



## مقابله با حملات تروریستی به زیرساخت‌های حیاتی یک کشور در قواعد حقوق بین‌الملل\*

اردشیر نعمت‌پور\*\* - دکتر مصطفی تقی‌زاده انصاری\*\*\*  
دکتر سکینه بیری گنبدی\*\*\*\*



This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

### چکیده

تروریسم در گذر زمان اشکال مختلفی به خود گرفته، اما جامعه حقوقی در سطح بین‌الملل همسو با این اشکال مدرن تروریسم حرکت نمی‌نماید و همواره یک یا چند گام عقب است. با توجه به اینکه زیرساخت‌های حیاتی مهمترین مجموعه‌های حیات بخش یک کشور هستند، حمله به آنها خسارات و آسیب‌های فراوان و بعضاً جبران‌ناپذیری وارد می‌کند تا از این طریق دولت هدف را وادار به پذیرش خواسته گروه‌های تروریستی نماید. حقوق بین‌الملل، اگر چه اسناد مهمی در زمینه مقابله با تروریسم در حوزه‌های هواپیمایی، ناوبری دریایی، هسته‌ای، گروگانگیری و... وجود دارد، اما خلاء یک سند بنیادین در زمینه مقابله با حملات تروریستی به زیرساخت‌های حیاتی یک کشور که هم حملات سایبری و هم فیزیکی را پوشش دهد، بسیار محسوس است. لذا این مقاله ضمن پرداختن به مسئله مهم زیرساخت‌های حیاتی و اسناد مربوط به مقابله با تروریسم، در پاسخ به سوال اصلی خود یعنی مقابله با حمله فیزیکی تروریستی به زیرساخت‌های حیاتی یک کشور تحت حاکمیت چه قاعده بین‌المللی قرار دارد می‌باشد. در این راستا از روش تحقیق تحلیلی-توصیفی با استفاده از ابزار کتابخانه‌ای بهره گرفته شده است. پس از بررسی این مقاله به این نتیجه رسیده است که در حقوق بین‌الملل برای مواجهه با حملات فیزیکی تروریست‌ها به زیرساخت‌های حیاتی کشورها خلاء قانونی وجود دارد و در نهایت تدوین و تصویب یک کنوانسیون بین‌المللی جهت مقابله با اینگونه حملات تروریستی پیشنهاد گردید.

**کلیدواژگان:** حملات تروریستی، زیرساخت‌های حیاتی، حمله سایبری، کنوانسیون‌های بین‌المللی

\* این مقاله برگرفته از رساله دکتری اردشیر نعمت‌پور با راهنمایی دکتر. مصطفی تقی‌زاده انصاری است.

\*\* دانشجوی دکتری حقوق بین‌الملل عمومی، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران.

\*\*\* نویسنده مسئول، استادیار گروه حقوق بین‌الملل، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران. ایمیل:

[mos.taghizadeh\\_ansari@iauctb.ac.ir](mailto:mos.taghizadeh_ansari@iauctb.ac.ir)

\*\*\*\* استادیار گروه علوم سیاسی و روابط بین‌الملل، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران.

## مقدمه

از دیرباز تا به امروز نگرش‌ها نسبت به تروریسم و مقابله با آن تغییرات زیادی داشته است. در حقوق بین‌الملل اقدامات مناسبی جهت مقابله با حملات تروریستی صورت گرفته است. کشورها در سطح بین‌المللی با هم به این توافق رسیده‌اند که برای مقابله با تروریسم و آثار زیانبار آن باید با یکدیگر همکاری نمایند. سازمان ملل کنوانسیون‌های مختلفی را برای مقابله با تهدید و حملات تروریستی در ابعاد مختلف حیات دولت‌ها تدوین و تصویب نموده است. اما آنچه نگارنده را ترغیب و تشویق به قلم فرسایی و پژوهش در این زمینه نمود، وجود خلاء حقوقی و تحقیقاتی در زمینه مقابله با حملات تروریستی به زیرساخت‌های حیاتی یک کشور است.

این پژوهش حملات تروریستی سایبری<sup>۱</sup> به زیرساخت‌های حیاتی<sup>۲</sup> یک کشور را تحت حاکمیت اسناد مختلف بین‌المللی یافت که بخشی از فقدان قدرت حقوقی بین‌المللی جهت تنظیم همکاری میان دولت‌ها<sup>۳</sup> را جبران می‌کند، اما دغدغه اصلی پژوهش حاضر نبود کنوانسیون و یا سند جامع و منحصر بفردی در خصوص مقابله با حملات فیزیکی تروریستی به زیرساخت‌های یک کشور است. بر این اساس، با بررسی اسناد موجود سعی بر این است که مفاد و قواعد قابل اعمال در زمینه حملات تروریستی به زیرساخت‌های حیاتی یک کشور بررسی شود و از این رهگذر به خلاءهای حقوقی موجود که زمینه شانه خالی کردن کشورها و گروه‌های تروریستی از مسئولیت حملات فیزیکی به زیرساخت‌های حیاتی دیگر کشورها را فراهم می‌آورد، رهنمون گردد. لذا سوال اصلی عبارت است از مقابله با حمله تروریستی به زیرساخت‌های یک کشور تحت حاکمیت چه قاعده بین‌المللی قرار دارد؟ فرضیه‌ای که نگارنده برای این پژوهش متصور است این است که به نظر می‌رسد که حقوق بین‌الملل در راستای مقابله با تهدیدات تروریستی قواعد مختلفی را در قالب قطعنامه و کنوانسیون‌های متعدد وضع نموده است اما در خصوص حملات تروریستی به زیرساخت‌های حیاتی یک کشور همچنان خلاء وجود دارد. در این راستا مقاله حاضر پس از پرداختن به پیشینه تحقیق مبانی نظری را مورد کنکاش قرار می‌دهد تا بتواند مطالب و اهداف مورد نظر خود را بطور شایسته تبیین و قابل درک نماید. در بخش بعد مقاله به مبحث اهداف و مصادیق زیرساخت‌های حیاتی پرداخته می‌شود و نهایتاً قواعد و اسناد موجود در حقوق بین‌الملل که حملات تروریستی به زیرساخت‌های حیاتی یک کشور را ملحوظ نظر قرار داده‌اند، ارائه می‌شود.

## ۱- پیشینه تحقیق

لئوپولد کروسزکا و همکاران در کتاب مجموعه مقالات خود «حفاظت از زیرساخت‌های

<sup>۱</sup>. Cyber Terrorism Attacks

<sup>۲</sup>. Critical Infrastructures

<sup>۳</sup>. States cooperation

حیاتی» (۲۰۲۱) به ابعاد مختلف این مسئله مهم پرداخته‌اند. در این کتاب بر روشهای نوآورانه و جدیدی برای حفاظت از زیرساخت‌های حیاتی را تاکید شده که از جمله آن استفاده از مواد و تجهیزات با ترکیبات خاصی جهت ساخت بناهای چنین زیرساخت‌هایی است. این کتاب عمدتاً در قلمرو کشور لهستان بحث می‌کند و گستره بین‌المللی چندانی ندارد. تفاوت آن با پژوهش حاضر نیز در همین است.

سازمان ملل (۲۰۱۸) در کتابچه «حفاظت از زیرساخت‌های حیاتی در برابر حملات تروریستی» بر مسئولیت‌های دولت‌ها در مقابله با حملات تروریستی به زیرساخت‌های سایبری تمرکز دارد. او سعی می‌نماید با تاکید بر نقش اساسی دولت‌ها در مقابله با تروریسم ابتکارات بین‌المللی در مقابله با این پدیده را تبیین نماید. تفاوت این اثر با مقاله حاضر عدم پرداختن به زیرساخت‌های حیاتی فیزیکی در حقوق بین‌الملل است.

ایرینه کوزیگو (۲۰۱۹) در مقاله «جرم‌انگاری تروریسم آنلاین اسناد مقدمات مطابق حقوق بین‌الملل» بر نحوه کنترل تروریسم سایبری و یا آنلاین در حقوق بین‌الملل تاکید می‌ورزد و به این سوال پاسخ می‌دهد که آیا اسناد الزام‌آور بین‌المللی در خصوص تروریسم و جرایم سازمان یافته یا جرایم مجازی می‌تواند مانع از اقدامات تروریسم سایبری بشود؟ نویسنده به این نتیجه می‌رسد که هیچ‌کدام از قوانین در حقوق بین‌الملل برای نظارت بر حملات تروریسم سایبری وجود ندارد. تفاوت عمده این مقاله با پژوهش حاضر در دو وجه است: یکی عدم پرداختن آن به حملات تروریستی فیزیکی و صرفاً تمرکز بر حملات سایبری و دیگری نپرداختن به مبحث زیرساخت‌های حیاتی کشورها است.

آنا ماریا سالیناس دو فریاس و همکاران (۲۰۱۲) در کتاب «مقابله با تروریسم: حقوق و رویه بین‌الملل» مقابله با تروریسم را به صورت کلی مورد بررسی قرار داده است. این اثر ابعاد مهم مقابله با تروریسم را مورد توجه قرار داده است و مقابله با تروریسم را در رژیم‌های حقوقی منطقه‌ای را بررسی نموده است؛ اما با هدف و موضوع پژوهش حاضر تفاوت عمده دارد. که بارزترین‌ها عدم پرداختن به گزاره‌های اصلی این پژوهش یعنی حملات تروریستی به زیرساخت‌های یک کشور است.

همانگونه که مشاهده می‌شود آثار مذکور به جنبه‌های مختلف حملات تروریستی پرداخته‌اند. در خصوص حمله تروریستی سایبری به زیرساخت‌های حیاتی پژوهش‌هایی وجود دارد اما در خصوص حمله تروریستی فیزیکی به زیرساخت‌های حیاتی یک کشور هیچ‌گونه پژوهشی صورت نگرفته است. بنابراین این پژوهش می‌تواند کاری نوین و متفاوت باشد.

## ۲- چارچوب مفهومی و مبانی نظری

این مقاله بر این نظریه استوار است که حقوق بین‌الملل از منظر معاهداتی و عملکردی تا چه میزان می‌تواند از بروز حملات تروریستی به زیرساخت‌های حیاتی پیشگیری کند و در این راستا

چه قواعدی را تدوین نموده و باید تصویب کند. ترور با اهداف مختلف سیاسی، اقتصادی و یا دینی صورت می‌گیرد که ممکن است آثار مخرب زیادی را به بار آورد مخصوصاً زمانی که زیرساخت‌های حیاتی یک کشور مورد هدف قرار بگیرد. از این رو ابتدا عبارات و اصطلاحات مهم را تعریف نماییم تا درک بهتری از این مسائل حاصل گردد.

### ۱-۲- تروریسم<sup>۱</sup>

تروریسم مفهومی گسترده دارد که اعمال آن در ابعاد مختلف زندگی می‌تواند تمام جنبه‌های آن را دربر بگیرد، برای نمونه تروریسم می‌تواند شامل اقداماتی خرابکاران در راستای از بین بردن منابع غذایی یک شهر یا منطقه باشد که نهایتاً هدف آن ایجاد رعب و وحشت و نیل به هدف است، یا حتی می‌تواند در زمینه‌های ورزشی صورت بگیرد و یا حتی در مبحث صدا و سیما یک کشور (همانند اقدام اخیر گروهک منافقین در صدا و سیمای ایران). بنابراین بر اساس نوع هدف، نوع حمله تروریستی نیز می‌تواند متفاوت باشد و گستره مفهومی وسیعتری را شامل گردد.

در قوانین ایالات متحده آمریکا تعریف تروریسم: «خشونت با قصد قبلی با انگیزه سیاسی که توسط گروه‌های با تابعیت فرعی یا نمایندگی‌های پنهان معمولاً با قصد تحت تاثیر قراردادن یک گروه علیه اهداف غیرنظامی صورت می‌گیرد» (U.S. Department of Justice, 2005, Sec. 0.85).

هرچند دیدگاه کشورها در خصوص تعریف تروریسم تفاوت دارد مثلاً در زبان فارسی و انگلیسی اما تروریسم مطابق تعریف فوق عناصر مهمی دارد: ۱- با قصد قبلی<sup>۲</sup> است، ۲- سیاسی<sup>۳</sup> است، ۳- هدفش غیرنظامیان<sup>۴</sup> است، ۴- توسط گروه‌های غیرنظامی صورت می‌گیرد.

نقدی که به این تعریف وارد است این است که صرفاً حملات تروریستی به افراد غیرنظامی جامعه را مد نظر قرارداده است، در حالی که شاهد تنوع حملات تروریستی در سطح جهان می‌باشیم. تروریست‌ها علاوه بر افراد غیرنظامی به زیرساخت‌های حیاتی کشورها نیز حمله می‌کنند تا هم خسارت به کشور هدف وارد سازند و هم قدرت خود را به نمایش بگذارند. از این رو، تعریف ارائه شده فوق دچار نقصان است.

ناگفته نماند تعریف تروریسم بخاطر برداشت‌های متفاوت از مفهوم آن با دشواری‌هایی همراه است. برخی محققان معتقدند تروریسم دارای مفاهیم مختلط از مفاهیم حقوقی، سیاسی و حتی اجتماعی می‌باشد. بنابراین، با توجه به ابعاد مختلفی که تروریسم دارد، امکان ارائه تعریفی مانع و جامع دشوار می‌شود.

<sup>1</sup>. Terrorism

<sup>2</sup>. Prior Intention

<sup>3</sup>. Political

<sup>4</sup>. Civilian Targets

<sup>5</sup>. Civilian Groups

تعریفی که می‌توان متناسب دانست بیان می‌کند: «تروریسم استفاده از اعمالی غیرقانونی<sup>۱</sup> که همراه با خشونت<sup>۲</sup> همراه بوده است که موجب ترس مردم به صورت فزاینده می‌شود. به عبارت دیگر تروریسم استفاده غیرقانونی از زور و خشونت که با ترس و وحشت فراگیر مردم همراه است، که علیه دولت و حاکمیت<sup>۳</sup> اعم از افراد یا اموال جهت ناکارآمد جلوه دادن دولت حاکم و رویگردانی مردم از آن و یا ایجاد ناکارآمدی یا اثبات ناکارآمدی دولت و با هدف ارباب و یا اجبار دولت و جمعیت مردمی غیرنظامی در سطوح مختلف، جهت پیشبرد اهداف سیاسی خود و تحقق اهداف نامشروع دیگر است، صورت می‌گیرد» (کاوایانی، ۱۳۹۶: ۴۹-۵۰)؛ (Kaviani, 2017: 49-50). این تعریف نسبت به تعریف فوق جامعیت بیشتری دارد و به حمله به مردم غیرنظامی محدود نگردیده است.

لازم به توضیح است، که حملات تروریستی به دو دسته تقسیم می‌گردد: ۱- حملات سایبری<sup>۴</sup>، ۲- حملات فیزیکی. در حقوق بین‌الملل قواعد و مقررات لازم جهت مقابله با حملات تروریستی سایبری وجود دارد، اما آنچه مغفول مانده است حملات تروریستی فیزیکی به زیرساخت‌های حیاتی می‌باشد که مقاله حاضر بر این امر اتمام دارد.

## ۲-۲- زیرساخت‌های حیاتی

یکی از مفاهیم مهم در حوزه حکمرانی مطلوب<sup>۵</sup> توجه به زیرساخت‌های حیاتی می‌باشد، لذا کشورها بر اساس سیاست‌های کلان خود اقدام به ترسیم و تعریف زیرساخت‌های حیاتی خود می‌نمایند. از این رو، قطعنامه ۲۳۴۴ (۲۰۱۷) تایید می‌کند که «هر کشور مشخص می‌کند چه چیزی زیرساخت حیاتی آن را تشکیل می‌دهد». با این حال، روش مجزایی را برای تفکیک زیرساخت‌های حیاتی از میان تعداد بیشماری از زیرساخت‌های واقع در کشورها، توصیه نمی‌کند. سایر اسناد بین‌المللی نیز دستور خاصی را ارائه نمی‌کنند. (Un Crisis Relief, 2019).

بنابراین، کشورها با صلاحدید خود در انتخاب معیارها برای شناسایی زیرساخت‌های فعال در قلمرو آنها آستانه «اهمیت» را اختیار می‌کنند. تمایز بین زیرساخت‌های حیاتی / مربوطه و آنهایی که باید وضعیت «حیاتی» پیدا کنند، نکته کلیدی است که بتوان اولویت منابع کمیاب را در حفاظت از دارایی‌ها و فرآیندهای گسترده قرار داد. کشورهای مختلف تعاریف متفاوتی از زیرساخت‌های

<sup>1</sup> .Illegal Acts

<sup>2</sup> .Violence

<sup>3</sup> .Sovereignty

<sup>4</sup> .Cyber attacks

<sup>5</sup> .Good Governance

<sup>6</sup> .Adopted by the Security Council at its 7882nd meeting on 13 February 2017

<sup>7</sup> .<https://www.un.org/counterterrorism/international-legal-instruments>

حیاتی ارائه داده‌اند (CTED and UNOCT, 2018: 32-33):

فرانسه: زیرساخت حیاتی هر تأسیسات، ساختاری است که آسیب، در دسترس نبودن یا تخریب آنها در نتیجه یک عمل سو، اقدام خرابکارانه یا تروریسم می‌تواند به طور مستقیم یا غیرمستقیم باشد: اگر فعالیت آن به سختی قابل جایگزینی باشد، ظرفیت جنگ را تحت فشار قرار می‌دهد یا پتانسیل اقتصادی، امنیت ملی یا بقای کشور یا تأثیر بر سلامتی یا زندگی جمعیت.

آمریکا: سیستم‌ها و دارایی‌ها، چه فیزیکی<sup>۲</sup> و چه مجازی<sup>۳</sup>، برای ایالات متحده چنان حیاتی هستند که ناتوانی یا نابودی این سیستم‌ها و دارایی‌ها تأثیرات ناتوانی بر امنیت، امنیت اقتصادی ملی، بهداشت عمومی یا امنیت ملی یا هر ترکیبی از این موارد دارد.

روسیه: زیرساخت‌های حیاتی فدراسیون روسیه هدفی است که نقض بهره برداری از آن منجر به از دست دادن کنترل، تخریب زیرساخت‌ها، تغییرات منفی برگشت ناپذیر (یا شکست) اقتصاد، موضوع فدراسیون روسیه یا اداری - سرزمینی می‌شود واحدها یا وخامت قابل توجهی در ایمنی افراد برای طولانی مدت.

پاکستان: زیرساخت‌های حیاتی زیرساخت‌هایی است که توسط هر دولتی تعیین شده است و سایر دارایی‌ها، سیستم‌ها و شبکه‌ها، اعم از فیزیکی یا مجازی، برای کشور یا ارگان‌های آن از جمله قضاوت بسیار حیاتی است که تخریب آنها ممکن است اثرات ناتوانی بر امنیت ملی داشته باشد اقتصاد، بهداشت عمومی، ایمنی یا موارد مرتبط با آن.

زیرساخت‌های حیاتی شامل سیستم‌ها، تأسیسات و دارایی‌های بسیار حیاتی است که تخریب یا ویران کردن آنها ممکن است تأثیر فلج‌کننده‌ای بر امنیت ملی، اقتصاد یا ایمنی عمومی، بهداشت یا رفاه داشته باشد. (USAGOV LOGO, 2007).

برخی دیگر معتقدند تعریف زیرساخت‌های به شبکه‌ها و سیستم‌هایی اطلاق می‌شود که یک دولت انتظار دارد به درستی عمل کنند، و در واقع «ستون فقرات دولت» در عرصه اقتصادی، اجتماعی و سیاسی می‌باشند (Mockaitis, 2006). این زیرساخت‌های حیاتی شامل سیستم‌های تولید و انتقال برق، قابلیت‌های آبی و فاضلاب، سیستم‌های مالی، شبکه‌های اجتماعی، ظرفیتهای لازم برای تولید و حمل و نقل مواد غذایی، قابلیت‌های صنعتی، شناسیات پزشکی می‌باشند، البته نباید امکانات تجاری و حمل و نقل را نادیده انگاشت، چرا که آنها شاهرگ‌های حیاتی یک کشور می‌باشند.

<sup>1</sup>. Systems

<sup>2</sup>. Physical

<sup>3</sup>. Cyber

<sup>4</sup>. Assets

<sup>5</sup>. Industrial Capabilities

در مجموع، زیرساخت‌های حیاتی مجموعه عناصر ساختاری به هم پیوسته ای است که یک سیستم بزرگ همراه با ابعاد تکنولوژی گسترده و ابعاد فیزیکی غیرعامل حرکت را تشکیل داده است. نکته مهم این است که این زیرساخت‌های حیاتی، ارائه دهنده خدمات اساسی و بنیادی است بنابراین چارچوب اصلی برای پشتیبانی از ساختارهای کلان امنیت ملی کشور و آحاد ملت می باشد (زرقانی و همکاران، ۱۳۹۵: ۸۹۰)؛ (Zarghani et.al., 2016: 890).

### ۳- تاریخچه موضوع

تروریسم پدیده‌ای است که تقریباً هم سن تاریخ بشر است. از منظر تاریخی تروریسم را به سه دوره تقسیم می‌کنند: ۱- سنتی<sup>۱</sup>، ۲- تروریسم نوین<sup>۲</sup>، ۳- تروریسم پسا مدرن<sup>۳</sup>. تروریسم سنتی که از انقلاب فرانسه نشأت می‌گیرد؛ که در آن زمان معنای مشخص امروزی را نداشته است. پس از این زمان بود که تروریسم از حالت مشروع و انحصاری حکومت خارج گردید و به سطح جامعه رسید (فیرحی و ظهیری، ۱۳۸۷: ۱۵۰-۱۵۱)؛ (Farihi & Zahiri, 2008: 150-151). همزمان با فعالیت‌های آنارشیست‌های روسی، تروریسم به معنای بیداری روحیه انقلاب در میان توده‌ها بود و به شورش‌های خشونت آمیز اطلاق می‌شد. آنارشیست‌های روسی بدون خجالت و ناراحتی خود را تروریست و تاکتیک خود را صراحتاً تروریسم اعلام می‌کردند. تاکتیکی که با قتل الکساندر دوم پادشاه روسیه در سال ۱۸۸۱ به نقطه اوج خود رسید (قلی‌زاده، ۱۳۹۵: ۱۳۰)؛ (Gholizadeh, 2016: 130).

یازدهم سپتامبر ۲۰۰۱ سرآغاز جدیدی در ماهیت تروریسم و دیدگاه جامعه بین‌الملل به پدیده تروریسم را ایجاد نمود در این زمان بود که ریاست جمهور وقت ایالات متحده آمریکا برای حمله به افغانستان از اصطلاح «جنگ علیه ترور»<sup>۴</sup> استفاده نمود. برخی محققین بر این نکته تاکید دارند که عرصه نوین تاریخچه تروریسم از زمان جنگ سرد آغاز شده است و در زمان ۱۱ سپتامبر ۲۰۰۱ به نهایت ظرفیت خود دست یافت (پورسعید، ۱۳۸۹: ۱۵۰-۱۵۱)؛ (Poursaeed, 2009: 150-151). بعد از این مرحله تروریسم پسامدرن ظهور می‌کند. تروریسم پسامدرن علیرغم جدید بودن ویژگی‌های دو نسل را داراست. تروریست‌های پسامدرن به دنبال ستیز کلیت مدرنیته جهانی شدن و نظم برآمده از این تفکرات در دنیای امروز است. تروریست پسامدرن از هر راهی اقدام می‌کند تا این نظم را با تمام دستاوردهایش به زیر بکشد و دنیایی آرمانی براساس تفکرات خویش برقرار کند (آل‌غفور و صادقیان، ۱۳۹۴: ۶۰۱)؛ (Aleghafour & Sadeghian, 2015: 601).

<sup>1</sup>. Traditional

<sup>2</sup>. Modern

<sup>3</sup>. Post Modern

<sup>4</sup>. War on Terror

#### ۴- تروریسم و حملات به زیرساخت‌های حیاتی در حقوق بین‌الملل

زیرساخت‌های حیاتی بر اساس جایگاه هر صنعت یا سازمان برای کشورها تعریف خاصی دارد. که به صورت عام می‌تواند در حقوق بین‌الملل مورد توجه قرار گیرد. تروریست‌ها بخاطر حساسیت این زیرساخت‌ها قصد ضربه زدن به آنها را دارند. از این رو این بخش به این مساله می‌پردازد.

##### ۱-۴- مصادیق زیرساخت‌های حیاتی

همه زیرساخت‌ها حیاتی نیستند. زیرساخت‌های حیاتی مجموعه‌ای از دارایی‌های مهم است. اموال چیزی است که دارای اهمیت بسیار بالایی است و می‌تواند شامل، مردم، املاک، با سیستم‌های اطلاعاتی باشد. زیرساخت‌های حیاتی به بهترین نحو توسط هر قلمرو و حاکمیت مجزا گزینش می‌شوند چرا که هر کشور شرایط خود را بهتر می‌شناسد. بنابراین ممکن است آنچه توسط یک کشور و یا دولت بعنوان زیرساخت حیاتی تلقی می‌گردد، توسط کشور دیگر به این میزان مهم نباشد. زیرساخت‌های حیاتی سیستم‌های پیچیده‌ای هستند که خدماتی را که زندگی هر روزه ما به آن وابسته است، تامین می‌کنند. زیرساخت‌های حیاتی دارایی‌های مهمی هستند که ما به آنها نیاز داریم (Bennett, 2007: 55).

زیرساخت‌های حیاتی می‌توانند ثابت یا متحرک باشند به عبارت حقوقی می‌توانند منقول<sup>۱</sup> و غیرمنقول<sup>۲</sup> باشند. دارایی‌های غیرمنقول آن است که در یک مکان ثابت است از جمله بیمارستان. اموال منقول آن است که از جایی به جایی دیگر قابل انتقال است. حملات علیه زیرساخت‌های حیاتی می‌تواند بصورت فیزیکی یا سایبری باشد. حمله فیزیکی<sup>۳</sup> آن است که در محل وقوع دارایی‌ها رخ می‌دهد و تسلیحات فیزیکی از جمله ابزار انفجاری در آنجا کار گذاشته می‌شود. حمله سایبری را می‌توان از فاصله بسیار دور از هدف انجام داد که از بستر شبکه اینترنت جهانی برای چنین حملاتی می‌توانند استفاده کنند.

می‌توان مصادیق زیرساخت‌های حیاتی را به دسته‌های ذیل تقسیم نمود: جمعیت، نفت و انرژی، بانک مرکزی، ارتباطات، خدمات (از جمله خدمات مالی، توزیع غذا و مراقبت‌های بهداشتی)، حمل و نقل، تاسیسات هسته‌ای، ساختمان‌های دولتی، سدها، دارایی‌ها و امکان تجاری، پایگاه‌ها و تاسیسات نظامی.

##### ۴-۲- آسیب پذیری و تهدیدپذیری زیرساخت‌های حیاتی

زیرساخت‌های حیاتی با توجه به نقش مهمی که در شریان حیاتی کشورها ایفا می‌کنند، مورد

<sup>۱</sup>. Movable

<sup>۲</sup>. Immovable

<sup>۳</sup>. Physical Attacks

<sup>۴</sup>. Vulnerabilities

<sup>۵</sup>. Treatability



توجه گروه‌های تروریستی واقع می‌شوند. به دو دلیل تروریست‌ها اقدام به حملات خود علیه زیرساخت‌های یک کشور می‌نمایند یکی میزان تاثیر گذاری آن بر کشور هدف و دیگر آسیب پذیری زیرساخت‌های حیاتی کشورها. بنابراین تهدیدات یا به دلیل آسیب پذیری در منابع سخت افزاری و نرم افزاری زیرساخت‌های حیاتی است و یا به دلیل قابلیت دسترسی فیزیکی تروریستها به این زیرساخت‌هاست. همین امر موجب میشود تروریست‌ها یا به صورت سایبری و نقص در منابع نرم افزاری و سخت افزاری و یا به صورت فیزیکی و حمله به زیرساخت‌ها امکان اجرای تهدید خود را داشته باشند.

انواع نقص‌ها<sup>۱</sup> در زیرساخت‌های حیاتی دو دسته هستند: یکی نقص‌های داخلی<sup>۲</sup> و دیگری نقص‌های خارجی<sup>۳</sup>. نقص‌های داخلی معادل تغییرات غیرطبیعی ناشی از درون خود سیستم است و نقص‌های خارجی به تعاملاتی مربوط می‌گردد که از خارج از سیستم نشات می‌گیرند مانند پدیده‌های طبیعی، اقدامات یا حوادث خرابکارانه (Alcaraz, 2015: 5).

بنابراین، گروه‌های تروریستی با سنجیدن موقعیت موجود اقدام به طراحی حمله به زیرساخت هدف می‌نمایند. باید در خاطر داشت که «تروریسم تهدید مهمی علیه صلح و امنیت بین‌المللی است» (مهرگان و همکاران، ۱۳۹۹: ۱۵۸)؛ (Mehregan et. Al, 2020: 158). گروه‌های تروریستی به هدفی حمله می‌کنند که از یک سو تاثیر بیشتری بر دولت مورد نظر داشته باشد و از سوی دیگر قابل حصول تر از سایر اهداف باشد (Atigui et.al., 2020: 193) آنها سعی می‌کنند با کمترین هزینه بیشترین خسارت را به کشور هدف وارد نمایند. مثلا، پالایشگاه‌های نفتی و گازی بدلیل عدم محافظت لازم توسط دولت‌ها و تاثیر بالای آنها در شریان اقتصادی آنها، سبب می‌شود گروه‌های تروریستی آن را یک هدف آسان جهت نیل به اهداف خود بدانند. مثالهای بارز آن، حمله موشکی تروریست داعش به سه مرکز نفتی سوریه در آغاز زمستان ۱۳۹۸، یا حمله پهپادی گروه‌های یمنی به پالایشگاه‌های آرامکو عربستان که منبع اصلی تولید نفت دولت عربستان سعودی می‌باشد، نمونه دیگر حمله گروه تروریستی داعش به پالایشگاه سینیا عراق در سال ۱۳۹۹ می‌باشد که ظرفیت روزانه آن ۳۰ هزار بشکه بود. (شانا، ۱۳۹۹)؛ (Shana, 2020).

نکته‌ای قابل ذکر این است که بخاطر در دسترس عموم بودن فضای مجازی یکی از جوانب آسیب‌پذیری زیرساخت‌ها بوسیله فضای مجازی صورت می‌گیرد. به بیان دیگر «استفاده تروریسم از اینترنت برای نیل به اهداف غیرقانونی خود» (کازرونی، ۱۳۹۵: ۱۷۱)؛ (Kazerouni, 2016: 171).

<sup>1</sup>. Defects

<sup>2</sup>. Internal Defects

<sup>3</sup>. External Defects

<sup>4</sup>. Drone Attacks

سبب می‌شود که زیرساخت‌های متصل به اینترنت به راحتی در معرض حملات تروریستی قرار گیرند.

مهمترین عنصر عمل تروریستی در جریان یک مخاصمه مسلحانه بین‌المللی، قصد گستراندن ترور میان غیر نظامیان می‌باشد. بر این اساس، اقدامات تروریستی همیشه یا شامل حمله بر علیه اهداف و اشخاص غیرنظامی است یا شامل حملات غیر قابل تفکیکی است که معمولاً به ترور و وحشت جمعیت غیر نظامی منجر می‌شود.

علاوه بر این، تروریست‌های برای حمله به یک هدف قبل از اقدام به عمل موارد مهمی را مدنظر قرار می‌دهند از جمله: نمادسازی، آسیب‌پذیری، ریسک، قابلیت انجام، تاثیر و بازخورد. این عوامل در تصمیم‌گیری ترویست‌های جهت حمله به یک زیرساخت حیاتی بسیار حائز اهمیت است. (Schmid, 2020, 847).

#### ۴-۳- همکاری کشورها، راهکار مقابله با تروریسم

همکاری دولت‌ها یکی از ابتکارات ملموس در سطح بین‌الملل و مورد تاکید حقوق بین‌الملل می‌باشد. به دلیل پیچیده بودن مساله تروریسم در طول تاریخ خود، کشورها برای حفظ امنیت ملی خود و رهایی از تهدیدات راهبردهای مختلفی بکار می‌برند. (نجف‌آبادی و همکاران، ۱۳۹۹: ۱۷۳) (Najafabadi et.al., 2020: 173). مقابله با این پدیده بین‌المللی نیاز به همکاری بین‌المللی دارد. همکاری بین‌المللی نیز، نیاز به ابزارهای خاصی دارد که بواسطه آنها بتوان پیشگیری از تروریسم را تضمین نمود. یکی از این ابزارها کنوانسیون‌های بین‌المللی هستند که در زمینه تروریسم منعقد شده‌اند (ملکی، ۱۳۹۵: ۷۲)؛ (Maleki, 2016: 72). یکی از پدیده‌های مخرب گروه‌های تروریستی است که همواره آسیب‌ها و خسارات جبران‌ناپذیری را به کشورها وارد نموده و بواسطه آن اقدام به ایجاد آشوب، هرج و مرج، اعتراضات داخلی و نهایتاً تغییر رژیم می‌نمایند. اگر یک کشور بخواهد به تنهایی با گروه‌های تروریستی مقابله کند شاید اقبال چیره شدن بر آنها را نداشته باشد و نهایتاً دولت حاکم را وادار به تسلیم در مقابل خواسته خود نمایند، اما اگر کشورها با هم همکاری و هم‌افزایی نمایند تهدیدات و حملات تروریستی در اکثر مواقع عقیم می‌ماند و با شکست مواجه می‌گردد.

از دیگر همکاری‌های بین‌المللی میان کشورها که باعث پیگرد و استرداد مجرمین تروریستی می‌شود، همکاری در زمینه کیفری است. مکانیسم‌های همکاری دوجانبه یا چندجانبه به جمع‌آوری مدارک معتبر برای رسیدگی به جرایم آنها در محاکم داخلی کمک می‌کند. علاوه بر این،

<sup>1</sup>. International Armed Conflict

کنوانسیون‌های حقوق بشردوستانه بین‌المللی<sup>۱</sup> و سازمان ملل ناظر بر استرداد مجرمین است که دولت‌ها را متعهد می‌نماید یا مجرمین را مسترد نماید یا مجازات (Sanchez Frias, 2020: 83). سازمان‌های بین‌المللی نیز از دیگر ابزارهای مهمی هستند که در کنار اقدامات فردی دولت‌ها، میتوانند زمینه‌های همکاری و معاضدت بین‌المللی برای مقابله با تروریسم به طور عام و پیشگیری از این پدیده را بطور خاص فراهم آورند. همانطور که قبلاً مورد اشاره واقع شد، تعهدات اولیه تعهداتی است که دولت‌ها بر مبنای اراده‌های همسو، خود را متعهد و مکلف به رعایت آنها می‌نمایند ماهیت فرامرزی پدیده تروریسم ایجاب می‌کند تا همکاری موثر بین‌المللی و منطقه‌ای در خصوص مسائل کیفری در رابطه با تروریسم و تعیین مقامات مربوطه برای هدایت چنین همکاری تضمین گردد. شاخه پیشگیری از تروریسم دفتر سازمان ملل در خصوص مواد مخدر و جرم کمک می‌کند تا توافقات همکاری مستحکمی میان کشورهای عضو با دیدگاه تسهیل درخواستهای همکاری حقوقی متقابل ایجاد گردد. (UNODC, 2019).

از نمونه‌های همکاری دولت‌ها می‌توان به گسترش همکاری‌های بین‌الملل در مسائل کیفری علیه مزدوران تروریست خارجی در خاورمیانه و آفریقای جنوبی که این شعبه توسعه یک شبکه همکاری تخصصی جدید تحت عنوان « کارگروه چند-سازمانی<sup>۲</sup> » را حمایت نمود که این کارگروه مشکل از نقاط قانونی امنیتی و قضایی بود که برای یک همکاری بهتر ضد تروریسمی در منطقه باهم کار می‌کنند.

برای مثال در سال ۲۰۱۸، اطلاعات بدست آمده توسط این کارگروه منجر به دستگیری و توقیف مواد اولیه شیمیایی برای یک دستگاه انفجاری شد که هدفشان استفاده از آن در یک حمله تروریستی بود (UNODC, 2019). که نشان دهنده تسهیل همکاری بین‌المللی میان دولت‌ها از طریق ابتکارات سازمان ملل در رابطه با مقابله با تروریسم می‌باشد.

این همکاری‌ها بصورت عام در خصوص مقابله با تروریسم داخلی و بین‌المللی می‌باشد که بصورت خاص در زمینه حفاظت از زیرساخت‌های کشورها نیز صدق پیدا می‌کند. سازمان ملل متحد با ملحوظ نظر قراردادن الزامات چارچوب حقوقی بین‌المللی برای مقابله با تروریسم به ویژه مفاد مربوط به گسترش همکاری برای مقابله با تروریسم، قطعنامه‌هایی را در شورای امنیت به تصویب رساند از جمله قطعنامه ۲۱۷۸ (۲۰۱۴)، ۲۳۲۲ (۲۰۱۶)، ۲۳۷۹ (۲۰۱۷) و ۲۳۹۶ (۲۰۱۷). در سطح منطقه‌ای نیز اقدامات حقوقی صورت گرفته، از جمله کنوانسیون عربی برای سرکوب تروریسم

<sup>1</sup>. International Humanitarian Law Conventions

<sup>2</sup>. [https://www.unodc.org/pdf/terrorism/MATF-2019/Fact\\_Sheet\\_MATF\\_-\\_CCPCJ\\_-\\_EN.pdf](https://www.unodc.org/pdf/terrorism/MATF-2019/Fact_Sheet_MATF_-_CCPCJ_-_EN.pdf), (2019).

<sup>3</sup>. Multi-Agency Task Force (MATF)

<sup>4</sup>. [https://www.unodc.org/pdf/terrorism/MATF-2019/Fact\\_Sheet\\_MATF\\_-\\_CCPCJ\\_-\\_EN.pdf](https://www.unodc.org/pdf/terrorism/MATF-2019/Fact_Sheet_MATF_-_CCPCJ_-_EN.pdf), (2019).

(۱۹۸۸) و کنوانسیون همکاری حقوقی مشترک در مقابله با تروریسم (۲۰۰۸) (UNODC, 2019). همچنین کشورها در مقابله با تروریسم ممکن است با همکاری یکدیگر به استفاده از زور متوسل شوند. که توسل به زور در برابر تروریسم با دو هدف صورت می‌گیرد: «۱- تلافی نظامی اقدام تروریستی تحت عنوان دفاع مشروع؛ ۲- از بین بردن تروریست‌ها پیش از انجام عملیات تروریستی» (علیخانی، ۱۳۹۴: ۴۰)؛ (Alikhani, 2015: 40).

کشورهای مختلف در سطح دنیا به رهبری سازمان ملل در امر مبارزه با تروریسم اعتقاد دارند و این اعتقاد نیز در عرصه عمل نیز ظهور پیدا کرده است که می‌توان به اقدام سازمان کشورهای اسلامی اشاره نمود که با توجه به دربرگرفتن تمام کشورهای اسلامی در جهان، بر لزوم رهبری سازمان ملل در اقدامات ضد تروریستی تأکید ورزید (سیمبر، ۱۳۸۴: ۱۶۰)؛ (Simbar, 2005: 160).

#### ۴-۴- اقدامات حقوقی جامع بین‌الملل در مقابله با حملات تروریستی

کشورها جهت همکاری‌های بین‌المللی اقداماتی مناسبی را صورت داده‌اند. آنچه مغفول مانده است، عدم توجه به زیرساخت‌های حیاتی کشورها در قواعد وضع شده در سطح بین‌المللی می‌باشد. ابعاد مختلف تهدیدات و حملات تروریستی در شماری از کنوانسیون‌های و پروتکل‌های بین‌المللی مورد توجه جامعه جهانی واقع شده است. این سیزده کنوانسیون به نوعی تعهداتی را برای دولت‌های عضو ایجاد می‌کند که از این طریق بتوانند همکاری‌های لازم را در این خصوص داشته باشند. در این بخش مروری خواهیم داشت بر کنوانسیون‌های مزبور.

همچنین کنوانسیون ممانعت و مجازات تروریسم ۱۹۳۷ (ژنو) اولین کنوانسیون در خصوص تروریسم است که سنگ بنای توجه جامعه بین‌المللی به مسئله تروریسم و مقابله با آن را بنا نهاده. سازمان ملل کنوانسیون‌های مقابله با تروریسم را به این شرح ارائه می‌کند: (United Nation, 2019).  
 ۱. اسناد مربوط به هواپیمای غیرنظامی: کنوانسیون ۱۹۶۳ در خصوص جرایم و برخی اقدامات مشخص ارتكابی در هواپیما، کنوانسیون ۱۹۷۰ برای مقابله با تسخیر غیرقانونی هواپیما، کنوانسیون ۱۹۷۱ برای مقابله با اقدامات غیرقانونی علیه امینی هواپیمای غیرنظامی، پروتکل ۱۹۸۸ برای مقابله با اقدامات غیرقانونی خشونت آمیز در فرودگاه‌های مربوط به هواپیمای غیرنظامی بین‌المللی، متمم به کنوانسیون مقابله با اقدامات غیرقانونی علیه ایمنی هواپیمای غیرنظامی، کنوانسیون ۲۰۱۰ مقابله با اقدامات غیرقانونی مربوط به هواپیمای غیرنظامی بین‌المللی، پروتکل ۲۰۱۰ متمم به کنوانسیون مقابله با تسخیر غیرقانونی هواپیما، پروتکل ۲۰۱۴ برای اصلاح کنوانسیون جرایم و اقدامات خاص ارتكابی در هواپیما؛

<sup>1</sup> [https://www.unodc.org/pdf/terrorism/MATF-2019/Fact\\_Sheet\\_MATF\\_-\\_CCPCI\\_-\\_EN.pdf](https://www.unodc.org/pdf/terrorism/MATF-2019/Fact_Sheet_MATF_-_CCPCI_-_EN.pdf), (2019).

<sup>2</sup> <https://www.un.org/counterterrorism/international-legal-instruments>, (19 November 2019).

<sup>3</sup> Instruments Regarding Civil Aviation

۲. اسناد مربوط به حفاظت از کارکنان بین‌المللی؛<sup>۱</sup> کنوانسیون ۱۹۷۳ در خصوص پیشگیری و مجازات جرایم علیه اشخاص حفاظت شده بین‌المللی، اسناد مربوط به گروگانگیری، کنوانسیون بین‌المللی ۱۹۷۹ مقابله با گروگانگیری؛

۳. اسناد مربوط به مواد هسته‌ای؛<sup>۲</sup> کنوانسیون ۱۹۸۰ در خصوص حفاظت فیزیکی از مواد هسته‌ای، صلاحات ۲۰۰۵ در خصوص کنوانسیون حفاظت فیزیکی از مواد هسته‌ای؛

۴. اسناد مربوط به ناوبری دریایی؛<sup>۳</sup> کنوانسیون ۱۹۸۸ برای مقابله با اقدامات غیرقانونی علیه ایمنی ناوبری دریایی، ناوبری دریایی، پروتکل ۲۰۰۵ به کنوانسیون مقابله با اقدامات غیرقانونی علیه ایمنی ناوبری دریایی، پروتکل ۱۹۸۸ برای مقابله با اقدامات غیرقانونی علیه ایمنی سکوهاى ثابت واقع در فلات قاره‌ای، پروتکل ۲۰۰۵ به پروتکل برای مقابله با اقدامات غیرقانونی علیه ایمنی سکوهاى ثابت واقع در فلات قاره‌ای؛

۵. اسناد مربوط به مواد منفجره؛<sup>۴</sup> کنوانسیون ۱۹۹۱ در خصوص تولید مواد منفجره پلاستیکی برای هدف اکتشاف؛

۶. اسناد مربوط به بمب گذاری تروریستی؛<sup>۵</sup> کنوانسیون بین‌المللی ۱۹۹۷ برای مقابله با بمب گذاری تروریستی؛

۷. اسناد مربوط به تامین مالی تروریسم؛<sup>۶</sup> کنوانسیون بین‌المللی ۱۹۹۹ برای مقابله با تامین مالی تروریسم؛

۸. اسناد مربوط به تروریسم هسته‌ای؛<sup>۷</sup> کنوانسیون بین‌المللی ۲۰۰۵ برای مقابله با اقدامات تروریسم هسته‌ای؛

تمام مفاد کنوانسیون‌های بین‌المللی زمانی قدرت اجرایی بالایی دارند که دولت‌ها به همکاری پردازند، بدین معنی که هر یک از اسناد وضع شده فوق در حوزه مقابله با تروریسم، نیازمند یک قوه اجرایی قوی است که منبعث از اراده دولت‌هاست. اگرچه در اسناد بین‌المللی فوق اشاره، برخی از زیرساخت‌های حیاتی کشورها تحت حاکمیت یک سند بین‌المللی در آمده است، اما بصورت تخصصی توجه به مقابله با حملات تروریستی به زیرساخت‌های حیاتی یک کشور که شریان حیات اقتصادی، اجتماعی و فرهنگی آن را تامین می‌کند، توجهی نشده است.

<sup>1</sup> .Instrument regarding the protection of international staf.

<sup>2</sup> .Insturment regarding the nuclear material

<sup>3</sup> . Instrument regarding the maritime navigation

<sup>4</sup> . Instrument regarding explosive materials

<sup>5</sup> .Instrument regarding terrorist bombings

<sup>6</sup> . Instrument regarding the financing of terrorism

<sup>7</sup> .Instrument regarding nuclear terrorism

#### ۴-۵- خلاء حقوقی موجود در خصوص تهدیدات و حملات تروریستی به زیر ساخت‌های حیاتی کشورها

خلاء قابل توجه در عرصه مقابله با حملات تروریستی در حقوق بین‌الملل می‌تواند باعث سوء استفاده کشورهای حامی تروریست گردد. برای مثال، اگر گروهی تروریستی به منابع نفتی یا زیرساخت‌های مخابراتی کشوری حمله نماید و موجبات خسارات غیرقابل جبرانی را فراهم کند، کدام کنوانسیون یا سند بین‌المللی که در حال حاضر برای مقابله با حملات تروریستی وضع شده است اعمال می‌گردد؟ مگر اینکه صرفاً به قواعد عمومی حقوق بین‌الملل استناد می‌گردد، کنوانسیون و یا سند خاصی برای مقابله با چنین حملاتی وجود دارد؟

خوشبختانه جامعه بین‌الملل اسناد لازم برای مقابله با حملات تروریستی سایبری به زیرساخت‌های حیاتی را وضع نموده است. ما خلاء اصلی در خصوص حملات فیزیکی تروریستی به زیرساخت‌های حیاتی می‌باشد. سازمان ملل در عرصه مقابله با تروریسم سایبری اقداماتی را انجام داده است که از جمله آن تأسیس کارگروه فناوریهای اطلاعاتی و ارتباطاتی است.

تأسیس کارگروه فناوریهای اطلاعاتی و ارتباطاتی سازمان ملل در نوامبر ۲۰۰۱، در پاسخ به درخواست شورای اقتصادی و اجتماعی سازمان ملل، گام مهمی بود. گروه ویژه موظف شد حمایت جهانی را برای دستیابی به اهداف توسعه هزاره با استفاده از فناوریهای اطلاعاتی و ارتباطاتی بسیج کند. در آوریل ۲۰۰۴، یک سمینار با موضوع «سیاست‌ها و مسائل امنیتی در فناوری اطلاعات» در مقر سازمان ملل برگزار شد. بخشی از این سمینار مربوط به آگاهی از آموزش فناوری اطلاعات بود که توسط گروه ویژه فناوریهای اطلاعاتی و ارتباطاتی و موسسه آموزش و تحقیقات سازمان ملل متحد سازماندهی شد در سال ۲۰۰۴، گروه ویژه کتابچه راهنمایی را منتشر کرد به نام «عدم امنیت اطلاعات - راهنمای بقا در سرزمین‌های ناشناخته تهدیدات سایبری و امنیت سایبری». این نشریه به طور کلی مشکل عدم امنیت اطلاعات را به تصویر می‌کشد و راه‌حل‌های احتمالی را برای پیشگیری و پاسخگویی به حوادث امنیتی (شامل استانداردها و بهترین روش‌ها) ارائه می‌دهد. علاوه بر این، این تلاش برای ایجاد آگاهی بیشتر در مورد خطرات فزاینده ولگردی مجازی، جرایم اینترنتی، تروریسم سایبری و جنگ سایبری که جنبه‌های ذاتی فرصت‌های جدید (مثبت و منفی) است که توسط فناوری‌های اطلاعاتی جدید گشوده شده است (Gelbstein & Kamal, 2002).

شورای امنیت قطعنامه‌هایی برای مقابله با حملات تروریستی سایبری به زیرساخت‌های حیاتی صادر نموده است. شورای امنیت نیز تصمیم خود را در قطعنامه ۱۳۷۳ (۲۰۰۱) یادآوری می‌کند که همه کشورها اقدامات تروریستی را به عنوان جرایم جدی کیفری در قوانین و مقررات داخلی تعیین می‌کنند و از کشورهای عضو می‌خواهد اطمینان حاصل کنند که مسئولیت کیفری حملات

<sup>1</sup>. United Nations Institute for Training and Research (UNITAR)

تروریستی را با هدف از بین بردن یا از کار انداختن زیرساخت‌های حیاتی، و همچنین برنامه‌ریزی، آموزش، و بودجه و پشتیبانی لجستیکی برای چنین حملاتی تعیین کرده‌اند (United Nations, 2001).  
قطعنامه فوق با ملزم کردن دولت‌ها به جرم‌انگاری اقدامات تروریستی که هدفشان فناوریهای اطلاعاتی و ارتباطاتی است سه هدف اساسی را متصور می‌گردد:

۱- تأمین سطح بازدارندگی کافی از طریق اعمال مجازات‌های جدی برای مرتکبان اقدامات تروریستی علیه زیرساخت‌های حیاتی.

۲- برای جلوگیری از برنامه‌های کیفری / تروریستی که متوجه زیرساخت‌های حیاتی است از طریق استفاده از حقوق کیفری به عنوان ابزاری پیشگیرانه. تمرکز پیشگیرانه قطعنامه ۲۳۴۱ (۲۰۱۷) به وضوح از این الزام ناشی می‌شود که کشورها باید «برنامه‌ریزی، آموزش و تأمین مالی و پشتیبانی لجستیکی» برای حملات تروریستی را جرم‌انگاری کنند.

۳- تعیین مبانی قانونی و پیش شرط‌های همکاری بین‌المللی روان در زمینه دادرسی کیفری در امور مربوط به زیرساخت‌های حیاتی.

یکی از ویژگی‌های قطعنامه ۲۳۴۱ (۲۰۱۷) در اولین سند شورای امنیت است که به ویژه از کشورها می‌خواهد اقدامات علیه زیرساخت‌های حیاتی را جرم بدانند. قطعنامه ۲۳۴۱ (۲۰۱۷) بر اساس تعدادی از قطعنامه‌های قبلاً تصویب شده است که شرایط کلی را برای تعیین مسئولیت کیفری مرتکبان اقدامات تروریستی تعیین می‌کند. ابزار برجسته در این زمینه (که (res.2341 (2017) به طور صریح به آن اشاره دارد) قطعنامه ۱۳۷۳ (۲۰۰۱) است. این ابزار بلافاصله پس از حوادث ۱۱ سپتامبر به تصویب رسید، مجموعه‌ای از الزامات عدالت کیفری از جمله تعهدات به موارد زیر را فراهم می‌کند (United Nations, 2001).

علاوه بر قطعنامه‌های شورای امنیت، مجموعه‌ای از معاهدات مربوط به پیشگیری و سرکوب تروریسم بین‌المللی الزامات جرم‌انگاری در حوزه زیرساخت‌های حیاتی را تعیین کرده است. فقدان توافق در مورد دامنه استفاده از یک کنوانسیون جامع که شامل همه جوانب و ظواهر تروریسم بین‌المللی باشد، این اسناد در یک دوره زمانی بیش از پنجاه سال به دنبال رویکرد بخشی به تصویب رسید. رویکرد افزایشی و عملی که توسط جامعه بین‌المللی دنبال می‌شود منجر به تصویب کنوانسیون‌ها و پروتکل‌هایی با تمرکز در زمینه‌هایی مانند امنیت دریایی و هوایمایی، بودجه هسته‌ای و تروریسم و... شده است.

در قطعنامه‌های شورای امنیت، در این کنوانسیون‌ها و پروتکل‌ها هیچ کلمه‌ای از «زیرساخت‌های حیاتی» ذکر نشده است. چرا که اکثر این ابزارها در زمانی تصویب شده‌اند که مفهوم «زیرساخت‌های حیاتی» هنوز خود را در گفتمان سیاست جهانی مبارزه با تروریسم جا نداده بود. با این حال، بیشتر آنها شامل مقررات جرم‌انگاری هستند که مستقیماً اقدامات سوء را با هدف تخریب

یا تداخل در عملکرد زیرساخت‌های حیاتی هدف قرار می‌دهند. تا آنجا که کشورها طرف چنین اسنادی هستند، موظفند با وضع رفتارهای مندرج در آن به عنوان جرایم کیفری در قوانین ملی، مقررات خود را اصلاح کنند. کشورهایی که بعضی از کنوانسیون‌ها و پروتکل‌های ضد تروریسم نیستند، از جمله با قطعنامه ۱۳۷۳ (۲۰۰۱)، آنها را تصویب و یا به آنها ملحق شوند (United Nations, 2001).

همچنین، چارچوب حقوقی جهانی برای مقابله با تروریسم، تعدادی از اسناد منطقه‌ای ضد تروریسم الزامات کیفری مربوط به زیرساخت‌های حیاتی را، به ویژه در زمینه زیرساخت‌های اطلاعات حیاتی ایجاد می‌کنند. کنوانسیون پیشگامانه در این زمینه، شورای اروپا در مورد جرایم رایانه‌ای در سال ۲۰۰۱ است که برای اولین بار در سطح بین‌المللی توصیفاتی درباره رفتار مجرمانه مربوط به نقض امنیت شبکه (علاوه بر ایجاد اختیارات و رویه‌هایی از جمله جستجو در شبکه‌های کامپیوتری و رهگیری). اخیراً، اتحادیه اروپا بخشنامه‌ای را تصویب کرده است که هدف آن، از جمله، هماهنگی قوانین کیفری کشورهای عضو در زمینه حملات علیه سیستم‌های اطلاعاتی است. نمونه اخیر دیگری، کنوانسیون ۲۰۱۴ اتحادیه آفریقا در مورد امنیت سایبری و حفاظت از داده‌ها است. (Brunner & Suter, 2008).

با تمام این اوصاف برای پر نمودن خلاء موجود، پیشنهاد می‌گردد در قالب یک کنوانسیون جامع بین‌المللی ابتدا تعریف جامع و مانعی از زیرساخت‌های حیاتی ارائه گردد و مصادیق آن برشمرده شود تا از تفاسیر مختلف در این زمینه پیشگیری شود. سپس، با توجه به اهمیت زیرساخت‌های حیاتی، کنوانسیون مزبور باید از ضمانت‌های اجرایی بالایی جهت متعهد و ملزم نمودن دولت‌ها در پیروی از آن داشته باشد. لازم به ذکر است بایستی تروریست دولتی نیز در این زمینه مورد توجه واقع شود تا بتواند ابعاد گسترده پدیده تروریسم را پوشش دهد.

## نتیجه‌گیری

پژوهشی که به آن پرداخته شد به دنبال پاسخ به این سوال بود که مقابله با حمله تروریستی به زیرساخت‌های حیاتی یک کشور تحت حاکمیت چه قاعده بین‌المللی قرار دارد؟ نتیجه‌ای که در پایان می‌توان گرفت محوریتش حول سوال فوق می‌باشد با این مضمون که حملات تروریستی بصورت عام در حقوق بین‌الملل تحت حاکمیت قواعد بین‌المللی می‌باشند، اما زمانی که بصورت خاص به آن نگرسته می‌شود، مشاهده می‌شود که حملات فیزیکی تروریستی به زیرساخت‌های حیاتی یک کشور و پرداختن به تبعات حقوقی آن در حقوق بین‌الملل در یک سند خاص حقوق

<sup>1</sup>. Critical Information Infrastructures



بین الملل یافت نمی‌شود. بنابراین، جامعه بین‌الملل در مواجهه با این حملات تروریستی با خلاء قواعد مواجه است و لذا نیازمند تدوین و تصویب یک کنوانسیون بین‌المللی جامع در این خصوص است. باید گفت حقوق بین‌الملل اسناد مختلفی برای نظارت بر حملات تروریستی به زیرساخت‌های حیاتی دارد، اما این اسناد صرفاً بر حملات تروریستی به زیرساخت‌های سایبری حاکمیت دارند. حملات فیزیکی به زیرساخت‌های حیاتی تحت حاکمیت هیچ کنوانسیون یا سند بین‌المللی جامعی نمی‌باشند. حملات سایبری از طریق حمله به منابع نرم افزاری یا سخت افزای هدف و ایجاد خسارات به آن صورت می‌گیرد بدون دخالت فیزیکی. اما حملات فیزیکی یا با استفاده از مواد منفجره و یا استفاده از پهپادها، موشک و... صورت می‌گیرد. در هر دو صورت زمانی که حمله به زیرساخت حیاتی یک کشور صورت بگیرد، ممکن است آنقدر خسارات غیرقابل جبران باشد که اقدامات بعد از حمله اثر چندانی نداشته باشد. همانگونه که در متن مقاله نیز به تفصیل به آن پرداخته شد؛ جامعه بین‌المللی، با توجه به اینکه اصطلاح «زیرساخت حیاتی» در ادبیات تحقیق حقوق بین‌الملل نوین است، توانسته همکاری میان دولت‌ها را در جهت مقابله با چنین حملاتی نظم ببخشد و از این رهگذر سبب کاهش حملات مزبور و خسارات ناشی از آن گردد. همانگونه که در فحوای کلام بیان شد، در حوزه حملات سایبری به زیرساخت‌های حیاتی، اقدامات مقتضی در عرصه تدوین و تصویب قواعد لازم الاجرا شده است، اما در حوزه حملات فیزیکی تروریستی به زیرساخت‌های حیاتی با خلاء قابل توجهی مواجه می‌باشد. در پاسخ به حل این خلاء، منسجم کردن همکاری و معاضدت بین‌المللی میان کشورها و تدوین و تصویب یک کنوانسیون جامع برای مقابله با حملات فیزیکی تروریستی به زیرساخت‌های حیاتی یک کشور پیشنهاد داده شد. ناگفته نماند که مصادیق زیرساخت‌های حیاتی در کشورهای مختلف متفاوت می‌باشد، پس لازم است ابتدا تعریف جامع و مانعی از زیرساخت‌های حیاتی ارائه گردد سپس مصادیق آن بصورت روشن مشخص گردد تا از تفاسیر غلط و مصادره به مطلوب کردن مفاهیم آن پیشگیری شود.

### منابع فارسی

۱. آل‌غفور، م.، صادقیان، ر. (۱۳۹۵). مدرنیزاسیون، جهانی شدن و پدیده تروریسم مدرن و پست‌مدرن، فصلنامه سیاست، شماره ۴(۳).
۲. حیدرقلی‌زاده، ج.، همکاران (۱۳۹۵). تحول تروریسم از منظر حقوق بین‌الملل، فصلنامه مطالعات حقوق بشر اسلامی.
۳. زرقانی، س.ح.، خوارزمی، ع. (۱۳۹۵). تحلیل تهدیدات تروریسم و امنیت زیرساخت‌های حیاتی یک شهر، همایش ملی پدافند غیرعامل و پایدار.
۴. سیمیر، ر. (۱۳۸۴). شکل‌گیری همکاری‌های بین‌المللی در مبارزه با تروریسم: فرصت‌ها، چالش‌ها و راه‌حل‌ها، فصلنامه تحقیقات سیاسی، ۲، ۱۴۷-۱۷۱.

۵. شانا (۱۳۹۹). حمله موشکی داعش به پالایشگاه نفت عراق، تارنمای خبری- تحلیلی شانا، در: <https://www.shana.ir/news/31018>
۶. علیخانی، م. (۱۳۹۴). قانون عدم استفاده از زور و دفاع از خود در شرایط قابل پیش بینی، فصلنامه مطالعات بین‌المللی، ۱۱(۴)، ۵۶-۲۱.
۷. فیرحی، د.، ظهیری، س. (۱۳۸۸). تروریسم، تعریف، تاریخچه و دستاوردهای موجود در تحلیل تروریسم، فصلنامه سیاست، ۳(۳).
۸. کازرونی، م (۱۳۹۵). چالش انطباق آزادی بیان با منع تروریسم برای استفاده از فضای مجازی، فصلنامه مطالعات بین‌المللی، ۱۲(۴)، ۱۹۸-۱۶۷.
۹. ملکی، م (۱۳۹۵). تعهدات حقوقی دولت‌ها برای پیشگیری از تروریسم بین‌المللی، پایان‌نامه کارشناسی ارشد، قم: دانشگاه قم.
۱۰. مهرگان، ع.، و همکاران. (۱۳۹۹). ضرورت اصلاح مأموریت کمیته بین‌المللی صلیب سرخ، فصلنامه مطالعات بین‌المللی، ۱۷(۲).
۱۱. نجف‌آبادی، س.، همکاران (۱۳۹۹). تحلیل آینده پژوهی حضور ناتو در خاورمیانه و مناطق اطراف ایران و تأثیر آن بر امنیت ملی جمهوری اسلامی ایران، فصلنامه مطالعات بین‌المللی، ۱۷(۳)، ۱۹۳-۱۶۹.

#### English References

1. Alcarz, Cristina., Zeadally Sherali. (2015).1 critical infrastructure protection: equirements and challenges for the 21<sup>st</sup> century, *International Journal of Critical Infrastructure Protection (IJCIP)*, 8. Elsevier Science.
2. Atigui, F. et.al.. (2020). “Vulnerability and Incident Propagation in Cyber-Physical Systems, in *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures*. Edited by John Soldatos, *James Philpot and Gabriele*, 193–205.
3. Brunner, E. M. and Suter, M. (2009). An Inventory of 25 National and 7 International Critical Information Infrastructures policies, *Center for Security Studies*, ETH Zurich.
4. CTED and UNOCT. (2018). The Protection of Critical Infrastructure against Terrorist Stacks: Compendium of Good Practices, *Interpol*.
5. Gelbstein, E. and Kamal, A. (2002). Information Insecurity – A Survival Guide to the Uncharted Territories of Cyber-Threats and Cyber-Security”, New York. <https://unp.un.org/details.aspx?entry=E04291#>
6. Mockaitis, T. R. (2006). *The New Terrorism: Myths and Rreality*, Praeger Security International, London: Westport
7. *UN Nations Office of Counter-Terrorism* (2019), International Legal Instruments, at:

- <https://www.un.org/counterterrorism/international-legal-instruments>.
8. Sánchez Frías, A. (2020). Bringing Terrorists to Justice in the Context of Armed Conflict: Interaction between International Humanitarian Law and the UN Conventions Against Terrorism. *Israel Law Review*, 53(1), 71–99. doi:10.1017/s0021223719000220.
  9. Schmid, A. (2020). Handbook of Terrorism Prevention and Preparedness, ICCT Press.
  10. Un Crisis Relief. (2019). "Yemen: The orst humanitarian crisis in the world", available in <https://www.un.org/counterterrorism/international-legal-instruments>
  11. United Nation. (2001). Security Council, available in S/RES/1373 (2001).
  12. UNODC. (2019). The Multi-Agency task force of the Middle East and North Africa Region, at: Multi-Agency Task Force (MATF) 3. <https://www.unodc.org/pdf/terrorism/MATF-2019/Fact>.
  13. USAGOV LOGO. (2007). U.S. Department of Homeland Security, *U.S. Department of Homeland Security*.

#### Translated References to English

1. Alcarz, Cristina., Zeadally Sherali. (2015).1 critical infrastructure protection: equirements and challenges for the 21<sup>st</sup> century, *International Journal of Critical Infrastructure Protection (IJCIP)*, 8. Elsevier Science.
2. Alghafour, M., Sadeghian, R. (2016). Modernization, globalization and modern and postmodern terrorism phenomenon, *Policy Journal*, Issue 4(3). **(In Persian)**
3. Alikhani, M. (2015). Non-use of force rule and self-defense in predictable conditions, *ISJ*, 4 (11). 21-56 **(In Persian)**
4. Atigui, F. et.al.. (2020). “Vulnerability and Incident Propagation in Cyber-Physical Systems, in Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures. Edited by John Soldatos, *James Philpot and Gabriele*, 193–205.
5. Brunner, E. M. and Suter, M. (2009). An Inventory of 25 National and 7 International Critical Information Infrastructures policies, *Center for Security Studies*, ETH Zurich.
6. CTED and UNOCT. (2018). The Protection of Critical Infrastructure against Terrorist Stacks: Compendium of Good Practices, *Interpol*.
7. Firahi, D. Zahiri, S. (2009). Terrorism, definition, history and existing achievements in analysis of terrorism, *Policy Journal*, Issue 3(3). **(In Persian)**

8. Gelbstein, E. and Kamal, A. (2002). Information Insecurity – A Survival Guide to the Uncharted Territories of Cyber-Threats and Cyber-Security”, New York. <https://unp.un.org/details.aspx?entry=E04291#>
9. Heidargholizadeh, J. et.al.. (2016). transformation of terrorism from the perspective of international law, *Journal of Islamic Human Rights Studies*. **(In Persian)**
10. Kazerouni, M. (2016). Challenge of adapting freedom of expression with prohibition of terrorism to use cyberspace, *International Studies Journal*, 12(4), 167-198. **(In Persian)**
11. Maleki, M. (2016). Legal obligations of the states to prevent international terrorism, M.A. thesis, Qom Uni. **(In Persian)**
12. Mehregan, A., et.al. (2020). the necessity for reforming the mission of International Red Cross Committee, *ISJ*, (17), 2. **(In Persian)**
13. Mockaitis, T. R. (2006). *The New Terrorism: Myths and Rreality*, Praeger Security International, London: Westport
14. Najafabadi, S. et.al.. (2020). Future study analysis of NATO presence in the middle east and areas around Iran and its effect on national security of the IRI., *International Studies Journal*, 17(3), 169-193. **(In Persian)**
15. *UN Nations Office of Counter-Terrorism* (2019), International Legal Instruments, at: <https://www.un.org/counterterrorism/international-legal-instruments>.
16. Sánchez Frías, A. (2020). Bringing Terrorists to Justice in the Context of Armed Conflict: Interaction between International Humanitarian Law and the UN Conventions Against Terrorism. *Israel Law Review*, 53(1), 71–99. doi:10.1017/s0021223719000220.
17. Schmid, A. (2020). *Handbook of Terrorism Prevention and Preparedness*, ICCT Press.
18. Shana (2021). *Daesh Rocket Attack on Iraqi Oil Refinery*, at: <https://www.shana.ir/news/31018> **(In Persian)**
19. Simbar, R. (2006). Formation of international cooperation in counterterrorism: opportunities, challenges and solutions, *Political Science Research*, 2, 147-171. **(In Persian)**
20. Un Crisis Relief. (2019). "Yemen: The orst humanitarian crisis in the world", available in <https://www.un.org/counterterrorism/international-legal-instruments>
21. United Nation. (2001). Security Council, available in S/RES/1373 (2001).
22. UNODC. (2019). *The Multi-Agency task force of the Middle East and North Africa*

- Region, at: Multi-Agency Task Force (MATF) 3.  
<https://www.unodc.org/pdf/terrorism/MATF-2019/Fact>.
23. USAGOV LOGO. (2007). U.S. Department of Homeland Security, *U.S. Department of Homeland Security*.
24. Zarghani, S.H., Kharazmi, O. A. (2016). Analysis of Terrorism Threats and Security of Critical infrastructures of a City, *National Conference on Non-Active Defense and Sustainable*. **(In Persian)**

