. در این نوع تروریسم زیرساخت‌های حیاتی کشور آسیب دیده و ک شور از پا یه و یران می شود (نمایان، ۱۳۹۲، ص ۱۲).

تروریسم یک تهدید جهانی بوده و آثار آن از سطح ملی فراتر رف ته ا ست. ج هانی شدن موجب تغییر رفتار و عملکرد تروریست‌ها نیز شده و آن ها با تجه یز خود به کامپیوترها و مهارت‌های تخصصی این بار زیر ساختهای ح یاتی ک شورها را هدف قرار می‌ده ند و نگرا نی ع مده ک شورها ام کان د ستیابی تروری ست‌ها به تجه یزات هسته‌ای است یا اینکه کنترل سیلوهای ه سته‌ای را از راه دور در د ست بگیر ند و با قطع سیستم خنک سازی سیلوها آنها را به انفجار سوق دهند مانند سهل انگاری هایی که در انفجار هسته‌ای چرنوبیل شاهد آن بودیم یا اینکه حملات تروریستی خود را با کمک از تسلیحات بیولوژیک یا شیمیایی توأم سازند. آنچه که بیش از همه آزار ده نده ا ست روش های نوینی ا ست که تروری ست‌های سایبری هر روز به آن متو سل می‌شوند که برای خود دولتها نیز تازگی داشته و آن ها را غافلگیر می‌ک ند و می‌توا ند یک وضعیت تکان دهنده در دنیا پد ید آورد و جا لب اینکه بر خی از ک شورها ه نوز خ طرات تروری سم سایبری را جدی نگرفته‌ا ند و چون تعر یف جامعی از جنا یت تروریسم سایبری وجود ندارد ارتکاب این جنایت متوقف نمی‌شود.

انگیزه بسیاری از حملات تروریستی سایبری، سیاسی بوده و به خ شونت عل یه اهداف غیرنظامی منجر می‌گردد. در این نوع حملات امنیت فیزی کی و اقت صادی یک جا صدمه می‌بیند و اعاده اطلاعات از دست رفته از سوی تروریست‌ها، گاهی غ یرممکن

1- Barry Colin
2- Denning

می‌گردد به ویژه که اگر یک نسخه پشتیبان از اطلاعات نداشته با شیم (هـ مان، ص ۱۶ تا ۱۴).

البته امکان دارد که تروریست‌های سایبری اهداف غیرسیاسی نیز داشته باشند که از طریق هک کردن، کاربرد غیرمجاز کامپیوترها و استفاده از پالس بمب (بمب ایمیلی) اهداف تروریستی خود را تعقیب می‌کنند و اصولاً برای این مجرمین سایبر تروریـ سم بر حـ ملات فیزیـ کی و سنتی تروریـ ست‌ها ترجیح دارد چون هم از راه دور اذ جام می‌شود و هم کم هزینه بوده و امکان دـ ستگیری بـ سیار ضعیف ا ست و آ سیب‌های وارده بسیار وسیع و هولناک است (قاسمی و باقرزاده، ۱۳۹۴، ص ۲۳۳– ۲۳۲).

مرکز مطالعات استراتژیک و بین‌المللی آمریکا از قول یک مـ قام عالی رتـ به ا علام کرد که یک تروریست سایبری قادر است با صرف یک میلـ یارد دلار هزیـ نه و ۲۰ نـ فر متخصص کامپیوتر کشور آمریکا را ورشکست نماید و به زانو در آورد. البـ ته گاهی ترور مقامات سیاسی یا گروگانگیری هم می‌توا ند دا خل در عملـ یات تروریـ ست‌های سایبری قرار بگیرد اما تخریب سامانه‌ها بـ سیار ناگوار و آ ثار مـ خرب آن می‌توا ند سالها باقی بماند (فتحی و شاهمرادی، ۱۳۹۶، ص ۸).

حقوق بین‌الملل به صراحت به تعر یف جـ نگ و حملـ له مـ سلحانه پرداخـ ته و ا علام داشته که در هر دو آنها شاهد کاربرد سلاح توسط نیروهای مسلح هـ ستیم که بـ ند ۴ ماده ۲ منشور آن را منع کرده ا ست با ا ین حال فـ قط در صورت تـ کرار یا شدت صدمات وارده از سوی تروریستهاست که می‌توان حـ ملات تروریـ ستی را یک حملـ له مسلحانه تلقی کرده و به مقابله با آن پرداخت (PARTSCH, 1982, p.25).

گروه‌ها یا شبکه‌های زیرزمینی در اکـ ثر موارد عا مل اذ جام حـ ملات تروریـ ستی سایبری هستند که هم از سوی دولتهای محل اقامت و هم کشور متبوعه تـ حت تعقـ یب هستند. در این گونه حـ ملات سیـ ستم‌ها و اطلا عات مو جود در آن به شدت آ سیب می‌بیند که این نوع مزاحمت ها به شهروندان و کـ شورها خـ سارت هنگفـ تی را وارد می‌کند. حمله‌ای که با ایـ جاد ر عب و وحـ شت از طر یق کامپیوتر ها توأم با شد یک تروریسم سایبری تلقی خواهد شد (بشارتی، ۱۳۹۸، ص ۶–۵).

هم اکنون بالاترین میزان خطر از سوی تروریست‌های سایبری آن ا ست آذ ها به سلاح‌های هسته‌ای و انواع بمب‌ها دسترسی پیدا کنند و یا کنـ ترل و شلیک سلاح‌های شیمیایی و بیو لوژیکی را در د ست بگیر ند (ضیائی پرور، ۱۳۸۶، ص ۳۵) و ا ین موضوع می‌تواند یک خطر جدی برای همه کشورها تلـ قی شود در عین حال تجر به ثابت کرده که تروریست‌ها، گروه‌هایی خود سر و غیرقابل کنترل هـ ستند که تذ ها به منافع خود و خشونت علیه دیگران می‌اندیشند و از هر نوع اخلاقـ یات اذ سانی فا صله می‌گیرند. علاوه از آن اگر کشورها با تعامل و همـ کاری به مقابلـ له با تروریـ ست‌های

سایبری مبادرت نورزند و از انجام تعهدات بین‌المللی ضد تروریستی سازمان ملل متحد اجتناب کنند دیر یا زود خودشان نیز با قطع اینترنت و حملات سایبری از سوی تروریست‌ها دچار مشکلات اقتصادی و اجتماعی خواهند شد و برای رهایی از این معضلات باید هزینه‌های سنگینی را متقبل شوند و مصائب بسیاری را متحمل گردند.

مفاد قطعنامه‌های شورای امنیت سازمان ملل متحد و مجمع عمومی بهترین تکنیک‌های سیاسی و حقوقی مقابله با تروریست‌ها و سرکوب آنها را مشخص کرده است که در صورت حمایت از سوی کشورهای جهان تروریستهای سایبری سرکوب شده و دنیا از شرارت آنها نجات خواهند یافت زیرا حملات تروریستهای سایبری می‌توانند بشریت را به عصر حجر سوق دهد و فقر و فلاکت را برای شهروندان دهکده جهانی به ارمغان بیاورد آثاری که مشابه آن را در جنگ‌های جهانی اول ۱۹۱۴ تا ۱۹۱۸ و جنگ جهانی دوم ۱۹۴۵ تا ۱۹۳۸ شاهدش بوده‌ایم.

٤. چالش‌های صلاحیت جهانی در مقابله با تروریسم سایبری

با توجه به این حقیقت که تروریسم سایبری نوع جدیدی از جرایم و اعمال تروریستی می‌باشد فلذا از نظر تشخیص صلاحیت جهانی برای مقابله با آن شک و تردید وجود دارد و ادبیات حقوقی در این زمینه بسیار ضعیف است برخی از کشورها تروریسم را از نظر حقوق کیفری تابع صلاحیت سرزمینی تعریف می‌کنند اما در مورد تروریسم سایبری قضیه کاملاً فرق می‌کند. تشخیص محل ارسال پیام‌های تخریبی سایبری از سوی تروریستها برای همه کشور یکسان نیست و تجهیزات فنی و مهارت و تخصص ویژه‌ای را می‌طلبد آیا می توان محل قرار گرفتن کامپیوترهای تروریست‌ها را مبنای صلاحیت قرارداد یا اینکه باید به زنجیره‌ای از حوادث اشاره کرد که در نهایت به تروریسم سایبری منجر شده است از سوی دیگر بر خلاف برخی از کشورها مانند آمریکا و انگلیس که صلاحیت سرزمینی خود را گسترش داده‌اند نمی‌توان از این نوع صلاحیت به طور موسع استفاده یا به آن استناد کرد زیرا موازین حقوق بین‌الملل گسترش صلاحیت کیفری سرزمینی را تخلف محسوب کرده و آن را مسئولیت‌آور قلمداد می‌کند.

در عین حال مبارزه با تروریست‌ها نیز باید بر مبنای قوانین و مقررات حقوق بین‌الملل و رعایت موازین حقوق بشر باشد و همکاری دولت‌ها برای پایان دادن به تروریسم سایبری به لحاظ ارتباطات اینترنتی ضرورتی غیرقابل انکار است در تبادل اطلاعات و هم در دستگیری، هم استرداد، تحویل مدارک و مجازات آنها چرا که مقابله با تروریسم واجد یک نفع مشترک برای همه کشورها و ملت‌های عضو دهکده جهانی است.

تروریسم سایبری واقعاً یک جرم علیه صلح و امنیت بشری است هر چند که چالش‌های حقوقی آن هنوز مرتفع نشده است شرط موفقیت مبارزه با جنایات تروریستی سایبری داشتن روحیه همکاری قضائی و استرداد مجرمین است و پیچیدگی‌های حقوقی اعمال صلاحیت کیفری دولت ها باید هر چه سریعتر بر طرف شوند؛

البته مشکل جمع‌آوری مدارک مثبته جرم تروریسم سایبری از دیگر معضلات صلاحیتی محاکم قضائی است با این حال جنایت تروریسم سایبری و صف و ماهیت بین‌المللی دارد و دستگیری و محاکمه و مجازات تبهکاران در آینده نزد یک جزو خواسته‌های به حق جامعه بین‌المللی خواهد شد در این زمینه می توان به ماده ۱۰۳ منشور سازمان ملل متحد[1] نیز استناد جست زیرا تروریسم سایبری هم یک جنایت شدید محسوب می‌گردد و هم یک جنایت مهم بین‌المللی (صالحی، ۱۳۹۸، ص ۱۹۸-۱۹۷). مقابله با تروریست‌ها قطعاً یک تعهدات عام الشمول نسبت به جامعه بین‌المللی است که یادآور حمایت از ارزشهای عالی بشری است که اجازه تخلف از آن به هیچ کشوری داده نشده است که در رای دیوان در قضیه بارسلونا تراکشن در سال ۱۹۷۰ به آن اشاره و تصریح شد (Ragazzi, 1997, p.20).

تروریسم ویژگیهای خاصی دارد [2] و سایبری قادر است که عامل و قوع جنگ های اطلاعاتی یا شبکه‌ای یا هسته‌ای و حتی بیولوژیکی باشد و امنیت داخلی و خارجی هر کشوری را در هر نقطه از جهان به خطر بیندازد اما سطح متفاوت پیشرفت سایبری کشورهای توسعه یافته و در حال توسعه موضوع تشخیص تروریست‌های سایبری و نوع صدمات وارده به کشورها و ملل را با چالش مواجه ساخته است برای مثال

---

۱ – ماده ۱۰۳ منشور: در صورت تعارض بین تعهدات اعضای ملل متحد به موجب این منشور و تعهدات آنها بر طبق هر موافقت نامه بین المللی دیگر تعهدات آنها به موجب این منشور مقدم خواهد بود (کمالان، ۱۳۹۸، ص ۱۲۴)

۲. برای مطالعه بیشتر ر.جوع شود: میربد، لیلا و سلیمی، صادق و نیاورانی، صابر و زمانی، سیدقاسم، «تروریسم سایبری: نقض حقوق بشر و آزادی های بنیادین»، فصلنامه حقوق پزشکی، ویژه نامه حقوق بشر و شهروندی، شماره ۶، ۱۳۹۸. میرعباسی، سیدباقر وکورکی نژاد قرایی، مجید، «قابلیت تحقق سایبر تروریسم و ارتباط آن با حق ذاتی دفاع مشروع مقرر در ماده ۵۱ منشور سازمان ملل متحد»، فصلنامه مطالعات حقوق عمومی، دوره ۴۸، شماره ۲، تابستان ۱۳۹۷. خلف رضائی، حسین، «حملات سایبری از منظر حقوق بین الملل (مطالعه موردی: استاکس‌نت) »، فصلنامه مجلس و راهبرد، سال بیستم، شماره ۷۳، بهار ۱۳۹۲. زرگان، جمیل و دهنوی، جلیل، «تهدیدات امنیتی بیوتروریسم و راههای مقابله با آن با رویکرد پدافند غیرعامل»، فصلنامه پژوهشهای حفاظتی- امنیتی دانشگاه جامع امام حسین (علیه السلام) ، سال پنجم، شماره‌ی ۱۹ (پاییز ۱۳۹۵). اصلانی، جبار و رنجبریان، امیرحسین، «بررسی تطبیقی و تحلیل تعریف حمله سایبری از منظر دکترین، رویه کشورها و سازمانهای بین المللی در حقوق بین‌الملل»، فصلنامه تحقیقات حقوقی شماره ۷۱، ۱۳۹۴.

کشور فقیری مانند سومالی امکاناتی برای شنا سایی، تعق یب و محاک مه و م جازات تروریست‌های سایبری ندارد حال آنکه کشور انگلیس یا آمری کا یا چین به سرعت می‌توانند به این نوع حملات خصمانه تروری ستی وا کنش سایبری ن شان دهـ ند و در زمینه اعمال صلاحیت ن یز از قوانین فرا مرزی خود ا ستفاده کرده و تبهـ کاران را دستگیر و مجازات نمایند و اساساً نیازی به اعمال صلاحیت جهانی ندارند زیرا آن ها قوانین داخلی خود را با تفسیر موسع به شکل جهانی اعمال می‌کنند که این هم اع طای ویژگی جهانی بودن حقوق کیفری به قوانین کیفری کشورهای مقتدر ج هان ا ست که قطعاً خلاف موازین حقوق بین‌الملل است (عیوضی و داداشی چکان، ۱۳۹۸، ص ۵۴).

اصولاً مقابله با تروریست‌های سایبری باید با شیوه‌های خاصی اند جام شود که نمی‌توان به آن عنوان جنگ داد بلکه نوعی واکنش دفاعی است که هدف آن سرکوب تروریست هاست چون هیچ نقطه‌ای از جهان را نمی‌توان مشمول منط قه آزاد حـ قوق بشری قلمداد کرد بنابراین با رعایت موازین حقوق بشر، تشخیص و تع یین صلاحیت قضائی حاکم بر دستگیری و محاکمه و مجازات تروریست‌های سایبری باید با نظارت قضایی سازمان ملل متحد باشد خواه صلاحیت مدنظر صلاحیت سرزمینی با شد یا صلاحیت جهانی که خوشبختانه تجربیات حقوقی جامعه بین‌المللی ن شان می‌د هد که جهان امروز به تدریج به سوی پذیرش صلاحیت ج هانی حـ تی در زمی نه مـ بارزه با تروریسم سایبری حرکت می‌کند (هافمن، ۱۳۸۵، ص ۱۳۹- ۱۳۸).

شورای امنیت سازمان ملل متحد با صدور قطعنامه‌های چـ ندی به ت شریح شیوه مقابله با تروریست‌ها پرداخ ته که مـ سدود کردن مـ نابع مالی تروری ست‌ها ی کی از آنهاست و همین طور قطعنامه‌های شماره: ۱۲۶۷، ۱۳۳۳، ۱۳۶۳، ۱۳۷۳، ۱۳۷۷، ۱۳۹۰، ۱۴۵۲، ۱۴۵۵ که بین سال‌های ۱۹۹۹ تا ۲۰۰۳ صادر شده‌اند که دقی قاً در مورد تروریست‌های سایبری نیز مصداق اجرایی دارد زیرا هدف مشترک همه تروری ست‌ها اعم از سایبری یا غیرسایبری ای جاد ر عب و وحـ شت و اظ هار و جود و به زا نو در آوردن ملل و دول جهان است (طیبی فرد، ۱۳۸۴، ص ۲۶۴).

البته با یک نتیجه گیری منطقی می‌توان مطمئن بود که چه صلاحیت سرزمینی لحاظ شود و چه صلاحیت ج هانی، در هر حال می توان مط مئن بود که اکثر یت کشورها در تلاشند که به تروریسم سنتی و تروریسم سایبری در حد توان و ظرف یت خود پایان دهند و این موضوع با ک مک سازمان مـ لل متـ حد و ک شورهای پی شرفته می‌تواند تحقق یابد و جهان را از شرارت سایبری تروریست‌ها خلاص نماید.

۵.تعهدات بین‌المللی کشورها در مقابله با تروریسم سایبری

از هر زاویه‌ای به مو ضوع تروریـ سم بن گریم ملاحـ ظه خواهیم کرد که حـ قوق بین‌الملل تکالیف جدی را بر دوش کشورها برای مبارزه با انواع تروریـ سم نـ هاده ا ما در مورد تروریسم سایبری حقوق بین‌الملل غافلگیر شده و مصوبه‌ای برای مقابـله با آن ندارد. از آنجا که تروریسم، حقوق بشر را مخاطب قرار داده و حقوق بشر با نـ ظم عمومی داخلی و بین‌المللی گره خورده است بنابراین می‌توان مطمئن بود که و جدان بشریت اجازه ارتکاب این اعمال را نمی‌دهد و باید با روش‌های قانونی نسبت به ا ین طاعون مدرن واکنش نشان داد.

بدین ترتیب از اینترنت می‌توان علیه تروریـ ست‌های سایبری ا ستفاده کرد و به شکل پدافند عامل و غیرعامل تمام حملات تروریستی آنها را خنثی و ناکام گذاشت اما شناسایی تروریست‌های سایبری باید با دقت و اعمال حاکمیت قانون به هـ مراه اد لـه کافی انجام شود تا مبارزه با تروریست‌های سایبری بهانه‌ای برای نقض حـ قوق بـ شر افراد بیگناه و قربانی توطئه تروریست‌ها نشود و حمایت قضائی از شهروندان بیگـ ناه می‌تواند اولین گام جدی در مقابله با تبهکاران سایبری باشند. تروریست‌های سایبری افراد متخصص در کار با کامپیوتر و شبکه‌ها هستند و کودن به حساب نمی‌آیـ ند ا ما از نظر حقوق جزا و جرمشناسی و موازین حـ قوق بین‌المـلل کج اندیـ شی، کـ جروی، توحش، نابودی و بدبینی را پیشه کرد ند که با واکنش های منا سب مقا مات صالح دولتها محـ کوم به شکـ ست ومـ جازات هـ ستند و ا ستیلای سایبری آن ها بر ز ندگی شهروندان و دولتها موقتی است و از این نکته غافلند که مـ نابع سخت ا فزاری و نرم افزاری کشورها توان حل مـ شکلات عظیم تر از تروریـ سم سایبری را دارد و هـ مین ظرفیت بالا در نهایت موجب دستگیری و کیفر آنها خواهد شد.

بنابراین دولتها باید با نظارت مستمر بر اینترنت و تعاملات مظنونین به تروریـ سم سایبری مانع از استخدام، بکارگیری، تربیت هکر و متوقف کردن حـ ملات تروریـ ستی در نطفه شوند ضمن آنکه باید نسبت به افزایش آگاهی های همـ گانی شهروندان هـ مه کشورها اقدام نمایند تا شهروند در دام عنکبوتی تروریست‌ها نیفتند.

علاوه از آن رعایت حقوق بشر باید با لحاظ منافع جمـ عی توأم گردد که در ا ین راستا توجه به ساز و کار پیـ شگیری، از اهمـ یت وا جد الو صفی بر خوردار ا ست. بنابراین جرم انگاری جرایم تروریستی سایبری گام بعدی در پایان دادن به تروریسم سایبری خواهد بود (قاسمی و باقرزاده، ۱۳۹۴، ص ۲۴۷ تا ۲۴۴).

شورای امنیت در قطعنامه ۱۳۷۳ از همه کشورها خوا ست که مانع تامین مالی اعمال تروریستی شده و آن را متوقف کنند همینطور مانع از عـ ضوگیری گروه های

تروریستی شوند و با تبادل اطلاعات به هشدار اولیه به سایر کشورها اقدام نمایند (Rosand, 2003, P. 335).

در فرازی دیگر از این قطعنامه آمده که اقدامات کشورها در اجرای قطعنامه ۱۳۷۳ شورای امنیت نباید به موازین بنیادین حقوق بین‌الملل صدمه وارد کند (Cassese, 2001, p. 993).

موضوع پیشگیری از جرم در قطعنامه‌های شماره ۱۹۹۵/۹ و ۲۰۰۲/۱۳ شورای اقتصادی و اجتماعی و همینطور قطعنامه شماره ۴۵/۱۱۲ سال ۱۹۹۰ مجمع عمومی سازمان ملل متحد به صراحت 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 محبوبی و نوری، ۱۳۹۹، ص ۱۵۵).

همینطور 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، ص ۱۶۶).

به نظر می‌رسد که مهم‌ترین مبنای تعهدات ضد تروریستی کشورهای عضو جامعه بین‌المللی اسناد بین‌الملل ذیل خواهند بود:

۱- کنوانسیون راجع به جلوگیری از اعمال غیر قانونی علیه امنیت هواپیمایی کشوری ۱۹۷۱ - ۲- کنواسیون جلوگیری از بمب گذاری تروریستی ۱۹۹۷- ۳- کنوانسیون سرکوب حمایت مالی از تروریسم ۱۹۹۹- ۴- کنوانسیون توکیو راجع به جرایم و برخی از اعمال ارتکابی دیگر در هواپیما ۱۹۶۳- ۵- اعلامیه راجع به اقدامات ناظر به امحای تروریسم بین‌المللی ۱۹۹۴- ۶- کنوانسیون اروپایی مقابله با تروریسم ۲۰۰۹ -۷- کنوانسیون سازمان ملل همکاری‌های منطقه‌ای آسیای جنوبی ۱۹۸۷- ۸- کنوانسیون سازمان کنفرانس اسلامی در زمینه مبارزه با تروریسم بین‌المللی ۱۹۹۹- ۹- معاهده همکاری میان دولت های عضو کشورهای مستقل مشترک المنافع در مبارزه با تروریسم ۱۹۹۹ - ۱۰- کنوانسیون سازمان وحدت آفریقا درباره پیشگیری و مبارزه با تروریسم و پروتکل الحاقی به آن ۲۰۰۴ و ۱۹۹۹- ۱۱- کنواسیون عربی مقابله با تروریسم ۱۹۹۸- ۱۲- توصیه نامه‌ها و کنواسیون جرایم سایبر شورای اروپا ۲۰۰۱؛ ۱۳- کنوانسیون سازمان کشورهای آمریکایی راجع به پیشگیری و مجازات اعمال تروریستی ۱۹۷۱ (قدیر و کاظمی فرو شانی، ۱۳۹۸، ص ۲۵۸ تا ۲۴۷ با تلخیص).

شورای امنیت سازمان ملل متحد از همه کشورها می‌خواهد که اقدامات قانونگذاری و قضایی را برای پیشگیری از حوادث تروریستی اتخاذ نمایند و تروریست‌ها را دستگیر، محاکمه و مجازات کنند (Bantekas, 2003, P. 315).

به نظر می‌رسد که مهمترین تعهد منعکس در معاهدات بین‌المللی ضد تروریسم، جرم انگاری اینگونه اعمال در قوانین کیفری است و اینکه دولت‌ها 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 جنایت تروریسم و تروریسم سایبری دارد که با توسعه صلاحیت قضایی کشورها انجام خواهد شد (دونل، ۱۳۹۱، ص ۲۴۱– ۲۴۰).

در فراز بعدی به زمینه اعمال صلاحیت جهانی در مقابله با تروریسم خواهیم پرداخت و موانع و چالش‌های پیش روی اعمال صلاحیت جهانی در رابطه تروریسم سایبری را تشریح خواهیم نمود.

٦.ضوابط اعمال صلاحیت جهانی در مقابله با تروریسم سایبری

پذیرش تدریجی صلاحیت جهانی در هزاره سوم مدیون قوانین کیفری کشور اتریش است که در سال ۱۸۰۳ اعلام شد و دادگاه این کشور مترقی اروپایی صلاحیت رسیدگی به جنایات ارتکابی اشخاص غیرمتبوعه را در سرزمینی بیگانه نیز دارا شدند و شامل آن دسته از جرایمی می‌گردد که همه کشورها از آن اظهار بیزاری جسته و آن را جرم می‌شناسند مانند نسل کشی یا دزدی دریایی و تجارت برده که این نوع رسیدگی بعدها از سوی مقامات قضایی انگلیس نیز پذیرفته شد و صلاحیت جهانی وارد نظام حقوقی کامن لا گردید که البته اکنون جرایم دیگری نیز به این مقوله پیوسته‌اند و قلمرو اعمال صلاحیت قضایی جهانی در حال گسترش است.

جلوگیری از بی‌کیفری و تلقی اعمال ناشایست به عنوان جرایم خطیر بین‌المللی انگیزه پذیرش اصل صلاحیت جهانی در میان کشورها بوده و هست که قطعاً با توجیهات حقوق بشری قابل پذیرش است. در خصوص اعمال صلاحیت این نکته حائز اهمیت است که مهمترین شرط اعمال این اصل، حضور و دستگیری متهم در کشور محل وقوع دادگاه رسیدگی کننده است همین طور شرط رفتار متقابل قانونی و سیاسی و یا شکایت شاکی و تقاضای پیگرد از سوی دولت زیان دیده می‌تواند زمینه ساز اجرای اصل صلاحیت جهانی باشد. اساساً زیربنای اعمال اصل صلاحیت

جهانی، رفتار و اعمال مغایر با قانون اخلاق جهانی ا ست که تو سط م جرم ذ قض و مختل گردیده است و در نتیجه اعمال و رفتار او نظم جهانی برای مدت ا ندکی مخ تل شده است. بعبارت دیگر اصل صلاحیت جهانی ناظر بر تصمیمات م لل مت مدن ج هان است که از بی‌نظمی گریزان بوده و ثبات و حاکمیت قانون را می‌طل بد و اع مال ا صل صلاحیت جهانی کاملاً در راستای تحقق و پاسداری از عدالت کیفری گام بر می‌دارد (حسینی نژاد، ۱۳۷۳، ۸۹ تا ۸۵).

شورای امنیت بلافاصله بعد از حادثه ۱۱ سپتامبر قطعنامه ۱۳۷۳ را صادر کرد که لحن کاملاً جهانی (اعمال صلاحیت جهانی) داشت و شورا تروریسم را تهد یدی جدی علیه صلح اعلام نمود و انواع تحریم‌ها را عل یه تروری ست‌ها ب کار ب ست و دولت ها را ملزم کرد که تعهدات الزام آوری در رابطه با تروریسم را بجا آور ند و دولت ها ا جازه دارند که برای دفاع از خود در قبال تروریسم متوسل به زور در قا لب ح قوقی د فاع مشروع موضوع ماده ۵۱ منشور شوند بدین ترتیب سرکوب تروریست‌ها شکل جدی تری به خود گرفت.دولت ها متع هد شدند که تروری سم را جرم اذ گاری نمای ند و در صورت محکومیت حتماً مجازات‌ها را به مرحله اجرا در آورند. از سوی دی گر دولت ها مکلفند که به پیشگیری از انجام حملات تروریستی مبادرت ورز ند و ت مام م سیرهای مدنظر تروریست‌ها را مسدود نمایند (شهریاری و یعقوبی، ۱۳۹۱، ص ۲۵۹).

مهمترین دلیل حمایت از اعمال صلاحیت جهانی در راب طه با تروری سم سایبری، همانا حمایت از حقوق بشر است که حملات سایبری تروریست‌ها می‌توا ند ارز شهای حقوق بشری را به خطر بیندازد و این ارزشها در سه نسل حقوق مدنی و سیا سی و حقوق اقتصادی، اجتماعی و فرهنگی و حقوق جمعی تج لی یافته‌ا ند (ذاکر یان، ۱۳۸۱، ص ۶۷).

اساساً یکی از دلایل تنفر جهانیان از تروریسم و تروریسم سایبری، ح ملات آذ ها به غیرنظامیان است که با اهداف سیاسی انجام می‌شود و دلیل آن هم ا ین ا ست که قتل عام غیرنظامیان می‌تواند به راحتی منجر به هرج و مرج در ک شور قر بانی گردد. البته مخاطب خشونت می‌تواند دولتها نیز باشد ا ما امکا نات و آ مادگی دولت ها برای تحمل چنین حملاتی آسیب‌پذیری آنها را کاهش می‌دهد (عبدالهی، ۱۳۹۱، ص ۱۸۹).

برای اعمال صلاحیت جهانی در رابطه با مقاب له عل یه تروری سم سایبری و حدت رفتار های قانوذ گذاری و ق ضایی ک شورها ضرورتی انکارنا پذیر ا ست و هم کاری کشورها تنها رهنمود صحیح برای مقابله با تروریسم سایبری در حال و آینده خواهد بود.

۷.موانع اعمال صلاحیت جهانی در مقابله با تروریسم سایبری

علی الاصول موضوع صلاحیت جهانی بیشتر ناظر بر جرایم هولناک حقوق بشری است اما موانع بسیاری در پیگرد و محاکمه و مجازات جنایتکاران تروریست سایبری وجود دارد که اهم آنها عبارت‌اند از:

یک. فقدان قوانین ملی و بین‌المللی کیفری و حقوقی راجع به مقابله با تروریست‌های سایبری؛

دو. فقدان سازو کارهای تخصصی که قادر به همکاری و هماهنگی تدابیر کیفری بر علیه تروریست‌های سایبری باشد؛

سه. وجود انواع مصونیت‌های و معافیت‌های کیفری از جمله لحاظ نمودن موقعیت و مقامات رسمی؛

چهار. صدور عفو های مکرر از سوی دولت های نو پا، ضعیف و ناتوان برای استقرار و تثبیت بهتر حاکمیت خرد؛

پنج. معضل مربوط به جمع آوری ادله اثبات جنایات تروریسم سایبری؛

شش. فقدان نظارت‌های بین‌المللی کارآمد جهت ارزیابی نحوه تعقیب، محاکمه و مجازات تروررست‌های سایبری (کامینگا، ۱۳۸۲، ص ۹۶ تا ۸۱ با تلخیص).

جامعه بین‌المللی هنوز موفق نشده که تعاملی میان صلاحیت قانونگذاری و صلاحیت قضایی کشورها در زمینه محاکمه و مجازات تروریست‌های سایبری ایجاد کند. سوال کلیدی آن است که کدام قانون دستگیری، محاکمه و مجازات تروریست‌های سایبری را تجویز می‌کند و کدام دادگاه در این زمینه صلاحیتدار است: دادگاه های بین‌المللی، دادگاه های ویژه بین‌المللی، دادگاه های محل دستگیری تروریستها، دادگاه محل وقوع جرم یا دیوان کیفری بین‌المللی. در عین حال از وحدت نظام‌های حقوقی در زمینه حقوق کیفری فرامرزی خبری نیست برای مثال مجازات اعمال تروریستی در کشوری حبس ابد است و در کشوری دیگر اعدام.

این تعارض چگونه باید حل شود به ویژه که مجرم تروریست تبعه کشوری باشد که مجازات اعدام را لغو کرده و مجرم در کشوری دستگیر شده که مجازات اعدام را با قاطعیت تمام اجرا می‌کنند چگونه باید تعیین تکلیف کرد؟

از سوی دیگر ملاحظات سیاسی به طور مستمر بر محاکمه تروریست‌های سایبری سایه افکنده و بلوک بندی کشورهای ابرقدرت شرق و غرب خط بطلان بر وحدت نظام‌های حقوقی و کیفری کشیده است در حالی که بر خی از جرایم هولناک حقوق بشری از دید همه کشورها و ملت‌ها قابل نکوهش، سرزنش و مجازات است که تروریسم سایبری تنها یکی از صدها جنایت بین‌المللی در حال وقوع است (حسینی نژاد، ۱۳۷۳، ص ۹۴).

جرایم تروریستی قطعاً همه ملاک های نقض حقوق بشر را دارا می‌باشد در صورتی که کشوری قربانی تروریست‌های سایبری شده می‌تواند از دیوان کیفری بین‌المللی درخواست مداخله و رسیدگی کیفری نماید با لحاظ ماده ۵ اساسنامه دیوان کیفری بین‌المللی هر چند که تروریسم صریحاً در اساسنامه دیوان تعریف نشده اما بسیاری از جنایات تروریست‌های سایبری می‌تواند هم جنایت ضد بشریت خطاب شوند و هم جنایت جنگی (رزمخواه، ۱۳۹۷، ص ۹۱).

البته باید در اصلاحات بعدی اساسنامه دیوان موضوع صلاحیت ذاتی و موضوعی دیوان در رابطه با تروریسم و تروریسم سایبری لحاظ شود تا دیوان صلاحیت رسیدگی به این جنایت را داشته باشد و ظاهراً هنوز با پذیرش بین‌المللی اصل صلاحیت جهانی فاصله بسیاری داریم (میرمحمد صادقی، ۱۳۸۷، ص ۹۹).

با توجه به اینکه بسیاری از کشورهای مقتدر جامعه بین‌المللی با عدم تعریف نهادهای حقوقی مانند تجاوز، تروریسم، جنبش‌های آزادی بخش و قواعد آمره حقوق بین‌الملل و تعهدات عام الشمول حقوق بین‌الملل مخالفند فلذا نباید انتظار داشت که در آینده نزدیک موضوع صلاحیت جهانی در موضوع جنایات شدیدی مانند تروریسم و تروریسم سایبری پذیرفته شود اما این حقیقت نمی‌تواند بهانه‌ای برای استمرار تلاش برای به کرسی نشاندن صلاحیت جهانی در آینده نزدیک باشد. موفقیت جامعه بین‌المللی در اعمال صلاحیت جهانی در گذشته می‌تواند الگویی برای تثبیت و پذیرش جنایاتی مانند تروریسم سایبری در حوزه صلاحیت جهانی در آینده باشد و چنین نیز خواهد شد زیرا نمی‌توان پذیرفت که کشوری یا دولتی از اینکه مخاطب رعب و وحشت تروریست‌های سایبری باشد استقبال کند و این نقطه قوت برای استقرار صلاحیت جهانی در حقوق بین‌الملل کیفری در آینده نزدیک خواهد بود.

نتیجه و پیشنهاد

با پذیرش این موضوع تروریسم سایبری چه به صورت موردی و چه به شکل مکرر حاکی از وقوع نوعی جنگ با ابعاد کوچکتر علیه کشورها و ملت هاست فلذا ضرورت دارد کشورهای عضو دهکده جهانی با رعایت همه انواع صلاحیت‌های قضایی محاکم داخلی و بین‌المللی – اعم اصل صلاحیت حمایتی، صلاحیت بر مبنای تابعیت و صلاحیت سرزمینی و صلاحیت تکمیلی – به مقابله جدی با تروریست‌های سایبری مبادرت ورزند و در موارد لزوم به صلاحیت جهانی محاکم قضایی بین‌المللی نیز متوسل شده و به بی‌کیفری تروریست‌های سایبری پایان دهند و به دفاع مشروع نظامی و سایبری متوسل شده و این شرارت سایبری را متوقف سازند زیرا فضای مجازی یادآور یک انقلاب نوین تکنولوژیکی است. هر چند مزایای

بسیاری برای بشریت دارد اما شرط آن، این است که به شکل صحیح از آن ا ستفاده شود و حاکمیت قانون و م حاکم ق ضایی را در ا ین ف ضای شبه کهک شانی بر قرار سازیم.

بنابراین، پیشنهاد تحقیق، تصویب دستورالعمل تالین ۲ و ۱ توسط سازمان پی مان آتلانتیک شمالی (ناتو) برای مقابله با جنگ سایبری و حملات م شابه، هر چ ند او لین گام موفقیت‌آمیز در این مسیر است اما پذیرش اصل صلاحیت ج هانی برای م حاکم قضایی بین‌المللی و همکاری جدی و توأم با قاطعیت کشورها با هم در ا ین خ صوص امری ضروری است.

فهرست منابع

۱. اصلانی، جبار و رنجبریان، امیرحسین (۱۳۹۴)، «بررسی تطبیقی و تحلیل تعریف حمله سایبری از منظر دکترین، رویه کشورها و سازمانهای بین‌المللی در حقوق بین‌الملل»، فصلنامه تحقیقات حقوقی شماره ۷۱. ۲۵۷-۲۷۸.

۲. بشارتی، محمدابراهیم (۱۳۹۸)، واکاوی جرم تروریسم سایبری از منظر حقوق و چالش‌های فرارو»، مجله علمی تخصصی انجمن علمی – پژوهشی فقه و حقوق قضایی، سال دهم، شماره ۱۴. ۱-۲۲.

۳. بعیدی نژاد، حمید و دریایی، محمدحسن و علی آبادی، مهدی (۱۳۸۴)، تحول در ساختار نظام ملل متحد، دفتر مطالعات سیاسی و بین‌المللی مرکز چاپ و انتشارات وزارت امور خارجه، تهران، چاپ اول.

٤. بیگی، جمال و احمدی سربرزه، مظفر و رحیمی، پوریا، (۱۳۹۸)، «تهدیدها و چالش‌های فضای مجازی و راهکارهای کاهش آن با پدافند سایبری»، دانشگاه آزاد اسلامی واحد مراغه، دومین کنفرانس ملی پدافند سایبری ۵ اردیبهشت. ص ۷۷۲-۷۵۶.

٥. ترابی، قاسم (۱۳۹۴)، «تکامل راهبرد ناتو در قبال جنگ سایبری، دلایل، ابعاد و مولفه ها»، فصلنامه مطالعات راهبردی، سال هجدهم، شماره اول، بهار . ص ۱۵۸-۱۳۳.

٦. جعفری، افشین و توتونچیان، مهری (۱۴۰۰)، «بررسی راه کارهای تحدید حملات سایبری از منظر حقوق بین‌الملل بشردوستانه»، ماهنامه حقوق شهروندی، شماره ۱۸، فروردین. ۳۵۱-۳۳۱.

۷. حسینی نژاد، حسینقلی (۱۳۷۳)، حقوق کیفری بین‌الملل، نشر میزان، تهران، چاپ اول.

۸. خلف رضائی، حسین (۱۳۹۲)، «حملات سایبری از منظر حقوق بین الملل (مطالعه موردی: استاکس‌نت) »، فصلنامه مجلس و راهبرد، سال بیستم، شماره ۷۳، ۱۲۵-۱۵۳.

۹. دونل، دانیل (۱۳۹۱)، «معاهدات بین‌المللی ضد تروریسم و اعمال تروریستی نیروهای مسلح در درگیری مسلحانه»، ترجمه پیمان نمایان و سبحان طیبی، ویژه نامه مجله حقوقی بین‌المللی، نشریه مرکز امور حقوقی بین‌المللی ریاست جمهوری، ۲۳۷-۲۶۲.

۱۰. ذاکریان، مهدوی (۱۳۸۱)، حقوق بشر در هزاره جدید، دانشکده حقوق و علوم سیاسی دانشگاه تهران، تهران، چاپ اول.
۱۱. زرگان، جمیل و دهنوی، جلیل (۱۳۹۵)، «تهدیدات امنیتی بیوتروریسم و راههای مقابله با آن با رویکرد پدافند غیرعامل»، فصلنامه پژوهشهای حفاظتی- امنیتی دانشگاه جامع امام حسین (علیه السلام) ، سال پنجم، شماره ۱۹، ۹۱-۱۱۰
۱۲. شهریاری، عبدالنعیم، و یعقوبی، اسماعیل، (۱۳۸۸)، «تهدید علیه صلح و امنیت بین‌المللی در رویه ی شورای امنیت با تاکید بر تروریسم»، سالنامه ایرانی حقوق بین‌الملل و تطبیقی، شماره پنجم، روزنامه رسمی کشور، تهران، چاپ اول. ۲۲۹-۲۶۹.
۱۳. صالحی، جواد (۱۳۹۸)، دسترسی به اطلاعات دیتاسنتر دولت خارجی در تقابل با اصول صلاحیت کیفری سرزمینی و اعمال حاکمیت در حقوق بین‌الملل»، مجله حقوق بین‌المللی، شماره ۶۰، ۱۵۸-۲۱۰.
۱٤. صلاحی، سهراب و کشفی، سیدمهدی (۱۳۹۵)، «جنگ سایبری از منظر حقوق بین‌الملل با نگاه به دستورالعمل تالین»، دو فصلنامه علمی- پژوهشی مطالعات قدرت نرم، سال ششم، شماره چهاردهم، ، ۲۸-۴۷.
۱۵. ضیائی پرور، حمید (۱۳۸۶). نظارت و اجرا موسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران، معاونت تولید، جنگ نرم۱: ویژه جنگ رایانه ای، انتشارات موسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران، تهران، چاپ دوم.
۱٦. ضیائی، سید یاسر و خلیل زاده، مونا (۱۳۹۲)، مسئولیت بین‌المللی دولت ناشی از حملات سایبری»، مجله پژوهش‌های حقوقی، شماره ۲۳، ۸۷-۱۱۲.
۱۷. طیبی فرد، امیرحسین، (۱۳۸۴)، «مبارزه با تامین مالی تروریسم در اسناد بین‌المللی»، مجله حقوقی، نشریه دفتر خدمات حقوقی بین‌المللی جمهوری اسلامی ایران، شماره سی و دوم، ۲۵۹-۳۰۵.
۱۸. عباسی کلیمانی، عاطفه و محبوبی، ملیکا و نوری، فاطمه (۱۳۹۹)، «راهبردهای نوین پیشگیری از وقوع تروریسم سایبری»، فصلنامه رهیافت پیشگیری از جرم، دوره ۳، شماره ۱، ۱۴۵-۱۷۲.
۱۹. عبدالهی، محسن (۱۳۹۱)، «چالش‌های مجمع عمومی سازمان ملل متحد در تدوین و توسعه حقوق مبارزه با تروریسم بین‌المللی»، در کتاب مجموعه مقالات همایش نقش مجمع عمومی سازمان ملل متحد در تدوین و توسعه تدریجی حقوق بین‌الملل دانشگاه تهران پنجم و ششم دی ماه ۱۳۸۹، انجمن ایرانی مطالعات سازمان ملل متحد، تهران، چاپ اول، ۱۸۷-۲۱۶.
۲۰. عیوضی، محمدرضا و داداشی چکان، محمدمهدی (۱۳۹۸)، «انواع تهدیدات در فضای سایبری و راهکارهای مقابله با آن»، دانشگاه آزاد اسلامی واحد مراغه، دومین کنفرانس ملی پدافند سایبری ۵ اردیبهشت، ۴۴-۵۹.
۲۱. فتحی، یونس و شاهمرادی، خیرالله (۱۳۹۶)، «تقابل حق حریم خصوصی اشخاص و امنیت ملی، در مقابله با تروریسم سایبری»، فصلنامه قضاوت، شماره ۱،۹۱-۲۴

۲۲. قاسمی، غلامعلی و باقرزاده، سجاد (۱۳۹۴)، جایگاه حقوق بشر در مبارزه با سایبر تروریسم، «مجله حقوقی بین‌المللی»، شماره ۵۲، ، ۲۲۷-۲۵۴.
۲۳. قدیر، محسن و کاظمی فروشانی، حسین (۱۳۹۸)، «بررسی تطبیقی حقوق کیفری ایران با اسناد بین‌المللی در زمینه مقابله و پیشگیری از وقوع تروریسم سایبری»، مجله حقوقی بین‌المللی، شماره ۶۰، ۲۳۷-۲۶۷.
۲٤. کمالان، سیدمهدی (۱۳۹۸)، منشور سازمان ملل متحد (انگلیسی به فارسی)، انتشارات کمالان، تهران، چاپ نهم.
۲۵. میربد، لیلا و سلیمی، صادق و نیاورانی، صابر و زمانی، سیدقاسم (۱۳۹۸)، «تروریسم سایبری: نقض حقوق بشر و آزادی های بنیادین»، فصلنامه حقوق پزشکی، ویژه نامه حقوق بشر و شهروندی، شماره ۶، ۲۲۴-۲۴۰.
۲٦. میرعباسی، سیدباقر وکورکی نژاد قرایی، مجید (۱۳۹۷)، «قابلیت تحقق سایبر تروریسم و ارتباط آن با حق ذاتی دفاع مشروع مقرر در ماده ۵۱ منشور سازمان ملل متحد»، فصلنامه مطالعات حقوق عمومی، دوره ۴۸، شماره ۲، ۲۶۱-۲۸۰.
۲۷. نمایان، پیمان (۱۳۹۲)، «مواجهه با تروریسم سایبری در حقوق بین‌الملل کیفری»، فصلنامه پژوهش‌های ارتباطی، سال بیستم، شماره (پیاپی ۷۳)، ۴۱-۹.
۲۸. هافمن، پل (۱۳۸۵)، «حقوق بشر و تروریسم»، ترجمه علیرضا ابراهیم گل، مجله حقوقی، نشریه مرکز امور حقوقی بین‌المللی معاونت حقوقی و امور مجلس ریاست جمهوری، شماره سی و چهارم، ۱۳۱-۱۵۵.

29. Bantekas, I. the International Law of Terrorist Financing, American Journal of International Law, vol. 97, 2003.
30. Cassese, A. Terrorism is also Disrupting some crucial categories of International law, European journal of international Law, vol. 12, November, 2001.
31. Friedlander, R.A. Terrorism, in: R. Bernhardt (ed.) Encyclopedial of public International Law [Instalment 9 (1986)].
32. Harris, D.J. Cases and Materials on International law, Fifth Edition, Sweet & Maxwell, London, 1998.
33. Partsch, K. J. ARMED CONFLICT, in: R. Bernhardt (ed.) Encyclopedial of public International Law [Instalment 3 (1982)].
34. Ragazzi, M. The concept of international obligations erga omnes, clarendon press, oxford, 1997.
35. 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.