فصلنامه پژوهش‌های ارتباطی/ سال بیستم/ شماره ۱ (پیاپی ۷۳) / بهار ۱۳۹۲/ ۴۲ ـ ۹
Quarterly Journal of Communication Research, 2013, Vol. 20, No. 1 (73), 9-42

مواجهه با تروریسم سایبری در حقوق بین‌الملل کیفری

پیمان نمامیان*

چکیده

تروریسم سایبری یکی از روزآمدترین مصادیق تروریسم است که به سبب بهره‌گیری غیرقانونی از فناوری و ابزارهای الکترونیکی و رایانه‌ای در فضای مجازی، به طور عمده از سوی بازیگرانی که به این علوم نوین دسترسی دارند وآنها را در راه اهداف راهبردی علیه ملت‌های جهان سوم به کار می‌گیرند، موجبات تهدیدهای فزاینده‌ای را در عرصه بین‌المللی فراهم کرده است. از این رو، فارغ از اینکه در اغلب موارد، غرب به عنوان منشأ اصلی راهبردی کردن تروریسم سایبری، خود مدعی مقابله با آن است، اسنادی بین‌المللی به منظور پیشگیری و سرکوب کلیه اشکال تروریسم به ویژه تروریسم سایبری، تدوین و تصویب شده است. که از منظر آسیب شناختی می‌توان گفت اسناد مزبور نه تنها توفیقی در مقابله با این پدیده نوظهور نداشته‌اند، بلکه شکاف‌های موجود و زمینه رشد و گسترش فزاینده آن را در عرصه‌های ملی و بین‌المللی فراهم کرده‌اند. به این ترتیب، در مقاله حاضر، ضمن بررسی و تبیین تروریسم سایبری و ارائه مفاهیم گوناگون از آن، اسناد بین‌المللی در چارچوب حقوق بین‌الملل کیفری مورد ارزیابی قرار خواهد گرفت.

کلید واژه‌ها: تروریسم سایبری، فضای مجازی، اسناد و کنوانسیون‌های بین‌المللی، حقوق بین‌الملل کیفری

---

* پژوهشگر حقوق کیفری، مدرس دانشگاه آزاد اسلامی واحد کرمانشاه Email: p_namamian1512@yahoo.com

تاریخ دریافت:۹۰/۱۱/۲۳ تجدید نظر: ۹۱/۲/۱۵ پذیرش نهایی: ۹۱/٤/۲۱

مقدمه

گسترش فزاینده «فناوری اطلاعاتی و ارتباطاتی[1]» منجر به تحول و دگرگونی جوامع در ابعاد مختلف سیاسی، امنیتی، اقتصادی و اجتماعی شده است. ویژگی‌های جوامع امروزی همچون «اقتصاد اطلاعاتی[2]»، «فرهنگ مجازی[3]» و کاهش اهمیت زمان و مکان در تعاملات اجتماعی، ویژگی متمایزی به هزاره سوم بخشیده که اصل بنیادین آن اهتمام محوری فرد در عرصه فعالیت‌های اجتماعی، سیاسی و اقتصادی با بهره‌گیری از ابزارهای نوین اطلاعاتی و ارتباطی است. در چنین فضایی که با عنوان «فضای مجازی[4]»توصیف می‌شود، تهدیدهای نوینی همانند جنگ مجازی، «جنگ اطلاعاتی[5]»، تروریسم سایبری، «پدیده هکرها[6]» و سرقت اطلاعات محرمانه نهادهای امنیتی و اطلاعاتی پدید آمده‌اند که می‌توانند امنیت ملی کشورها را با چالش جدی مواجه سازند. به علاوه، پیشرفت فنی در زمینه ارتباطات، موجب ظهور قواعد حقوقی و به تبع آن، رفتارهای نوین فاصله‌گیر از هنجارها شده است که این موضوع، نه تنها اموال، بلکه اشخاص و دولت‌ها را نیز در بر می‌گیرد و آنها را تحت حمایت قرار می‌دهد (جلالی‌فراهانی، ۱۳۸۷، صص ٤١ـ ٤٠).

در این میان، یکی از مهم‌ترین تهدیدهای نوظهور، تروریسم سایبری است که به واسطه کاربست فزاینده فناوری‌های اطلاعاتی و ارتباطاتی از سوی دولت‌ها برای تسریع، افزایش کارایی و کاهش هزینه‌های مرتبط با خدمت رسانی به شهروندان، اهمیت فزاینده‌ای پیدا کرده است. به گونه‌ای که حتی دولت‌ها نیز از تروریسم سایبری به عنوان ابزاری در الگوهای تنازعی خود استفاده می‌کنند. در این میان، مهم‌ترین مولدهای ناامن‌کننده فضای مجازی در بُعد تروریسم، در دو گروه عمده طبقه‌بندی می‌شوند؛ گروه اول، کسانی که به یک کشور خارجی وابسته‌اند، از قبیل بخش‌های نظامی، سازمان‌های امنیتی و شرکت‌هایی که وابستگی زیادی به دولت آن کشور دارند؛ و گروه دوم؛ تروریست‌ها و گروه‌های افراطی. این افراد، ممکن است به دولت خاصی وابستگی نداشته باشند، ولی در جهت اهداف خود اقدام به خرابکاری مبادرت می‌کنند (نورمحمدی، ۱۳۹۰، ص ۷۷).

---

1. communication and information technology
2. information economy
3. virtual culture
4. cyber space
5. information warface
6. hacker

با این حال، «تروریسم سایبری» را می‌توان چهره جدیدی از تروریسم دانست که گسترش فناوری و خلق فضای مجازی، آن را ایجاد کرده است (پاکزاد، ۱۳۷۵، ص ۲). در حقیقت، فناوری ابزار جدیدی را در اختیار تروریست‌ها قرار داده است که با استفاده از آن و بدون آنکه خطرهای سایر اقسام تروریسم را برای آنها در پی داشته باشد، می‌توانند اهداف وحشت بار خود را پی بگیرند. گسترش استفاده از این فضای مجازی که از دهه ۱۹۹۰ شدت گرفته است، امکان رسیدن تروریست‌ها به اهدافشان را بیشتر کرده است. حضور میلیون‌ها کاربر در دنیای مجازی، همراه با شرکت‌ها، کارخانجات و صنایع عمده بسیار که در اغلب موارد از قابلیت آسیب‌پذیری بالایی برخوردارند، خطر استفاده سوء از فضای مجازی را بیشتر کرده و جذابیت آن را نیز افزایش داده است (کارگری، ۱۳۹۰، صص ۷۳ـ ۷۲).

بر پایه آنچه اظهار شد می‌توان تصریح کرد که برای بهره‌برداری صحیح و مفید از امکانات سایبری باید هنجارهایی را مقرر کرد و با ناهنجاری‌ها به مقابله پرداخت. این هنجارها باید بر مبنای ویژگی‌های منحصر به فرد در فضای سایبر تدوین شوند (رضوی، ۱۳۸۸، صص ۱٦٥ـ ۱٦۱). از این رو، برای پیشگیری از تهدیدهای ناشی از ناهنجاری‌های برآمده از فضای سایبری، تاکنون اسناد متعددی به تصویب رسیده است اما با وجود تنوع این اسناد در نظام‌های ملی و بین‌المللی، متأسفانه هیچ یک از آنها موجبات تحقق وضعیتی مطلوب را در مواجهه با تهدیدها فراهم نکرده است.

پیشینه پژوهش

جرایم سایبری از زمان پیدایش تاکنون، با سه نسل یا تیپ مواجه بوده است. دهه‌های شصت، هفتاد و اوایل هشتاد، زمان حاکمیت نسل اول، با عنوان جرایم رایانه‌ای است. در این زمان، در خصوص جرایم، محوریت بحث با رایانه و از این رو، تعداد توصیف‌های مجرمانه بسیار کم بود.

به تدریج در دهه هشتاد تا اوایل دهه نود، نسل دوم به میان آمد و بحث محتوا مطرح شد یعنی موضوع جرایم داده و اطلاعات مورد توجه قرار گرفت.

پس از چهار یا پنج سال، حاکمیت نسل سوم که از آن به جرایم سایبری یاد می‌کنیم، فرا رسید. ویژگی این نسل، تجمیع رایانه با مودم و مخابرات (اعم از ماهواره)

با حالت‌های شبیه‌سازی و مجازی‌سازی است. در این نسل، تأکید بر رایانه نیست؛ بلکه رایانه خود وسیله ارتکاب جرم است. جرایم نسل سوم در بستر ابر شاهراه‌های الکترونیکی اطلاعاتی و ارتباطی به وقوع می‌پیوندند (گرایلی، ۱۳۸۹، صص ۱٦۱ــ ۱٦۰ و ابوالمعالی الحسینی و علیزاده طباطبایی، ۱۳۸۷، صص ۱٤۷ـ ۱٤۳).

اگر در چهار دهه حاکمیت جرایم رایانه، شاهد جرایم انگشت‌شماری بوده‌ایم؛ در فضای سایبر، پنج دسته اصلی جرم وجود دارد که هر کدام بالغ بر چندین عنوان مادر و عمده می‌شوند چنان که شاید تعداد مصادیق عمد و غیرعمد آن بالغ بر ۲۰۰ عنوان مجرمانه شود (شیرزاد، ۱۳۸۸، صص ٤۲ـ ۳۸).

با این حال، واژه سایبر تروریسم در دهه ۱۹۸۰ از سوی باری کالین[1] ابداع شد. از طرفی شاید بتوان گفت جامع‌ترین تعریف از سایبر تروریسم را دنینگ[2] ارائه کرده است.

تعریف وی از سایبر تروریسم چنین است: «سایبر تروریسم، حاصل تلاقی تروریسم و فضای مجازی است». سایبر تروریسم، بیشتر به معنای حمله یا تهدید به حمله علیه رایانه‌ها، شبکه‌های رایانه‌ای و اطلاعات ذخیره شده در آنهاست، هنگامی که به منظور ترساندن یا مجبور کردن دولت یا اتباع آن برای پیشبرد اهداف سیاسی یا اجتماعی خاص اعمال می‌شود (سیمبر، ۱۳۸۰، ص۷۰). هر حمله، برای اینکه به عنوان سایبر تروریسم شناخته شود، باید به خشونت علیه اشخاص یا دارایی‌ها بینجامد یا دست‌کم، آسیب کافی برای ایجاد ترس را باعث شود. برای مثال می‌توان از حملاتی که منجر به مرگ یا صدمات بدنی، انفجار، سقوط هواپیما، آلودگی آب یا خسارهای متعدد اقتصادی می‌شوند، نام برد. حملات جدی علیه زیر ساخت‌های حیاتی نیز بسته به نوع شدت و تأثیر می‌تواند اقدامی سایبر تروریستی باشد اما حملاتی که خدمات عمومی غیرحیاتی را مختل می کنند یا تنها سر و صدای پرهزینه‌ای را موجب می‌شوند، را نمی‌توان به عنوان سایبر تروریسم طبقه‌بندی کرد (انعامی و طابنده، ۱۳۹۰، صص ۳۰ـ ۲۹).

ارتباط تروریسم و رسانه

فناوری اطلاعاتی، ارتباطاتی و رسانه‌ها بنیان جوامع مدرن معاصر را در دهه‌های اخیر شکل داده است و به لحاظ سیر تاریخی، این دوره، به دوره جامعه اطلاعاتی، جامعه

1. Barry Collin 2. Denning

شبکه‌ای، جامعه مجازی، جامعه دیجیتالی و غیره موسوم شده است. ظهور این فناوری‌ها و ایجاد تحولات بنیانی در جوامع از این طریق، با هدف ساماندهی و تعاملات سیاسی، اجتماعی، اقتصادی و فرهنگی بشر بوده است (حاجیانی، ۱۳۸۸، صص ۱۰۳_ ۹۷).

با این حال، جامعه موسوم به جامعه اطلاعاتی و ارتباطی جامعه‌ای است که نقطه مرکزی آن، موفقیت عملی در پردازش، ذخیره و انتقال اطلاعات و کاربرد فناوری‌های اطلاعاتی و ارتباطی است و قابلیت گسترش به کل جهان را دارد. از این رو، می‌توان شبکه اطلاعاتی و ارتباطاتی را در عصر فناوری اطلاعات و ارتباطات به مثابه شبکه برق در عصر صنعتی دانست. به این ترتیب، چنین جامعه‌ای را می‌توان این گونه توصیف کرد: «جامعه اطلاعاتی درواقع، تولید، پردازش و انتقال حجم عظیمی از داده‌ها درباره کلیه حوزه‌های فردی، ملی، اجتماعی، تجاری، اقتصادی و نظامی است» به هر روی، هر اندازه که فناوری روز به افق‌های نوین دست می‌یابد، دگردیسی نوینی در فرایند شکل‌گیری و رفتار نهادها و سازمان‌ها و به طور کلی، زیرساخت تعاملات اجتماعی، سیاسی، اقتصادی و فرهنگی بشر ایجاد می‌شود (بختیاری و همکاران، ۱۳۸۹، صص ۱۱۰_ ۱۰۶).

با این اوضاع اکثر مطالعاتی که در زمینه ارتباط میان تروریسم و رسانه صورت گرفته است، تمرکز خود را بر پاسخی که از طرف رسانه نسبت به رویدادهای تروریستی داده می‌شود، قرار داده‌اند. آنها به طور کلی به این نتیجه رسیده‌اند که ارتباط میان تروریسم و رسانه، ارتباطی همزیستانه است و گروه‌های تروریستی از رسانه به عنوان ابزاری برای رساندن پیام‌های خود به گروه مخاطبان هدف استفاده می‌کنند. رسانه‌های جمعی نوین تنها با اعلام آنچه انقلابیون انجام می‌دهند، ابزارهای مهمی برای تبلیغات هستند. جنگ اعصاب یا جنگ روانی، یکی از روش‌های مبارزه بر پایه کاربرد مستقیم یا غیرمستقیم رسانه‌های جمعی است. واژه «تروریسم رسانه‌ای» برای اشاره به روش‌های پیچیده بهره‌برداری تروریست‌ها از پوشش رسانه‌ای اعمال خود، به وجود آمده است. تروریست‌ها در صورت اعلام نکردن هویت خود و یا طرح تقاضا و هشدار مورد نظر، هرگز از عملیات خشونت‌آمیز خود سود نمی‌برند. تروریست‌های رسانه‌گرا از پنج اصل پیروی می‌کنند که عبارت‌اند از:

– اعمال آنها با هدف جلب نظر شهروندان صورت می‌گیرد و ماهیت تاکتیکی دارد.
– قربانیان به گونه‌ای انتخاب می‌شوند که حداکثر ترس را در مردم ایجاد کنند و بیشترین تأثیر را بر آنها بگذارند.
– رسانه‌ها خشونت تروریست‌ها را پوشش می‌دهند.
– تروریسم موجب هدایت و همچنین فریب رسانه‌ها برای پوشش تبلیغاتی اعمال تروریستی است.
– دولت‌ها چاره‌ای ندارند جز آنکه خبر ترورها را سانسور کنند و یا آن را از طریق رسانه‌ها پخش کنند. شکی نیست که در ادبیات تحقیقاتی تروریسم، رسانه‌ها زمینه‌ساز تقلید اعمال تروریستی به شمار می‌روند.

مفهوم‌شناسی تروریسم سایبری: ارزیابی تفسیری

یکی از پدیده‌های مهم و بحث برانگیز بین‌المللی، منطقه‌ای و داخلی در دهه نخست سده ۲۱ و یکی از اساسی‌ترین معضل‌ها و چالش‌های جامعه جهانی در خصوص حقوق ملت‌ها و ثبات بین‌المللی مسئله تروریسم بوده است (کرم‌زاده، ۱۳۸۱ و صادقی حقیقی، ۱۳۸۳).

در عصر ما، تروریسم از تهدیدی ملی به تهدیدی بین‌المللی و جهانی مبدل شده است و حتی این نگرانی وجود دارد که با گسترش آن صلح و امنیت بین‌المللی به مخاطره بیفتد. در عصر جهانی شدن و پیشرفت فناوری، دیگر تروریسم در مرزهای ملی و منطقه‌ای محصور نمی‌ماند. تروریست‌ها همگام با روند جهانی شدن، پیشرفت کرده‌اند، اما هرگز در قید و بندهای بین‌المللی ناشی از آن گرفتار نیامده‌اند. از این رو هیچ منطقه، دولت یا ملتی از اقدامات آنها در امان نمی‌ماند. گروه‌های تروریستی با انگیزه‌های گوناگون دست به عملیات تروریستی می‌زنند و نگرانی از احتمال وقوع این گونه عملیات زمانی بیشتر می‌شود آنان از تسلیحات هسته‌ای، شیمیایی و بیولوژیک استفاده کنند (رابرت[1] و هایر[2]، ۲۰۰۱ و الکساندر[3]، ۲۰۰۱).

هر چند این تهدیدها در حال حاضر، به صورت بالفعل صلح و امنیت بین‌المللی را تخریب می‌کنند، باید اذعان کرد که تروریسم سایبری، تهدیدی بالقوه علیه جامعه بین‌المللی است که روش نوینی از اقدامات تروریستی به شمار می‌رود و نه نوع دیگری

1. Robert 2. Heyer 3. Alexander

از تروریسم (استارک[1]، ۱۹۹۹، ص ۹)؛ چنان که مجمع عمومی سازمان ملل در سال ۱۹۹۵ با صدور قطعنامه‌ای این موضوع را مورد عنایت قرار داد.(۱)

تروریسم سایبری که ازجمله مصادیق جرایم تروریستی نوین است، زنگ خطری جدی برای تمام مردم دنیا و نیز دولت‌ها تلقی می‌شود.

با وجود این، فرایند برخورد با تروریسم سایبری به نسبت تروریسم کلاسیک و سنتی نه در سطح تقنینی و نه در سطح حمایت‌های اجتماعی، چندان قابل ملاحظه و توجه نیست. در کنار این مسائل، اساسی‌ترین مشکل در برخورد با این پدیده، فقدان تعریفی صحیح و جامع از آن است. تلاش‌های بین‌المللی گسترده‌ای در این زمینه صورت نگرفته و سندی به تصویب دولت‌ها نرسیده است.

نکته مورد اهتمام در خصوص «فضای مجازی» این است که فضای مزبور، چه حوزه و کدام سیستم‌ها را تحت پوشش قرار می‌دهد؟ آیا تنها سیستم رایانه‌ای معمولی و سامانه دنیای مجازی اینترنت را در بر می‌گیرد؟ به نظر می‌رسد علاوه بر سیستم یاد شده، هر گونه دستگاهی را که دارای برنامه‌ای باشد، شامل می‌شود (زراعت و دانشوری، ۱۳۸۹، صص ۱٤٥ـ ۱٤٤).

در تأیید این نظر علاوه بر «فرهنگ آکسفورد[2]» که در مقام تعریف «سایبر» بیان می‌دارد: «مرتبط شدن با شبکه‌های مخابراتی الکترونیک بویژه اینترنت(۲)»، بند یک ماده اول «کنوانسیون بوداپست» نیز که تنها کنوانسیون موجود در باب جرایم رایانه‌ای است، سیستم رایانه‌ای را این گونه تعریف می‌کند: «سیستم کامپیوتری عبارت است از یک دستگاه یا مجموعه‌ای از دستگاه‌های متصل یا مرتبط به هم که به وسیله یک برنامه، داده‌های دیجیتال را به طور خودکار پردازش می‌کند(۳)».

البته تعاریف کامل‌تر و جامع‌تری نیز در این زمینه قابل ارائه است؛ ازجمله: «تروریسم سایبری، عبارت است از حمله عمدی با انگیزه سیاسی علیه اطلاعات، سیستم‌های کامپیوتری، برنامه‌های کامپیوتری و داده‌ها که به وسیله گروه‌های خرده ملی یا عوامل مخفی به خشونت علیه اهداف غیرنظامی منجر شود» (زراعت و دانشوری، ۱۳۸۹، ص ۱٤٦).

برخی، تروریسم سایبری را به عنوان حملات از قبل طراحی شده با انگیزه‌های سیاسی تعریف می‌کنند که علیه سیستم‌های رایانه‌ای، برنامه‌های رایانه‌ای و اطلاعات

1. Stark 2. Oxford English Dictionary

ذخیره شده در فضای مجازی صورت می گیرد، با این شرط که این اقدام‌های منجر به خشونت علیه اهداف غیرنظامی از سوی عاملان مخفی یا گروه‌های ملی شود. این تعریف که تعریفی نتیجه‌گراست، نمی تواند درست باشد، زیرا آنچه سایبری بودن یک اقدام تروریستی را تعریف می‌کند، ابزارِ بزه تروریستی است، نه نتیجه آن. بدون تردید، تخریب مادّی یک رایانه، انفجار یک مرکز رایانه‌ای یا اقداماتی از این دست، گرچه در عمل نتیجه خود را به صورت اختلال در سیستم رایانه‌ای بر جای می گذارد، اما نمی‌تواند بزه سایبری تلقی شود. از سوی دیگر، برخی معتقدند که تروریسم سایبری، عبارت است از استفاده از شبکه رایانه ای به عنوان ابزاری برای از کار انداختن زیرساخت های اساسی و تحت تأثیر قرار دادن یا وادار کردن دولت یا جمعیت غیرنظامی؛ مراد از زیرساخت اساسی نیز سیستم‌ها یا تأسیساتی هستند که در صورتِ تخریب، بر امنیّت فیزیکی، امنیت اقتصادی و یا سلامتی عمومی تأثیر می‌گذارند و خود، شاملِ صنایع یا فعالیت های غذایی، انرژی، حمل و نقل، بانکداری، ارتباطات، دولت و یا فضای مجازی می شوند(اُون[1]، ۲۰۰۸، ص ۳۶).

در کنار این دو تعریف، گروهی دیگر تروریسم سایبری را بر اساس ابزار و نتیجه تعریف کرده‌اند. طبق این تعریف، تروریسم سایبری عبارت است از اقدامی که با استفاده از رایانه برای انجام حملات غیرقانونی و تهدید به حمله علیه رایانه‌ها، شبکه‌ها و اطلاعات ذخیره شده الکترونیکی صورت می‌گیرد و منظور از آن، ایجاد رعب و وحشت در قربانی، و یا وارد آوردن صدمه به او است (عباسی، ۱۳۸۳، ص ۳ و کارگری، ۱۳۹۰، ص ۷٤).

با این حال، ضرورت ارائه تعریفی جامع و مانع از تروریسم سایبری که در ضمن، مورد توافق همه کشورها نیز باشد، بر اساسِ اصل «هیچ جرم و هیچ مجازاتی بدون قانون متصور نیست» آشکار و بدیهی است. به طور کلی، با وجود تلاش‌های بین‌المللی، تاکنون هیچ تعریفی که مورد توافق همه کشورها باشد، از پدیده تروریسم ارائه نشده است. اگر توافقی بر سر تعریف بین‌المللی تروریسم حاصل شود و منجر به تصویب کنوانسیونی در عرصه بین‌المللی گردد، قوانین داخلی به میزان کمتری به مرحله اجرا در خواهد آمد و از بسیاری از چالش‌ها و نزاع‌های بین‌المللی خواهند کاست. البته، این

1. Owen

نکته را نیز باید در نظر داشت که ارائه تعریفی کلی از پدیده تروریسم سایبری (و به طور کلی سایر جرایم تروریستی) گذشته از برخی محاسن، بسیار خطرناک خواهد بود؛ چرا که احتمال سوء استفاده قدرت‌های حاکم و تفسیر خودسرانه و دلخواه آنها وجود دارد (نجفی ابرندآبادی، ۱۳۸٦).

تروریسم سایبری به مثابه تهدیدی نوین

گروه‌های تروریستی از اینترنت برای اهداف گوناگونی همچون اطلاع‌رسانی، تبلیغات، جذب نیروی انسانی و جمع‌آوری اطلاعات استفاده می‌کنند (ویمان[1]، ۲۰۰٦). شبکه اطلاع‌رسانی رایانه‌ای برای تروریست‌های اطلاع‌رسان، مطلوب به نظر می‌رسد؛ چرا که به دلیل متمرکز نبودن، کنترل یا محدودسازی آن دشوار است و امکان دستیابی را برای هر شخصی ممکن می‌سازد. با این حال، به طریق دیگری هم می‌توان هم به عنوان یک ابزار مستقیم برای حمله و هم به عنوان یک سلاح مستقیم از فضای مجازی استفاده کرد (گوردون[2]، ۲۰۰۷، صص ۹ـ ۸).

یک راه استفاده از سلاح فضای سایبری، حملات سایبری به وب سایت‌هاست؛ برای مثال، حملاتی که در مناقشه «هند ـ پاکستان» و درگیری «رژیم صهیونیستی ـ فلسطین» یا حمله به وب سایت‌های ناتو در خلال بحران کوزوو در اوایل دهه ۱۹۹۰شکل گرفته‌اند (پریچارد[3] و مک‌دونالد[4]، ۲۰۰٤، صص ۲۸۱ـ ۲۷۹). این حملات، هنوز تروریستی به شمار نمی‌روند؛ چون باعث صدمات جانی نمی‌شوند و نیت آنها اعمال نفوذ بر یک دولت نیست؛ به واسطه تعریف تروریسم در کنوانسیون بین‌المللی، سرکوب تأمین مالی تروریسم الزامی شمرده می شود. راه دیگری برای استفاده از فضای مجازی به عنوان یک سلاح، «تروریسم سایبری» است. با این حال، تروریسم سایبری؛ یعنی استفاده از شبکه‌های رایانه‌ای برای ایجاد صدمات جانی یا سابوتاژ (خرابکاری) در زیرساخت‌های بحرانی کشور به طریقی که منجر به صدمات جانی بشود (دیه‌نینگ[5]، ۲۰۰۰). البته، برخی دیگر انواع شبکه‌هایی را که هدف حملات تروریسم سایبری هستند، متمایز کرده‌اند:

1. Weimann 2. Gordon 3. Prichard
4. MacDonald 5. Denning

شبکه دفاع نظامی و غیرنظامی، شبکه های دولتی (پلیس و آتش نشانی)؛ شبکه‌های تحت تملک خصوصی یا دولتی که برای کنترل خدمات شهری همگانی به کار می‌روند و سایر شبکه‌های فراهم‌کننده خدمات زیرساخت (آب، برق)؛ و شبکه‌های همگانی مورد استفاده مصرف‌کنندگان و مشاغل در زمینه اطلاع رسانی، آموزش و ... (تراچمان[1]، ۲۰۰٤).

همان گونه که گفته شد، تروریسم سایبری به زیرساخت‌های رایانه‌ای شده‌ای که جوامع پیشرفته به آن وابسته شده‌اند، صدمه می‌زند. پس، میزان آسیب‌پذیری جوامع مختلف از تروریسم سایبری بر حسب میزان وابستگی آنها به فناوری و شبکه‌های رایانه‌ای متفاوت خواهد بود. بنابراین، هر چه وابستگی یک کشور به شبکه‌های پردازش اطلاعات و ارتباطات الکترونیکی بیشتر باشد آسیب‌پذیری آن از تروریسم سایبری بیشتر خواهد بود. همان گونه که «ریچارد کلارک» در سال ۱۹۹۹ مطرح کرده است: «اگر متصل باشید [به اینترنت] آسیب‌پذیر هستید» (کلارک[2]، ۲۰۰۰-۱۹۹۹، صص ۲۹ـ ۲۸).

یک ویژگی متمایز دیگر برای تروریسم سایبری هزینه‌های به نسبت پایین آن است. حمله تروریستی در جهان فیزیکی، مستلزم جذب یک اجراکننده، تجهیز او به سلاح یا مواد منفجره و اطمینان از عبور او از تمام ایست‌های بازرسی امنیتی تا مکان تعیین شده است. از طرف دیگر، تروریسم سایبری به احتمال قوی این هزینه‌ها را برای ترویست پس‌انداز می‌کند و این موانع را از سر راه برمی‌دارد. اقدام به حمله سایبری مشتمل بر خرید سلاح یا حضور واقعی در مکان حمله نیست. تمام آنچه تروریست سایبری نیاز دارد یک رایانه خوب و مهارت هک کردن بیشتر از حریف اوست (نورمحمدی، ۱۳۹۰، صص ۸٦ ـ ۸٤).

با وجود تمام پیش‌بینی‌های صورت گرفته از تهدیدهای ناشی از تروریسم سایبری، تاکنون یک مورد از تروریسم سایبری واقعی ثبت نشده است. این امر مسلم، مردم را به این فکر وامی‌دارد که پیش‌بینی‌ها در مورد تروریسم سایبری اغراق‌آمیز هستند. با وجود این، لازم است به بررسی دقیق مسئله پرداخته شود. به بیان دیگر، اینکه واقعه‌ای هنوز رخ نداده، احتمال وقوع آن در آینده را متأثر نمی‌سازد. ابرقدرت‌های نظام بین‌المللی مدت‌هاست که در حال آماده‌سازی یک سناریو برای جنگ هسته‌ای هستند، ولو این آماده‌سازی مبتنی بر واقعه‌ای باشد که خوشبختانه هنوز به وقوع نپیوسته است.

1. Trachtman 2. Clarke

نگرش اسناد بین‌المللی در مواجهه با تروریسم سایبری

۱. کنوانسیون مونترال

ماده نخست کنوانسیون مونترال (کنوانسیون در مورد سرکوب اعمال غیرقانونی علیه ایمنی هواپیمایی کشوری) جرایم را در چارچوب اجرای کنوانسیون تعریف کرده است. بعضی کشورها طی ژرف‌اندیشی در مورد پیش‌نویس کنوانسیون، رویکرد برشمردن را ترجیح می‌دادند که تعداد محدودی از جرایم خاص را فهرست می‌کرد[٤]؛ در حالی که سایرین طرفدار یک تعریف عمومی بودند.[٥] استدلال گروه دوم، این بود که پذیرش فهرست جرایم لزوماً به این معناست که اعمال آینده که در زمان پیش نویس کنوانسیون غیرقابل پیش‌بینی بودند، خارج از چارچوب اجرای کنوانسیون قرار خواهند گرفت (آبراموسکی[1]، ۱۹۷۵، صص ۲۸۰ـ ۲٦۸). پس از بحث و جدل هر چند تعریف به صورت کاملاً جامع پیش‌نویس شد، اما باعث شک و تردید در مورد اختلاف واقعی این دو رویکرد شد. ماده (۱) ۱ پنج جرم جایگزین ارتکابی از سوی مجرم اصلی را اعلام کرده و ماده (۲) ۱ مبادرت و معاونت جرم‌انگاری کرده است (کوشا و نمامیان، ۱۳۸۷؛ نمامیان، ۱۳۸۸ و گلدوزیان و نمامیان، ۱۳۸۹). با توجه به تهدید تروریسم سایبری که در زمان پیش‌نویس کنوانسیون مونترال مقرر نشده، این مسئله به ذهن متبادر می‌شود که آیا جرایم مقرر در ماده ۱ برای تروریسم سایبری کاربردپذیر هستند؟ کنوانسیون مونترال برخلاف سایر کنوانسیون‌ها، بندی از تعاریف را در بر ندارد که به تفسیر مقرره‌های آن کمک کند. بنابراین، تحلیل حقوقی متن بر پایه مبانی تفسیر مقرر شده در کنوانسیون وین و سایر رهنمودهای تفسیر استوار است که اصولاً شامل پروتکل‌های کنفرانس مونترال که پیش‌نویس کنوانسیون را تصویب کرد[٦] و ادبیات مربوط می‌شود (کوهن[2]، ۲۰۱۰، ص ١٦).

نقطه آغاز بحث، هر پنج مورد مقرر شده در ماده ۱ است که گویای این برداشت کلی است که منظور کنوانسیون به جای حفظ جان انسان، حفظ سلامت هواپیمای در حال پرواز بوده است. بنابراین، به خطر انداختن عمدی جان یک مسافر بدون به خطر انداختن ایمنی هواپیما از جرم های تحت پوشش این کنوانسیون نیست.

---

1. Abramovsky 2. Cohen

از طرف دیگر، می توان استدلال کرد کـه درواقـع نمـی‌تـوانیم ایـن دو عنصـر را از یکدیگر جدا کنیم؛ کسی نمی‌تواند ایمنی هواپیما را بدون به خطر انداختن جان خدمه و مسافران آن به خطر بیندازد همچنانکه نمی‌تواند جان خدمه و مسافران را بدون به خطـر انداختن ایمنی هواپیما در معرض خطر قرار دهد.(۷)

شایان ذکر است که مطابق با مفاد مقرر در ماده ۱ هیچ شرط الزامـی وجـود نـدارد کـه مرتکب جرم یا معاون او سوار بر هواپیما باشد. این ویژگی دیگر کنوانسیون مونترال است که باعث شده است از کنوانسیون لاهه پیشرفته‌تر باشد. بـرخلاف کنوانسـیون‌هـای لاهـه، مقرره‌های کنوانسیون مونترال در شرایطی که مجرم سوار بر هواپیما یـا روی زمـین باشـد، کاربردپذیرند و این، باعث افزایش احتمال مناسب بودن کنوانسیون مونترال برای رسـیدگی به تروریسم سایبری علیه یک هواپیما می‌شود؛ زیرا همان گونه که در قبل ذکر شد یکی از مزیت‌های تروریسم سایبری توان اجرای حمله از مکانی دوردست است (همان، ص ۱۹).

کنوانسیون مونترال به جرایم ارتکابی در یـک هواپیمـای مـورد اسـتفاده نیـز کـه بـا هواپیمای در حال پرواز فرق دارد، نیز رسیدگی می‌کند.(۸) این امر، باعث تمدیـد مـدت زمان کاربرد مقرره‌های کنوانسیون می‌شود. بیشـتر کشـورهای شـرکت‌کننـده، در مـورد پذیرش پیش‌نویس کنوانسیون درباره «مورد استفاده بودن هواپیما» تردیـد داشـتند. آنهـا، معتقد بودند تا زمانی کـه مجـرم سـوار بـر هواپیمـا مشـمول دسـتگیری و محاکمـه در کشوری باشد که هواپیما در آنجا به تصرف درآمده، هیچ نیازی به مداخلـه بـین‌المللـی وجود ندارد. این نکته مبین آن است که به ظاهر محدودیت کنوانسـیون مجـازات ماننـد قبل است نه پیشگیری.

تحلیل زیر بر اساس این نقاط، ابتدا، این مسئله را مورد بررسی قرار می‌دهد که آیا مـوارد متفاوتی که در ماده ۱ مقرر شده‌اند، برای تروریسم سایبری کاربردپذیر هستند یا خیر، شـایان به ذکر است که جنبه اصلی تحلیل بیشتر یک جنبه حقوقی است تا یک جنبه فنی.

الف) قانون خشونت علیه شخصی که در هواپیماست و احتمالاً ایمنی هواپیما را بـه خطر می‌اندازد: ماده (الف) (۱) ۱ برای پیشگیری و مجازات اعمال خشـونت‌آمیـز علیـه مسافران هواپیما منظور شده است. واژه «قانون خشونت» درواقع، گسترده‌تـر از عبـارت پیش‌نویس اصلی کنوانسیون است.(۹) پیش نویس اصلی تصریح کرده است مـاده (الـف) (۱) ۱ در صورتی کاربردپذیر است که مجرم مرتکب حمله مسلحانه به یک شـخص در

هواپیما بشود. به کارگیری واژه قانون خشونت، باعث محدود شدن کاربردپذیری این مقرره برای استفاده از سلاح‌های خاص یا محدود کردن جرم به اعمالی که جان قربانی را به خطر می‌اندازند، نمی‌شود (توماس[1] و کربی[2]، ۱۹۷۳، صص ۱۶۵ـ۱۶۳).

مسئله‌ای که به ذهن متبادر می‌شود این است که «آیا می توان عمل خشونت آمیز علیه شخصی را که سوار بر هواپیمای در حال پرواز است از طریق تروریسم سایبری صورت داد؟ پاسخ به این پرسش، به معنای واژه خشونت بستگی دارد. به طور معمول، خشونت با یک عنصر فیزیکی ارتباط دارد، اما این عنصر فیزیکی در چارچوب‌های متعددی به اثبات می‌رسد. طبق تعریف فرهنگ لغت حقوقی «بلاک»، عنصر فیزیکی به مهاجم مربوط می‌شود. بر اساس این دیدگاه، خشونت؛ یعنی اعمال زورِ غیر موجه.(۱۰) اگر قرار بود این تفسیر را بپذیریم، با توجه به اینکه تروریسم سایبری از زور فیزیکی استفاده نمی‌کند، از حیطه ماده (الف) (۱) ۱ حذف می‌شد.

طبق دومین تفسیرِ ممکن، می‌توان گفت عنصر فیزیکی به مرتکب جرم اطلاق نمی‌شود، بلکه به قربانی نسبت داده می‌شود. بنابراین، خشونت زمانی اثبات می‌شود که صدمه بدنی به قربانی یک عمل خاص وارد شده باشد.(۱۱) این دیدگاه در ژرف‌اندیشی کنفرانس سازمان بین‌المللی هواپیمایی کشوری منعکس شده است. از آنجا که تروریسم سایبری می‌تواند منجر به صدمه بدنی اشخاص برای مثال، با سقوط هواپیما یا صدمه به سیستم فشار هوا بشود، به روشنی می‌تواند نوعی جرم در حیطه ماده (الف) (۱) ۱ تلقی شود. از این رو، کاربرد مورد (الف) برای یک حمله تروریستی شبکه‌ای به هواپیما امکان‌پذیر خواهد بود (کوهن، ۲۰۱۰، ص ۲۸).

ب) نابود کردن یا آسیب‌زدن به یک هواپیمای مورد استفاده به نحوی که توان پرواز را از آن بگیرد یا به طور احتمالی، ایمنی آن را برای در حال پرواز به خطر بیندازد: ماده (ب) (۱) ۱ عمل سابوتاژ علیه خود هواپیما را قابل جزا می‌داند. نابودی یا صدمه باید در حالی که هواپیما مورد استفاده قرار می‌گیرد، وارد شود؛ اما عمل خاصی که باعث نابودی هواپیما بشود، می‌تواند قبل از مورد استفاده قرار گرفتن هواپیما انجام گیرد (توماس و کربی، ۱۹۷۳، ص ۱۶۵). این، باعث طولانی‌تر شدن دوره کاربردپذیری کنوانسیون می‌شود.

---

1. Thomas 2. Kirby

مورد (ب) دو عنصر کلیدی را در بردارد: اول؛ عملی که مجرم انجام داده باید یک هواپیمای مورد استفاده را نابود کند یا باعث صدمه دیدن آن بشود. دوم؛ این عمل باید منجر به از کار افتادن هواپیما یا پرواز، اما به خطر افتادن ایمنی آن در پرواز بشود. درست همچون واژه «خشونت» در مورد (الف) احتمال دارد نابودی یا صدمه‌ای که مورد (ب) به آن اشاره کرده، برای پوشش دادن به صدمه یا نابودی فیزیکی در نظر گرفته شده باشد(کوهن، ۲۰۱۰، ص ۲۱).

ج) قرار دادن یا تسهیل قرار دادن ادوات یا ماده به هر وسیله‌ای که باشد، در هواپیمای مورد استفاده که به طور احتمالی آن هواپیما را نابود کند یا صدمه‌ای به آن وارد کند که توان پرواز را از آن بگیرد یا منجر به صدمه‌ای بشود که به طور محتمل ایمنی آن در پرواز را به خطر بیندازد: ماده (ج) (۱) ۱ در اصل، برای پرداختن به موقعیت‌هایی منظور شد که در آن مواد منفجره یا ادوات آتش‌زا وارد هواپیما می‌شوند (توماس و کربی، ۱۹۷۳، ص ١٦٦). عبارت «به هر وسیله‌ای که باشد»، ابتدا با هدف در برگیری اعمالی مانند استفاده از نامه یا بسته‌های غذایی هواپیمایی برای کار گذاشتن ادوات آتش‌زا در داخل هواپیما مطرح شد.[۱۲] پیشنهاد نماینده مصر برای جایگزینی عبارت اول، با واژه کلی «هر چیز» رد شد و پروتکل‌های کنفرانس مونترال نشان می‌دادند که «به هر وسیله‌ای که باشد» تمام احتمالات را در برمی‌گیرد.[۱۳] با در نظر گرفتن این برداشت کلی، می‌توانیم «به هر وسیله‌ای که باشد» را به مثابه تروریسم سایبری تعبیر کنیم.

د) نابودی یا صدمه زدن به تأسیسات هوانوردی یا تداخل در عملکرد آن، در صورتی که چنین عملی ایمنی هواپیما را در پرواز به خطر بیندازد: ماده (د) (۱) ۱ موقعیت‌هایی را شامل می‌شود که عمل تداخل در عملکرد ارتباطات هوانوردی به طور عمد انجام شود (توماس و کربی، ۱۹۷۳، ص١٦٦). پیرو ماده ۲۸ کنوانسیون شیکاگو؛ تأسیسات هوانوردی؛ یعنی برج مراقبت فرودگاه خدمات رادیویی و هواشناسی کاربردی در پروازهای بین‌المللی.[١٤]

همانند مورد (ب) به نظر می‌رسد که تروریسم سایبری قادر به اجرای نابودی یا صدمه زدن به تأسیسات هوانوردی باشد. در ضمن، تداخل در عملکرد نیز از طریق تروریسم سایبری امکان پذیر است. به گفته «مایکل اورون»، مهندس هواپیما و نماینده

اسبق در بوئینگ[۱۵]، سیستم هوانوردی داخل هواپیما به گونه‌ای طراحی شده است که یک سیستم مداربسته و مستقل باشد. یعنی سنسورهای روی بدنه هواپیما که دما و ارتفاع را اندازه می‌گیرند هرگز در معرض اختلال خارجی قرار نگیرند.

هر چند این مسئله می‌تواند تسکینی برای نگرانی در مورد حمله تروریست‌های سایبری به سنسورها باشد، تأسیسات هوانوردی دیگری نیز وجود دارند که وابسته به ارتباطات بین رایانه‌های زمینی و رایانه‌های داخل هواپیما هستند. شایان ذکر است که مورد (د) آستانه‌ای را تنها برای احتمال به خطر افتادن ایمنی هواپیما در پرواز تعیین کرده است. با توجه به این مسئله، تصور تداخل رایانه‌ای با خط ارتباطی بین زمین و هواپیما امکان‌پذیر است. این کار به طریقی انجام می‌شود که با اختلال در عملکرد تأسیسات هوانوردی ایمنی پرواز را به خطر بیندازد یا در تأسیسات زمینی هدایت‌کننده هواپیما برای فرود یا بلند شدن ایجاد مشکل کند (کوهن، ۲۰۱۰، ص ۲۲).

هـ) اطلاع‌رسانی نادرست که به موجب آن ایمنی هواپیمای در حال پرواز، با خطر مواجه شود: ماده (هـ) (۱) ۱ شامل موقعیت‌هایی می‌شود که شخصی که خودش سوار هواپیما نیست، کنترل آن را در دست بگیرد. به گفته ناظر فدراسیون بین‌المللی انجمن خلبان‌های هواپیمایی در کنفرانس مونترال، چنین اعمالی برای منحرف کردن هواپیما به سمت فرودگاه واقع در منطقه‌ای انجام می‌شوند که نقشه آن در هواپیما وجود ندارد.[۱۶] این گونه اقدامات، ایمنی هواپیما را در هنگام پرواز به شدت به خطر می‌اندازند؛ از این رو، شرط الزامی آگاهی، باعث حذف مواردی می‌شود که اطلاع‌رسانی از روی حسن نیت صورت گرفته است.

به کارگیری عبارت «اطلاع‌رسانی» جرم مقرر شده در مورد (هـ) را برای تروریسم سایبری کاربردپذیر می‌سازد. زمانی که پیش‌نویس مورد (هـ) تهیه شد، سناریوی مرتبط با آن، انتقال صوتی بین زمین و هواپیما بود، اما در دنیای امروز و با پیشرفت فناوری این انتقال می‌تواند به طور مستقیم بین رایانه‌های زمینی و رایانه‌های داخل هواپیما صورت بگیرد. به گفته امیر کوهن کارشناس سیستم‌های ارتباطی، سیستم ارتباطی هواپیما، ارتباط صوتی را به ارتباط دادگانی تبدیل می‌کند و این کمک بزرگی به ایمنی پرواز است زیرا کنترل زمینی را قادر به نظارت دقیق‌تر بر فعالیت‌های هواپیما در زمان واقعی می‌سازد. با این حال، ارتباط بی‌سیم بین سیستم رایانه‌ای هواپیما و کنترل زمینی،

منجر به آسیب‌پذیری‌هایی می‌شود که آن را همانند هر سیستم ارتباط رایانه‌ای دیگر برای تروریسم سایبری آشکار می‌سازد. در سال ۱۹۸۸ پروتکل الحاقی به کنوانسیون مونترال پذیرفته شد.(۱۷)

۲. راهبرد کنوانسیون بین‌المللی منع بمب‌گذاری‌های تروریستی

ماده ۲ کنوانسیون بین‌المللی، بمب‌گذاری‌های تروریستی جرایم را در چارچوب اجرای کنوانسیون تعریف کرده است. این ماده، شامل سه دسته از جرایم می‌شود: جرایم ارتکابی از سوی مرتکب اصلی، مبادرت به ارتکاب جرم و هر نوع معاونت در جرم‌بندهای زیر به ارزیابی کاربردپذیری کنوانسیون بین‌المللی بمب‌گذاری‌های تروریستی در مورد تروریسم سایبری پرداخته‌اند.

جرایم مندرج در ماده (۱) ۲ کنوانسیون بین‌المللی منع بمب‌گذاری‌های تروریستی، عناصر متعددی را در برمی‌گیرند؛ چرا که تروریسم سایبری و تروریسم فیزیکی فقط از نظر عمل انجام شده با یکدیگر تفاوت دارند و از نظر حالت ذهنی تروریست مجری آن عمل، فرقی بین آنها نیست. دو گزینه مرتبط با نیت مجرم، تحلیل نخواهند شد. تروریست شبکه‌ای همان مقاصد یک ترویست عادی را دارد و از این رو، هیچ تفاوت حقوقی در اطلاق قصد به آن وجود ندارد. بحث زیر به بررسی کاربردپذیری قوانین توصیف شده در ماده مذکور برای سناریوی تروریسم سایبری می‌پردازد. جرم، ایجاب می‌کند که مرتکب جرم یکی از چهار فعل (همانند پرتاب، کار گذاشتن، شلیک، یا منفجر کردن مواد انفجاری یا ادوات مرگبار دیگر) را بر علیه یکی از چهار مکان همچون مکان عمومی، تأسیسات کشوری یا دولتی، سیستم حمل و نقل عمومی یا تأسیسات زیرساختی به انجام برساند. کاربرد بخش (۱) ۲ برای حملات تروریستی سایبری در وهله اول منوط به معنایی است که به عبارت «مواد منفجره یا ادوات مرگبار دیگر» داده می‌شود.

طبق تعریف مقرر شده در ماده (۳) ۱ مواد منفجره یا ادوات مرگبار دیگر، یکی از دو تفسیر احتمالی را بیان می‌کند؛ نخست، می‌تواند به این معنا باشد: ماده منفجره یا سلاح و ادوات آتش‌زا که برای تسبیب مرگ، جراحات بدنی جدی یا ضرر مالی اساسی طراحی شده یا قابلیت آن را داشته باشد. یک زیر ساخت رایانه‌ای شده احتمالاً واجد شرایط این تفسیر نیست. می‌توان از رایانه برای چکاندن بمب استفاده کرد، اما رایانه به

خودی خود نمی‌تواند مانند یک بمب عمل کند. تنها راه ایجاد انفجار مرتبط با زیرساخت رایانه‌ای، نصب یک بمب خارجی روی رایانه یا استفاده از رایانه به عنوان دکمه قرمز چکاندن منفجرکننده است (کوهن، ۲۰۱۰، صص ۲۵ـ ۲٤).

دومین تفسیر ممکن برای تعریف یاد شده، یک افزودنی متعاقب به بحث و مذاکره کار گروه بود که انواع گوناگون موادی را مشخص می‌کند که رها کردنشان می‌تواند جان مردم را به خطر بیندازد.[۱۸] طبق ماده (ب) (۳) ۱ ماده منفجره یا سایر ادوات مرگبار، می‌تواند سلاح یا ادواتی باشد که برای تسبیب مرگ، جراحات بدنی جدی یا ضرر مالی اساسی از طریق رهاسازی، انتشار، یا تصادم مواد شیمیایی سنتی، عوامل زیستی یا سموم یا مواد مشابه یا تشعشع و ماده رادیو اکتیو طراحی شده یا قابلیت آن را داشته باشد. این تعریف، برخلاف تفسیر اول، به طور کامل برازنده شرح حال تروریسم سایبری است. در پایان اینکه کنوانسیون بمب گذاری تفسیری نسبت به انعطاف‌پذیر از جرایم مندرج در ماده ۲ ارائه می‌کند. هر عنصر جرم می‌تواند مظهر معانی بسیار گسترده‌ای باشد که پوششی را برای کنوانسیون ایجاد می‌کند. به واسطه این واقعیت، یک مجرم در چارچوب کنوانسیون بین‌المللی سرکوب بمب‌گذاری‌های تروریستی می‌تواند یک تروریست سایبری هم باشد؛ به این ترتیب که سیستم‌های رایانه‌ای را به گونه‌ای مختل کند که باعث رها شدن مواد خطرناک در اماکن عمومی یا بر ضد آن بشود (نمامیان، ۱۳۹۱، صص ۱٤۹ـ ۱٤۸).

۳. پیش‌نویس کنوانسیون جامع مقابله با تروریسم بین‌المللی

در سال ۱۹۹٦ هند پیش‌نویس کنوانسیون جامع مقابله با تروریسم بین‌المللی را به منظور بررسی توسط کشورهای عضو، برای دبیر کل سازمان ملل متحد ارسال کرد.[۱۹] پیش‌نویس کنوانسیون پیشنهادی هند، چندین بار بازنگری و اصلاح شد تا اینکه کمیته موردی در سال ۲۰۰۲ آخرین پیش‌نویس را منتشر کرد.[۲۰] پیش‌نویس کنوانسیون از جهات متعدد به کنوانسیون‌های قبلی شباهت دارد.[۲۱] اصلاحاتی که پیش‌نویس کنوانسیون ارائه کرده است با پوشش‌دهی تمام اعمال تروریستی و تا حد، بیشتری با پوشش‌دهی تعهد نسبت به پیشگیری و همکاری ارتباط دارد.

ادبیات حقوقی، نقش پیش‌نویس کنوانسیون را در تقبیح تروریسم از سوی جامعه

بین‌الملل مشخص کرده است.(۲۲) البته پیش‌نویس کنوانسیون کشورهای حامی تروریسم را در جانب تدافعی قرار می‌دهد (لیپمن[1]، ۲۰۰۳، ص ۳۵۸). علاوه بر این، پیش‌نویس کنوانسیون مکمل و راهنمای کار کمیته ضد تروریسم است که توسط شورای امنیت تشکیل شده است.(۲۳)

پیش‌نویس کنوانسیون تنها تعریف محدودی از تروریسم را در بردارد (هافنر[2]، ۲۰۰۳، ص ۱۵٦). هرگاه قرار باشد پیش‌نویس کنوانسیون مبنای جامعی را برای مبارزه با تروریسم بین‌المللی فراهم سازد، باید برای تمام اعمال، روش‌ها، و شیوه‌های تروریسم در هر جا و از سوی هر کس، کاربردپذیر باشد (هالبرستام[3]، ۲۰۰۳، ص ٥٨٤). مشکل این تعریف در دو موضوع اساسی بیان می‌شود؛ اجرای اعمال تروریستی در خلال درگیری مسلحانه و پناه دادن به تروریست‌های تحت حمایت کشورها و تبانی کردن برای جرایم تروریستی (گرانت[4]، ۲۰۰۵، ص ٤۲۸). با وجود این نقطه ضعف‌ها، پیش‌نویس کنوانسیون همچنان گام مهمی به سمت یکپارچه ساختن همکاری بین‌المللی علیه تروریسم به شمار می‌رود، کاربردپذیری پیش‌نویس کنوانسیون برای تروریسم سایبری، با توجه به جرم تعریف شده در پیش‌نویس بررسی می‌شود؛ اما، شایان ذکر است که پیشگفتار پیش‌نویس کنوانسیون چارچوب اجرای کنوانسیون را برای بررسی طبقه کلی «اعمال، روش‌ها و شیوه‌های تروریسم»(۲٤) مشخص کرده است و از این رو، آستانه به نسبت پایینی را مقرر کرده که بر اساس آن می‌توان تروریسم سایبری را در چارچوب اجرای پیش‌نویس کنوانسیون قرار داد.

طبق پیش‌نویس کنوانسیون، هر کشور عضو می‌پذیرد جرایم مندرج در ماده ۲ را به موجب حقوق داخلی خود، جرم کیفری قلمداد کند.(۲۵) پیش‌نویس کنوانسیون به مسائل صلاحیت قضایی، همکاری بین کشورها، محاکمه و اجرای معیارها و مانند آن نیز پرداخته است. ماده (ب) (۱) ۲ تصریح می‌کند: هر شخص در حیطه معنایی این کنوانسیون، در صورتی مرتکب جرم شده که به هر طریق و وسیله، به طور غیرقانونی و عمدی، باعث صدمات جدی به اموال دولتی یا شخصی، ازجمله اماکن عمومی، تأسیسات کشوری یا دولتی، سیستم حمل و نقل عمومی و تأسیسات زیرساختی یا

1. Lippman 2. Hafner 3. Halberstam
4. Grant

محیط زیست شود تا از طریق مرعوب ساختن مردم، یک دولت یا سازمان بین‌المللی را به انجام یا خودداری از انجام هر عملی وادار کند.

اشاره ماده (ب) (۱) ۲ به «هر طریق و وسیله» در کنار تعریف «تأسیسات زیرساختی» ازجمله ارتباطات، مخابرات و شبکه‌های اطلاعاتی، کاربرد جرم مندرج در پیش‌نویس کنوانسیون را برای حملات تروریستی سایبری امکان‌پذیر می‌سازد. زبانِ آن به قدری گسترده و واضح است که می‌تواند به طور مستقیم به تروریسم سایبری رسیدگی کند؛ مزیت اصلی آن نیز این است که نیازی به تکیه کردن بر روش‌های تفسیری ندارد تا مورد مخالفت نمایندگان یک مکتب فکری یا حقوقی متفاوت قرار بگیرد (کوهن، ۲۰۱۰، صص ۲۸ـ۲۶).

٤. کنوانسیون جرم سایبری شورای اروپا

در سال ۲۰۰۱ شورای اروپا «کنوانسیون جرم سایبری» را تصویب کرد.(۲۶) کنوانسیون جرم سایبری، دستاورد چهار سال تلاش کارشناسان شورای اروپا، ایالات متحده، کانادا، ژاپن و کشورهای دیگر است که در انتظار امضای تمامی کشورهاست. هدف اصلی کنوانسیون جرم سایبری، پیگیری یک سیاست کیفری هماهنگ و مشترک با هدف حفاظت از جامعه در برابر جرم سایبری، بویژه با به کارگیری قانونگذاری مناسب و تقویت همکاری بین‌المللی است.

هر چند اصطلاح «جرم سایبری» به مضمون جرمی است که در اینترنت یا از طریق اینترنت واقع می‌شود، حیطه عمل کنوانسیون جرم سایبری فراتر از این حد و شامل جرایمی است که با استفاده از رایانه واقع می‌شوند یا جرایمی که در کل، رایانه‌ها را دخالت می‌دهند (مارلر[1]، ۲۰۰۲، ص ٤۳).

برای اثبات مسئولیت کیفری، تمام جرایم مذکور در کنوانسیون جرم سایبری باید به طور عمد صورت گرفته باشند. بنابراین، پرسش مقدماتی که مطرح می‌شود این است که آیا قصد ارتکاب جرم یک تبهکار سایبری با قصد ارتکاب جرم یک تروریست سایبری فرق دارد؟ همان گونه که گفته شد، قصد صرف برای به اجرا درآوردن یک حمله، از آن حمله‌ای تروریستی نمی‌سازد. در خصوص تروریست، برخلاف تبهکار،

1. Marler

لازم است که قصد، اجرای حمله به منظور اعمال نفوذ بر سیاستگذاران باشد. بنابراین، معلوم نیست که واژه «به طور عمد» در کنوانسیون جرم سایبری این نوع قصد را تحت پوشش قرار دهد.

با این حال، اگر فرض کنیم که قصد خاص تروریست‌ها با در نظر گرفتن واژه «قصد» در کنوانسیون جرم سایبری به اثبات می‌رسد، بیشتر جرایم مندرج در کنوانسیون برای تروریسم سایبری کاربردپذیر خواهند بود. حملات تروریستی سایبری از طریق دسترسی غیرقانونی به سیستم‌های رایانه‌ای بدون حق[۲۷]، یا از طریق رهگیری انتقال داده‌های الکترونیکی غیرعلنی قابل اجرا هستند.[۲۸] همچنین، می توان تصور کرد که صدمه زدن به یکپارچگی و کارکرد مناسب رایانه یا استفاده از برنامه‌ها و داده‌های ذخیره شده رایانه‌ای از جمله موارد یک حمله تروریستی سایبری خواهند بود.[۲۹] به همین ترتیب، بقیه جرایم مقرر شده در کنوانسیون جرم سایبری نیز می‌توانند در طول یک حمله تروریستی سایبری؛ برای مثال، متوقف کردن سیستم رایانه‌ای[۳۰]، استفاده نادرست از دستگاه‌ها[۳۱] و جعل رایانه‌ای و کلاهبرداری صورت بگیرند.[۳۲] «جرایم خاص مرتبط با هرزه‌نگاری برای کودکان[۳۳]» و «حقوق مالکیت فکری[۳٤]» ارتباط کمتری با فعالیت‌های تروریسم سایبری دارند (کوهن، ۲۰۱۰، صص ۳۵ـ ۳٤).

در نهایت، کنوانسیون جرم سایبری شورای اروپا، تنها بعضی از جرایمی را در برگرفته که از طریق تروریسم سایبری قابل اجرا هستند. با وجود این، قصد ارتکاب جرم تنها همان قصد است و این قصد، منحصر به فردی که مؤلفه مرتبط با تروریسم در نظر گرفته می‌شود و عواقب و صدمات فوری را مدنظر قرار می‌دهد، نیست. علاوه بر این، از میان کشورهایی که کنوانسیون را برای امضا به آنها ارائه کرده‌اند، تنها بیست‌وشش کشور بر آن صحه گذاشتند. این واقعیت، نشان‌دهنده آن است که اراده و تمایل سیاسی دولت‌ها نقشی حیاتی در تعیین اثربخشی اسناد حقوقی ایفا می‌کند؛ به این ترتیب، حتی، اگر کنوانسیون جرم سایبری شامل «قصد ارتکاب جرم» مرتبط با تروریسم بود، باز هم طرفداری کشورها عاملی کلیدی در بررسی ارزش آن به شما می‌رود (نمامیان، ۱۳۹۱، صص ۱۵۳ـ ۱۵۲).

۵. پیش‌نویس کنوانسیون استانفورد در مورد جرم سایبری و تروریسم

در اگوست ۲۰۰۰ کارشناسان «دانشگاه استانفورد» طرحی پیشنهادی را برای کنوانسیون

بین‌المللی جرم و تروریسم سایبری ارائه کردند (پیش‌نویس استانفورد) (سوفایر[1] و گودمن[2]، ۲۰۰۰، ص ۲۵۷). این پیش‌نویس که مبتنی بر کنوانسیون جرم سایبری شورای اروپاست، جرم‌انگاری رفتارهای متعدد از قبیل استفاده از سیستم‌های سایبری برای اجرای جرایم تعیین شده در سایر معاهدات خاص(۳۵) و هدف‌گیری زیرساخت‌های بحرانی را پیشنهاد داده است.(۳۶) از طرفی، پیش‌نویس یاد شده تأسیس یک آژانس بین‌المللی را نیز برای حفاظت از زیر ساخت اطلاعاتی پیشنهاد داده که جایگاهی برای کنکاش در خصوص وضع استانداردها و شیوه‌های مرتبط با امنیت سایبری است.(۳۷)

پیش‌نویس استانفورد، بر خلاف کنوانسیون جرم سایبری شورای اروپا، به طور اختصاصی به تطابق بین زیرساخت مبتنی بر ارتباطات رایانه‌ای و تروریسم می‌پردازد. این پیش‌نویس با جنبه‌هایی از اعمال شبکه‌ای بی‌ارتباط است که می‌توانند جرم سایبری باشند، اما تروریسم سایبری محسوب نمی‌شوند. پیش‌نویس استانفورد برخلاف پیش‌نویس کنوانسیون جامع، به وضوح تصریح کرده است که برای فعالیت‌های مربوط به درگیری مسلحانه جاری کاربردی ندارد.(۳۸)

با وجود این، از زمانِ پیش‌نویس، دو پیشرفت مهم صورت گرفته که می‌توانند کنوانسیون تروریسم سایبری را منسوخ کنند:

اول؛ این کنوانسیون چارچوبی را به وجود آورده که به مسائل متعددی که در پیش‌نویس استانفورد نیز مطرح شده‌اند، می‌پردازد. این علامت سؤال پیش روی موافقان پیش‌نویس استانفورد قرار می‌گیرد که «آیا لازم است با مسائل عدیده به طور یکسان در هر دو سند برخورد شود یا اینکه کنوانسیون جرم سایبری کفایت می‌کند؟»

دوم؛ پیش‌نویس کنوانسیون جامع هنوز در دست اجراست و همان گونه که پیش از این ملاحظه شد، تعریف جرایم در آن می‌تواند تروریسم سایبری را نیز در بر بگیرد.

از طرف دیگر، در این زمینه یک کنوانسیون مستقل می‌تواند سند مناسب و تمام عیاری برای پرداختن به تروریسم سایبری باشد. یک کنوانسیون مجزا می‌تواند بندهای خاصی را ارائه کند که برای بررسی ویژگی‌های خاص تروریسم سایبری منظور شده‌اند. چنین کنوانسیونی، می‌تواند سازوکارهای نامبرده و رویه‌های همکاری دوجانبه مرتبط با تروریسم سایبری را مقرر کند اما امکان دارد به واسطه ماهیت عمومی‌تری که دارد، از

1. Sofaer 2. Goodman

کنوانسیون جامع حذف شود؛ مانع اصلی در خصوص چنین راهکاری، فقدان فعلی پیش‌نویس به روز شده برای ارائه به کمیته ششم، یا هر جایگاه کنکاش دیگری است که مختص به این مسئله باشد (نمامیان، ۱۳۹۱، صص ۱۵۵ـ ۱۵٤).

٦. اساسنامه دیوان کیفری بین‌المللی

دیوان بین‌المللی کیفری که اساسنامه آن در کنفرانس دیپلماتیک رُم به تأیید نمایندگان ۱۲۰ دولت رسیده و از سال ۲۰۰۲ نیز لازم الاجرا شده است، اولین محکمه دایمی است که به منظور رسیدگی به مهم‌ترین جنایات بین‌المللی تأسیس یافته است (شباس[1]، ۲۰۰٤ و کاسسه[2]، ۲۰۰۸)[(۳۹)] لازم است یادآوری شود که تروریسم به واسطه دلایل متعددی که در نهایت منجر به فقدان تعریفی حقوقی از آن شد، از اساسنامه دیوان حذف شده است؛ به علاوه، بعضی اعمال تروریستی به قدر کافی خطیر پنداشته نمی‌شدند که محاکمه از طریق دیوان کیفری بین‌المللی را الزامی کنند[(٤٠)] و از این رو، نگرانی قابل توجهی در مورد سیاسی شدن دیوان در اثر گنجاندن جرایم تروریستی در اساسنامه وجود داشت (ماچ[3]، ۲۰۰٦، ص ۱۲٦).

به این ترتیب، به نظر می‌رسد که دلیل پرداخته نشدن به موضوع تروریسم در اساسنامه رُم این بوده است که توافقنامه‌های قراردادی موجود چنین توصیه کرده بودند. برای مثال، موضوع نسل‌کشی که در سال ۱۹٤۸ مورد بررسی قرار گرفت[(٤۱)]، بار دیگر، در اساسنامه رم تکرار شد و در اساسنامه دیوان کیفری بین‌المللی صلاحیت قضایی در مورد نسل‌کشی را به جای سپردن آن به کاربرد صلاحیت قضایی جامع کشورها، به دیوان کیفری بین‌المللی بخشید (کوشا و نمامیان، ۱۳۸۹ و نمامیان، ۱۳۹۰).

البته، شایان ذکر است که متأسفانه دلایل متعددی؛ همچون نبود توافق نظر پیرامون چارچوب پیشنهادی در خصوص تعریف تروریسم و نبود اجماع دولت‌های عضو در خصوص تبیین اقدامات تروریستی و ارتباط بسیار نزدیک آن با اقدامات نهضت‌های آزادی‌بخش، موجب شده است که مانند گذشته، بدون سیاستی واحد و متقن در تعیین تکلیف چارچوب تروریسم، وضعیت و جایگاه آن در اساسنامه در هاله‌ای از ابهام باشد.

با این اوصاف، درج جرم تروریسم در اساسنامه رُم، مزیت‌های مهمی در پی خواهد

1. Schabas 2. Cassese 3. Much

داشت؛ برای مثال، می‌تواند در کشاندن تروریست‌ها به دادگاه و محضر عدالت به کشورها کمک کند و در عین حال، بر ضعف داخلی که مانع از محاکمه تروریست‌ها در دادگاه‌های محلی می‌شود، فایق آید؛ همچنین یک پیام سیاسی تأکید را در مورد خطیر بودن تروریسم بین‌المللی از نظر جامعه بین‌المللی ارسال کند.

نتیجه اینکه در چارچوب نظام حقوق بین‌الملل کیفری، تا زمانی که تعریف مشخصی از تروریسم به عنوان یک جرم بین‌المللی در اساسنامه رُم وجود نداشته باشد، پرداختن به این موضوع بی‌ثمر است. همچنین در حال حاضر، تشخیص اینکه در این زمینه تغییری ایجاد خواهد شد یا اینکه تروریسم همچنان خارج از اساسنامه رُم باقی خواهد ماند، بر عهده کنفرانس بازنگری است (نامیان، ۱۳۹۱، صص ۱۵۸ـ ۱۵۵).

۷. قطعنامه ۱۳۷۳ شورای امنیت

اقتدار شورای امنیت پذیرش تصمیماتی که از نظر قانونی الزام آورند، (البته این اقتدار به واسطه تأکید مصرح در ماده ۲۵ منشور ملل متحد به شورای امنیت اعطا شده است)[۴۲] ابزار اجرایی پر قدرت، مؤثر و شناخته شده‌ای است که کاربردی جهانی در مورد کلیه دولت‌های عضو سازمان ملل متحد دارد (شا[1]، ۲۰۰۶، ص ۷۱۶). در کشورهایی که حقوق بین‌الملل به طور مستقیم جذب نظام حقوقی داخلی شده است (یعنی نظام تک‌قطبی، به جای نظام چندقطبی رواج دارد) جایگاهی در قانونگذاری الزام‌آور داخلی به قطعنامه‌های شورای امنیت اختصاص می‌یابد. یک مصداق روشن آن، قطعنامه ۱۳۷۳[۴۳] است که گویای اقتدار شورای امنیت برای اخذ الزامات گوناگون از کنوانسیون‌های بین‌المللی ضد تروریسم و به کارگیری آنها برای کلیه دولت‌های عضو سازمان ملل متحد است؛ بدون در نظر گرفتن اینکه آن کنوانسیون‌ها را به امضا رسانده باشند یا خیر (نامیان و عباسی، ۱۳۹۱، صص ۱۸۹ـ ۱۸۸).

هنگام بررسی توسل به شورای امنیت به عنوان راهی برای مبارزه با تروریسم سایبری باید مسئله مشروعیت را مدنظر قرار داد. از طرف دیگر، این گروه انحصاری شامل پانزده عضو است که به سایر نهادهای سازمان ملل‌متحد پاسخگو نیستند

1. Shah

(جانستون[1]، ۲۰۰۸، صص ۳۰۸ـ ۲۷۵). هر یک از پنج عضو دایمی از قدرت وتو کردن هر قطعنامه‌ای که با آن مخالف دارد، برخوردار است و نیازی به توجیه مخالفت خود ندارد. همین امر، موجب ارتقای معیار سیاسی شورا می‌شود (گرونبرگ[2]، ۲۰۰۹، صص ۵۱۱ ـ٤٦٩). از طرف دیگر، شورا می‌تواند بلافاصله به تهدیدهای جهانی اضطراری، بویژه در مواردی که حقوق بین‌الملل پاسخگو نیست، واکنش نشان دهد (روساند[3]، ۲۰۰۵، ص ۷۱۷).

نتیجه‌گیری

جامعه بین‌الملل، فرصت نادر و منحصر به فردی برای اتخاذ رویکردی پیشگیرانه و تدوین چارچوبی حقوقی دارد تا اطمینان دهد که جامعه بین‌الملل از آمادگی لازم برای یک حمله تروریستی سایبری دارد. بسیاری از سران کشورهای غربی و همچنین تعداد بی‌شماری از دانشمندان، تروریسم سایبری را گام بعدی تکامل تروریسم نامیده‌اند. تنها کار منطقی این است که با چنین تهدیدی مانند دیگر تظاهرات تروریسم برخورد کنیم؛ یعنی از طریق یک ممنوعیت شدید و روشن بر اساس حقوق بین‌الملل.

تروریسم سایبری که با ویژگی‌های متمایزکننده‌ای مشخص می‌شود، این چالش را که آیا برنامه ضد تروریستی حاضر کفایت می‌کند یا باید اسناد جدیدی تنظیم شود، پیش روی حقوقدانان بین‌الملل قرار می‌دهد. مفاد کنوانسیون‌های ضد تروریسم مورد بررسی با مرور زمان پیشرفت کرده است. حقوق از واژه‌شناسی به نسبت محدود کنوانسیون مونترال کامل‌تر شده تا عباراتی مانند «هر گونه ادوات دیگر» یا «به هر وسیله» را در کنوانسیون بین‌المللی سرکوب بمب‌گذاری‌های تروریستی در بر بگیرد. مورد دوم؛ تفسیر انعطاف‌پذیرتر شروط حقوقی را که باید به منظور اثبات مسئولیت قانونی در برابر تروریست‌های سایبری برآورده شوند؛ ممکن می‌سازد. قابل تصور است که این تفاوت‌ها که ناشی از پیشرفت و توسعه سریع فناوری مدرن در سه دهه اخیر هستند، منجر به تفاهم در میان جامعه حقوقی بر سر این موضوع شده که تروریسم می‌تواند خود را از طریق این فناوری‌ها نشان دهد. بنابراین، پیش‌نویس کردن کنوانسیون‌ها حساسیت بیشتری نسبت به ضرورت سازگاری با پیشرفت‌های آینده پیدا کرده است.

---

1. Johnstone 2. Gruenberg 3. Rosand

همان گونه که شرح و تفصیل آن گذشت، کاربردپذیری این دو کنوانسیون برای تروریسم سایبری امکان‌پذیر است، اما تا زمانی که ممنوعیتی مشخص برای هر نوع به کارگیری زیر ساخت رایانه‌ای در خصوص اهداف تروریستی وجود نداشته باشد، تحلیل پیشنهادی یاد شده، تنها نشان‌دهنده یک مکتب فکری خواهد بود. راه‌های دیگری هم وجود دارد تا تفسیرها بتوانند تروریسم سایبری را از چارچوب اجرای کنوانسیون‌های یاد شده خارج کنند. با توجه به اینکه تفسیر ارائه شده از متن است، دلایلی برای وجود برخی چالش‌ها باقی می‌ماند. به همین دلیل، بررسی دقیق مسائل برای ممنوعیت صریح تروریسم سایبری مورد اهتمام است. با این حال، تا زمانی که یک ممنوعیتی قاطعانه برای تمام روش‌ها و اشکال تروریسم سایبری وجود نداشته باشد، آن طور که شایسته و بایسته است نمی‌توان برای مقابله با این مسئله آماده بود.

ممنوعیت مستقیم بر تروریسم سایبری می‌تواند اشکال متعددی به خود بگیرد. دست‌کم، پنج اقدام ممکن دیگر برای هدف‌گیری تروریسم سایبری وجود دارد. هر یک از این گزینه‌ها، مزایا و معایب خاص خود را دارند و همین، از نهایی شدن آنها به عنوان یک سند حقوقی ضد تروریسم سایبری جلوگیری می‌کند. هر چند برخی از ابزارها، می‌توانند راه به نسبت مؤثری فراهم کنند، حیطه اجرای آنها به نوعی محدود می‌باشد. سایر ابزارها پوشش‌دهی وسیع‌تری دارند، اما در عین حال مناسب تروریسم سایبری نیستند (مک‌سلند[1]، ۲۰۰۹).

ترکیبی از اسناد گوناگون، می‌تواند روش بهتری برای بررسی این مسئله مهم باشد. چنین برنامه‌ای شامل ممنوعیت واضح تروریسم سایبری از طریق پیش‌نویس کنوانسیون جامع یا از طریق کنوانسیون‌های منطقه‌ای در کنار قطعنامه شورای امنیت به موجب فصل هفتم منشور ملل متحد و همچنین جرم‌انگاری تروریسم سایبری در اساسنامه رُم و یا اصلاحیه کنوانسیون جرم سایبری شورای اروپاست.

این روند، موجبات بهبود سریع شکاف موجود در حقوق بین‌الملل را در خصوص با تروریسم سایبری ممکن می‌سازد. به علاوه، اجازه می‌دهد جامعه بین‌الملل به جای توسل به تفسیر معاهده‌ای، یک مبنای حقوقی مستقیم را برای مبارزه با تروریسم

1. McClelland

سایبری در اختیار داشته باشد. علاوه بر این، اتکا به اسناد گوناگون بـه مشـروعیت ایـن برنامه کمک می‌کند؛ چرا که منجر به متوازن کردن قطعنامه لازم‌الاجرای شـورای امنیـت با توانایی کشورها برای پیروی از مقرره‌های سایر کنوانسیون‌ها بر حسب نظـام حقـوقی داخلی آنها می‌شود.

در پایان به نظر می‌رسد که با توجه به رشد فزاینـده اسـتفاده از اینترنـت و حرکـت شتابان کشورها به سوی الکترونیکی کردن خدمات اجتماعی، اقتصادی و تـأثیر انقـلاب اطلاعاتی بر بهبود فناوری‌های نظامی، امنیت بین‌المللی در سال‌های آتـی بـا تهدیـدها و چالش‌های نوینی مواجه خواهد شد. بدیهی است که کاهش آسیب‌پـذیری‌هـا و تقویـت امنیت و صلح در مقابل تهدیـدات نوظهـور و بـازیگران جدیـد و رهـایی از تروریسـم سایبری، مستلزم پرداختن به مطالعات آینده‌پژوهی در زمینه تأثیر انقـلاب اطلاعـاتی بـر امنیت ملی، تهدیدهای فضای سایبر و ارتقای قابلیت‌های فنی و آگاهی عمـومی از ایـن تهدیدها و همچنین در بهره‌گیری در خصوص دانش و اطلاعات مرتبط است.

امید است ابتکار ائتلاف جهانی علیه تروریسم، با پوشـش دادن بـه ابعـاد تروریسـم سایبری و دیگر برایندهای فناوری و علوم جدیـد در ایـن حـوزه، بـه ایجـاد عرصـه‌ای جدید از تعامل و همفکری نخبگان برای دستیابی به صلح عادلانه همت گمـارد؛ صـلح عادلانه‌ای که تنها در پرتو تعامل و همفکری نخبگان و سازمان‌های مردم نهاد و با تفکـر جهانی به آینده و سرنوشت بشریت به عنوان اعضای خانواده‌ای واحـد، قابـل تحلیـل و دستیابی خواهد بود.

پی‌نوشت

1. U.N.G.A/Resolution/50/53, Measures to Eliminate International Terrorism, 11 Dec, 1995.

۲. شایان ذکر است واژه«سایبر» در فارسی به «مجاز و مجازی» ترجمه شده است؛ اما این ترجمه گویای دقیق ایـن واژه نیست زیرا فضای سایبر حقیقی و واقعی نه دروغین و مجازی و تنهـا بـه شـکل مـادی و ملمـوس احساس شدنی نیست و این نکته کافی نیست که بـه آن مجـاز و مجـازی اطـلاق شـود. واژه سـایبر در اصطلاح به همه محیط‌هایی گفته می‌شود که فعالیت آن‌ها بر مبنای پردازش است و طبق سـامانه صـفر و یک کار می‌کنند(رک: زندی، ۱۳۸۹۰،صص ٤٠- ۳۸).

3. Cyber crime convention, http://convention,coe.int/treaty/en/ treaties/html/.

4. ICAO, International Conference on Air Law: Minutes and Documents, ICAO Doc. 9801, p. 21, Delegates of France and Japan (hereinafter: "ICAO Documents").
5. Id., p.21, 27, Delegates of Canada and the People's Republic of the Congo.
6. Vienna Convention, supra note
7. ICAO Documents, Delegate of the United Kingdom, supra note 64, at 27.
8. See: Article 2 of the Montreal Convention
9. Id, at 284
10. BLACK'S LAW DICTIONARY 1570 (6th ed. 1990).
11. .ICAO Documents, supra note 64, at 139
12. ICAO Documents, supra note 64, at 38
13. Id, at 108
14. Chicago Convention, supra note 54
15. Interview with Michael Oron, aircraft engineer and former El-Al representative at Boeing.
16. Chicago Convention, supra note 64, at 42
17. Amir Cohen is the C.E.O. of SigNext Wireless Ltd
18. General Assembly, Report of the Working Group to the Sixth Committee on: Measures to Eliminate International Terrorism, U.N. Doc. A/C.6/52/L.3, at 36-37 (10 October 1997).
19. Letter dated 01/11/96 from the permanent representative of India to the United Nations addressed to the Secretary General, UN Doc. A/C.6/51/6 (Nov. 1, 1996).
20. Report of the Ad Hoc Committee, supra note 15
21. Asli U. Bali, International Law and the Challenge of Terrorism, 9 J. ISLAMIC L. &CULT.1, 19 (2004).
22. Report of the Ad Hoc Committee, Supra note 15, Annex I.A, 8
23. Report of the Ad Hoc Committee, Supra note 15, Annex I.A, 2
24. Draft Convention, Report of the Ad-Hoc Committee established by General Assembly resolution 51/210 of December 1996, General Assembley Official Records, fifty-seven session, Supplement no. 37 UN Doc.
25. Id., Article 4

26. Council of Europe Convention on Cybercrime, Nov. 8, 2001, E.T.S. 185. (hereinafter "Convention on Cybercrime").
27. Convention on Cybercrime, supra note 123, E.T.S. 185 at 2.
28. Id, at 3
29. Id, at 4
30. Id, at 5
31. Id, at 6
32. Id, at 7, 8
33. Id, at 9
34. Id, at 10
35. Article 3 refers to the following: Tokyo Convention, supra note 14; Hague Convention, supra note 14; Montreal Convention, supra note 14; Hostage Convention, supra note 14; Terrorist Bombings Convention, supra note 14
36. Convention on Cybercrime, supra note 123, E.T.S. 185 at Art. 3.
37. Id. at Art. 12
38. Id. at Art. 20
39. Rome Statute of the International Criminal Court, Jul. 17, 1998, 2187 U.N.T.S. 90. (hereinafter "Rome Statute"). For a thorough discussion on the International Criminal Court.
40. See: Article 1 of the Rome Statute
41. The Convention on the Prevention and Punishment of the Crime of Genocide, Dec. 9, 1948, 78 U.N.T.S. 277.
42. See: UN Charter Article 25
43. Resolution 1373, supra note 18, U.N. Doc. S/RES/1189

منابع

ابوالمعالی الحسینی، سید وحید و علیزاده طباطبایی، زهرا سادات. (۱۳۸۷). حقوق امنیت اطلاعات شبکه. **فصلنامه فقه و حقوق، ۵** (۱۹).

انعامی، سهراب و طابنده، سمیرا. (۱۳۹۰). **گونه‌شناسی تروریسم: بررسی موضوعی، در: تروریسم و مقابله با آن** (به اهتمام عباسعلی کدخدایی و نادر ساعد). تهران: انتشارات مجمع جهانی صلح.

بختیاری و همکاران. (۱۳۸۹). سایبر تروریسم در جامعه شبکه‌ای. **فصلنامه مطالعات بین‌المللی پلیس**، ۱ (٤).

پاکزاد، بتول. (۱۳۷۵). **جرایم کامپیوتری**. پایان‌نامه کارشناسی ارشد، تهران: دانشگاه شهید بهشتی.

جلالی‌فراهانی، امیرحسین. (۱۳۸۷). جنبه‌های حقوقی اقدامات کیفری بین‌المللی مجرمان قانون در قبال جرایم سایبر. **فصلنامه پیشگیری از جرم**، ۳ (۸).

جلالی‌فراهانی، امیرحسین. (۱۳۸۸). نهادسازی برای پیشگیری از جرایم رایانه‌ای (با نگاهی به قانون جرایم رایانه‌ای). **مجموعه مقالات نخستین همایش ملی پیشگیری از جرم با محوریت رویکرد چند نهادی به پیشگیری از وقوع جرم**، تهران: دفتر تحقیقات کاربردی پلیس پیشگیری از جرم ناجا.

حاجیانی، ابراهیم. (۱۳۸۸). کاربرد تحلیل شبکه‌ای در پیشگیری از جرایم سازمان‌یافته. **مجموعه مقالات نخستین همایش ملی پیشگیری از جرم با محوریت رویکرد جامعه‌شناختی**، تهران: دفتر تحقیقات کاربردی پلیس پیشگیری از جرم ناجا.

رضوی، محمد. (۱۳۸۸). پیشگیری انتظامی از جرایم سایبری. **مجموعه مقالات نخستین همایش ملی پیشگیری از جرم با محوریت پیشگیری از جرم**، تهران: دفتر تحقیقات کاربردی پلیس پیشگیری از جرم ناجا.

زراعت، عباس و دانشوری، اسدالله. (۱۳۸۹). تبیین ماهیت و جایگاه حقوقی ـ اجتماعی تروریسم سایبری. **فصلنامه حقوق**، ۷.

زندی، محمدرضا. (۱۳۹۰). **تحقیقات مقدماتی در جرایم سایبری**. تهران: جنگل.

سیمبر، رضا. (۱۳۸۰). تروریسم در روابط بین‌الملل: چالش‌ها و راهبردها. **فصلنامه راهبرد**، ۲۱.

شیرزاد، کامران. (۱۳۸۸). **جرایم رایانه‌ای**. تهران: بهینه فراگیر.

صادقی حقیقی، دیدخت. (۱۳۸۳). نهضت‌های رهایی بخش ملی و تروریسم بین‌الملل از دید حقوق بین‌الملل. **ماهنامه اطلاعات سیاسی اقتصادی**، ۱۸، صص ۲۰٦ـ ۲۰۱.

عباسی، مهدی. (۱۳۸۳). اینترنت؛ ابزار سیاست (تروریسم مجازی؛ تهدیدی برای آینده). **نشریه فرهنگی و فناوری**، ۱ (۳).

کارگری، نوروز. (۱۳۹۰). **مفهوم‌یابی و گونه‌شناسی تروریسم، در: تروریسم و مقابله با آن** (به اهتمام عباسعلی کدخدایی و نادر ساعد). تهران: انتشارات مجمع جهانی صلح اسلامی.

کرم‌زاده، سیامک. (۱۳۸۱). کنوانسیون‌های ضد تروریزم و مسئله صلاحیت دولت‌ها در تعقیب و مجازات متهمان به ارتکاب اعمال تروریستی. **نامه مفید**، ۸ (۳۳).

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

کوشا، جعفر و نامیان، پیمان. (۱۳۸۹). **جرم‌انگاری تروریسم و مسئله صلاحیت دیوان کیفری بین‌المللی، در: حق بر صلح عادلانه** (به اهتمام نادر ساعد). تهران: انتشارات مجمع جهانی صلح اسلامی.

گرایلی، محمدباقر. (۱۳۸۹). بررسی جعل و تخریب و اخلال رایانه‌ای. **فصلنامه آموزه‌های حقوقی**، ۱۷.

گلدوزیان، ایرج و نامیان، پیمان. (۱۳۸۹). راهبرد حقوق بین‌الملل کیفری در مواجهه با تروریسم. **فصلنامه حقوق**، ۷.

نجفی ابرندآبادی، علی‌حسین. (۱۳۸٦). **تقریرات جرم‌شناسی (جرم‌شناسی تروریسم)**. تهران: دانشکده حقوق (پردیس قم).

نامیان، پیمان و عباسی، صمد. (۱۳۹۱). تأملی در قطعنامه ۱۳۷۳ شورای امنیت: تغییر ماهیت در تعهدات و الزامات حقوقی مبارزه با تروریسم. **فصلنامه مطالعات بین‌المللی پلیس**، ٦.

نامیان، پیمان. (۱۳۸۸). بررسی دلایل جرم‌انگاری تروریسم در اسناد بین‌المللی. **فصلنامه حقوق و مصلحت**، ٤.

نامیان، پیمان. (۱۳۹۰). صلاحیت قضایی دیوان کیفری بین‌المللی در رسیدگی به تروریسم. **فصلنامه مطالعات راهبردی**، ۵۱.

نامیان، پیمان. (۱۳۹۱). **حقوق بین‌الملل کیفری: چالش‌ها، هنجارها و راهبردهای مبارزه با تروریسم**. تهران: مجد.

نورمحمدی، مرتضی. (۱۳۹۰)، **سایبر تروریسم؛ تروریسم در عصر اطلاعات، در: تروریسم و مقابله با آن** (به اهتمام عباسعلی کدخدایی و نادر ساعد). تهران: انتشارات مجمع جهانی صلح اسلامی.

Abramovsky, A. (1975). Multilateral Conventions for the Suppression of Unlawful Seizure and Interference with Aircraft, Part II: **The Montreal Convention, 14 (2) colum. J. Transnat'l l,** Vol. 14, No. 2.

Alexander, Y. (2001). **Super Terrorism: Biologicl and Nuclear**, New York, Transnational Publisher.

Cassese, A. (2008). **International criminal law,** Cambridge University Press.

Clarke, R. (1999-2000). Threats to U.S. National Security: Proposed Partnership Initiatives Towards Preventing Cyber Terrorist Attacks, **DEPAUL BUS.** L.J, No. 12.

Cohen, A. (2010). Cyberterrorism: Are we Legally Ready?, **The Journal of International Business & Law,** Vol. 4, No. 15.

Denning, D. (2000). **Cyberterrorism, Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services,** U.S. House of Representatives, May 23, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

Gordon, S. (2007). **Cyberterrorism?,** Symantec and the Symantec Logo are U.S. Registered Trademarks of Symantec Corporation: Symantec Security Response.

Grant, J. (2005). Beyond Montreal Convention, Case w. Res. **J**. **Int''l l,** No. 37.

Gruenberg, J. (2009). An Analysis of United Nations Security Council Resolution: Are All Countries Treated Equally?, **CASEW. RES. J. INT'L L,** No. 41.

Hafner, G. (2003). Certain Issues of the Work of the Sixth Committee at the Fifty-Sixth General Assembly, **AM. J. INT'L L,** No. 97.

Halberstam, M. (2003). The Evolution of the United Nations Position on Terrorism: from Exempting National Liberation Movements to Criminalizing Terrorism Wherever and by Whomever Committed, **Colum. J. Transnat'l l,** No. 41.

Johnstone, I. (2008). Legislation and Adjudication in the UN Security Council: Bringing Down the Deliberative Deficit**, AM. J. INT'L L,** No. 102.

Lippman, M. (2003). The New Terrorism and International Law, **Tulsa J. Comp. & INT'L L,** No. 10.

Marler, S. (2002). The Convention on Cyber-Crime: Should the United States Ratify? **NEW ENG. L. REV,** No. 37.

McClelland, H.R. (2009). **Cyber Security Strategy, Commonwealth of Australia,** at http://www.ag.gov.au/cca

Much, C. (2006). The International Criminal Court (ICC) and Terrorism as an International crime, **MICH. ST. J. INT'L L,** No. 14.

Owen, R.S. (2008). Infrastructure of Cyberwarfare, in: Jonczewski, Lech. J and Colardik, Adrew. M (eds), **Cyber Warfare and Cyberterrorism**, New York: Information Science Reference.

Prichard, J. & MacDonald, L. (2004). Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks, J. **Info. Tech. Edu,** No. 3.

Robert, J. & heyer. D. (2001). **Introduction to NBC Terrorism, Hazardous Materials Specialist,** Red Bank, New Gersey, (www,disasters.org) octobr 15.

Rosand, E. (2005). The Security Council as "Global Legislator": Ultra Vires or Ultra Innovative?, **FORDHAM INT'L L.J,** No. 28.

Schabas, W. (2004). **An Introduction to the International Criminal Court,** Cambridge University Press.

Shah, P. (2006). Assisting and Empowering Women Facing Natural Disasters: Drawing from Security Council Resolution 1325, **COLUM. J. GENDER & L,** Vol. 15, No. 3.

Sofaer, A. & Goodman, E. (2000). **A Proposal for an International Convention on Cyber Crime and Terrorism,** Hoover Institution, Stanford University.

Stark, R. (1999). Cyber Terrorism, Rethinking New TechnoIogy, **Department of DeFenseand-Startegic Studies.**

Thomas, C. & Kirby, M. (1973). The Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, **INT'L & COMP. L.Q,** Vol. 22, No.1.

Trachtman, J. (2004). **Global Cyberterrorism, Jurisdiction, and International Organization,** Jul. 20, Available, at: http://www.ssrn.com/abstract=566361

Weimann, G. (2006). **Terror On the Internet: the New Arena, the New Challenges, Commlaw Conspectus.**